# StorageGRID 11.5のドキュメント

StorageGRID 11.5

NetApp
November 07, 2024

This PDF was generated from https://docs.netapp.com/ja-jp/storagegrid-115/index.html on November 07, 2024. Always check docs.netapp.com for the latest.

# 目次


StorageGRID 11.5のドキュメント . . . 1
リリースノート . . . 2
はじめに . . . 3
- グリッド入門 . . . 3
- ネットワークのガイドライン . . . 73

ソフトウェアをインストールしてアップグレードする . . . 105
- Red Hat Enterprise Linux または CentOS をインストールします . . . 105
- Ubuntu または Debian をインストールします . . . 178
- VMware をインストールする . . . 252
- ソフトウェアをアップグレードする . . . 304

ハードウェアを設置して保守する . . . 347
- SG6000 ストレージアプライアンス . . . 347
- SG5700 ストレージアプライアンス . . . 528
- SG5600 ストレージアプライアンス . . . 659
- SG100およびSG1000サービスアプライアンス . . . 783

構成と管理 . . . 899
- StorageGRID の管理 . . . 899
- ILM を使用してオブジェクトを管理する . . . 1180
- システムの保護対策 . . . 1355
- StorageGRID for FabricPool を設定します . . . 1363

StorageGRID を使用します . . . 1384
- テナントアカウントを使用する . . . 1384
- S3 を使用する . . . 1492
- Swift を使用します . . . 1618

監視とトラブルシューティング . . . 1651
- StorageGRID システムを監視する . . . 1651
- StorageGRID システムのトラブルシューティングを行う . . . 1956
- 監査ログを確認します . . . 2020

メンテナンス . . . 2115
- グリッドを展開します . . . 2115
- リカバリを維持します . . . 2172

NetApp StorageGRIDのその他のバージョンのマニュアル . . . 2420

法的通知 . . . 2421
- 著作権 . . . 2421
- 商標 . . . 2421
- 特許 . . . 2421
- プライバシーポリシー . . . 2421
- オープンソース . . . 2421

# StorageGRID 11.5のドキュメント

# リリースノート

新機能、削除および廃止された機能、解決済みの問題、および既知の問題に関するリリース固有の情報を取得します。

このドキュメントサイトにはリリースノートがあります。NetApp Support Siteのクレデンシャルでログインするように求められます。

- "HTML"
- "PDF"

# はじめに

## グリッド入門

NetApp StorageGRID システムの基本をご紹介します。

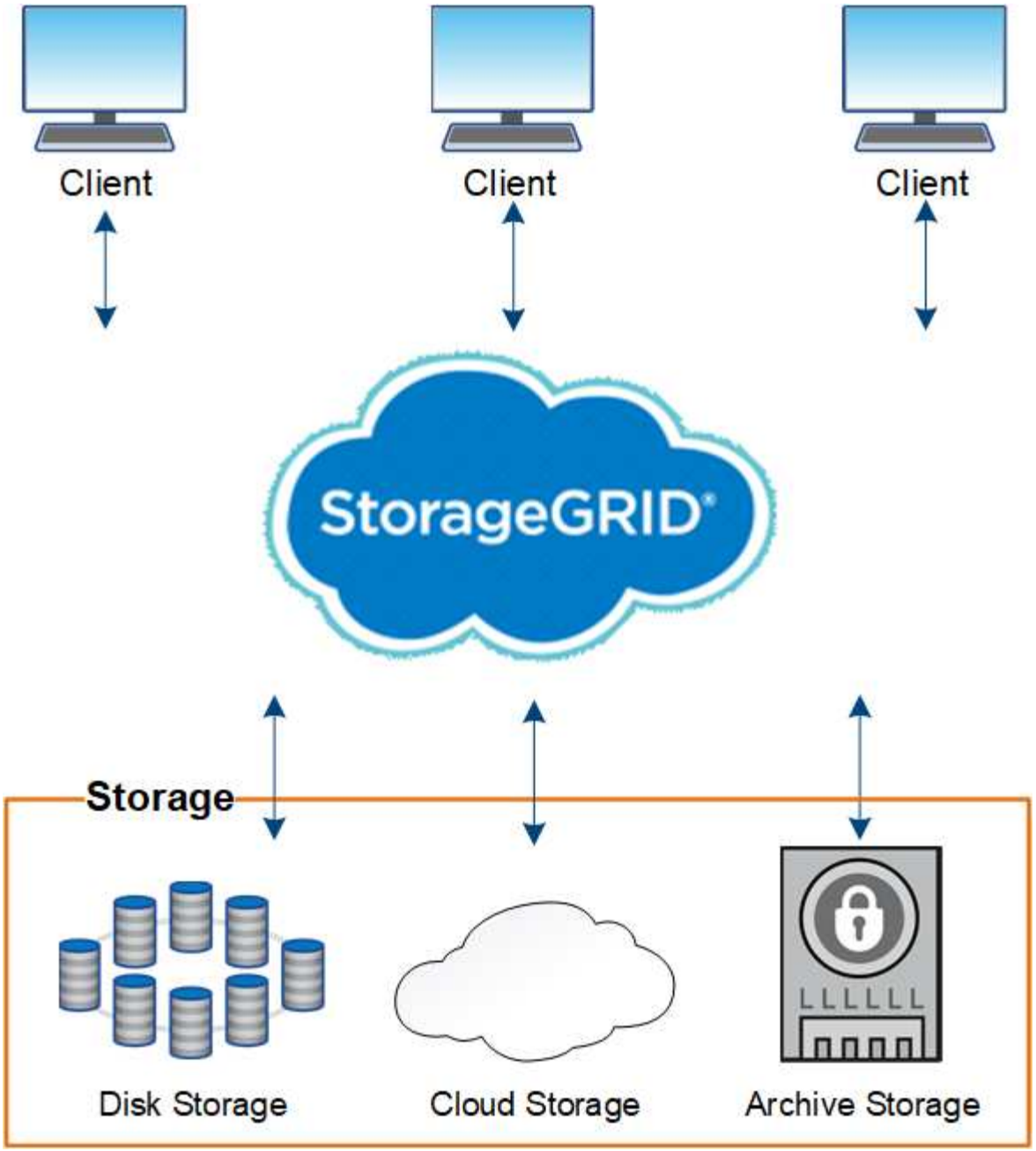
- "StorageGRID について"
- "StorageGRID のアーキテクチャとネットワークトポロジ"
- "StorageGRID によるデータの管理方法"
- "Grid Managerの概要"
- "Tenant Managerの概要"
- "StorageGRID を使用する"

### StorageGRID について

NetApp StorageGRID は、ソフトウェアで定義されるオブジェクトベースのストレージ解決策 で、 Amazon Simple Storage Service （ S3 ） API や OpenStack Swift API などの業界標準のオブジェクト API をサポートします。

StorageGRID は、大規模な非構造化データを長期間保管するためのセキュアなストレージを提供します。メタデータベースの統合ライフサイクル管理ポリシーによって、データのライフサイクルを通して最適な保存先が選択されます。コンテンツは適切な場所、適切なタイミングで、適切なストレージ階層に配置されるため、コストを削減できます。

StorageGRID は、地理的に分散した冗長で種類の異なる複数のノードで構成されており、既存および次世代のクライアントアプリケーションと統合できます。




StorageGRID システムには次の利点があります。

- 非構造化データ用に地理的に分散したデータリポジトリを拡張性にきわめて優れ、使いやすくなっています。
- 標準のオブジェクトストレージプロトコル。
  - Amazon Web Services Simple Storage Service （ S3 ）
  - OpenStack Swift
- ハイブリッドクラウドの実現：ポリシーベースの情報ライフサイクル管理（ ILM ）を使用して、 Amazon Web Services （ AWS ）や Microsoft Azure などのパブリッククラウドにオブジェクトを格納できます。StorageGRID プラットフォームサービスを使用すると、パブリッククラウドでコンテンツのレプリケーション、イベント通知、メタデータの検索を行うことができます。
- 柔軟なデータ保護で、データの保持性と可用性を確保レプリケーションと階層型イレイジャーコーディングを使用してデータを保護できます。保存データと転送中データの検証により、長期保持の整合性を確保

します。

- 動的なデータライフサイクル管理でストレージコストの管理を支援オブジェクトレベルでデータのライフサイクルを管理する ILM ルールを作成し、データの格納場所、保持性、パフォーマンス、コスト、保持期間を調整できます。テープを統合アーカイブ階層として使用できます。
- データストレージの高可用性と一部の管理機能。ロードバランシングの統合により、 StorageGRID リソース全体のデータ負荷を最適化します。
- 複数のストレージテナントアカウントをサポート。システムに格納されているオブジェクトをエンティティごとに分離できます。
- 包括的なアラートシステム、グラフィカルダッシュボード、すべてのノードとサイトの詳細なステータスなど、 StorageGRID システムの健全性を監視するための多数のツールが用意されています。
- ソフトウェアベースまたはハードウェアベースの導入をサポート。StorageGRID は次のいずれかに導入できます。
  - VMware で実行される仮想マシン。
  - Linuxホスト上のDockerコンテナ。
  - StorageGRID 社が開発したアプライアンス。ストレージアプライアンスはオブジェクトストレージを提供します。サービスアプライアンスは、グリッド管理サービスとロードバランシングサービスを提供します。
- 以下の規制に関連するストレージ要件に準拠しています。
  - 取引所会員や株式仲買業者を規制するための 17 CFR § 240.17a-4 （ f ）における証券取引委員会（ SEC ）
  - 金融業界規制機関（ FINRA ）ルール 4511 （ c ）。 SEC ルール 17a-4 （ f ）の形式とメディア要件は先延ばしになります。
  - 商品先物取引を規制するための 17 CFR § 1.31 （ c ） - （ d ）規制の商品先物取引委員会（ CFTC ）
- 無停止のアップグレード処理とメンテナンス処理。アップグレード、拡張、運用停止、メンテナンスの実行中も、コンテンツにアクセスできます。
- フェデレーテッドアイデンティティ管理。ユーザ認証を行うために、 Active Directory 、 OpenLDAP 、または Oracle のディレクトリサービスと統合します。Security Assertion Markup Language 2.0 （ SAML 2.0 ）規格を使用してシングルサインオン（ SSO ）をサポートし、 StorageGRID と Active Directory フェデレーションサービス（ AD FS ）間で認証および許可データをやり取りします。

関連情報

"StorageGRID を使用したハイブリッドクラウド"

"StorageGRID のアーキテクチャとネットワークトポロジ"

"StorageGRID アクセスの制御"

"テナントとクライアント接続の管理"

"情報ライフサイクル管理の使用"

"StorageGRID 処理の監視"

"ネットワークの設定"

"メンテナンス手順の実行"

## StorageGRID を使用したハイブリッドクラウド

ハイブリッドクラウド構成で StorageGRID を使用するには、ポリシーベースのデータ管理を実装してクラウドストレージプールにオブジェクトを格納し、 StorageGRID プラットフォームサービスを利用し、さらに NetApp FabricPool を使用して StorageGRID にデータを移動します。

### クラウドストレージプール

クラウドストレージプールを使用すると、 StorageGRID システムの外部にオブジェクトを格納できます。たとえば、 Amazon S3 Glacier 、 S3 Glacier Deep Archive 、 Microsoft Azure Blob Storage のアーカイブアクセス階層など、アクセス頻度の低いオブジェクトを低コストのクラウドストレージに移動できます。また、 StorageGRID オブジェクトのクラウドバックアップを保持しておくことで、ストレージボリュームやストレージノードの障害によって失われたデータをリカバリすることができます。

クラウドストレージプールターゲットからオブジェクトを読み出すレイテンシが増加しているため、 FabricPool でクラウドストレージプールを使用することはサポートされていません。

### S3 プラットフォームサービス

S3 プラットフォームサービスでは、リモートサービスをオブジェクトレプリケーション、イベント通知、または検索統合のエンドポイントとして使用できます。プラットフォームサービスはグリッドの ILM ルールとは独立して動作し、個々の S3 バケットで有効化されます。サポートされるサービスは次のとおりです。

- CloudMirror レプリケーションサービスでは、指定したオブジェクトが Amazon S3 または別の StorageGRID システムにあるターゲット S3 バケットに自動的にミラーリングされます。
- イベント通知サービスでは、指定した操作に関するメッセージが、 Simple Notification Service （ SNS ）イベントの受信をサポートする外部のエンドポイントに送信されます。
- 検索統合サービスでは、サードパーティのツールでメタデータの検索、可視化、分析を行うために、外部の Elasticsearch サービスにオブジェクトメタデータが送信されます。

たとえば、 CloudMirror レプリケーションを使用して特定の顧客レコードを Amazon S3 にミラーリングし、 AWS サービスを利用してデータを分析することができます。

### StorageGRID による ONTAP データの階層化

FabricPool を使用してデータを StorageGRID に階層化することで、 ONTAP ストレージのコストを削減できます。FabricPool はネットアップデータファブリックのテクノロジで、オンプレミスまたはオフプレミスの低コストのオブジェクトストレージ階層へデータを自動で階層化することができます。

手動の階層化ソリューションとは異なり、 FabricPool はデータの階層化を自動化してストレージコストを削減することで、総所有コストを削減します。StorageGRID を含むパブリッククラウドとプライベートクラウドに階層化することで、クラウドエコノミクスのメリットを実現します。

関連情報

"StorageGRID の管理"

"テナントアカウントを使用する"

"ILM を使用してオブジェクトを管理する"

"StorageGRID for FabricPool を設定します"

## StorageGRID のアーキテクチャとネットワークトポロジ

StorageGRID システムは、 1 つ以上のデータセンターサイトにある複数のタイプのグリッドノードで構成されます。

追加情報 のStorageGRID ネットワークトポロジ、要件、およびグリッド通信については、ネットワークガイドラインを参照してください。

関連情報

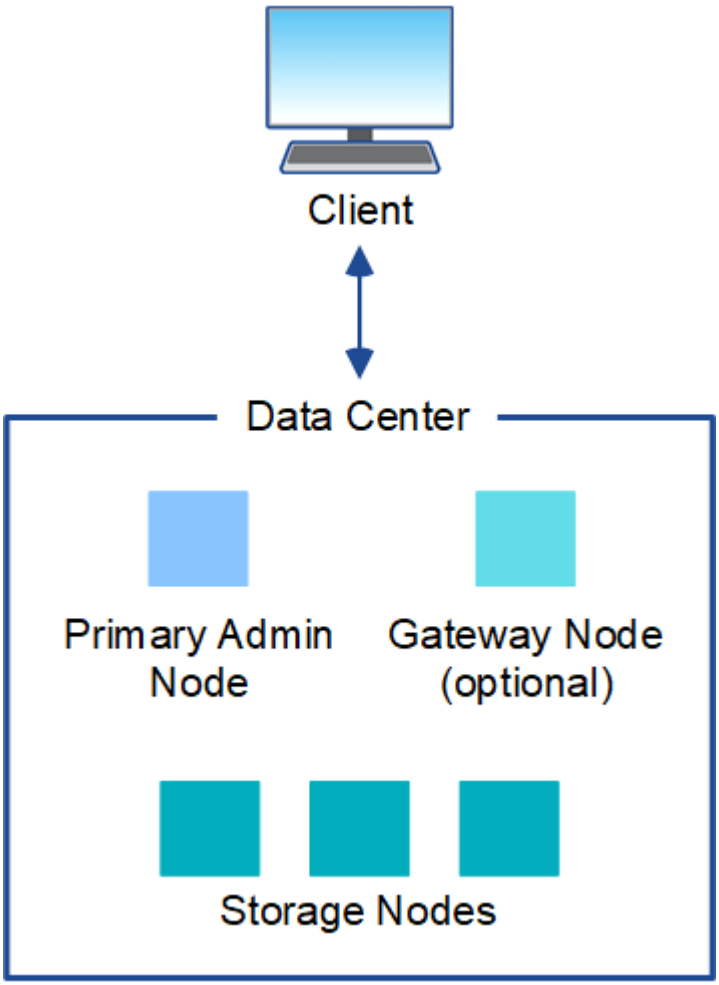
"ネットワークガイドライン"

### 導入トポロジ

StorageGRID システムは、単一のデータセンターサイトにも複数のデータセンターサイトにも導入できます。

#### 単一サイト

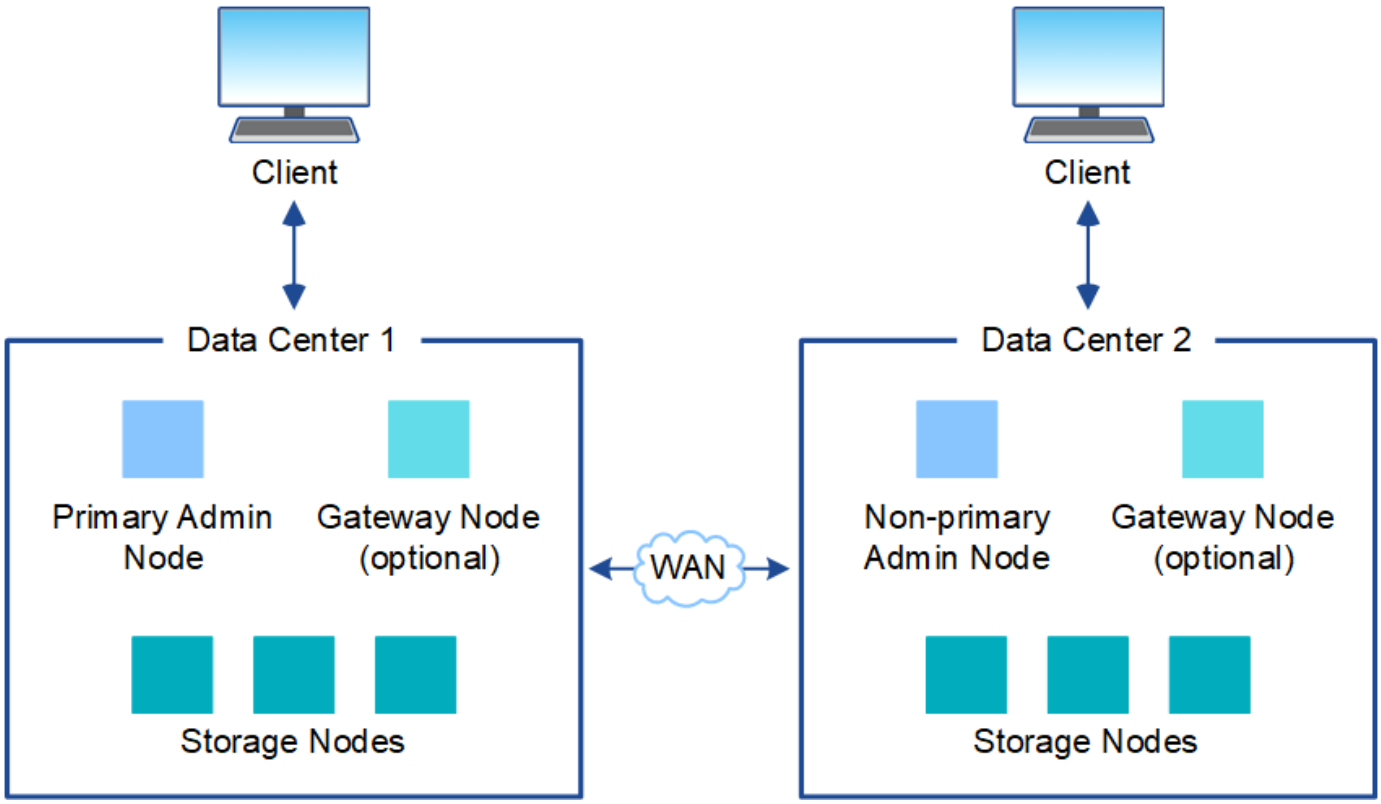
単一サイトに導入する場合は、 StorageGRID システムのインフラと運用が一元化されます。



### 複数のサイト

複数サイトに導入する場合は、サイトごとに異なるタイプと数の StorageGRID リソースをインストールできます。たとえば、あるデータセンターが別のデータセンターよりも多くのストレージを必要とする場合があります。

地震の断層線や洪水時の氾濫原など、さまざまなサイトが異なる障害領域の地理的に異なる場所に配置されることがよくあります。データ共有とディザスタリカバリは、他のサイトに自動的にデータを分散することで実現されます。



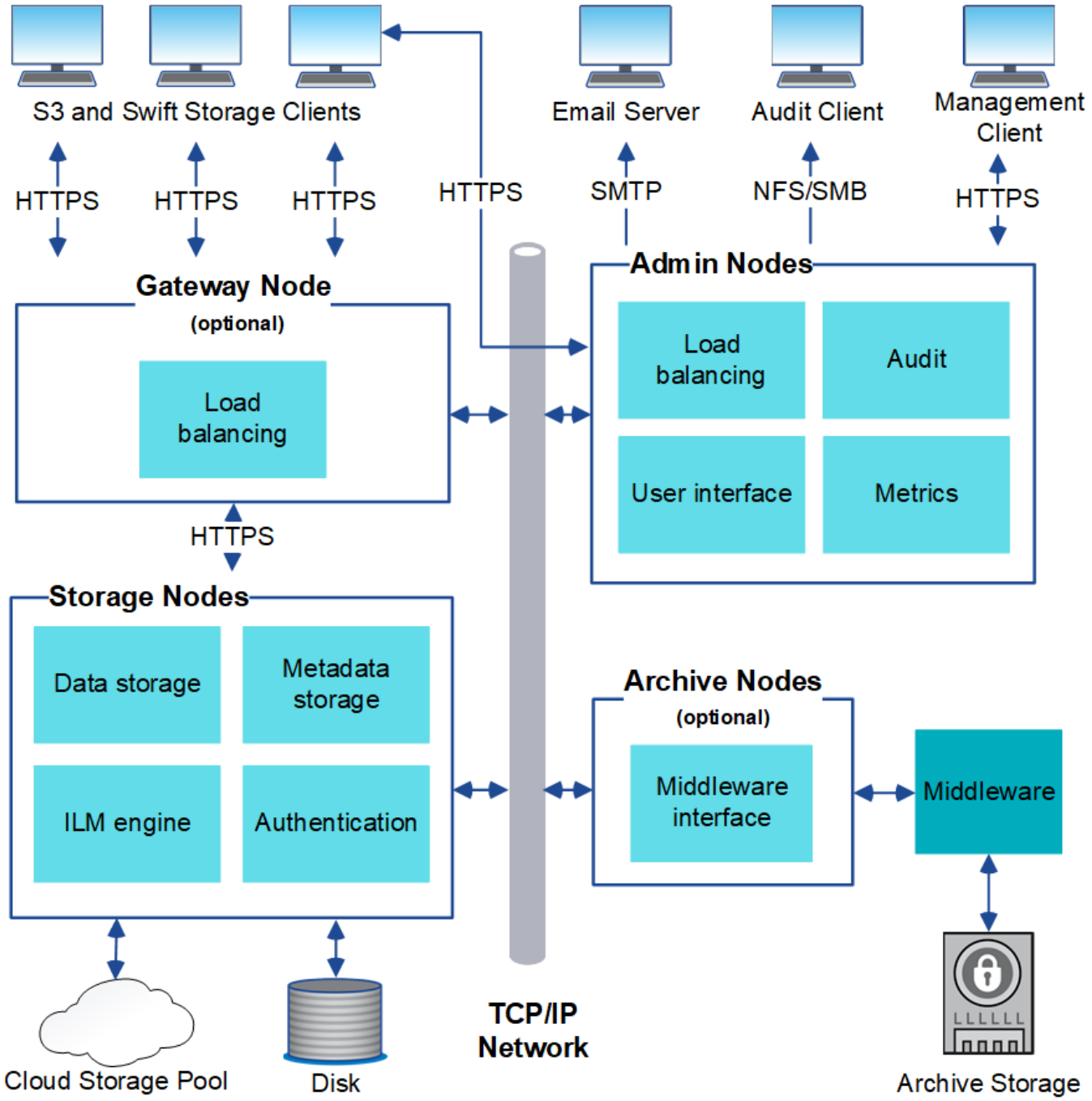

単一のデータセンター内に複数の論理サイトを配置して、分散レプリケーションとイレイジャーコーディングによって可用性と耐障害性を向上させることもできます。

### グリッドノードの冗長性

単一サイト環境またはマルチサイト環境では、冗長性を確保するために複数の管理ノードまたはゲートウェイノードを含めることができます。たとえば、 1 つのサイトまたは複数のサイトに複数の管理ノードをインストールできます。ただし、各 StorageGRID システムで使用できるプライマリ管理ノードは 1 つだけです。

## システムアーキテクチャ

次の図は、 StorageGRID システムにおけるグリッドノードの配置を示しています。




S3 および Swift クライアントは、 StorageGRID でオブジェクトの格納と読み出しを行います。他のクライアントは、 E メール通知の送信と StorageGRID 管理インターフェイスへのアクセスに使用されるほか、必要に応じて監査共有へのアクセスに使用されます。

S3 および Swift クライアントは、ゲートウェイノードまたは管理ノードに接続して、ストレージノードへのロードバランシングインターフェイスを使用できます。または、 S3 / Swift クライアントは HTTPS を使用してストレージノードに直接接続できます。

オブジェクトは、 StorageGRID 内で、ソフトウェアベースまたはハードウェアベースのストレージノード、テープなどの外部アーカイブメディア、または外部の S3 バケットや Azure BLOB ストレージコンテナで構成されるクラウドストレージプールに格納できます。

関連情報

"StorageGRID の管理"

グリッドノードおよびサービス

StorageGRID システムの基本的なビルディングブロックはグリッドノードです。ノードはサービスを備えています。サービスは、グリッドノードに一連の機能を提供するソフトウェアモジュールです。

StorageGRID システムは、次の 4 種類のグリッドノードを使用します。

- * 管理ノード * は、システムの設定、監視、ロギングなどの管理サービスを提供します。Grid Manager にサインインすると、管理ノードに接続されます。各グリッドにはプライマリ管理ノードが 1 つ必要であり、冗長性を確保するために非プライマリ管理ノードを追加で配置できます。どの管理ノードにも接続が可能で、各管理ノードに表示される StorageGRID システムのビューもほぼ同じです。ただし、メンテナンス手順はプライマリ管理ノードを使用して実行する必要があります。

  管理ノードを使用して、 S3 および Swift クライアントトラフィックの負荷を分散することもできます。

- * ストレージノード * ：オブジェクトデータとメタデータを管理、格納します。各 StorageGRID システムには、少なくとも 3 つのストレージノードが必要です。サイトが複数ある場合は、 StorageGRID システム内の各サイトにも 3 つのストレージノードが必要です。
- * ゲートウェイノード（オプション） * クライアントアプリケーションが StorageGRID への接続に使用できるロードバランシングインターフェイスを提供します。ロードバランサによってクライアントが最適なストレージノードにシームレスに転送されるため、ノードやサイト全体の障害が透過的に処理されます。ゲートウェイノードと管理ノードを組み合わせてロードバランシングを行うことも、サードパーティ製の HTTP ロードバランサを実装することもできます。
- * アーカイブノード（オプション） * オブジェクトデータをテープにアーカイブするためのインターフェイスを提供します。

ソフトウェアベースのノード

ソフトウェアベースのグリッドノードは、次の方法で導入できます。

- VMware vSphere Web Clientで仮想マシン（VM）として導入する
- Linuxホスト上のDockerコンテナ内に導入。次のオペレーティングシステムがサポートされています。
  - Red Hat Enterprise Linux の場合
  - CentOS の場合
  - Ubuntu
  - Debian

サポートされているバージョンの一覧については、 NetApp Interoperability Matrix Tool を参照してください。

**StorageGRID** アプライアンスノード

StorageGRID ハードウェアアプライアンスは、 StorageGRID システム専用に設計されています。一部のアプライアンスはストレージノードとして使用できます。その他のアプライアンスは、管理ノードまたはゲートウェイノードとして使用できます。アプライアンスノードをソフトウェアベースのノードと組み合わせることができます。あるいは、外部のハイパーバイザー、ストレージ、コンピューティングハードウェアに依存しない、専用のアプライアンスのみで構成されたグリッドを導入することもできます。

StorageGRID アプライアンスには、次の 4 種類があります。

- SG100 および SG1000 サービスアプライアンス * は、それぞれプライマリ管理ノード、非プライマリ管理ノード、またはゲートウェイノードとして機能する 1 ラックユニット（ 1U ）サーバです。両方のアプライアンスをゲートウェイノードと管理ノード（プライマリノードと非プライマリノード）として同時に動作させることができます。
- SG6000 ストレージアプライアンス * は、 1U SG6000-CN コンピューティングコントローラと 2U または 4U ストレージコントローラシェルフを組み合わせたストレージノードとして機能します。SG6000 には次の 2 つのモデルがあります。
  - * SGF6024 * ： SG6000-CN コンピューティングコントローラと、 24 本のソリッドステートドライブ（ SSD ）と冗長ストレージコントローラを搭載した 2U ストレージコントローラシェルフを組み合わせたものです。
  - * SG6060 * ： SG6000-CN コンピューティングコントローラを、 58 本の NL-SAS ドライブ、 2 本の SSD 、冗長ストレージコントローラを搭載した 4U エンクロージャと組み合わせます。各 SG6060 アプライアンスは、 1 台または 2 台の 60 ドライブ拡張シェルフをサポートし、オブジェクトストレージ専用のドライブを最大で 178 本提供します。
- SG5700 ストレージアプライアンス * は、ストレージとコンピューティングを統合したプラットフォームであり、ストレージノードとして機能します。SG5700 には次の 2 つのモデルがあります。
  - * SG5712 * ： NL-SAS ドライブ 12 本と統合ストレージ / コンピューティングコントローラを搭載した 2U エンクロージャ。
  - * SG5760 * ： 60 本の NL-SAS ドライブと統合されたストレージ / コンピューティングコントローラを搭載した 4U エンクロージャ。
- SG5600 ストレージアプライアンス * は、ストレージノードとして機能する、ストレージとコンピューティングを統合したプラットフォームです。SG5600 には、次の 2 つのモデルがあります。
  - * SG5612 * ： 12 本の NL-SAS ドライブと統合されたストレージ / コンピューティングコントローラを搭載した 2U エンクロージャ。
  - * SG5660 * ： 60 本の NL-SAS ドライブと統合されたストレージおよびコンピューティングコントローラを搭載した 4U エンクロージャ。

詳細な仕様については、NetApp Hardware Universe を参照してください。

管理ノードのプライマリサービス

次の表に、管理ノードのプライマリサービスを示します。ただし、この表にはすべてのノードサービスが表示されるわけではありません。

| サービス | キー機能 |
| --- | --- |
| Audit Management System （ AMS ） | システムアクティビティを追跡します。 |
| Configuration Management Node （ CMN ） | システム全体の設定を管理します。プライマリ管理ノードのみ |
| 管理アプリケーションプログラミングインターフェイス（ mgmt-api ） | グリッド管理 API とテナント管理 API からの要求を処理します。 |

| サービス | キー機能 |
| --- | --- |
| 高可用性 | 管理ノードとゲートウェイノードのグループのハイアベイラビリティ仮想 IP アドレスを管理します。<br><br>• 注： * このサービスはゲートウェイノードにも搭載されています。 |
| ロードバランサ | クライアントからストレージノードへの S3 および Swift トラフィックのロードバランシングを実現します。<br><br>• 注： * このサービスはゲートウェイノードにも搭載されています。 |
| ネットワーク管理システム（ NMS ） | Grid Manager の機能を提供します。 |
| Prometheus | 指標を収集して格納します。 |
| SSM （サーバステータスモニタ） | オペレーティングシステムと基盤のハードウェアを監視します。 |

ストレージノードのプライマリサービス

次の表は、ストレージノードのプライマリサービスを示しています。ただし、この表にはすべてのノードサービスが含まれているわけではありません。

ADC サービスや RSM サービスのように、通常は各サイトの 3 つのストレージノードにしか存在しないサービスもあります。

| サービス | キー機能 |
| --- | --- |
| アカウント（ acct ） | テナントアカウントを管理します。 |
| Administrative Domain Controller （ ADC ；管理ドメインコントローラ） | トポロジとグリッド全体の構成を管理します。 |
| Cassandra | オブジェクトメタデータを格納し、保護します。 |
| Cassandra Reaper | オブジェクトメタデータの自動修復を実行します。 |
| チャンク | イレイジャーコーディングされたデータフラグメントとパリティフラグメントを管理します。 |
| Data Mover （ DMV ） | クラウドストレージプールにデータを移動します。 |
| Distributed Data Store （ DDS ） | オブジェクトメタデータストレージを監視します。 |

| サービス | キー機能 |
| --- | --- |
| ID （ idnt ） | LDAP および Active Directory から取得したユーザ ID を統合する |
| Local Distribution Router （ LDR ）（ローカル分散ルータ（ LDR ） | オブジェクトストレージプロトコル要求を処理し、ディスク上のオブジェクトデータを管理します。 |
| Replicated State Machine （ RSM ） | S3 プラットフォームサービス要求がそれぞれのエンドポイントに送信されるようにします。 |
| SSM （サーバステータスモニタ） | オペレーティングシステムと基盤のハードウェアを監視します。 |

ゲートウェイノードのプライマリサービス

次の表に、ゲートウェイノードのプライマリサービスを示します。ただし、この表にはすべてのノードサービスが表示されるわけではありません。

| サービス | キー機能 |
| --- | --- |
| Connection Load Balancer （ CLB ；接続ロードバランサ） | クライアントからストレージノードへの S3 および Swift トラフィックのレイヤ 3 とレイヤ 4 のロードバランシングを実現します。従来のロードバランシングメカニズムです。<br>• 注： * CLB サービスは廃止されました。 |
| 高可用性 | 管理ノードとゲートウェイノードのグループのハイアベイラビリティ仮想 IP アドレスを管理します。<br>• 注： * このサービスは管理ノードにも搭載されています。 |
| ロードバランサ | クライアントからストレージノードへの S3 および Swift トラフィックのレイヤ 7 のロードバランシングを実現します。これは推奨されるロードバランシングメカニズムです。<br>• 注： * このサービスは管理ノードにも搭載されています。 |
| SSM （サーバステータスモニタ） | オペレーティングシステムと基盤のハードウェアを監視します。 |

アーカイブノードのプライマリサービス

次の表に、アーカイブノードのプライマリサービスを示します。ただし、このテーブルにはすべてのノードサービスが表示されるわけではありません。

| サービス | キー機能 |
| --- | --- |
| アーカイブ（ ARC ） | Tivoli Storage Manager （ TSM ）外部テープストレージシステムと通信します。 |

| サービス | キー機能 |
| --- | --- |
| SSM （サーバステータスモニタ） | オペレーティングシステムと基盤のハードウェアを監視します。 |

**StorageGRID** サービス

StorageGRID サービスの一覧を以下に示します。

- * アカウントサービスフォワーダ *

  ロードバランササービスがリモートホスト上のアカウントサービスを照会するためのインターフェイスを提供し、ロードバランサエンドポイントの設定変更をロードバランササービスに通知します。ロードバランササービスは管理ノードとゲートウェイノードにあります。

- * ADC サービス（ Administrative Domain Controller ） *

  トポロジ情報を管理し、認証サービスを提供するとともに、 LDR サービスおよび CMN サービスから送られるクエリに応答します。ADC サービスは、サイトにインストールされた最初の 3 つのストレージノードのそれぞれに存在します。

- * AMS サービス ( 監査管理システム )*

  監査対象のすべてのシステムイベントとトランザクションを監視し、テキストログファイルに記録します。AMS サービスは管理ノードにあります。

- * ARC サービス（アーカイブ） *

  S3 インターフェイス経由のクラウドや TSM ミドルウェア経由のテープなど、外部アーカイブストレージへの接続を設定するための管理インターフェイスを提供します。ARC サービスはアーカイブノードにあります。

- * Cassandra Reaper サービス *

  オブジェクトメタデータの自動修復を実行します。Cassandra Reaper サービスはすべてのストレージノードにあります。

- * チャンクサービス *

  イレイジャーコーディングされたデータフラグメントとパリティフラグメントを管理します。チャンクサービスはストレージノードにあります。

- * CLB サービス（ Connection Load Balancer ） *

  HTTP 経由で接続するクライアントアプリケーションに StorageGRID へのゲートウェイを提供する、廃止されたサービス。CLB サービスはゲートウェイノードにあります。CLB サービスは廃止されました。CLB サービスは今後の StorageGRID リリースで削除される予定です。

- * CMN サービス（ Configuration Management Node ） *

  システム全体の設定とグリッドタスクを管理します。各グリッドには 1 つの CMN サービスが用意されています。このサービスはプライマリ管理ノードにあります。

- * DDS サービス ( 分散データストア )*

  Cassandra データベースとのインターフェイスを提供してオブジェクトメタデータを管理します。DDS サービスはストレージノードにあります。

- * DMV サービス（ Data Mover ） *

  データをクラウドエンドポイントに移動します。DMV サービスはストレージノードにあります。

- * ダイナミック IP サービス *

  IP の動的な変更がないかグリッドを監視し、ローカル設定を更新します。動的 IP （ dynip ）サービスはすべてのノードにあります。

- * Grafana サービス *

  Grid Manager に表示される指標に使用されます。Grafana サービスは管理ノードにあります。

- * 高可用性サービス *

  High Availability Groups ページで構成されたノードのハイアベイラビリティ仮想 IP を管理します。ハイアベイラビリティサービスは管理ノードとゲートウェイノードにあります。このサービスはキープアライブサービスとも呼ばれます。

- * アイデンティティ (idnt) サービス *

  LDAP および Active Directory から取得したユーザ ID を統合するID サービス（ idnt ）は各サイトの 3 つのストレージノードにあります。

- * ロードバランササービス *

  クライアントからストレージノードへの S3 および Swift トラフィックのロードバランシングを実現します。ロードバランサエンドポイントの設定ページで設定できます。ロードバランササービスは管理ノードとゲートウェイノードにあります。このサービスは nginx-gw サービスとも呼ばれます。

- * LDR サービス（ Local Distribution Router ） *

  グリッド内のコンテンツの格納と転送を管理します。LDR サービスはストレージノードにあります。

- *MISCd Information Service Control Daemon サービス *

  他のノード上のサービスの照会と管理、およびノードの環境設定の管理（他のノードで実行されているサービスの状態の照会など）を行うためのインターフェイスを提供します。MISCd サービスはすべてのノードにあります。

- * nginx サービス *

  は、各種のグリッドサービス（ Prometheus や動的 IP など）が HTTPS API を介して他のノード上のサービスと通信できるようにするための、認証およびセキュアな通信のメカニズムとして機能します。nginx サービスはすべてのノードにあります。

- * nginx-gw サービス *

ロードバランササービスの電源を投入します。nginx-gw サービスは管理ノードとゲートウェイノードにあります。

- * NMS サービス（ネットワーク管理システム） *

  Grid Manager を介して表示される監視、レポート、および設定のオプションを強化します。NMS サービスは管理ノードにあります。

- * 持続性サービス *

  リブート後も維持する必要があるルートディスク上のファイルを管理します。永続化サービスはすべてのノードにあります。

- * Prometheus サービス *

  すべてのノードのサービスから時系列の指標を収集します。Prometheus サービスは管理ノードにあります。

- * RSM サービス（ Replicated State Machine Service ） *

  プラットフォームサービス要求がそれぞれのエンドポイントに送信されるようにします。RSM サービスは、 ADC サービスを使用するストレージノードにあります。

- * SSM サービス（ Server Status Monitor ） *

  ハードウェアの状態を監視して NMS サービスに報告します。SSM サービスのインスタンスは、すべてのグリッドノードにあります。

- * トレースコレクタサービス *

  トレース収集を実行し、テクニカルサポートが使用する情報を収集します。TRACE コレクタサービスはオープンソースの Jaeger ソフトウェアを使用し、管理ノードに存在します。

関連情報

"NetApp Interoperability Matrix Tool で確認できます"

"NetApp Hardware Universe の略"

"VMware をインストールする"

"Red Hat Enterprise Linux または CentOS をインストールします"

"Ubuntu または Debian をインストールします"

"SG100 SG1000サービスアプライアンス"

"SG6000 ストレージアプライアンス"

"SG5700 ストレージアプライアンス"

"SG5600 ストレージアプライアンス"

"StorageGRID の管理"

# StorageGRID によるデータの管理方法

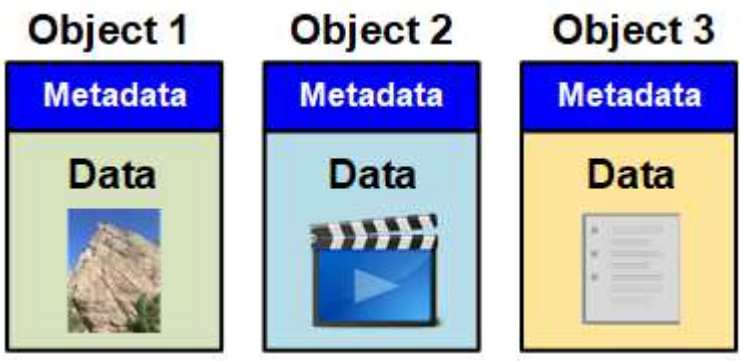
StorageGRID システムの使用を開始する前に、 StorageGRID システムによるデータの管理方法を理解しておくと役立ちます。

- "オブジェクトとは"
- "オブジェクトデータを保護する方法"
- "オブジェクトのライフサイクル"

## オブジェクトとは

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

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




### オブジェクトデータ

写真、映画、診療記録など、あらゆるものが含まれます。

### オブジェクトメタデータ

オブジェクトメタデータは、オブジェクトについて記述された任意の情報です。StorageGRID では、オブジェクトメタデータを使用してグリッド全体のすべてのオブジェクトの場所を追跡し、各オブジェクトのライフサイクルを継続的に管理します。

オブジェクトメタデータには、次のような情報が含まれます。

- システムメタデータ（各オブジェクトの一意の ID （ UUID ）、オブジェクト名、 S3 バケットまたは Swift コンテナの名前、テナントアカウントの名前または ID 、オブジェクトの論理サイズ、オブジェクトの作成日時など）、 オブジェクトが最後に変更された日時。
- 各オブジェクトコピーまたはイレイジャーコーディングフラグメントの現在の格納場所。
- オブジェクトに関連付けられているユーザメタデータ。

オブジェクトメタデータはカスタマイズと拡張が可能なため、アプリケーションに合わせて柔軟に設定できます。

StorageGRID がオブジェクトメタデータを格納する方法と場所の詳細については、を参照してください "オブジェクトメタデータストレージの管理"。

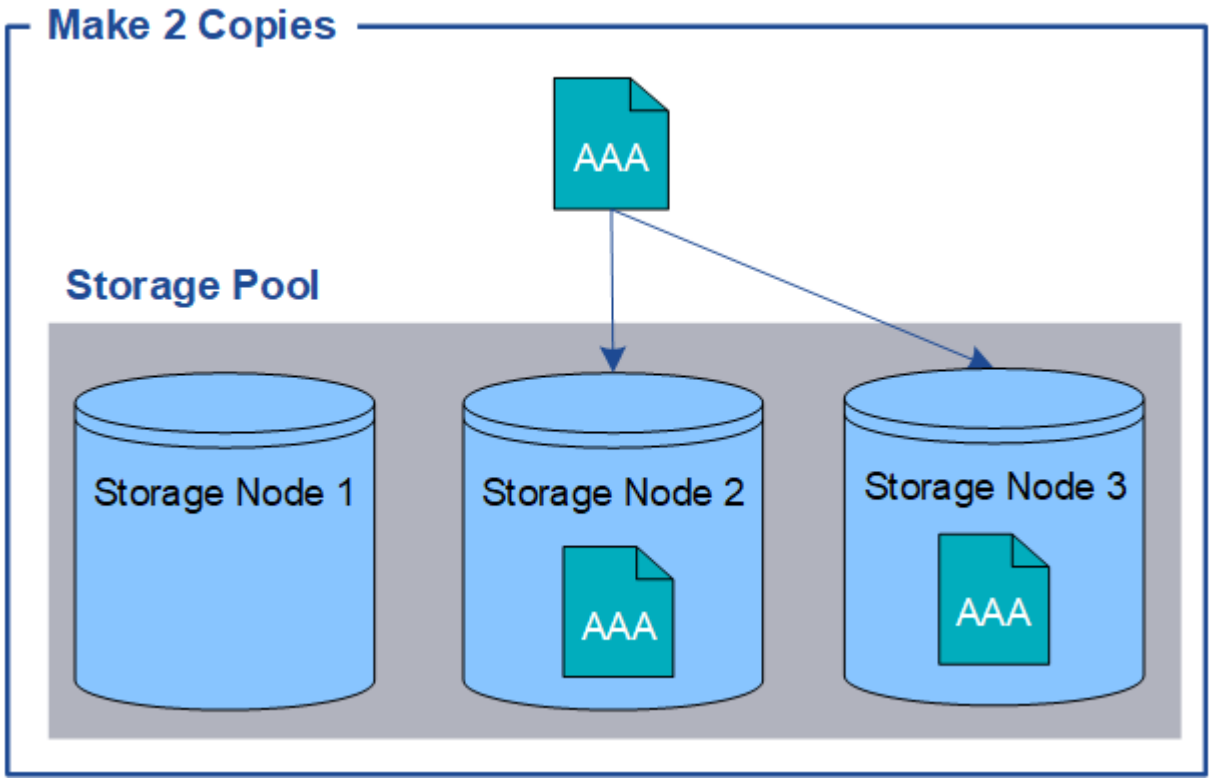
### オブジェクトデータを保護する方法

StorageGRID システムは、オブジェクトデータを損失から保護するための 2 つのメカニズム、レプリケーションとイレイジャーコーディングを提供します。

#### レプリケーション

レプリケートコピーを作成するように設定された情報ライフサイクル管理（ ILM ）ルールにオブジェクトが一致した場合、 StorageGRID システムはオブジェクトデータの完全なコピーを作成して、ストレージノード、アーカイブノード、またはクラウドストレージプールに格納します。ILM ルールは、作成するコピーの数と保存先、およびシステムでのコピーの保持期間を決定します。ストレージノードの損失などが原因でコピーが失われても、 StorageGRID システムの別の場所にコピーがあれば、オブジェクトを引き続き利用できます。

次の例では、 Make 2 Copies ルールによって、 3 つのストレージノードからなるストレージプールに各オブジェクトのレプリケートコピーを 2 つずつ配置するように指定しています。

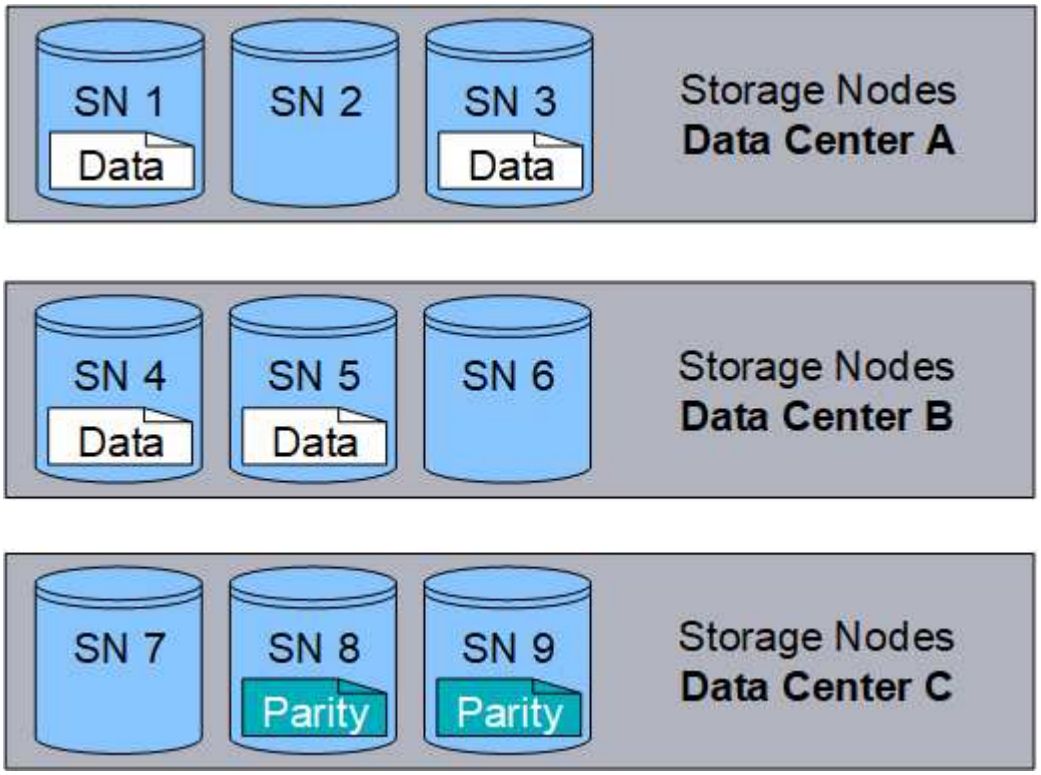



#### イレイジャーコーディング

StorageGRID がイレイジャーコーディングコピーを作成するために設定された ILM ルールとオブジェクトを照合する場合は、オブジェクトデータを複数のデータフラグメントに分割し、追加のパリティフラグメントを計算して、各フラグメントを別のストレージノードに格納します。アクセスされたオブジェクトは、格納されたフラグメントを使用して再アセンブルされます。データフラグメントまたはパリティフラグメントが破損したり失われたりしても、イレイジャーコーディングアルゴリズムが残りのデータフラグメントとパリティフラ

グメントを使用してそのフラグメントを再作成します。使用されるイレイジャーコーディングスキームは、ILM ルールとイレイジャーコーディングプロファイルによって決定します。

次の例は、オブジェクトのデータにイレイジャーコーディングを使用する方法を示しています。この例の ILM ルールでは 4+2 のイレイジャーコーディングスキームを使用します。各オブジェクトは 4 つのデータフラグメントに等分され、オブジェクトデータから 2 つのパリティフラグメントが計算されます。ノードやサイトの障害時にもデータが保護されるよう、 6 つの各フラグメントは 3 つのデータセンターの別々のストレージノードに格納されます。




関連情報

"ILM を使用してオブジェクトを管理する"

"情報ライフサイクル管理の使用"

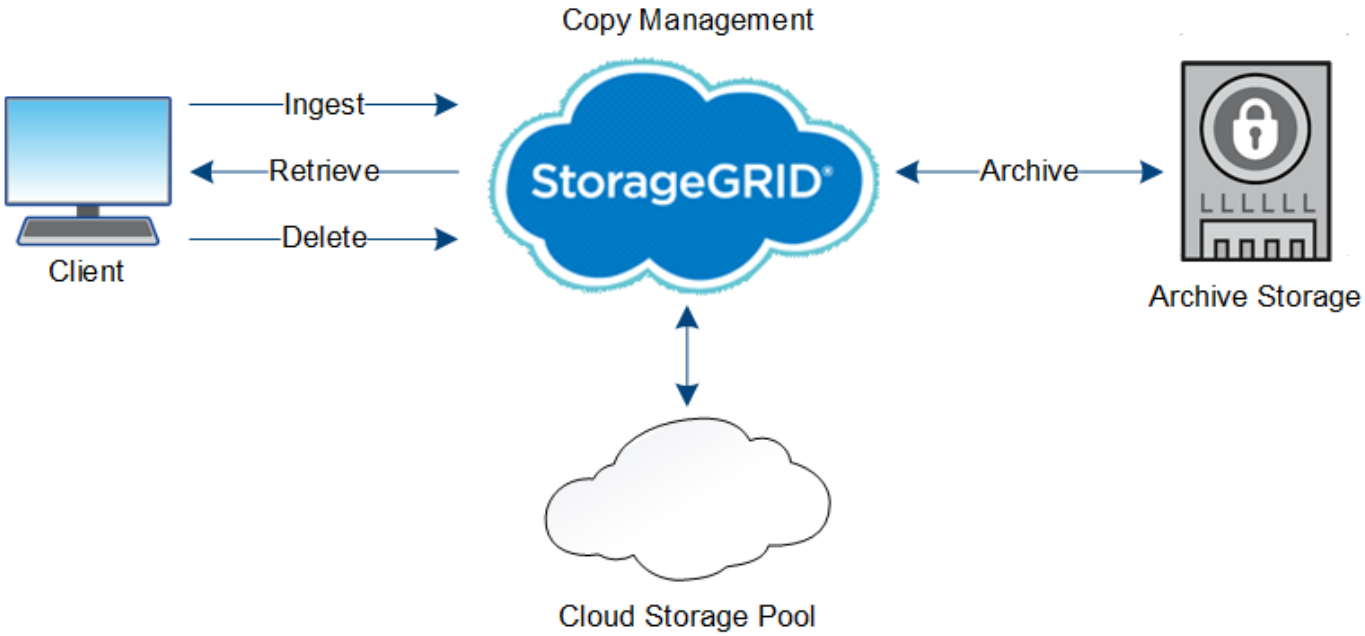
オブジェクトのライフサイクル

## オブジェクトのライフサイクルは、さまざまなステージで構成されます。各ステージは、オブジェクトで行われる処理を表しています。

オブジェクトのライフサイクルは、取り込み、コピー管理、読み出し、削除の各処理で構成されます。

- * 取り込み： S3 または Swift クライアントアプリケーションから、 HTTP 経由で StorageGRID システムにオブジェクトを保存するプロセスです。このステージでは、 StorageGRID システムがオブジェクトの管理を開始します。
- * コピー管理 * ：アクティブな ILM ポリシーの ILM ルールで説明されているように、 StorageGRID でレプリケートコピーとイレイジャーコーディングコピーを管理するプロセス。コピー管理ステージでは、StorageGRID が指定された数とタイプのオブジェクトコピーをストレージノード、クラウドストレージプール、またはアーカイブノードに作成して保持することで、オブジェクトデータを損失から保護します。

- * Retrieve * ： StorageGRID システムに格納されたオブジェクトにクライアントアプリケーションがアクセスするプロセス。クライアントがオブジェクトを読み取ると、オブジェクトがストレージノード、クラウドストレージプール、またはアーカイブノードから読み出されます。
- * 削除 * ：グリッドからすべてのオブジェクトコピーを削除するプロセス。オブジェクトは、クライアントアプリケーションが StorageGRID システムに削除要求を送信することで削除されるか、オブジェクトの有効期間が終了したときに StorageGRID が実行する自動プロセスによって削除されます。




関連情報

"ILM を使用してオブジェクトを管理する"

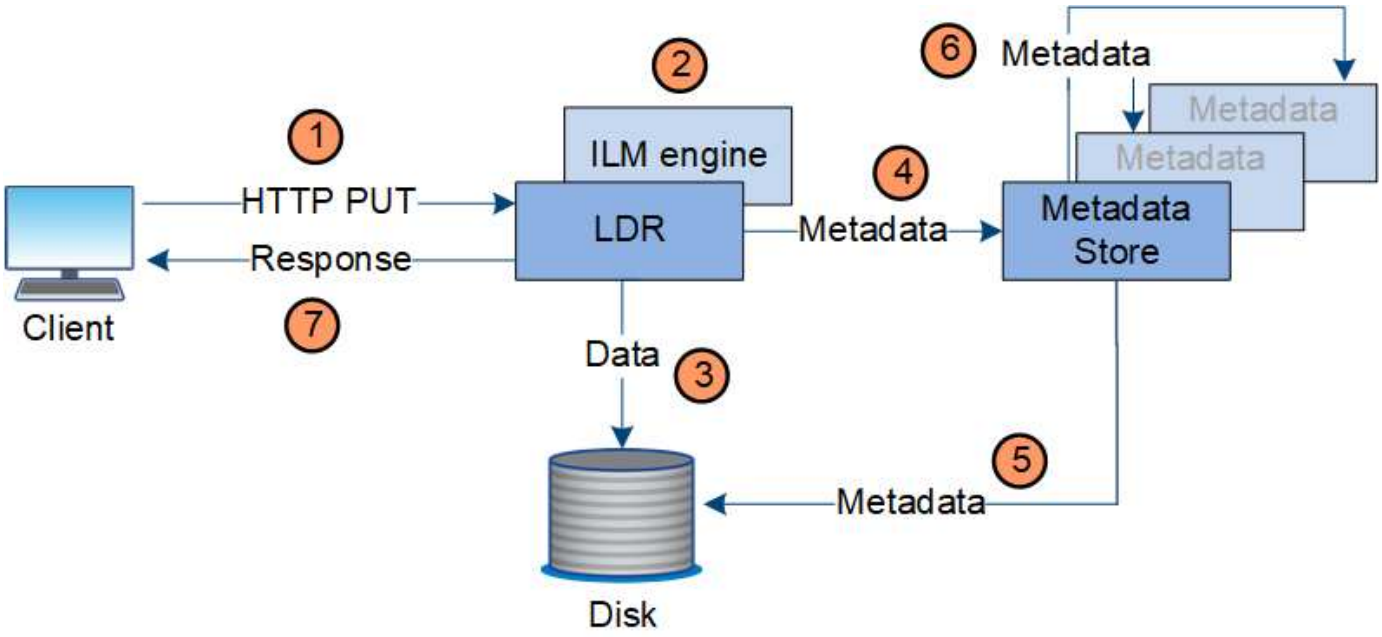
"情報ライフサイクル管理の使用"

取り込みのデータフロー

## 取り込み処理、つまり保存の処理は、クライアントと StorageGRID システム間の定義されたデータフローで構成されます。

データフロー

クライアントからStorageGRID システムにオブジェクトを保存すると、ストレージノード上のLDRサービスが要求を処理し、メタデータとデータをディスクに格納します。




1. クライアントアプリケーションでオブジェクトが作成され、 HTTP PUT 要求を使用して StorageGRID システムに送信されます。
2. オブジェクトがシステムの ILM ポリシーに照らして評価されます。
3. LDR サービスが、オブジェクトデータをレプリケートコピーまたはイレイジャーコーディングコピーとして保存します。（上の図ではレプリケートコピーをディスクに格納する処理を簡単に示しています）。
4. LDR サービスが、オブジェクトメタデータストアにメタデータを送信します。
5. メタデータストアが、オブジェクトメタデータをディスクに保存します。
6. メタデータストアが、他のストレージノードにオブジェクトメタデータのコピーを伝播します。これらのコピーはディスクにも保存されます。
7. LDR サービスからクライアントに、オブジェクトが取り込まれたことを確認する「 HTTP 200 OK 」の応答が返されます。

コピー管理

## オブジェクトデータは、アクティブな ILM ポリシーとその ILM ルールによって管理されます。ILM ルールは、レプリケートコピーまたはイレイジャーコーディングコピーを作成してオブジェクトデータを損失から保護します。

必要なオブジェクトコピーのタイプや場所は、オブジェクトのライフサイクルにおけるタイミングによって異なります。オブジェクトが必要に応じて配置されるように、 ILM ルールが定期的に評価されます。

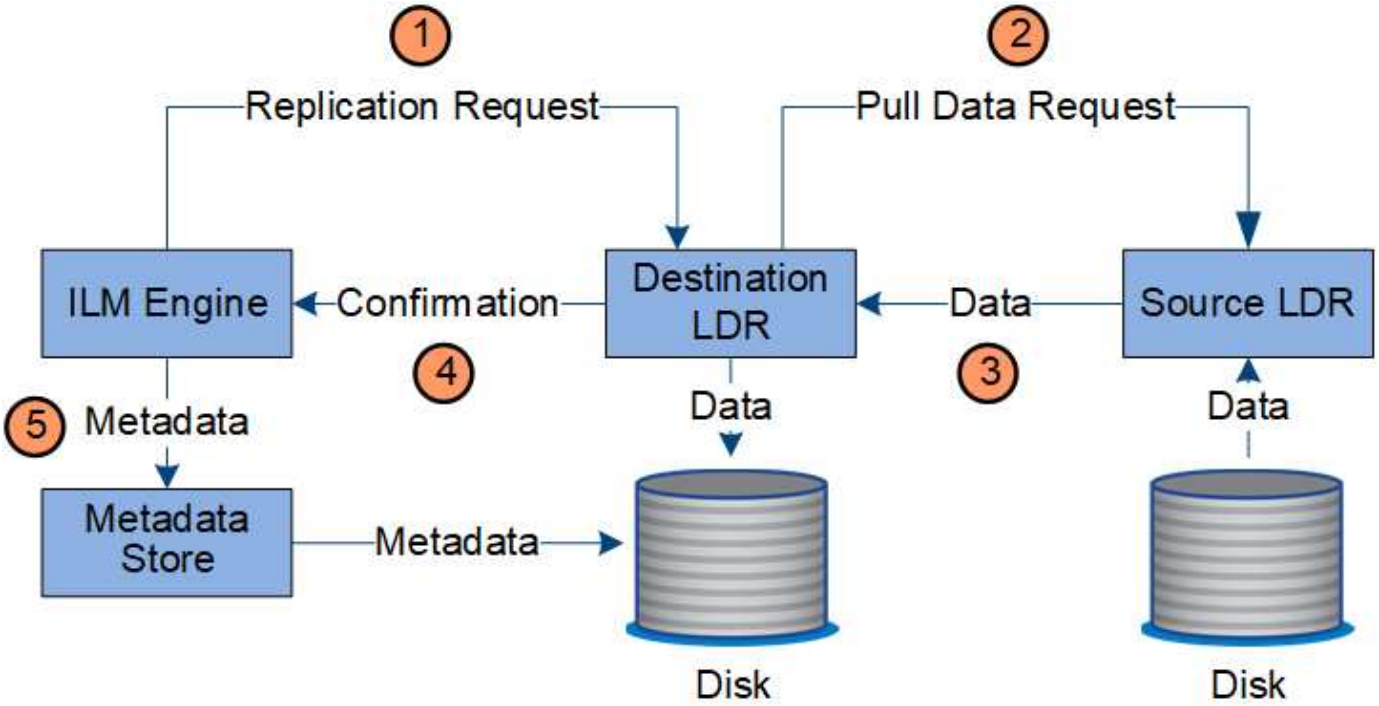
オブジェクトデータは LDR サービスで管理されます。

### コンテンツの保護：レプリケーション

ILM ルールのコンテンツ配置手順でオブジェクトデータのレプリケートコピーが必要とされている場合は、設定されたストレージプールを構成するストレージノードによってコピーが作成されてディスクに格納されます。

データフロー

レプリケーションの動作は LDR サービスの ILM エンジンで制御され、正しい数のコピーが正しい場所に正しい期間にわたって格納されます。



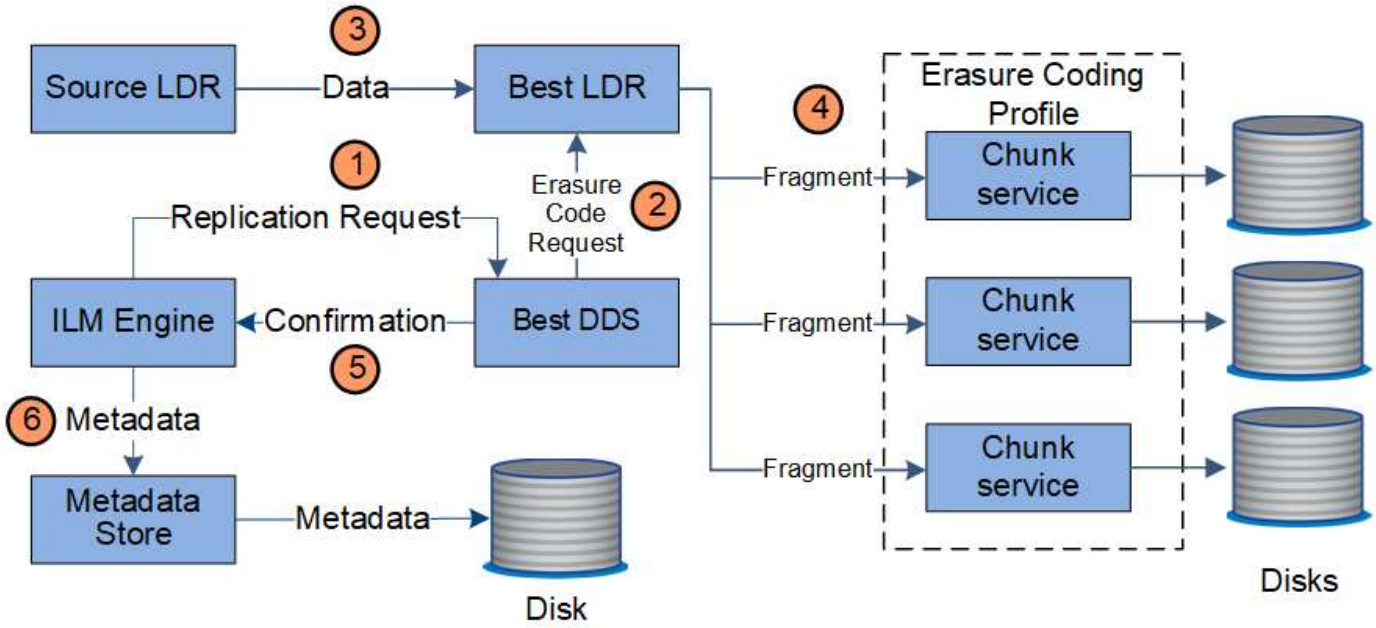

1. ILM エンジンが、 ILM ルールで指定されたストレージプール内で最適なデスティネーション LDR サービスを ADC サービスに照会します。その後、レプリケーションを開始するコマンドをその LDR サービスに送信します。
2. デスティネーション LDR サービスから、 ADC サービスを照会することで最適なソースの場所が特定されます。その後、レプリケーション要求をソース LDR サービスに送信します。
3. ソース LDR サービスからデスティネーション LDR サービスにコピーが送信されます。
4. デスティネーション LDR サービスから ILM エンジンに、オブジェクトデータが格納されたことが通知されます。
5. ILM エンジンが、メタデータストアのオブジェクトの場所を示すメタデータを更新します。

コンテンツの保護：イレイジャーコーディング

オブジェクトデータのイレイジャーコーディングコピーを作成するように ILM ルールで規定されている場合は、オブジェクトデータが該当するイレイジャーコーディングスキームに基づいてデータとパリティのフラグメントに分割され、イレイジャーコーディングプロファイルに設定されたストレージノードにそれらのフラグメントが分散して格納されます。

データフロー

LDR サービスのコンポーネントである ILM エンジンは、イレイジャーコーディングを制御し、イレイジャーコーディングプロファイルを確実にオブジェクトデータに適用します。



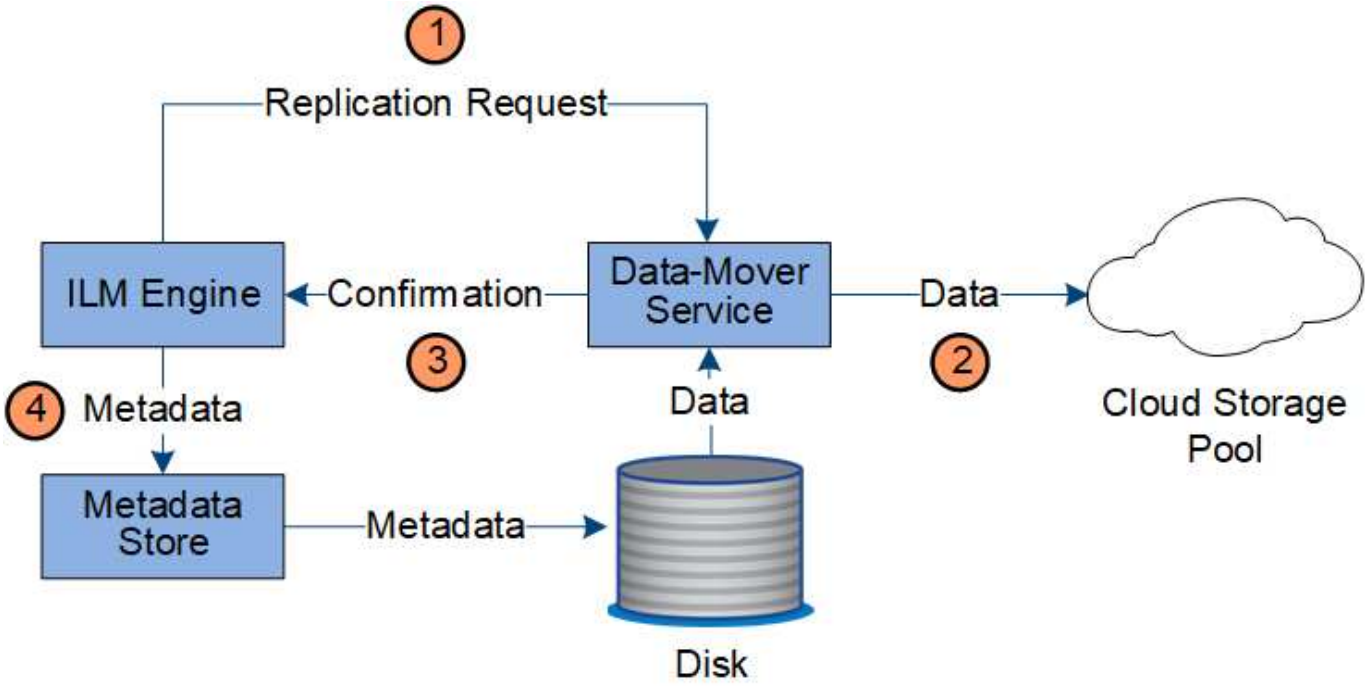

1. ILM エンジンから、 ADC サービスを照会することでイレイジャーコーディング処理の実行に最も適した DDS サービスが特定され、そのサービスに「開始」要求を送信します。
2. DDS サービスが、オブジェクトデータのイレイジャーコーディングを実行するように LDR に指示します。
3. ソース LDR サービスから、イレイジャーコーディングの対象として選択された LDR サービスにコピーが送信されます。
4. LDR サービスにより、オブジェクトデータが適切な数のパリティとデータのフラグメントに分割され、それらのフラグメントがイレイジャーコーディングプロファイルのストレージプールを構成するストレージノード（チャンクサービス）に分散されます。
5. LDR サービスから ILM エンジンに、オブジェクトデータの配信が完了したことが通知されます。
6. ILM エンジンが、メタデータストアのオブジェクトの場所を示すメタデータを更新します。

コンテンツの保護：クラウドストレージプール

ILMルールのコンテンツ配置手順でオブジェクトデータのレプリケートコピーをクラウドストレージプールに格納するように要求されている場合は、クラウドストレージプール用に指定された外部のS3バケットまたはAzure Blob Storageコンテナにオブジェクトデータが移動されます。

データフロー

LDR サービスのコンポーネントである ILM エンジンと、クラウドストレージプールへのオブジェクトの移動は Data Mover サービスによって制御されます。

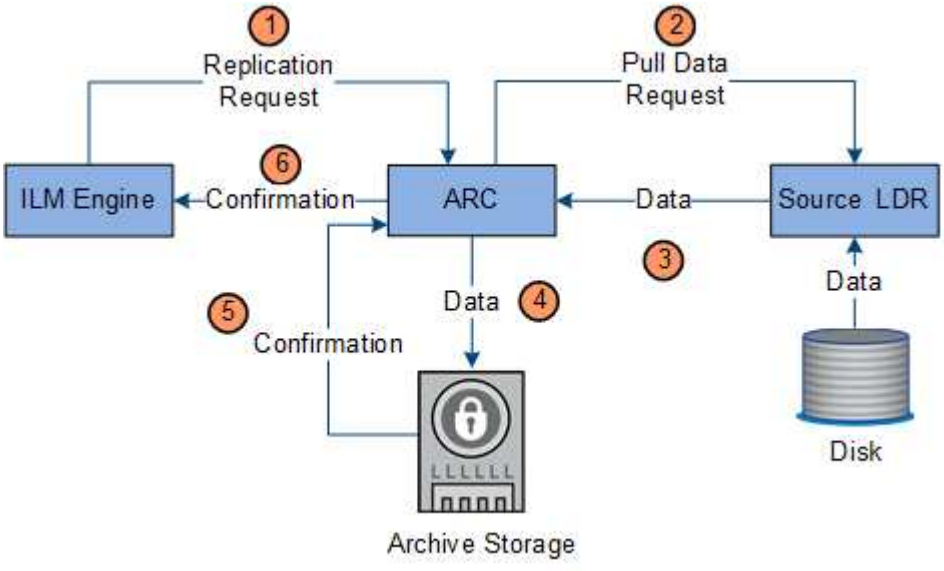



1. ILM エンジンが、クラウドストレージプールにレプリケートするための Data Mover サービスを選択します。
2. Data Mover サービスが、オブジェクトデータをクラウドストレージプールに送信します。
3. Data Mover サービスが、オブジェクトデータが格納されたことを ILM エンジンに通知します。
4. ILM エンジンが、メタデータストアのオブジェクトの場所を示すメタデータを更新します。

コンテンツの保護：アーカイブ

アーカイブ処理は、 StorageGRID システムとクライアントの間の定義されたデータフローで構成されます。

オブジェクトデータのコピーをアーカイブするように ILM ポリシーで規定されている場合は、 LDR サービスのコンポーネントである ILM エンジンがアーカイブノードに要求を送信し、アーカイブノードがオブジェクトデータのコピーを対象のアーカイブストレージシステムに送信します。



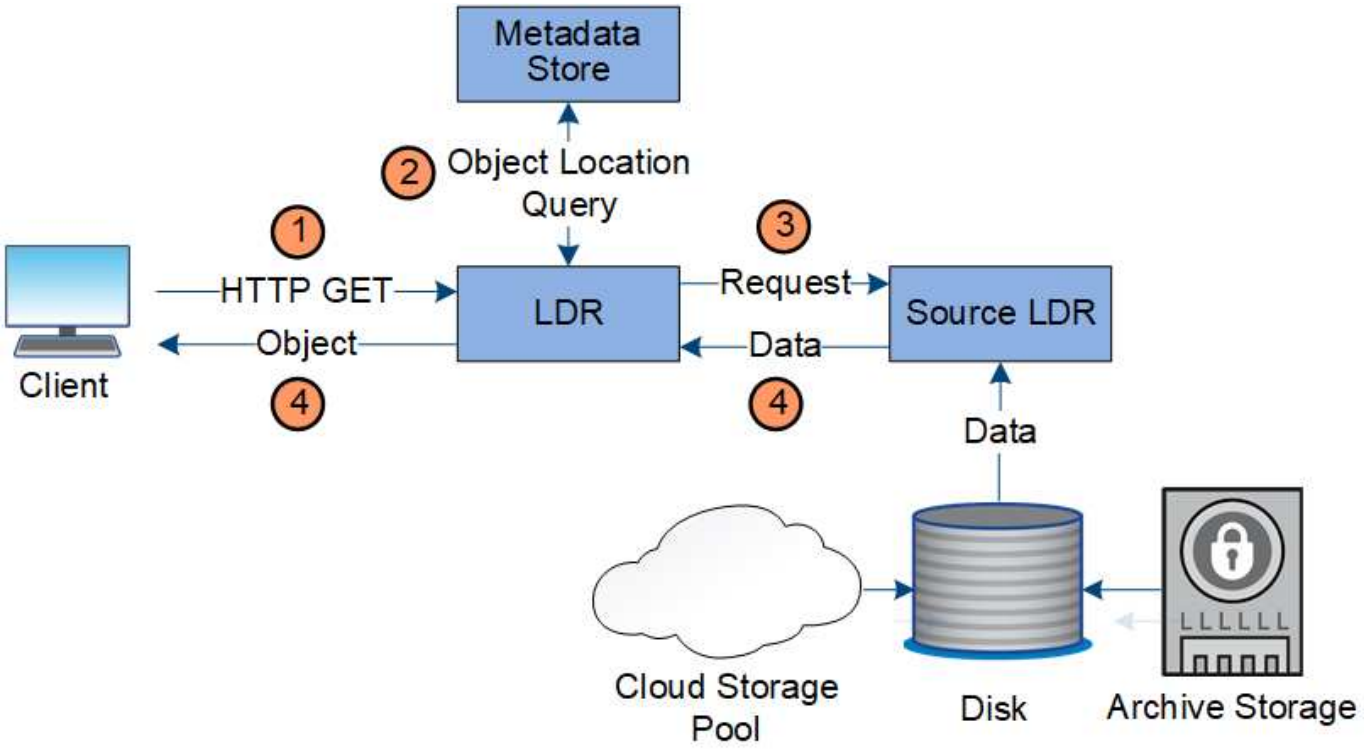
1. ILM エンジンが ARC サービスに要求を送信し、アーカイブメディアにコピーを格納するように指示します。
2. ARC サービスから、 ADC サービスを照会することで最適なソースの場所が特定され、ソース LDR サービスに要求が送信されます。
3. ARC サービスが、 LDR サービスからオブジェクトデータを読み出します。
4. ARC サービスが、対象のアーカイブメディアにオブジェクトデータを送信します。
5. アーカイブメディアから ARC サービスに、オブジェクトデータが格納されたことが通知されます。
6. ARC サービスから ILM エンジンに、オブジェクトデータが格納されたことが通知されます。

読み出しのデータフロー

## 読み出し処理は、 StorageGRID システムとクライアントの間の定義されたデータフローで構成されます。システムは、属性を使用して、ストレージノードからのオブジェクトの読み出し、または必要に応じてクラウドストレージプールまたはアーカイブノードからのオブジェクトの読み出しを追跡します。

ストレージノードの LDR サービスから、メタデータストアを照会することでオブジェクトデータの場所が特定され、ソース LDR サービスからオブジェクトデータが読み出されます。基本的には、ストレージノードからの読み出しが優先されます。ストレージノードからオブジェクトを読み出せない場合は、クラウドストレージプールまたはアーカイブノードに読み出し要求が転送されます。

オブジェクトコピーが AWS Glacier ストレージまたは Azure Archive 階層にしかない場合、クライアントアプリケーションは、読み出し可能なコピーをクラウドストレージプールにリストアするために S3 POST Object restore 要求を問題 で実行する必要があります。




1. LDR サービスがクライアントアプリケーションから読み出し要求を受信

2. LDR サービスからメタデータストアを照会することで、オブジェクトデータの場所とメタデータが特定されます。
3. LDR サービスからソース LDR サービスに読み出し要求が転送されます。
4. ソース LDR サービスから照会元の LDR サービスにオブジェクトデータが返され、システムからクライアントアプリケーションにオブジェクトが返されます。

データフローを削除します

## クライアントが削除処理を実行するか、またはオブジェクトの有効期間が終了して自動削除がトリガーされると、 StorageGRID システムからすべてのオブジェクトコピーが削除されます。オブジェクト削除のデータフローが定義されています。

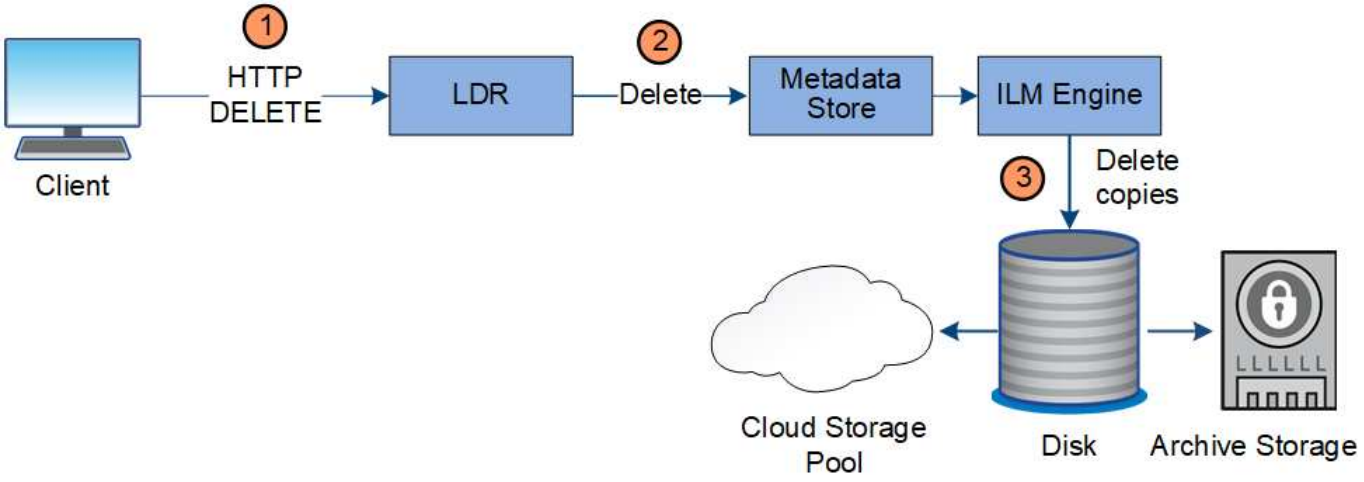
削除階層

StorageGRID では、オブジェクトを保持するか削除するかを制御する方法がいくつかあります。オブジェクトは、クライアント要求に応じて削除することも、自動で削除することもできますStorageGRID は、 S3 バケットライフサイクルと ILM の配置手順よりも優先される S3 オブジェクトロックの設定をクライアントの削除要求よりも常に優先します。

- * S3 オブジェクトのロック * ：グリッドでグローバルな S3 オブジェクトのロック設定が有効になっている場合、 S3 クライアントは S3 オブジェクトのロックを有効にしたバケットを作成し、 S3 REST API を使用して、そのバケットに追加された各オブジェクトバージョンの最新の保持設定とリーガルホールド設定を指定できます。
  - リーガルホールドの対象になっているオブジェクトバージョンは、どの方法でも削除できません。
  - オブジェクトバージョンの retain-until - date に到達するまでは、どのメソッドでもそのバージョンを削除することはできません。
  - S3 オブジェクトロックが有効になっているバケット内のオブジェクトは、 ILM によって「無期限」に保持されます。ただし、それまでの保持期間が終了したあとは、クライアント要求やバケットライフサイクルの終了によってオブジェクトバージョンを削除できます。
- * クライアントの削除要求 * ： S3 または Swift クライアントは、オブジェクトの削除要求を問題 できます。クライアントがオブジェクトを削除すると、そのオブジェクトのすべてのコピーが StorageGRID システムから削除されます。
- * S3 バケットライフサイクル * ： S3 クライアントは、 Expiration アクションを指定するライフサイクル設定をバケットに追加できます。バケットライフサイクルが設定されている場合、クライアントが先にオブジェクトを削除しないかぎり、 Expiration アクションで指定された日付または日数が経過した時点で、StorageGRID はオブジェクトのすべてのコピーを自動的に削除します。
- * ILM の配置手順 * ：バケットで S3 オブジェクトロックが有効になっておらず、バケットライフサイクルがない場合、 StorageGRID は ILM ルールの最後の期間が終了してオブジェクトにそれ以降の配置が指定されていないときにオブジェクトを自動的に削除します。

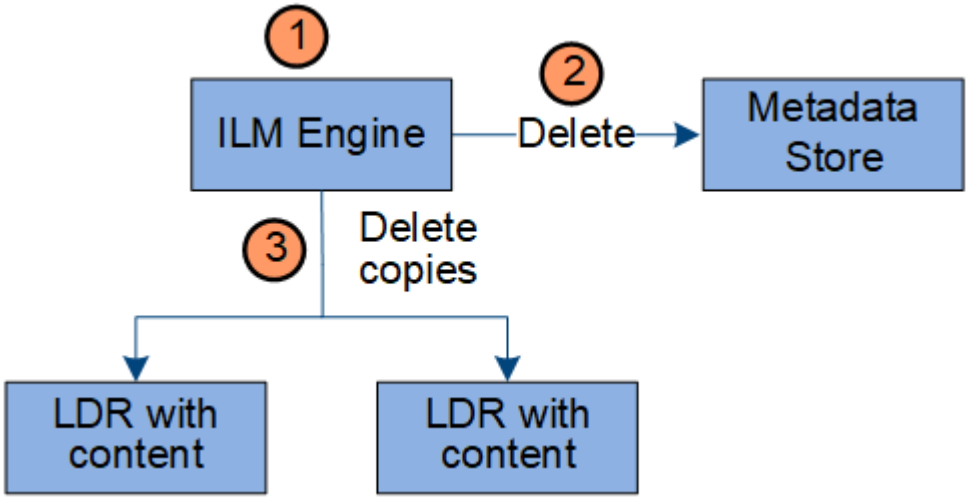
> S3 バケットライフサイクルの Expiration アクションは、常に ILM 設定よりも優先されます。その結果、 ILM のオブジェクト配置手順がすべて終了したあとも、オブジェクトがグリッドに保持されることがあります。

クライアント削除のデータフロー




1. LDR サービスがクライアントアプリケーションから削除要求を受信
2. LDR サービスが、メタデータストアを更新してオブジェクトをクライアント要求に対して見かけ上削除し、 ILM エンジンにオブジェクトデータのすべてのコピーの削除を指示します。
3. オブジェクトがシステムから削除されます。メタデータストアが更新されてオブジェクトメタデータが削除されます。

**ILM** による削除のデータフローを示します




1. オブジェクトの削除が必要であることを ILM エンジンが確認します。
2. ILM エンジンがメタデータストアに通知します。メタデータストアがオブジェクトメタデータを更新して、オブジェクトをクライアント要求に対して見かけ上削除します。
3. ILM エンジンがオブジェクトのすべてのコピーを削除します。メタデータストアが更新されてオブジェクトメタデータが削除されます。

## Grid Managerの概要

Grid Manager はブラウザベースのグラフィカルインターフェイスで、 StorageGRID システムの設定、管理、監視に使用できます。

Grid Manager にサインインすると、管理ノードに接続されます。各 StorageGRID システムには、 1 つのプラ

イマリ管理ノードと、任意の数のプライマリ以外の管理ノードが含まれています。どの管理ノードにも接続が可能で、各管理ノードに表示される StorageGRID システムのビューもほぼ同じです。

Grid Managerには、サポートされているWebブラウザからアクセスできます。

**Web** ブラウザの要件

サポートされている Web ブラウザを使用する必要があります。

| **Web** ブラウザ | サポートされる最小バージョン |
| --- | --- |
| Google Chrome | 87 |
| Microsoft Edge の場合 | 87 |
| Mozilla Firefox | 84 |

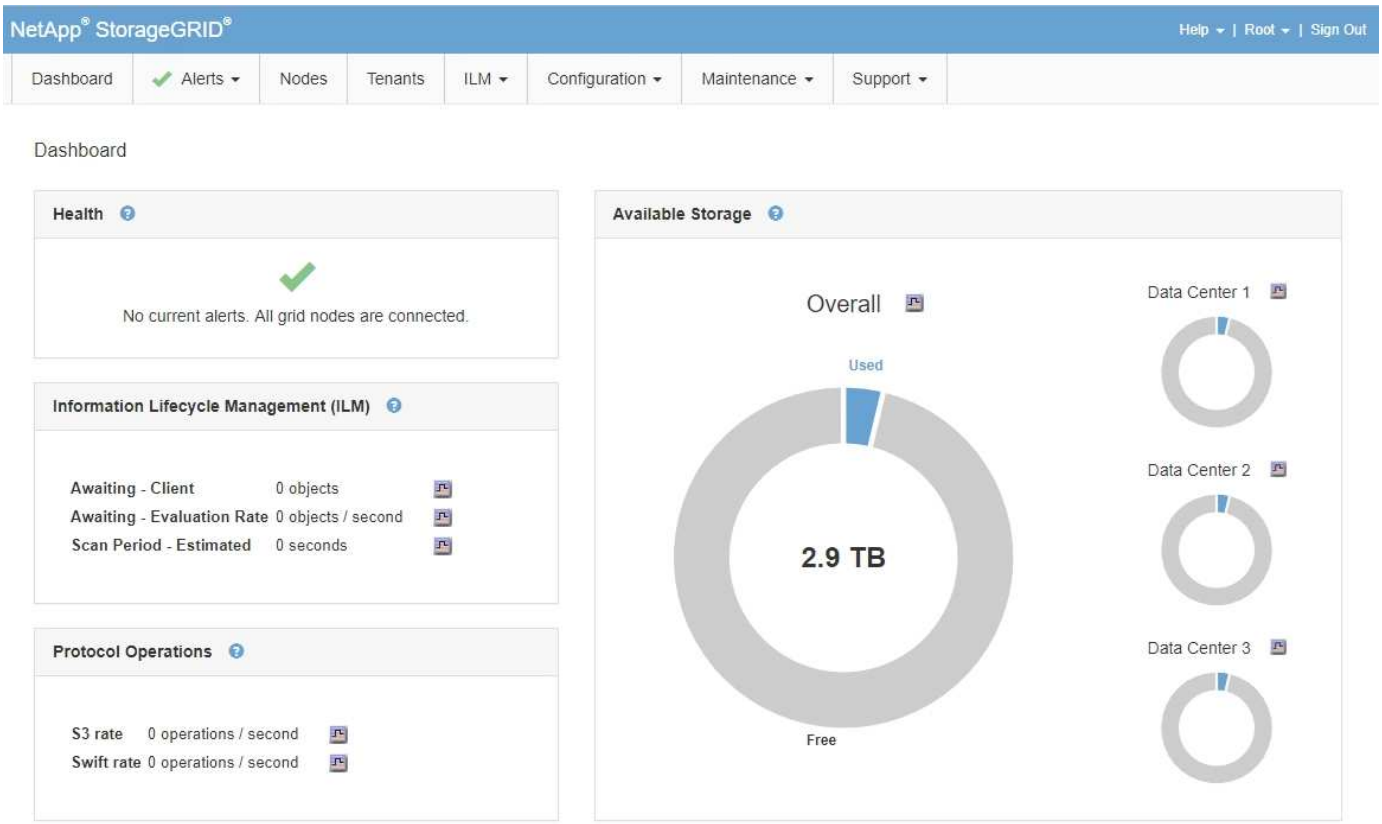
ブラウザウィンドウの幅を推奨される値に設定してください。

| ブラウザの幅 | ピクセル |
| --- | --- |
| 最小（ Minimum ） | 1024 |
| 最適 | 1280 |

**Grid Manager** ダッシュボード

Grid Manager に初めてサインインするときは、ダッシュボードを使用してシステムのアクティビティを一目で監視できます。

ダッシュボードには、システムの健常性、ストレージの使用状況、 ILM プロセス、 S3 および Swift 処理に関する概要情報が表示されます。



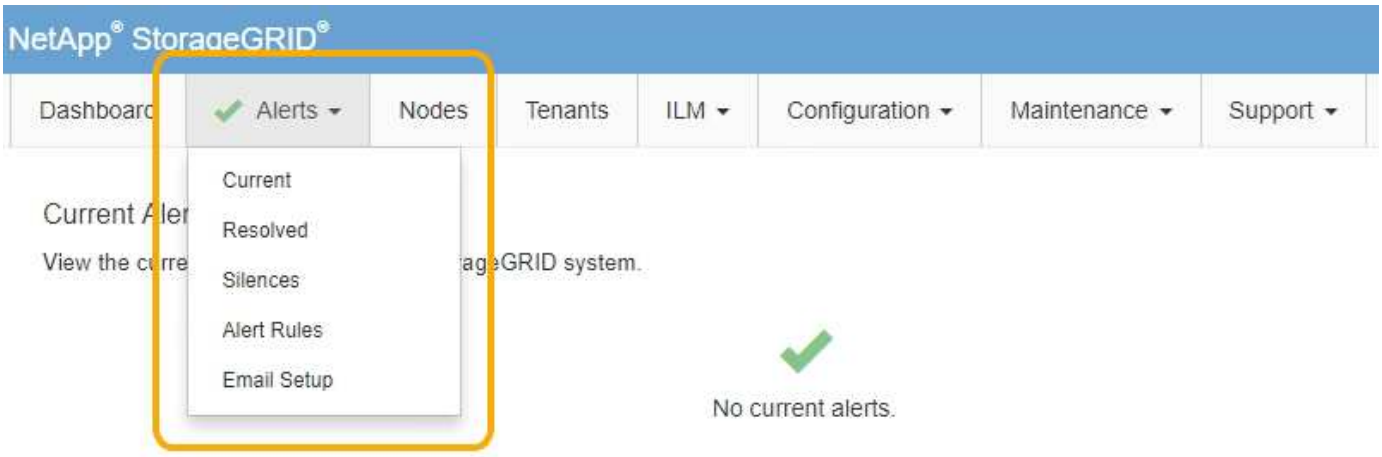

各パネルの情報の説明については、ヘルプアイコンをクリックしてください をクリックしてください。

関連情報

"トラブルシューティングを監視します"

［ アラート ］ メニュー

[Alerts] メニューには、 StorageGRID の動作中に発生する可能性のある問題を検出、評価、解決するための使いやすいインターフェイスが用意されています。




[Alerts] メニューでは ' 次の操作を実行できます

- 現在のアラートを確認します

- 解決済みのアラートを確認
- サイレンスを設定してアラート通知を停止する
- アラート通知用の E メールサーバを設定します
- アラートをトリガーする条件のアラートルールを定義

関連情報

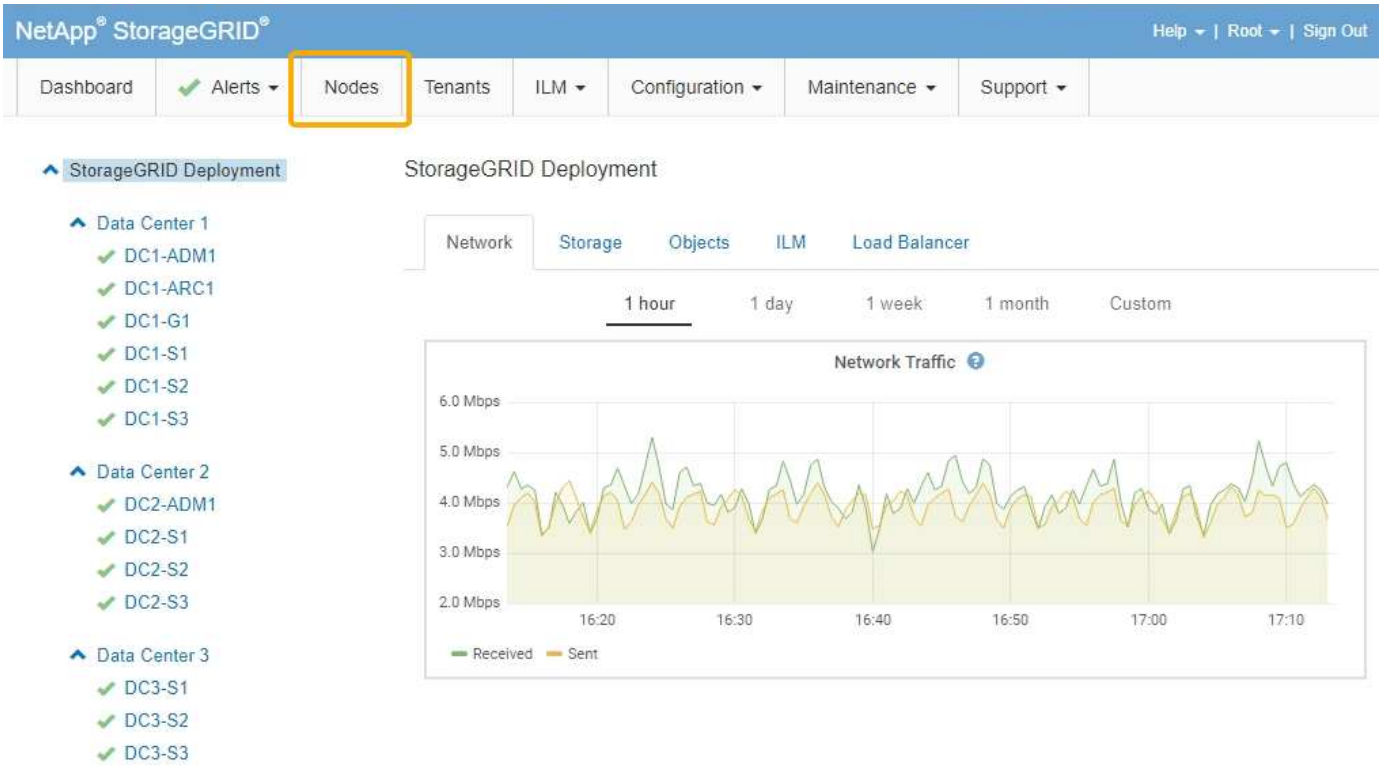
"アラートの監視と管理"

"トラブルシューティングを監視します"

### Nodes ヘエシ

Nodes ページには、グリッド全体、グリッド内の各サイト、およびサイトの各ノードに関する情報が表示されます。

ノードのホームページには、グリッド全体の複数の指標の合計が表示されます。特定のサイトまたはノードの情報を表示するには、左側の該当するリンクをクリックします。




関連情報

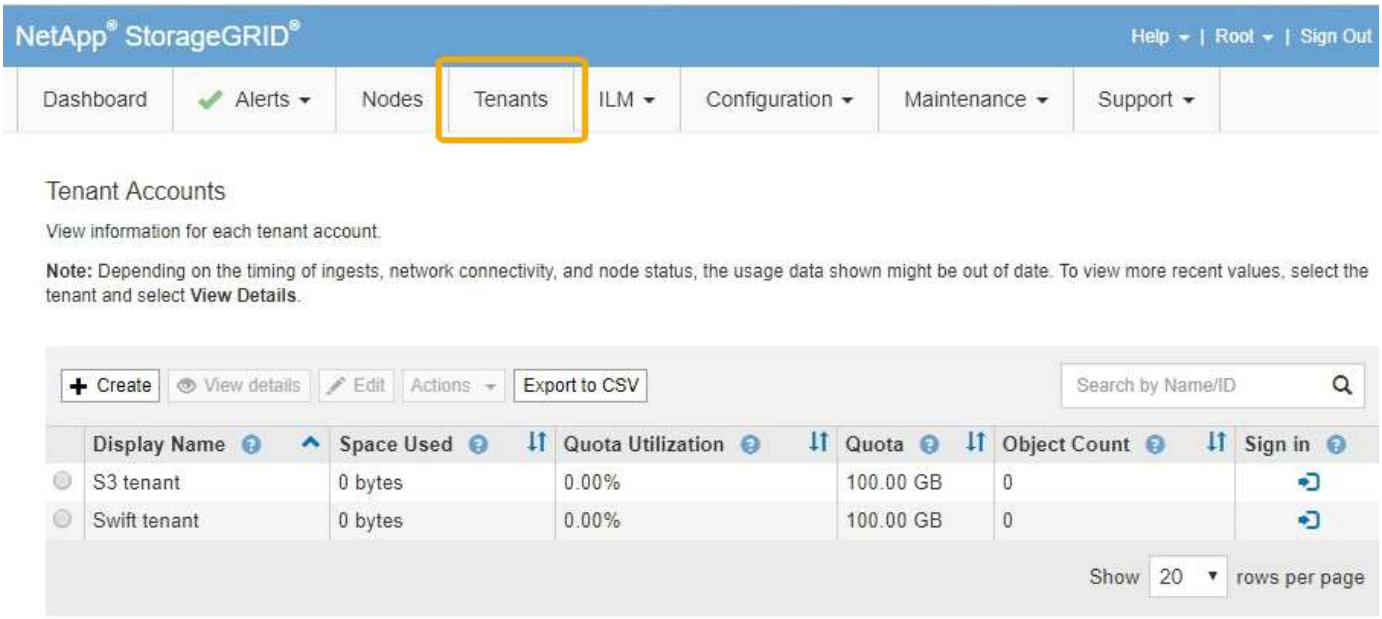
"Nodesページを表示します"

"トラブルシューティングを監視します"

テナントアカウントヘエシ

Tenant Accountsページでは、StorageGRID システムのストレージテナントアカウントを作成および監視できます。オブジェクトの格納と読み出しを実行できるユーザを指定し、どの機能を利用可能とするかを指定するには、少なくとも 1 つのテナントアカウントを作成する必要があります。

テナントアカウントページには、使用されているストレージの容量やオブジェクトの数など、各テナントの使用状況の詳細も表示されます。テナントの作成時にクォータを設定すると、そのクォータのうちどれくらいが使用されているかを確認できます。




関連情報

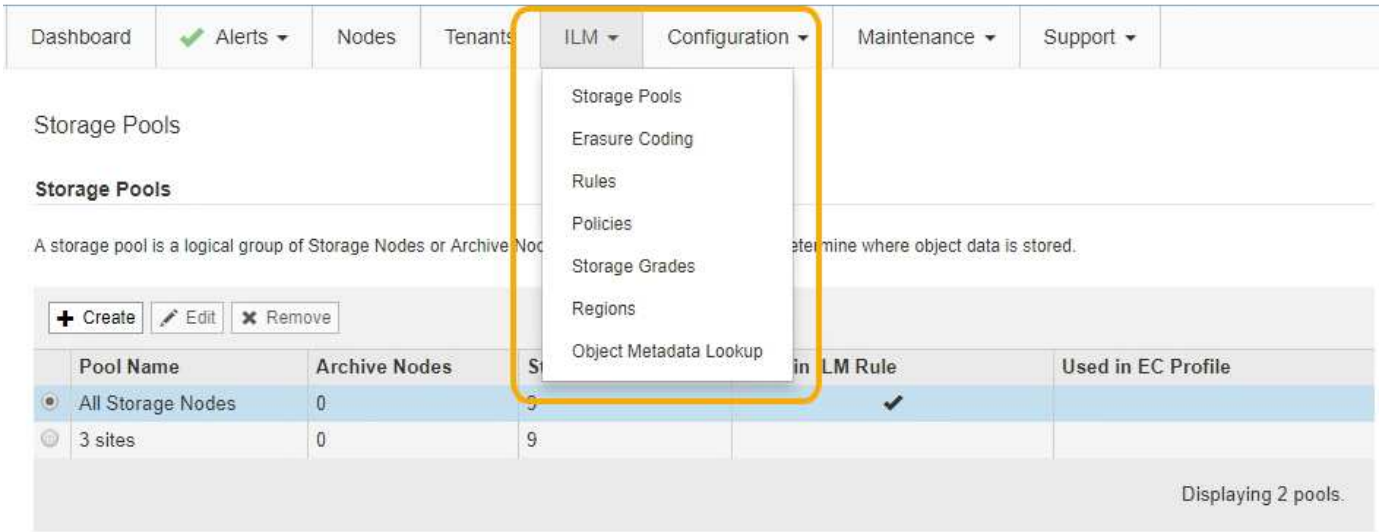
"テナントとクライアント接続の管理"

"StorageGRID の管理"

"テナントアカウントを使用する"

**ILM** メニュー

ILM メニューでは、データの保持と可用性を制御する情報ライフサイクル管理（ ILM ）のルールとポリシーを設定できます。オブジェクト ID を入力して、そのオブジェクトのメタデータを表示することもできます。




関連情報

"情報ライフサイクル管理の使用"

"ILM を使用してオブジェクトを管理する"

設定メニュー

[Configuration]メニューでは、ネットワーク設定、システム設定、モニタリングオプション、およびアクセスコントロールオプションを指定できます。

関連情報

"ネットワークの設定"

"テナントとクライアント接続の管理"

"監査メッセージの確認"

"StorageGRID アクセスの制御"

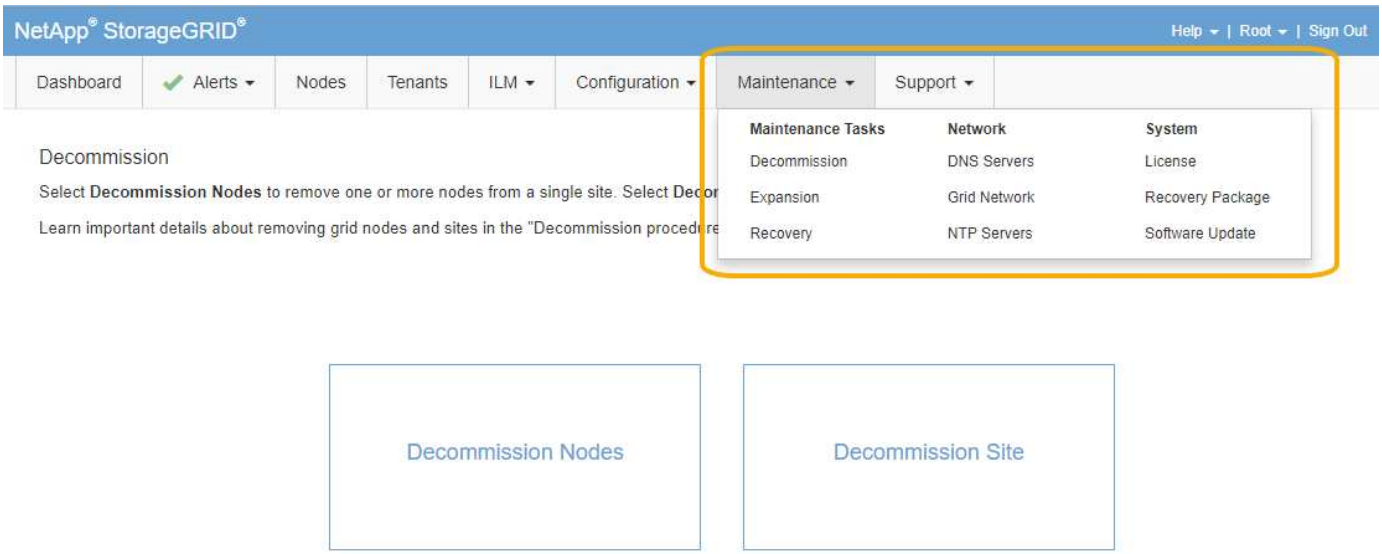
"StorageGRID の管理"

"トラブルシューティングを監視します"

"監査ログを確認します"

メンテナンスメニュー

Maintenance（メンテナンス）メニューでは、メンテナンスタスク、ネットワークタスク、およびシステムタスクを実行できます。




メンテナンスタスク

保守作業には次のものが含ま

- 運用停止処理：使用されていないグリッドノードとサイトを削除します。
- 新しいグリッドノードとサイトを追加するための拡張処理。
- 障害が発生したノードの交換とデータのリストアに使用するリカバリ処理。

ネットワーク

Maintenanceメニューから実行できるネットワークタスクは次のとおりです。

- DNS サーバの情報を編集します。
- グリッドネットワークで使用されるサブネットを設定します。
- NTP サーバの情報を編集しています。

システム

Maintenanceメニューから実行できるシステムタスクは次のとおりです。

- 現在の StorageGRID ライセンスの詳細を確認するか、新しいライセンスをアップロードしています。
- リカバリパッケージを生成しています。
- 選択したアプライアンスで、ソフトウェアのアップグレード、ホットフィックス、 SANtricity OS ソフトウェアの更新など、 StorageGRID ソフトウェアの更新を実行する。

関連情報

"メンテナンス手順の実行"

"リカバリパッケージをダウンロードしています"

"グリッドを展開します"

"ソフトウェアをアップグレードする"

""

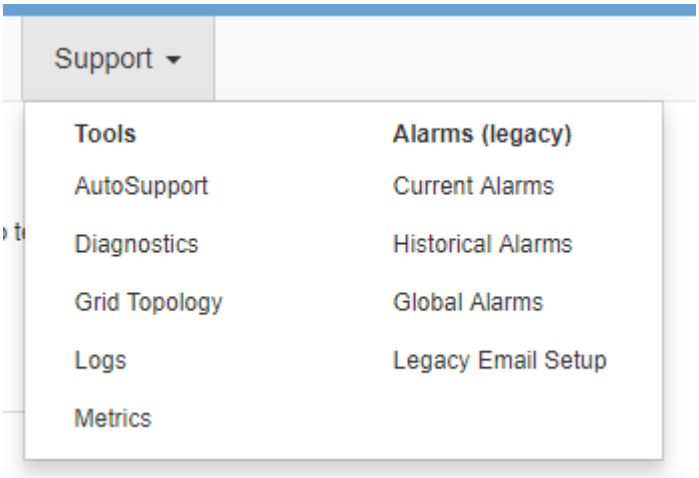
"SG6000 ストレージアプライアンス"

"SG5700 ストレージアプライアンス"

"SG5600 ストレージアプライアンス"

サポートメニュー

Support （サポート）メニューには、テクニカルサポートがシステムの分析とトラブルシューティングに役立つオプションが表示されます。[ サポート ] メニューには、 [ ツール ] と [ アラーム ] （レガシー）の 2 つの部分があります。




ツール

[ サポート（ Support ） ] メニューの [ ツール（ Tools ） ] セクションから、次の操作を実行できます。

- AutoSupport を有効にします。
- グリッドの現在の状態に対して一連の診断チェックを実行します。
- グリッドトポロジツリーにアクセスして、グリッドノード、サービス、および属性に関する詳細情報を表示します。
- ログファイルとシステムデータを取得します。
- 詳細な指標やチャートを確認

[*Metrics] オプションで使用できるツールは、テクニカル・サポートが使用することを目的としています。これらのツールの一部の機能およびメニュー項目は、意図的に機能しないようになっています。

アラーム（レガシー）

サポートメニューのアラーム（レガシー）セクションでは、現在のアラーム、履歴アラーム、グローバルアラームを確認したり、従来のアラームとAutoSupport のEメール通知を設定したりできます。

関連情報

"StorageGRID のアーキテクチャとネットワークトポロジ"

"StorageGRID 属性"

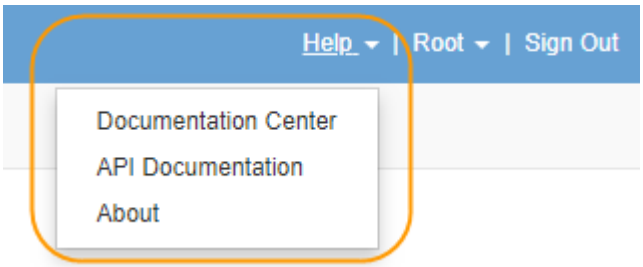
"StorageGRID サポートオプションを使用する"

"StorageGRID の管理"

"トラブルシューティングを監視します"

ヘルプメニュー

ヘルプオプションを使用すると、最新リリースの StorageGRID ドキュメントセンターや API ドキュメントにアクセスできます。現在インストールされている StorageGRID のバージョンを確認することもできます。




関連情報

"StorageGRID の管理"

## Tenant Managerの概要

Tenant Manager は、テナントユーザがストレージアカウントを設定、管理、および監視するためにアクセスするブラウザベースのグラフィカルインターフェイスです。

Tenant Manager にサインインしたテナントユーザは管理ノードに接続しています。

関連情報

"Grid Managerの概要"

"テナントアカウントを使用する"

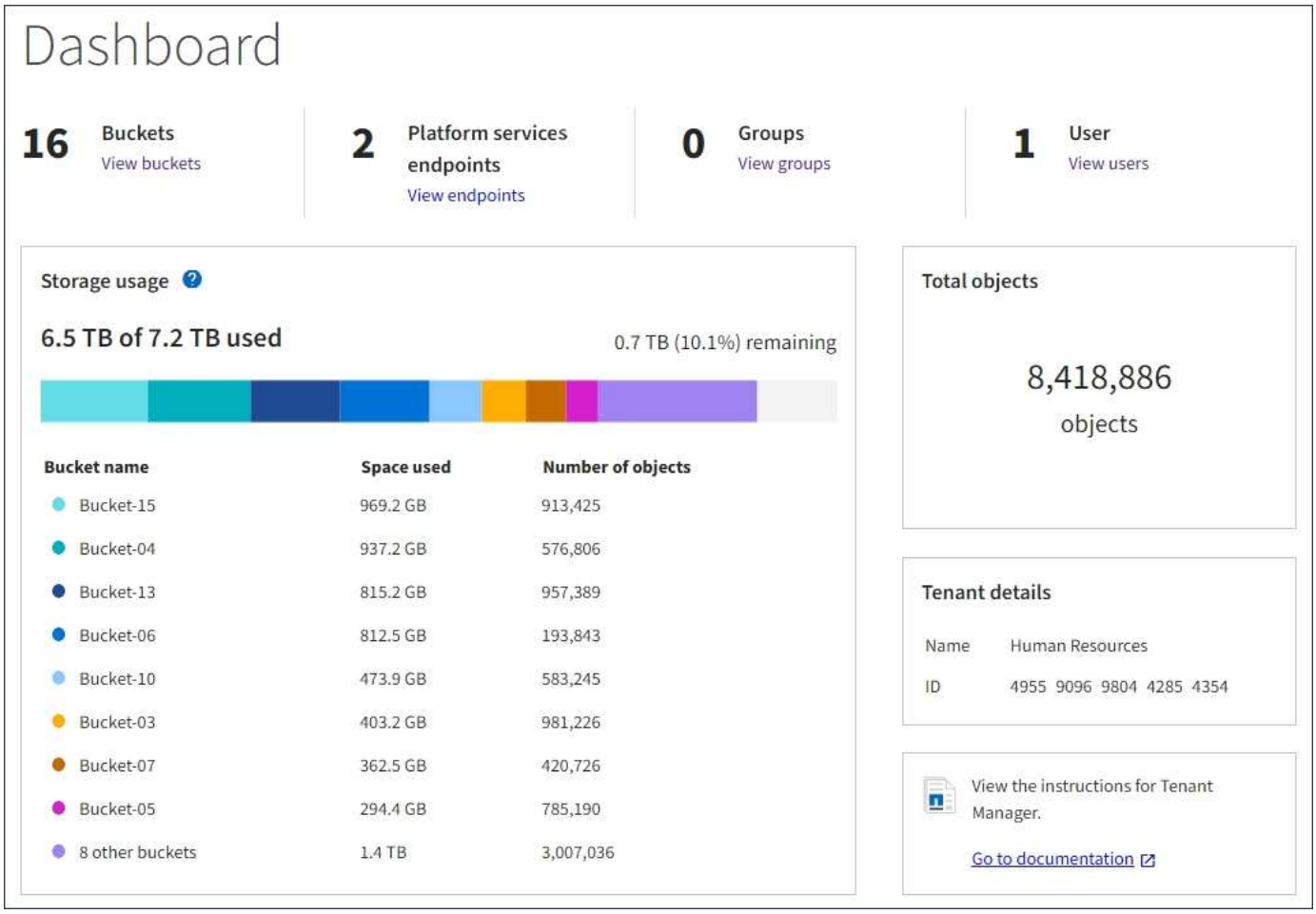
### Tenant Manager のダッシュボード

グリッド管理者が Grid Manager またはグリッド管理 API を使用してテナントアカウントを作成すると、テナントユーザが Tenant Manager にサインインできるようになります。

Tenant Manager のダッシュボードでは、テナントユーザがストレージの使用状況を一目で監視できます。ストレージの使用状況パネルには、テナントの最大バケット（ S3 ）またはコンテナ（ Swift ）のリストが含まれます。Space Used の値は、バケットまたはコンテナ内のオブジェクトデータの合計量です。棒グラフは、これらのバケットまたはコンテナの相対サイズを表します。

棒グラフの上に表示される値は、テナントのすべてのバケットまたはコンテナに使用されているスペースの合計です。テナントで使用可能な最大ギガバイト数、テラバイト数、またはペタバイト数をアカウント作成時に

指定した場合は、使用されているクォータの量と残りのクォータも表示されます。




ストレージメニュー（ **S3** テナントのみ）

ストレージのメニューは S3 テナントアカウントに対してのみ表示されます。S3 ユーザはこのメニューを使用して、アクセスキーの管理、バケットの作成と削除、プラットフォームサービスエンドポイントの管理を行うことができます。

アクセスキー

S3 テナントユーザは次のようにアクセスキーを管理できます。

- Manage Your Own S3 Credentials 権限が設定されたユーザは、自分の S3 アクセスキーを作成または削除

できます。

- Root Access 権限が設定されたユーザは、 S3 root アカウント、自分のアカウント、およびその他すべてのユーザのアクセスキーを管理できます。root アクセスキーは、バケットポリシーで root アクセスキーが明示的に無効になっていないかぎり、テナントのバケットとオブジェクトへのフルアクセスも提供します。

> 他のユーザのアクセスキーの管理は、 Access Management メニューから行います。

バケット

適切な権限を持つ S3 テナントユーザは、バケットに関連する次のタスクを実行できます。

- バケットを作成する
- 新しいバケットの S3 オブジェクトロックを有効にする（ StorageGRID システムで S3 オブジェクトロックが有効になっていることを前提）
- 整合性レベル設定を更新します
- Cross-Origin Resource Sharing （ CORS ）の設定
- テナントに属するバケットの最終アクセス日時の更新設定の有効化または無効化
- 空のバケットを削除します

グリッド管理者がテナントアカウントにプラットフォームサービスの使用を許可した場合、適切な権限を持つ S3 テナントユーザは次のタスクも実行できます。

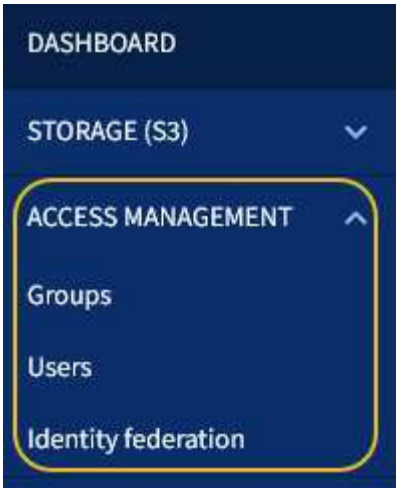
- S3 イベント通知の設定。この通知は、 AWS Simple Notification Service ™（ SNS ）をサポートするデスティネーションサービスに送信できます。
- CloudMirror レプリケーションの設定。テナントから外部の S3 バケットにオブジェクトが自動的にレプリケートされるようにすることができます。
- 検索統合の設定。検索統合は、オブジェクトの作成、削除、またはそのメタデータやタグの更新が行われるたびに、デスティネーションの検索インデックスにオブジェクトメタデータを送信します。

プラットフォームサービスのエンドポイント

グリッド管理者がテナントアカウントにプラットフォームサービスの使用を許可した場合、 Manage Endpoints 権限のある S3 テナントユーザは、各プラットフォームサービスのデスティネーションエンドポイントを設定できます。

### **Access** 管理メニュー

アクセス管理メニューを使用すると、 StorageGRID テナントでフェデレーテッドアイデンティティソースからユーザグループをインポートして、管理権限を割り当てることができます。StorageGRID システム全体でシングルサインオン（ SSO ）が有効になっていないかぎり、テナントがローカルテナントグループおよびユーザを管理することもできます。




## StorageGRID を使用する

グリッドノードとStorageGRID ネットワークのインストールが完了したら、StorageGRID の設定と使用を開始できます。システム管理機能へのユーザアクセスの制御、テナントアカウントの設定、クライアント接続の管理、設定オプションの設定、ILMによるオブジェクトの場所の管理、StorageGRID システムの健全性と日常のアクティビティの監視、定期的/非定期的なメンテナンスなどのタスクを実行します。

- "StorageGRID アクセスの制御"
- "テナントとクライアント接続の管理"
- "ネットワークの設定"
- "システム設定を構成しています"
- "情報ライフサイクル管理の使用"
- "StorageGRID 処理の監視"
- "メンテナンス手順の実行"
- "StorageGRID サポートオプションを使用する"

### StorageGRID アクセスの制御

StorageGRID にアクセスできるユーザ、およびユーザが実行できるタスクを制御するには、グループとユーザを作成またはインポートし、各グループに権限を割り当てます。必要に応じて、シングルサインオン（ SSO ）を有効にしたり、クライアント証明書を作成したり、グリッドのパスワードを変更したりできます。

#### Grid Managerへのアクセスの制御

Grid Manager およびグリッド管理 API にアクセスできるユーザを指定するには、アイデンティティフェデレーションサービスからグループとユーザをインポートするか、またはローカルのグループおよびユーザを設定します。

アイデンティティフェデレーションを使用すると、グループやユーザを迅速に設定できます。また、ユーザは使い慣れたクレデンシャルを使用して StorageGRID にサインインできます。Active Directory 、 OpenLDAP

、または Oracle Directory Server を使用する場合は、アイデンティティフェデレーションを設定できます。

別の LDAP v3 サービスを使用する場合は、テクニカルサポートにお問い合わせください。

各ユーザが実行できるタスクを指定するには、各グループに異なる権限を割り当てます。たとえば、あるグループのユーザには ILM ルールを管理する権限を、別のグループのユーザにはメンテナンスタスクを実行する権限を与えることができます。システムにアクセスするには、ユーザが少なくとも 1 つのグループに属している必要があります。

必要に応じて、グループを読み取り専用に設定することができます。読み取り専用グループのユーザは、設定と機能のみを表示できます。Grid Manager API や Grid 管理 API で変更や処理を行うことはできません。

#### シングルサインオンの有効化

StorageGRID システムでは、 Security Assertion Markup Language 2.0 （ SAML 2.0 ）標準を使用したシングルサインオン（ SSO ）がサポートされます。SSO が有効な場合は、 Grid Manager 、 Tenant Manager 、 Grid 管理 API 、またはテナント管理 API にアクセスするすべてのユーザを外部のアイデンティティプロバイダによって認証する必要があります。ローカルユーザは StorageGRID にサインインできません。

SSO が有効な場合にユーザが StorageGRID にサインインすると、組織の SSO ページにリダイレクトされてクレデンシャルが検証されます。1 つの管理ノードからサインアウトしたユーザは、自動的にすべての管理ノードからサインアウトされます。

#### クライアント証明書を使用

クライアント証明書を使用すると、許可された外部クライアントがStorageGRID Prometheusデータベースにアクセスできるようになります。クライアント証明書は、外部ツールを使用してStorageGRID を監視するためのセキュアな方法を提供します。独自のクライアント証明書を指定するか、Grid Managerを使用して証明書を生成できます。

#### グリッドのパスワードの変更

プロビジョニングパスフレーズは、多くのインストールやメンテナンスの手順、および StorageGRID リカバリパッケージのダウンロードで必要になります。また、 StorageGRID システムのグリッドトポロジ情報と暗号化キーのバックアップをダウンロードする際にもパスフレーズが必要です。このパスフレーズは必要に応じて変更できます。

関連情報

"StorageGRID の管理"

"テナントアカウントを使用する"

### テナントとクライアント接続の管理

グリッド管理者は、 S3 および Swift クライアントがオブジェクトの格納および読み出しに使用するテナントアカウントを作成して管理し、またクライアントが StorageGRID システムに接続する方法を制御する設定オプションを管理します。

#### テナントアカウント

テナントアカウントを使用すると、 StorageGRID システムでオブジェクトの格納と読み出しを実行できるユーザを指定し、どの機能を利用可能とするかを設定できます。テナントアカウントは、 S3 REST API または

Swift REST API をサポートするクライアントアプリケーションが、 StorageGRID でオブジェクトの格納や読み出しを行うことを可能にします。テナントアカウントでは、それぞれ S3 クライアントプロトコルまたは Swift クライアントプロトコルのどちらかを使用します。

StorageGRID システムにオブジェクトを格納するために使用されるクライアントプロトコルごとに、テナントアカウントを少なくとも 1 つ作成する必要があります。必要に応じて、システムに格納されているオブジェクトをエンティティごとに分ける場合は、追加のテナントアカウントを作成します。各テナントアカウントには、フェデレーテッド / ローカルグループとユーザ、および独自のバケット（ Swift の場合はコンテナ）とオブジェクトがあります。

Grid Manager またはグリッド管理 API を使用してテナントアカウントを作成できます。テナントアカウントを作成する際には次の情報を指定します。

- テナントの表示名（テナントのアカウント ID は自動的に割り当てられ、変更できません）。
- テナントアカウントが S3 と Swift のどちらを使用するか。
- S3 テナントアカウントの場合：テナントアカウントにプラットフォームサービスの使用を許可するかどうか。プラットフォームサービスの使用が許可されている場合は、グリッドがその使用をサポートするように設定されている必要があります。
- 必要に応じて、テナントアカウントのストレージクォータ — テナントのオブジェクトで使用可能な最大ギガバイト数、テラバイト数、ペタバイト数。テナントのストレージクォータは、物理容量（ディスクのサイズ）ではなく、論理容量（オブジェクトのサイズ）を表します。
- StorageGRID システムでアイデンティティフェデレーションが有効になっている場合は、テナントアカウントを設定するための Root Access 権限が割り当てられているフェデレーテッドグループ。
- StorageGRID システムでシングルサインオン（ SSO ）が使用されていない場合は、テナントアカウントが独自のアイデンティティソースを使用するか、グリッドのアイデンティティソースを共有するか、およびテナントのローカル root ユーザの初期パスワード。

S3 テナントアカウントが規制要件に準拠する必要がある場合、グリッド管理者は StorageGRID システムに対して S3 オブジェクトのグローバルロック設定を有効にできます。システムで S3 オブジェクトのロックが有効になっている場合、すべての S3 テナントアカウントで S3 オブジェクトのロックを有効にしたバケットを作成し、そのバケット内のオブジェクトバージョンの保持設定とリーガルホールド設定を指定できます。

テナントアカウントが作成されると、テナントユーザが Tenant Manager にサインインできるようになります。

#### StorageGRID ノードへのクライアント接続

テナントユーザが S3 または Swift クライアントを使用して StorageGRID でデータの格納や読み出しを行う前に、それらのクライアントが StorageGRID ノードに接続する方法を決定する必要があります。

クライアントアプリケーションは、次のいずれかに接続することで、オブジェクトを格納または読み出すことができます。

- 管理ノードまたはゲートウェイノード上のロードバランササービス。これが推奨される接続です。
- ゲートウェイノード上の CLB サービス。

  CLB サービスは廃止されました。

- 外部ロードバランサを使用するかどうかに関係なく、ストレージノードに追加されます。

クライアントがロードバランササービスを使用できるように StorageGRID を設定する場合は、次の手順を実行します。

1. ロードバランササービスのエンドポイントを設定する。管理ノードまたはゲートウェイノード上のロードバランササービスは、クライアントアプリケーションからの受信ネットワーク接続を複数のストレージノードに分散します。ロードバランサエンドポイントを作成する際には、ポート番号、エンドポイントで HTTP / HTTPS 接続を許可するかどうか、エンドポイントを使用するクライアントのタイプ（ S3 または Swift ）、 HTTPS 接続に使用する証明書（該当する場合）を指定します。
2. ノードのクライアントネットワークへの接続がすべてロードバランサエンドポイントで行われるようにする場合は、ノードのクライアントネットワークを信頼されていないものとして指定します。
3. 必要に応じてハイアベイラビリティ（ HA ）グループを設定します。HA グループを作成すると、複数の管理ノードとゲートウェイノードのインターフェイスがアクティブ / バックアップ構成に追加されます。クライアント接続は、 HA グループの仮想 IP アドレスを使用して確立されます。

関連情報

"StorageGRID の管理"

"テナントアカウントを使用する"

"S3 を使用する"

"Swift を使用します"

"Tenant Managerの概要"

"ネットワークの設定"

ネットワークの設定

## グリッドマネージャからさまざまなネットワーク設定を行い、 StorageGRID システムの動作を微調整できます。

ドメイン名

S3 仮想ホスト形式の要求をサポートする場合は、 S3 クライアントの接続先となるエンドポイントのドメイン名のリストを設定する必要があります。たとえば、s3.example.com、s3.example.co.uk、s3-east.example.comなどです。

設定済みのサーバ証明書とエンドポイントのドメイン名が一致している必要があります。

ハイアベイラビリティグループ

ハイアベイラビリティグループは、仮想IPアドレス（VIP）を使用してゲートウェイノードまたは管理ノードサービスへのアクティブ/バックアップアクセスを提供します。HAグループは、管理ノードとゲートウェイノード上の1つ以上のネットワークインターフェイスで構成されます。HAグループを作成するときは、グリッドネットワーク（eth0）またはクライアントネットワーク（eth2）に属するネットワークインターフェイスを選択します。

管理ネットワークではHA VIPはサポートされません。

HAグループは、グループ内のアクティブインターフェイスに追加された仮想IPアドレスを1つ以上維持します。アクティブインターフェイスが使用できなくなった場合、仮想IPアドレスは別のインターフェイスに移動します。このフェイルオーバープロセスにかかる時間は通常数秒です。クライアントアプリケーションへの影響はほとんどなく、通常の再試行で処理を続行できます。

ハイアベイラビリティ（HA）グループはいくつかの理由で使用できます。

- HA グループは、 Grid Manager または Tenant Manager への可用性の高い管理接続を提供します。
- HA グループは、 S3 / Swift クライアントに可用性の高いデータ接続を提供できます。
- インターフェイスが 1 つしかない HA グループでは、多数の VIP アドレスを指定したり、 IPv6 アドレスを明示的に設定したりできます。

リンクコスト

サイト間のレイテンシに合わせてリンクコストを調整できます。データセンターサイトが複数ある場合は、要求されたサービスを提供するデータセンターサイトの優先順位がリンクコストによって決まります。

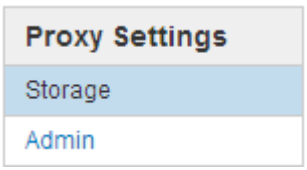
ロードバランサエンドポイント

ロードバランサを使用して、 S3 / Swift クライアントからの取り込み / 読み出しワークロードを処理できます。ロードバランシングは、複数のストレージノードにワークロードと接続を分散することで、速度と接続容量を最大化します。

管理ノードとゲートウェイノードに含まれる StorageGRID ロードバランササービスを使用する場合は、 1 つ以上のロードバランサエンドポイントを設定する必要があります。各エンドポイントは、ストレージノードへの S3 および Swift 要求に使用するゲートウェイノードまたは管理ノードポートを定義します。

プロキシ設定

S3 プラットフォームサービスまたはクラウドストレージプールを使用している場合は、ストレージノードと外部の S3 エンドポイントの間に非透過型プロキシサーバを設定できます。HTTPS または HTTP を使用して AutoSupport メッセージを送信する場合は、管理ノードとテクニカルサポートの間に非透過型プロキシサーバを設定できます。




サーバ証明書

次の2種類のサーバ証明書をアップロードできます。

- 管理インターフェイスのサーバ証明書。管理インターフェイスへのアクセスに使用される証明書です。
- オブジェクトストレージAPIサービスエンドポイントのサーバ証明書。ストレージノードに直接接続する場合、またはゲートウェイノードでCLBサービスを使用する場合に、S3およびSwiftエンドポイントを保護する証明書です。

CLB サービスは廃止されました。

ロードバランサ証明書は、ロードバランサエンドポイントのページで設定されます。キー管理サーバ（KMS）の証明書は、キー管理サーバのページで設定します。

### トラフィック分類ポリシー

トラフィック分類ポリシーを使用すると、特定のバケット、テナント、クライアントサブネット、またはロードバランサエンドポイントに関連するトラフィックなど、さまざまなタイプのネットワークトラフィックを識別して処理するためのルールを作成できます。これらのポリシーは、トラフィックの制限と監視に役立ちます。

### 信頼されていないクライアントネットワーク

クライアントネットワークを使用している場合は、各ノードのクライアントネットワークを信頼されていないものと指定することで、 StorageGRID を悪意のある攻撃から保護できます。ノードのクライアントネットワークが信頼されていない場合、ノードはロードバランサエンドポイントとして明示的に設定されたポートのインバウンド接続だけを受け入れます。

たとえば、 HTTPS S3 要求を除くクライアントネットワーク上のすべてのインバウンドトラフィックをゲートウェイノードで拒否できます。あるいは、ストレージノードからの S3 プラットフォームサービスのアウトバウンドトラフィックを有効にして、クライアントネットワークでのそのストレージノードへのインバウンド接続を禁止することができます。

### 関連情報

"StorageGRID の管理"

"テナントとクライアント接続の管理"

## システム設定を構成しています

グリッドマネージャからさまざまなシステム設定を行い、 StorageGRID システムの動作を微調整できます。

### 表示オプション

表示オプションでは、ユーザセッションのタイムアウト時間を指定したり、レガシーアラームやイベントトリガー型 AutoSupport メッセージに関する E メール通知を停止したりできます。

### グリッドオプション

グリッドオプションを使用すると、 StorageGRID システムに格納されているすべてのオブジェクトについて、格納オブジェクトの圧縮や格納オブジェクトの暗号化などの設定を行うことができます。設定を行うことができます。

これらのオプションを使用して、 S3 および Swift クライアント処理のグローバル設定を指定することもできます。

### キー管理サーバ

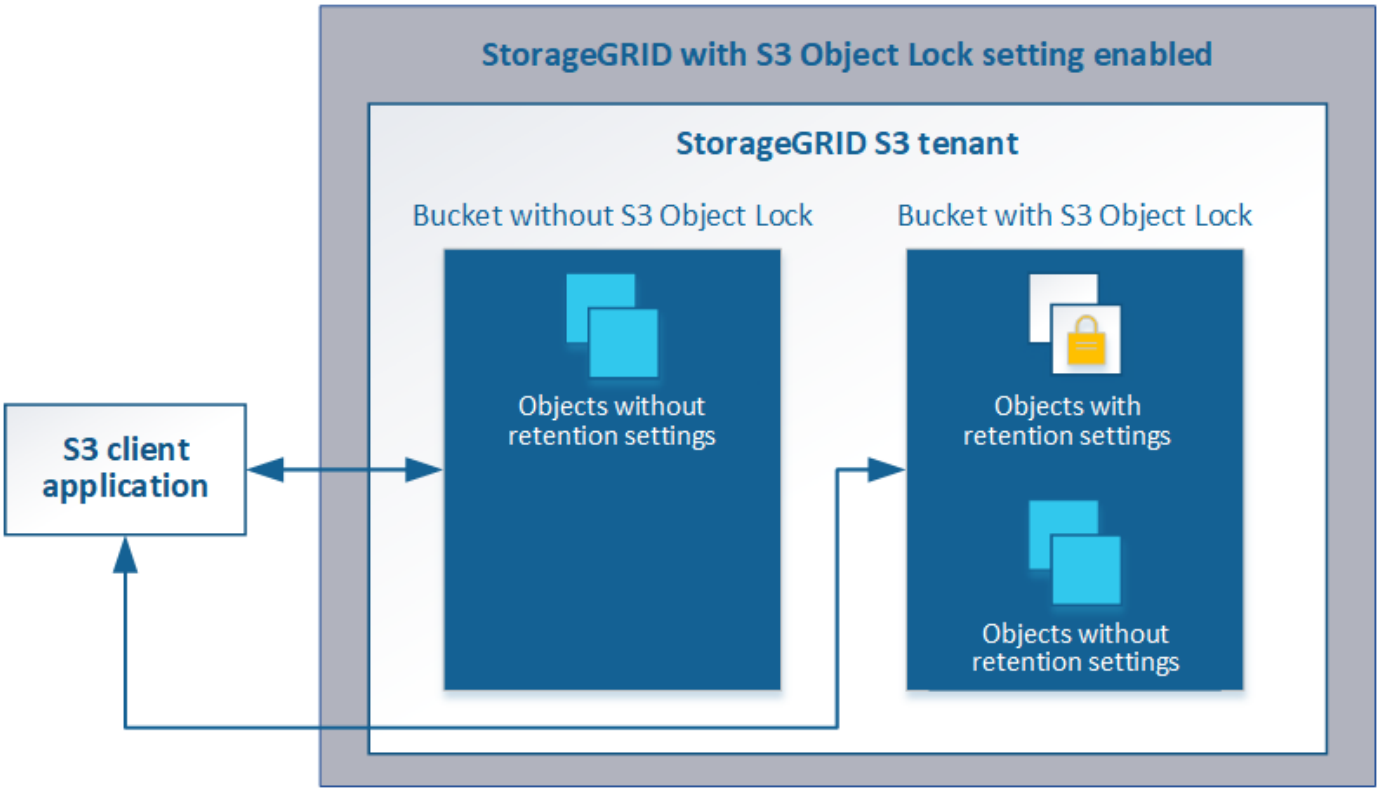
1 つ以上の外部キー管理サーバ（ KMS ）を設定して、 StorageGRID サービスとストレージアプライアンスに暗号化キーを提供できます。KMS や KMS の各クラスタは、 Key Management Interoperability Protocol （ KMIP ）を使用して、関連する StorageGRID サイトにあるアプライアンスノードに暗号化キーを提供します。キー管理サーバを使用すると、アプライアンスをデータセンターから削除した場合でも StorageGRID データを保護できます。アプライアンスのボリュームを暗号化すると、ノードが KMS と通信できないかぎり、

アプライアンスのデータにアクセスすることはできません。

暗号化キー管理を使用するには、インストール時にアプライアンスをグリッドに追加する前に、アプライアンスごとに * Node Encryption * の設定を有効にする必要があります。

**S3** オブジェクトのロック

StorageGRID S3 オブジェクトロック機能は、 Amazon Simple Storage Service （ Amazon S3 ）での S3 オブジェクトロックに相当するオブジェクト保護解決策 です。StorageGRID システムに対してグローバルな S3 オブジェクトロック設定を有効にすると、 S3 テナントアカウントで S3 オブジェクトのロックを有効にした状態でバケットを作成できるようになります。テナントは、 S3 クライアントアプリケーションを使用して、オプションでバケット内のオブジェクトの保持設定（終了日、リーガルホールド、またはその両方）を指定できます。




ストレージオプション

ストレージオプションでは、オブジェクトのセグメント化を制御したり、ストレージのウォーターマークを定義してストレージノードの使用可能なストレージスペースを管理したりできます。

情報ライフサイクル管理の使用

情報ライフサイクル管理（ ILM ）を使用して、 StorageGRID システム内のすべてのオブジェクトの配置、期間、データ保護を制御します。ILM ルールは、 StorageGRID が時間の経過に伴ってオブジェクトを格納する方法を決定します1 つ以上の ILM ルールを設定して ILM ポリシーに追加します。

ILM ルールでは次の項目を定義

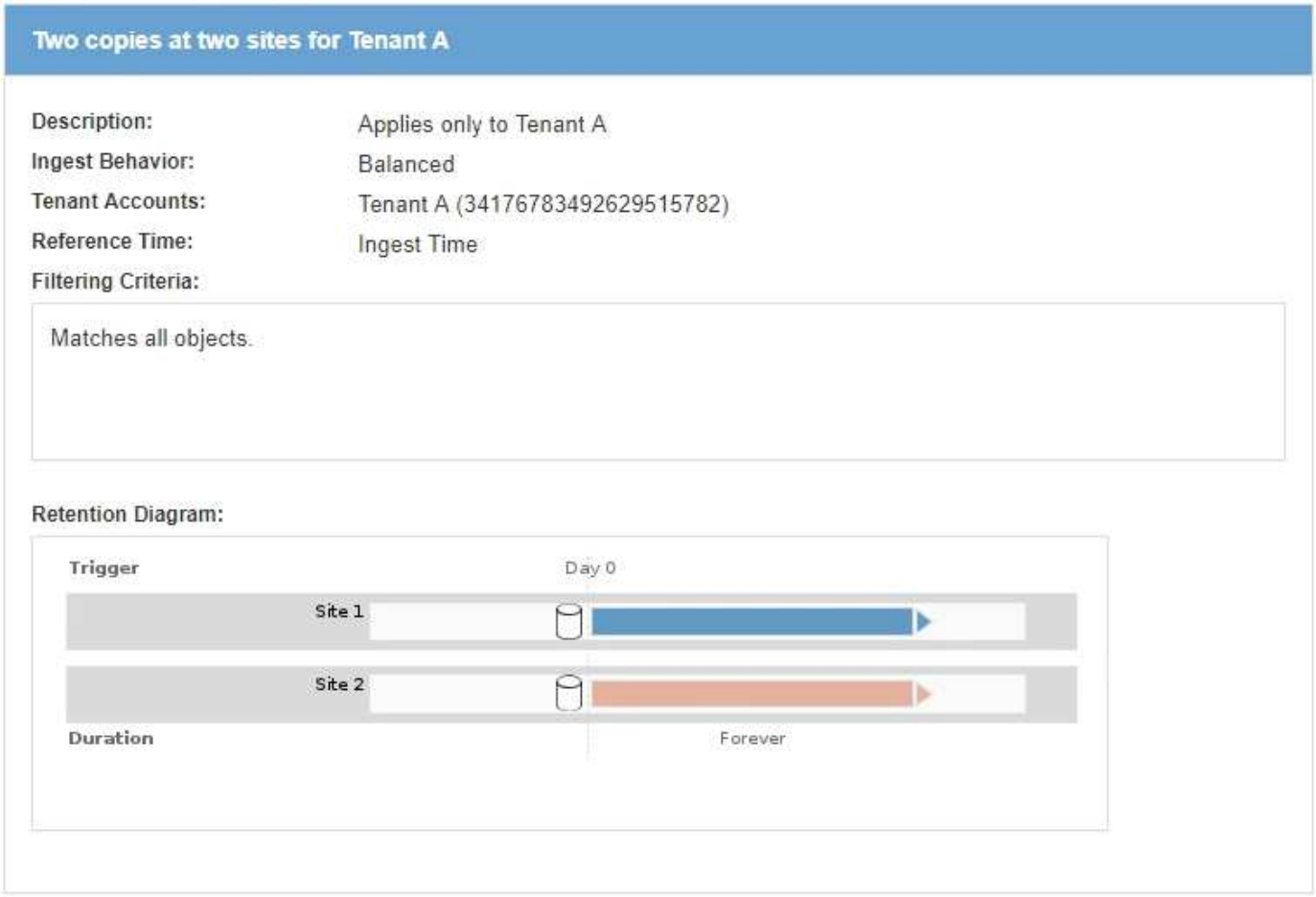
- 格納するオブジェクト。ルールはすべてのオブジェクトに適用することも、ルール環境 を構成するオブジェクトを特定するフィルタを指定することもできます。たとえば、特定のテナントアカウント、特定の S3 バケットまたは Swift コンテナ、または特定のメタデータ値に関連付けられたオブジェクトにのみルールを適用できます。
- ストレージのタイプと場所。オブジェクトは、ストレージノード、クラウドストレージプール、またはアーカイブノードに格納できます。
- 作成するオブジェクトコピーのタイプ。コピーはレプリケートまたはイレイジャーコーディングできます。
- レプリケートコピーの場合は、作成されるコピーの数。
- イレイジャーコーディングコピーにはイレイジャーコーディングスキームを使用します。
- オブジェクトのストレージの場所とコピーのタイプの経時的変化。
- オブジェクトがグリッドに取り込まれるときにオブジェクトデータを保護する方法（同期配置またはデュアルコミット）。

オブジェクトメタデータは ILM ルールによって管理されません。代わりに、オブジェクトメタデータはメタデータストア内の Cassandra データベースに格納されます。データを損失から保護するために、オブジェクトメタデータの 3 つのコピーが各サイトで自動的に維持されます。コピーはすべてのストレージノードに均等に分散されます。

#### **ILM** ルールの例

次の ILM ルールの例では、テナント A に属するオブジェクトの環境 を設定しますこれらのオブジェクトのレプリケートコピーを 2 つ作成し、各コピーを別々のサイトに格納します。この 2 つのコピーは「無期限」に保持されます。つまり、 StorageGRID はこれらのコピーを自動的に削除しません。これらのオブジェクトは、クライアントの削除要求によって削除されるか、バケットライフサイクルが終了するまで、StorageGRID によって保持されます。

このルールでは、取り込み動作に Balanced オプションが使用されます。 2 つのサイトの配置手順は、テナント A がオブジェクトを StorageGRID に保存するとすぐに適用されます。ただし、両方の必要なコピーをただちに作成することはできません。たとえば、テナント A がオブジェクトを保存したときにサイト 2 に到達できない場合、 StorageGRID はサイト 1 のストレージノードに 2 つの中間コピーを作成します。サイト 2 が使用可能になると、 StorageGRID はそのサイトで必要なコピーを作成します。




**ILM** ポリシーによるオブジェクトの評価方法

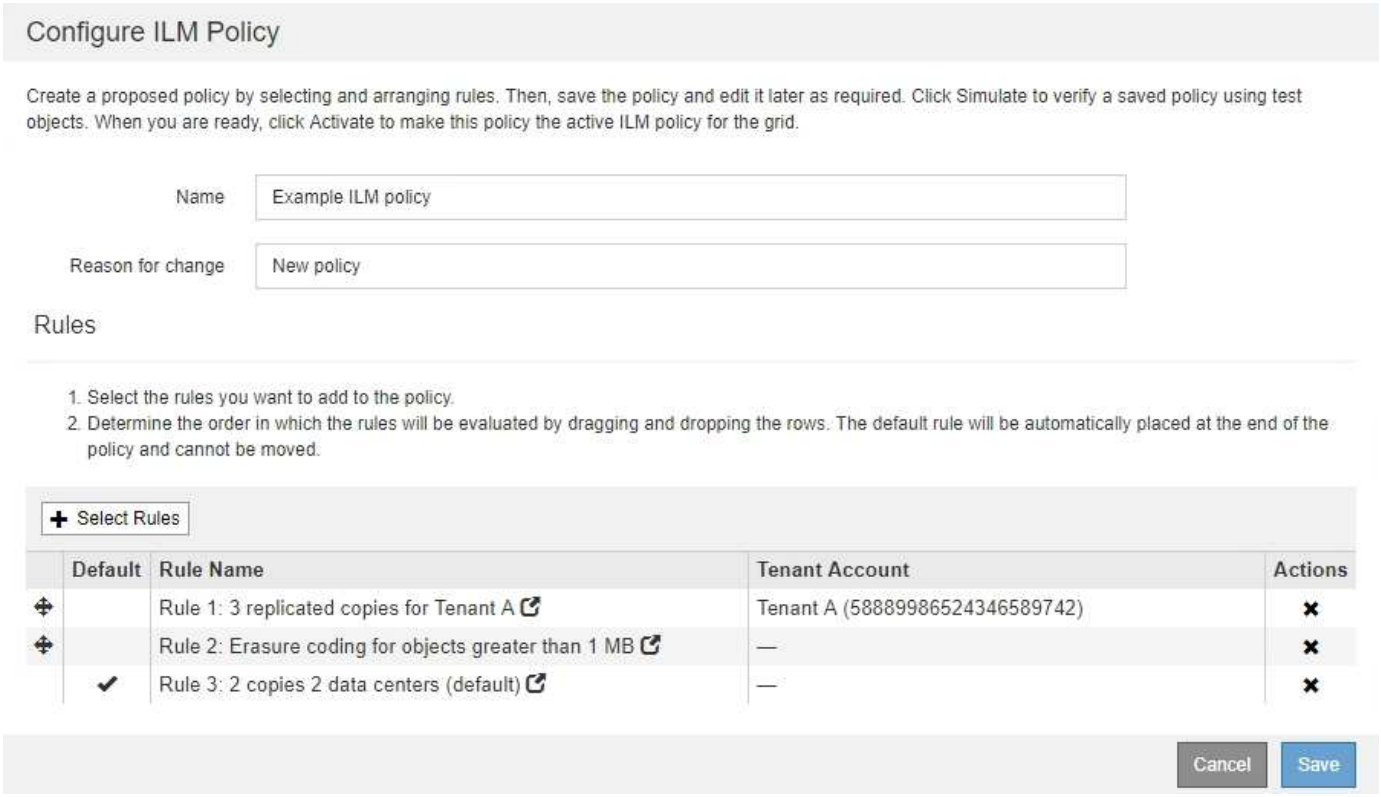
StorageGRID システムのアクティブな ILM ポリシーは、すべてのオブジェクトの配置、期間、データ保護を制御します。

クライアントがオブジェクトを StorageGRID に保存すると、オブジェクトはアクティブポリシー内の順序付けられた ILM ルールに照らして次のように評価されます。

1. ポリシー内の最初のルールのフィルタがオブジェクトに一致すると、オブジェクトはそのルールの取り込み動作に従って取り込まれ、そのルールの配置手順に従って格納されます。
2. 最初のルールのフィルタがオブジェクトに一致しない場合、オブジェクトは一致が見つかるまでポリシー内の後続の各ルールに照らして評価されます。
3. どのルールもオブジェクトに一致しない場合は、ポリシー内のデフォルトルールの取り込み動作と配置手順が適用されます。デフォルトルールはポリシー内の最後のルールであり、フィルタは使用できません。

**ILM** ポリシーの例

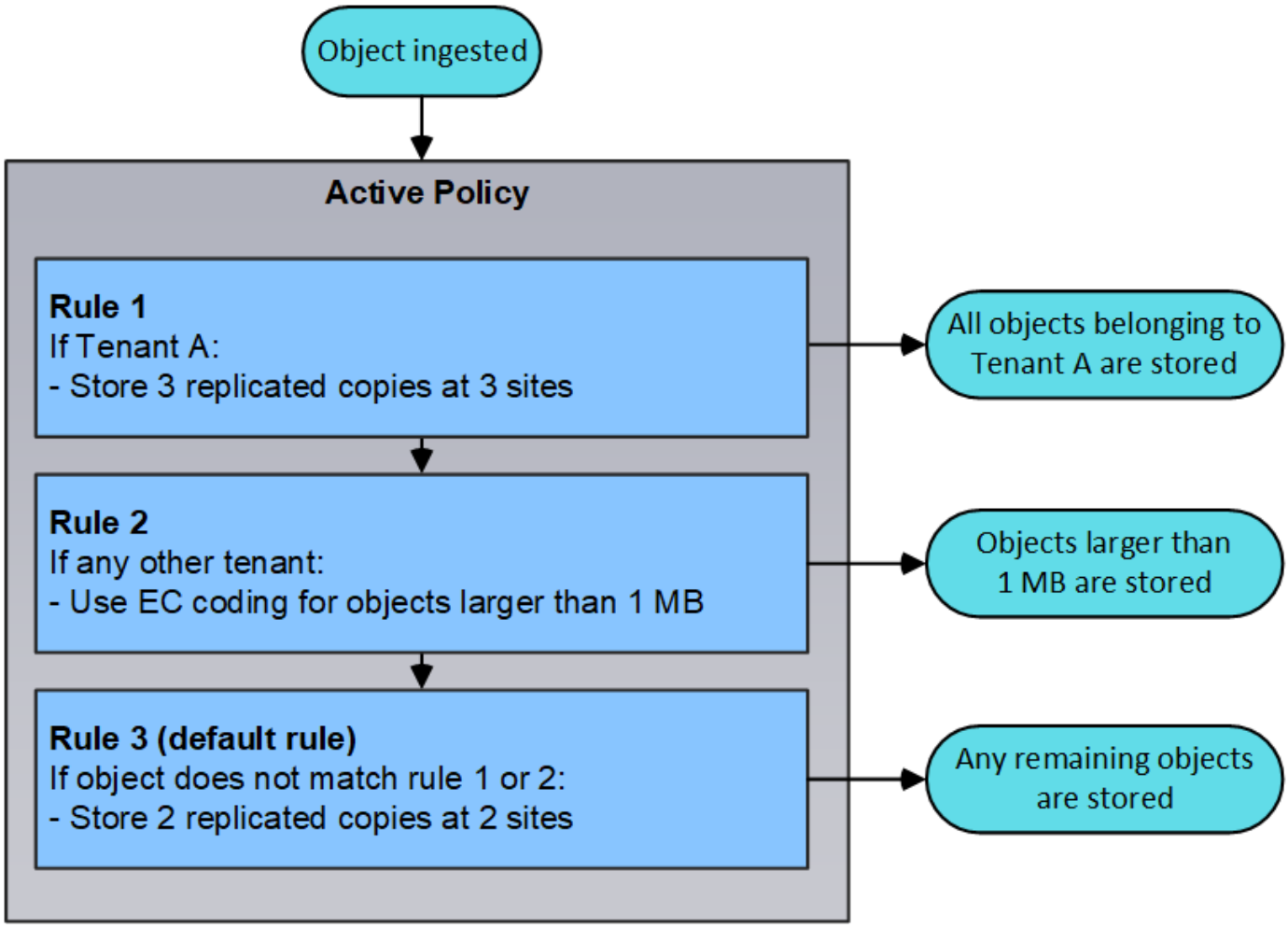
この例の ILM ポリシーは 3 つの ILM ルールを使用します。




この例では、ルール 1 はテナント A に属するすべてのオブジェクトに一致しますこれらのオブジェクトは、3 つのサイトに 3 つのレプリケートコピーとして格納されます。他のテナントに属するオブジェクトはルール 1 に一致しないため、ルール 2 に照らして評価されます。

ルール2では、他のテナントのすべてのオブジェクトが一致しますが、1MBより大きいオブジェクトのみが該当します。これらのオブジェクトは、 3 つのサイトで 6+3 のイレイジャーコーディングを使用して格納されます。ルール 2 がオブジェクト 1MB 以下に一致しないため、これらのオブジェクトはルール 3 に照らして評価されます。

ルール 3 はポリシー内の最後のルールで、デフォルトのルールであり、フィルタは使用しません。ルール 3 では、ルール 1 またはルール 2 に一致しないすべてのオブジェクトのレプリケートコピーを 2 つ作成します（ 1MB 以下のテナント A に属していないオブジェクト）。




- 関連情報 *

"ILM を使用してオブジェクトを管理する"

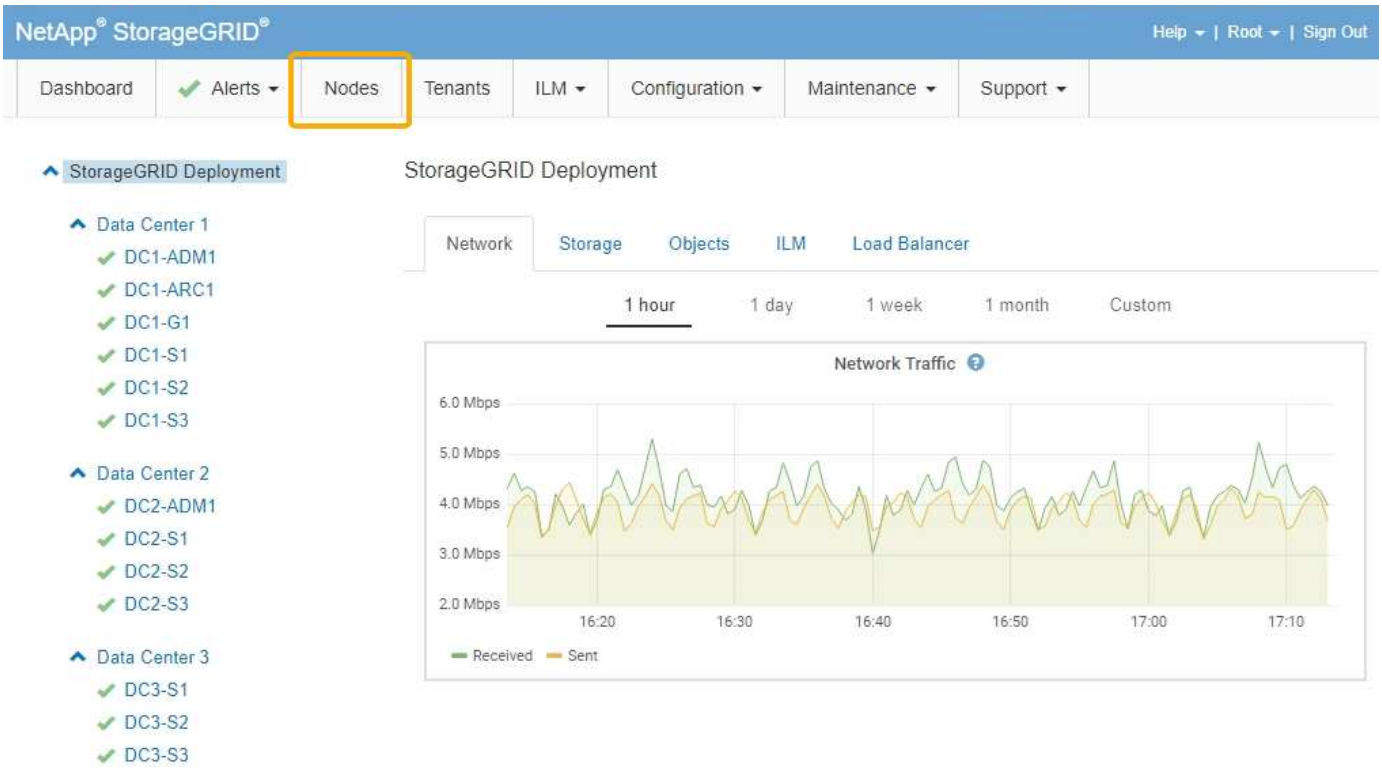
**StorageGRID** 処理の監視

Grid Managerでは、StorageGRID システムの日 々 のアクティビティを監視するための、健常性を含む情報を提供します。

- "Nodesページを表示します"
- "アラートの監視と管理"
- "SNMPによる監視を使用する"
- "監査メッセージの確認"

**Nodes**ページを表示します

StorageGRID システムに関する詳しい情報がダッシュボードに表示されるよりも必要な場合は、ノードページを使用して、グリッド全体、グリッド内の各サイト、およびサイトの各ノードの指標を表示できます。




左側のツリービューには、StorageGRID システム内のすべてのサイトおよびすべてのノードが表示されます。各ノードのアイコンは、ノードが接続されているかどうか、またはアクティブなアラートがあるかどうかを示します。

接続状態アイコン

ノードがグリッドから切断されている場合、ツリービューには、基盤となるアラートのアイコンではなく、青またはグレーの接続状態アイコンが表示されます。

- * 接続されていません - 不明 * ：不明な理由でノードがグリッドに接続されていません。たとえば、ノード間のネットワーク接続が失われた、電源が切れたなどの原因が考えられます。* Unable to communicate with node * アラートがトリガーされる場合もあります。他のアラートもアクティブになる可能性があります。この状況にはすぐに対処する必要があります。

> 管理されたシャットダウン処理の実行中に、ノードが Unknown と表示されることがありますこのような場合、 Unknown 状態は無視してかまいません。

- * 接続されていません - 管理上の理由により停止して ：ノードが想定される理由でグリッドに接続されていません。たとえば、ノードまたはノード上のサービスが正常にシャットダウンされた、ノードがリブート中である、ソフトウェアのアップグレード中であるなどの原因が考えられます。1 つ以上のアラートがアクティブになっている可能性もあります。

警告アイコン

ノードがグリッドに接続されている場合、ノードに現在アラートがあるかどうかに応じて、ツリービューには次のアイコンのいずれかが表示されます。

- * 重要 * ：異常な状態で、 StorageGRID のノードやサービスの通常の動作が停止しています。基盤となる問題 にすぐに対処する必要があります。問題 が解決されないと、サービスの停止やデータの損失を招くおそれがあります。

- * メジャー * ：異常な状態で、現在の処理に影響しているか、重大アラートのしきい値に近づいています。Major アラートを調査し、根本的な問題に対処して、異常な状態が発生した場合に StorageGRID のノードやサービスが正常に動作しなくなる事態を防ぐ必要があります。
- * マイナー * ：システムは正常に動作していますが、継続するとシステムの動作に影響する可能性がある異常な状態が発生しています。自動的にクリアされない Minor アラートを監視し、解決して、深刻な問題が生じないようにする必要があります。
- * 標準 * ：アクティブなアラートはなく、ノードがグリッドに接続されています。

システム、サイト、またはノードの詳細を表示する

利用可能な情報を表示するには、左側の該当するリンクをクリックします。

- グリッド名を選択すると、 StorageGRID システム全体の統計が要約して表示されます。（スクリーンショットには、 StorageGRID Deployment という名前のシステムが示されています）。
- 特定のデータセンターサイトを選択すると、そのサイトのすべてのノードの統計が要約して表示されます。
- 特定のノードを選択すると、そのノードの詳細情報が表示されます。

関連情報

"トラブルシューティングを監視します"

**Nodes** ページのタブ

ノード（ Nodes ）ページの上部にあるタブは、左側のツリーから選択した内容に基づいています。

| タブ名 | 説明 | に含まれます |
| --- | --- | --- |
| 概要 | • 各ノードの基本情報が表示されます。<br>• ノードに影響を与えている未確認のアラームが表示されます。 | すべてのノード |
| ハードウェア | • 各ノードの CPU 利用率とメモリの使用状況が表示されます<br>• アプライアンスノードについては、ハードウェア情報も表示されます。 | すべてのノード |
| ネットワーク | ネットワークインターフェイス間で送受信されるネットワークトラフィックを示すグラフが表示されます。 | すべてのノード、各サイト、グリッド全体 |

| タブ名 | 説明 | に含まれます |
| --- | --- | --- |
| ストレージ | • 各ノードのディスクデバイスとボリュームの詳細が表示されます。<br>• ストレージノード、各サイト、およびグリッド全体の場合、オブジェクトデータストレージとメタデータストレージの使用量の推移を示すグラフが表示されます。 | すべてのノード、各サイト、グリッド全体 |
| イベント | ネットワークエラーなどのエラーを含む、システムエラーまたは障害イベントの数を表示します。 | すべてのノード |
| オブジェクト | • S3 および Swift の取り込み速度と読み出し速度に関する情報が表示されます。<br>• ストレージノードの場合、オブジェクト数や、メタデータストアのクエリとバックグラウンド検証に関する情報が表示されます。 | ストレージノード、各サイト、グリッド全体 |
| ILM | 情報ライフサイクル管理（ ILM ）処理に関する情報が表示されます。<br>• ストレージノードの場合、 ILM 評価およびイレイジャーコーディングオブジェクトのバックグラウンド検証に関する詳細が表示されます。<br>• 各サイトおよびグリッド全体の場合、 ILM キューの状況の推移を示すグラフが表示されます。<br>• グリッド全体の場合、 ILM によるすべてのオブジェクトのフルスキャンが完了するまでの推定時間が表示されます。 | ストレージノード、各サイト、グリッド全体 |
| ロードバランサ | ロードバランササービスに関連するパフォーマンスグラフと診断グラフが表示されます。<br>• 各サイトの場合、そのサイトのすべてのノードの統計が要約して表示されます。<br>• グリッド全体の場合、すべてのサイトの統計が要約して表示されます。 | 管理ノードとゲートウェイノード、各サイト、およびグリッド全体 |
| プラットフォームサービス | サイトでの S3 プラットフォームサービスの処理に関する情報が表示されます。 | 各サイト |

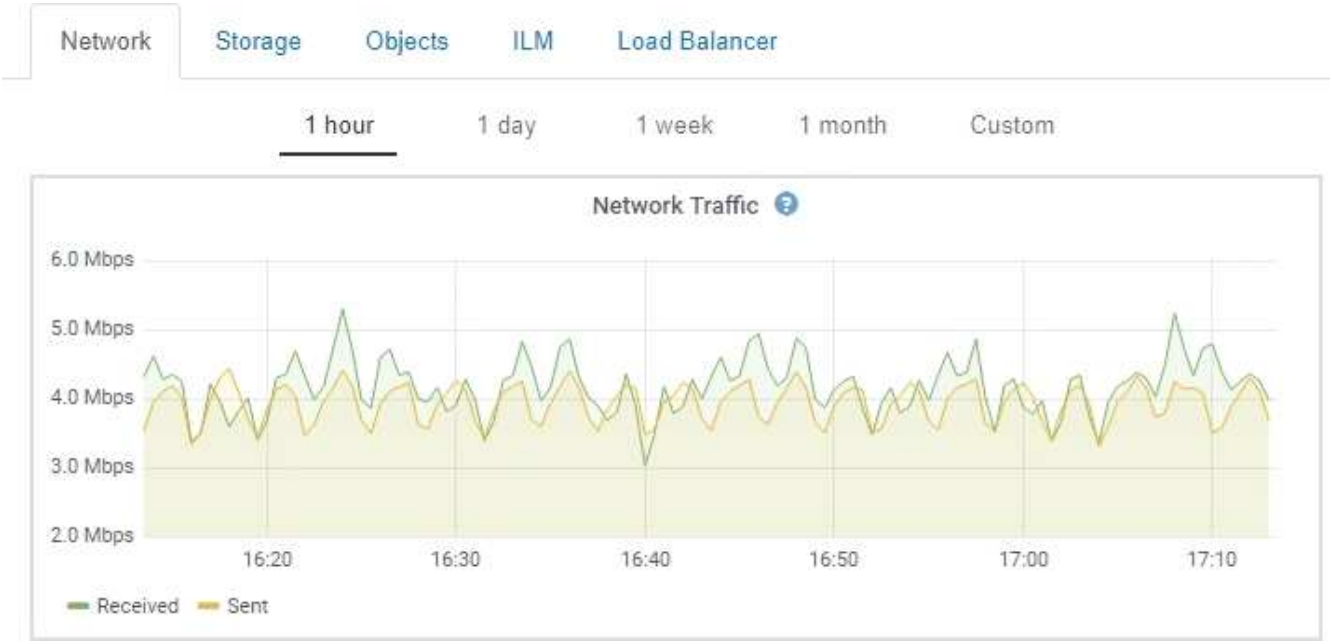
| タブ名 | 説明 | に含まれます |
| --- | --- | --- |
| SANtricity システムマネージャ | SANtricity システムマネージャへのアクセスを許可します。SANtricity System Manager では、ストレージコントローラのハードウェア診断および環境情報と、ドライブに関連する問題を確認できます。 | ストレージアプライアンスノード<br><br>*注：*ストレージ・アプライアンスのコントローラ・ファームウェアが8.70未満の場合、SANtricity のSystem Managerタブは表示されません。 |

**Prometheus** 指標

## 管理ノードの Prometheus サービスは、すべてのノード上のサービスから時系列の指標を収集します。

Prometheus で収集された指標は、 Grid Manager のさまざまな場所で使用されます。

- * Nodes ページ * ： Nodes ページで使用できるタブのグラフとチャートでは、 Grafana 視覚化ツールを使用して、 Prometheus で収集された時系列の指標を表示します。Grafana はグラフ形式とチャート形式で時系列のデータを表示し、 Prometheus はバックエンドのデータソースとして機能します。




- * アラート * ： Prometheus 指標を使用するアラートルールの条件が true と評価されると、特定の重大度レベルでアラートがトリガーされます。
- * グリッド管理 API * ： Prometheus 指標をカスタムのアラートルールまたは外部の自動化ツールで使用して、 StorageGRID システムを監視できます。Prometheus指標の完全なリストは、グリッド管理API（* Help > API Documentation > Metrics *）で入手できます。使用可能な指標の数は1、000を超えますが、StorageGRID の最も重要な処理を監視するために必要な指標は比較的少数です。

名前に *private* が含まれる指標は内部専用です。 StorageGRID のリリースごとに予告なく変更されることがあります。

- サポート*>*ツール*>*診断*ページと*サポート*>*ツール*>*メトリクス*ページ：これらのページは主にテクニカルサポートが使用するためのもので、Prometheus指標の値を使用する多数のツールとグラフを提供します。

[Metrics] ページの一部の機能やメニュー項目は意図的に機能しないため、変更される場合があります。

関連情報

"アラートの監視と管理"

"StorageGRID サポートオプションを使用する"

"トラブルシューティングを監視します"

**StorageGRID** 属性

属性は、 StorageGRID システムの多くの機能について、値とステータスを報告します。属性値は、グリッドノードごと、サイトごと、およびグリッド全体について収集されます。

StorageGRID 属性は、グリッドマネージャのさまざまな場所で使用されます。

- * Nodes ページ * ： Nodes ページに表示される値の多くは StorageGRID 属性です。（ Prometheus 指標はノードのページにも表示されます）。
- * アラーム * ：属性が定義されたしきい値に達すると、特定の重大度レベルで StorageGRID アラーム（レガシーシステム）がトリガーされます。
- グリッドトポロジツリー：属性値はグリッドトポロジツリー（* Support > Tools > Grid Topology *）に表示されます。
- * Events * ：システムイベントは、特定の属性がネットワークエラーなどのエラーや障害をノードに記録したときに発生します。

属性値

属性のレポートはベストエフォートベースで行われ、 100% 正確とは限りません。サービスのクラッシュ時や障害が発生したグリッドノードのリビルド中など、一部の状況では属性の更新が失われることがあります。

また、伝播にかかる時間により、属性のレポート作成に遅れが生じることがあります。ほとんどの属性については、更新された値は一定の間隔で StorageGRID システムに送信されます。更新がシステムで認識されるまでに数分かかる場合があり、ほぼ同時に行った 2 つの属性変更が同時に報告されないこともあります。

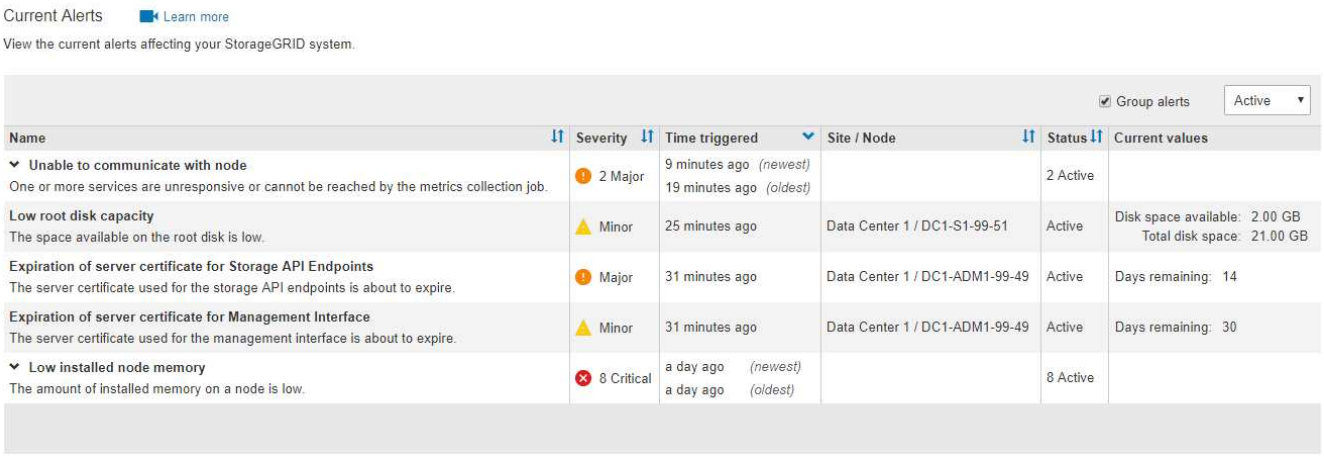
関連情報

"トラブルシューティングを監視します"

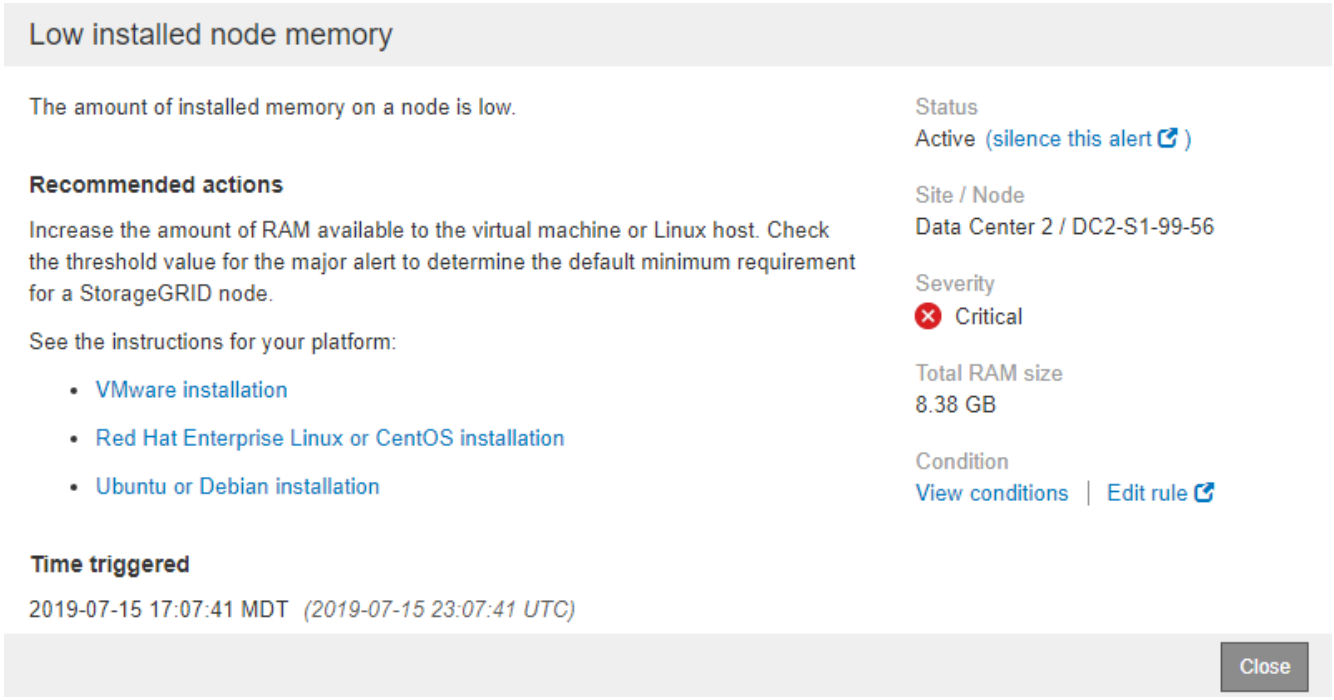
# アラートシステムでは、 StorageGRID の運用中に発生する問題を、使いやすいインターフェイスを通じて検出し、評価し、解決することができます。

アラートシステムは、 StorageGRID システムで発生する可能性のある問題を監視する主要なツールです。

- アラートシステムは、システムで実行可能な問題に焦点を当てます。アラートは、無視しても安全なイベントではなく、すぐに対処が必要なイベントに対してトリガーされます。
- Current Alerts （現在のアラート）ページと Resolved Alerts （解決済みアラート）ページは、現在および過去の問題を表示するための使いやすいインターフェイスです。リストは、個々のアラートやアラートグループでソートできます。たとえば、すべてのアラートをノード / サイトでソートして、特定のノードに影響しているアラートを確認できます。または、グループ内のアラートを時間でソートして、特定のアラートの最新のインスタンスを確認することもできます。
- 同じ種類の複数のアラートが 1 つの E メールにグループ化され、通知の数が削減されます。また、同じタイプの複数のアラートが、現在のアラートおよび解決済みのアラートページにグループとして表示されます。アラートグループを展開または縮小すると、個々のアラートの表示と非表示を切り替えることができます。たとえば、複数のノードが「 Unable to communicate with node * 」アラートを報告している場合、送信される E メールは 1 通だけで、現在のアラートページにはグループとして表示されます。




- アラートには、問題の内容をより迅速に把握できるように、わかりやすい名前と説明が使用されます。アラート通知には、影響を受けるノードとサイトに関する詳細、アラートの重大度、アラートルールがトリガーされた時刻、およびアラートに関連する指標の現在の値が含まれます。
- アラート E メール通知および現在のアラートおよび解決済みアラートのページに表示されるアラートリストは、アラートを解決するための推奨される対処方法を提供します。これらの対処方法には、 StorageGRID のマニュアルへの直接リンクが含まれていることが多く、より詳細なトラブルシューティング手順を見つけてアクセスしやすくなっています。




従来のアラームシステムは引き続きサポートされますが、アラートシステムには大きなメリットがあり、使いやすくなっています。

アラートの管理

すべての StorageGRID ユーザがアラートを表示できます。Root Access 権限または Manage Alerts 権限がある場合は、次のようにアラートを管理することもできます。

- あるアラートのいくつかの重大度の通知を一時的に停止する必要がある場合は、特定のアラートルールを簡単に一定期間サイレント化することができます。アラートルールは、グリッド全体、単一サイト、または単一ノードでサイレント化できます。
- 必要に応じてデフォルトのアラートルールを編集できます。アラートルールは完全に無効にすることも、トリガー条件と期間を変更することもできます。
- 環境に応じた特定の条件を対象にカスタムのアラートルールを作成して、独自の対処方法を提供できます。カスタムアラートの条件を定義するには、グリッド管理 API の指標セクションで使用できる Prometheus 指標を使用して式を作成します。

  たとえば次の式では、あるノードに搭載された RAM の容量が 24 、 000 、 000 、 000 バイト（ 24GB ）未満である場合にアラートがトリガーされます。

```
node_memory_MemTotal < 24000000000
```

- 関連情報 *

"トラブルシューティングを監視します"

# 簡易ネットワーク管理プロトコル（ SNMP ）を使用して StorageGRID を監視する場合は、グリッドマネージャを使用して SNMP エージェントを設定できます。

各 StorageGRID ノードは、管理情報ベース（ MIB ）を提供する SNMP エージェントまたはデーモンを実行します。StorageGRID の MIB には、アラートおよびアラームのテーブルおよび通知定義が含まれています。各 StorageGRID ノードは MIB-II オブジェクトのサブセットもサポートしています。

最初は、すべてのノードで SNMP が無効になっています。SNMP エージェントを設定すると、すべての StorageGRID ノードに同じ設定が適用されます。

StorageGRID SNMP エージェントは、 3 つのバージョンの SNMP プロトコルをすべてサポートします。エージェントは、クエリに対して読み取り専用 MIB アクセスを提供し、次の 2 種類のイベントベース通知を管理システムに送信できます。

- * トラップ * は、管理システムによる確認応答を必要としない SNMP エージェントによって送信される通知です。トラップは、アラートがトリガーされているなど、 StorageGRID 内で何らかの問題が発生したことを管理システムに通知するために使用されます。トラップは、 SNMP の 3 つのバージョンすべてでサポートされています。
- * informs * はトラップに似ていますが、管理システムからの確認応答が必要です。SNMP エージェントが一定時間内に確認応答を受信しなかった場合、確認応答を受信するか、最大再試行値に達するまで、通知を再送信します。インフォームは SNMPv2c および SNMPv3 でサポートされます。

トラップ通知およびインフォーム通知は、次の場合に送信されます。

- デフォルトまたはカスタムのアラートはいずれかの重大度レベルでトリガーされます。アラートの SNMP 通知を停止するには、アラートのサイレンスを設定する必要があります。アラート通知は、優先送信者として設定された管理ノードから送信されます。
- 特定のアラーム（従来型システム）は、指定した重大度レベル以上でトリガーされます。

> SNMP 通知は、すべてのアラームまたはすべてのアラーム重大度について送信されるわけではありません。

- 関連情報 *

"トラブルシューティングを監視します"



# 監査メッセージは、 StorageGRID システムの詳細な運用状況を的確に把握するために役立ちます。監査ログを使用して、問題のトラブルシューティングやパフォーマンスの評価を行うことができます。

通常のシステム運用中、すべての StorageGRID サービスは次の監査メッセージを生成します。

- システム監査メッセージは、監査システム自体、グリッドノードの状態、システム全体のタスクアクティビティ、およびサービスバックアップ処理に関連します。
- オブジェクトストレージの監査メッセージは、オブジェクトの格納と読み出し、グリッドノードからグリッドノードへの転送、検証など、 StorageGRID 内のオブジェクトの格納と管理に関連します。

- クライアント読み取り / 書き込み監査メッセージは、 S3 または Swift クライアントアプリケーションがオブジェクトの作成、変更、または読み出しの要求を行うときに記録されます。
- 管理監査メッセージには、管理 API に対するユーザ要求が記録されます。

各管理ノードで、監査メッセージがテキストファイルに保存されます。監査共有には、アクティブファイル（ audit.log ）と、圧縮された過去の監査ログが含まれています。

監査ログへのアクセスを簡単にするためには、NFSとCIFSの両方についてクライアントから監査共有へのアクセスを設定します（現在CIFSは廃止）。管理ノードのコマンドラインから直接監査ログファイルにアクセスすることもできます。

監査ログファイル、監査メッセージの形式、監査メッセージの種類、および監査メッセージを分析するためのツールの詳細については、監査メッセージに関する手順を参照してください。監査クライアントアクセスの設定方法については、 StorageGRID の管理手順を参照してください。

関連情報

"監査ログを確認します"

"StorageGRID の管理"

メンテナンス手順の実行

StorageGRID システムを最新の状態に保ち、効率的に実行するために、さまざまなメンテナンス手順を実行します。Grid Manager には、メンテナンスタスクを実行するプロセスを支援するツールとオプションが用意されている。

ソフトウェアの更新

Grid Manager の Software Update ページでは、次の 3 種類のソフトウェア更新を実行できます。

- StorageGRID ソフトウェアのアップグレード
- StorageGRID ホットフィックス
- SANtricity OS のアップグレード

**StorageGRID** ソフトウェアのアップグレード

新しい StorageGRID 機能リリースが利用可能になったときは、ソフトウェアアップグレードページの指示に従って、必要なファイルをアップロードし、 StorageGRID システムをアップグレードします。プライマリ管理ノードから、すべてのデータセンターサイトのすべてのグリッドノードをアップグレードする必要があります。

StorageGRID ソフトウェアのアップグレード中も、クライアントアプリケーションはオブジェクトデータの取り込みと読み出しを継続できます。

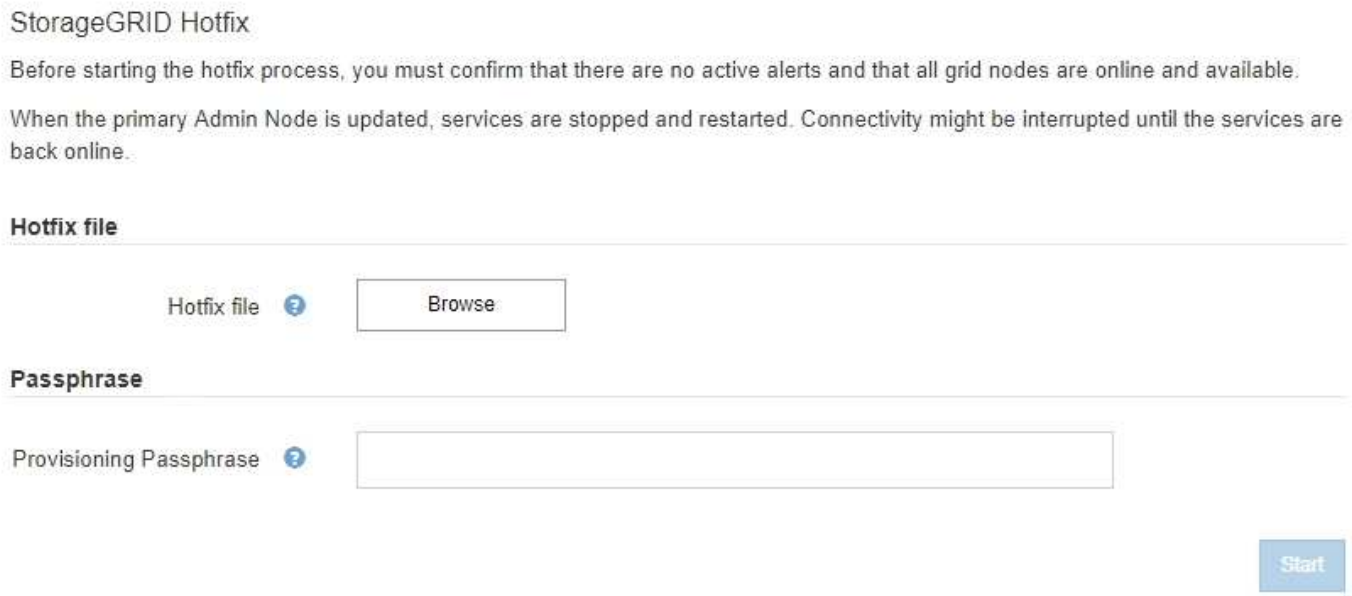
ホットフィックス

次のフィーチャーリリースまでの間にソフトウェアの問題が検出されて解決された場合は、 StorageGRID システムにホットフィックスを適用する必要があります。

StorageGRID のホットフィックスには、フィーチャーパックまたはフィーチャーパックに含まれないソフト

ウェアの変更が含まれます。今後のリリースにも同じ変更が含まれます。

以下に示す StorageGRID ホットフィックスページでは、ホットフィックスファイルをアップロードできます。



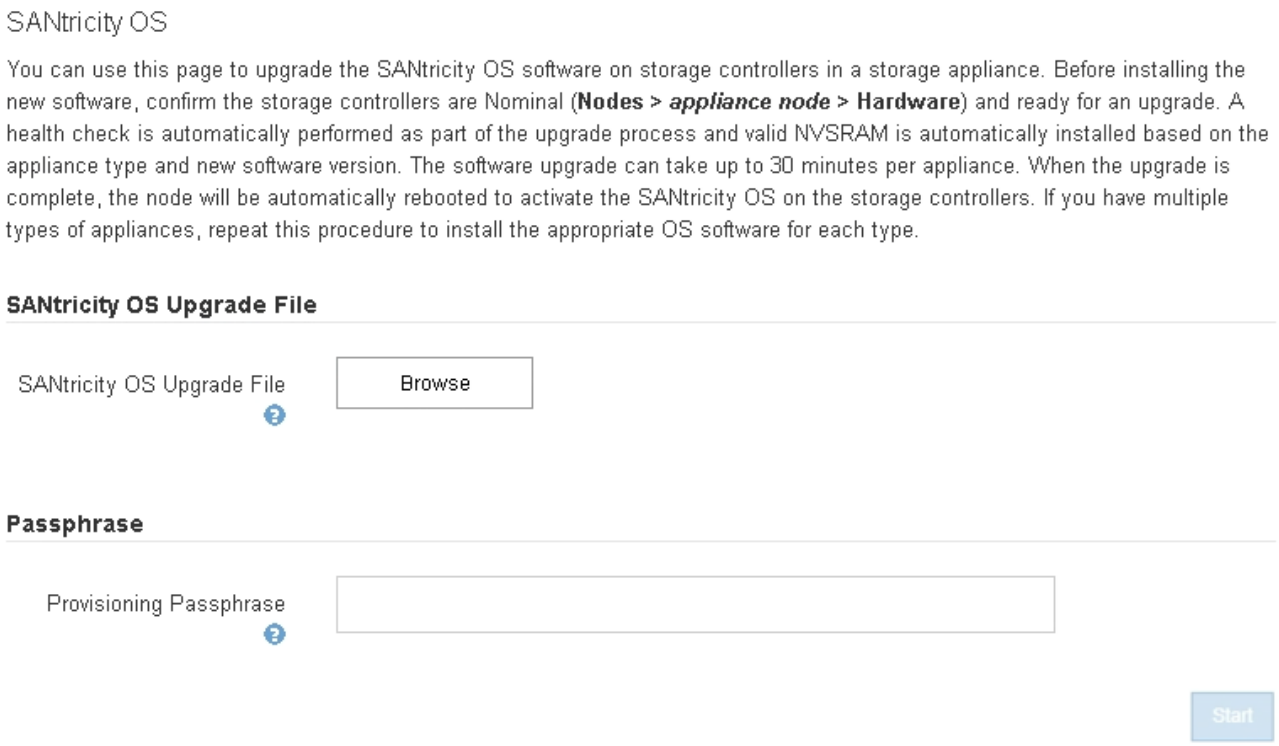

ホットフィックスは、最初にプライマリ管理ノードに適用されます。その後、 StorageGRID システム内のすべてのノードで同じソフトウェアバージョンが実行されるまで、他のグリッドノードへのホットフィックスの適用を承認する必要があります。個々のグリッドノード、グリッドノードのグループ、またはすべてのグリッドノードを選択して、承認順序をカスタマイズできます。

新しいバージョンのホットフィックスによってすべてのグリッドノードが更新されますが、ホットフィックスの実際の変更内容が、特定のタイプのノードの特定のサービスにしか影響しない場合があります。たとえば、あるホットフィックスが、ストレージノード上の LDR サービスにしか影響しない場合があります。

**SANtricity OS** のアップグレード

ストレージアプライアンスのストレージコントローラが適切に機能しない場合は、コントローラの SANtricity OS ソフトウェアのアップグレードが必要となることがあります。SANtricity OS ファイルを StorageGRID システムのプライマリ管理ノードにアップロードし、 Grid Manager からアップグレードを適用できます。

以下の SANtricity ページでは、 SANtricity OS アップグレードファイルをアップロードできます。

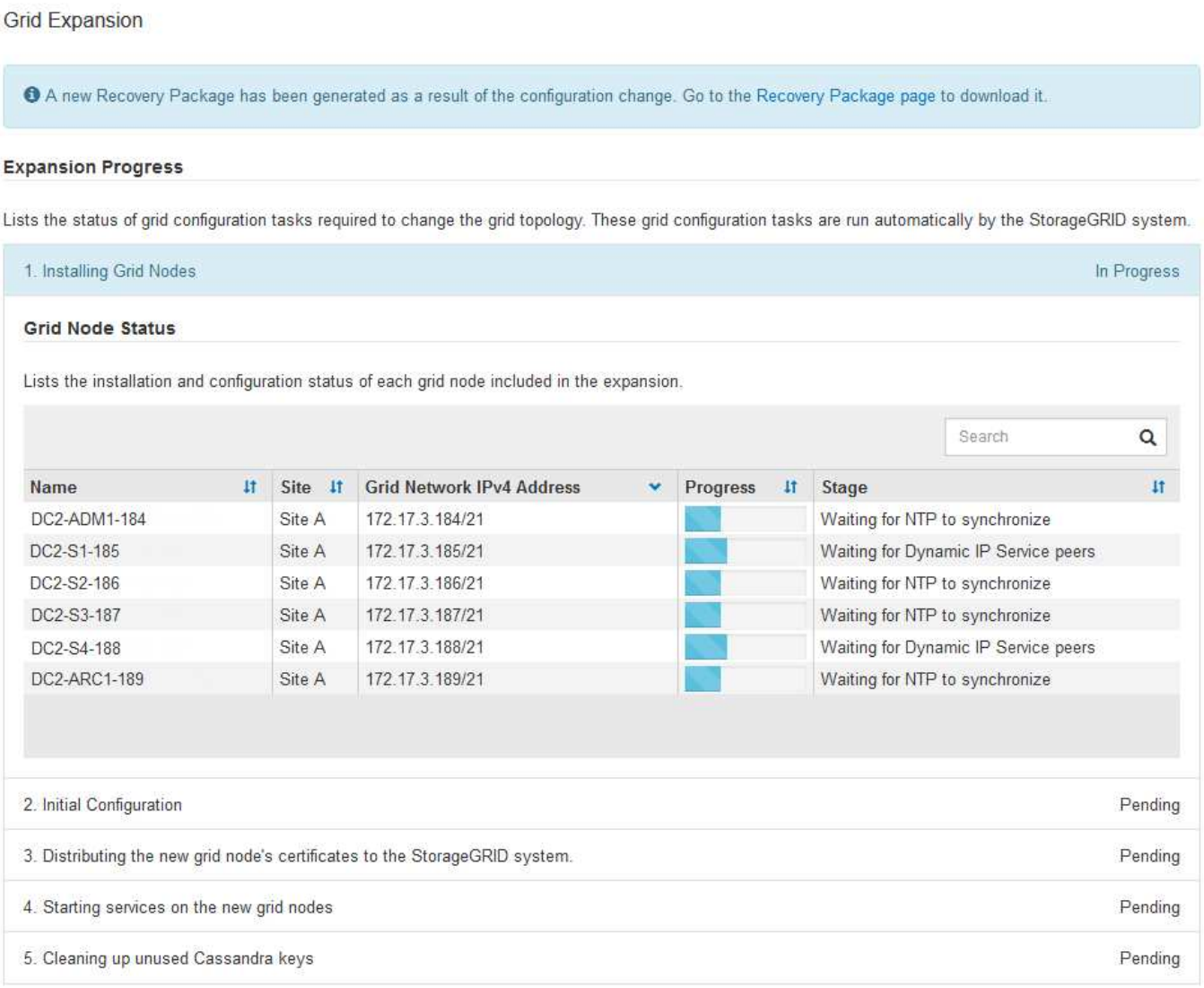



ファイルをアップロードしたあと、個々のストレージノードまたはすべてのノードでアップグレードを承認できます。ノードを選択的に承認できるため、アップグレードのスケジュールを簡単に設定できます。アップグレード用にノードを承認すると、システムによってヘルスチェックが実行され、ノードに適用できる場合はアップグレードがインストールされます。

拡張手順

StorageGRID システムを拡張するには、ストレージノードにストレージボリュームを追加するか、既存のサイトに新しいグリッドノードを追加するか、新しいデータセンターサイトを追加します。ストレージノードで SG6060 ストレージアプライアンスを使用している場合は、拡張シェルフを 1 台または 2 台追加して、ノードのストレージ容量を 2 倍または 3 倍にすることができます。

拡張は現在のシステムの処理を中断せずに実行できます。ノードまたはサイトを追加するときは、まず新しいノードを導入し、そのあとにグリッドの拡張ページから拡張手順 を実行します。

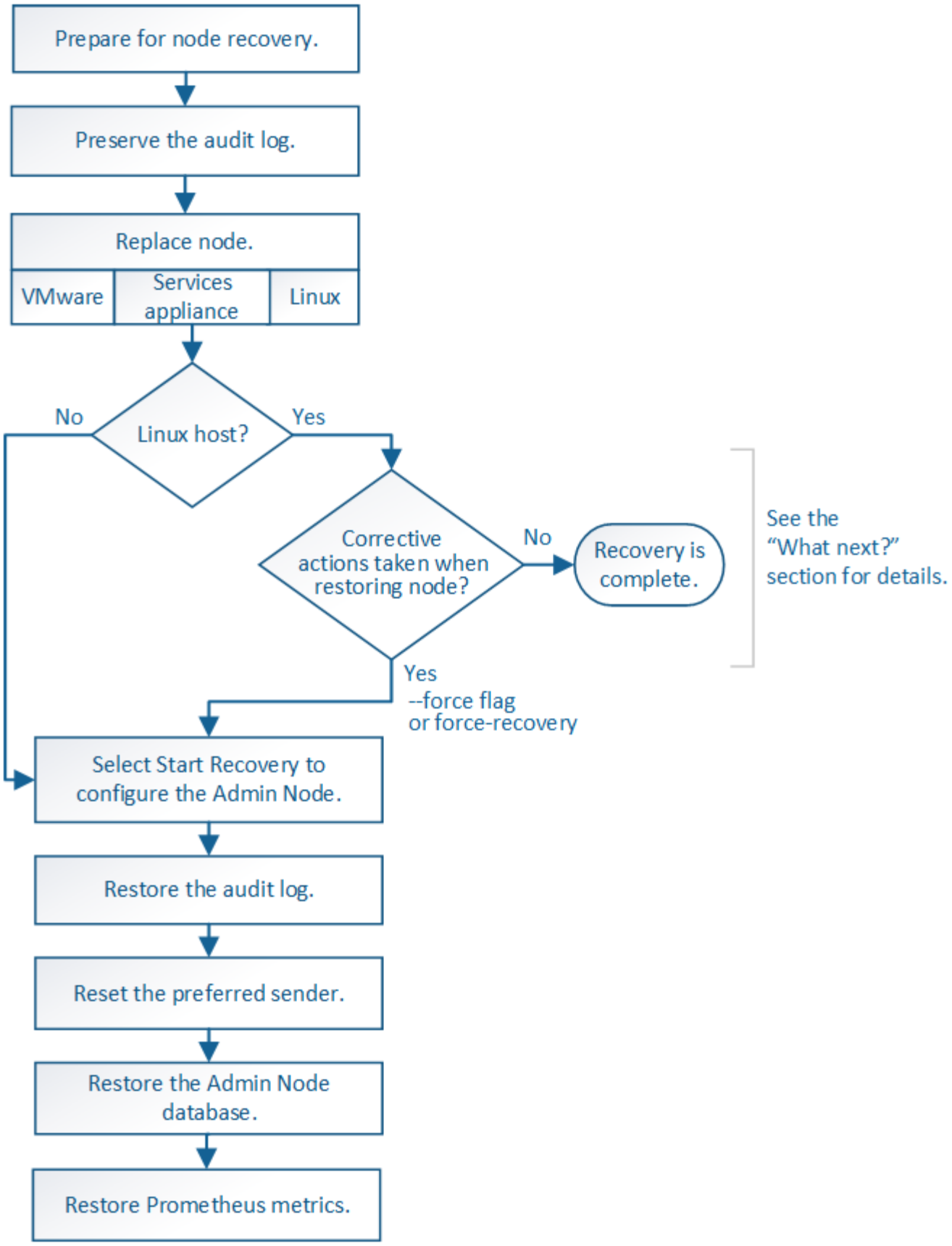



ノードのリカバリ手順

グリッドノードの障害は、ハードウェア、仮想化、オペレーティングシステム、またはソフトウェアの障害によってそのノードが動作しなくなったり、信頼性が低下した場合に発生することがあります。

グリッドノードのリカバリ手順は、グリッドノードがホストされているプラットフォームと、そのグリッドノードのタイプによって異なります。グリッドノードのタイプごとに、厳密に従う必要があるリカバリ手順 があります。通常は、障害グリッドノードのデータをできるだけ保持し、障害ノードを修理または交換し、リカバリページを使用して交換用ノードを設定し、ノードのデータをリストアします。

たとえば、次のフローチャートは、管理ノードで障害が発生した場合のリカバリ用手順 を示しています。




運用停止手順

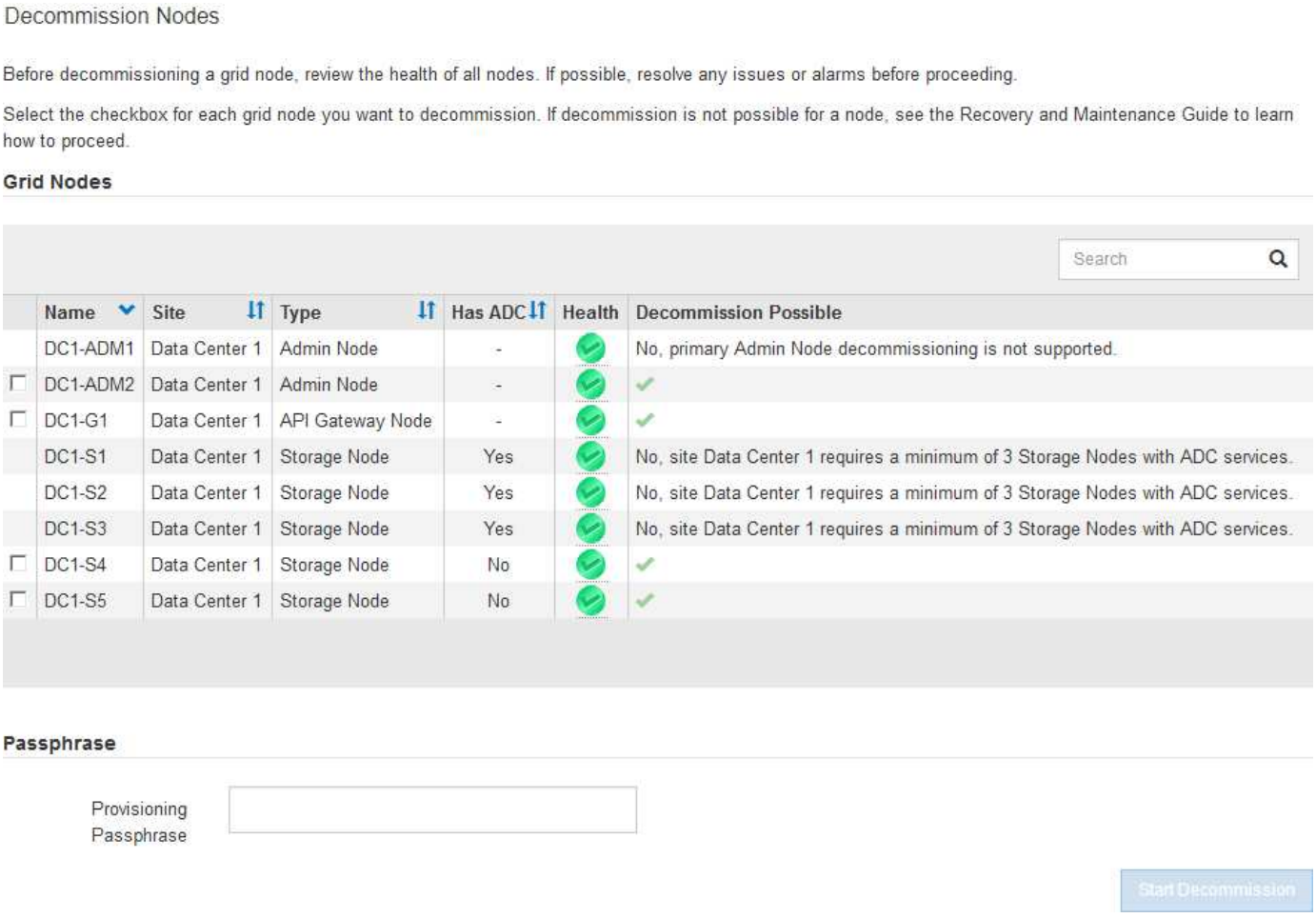
グリッドノードまたはデータセンターサイト全体を StorageGRID システムから完全に削除できます。

たとえば、次のような場合は 1 つ以上のグリッドノードの運用を停止できます。

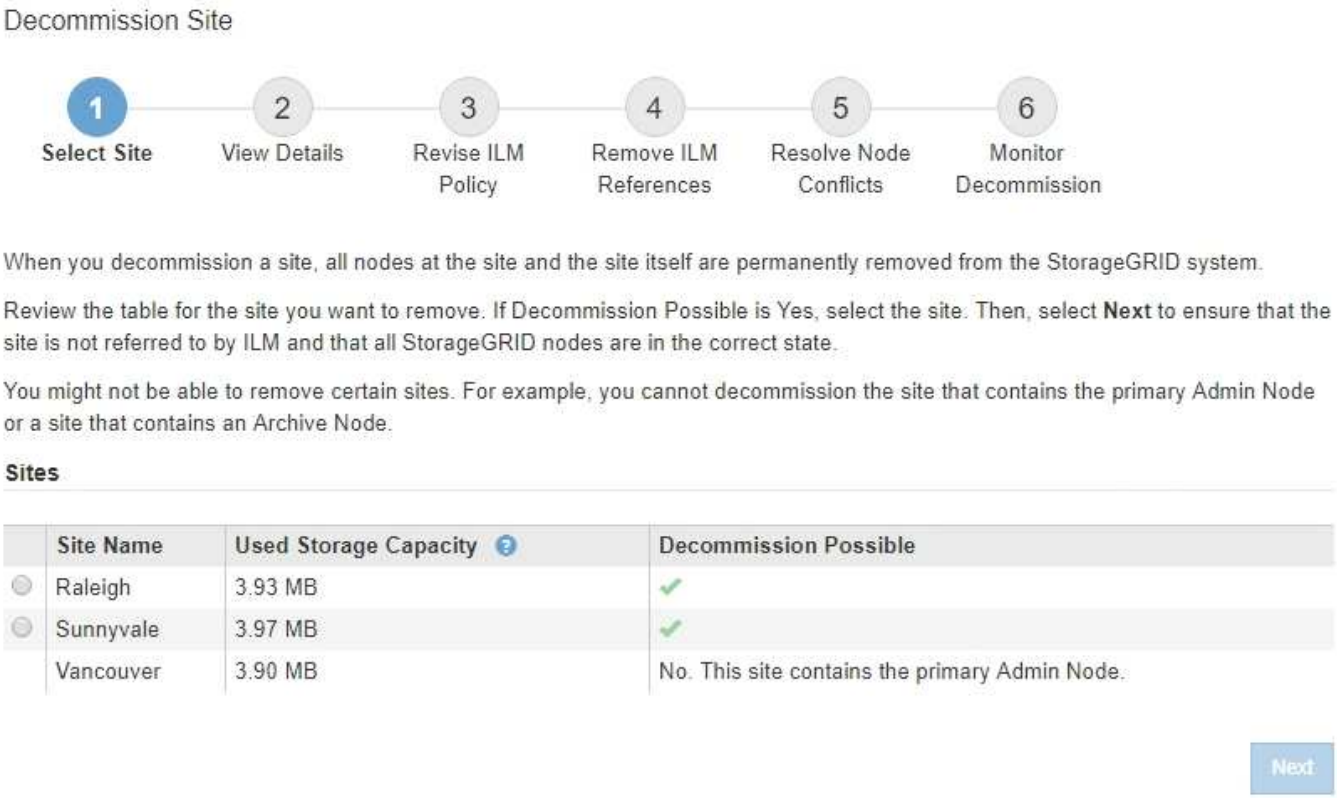
- システムに大きなストレージノードを追加したあとに、オブジェクトを保持したまま小さなストレージノードを 1 つ以上削除する場合。
- 総ストレージ容量を減らす必要がある場合。
- ゲートウェイノードまたは非プライマリ管理ノードが不要になった場合。
- 切断されていて、リカバリしたりオンラインに戻したりすることができないノードがグリッドに含まれている場合。

Grid Manager の運用停止ページを使用して、次のタイプのグリッドノードを削除できます。

- ストレージノード：特定の要件を満たすのに十分なノードがサイトに残っていない場合
- ゲートウェイノード
- 非プライマリ管理ノード




Grid Manager の運用停止サイトページを使用してサイトを削除できます。接続されたサイトの運用停止では、運用サイトが削除され、データが保持されます。切断されたサイトの運用停止処理によって障害が発生したサイトが削除されますが、データは保持されませDecommission Site ウィザードでは、サイトの選択、サイトの詳細の表示、 ILM ポリシーの改訂、 ILM ルールからのサイト参照の削除、およびノードの競合の解決のプロセスを実行できます。




ネットワークのメンテナンス手順

実行する必要があるネットワークメンテナンス手順には、次のものがあります。

- グリッドネットワークのサブネットを更新しています
- グリッドの導入時に最初に設定されたネットワーク設定を変更する場合は、 IP 変更ツールを使用します
- Domain Name System （ DNS ；ドメインネームシステム）サーバの追加、削除、更新
- ネットワークタイムプロトコル（ NTP ）サーバの追加、削除、更新：グリッドノード間でデータが正確に同期されるようにします
- グリッドから分離された可能性があるノードへのネットワーク接続のリストア

ホストレベルおよびミドルウェアの手順

一部のメンテナンス手順は、 Linux または VMware に導入されている StorageGRID ノード、または StorageGRID 解決策 のその他のコンポーネントに固有のものです。たとえば、グリッドノードを別の Linux ホストに移行したり、 Tivoli Storage Manager （ TSM ）に接続されているアーカイブノードでメンテナンスを実行したりすることができます。

アプライアンスノードのクローニング

アプライアンスノードのクローニングを使用すると、グリッド内の既存のアプライアンスノード（ソース）を、同じ論理 StorageGRID サイトに含まれる互換性のあるアプライアンス（ターゲット）に簡単に置き換えることができます。このプロセスでは、すべてのデータが新しいアプライアンスに転送され、古いアプライアンスノードを交換するためにアプライアンスが稼働中になり、古いアプライアンスは設置前の状態になります。クローニングは、ハードウェアのアップグレードプロセスを提供します。アップグレードプロセスは簡単に実行でき、アプライアンスを交換する方法の 1 つとしても利用できます。

*** Gridノードの手順***

特定のグリッドノードで特定の手順を実行する必要がある場合があります。たとえば、グリッドノードのリブートや、特定のグリッドノードサービスの手動による停止と再起動が必要になることがあります。グリッドノードの作業手順には、 Grid Manager から実行できるものと、グリッドノードにログインしてノードのコマンドラインから実行する必要があるものがあります。

関連情報

"StorageGRID の管理"

"ソフトウェアをアップグレードする"

"グリッドを展開します"

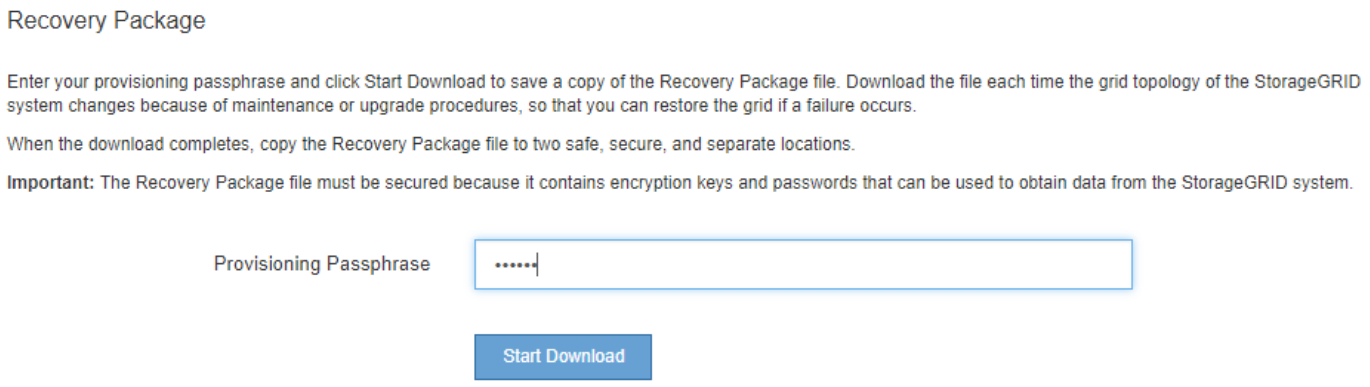
""

リカバリパッケージをダウンロードしています

## リカバリパッケージはダウンロード可能な .zip ファイルで、 StorageGRID システムのインストール、拡張、アップグレード、および保守に必要な導入環境に固有のファイルとソフトウェアが含まれています。

リカバリパッケージファイルには、システム固有の設定および統合情報も含まれます。これには、サーバのホスト名と IP アドレス、およびシステムのメンテナンス、アップグレード、拡張の際に必要となる機密性の高いパスワードが含まれます。リカバリパッケージは、プライマリ管理ノードを障害からリカバリする場合に必要です。

StorageGRID システムをインストールするときは、リカバリパッケージファイルをダウンロードし、このファイルのコンテンツに正常にアクセスできることを確認する必要があります。このファイルは、StorageGRID システムのグリッドトポロジの変更に伴い、メンテナンスやアップグレードの手順が必要になった場合にも、毎回ダウンロードする必要があります。




リカバリパッケージファイルをダウンロードしてコンテンツを展開できることを確認したら、 2 つの安全な場所にリカバリパッケージファイルをコピーします。

リカバリパッケージファイルには StorageGRID システムからデータを取得するための暗号キーとパスワードが含まれているため、安全に保管する必要があります。

関連情報

"ソフトウェアをアップグレードする"

"グリッドを展開します"

""

**StorageGRID** サポートオプションを使用する

# Grid Manager には、 StorageGRID システムで問題 が発生した場合にテクニカルサポートと連携するためのオプションが用意されています。

**AutoSupport** を設定しています

AutoSupport 機能を使用すると、 StorageGRID システムのヘルスメッセージおよびステータスメッセージをテクニカルサポートに送信できます。AutoSupport を使用すると、問題の特定と解決にかかる時間を大幅に短縮できます。また、システムのストレージニーズを監視し、新しいノードやサイトを追加する必要があるかどうかを判断するための支援も行います。必要に応じて、 1 つの別の送信先に AutoSupport メッセージを送信するように設定できます。

**AutoSupport** メッセージに含まれる情報

AutoSupport メッセージには次のような情報が含まれます。

- StorageGRID ソフトウェアのバージョン
- オペレーティングシステムのバージョン
- システムレベルおよび場所レベルの属性情報
- 最新のアラートとアラーム（従来型システム）
- 履歴データを含む、すべてのグリッドタスクの現在のステータス
- ノード*>*_node_name >* Events *ページにリストされているイベント情報
- 管理ノードデータベースの使用率
- 失われた、または欠落しているオブジェクトの数
- Grid の設定
- NMS エンティティ
- アクティブな ILM ポリシー
- プロビジョニングされたグリッド仕様ファイル
- 診断メトリック

AutoSupport 機能および個々の AutoSupport オプションは、 StorageGRID の初回インストール時に有効にするか、あとから有効にすることができます。AutoSupport が有効になっていない場合は、Grid ManagerDashboardにメッセージが表示されます。このメッセージには、 AutoSupport 設定ページへのリンクが含まれています。

「x」記号を選択できます をクリックしてメッセージを閉じます。このメッセージは、AutoSupport が無効なままであっても、ブラウザキャッシュがクリアされるまで表示されません。

### Active IQ を使用する

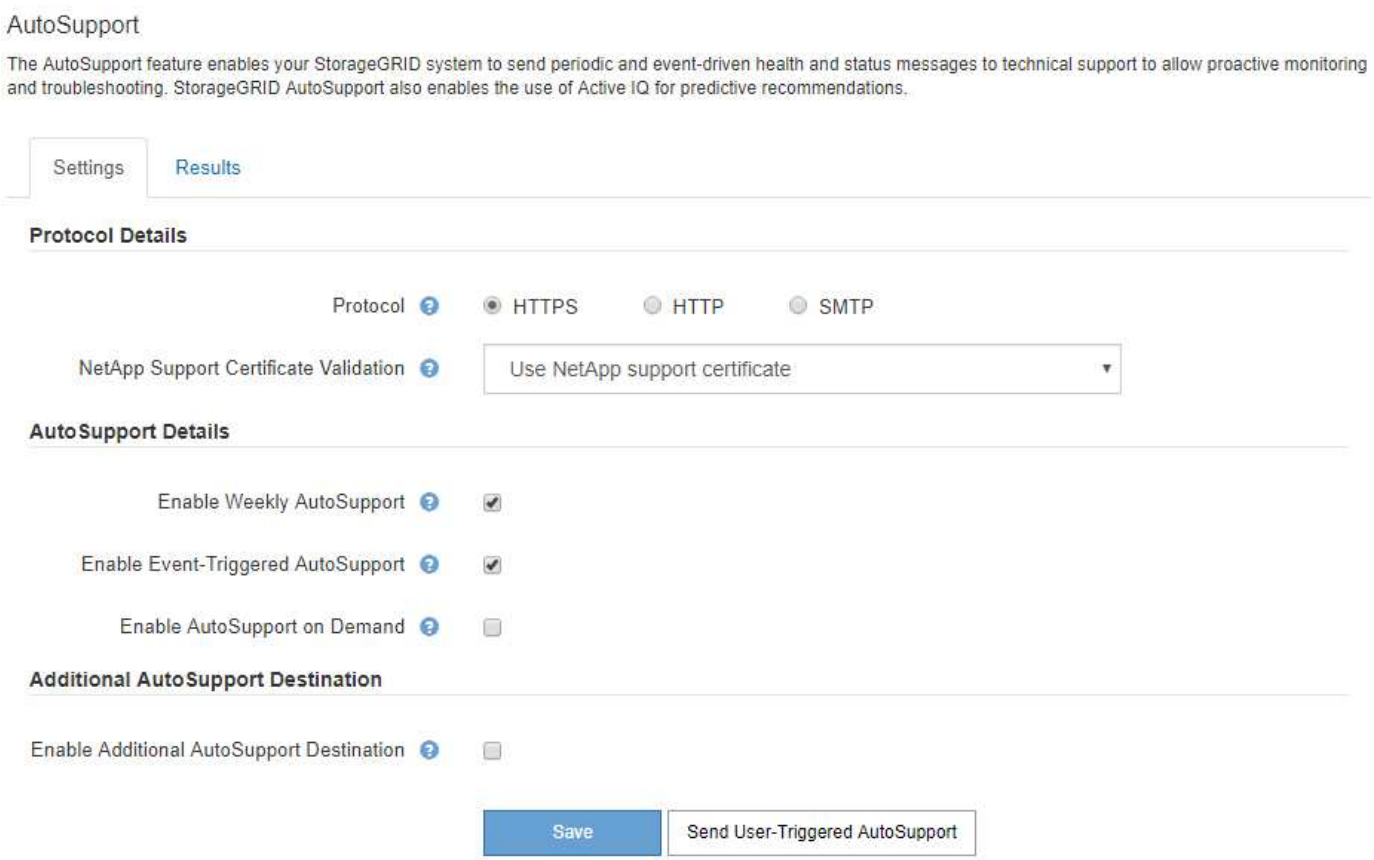
Active IQ は、ネットアップのインストールベースが提供する予測分析と集合知を活用する、クラウドベースのデジタルアドバイザです。継続的なリスク評価、予測アラート、規範となるガイダンス、自動化されたアクションによって、問題が発生する前に予防できます。これにより、システムの健全性が向上し、システムの可用性が向上します。

NetApp Support Siteの Active IQ ダッシュボードと機能を使用する場合は、 AutoSupport を有効にする必要があります。

"Active IQ Digital Advisorのドキュメント"

### AutoSupport 設定にアクセスしています

AutoSupport はGrid Manager（* Support > Tools > AutoSupport *）を使用して設定します。「 * AutoSupport * 」ページには、 * 設定 * と * 結果 * の 2 つのタブがあります。



### AutoSupport メッセージを送信するためのプロトコル

AutoSupport メッセージの送信には、次の 3 つのプロトコルのいずれかを選択できます。

- HTTPS
- HTTP
- SMTP

HTTPS または HTTP を使用して AutoSupport メッセージを送信する場合は、管理ノードとテクニカルサポートの間に非透過型プロキシサーバを設定できます。

SMTP を AutoSupport メッセージのプロトコルとして使用する場合は、 SMTP メールサーバを設定する必要があります。

### AutoSupport オプション

AutoSupport メッセージをテクニカルサポートに送信するには、次のオプションを任意に組み合わせて使用できます。

- * 週単位 * ： AutoSupport メッセージを週に 1 回自動的に送信します。デフォルト設定： Enabled （有効）。
- * イベントトリガー型 * ： 1 時間ごと、または重大なシステムイベントが発生したときに、 AutoSupport メッセージを自動的に送信します。デフォルト設定： Enabled （有効）。
- * On Demand * ： StorageGRID システムが AutoSupport メッセージを自動的に送信するようテクニカルサポートから要求できます。これは、問題 がアクティブに機能している場合に便利です（ HTTPS AutoSupport 転送プロトコルが必要）。デフォルト設定： Disabled （無効）。
- * User-triggered * ： AutoSupport メッセージをいつでも手動で送信します。

関連情報

"StorageGRID の管理"

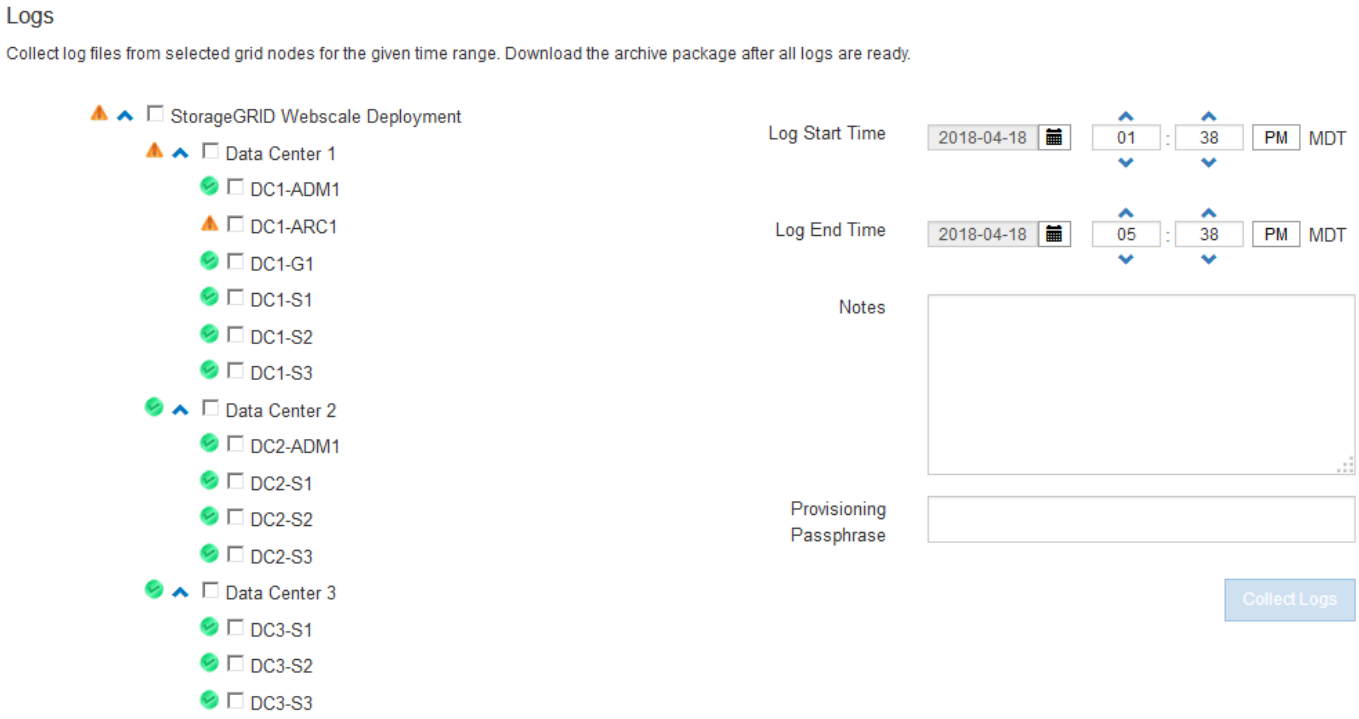
"ネットワークの設定"

#### StorageGRID ログを収集しています

問題をトラブルシューティングするために、ログファイルを収集してテクニカルサポートに転送することが必要になる場合があります。

StorageGRID は、ログファイルを使用して、イベント、診断メッセージ、およびエラー状態をキャプチャします。bycast.log ファイルは、すべてのグリッドノードに対して作成される主要なトラブルシューティングファイルです。StorageGRID では、個々の StorageGRID サービスのログファイル、導入とメンテナンス作業に関連するログファイル、サードパーティアプリケーションに関連するログファイルも作成されます。

適切な権限を持つユーザと StorageGRID システムのプロビジョニングパスフレーズを知っているユーザは、グリッドマネージャの Logs ページを使用して、ログファイル、システムデータ、および設定データを収集できます。ログを収集する際には、 1 つ以上のノードを選択し、期間を指定します。データが収集され、にアーカイブされます `.tar.gz` ファイル。ローカルコンピュータにダウンロードできます。このファイルには、グリッドノードごとに 1 つのログファイルがアーカイブされています。




関連情報

"トラブルシューティングを監視します"

"StorageGRID の管理"

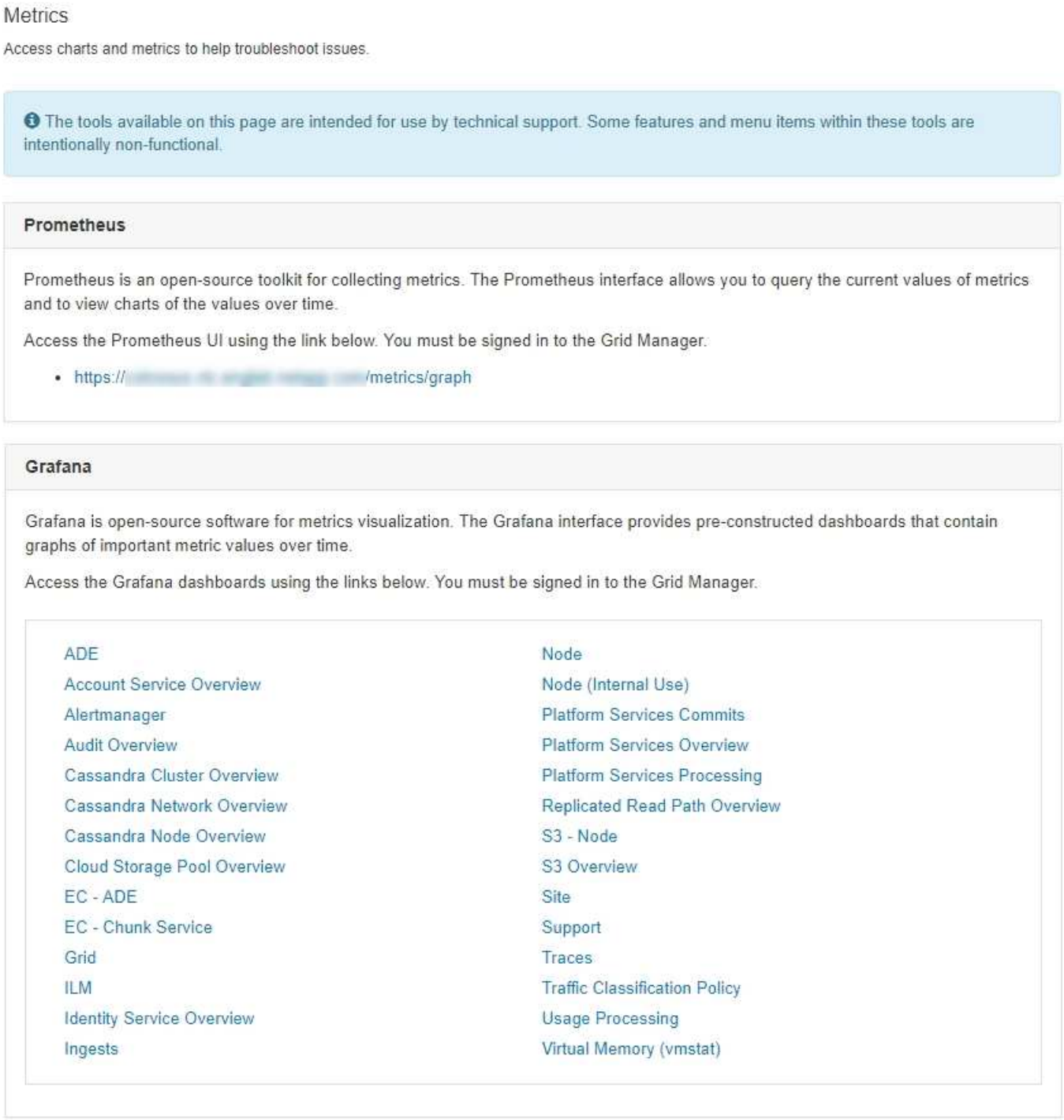
指標を使用した診断の実行

問題 のトラブルシューティングでは、テクニカルサポートと協力して StorageGRID システムの詳細な指標とグラフを確認することができます。また、構築済みの診断クエリを実行して、 StorageGRID システムのキーの値をプロアクティブに評価することもできます。

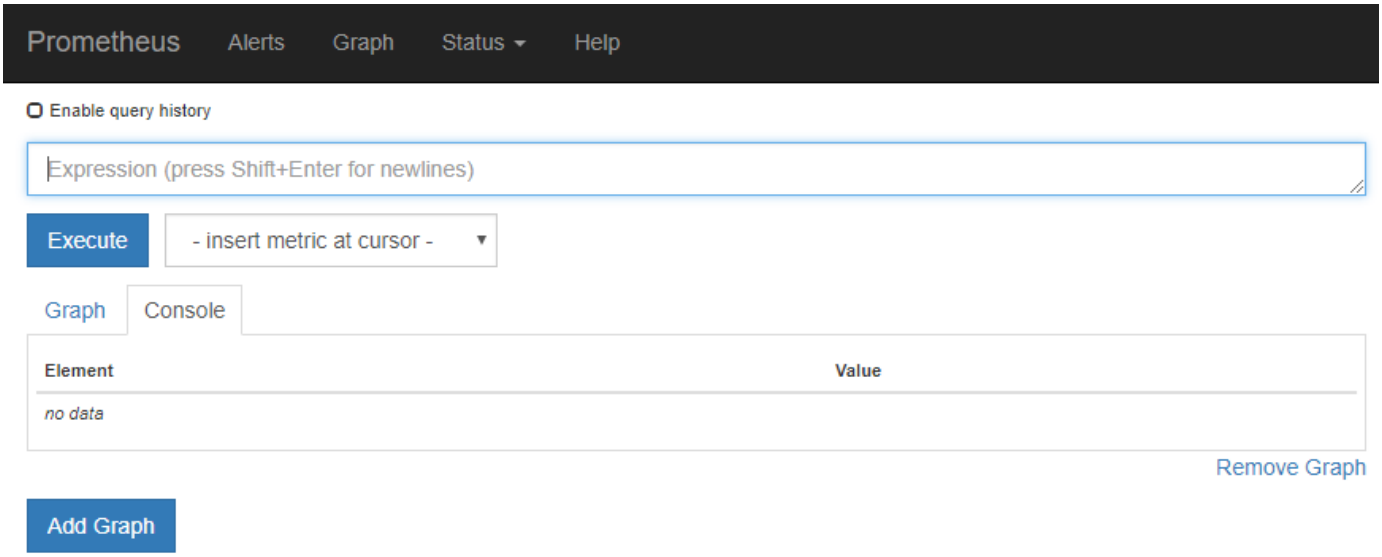
指標ページ

Metrics ページでは、 Prometheus および Grafana のユーザインターフェイスへのアクセスが可能です。Prometheus は指標を収集するオープンソースソフトウェアです。Grafana は指標を視覚化するオープンソースソフトウェアです。

Metrics ページで使用可能なツールは、テクニカルサポートが使用することを目的としています。これらのツールの一部の機能およびメニュー項目は意図的に機能しないため、変更される場合があります。




Metrics ページの Prometheus セクションのリンクを使用すると、 StorageGRID 指標の現在の値を照会し、その値の推移をグラフで確認できます。

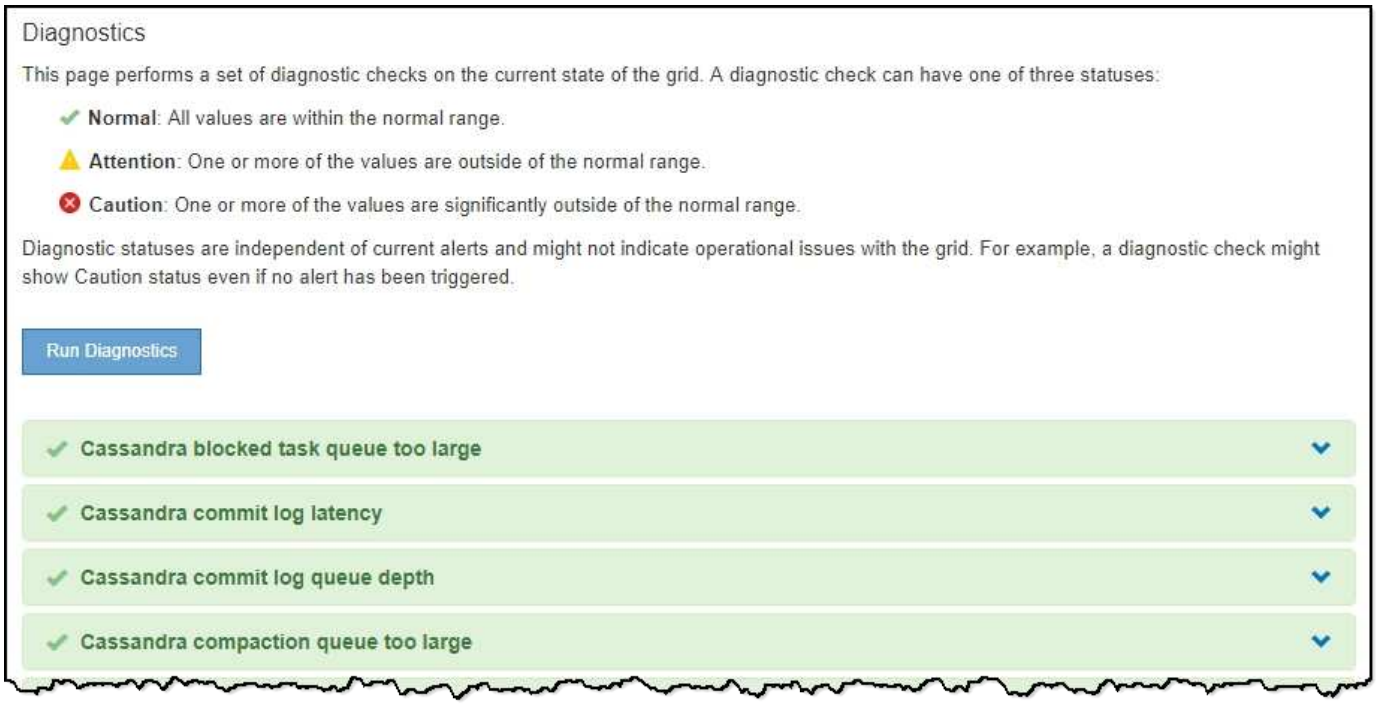



名前に *private* が含まれる指標は内部専用です。 StorageGRID のリリースごとに予告なく変更されることがあります。

Metrics ページの Grafana セクションのリンクを使用すると、時間の経過とともに StorageGRID 指標のグラフを含む構築済みのダッシュボードにアクセスできます。

### **Diagnostics** （診断）ページ

Diagnostics （診断）ページでは、グリッドの現在の状態に対して事前に構築された診断チェックのセットが実行されます。この例では、すべての診断のステータスは Normal です。




特定の診断をクリックすると、診断とその現在の結果の詳細が表示されます。

この例では、 StorageGRID システム内のすべてのノードの現在の CPU 利用率が表示されています。すべてのノードの値が警告と警告のしきい値を下回っているため、診断の全体的なステータスは「正常」です。

CPU utilization

Checks the current CPU utilization on each node.

To view charts of CPU utilization and other per-node metrics, access the **Node** Grafana dashboard.

**Status** Normal

**Prometheus query**

```
sum by (instance) (sum by (instance, mode) (irate(node_cpu_seconds_total{mode!="idle"}[5m])) / count by (instance, mode)(node_cpu_seconds_total{mode!="idle"}))
```

View in Prometheus

**Thresholds**

Attention >= 75%

Caution >= 95%

| Status | Instance | CPU Utilization |
|---|---|---|
| ✔ | DC1-ADM1 | 2.598% |
| ✔ | DC1-ARC1 | 0.937% |
| ✔ | DC1-G1 | 2.119% |
| ✔ | DC1-S1 | 8.708% |
| ✔ | DC1-S2 | 8.142% |
| ✔ | DC1-S3 | 9.669% |
| ✔ | DC2-ADM1 | 2.515% |
| ✔ | DC2-ARC1 | 1.152% |
| ✔ | DC2-S1 | 8.204% |
| ✔ | DC2-S2 | 5.000% |
| ✔ | DC2-S3 | 10.469% |

関連情報

"トラブルシューティングを監視します"

# ネットワークのガイドライン

StorageGRID アーキテクチャとネットワークトポロジについて説明します。ネットワークの設定とプロビジョニングの要件を理解します。

- "StorageGRID ネットワークの概要"
- "ネットワークの要件とガイドライン"
- "環境固有のネットワークに関する考慮事項"
- "ネットワークのインストールとプロビジョニング"
- "インストール後のガイドライン"
- "ネットワークポートのリファレンス"

## StorageGRID ネットワークの概要

StorageGRID システムのネットワークを設定するには、イーサネットスイッチング、TCP/IP ネットワーク、サブネット、ネットワークルーティング、およびファイアウォールに関する高度な経験が必要です。

ネットワークを設定する前に、_グリッド入門_の説明に従ってStorageGRID アーキテクチャについて理解しておいてください。

StorageGRID を導入して設定する前に、ネットワークインフラを設定する必要があります。通信は、グリッド内のすべてのノード間、およびグリッドと外部のクライアントとサービスの間で発生する必要があります。

外部クライアントや外部サービスは、次のような機能を実行するために StorageGRID ネットワークに接続する必要があります。

- オブジェクトデータを格納し、読み出す
- E メール通知を受信
- StorageGRID 管理インターフェイス（ Grid Manager およびテナントマネージャ）へのアクセス
- 監査共有へのアクセス（オプション）
- 次のようなサービスを提供します。
  - ネットワークタイムプロトコル NTP
  - Domain Name System （ DNS ；ドメインネームシステム）
  - キー管理サーバ（ KMS ）

これらの機能を使用するトラフィックなどを処理するには、 StorageGRID ネットワークが適切に設定されている必要があります。

使用する3つのStorageGRID ネットワークのうち、どのネットワークをどのように設定するかを決定したら、適切な手順に従ってStorageGRID ノードを設置して設定できます。

関連情報

"グリッド入門"

"StorageGRID の管理"

"リリースノート"

"Red Hat Enterprise Linux または CentOS をインストールします"

"Ubuntu または Debian をインストールします"

"VMware をインストールする"

"SG100 SG1000サービスアプライアンス"

"SG6000 ストレージアプライアンス"

"SG5700 ストレージアプライアンス"

"SG5600 ストレージアプライアンス"

**StorageGRID** のネットワークタイプ

StorageGRID システムのグリッドノードは、 _ グリッドトラフィック _ 、 _ 管理トラフィック _ 、および _ クライアントトラフィック _ を処理します。この 3 種類のトラフィックを管理し、制御とセキュリティを提供するには、ネットワークを適切に設定する必要があります。

トラフィックタイプ

| トラフィックタイプ | 説明 | ネットワークの種類 |
| --- | --- | --- |
| グリッドトラフィック | グリッド内のすべてのノードの間で伝送される、内部 StorageGRID トラフィック。このネットワークを介して、すべてのグリッドノードが他のすべてのグリッドノードと通信できる必要があります。 | グリッドネットワーク（必須） |
| 管理トラフィック | システムの管理とメンテナンスに使用されるトラフィック。 | 管理ネットワーク（オプション） |
| クライアントトラフィック | S3 および Swift クライアントからのオブジェクトストレージ要求をすべて含む、外部のクライアントアプリケーションとグリッドの間で伝送されるトラフィック。 | クライアントネットワーク（オプション） |

ネットワークは次の方法で設定できます。

- Grid ネットワークのみ
- グリッドネットワークと管理ネットワーク

- グリッドネットワークとクライアントネットワーク
- グリッドネットワーク、管理ネットワーク、クライアントネットワーク

グリッドネットワークは必須であり、すべてのグリッドトラフィックを管理できます。管理ネットワークとクライアントネットワークは、インストール時に追加することも、あとで追加して要件の変化に対応することもできます。管理ネットワークとクライアントネットワークはオプションですが、これらのネットワークを使用して管理トラフィックとクライアントトラフィックを処理する場合は、グリッドネットワークを分離してセキュリティを確保することができます。

#### ネットワークインターフェイス

StorageGRID ノードは、次の特定のインターフェイスを使用して各ネットワークに接続されます。

| ネットワーク | インターフェイス名 |
|---|---|
| グリッドネットワーク（必須） | eth0 |
| 管理ネットワーク（オプション） | Eth1 |
| クライアントネットワーク（オプション） | eth2 |

仮想ポートまたは物理ポートのノードネットワークインターフェイスへのマッピングの詳細については、インストール手順を参照してください。

ノードで有効にするネットワークごとに、次の項目を設定する必要があります。

- IP アドレス
- サブネットマスク
- ゲートウェイの IP アドレス

各グリッドノードの 3 つのネットワークのそれぞれについて、 IP アドレス / マスク / ゲートウェイの組み合わせを 1 つだけ設定できます。ネットワークにゲートウェイを設定しない場合は、 IP アドレスをゲートウェイアドレスとして使用する必要があります。

ハイアベイラビリティ（HA）グループは、グリッドネットワークまたはクライアントネットワークのインターフェイスに仮想IPアドレスを追加する機能です。詳細については、 StorageGRID の管理手順を参照してください。

#### **Grid** ネットワーク

グリッドネットワークは必須です。このネットワークは、すべての内部 StorageGRID トラフィックに使用されます。グリッドネットワークは、グリッド内のすべてのノード間、すべてのサイトおよびサブネットを接続します。グリッドネットワーク上のすべてのノードが他のすべてのノードと通信できる必要があります。グリッドネットワークは複数のサブネットで構成できます。NTP などの重要なグリッドサービスを含むネットワークも、グリッドサブネットとして追加できます。

StorageGRID では、ノード間の Network Address Translation （ NAT; ネットワークアドレス変換）はサポートされません。

管理ネットワークとクライアントネットワークが設定されている場合でも、グリッドネットワークはすべての管理トラフィックとすべてのクライアントトラフィックに使用できます。ノードにクライアントネットワークが設定されていないかぎり、グリッドネットワークゲートウェイがノードのデフォルトゲートウェイになります。

> グリッドネットワークを設定するときは、オープンなインターネット上のネットワークなど、信頼されていないクライアントからネットワークが保護されていることを確認する必要があります。

グリッドネットワークに関する次の要件および詳細に注意してください。

- グリッドサブネットが複数ある場合は、グリッドネットワークゲートウェイを設定する必要があります。
- グリッドの設定が完了するまでは、グリッドネットワークゲートウェイがノードのデフォルトゲートウェイになります。
- グローバルなグリッドネットワークサブネットリストで設定されているすべてのサブネットへの静的ルートが、すべてのノードに対して自動的に生成されます。
- クライアントネットワークを追加すると、グリッドの設定が完了した時点で、デフォルトゲートウェイがグリッドネットワークのゲートウェイからクライアントネットワークゲートウェイに切り替わります。

#### 管理ネットワーク

管理ネットワークはオプションです。このオプションを設定すると、システムの管理トラフィックやメンテナンストラフィックに使用できます。管理ネットワークは通常はプライベートネットワークであり、ノード間でルーティング可能にする必要はありません。

管理ネットワークを有効にするグリッドノードを選択できます。

管理ネットワークを使用する場合、管理トラフィックとメンテナンストラフィックがグリッドネットワークを経由する必要はありません。管理ネットワークの一般的な用途としては、Grid Managerユーザインターフェイスへのアクセス、NTP、DNS、外部キー管理（KMS）、Lightweight Directory Access Protocol（LDAP）などの重要なサービスへのアクセス、管理ノード上の監査ログへのアクセス、メンテナンスとサポート用のSecure Shell Protocol（SSH）アクセスがあります。

管理ネットワークが内部のグリッドトラフィックに使用されることはありません。管理ネットワークゲートウェイが提供され、管理ネットワークが複数の外部サブネットと通信できるようになります。ただし、管理ネットワークゲートウェイがノードのデフォルトゲートウェイとして使用されることはありません。

管理ネットワークに関する次の要件および詳細に注意してください。

- 管理ネットワークサブネットの外部から接続を行う場合や複数の管理ネットワークサブネットを設定する場合は、管理ネットワークゲートウェイが必要です。
- ノードの管理ネットワークサブネットリストで設定されているサブネットごとに静的ルートが作成されます。

#### クライアントネットワーク

クライアントネットワークはオプションです。設定すると、 S3 や Swift などのクライアントアプリケーションからのグリッドサービスへのアクセスを提供するために使用されます。外部リソース（クラウドストレージプールや StorageGRID CloudMirror レプリケーションサービスなど）から StorageGRID データにアクセスできるようにする場合は、外部リソースもクライアントネットワークを使用できます。グリッドノードは、クライアントネットワークゲートウェイ経由で到達できるすべてのサブネットと通信できます。

クライアントネットワークを有効にするグリッドノードを選択できます。すべてのノードが同じクライアントネットワーク上に存在する必要はなく、ノードがクライアントネットワーク経由で相互に通信することはありません。クライアントネットワークは、グリッドのインストールが完了するまで動作状態になりません。

セキュリティを強化するために、ノードのクライアントネットワークインターフェイスを信頼されていないものと指定し、クライアントネットワークで許可される接続をより厳しく制限できます。ノードのクライアントネットワークインターフェイスが信頼されていない場合、このインターフェイスは CloudMirror レプリケーションで使用される接続などのアウトバウンド接続を受け入れますが、ロードバランサエンドポイントとして明示的に設定されているポートのインバウンド接続だけを受け入れます。信頼されていないクライアントネットワーク機能とロードバランササービスの詳細については、StorageGRID の管理手順を参照してください。

クライアントネットワークを使用する場合、クライアントトラフィックがグリッドネットワークを経由する必要はありません。グリッドネットワークトラフィックは、ルーティングされないセキュアなネットワークに分離できます。クライアントネットワークでは、多くの場合、次のノードタイプが設定されます。

- ゲートウェイノード。グリッドへの StorageGRID ロードバランササービスおよび S3 / Swift クライアントアクセスを提供するためです。
- ストレージノード： S3 および Swift プロトコルへのアクセス、およびクラウドストレージプールと CloudMirror レプリケーションサービスへのアクセスを提供するため。
- 管理ノード。テナントユーザが管理ネットワークを使用せずにTenant Managerに接続できるようにするために使用します。

クライアントネットワークについては、次の点に注意してください。

- クライアントネットワークを設定する場合は、クライアントネットワークゲートウェイが必要です。
- グリッドの設定が完了すると、クライアントネットワークのゲートウェイがグリッドノードのデフォルトルートになります。

関連情報

"ネットワークの要件とガイドライン"

"StorageGRID の管理"

"SG100 SG1000サービスアプライアンス"

"SG6000 ストレージアプライアンス"

"SG5700 ストレージアプライアンス"

"Red Hat Enterprise Linux または CentOS をインストールします"

"Ubuntu または Debian をインストールします"

"VMware をインストールする"

ネットワークトポロジの例

単一サイト環境またはマルチサイト環境のネットワークトポロジを設計する際に、必要なグリッドネットワークに加え、管理ネットワークとクライアントネットワークのインターフェイスを設定するかどうかを選択できます。

内部ポートには、グリッドネットワーク経由でのみアクセスできます。外部ポートには、すべてのタイプのネットワークからアクセスできます。この柔軟性により、 StorageGRID 展開の設計と、スイッチおよびファイアウォールでの外部 IP およびポートフィルタリングの設定に複数のオプションを使用できます。内部ポートと外部ポートの詳細については、ネットワークポートリファレンスを参照してください。

ノードのクライアントネットワークインターフェイスを信頼されていないものとして指定する場合は、インバウンドトラフィックを受け入れるようにロードバランサエンドポイントを設定します。信頼されていないクライアントネットワークとロードバランサエンドポイントの設定については、StorageGRID の管理手順を参照してください。

関連情報

"StorageGRID の管理"

"ネットワークポートのリファレンス"

グリッドネットワークトポロジ

## グリッドネットワークのみを設定すると、最もシンプルなネットワークトポロジが作成されます。

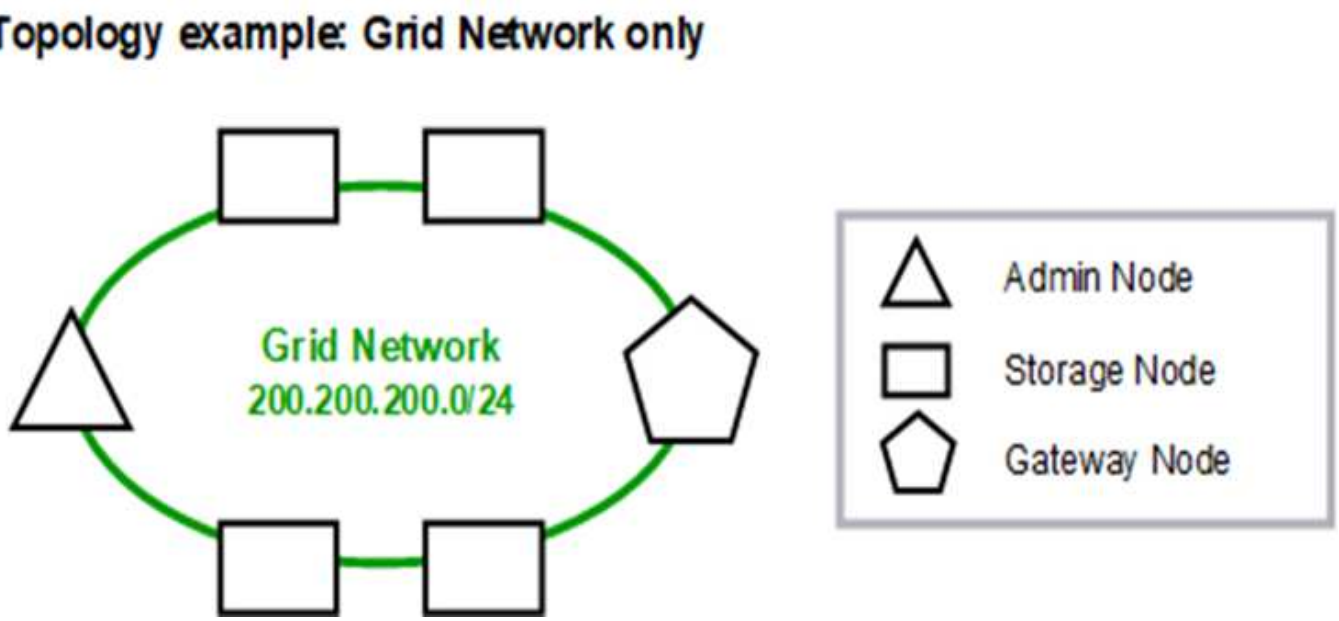
グリッドネットワークを設定するときは、各グリッドノードの eth0 インターフェイスについて、ホスト IP アドレス、サブネットマスク、およびゲートウェイ IP アドレスを確立します。

設定時に、グリッドネットワークサブネットリスト（ GNSL ）にすべてのグリッドネットワークサブネットを追加する必要があります。このリストには、すべてのサイトのすべてのサブネットが含まれ、 NTP 、 DNS 、 LDAP などの重要なサービスへのアクセスを提供する外部サブネットも含まれます。

インストール時に、グリッドネットワークのインターフェイスでは、 GNSL に含まれるすべてのサブネットに静的ルートが適用され、設定されている場合はノードのデフォルトルートがグリッドネットワークゲートウェイに設定されます。クライアントネットワークがなく、グリッドネットワークゲートウェイがノードのデフォルトルートである場合、 GNSL は必要ありません。グリッド内の他のすべてのノードへのホストルートも生成されます。

この例では、 S3 および Swift クライアント要求と管理機能およびメンテナンス機能に関連するトラフィックを含むすべてのトラフィックが、同じネットワークを共有しています。

> このトポロジは、外部からは使用できない単一サイトの配置、概念実証またはテスト用の配置、またはサードパーティのロードバランサがクライアントアクセス境界として機能する場合に適しています。可能な場合は、グリッドネットワークを内部トラフィック専用にします。管理ネットワークとクライアントネットワークの両方に、内部サービスへの外部トラフィックをブロックするファイアウォール制限が追加されています。グリッドネットワークを使用した外部クライアントトラフィックの処理はサポートされていますが、この使用によって保護レイヤが少なくなります。




*Provisioned*

**GNSL → 200.200.200.0/24**

| | Grid Network | |
|---|---|---|
| **Nodes** | **IP/mask** | **Gateway** |
| Admin | 200.200.200.32/24 | 200.200.200.1 |
| Storage | 200.200.200.33/24 | 200.200.200.1 |
| Storage | 200.200.200.34/24 | 200.200.200.1 |
| Storage | 200.200.200.35/24 | 200.200.200.1 |
| Storage | 200.200.200.36/24 | 200.200.200.1 |
| Gateway | 200.200.200.37/24 | 200.200.200.1 |

*System Generated*

| **Nodes** | **Routes** | | | **Type** | **From** |
|---|---|---|---|---|---|
| All | 0.0.0.0/0 | → | 200.200.200.1 | Default | Grid Network gateway |
| | 200.200.200.0/24 | → | eth0 | Link | Interface IP/mask |

管理ネットワークトポロジ

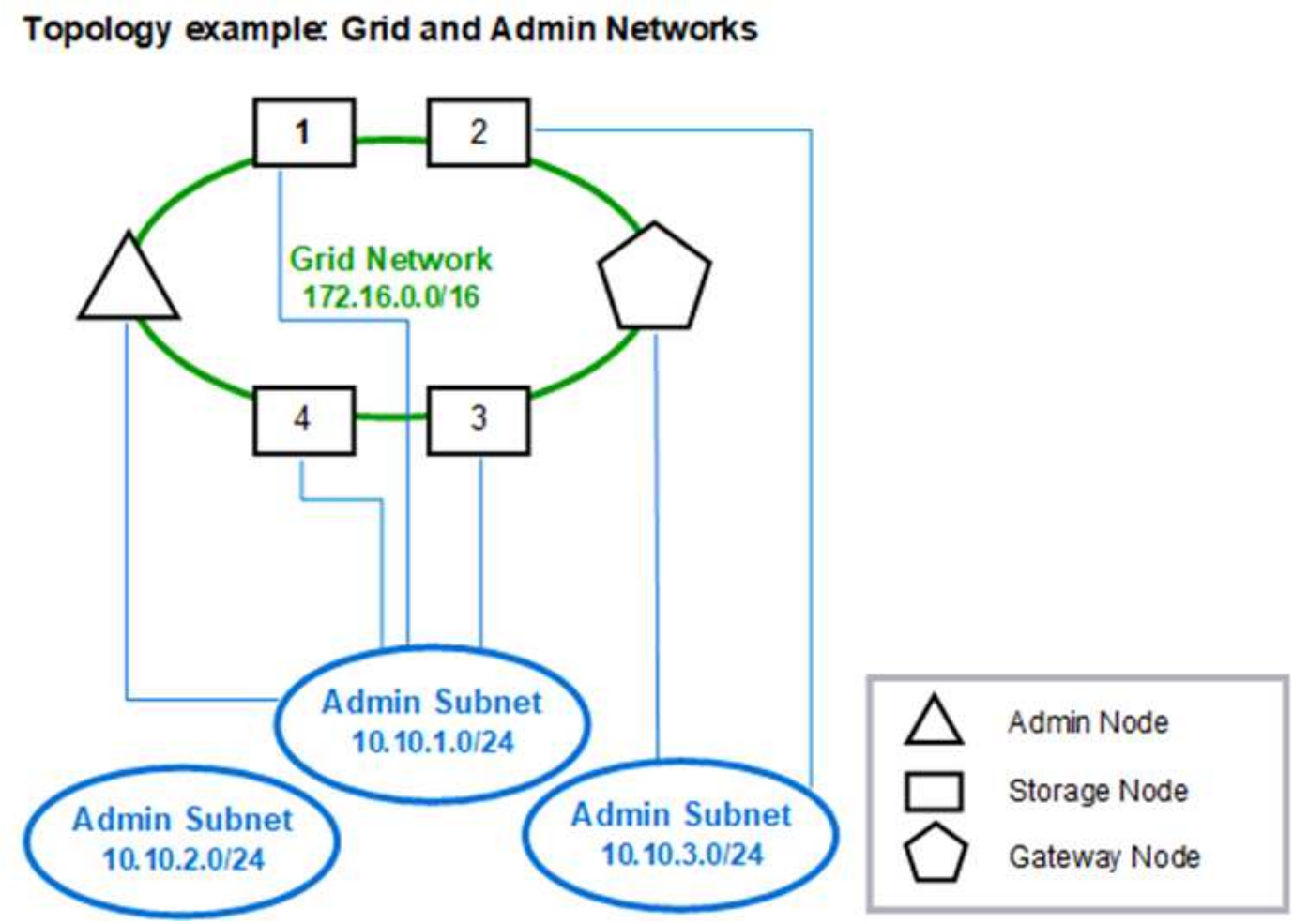
## 管理ネットワークの使用はオプションです。管理ネットワークとグリッドネットワークを使用する方法の 1 つは、ノードごとにルーティング可能なグリッドネットワークと境界で保護された管理ネットワークを設定することです。

管理ネットワークを設定するときは、各グリッドノードの eth1 インターフェイスについて、ホスト IP アドレス、サブネットマスク、およびゲートウェイ IP アドレスを確立します。

管理ネットワークは各ノードに一意にすることができ、複数のサブネットで構成することができます。各ノードで Admin External Subnet List （ AESL ）を設定できます。AESL リストには、各ノードの管理ネットワーク経由で到達できるサブネットが表示されます。AESL には、 NTP 、 DNS 、 KMS 、 LDAP など、管理ネットワーク経由でアクセスするすべてのサービスのサブネットも含める必要があります。AESL に含まれるサブ

ネットごとに静的ルートが適用されます。

次の例では、 S3 および Swift クライアント要求とオブジェクト管理に関連するトラフィックにグリッドネットワークが使用されています。一方、管理機能には管理ネットワークが使用されます。



*Provisioned*

**GNSL → 172.16.0.0/16**

**AESL (all) → 10.10.1.0/24 10.10.2.0/24 10.10.3.0/24**

| | Grid Network | | Admin Network | |
|---|---|---|---|---|
| **Nodes** | **IP/mask** | **Gateway** | **IP/mask** | **Gateway** |
| Admin | 172.16.200.32/24 | 172.16.200.1 | 10.10.1.10/24 | 10.10.1.1 |
| Storage 1 | 172.16.200.33/24 | 172.16.200.1 | 10.10.1.11/24 | 10.10.1.1 |
| Storage 2 | 172.16.200.34/24 | 172.16.200.1 | 10.10.3.65/24 | 10.10.3.1 |
| Storage 3 | 172.16.200.35/24 | 172.16.200.1 | 10.10.1.12/24 | 10.10.1.1 |
| Storage 4 | 172.16.200.36/24 | 172.16.200.1 | 10.10.1.13/24 | 10.10.1.1 |
| Gateway | 172.16.200.37/24 | 172.16.200.1 | 10.10.3.66/24 | 10.10.3.1 |

*System Generated*

| **Nodes** | **Routes** | | | **Type** | **From** |
|---|---|---|---|---|---|
| All | 0.0.0.0/0 | → | 172.16.200.1 | Default | Grid Network gateway |
| Admin, Storage 1, 3, and 4 | 172.16.0.0/16 | → | eth0 | Static | GNSL |
| | 10.10.1.0/24 | → | eth1 | Link | Interface IP/mask |
| | 10.10.2.0/24 | → | 10.10.1.1 | Static | AESL |
| | 10.10.3.0/24 | → | 10.10.1.1 | Static | AESL |
| Storage 2, Gateway | 172.16.0.0/16 | → | eth0 | Static | GNSL |
| | 10.10.1.0/24 | → | 10.10.3.1 | Static | AESL |
| | 10.10.2.0/24 | → | 10.10.3.1 | Static | AESL |
| | 10.10.3.0/24 | → | eth1 | Link | Interface IP/mask |

クライアントネットワークトポロジ

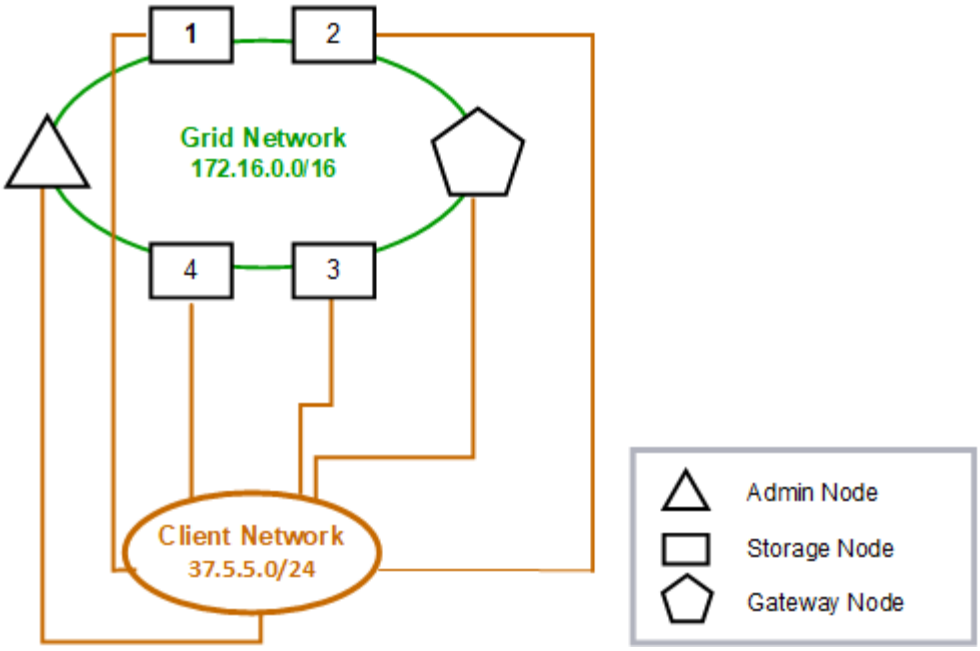
クライアントネットワークの使用はオプションです。クライアントネットワークを使用すると、クライアントネットワークのトラフィック（ S3 や Swift など）をグリッドの内部トラフィックから分離できるため、グリッドネットワークのセキュリティを強化できます。管理ネットワークが設定されていない場合、管理トラフィックはクライアントネットワークまたはグリッドネットワークのどちらでも処理できます。

クライアントネットワークを構成するときは、構成済みノードの eth2 インターフェイスについて、ホスト IP アドレス、サブネットマスク、およびゲートウェイ IP アドレスを確立します。各ノードのクライアントネットワークは、他のノードのクライアントネットワークとは独立している可能性があります。

インストール時にノードのクライアントネットワークを設定すると、インストールの完了時にノードのデフォルトゲートウェイがグリッドネットワークゲートウェイからクライアントネットワークゲートウェイに切り替わります。クライアントネットワークをあとで追加した場合、ノードのデフォルトゲートウェイが同じように切り替わります。

次の例では、クライアントネットワークが S3 および Swift クライアント要求と管理機能に使用され、グリッドネットワークが内部のオブジェクト管理処理専用となっています。

**Topology example: Grid and Client Networks**




*Provisioned*

**GNSL → 172.16.0.0/16**

| Nodes | Grid Network IP/mask | Client Network IP/mask | Client Network Gateway |
|---|---|---|---|
| Admin | 172.16.200.32/24 | 37.5.5.10/24 | 37.5.5.1 |
| Storage | 172.16.200.33/24 | 37.5.5.11/24 | 37.5.5.1 |
| Storage | 172.16.200.34/24 | 37.5.5.12/24 | 37.5.5.1 |
| Storage | 172.16.200.35/24 | 37.5.5.13/24 | 37.5.5.1 |
| Storage | 172.16.200.36/24 | 37.5.5.14/24 | 37.5.5.1 |
| Gateway | 172.16.200.37/24 | 37.5.5.15/24 | 37.5.5.1 |

*System Generated*

| Nodes | Routes | | | Type | From |
|---|---|---|---|---|---|
| All | 0.0.0.0/0 | → | 37.5.5.1 | Default | Client Network gateway |
| | 172.16.0.0/16 | → | eth0 | Link | Interface IP/mask |
| | 37.5.5.0/24 | → | eth2 | Link | Interface IP/mask |

**3** つのネットワークすべてのトポロジ

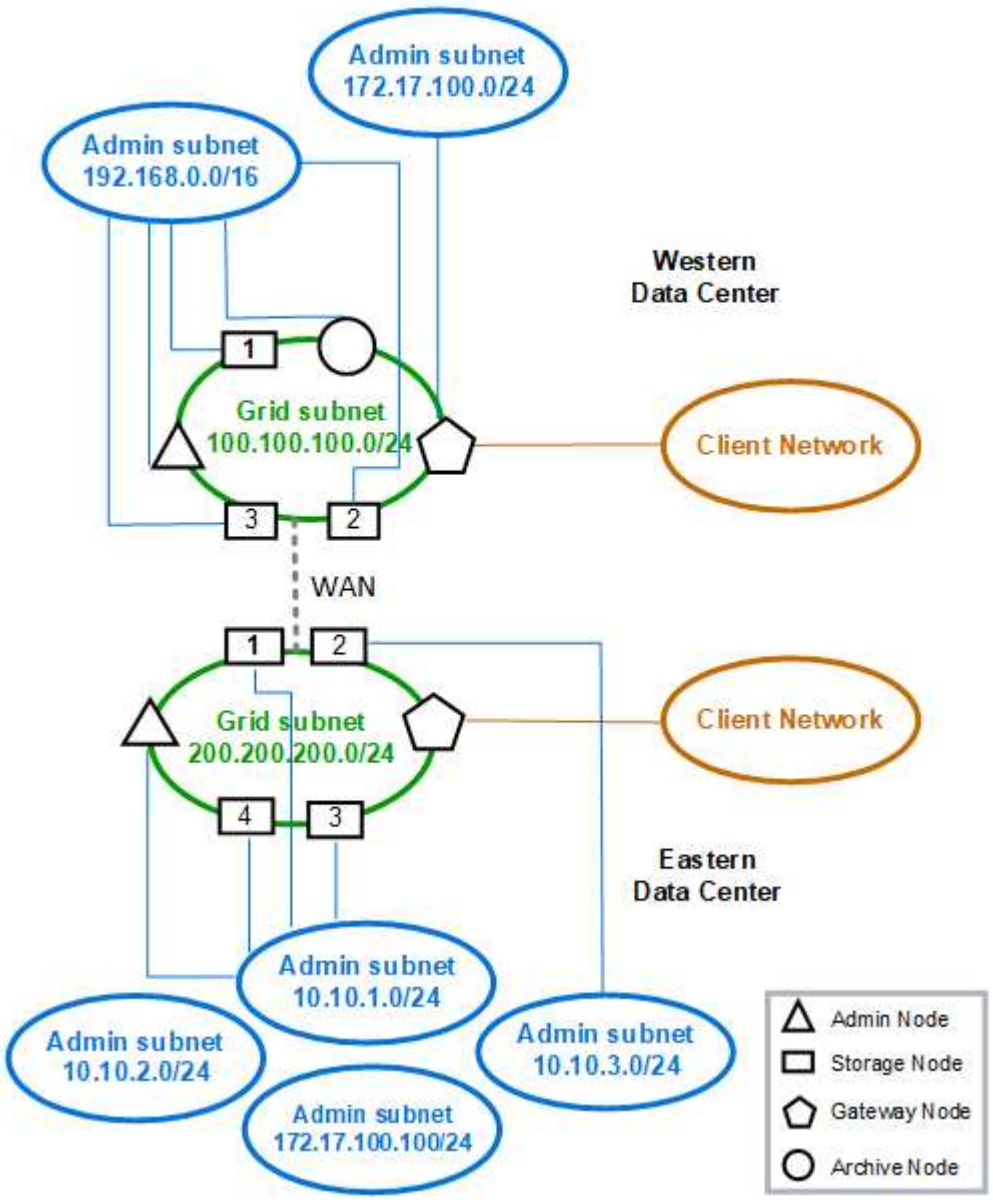
3 つのネットワークをすべて組み合わせて、プライベートグリッドネットワーク、サイトごとに境界を設定した管理ネットワーク、およびオープンなクライアントネットワー

クで構成されるネットワークトポロジを構成できます。ロードバランサエンドポイントと信頼されていないクライアントネットワークを使用すると、必要に応じてセキュリティを強化できます。

次の例では、

- グリッドネットワークは、内部のオブジェクト管理処理に関連するネットワークトラフィックに使用されます。
- 管理ネットワークは、管理機能に関連するトラフィックに使用されます。
- クライアントネットワークは、 S3 および Swift クライアント要求に関連するトラフィックに使用されます。

**Topology example: Grid, Admin, and Client Networks**



# ネットワーク要件

## 計画した StorageGRID ネットワーク設計を、現在のネットワークインフラと構成がサポートできることを確認する必要があります。

### 一般的なネットワーク要件

すべての StorageGRID 環境で次の接続がサポートされている必要があります。

これらの接続は、ネットワークトポロジの例に示すように、グリッドネットワーク、管理ネットワーク、クライアントネットワーク、またはこれらのネットワークの組み合わせを介して発生します。

- * 管理接続 * ：通常は SSH 経由で、管理者からノードへのインバウンド接続。Grid Manager 、テナントマネージャ、および StorageGRID アプライアンスインストーラへの Web ブラウザアクセス
- *NTP サーバ接続 *: 受信 UDP 応答を受信するアウトバウンド UDP 接続。

  プライマリ管理ノードが、少なくとも 1 つの NTP サーバにアクセスできる必要があります。
- *DNS サーバ接続 *: 受信 UDP 応答を受信するアウトバウンド UDP 接続。
- *LDAP/Active Directory サーバ接続 *: ストレージノード上のアイデンティティサービスからのアウトバウンド TCP 接続。
- * AutoSupport *：管理ノードからeithersupport.netapp.comまたはお客様が設定したプロキシへのアウトバウンドTCP接続。
- * 外部キー管理サーバ * ：ノード暗号化が有効な各アプライアンスノードからのアウトバウンド TCP 接続。
- S3 および Swift クライアントからのインバウンド TCP 接続。
- CloudMirrorレプリケーションやクラウドストレージプールなどのStorageGRID プラットフォームサービスからのアウトバウンド要求。

デフォルトのルーティングルールを使用して、プロビジョニングされた NTP サーバや DNS サーバと StorageGRID が通信できない場合は、 DNS サーバと NTP サーバの IP アドレスが指定されていれば、すべてのネットワーク（グリッド、管理、クライアント）で自動的に接続が試行されます。NTP サーバまたは DNS サーバにネットワーク経由でアクセスできる場合は、 StorageGRID によって追加のルーティングルールが自動的に作成され、以降のすべてのネットワーク接続試行に使用されるようになります。

> これらの自動検出されたホストルートは使用できますが、通常は、自動検出が失敗した場合に接続を確保するために、 DNS ルートと NTP ルートを手動で設定する必要があります。

導入時にオプションの管理ネットワークとクライアントネットワークを設定する準備ができていなかった場合は、設定手順でグリッドノードを承認する際にこれらのネットワークを設定できます。また、リカバリとメンテナンスの手順に従ってIP変更ツールを使用すると、インストールの完了後にこれらのネットワークを設定することもできます。

### 管理ノードとゲートウェイノードの接続

管理ノードは、開いているインターネット上のノードなど、信頼されていないクライアントから常に保護する必要があります。グリッドネットワーク上、管理ネットワーク上、またはクライアントネットワーク上のどの管理ノードにも、信頼されていないクライアントがアクセスできないようにする必要があります。

ハイアベイラビリティグループに追加する管理ノードとゲートウェイノードには静的 IP アドレスを設定する必要があります。StorageGRID の管理手順のハイアベイラビリティグループに関する情報を参照してください。

### ネットワークアドレス変換（ **NAT** ）の使用

グリッドノード間または StorageGRID サイト間のグリッドネットワークでは、ネットワークアドレス変換（ NAT ）を使用しないでください。グリッドネットワークにプライベート IPv4 アドレスを使用する場合は、使用するアドレスに各サイトのすべてのグリッドノードから直接ルーティングできる必要があります。ただし、必要に応じて、ゲートウェイノードにパブリック IP アドレスを指定するなど、外部クライアントとグリッドノードの間で NAT を使用できます。NAT を使用してパブリックネットワークセグメントをブリッジする方法は、グリッド内のすべてのノードに対して透過的なトンネリングアプリケーションを採用する場合、つまりグリッドノードがパブリック IP アドレスを認識する必要がない場合にのみサポートされます。

### 関連情報

"グリッド入門"

"StorageGRID の管理"

""

## ネットワーク固有の要件

## 各 StorageGRID ネットワークタイプの要件に従ってください。

### ネットワークゲートウェイおよびルータ

- 設定する場合、特定のネットワークのゲートウェイは、そのネットワークのサブネット内になければなりません。
- 静的アドレス指定を使用してインターフェイスを設定する場合は、 0.0.0.0 以外のゲートウェイアドレスを指定する必要があります。
- ゲートウェイがない場合は、ゲートウェイアドレスをネットワークインターフェイスの IP アドレスに設定することを推奨します。

### サブネット

各ネットワークは、ノード上の他のネットワークと重複しない、専用のサブネットに接続する必要があります。

導入時に、 Grid Manager によって次の制限事項が適用されます。これらの情報は、導入前のネットワーク計画に役立ちます。

- ネットワーク IP アドレスのサブネットマスクを 255.255.255.254 または 255.255.255.0 （ CIDR 表記では /31 または /32 ）にすることはできません。
- ネットワークインターフェイスの IP アドレスとサブネットマスク（ CIDR ）によって定義されたサブネットは、同じノードに設定されている他のインターフェイスのサブネットと重複することはできません。
- 各ノードのグリッドネットワークサブネットを GNSL に含める必要があります。
- 管理ネットワークのサブネットは、グリッドネットワークのサブネット、クライアントネットワークのサブネット、または GNSL のサブネットと重複することはできません。

- AESL 内のサブネットを GNSL 内のどのサブネットとも重複させることはできません。
- クライアントネットワークのサブネットは、グリッドネットワークのサブネット、管理ネットワークのサブネット、 GNSL のサブネット、または AESL に含まれるすべてのサブネットと重複することはできません。

**Grid** ネットワーク

- 導入時に、各グリッドノードがグリッドネットワークに接続され、ノード導入時に指定したネットワーク設定を使用してプライマリ管理ノードと通信できる必要があります。
- 通常のグリッド運用中は、各グリッドノードがグリッドネットワークを介して他のすべてのグリッドノードと通信できる必要があります。

> グリッドネットワークは、各ノード間で直接ルーティングできる必要があります。ノード間の Network Address Translation （ NAT ；ネットワークアドレス変換）はサポートされていません。

- グリッドネットワークが複数のサブネットで構成されている場合は、グリッドネットワークサブネットリスト（ GNSL ）に追加します。GNSL のサブネットごとに、すべてのノードにスタティックルートが作成されます。

管理ネットワーク

管理ネットワークはオプションです。管理ネットワークを設定する場合は、次の要件およびガイドラインに従ってください。

管理ネットワークの一般的な用途としては、管理接続、 AutoSupport 、 KMS 、 NTP 、 DNS 、 LDAP などの重要なサーバへの接続がグリッドネットワークまたはクライアントネットワーク経由で提供されない場合などがあります。

> 必要なネットワークサービスおよびクライアントにアクセス可能であれば、管理ネットワークおよび AESL は各ノードで一意にすることができます。

> 外部サブネットからのインバウンド接続を有効にするには、管理ネットワークに少なくとも 1 つのサブネットを定義する必要があります。AESL に含まれる各サブネットの静的ルートがノードごとに自動的に生成されます。

クライアントネットワーク

クライアントネットワークはオプションです。クライアントネットワークを設定する場合は、次の考慮事項に注意してください。

クライアントネットワークは、 S3 および Swift クライアントからのトラフィックをサポートするように設計されています。設定すると、クライアントネットワークゲートウェイがノードのデフォルトゲートウェイになります。

クライアントネットワークを使用する場合は、明示的に設定されたロードバランサエンドポイントでのみインバウンドクライアントトラフィックを受け入れることで、悪意のある攻撃から StorageGRID を保護できます。StorageGRID の管理手順のロードバランシングと信頼されていないクライアントネットワークの管理に関する情報を参照してください。

関連情報

"StorageGRID の管理"

## 環境固有のネットワークに関する考慮事項

使用する導入プラットフォームによっては、StorageGRID ネットワーク設計に関する追加の考慮事項が生じることがあります。

グリッドノードは次のように導入できます。

- VMware vSphere Web Clientで仮想マシンとして導入される、ソフトウェアベースのグリッドノード
- Linuxホスト上のDockerコンテナ内に導入された、ソフトウェアベースのグリッドノード
- アプライアンスベースのノード

グリッドノードに関する追加情報 の場合は、_グリッド入門_を参照してください。

関連情報

"グリッド入門"

### Linux の導入

効率性、信頼性、セキュリティを確保するため、StorageGRID システムはDockerコンテナの集合としてLinux上で動作します。StorageGRID システムではDocker関連のネットワーク構成は必要ありません。

コンテナネットワークインターフェイスには、 VLAN ペアや仮想イーサネット（ veth ）ペアなどの非ボンドデバイスを使用します。このデバイスをノード構成ファイルのネットワークインターフェイスとして指定してください。

> ボンドデバイスやブリッジデバイスをコンテナネットワークインターフェイスとして直接使用しないでください。このようにすると、 macvlan を使用してコンテナネームスペース内のボンドデバイスとブリッジデバイスを使用するカーネル問題 が原因でノードの起動が妨げられる可能性があります。

Red Hat Enterprise Linux/CentOSまたはUbuntu / Debianの環境でのインストール手順を参照してください。

関連情報

"Red Hat Enterprise Linux または CentOS をインストールします"

"Ubuntu または Debian をインストールします"

### Docker環境向けのホストネットワーク構成

DockerコンテナプラットフォームでStorageGRID の導入を開始する前に、各ノードで使用するネットワーク（グリッド、管理、クライアント）を決めます。各ノードのネットワークインターフェイスが正しい仮想または物理ホストインターフェイスに設定されていること、および各ネットワークに十分な帯域幅があることを確認してください。

### 物理ホスト

物理ホストを使用してグリッドノードをサポートする場合は、次の手順を実行します。

- すべてのホストで各ノードインターフェイスに同じホストインターフェイスを使用していることを確認します。この方法により、ホストの構成が簡易化され、将来のノードの移行にも対応できます
- 物理ホスト自体の IP アドレスを取得します。

> ホスト上の物理インターフェイスは、ホスト自体と、ホスト上で実行されている 1 つ以上のノードで使用できます。このインターフェイスを使用するホストまたはノードには、一意の IP アドレスを割り当てる必要があります。ホストとノードは IP アドレスを共有できません。

- ホストに必要なポートを開きます。

### 最小帯域幅の推奨値

次の表に、 StorageGRID ノードのタイプとネットワークのタイプ別に推奨される最小帯域幅を示します。それぞれの物理ホストまたは仮想ホストについて、そのホストで実行する StorageGRID ノードの総数とタイプに応じて、アグリゲートの最小帯域幅要件を満たすように十分なネットワーク帯域幅を確保する必要があります。

| ノードのタイプ | ネットワークのタイプ | | |
|---|---|---|---|
| | グリッド（ Grid ） | 管理 | クライアント |
| 管理 | 10 Gbps | 1 Gbps | 1 Gbps |
| ゲートウェイ | 10 Gbps | 1 Gbps | 10 Gbps |
| ストレージ | 10 Gbps | 1 Gbps | 10 Gbps |
| Archive サービスの略 | 10 Gbps | 1 Gbps | 10 Gbps |

> この表には、共有ストレージへのアクセスに必要な SAN の帯域幅は含まれていません。イーサネット経由（ iSCSI または FCoE ）でアクセスする共有ストレージを使用する場合は、各ホストで物理インターフェイスを別途プロビジョニングして十分な SAN の帯域幅を確保する必要があります。ボトルネックにならないように、各ホストの SAN の帯域幅として、そのホストで実行されるすべてのストレージノードの総ネットワーク帯域幅とほぼ同じ帯域幅を確保します。

上記の表を参照して、それぞれのホストに最小限必要なネットワークインターフェイスの数を確認します。これは、そのホストで実行する StorageGRID ノードの数とタイプで決まります。

たとえば、単一のホストで管理ノード、ゲートウェイノード、およびストレージノードを 1 つずつ実行するには、次の手順を実行します。

- 管理ノードにグリッドネットワークと管理ネットワークを接続する（必要な帯域幅： 10 + 1 = 11Gbps ）
- ゲートウェイノードにグリッドネットワークとクライアントネットワークを接続する（必要な帯域幅： 10 + 10 = 20Gbps ）

- ストレージノードにグリッドネットワークを接続する（必要な帯域幅： 10Gbps ）

このシナリオでは、少なくとも 11+20+10=41 Gbps のネットワーク帯域幅を提供する必要があります。 2 つの 40Gbps インターフェイスまたは 5 つの 10Gbps インターフェイスで対応できます。これらは潜在的にトランクに集約され、ホストを含む物理データセンターに対してローカルなグリッド、管理、およびクライアントのサブネットを伝送する 3 つ以上の VLAN によって共有されます。

StorageGRID クラスタのホストの物理リソースおよびネットワークリソースを設定してStorageGRID を導入する準備として推奨される方法については、使用しているLinuxプラットフォームのインストール手順のホストネットワークの設定に関する情報を参照してください。

関連情報

"Red Hat Enterprise Linux または CentOS をインストールします"

"Ubuntu または Debian をインストールします"

プラットフォームサービスとクラウドストレージプール用のネットワークとポート

## StorageGRID プラットフォームサービスまたはクラウドストレージプールを使用する場合は、デスティネーションエンドポイントに到達できるようにグリッドネットワークとファイアウォールを設定する必要があります。プラットフォームサービスには、検索統合、イベント通知、CloudMirrorレプリケーションを提供する外部サービスが含まれます。

プラットフォームサービスには、 StorageGRID ADC サービスをホストするストレージノードから外部サービスエンドポイントへのアクセスが必要です。アクセスの提供例は次のとおりです。

- ADC サービスがあるストレージノードで、ターゲットエンドポイントにルーティングする AESL エントリを使用して一意の管理ネットワークを設定します。
- クライアントネットワークが提供するデフォルトルートを使用します。この例では、信頼されていないクライアントネットワーク機能を使用して、インバウンド接続を制限できます。

また、クラウドストレージプールは、ストレージノードから、 Amazon S3 Glacier や Microsoft Azure BLOB ストレージなどの使用する外部サービスが提供するエンドポイントへのアクセスを必要とします。

デフォルトでは、プラットフォームサービスとクラウドストレージプールの通信には次のポートが使用されます。

- **80**：で始まるエンドポイントURIの場合 `http`
- **442**：で始まるエンドポイントURI `https`

エンドポイントの作成時または編集時に別のポートを指定できます。

非透過型プロキシサーバを使用する場合は、プロキシの設定で、インターネット上のエンドポイントなどの外部エンドポイントへのメッセージの送信を許可する必要もあります。プロキシの設定方法については、StorageGRID の管理を参照してください。

信頼されていないクライアントネットワークの詳細については、StorageGRID の管理手順を参照してください。プラットフォームサービスの詳細については、テナントアカウントの使用手順を参照してください。クラウドストレージプールの詳細については、情報ライフサイクル管理を使用してオブジェクトを管理する手順を参照してください。

関連情報

"ネットワークポートのリファレンス"

"グリッド入門"

"StorageGRID の管理"

"テナントアカウントを使用する"

"ILM を使用してオブジェクトを管理する"

アプライアンスノード

## StorageGRID アプライアンスのネットワークポートは、スループット、冗長性、およびフェイルオーバーの要件を満たすポートボンディングモードを使用するように設定できます。

StorageGRID アプライアンスの 10 / 25GbE ポートは、グリッドネットワークおよびクライアントネットワークへの接続用に、固定またはアグリゲートのボンディングモードで設定できます。

1GbE 管理ネットワークポートは、管理ネットワークへの接続に独立モードまたはアクティブ / バックアップモードを設定できます。

アプライアンスのインストールとメンテナンスの手順のポートボンディングモードに関する情報を参照してください。

関連情報

"SG100 SG1000サービスアプライアンス"

"SG6000 ストレージアプライアンス"

"SG5700 ストレージアプライアンス"

"SG5600 ストレージアプライアンス"

# ネットワークのインストールとプロビジョニング

## ノードの導入時とグリッドの設定時にグリッドネットワークとオプションの管理ネットワークおよびクライアントネットワークがどのように使用されるかを理解しておく必要があります。

ノードの初期導入

ノードを最初に導入するときは、ノードをグリッドネットワークに接続して、ノードがプライマリ管理ノードにアクセスできるようにする必要があります。グリッドネットワークが分離されている場合は、グリッドネットワークの外部からアクセスして設定とインストールを実行できるように、プライマリ管理ノードに管理ネットワークを設定できます。

ゲートウェイが設定されているグリッドネットワークは、導入時にノードのデフォルトゲートウェイになります。デフォルトゲートウェイを使用すると、グリッドを設定する前に、別々のサブネットにあるグリッドノー

ドがプライマリ管理ノードと通信できるようになります。

必要に応じて、 NTP サーバを含むサブネットや Grid Manager または API へのアクセスを必要とするサブネットを、グリッドサブネットとして設定することもできます。

### プライマリ管理ノードへの自動ノード登録

導入されたノードは、グリッドネットワークを使用してプライマリ管理ノードに登録されます。その後、グリッドマネージャ、を使用できます `configure-storagegrid.py` Pythonスクリプト、またはインストールAPIを使用して、グリッドを設定し、登録済みのノードを承認します。グリッド設定時に、複数のグリッドサブネットを設定できます。グリッドの設定が完了すると、グリッドネットワークゲートウェイを経由するこれらのサブネットへの静的ルートが各ノードに作成されます。

### 管理ネットワークまたはクライアントネットワークを無効にします

管理ネットワークまたはクライアントネットワークを無効にする場合は、ノードの承認プロセス中にそれらのネットワークから設定を削除するか、インストールの完了後にIP変更ツールを使用できます。リカバリとメンテナンスの手順のネットワークメンテナンスの手順に関する情報を参照してください。

関連情報

""

## インストール後のガイドライン

グリッドノードの導入と設定が完了したら、 DHCP アドレスおよびネットワーク設定の変更について、次のガイドラインに従ってください。

- DHCP を使用して IP アドレスを割り当てた場合は、使用しているネットワーク上の各 IP アドレスに対して DHCP 予約を設定します。

  DHCP は導入フェーズでのみ設定できます。設定時に DHCP を設定することはできません。

  > IP アドレスが変わるとノードがリブートします。 DHCP アドレスの変更が同時に複数のノードに影響を及ぼす場合、原因 が停止する可能性があります。

- グリッドノードの IP アドレス、サブネットマスク、およびデフォルトゲートウェイを変更する場合は、 IP 変更手順を使用する必要があります。リカバリとメンテナンスの手順のIPアドレスの設定に関する情報を参照してください。
- ルーティングやゲートウェイの変更など、ネットワーク設定を変更すると、プライマリ管理ノードおよびその他のグリッドノードへのクライアント接続が失われる可能性があります。ネットワークの変更内容によっては、接続の再確立が必要になる場合があります。

関連情報

"Red Hat Enterprise Linux または CentOS をインストールします"

"Ubuntu または Debian をインストールします"

"VMware をインストールする"

"SG100 SG1000サービスアプライアンス"

"SG6000 ストレージアプライアンス"

"SG5700 ストレージアプライアンス"

"SG5600 ストレージアプライアンス"

""

## ネットワークポートのリファレンス

ネットワークインフラが、グリッド内のノード間、および外部のクライアントやサービスとの間で内部通信および外部通信を可能にすることを確認する必要があります。内部および外部のファイアウォール、スイッチングシステム、およびルーティングシステム全体へのアクセスが必要な場合があります。

内部でのグリッドノードの通信と外部との通信に表示される詳細を使用して、必要な各ポートの設定方法を確認します。

- "内部でのグリッドノードの通信"
- "外部との通信"

### 内部でのグリッドノードの通信

StorageGRID の内部ファイアウォールは、ポート 22 、 80 、 123 、 443 を除き、グリッドネットワーク上の特定のポートへの受信接続のみを許可します（外部通信に関する情報を参照）。ロードバランサエンドポイントで定義されたポートにも接続が許可されます。

> グリッドノード間で Internet Control Message Protocol （ ICMP ）トラフィックを有効にすることを推奨します。ICMP トラフィックを許可すると、グリッドノードに到達できない場合のフェイルオーバーパフォーマンスを向上させることができます。

StorageGRID では、 ICMP と表に記載されているポートに加えて、 Virtual Router Redundancy Protocol （ VRRP; 仮想ルータ冗長プロトコル）を使用します。VRRP は、 IP プロトコル番号 112 を使用するインターネットプロトコルです。StorageGRID は、ユニキャストモードでのみ VRRP を使用します。VRRPが必要なのは、ハイアベイラビリティ（HA）グループが設定されている場合だけです。

#### **Linux** ベースのノードについてはガイドラインを参照してください

これらのいずれかのポートへのアクセスがエンタープライズネットワークポリシーで制限されている場合は、導入設定パラメータを使用して導入時にポートを再マッピングできます。ポートの再マッピングと導入設定パラメータの詳細については、Linuxプラットフォームのインストール手順を参照してください。

#### **VMware** ベースのノードについてのガイドラインを参照してください

次のポートは、 VMware ネットワーク外部のファイアウォール制限を定義する必要がある場合にのみ設定してください。

これらのいずれかのポートへのアクセスがエンタープライズネットワークポリシーによって制限される場合は、ノードを導入する際に VMware vSphere Web Client を使用してポートを再マッピングするか、またはグ

リッドノードの導入を自動化する際に構成ファイルの設定を使用してポートを再マッピングできます。ポートの再マッピングと導入設定パラメータの詳細については、VMwareのインストール手順を参照してください。

アプライアンスストレージノードのガイドライン

これらのいずれかのポートへのアクセスがエンタープライズネットワークポリシーで制限されている場合は、StorageGRID アプライアンスインストーラを使用してポートを再マッピングできます。アプライアンスのポート再マッピングの詳細については、ストレージアプライアンスのインストール手順を参照してください。

**StorageGRID** の内部ポート

| ポート | tcp または udp です | 移動元 | 終了： | 詳細 |
|---|---|---|---|---|
| 22 | TCP | プライマリ管理ノード | すべてのノード | メンテナンス手順では、プライマリ管理ノードがポート 22 で SSH を使用して他のすべてのノードと通信できる必要があります。他のノードからの SSH トラフィックの許可は任意です。 |
| 80 | TCP | アプライアンス | プライマリ管理ノード | StorageGRID アプライアンスが、インストールを開始する目的でプライマリ管理ノードと通信するために使用します。 |
| 123 | UDP | すべてのノード | すべてのノード | ネットワークタイムプロトコルサービス。すべてのノードは、 NTP を使用して他のすべてのノードと時間を同期します。 |
| 443 | TCP | すべてのノード | プライマリ管理ノード | インストールおよびその他のメンテナンス手順の実行中に、プライマリ管理ノードにステータスを通知するために使用します。 |
| 1139 | TCP | ストレージノード | ストレージノード | ストレージノード間の内部トラフィック。 |

| | | | | |
|---|---|---|---|---|
| 1501 年 | TCP | すべてのノード | ADC を採用するストレージノード | レポート、監査、および設定の内部トラフィック。 |
| 1502 | TCP | すべてのノード | ストレージノード | S3 および Swift 関連の内部トラフィック。 |
| 1504. | TCP | すべてのノード | 管理ノード | NMS サービスのレポートおよび設定の内部トラフィック。 |
| 1505. | TCP | すべてのノード | 管理ノード | AMS サービスの内部トラフィック。 |
| 1506. | TCP | すべてのノード | すべてのノード | サーバステータスの内部トラフィック。 |
| 1507 | TCP | すべてのノード | ゲートウェイノード | ロードバランサの内部トラフィック。 |
| 1508 | TCP | すべてのノード | プライマリ管理ノード | 設定管理の内部トラフィック。 |
| 1509. | TCP | すべてのノード | アーカイブノード | アーカイブノードの内部トラフィック。 |
| 1511. | TCP | すべてのノード | ストレージノード | メタデータの内部トラフィック。 |
| 5353 | UDP | すべてのノード | すべてのノード | 必要に応じて、フルグリッドの IP 変更、およびインストール、拡張、リカバリ時のプライマリ管理ノードの検出に使用します。 |
| 7001 | TCP | ストレージノード | ストレージノード | Cassandra TLS ノード間クラスタ通信。 |
| 7443 | TCP | すべてのノード | 管理ノード | メンテナンス手順およびエラーレポート用の内部トラフィック。 |

| | | | | |
|---|---|---|---|---|
| 9042 | TCP | ストレージノード | ストレージノード | Cassandra クライアントポート。 |
| 9999 | TCP | すべてのノード | すべてのノード | 複数のサービスの内部トラフィック。メンテナンス手順、指標、およびネットワークの更新が含まれます。 |
| 10226 | TCP | ストレージノード | プライマリ管理ノード | StorageGRID アプライアンスが、 E シリーズの SANtricity System Manager からプライマリ管理ノードに AutoSupport メッセージを転送するために使用します。 |
| 11139 | TCP | アーカイブ / ストレージノード | アーカイブ / ストレージノード | ストレージノードとアーカイブノード間の内部トラフィック。 |
| 18000 年 | TCP | 管理 / ストレージノード | ADC を採用するストレージノード | アカウントサービスの内部トラフィック。 |
| 18001 | TCP | 管理 / ストレージノード | ADC を採用するストレージノード | アイデンティティフェデレーションの内部トラフィック。 |
| 18002 | TCP | 管理 / ストレージノード | ストレージノード | オブジェクトプロトコルに関連する内部 API トラフィック。 |
| 18003 年 | TCP | 管理 / ストレージノード | ADC を採用するストレージノード | プラットフォームサービスの内部トラフィック。 |
| 18017 年 | TCP | 管理 / ストレージノード | ストレージノード | クラウドストレージプールの Data Mover サービスの内部トラフィック。 |

| | | | | |
|---|---|---|---|---|
| 18019 年になります | TCP | ストレージノード | ストレージノード | イレイジャーコーディング用のチャンクサービスの内部トラフィック。 |
| 18082 年 | TCP | 管理 / ストレージノード | ストレージノード | S3 関連の内部トラフィック。 |
| 18083 年 | TCP | すべてのノード | ストレージノード | Swift 関連の内部トラフィック。 |
| 18200 年 | TCP | 管理 / ストレージノード | ストレージノード | クライアント要求に関する追加の統計。 |
| 19000 年 | TCP | 管理 / ストレージノード | ADC を採用するストレージノード | Keystone サービスの内部トラフィック。 |

- 関連情報 *

"外部との通信"

"Red Hat Enterprise Linux または CentOS をインストールします"

"Ubuntu または Debian をインストールします"

"VMware をインストールする"

"SG100 SG1000サービスアプライアンス"

"SG6000 ストレージアプライアンス"

"SG5700 ストレージアプライアンス"

"SG5600 ストレージアプライアンス"

外部との通信

クライアントは、コンテンツの取り込みと読み出しを行うためにグリッドノードと通信する必要があります。使用するポートは、選択したオブジェクトストレージプロトコルによって異なります。これらのポートはクライアントからアクセスできる必要があります。

エンタープライズネットワークポリシーでいずれかのポートへのアクセスが制限されている場合は、ロードバランサエンドポイントを使用してユーザ定義のポートへのアクセスを許可できます。信頼されていないクライアントネットワーク機能を使用すると、ロードバランサエンドポイントポートにのみアクセスを許可できます。

SMTP 、 DNS 、 SSH 、 DHCP などのシステムとプロトコルを使用するには、ノードを導入する際にポートを再マッピングする必要があります。ただし、バランサエンドポイントを再マッピングしないでください。ポートの再マッピングの詳細については、ご使用のプラットフォームのインストール手順を参照してください。

次の表に、ノードに着信するトラフィックに使用されるポートを示します。

このリストには、ロードバランサエンドポイントとして設定されている可能性のあるポートは含まれていません。詳細については、ロードバランサエンドポイントの設定手順を参照してください。

| ポート | **tcp** または **udp** です | プロトコル | 移動元 | 終了： | 詳細 |
|---|---|---|---|---|---|
| 22 | TCP | SSH | サービスラップトップ | すべてのノード | コンソールの手順を実行するには、 SSH アクセスまたはコンソールアクセスが必要です。必要に応じて、ポート 22 の代わりに 2022 を使用できます。 |
| 25 | TCP | SMTP | 管理ノード | E メールサーバ | アラートおよび E メールベースの AutoSupport に使用されます。Email Servers ページを使用して、デフォルトのポート設定である 25 を上書きできます。 |
| 53 | TCP / UDP | DNS | すべてのノード | DNS サーバ | ドメインネームシステムに使用します。 |
| 67 | UDP | DHCP | すべてのノード | DHCP サービス | 必要に応じて、 DHCP ベースのネットワーク設定のサポートに使用します。dhclient サービスは、静的に設定されたグリッドに対しては実行されません。 |
| 68 | UDP | DHCP | DHCP サービス | すべてのノード | 必要に応じて、 DHCP ベースのネットワーク設定のサポートに使用します。dhclient サービスは、静的 IP アドレスを使用するグリッドに対しては実行されません。 |
| 80 | TCP | HTTP | ブラウザ | 管理ノード | ポート 80 は、管理ノードのユーザインターフェイス用のポート 443 にリダイレクトされます。 |

| ポート | **tcp** または **udp** です | プロトコル | 移動元 | 終了： | 詳細 |
| --- | --- | --- | --- | --- | --- |
| 80 | TCP | HTTP | ブラウザ | アプライアンス | ポート 80 は、 StorageGRID アプライアンスインストーラ用のポート 8443 にリダイレクトされます。 |
| 80 | TCP | HTTP | ADC を採用するストレージノード | AWS | AWS または HTTP を使用するその他の外部サービスに送信されるプラットフォームサービスのメッセージに使用します。エンドポイントの作成時に、テナントのデフォルトの HTTP ポート設定である 80 よりも優先される。 |
| 80 | TCP | HTTP | ストレージノード | AWS | HTTP を使用する AWS ターゲットに送信されるクラウドストレージプール要求。クラウドストレージプールを設定するときに、グリッド管理者がデフォルトの HTTP ポート設定である 80 を上書きできます。 |
| 111 | TCP / UDP | rpcbind | NFS クライアント | 管理ノード | NFS ベースの監査エクスポート（ portmap ）で使用します。<br>• 注：このポートは、 NFS ベースの監査エクスポートが有効になっている場合にのみ必要です。 |
| 123 | UDP | NTP | プライマリ NTP ノード | 外部 NTP | ネットワークタイムプロトコルサービス。プライマリ NTP ソースとして選択されたノードは、クロックの時間と外部 NTP の時間ソースとの同期も行います。 |
| 137 | UDP | NETBIOS | SMB クライアント | 管理ノード | NetBIOS サポートを必要とするクライアントの SMB ベースの監査エクスポートで使用します。<br>• 注：このポートは、 SMB ベースの監査エクスポートが有効になっている場合にのみ必要です。 |

| ポート | **tcp** または **udp** です | プロトコル | 移動元 | 終了： | 詳細 |
| --- | --- | --- | --- | --- | --- |
| 138 | UDP | NETBIOS | SMB クライアント | 管理ノード | NetBIOS サポートを必要とするクライアントの SMB ベースの監査エクスポートで使用します。<br>• 注：このポートは、 SMB ベースの監査エクスポートが有効になっている場合にのみ必要です。 |
| 139 | TCP | SMB | SMB クライアント | 管理ノード | NetBIOS サポートを必要とするクライアントの SMB ベースの監査エクスポートで使用します。<br>• 注：このポートは、 SMB ベースの監査エクスポートが有効になっている場合にのみ必要です。 |
| 161 | TCP / UDP | SNMP | SNMP クライアント | すべてのノード | SNMP ポーリングに使用します。すべてのノードは基本情報を提供し、管理ノードはアラートデータとアラームデータも提供します。設定時のデフォルトの UDP ポートは 161 です。<br>• 注：このポートは必須です。 SNMP が設定されている場合にのみノードファイアウォールで開かれます。SNMP を使用する場合は、代替ポートを設定できます。<br>• 注： StorageGRID での SNMP の使用については、ネットアップの営業担当者にお問い合わせください。 |

| ポート | **tcp** または **udp** です | プロトコル | 移動元 | 終了： | 詳細 |
| --- | --- | --- | --- | --- | --- |
| 162 | TCP / UDP | SNMP 通知 | すべてのノード | 通知の送信先 | アウトバウンド SNMP 通知およびトラップのデフォルトの UDP ポートは 162 です。<br>• 注：このポートは、SNMP が有効で通知の送信先が設定されている場合にのみ必要です。SNMP を使用する場合は、代替ポートを設定できます。<br>• 注： StorageGRID での SNMP の使用については、ネットアップの営業担当者にお問い合わせください。 |
| 389 | TCP / UDP | LDAP | ADC を採用するストレージノード | Active Directory / LDAP | アイデンティティフェデレーション用の Active Directory または LDAP サーバに接続するために使用します。 |
| 443 | TCP | HTTPS | ブラウザ | 管理ノード | Grid Manager と Tenant Manager にアクセスするために Web ブラウザと管理 API クライアントで使用します。 |
| 443 | TCP | HTTPS | 管理ノード | Active Directory | シングルサインオン（ SSO ）が有効な場合に、 Active Directory に接続する管理ノードで使用します。 |
| 443 | TCP | HTTPS | アーカイブノード | Amazon S3 | アーカイブノードから Amazon S3 にアクセスするために使用します。 |
| 443 | TCP | HTTPS | ADC を採用するストレージノード | AWS | AWS または HTTPS を使用するその他の外部サービスに送信されるプラットフォームサービスのメッセージに使用します。エンドポイントの作成時に、テナントがデフォルトの HTTP ポート設定である 443 を上書きできる。 |

| ポート | **tcp** または **udp** です | プロトコル | 移動元 | 終了： | 詳細 |
| --- | --- | --- | --- | --- | --- |
| 443 | TCP | HTTPS | ストレージノード | AWS | HTTPS を使用する AWS ターゲットに送信されるクラウドストレージプール要求。クラウドストレージプールの設定時に、グリッド管理者がデフォルトの HTTPS ポート設定である 443 を上書きできます。 |
| 445 | TCP | SMB | SMB クライアント | 管理ノード | SMB ベースの監査エクスポートで使用します。<br>• 注：このポートは、 SMB ベースの監査エクスポートが有効になっている場合にのみ必要です。 |
| 903. | TCP | NFS | NFS クライアント | 管理ノード | NFSベースの監査エクスポートで使用します（`rpc.mountd`）。<br>• 注：このポートは、 NFS ベースの監査エクスポートが有効になっている場合にのみ必要です。 |
| 2022 | TCP | SSH | サービスラップトップ | すべてのノード | コンソールの手順を実行するには、 SSH アクセスまたはコンソールアクセスが必要です。必要に応じて、 2022 の代わりにポート 22 を使用できます。 |
| 2049 | TCP | NFS | NFS クライアント | 管理ノード | NFS ベースの監査エクスポート（ NFS ）で使用します。<br>• 注：このポートは、 NFS ベースの監査エクスポートが有効になっている場合にのみ必要です。 |

| ポート | **tcp** または **udp** です | プロトコル | 移動元 | 終了： | 詳細 |
| --- | --- | --- | --- | --- | --- |
| 5696 | TCP | KMIP | アプライアンス | KMS | ノードの暗号化用に設定されたアプライアンスから Key Management Server （ KMS ）へのキー管理 Interoperability Protocol （ KMIP ）の外部トラフィック（ StorageGRID アプライアンスインストーラの KMS 構成のページで別のポートを指定している場合を除く）。 |
| 8022 | TCP | SSH | サービスラップトップ | すべてのノード | ポート 8022 で SSH を使用すると、サポートとトラブルシューティング用に、アプライアンスと仮想ノードプラットフォーム上のベースのオペレーティングシステムへのアクセスが許可されます。このポートは Linux ベース（ベアメタル）ノードには使用されず、グリッドノード間または通常運用時にアクセス可能である必要はありません。 |
| 「 8082 」 | TCP | HTTPS | S3 クライアント | ゲートウェイノード | ゲートウェイノードへのS3関連の外部トラフィック（HTTPS）。 |
| 8083 | TCP | HTTPS | Swift クライアント | ゲートウェイノード | ゲートウェイノードへのSwift関連の外部トラフィック（HTTPS）。 |
| 8084 | TCP | HTTP | S3 クライアント | ゲートウェイノード | ゲートウェイノードへのS3関連の外部トラフィック（HTTP）。 |
| 8085 | TCP | HTTP | Swift クライアント | ゲートウェイノード | ゲートウェイノードへのSwift関連の外部トラフィック（HTTP）。 |
| 8443 | TCP | HTTPS | ブラウザ | 管理ノード | 任意。Grid Manager にアクセスするために Web ブラウザと管理 API クライアントで使用されます。を使用して、 Grid Manager と Tenant Manager の通信を分離できます。 |

| ポート | **tcp** または **udp** です | プロトコル | 移動元 | 終了： | 詳細 |
| --- | --- | --- | --- | --- | --- |
| 9022 | TCP | SSH | サービスラップトップ | アプライアンス | サポートとトラブルシューティングのために、構成前モードでの StorageGRID アプライアンスへのアクセスを許可します。このポートは、グリッドノード間で、または通常運用時にアクセス可能である必要はありません。 |
| 9091 | TCP | HTTPS | 外部の Grafana サービス | 管理ノード | 外部の Grafana サービスが StorageGRID Prometheus サービスへのセキュアなアクセスに使用します。<br><br>• 注：このポートは、証明書ベースの Prometheus アクセスが有効になっている場合にのみ必要です。 |
| ポート 1 | TCP | HTTPS | ブラウザ | 管理ノード | 任意。Tenant Manager にアクセスするために Web ブラウザと管理 API クライアントで使用します。を使用して、Grid Manager と Tenant Manager の通信を分離できます。 |
| 18082 年 | TCP | HTTPS | S3 クライアント | ストレージノード | ストレージノードへのS3関連の外部トラフィック（HTTPS）。 |
| 18083 年 | TCP | HTTPS | Swift クライアント | ストレージノード | ストレージノードへのSwift関連の外部トラフィック（HTTPS）。 |
| 18084 年 | TCP | HTTP | S3 クライアント | ストレージノード | ストレージノードへのS3関連の外部トラフィック（HTTP）。 |
| 18085 年になります | TCP | HTTP | Swift クライアント | ストレージノード | ストレージノードへのSwift関連の外部トラフィック（HTTP）。 |

関連情報

"内部でのグリッドノードの通信"

"Red Hat Enterprise Linux または CentOS をインストールします"

"Ubuntu または Debian をインストールします"

"VMware をインストールする"

"SG100 SG1000サービスアプライアンス"

"SG6000 ストレージアプライアンス"

"SG5700 ストレージアプライアンス"

"SG5600 ストレージアプライアンス"

# ソフトウェアをインストールしてアップグレードする

## Red Hat Enterprise Linux または CentOS をインストールします

Red Hat Enterprise LinuxまたはCentOSの環境にStorageGRID ソフトウェアをインストールする方法について説明します。

- "インストールの概要"
- "計画と準備"
- "仮想グリッドノードの導入"
- "グリッドの設定とインストールの完了"
- "インストールの自動化"
- "インストール REST API の概要"
- "次の手順"
- "インストールに関する問題のトラブルシューティング"
- "/etc/sysconfig/network-scripts の例"

### インストールの概要

Red Hat Enterprise Linux （ RHEL ）環境または CentOS Linux 環境への StorageGRID システムのインストールは、主に 3 つの手順で行われます。

1. * 準備 * ：計画と準備の際に、次のタスクを実行します。
   - StorageGRID のハードウェア要件とストレージ要件について説明します。
   - ネットワークを適切に設定するためのStorageGRID ネットワークの詳細について説明します。詳細については、StorageGRID のネットワークに関するガイドラインを参照してください。
   - StorageGRID グリッドノードのホストとして使用する物理サーバまたは仮想サーバを決めて準備する。
   - 準備したサーバで、次の作業を行います。
     - Linux をインストールします
     - ホストネットワークを設定する
     - ホストストレージを設定する
     - Docker をインストールする
     - StorageGRID ホストサービスをインストールする
2. * 導入 * ：適切なユーザインターフェイスを使用してグリッドノードを導入します。導入したグリッドノードは、 StorageGRID システムの一部として作成され、 1 つ以上のネットワークに接続されます。
   a. Linux のコマンドライン構成ファイルとノード構成ファイルを使用して、手順 1 で準備したホストに

ソフトウェアベースのグリッドノードを導入します。

b. StorageGRID アプライアンスノードを導入するには、 StorageGRID アプライアンスインストーラを使用します。

> ハードウェア固有の設置と統合の手順は、 StorageGRID インストール手順 には含まれていません。StorageGRID アプライアンスのインストール方法については、使用するアプライアンスのインストールとメンテナンスの手順を参照してください。

3. 構成：すべてのノードが導入されたら、StorageGRIDWebscaleを使ってグリッドを構成し、インストールを完了します。

ここでは、標準的なアプローチで StorageGRID システムを導入して設定する方法を推奨します。次の代替アプローチに関する情報も参照してください。

- Ansible、Puppet、Chefなどの標準的なオーケストレーションフレームワークを使用して、RHELまたはCentOSのインストール、ネットワークとストレージの設定、DockerとStorageGRID ホストサービスのインストール、および仮想グリッドノードの導入を行う。
- Python 設定スクリプト（インストールアーカイブに付属）を使用して、 StorageGRID システムの導入と設定を自動化します。
- Python 設定スクリプト（インストールアーカイブまたは StorageGRID アプライアンスインストーラで入手可能）を使用して、アプライアンスグリッドノードの導入と設定を自動化する。
- StorageGRID 環境を高度に開発する場合は、インストール REST API を使用して StorageGRID グリッドノードのインストールを自動化します。

関連情報

"計画と準備"

"仮想グリッドノードの導入"

"グリッドの設定とインストールの完了"

"インストールの自動化"

"インストール REST API の概要"

"ネットワークガイドライン"

## 計画と準備

### グリッドノードの導入および StorageGRID グリッドの設定を行う前に、手順 を完了するためのステップと要件を把握しておく必要があります。

StorageGRID の導入手順と設定手順を実行するには、 StorageGRID システムのアーキテクチャと運用に関する十分な知識が必要です。

一度に 1 つ以上のサイトを導入できますが、ストレージノードが少なくとも 3 つ必要であるという最小要件をすべてのサイトが満たしている必要があります。

StorageGRID のインストールを開始する前に、次の作業を実行する必要があります

- ノードごとの CPU や RAM の最小要件など、 StorageGRID のコンピューティング要件を確認します。
- トラフィックの分離、セキュリティ、および管理性の向上のために複数のネットワークをサポートする StorageGRID の仕組みについて理解し、 StorageGRID の各ノードに接続するネットワークを決めます。

  StorageGRID のネットワークに関するガイドラインを参照してください。

- 各タイプのグリッドノードのストレージ要件とパフォーマンス要件を把握します。
- 導入予定の StorageGRID ノードの数とタイプに応じて、それらをサポートできる十分なリソースを備えた一連のサーバ（物理、仮想、またはその両方）を特定します。
- 物理ホストに対して、サービスを中断することなく定期的なメンテナンスを実行する場合は、ノード移行の要件を確認します。
- すべてのネットワーク情報を事前に収集します。DHCP を使用している場合を除き、各グリッドノードに割り当てる IP アドレス、および使用される Domain Name System （ DNS ；ドメインネームシステム）サーバと Network Time Protocol （ NTP ；ネットワークタイムプロトコル）サーバの IP アドレスを収集してください。
- StorageGRID アプライアンスを含む必要なすべてのハードウェアを仕様に従って設置、接続、設定します。

  ハードウェア固有の設置と統合の手順は、 StorageGRID インストール手順 には含まれていません。StorageGRID アプライアンスのインストール方法については、使用するアプライアンスのインストールとメンテナンスの手順を参照してください。

- 使用する導入ツールと設定ツールを決定します。

関連情報

"ネットワークガイドライン"

"SG100 SG1000サービスアプライアンス"

"SG6000 ストレージアプライアンス"

"SG5700 ストレージアプライアンス"

"SG5600 ストレージアプライアンス"

前提要件

## StorageGRID をインストールする前に、必要な情報やデータ、機器を揃えておく必要があります。

| 項目 | 注： |
| --- | --- |
| NetApp StorageGRID ライセンス | デジタル署名された有効なネットアップライセンスが必要です。<br>• 注： StorageGRID インストールアーカイブには、グリッドのテストとコンセプトの実証に使用できる非本番環境のライセンスが含まれています。 |

| 項目 | 注： |
| --- | --- |
| StorageGRID インストールアーカイブ | StorageGRID インストールアーカイブをダウンロードし、ファイルを展開する必要があります。 |
| サービスラップトップ | StorageGRID システムは、サービスラップトップを介してインストールされます。<br><br>サービスラップトップには次のものが必要です。<br><br>• ネットワークポート<br>• SSH クライアント（ PuTTY など）<br>• サポートされている Web ブラウザ |
| StorageGRID のドキュメント | • リリースノート<br>• StorageGRID の管理手順 |

関連情報

"StorageGRID インストールファイルのダウンロードと展開"

"Web ブラウザの要件"

"StorageGRID の管理"

"リリースノート"

**StorageGRID** インストールファイルのダウンロードと展開

## StorageGRID インストールアーカイブをダウンロードし、必要なファイルを展開する必要があります。

手順

1. ネットアップの StorageGRID ダウンロードページにアクセスします。

   "ネットアップのダウンロード： StorageGRID"

2. 最新のリリースをダウンロードするボタンを選択するか、ドロップダウンメニューから別のバージョンを選択して、「 * Go * 」を選択します。
3. ネットアップアカウントのユーザ名とパスワードを使用してサインインします。
4. 「注意 / 必ずお読みください」という記述が表示されたら、それを読んでチェックボックスを選択してください。

   StorageGRID リリースのインストール後に、必要な修正プログラムを適用する必要があります。詳細については、リカバリおよびメンテナンスの手順にあるホットフィックス手順 を参照してください。

5. エンドユーザライセンス契約を読み、チェックボックスをオンにして、「 * 同意して続行 * 」を選択します。

6. [Install StorageGRID *（インストールソフトウェアのインストール）]列で、適切なソフトウェアを選択します。

   をダウンロードします `.tgz` または `.zip` 使用するプラットフォームに対応したアーカイブファイルです。

   これらの圧縮ファイルには、Red Hat Enterprise LinuxまたはCentOSのRPMファイルとスクリプトが含まれています。

   を使用します `.zip` ファイルサービスラップトップでWindowsを実行している場合。

7. アーカイブファイルを保存して展開します。
8. 次のリストから必要なファイルを選択します。

   必要なファイルは、計画したグリッドトポロジおよび StorageGRID システムの導入方法によって異なります。

   次の表に示すパスは、展開されたインストールアーカイブによってインストールされた最上位ディレクトリに対する相対パスです。

| パスとファイル名 | 説明 |
| --- | --- |
| | StorageGRID ダウンロードファイルに含まれているすべてのファイルについて説明するテキストファイル。 |
| | 製品サポートのない無償ライセンス。 |
| | RHEL ホストまたは CentOS ホストに StorageGRID ノードイメージをインストールするための RPM パッケージ。 |
| | RHEL ホストまたは CentOS ホストに StorageGRID ホストサービスをインストールするための RPM パッケージ。 |
| 導入スクリプトツール | 説明 |
| | StorageGRID システムの設定を自動化するための Python スクリプト。 |
| | StorageGRID アプライアンスの設定を自動化するための Python スクリプト。 |
| | で使用するサンプル構成ファイル `configure-storagegrid.py` スクリプト： |
| | シングルサインオンが有効な場合にグリッド管理 API にサインインするために使用できる Python スクリプトの例。 |

| パスとファイル名 | 説明 |
| --- | --- |
| | で使用する空の構成ファイル `configure-storagegrid.py` スクリプト： |
| | StorageGRID コンテナ導入用の RHEL ホストまたは CentOS ホストを設定するためのサンプルの Ansible のロールとプレイブック。必要に応じて、ロールまたはプレイブックをカスタマイズできます。 |

関連情報

""

**CPU** と **RAM** の要件

## StorageGRID ソフトウェアをインストールする前に、ハードウェアの確認と設定を行って、 StorageGRID システムをサポートできる状態にしておきます。

サポートされているサーバについては、 Interoperability Matrix を参照してください。

各 StorageGRID ノードに必要な最小リソースは次のとおりです。

- CPU コア：ノードあたり 8 個
- RAM ：システムで実行されている StorageGRID 以外のソフトウェアの合計 RAM 容量によって、ノードあたり 24 GB 以上、システム RAM の合計容量から 2 ~ 16 GB 削減されます

それぞれの物理ホストまたは仮想ホストで実行する StorageGRID ノードの数が、利用可能な CPU コアや物理 RAM を超えないようにしてください。ホストが StorageGRID 専用ではない場合（非推奨）は、他のアプリケーションのリソース要件も考慮する必要があります。

> CPU とメモリの使用状況を定期的に監視して、ワークロードに継続的に対応できるようにします。たとえば、仮想ストレージノードの RAM 割り当てと CPU 割り当てを 2 倍にすると、StorageGRID アプライアンスノードの場合と同様のリソースが提供されます。また、ノードあたりのメタデータの量が 500GB を超える場合は、ノードあたりの RAM を 48GB 以上に増やすことを検討してください。オブジェクトメタデータストレージの管理、 Metadata Reserved Space 設定の拡張、 CPU とメモリの使用状況の監視については、 StorageGRID の管理、監視、アップグレードの手順を参照してください。

基盤となる物理ホストでハイパースレッディングが有効である場合は、ノードあたり 8 個の仮想コア（ 4 個の物理コア）で構成できます。基盤となる物理ホストでハイパースレッディングが有効でない場合は、ノードあたり 8 個の物理コアを用意する必要があります。

仮想マシンをホストとして使用する場合、 VM のサイズと数を制御可能であれば、 StorageGRID ノードごとに 1 つの VM を使用し、それに応じて VM のサイズを設定する必要があります。

本番環境では、複数のストレージノードを同じ物理ストレージハードウェアまたは仮想ホストで実行しないでください。単一の StorageGRID 環境の各ストレージノードをそれぞれ独自の分離された障害ドメインに配置するようにします。単一のハードウェア障害が単一のストレージノードにしか影響しないようにすることで、オブジェクトデータの耐久性と可用性を最大限に高めることができます。

ストレージ要件に関する情報も参照してください。

関連情報

"NetApp Interoperability Matrix Tool で確認できます"

"ストレージとパフォーマンスの要件"

"StorageGRID の管理"

"トラブルシューティングを監視します"

"ソフトウェアをアップグレードする"

ストレージとパフォーマンスの要件

## 初期設定と将来のストレージ拡張に対応できる十分なスペースを確保できるよう、StorageGRID ノードのストレージ要件を把握しておく必要があります。

StorageGRID ノードに必要なストレージは、 3 つの論理カテゴリに分類されます。

- * コンテナプール * - ノードコンテナ用のパフォーマンス階層（ 10K SAS または SSD ）のストレージ。 StorageGRID ノードをサポートするホストに Docker をインストールして設定するときに、 Docker ストレージドライバに割り当てられます。
- * システムデータ *— システムデータとトランザクションログのノード単位の永続的ストレージ用のパフォーマンス階層（ 10K SAS または SSD ）ストレージ。 StorageGRID ホストサービスで個々のノードにマッピングされて使用されます。
- * オブジェクトデータ *— オブジェクトデータとオブジェクトメタデータの永続的なストレージを実現するパフォーマンス階層（ 10K SAS または SSD ）のストレージと大容量階層（ NL-SAS / SATA ）のストレージ。

カテゴリに関係なく、いずれのストレージにも RAID ベースのブロックデバイスを使用する必要があります。非冗長ディスク、 SSD 、または JBOD はサポートされていません。いずれのカテゴリのストレージにも、共有またはローカルのどちらかの RAID ストレージを使用できます。ただし、 StorageGRID のノード移行機能を使用する場合は、システムデータとオブジェクトデータの両方を共有ストレージに格納する必要があります。

パフォーマンス要件

コンテナプールのボリューム、システムデータのボリューム、およびオブジェクトメタデータのボリュームのパフォーマンスは、システム全体のパフォーマンスに大きく影響します。ボリュームのディスクパフォーマンスが、レイテンシ、 1 秒あたりの入出力操作（ IOPS ）、スループットの点で適切になるように、それらのボリュームにはパフォーマンス階層（ 10K SAS または SSD ）のストレージを使用します。オブジェクトデータの永続的なストレージには、大容量階層（ NL-SAS / SATA ）のストレージを使用できます。

コンテナプール、システムデータ、およびオブジェクトデータ用のボリュームでは、ライトバックキャッシュを有効にする必要があります。キャッシュは、保護されたメディアまたは永続的なメディアに配置する必要があります。

**NetApp AFF** ストレージを使用するホストの要件

StorageGRID ノードが NetApp AFF システムから割り当てられたストレージを使用している場合は、ボリュームで FabricPool 階層化ポリシーが有効になっていないことを確認してください。StorageGRID ノードで使用するボリュームで FabricPool による階層化を無効にすることで、トラブルシューティングとストレージの

処理がシンプルになります。

> StorageGRID を使用して StorageGRID に関連するデータを FabricPool 自体に階層化しないでください。StorageGRID データを StorageGRID に階層化すると、トラブルシューティングと運用がより複雑になります。

必要なホストの数

各 StorageGRID サイトに、少なくとも 3 つのストレージノードが必要です。

> 本番環境では、 1 つの物理ホストまたは仮想ホストで複数のストレージノードを実行しないでください。各ストレージノードに専用のホストを使用すると、分離された障害ドメインが提供されます。

管理ノードやゲートウェイノードなど、他のタイプのノードは、同じホストに導入するか、必要に応じて独自の専用ホストに導入することができます。

各ホストのストレージボリュームの数

次の表に、ホストに導入するノードの種類別に、各ホストに必要なストレージボリューム（ LUN ）の数と各 LUN に必要な最小サイズを示します。

テストで使用できる LUN の最大サイズは 39TB です。

> これらはホストごとの数値を示したものであり、グリッド全体の数値ではありません。

| **LUN** の目的 | ストレージのカテゴリ | **LUN** の数 | **LUN** あたりの最小サイズ |
|---|---|---|---|
| Docker ストレージプール | コンテナプール | 1. | ノードの総数 × 100GB |
| `/var/local` ボリューム | システムデータ | このホストのノードごとに 1 個 | 90GB |
| ストレージノード | オブジェクトデータ | このホストのストレージノードごとに 3 個<br>• 注：ソフトウェアベースのストレージノードには 1~16 個のストレージボリュームを設定できます。 3 個以上のストレージボリュームを推奨します。 | 4、000GBを参照してください ストレージノードのストレージ要件 を参照してください。 |
| 管理ノードの監査ログ | システムデータ | このホストの管理ノードごとに 1 個 | 200GB |

| LUN の目的 | ストレージのカテゴリ | LUN の数 | LUN あたりの最小サイズ |
| --- | --- | --- | --- |
| 管理ノードのテーブル | システムデータ | このホストの管理ノードごとに 1 個 | 200GB |

設定されている監査レベル、 S3 オブジェクトキー名などのユーザ入力のサイズ、保持する必要がある監査ログデータの量によっては、各管理ノードの監査ログ LUN のサイズを増やす必要があります。原則として、 S3 処理ごとに約 1 KB の監査データが生成されることから、 200GB の LUN で 1 日あたり 7 、 000 万件の処理、 1 秒あたり 2 ~ 3 日間で 800 件の処理がサポートされることになります。

ホストの最小ストレージスペース

次の表に、各タイプのノードに必要な最小ストレージスペースを示します。この表を参照して、ホストに導入するノードの種類に応じて、ストレージカテゴリごとにホストで確保しなければならない最小ストレージ容量を決定できます。

ディスクの Snapshot を使用してグリッドノードをリストアすることはできません。各タイプのノードのリカバリとメンテナンスの手順を参照してください。

| ノードのタイプ | コンテナプール | システムデータ | オブジェクトデータ |
| --- | --- | --- | --- |
| ストレージノード | 100 GB | 90GB | 4 、 000GB |
| 管理ノード | 100 GB | 490GB （ 3 個の LUN ） | _ 該当なし _ |
| ゲートウェイノード | 100 GB | 90GB | _ 該当なし _ |
| アーカイブノード | 100 GB | 90GB | _ 該当なし _ |

例：ホストのストレージ要件の計算

同じホストに 3 つのノードを導入することを計画しているとします。ストレージノードが 1 つ、管理ノードが 1 つ、ゲートウェイノードが 1 つです。ホストには少なくとも 9 個のストレージボリュームを用意する必要があります。ノードコンテナ用にパフォーマンス階層のストレージが 300GB 以上、システムデータとトランザクションログ用にパフォーマンス階層のストレージが 670GB 以上、オブジェクトデータ用に容量階層のストレージが 12TB 以上、それぞれ必要になります。

| ノードのタイプ | LUN の目的 | LUN の数 | LUN サイズ |
| --- | --- | --- | --- |
| ストレージノード | Docker ストレージプール | 1. | 300GB （ 100GB/ ノード ） |
| ストレージノード | `/var/local` ボリューム | 1. | 90GB |
| ストレージノード | オブジェクトデータ | 3. | 4 、 000GB |

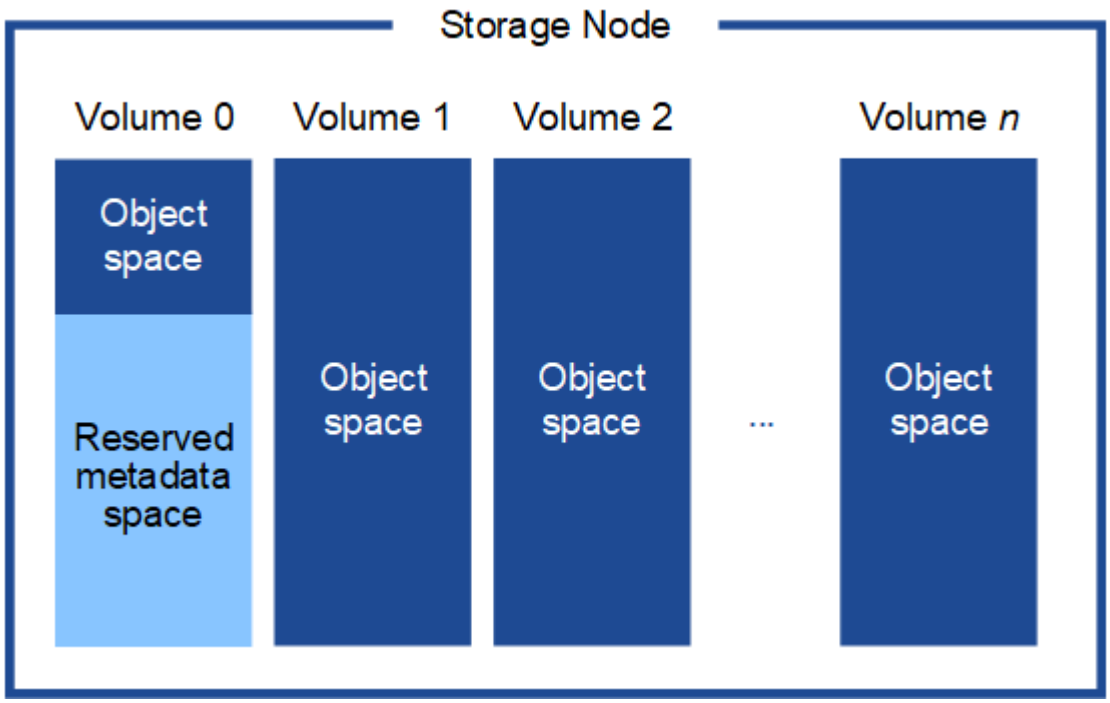
| ノードのタイプ | LUN の目的 | LUN の数 | LUN サイズ |
| --- | --- | --- | --- |
| 管理ノード | /var/local ボリューム | 1. | 90GB |
| 管理ノード | 管理ノードの監査ログ | 1. | 200GB |
| 管理ノード | 管理ノードのテーブル | 1. | 200GB |
| ゲートウェイノード | /var/local ボリューム | 1. | 90GB |
| • 合計 * | | • 9 * | • コンテナプール： * 300GB<br>• システムデータ： *670GB<br>• オブジェクトデータ： 12 、 000GB |

ストレージノードのストレージ要件

ソフトウェアベースのストレージノードのストレージボリューム数は 1~16 個までにすることを推奨します。-3 個以上のストレージボリュームを使用することを推奨します。各ストレージボリュームのサイズは 4TB 以上にします。

アプライアンスストレージノードには、最大 48 個のストレージボリュームを設定できます。

図に示すように、 StorageGRID は各ストレージノードのストレージボリューム 0 にオブジェクトメタデータ用のスペースをリザーブします。ストレージボリューム 0 の残りのスペースとストレージノード内のその他のストレージボリュームは、オブジェクトデータ専用に使用されます。



冗長性を確保し、オブジェクトメタデータを損失から保護するために、 StorageGRID は各サイトのシステム内のすべてのオブジェクトにメタデータのコピーを 3 つずつ格納します。オブジェクトメタデータの 3 つのコピーが各サイトのすべてのストレージノードに均等に分散されます。

新しいストレージノードのボリューム 0 にスペースを割り当てる場合は、そのノードのすべてのオブジェクトメタデータの一部に対して十分なスペースを確保する必要があります。

- 少なくとも 4TB をボリューム 0 に割り当てる必要があります。

> ストレージノードでストレージボリュームを 1 つしか使用していない場合に、そのボリュームに 4TB 以下を割り当てると、ストレージノードが起動時にストレージ読み取り専用状態になり、オブジェクトメタデータのみが格納される可能性があります。

- 新しいStorageGRID 11.5システムをインストールするときに、各ストレージノードに128GB以上のRAMがある場合は、ボリューム0に8TB以上を割り当てる必要があります。ボリューム 0 に大きな値を設定すると、各ストレージノードでメタデータに使用できるスペースが増加する可能性があります。
- サイトに複数のストレージノードを設定する場合は、可能であればボリューム 0 にも同じ設定を使用します。サイトにサイズが異なるストレージノードがある場合、ボリューム 0 が最も小さいストレージノードがそのサイトのメタデータ容量を決定します。

詳細については、StorageGRID の管理手順を参照し、「オブジェクト・メタデータ・ストレージの管理」を検索してください。

"StorageGRID の管理"

関連情報

"ノードコンテナの移行要件"

""

ノードコンテナの移行要件

## ノード移行機能を使用すると、ホスト間でノードを手動で移動できます。通常、両方のホストが同じ物理データセンターにあります。

ノード移行を使用すると、グリッドの運用を中断せずに物理ホストのメンテナンスを実行できます。単に、すべての StorageGRID ノードを一度に 1 つずつ別のホストに移動してから、物理ホストをオフラインにします。ノードを 1 つずつ移行するため、それぞれのダウンタイムはごくわずかであり、グリッドサービスの運用や可用性には影響しません。

StorageGRID のノード移行機能を使用する場合は、いくつかの追加の要件を満たす必要があります。

- 単一の物理データセンターのホスト間で一貫したネットワークインターフェイス名を使用する必要があります
- StorageGRID のメタデータとオブジェクトのリポジトリボリューム用に、単一の物理データセンターのすべてのホストからアクセスできる共有ストレージを用意する必要があります。たとえば、 NetApp E シリーズストレージアレイなどを使用できます。

仮想ホストを使用する場合、基盤となるハイパーバイザーレイヤで VM の移行がサポートされていれば、その機能を StorageGRID のノード移行機能の代わりに使用することができます。その場合、これらの追加要件は無視してかまいません。

移行またはハイパーバイザーのメンテナンスを実行する前に、ノードを正常にシャットダウンしてください。グリッドノードのシャットダウンについては、リカバリとメンテナンスの手順を参照してください。

#### VMware のライブマイグレーションはサポートされていません

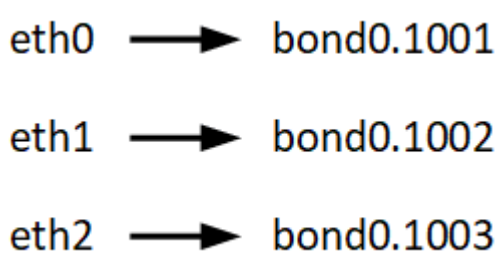
OpenStack Live Migration と VMware のライブ vMotion 原因 ：仮想マシンのクロック時間を急に進むことができるため、どのタイプのグリッドノードでもサポートされていません。まれにではありますが、クロック時間が不正確だとデータや設定の更新が失われることがあります。

コールドマイグレーションはサポートされています。コールドマイグレーションでは、 StorageGRID ノードをホスト間で移行する前にシャットダウンします。リカバリとメンテナンスの手順で、グリッドノードをシャットダウンする方法については、手順 を参照してください。

#### 一貫したネットワークインターフェイス名

ノードを別のホストに移動するにあたり、 StorageGRID ホストサービスでは、ノードが現在の場所で使用している外部ネットワーク接続を新しい場所でもそのまま使用できるようにする必要があります。これは、ホスト内で一貫したネットワークインターフェイス名を使用することで実現されます。

たとえば、 Host1 で実行されている StorageGRID NodeA で、インターフェイスのマッピングが次のように設定されているとします。




矢印の左側は、 StorageGRID コンテナ内から見た従来のインターフェイス（グリッドネットワーク、管理ネットワーク、およびクライアントネットワークのインターフェイス）です。矢印の右側は、これらのネットワークを提供する実際のホストインターフェイスに対応しています。この 3 つの VLAN インターフェイスは、同じ物理インターフェイスボンドに従属します。

この NodeA を Host2 に移行するとします。Host2 に bond0.1001 、 bond0.1002 、および bond0.1003 という名前のインターフェイスがある場合、 Host2 では同じ名前のインターフェイスが Host1 と同じ接続を提供すると仮定して、移動が許可されます。Host2 に同じ名前のインターフェイスがなければ、移動は許可されません。

複数のホスト間で一貫したネットワーク・インターフェイス名を得るには’さまざまな方法があります例については’ホスト・ネットワークの構成を参照してください

#### 共有ストレージ

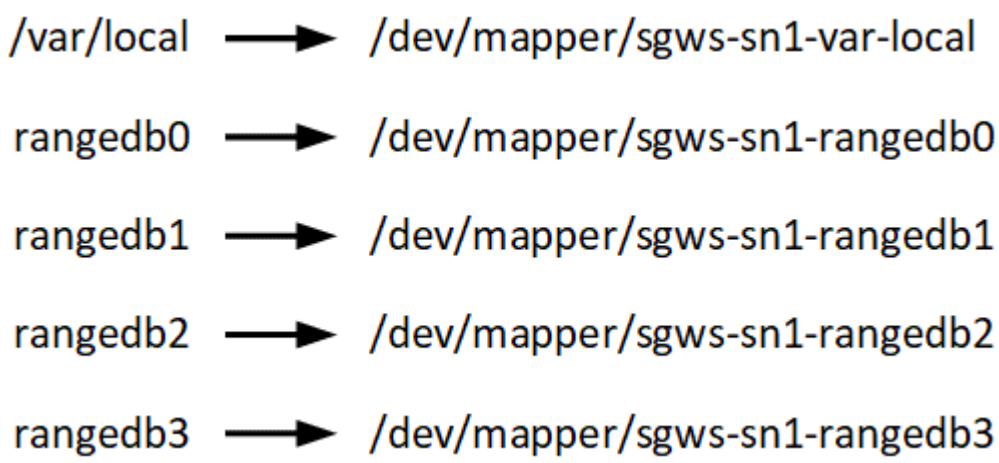
オーバーヘッドを抑えて迅速にノードを移行するために、 StorageGRID のノード移行機能ではノードのデータの物理的な移動は行いません。代わりに、エクスポート処理とインポート処理を組み合わせて、次のようにノードが移行されます。

1. 「ノードのエクスポート」操作中に、 HostA で実行されているノードコンテナから永続的な状態の少量のデータが抽出され、そのノードのシステムデータボリュームにキャッシュされます。そのあと、 HostA のノードコンテナのインスタンス化が解除されます。

2. 「ノードのインポート」操作中に、 HostA と同じネットワークインターフェイスマッピングおよびブロックストレージマッピングを使用する HostB 上のノードコンテナがインスタンス化されます。次に、キャッシュされた永続状態データが新しいインスタンスに挿入されます。

この処理では、ノードのすべてのシステムデータボリュームとオブジェクトストレージボリュームに HostA と HostB の両方からアクセスできないと移行は実行できません。また、 HostA と HostB で同じ LUN を参照するように、同じ名前を使用してノードにマッピングされている必要があります。

次の例は、StorageGRID ストレージノードのブロックデバイスマッピング用の解決策 を示しています。これらのホストではDMマルチパスを使用しており、でaliasフィールドを使用しています `/etc/multipath.conf` すべてのホストで使用できる一貫性のあるわかりやすいブロックデバイス名を提供します。




関連情報

"ホストネットワークを設定する"

""

**Web** ブラウザの要件

サポートされている Web ブラウザを使用する必要があります。

| **Web** ブラウザ | サポートされる最小バージョン |
| --- | --- |
| Google Chrome | 87 |
| Microsoft Edge の場合 | 87 |
| Mozilla Firefox | 84 |

ブラウザウィンドウの幅を推奨される値に設定してください。

| ブラウザの幅 | ピクセル |
| --- | --- |
| 最小（ Minimum ） | 1024 |

| ブラウザの幅 | ピクセル |
| --- | --- |
| 最適 | 1280 |

導入ツール

## StorageGRID のインストールのすべてまたは一部を自動化するとメリットが得られる場合があります。

導入を自動化すると、次のいずれかの場合に役立ちます。

- 物理ホストや仮想ホストの導入と設定に Ansible 、 Puppet 、 Chef などの標準のオーケストレーションフレームワークをすでに使用している場合。
- 複数の StorageGRID インスタンスを導入する場合。
- 大規模で複雑な StorageGRID インスタンスを導入する場合。

StorageGRID ホストサービスはパッケージでインストールされ、構成ファイルで制御されます。構成ファイルは、手動インストール時に対話形式で作成できるほか、あらかじめ用意して（またはプログラム化して）標準のオーケストレーションフレームワークを使用した自動インストールに使用できます。StorageGRID には、 StorageGRID アプライアンスと StorageGRID システム全体（「グリッド」）の設定を自動化するためのオプションの Python スクリプトが用意されています。これらのスクリプトは直接使用することも、StorageGRID インストール REST API の使用方法を調べることもできます。グリッドの導入ツールや設定ツールを独自に開発する際の参考としても使用できます。

StorageGRID の導入のすべてまたは一部を自動化する場合は'インストール・プロセスを開始する前に'インストールの自動化を参照してください

関連情報

"インストール REST API の概要"

"インストールの自動化"

ホストを準備します

## StorageGRID の物理ホストまたは仮想ホストの準備作業として、次の手順を実行する必要があります。これらの手順は、Ansible、Puppet、Chefなどの標準のサーバ設定フレームワークを使用して、ほとんどまたはすべて自動化することができます。

関連情報

"StorageGRID ホストサービスのインストールと設定を自動化する"

**Linux** をインストールしています

## すべてのグリッドのホストに Red Hat Enterprise Linux または CentOS Linux をインストールする必要があります。サポートされているバージョンの一覧については、 NetApp Interoperability Matrix Tool を参照してください。

手順

1. ディストリビュータの指示または標準の手順 に従って、すべての物理グリッドホストまたは仮想グリッドホストに Linux をインストールします。

   標準の Linux インストーラを使用している場合は、可能であれば「コンピューティングノード」のソフトウェア構成、または「最小限のインストール」ベース環境を選択することを推奨します。グラフィカルデスクトップ環境はインストールしないでください。

2. Extras チャネルを含むすべてのホストがパッケージリポジトリにアクセスできることを確認します。

   これらの追加パッケージは、このインストール手順 の後半で必要になる場合があります。

3. スワップが有効になっている場合：

   a. 次のコマンドを実行します。 `$ sudo swapoff --all`

   b. からすべてのスワップエントリを削除します `/etc/fstab` をクリックして設定を保持します。

   スワップを完全に無効にできないと、パフォーマンスが大幅に低下する可能性があります

関連情報

"NetApp Interoperability Matrix Tool で確認できます"

ホストネットワークを設定する

## ホストへの Linux のインストールの完了後、このあとに導入する StorageGRID ノードにマッピングする一連のネットワークインターフェイスを準備するために、各ホストでいくつかの追加の設定が必要になることがあります。

必要なもの

- StorageGRID のネットワークに関するガイドラインを確認しておきます。

  "ネットワークガイドライン"

- ノードコンテナの移行要件に関する情報を確認しておく必要があります。

  "ノードコンテナの移行要件"

- 仮想ホストを使用している場合は、MACアドレスのクローニングに関する考慮事項と推奨事項を確認してから、ホストネットワークを設定してください。

  "MAC アドレスのクローニングに関する考慮事項と推奨事項"

VM をホストとして使用する場合は、仮想ネットワークアダプタとして VMXNET 3 を選択する必要があります。VMware E1000 ネットワークアダプタは、特定の Linux のディストリビューションで導入された StorageGRID コンテナで接続の問題が発生しました。

このタスクについて

グリッドノードは、グリッドネットワークにアクセスできる必要があります。また、管理ネットワークとクライアントネットワークにアクセスすることもできます。このアクセスを確立するには、ホストの物理インター

フェイスを各グリッドノードの仮想インターフェイスに関連付けるマッピングを作成します。ホストインターフェイスを作成するときにわかりやすい名前を使用すると、すべてのホストへの導入が簡単になり、移行も可能になります。

ホストと 1 つ以上のノードで、同じインターフェイスを共有できます。たとえば、ホストアクセス用とノード管理ネットワークアクセス用のインターフェイスに同じものを使用すると、ホストとノードをメンテナンスしやすくなります。ホストと個々のノードで同じインターフェイスを共有できますが、 IP アドレスはすべて異なっている必要があります。IP アドレスはノード間やホストと任意のノード間で共有できません。

グリッドネットワークのインターフェイスについては、ホストのすべての StorageGRID ノードで同じホストネットワークインターフェイスを使用したり、ノードごとに異なるホストネットワークインターフェイスを使用したり、任意のインターフェイスを使用したりできます。ただし、通常は、単一のホストのグリッドネットワークと管理ネットワークの両方のインターフェイス、またはいずれかのノードのグリッドネットワークのインターフェイスと別のホストのクライアントネットワークのインターフェイスに同じホストネットワークインターフェイスを使用することはありません。

このタスクはさまざまな方法で実行できます。たとえば、仮想マシンをホストとする環境でホストごとに 1 つまたは 2 つの StorageGRID ノードを導入する場合は、ハイパーバイザーで正しい数のネットワークインターフェイスを作成し、 1 対 1 のマッピングを使用できます。本番環境用のベアメタルホストに複数のノードを導入する場合は、 Linux ネットワークスタックの VLAN と LACP のサポートを利用してフォールトトレランスと帯域幅の共有を実現できます。以降のセクションでは、これら両方の例について詳細なアプローチを紹介します。これらのいずれかを使用する必要はありません。それぞれのニーズに合わせてアプローチを選択できます。

> ボンドデバイスやブリッジデバイスをコンテナネットワークインターフェイスとして直接使用しないでください。これにより、カーネル問題 が原因で発生するノードの起動が妨げられ、コンテナネームスペース内のボンドデバイスおよびブリッジデバイスで MACVLAN が使用される可能性があります。代わりに、 VLAN ペアや仮想イーサネット（ veth ）ペアなどの非ボンディングデバイスを使用してください。このデバイスをノード構成ファイルのネットワークインターフェイスとして指定してください。

関連情報

"ネットワークガイドライン"

"ノードコンテナの移行要件"

"ノード構成ファイルを作成しています"

### MAC アドレスのクローニングに関する考慮事項と推奨事項

MACアドレスのクローニングでは、Dockerコンテナでホストの MACアドレスが使用され、指定したアドレスまたはランダムに生成されたアドレスの MACアドレスがホストで使用されます。プロミスキャスモードのネットワーク設定を使用しないようにするには、 MAC アドレスのクローニングを使用します。

### MAC クローニングのイネーブル化

環境によっては、管理ネットワーク、グリッドネットワーク、およびクライアントネットワークに専用の仮想 NIC を使用できるため、 MAC アドレスのクローニングによってセキュリティを強化できます。Dockerコンテナでホスト上の専用NICのMACアドレスを使用すると、プロミスキャスモードのネットワーク設定を回避できます。

MAC アドレスクローニングは、仮想サーバ環境で使用するためのものであり、物理アプライアンスのすべての構成で正常に機能しない場合があります。

MAC クローニングのターゲットインターフェイスがビジー状態のためにノードを起動できない場合は、ノードを起動する前にリンクを「停止」に設定しなければならないことがあります。また、リンクが稼働しているときに仮想環境でネットワークインターフェイス上の MAC クローニングが実行されないことがあります。インターフェイスがビジーなためにノードで MAC アドレスの設定が失敗してノードが起動しなかった場合は、問題 を修正する前にリンクを「停止」に設定することがあります。

MAC アドレスクローニングは、デフォルトでは無効になっており、ノード設定キーで設定する必要があります。StorageGRID をインストールするときに有効にする必要があります。

ネットワークごとに 1 つのキーがあります。

- `ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`
- `GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`
- `CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`

キーを「true」に設定すると、DockerコンテナでホストのNICのMACアドレスが使用されます。さらに、ホストは指定されたコンテナネットワークの MAC アドレスを使用します。デフォルトでは、コンテナアドレスはランダムに生成されたアドレスですが、を使用して設定した場合は、です `_NETWORK_MAC` ノード設定キー。アドレスを代わりに使用します。ホストとコンテナの MAC アドレスは常に異なります。

ハイパーバイザーでプロミスキャスモードも有効にせずに仮想ホストの MAC クローニングを有効にすると、ホストのインターフェイスを使用して原因 Linux ホストのネットワークが停止する可能性があります。

**MAC** クローン作成の使用例

MAC クローニングでは、次の 2 つのユースケースを検討します。

- MACクローン作成が有効になっていない場合 `_CLONE_MAC` ノード構成ファイルのキーが設定されていないか「false」に設定されていない場合、ホストはホストNIC MACを使用し、にMACを指定しないかぎりコンテナにStorageGRIDによって生成されたMACが含まれます `_NETWORK_MAC` キーを押します。アドレスがに設定されている場合 `_NETWORK_MAC` キーを指定すると、コンテナのアドレスがに指定されます `_NETWORK_MAC` キーを押します。このキーの設定では、プロミスキャスモードを使用する必要があります。
- MACクローン作成が有効になっている場合 `_CLONE_MAC` ノード構成ファイルのキーは「true」に設定されています。コンテナではホストNIC MACを使用し、でMACを指定しないかぎりStorageGRIDによって生成されたMACをホストで使用します `_NETWORK_MAC` キーを押します。アドレスがに設定されている場合 `_NETWORK_MAC` キー。ホストは、生成されたアドレスではなく、指定されたアドレスを使用します。このキーの設定では、プロミスキャスモードは使用しないでください。

MAC アドレスのクローニングを使用せずに、ハイパーバイザーによって割り当てられた MAC アドレス以外の MAC アドレスのデータをすべてのインターフェイスが送受信できるようにする場合は、次の手順を実行します。 仮想スイッチおよびポートグループレベルのセキュリティプロパティが、無差別モード、 MAC アドレスの変更、および Forged Transmits の **Accept** に設定されていることを確認します。仮想スイッチに設定された値は、ポートグループレベルの値によって上書きできるため、両方のレベルで設定が同じであることを確認してください。

MAC クローニングをイネーブルにするには、を参照してください "ノード構成ファイルの作成手順"。

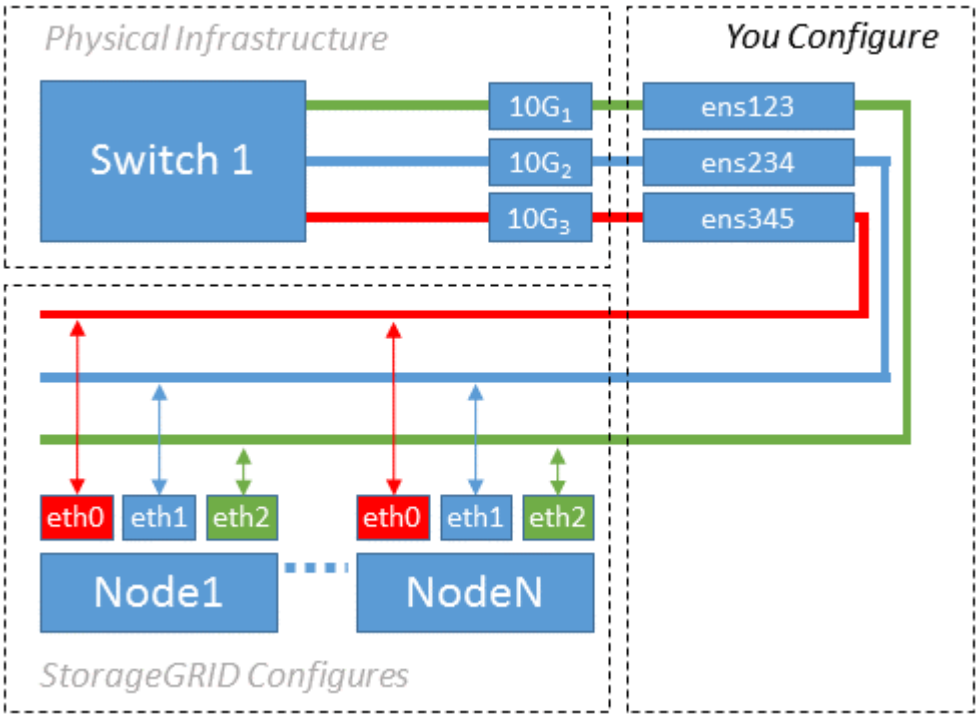
**MAC** クローニングの例

MAC アドレスが 11 ： 22 ： 33 ： 44 ： 55 ： 66 のホストでインターフェイス ens256 の MAC クローニングをイネーブルにし、ノード構成ファイルで次のキーを使用する例：

- `ADMIN_NETWORK_TARGET = ens256`
- `ADMIN_NETWORK_MAC = b2:9c:02:c2:27:10`
- `ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC = true`
- 結果 * ： ens256 のホスト MAC は b2 ： 9C ： 02 ： c2 ： 27 ： 10 で、管理ネットワーク MAC は 11 ： 22 ： 33 ： 44 ： 55 ： 66 です

例 **1** ：物理 **NIC** または仮想 **NIC** への **1** 対 **1** のマッピング

例 1 では、ホスト側の設定がほとんどまたはまったく必要ない単純な物理インターフェイスのマッピングについて説明します。




Linuxオペレーティングシステムによってが作成されます `ensXYZ` インターフェイスは、インストール時、ブート時、またはインターフェイスがホットアドされたときに自動的に実行されます。インターフェイスがブート後に自動的に起動するように設定されていることを確認する以外に必要な設定はありません。どちらを決定

する必要があります `ensXYZ` は、あとで設定プロセスで正しいマッピングを指定できるように、どのStorageGRID ネットワーク（グリッド、管理、またはクライアント）に対応しています。

この図は複数の StorageGRID ノードを示していますが、通常はこの構成をシングルノードの VM に使用します。

スイッチ 1 が物理スイッチの場合は、インターフェイス 10G1 ～ 10G3 に接続されたポートをアクセスモードに設定し、適切な VLAN に配置する必要があります。

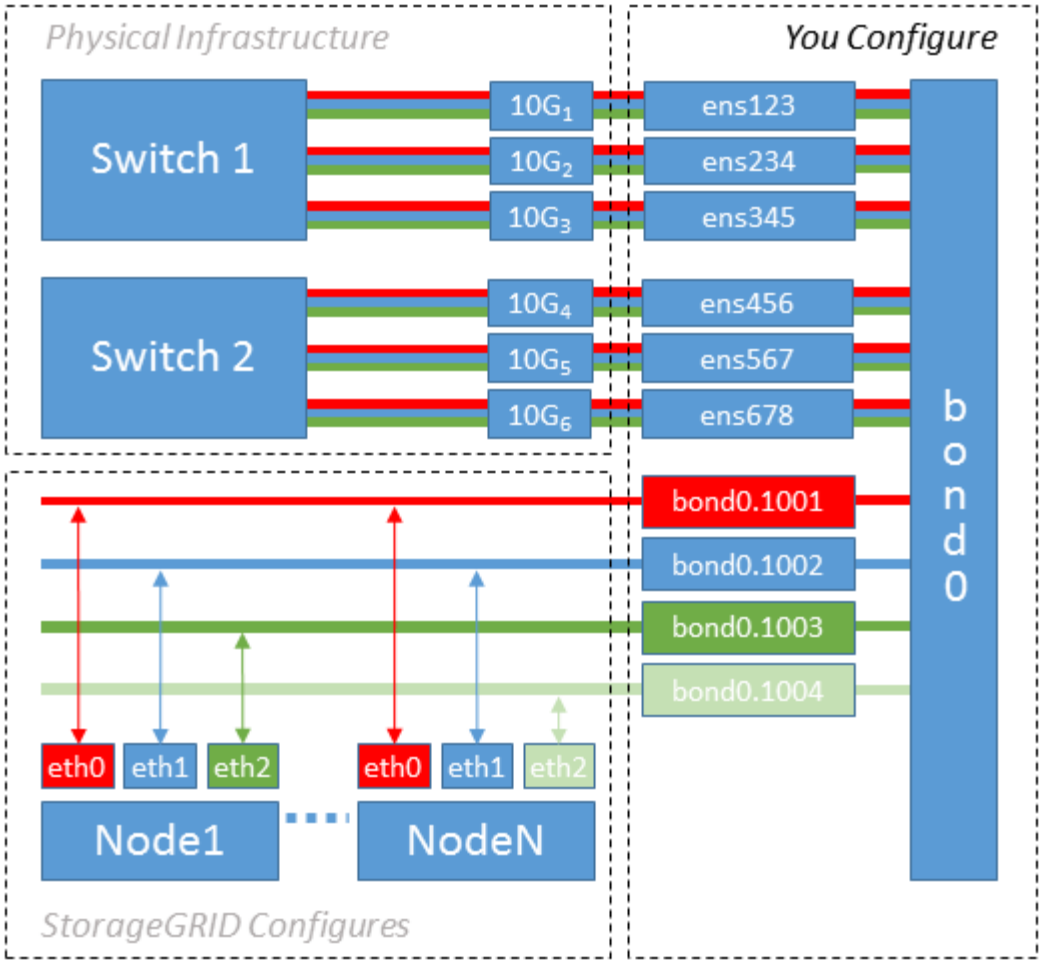
例 **2** ： **LACP** ボンドを使用した **VLAN** の伝送

例 2 は、ネットワークインターフェイスのボンディングおよび使用している Linux ディストリビューションでの VLAN インターフェイスの作成に関する十分な知識があることを前提としています。

例 2 では、汎用の柔軟な VLAN ベースのスキームを使用して、使用可能なすべてのネットワーク帯域幅を単一のホスト上のすべてのノードで共有する方法について説明します。この例は、ベアメタルホストに特に該当します。

この例を理解するために、各データセンターにグリッドネットワーク、管理ネットワーク、クライアントネットワーク用に 3 つのサブネットがあるとします。サブネットは個別の VLAN （ 1001 、 1002 、 1003 ）上にあり、 LACP ボンディングされたトランクポート（ bond0 ）でホストに提示されます。この場合、ボンドに bond0.1001 、 bond0.1002 、および bond0.1003 の 3 つの VLAN インターフェイスを設定します。

同じホスト上のノードネットワークに別々の VLAN とサブネットが必要な場合は、ボンドに VLAN インターフェイスを追加してホストにマッピングできます（図の bond0.1004 と表示）。




手順

1. StorageGRID ネットワークの接続に使用するすべての物理ネットワークインターフェイスを単一の LACP ボンドとしてまとめます。

   すべてのホストのボンドに同じ名前（ bond0 など）を使用してください。

2. このボンドを関連する「物理デバイス」として使用するVLANインターフェイスを作成します," `using the standard VLAN interface naming convention `physdev-name.VLAN ID`。

   手順 1 と 2 のそれぞれについて、ネットワークリンクの反対側の終端にあるエッジスイッチで適切な設定を行う必要があります。エッジスイッチのポートも LACP ポートチャネルに集約してトランクとして設定し、必要なすべての VLAN を許可する必要があります。

   このホストごとのネットワーク構成スキームに使用できるサンプルのインターフェイス構成ファイルが提供されています。

関連情報

"/etc/sysconfig/network-scripts の例"

ホストストレージを設定しています

## 各ホストにブロックストレージボリュームを割り当てる必要があります。

必要なもの

以下のトピックで、このタスクを実行するために必要な情報を確認しておきます。

- "ストレージとパフォーマンスの要件"
- "ノードコンテナの移行要件"

このタスクについて

ブロック・ストレージ・ボリューム（ LUN ）をホストに割り当てるときは ' ストレージ要件の表を使用して ' 次の項目を決定します

- 各ホストに必要なボリュームの数（そのホストに導入するノードの数とタイプに応じて異なる）
- 各ボリュームのストレージのカテゴリ（システムデータまたはオブジェクトデータ）
- 各ボリュームのサイズ

ホストに StorageGRID ノードを導入するときは、この情報に加え、各物理ボリュームに Linux から割り当てられた永続的な名前を使用します。

これらのボリュームがホストに認識されることだけ確認すれば、ボリュームをパーティショニング、フォーマット、マウントする必要はありません。

「raw」形式の特殊なデバイス・ファイルは使用しないでください (`/dev/sdb`たとえば、）ボリューム名のリストを作成する際に、これらのファイルはホストのリブート時に変わることがあり、システムの適切な運用に影響します。`iSCSI LUN`およびデバイスマッパーマルチパスを使用する場合は、でマルチパスのエイリアスを使用することを検討してください `/dev/mapper` ディレクトリ、特にSANトポロジに共有ストレージへの冗長ネットワークパスが含まれている場合。または、システムで作成されたのソフトリンクをで使用することもできます `/dev/disk/by-path/` をクリックします。

例：

```
ls -l
$ ls -l /dev/disk/by-path/
total 0
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:00:07.1-ata-2 -> ../../sr0
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0 ->
../../sda
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part1
-> ../../sda1
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part2
-> ../../sda2
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:1:0 ->
../../sdb
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:2:0 ->
../../sdc
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:3:0 ->
../../sdd
```

結果はインストールごとに異なります。

これらのブロックストレージボリュームのそれぞれにわかりやすい名前を割り当てると、 StorageGRID の最初のインストールや以降のメンテナンスの手順が簡単になります。デバイスマッパーマルチパスドライバを使用して共有ストレージボリュームへのアクセスを冗長化する場合は、を使用することができます `alias` フィールドに入力します `/etc/multipath.conf` ファイル。

例：

```
multipaths {
     multipath {
          wwid 3600a09800059d6df00005df2573c2c30
          alias docker-storage-volume-hostA
     }
     multipath {
          wwid 3600a09800059d6df00005df3573c2c30
          alias sgws-adm1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df4573c2c30
          alias sgws-adm1-audit-logs
     }
     multipath {
          wwid 3600a09800059d6df00005df5573c2c30
          alias sgws-adm1-tables
     }
     multipath {
          wwid 3600a09800059d6df00005df6573c2c30
          alias sgws-gw1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df7573c2c30
          alias sgws-sn1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df7573c2c30
          alias sgws-sn1-rangedb-0
     }
     …
```

これにより、でブロックデバイスとして表示されるエイリアスが原因 されます `/dev/mapper` ホスト上のディレクトリ。設定処理やメンテナンス処理の際にブロックストレージボリュームの指定が必要となったときに、わかりやすい、検証が容易な名前を指定できます。

StorageGRID のノード移行やデバイスマッパーマルチパスの使用をサポートするために共有ストレージを設定する場合は、共通のファイルを作成してインストールすることができます `/etc/multipath.conf` 共同配置されたすべてのホスト。各ホストで使用する Docker ストレージボリュームが異なる点に注意してください。エイリアスを使用し、各 Docker ストレージボリュームの LUN のエイリアスにターゲットのホスト名を含めると覚えやすいので、この方法で設定することを推奨します。

関連情報

"Docker をインストールする"

**Docker**ストレージボリュームを設定する

## Dockerをインストールする前に、Dockerストレージボリュームをフォーマットして、にマウントする必要があります `/var/lib/docker`。

このタスクについて

Dockerストレージボリュームにローカルストレージを使用する予定で、を含むホストパーティションに十分なスペースがある場合は、以下の手順をスキップできます `/var/lib`。

手順

1. Docker ストレージボリュームにファイルシステムを作成します。

```
sudo mkfs.ext4 docker-storage-volume-device
```

2. Docker ストレージボリュームをマウントします。

```
sudo mkdir -p /var/lib/docker
sudo mount docker-storage-volume-device /var/lib/docker
```

3. /etc/fstab に docker -storage-volume-device のエントリを追加します。

   これにより、ホストのリブート後にストレージボリュームが自動的に再マウントされます。

**Docker** をインストールする

## Red Hat Enterprise LinuxまたはCentOSでは、StorageGRID システムはDockerコンテナの集合として実行されます。StorageGRID をインストールする前に、 Docker をインストールする必要があります。

手順

1. 使用している Linux ディストリビューションの手順に従って Docker をインストールします。

   Docker が Linux ディストリビューションに含まれていない場合は、 Docker の Web サイトからダウンロードできます。

2. 次の 2 つのコマンドを実行して、 Docker が有効化され、起動されたことを確認します。

```
sudo systemctl enable docker
```

```
sudo systemctl start docker
```

3. 次のコマンドを入力して、必要なバージョンの Docker がインストールされたことを確認します。

```
sudo docker version
```

クライアントとサーバのバージョンが1.10.3以降である必要があります。

```
Client:
  Version: 1.10.3
  API version: 1.22
  Package version: docker-common-1.10.3-46.el7.14.x86_64
  Go version: go1.6.2
  Git commit: 5206701-unsupported
  Built: Mon Aug 29 14:00:01 2016
  OS/Arch: linux/amd64

Server:
  Version: 1.10.3
  API version: 1.22
  Package version: docker-common-1.10.3-46.el7.14.x86_64
  Go version: go1.6.2
  Git commit: 5206701-unsupported
  Built: Mon Aug 29 14:00:01 2016
  OS/Arch: linux/amd64
```

関連情報

"ホストストレージを設定しています"

**StorageGRID** ホストサービスをインストールしています

## StorageGRID ホストサービスをインストールするには、 StorageGRID RPM パッケージを使用します。

このタスクについて

以下の手順では、 RPM パッケージからホストサービスをインストールする方法について説明します。また、インストールアーカイブに含まれている Yum リポジトリメタデータを使用して、 RPM パッケージをリモートでインストールすることもできます。使用している Linux オペレーティングシステムの Yum リポジトリに

関する手順を参照してください。

手順

1. 各ホストに StorageGRID RPM パッケージをコピーするか、共有ストレージに置きます。

   たとえば、に配置します `/tmp` ディレクトリ。次の手順でコマンドの例を使用できます。

2. 各ホストに root アカウントまたは sudo 権限を持つアカウントでログインし、次のコマンドをこの順序で実行します。

```
sudo yum --nogpgcheck localinstall /tmp/StorageGRID-Webscale-Images-version-SHA.rpm
```

```
sudo yum --nogpgcheck localinstall /tmp/StorageGRID-Webscale-Service-version-SHA.rpm
```

> まずイメージパッケージをインストールし、次にサービスパッケージをインストールする必要があります。

> パッケージを以外のディレクトリに配置した場合は `/tmp`をクリックし、使用したパスに応じてコマンドを変更します。

## 仮想グリッドノードの導入

Red Hat Enterprise LinuxホストまたはCentOSホストに仮想グリッドノードを導入するには、すべてのノードのノード構成ファイルを作成し、それらのファイルを検証してから、StorageGRID ホストサービスを開始してノードを起動します。StorageGRID アプライアンスストレージノードを導入する必要がある場合は、すべての仮想ノードを導入したあとに、アプライアンスのインストールとメンテナンスの手順を参照してください。

- "ノード構成ファイルを作成しています"
- "StorageGRID 構成を検証しています"
- "StorageGRID ホストサービスを開始しています"

関連情報

"SG100 SG1000サービスアプライアンス"

"SG5600 ストレージアプライアンス"

"SG5700 ストレージアプライアンス"

"SG6000 ストレージアプライアンス"

# ノード構成ファイルは、ノードを起動して適切なネットワークおよびブロックストレージリソースに接続するために StorageGRID ホストサービスで必要となる情報をまとめた小さいテキストファイルです。ノード構成ファイルは仮想ノードに使用され、アプライアンスノードには使用されません。

## ノード構成ファイルの配置場所

各StorageGRID ノードの構成ファイルをに配置する必要があります `/etc/storagegrid/nodes` ノードを実行するホスト上のディレクトリ。たとえば、HostAで管理ノード、ゲートウェイノード、およびストレージノードを1つずつ実行する場合は、3つのノード構成ファイルをに配置する必要があります `/etc/storagegrid/nodes` をクリックします。構成ファイルは、 vim や nano などのテキストエディタを使用して各ホストで直接作成することも、別の場所で作成して各ホストに移動することもできます。

## ノード構成ファイルの名前

構成ファイルの名前は、の形式で指定します `node-name.conf`、ここで `node-name` は、ノードに割り当てる名前です。この名前は StorageGRID インストーラに表示され、ノード移行などのノードのメンテナンス処理で使用されます。

ノード名は次のルールに従って付ける必要があります。

- 一意である必要があります
- 1 文字目はアルファベットにする必要があります
- A~Z と a~z のアルファベットを使用できます
- 0~9 の数字を使用できます
- 1 つまたは複数のハイフン（ `-` ）を含めることができます。
- を含めない32文字以内で指定します `.conf` 内線番号

内のすべてのファイル `/etc/storagegrid/nodes` この命名規則に従っていないデータは、ホストサービスで解析されません。

グリッドでマルチサイトトポロジを使用する場合の一般的なノード名は次のようになります。

```
site-nodetype-nodenumber.conf
```

たとえば、のように指定します `dc1-adm1.conf` データセンター1の最初の管理ノード用、および `dc2-sn3.conf` データセンター2の3つ目のストレージノード。ただし、すべてのノード名がルールに従っていれば、別の名前にしてもかまいません。

## ノード構成ファイルの内容

構成ファイルには、キーと値のペアが 1 行に 1 つずつ含まれています。キーと値のペアごとに、次のルールに従う必要があります。

- キーと値は等号で区切る必要があります (=)と空白(オプション)。

- キーにスペースを含めることはできません。
- 値にはスペースを含めることができます。
- 先頭または末尾の空白は無視されます。

キーの種類に応じて、すべてのノードで必要なものと省略可能なもの、特定のノードタイプでのみ必要なものがあります。

次の表に、サポートされているすべてのキーについて、使用可能な値を示します。中央の列：

- R * ：必須 + BP ：ベストプラクティス + O ：オプション

| キーを押します | **R** 、 **BP** 、または **O** | 価値 |
| --- | --- | --- |
| ADMIN_IP を指定します | BP | このノードが属するグリッドのプライマリ管理ノードのグリッドネットワークの IPv4 アドレス。GRID_NETWORK_IP で指定した値を Node_type=VM_Admin_Node および ADMIN_NETWORK_role = Primary のグリッドノードに使用します。このパラメータを省略すると、 mDNS を使用してプライマリ管理ノードの検出が試行されます。<br><br>「グリッドノードによるプライマリ管理ノードの検出」を参照してください。<br><br>• 注 * ：この値は無視されます。また、プライマリ管理ノードでは禁止される場合があります。 |
| ADMIN_NETWORK_CONFIG | o | DHCP 、 STATIC 、または DISABLED |
| ADMIN_NETWORK_ESL | o | このノードが管理ネットワークゲートウェイ経由で通信する CIDR 表記のサブネットをカンマで区切ったリスト。<br><br>例：172.16.0.0/21、172.17.0.0/21 |

| キーを押します | **R** 、 **BP** 、または **O** | 価値 |
| --- | --- | --- |
| ADMIN_NETWORK_GATEWAY | O （ * R * ） | このノードのローカルの管理ネットワークゲートウェイの IPv4 アドレス。ADMIN_NETWORK_IP および ADMIN_NETWORK_MASK で定義されるサブネットに属している必要があります。この値は、 DHCP によって設定されたネットワークでは無視されます。<br><br>• 注 * ：このパラメータは、 ADMIN_NETWORK_ESL が指定されている場合は必須です。<br><br>例<br><br>• 1.1.1.1<br>• 10.224.81 |
| ADMIN_NETWORK_IP | o | このノードの管理ネットワークにおける IPv4 アドレス。このキーが必要なのは、 ADMIN_NETWORK_CONFIG = STATIC の場合だけです。それ以外の値の場合は指定しないでください。<br><br>例<br><br>• 1.1.1.1<br>• 10.224.81 |
| ADMIN_NETWORK_MAC | o | コンテナ内の管理ネットワークインターフェイスの MAC アドレス。<br><br>このフィールドはオプションです。省略すると、 MAC アドレスが自動的に生成されます。<br><br>6 つの 16 進数値をコロンで区切って指定する必要があります。<br><br>例：b2：9C：02：c2：27：10 |

| キーを押します | **R** 、 **BP** 、または **O** | 価値 |
| --- | --- | --- |
| ADMIN_NETWORK_MASK | o | このノードの管理ネットワークにおける IPv4 ネットマスク。このキーが必要なのは、ADMIN_NETWORK_CONFIG = STATIC の場合だけです。それ以外の値の場合は指定しないでください。<br><br>例<br><br>• 255.255.255.0<br>• 255.255.248.0と入力します |
| ADMIN_NETWORK_MTU を指定します | o | このノードの管理ネットワークでの最大伝送ユニット（ MTU ）。ADMIN_NETWORK_CONFIG = DHCP の場合は指定しないでください。この値を指定する場合、 1280 ～ 9216 の範囲で指定する必要があります。省略すると、 1500 が使用されます。<br><br>ジャンボフレームを使用する場合は、 MTU を 9000 などのジャンボフレームに適した値に設定します。それ以外の場合は、デフォルト値のままにします。<br><br>• 重要 * ：ネットワークの MTU 値は、ノードが接続されているスイッチポートに設定された値と一致する必要があります。そうしないと、ネットワークパフォーマンスの問題やパケット損失が発生する可能性があります。<br><br>例<br><br>• 1 、 500<br>• 8、192です |

| キーを押します | **R** 、 **BP** 、または **O** | 価値 |
| --- | --- | --- |
| ADMIN_NETWORK_TARGET | BP | StorageGRID ノードで管理ネットワークのアクセスに使用するホストデバイスの名前。ネットワークインターフェイス名のみがサポートされています。通常、GRID_NETWORK_TARGET または CLIENT_NETWORK _TARGET に指定したインターフェイス名とは別のインターフェイス名を使用します。<br><br>• 注：ボンドデバイスやブリッジデバイスをネットワークターゲットとして使用しないでください。ボンドデバイスの上に VLAN （または他の仮想インターフェイス）を設定するか、ブリッジと仮想イーサネット（ veth ）のペアを使用します。<br><br>*ベストプラクティス：*管理ネットワークのIPアドレスは、このノードで最初は使用しない場合でも値を指定してください。そうすることで、ホストでノードの設定を再度行わなくても、管理ネットワークの IP アドレスをあとから追加することができます。<br><br>例<br><br>• bond0.1002<br>• ens256 |
| ADMIN_NETWORK_TARGET タイプ | o | インターフェイス<br><br>（サポートされている値はこれだけです）。 |

| キーを押します | **R** 、 **BP** 、または **O** | 価値 |
| --- | --- | --- |
| ADMIN_NETWORK_TARGET _TYPE_interface_clone_MAC | BP | 正しいか間違っているか<br><br>StorageGRID コンテナで管理ネットワークのホストターゲットインターフェイスの MAC アドレスを使用するには、キーを「 true 」に設定して原因 に設定します。<br><br>• ベストプラクティス：プロミスキャスモードが必要なネットワークでは、「 ADMIN_NETWORK_TARGET_ TYPE_interface_clone_MAC 」キーを使用してください。<br><br>MACクローニングの詳細については、MACアドレスクローニングの考慮事項と推奨事項を参照してください。<br><br>"MAC アドレスのクローニングに関する考慮事項と推奨事項" |
| ADMIN_NETWORK_ROLE | • R * | Primary または Non-Primary<br><br>このキーが必要なのは、 node_type が VM_Admin_Node の場合だけです。それ以外のタイプのノードの場合は指定しないでください。 |

| キーを押します | **R** 、 **BP** 、または **O** | 価値 |
| --- | --- | --- |
| BLOBK_DEVICE_AUDIT_logs | • R * | このノードで監査ログの永続的なストレージに使用するブロックデバイススペシャルファイルのパスと名前。このキーが必要なのは、node_type が VM_Admin_Node のノードだけです。それ以外のタイプのノードの場合は指定しないでください。<br><br>例<br><br>• `/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`<br>• `/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`<br>• `/dev/mapper/sgws-adm1-audit-logs` |

| キーを押します | **R** 、 **BP** 、または **O** | 価値 |
| --- | --- | --- |
| BLOCK_DEVICE_RANGEDB_00<br><br>BLOCK_DEVICE_RANGEDB_01<br><br>BLOCK_DEVICE_RANGEDB_02<br><br>BLOCK_DEVICE_RANGEDB_03<br><br>BLOCK_DEVICE_RANGEDB_04<br><br>BLOCK_DEVICE_RANGEDB_05<br><br>BLOCK_DEVICE_RANGEDB_06<br><br>BLOCK_DEVICE_RANGEDB_07<br><br>BLOCK_DEVICE_RANGEDB_08<br><br>BLOCK_DEVICE_RANGEDB_09<br><br>BLOCK_DEVICE_RANGEDB_10<br><br>BLOCK_DEVICE_RANGEDB_11<br><br>BLOCK_DEVICE_RANGEDB_12<br><br>BLOCK_DEVICE_RANGEDB_13<br><br>BLOCK_DEVICE_RANGEDB_14<br><br>BLOCK_DEVICE_RANGEDB_15 | • R * | このノードでオブジェクトの永続的なストレージに使用するブロックデバイススペシャルファイルのパスと名前。このキーが必要なのは、 node_type が VM_Storage_Node のノードだけです。それ以外のタイプのノードの場合は指定しないでください。<br><br>BLOCK_DEVICE_RANGEDB_00のみが必須で、それ以外は省略可能で<br>す。BLOCK_DEVICE_RANGEDB_00に指定するブロックデバイスは4TB以上である必要があります。それ以外は4TB未満でもかまいません。<br><br>*注：ギャップを残さないでください。BLOCK_DEVICE_RANGEDB_05を指定する場合<br>は、BLOCK_DEVICE_RANGEDB_04も指定されている必要があります。<br><br>例<br><br>• `/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`<br>• `/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`<br>• `/dev/mapper/sgws-sn1-rangedb-0` |

| キーを押します | **R** 、 **BP** 、または **O** | 価値 |
| --- | --- | --- |
| BLOBK_DEVICE_tables | • R * | このノードでデータベーステーブルの永続的なストレージに使用するブロックデバイススペシャルファイルのパスと名前。このキーが必要なのは、 node_type が VM_Admin_Node のノードだけです。それ以外のタイプのノードの場合は指定しないでください。<br><br>例<br><br>• `/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`<br>• `/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`<br>• `/dev/mapper/sgws-adm1-tables` |
| BLOBK_DEVICE_VAR_LOCAL です | • R * | このノードが /var/local の永続的ストレージに使用するブロックデバイススペシャルファイルのパスと名前。<br><br>例<br><br>• `/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`<br>• `/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`<br>• `/dev/mapper/sgws-sn1-var-local` |
| CLIENT_NETWORK_CONFIG | o | DHCP 、 STATIC 、または DISABLED |

| キーを押します | **R** 、 **BP** 、または **O** | 価値 |
| --- | --- | --- |
| CLIENT_NETWORK_GATEWAY | o | このノードのローカルのクライアントネットワークゲートウェイの IPv4 アドレス。 CLIENT_NETWORK_IP および CLIENT_NETWORK_MASK で定義されるサブネットに属している必要があります。この値は、 DHCP によって設定されたネットワークでは無視されます。<br><br>例<br><br>• 1.1.1.1<br>• 10.224.81 |
| CLIENT_NETWORK_IP | o | このノードのクライアントネットワークにおける IPv4 アドレス。このキーが必要なのは、 CLIENT_NETWORK_CONFIG = STATIC の場合だけです。それ以外の値の場合は指定しないでください。<br><br>例<br><br>• 1.1.1.1<br>• 10.224.81 |
| CLIENT_NETWORK_MAC | o | コンテナ内のクライアントネットワークインターフェイスの MAC アドレス。<br><br>このフィールドはオプションです。省略すると、 MAC アドレスが自動的に生成されます。<br><br>6 つの 16 進数値をコロンで区切って指定する必要があります。<br><br>例：b2：9C：02：c2：27：20 |

| キーを押します | **R** 、 **BP** 、または **O** | 価値 |
| --- | --- | --- |
| CLIENT_NETWORK_MASK | o | このノードのクライアントネットワークにおける IPv4 ネットマスク。このキーが必要なのは、CLIENT_NETWORK_CONFIG = STATIC の場合だけです。それ以外の値の場合は指定しないでください。<br><br>例<br><br>• 255.255.255.0<br>• 255.255.248.0と入力します |
| CLIENT_NETWORK_MTU | o | このノードのクライアントネットワークでの最大伝送ユニット（ MTU<br>）。CLIENT_NETWORK_CONFIG = DHCP の場合は指定しないでください。この値を指定する場合、 1280 ～ 9216 の範囲で指定する必要があります。省略すると、 1500 が使用されます。<br><br>ジャンボフレームを使用する場合は、 MTU を 9000 などのジャンボフレームに適した値に設定します。それ以外の場合は、デフォルト値のままにします。<br><br>• 重要 * ：ネットワークの MTU 値は、ノードが接続されているスイッチポートに設定された値と一致する必要があります。そうしないと、ネットワークパフォーマンスの問題やパケット損失が発生する可能性があります。<br><br>例<br><br>• 1 、 500<br>• 8、192です |

| キーを押します | **R** 、 **BP** 、または **O** | 価値 |
| --- | --- | --- |
| client_network_target です | BP | StorageGRID ノードでクライアントネットワークのアクセスに使用するホストデバイスの名前。ネットワークインターフェイス名のみがサポートされています。通常、GRID_NETWORK_TARGET または ADMIN_NETWORK_TARGET に指定したインターフェイス名とは別のインターフェイス名を使用します。<br><br>• 注：ボンドデバイスやブリッジデバイスをネットワークターゲットとして使用しないでください。ボンドデバイスの上に VLAN （または他の仮想インターフェイス）を設定するか、ブリッジと仮想イーサネット（ veth ）のペアを使用します。<br>• ベストプラクティス： * クライアントネットワークの IP アドレスは、このノードで最初は使用しない場合でも値を指定してください。そうすることで、ホストでノードの設定を再度行わなくても、クライアントネットワークの IP アドレスをあとから追加することができます。<br><br>例<br><br>• bond0.1003<br>• ens423 |
| client_network_target_type | o | インターフェイス<br><br>（この値のみがサポートされています）。 |

| キーを押します | **R** 、 **BP** 、または **O** | 価値 |
| --- | --- | --- |
| client_network_target_type _interface_clone_MAC | BP | 正しいか間違っているか<br><br>クライアントネットワークでホストターゲットインターフェイスの MAC アドレスを使用するには、キーを「 true 」に設定して StorageGRID コンテナを原因 します。<br><br>• ベストプラクティス：プロミスキャスモードが必要なネットワークでは、client_network_target_type _interface_clone_MAC キーを使用してください。<br><br>MACクローニングの詳細については、MACアドレスクローニングの考慮事項と推奨事項を参照してください。<br><br>"MAC アドレスのクローニングに関する考慮事項と推奨事項" |
| GRID_NETWORK_CONFIG | BP | STATIC または DHCP<br><br>（指定しない場合のデフォルトは STATIC ） |
| GRID_NETWORK_GATEWAY | • R * | このノードのローカルのグリッドネットワークゲートウェイの IPv4 アドレス。 GRID_NETWORK_IP および GRID_NETWORK_MASK で定義されるサブネットに属している必要があります。この値は、DHCP によって設定されたネットワークでは無視されます。<br><br>グリッドネットワークのサブネットが 1 つだけでゲートウェイがない場合は、サブネットの標準のゲートウェイアドレス（ X.Y.Z.1 ）か、このノードの GRID_NETWORK_IP の値を使用します。このどちらかの値にしておけば、以降にグリッドネットワークを拡張するときに処理が簡単になります。 |

| キーを押します | **R** 、 **BP** 、または **O** | 価値 |
| --- | --- | --- |
| GRID_NETWORK_IP | • R * | このノードのグリッドネットワークにおける IPv4 アドレス。このキーが必要なのは、GRID_NETWORK_CONFIG = STATIC の場合だけです。それ以外の値の場合は指定しないでください。<br><br>例<br><br>• 1.1.1.1<br>• 10.224.81 |
| GRID_NETWORK_MAC | o | コンテナ内のグリッドネットワークインターフェイスの MAC アドレス。<br><br>このフィールドはオプションです。省略すると、 MAC アドレスが自動的に生成されます。<br><br>6 つの 16 進数値をコロンで区切って指定する必要があります。<br><br>例：b2：9C：02：c2：27：30 |
| GRID_NETWORK_MASK | o | このノードのグリッドネットワークにおける IPv4 ネットマスク。このキーが必要なのは、GRID_NETWORK_CONFIG = STATIC の場合だけです。それ以外の値の場合は指定しないでください。<br><br>例<br><br>• 255.255.255.0<br>• 255.255.248.0と入力します |

| キーを押します | **R** 、 **BP** 、または **O** | 価値 |
| --- | --- | --- |
| GRID_NETWORK_MTU | o | このノードのグリッドネットワークでの最大伝送ユニット（ MTU ）。GRID_NETWORK_CONFIG = DHCP の場合は指定しないでください。この値を指定する場合、 1280 ～ 9216 の範囲で指定する必要があります。省略すると、 1500 が使用されます。<br><br>ジャンボフレームを使用する場合は、 MTU を 9000 などのジャンボフレームに適した値に設定します。それ以外の場合は、デフォルト値のままにします。<br><br>• 重要 * ：ネットワークの MTU 値は、ノードが接続されているスイッチポートに設定された値と一致する必要があります。そうしないと、ネットワークパフォーマンスの問題やパケット損失が発生する可能性があります。<br>• 重要 * ：ネットワークパフォーマンスを最大限に高めるには、すべてのノードのグリッドネットワークインターフェイスで MTU 値がほぼ同じになるように設定する必要があります。個々のノードのグリッドネットワークの MTU 設定に大きな違いがある場合は、 * Grid Network MTU mismatch * アラートがトリガーされます。MTU 値はすべてのネットワークタイプで同じである必要はありません。<br><br>例<br><br>• 1 、 500<br>• 8、192です |

| キーを押します | **R** 、 **BP** 、または **O** | 価値 |
| --- | --- | --- |
| GRID_NETWORK_TARGET | • R * | StorageGRID ノードでグリッドネットワークのアクセスに使用するホストデバイスの名前。ネットワークインターフェイス名のみがサポートされています。通常、ADMIN_NETWORK_TARGET または ADMIN_NETWORK_TARGET に指定したインターフェイス名とは別のインターフェイス名を使用します。<br><br>• 注：ボンドデバイスやブリッジデバイスをネットワークターゲットとして使用しないでください。ボンドデバイスの上に VLAN （または他の仮想インターフェイス）を設定するか、ブリッジと仮想イーサネット（ veth ）のペアを使用します。<br><br>例<br><br>• bond0.1001<br>• ens192 |
| GRID_NETWORK_TARGET タイプ | o | インターフェイス<br><br>（サポートされている値はこれだけです）。 |

| キーを押します | **R** 、 **BP** 、または **O** | 価値 |
| --- | --- | --- |
| GRID_NETWORK_TARGET<br>_TYPE_interface_clone_MAC | • BP * | 正しいか間違っているか<br><br>グリッドネットワーク上のホストターゲットインターフェイスの MAC アドレスを使用するには、キーの値を「 true 」に設定して StorageGRID コンテナを原因 に設定します。<br><br>• ベストプラクティス：プロミスキャスモードが必要なネットワークでは、GRID_NETWORK_TARGET<br>_TYPE_interface_clone_MAC キーを使用してください。<br><br>MACクローニングの詳細については、MACアドレスクローニングの考慮事項と推奨事項を参照してください。<br><br>"MAC アドレスのクローニングに関する考慮事項と推奨事項" |

| キーを押します | **R** 、 **BP** 、または **O** | 価値 |
| --- | --- | --- |
| MAXIMUM_RAM | o | このノードに使用を許可する RAM の最大容量。このキーを省略した場合、ノードでメモリは制限されません。本番用のノードについて設定するときは、システム RAM の合計容量よりも 24GB 以上、16~32GB 以上小さい値を指定してください。<br><br>• 注 * ： RAM 値は、ノードの実際のメタデータ用リザーブスペースに影響します。Metadata Reserved Spaceとは何かを概要 でStorageGRID を管理する手順を参照してください。<br><br>このフィールドの形式はです `<number><unit>`、ここで `<unit>` は、です `b`、 `k`、 `m`または `g`。<br><br>例<br><br>24G<br><br>38654705664b<br><br>• 注：このオプションを使用する場合は、 memory cgroups のカーネルサポートを有効にする必要があります。 |
| Node_type のように指定します | • R * | ノードのタイプ：<br><br>• VM_Admin_Nodeの略<br>• VM_Storage_Nodeの略<br>• VM_Archive_Nodeの略<br>• VM_API_Gateway |

| キーを押します | **R** 、 **BP** 、または **O** | 価値 |
| --- | --- | --- |
| PORT_REMAP を参照してください | o | ノードが内部でのグリッドノードの通信または外部との通信に使用するポートを再マッピングします。ポートの再マッピングが必要になるのは、 StorageGRID で使用される 1 つ以上のポートがエンタープライズネットワークポリシーで制限されている場合です。詳細については、「内部グリッドノードの通信」または「外部通信」を参照してください。<br><br>• 重要 * ：ロードバランサエンドポイントの設定に使用する予定のポートを再マッピングしないでください。<br>• 注： PORT_REMAP のみを設定すると、指定したマッピングがインバウンド通信とアウトバウンド通信の両方に使用されます。PORT_REMAP_INBOUND を併せて指定した場合は、 PORT_REMAP がアウトバウンド通信のみに適用されます。<br><br>使用される形式は次のとおりです。 `<network type>/<protocol>/<default port used by grid node>/<new port>`、ここで `<network type>` はgrid、admin、clientのいずれかで、protocolはtcpまたはudpです。<br><br>例：<br><br>`PORT_REMAP = client/tcp/18082/443` |

| キーを押します | **R** 、 **BP** 、または **O** | 価値 |
| --- | --- | --- |
| PORT_REMAP_INBOUND | o | 指定したポートのインバウンド通信を再マッピングします。PORT_REMAP_INBOUND を指定して PORT_REMAP に値を指定しなかった場合は、ポートのアウトバウンド通信が変更されません。<br><br>• 重要 * ：ロードバランサエンドポイントの設定に使用する予定のポートを再マッピングしないでください。<br><br>使用される形式は次のとおりです。 `<network type>/<protocol:>/<remapped port >/<default port used by grid node>`、ここで `<network type>` はgrid、admin、clientのいずれかで、protocolはtcpまたはudpです。<br><br>例：<br><br>`PORT_REMAP_INBOUND = grid/tcp/3022/22` |

関連情報

"グリッドノードによるプライマリ管理ノードの検出"

"ネットワークガイドライン"

"StorageGRID の管理"

グリッドノードによるプライマリ管理ノードの検出

## グリッドノードは、設定や管理のためにプライマリ管理ノードと通信します。各グリッドノードがグリッドネットワーク上のプライマリ管理ノードの IP アドレスを認識している必要があります。

グリッドノードからプライマリ管理ノードにアクセスできるようにするために、ノードを導入する際に次のいずれかを実行します。

- ADMIN_IP パラメータを使用して、プライマリ管理ノードの IP アドレスを手動で入力します。
- ADMIN_IP パラメータを省略して、グリッドノードで自動的に値が検出されるようにします。自動検出は、グリッドネットワークで DHCP を使用してプライマリ管理ノードに IP アドレスを割り当てる場合に特に便利です。

プライマリ管理ノードの自動検出には、 mDNS （ multicast Domain Name System ）が使用されます。プライマリ管理ノードは、最初に起動されるときに、 mDNS を使用してそのノードの IP アドレスを公開します。同じサブネット上の他のノードは、この IP アドレスを自動的に照会して取得します。ただし、通常はマルチキャスト IP トラフィックをサブネット間でルーティングできないため、他のサブネット上のノードはプライマリ管理ノードの IP アドレスを直接取得できません。

自動検出を使用する場合：

- プライマリ管理ノードが直接接続されていないサブネットの少なくとも 1 つのグリッドノードで、 ADMIN_IP 設定を指定する必要があります。このグリッドノードがプライマリ管理ノードの IP アドレスを公開することで、サブネット上の他のノードが mDNS を使用して IP アドレスを検出できるようになります。
- ネットワークインフラがサブネット内のマルチキャスト IP トラフィックの転送をサポートしていることを確認します。

ノード構成ファイルの例

## ここでは、 StorageGRID システムで使用するノード構成ファイルを設定する際の参考として、すべてのタイプのグリッドノードのノード構成ファイルの例を示します。

ほとんどのノードについては、 Grid Manager またはインストール API を使用してグリッドを設定するときに、管理ネットワークとクライアントネットワークのアドレス情報（ IP 、マスク、ゲートウェイなど）を追加できます。ただし、プライマリ管理ノードは例外です。グリッドの設定を行うためにプライマリ管理ノードの管理ネットワークの IP を参照する必要がある場合（グリッドネットワークがルーティングされていない場合など）は、プライマリ管理ノードのノード構成ファイルで管理ネットワーク接続を設定する必要があります。次の例を参照してください。

ここに示す例では、クライアントネットワークがデフォルトで無効になっていても、クライアントネットワークターゲットがベストプラクティスとして設定されています。

プライマリ管理ノードの例

ファイル名の例： `/etc/storagegrid/nodes/dc1-adm1.conf`

- ファイルの内容の例： *

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Primary
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adm1-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adm1-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adm1-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.2
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1

ADMIN_NETWORK_CONFIG = STATIC
ADMIN_NETWORK_IP = 192.168.100.2
ADMIN_NETWORK_MASK = 255.255.248.0
ADMIN_NETWORK_GATEWAY = 192.168.100.1
ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0.0/21,172.17.0.0/21
```

ストレージノードの例

ファイル名の例： `/etc/storagegrid/nodes/dc1-sn1.conf`

- ファイルの内容の例： *

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/dc1-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/dc1-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/dc1-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/dc1-sn1-rangedb-3
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

アーカイブノードの例

ファイル名の例： `/etc/storagegrid/nodes/dc1-arc1.conf`

- ファイルの内容の例： *

```
NODE_TYPE = VM_Archive_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-arc1-var-local
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.4
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

ゲートウェイノードの例

ファイル名の例： `/etc/storagegrid/nodes/dc1-gw1.conf`

- ファイルの内容の例： *

```
NODE_TYPE = VM_API_Gateway
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-gw1-var-local
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.5
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

非プライマリ管理ノードの例

ファイル名の例： `/etc/storagegrid/nodes/dc1-adm2.conf`

- ファイルの内容の例： *

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Non-Primary
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adm2-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adm2-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adm2-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.6
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

**StorageGRID** 構成を検証しています

## で構成ファイルを作成した後 `/etc/storagegrid/nodes` 各StorageGRID ノードについて、これらのファイルの内容を検証する必要があります。

構成ファイルの内容を検証するには、各ホストで次のコマンドを実行します。

```
sudo storagegrid node validate all
```

ファイルが正しい場合は、次の例に示すように、各構成ファイルの出力に * PASSED * と表示されます。

```
Checking for misnamed node configuration files… PASSED
Checking configuration file for node dc1-adm1… PASSED
Checking configuration file for node dc1-gw1… PASSED
Checking configuration file for node dc1-sn1… PASSED
Checking configuration file for node dc1-sn2… PASSED
Checking configuration file for node dc1-sn3… PASSED
Checking for duplication of unique values between nodes… PASSED
```

自動インストールの場合は、を使用してこの出力を抑制できます `-q` または `--quiet` のオプションを指定します `storagegrid` コマンド（例： `storagegrid --quiet…`）。出力を抑制した場合、構成で警告またはエラーが検出されたときはゼロ以外の終了値が返されます。

構成ファイルが正しくない場合、次の例に示すように、問題は * WARNING * および * ERROR * として表示されます。構成エラーが見つかった場合は、インストールを続行する前に修正する必要があります。

```
Checking for misnamed node configuration files…
  WARNING: ignoring /etc/storagegrid/nodes/dc1-adm1
  WARNING: ignoring /etc/storagegrid/nodes/dc1-sn2.conf.keep
  WARNING: ignoring /etc/storagegrid/nodes/my-file.txt
Checking configuration file for node dc1-adm1…
  ERROR: NODE_TYPE = VM_Foo_Node
         VM_Foo_Node is not a valid node type.  See *.conf.sample
  ERROR: ADMIN_ROLE = Foo
         Foo is not a valid admin role.  See *.conf.sample
  ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-gw1-var-local
         /dev/mapper/sgws-gw1-var-local is not a valid block device
Checking configuration file for node dc1-gw1…
  ERROR: GRID_NETWORK_TARGET = bond0.1001
         bond0.1001 is not a valid interface.  See `ip link show`
  ERROR: GRID_NETWORK_IP = 10.1.3
         10.1.3 is not a valid IPv4 address
  ERROR: GRID_NETWORK_MASK = 255.248.255.0
         255.248.255.0 is not a valid IPv4 subnet mask
Checking configuration file for node dc1-sn1…
  ERROR: GRID_NETWORK_GATEWAY = 10.2.0.1
         10.2.0.1 is not on the local subnet
  ERROR: ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0foo
         Could not parse subnet list
Checking configuration file for node dc1-sn2… PASSED
Checking configuration file for node dc1-sn3… PASSED
Checking for duplication of unique values between nodes…
  ERROR: GRID_NETWORK_IP = 10.1.0.4
         dc1-sn2 and dc1-sn3 have the same GRID_NETWORK_IP
  ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn2-var-local
         dc1-sn2 and dc1-sn3 have the same BLOCK_DEVICE_VAR_LOCAL
  ERROR: BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn2-rangedb-0
         dc1-sn2 and dc1-sn3 have the same BLOCK_DEVICE_RANGEDB_00
```

**StorageGRID** ホストサービスを開始しています

StorageGRID ノードを起動し、ホストのリブート後もノードが再起動されるようにするには、 StorageGRID ホストサービスを有効にして開始する必要があります。

手順

1. 各ホストで次のコマンドを実行します。

```
sudo systemctl enable storagegrid
sudo systemctl start storagegrid
```

2. 次のコマンドを実行して、導入の進行状況を確認します。

```
sudo storagegrid node status node-name
```

ステータスが「 not-running 」または「 stopped 」のノードに対して、次のコマンドを実行します。

```
sudo storagegrid node start node-name
```

3. StorageGRID ホストサービスを以前に有効にして開始している場合（またはサービスを有効にして開始したかどうかがわからない場合）は、次のコマンドも実行します。

```
sudo systemctl reload-or-restart storagegrid
```

## グリッドの設定とインストールの完了

### プライマリ管理ノード上のグリッドマネージャからStorageGRID システムを設定すると、インストールが完了します。

- "Grid Managerに移動します"
- "StorageGRID ライセンス情報の指定"
- "サイトの追加"
- "グリッドネットワークのサブネットの指定"
- "保留中のグリッドノードを承認します"
- "Network Time Protocolサーバ情報の指定"
- "Domain Name Systemサーバ情報の指定"
- "StorageGRID システムのパスワードの指定"
- "設定を確認し、インストールを完了します"
- "インストール後のガイドライン"

**Grid Manager**に移動します

### StorageGRID システムの設定に必要なすべての情報については、グリッドマネージャを使用して定義します。

必要なもの

プライマリ管理ノードが導入され、最初の起動シーケンスが完了している必要があります。

手順

1. Web ブラウザを開き、次のいずれかのアドレスに移動します。

`https://primary_admin_node_ip`

`client_network_ip`

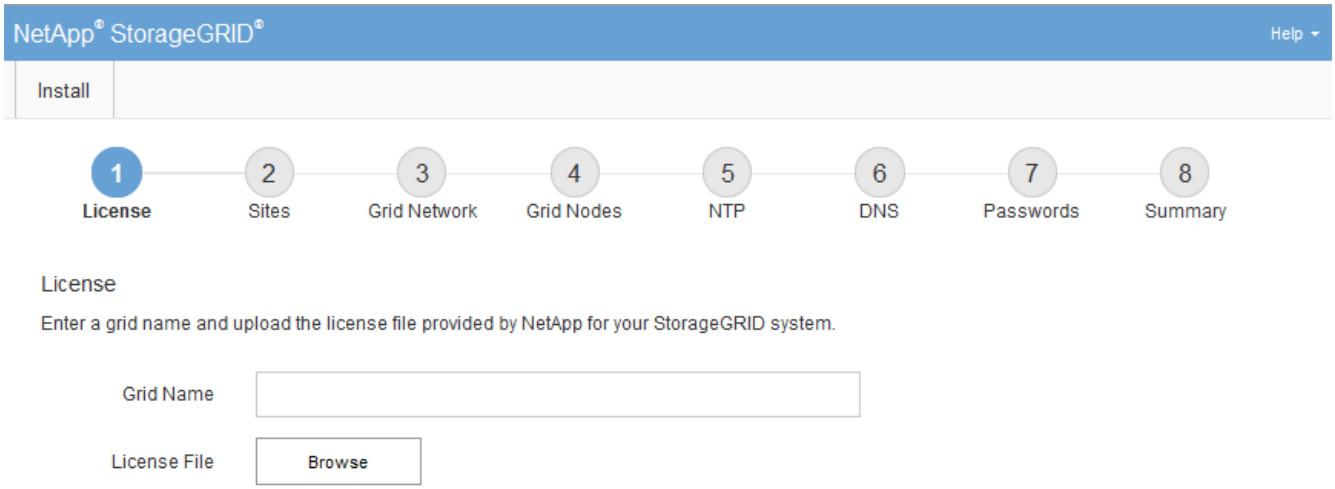
ポート 8443 でグリッドマネージャにアクセスすることもできます。

`https://primary_admin_node_ip:8443`

ネットワーク設定に応じて、グリッドネットワーク上または管理ネットワーク上のプライマリ管理ノード IP の IP アドレスを使用できます。

2. StorageGRID システムのインストール * をクリックします。

StorageGRID システムの設定に使用したページが表示されます。




**StorageGRID** ライセンス情報の指定

## StorageGRID システムの名前を指定し、ネットアップから提供されたライセンスファイルをアップロードする必要があります。

手順

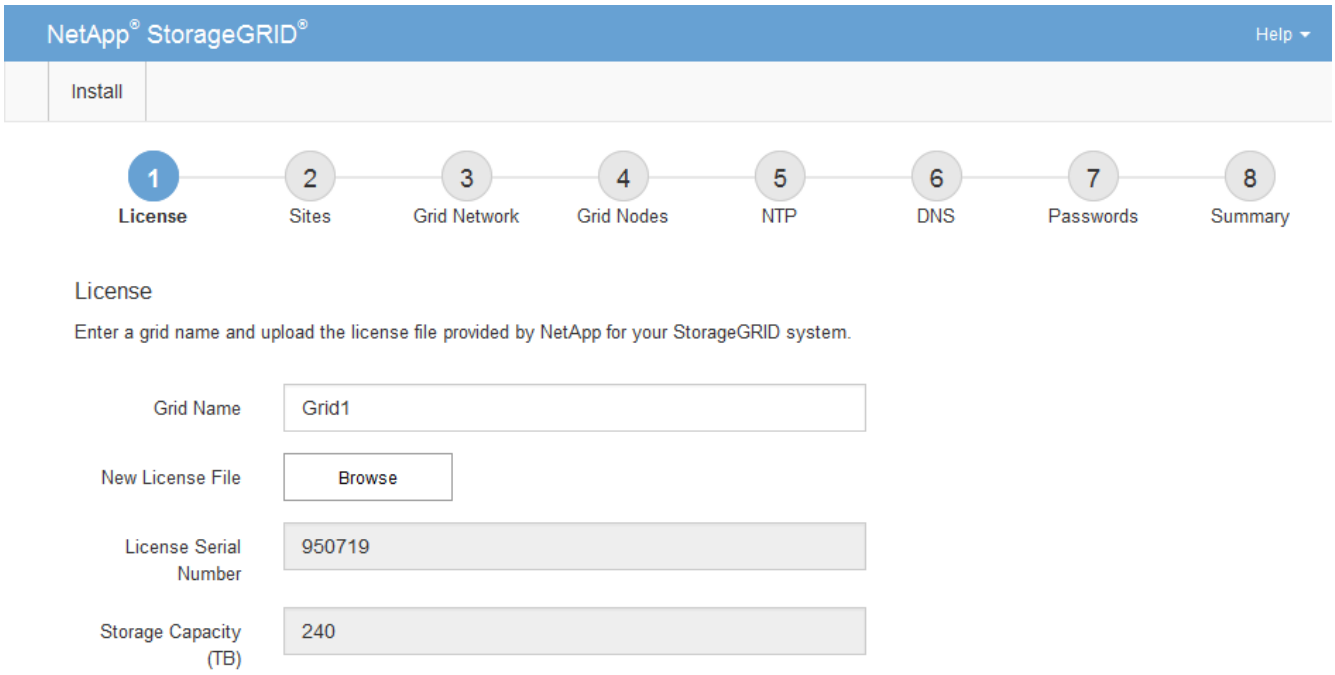
1. [ ライセンス ] ページで、 StorageGRID システムの名前として「 * グリッド名 * 」を入力します。

インストール後、ノードメニューの上部に名前が表示されます。

2. [* Browse]をクリックして、ネットアップライセンスファイルを探します (`NLFunique_id.txt`)をクリックし、*開く*をクリックします。

ライセンスファイルが検証され、シリアル番号とライセンスされたストレージ容量が表示されます。

StorageGRID インストールアーカイブには、製品サポートのない無償ライセンスが含まれています。インストール後に、サポートを提供するライセンスに更新できます。




3. 「 * 次へ * 」をクリックします。

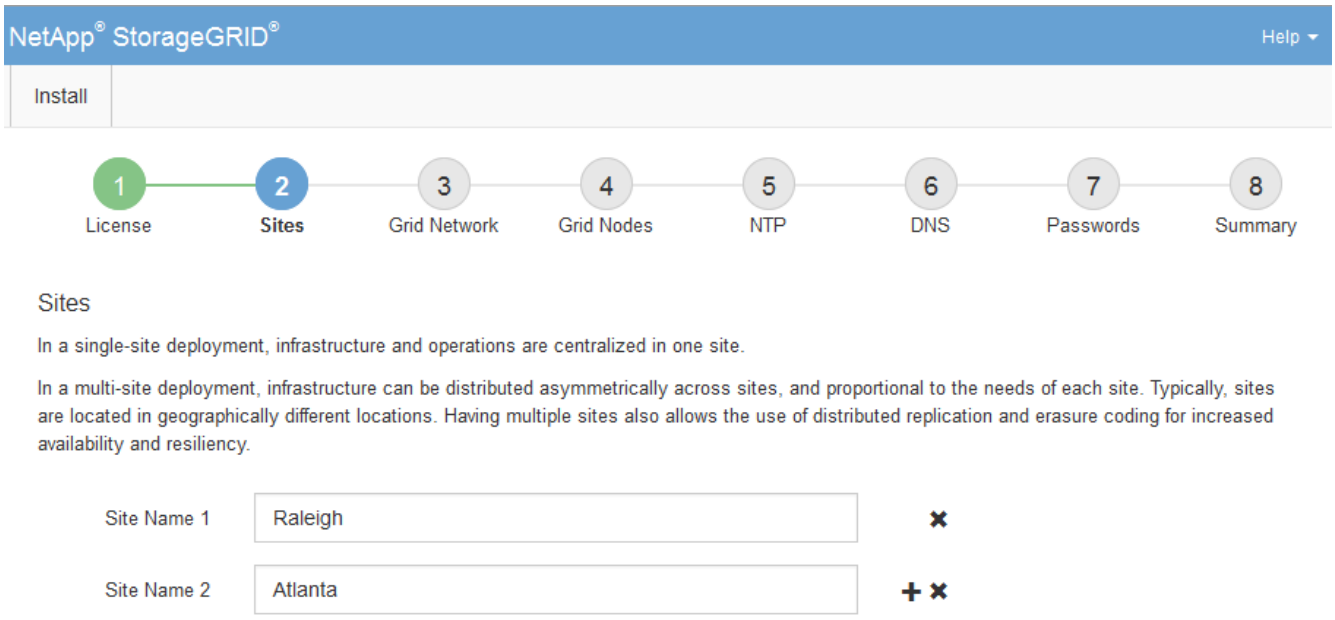
サイトの追加

StorageGRID をインストールするときに、サイトを少なくとも 1 つ作成する必要があります。StorageGRID システムの信頼性を高め、ストレージ容量を増やすために、追加のサイトを作成することができます。

手順

1. [ サイト ] ページで、 * サイト名 * を入力します。
2. サイトを追加するには、最後のサイトエントリの横にあるプラス記号をクリックし、新しい * サイト名 * テキストボックスに名前を入力します。

   グリッドトポロジに必要な数のサイトを追加します。サイトは最大 16 個まで追加できます。




3. 「 * 次へ * 」をクリックします。

グリッドネットワークのサブネットの指定

## グリッドネットワークで使用されるサブネットを指定する必要があります。

このタスクについて

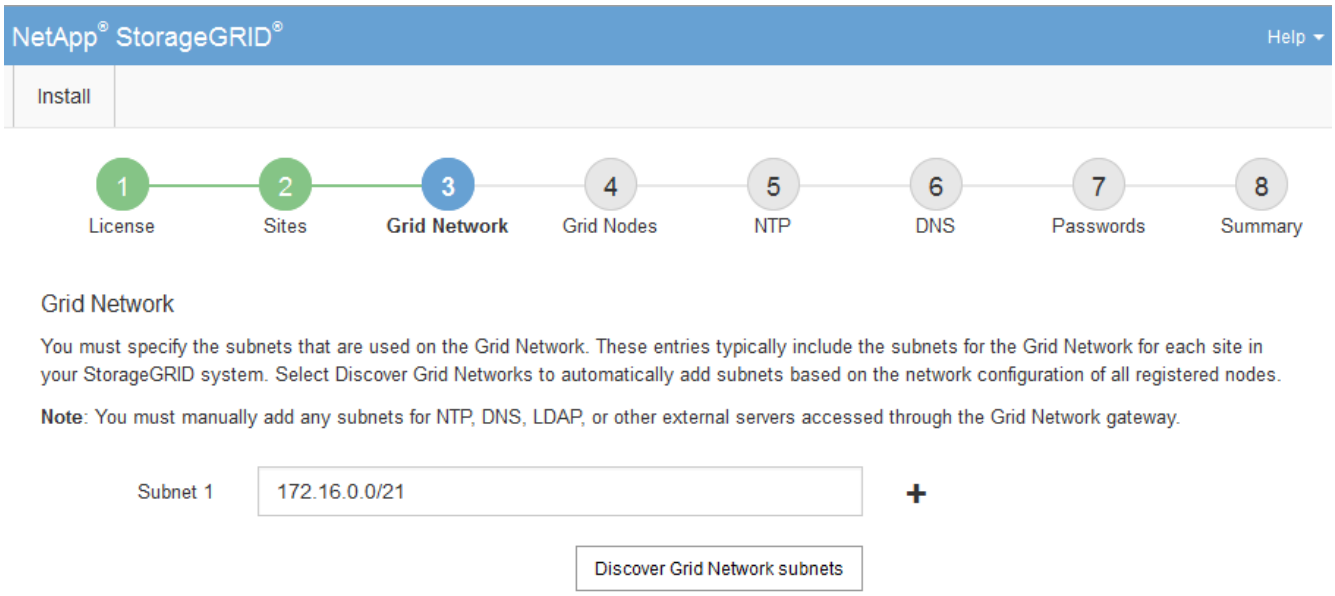
サブネットエントリには、 StorageGRID システム内の各サイトのグリッドネットワークのサブネット、およびグリッドネットワーク経由でアクセスできる必要があるサブネットが含まれます。

グリッドサブネットが複数ある場合は、グリッドネットワークゲートウェイが必要です。指定するすべてのグリッドサブネットが、このゲートウェイ経由でアクセス可能であることが必要です。

手順

1. [* サブネット 1*] テキストボックスで、少なくとも 1 つのグリッドネットワークの CIDR ネットワークアドレスを指定します。
2. 最後のエントリの横にあるプラス記号をクリックして、追加のネットワークエントリを追加します。

   少なくとも 1 つのノードがすでに導入されている場合は、 * グリッドネットワークのサブネットの検出 * をクリックすると、 Grid Manager に登録されているグリッドノードから報告されたサブネットが Grid ネットワークサブネットリストに自動的に追加されます。




3. 「 * 次へ * 」をクリックします。

保留中のグリッドノードを承認します

## 各グリッドノードは、 StorageGRID システムに追加する前に承認する必要があります。

必要なもの

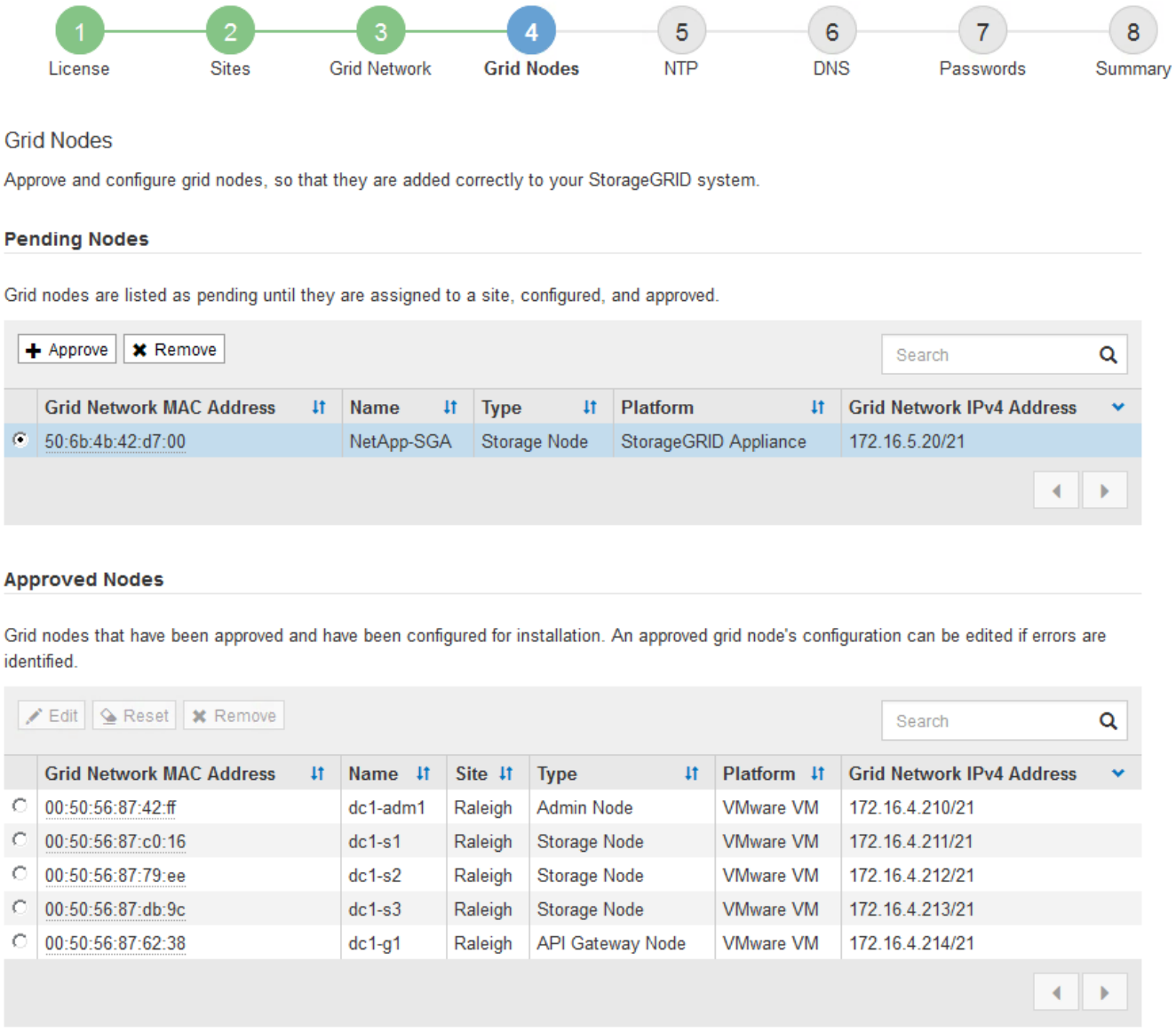
仮想アプライアンスおよびStorageGRID アプライアンスのグリッドノードをすべて導入しておく必要があります。

手順

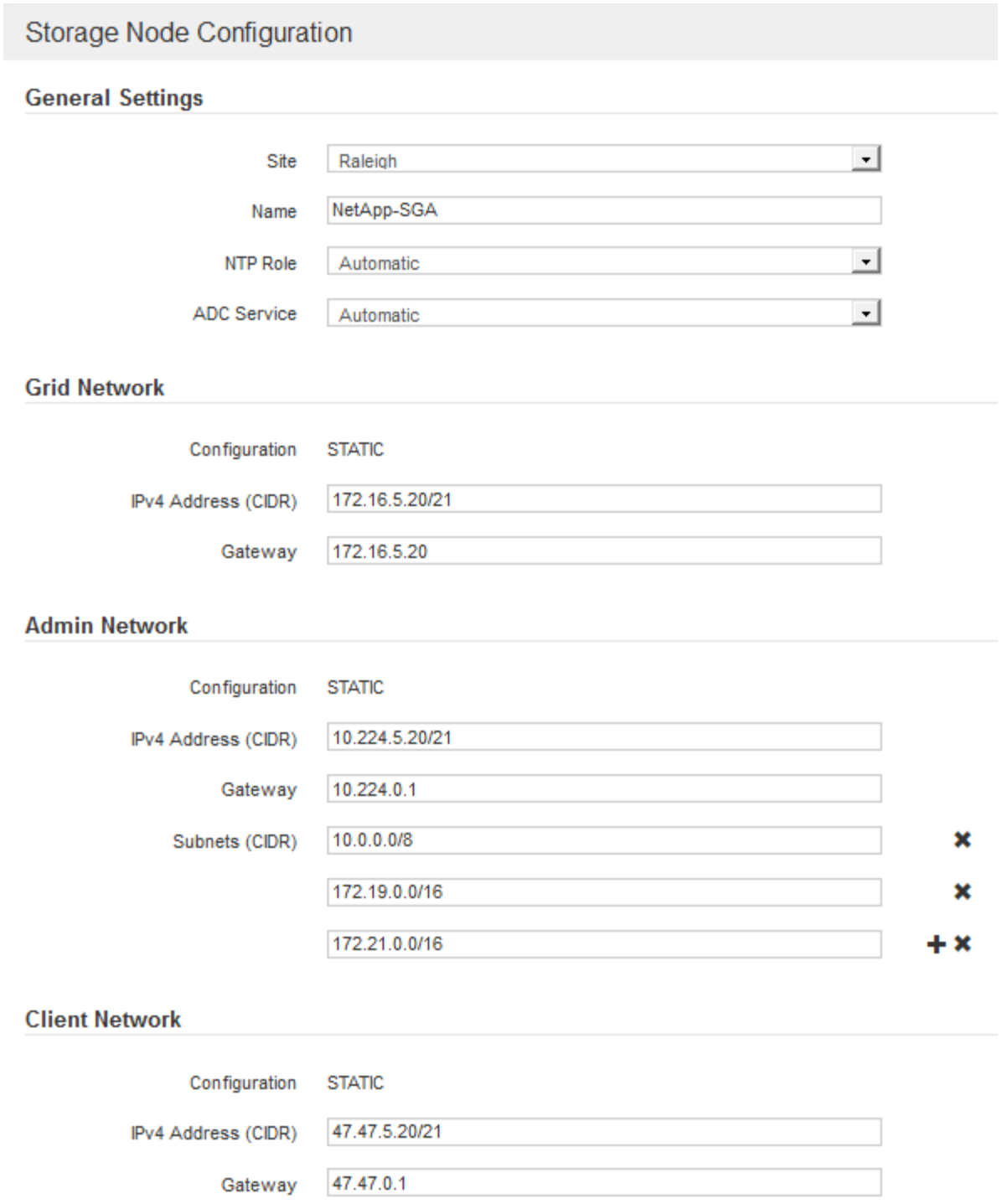
1. Pending 状態のノードのリストを確認し、導入したすべてのグリッドノードが表示されていることを確認します。

   見つからないグリッドノードがある場合は、正常に導入されたことを確認します。

2. 承認する保留中のノードの横にあるラジオボタンを選択します。




3. [ 承認（ Approve ） ] をクリックします
4. [ 一般設定 ] で、必要に応じて次のプロパティの設定を変更します。




◦ * Site * ：このグリッドノードが関連付けられるサイトの名前。

◦ * 名前 * ：ノードに割り当てられる名前。 Grid Manager に表示される名前。デフォルトでは、ノードの設定時に指定した名前が付けられます。インストールプロセスのこのステップでは、必要に応じて名前を変更できます。

インストールの完了後にノードの名前を変更することはできません。

VMware ノードの場合はここで名前を変更できますが、 vSphere で仮想マシンの名前は変更されません。

- * NTP Role * ：グリッドノードのネットワークタイムプロトコル（ NTP ）ロール。オプションは * Automatic * 、 * Primary * 、 * Client * です。「 * 自動」を選択すると、管理ノード、 ADC サービスを採用するストレージノード、ゲートウェイノード、および静的な IP アドレスでないグリッドノードにプライマリロールが割り当てられます。他のすべてのグリッドノードにはクライアントロールが割り当てられます。

  各サイトの少なくとも 2 つのノードが、少なくとも 4 つの外部 NTP ソースにアクセスできることを確認します。NTP ソースにアクセスできるノードがサイトに 1 つしかないと、そのノードがダウンした場合にタイミングの問題が生じます。また、各サイトで 2 つのノードをプライマリ NTP ソースとして指定することにより、サイトがグリッドの他の部分から分離されても、正確なタイミングが保証されます。

- * ADC service * （ストレージノードのみ）：「 * Automatic * 」を選択して、ノードに Administrative Domain Controller （ ADC ）サービスが必要かどうかをシステムに通知します。ADC サービスは、グリッドサービスの場所と可用性を追跡します。各サイトで少なくとも 3 つのストレージノードに ADC サービスが含まれている必要があります。導入後のノードに ADC サービスを追加することはできません。

5. グリッドネットワークで、必要に応じて次のプロパティの設定を変更します。

   - * IPv4 Address （ CIDR ） * ：グリッドネットワークインターフェイス（コンテナ内の eth0 ）の CIDR ネットワークアドレス。例： 192.168.1.234/21
   - * ゲートウェイ * ：グリッドネットワークゲートウェイ。例： 192.168.0.1

     グリッドサブネットが複数ある場合は、ゲートウェイが必要です。

     グリッドネットワーク設定で DHCP を選択した場合は、ここで値を変更すると、新しい値がノード上の静的アドレスとして設定されます。設定された IP アドレスが DHCP アドレスプールにないことを確認する必要があります。

6. グリッドノードの管理ネットワークを設定する場合は、必要に応じて管理ネットワークセクションで設定を追加または更新します。

   サブネット（ CIDR ） * テキストボックスに、このインターフェイスから発信されるルートの宛先サブネットを入力します。管理サブネットが複数ある場合は、管理ゲートウェイが必要です。

   管理ネットワーク設定で DHCP を選択した場合は、ここで値を変更すると、新しい値がノード上の静的アドレスとして設定されます。設定された IP アドレスが DHCP アドレスプールにないことを確認する必要があります。

   - アプライアンス： StorageGRID アプライアンスでは、 StorageGRID アプライアンスインストーラを使用した初回インストール時に管理ネットワークが設定されなかった場合、このグリッドマネージャのダイアログボックスで管理ネットワークを設定することはできません。代わりに、次の手順を実行する必要があります。

     a. アプライアンスをリブートします。アプライアンスインストーラで、 * Advanced * > * Reboot * を選択します。

        リブートには数分かかることがあります。

     b. [Configure Networking*] > [**Link Configuration**] を選択し、適切なネットワークを有効にします。

c. [Configure Networking*]>[**IP Configuration**] を選択し、有効なネットワークを設定します。

d. ホームページに戻り、「インストールの開始」をクリックします。

e. Grid Manager で、ノードが承認済みノード（ Approved Nodes ）テーブルにリストされている場合は、ノードをリセットします。

f. Pending Nodes テーブルからノードを削除します。

g. ノードが Pending Nodes リストに再表示されるまで待ちます。

h. 適切なネットワークを設定できることを確認します。IP Configuration ページで指定した情報があらかじめ入力されている必要があります。

追加情報 の場合は、使用しているアプライアンスモデルのインストールとメンテナンスの手順を参照してください。

7. グリッドノードのクライアントネットワークを設定する場合は、必要に応じてクライアントネットワークセクションで設定を追加または更新します。クライアントネットワークを設定する場合はゲートウェイが必要になります。これは、インストール後にノードのデフォルトゲートウェイになります。

クライアントネットワーク設定で DHCP を選択した場合は、ここで値を変更すると、新しい値がノード上の静的アドレスとして設定されます。設定された IP アドレスが DHCP アドレスプールにないことを確認する必要があります。

◦ アプライアンス： StorageGRID アプライアンスでは、 StorageGRID アプライアンスインストーラを使用した初回インストール時にクライアントネットワークが設定されなかった場合、このグリッドマネージャのダイアログボックスでクライアントネットワークを設定することはできません。代わりに、次の手順を実行する必要があります。

a. アプライアンスをリブートします。アプライアンスインストーラで、 * Advanced * > * Reboot * を選択します。

リブートには数分かかることがあります。

b. [Configure Networking*] > [**Link Configuration**] を選択し、適切なネットワークを有効にします。

c. [Configure Networking*]>[**IP Configuration**] を選択し、有効なネットワークを設定します。

d. ホームページに戻り、「インストールの開始」をクリックします。

e. Grid Manager で、ノードが承認済みノード（ Approved Nodes ）テーブルにリストされている場合は、ノードをリセットします。

f. Pending Nodes テーブルからノードを削除します。

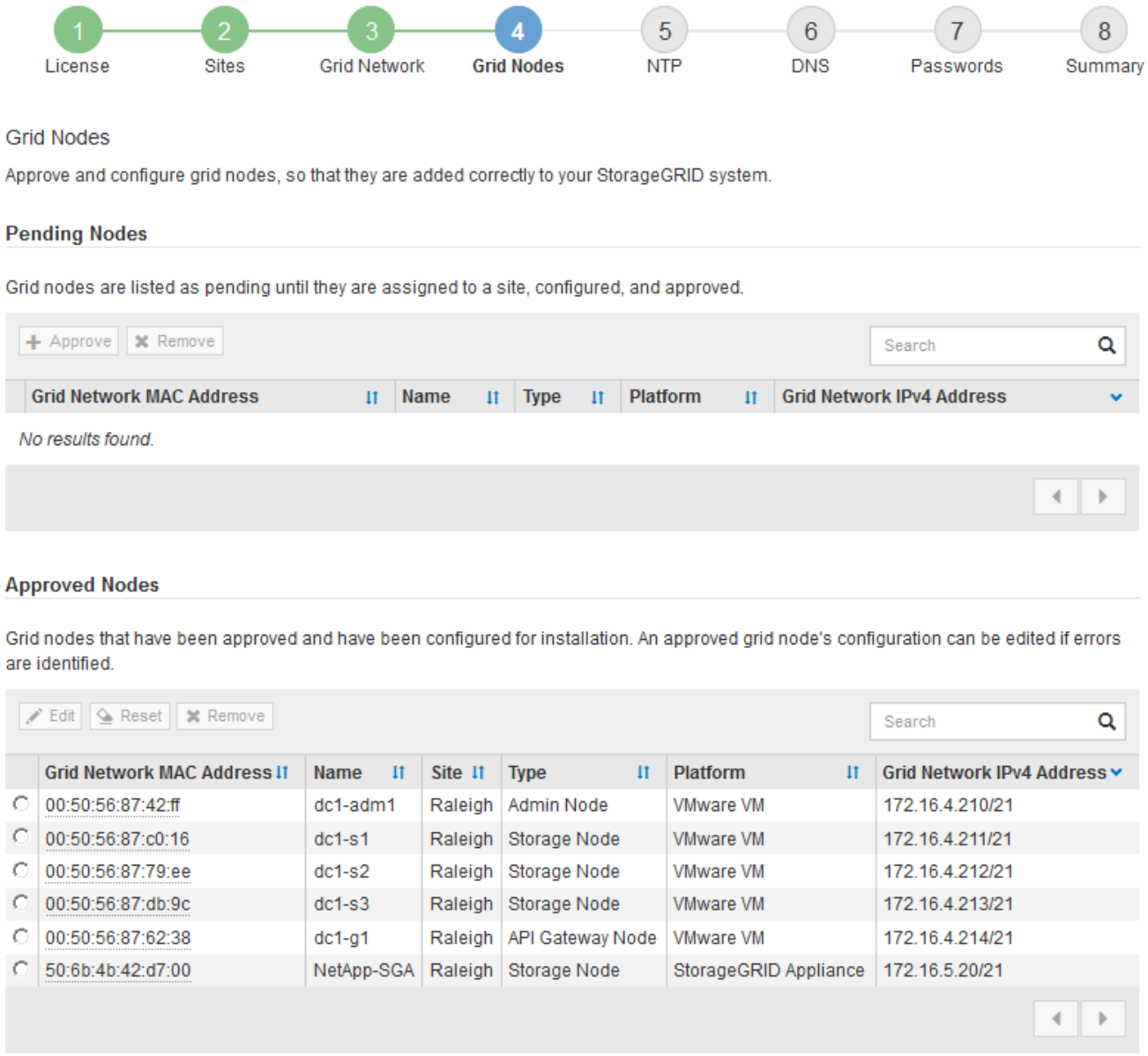
g. ノードが Pending Nodes リストに再表示されるまで待ちます。

h. 適切なネットワークを設定できることを確認します。IP Configuration ページで指定した情報があらかじめ入力されている必要があります。

追加情報 の場合は、使用しているアプライアンスのインストールとメンテナンスの手順を参照してください。

8. [ 保存（ Save ） ] をクリックします。

グリッドノードエントリが [ 承認済みノード（ Approved Nodes ） ] リストに移動します。




9. 承認する保留中のグリッドノードごとに、上記の手順を繰り返します。

   グリッドに必要なすべてのノードを承認する必要があります。ただし、サマリページで * インストール * をクリックする前に、いつでもこのページに戻ることができます。承認済みグリッドノードのプロパティを変更するには、ラジオボタンを選択し、 * 編集 * をクリックします。

10. グリッドノードの承認が完了したら、 * 次へ * をクリックします。

### Network Time Protocolサーバ情報の指定

別々のサーバで実行された処理を常に同期された状態にするには、 StorageGRID システムの NTP 設定情報を指定する必要があります。

このタスクについて

NTP サーバの IPv4 アドレスを指定する必要があります。

外部 NTP サーバを指定する必要があります。指定した NTP サーバで NTP プロトコルが使用されている必要

があります。

時間のずれに伴う問題を防ぐには、 Stratum 3 またはそれより上位の NTP サーバ参照を 4 つ指定する必要があります。

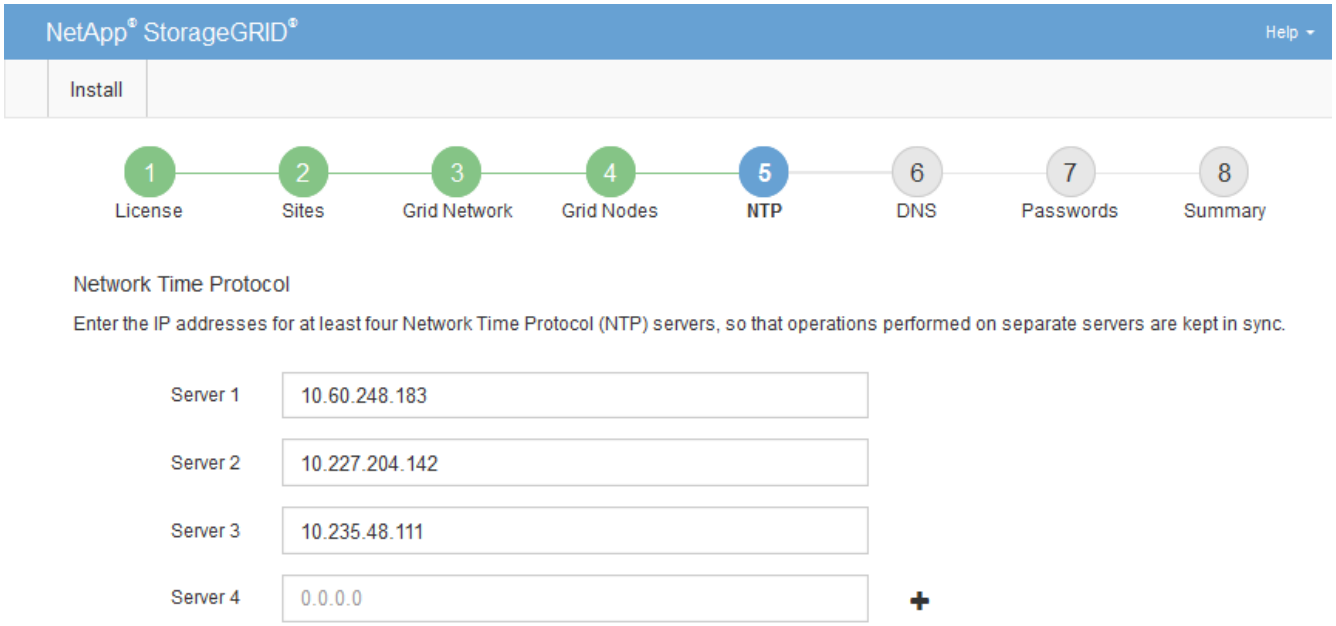
> 本番レベルの StorageGRID インストール環境で外部 NTP ソースを指定する場合は、 Windows Server 2016 より前のバージョンの Windows で Windows Time （ W32Time ）サービスを使用しないでください。以前のバージョンの Windows のタイムサービスは精度が十分でないため、 StorageGRID などの高精度環境での使用は Microsoft でサポートされていません。を参照してください "高精度環境用に Windows タイムサービスを構成するためのサポート境界"。

外部 NTP サーバは、以前にプライマリ NTP ロールを割り当てていたノードによって使用されます。

> 各サイトの少なくとも 2 つのノードが、少なくとも 4 つの外部 NTP ソースにアクセスできることを確認します。NTP ソースにアクセスできるノードがサイトに 1 つしかないと、そのノードがダウンした場合にタイミングの問題が生じます。また、各サイトで 2 つのノードをプライマリ NTP ソースとして指定することにより、サイトがグリッドの他の部分から分離されても、正確なタイミングが保証されます。

手順

1. [* サーバー 1 * から * サーバー 4 * ] テキストボックスに、少なくとも 4 つの NTP サーバーの IPv4 アドレスを指定します。
2. 必要に応じて、最後のエントリの横にあるプラス記号を選択して、サーバエントリを追加します。




3. 「 * 次へ * 」を選択します。

**Domain Name System**サーバ情報の指定

## IP アドレスの代わりにホスト名を使用して外部サーバにアクセスできるようにするには、 StorageGRID システムの DNS 情報を指定する必要があります。

このタスクについて

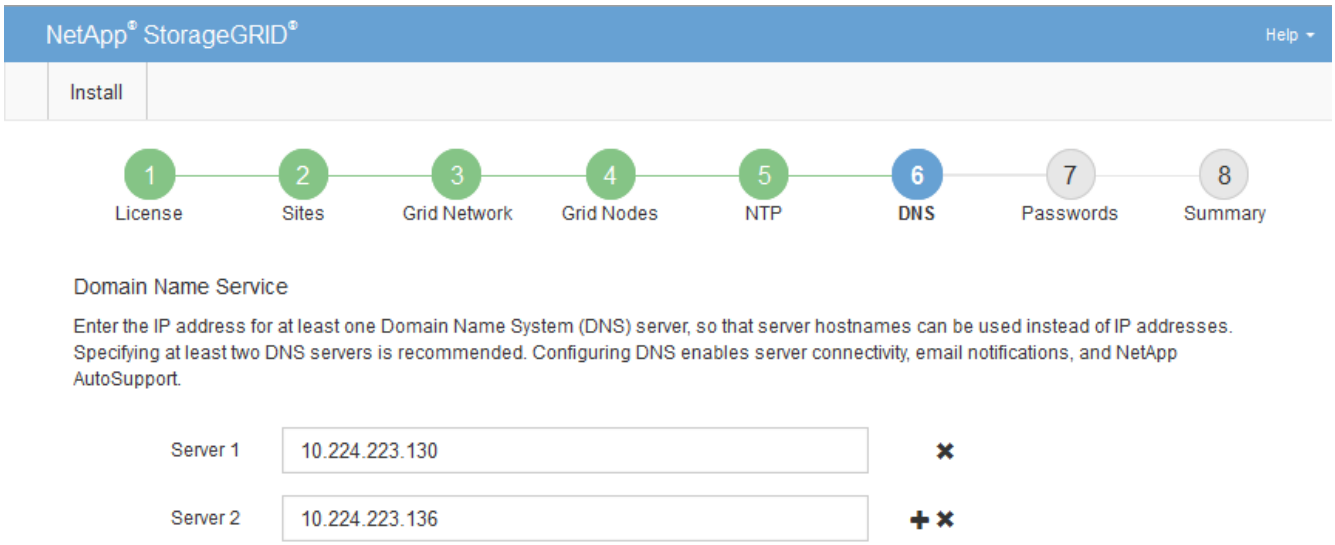
DNS サーバ情報を指定すると、 E メール通知や AutoSupport に、 IP アドレスではなく Fully Qualified Domain Name （ FQDN ；完全修飾ドメイン名）ホスト名を使用できます。DNS サーバは少なくとも 2 つ指定することを推奨します。

> DNS サーバの IPv4 アドレスは 2~6 個指定します。ネットワーク分離が発生した場合に各サイトがローカルにアクセスできる DNS サーバを選択する必要があります。これにより、分離されたサイトは引き続き DNS サービスにアクセスできます。グリッド全体の DNS サーバリストを設定したあとに、ノードごとに DNS サーバリストをカスタマイズできます。詳細については、リカバリおよびメンテナンスの手順にある DNS 設定の変更に関する情報を参照してください。

DNS サーバ情報を省略したり誤って設定したりすると、各グリッドノードの SSM サービスで DNST アラームがトリガーされます。このアラームは、 DNS が正しく設定され、新しいサーバ情報がすべてのグリッドノードに配信された時点で解除されます。

手順

1. 「 * サーバー 1 * 」テキストボックスで、少なくとも 1 つの DNS サーバーの IPv4 アドレスを指定します。
2. 必要に応じて、最後のエントリの横にあるプラス記号を選択して、サーバエントリを追加します。




少なくとも 2 つの DNS サーバを指定することを推奨します。DNS サーバは 6 つまで指定できます。

3. 「 * 次へ * 」を選択します。

**StorageGRID** システムのパスワードの指定

## StorageGRID システムのインストールの一環として、システムの保護とメンテナンス作業に使用するパスワードを入力する必要があります。

このタスクについて

Install Passwords ページを使用して、プロビジョニングパスフレーズとグリッド管理 root ユーザのパスワードを指定します。

- プロビジョニングパスフレーズは暗号化キーとして使用され、 StorageGRID システムでは格納されません。

- リカバリパッケージのダウンロードなど、インストール、拡張、メンテナンスの手順用のプロビジョニングパスフレーズが必要です。そのため、プロビジョニングパスフレーズは安全な場所に保存しておくことが重要です。
- 現在のプロビジョニングパスフレーズがある場合は、 Grid Manager からプロビジョニングパスフレーズを変更できます。
- Grid 管理 root ユーザのパスワードは Grid Manager を使用して変更できる。
- ランダムに生成されたコマンドラインコンソールとSSHパスワードは、リカバリパッケージのPasswords.txtファイルに保存されます。

手順

1. 「 * プロビジョニングパスフレーズ * 」に、 StorageGRID システムのグリッドトポロジを変更するために必要なプロビジョニングパスフレーズを入力します。

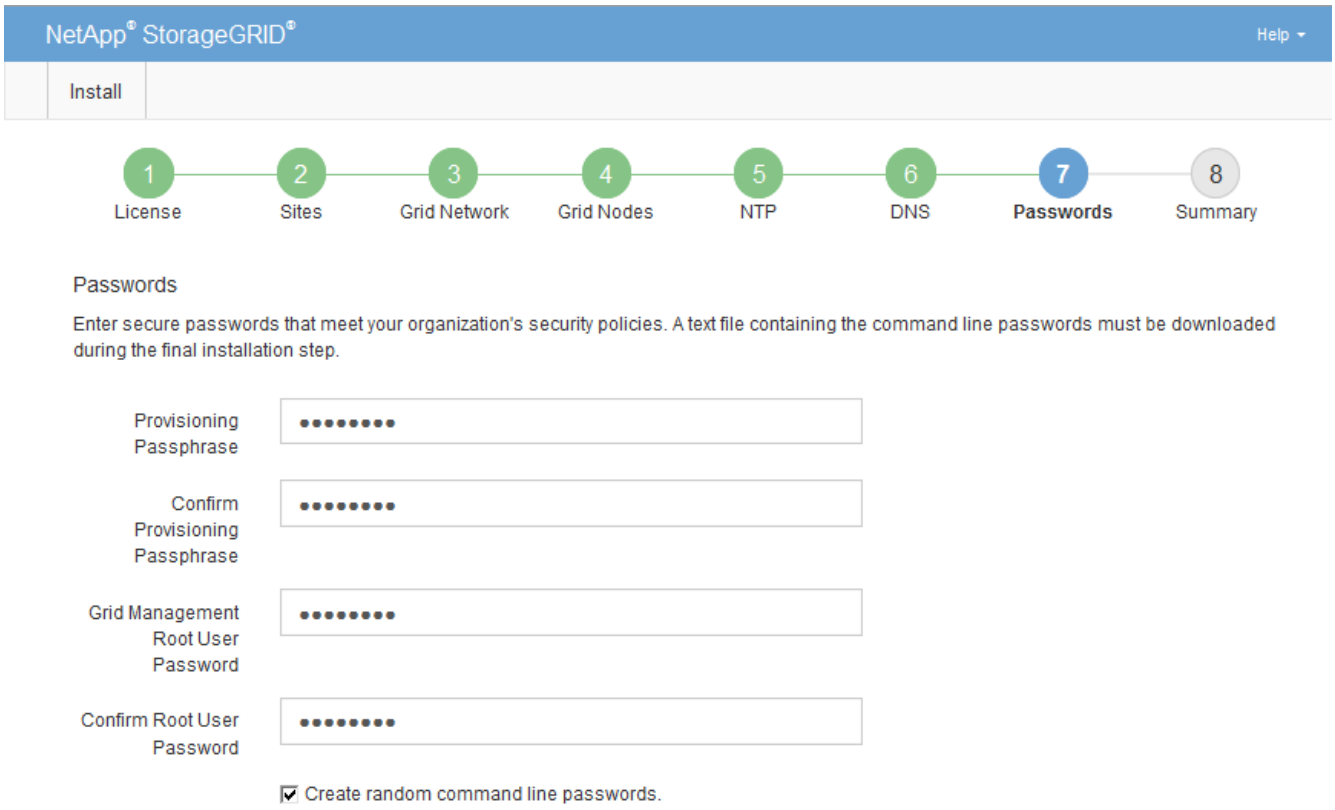
   プロビジョニングパスフレーズは安全な場所に保存してください。

   > インストールの完了後にプロビジョニングパスフレーズを変更する場合は、 Grid Manager を使用してください。[構成（Configuration ）]>[*アクセス制御（* Access Control ）]>[ Gridパスワード*（* Grid

2. [Confirm Provisioning Passphrase* （プロビジョニングパスフレーズの確認） ] にプロビジョニングパスフレーズを再入力して確定します。
3. * Grid Management Root User Password * に、 Grid Manager に「 root 」ユーザとしてアクセスするために使用するパスワードを入力します。

   パスワードは安全な場所に保管してください。

4. Confirm Root User Password * で、 Grid Manager のパスワードを再入力して確認します。




5. コンセプトの実証やデモを目的としてグリッドをインストールする場合は、必要に応じて、 * ランダムなコマンドラインパスワードの作成 * チェックボックスの選択を解除します。

   本番環境では、セキュリティ上の理由から常にランダムパスワードを使用する必要があります。デフォルトのパスワードを使用してコマンドラインから "root" または "admin" アカウントを使用してグリッドノードにアクセスする場合は、デモ用グリッドの * ランダムなコマンドラインパスワードの作成 * のみを選択解除します。

   リカバリパッケージファイルをダウンロードするように求められます (`sgws-recovery-package-id-revision.zip`)サマリページで*Install*をクリックした後。インストールを完了するには、このファイルをダウンロードする必要があります。システムへのアクセスに必要なパスワードは、に保存されています `Passwords.txt` リカバリパッケージファイルに含まれているファイル。

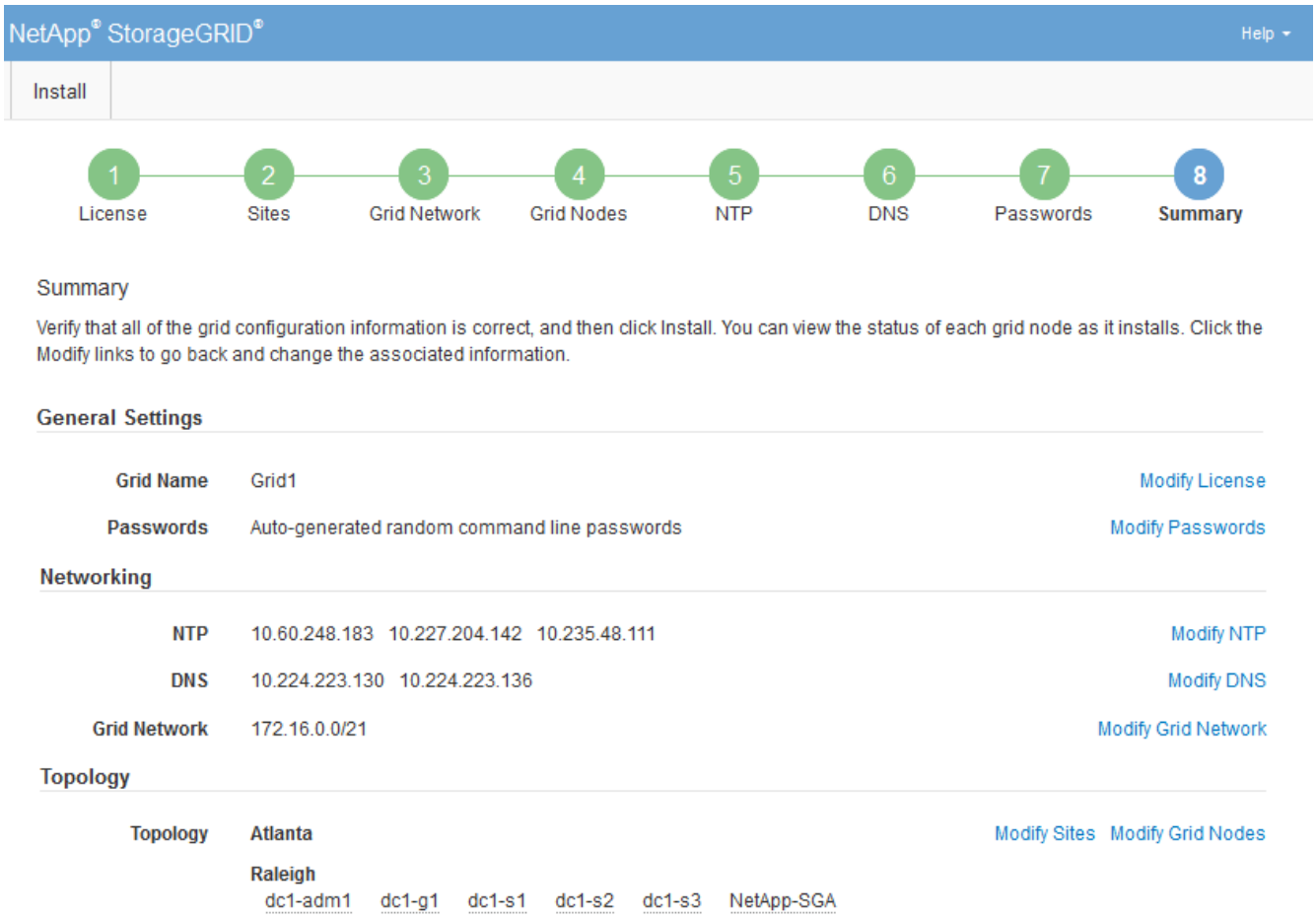
6. 「 * 次へ * 」をクリックします。

設定を確認し、インストールを完了します

インストールを正常に完了するために、入力した設定情報をよく確認する必要があります。

手順

1. 「 * 概要 * 」ページを表示します。




2. グリッドの設定情報がすべて正しいことを確認します。Summary （サマリ）ページの Modify （変更）リンクを使用して、戻ってエラーを修正します。
3. 「 * Install * 」をクリックします。

> クライアントネットワークを使用するようにノードが設定されている場合、 * Install * をクリックすると、そのノードのデフォルトゲートウェイがグリッドネットワークからクライアントネットワークに切り替わります。接続を失った場合は、アクセス可能なサブネット経由でプライマリ管理ノードにアクセスしていることを確認する必要があります。を参照してください "ネットワークのガイドライン" を参照してください。

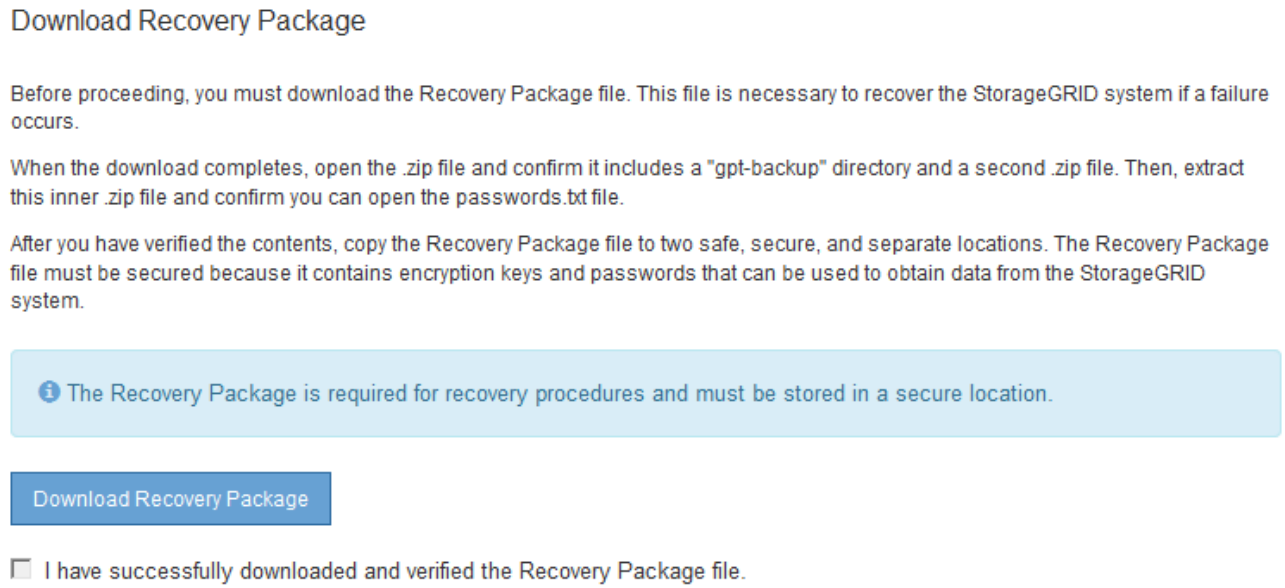
4. [ リカバリパッケージのダウンロード ] をクリックします。

   グリッドトポロジを定義するポイントまでインストールが進むと、リカバリパッケージファイルをダウンロードするように求められます (`.zip`) をクリックし、このファイルの内容に正常にアクセスできることを確認します。リカバリパッケージファイルのダウンロードが必要となるのは、グリッドノードで障害が発生した場合に StorageGRID システムをリカバリできるようにするためです。インストールはバックグラウンドで続行されますが、このファイルをダウンロードして検証するまでは、インストールを完了して StorageGRID システムにアクセスすることができません。

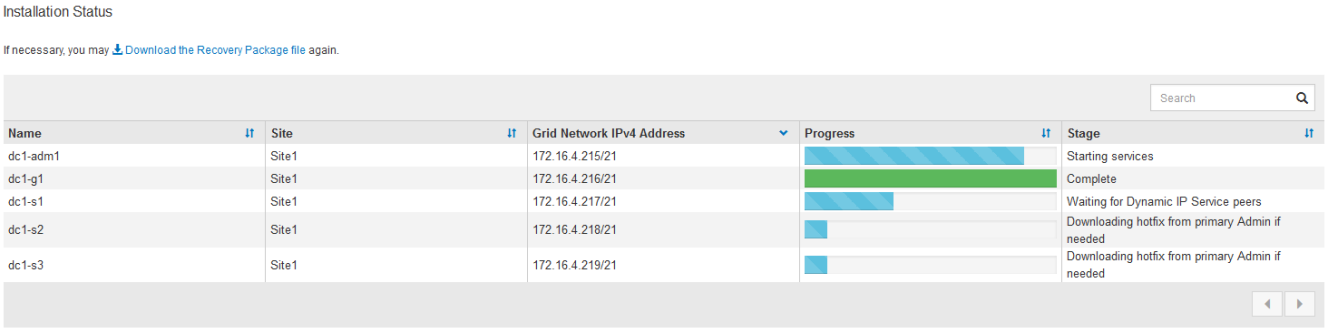
5. の内容を展開できることを確認します `.zip` ファイルを作成し、安全で安全な2つの場所に保存します。

> リカバリパッケージファイルには StorageGRID システムからデータを取得するための暗号キーとパスワードが含まれているため、安全に保管する必要があります。

6. [I have successfully downloaded and verified the Recovery Package file*] チェックボックスをオンにし、 [ 次へ ] をクリックします。




インストールがまだ進行中の場合は、ステータスページが表示されます。このページには、グリッドノードごとのインストールの進捗状況が表示されます。




すべてのグリッドノードが完了ステージに到達すると、 Grid Manager のサインインページが表示されます。

7. 「 root 」ユーザおよびインストール時に指定したパスワードを使用して Grid Manager にサインインします。

インストール後のガイドライン

## グリッドノードの導入と設定が完了したら、 DHCP アドレスおよびネットワーク設定の変更について、次のガイドラインに従ってください。

- DHCP を使用して IP アドレスを割り当てた場合は、使用しているネットワーク上の各 IP アドレスに対して DHCP 予約を設定します。

  DHCP は導入フェーズでのみ設定できます。設定時に DHCP を設定することはできません。

IP アドレスが変わるとノードがリブートします。 DHCP アドレスの変更が同時に複数のノードに影響を及ぼす場合、原因 が停止する可能性があります。

- グリッドノードの IP アドレス、サブネットマスク、およびデフォルトゲートウェイを変更する場合は、IP 変更手順を使用する必要があります。リカバリとメンテナンスの手順のIPアドレスの設定に関する情報を参照してください。
- ルーティングやゲートウェイの変更など、ネットワーク設定を変更すると、プライマリ管理ノードおよびその他のグリッドノードへのクライアント接続が失われる可能性があります。ネットワークの変更内容によっては、接続の再確立が必要になる場合があります。

# インストールの自動化

## StorageGRID ホストサービスのインストール、およびグリッドノードの設定を自動化することができます。

このタスクについて

導入を自動化すると、次のいずれかの場合に役立ちます。

- 物理ホストや仮想ホストの導入と設定に Ansible 、 Puppet 、 Chef などの標準のオーケストレーションフレームワークをすでに使用している場合。
- 複数の StorageGRID インスタンスを導入する場合。
- 大規模で複雑な StorageGRID インスタンスを導入する場合。

StorageGRID ホストサービスはパッケージでインストールされ、構成ファイルで制御されます。構成ファイルは、手動インストール時に対話形式で作成できるほか、あらかじめ用意して（またはプログラム化して）標準のオーケストレーションフレームワークを使用した自動インストールに使用できます。StorageGRID には、 StorageGRID アプライアンスと StorageGRID システム全体（「グリッド」）の設定を自動化するためのオプションの Python スクリプトが用意されています。これらのスクリプトは直接使用することも、StorageGRID インストール REST API の使用方法を調べることもできます。グリッドの導入ツールや設定ツールを独自に開発する際の参考としても使用できます。

StorageGRID の導入のすべてまたは一部を自動化する場合は'インストール・プロセスを開始する前に'インストールの自動化を参照してください

**StorageGRID** ホストサービスのインストールと設定を自動化する

## StorageGRID ホストサービスのインストールは、 Ansible 、 Puppet 、 Chef 、 Fabric 、 SaltStack などの標準のオーケストレーションフレームワークを使用して自動化できます。

StorageGRID ホストサービスはRPM形式でパッケージ化されており、あらかじめ構成ファイルを用意して（またはプログラム化して）おくことで自動インストールが可能です。すでに RHEL または CentOS のインストールおよび設定に標準的なオーケストレーションフレームワークを使用している場合は、プレイブックやレシピに StorageGRID を追加する方が簡単です。

サンプルのAnsibleのロールとプレイブックは、のインストールアーカイブに含まれています `/extras` フォルダ。Ansibleプレイブックは、の仕組みを示しています `storagegrid` 役割は、ホストを準備し、ターゲットサーバーにStorageGRID をインストールすることです。必要に応じて、ロールまたはプレイブックをカスタマイズできます。

サンプルのプレイブックには、 StorageGRID ホストサービスを開始する前にネットワークデバイスを作成するために必要な手順は含まれていません。これらの手順は、最終的な確認と使用の前に追加してください。

ホストの準備と仮想グリッドノードの導入の手順をすべて自動化することができます。

**StorageGRID** の設定の自動化

## グリッドノードを導入したら、 StorageGRID システムの設定を自動化できます。

必要なもの

- インストールアーカイブにある次のファイルの場所を確認しておきます。

| ファイル名 | 説明 |
| --- | --- |
| `configure-storagegrid.py` | 設定を自動化するための Python スクリプト |
| `configure-storagegrid.sample.json` | スクリプトで使用するサンプル構成ファイル |
| `configure-storagegrid.blank.json` | スクリプトで使用する空の構成ファイルです |

- を作成しておきます `configure-storagegrid.json` 構成ファイルこのファイルを作成するには、サンプル構成ファイルを変更します (`configure-storagegrid.sample.json`)または空の構成ファイル (`configure-storagegrid.blank.json`) 。

このタスクについて

を使用できます `configure-storagegrid.py` Pythonスクリプトおよび `configure-storagegrid.json` StorageGRID システムの設定を自動化するための構成ファイル。

また、 Grid Manager またはインストール API を使用してシステムを設定することもできます。

手順

1. Python スクリプトを実行するために使用する Linux マシンにログインします。
2. インストールアーカイブを展開したディレクトリに移動します。

   例：

   ```
   cd StorageGRID-Webscale-version/platform
   ```

   ここで、 `platform` はです `debs`、 `rpms`または `vsphere`。

3. Python スクリプトを実行し、作成した構成ファイルを使用します。

   例：

```
./configure-storagegrid.py ./configure-storagegrid.json --start-install
```

結果

リカバリパッケージ .zip 設定プロセスでファイルが生成され、インストールと設定を実行するディレクトリにダウンロードされます。グリッドノードで障害が発生した場合に StorageGRID システムをリカバリできるようにするために、リカバリパッケージファイルをバックアップする必要があります。たとえば、バックアップされたセキュアなネットワーク上の場所や、安全なクラウドストレージ上の場所にコピーします。

リカバリパッケージファイルには StorageGRID システムからデータを取得するための暗号キーとパスワードが含まれているため、安全に保管する必要があります。

ランダムパスワードを生成するように指定した場合は、を展開する必要があります Passwords.txt ファイルを開き、StorageGRID システムへのアクセスに必要なパスワードを探します。

```
#######################################################################
##### The StorageGRID "recovery package" has been downloaded as: #####
#####           ./sgws-recovery-package-994078-rev1.zip           #####
#####   Safeguard this file as it will be needed in case of a     #####
#####                 StorageGRID node recovery.                  #####
#######################################################################
```

StorageGRID システムがインストールおよび設定されると、確認メッセージが表示されます。

```
StorageGRID has been configured and installed.
```

関連情報

"グリッドの設定とインストールの完了"

"インストール REST API の概要"

# インストール **REST API** の概要

## StorageGRID には、インストールタスクを実行するための StorageGRID インストール API が用意されています。

API のドキュメントは、 Swagger オープンソース API プラットフォームで提供されています。Swagger では、ユーザインターフェイスを使用してパラメータやオプションを変更した場合の API の動作を確認しながら、 API の開発を進めることができます。このドキュメントは、標準的な Web テクノロジと JavaScript Object Notation （ JSON ）データ形式について十分理解していることを前提としています。

API Docs Web ページを使用して実行する API 処理はすべてその場で実行されます。設定データやその他のデータを誤って作成、更新、または削除しないように注意してください。

各 REST API コマンドは、 API の URL 、 HTTP アクション、必須またはオプションの URL パラメータ、お

よび想定される API 応答で構成されます。

**StorageGRID** インストール **API**

StorageGRID インストール API は、 StorageGRID システムを最初に設定するとき、およびプライマリ管理ノードのリカバリを実行する必要がある場合にのみ使用できます。インストール API には、 Grid Manager から HTTPS 経由でアクセスできます。

API のドキュメントにアクセスするには、プライマリ管理ノードのインストール用 Web ページに移動し、メニューバーから * Help * > * API Documentation * を選択します。

StorageGRID インストール API には次のセクションがあります。

- *config *-- API の製品リリースとバージョンに関連する操作。製品リリースバージョンおよびそのリリースでサポートされる API のメジャーバージョンを一覧表示できます。
- * grid * — グリッドレベルの設定操作。グリッドの詳細、グリッドネットワークのサブネット、グリッドパスワード、 NTP および DNS サーバの IP アドレスなど、グリッド設定を取得および更新できます。
- *nodes * — ノードレベルの設定操作。グリッドノードのリストを取得できるほか、グリッドノードの削除、設定、表示、およびグリッドノードの設定のリセットを行うことができます。
- *provision * — プロビジョニング操作。プロビジョニング処理を開始し、プロビジョニング処理のステータスを表示できます。
- * recovery * - プライマリ管理ノードのリカバリ処理。情報のリセット、リカバリパッケージのアップロード、リカバリの開始、およびリカバリ処理のステータスの表示を行うことができます。
- * recovery-package * — リカバリパッケージをダウンロードする処理。
- *sites * — サイトレベルの設定操作。サイトを作成、表示、削除、および変更できます。

## 次の手順

## インストールが完了したら、統合と設定のための一連の手順を実行する必要があります。手順には必須のものとオプションのものがあります。

必要な作業

- StorageGRID システムにオブジェクトを格納するために使用されるクライアントプロトコル（ Swift または S3 ）ごとに、テナントアカウントを作成します。
- グループとユーザアカウントを設定してシステムアクセスを制御します。管理者グループおよびユーザをインポートできるように、必要に応じて、フェデレーテッドアイデンティティソース（ Active Directory や OpenLDAP など）を設定できます。または、ローカルグループやユーザを作成することもできます。
- StorageGRID システムにオブジェクトをアップロードするために使用する S3 または Swift API クライアントアプリケーションを統合し、テストします。
- 準備ができたら、オブジェクトデータの保護に使用する情報ライフサイクル管理（ ILM ）ルールと ILM ポリシーを設定します。

StorageGRID をインストールすると、デフォルトの ILM ポリシーである Baseline 2 Copies Policy がアクティブになります。このポリシーには組み込みの ILM ルール（ Make 2 Copies ）が含まれており、他のポリシーがアクティブ化されていない場合に適用されます。

- インストール環境にアプライアンスストレージノードが含まれている場合は、 SANtricity ソフトウェアを使用して次の作業を実行します。
  - 各 StorageGRID アプライアンスに接続します。
  - AutoSupport データの受信を確認します。
- StorageGRID システムにアーカイブノードが含まれている場合は、アーカイブノードからターゲットの外部アーカイブストレージシステムへの接続を設定します。

> アーカイブノードが Tivoli Storage Manager を外部アーカイブストレージシステムとして使用する場合は、 Tivoli Storage Manager を設定する必要もあります。

- StorageGRID システムのセキュリティ設定ガイドラインに従ってセキュリティリスクを排除します。
- システムアラートの E メール通知を設定します。

任意のタスク

- （レガシー）アラームシステムから通知を受信するには、アラーム用のメーリングリストおよび E メール通知を設定します。
- 導入を計画し、リカバリパッケージを生成したあとにグリッドノードの IP アドレスが変わった場合は、それらの IP アドレスを更新します。リカバリとメンテナンスの手順の IP アドレスの変更に関する情報を参照してください。
- 必要に応じて、ストレージ暗号化を設定します。
- 必要に応じて、ストレージの圧縮を設定し、格納されているオブジェクトのサイズを削減します。
- 監査クライアントアクセスを設定します。NFS または CIFS ファイル共有を通じて、監査を目的としたシステムへのアクセスを設定できます。StorageGRID の管理手順を参照してください。

> CIFS / Samba を使用した監査エクスポートは廃止されており、 StorageGRID の今後のリリースで削除される予定です。

## インストールに関する問題のトラブルシューティング

StorageGRID システムのインストール中に問題が発生した場合は、インストールログファイルにアクセスできます。テクニカルサポートが問題を解決するためにインストールログファイルを使用することもあります。

次のインストールログファイルは、各ノードを実行しているコンテナからアクセスできます。

- `/var/local/log/install.log` （すべてのグリッドノードに存在）
- `/var/local/log/gdu-server.log` （プライマリ管理ノードに存在）

次のインストールログファイルは、ホストからアクセスできます。

- `/var/log/storagegrid/daemon.log`
- `/var/log/storagegrid/nodes/node-name.log`

ログファイルへのアクセス方法については、 StorageGRID の監視とトラブルシューティングの手順を参照し

てください。アプライアンスの設置に関する問題のトラブルシューティングについては、使用しているアプライアンスの設置とメンテナンスの手順を参照してください。その他のサポートが必要な場合は、テクニカルサポートにお問い合わせください。

関連情報

"トラブルシューティングを監視します"

"SG100 SG1000サービスアプライアンス"

"SG6000 ストレージアプライアンス"

"SG5700 ストレージアプライアンス"

"SG5600 ストレージアプライアンス"

"ネットアップサポート"

## /etc/sysconfig/network-scripts の例

以下のサンプルファイルを使用して、4つのLinux物理インターフェイスを1つのLACPボンドにまとめ、3つのVLANインターフェイスを確立して、StorageGRID のグリッドネットワーク、管理ネットワーク、およびクライアントネットワークのインターフェイス用にボンドを分割します。

物理インターフェイス

リンクの反対側のスイッチでも、 4 つのポートを 1 つの LACP トランクまたはポートチャネルとして扱い、少なくともタグで参照された 3 つの VLAN を通過させる必要があります。

**/etc/sysconfig/network-scripts/ifcfg-ens160**

```
TYPE=Ethernet
NAME=ens160
UUID=011b17dd-642a-4bb9-acae-d71f7e6c8720
DEVICE=ens160
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

**/etc/sysconfig/network-scripts/ifcfg-ens192**

```
TYPE=Ethernet
NAME=ens192
UUID=e28eb15f-76de-4e5f-9a01-c9200b58d19c
DEVICE=ens192
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

**/etc/sysconfig/network-scripts/ifcfg-ens224**

```
TYPE=Ethernet
NAME=ens224
UUID=b0e3d3ef-7472-4cde-902c-ef4f3248044b
DEVICE=ens224
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

**/etc/sysconfig/network-scripts/ifcfg-ens256**

```
TYPE=Ethernet
NAME=ens256
UUID=7cf7aabc-3e4b-43d0-809a-1e2378faa4cd
DEVICE=ens256
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

ボンドインターフェイス

**/etc/sysconfig/network-scripts/ifcfg-bond0**

```
DEVICE=bond0
TYPE=Bond
BONDING_MASTER=yes
NAME=bond0
ONBOOT=yes
BONDING_OPTS=mode=802.3ad
```

**VLAN** インターフェイス

**/etc/sysconfig/network-scripts/ifcfg-bond0.1001**

```
VLAN=yes
TYPE=Vlan
DEVICE=bond0.1001
PHYSDEV=bond0
VLAN_ID=1001
REORDER_HDR=0
BOOTPROTO=none
UUID=296435de-8282-413b-8d33-c4dd40fca24a
ONBOOT=yes
```

**/etc/sysconfig/network-scripts/ifcfg-bond0.1002**

```
VLAN=yes
TYPE=Vlan
DEVICE=bond0.1002
PHYSDEV=bond0
VLAN_ID=1002
REORDER_HDR=0
BOOTPROTO=none
UUID=dbaaec72-0690-491c-973a-57b7dd00c581
ONBOOT=yes
```

**/etc/sysconfig/network-scripts/ifcfg-bond0.1003**

```
VLAN=yes
TYPE=Vlan
DEVICE=bond0.1003
PHYSDEV=bond0
VLAN_ID=1003
REORDER_HDR=0
BOOTPROTO=none
UUID=d1af4b30-32f5-40b4-8bb9-71a2fbf809a1
ONBOOT=yes
```

# Ubuntu または Debian をインストールします

UbuntuまたはDebianの環境にStorageGRID ソフトウェアをインストールする方法について説明します。

- "インストールの概要"
- "計画と準備"

- "仮想グリッドノードの導入"
- "グリッドの設定とインストールの完了"
- "インストールの自動化"
- "インストール REST API の概要"
- "次の手順"
- "インストールに関する問題のトラブルシューティング"
- "/etc/network/interfaces の例"

## インストールの概要

Ubuntu または Debian 環境への StorageGRID システムのインストールは、主に 3 つの手順で行われます。

1. * 準備 * ：計画と準備の際に、次のタスクを実行します。
   - StorageGRID のハードウェア要件とストレージ要件について説明します。
   - ネットワークを適切に設定するためのStorageGRID ネットワークの詳細について説明します。詳細については、StorageGRID のネットワークに関するガイドラインを参照してください。
   - StorageGRID グリッドノードのホストとして使用する物理サーバまたは仮想サーバを決めて準備する。
   - 準備したサーバで、次の作業を行います。
     - Ubuntu または Debian をインストールします
     - ホストネットワークを設定する
     - ホストストレージを設定する
     - Docker をインストールする
     - StorageGRID ホストサービスをインストールする
2. * 導入 * ：適切なユーザインターフェイスを使用してグリッドノードを導入します。導入したグリッドノードは、 StorageGRID システムの一部として作成され、 1 つ以上のネットワークに接続されます。
   a. UbuntuまたはDebianのコマンドライン構成ファイルを使用して、手順1で準備したホストに仮想グリッドノードを導入します。
   b. StorageGRID アプライアンスノードを導入するには、 StorageGRID アプライアンスインストーラを使用します。

   > ハードウェア固有の設置と統合の手順は、 StorageGRID インストール手順 には含まれていません。StorageGRID アプライアンスのインストール方法については、使用するアプライアンスのインストールとメンテナンスの手順を参照してください。

3. * 設定 * ：すべてのノードを導入したら、 Grid Manager を使用してグリッドを設定し、インストールを完了します。

以下の手順では、 Ubuntu または Debian 環境に StorageGRID システムを導入して設定するための標準的なアプローチを推奨しています。次の代替アプローチに関する情報も参照してください。

- Ansible 、 Puppet 、 Chef などの標準的なオーケストレーションフレームワークを使用して、 Ubuntu または Debian のインストール、ネットワークとストレージの設定、 Docker と StorageGRID ホストサービスのインストール、および仮想グリッドノードの導入を行う。
- Python 設定スクリプト（インストールアーカイブに付属）を使用して、 StorageGRID システムの導入と設定を自動化します。
- Python 設定スクリプト（インストールアーカイブまたは StorageGRID アプライアンスインストーラで入手可能）を使用して、アプライアンスグリッドノードの導入と設定を自動化する。
- StorageGRID 環境を高度に開発する場合は、インストール REST API を使用して StorageGRID グリッドノードのインストールを自動化します。

関連情報

"計画と準備"

"仮想グリッドノードの導入"

"グリッドの設定とインストールの完了"

"StorageGRID ホストサービスのインストールと設定を自動化する"

"インストール REST API の概要"

"ネットワークガイドライン"

# 計画と準備

## グリッドノードの導入および StorageGRID グリッドの設定を行う前に、手順 を完了するためのステップと要件を把握しておく必要があります。

StorageGRID の導入手順と設定手順を実行するには、 StorageGRID システムのアーキテクチャと運用に関する十分な知識が必要です。

一度に 1 つ以上のサイトを導入できますが、ストレージノードが少なくとも 3 つ必要であるという最小要件をすべてのサイトが満たしている必要があります。

StorageGRID のインストールを開始する前に、次の作業を実行する必要があります

- ノードごとの CPU や RAM の最小要件など、 StorageGRID のコンピューティング要件を確認します。
- トラフィックの分離、セキュリティ、および管理性の向上のために複数のネットワークをサポートする StorageGRID の仕組みについて理解し、 StorageGRID の各ノードに接続するネットワークを決めます。

  StorageGRID のネットワークに関するガイドラインを参照してください。

- 各タイプのグリッドノードのストレージ要件とパフォーマンス要件を把握します。
- 導入予定の StorageGRID ノードの数とタイプに応じて、それらをサポートできる十分なリソースを備えた一連のサーバ（物理、仮想、またはその両方）を特定します。
- 物理ホストに対して、サービスを中断することなく定期的なメンテナンスを実行する場合は、ノード移行の要件を確認します。
- すべてのネットワーク情報を事前に収集します。DHCP を使用している場合を除き、各グリッドノードに

割り当てる IP アドレス、および使用される Domain Name System （ DNS ；ドメインネームシステム）サーバと Network Time Protocol （ NTP ；ネットワークタイムプロトコル）サーバの IP アドレスを収集してください。

- StorageGRID アプライアンスを含む必要なすべてのハードウェアを仕様に従って設置、接続、設定します。

> ハードウェア固有の設置と統合の手順は、 StorageGRID インストール手順 には含まれていません。StorageGRID アプライアンスのインストール方法については、使用するアプライアンスのインストールとメンテナンスの手順を参照してください。

- 使用する導入ツールと設定ツールを決定します。

関連情報

"ネットワークガイドライン"

"SG100 SG1000サービスアプライアンス"

"SG6000 ストレージアプライアンス"

"SG5700 ストレージアプライアンス"

"SG5600 ストレージアプライアンス"

"ノードコンテナの移行要件"

前提要件

## StorageGRID をインストールする前に、必要な情報やデータ、機器を揃えておく必要があります。

| 項目 | 注： |
| --- | --- |
| NetApp StorageGRID ライセンス | デジタル署名された有効なネットアップライセンスが必要です。<br><br>• 注： StorageGRID インストールアーカイブには、グリッドのテストとコンセプトの実証に使用できる非本番環境のライセンスが含まれています。 |
| StorageGRID インストールアーカイブ | StorageGRID インストールアーカイブをダウンロードし、ファイルを展開する必要があります。 |

| 項目 | 注： |
| --- | --- |
| サービスラップトップ | StorageGRID システムは、サービスラップトップを介してインストールされます。<br><br>サービスラップトップには次のものが必要です。<br><br>• ネットワークポート<br>• SSH クライアント（ PuTTY など）<br>• サポートされている Web ブラウザ |
| StorageGRID のドキュメント | • リリースノート<br>• StorageGRID の管理手順 |

関連情報

"StorageGRID インストールファイルのダウンロードと展開"

"Web ブラウザの要件"

"StorageGRID の管理"

"リリースノート"

**StorageGRID** インストールファイルのダウンロードと展開

## StorageGRID インストールアーカイブをダウンロードし、必要なファイルを展開する必要があります。

手順

1. ネットアップの StorageGRID ダウンロードページにアクセスします。

   "ネットアップのダウンロード： StorageGRID"

2. 最新のリリースをダウンロードするボタンを選択するか、ドロップダウンメニューから別のバージョンを選択して、「 * Go * 」を選択します。
3. ネットアップアカウントのユーザ名とパスワードを使用してサインインします。
4. 「注意 / 必ずお読みください」という記述が表示されたら、それを読んでチェックボックスを選択してください。

   StorageGRID リリースのインストール後に、必要な修正プログラムを適用する必要があります。詳細については、リカバリおよびメンテナンスの手順にあるホットフィックス手順 を参照してください。

5. エンドユーザライセンス契約を読み、チェックボックスをオンにして、「 * 同意して続行 * 」を選択します。

   選択したバージョンのダウンロードページが表示されます。このページには 3 つの列があります。

6. [Install StorageGRID *（インストールソフトウェアのインストール）]列で、適切なソフトウェアを選択し

ます。

を選択します `.tgz` または `.zip` 使用するプラットフォームに対応したアーカイブファイルです。

- `StorageGRID-Webscale-version-DEB-uniqueID.zip`
- `StorageGRID-Webscale-version-DEB-uniqueID.tgz`

圧縮ファイルには、UbuntuまたはDebianのDEBファイルとスクリプトが含まれています。

を使用します `.zip` ファイルサービスラップトップでWindowsを実行している場合。

7. アーカイブファイルを保存して展開します。
8. 次のリストから必要なファイルを選択します。

必要なファイルは、計画したグリッドトポロジおよび StorageGRID グリッドの導入方法によって異なります。

次の表に示すパスは、展開されたインストールアーカイブによってインストールされた最上位ディレクトリに対する相対パスです。

| パスとファイル名 | 説明 |
| --- | --- |
| | StorageGRID ダウンロードファイルに含まれているすべてのファイルについて説明するテキストファイル。 |
| | テスト環境およびコンセプトの実証環境に使用できる、非本番環境のネットアップライセンスファイル。 |
| | Ubuntu ホストまたは Debian ホストに StorageGRID ノードイメージをインストールするための DEB パッケージ。 |
| | ファイルのMD5チェックサム `/debs/storagegrid-webscale-images-version-SHA.deb`。 |
| | Ubuntu ホストまたは Debian ホストに StorageGRID ホストサービスをインストールするための DEB パッケージ。 |
| 展開スクリプトツール | • 概要 * |
| | StorageGRID システムの設定を自動化するための Python スクリプト。 |
| | StorageGRID アプライアンスの設定を自動化するための Python スクリプト。 |
| | シングルサインオンが有効な場合にグリッド管理 API にサインインするために使用できる Python スクリプトの例。 |

| パスとファイル名 | 説明 |
| --- | --- |
| | で使用するサンプル構成ファイル `configure-storagegrid.py` スクリプト： |
| | で使用する空の構成ファイル `configure-storagegrid.py` スクリプト： |
| | StorageGRID コンテナ導入用の Ubuntu ホストまたは Debian ホストを設定するためのサンプルの Ansible のロールとプレイブック。必要に応じて、ロールまたはプレイブックをカスタマイズできます。 |

関連情報

""

**CPU** と **RAM** の要件

## StorageGRID ソフトウェアをインストールする前に、ハードウェアの確認と設定を行って、 StorageGRID システムをサポートできる状態にしておきます。

サポートされているサーバについては、 Interoperability Matrix を参照してください。

各 StorageGRID ノードに必要な最小リソースは次のとおりです。

- CPU コア：ノードあたり 8 個
- RAM ：システムで実行されている StorageGRID 以外のソフトウェアの合計 RAM 容量によって、ノードあたり 24 GB 以上、システム RAM の合計容量から 2 ~ 16 GB 削減されます

それぞれの物理ホストまたは仮想ホストで実行する StorageGRID ノードの数が、利用可能な CPU コアや物理 RAM を超えないようにしてください。ホストが StorageGRID 専用ではない場合（非推奨）は、他のアプリケーションのリソース要件も考慮する必要があります。

> CPU とメモリの使用状況を定期的に監視して、ワークロードに継続的に対応できるようにします。たとえば、仮想ストレージノードの RAM 割り当てと CPU 割り当てを 2 倍にすると、StorageGRID アプライアンスノードの場合と同様のリソースが提供されます。また、ノードあたりのメタデータの量が 500GB を超える場合は、ノードあたりの RAM を 48GB 以上に増やすことを検討してください。オブジェクトメタデータストレージの管理、 Metadata Reserved Space 設定の拡張、 CPU とメモリの使用状況の監視については、 StorageGRID の管理、監視、アップグレードの手順を参照してください。

基盤となる物理ホストでハイパースレッディングが有効である場合は、ノードあたり 8 個の仮想コア（ 4 個の物理コア）で構成できます。基盤となる物理ホストでハイパースレッディングが有効でない場合は、ノードあたり 8 個の物理コアを用意する必要があります。

仮想マシンをホストとして使用する場合、 VM のサイズと数を制御可能であれば、 StorageGRID ノードごとに 1 つの VM を使用し、それに応じて VM のサイズを設定する必要があります。

本番環境では、複数のストレージノードを同じ物理ストレージハードウェアまたは仮想ホストで実行しないでください。単一の StorageGRID 環境の各ストレージノードをそれぞれ独自の分離された障害ドメインに配置するようにします。単一のハードウェア障害が単一のストレージノードにしか影響しないようにすることで、

オブジェクトデータの耐久性と可用性を最大限に高めることができます。

ストレージ要件に関する情報も参照してください。

関連情報

"NetApp Interoperability Matrix Tool で確認できます"

"ストレージとパフォーマンスの要件"

"StorageGRID の管理"

"トラブルシューティングを監視します"

"ソフトウェアをアップグレードする"

ストレージとパフォーマンスの要件

# 初期設定と将来のストレージ拡張に対応できる十分なスペースを確保できるよう、StorageGRID ノードのストレージ要件を把握しておく必要があります。

StorageGRID ノードに必要なストレージは、 3 つの論理カテゴリに分類されます。

- * コンテナプール * - ノードコンテナ用のパフォーマンス階層（ 10K SAS または SSD ）のストレージ。 StorageGRID ノードをサポートするホストに Docker をインストールして設定するときに、 Docker ストレージドライバに割り当てられます。
- * システムデータ * — システムデータとトランザクションログのノード単位の永続的ストレージ用のパフォーマンス階層（ 10K SAS または SSD ）ストレージ。 StorageGRID ホストサービスで個々のノードにマッピングされて使用されます。
- * オブジェクトデータ * — オブジェクトデータとオブジェクトメタデータの永続的なストレージを実現するパフォーマンス階層（ 10K SAS または SSD ）のストレージと大容量階層（ NL-SAS / SATA ）のストレージ。

カテゴリに関係なく、いずれのストレージにも RAID ベースのブロックデバイスを使用する必要があります。非冗長ディスク、 SSD 、または JBOD はサポートされていません。いずれのカテゴリのストレージにも、共有またはローカルのどちらかの RAID ストレージを使用できます。ただし、 StorageGRID のノード移行機能を使用する場合は、システムデータとオブジェクトデータの両方を共有ストレージに格納する必要があります。

パフォーマンス要件

コンテナプールのボリューム、システムデータのボリューム、およびオブジェクトメタデータのボリュームのパフォーマンスは、システム全体のパフォーマンスに大きく影響します。ボリュームのディスクパフォーマンスが、レイテンシ、 1 秒あたりの入出力操作（ IOPS ）、スループットの点で適切になるように、それらのボリュームにはパフォーマンス階層（ 10K SAS または SSD ）のストレージを使用します。オブジェクトデータの永続的なストレージには、大容量階層（ NL-SAS / SATA ）のストレージを使用できます。

コンテナプール、システムデータ、およびオブジェクトデータ用のボリュームでは、ライトバックキャッシュを有効にする必要があります。キャッシュは、保護されたメディアまたは永続的なメディアに配置する必要があります。

#### NetApp AFF ストレージを使用するホストの要件

StorageGRID ノードが NetApp AFF システムから割り当てられたストレージを使用している場合は、ボリュームで FabricPool 階層化ポリシーが有効になっていないことを確認してください。StorageGRID ノードで使用するボリュームで FabricPool による階層化を無効にすることで、トラブルシューティングとストレージの処理がシンプルになります。

> StorageGRID を使用して StorageGRID に関連するデータを FabricPool 自体に階層化しないでください。StorageGRID データを StorageGRID に階層化すると、トラブルシューティングと運用がより複雑になります。

##### 必要なホストの数

各 StorageGRID サイトに、少なくとも 3 つのストレージノードが必要です。

> 本番環境では、 1 つの物理ホストまたは仮想ホストで複数のストレージノードを実行しないでください。各ストレージノードに専用のホストを使用すると、分離された障害ドメインが提供されます。

管理ノードやゲートウェイノードなど、他のタイプのノードは、同じホストに導入するか、必要に応じて独自の専用ホストに導入することができます。

##### 各ホストのストレージボリュームの数

次の表に、ホストに導入するノードの種類別に、各ホストに必要なストレージボリューム（ LUN ）の数と各 LUN に必要な最小サイズを示します。

テストで使用できる LUN の最大サイズは 39TB です。

> これらはホストごとの数値を示したものであり、グリッド全体の数値ではありません。

| **LUN** の目的 | ストレージのカテゴリ | **LUN** の数 | **LUN** あたりの最小サイズ |
|---|---|---|---|
| Docker ストレージプール | コンテナプール | 1. | ノードの総数 × 100GB |
| `/var/local` ボリューム | システムデータ | このホストのノードごとに 1 個 | 90GB |
| ストレージノード | オブジェクトデータ | このホストのストレージノードごとに 3 個<br>• 注：ソフトウェアベースのストレージノードには 1~16 個のストレージボリュームを設定できます。 3 個以上のストレージボリュームを推奨します。 | 4、000GB詳細については、ストレージノードのストレージ要件を参照してください。 |

| LUN の目的 | ストレージのカテゴリ | LUN の数 | LUN あたりの最小サイズ |
| --- | --- | --- | --- |
| 管理ノードの監査ログ | システムデータ | このホストの管理ノードごとに 1 個 | 200GB |
| 管理ノードのテーブル | システムデータ | このホストの管理ノードごとに 1 個 | 200GB |

設定されている監査レベル、 S3 オブジェクトキー名などのユーザ入力のサイズ、保持する必要がある監査ログデータの量によっては、各管理ノードの監査ログ LUN のサイズを増やす必要があります。原則として、 S3 処理ごとに約 1 KB の監査データが生成されることから、 200GB の LUN で 1 日あたり 7 、 000 万件の処理、 1 秒あたり 2 ~ 3 日間で 800 件の処理がサポートされることになります。

ホストの最小ストレージスペース

次の表に、各タイプのノードに必要な最小ストレージスペースを示します。この表を参照して、ホストに導入するノードの種類に応じて、ストレージカテゴリごとにホストで確保しなければならない最小ストレージ容量を決定できます。

ディスクの Snapshot を使用してグリッドノードをリストアすることはできません。各タイプのノードのリカバリとメンテナンスの手順を参照してください。

| ノードのタイプ | コンテナプール | システムデータ | オブジェクトデータ |
| --- | --- | --- | --- |
| ストレージノード | 100 GB | 90GB | 4 、 000GB |
| 管理ノード | 100 GB | 490GB （ 3 個の LUN ） | _ 該当なし _ |
| ゲートウェイノード | 100 GB | 90GB | _ 該当なし _ |
| アーカイブノード | 100 GB | 90GB | _ 該当なし _ |

例：ホストのストレージ要件の計算

同じホストに 3 つのノードを導入することを計画しているとします。ストレージノードが 1 つ、管理ノードが 1 つ、ゲートウェイノードが 1 つです。ホストには少なくとも 9 個のストレージボリュームを用意する必要があります。ノードコンテナ用にパフォーマンス階層のストレージが 300GB 以上、システムデータとトランザクションログ用にパフォーマンス階層のストレージが 670GB 以上、オブジェクトデータ用に容量階層のストレージが 12TB 以上、それぞれ必要になります。

| ノードのタイプ | LUN の目的 | LUN の数 | LUN サイズ |
| --- | --- | --- | --- |
| ストレージノード | Docker ストレージプール | 1. | 300GB （ 100GB/ ノード ） |
| ストレージノード | `/var/local` ボリューム | 1. | 90GB |

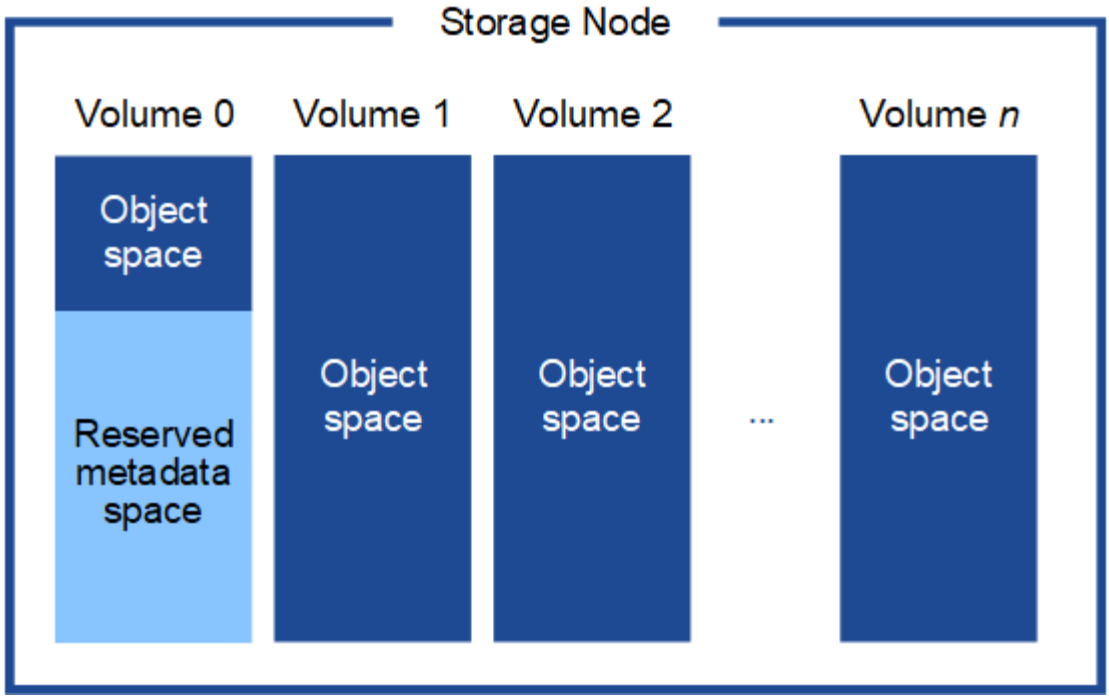
| ノードのタイプ | **LUN** の目的 | **LUN** の数 | **LUN** サイズ |
| --- | --- | --- | --- |
| ストレージノード | オブジェクトデータ | 3. | 4 、 000GB |
| 管理ノード | `/var/local` ボリューム | 1. | 90GB |
| 管理ノード | 管理ノードの監査ログ | 1. | 200GB |
| 管理ノード | 管理ノードのテーブル | 1. | 200GB |
| ゲートウェイノード | `/var/local` ボリューム | 1. | 90GB |
| • 合計 * | | • 9 * | • コンテナプール： * 300GB<br>• システムデータ： *670GB<br>• オブジェクトデータ ： 12 、 000GB |

ストレージノードのストレージ要件

ソフトウェアベースのストレージノードのストレージボリューム数は 1~16 個までにすることを推奨します。-3 個以上のストレージボリュームを使用することを推奨します。各ストレージボリュームのサイズは 4TB 以上にします。

アプライアンスストレージノードには、最大 48 個のストレージボリュームを設定できます。

図に示すように、 StorageGRID は各ストレージノードのストレージボリューム 0 にオブジェクトメタデータ用のスペースをリザーブします。ストレージボリューム 0 の残りのスペースとストレージノード内のその他のストレージボリュームは、オブジェクトデータ専用に使用されます。




冗長性を確保し、オブジェクトメタデータを損失から保護するために、 StorageGRID は各サイトのシステム内のすべてのオブジェクトにメタデータのコピーを 3 つずつ格納します。オブジェクトメタデータの 3 つのコピーが各サイトのすべてのストレージノードに均等に分散されます。

新しいストレージノードのボリューム 0 にスペースを割り当てる場合は、そのノードのすべてのオブジェクトメタデータの一部に対して十分なスペースを確保する必要があります。

- 少なくとも 4TB をボリューム 0 に割り当てる必要があります。

> ストレージノードでストレージボリュームを 1 つしか使用していない場合に、そのボリュームに 4TB 以下を割り当てると、ストレージノードが起動時にストレージ読み取り専用状態になり、オブジェクトメタデータのみが格納される可能性があります。

- 新しいStorageGRID 11.5システムをインストールするときに、各ストレージノードに128GB以上のRAMがある場合は、ボリューム0に8TB以上を割り当てる必要があります。ボリューム 0 に大きな値を設定すると、各ストレージノードでメタデータに使用できるスペースが増加する可能性があります。
- サイトに複数のストレージノードを設定する場合は、可能であればボリューム 0 にも同じ設定を使用します。サイトにサイズが異なるストレージノードがある場合、ボリューム 0 が最も小さいストレージノードがそのサイトのメタデータ容量を決定します。

詳細については、StorageGRID の管理手順を参照し、「オブジェクト・メタデータ・ストレージの管理」を検索してください。

"StorageGRID の管理"

関連情報

"ノードコンテナの移行要件"

""

# ノード移行機能を使用すると、ホスト間でノードを手動で移動できます。通常、両方のホストが同じ物理データセンターにあります。

ノード移行を使用すると、グリッドの運用を中断せずに物理ホストのメンテナンスを実行できます。単に、すべての StorageGRID ノードを一度に 1 つずつ別のホストに移動してから、物理ホストをオフラインにします。ノードを 1 つずつ移行するため、それぞれのダウンタイムはごくわずかであり、グリッドサービスの運用や可用性には影響しません。

StorageGRID のノード移行機能を使用する場合は、いくつかの追加の要件を満たす必要があります。

- 単一の物理データセンターのホスト間で一貫したネットワークインターフェイス名を使用する必要があります
- StorageGRID のメタデータとオブジェクトのリポジトリボリューム用に、単一の物理データセンターのすべてのホストからアクセスできる共有ストレージを用意する必要があります。たとえば、 NetApp E シリーズストレージアレイなどを使用できます。

仮想ホストを使用する場合、基盤となるハイパーバイザーレイヤで VM の移行がサポートされていれば、その機能を StorageGRID のノード移行機能の代わりに使用することができます。その場合、これらの追加要件は無視してかまいません。

移行またはハイパーバイザーのメンテナンスを実行する前に、ノードを正常にシャットダウンしてください。グリッドノードのシャットダウンについては、リカバリとメンテナンスの手順を参照してください。

### **VMware** のライブマイグレーションはサポートされていません

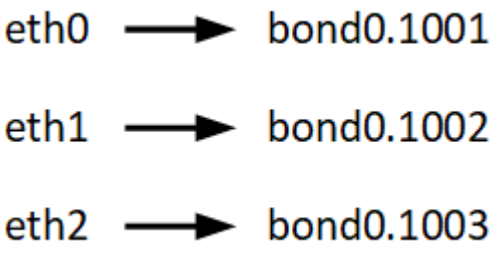
OpenStack Live Migration と VMware のライブ vMotion 原因 ：仮想マシンのクロック時間を急に進むことができるため、どのタイプのグリッドノードでもサポートされていません。まれにではありますが、クロック時間が不正確だとデータや設定の更新が失われることがあります。

コールドマイグレーションはサポートされています。コールドマイグレーションでは、 StorageGRID ノードをホスト間で移行する前にシャットダウンします。リカバリとメンテナンスの手順で、グリッドノードをシャットダウンする方法については、手順 を参照してください。

### 一貫したネットワークインターフェイス名

ノードを別のホストに移動するにあたり、 StorageGRID ホストサービスでは、ノードが現在の場所で使用している外部ネットワーク接続を新しい場所でもそのまま使用できるようにする必要があります。これは、ホスト内で一貫したネットワークインターフェイス名を使用することで実現されます。

たとえば、 Host1 で実行されている StorageGRID NodeA で、インターフェイスのマッピングが次のように設定されているとします。



矢印の左側は、 StorageGRID コンテナ内から見た従来のインターフェイス（グリッドネットワーク、管理ネットワーク、およびクライアントネットワークのインターフェイス）です。矢印の右側は、これらのネットワークを提供する実際のホストインターフェイスに対応しています。この 3 つの VLAN インターフェイスは、同じ物理インターフェイスボンドに従属します。

この NodeA を Host2 に移行するとします。Host2 に bond0.1001 、 bond0.1002 、および bond0.1003 という名前のインターフェイスがある場合、 Host2 では同じ名前のインターフェイスが Host1 と同じ接続を提供すると仮定して、移動が許可されます。Host2 に同じ名前のインターフェイスがなければ、移動は許可されません。

複数のホスト間で一貫したネットワーク・インターフェイス名を得るには'さまざまな方法があります例については'ホスト・ネットワークの構成を参照してください

共有ストレージ

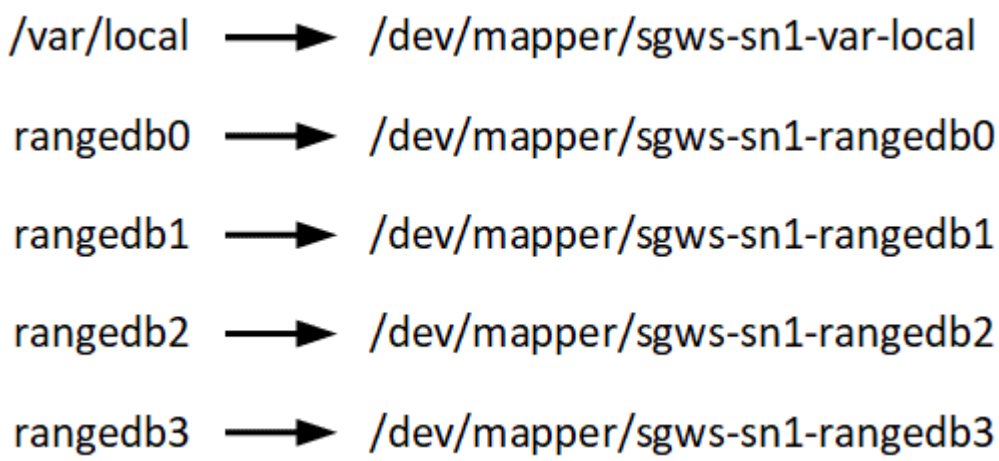
オーバーヘッドを抑えて迅速にノードを移行するために、 StorageGRID のノード移行機能ではノードのデータの物理的な移動は行いません。代わりに、エクスポート処理とインポート処理を組み合わせて、次のようにノードが移行されます。

手順

1. 「ノードのエクスポート」操作中に、 HostA で実行されているノードコンテナから永続的な状態の少量のデータが抽出され、そのノードのシステムデータボリュームにキャッシュされます。そのあと、 HostA のノードコンテナのインスタンス化が解除されます。
2. 「ノードのインポート」操作中に、 HostA と同じネットワークインターフェイスマッピングおよびブロックストレージマッピングを使用する HostB 上のノードコンテナがインスタンス化されます。次に、キャッシュされた永続状態データが新しいインスタンスに挿入されます。

この処理では、ノードのすべてのシステムデータボリュームとオブジェクトストレージボリュームに HostA と HostB の両方からアクセスできないと移行は実行できません。また、 HostA と HostB で同じ LUN を参照するように、同じ名前を使用してノードにマッピングされている必要があります。

次の例は、StorageGRID ストレージノードのブロックデバイスマッピング用の解決策 を示しています。これらのホストではDMマルチパスを使用しており、でaliasフィールドを使用しています `/etc/multipath.conf` すべてのホストで使用できる一貫性のあるわかりやすいブロックデバイス名を提供します。




関連情報

"ホストネットワークを設定する"

""

**Web** ブラウザの要件

## サポートされている Web ブラウザを使用する必要があります。

| **Web** ブラウザ | サポートされる最小バージョン |
|---|---|
| Google Chrome | 87 |
| Microsoft Edge の場合 | 87 |
| Mozilla Firefox | 84 |

ブラウザウィンドウの幅を推奨される値に設定してください。

| ブラウザの幅 | ピクセル |
|---|---|
| 最小（ Minimum ） | 1024 |
| 最適 | 1280 |

導入ツール

## StorageGRID のインストールのすべてまたは一部を自動化するとメリットが得られる場合があります。

導入を自動化すると、次のいずれかの場合に役立ちます。

- 物理ホストや仮想ホストの導入と設定に Ansible 、 Puppet 、 Chef などの標準のオーケストレーションフレームワークをすでに使用している場合。
- 複数の StorageGRID インスタンスを導入する場合。
- 大規模で複雑な StorageGRID インスタンスを導入する場合。

StorageGRID ホストサービスはパッケージでインストールされ、構成ファイルで制御されます。構成ファイルは、手動インストール時に対話形式で作成できるほか、あらかじめ用意して（またはプログラム化して）標準のオーケストレーションフレームワークを使用した自動インストールに使用できます。StorageGRID には、 StorageGRID アプライアンスと StorageGRID システム全体（「グリッド」）の設定を自動化するためのオプションの Python スクリプトが用意されています。これらのスクリプトは直接使用することも、StorageGRID インストール REST API の使用方法を調べることもできます。グリッドの導入ツールや設定ツールを独自に開発する際の参考としても使用できます。

StorageGRID の導入のすべてまたは一部を自動化する場合は'インストール・プロセスを開始する前に'インストールの自動化を参照してください

関連情報

"インストールの自動化"

ホストを準備します

StorageGRID の物理ホストまたは仮想ホストの準備作業として、次の手順を実行する必要があります。これらの手順は、Ansible、Puppet、Chefなどの標準のサーバ設定フレームワークを使用して、ほとんどまたはすべて自動化することができます。

関連情報

"StorageGRID ホストサービスのインストールと設定を自動化する"

#### Linux をインストールしています

Ubuntu または Debian をすべてのグリッドホストにインストールする必要があります。サポートされているバージョンの一覧については、 NetApp Interoperability Matrix Tool を参照してください。

手順

1. ディストリビュータの指示または標準の手順 に従って、UbuntuまたはDebianをすべての物理グリッドホストまたは仮想グリッドホストにインストールします。

   グラフィカルデスクトップ環境はインストールしないでください。Ubuntu をインストールする場合は、 * 標準のシステムユーティリティ * を選択する必要があります。Ubuntu ホストへの SSH アクセスを有効にするには、 * OpenSSH サーバ * を選択することを推奨します。その他のオプションはすべて選択しないままにすることができます

2. すべてのホストが Ubuntu または Debian のパッケージリポジトリにアクセスできることを確認します。
3. スワップが有効になっている場合：

   a. 次のコマンドを実行します。 `$ sudo swapoff --all`

   b. からすべてのスワップエントリを削除します `/etc/fstab` をクリックして設定を保持します。

   スワップを完全に無効にできないと、パフォーマンスが大幅に低下する可能性があります

関連情報

"NetApp Interoperability Matrix Tool で確認できます"

#### AppArmorプロファイルのインストールの概要

自社で導入した Ubuntu 環境を運用し、 AppArmor の必須のアクセス制御システムを使用している場合、ベースシステムにインストールするパッケージに関連付けられた AppArmor プロファイルが、 StorageGRID と一緒にインストールされた対応するパッケージによってブロックされる可能性があります。

デフォルトでは、 AppArmor プロファイルは、ベースのオペレーティングシステムにインストールするパッケージに対してインストールされます。StorageGRID システムコンテナからこれらのパッケージを実行すると、 AppArmor プロファイルがブロックされます。DHCP 、 MySQL 、 NTP 、 tcdump のベースパッケージ

が AppArmor と競合するほか、これら以外のベースパッケージも競合する可能性があります。

AppArmor プロファイルの対処方法としては、次の 2 つの選択肢があります。

- ベースシステムにインストールされたパッケージのうち、 StorageGRID システムコンテナに含まれるパッケージと重複するパッケージのプロファイルを個々に無効にする。各プロファイルを無効にすると、 StorageGRID ログファイルに AppArmor が有効であることを示すエントリが表示されます。

  次のコマンドを使用します。

  ```
  sudo ln -s /etc/apparmor.d/<profile.name> /etc/apparmor.d/disable/
  sudo apparmor_parser -R /etc/apparmor.d/<profile.name>
  ```

- 例： *

  ```
  sudo ln -s /etc/apparmor.d/bin.ping /etc/apparmor.d/disable/
  sudo apparmor_parser -R /etc/apparmor.d/bin.ping
  ```

- AppArmor 全体を無効にする。Ubuntu 9.10 以降の場合は、 Ubuntu のオンラインコミュニティに記載されている手順に従います。 "AppArmor を無効にします"。

  AppArmor を無効にしたあとは、 StorageGRID ログファイルに AppArmor が有効であることを示すエントリは表示されません。

ホストネットワークを設定する

## ホストへの Linux のインストールの完了後、このあとに導入する StorageGRID ノードにマッピングする一連のネットワークインターフェイスを準備するために、各ホストでいくつかの追加の設定が必要になることがあります。

必要なもの

- StorageGRID のネットワークに関するガイドラインを確認しておきます。

  "ネットワークガイドライン"

- ノードコンテナの移行要件に関する情報を確認しておく必要があります。

  "ノードコンテナの移行要件"

- 仮想ホストを使用している場合は、MACアドレスのクローニングに関する考慮事項と推奨事項を確認してから、ホストネットワークを設定してください。

  "MAC アドレスのクローニングに関する考慮事項と推奨事項"

> VM をホストとして使用する場合は、仮想ネットワークアダプタとして VMXNET 3 を選択する必要があります。VMware E1000 ネットワークアダプタは、特定の Linux のディストリビューションで導入された StorageGRID コンテナで接続の問題が発生しました。

このタスクについて

グリッドノードは、グリッドネットワークにアクセスできる必要があります。また、管理ネットワークとクライアントネットワークにアクセスすることもできます。このアクセスを確立するには、ホストの物理インターフェイスを各グリッドノードの仮想インターフェイスに関連付けるマッピングを作成します。ホストインターフェイスを作成するときにわかりやすい名前を使用すると、すべてのホストへの導入が簡単になり、移行も可能になります。

ホストと 1 つ以上のノードで、同じインターフェイスを共有できます。たとえば、ホストアクセス用とノード管理ネットワークアクセス用のインターフェイスに同じものを使用すると、ホストとノードをメンテナンスしやすくなります。ホストと個々のノードで同じインターフェイスを共有できますが、 IP アドレスはすべて異なっている必要があります。IP アドレスはノード間やホストと任意のノード間で共有できません。

グリッドネットワークのインターフェイスについては、ホストのすべての StorageGRID ノードで同じホストネットワークインターフェイスを使用したり、ノードごとに異なるホストネットワークインターフェイスを使用したり、任意のインターフェイスを使用したりできます。ただし、通常は、単一のホストのグリッドネットワークと管理ネットワークの両方のインターフェイス、またはいずれかのノードのグリッドネットワークのインターフェイスと別のホストのクライアントネットワークのインターフェイスに同じホストネットワークインターフェイスを使用することはありません。

このタスクはさまざまな方法で実行できます。たとえば、仮想マシンをホストとする環境でホストごとに 1 つまたは 2 つの StorageGRID ノードを導入する場合は、ハイパーバイザーで正しい数のネットワークインターフェイスを作成し、 1 対 1 のマッピングを使用できます。本番環境用のベアメタルホストに複数のノードを導入する場合は、 Linux ネットワークスタックの VLAN と LACP のサポートを利用してフォールトトレランスと帯域幅の共有を実現できます。以降のセクションでは、これら両方の例について詳細なアプローチを紹介します。これらのいずれかを使用する必要はありません。それぞれのニーズに合わせてアプローチを選択できます。

> ボンドデバイスやブリッジデバイスをコンテナネットワークインターフェイスとして直接使用しないでください。これにより、カーネル問題 が原因で発生するノードの起動が妨げられ、コンテナネームスペース内のボンドデバイスおよびブリッジデバイスで MACVLAN が使用される可能性があります。代わりに、 VLAN ペアや仮想イーサネット（ veth ）ペアなどの非ボンディングデバイスを使用してください。このデバイスをノード構成ファイルのネットワークインターフェイスとして指定してください。

**MAC** アドレスのクローニングに関する考慮事項と推奨事項

MACアドレスのクローニングでは、Dockerコンテナでホストの**MAC**アドレスが使用され、指定したアドレスまたはランダムに生成されたアドレスの**MAC**アドレスがホストで使用されます。プロミスキャスモードのネットワーク設定を使用しないようにするには、 MAC アドレスのクローニングを使用します。

**MAC** クローニングのイネーブル化

環境によっては、管理ネットワーク、グリッドネットワーク、およびクライアントネットワークに専用の仮想 NIC を使用できるため、 MAC アドレスのクローニングによってセキュリティを強化できます。Dockerコンテナでホスト上の専用NICのMACアドレスを使用すると、プロミスキャスモードのネットワーク設定を回避できます。

> MAC アドレスクローニングは、仮想サーバ環境で使用するためのものであり、物理アプライアンスのすべての構成で正常に機能しない場合があります。

MAC クローニングのターゲットインターフェイスがビジー状態のためにノードを起動できない場合は、ノードを起動する前にリンクを「停止」に設定しなければならないことがあります。また、リンクが稼働しているときに仮想環境でネットワークインターフェイス上の MAC クローニングが実行されないことがあります。インターフェイスがビジーなためにノードで MAC アドレスの設定が失敗してノードが起動しなかった場合は、問題 を修正する前にリンクを「停止」に設定することがあります。

MAC アドレスクローニングは、デフォルトでは無効になっており、ノード設定キーで設定する必要があります。StorageGRID をインストールするときに有効にする必要があります。

ネットワークごとに 1 つのキーがあります。

- `ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`
- `GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`
- `CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`

キーを「true」に設定すると、DockerコンテナでホストのNICのMACアドレスが使用されます。さらに、ホストは指定されたコンテナネットワークの MAC アドレスを使用します。デフォルトでは、コンテナアドレスはランダムに生成されたアドレスですが、を使用して設定した場合は、です `_NETWORK_MAC` ノード設定キー。アドレスを代わりに使用します。ホストとコンテナの MAC アドレスは常に異なります。

ハイパーバイザーでプロミスキャスモードも有効にせずに仮想ホストの MAC クローニングを有効にすると、ホストのインターフェイスを使用して原因 Linux ホストのネットワークが停止する可能性があります。

**MAC** クローン作成の使用例

MAC クローニングでは、次の 2 つのユースケースを検討します。

- MACクローン作成が有効になっていない場合 `_CLONE_MAC` ノード構成ファイルのキーが設定されていないか「false」に設定されていない場合、ホストはホストNIC MACを使用し、にMACを指定しないかぎりコンテナにStorageGRIDによって生成されたMACが含まれます `_NETWORK_MAC` キーを押します。アドレスがに設定されている場合 `_NETWORK_MAC` キーを指定すると、コンテナのアドレスがに指定されます `_NETWORK_MAC` キーを押します。このキーの設定では、プロミスキャスモードを使用する必要があります。
- MACクローン作成が有効になっている場合 `_CLONE_MAC` ノード構成ファイルのキーは「true」に設定されています。コンテナではホストNIC MACを使用し、でMACを指定しないかぎりStorageGRIDによって生成されたMACをホストで使用します `_NETWORK_MAC` キーを押します。アドレスがに設定されている場合 `_NETWORK_MAC` キー。ホストは、生成されたアドレスではなく、指定されたアドレスを使用します。このキーの設定では、プロミスキャスモードは使用しないでください。

MAC アドレスのクローニングを使用せずに、ハイパーバイザーによって割り当てられた MAC アドレス以外の MAC アドレスのデータをすべてのインターフェイスが送受信できるようにする場合は、次の手順を実行します。 仮想スイッチおよびポートグループレベルのセキュリティプロパティが、無差別モード、 MAC アドレスの変更、および Forged Transmits の **Accept** に設定されていることを確認します。仮想スイッチに設定された値は、ポートグループレベルの値によって上書きできるため、両方のレベルで設定が同じであることを確認してください。

MACクローニングをイネーブルにするには、ノードコンフィギュレーションファイルの作成手順を参照してください。

"ノード構成ファイルを作成しています"

**MAC** クローニングの例

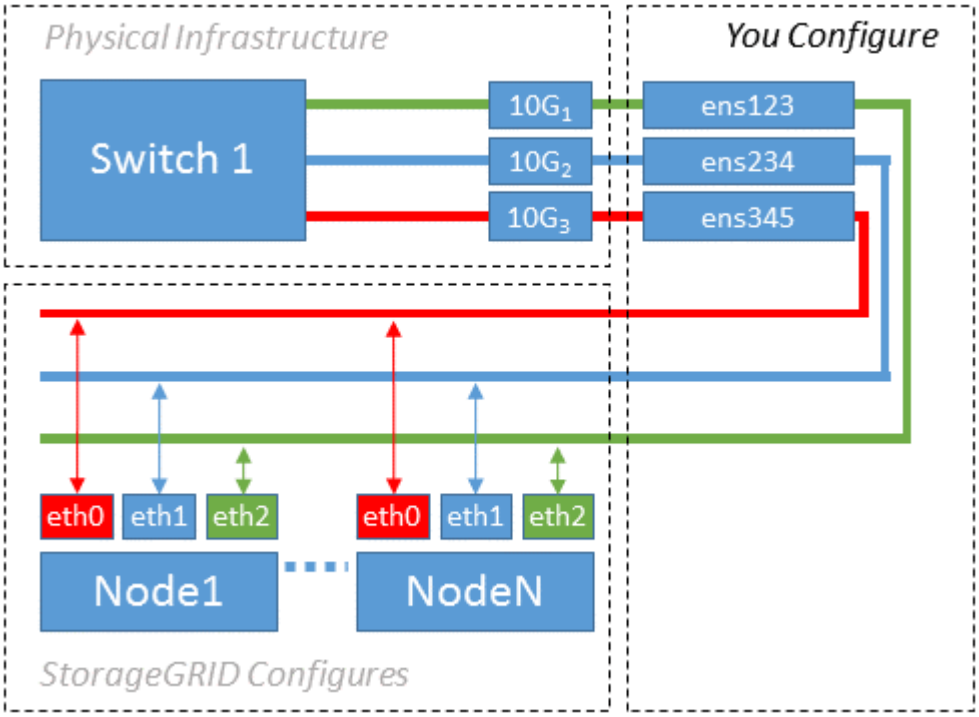
MAC アドレスが 11 ： 22 ： 33 ： 44 ： 55 ： 66 のホストでインターフェイス ens256 の MAC クローニングをイネーブルにし、ノード構成ファイルで次のキーを使用する例：

- `ADMIN_NETWORK_TARGET = ens256`
- `ADMIN_NETWORK_MAC = b2:9c:02:c2:27:10`
- `ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC = true`

結果： ens256 のホスト MAC は b2 ： 9C ： 02 ： c2 ： 27 ： 10 、管理ネットワーク MAC は 11 ： 22 ： 33 ： 44 ： 55 ： 66 になります

例 **1** ：物理 **NIC** または仮想 **NIC** への **1** 対 **1** のマッピング

例 1 では、ホスト側の設定がほとんどまたはまったく必要ない単純な物理インターフェイスのマッピングについて説明します。




Linux オペレーティングシステムは、インストールまたはブート時、またはインターフェイスのホットアド時に ensXYZ インターフェイスを自動的に作成します。インターフェイスがブート後に自動的に起動するように設定されていることを確認する以外に必要な設定はありません。あとで設定プロセスでマッピングを正しく指定できるように、どの ensXYZ がどの StorageGRID ネットワーク（グリッド、管理、またはクライアント）に対応しているかを決定する必要があります。

この図は複数の StorageGRID ノードを示していますが、通常はこの構成をシングルノードの VM に使用します。

スイッチ 1 が物理スイッチの場合は、インターフェイス 10G1 10G 3 に接続されたポートをアクセスモードとして設定し、適切な VLAN に配置します。

例 2 ： LACP ボンドを使用した VLAN の伝送

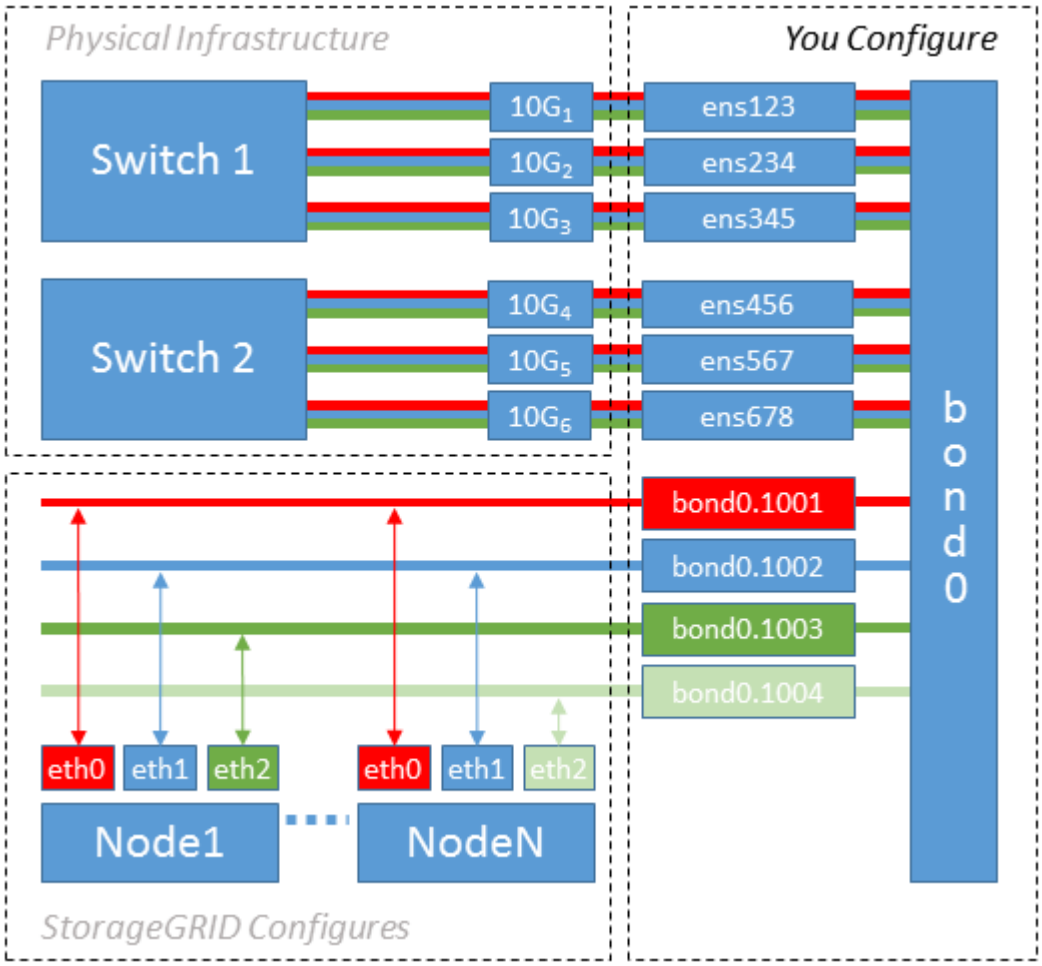
例 2 は、ネットワークインターフェイスのボンディングおよび使用している Linux ディストリビューションでの VLAN インターフェイスの作成に関する十分な知識があることを前提としています。

このタスクについて

例 2 では、汎用の柔軟な VLAN ベースのスキームを使用して、使用可能なすべてのネットワーク帯域幅を単一のホスト上のすべてのノードで共有する方法について説明します。この例は、ベアメタルホストに特に該当します。

この例を理解するために、各データセンターにグリッドネットワーク、管理ネットワーク、クライアントネットワーク用に 3 つのサブネットがあるとします。サブネットは個別の VLAN （ 1001 、 1002 、 1003 ）上にあり、 LACP ボンディングされたトランクポート（ bond0 ）でホストに提示されます。この場合、ボンドに bond0.1001 、 bond0.1002 、および bond0.1003 の 3 つの VLAN インターフェイスを設定します。

同じホスト上のノードネットワークに別々の VLAN とサブネットが必要な場合は、ボンドに VLAN インターフェイスを追加してホストにマッピングできます（図の bond0.1004 と表示）。




手順

1. StorageGRID ネットワークの接続に使用するすべての物理ネットワークインターフェイスを単一の LACP ボンドとしてまとめます。

すべてのホストのボンドに同じ名前（ bond0 など）を使用してください。

2. このボンドを関連する「物理デバイス」として使用するVLANインターフェイスを作成します," `using the standard VLAN interface naming convention `physdev-name.VLAN ID`。

   手順 1 と 2 のそれぞれについて、ネットワークリンクの反対側の終端にあるエッジスイッチで適切な設定を行う必要があります。エッジスイッチのポートも LACP ポートチャネルに集約してトランクとして設定し、必要なすべての VLAN を許可する必要があります。

   このホストごとのネットワーク構成スキームに使用できるサンプルのインターフェイス構成ファイルが提供されています。

関連情報

"/etc/network/interfaces の例"

ホストストレージを設定しています

# 各ホストにブロックストレージボリュームを割り当てる必要があります。

必要なもの

以下のトピックで、このタスクを実行するために必要な情報を確認しておきます。

"ストレージとパフォーマンスの要件"

"ノードコンテナの移行要件"

このタスクについて

ブロック・ストレージ・ボリューム（ LUN ）をホストに割り当てるときは ' ストレージ要件の表を使用して ' 次の項目を決定します

- 各ホストに必要なボリュームの数（そのホストに導入するノードの数とタイプに応じて異なる）
- 各ボリュームのストレージのカテゴリ（システムデータまたはオブジェクトデータ）
- 各ボリュームのサイズ

ホストに StorageGRID ノードを導入するときは、この情報に加え、各物理ボリュームに Linux から割り当てられた永続的な名前を使用します。

これらのボリュームがホストに認識されることだけ確認すれば、ボリュームをパーティショニング、フォーマット、マウントする必要はありません。

「raw」形式の特殊なデバイス・ファイルは使用しないでください (`/dev/sdb`たとえば、）ボリューム名のリストを作成する際に、これらのファイルはホストのリブート時に変わることがあり、システムの適切な運用に影響します。`iSCSI LUN`およびデバイスマッパーマルチパスを使用する場合は、でマルチパスのエイリアスを使用することを検討してください `/dev/mapper` ディレクトリ、特にSANトポロジに共有ストレージへの冗長ネットワークパスが含まれている場合。または、システムで作成されたのソフトリンクをで使用することもできます `/dev/disk/by-path/` をクリックします。

例：

```
ls -l
$ ls -l /dev/disk/by-path/
total 0
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:00:07.1-ata-2 -> ../../sr0
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0 ->
../../sda
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part1
-> ../../sda1
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part2
-> ../../sda2
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:1:0 ->
../../sdb
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:2:0 ->
../../sdc
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:3:0 ->
../../sdd
```

結果はインストールごとに異なります。

これらのブロックストレージボリュームのそれぞれにわかりやすい名前を割り当てると、 StorageGRID の最初のインストールや以降のメンテナンスの手順が簡単になります。デバイスマッパーマルチパスドライバを使用して共有ストレージボリュームへのアクセスを冗長化する場合は、を使用することができます `alias` フィールドに入力します `/etc/multipath.conf` ファイル。

例：

```
multipaths {
      multipath {
            wwid 3600a09800059d6df00005df2573c2c30
            alias docker-storage-volume-hostA
      }
      multipath {
            wwid 3600a09800059d6df00005df3573c2c30
            alias sgws-adm1-var-local
      }
      multipath {
            wwid 3600a09800059d6df00005df4573c2c30
            alias sgws-adm1-audit-logs
      }
      multipath {
            wwid 3600a09800059d6df00005df5573c2c30
            alias sgws-adm1-tables
      }
      multipath {
            wwid 3600a09800059d6df00005df6573c2c30
            alias sgws-gw1-var-local
      }
      multipath {
            wwid 3600a09800059d6df00005df7573c2c30
            alias sgws-sn1-var-local
      }
      multipath {
            wwid 3600a09800059d6df00005df7573c2c30
            alias sgws-sn1-rangedb-0
      }
      …
```

これにより、でブロックデバイスとして表示されるエイリアスが原因 されます `/dev/mapper` ホスト上のディレクトリ。設定処理やメンテナンス処理の際にブロックストレージボリュームの指定が必要となったときに、わかりやすい、検証が容易な名前を指定できます。

> StorageGRID のノード移行やデバイスマッパーマルチパスの使用をサポートするために共有ストレージを設定する場合は、共通のファイルを作成してインストールすることができます `/etc/multipath.conf` 共同配置されたすべてのホスト。各ホストで使用する Docker ストレージボリュームが異なる点に注意してください。エイリアスを使用し、各 Docker ストレージボリュームの LUN のエイリアスにターゲットのホスト名を含めると覚えやすいので、この方法で設定することを推奨します。

関連情報

"ストレージとパフォーマンスの要件"

"ノードコンテナの移行要件"

**Docker**ストレージボリュームを設定する

## Dockerをインストールする前に、Dockerストレージボリュームをフォーマットして、にマウントする必要があります `/var/lib/docker`。

このタスクについて

Dockerストレージボリュームにローカルストレージを使用する予定で、を含むホストパーティションに十分なスペースがある場合は、以下の手順をスキップできます `/var/lib`。

手順

1. Docker ストレージボリュームにファイルシステムを作成します。

```
sudo mkfs.ext4 docker-storage-volume-device
```

2. Docker ストレージボリュームをマウントします。

```
sudo mkdir -p /var/lib/docker
sudo mount docker-storage-volume-device /var/lib/docker
```

3. /etc/fstab に docker -storage-volume-device のエントリを追加します。

   これにより、ホストのリブート後にストレージボリュームが自動的に再マウントされます。

**Docker** をインストールする

## StorageGRID システムは、 Docker コンテナの集合として Linux 上で実行されます。StorageGRID をインストールする前に、 Docker をインストールする必要があります。

手順

1. 使用している Linux ディストリビューションの手順に従って Docker をインストールします。

   Docker が Linux ディストリビューションに含まれていない場合は、 Docker の Web サイトからダウンロードできます。

2. 次の 2 つのコマンドを実行して、 Docker が有効化され、起動されたことを確認します。

```
sudo systemctl enable docker
```

```
sudo systemctl start docker
```

3. 次のコマンドを入力して、必要なバージョンの Docker がインストールされたことを確認します。

```
sudo docker version
```

クライアントとサーバのバージョンが1.10.3以降である必要があります。

```
Client:
  Version:      1.10.3
  API version:  1.22
  Go version:   go1.6.1
  Git commit:   20f81dd
  Built:        Wed, 20 Apr 2016 14:19:16 -0700
  OS/Arch:      linux/amd64

Server:
  Version:      1.10.3
  API version:  1.22
  Go version:   go1.6.1
  Git commit:   20f81dd
  Built:        Wed, 20 Apr 2016 14:19:16 -0700
  OS/Arch:      linux/amd64
```

関連情報

"ホストストレージを設定しています"

**StorageGRID** ホストサービスをインストールしています

## StorageGRID ホストサービスをインストールするには、 StorageGRID の DEB パッケージを使用します。

このタスクについて

以下の手順では、 DEB パッケージからホストサービスをインストールする方法を説明します。また、インストールアーカイブに含まれている APT リポジトリメタデータを使用して、 DEB パッケージをリモートでインストールすることもできます。使用している Linux オペレーティングシステムの APT リポジトリに関する手順を参照してください。

手順

1. StorageGRID の DEB パッケージを個々のホストにコピーするか、共有ストレージに置きます。

   たとえば、に配置します `/tmp` ディレクトリ。次の手順でコマンドの例を使用できます。

2. 各ホストに root アカウントまたは sudo 権限を持つアカウントでログインし、次のコマンドを実行します。

   をインストールする必要があります `images` パッケージを最初に、および `service` パッケージ2番目。パッケージを以外のディレクトリに配置した場合は `/tmp`をクリックし、使用したパスに応じてコマンドを変更します。

```
sudo dpkg --install /tmp/storagegrid-webscale-images-version-SHA.deb
```

```
sudo dpkg --install /tmp/storagegrid-webscale-service-version-SHA.deb
```

StorageGRID パッケージをインストールするには、 Python 2.7 がインストールされている必要があります。。 `sudo dpkg --install /tmp/storagegrid-webscale-images-version-SHA.deb` 完了するまでコマンドは失敗します。

## 仮想グリッドノードの導入

UbuntuまたはDebian環境にグリッドノードを導入する際には、すべてのノードのノード構成ファイルを作成して検証し、StorageGRID ホストサービスを開始してノードを起動します。StorageGRID アプライアンスストレージノードを導入する必要がある場合は、すべての仮想ノードを導入したあとに、アプライアンスのインストールとメンテナンスの手順を参照してください。

- "ノード構成ファイルを作成しています"
- "StorageGRID 構成を検証しています"
- "StorageGRID ホストサービスを開始しています"

関連情報

"SG100 SG1000サービスアプライアンス"

"SG5600 ストレージアプライアンス"

"SG5700 ストレージアプライアンス"

"SG6000 ストレージアプライアンス"

### ノード構成ファイルを作成しています

ノード構成ファイルは、ノードを起動して適切なネットワークおよびブロックストレージリソースに接続するために StorageGRID ホストサービスで必要となる情報をまとめた小さいテキストファイルです。ノード構成ファイルは仮想ノードに使用され、アプライアンスノードには使用されません。

#### ノード構成ファイルの配置場所

各StorageGRID ノードの構成ファイルをに配置する必要があります `/etc/storagegrid/nodes` ノードを実行するホスト上のディレクトリ。たとえば、HostAで管理ノード、ゲートウェイノード、およびストレージノードを1つずつ実行する場合は、3つのノード構成ファイルをに配置する必要があります `/etc/storagegrid/nodes` をクリックします。構成ファイルは、 vim や nano などのテキストエディタを使用して各ホストで直接作成することも、別の場所で作成して各ホストに移動することもできます。

### ノード構成ファイルの名前

構成ファイルの名前は、の形式で指定します `<node-name>.conf`、ここで `<node-name>` は、ノードに割り当てる名前です。この名前は StorageGRID インストーラに表示され、ノード移行などのノードのメンテナンス処理で使用されます。

ノード名は次のルールに従って付ける必要があります。

- 一意である必要があります
- 1 文字目はアルファベットにする必要があります
- A~Z と a~z のアルファベットを使用できます
- 0~9 の数字を使用できます
- 1 つまたは複数のハイフン（ - ）を含めることができます。
- を含めない32文字以内で指定します `.conf` 内線番号

内のすべてのファイル `/etc/storagegrid/nodes` この命名規則に従っていないデータは、ホストサービスで解析されません。

グリッドでマルチサイトトポロジを使用する場合の一般的なノード名は次のようになります。

```
<site>-<node type>-<node number>.conf
```

たとえば、のように指定します `dc1-adm1.conf` データセンター1の最初の管理ノード用、および `dc2-sn3.conf` データセンター2の3つ目のストレージノード。ただし、すべてのノード名がルールに従っていれば、別の名前にしてもかまいません。

### ノード構成ファイルの内容

構成ファイルには、キーと値のペアが 1 行に 1 つずつ含まれています。キーと値のペアごとに、次のルールに従う必要があります。

- キーと値は等号で区切る必要があります (=)と空白(オプション)。
- キーにスペースを含めることはできません。
- 値にはスペースを含めることができます。
- 先頭または末尾の空白は無視されます。

キーの種類に応じて、すべてのノードで必要なものと省略可能なもの、特定のノードタイプでのみ必要なものがあります。

次の表に、サポートされているすべてのキーについて、使用可能な値を示します。中央の列：

- R * ：必須 + BP ：ベストプラクティス + O ：オプション

| キーを押します | **R** 、 **BP** 、または **O** | 価値 |
| --- | --- | --- |
| ADMIN_IP を指定します | BP | このノードが属するグリッドのプライマリ管理ノードのグリッドネットワークの IPv4 アドレス。GRID_NETWORK_IP で指定した値を Node_type=VM_Admin_Node および ADMIN_NETWORK_role = Primary のグリッドノードに使用します。このパラメータを省略すると、 mDNS を使用してプライマリ管理ノードの検出が試行されます。<br><br>「グリッドノードによるプライマリ管理ノードの検出」を参照してください。<br><br>• 注 * ：この値は無視されます。また、プライマリ管理ノードでは禁止される場合があります。 |
| ADMIN_NETWORK_CONFIG | o | DHCP 、 STATIC 、または DISABLED |
| ADMIN_NETWORK_ESL | o | このノードが管理ネットワークゲートウェイ経由で通信する CIDR 表記のサブネットをカンマで区切ったリスト。<br><br>例：172.16.0.0/21、172.17.0.0/21 |
| ADMIN_NETWORK_GATEWAY | O （ * R * ） | このノードのローカルの管理ネットワークゲートウェイの IPv4 アドレス。ADMIN_NETWORK_IP および ADMIN_NETWORK_MASK で定義されるサブネットに属している必要があります。この値は、 DHCP によって設定されたネットワークでは無視されます。<br><br>• 注 * ：このパラメータは、 ADMIN_NETWORK_ESL が指定されている場合は必須です。<br><br>例<br><br>• 1.1.1.1<br>• 10.224.81 |

| キーを押します | **R** 、 **BP** 、または **O** | 価値 |
| --- | --- | --- |
| ADMIN_NETWORK_IP | o | このノードの管理ネットワークにおける IPv4 アドレス。このキーが必要なのは、 ADMIN_NETWORK_CONFIG = STATIC の場合だけです。それ以外の値の場合は指定しないでください。<br><br>例<br><br>• 1.1.1.1<br>• 10.224.81 |
| ADMIN_NETWORK_MAC | o | コンテナ内の管理ネットワークインターフェイスの MAC アドレス。<br><br>このフィールドはオプションです。省略すると、 MAC アドレスが自動的に生成されます。<br><br>6 つの 16 進数値をコロンで区切って指定する必要があります。<br><br>例：b2：9C：02：c2：27：10 |
| ADMIN_NETWORK_MASK | o | このノードの管理ネットワークにおける IPv4 ネットマスク。このキーが必要なのは、 ADMIN_NETWORK_CONFIG = STATIC の場合だけです。それ以外の値の場合は指定しないでください。<br><br>例<br><br>• 255.255.255.0<br>• 255.255.248.0と入力します |

| キーを押します | **R** 、 **BP** 、または **O** | 価値 |
| --- | --- | --- |
| ADMIN_NETWORK_MTU を指定します | o | このノードの管理ネットワークでの最大伝送ユニット（ MTU ）。ADMIN_NETWORK_CONFIG = DHCP の場合は指定しないでください。この値を指定する場合、 1280 ～ 9216 の範囲で指定する必要があります。省略すると、 1500 が使用されます。<br><br>ジャンボフレームを使用する場合は、 MTU を 9000 などのジャンボフレームに適した値に設定します。それ以外の場合は、デフォルト値のままにします。<br><br>• 重要 * ：ネットワークの MTU 値は、ノードが接続されているスイッチポートに設定された値と一致する必要があります。そうしないと、ネットワークパフォーマンスの問題やパケット損失が発生する可能性があります。<br><br>例<br><br>• 1 、 500<br>• 8、192です |

| キーを押します | **R** 、 **BP** 、または **O** | 価値 |
| --- | --- | --- |
| ADMIN_NETWORK_TARGET | BP | StorageGRID ノードで管理ネットワークのアクセスに使用するホストデバイスの名前。ネットワークインターフェイス名のみがサポートされています。通常、GRID_NETWORK_TARGET または CLIENT_NETWORK _TARGET に指定したインターフェイス名とは別のインターフェイス名を使用します。<br><br>• 注：ボンドデバイスやブリッジデバイスをネットワークターゲットとして使用しないでください。ボンドデバイスの上に VLAN （または他の仮想インターフェイス）を設定するか、ブリッジと仮想イーサネット（ veth ）のペアを使用します。<br><br>*ベストプラクティス：*管理ネットワークのIPアドレスは、このノードで最初は使用しない場合でも値を指定してください。そうすることで、ホストでノードの設定を再度行わなくても、管理ネットワークの IP アドレスをあとから追加することができます。<br><br>例<br><br>• bond0.1002<br>• ens256 |
| ADMIN_NETWORK_TARGET タイプ | o | インターフェイス<br><br>（サポートされている値はこれだけです）。 |

| キーを押します | **R** 、 **BP** 、または **O** | 価値 |
| --- | --- | --- |
| ADMIN_NETWORK_TARGET_TYPE_interface_clone_MAC | BP | 正しいか間違っているか<br><br>StorageGRID コンテナで管理ネットワークのホストターゲットインターフェイスの MAC アドレスを使用するには、キーを「 true 」に設定して原因 に設定します。<br><br>• ベストプラクティス：プロミスキャスモードが必要なネットワークでは、「 ADMIN_NETWORK_TARGET_TYPE_interface_clone_MAC 」キーを使用してください。<br><br>MACクローニングの詳細については、MACアドレスクローニングの考慮事項と推奨事項を参照してください。<br><br>"MAC アドレスのクローニングに関する考慮事項と推奨事項" |
| ADMIN_NETWORK_ROLE | • R * | Primary または Non-Primary<br><br>このキーが必要なのは、 node_type が VM_Admin_Node の場合だけです。それ以外のタイプのノードの場合は指定しないでください。 |

| キーを押します | **R** 、 **BP** 、または **O** | 価値 |
| --- | --- | --- |
| BLOBK_DEVICE_AUDIT_logs | • R * | このノードで監査ログの永続的なストレージに使用するブロックデバイススペシャルファイルのパスと名前。このキーが必要なのは、node_type が VM_Admin_Node のノードだけです。それ以外のタイプのノードの場合は指定しないでください。<br><br>例<br><br>• `/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`<br>• `/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`<br>• `/dev/mapper/sgws-adm1-audit-logs` |

| キーを押します | **R** 、 **BP** 、または **O** | 価値 |
| --- | --- | --- |
| BLOCK_DEVICE_RANGEDB_00<br><br>BLOCK_DEVICE_RANGEDB_01<br><br>BLOCK_DEVICE_RANGEDB_02<br><br>BLOCK_DEVICE_RANGEDB_03<br><br>BLOCK_DEVICE_RANGEDB_04<br><br>BLOCK_DEVICE_RANGEDB_05<br><br>BLOCK_DEVICE_RANGEDB_06<br><br>BLOCK_DEVICE_RANGEDB_07<br><br>BLOCK_DEVICE_RANGEDB_08<br><br>BLOCK_DEVICE_RANGEDB_09<br><br>BLOCK_DEVICE_RANGEDB_10<br><br>BLOCK_DEVICE_RANGEDB_11<br><br>BLOCK_DEVICE_RANGEDB_12<br><br>BLOCK_DEVICE_RANGEDB_13<br><br>BLOCK_DEVICE_RANGEDB_14<br><br>BLOCK_DEVICE_RANGEDB_15 | • R * | このノードでオブジェクトの永続的なストレージに使用するブロックデバイススペシャルファイルのパスと名前。このキーが必要なのは、 node_type が VM_Storage_Node のノードだけです。それ以外のタイプのノードの場合は指定しないでください。<br><br>BLOCK_DEVICE_RANGEDB_00のみが必須で、それ以外は省略可能で<br>す。BLOCK_DEVICE_RANGEDB_00に指定するブロックデバイスは4TB以上である必要があります。それ以外は4TB未満でもかまいません。<br><br>*注：ギャップを残さないでください。BLOCK_DEVICE_RANGEDB_05を指定する場合<br>は、BLOCK_DEVICE_RANGEDB_04も指定されている必要があります。<br><br>例<br><br>• `/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`<br>• `/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`<br>• `/dev/mapper/sgws-sn1-rangedb-0` |

| キーを押します | **R** 、 **BP** 、または **O** | 価値 |
| --- | --- | --- |
| BLOBK_DEVICE_tables | • R * | このノードでデータベーステーブルの永続的なストレージに使用するブロックデバイススペシャルファイルのパスと名前。このキーが必要なのは、 node_type が VM_Admin_Node のノードだけです。それ以外のタイプのノードの場合は指定しないでください。<br><br>例<br><br>• `/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`<br>• `/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`<br>• `/dev/mapper/sgws-adm1-tables` |
| BLOBK_DEVICE_VAR_LOCAL です | • R * | このノードが /var/local の永続的ストレージに使用するブロックデバイススペシャルファイルのパスと名前。<br><br>例<br><br>• `/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`<br>• `/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`<br>• `/dev/mapper/sgws-sn1-var-local` |
| CLIENT_NETWORK_CONFIG | o | DHCP 、 STATIC 、または DISABLED |

| キーを押します | **R** 、 **BP** 、または **O** | 価値 |
| --- | --- | --- |
| CLIENT_NETWORK_GATEWAY | o | このノードのローカルのクライアントネットワークゲートウェイの IPv4 アドレス。CLIENT_NETWORK_IP および CLIENT_NETWORK_MASK で定義されるサブネットに属している必要があります。この値は、DHCP によって設定されたネットワークでは無視されます。<br><br>例<br><br>• 1.1.1.1<br>• 10.224.81 |
| CLIENT_NETWORK_IP | o | このノードのクライアントネットワークにおける IPv4 アドレス。このキーが必要なのは、CLIENT_NETWORK_CONFIG = STATIC の場合だけです。それ以外の値の場合は指定しないでください。<br><br>例<br><br>• 1.1.1.1<br>• 10.224.81 |
| CLIENT_NETWORK_MAC | o | コンテナ内のクライアントネットワークインターフェイスの MAC アドレス。<br><br>このフィールドはオプションです。省略すると、 MAC アドレスが自動的に生成されます。<br><br>6 つの 16 進数値をコロンで区切って指定する必要があります。<br><br>例：b2：9C：02：c2：27：20 |

| キーを押します | **R** 、 **BP** 、または **O** | 価値 |
| --- | --- | --- |
| CLIENT_NETWORK_MASK | o | このノードのクライアントネットワークにおける IPv4 ネットマスク。このキーが必要なのは、CLIENT_NETWORK_CONFIG = STATIC の場合だけです。それ以外の値の場合は指定しないでください。<br><br>例<br><br>• 255.255.255.0<br>• 255.255.248.0と入力します |
| CLIENT_NETWORK_MTU | o | このノードのクライアントネットワークでの最大伝送ユニット（ MTU<br>）。CLIENT_NETWORK_CONFIG = DHCP の場合は指定しないでください。この値を指定する場合、 1280 ～ 9216 の範囲で指定する必要があります。省略すると、 1500 が使用されます。<br><br>ジャンボフレームを使用する場合は、 MTU を 9000 などのジャンボフレームに適した値に設定します。それ以外の場合は、デフォルト値のままにします。<br><br>• 重要 * ：ネットワークの MTU 値は、ノードが接続されているスイッチポートに設定された値と一致する必要があります。そうしないと、ネットワークパフォーマンスの問題やパケット損失が発生する可能性があります。<br><br>例<br><br>• 1 、 500<br>• 8、192です |

| キーを押します | **R** 、 **BP** 、または **O** | 価値 |
| --- | --- | --- |
| client_network_target です | BP | StorageGRID ノードでクライアントネットワークのアクセスに使用するホストデバイスの名前。ネットワークインターフェイス名のみがサポートされています。通常、GRID_NETWORK_TARGET または ADMIN_NETWORK_TARGET に指定したインターフェイス名とは別のインターフェイス名を使用します。<br><br>• 注：ボンドデバイスやブリッジデバイスをネットワークターゲットとして使用しないでください。ボンドデバイスの上に VLAN （または他の仮想インターフェイス）を設定するか、ブリッジと仮想イーサネット（ veth ）のペアを使用します。<br>• ベストプラクティス： * クライアントネットワークの IP アドレスは、このノードで最初は使用しない場合でも値を指定してください。そうすることで、ホストでノードの設定を再度行わなくても、クライアントネットワークの IP アドレスをあとから追加することができます。<br><br>例<br><br>• bond0.1003<br>• ens423 |
| client_network_target_type | o | インターフェイス<br><br>（この値のみがサポートされています）。 |

| キーを押します | **R** 、 **BP** 、または **O** | 価値 |
| --- | --- | --- |
| client_network_target_type _interface_clone_MAC | BP | 正しいか間違っているか<br><br>クライアントネットワークでホストターゲットインターフェイスの MAC アドレスを使用するには、キーを「 true 」に設定して StorageGRID コンテナを原因 します。<br><br>• ベストプラクティス：プロミスキャスモードが必要なネットワークでは、client_network_target_type _interface_clone_MAC キーを使用してください。<br><br>MACクローニングの詳細については、MACアドレスクローニングの考慮事項と推奨事項を参照してください。<br><br>"MAC アドレスのクローニングに関する考慮事項と推奨事項" |
| GRID_NETWORK_CONFIG | BP | STATIC または DHCP<br><br>（指定しない場合のデフォルトは STATIC ） |
| GRID_NETWORK_GATEWAY | • R * | このノードのローカルのグリッドネットワークゲートウェイの IPv4 アドレス。 GRID_NETWORK_IP および GRID_NETWORK_MASK で定義されるサブネットに属している必要があります。この値は、DHCP によって設定されたネットワークでは無視されます。<br><br>グリッドネットワークのサブネットが 1 つだけでゲートウェイがない場合は、サブネットの標準のゲートウェイアドレス（ X.Y.Z.1 ）か、このノードの GRID_NETWORK_IP の値を使用します。このどちらかの値にしておけば、以降にグリッドネットワークを拡張するときに処理が簡単になります。 |

| キーを押します | **R** 、 **BP** 、または **O** | 価値 |
| --- | --- | --- |
| GRID_NETWORK_IP | • R * | このノードのグリッドネットワークにおける IPv4 アドレス。このキーが必要なのは、GRID_NETWORK_CONFIG = STATIC の場合だけです。それ以外の値の場合は指定しないでください。<br><br>例<br><br>• 1.1.1.1<br>• 10.224.81 |
| GRID_NETWORK_MAC | o | コンテナ内のグリッドネットワークインターフェイスの MAC アドレス。<br><br>このフィールドはオプションです。省略すると、 MAC アドレスが自動的に生成されます。<br><br>6 つの 16 進数値をコロンで区切って指定する必要があります。<br><br>例：b2：9C：02：c2：27：30 |
| GRID_NETWORK_MASK | o | このノードのグリッドネットワークにおける IPv4 ネットマスク。このキーが必要なのは、GRID_NETWORK_CONFIG = STATIC の場合だけです。それ以外の値の場合は指定しないでください。<br><br>例<br><br>• 255.255.255.0<br>• 255.255.248.0と入力します |

| キーを押します | **R** 、 **BP** 、または **O** | 価値 |
| --- | --- | --- |
| GRID_NETWORK_MTU | o | このノードのグリッドネットワークでの最大伝送ユニット（ MTU ）。GRID_NETWORK_CONFIG = DHCP の場合は指定しないでください。この値を指定する場合、 1280 ～ 9216 の範囲で指定する必要があります。省略すると、 1500 が使用されます。<br><br>ジャンボフレームを使用する場合は、 MTU を 9000 などのジャンボフレームに適した値に設定します。それ以外の場合は、デフォルト値のままにします。<br><br>• 重要 * ：ネットワークの MTU 値は、ノードが接続されているスイッチポートに設定された値と一致する必要があります。そうしないと、ネットワークパフォーマンスの問題やパケット損失が発生する可能性があります。<br>• 重要 * ：ネットワークパフォーマンスを最大限に高めるには、すべてのノードのグリッドネットワークインターフェイスで MTU 値がほぼ同じになるように設定する必要があります。個々のノードのグリッドネットワークの MTU 設定に大きな違いがある場合は、 * Grid Network MTU mismatch * アラートがトリガーされます。MTU 値はすべてのネットワークタイプで同じである必要はありません。<br><br>例<br><br>• 1 、 500<br>• 8、192です |

| キーを押します | **R** 、 **BP** 、または **O** | 価値 |
| --- | --- | --- |
| GRID_NETWORK_TARGET | • R * | StorageGRID ノードでグリッドネットワークのアクセスに使用するホストデバイスの名前。ネットワークインターフェイス名のみがサポートされています。通常、ADMIN_NETWORK_TARGET または ADMIN_NETWORK_TARGET に指定したインターフェイス名とは別のインターフェイス名を使用します。<br><br>• 注：ボンドデバイスやブリッジデバイスをネットワークターゲットとして使用しないでください。ボンドデバイスの上に VLAN （または他の仮想インターフェイス）を設定するか、ブリッジと仮想イーサネット（ veth ）のペアを使用します。<br><br>例<br><br>• bond0.1001<br>• ens192 |
| GRID_NETWORK_TARGET タイプ | o | インターフェイス<br><br>（サポートされている値はこれだけです）。 |

| キーを押します | **R** 、 **BP** 、または **O** | 価値 |
| --- | --- | --- |
| GRID_NETWORK_TARGET<br>_TYPE_interface_clone_MAC | • BP * | 正しいか間違っているか<br><br>グリッドネットワーク上のホストターゲットインターフェイスの MAC アドレスを使用するには、キーの値を「 true 」に設定して StorageGRID コンテナを原因 に設定します。<br><br>• ベストプラクティス：プロミスキャスモードが必要なネットワークでは、GRID_NETWORK_TARGET<br>_TYPE_interface_clone_MAC キーを使用してください。<br><br>MACクローニングの詳細については、MACアドレスクローニングの考慮事項と推奨事項を参照してください。<br><br>"MAC アドレスのクローニングに関する考慮事項と推奨事項" |

| キーを押します | **R** 、 **BP** 、または **O** | 価値 |
| --- | --- | --- |
| MAXIMUM_RAM | o | このノードに使用を許可する RAM の最大容量。このキーを省略した場合、ノードでメモリは制限されません。本番用のノードについて設定するときは、システム RAM の合計容量よりも 24GB 以上、16~32GB 以上小さい値を指定してください。<br><br>• 注 * ： RAM 値は、ノードの実際のメタデータ用リザーブスペースに影響します。Metadata Reserved Spaceとは何かを概要 でStorageGRID を管理する手順を参照してください。<br><br>このフィールドの形式はです `<number><unit>`、ここで `<unit>` は、です `b`、 `k`、 `m`または `g`。<br><br>例<br><br>24G<br><br>38654705664b<br><br>• 注：このオプションを使用する場合は、 memory cgroups のカーネルサポートを有効にする必要があります。 |
| Node_type のように指定します | • R * | ノードのタイプ：<br><br>• VM_Admin_Nodeの略<br>• VM_Storage_Nodeの略<br>• VM_Archive_Nodeの略<br>• VM_API_Gateway |

| キーを押します | **R** 、 **BP** 、または **O** | 価値 |
| --- | --- | --- |
| PORT_REMAP を参照してください | o | ノードが内部でのグリッドノードの通信または外部との通信に使用するポートを再マッピングします。ポートの再マッピングが必要になるのは、 StorageGRID で使用される 1 つ以上のポートがエンタープライズネットワークポリシーで制限されている場合です。詳細については、「内部グリッドノードの通信」または「外部通信」を参照してください。<br><br>• 重要 * ：ロードバランサエンドポイントの設定に使用する予定のポートを再マッピングしないでください。<br>• 注： PORT_REMAP のみを設定すると、指定したマッピングがインバウンド通信とアウトバウンド通信の両方に使用されます。PORT_REMAP_INBOUND を併せて指定した場合は、 PORT_REMAP がアウトバウンド通信のみに適用されます。<br><br>使用される形式は次のとおりです。 `<network type>/<protocol>/<default port used by grid node>/<new port>`network typeはgrid、admin、clientのいずれかで、protocolはTCPまたはUDPです。<br><br>例：<br><br>`PORT_REMAP = client/tcp/18082/443` |

| キーを押します | **R** 、 **BP** 、または **O** | 価値 |
| --- | --- | --- |
| PORT_REMAP_INBOUND | o | 指定したポートのインバウンド通信を再マッピングします。PORT_REMAP_INBOUND を指定して PORT_REMAP に値を指定しなかった場合は、ポートのアウトバウンド通信が変更されません。<br><br>• 重要 * ：ロードバランサエンドポイントの設定に使用する予定のポートを再マッピングしないでください。<br><br>使用される形式は次のとおりです。 `<network type>/<protocol:>/<remapped port >/<default port used by grid node>`network typeはgrid、admin、clientのいずれかで、protocolはTCPまたはUDPです。<br><br>例：<br><br>`PORT_REMAP_INBOUND = grid/tcp/3022/22` |

関連情報

"グリッドノードによるプライマリ管理ノードの検出"

"ネットワークガイドライン"

"StorageGRID の管理"

グリッドノードによるプライマリ管理ノードの検出

## グリッドノードは、設定や管理のためにプライマリ管理ノードと通信します。各グリッドノードがグリッドネットワーク上のプライマリ管理ノードの IP アドレスを認識している必要があります。

グリッドノードからプライマリ管理ノードにアクセスできるようにするために、ノードを導入する際に次のいずれかを実行します。

- ADMIN_IP パラメータを使用して、プライマリ管理ノードの IP アドレスを手動で入力します。
- ADMIN_IP パラメータを省略して、グリッドノードで自動的に値が検出されるようにします。自動検出は、グリッドネットワークで DHCP を使用してプライマリ管理ノードに IP アドレスを割り当てる場合に特に便利です。

プライマリ管理ノードの自動検出には、 mDNS （ multicast Domain Name System ）が使用されます。プライマリ管理ノードは、最初に起動されるときに、 mDNS を使用してそのノードの IP アドレスを公開します。同じサブネット上の他のノードは、この IP アドレスを自動的に照会して取得します。ただし、通常はマルチキャスト IP トラフィックをサブネット間でルーティングできないため、他のサブネット上のノードはプライマリ管理ノードの IP アドレスを直接取得できません。

自動検出を使用する場合：

- プライマリ管理ノードが直接接続されていないサブネットの少なくとも 1 つのグリッドノードで、 ADMIN_IP 設定を指定する必要があります。このグリッドノードがプライマリ管理ノードの IP アドレスを公開することで、サブネット上の他のノードが mDNS を使用して IP アドレスを検出できるようになります。
- ネットワークインフラがサブネット内のマルチキャスト IP トラフィックの転送をサポートしていることを確認します。

ノード構成ファイルの例

## ここでは、 StorageGRID システムで使用するノード構成ファイルを設定する際の参考として、すべてのタイプのグリッドノードのノード構成ファイルの例を示します。

ほとんどのノードについては、 Grid Manager またはインストール API を使用してグリッドを設定するときに、管理ネットワークとクライアントネットワークのアドレス情報（ IP 、マスク、ゲートウェイなど）を追加できます。ただし、プライマリ管理ノードは例外です。グリッドの設定を行うためにプライマリ管理ノードの管理ネットワークの IP を参照する必要がある場合（グリッドネットワークがルーティングされていない場合など）は、プライマリ管理ノードのノード構成ファイルで管理ネットワーク接続を設定する必要があります。次の例を参照してください。

ここに示す例では、クライアントネットワークがデフォルトで無効になっていても、クライアントネットワークターゲットがベストプラクティスとして設定されています。

プライマリ管理ノードの例

ファイル名の例： `/etc/storagegrid/nodes/dc1-adm1.conf`

- ファイルの内容の例： *

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Primary
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adm1-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adm1-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adm1-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.2
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1

ADMIN_NETWORK_CONFIG = STATIC
ADMIN_NETWORK_IP = 192.168.100.2
ADMIN_NETWORK_MASK = 255.255.248.0
ADMIN_NETWORK_GATEWAY = 192.168.100.1
ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0.0/21,172.17.0.0/21
```

ストレージノードの例

ファイル名の例： `/etc/storagegrid/nodes/dc1-sn1.conf`

- ファイルの内容の例： *

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/dc1-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/dc1-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/dc1-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/dc1-sn1-rangedb-3
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

アーカイブノードの例

ファイル名の例： `/etc/storagegrid/nodes/dc1-arc1.conf`

- ファイルの内容の例： *

```
NODE_TYPE = VM_Archive_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-arc1-var-local
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.4
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

ゲートウェイノードの例

ファイル名の例： `/etc/storagegrid/nodes/dc1-gw1.conf`

- ファイルの内容の例： *

```
NODE_TYPE = VM_API_Gateway
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-gw1-var-local
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.5
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

非プライマリ管理ノードの例

ファイル名の例： `/etc/storagegrid/nodes/dc1-adm2.conf`

- ファイルの内容の例： *

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Non-Primary
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adm2-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adm2-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adm2-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.6
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

**StorageGRID** 構成を検証しています

## で構成ファイルを作成した後 `/etc/storagegrid/nodes` 各StorageGRID ノードについて、これらのファイルの内容を検証する必要があります。

構成ファイルの内容を検証するには、各ホストで次のコマンドを実行します。

```
sudo storagegrid node validate all
```

ファイルが正しい場合は、次の例に示すように、各構成ファイルの出力に * PASSED * と表示されます。

```
Checking for misnamed node configuration files… PASSED
Checking configuration file for node dc1-adm1… PASSED
Checking configuration file for node dc1-gw1… PASSED
Checking configuration file for node dc1-sn1… PASSED
Checking configuration file for node dc1-sn2… PASSED
Checking configuration file for node dc1-sn3… PASSED
Checking for duplication of unique values between nodes… PASSED
```

自動インストールの場合は、を使用してこの出力を抑制できます `-q` または `--quiet` のオプションを指定します `storagegrid` コマンド（例： `storagegrid --quiet…`）。出力を抑制した場合、構成で警告またはエラーが検出されたときはゼロ以外の終了値が返されます。

構成ファイルが正しくない場合、次の例に示すように、問題は * WARNING * および * ERROR * として表示されます。構成エラーが見つかった場合は、インストールを続行する前に修正する必要があります。

```
Checking for misnamed node configuration files…
  WARNING: ignoring /etc/storagegrid/nodes/dc1-adm1
  WARNING: ignoring /etc/storagegrid/nodes/dc1-sn2.conf.keep
  WARNING: ignoring /etc/storagegrid/nodes/my-file.txt
Checking configuration file for node dc1-adm1…
  ERROR: NODE_TYPE = VM_Foo_Node
         VM_Foo_Node is not a valid node type.  See *.conf.sample
  ERROR: ADMIN_ROLE = Foo
         Foo is not a valid admin role.  See *.conf.sample
  ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-gw1-var-local
         /dev/mapper/sgws-gw1-var-local is not a valid block device
Checking configuration file for node dc1-gw1…
  ERROR: GRID_NETWORK_TARGET = bond0.1001
         bond0.1001 is not a valid interface.  See `ip link show`
  ERROR: GRID_NETWORK_IP = 10.1.3
         10.1.3 is not a valid IPv4 address
  ERROR: GRID_NETWORK_MASK = 255.248.255.0
         255.248.255.0 is not a valid IPv4 subnet mask
Checking configuration file for node dc1-sn1…
  ERROR: GRID_NETWORK_GATEWAY = 10.2.0.1
         10.2.0.1 is not on the local subnet
  ERROR: ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0foo
         Could not parse subnet list
Checking configuration file for node dc1-sn2… PASSED
Checking configuration file for node dc1-sn3… PASSED
Checking for duplication of unique values between nodes…
  ERROR: GRID_NETWORK_IP = 10.1.0.4
         dc1-sn2 and dc1-sn3 have the same GRID_NETWORK_IP
  ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn2-var-local
         dc1-sn2 and dc1-sn3 have the same BLOCK_DEVICE_VAR_LOCAL
  ERROR: BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn2-rangedb-0
         dc1-sn2 and dc1-sn3 have the same BLOCK_DEVICE_RANGEDB_00
```

**StorageGRID** ホストサービスを開始しています

## StorageGRID ノードを起動し、ホストのリブート後もノードが再起動されるようにするには、 StorageGRID ホストサービスを有効にして開始する必要があります。

手順

1. 各ホストで次のコマンドを実行します。

```
sudo systemctl enable storagegrid
sudo systemctl start storagegrid
```

2. 次のコマンドを実行して、導入の進行状況を確認します。

```
sudo storagegrid node status node-name
```

ステータスが「 Not Running 」または「 Stopped 」のノードに対して、次のコマンドを実行します。

```
sudo storagegrid node start node-name
```

3. StorageGRID ホストサービスを以前に有効にして開始している場合（またはサービスを有効にして開始したかどうかがわからない場合）は、次のコマンドも実行します。

```
sudo systemctl reload-or-restart storagegrid
```

## グリッドの設定とインストールの完了

### プライマリ管理ノード上のグリッドマネージャからStorageGRID システムを設定すると、インストールが完了します。

- "Grid Managerに移動します"
- "StorageGRID ライセンス情報の指定"
- "サイトの追加"
- "グリッドネットワークのサブネットの指定"
- "保留中のグリッドノードを承認します"
- "Network Time Protocolサーバ情報の指定"
- "Domain Name Systemサーバ情報の指定"
- "StorageGRID システムのパスワードの指定"
- "設定を確認し、インストールを完了します"
- "インストール後のガイドライン"

**Grid Manager**に移動します

### StorageGRID システムの設定に必要なすべての情報については、グリッドマネージャを使用して定義します。

必要なもの

プライマリ管理ノードが導入され、最初の起動シーケンスが完了している必要があります。

手順

1. Web ブラウザを開き、次のいずれかのアドレスに移動します。

```
https://primary_admin_node_ip

client_network_ip
```

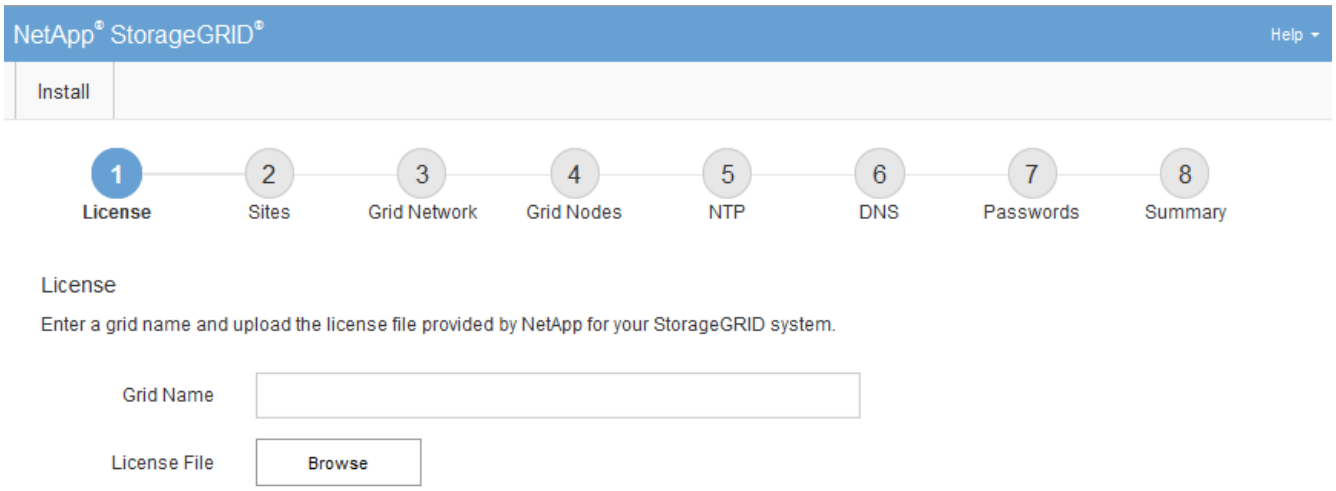
ポート 8443 でグリッドマネージャにアクセスすることもできます。

```
https://primary_admin_node_ip:8443
```

ネットワーク設定に応じて、グリッドネットワーク上または管理ネットワーク上のプライマリ管理ノード IP の IP アドレスを使用できます。

1. StorageGRID システムのインストール * をクリックします。

   StorageGRID グリッドを設定するためのページが表示されます。




**StorageGRID** ライセンス情報の指定

## StorageGRID システムの名前を指定し、ネットアップから提供されたライセンスファイルをアップロードする必要があります。

手順

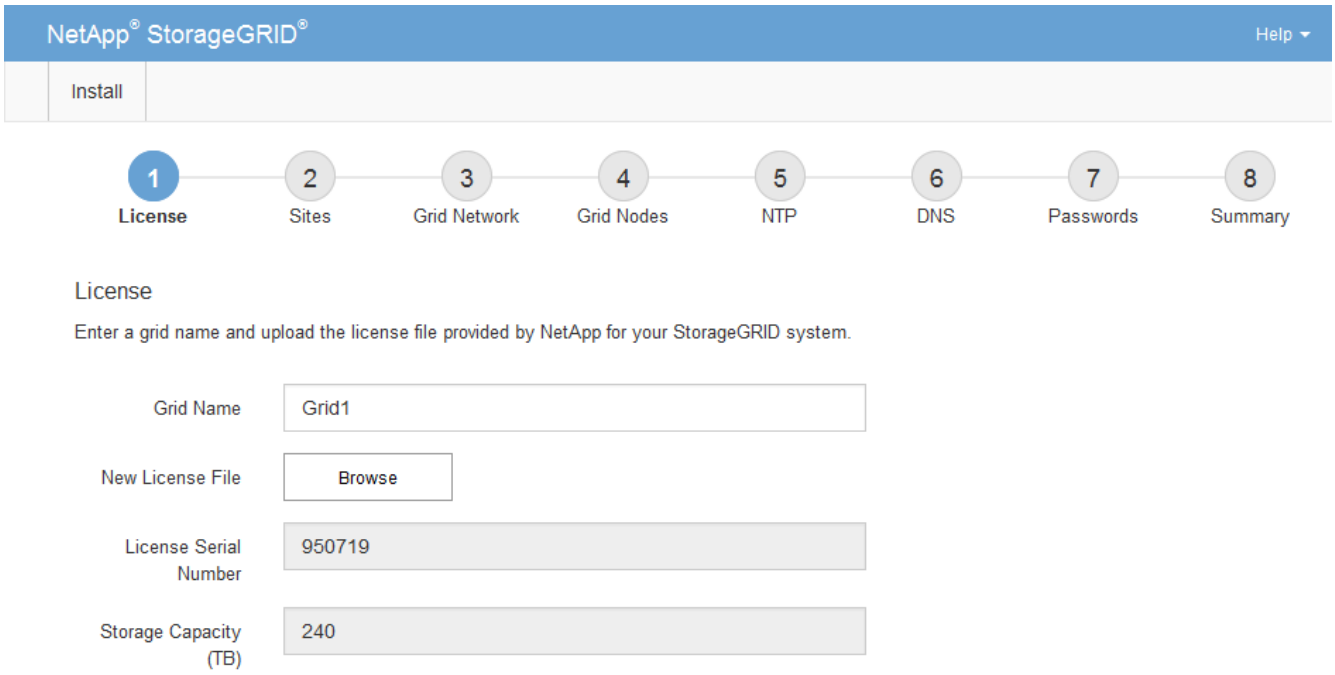
1. [ ライセンス ] ページで、 StorageGRID システムの名前として「 * グリッド名 * 」を入力します。

   インストール後、ノードメニューの上部に名前が表示されます。

2. [* Browse]をクリックして、ネットアップライセンスファイルを探します (`NLFunique_id.txt`)をクリックし、*開く*をクリックします。

   ライセンスファイルが検証され、シリアル番号とライセンスされたストレージ容量が表示されます。

   StorageGRID インストールアーカイブには、製品サポートのない無償ライセンスが含まれています。インストール後に、サポートを提供するライセンスに更新できます。



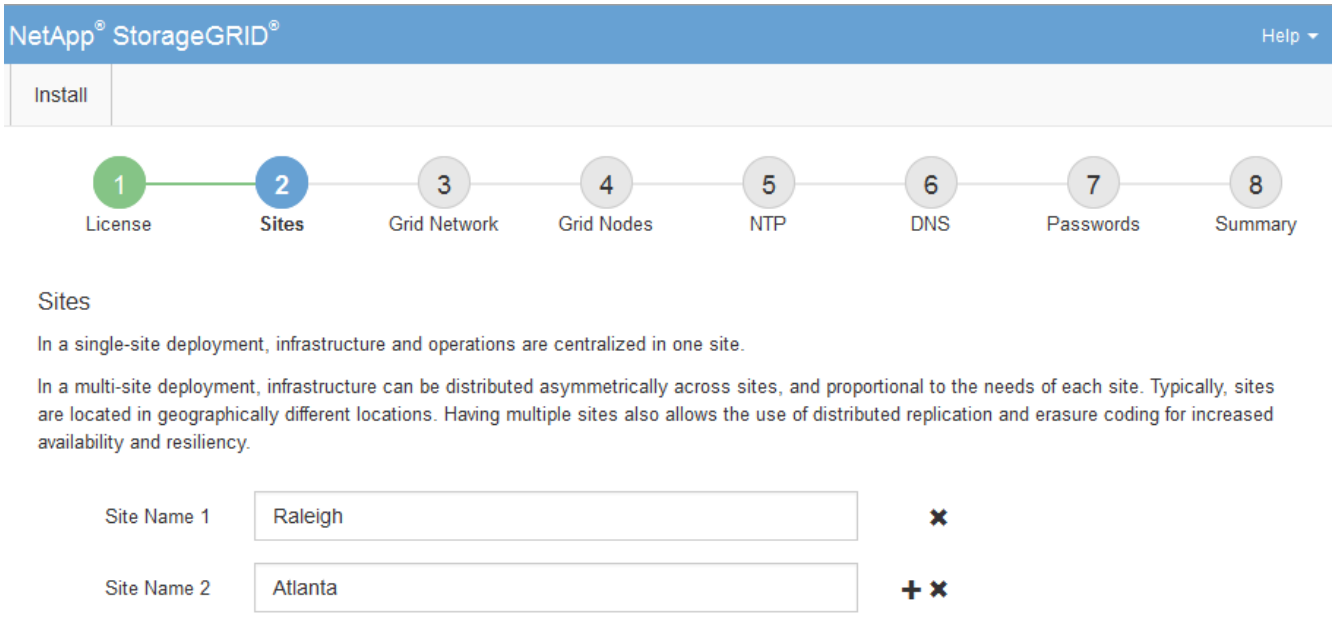

3. 「 * 次へ * 」をクリックします。

サイトの追加

StorageGRID をインストールするときに、サイトを少なくとも 1 つ作成する必要があります。StorageGRID システムの信頼性を高め、ストレージ容量を増やすために、追加のサイトを作成することができます。

1. [ サイト ] ページで、 * サイト名 * を入力します。
2. サイトを追加するには、最後のサイトエントリの横にあるプラス記号をクリックし、新しい * サイト名 * テキストボックスに名前を入力します。

   グリッドトポロジに必要な数のサイトを追加します。サイトは最大 16 個まで追加できます。



3. 「 * 次へ * 」をクリックします。

グリッドネットワークのサブネットの指定

## グリッドネットワークで使用されるサブネットを指定する必要があります。

このタスクについて

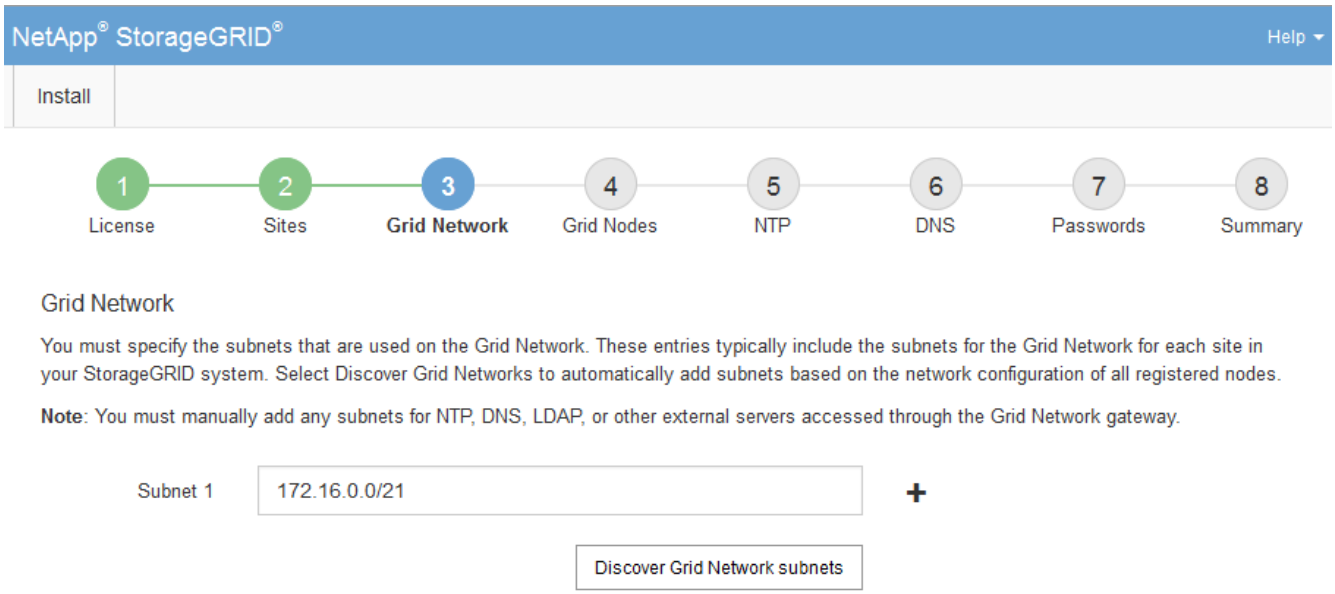
サブネットエントリには、 StorageGRID システム内の各サイトのグリッドネットワークのサブネット、およびグリッドネットワーク経由でアクセスできる必要があるサブネットが含まれます。

グリッドサブネットが複数ある場合は、グリッドネットワークゲートウェイが必要です。指定するすべてのグリッドサブネットが、このゲートウェイ経由でアクセス可能であることが必要です。

手順

1. [* サブネット 1*] テキストボックスで、少なくとも 1 つのグリッドネットワークの CIDR ネットワークアドレスを指定します。
2. 最後のエントリの横にあるプラス記号をクリックして、追加のネットワークエントリを追加します。

   少なくとも 1 つのノードがすでに導入されている場合は、 * グリッドネットワークのサブネットの検出 * をクリックすると、 Grid Manager に登録されているグリッドノードから報告されたサブネットが Grid ネットワークサブネットリストに自動的に追加されます。




3. 「 * 次へ * 」をクリックします。

保留中のグリッドノードを承認します

## 各グリッドノードは、 StorageGRID システムに追加する前に承認する必要があります。

必要なもの

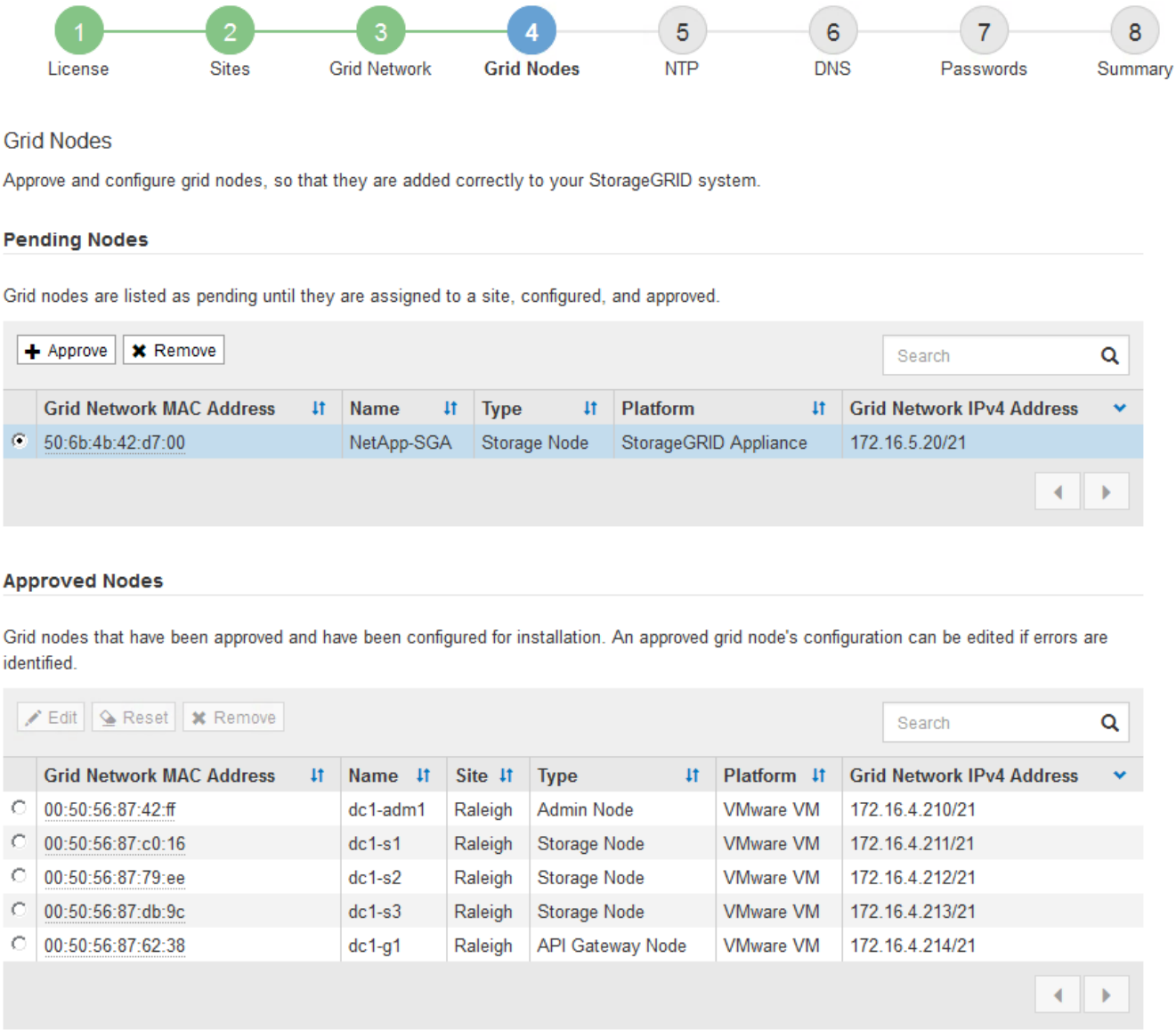
仮想アプライアンスおよびStorageGRID アプライアンスのグリッドノードをすべて導入しておく必要があります。

手順

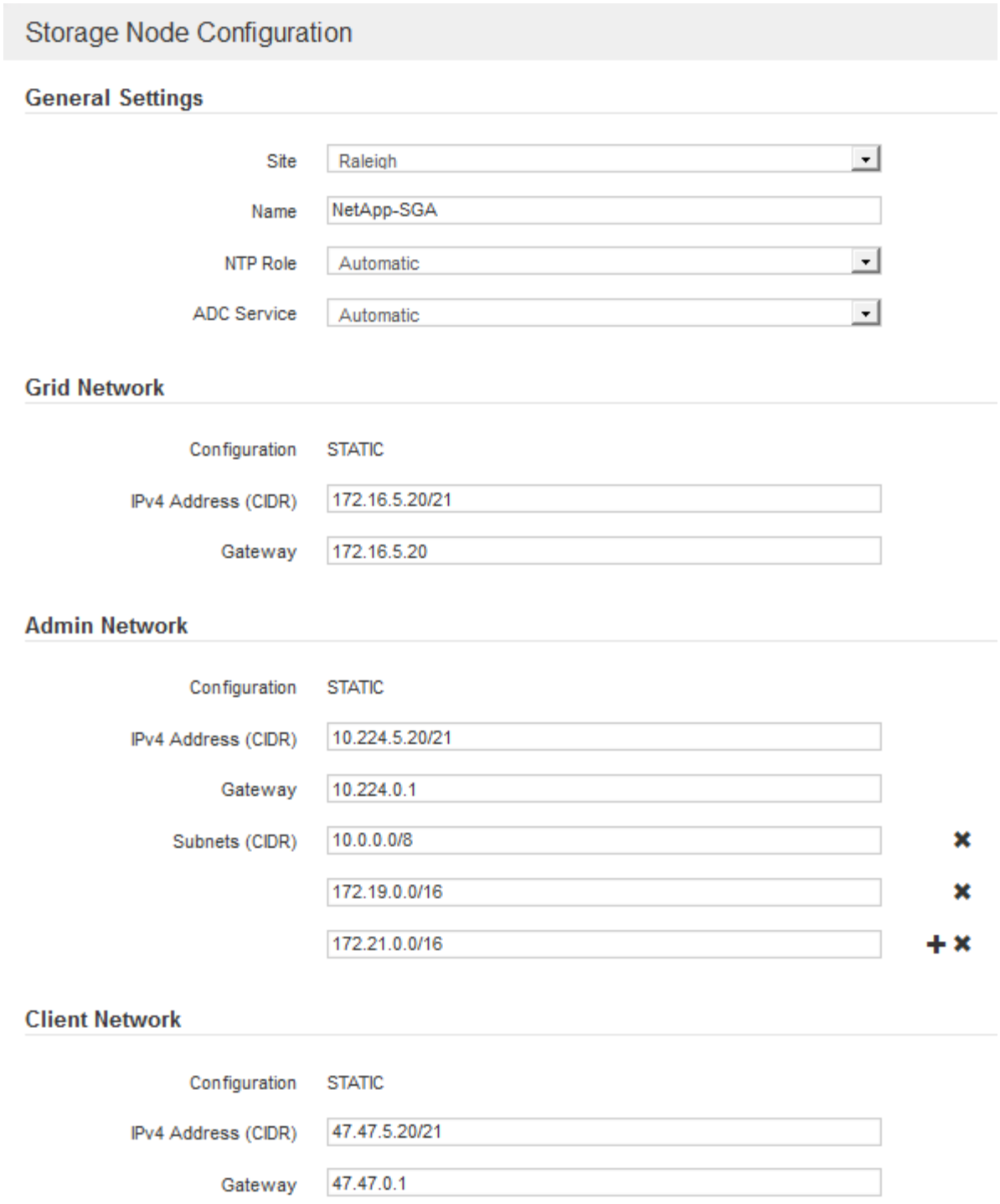
1. Pending 状態のノードのリストを確認し、導入したすべてのグリッドノードが表示されていることを確認します。

   見つからないグリッドノードがある場合は、正常に導入されたことを確認します。

2. 承認する保留中のノードの横にあるラジオボタンを選択します。




3. [ 承認（ Approve ） ] をクリックします
4. [ 一般設定 ] で、必要に応じて次のプロパティの設定を変更します。




◦ * Site * ：このグリッドノードが関連付けられるサイトの名前。

◦ * 名前 * ：ノードに割り当てられる名前。 Grid Manager に表示される名前。デフォルトでは、ノードの設定時に指定した名前が付けられます。インストールプロセスのこのステップでは、必要に応じて名前を変更できます。

インストールの完了後にノードの名前を変更することはできません。

VMware ノードの場合はここで名前を変更できますが、 vSphere で仮想マシンの名前は変更されません。

- * NTP Role * ：グリッドノードのネットワークタイムプロトコル（ NTP ）ロール。オプションは * Automatic * 、 * Primary * 、 * Client * です。「 * 自動」を選択すると、管理ノード、 ADC サービスを採用するストレージノード、ゲートウェイノード、および静的な IP アドレスでないグリッドノードにプライマリロールが割り当てられます。他のすべてのグリッドノードにはクライアントロールが割り当てられます。

  > 各サイトの少なくとも 2 つのノードが、少なくとも 4 つの外部 NTP ソースにアクセスできることを確認します。NTP ソースにアクセスできるノードがサイトに 1 つしかないと、そのノードがダウンした場合にタイミングの問題が生じます。また、各サイトで 2 つのノードをプライマリ NTP ソースとして指定することにより、サイトがグリッドの他の部分から分離されても、正確なタイミングが保証されます。

- * ADC service * （ストレージノードのみ）：「 * Automatic * 」を選択して、ノードに Administrative Domain Controller （ ADC ）サービスが必要かどうかをシステムに通知します。ADC サービスは、グリッドサービスの場所と可用性を追跡します。各サイトで少なくとも 3 つのストレージノードに ADC サービスが含まれている必要があります。導入後のノードに ADC サービスを追加することはできません。

5. グリッドネットワークで、必要に応じて次のプロパティの設定を変更します。

   - * IPv4 Address （ CIDR ） * ：グリッドネットワークインターフェイス（コンテナ内の eth0 ）の CIDR ネットワークアドレス。例： 192.168.1.234/21
   - * ゲートウェイ * ：グリッドネットワークゲートウェイ。例： 192.168.0.1

     グリッドサブネットが複数ある場合は、ゲートウェイが必要です。

   > グリッドネットワーク設定で DHCP を選択した場合は、ここで値を変更すると、新しい値がノード上の静的アドレスとして設定されます。設定された IP アドレスが DHCP アドレスプールにないことを確認する必要があります。

6. グリッドノードの管理ネットワークを設定する場合は、必要に応じて管理ネットワークセクションで設定を追加または更新します。

   サブネット（ CIDR ） * テキストボックスに、このインターフェイスから発信されるルートの宛先サブネットを入力します。管理サブネットが複数ある場合は、管理ゲートウェイが必要です。

   > 管理ネットワーク設定で DHCP を選択した場合は、ここで値を変更すると、新しい値がノード上の静的アドレスとして設定されます。設定された IP アドレスが DHCP アドレスプールにないことを確認する必要があります。

   - アプライアンス： StorageGRID アプライアンスでは、 StorageGRID アプライアンスインストーラを使用した初回インストール時に管理ネットワークが設定されなかった場合、このグリッドマネージャのダイアログボックスで管理ネットワークを設定することはできません。代わりに、次の手順を実行する必要があります。

     a. アプライアンスをリブートします。アプライアンスインストーラで、 * Advanced * > * Reboot * を選択します。

        リブートには数分かかることがあります。

     b. [Configure Networking*] > [**Link Configuration**] を選択し、適切なネットワークを有効にします。

c. [Configure Networking*]>[**IP Configuration**] を選択し、有効なネットワークを設定します。

d. ホームページに戻り、「インストールの開始」をクリックします。

e. Grid Manager で、ノードが承認済みノード（ Approved Nodes ）テーブルにリストされている場合は、ノードをリセットします。

f. Pending Nodes テーブルからノードを削除します。

g. ノードが Pending Nodes リストに再表示されるまで待ちます。

h. 適切なネットワークを設定できることを確認します。IP Configuration ページで指定した情報があらかじめ入力されている必要があります。

追加情報 の場合は、使用しているアプライアンスモデルのインストールとメンテナンスの手順を参照してください。

7. グリッドノードのクライアントネットワークを設定する場合は、必要に応じてクライアントネットワークセクションで設定を追加または更新します。クライアントネットワークを設定する場合はゲートウェイが必要になります。これは、インストール後にノードのデフォルトゲートウェイになります。

クライアントネットワーク設定で DHCP を選択した場合は、ここで値を変更すると、新しい値がノード上の静的アドレスとして設定されます。設定された IP アドレスが DHCP アドレスプールにないことを確認する必要があります。

◦ アプライアンス： StorageGRID アプライアンスでは、 StorageGRID アプライアンスインストーラを使用した初回インストール時にクライアントネットワークが設定されなかった場合、このグリッドマネージャのダイアログボックスでクライアントネットワークを設定することはできません。代わりに、次の手順を実行する必要があります。

a. アプライアンスをリブートします。アプライアンスインストーラで、 * Advanced * > * Reboot * を選択します。

リブートには数分かかることがあります。

b. [Configure Networking*] > [**Link Configuration**] を選択し、適切なネットワークを有効にします。

c. [Configure Networking*]>[**IP Configuration**] を選択し、有効なネットワークを設定します。

d. ホームページに戻り、「インストールの開始」をクリックします。

e. Grid Manager で、ノードが承認済みノード（ Approved Nodes ）テーブルにリストされている場合は、ノードをリセットします。

f. Pending Nodes テーブルからノードを削除します。

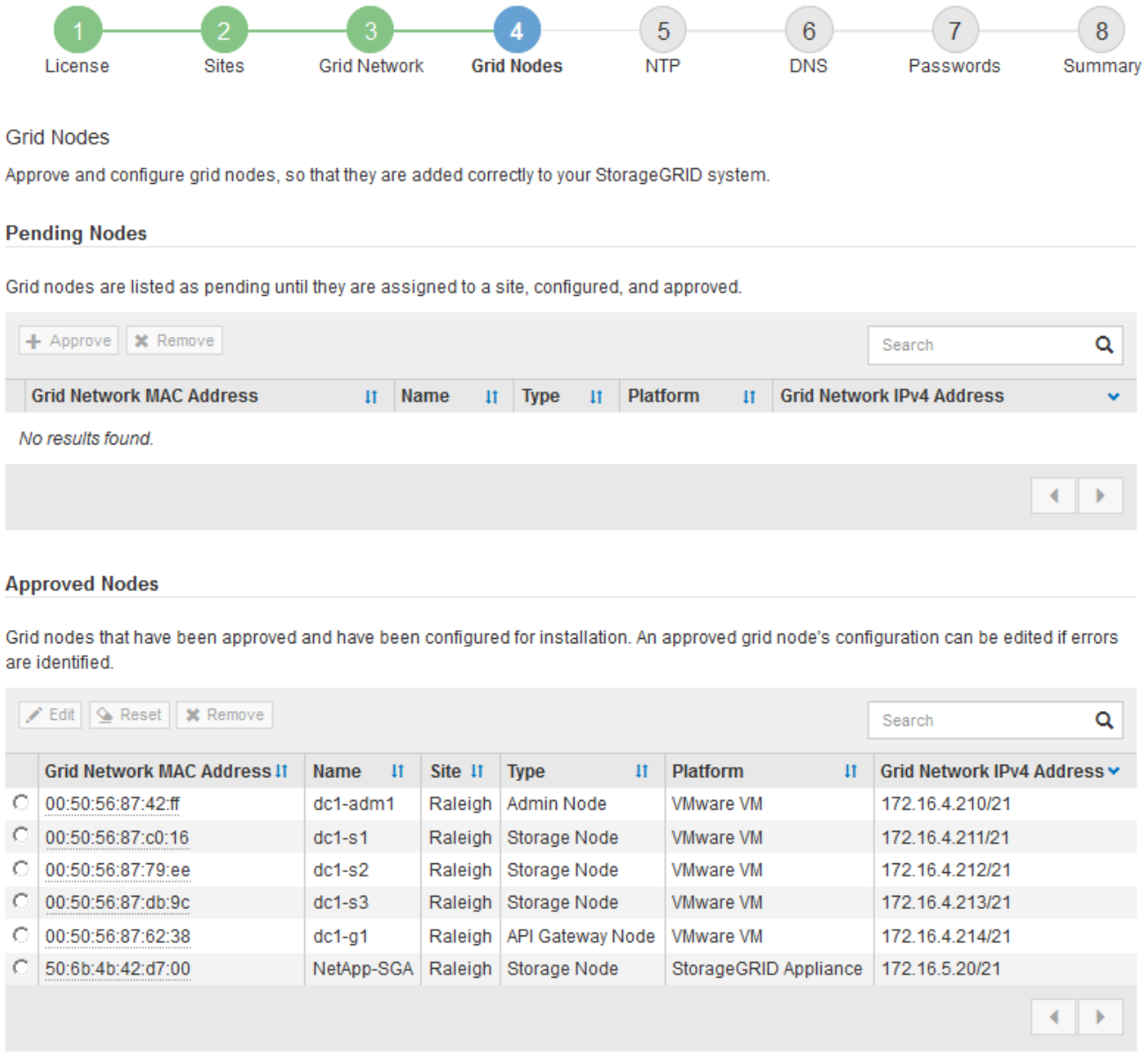
g. ノードが Pending Nodes リストに再表示されるまで待ちます。

h. 適切なネットワークを設定できることを確認します。IP Configuration ページで指定した情報があらかじめ入力されている必要があります。

追加情報 の場合は、使用しているアプライアンスのインストールとメンテナンスの手順を参照してください。

8. [ 保存（ Save ） ] をクリックします。

グリッドノードエントリが [ 承認済みノード（ Approved Nodes ） ] リストに移動します。




9. 承認する保留中のグリッドノードごとに、上記の手順を繰り返します。

   グリッドに必要なすべてのノードを承認する必要があります。ただし、サマリページで * インストール * をクリックする前に、いつでもこのページに戻ることができます。承認済みグリッドノードのプロパティを変更するには、ラジオボタンを選択し、 * 編集 * をクリックします。

10. グリッドノードの承認が完了したら、 * 次へ * をクリックします。

### Network Time Protocolサーバ情報の指定

別々のサーバで実行された処理を常に同期された状態にするには、 StorageGRID システムの NTP 設定情報を指定する必要があります。

このタスクについて

NTP サーバの IPv4 アドレスを指定する必要があります。

外部 NTP サーバを指定する必要があります。指定した NTP サーバで NTP プロトコルが使用されている必要

があります。

時間のずれに伴う問題を防ぐには、 Stratum 3 またはそれより上位の NTP サーバ参照を 4 つ指定する必要があります。

本番レベルの StorageGRID インストール環境で外部 NTP ソースを指定する場合は、 Windows Server 2016 より前のバージョンの Windows で Windows Time （ W32Time ）サービスを使用しないでください。以前のバージョンの Windows のタイムサービスは精度が十分でないため、 StorageGRID などの高精度環境での使用は Microsoft でサポートされていません。

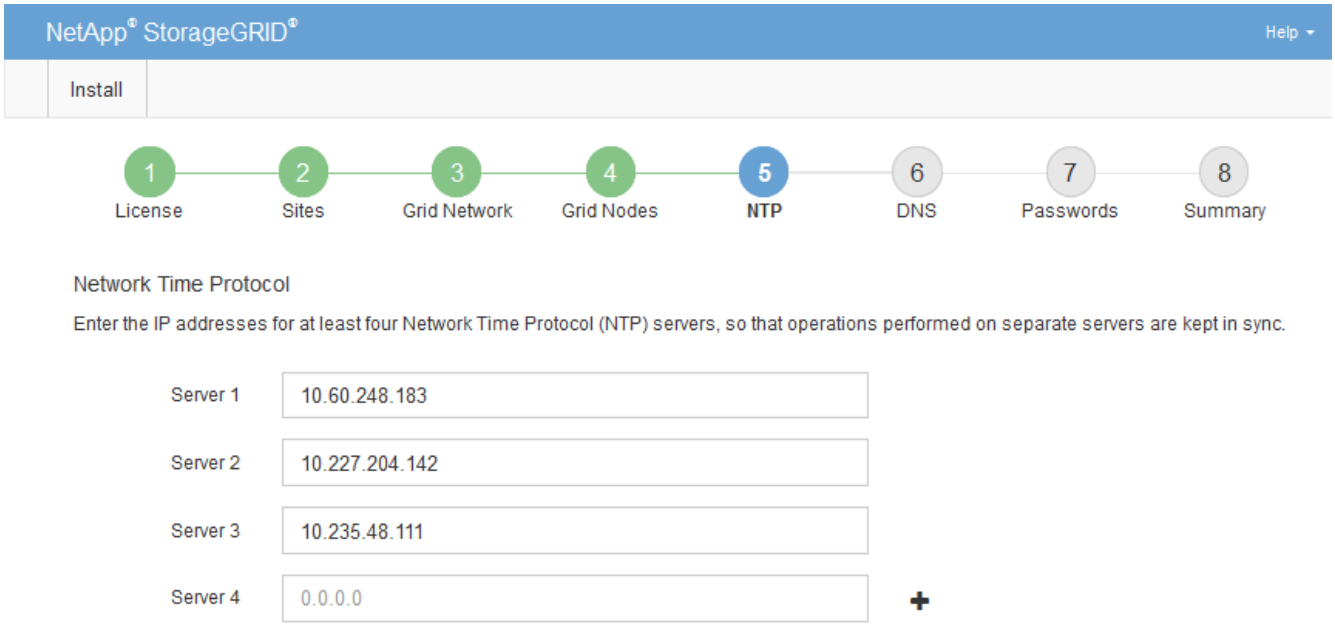
"高精度環境用に Windows タイムサービスを構成するためのサポート境界"

外部 NTP サーバは、以前にプライマリ NTP ロールを割り当てていたノードによって使用されます。

各サイトの少なくとも 2 つのノードが、少なくとも 4 つの外部 NTP ソースにアクセスできることを確認します。NTP ソースにアクセスできるノードがサイトに 1 つしかないと、そのノードがダウンした場合にタイミングの問題が生じます。また、各サイトで 2 つのノードをプライマリ NTP ソースとして指定することにより、サイトがグリッドの他の部分から分離されても、正確なタイミングが保証されます。

手順

1. [* サーバー 1 * から * サーバー 4 * ] テキストボックスに、少なくとも 4 つの NTP サーバーの IPv4 アドレスを指定します。
2. 必要に応じて、最後のエントリの横にあるプラス記号を選択して、サーバエントリを追加します。




3. 「 * 次へ * 」を選択します。

関連情報

"ネットワークガイドライン"

**Domain Name System**サーバ情報の指定

## IP アドレスの代わりにホスト名を使用して外部サーバにアクセスできるようにするには、 StorageGRID システムの DNS 情報を指定する必要があります。

このタスクについて

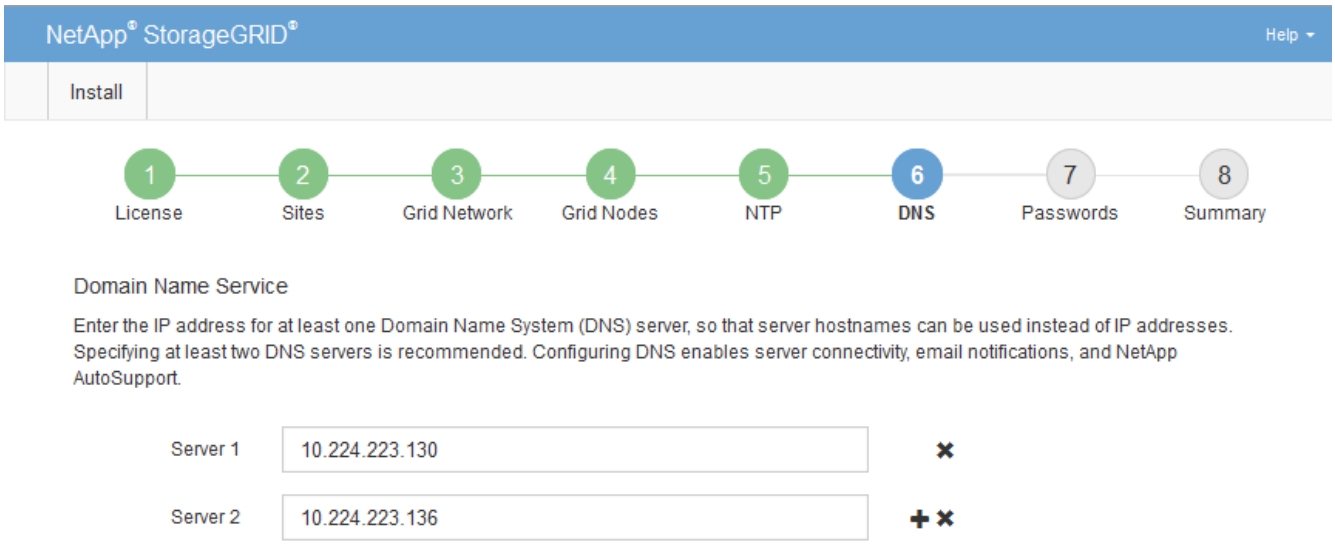
DNS サーバ情報を指定すると、 E メール通知や AutoSupport に、 IP アドレスではなく Fully Qualified Domain Name （ FQDN ；完全修飾ドメイン名）ホスト名を使用できます。DNS サーバは少なくとも 2 つ指定することを推奨します。

> DNS サーバの IPv4 アドレスは 2~6 個指定します。ネットワーク分離が発生した場合に各サイトがローカルにアクセスできる DNS サーバを選択する必要があります。これにより、分離されたサイトは引き続き DNS サービスにアクセスできます。グリッド全体の DNS サーバリストを設定したあとに、ノードごとに DNS サーバリストをカスタマイズできます。詳細については、リカバリおよびメンテナンスの手順にある DNS 設定の変更に関する情報を参照してください。

DNS サーバ情報を省略したり誤って設定したりすると、各グリッドノードの SSM サービスで DNST アラームがトリガーされます。このアラームは、 DNS が正しく設定され、新しいサーバ情報がすべてのグリッドノードに配信された時点で解除されます。

手順

1. 「 * サーバー 1 * 」テキストボックスで、少なくとも 1 つの DNS サーバーの IPv4 アドレスを指定します。
2. 必要に応じて、最後のエントリの横にあるプラス記号を選択して、サーバエントリを追加します。




少なくとも 2 つの DNS サーバを指定することを推奨します。DNS サーバは 6 つまで指定できます。

3. 「 * 次へ * 」を選択します。

**StorageGRID** システムのパスワードの指定

## StorageGRID システムのインストールの一環として、システムの保護とメンテナンス作業に使用するパスワードを入力する必要があります。

このタスクについて

Install Passwords ページを使用して、プロビジョニングパスフレーズとグリッド管理 root ユーザのパスワードを指定します。

- プロビジョニングパスフレーズは暗号化キーとして使用され、 StorageGRID システムでは格納されません。
- リカバリパッケージのダウンロードなど、インストール、拡張、メンテナンスの手順用のプロビジョニングパスフレーズが必要です。そのため、プロビジョニングパスフレーズは安全な場所に保存しておくことが重要です。
- 現在のプロビジョニングパスフレーズがある場合は、 Grid Manager からプロビジョニングパスフレーズを変更できます。
- Grid 管理 root ユーザのパスワードは Grid Manager を使用して変更できる。
- ランダムに生成されたコマンドラインコンソールとSSHパスワードは、リカバリパッケージのPasswords.txtファイルに保存されます。

手順

1. 「 * プロビジョニングパスフレーズ * 」に、 StorageGRID システムのグリッドトポロジを変更するために必要なプロビジョニングパスフレーズを入力します。

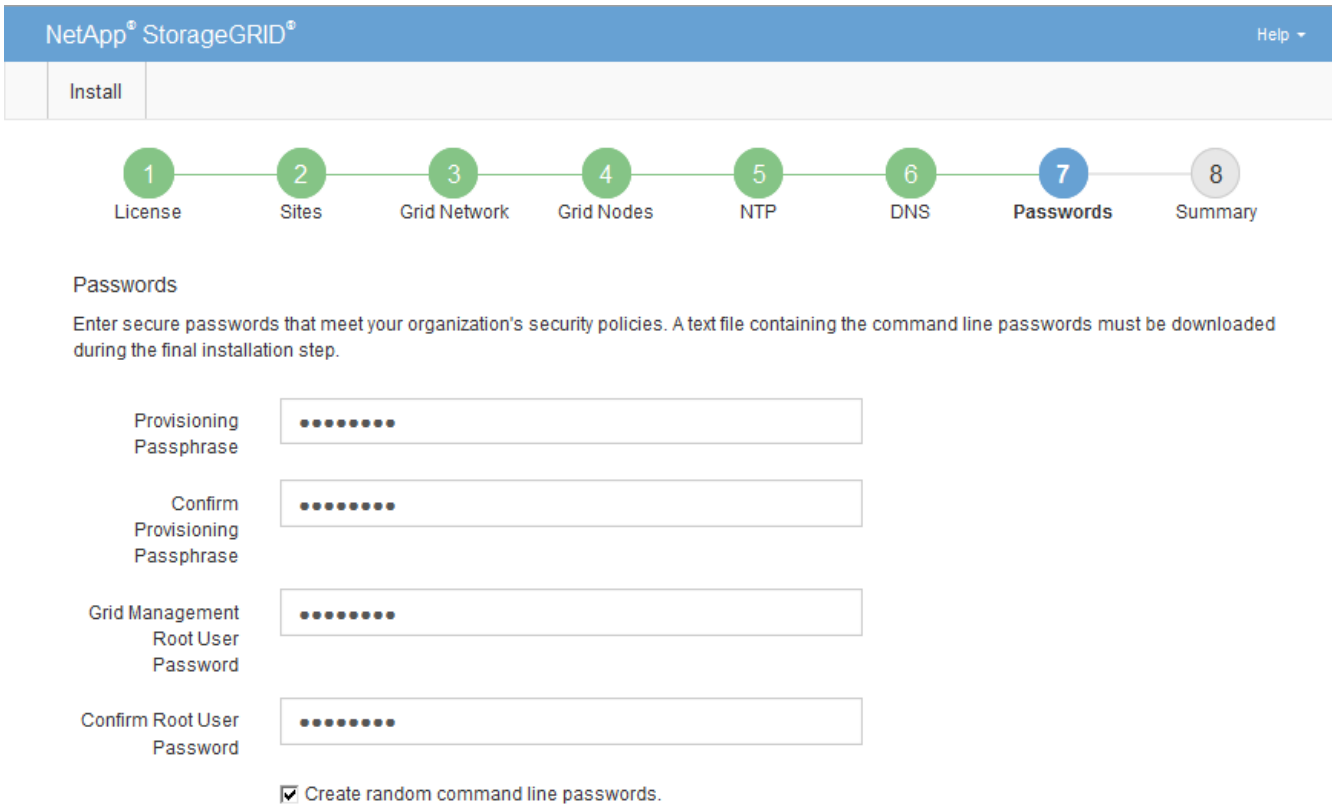
   プロビジョニングパスフレーズは安全な場所に保存してください。

   > インストールの完了後にプロビジョニングパスフレーズを変更する場合は、 Grid Manager を使用してください。[構成（Configuration ）**]>[***アクセス制御（* Access Control ）**]>[** Gridパスワード*（* Grid

2. [Confirm Provisioning Passphrase* （プロビジョニングパスフレーズの確認） ] にプロビジョニングパスフレーズを再入力して確定します。
3. * Grid Management Root User Password * に、 Grid Manager に「 root 」ユーザとしてアクセスするために使用するパスワードを入力します。

   パスワードは安全な場所に保管してください。

4. Confirm Root User Password * で、 Grid Manager のパスワードを再入力して確認します。




5. コンセプトの実証やデモを目的としてグリッドをインストールする場合は、必要に応じて、 * ランダムなコマンドラインパスワードの作成 * チェックボックスの選択を解除します。

   本番環境では、セキュリティ上の理由から常にランダムパスワードを使用する必要があります。デフォルトのパスワードを使用してコマンドラインから "root" または "admin" アカウントを使用してグリッドノードにアクセスする場合は、デモ用グリッドの * ランダムなコマンドラインパスワードの作成 * のみを選択解除します。

   リカバリパッケージファイルをダウンロードするように求められます (`sgws-recovery-package-id-revision.zip`)サマリページで*Install*をクリックした後。インストールを完了するには、このファイルをダウンロードする必要があります。システムへのアクセスに必要なパスワードは、リカバリパッケージファイル内の Passwords.txt ファイルに保存されています。

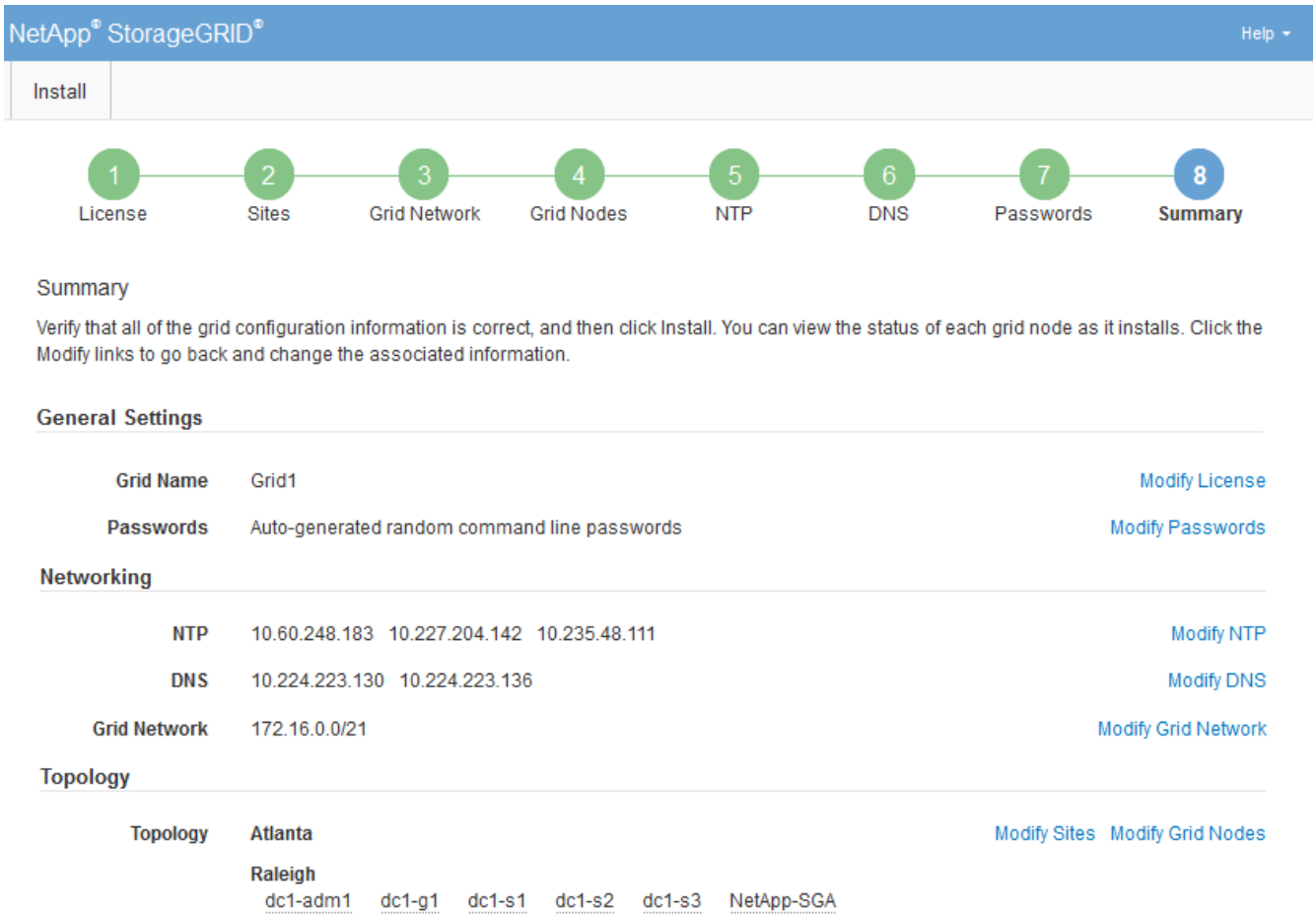
6. 「 * 次へ * 」をクリックします。

設定を確認し、インストールを完了します

インストールを正常に完了するために、入力した設定情報をよく確認する必要があります。

手順

1. 「 * 概要 * 」ページを表示します。




2. グリッドの設定情報がすべて正しいことを確認します。Summary （サマリ）ページの Modify （変更）リンクを使用して、戻ってエラーを修正します。
3. 「 * Install * 」をクリックします。

> クライアントネットワークを使用するようにノードが設定されている場合、 * Install * をクリックすると、そのノードのデフォルトゲートウェイがグリッドネットワークからクライアントネットワークに切り替わります。接続を失った場合は、アクセス可能なサブネット経由でプライマリ管理ノードにアクセスしていることを確認する必要があります。を参照してください "ネットワークのガイドライン" を参照してください。

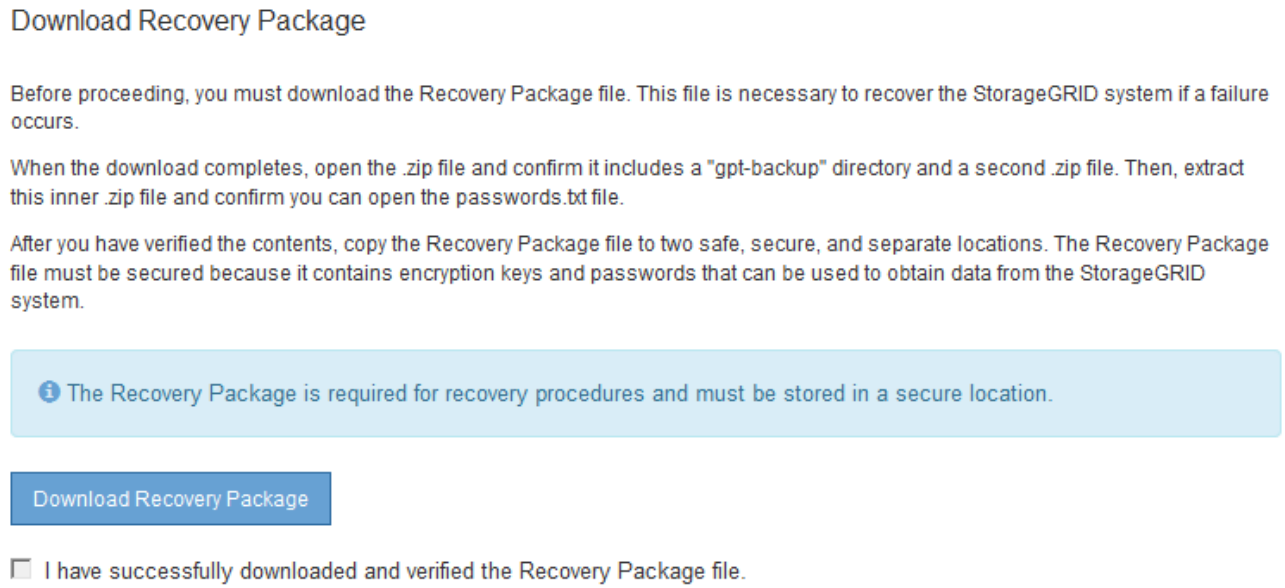
4. [ リカバリパッケージのダウンロード ] をクリックします。

   グリッドトポロジを定義するポイントまでインストールが進むと、リカバリパッケージファイルをダウンロードするように求められます (`.zip`) をクリックし、このファイルの内容に正常にアクセスできることを確認します。リカバリパッケージファイルのダウンロードが必要となるのは、グリッドノードで障害が発生した場合に StorageGRID システムをリカバリできるようにするためです。インストールはバックグラウンドで続行されますが、このファイルをダウンロードして検証するまでは、インストールを完了して StorageGRID システムにアクセスすることができません。

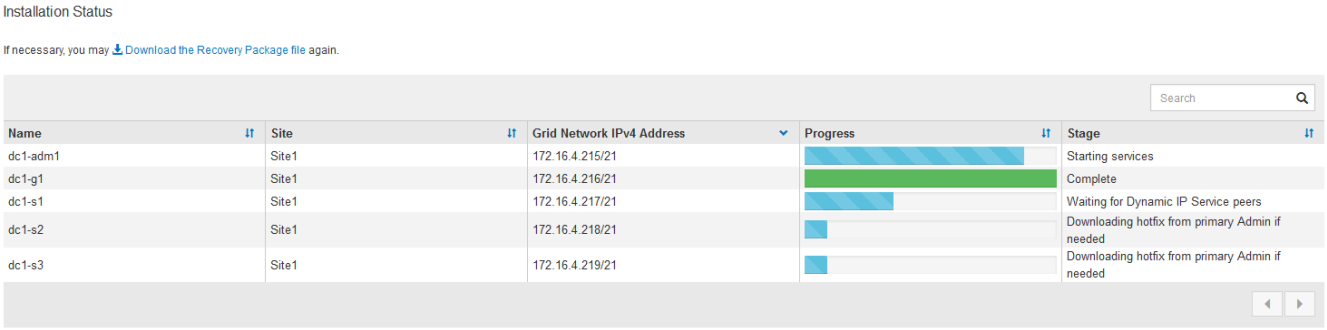
5. の内容を展開できることを確認します `.zip` ファイルを作成し、安全で安全な2つの場所に保存します。

> リカバリパッケージファイルには StorageGRID システムからデータを取得するための暗号キーとパスワードが含まれているため、安全に保管する必要があります。

6. [I have successfully downloaded and verified the Recovery Package file*] チェックボックスをオンにし、 [ 次へ ] をクリックします。




インストールがまだ進行中の場合は、ステータスページが表示されます。このページには、グリッドノードごとのインストールの進捗状況が表示されます。




すべてのグリッドノードが完了ステージに到達すると、 Grid Manager のサインインページが表示されます。

7. 「 root 」ユーザおよびインストール時に指定したパスワードを使用して Grid Manager にサインインします。

インストール後のガイドライン

## グリッドノードの導入と設定が完了したら、 DHCP アドレスおよびネットワーク設定の変更について、次のガイドラインに従ってください。

- DHCP を使用して IP アドレスを割り当てた場合は、使用しているネットワーク上の各 IP アドレスに対して DHCP 予約を設定します。

  DHCP は導入フェーズでのみ設定できます。設定時に DHCP を設定することはできません。

IP アドレスが変わるとノードがリブートします。 DHCP アドレスの変更が同時に複数のノードに影響を及ぼす場合、原因 が停止する可能性があります。

- グリッドノードの IP アドレス、サブネットマスク、およびデフォルトゲートウェイを変更する場合は、IP 変更手順を使用する必要があります。リカバリとメンテナンスの手順のIPアドレスの設定に関する情報を参照してください。
- ルーティングやゲートウェイの変更など、ネットワーク設定を変更すると、プライマリ管理ノードおよびその他のグリッドノードへのクライアント接続が失われる可能性があります。ネットワークの変更内容によっては、接続の再確立が必要になる場合があります。

## インストールの自動化

### StorageGRID ホストサービスのインストール、およびグリッドノードの設定を自動化することができます。

このタスクについて

導入を自動化すると、次のいずれかの場合に役立ちます。

- 物理ホストや仮想ホストの導入と設定に Ansible 、 Puppet 、 Chef などの標準のオーケストレーションフレームワークをすでに使用している場合。
- 複数の StorageGRID インスタンスを導入する場合。
- 大規模で複雑な StorageGRID インスタンスを導入する場合。

StorageGRID ホストサービスはパッケージでインストールされ、構成ファイルで制御されます。構成ファイルは、手動インストール時に対話形式で作成できるほか、あらかじめ用意して（またはプログラム化して）標準のオーケストレーションフレームワークを使用した自動インストールに使用できます。StorageGRID には、 StorageGRID アプライアンスと StorageGRID システム全体（「グリッド」）の設定を自動化するためのオプションの Python スクリプトが用意されています。これらのスクリプトは直接使用することも、StorageGRID インストール REST API の使用方法を調べることもできます。グリッドの導入ツールや設定ツールを独自に開発する際の参考としても使用できます。

**StorageGRID** ホストサービスのインストールと設定を自動化する

### StorageGRID ホストサービスのインストールは、 Ansible 、 Puppet 、 Chef 、 Fabric 、 SaltStack などの標準のオーケストレーションフレームワークを使用して自動化できます。

StorageGRID ホストサービスは、 DEB 形式でパッケージ化されており、あらかじめ構成ファイルを用意して（またはプログラム化して）おくことで自動インストールが可能です。すでに Ubuntu または Debian のインストールおよび設定に標準的なオーケストレーションフレームワークを使用している場合は、プレイブックやレシピに StorageGRID を追加する方が簡単です。

次のタスクを自動化できます。

1. Linux をインストールしています
2. Linux の設定
3. StorageGRID の要件を満たすホストネットワークインターフェイスを設定する

4. StorageGRID の要件を満たすホストストレージを構成する
5. Docker をインストールする
6. StorageGRID ホストサービスをインストールしています
7. でのStorageGRID ノード構成ファイルの作成 `/etc/storagegrid/nodes`
8. StorageGRID ノード構成ファイルを検証しています
9. StorageGRID ホストサービスを開始しています

サンプルの **Ansible** のロールとプレイブック

サンプルの Ansible のロールとプレイブックは、 /extras フォルダに含まれるインストールアーカイブに含まれています。Ansibleプレイブックは、の仕組みを示しています `storagegrid` 役割ホストを準備し、ターゲットサーバーにStorageGRID をインストールします。必要に応じて、ロールまたはプレイブックをカスタマイズできます。

**StorageGRID** の設定の自動化

## グリッドノードを導入したら、 StorageGRID システムの設定を自動化できます。

必要なもの

- インストールアーカイブにある次のファイルの場所を確認しておきます。

| ファイル名 | 説明 |
| --- | --- |
| `configure-storagegrid.py` | 設定を自動化するための Python スクリプト |
| `configure-storagegrid.sample.json` | スクリプトで使用するサンプル構成ファイル |
| `configure-storagegrid.blank.json` | スクリプトで使用する空の構成ファイルです |

- を作成しておきます `configure-storagegrid.json` 構成ファイルこのファイルを作成するには、サンプル構成ファイルを変更します (`configure-storagegrid.sample.json`)または空の構成ファイル (`configure-storagegrid.blank.json`）。

このタスクについて

を使用できます `configure-storagegrid.py` Pythonスクリプトおよび `configure-storagegrid.json` StorageGRID システムの設定を自動化するための構成ファイル。

また、 Grid Manager またはインストール API を使用してシステムを設定することもできます。

手順

1. Python スクリプトを実行するために使用する Linux マシンにログインします。
2. インストールアーカイブを展開したディレクトリに移動します。

   例：

```
cd StorageGRID-Webscale-version/platform
```

ここで、 `platform` はです `debs`、 `rpms`または `vsphere`。

3. Python スクリプトを実行し、作成した構成ファイルを使用します。

例：

```
./configure-storagegrid.py ./configure-storagegrid.json --start-install
```

結果

リカバリパッケージ `.zip` 設定プロセスでファイルが生成され、インストールと設定を実行するディレクトリにダウンロードされます。グリッドノードで障害が発生した場合に StorageGRID システムをリカバリできるようにするために、リカバリパッケージファイルをバックアップする必要があります。たとえば、バックアップされたセキュアなネットワーク上の場所や、安全なクラウドストレージ上の場所にコピーします。

リカバリパッケージファイルには StorageGRID システムからデータを取得するための暗号キーとパスワードが含まれているため、安全に保管する必要があります。

ランダムパスワードを生成するように指定した場合は、を展開する必要があります `Passwords.txt` ファイルを開き、StorageGRID システムへのアクセスに必要なパスワードを探します。

```
######################################################################
##### The StorageGRID "recovery package" has been downloaded as: #####
#####           ./sgws-recovery-package-994078-rev1.zip          #####
#####   Safeguard this file as it will be needed in case of a    #####
#####                 StorageGRID node recovery.                 #####
######################################################################
```

StorageGRID システムがインストールおよび設定されると、確認メッセージが表示されます。

```
StorageGRID has been configured and installed.
```

関連情報

"グリッドの設定とインストールの完了"

"インストール REST API の概要"

## インストール **REST API** の概要

StorageGRID には、インストールタスクを実行するための StorageGRID インストール API が用意されています。

API のドキュメントは、 Swagger オープンソース API プラットフォームで提供されています。Swagger では、ユーザインターフェイスを使用してパラメータやオプションを変更した場合の API の動作を確認しながら、 API の開発を進めることができます。このドキュメントは、標準的な Web テクノロジと JavaScript Object Notation （ JSON ）データ形式について十分理解していることを前提としています。

API Docs Web ページを使用して実行する API 処理はすべてその場で実行されます。設定データやその他のデータを誤って作成、更新、または削除しないように注意してください。

各 REST API コマンドは、 API の URL 、 HTTP アクション、必須またはオプションの URL パラメータ、および想定される API 応答で構成されます。

**StorageGRID** インストール **API**

StorageGRID インストール API は、 StorageGRID システムを最初に設定するとき、およびプライマリ管理ノードのリカバリを実行する必要がある場合にのみ使用できます。インストール API には、 Grid Manager から HTTPS 経由でアクセスできます。

API のドキュメントにアクセスするには、プライマリ管理ノードのインストール用 Web ページに移動し、メニューバーから * Help * > * API Documentation * を選択します。

StorageGRID インストール API には次のセクションがあります。

- *config *-- API の製品リリースとバージョンに関連する操作。製品リリースバージョンおよびそのリリースでサポートされる API のメジャーバージョンを一覧表示できます。
- * grid * — グリッドレベルの設定操作。グリッドの詳細、グリッドネットワークのサブネット、グリッドパスワード、 NTP および DNS サーバの IP アドレスなど、グリッド設定を取得および更新できます。
- *nodes * — ノードレベルの設定操作。グリッドノードのリストを取得できるほか、グリッドノードの削除、設定、表示、およびグリッドノードの設定のリセットを行うことができます。
- *provision * — プロビジョニング操作。プロビジョニング処理を開始し、プロビジョニング処理のステータスを表示できます。
- * recovery * - プライマリ管理ノードのリカバリ処理。情報のリセット、リカバリパッケージのアップロード、リカバリの開始、およびリカバリ処理のステータスの表示を行うことができます。
- * recovery-package * — リカバリパッケージをダウンロードする処理。
- *sites * — サイトレベルの設定操作。サイトを作成、表示、削除、および変更できます。

関連情報

"インストールの自動化"

## 次の手順

## インストールが完了したら、統合と設定のための一連の手順を実行する必要があります。手順には必須のものとオプションのものがあります。

必要な作業

- StorageGRID システムにオブジェクトを格納するために使用されるクライアントプロトコル（ Swift または S3 ）ごとに、テナントアカウントを作成します。

- グループとユーザアカウントを設定してシステムアクセスを制御します。管理者グループおよびユーザをインポートできるように、必要に応じて、フェデレーテッドアイデンティティソース（ Active Directory や OpenLDAP など）を設定できます。または、ローカルグループやユーザを作成することもできます。
- StorageGRID システムにオブジェクトをアップロードするために使用する S3 または Swift API クライアントアプリケーションを統合し、テストします。
- 準備ができたら、オブジェクトデータの保護に使用する情報ライフサイクル管理（ ILM ）ルールと ILM ポリシーを設定します。

> StorageGRID をインストールすると、デフォルトの ILM ポリシーである Baseline 2 Copies Policy がアクティブになります。このポリシーには組み込みの ILM ルール（ Make 2 Copies ）が含まれており、他のポリシーがアクティブ化されていない場合に適用されます。

- インストール環境にアプライアンスストレージノードが含まれている場合は、 SANtricity ソフトウェアを使用して次の作業を実行します。
  - 各 StorageGRID アプライアンスに接続します。
  - AutoSupport データの受信を確認します。
- StorageGRID システムにアーカイブノードが含まれている場合は、アーカイブノードからターゲットの外部アーカイブストレージシステムへの接続を設定します。

> アーカイブノードが Tivoli Storage Manager を外部アーカイブストレージシステムとして使用する場合は、 Tivoli Storage Manager を設定する必要もあります。

- StorageGRID システムのセキュリティ設定ガイドラインに従ってセキュリティリスクを排除します。
- システムアラートの E メール通知を設定します。

任意のタスク

- （レガシー）アラームシステムから通知を受信するには、アラーム用のメーリングリストおよび E メール通知を設定します。
- 導入を計画し、リカバリパッケージを生成したあとにグリッドノードの IP アドレスが変わった場合は、それらの IP アドレスを更新します。リカバリとメンテナンスの手順の IP アドレスの変更に関する情報を参照してください。
- 必要に応じて、ストレージ暗号化を設定します。
- 必要に応じて、ストレージの圧縮を設定し、格納されているオブジェクトのサイズを削減します。
- 監査クライアントアクセスを設定します。NFS または CIFS ファイル共有を通じて、監査を目的としたシステムへのアクセスを設定できます。StorageGRID の管理手順を参照してください。

> CIFS / Samba を使用した監査エクスポートは廃止されており、 StorageGRID の今後のリリースで削除される予定です。

## インストールに関する問題のトラブルシューティング

StorageGRID システムのインストール中に問題が発生した場合は、インストールログファイルにアクセスできます。テクニカルサポートが問題を解決するためにインストール

ログファイルを使用することもあります。

次のインストールログファイルは、各ノードを実行しているコンテナからアクセスできます。

- `/var/local/log/install.log` （すべてのグリッドノードに存在）
- `/var/local/log/gdu-server.log` （プライマリ管理ノードに存在）

次のインストールログファイルは、ホストからアクセスできます。

- `/var/log/storagegrid/daemon.log`
- `/var/log/storagegrid/nodes/<node-name>.log`

ログファイルへのアクセス方法については、 StorageGRID の監視とトラブルシューティングの手順を参照してください。アプライアンスの設置に関する問題のトラブルシューティングについては、使用しているアプライアンスの設置とメンテナンスの手順を参照してください。その他のサポートが必要な場合は、テクニカルサポートにお問い合わせください。

関連情報

"トラブルシューティングを監視します"

"SG100 SG1000サービスアプライアンス"

"SG6000 ストレージアプライアンス"

"SG5700 ストレージアプライアンス"

"SG5600 ストレージアプライアンス"

"ネットアップサポート"

## /etc/network/interfaces の例

。 `/etc/network/interfaces` ファイルは3つのセクションに分かれており、それぞれに物理インターフェイス、ボンドインターフェイス、VLANインターフェイスが定義されます。以下の 3 つのセクションサンプルを 1 つのファイルに統合すれば、 4 つの Linux 物理インターフェイスを 1 つの LACP ボンドにまとめ、そのボンドを StorageGRID のグリッドネットワーク、管理ネットワーク、およびクライアントネットワークのインターフェイスとして使用するための 3 つの VLAN インターフェイスを確立できます。

物理インターフェイス

リンクの反対側のスイッチでも、 4 つのポートを 1 つの LACP トランクまたはポートチャネルとして扱い、少なくともタグで参照された 3 つの VLAN を通過させる必要があります。

```
# loopback interface
auto lo
iface lo inet loopback

# ens160 interface
auto ens160
iface ens160 inet manual
    bond-master bond0
    bond-primary en160

# ens192 interface
auto ens192
iface ens192 inet manual
    bond-master bond0

# ens224 interface
auto ens224
iface ens224 inet manual
    bond-master bond0

# ens256 interface
auto ens256
iface ens256 inet manual
    bond-master bond0
```

ボンドインターフェイス

```
# bond0 interface
auto bond0
iface bond0 inet manual
    bond-mode 4
    bond-miimon 100
    bond-slaves ens160 ens192 end224 ens256
```

**VLAN** インターフェイス

```
# 1001 vlan
auto bond0.1001
iface bond0.1001 inet manual
vlan-raw-device bond0

# 1002 vlan
auto bond0.1002
iface bond0.1002 inet manual
vlan-raw-device bond0

# 1003 vlan
auto bond0.1003
iface bond0.1003 inet manual
vlan-raw-device bond0
```

# VMware をインストールする

VMware環境にStorageGRID をインストールする方法について説明します。

- "インストールの概要"
- "計画と準備"
- "VMware vSphere Web Clientでの仮想マシングリッドノードの導入"
- "グリッドの設定とインストールの完了"
- "インストールの自動化"
- "インストール REST API の概要"
- "次の手順"
- "インストールに関する問題のトラブルシューティング"

## インストールの概要

VMware 環境への StorageGRID システムのインストールは、主に 3 つの手順で行われます。

1. * 準備 * ：計画と準備の際に、次のタスクを実行します。
    - StorageGRID のハードウェア、ソフトウェア、仮想マシン、ストレージ、パフォーマンスの要件について説明します。
    - ネットワークを適切に設定するためのStorageGRID ネットワークの詳細について説明します。詳細については、StorageGRID のネットワークに関するガイドラインを参照してください。
    - StorageGRID グリッドノードのホストとして使用する物理サーバを決めて準備する。
    - 準備したサーバで、次の作業を行います。
        - VMware vSphere ハイパーバイザーをインストールする

- ESX ホストを設定
- VMware vSphere および vCenter をインストールして設定

2. * 導入 * ： VMware vSphere Web Client を使用してグリッドノードを導入します。導入したグリッドノードは、 StorageGRID システムの一部として作成され、 1 つ以上のネットワークに接続されます。
   a. VMware vSphere Web Client 、 .vmdk ファイル、および一連の .ovf ファイルテンプレートを使用して、手順 1 で準備したサーバにソフトウェアベースのノードを仮想マシン（ VM ）として導入します。
   b. StorageGRID アプライアンスノードを導入するには、 StorageGRID アプライアンスインストーラを使用します。

> ハードウェア固有の設置と統合の手順は、 StorageGRID インストール手順 には含まれていません。StorageGRID アプライアンスのインストール方法については、使用するアプライアンスのインストールとメンテナンスの手順を参照してください。

3. 構成：すべてのノードが導入されたら、StorageGRIDWebscaleを使ってグリッドを構成し、インストールを完了します。

ここでは、標準的なアプローチで StorageGRID システムを VMware 環境に導入して設定する方法を推奨します。次の代替アプローチに関する情報も参照してください。

- deploy-vsphere-ovftool.sh Bash スクリプト（インストールアーカイブから入手可能）を使用して VMware vSphere にグリッドノードを導入します。
- Python 設定スクリプト（インストールアーカイブに付属）を使用して、 StorageGRID システムの導入と設定を自動化します。
- Python 設定スクリプト（インストールアーカイブまたは StorageGRID アプライアンスインストーラで入手可能）を使用して、アプライアンスグリッドノードの導入と設定を自動化する。
- StorageGRID 環境を高度に開発する場合は、インストール REST API を使用して StorageGRID グリッドノードのインストールを自動化します。

関連情報

"計画と準備"

"VMware vSphere Web Clientでの仮想マシングリッドノードの導入"

"グリッドの設定とインストールの完了"

"インストールの自動化"

"インストール REST API の概要"

"ネットワークガイドライン"

## 計画と準備

### グリッドノードの導入および StorageGRID グリッドの設定を行う前に、手順 を完了するためのステップと要件を把握しておく必要があります。

StorageGRID の導入手順と設定手順を実行するには、 StorageGRID システムのアーキテクチャと運用機能に

関する十分な知識が必要です。

一度に 1 つ以上のサイトを導入できますが、ストレージノードが少なくとも 3 つ必要であるという最小要件をすべてのサイトが満たしている必要があります。

ノード導入とグリッド設定の手順 を開始する前に、次の作業を完了しておく必要があります。

- StorageGRID の導入を計画します。
- StorageGRID アプライアンスを含む必要なすべてのハードウェアを仕様に従って設置、接続、設定します。

> ハードウェア固有の設置と統合の手順は、 StorageGRID インストール手順 には含まれていません。StorageGRID アプライアンスのインストール方法については、使用するアプライアンスのインストールとメンテナンスの手順を参照してください。

- 使用可能なネットワークオプションおよび各ネットワークオプションをグリッドノードで実装する方法を把握しておきます。StorageGRID のネットワークに関するガイドラインを参照してください。
- すべてのネットワーク情報を事前に収集します。DHCP を使用している場合を除き、各グリッドノードに割り当てる IP アドレス、および使用される Domain Name System （ DNS ；ドメインネームシステム）サーバと Network Time Protocol （ NTP ；ネットワークタイムプロトコル）サーバの IP アドレスを収集してください。
- 使用する導入ツールと設定ツールを決定します。

関連情報

"ネットワークガイドライン"

"SG100 SG1000サービスアプライアンス"

"SG6000 ストレージアプライアンス"

"SG5700 ストレージアプライアンス"

"SG5600 ストレージアプライアンス"

前提要件

## StorageGRID をインストールする前に、必要な情報やデータ、機器を揃えておく必要があります。

| 項目 | 注： |
| --- | --- |
| NetApp StorageGRID ライセンス | デジタル署名された有効なネットアップライセンスが必要です。<br>• 注： StorageGRID インストールアーカイブには、製品サポートのない無償ライセンスが含まれています。 |
| VMware用のStorageGRID インストールアーカイブ | StorageGRID インストールアーカイブをダウンロードし、ファイルを展開する必要があります。 |

| 項目 | 注： |
| --- | --- |
| VMware のソフトウェアとドキュメント | インストール時に、VMware vSphere Web Clientで仮想マシンに仮想グリッドノードを導入します。サポートされるバージョンについては、Interoperability Matrixを参照してください。 |
| サービスラップトップ | StorageGRID システムは、サービスラップトップを介してインストールされます。サービスラップトップには次のものが必要です。<br>• ネットワークポート<br>• SSH クライアント（ PuTTY など）<br>• サポートされている Web ブラウザ |
| StorageGRID のドキュメント | • リリースノート<br>• StorageGRID の管理手順 |

関連情報

"NetApp Interoperability Matrix Tool で確認できます"

"StorageGRID インストールファイルのダウンロードと展開"

"Web ブラウザの要件"

"StorageGRID の管理"

"リリースノート"

**StorageGRID** インストールファイルのダウンロードと展開

## StorageGRID インストールアーカイブをダウンロードし、ファイルを展開する必要があります。

手順

1. ネットアップの StorageGRID ダウンロードページにアクセスします。

   "ネットアップのダウンロード： StorageGRID"

2. 最新のリリースをダウンロードするボタンを選択するか、ドロップダウンメニューから別のバージョンを選択して、「 * Go * 」を選択します。
3. ネットアップアカウントのユーザ名とパスワードを使用してサインインします。
4. 「注意 / 必ずお読みください」という記述が表示されたら、それを読んでチェックボックスを選択してください。

   StorageGRID リリースのインストール後に、必要な修正プログラムを適用する必要があります。詳細については、リカバリおよびメンテナンスの手順にあるホットフィックス手順 を参照してください。

5. エンドユーザライセンス契約を読み、チェックボックスをオンにして、「 * 同意して続行 * 」を選択しま

す。

6. [Install StorageGRID *（インストールソフトウェアのインストール）]列で、適切なソフトウェアを選択します。

   をダウンロードします `.tgz` または `.zip` 使用するプラットフォームに対応したアーカイブファイルです。

   - `StorageGRID-Webscale-version-VMware-uniqueID.zip`
   - `StorageGRID-Webscale-version-VMware-uniqueID.tgz`

   を使用します `.zip` ファイルサービスラップトップでWindowsを実行している場合。

1. アーカイブファイルを保存して展開します。
2. 次のリストから必要なファイルを選択します。

   必要なファイルは、計画したグリッドトポロジおよび StorageGRID システムの導入方法によって異なります。

   次の表に示すパスは、展開されたインストールアーカイブによってインストールされた最上位ディレクトリに対する相対パスです。

| パスとファイル名 | 説明 |
| --- | --- |
| | StorageGRID ダウンロードファイルに含まれているすべてのファイルについて説明するテキストファイル。 |
| | 製品サポートのない無償ライセンス。 |
| | グリッドノード仮想マシンを作成するためのテンプレートとして使用される仮想マシンディスクファイル。 |
| | Open Virtualization Formatテンプレートファイル (`.ovf`)とマニフェストファイル (`.mf`）を使用してください。 |
| | テンプレートファイル (`.ovf`)とマニフェストファイル (`.mf`）。非プライマリ管理ノードを導入する場合に使用します。 |
| | テンプレートファイル (`.ovf`)とマニフェストファイル (`.mf`）を使用してアーカイブノードを導入します。 |
| | テンプレートファイル (`.ovf`)とマニフェストファイル (`.mf`）を選択します。 |

| パスとファイル名 | 説明 |
| --- | --- |
| | テンプレートファイル (.ovf)とマニフェストファイル (.mf）を選択します。 |
| 導入スクリプトツール | 説明 |
| | 仮想グリッドノードの導入を自動化するための Bash シェルスクリプト。 |
| | で使用するサンプル構成ファイル deploy-vsphere-ovftool.sh スクリプト： |
| | StorageGRID システムの設定を自動化するための Python スクリプト。 |
| | StorageGRID アプライアンスの設定を自動化するための Python スクリプト。 |
| | シングルサインオンが有効な場合にグリッド管理 API にサインインするために使用できる Python スクリプトの例。 |
| | で使用するサンプル構成ファイル configure-storagegrid.py スクリプト： |
| | で使用する空の構成ファイル configure-storagegrid.py スクリプト： |

関連情報

""

ソフトウェア要件

## 仮想マシンを使用すると、あらゆるタイプの StorageGRID グリッドノードをホストできます。VMware サーバにインストールされたグリッドノードごとに 1 つの仮想マシンが必要です。

#### VMware vSphere ハイパーバイザー

準備が整った物理サーバに VMware vSphere ハイパーバイザーをインストールする必要があります。VMware ソフトウェアをインストールする前に、ハードウェアが正しく設定されている必要があります（ファームウェアバージョンと BIOS 設定を含む）。

- インストールする StorageGRID システムのネットワークをサポートできるように、ハイパーバイザーのネットワークを設定します。

"ネットワークのガイドライン"

- データストアが、グリッドノードをホストするために必要な仮想マシンと仮想ディスクに十分な大きさであることを確認します。
- 複数のデータストアを作成する場合は、仮想マシン作成時に各グリッドノードに使用するデータストアを簡単に識別できるよう、各データストアに名前を付けます。

**ESX** ホストの設定要件

各 ESX ホストでネットワークタイムプロトコル（ NTP ）を適切に設定する必要があります。ホストの時刻が正しくないと、データ損失などのマイナスの影響が生じる可能性があります。

**VMware** の設定要件

StorageGRID グリッドノードを導入する前に、 VMware vSphere および vCenter をインストールして設定する必要があります。

VMware vSphere ハイパーバイザーおよび VMware vCenter Server ソフトウェアのサポート対象のバージョンについては、 Interoperability Matrix を参照してください。

これらの VMware 製品をインストールするために必要な手順については、 VMware のドキュメントを参照してください。

関連情報

"NetApp Interoperability Matrix Tool で確認できます"

**CPU** と **RAM** の要件

## StorageGRID ソフトウェアをインストールする前に、ハードウェアの確認と設定を行って、 StorageGRID システムをサポートできる状態にしておきます。

サポートされているサーバについては、 Interoperability Matrix を参照してください。

各 StorageGRID ノードに必要な最小リソースは次のとおりです。

- CPU コア：ノードあたり 8 個
- RAM ：システムで実行されている StorageGRID 以外のソフトウェアの合計 RAM 容量によって、ノードあたり 24 GB 以上、システム RAM の合計容量から 2 ~ 16 GB 削減されます

それぞれの物理ホストまたは仮想ホストで実行する StorageGRID ノードの数が、利用可能な CPU コアや物理 RAM を超えないようにしてください。ホストが StorageGRID 専用ではない場合（非推奨）は、他のアプリケーションのリソース要件も考慮する必要があります。

CPU とメモリの使用状況を定期的に監視して、ワークロードに継続的に対応できるようにします。たとえば、仮想ストレージノードの RAM 割り当てと CPU 割り当てを 2 倍にすると、StorageGRID アプライアンスノードの場合と同様のリソースが提供されます。また、ノードあたりのメタデータの量が 500GB を超える場合は、ノードあたりの RAM を 48GB 以上に増やすことを検討してください。オブジェクトメタデータストレージの管理、 Metadata Reserved Space 設定の拡張、 CPU とメモリの使用状況の監視については、 StorageGRID の管理、監視、アップグレードの手順を参照してください。

基盤となる物理ホストでハイパースレッディングが有効である場合は、ノードあたり 8 個の仮想コア（ 4 個の物理コア）で構成できます。基盤となる物理ホストでハイパースレッディングが有効でない場合は、ノードあたり 8 個の物理コアを用意する必要があります。

仮想マシンをホストとして使用する場合、 VM のサイズと数を制御可能であれば、 StorageGRID ノードごとに 1 つの VM を使用し、それに応じて VM のサイズを設定する必要があります。

本番環境では、複数のストレージノードを同じ物理ストレージハードウェアまたは仮想ホストで実行しないでください。単一の StorageGRID 環境の各ストレージノードをそれぞれ独自の分離された障害ドメインに配置するようにします。単一のハードウェア障害が単一のストレージノードにしか影響しないようにすることで、オブジェクトデータの耐久性と可用性を最大限に高めることができます。

ストレージ要件に関する情報も参照してください。

関連情報

"NetApp Interoperability Matrix Tool で確認できます"

"ストレージとパフォーマンスの要件"

"StorageGRID の管理"

"トラブルシューティングを監視します"

"ソフトウェアをアップグレードする"

ストレージとパフォーマンスの要件

## 初期設定と将来のストレージ拡張に対応するための十分なスペースを確保できるよう、仮想マシンでホストされている StorageGRID ノードのストレージ要件とパフォーマンス要件を把握しておく必要があります。

### パフォーマンス要件

OS ボリュームおよび最初のストレージボリュームのパフォーマンスは、システム全体のパフォーマンスに大きく影響します。これらのボリュームのディスクパフォーマンスが、レイテンシ、 1 秒あたりの入出力操作（ IOPS ）、スループットの点で適切であることを確認してください。

すべての StorageGRID ノードで、 OS ドライブとすべてのストレージボリュームのライトバックキャッシュを有効にする必要があります。キャッシュは、保護されたメディアまたは永続的なメディアに配置する必要があります。

#### **NetApp AFF** ストレージを使用する仮想マシンの要件

NetApp AFF システムからストレージが割り当てられた仮想マシンとして StorageGRID ノードを導入する場合は、ボリュームで FabricPool 階層化ポリシーが有効になっていないことを確認しておきます。たとえば、StorageGRID ノードが VMware ホスト上の仮想マシンとして実行されている場合は、ノードのデータストアの作成元のボリュームで FabricPool 階層化ポリシーが有効になっていないことを確認します。StorageGRID ノードで使用するボリュームで FabricPool による階層化を無効にすることで、トラブルシューティングとストレージの処理がシンプルになります。

StorageGRID を使用して StorageGRID に関連するデータを FabricPool 自体に階層化しないでください。StorageGRID データを StorageGRID に階層化すると、トラブルシューティングと運用がより複雑になります。

### 必要な仮想マシンの数

各 StorageGRID サイトに、少なくとも 3 つのストレージノードが必要です。

本番環境では、 1 台の仮想マシンサーバで複数のストレージノードを実行しないでください。各ストレージノードに専用の仮想マシンホストを使用すると、分離された障害ドメインが提供されます。

管理ノードやゲートウェイノードなど、他のタイプのノードは、同じ仮想マシンホストに導入するか、必要に応じて独自の専用の仮想マシンホストに導入することができます。ただし、同じタイプのノードが複数ある（たとえば、 2 つのゲートウェイノード）場合は、すべてのインスタンスを同じ仮想マシンホストにインストールしないでください。

### ノードタイプ別のストレージ要件

本番環境では、 StorageGRID グリッドノードの仮想マシンが、ノードのタイプに応じて、さまざまな要件を満たしている必要があります。

ディスクの Snapshot を使用してグリッドノードをリストアすることはできません。各タイプのノードのリカバリとメンテナンスの手順を参照してください。

| ノードタイプ（ **Node Type** ） | ストレージ |
| --- | --- |
| 管理ノード | OS 用に 100GB の LUN<br><br>管理ノードのテーブル用に 200GB の LUN<br><br>管理ノードの監査ログ用に 200GB の LUN |
| ストレージノード | OS 用に 100GB の LUN<br><br>このホストのストレージノードごとに 3 個の LUN<br><br>• 注 * ： 1 個のストレージノードには 1~16 個のストレージ LUN を設定できます。 3 個以上のストレージ LUN を推奨します。<br><br>LUN あたりの最小サイズ： 4TB<br><br>検証済みの最大 LUN サイズ： 39TB 。 |
| ゲートウェイノード | OS 用に 100GB の LUN |
| アーカイブノード | OS 用に 100GB の LUN |

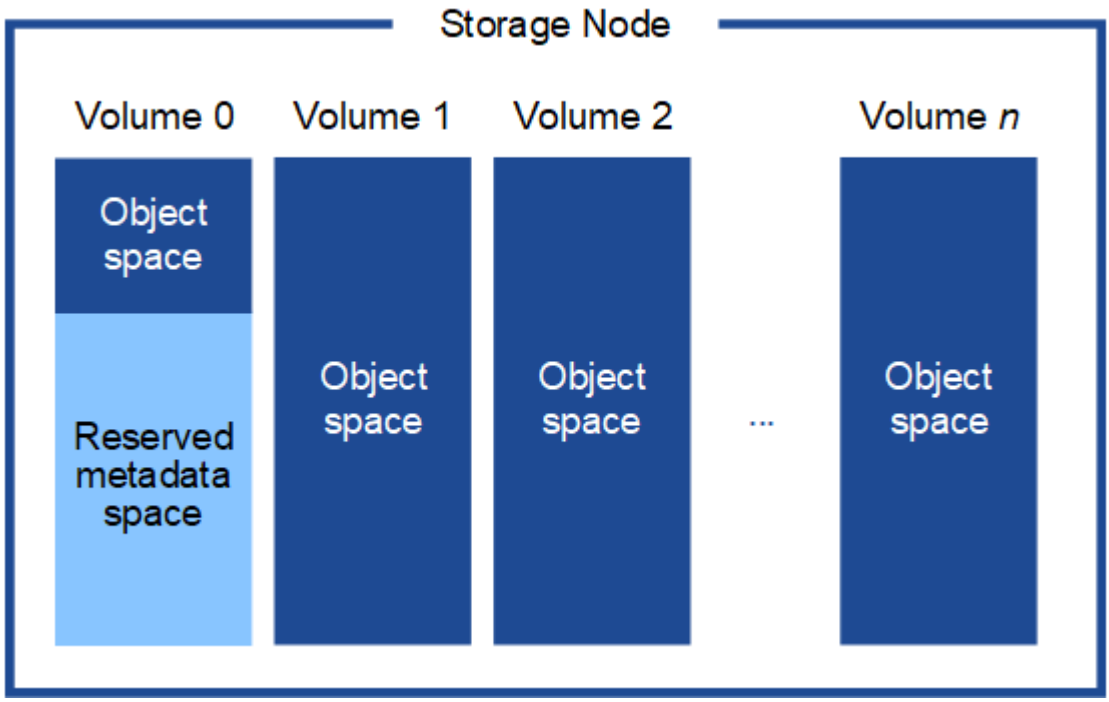
設定されている監査レベル、 S3 オブジェクトキー名などのユーザ入力のサイズ、保持する必要がある監査ログデータの量によっては、各管理ノードの監査ログ LUN のサイズを増やす必要があります。原則として、 S3 処理ごとに約 1 KB の監査データが生成されることから、 200GB の LUN で 1 日あたり 7 、 000 万件の処理、 1 秒あたり 2 ~ 3 日間で 800 件の処理がサポートされることになります。

ストレージノードのストレージ要件

ソフトウェアベースのストレージノードのストレージボリューム数は 1~16 個までにすることを推奨します。 -3 個以上のストレージボリュームを使用することを推奨します。各ストレージボリュームのサイズは 4TB 以上にします。

アプライアンスストレージノードには、最大 48 個のストレージボリュームを設定できます。

図に示すように、 StorageGRID は各ストレージノードのストレージボリューム 0 にオブジェクトメタデータ用のスペースをリザーブします。ストレージボリューム 0 の残りのスペースとストレージノード内のその他のストレージボリュームは、オブジェクトデータ専用に使用されます。




冗長性を確保し、オブジェクトメタデータを損失から保護するために、 StorageGRID は各サイトのシステム内のすべてのオブジェクトにメタデータのコピーを 3 つずつ格納します。オブジェクトメタデータの 3 つのコピーが各サイトのすべてのストレージノードに均等に分散されます。

新しいストレージノードのボリューム 0 にスペースを割り当てる場合は、そのノードのすべてのオブジェクトメタデータの一部に対して十分なスペースを確保する必要があります。

- 少なくとも 4TB をボリューム 0 に割り当てる必要があります。

ストレージノードでストレージボリュームを 1 つしか使用していない場合に、そのボリュームに 4TB 以下を割り当てると、ストレージノードが起動時にストレージ読み取り専用状態になり、オブジェクトメタデータのみが格納される可能性があります。

- 新しいStorageGRID 11.5システムをインストールするときに、各ストレージノードに128GB以上のRAMがある場合は、ボリューム0に8TB以上を割り当てる必要があります。ボリューム 0 に大きな値を設定すると、各ストレージノードでメタデータに使用できるスペースが増加する可能性があります。
- サイトに複数のストレージノードを設定する場合は、可能であればボリューム 0 にも同じ設定を使用します。サイトにサイズが異なるストレージノードがある場合、ボリューム 0 が最も小さいストレージノードがそのサイトのメタデータ容量を決定します。

詳細については、StorageGRID の管理手順を参照し、「オブジェクト・メタデータ・ストレージの管理」を検索してください。

"StorageGRID の管理"

関連情報

""

**Web** ブラウザの要件

サポートされている Web ブラウザを使用する必要があります。

| **Web** ブラウザ | サポートされる最小バージョン |
|---|---|
| Google Chrome | 87 |
| Microsoft Edge の場合 | 87 |
| Mozilla Firefox | 84 |

ブラウザウィンドウの幅を推奨される値に設定してください。

| ブラウザの幅 | ピクセル |
|---|---|
| 最小（ Minimum ） | 1024 |
| 最適 | 1280 |

## **VMware vSphere Web Client**での仮想マシングリッドノードの導入

VMware vSphere Web Client を使用して、各グリッドノードを仮想マシンとして導入します。導入時に、各グリッドノードが作成されて1つ以上のネットワークに接続されます。StorageGRID アプライアンスストレージノードを導入する必要がある場合は、すべての仮想マシングリッドノードを導入したあとに、アプライアンスのインストールとメンテナンスの手順を参照してください。

- "導入環境に関する情報を収集"
- "グリッドノードによるプライマリ管理ノードの検出"
- "仮想マシンとしてのStorageGRID ノードの導入"

関連情報

"SG100 SG1000サービスアプライアンス"

"SG5600 ストレージアプライアンス"

"SG5700 ストレージアプライアンス"

"SG6000 ストレージアプライアンス"

導入環境に関する情報を収集

## グリッドノードを導入する前に、ネットワーク設定と VMware 環境に関する情報を収集する必要があります。

**VMware** の情報

導入環境にアクセスし、 VMware 環境に関する情報、グリッドネットワーク、管理ネットワーク、クライアントネットワーク用に作成されたネットワークに関する情報、およびストレージノードで使用する予定のストレージボリュームタイプに関する情報を収集する必要があります。

VMware 環境に関する次の情報を収集する必要があります。

- 導入を完了するための適切な権限を持つ VMware vSphere アカウントのユーザ名とパスワード。
- 各 StorageGRID グリッドノード仮想マシンのホスト、データストア、およびネットワーク設定に関する情報。

> VMware のライブ vMotion を使用すると仮想マシンのクロック時間が急に進むため、この機能はどのタイプのグリッドノードでもサポートされていません。まれにではありますが、クロック時間が不正確だとデータや設定の更新が失われることがあります。

グリッドネットワークの情報

StorageGRID グリッドネットワーク（必須）用に作成された VMware ネットワークに関する次の情報を収集する必要があります。

- ネットワーク名。
- DHCP を使用しない場合は、各グリッドノードのネットワークに関する必須の詳細情報（ IP アドレス、ゲートウェイ、およびネットワークマスク）。
- DHCP を使用しない場合は、グリッドネットワーク上のプライマリ管理ノードの IP アドレス。詳細については、「グリッドノードによるプライマリ管理ノードの検出」を参照してください。

管理ネットワークの情報

ノードがオプションの StorageGRID 管理ネットワークに接続される場合は、このネットワーク用に作成された VMware ネットワークに関する次の情報を収集する必要があります。

- ネットワーク名。
- 静的または DHCP のいずれかの IP アドレスの割り当てに使用する方法。
- 静的 IP アドレスを使用する場合は、各グリッドノードのネットワークに関する必須の詳細情報（ IP アド

レス、ゲートウェイ、ネットワークマスク）。

- 管理ネットワークの外部サブネットリスト（ ESL ）。

クライアントネットワークの情報

ノードがオプションの StorageGRID クライアントネットワークに接続される場合は、このネットワーク用に作成された VMware ネットワークに関する次の情報を収集する必要があります。

- ネットワーク名。
- 静的または DHCP のいずれかの IP アドレスの割り当てに使用する方法。
- 静的 IP アドレスを使用する場合は、各グリッドノードのネットワークに関する必須の詳細情報（ IP アドレス、ゲートウェイ、ネットワークマスク）。

仮想ストレージノードのストレージボリューム

仮想マシンベースのストレージノードに関する次の情報を収集する必要があります。

- 追加するストレージボリューム（ストレージ LUN ）の数とサイズ。「ストレージとパフォーマンスの要件」を参照してください。

グリッドの設定情報

グリッドを設定するための情報を収集する必要があります。

- Grid ライセンス
- Network Time Protocol （ NTP ；ネットワークタイムプロトコル）サーバの IP アドレス
- Domain Name System （ DNS ；ドメインネームシステム）サーバの IP アドレス

関連情報

"グリッドノードによるプライマリ管理ノードの検出"

"ストレージとパフォーマンスの要件"

グリッドノードによるプライマリ管理ノードの検出

## グリッドノードは、設定や管理のためにプライマリ管理ノードと通信します。各グリッドノードがグリッドネットワーク上のプライマリ管理ノードの IP アドレスを認識している必要があります。

グリッドノードからプライマリ管理ノードにアクセスできるようにするために、ノードを導入する際に次のいずれかを実行します。

- ADMIN_IP パラメータを使用して、プライマリ管理ノードの IP アドレスを手動で入力します。
- ADMIN_IP パラメータを省略して、グリッドノードで自動的に値が検出されるようにします。自動検出は、グリッドネットワークで DHCP を使用してプライマリ管理ノードに IP アドレスを割り当てる場合に特に便利です。

プライマリ管理ノードの自動検出には、 mDNS （ multicast Domain Name System ）が使用されます。プライマリ管理ノードは、最初に起動されるときに、 mDNS を使用してそのノードの IP アドレスを公開します。

同じサブネット上の他のノードは、この IP アドレスを自動的に照会して取得します。ただし、通常はマルチキャスト IP トラフィックをサブネット間でルーティングできないため、他のサブネット上のノードはプライマリ管理ノードの IP アドレスを直接取得できません。

自動検出を使用する場合：

- プライマリ管理ノードが直接接続されていないサブネットの少なくとも 1 つのグリッドノードで、 ADMIN_IP 設定を指定する必要があります。このグリッドノードがプライマリ管理ノードの IP アドレスを公開することで、サブネット上の他のノードが mDNS を使用して IP アドレスを検出できるようになります。
- ネットワークインフラがサブネット内のマルチキャスト IP トラフィックの転送をサポートしていることを確認します。

仮想マシンとしての**StorageGRID** ノードの導入

VMware vSphere Web Client を使用して、各グリッドノードを仮想マシンとして導入します。導入時に、各グリッドノードが作成されて、 1 つ以上の StorageGRID ネットワークに接続されます。必要に応じて、ノードポートを再マッピングしたり、ノードの CPU やメモリの設定を増やしたりして、電源をオンにすることができます。

必要なもの

- 計画と準備に関するトピックを確認し、ソフトウェア、CPUとRAM、ストレージとパフォーマンスの要件を把握しておきます。

  "計画と準備"

- VMware vSphere ハイパーバイザーについて理解し、この環境で仮想マシンの導入を経験している必要があります。

  。 `open-vm-tools` パッケージはVMware Toolsに似たオープンソースの実装で、StorageGRID 仮想マシンに含まれています。VMware Tools を手動でインストールする必要はありません。

- VMware 用の正しいバージョンの StorageGRID インストールアーカイブをダウンロードして展開しておきます。

  拡張またはリカバリ処理の一環として新しいノードを導入する場合は、グリッドで現在実行されているバージョンの StorageGRID を使用する必要があります。

- StorageGRID 仮想マシンディスクが必要です (`.vmdk`）ファイル：

```
NetApp-<em>SG-version</em>-SHA.vmdk
```

- を使用することができます `.ovf` および `.mf` 導入するグリッドノードのタイプごとに、次のファイルを用意します。

| ファイル名 | 説明 |
| --- | --- |
| vsphere-primary-admin.ovf vsphere-primary-admin.mf | プライマリ管理ノードのテンプレートファイルとマニフェストファイル。 |
| vsphere-non-primary-admin.ovf vsphere-non-primary-admin.mf | 非プライマリ管理ノードのテンプレートファイルとマニフェストファイル。 |
| vsphere-archive.ovf vsphere-archive.mf | アーカイブノードのテンプレートファイルとマニフェストファイル。 |
| vsphere-gateway.ovf vsphere-gateway.mf | ゲートウェイノードのテンプレートファイルとマニフェストファイル。 |
| vsphere-storage.ovf vsphere-storage.mf | ストレージノードのテンプレートファイルとマニフェストファイル。 |

- 。 `.vdmk`、 `.ovf`および `.mf` ファイルはすべて同じディレクトリにあります。
- 障害ドメインを最小限に抑えるための計画が必要です。たとえば、すべてのゲートウェイノードを 1 台の仮想マシンサーバに導入することは避けてください。

> 本番環境では、 1 台の仮想マシンサーバで複数のストレージノードを実行しないでください。各ストレージノードに専用の仮想マシンホストを使用すると、分離された障害ドメインが提供されます。

- 拡張またはリカバリ処理の一環としてノードを導入する場合は、StorageGRID システムの拡張手順またはリカバリとメンテナンスの手順を参照してください。
  - "グリッドを展開します"
  - ""
- NetApp AFF システムからストレージが割り当てられた仮想マシンとして StorageGRID ノードを導入する場合は、ボリュームで FabricPool 階層化ポリシーが有効になっていないことを確認しておきます。たとえば、 StorageGRID ノードが VMware ホスト上の仮想マシンとして実行されている場合は、ノードのデータストアの作成元のボリュームで FabricPool 階層化ポリシーが有効になっていないことを確認します。StorageGRID ノードで使用するボリュームで FabricPool による階層化を無効にすることで、トラブルシューティングとストレージの処理がシンプルになります。

> StorageGRID を使用して StorageGRID に関連するデータを FabricPool 自体に階層化しないでください。StorageGRID データを StorageGRID に階層化すると、トラブルシューティングと運用がより複雑になります。

このタスクについて

最初に VMware ノードを導入するとき、拡張時に新しい VMware ノードを追加するとき、またはリカバリ処理の一環として VMware ノードを交換するときは、次の手順に従います。手順でメモした場合を除き、ノード導入手順 は管理ノード、ストレージノード、ゲートウェイノード、アーカイブノードなど、すべてのタイプのノードで同じです。

新しい StorageGRID システムを設置する場合は、次の手順を実行します。

- プライマリ管理ノードは、他のグリッドノードを導入する前に導入する必要があります。
- 各仮想マシンがグリッドネットワーク経由でプライマリ管理ノードに接続できることを確認する必要があります。
- グリッドを設定する前に、すべてのグリッドノードを導入する必要があります。

拡張またはリカバリ処理を実行する場合は、次の手順を実行します。

- 新しい仮想マシンがグリッドネットワーク経由でプライマリ管理ノードに接続できることを確認する必要があります。

ノードのポートを再マッピングする必要がある場合は、ポートの再マッピングの設定が完了するまで新しいノードの電源をオンにしないでください。

手順

1. vCenter を使用して OVF テンプレートを導入

   URL を指定する場合は、次のファイルを含むフォルダを指定します。それ以外の場合は、ローカルディレクトリから各ファイルを選択します。

   ```
   NetApp-<em>SG-version</em>-SHA.vmdk
   vsphere-<em>node</em>.ovf
   vsphere-<em>node</em>.mf
   ```

   たとえば、導入する最初のノードがこのファイルに含まれている場合は、次のファイルを使用して StorageGRID システムのプライマリ管理ノードを導入します。

   ```
   NetApp-<em>SG-version</em>-SHA.vmdk
   sphere-primary-admin.ovf
   sphere-primary-admin.mf
   ```

2. 仮想マシンの名前を指定します。

   標準的には、仮想マシンとグリッドノードに同じ名前を使用します。

3. 仮想マシンを適切な vApp またはリソースプールに配置します。
4. プライマリ管理ノードを導入する場合は、エンドユーザライセンス契約を読んで同意します。

   vCenterのバージョンによっては、使用する手順の順序は、エンドユーザライセンス契約を承諾し、仮想マシンの名前を指定し、データストアを選択する場合とで異なります

5. 仮想マシンのストレージを選択します。

   リカバリ処理の一環としてノードを導入する場合は、の手順を実行します ストレージリカバリ手順 新しい仮想ディスクを追加するには、障害が発生したグリッドノードから仮想ハードディスクを再接続するか、その両方を実行します。

ストレージノードを導入する際は、ストレージボリュームを 3 個以上使用し、各ストレージボリュームのサイズを 4TB 以上にします。ボリューム 0 に少なくとも 4TB 割り当てる必要があります。

> ストレージノードの .ovf ファイルは、ストレージ用の複数の VMDK を定義します。これらの VMDK がストレージ要件を満たしていない場合は、ノードの電源を入れる前に、それらの VMDK を削除し、ストレージに適切な VMDK または RDM を割り当てる必要があります。VMware 環境で一般に使用され、管理も容易であるのは VMDK ですが、大きなオブジェクトサイズ（たとえば 100MB 超）を使用するワークロードのパフォーマンスは RDM の方が高くなります。

6. ネットワークを選択します。

   各ソースネットワークのデスティネーションネットワークを選択して、ノードで使用する StorageGRID ネットワークを決定します。

   - グリッドネットワークは必須です。vSphere 環境でデスティネーションネットワークを選択する必要があります。
   - 管理ネットワークを使用する場合は、 vSphere 環境で別のデスティネーションネットワークを選択します。管理ネットワークを使用しない場合は、グリッドネットワークと同じ送信先を選択します。
   - クライアントネットワークを使用する場合は、 vSphere 環境で別のデスティネーションネットワークを選択します。クライアントネットワークを使用しない場合は、グリッドネットワークと同じデスティネーションを選択します。

7. [ テンプレートのカスタマイズ（ Customize Template ） ] で、必要な StorageGRID ノードプロパティを設定します。

   a. ノード名 * を入力します。

      > グリッドノードをリカバリする場合は、リカバリするノードの名前を入力する必要があります。

   b. * グリッドネットワーク（ eth0 ） * セクションで、 * グリッドネットワーク IP 設定 * に静的または DHCP を選択します。

      - 静的を選択した場合は、 * グリッドネットワーク IP * 、 * グリッドネットワークマスク * 、 * グリッドネットワークゲートウェイ * 、 * グリッドネットワーク MTU * を入力します。
      - DHCP を選択した場合は、 * グリッドネットワーク IP * 、 * グリッドネットワークマスク * 、 * グリッドネットワークゲートウェイ * が自動的に割り当てられます。

   c. 「 * Primary Admin IP * 」フィールドに、グリッドネットワークのプライマリ管理ノードの IP アドレスを入力します。

      > この手順は、導入するノードがプライマリ管理ノードの場合は必要ありません。

   プライマリ管理ノードの IP アドレスを省略すると、プライマリ管理ノードまたは ADMIN_IP が設定された少なくとも 1 つのグリッドノードが同じサブネットにある場合は、 IP アドレスが自動的に検出されます。ただし、ここでプライマリ管理ノードの IP アドレスを設定することを推奨します。

   a. 「 * Admin Network （ eth1 ） * 」セクションで、「 * Admin network IP configuration * 」に対して「 static 」、「 dhcp 」、または「 disabled 」を選択します。

      - 管理ネットワークを使用しない場合は、 disabled を選択し、管理ネットワーク IP に * 0.0.0.0 * を

入力します。他のフィールドは空白のままにすることができます。

- 静的を選択した場合は、 * 管理ネットワーク IP * 、 * 管理ネットワークマスク * 、 * 管理ネットワークゲートウェイ * 、 * 管理ネットワーク MTU * を入力します。
- 静的を選択した場合は、 * 管理ネットワークの外部サブネットリスト * を入力します。ゲートウェイも設定する必要があります。
- DHCP を選択した場合は、 * 管理ネットワーク IP * 、 * 管理ネットワークマスク * 、および * 管理ネットワークゲートウェイ * が自動的に割り当てられます。

b. クライアントネットワーク（ eth2 ） * セクションで、 * クライアントネットワーク IP 構成 * の静的、 DHCP 、または無効を選択します。

- クライアントネットワークを使用しない場合は、無効を選択し、クライアントネットワーク IP に「 * 0.0.0.0 * 」と入力します。他のフィールドは空白のままにすることができます。
- 静的を選択した場合は、 * クライアントネットワーク IP * 、 * クライアントネットワークマスク * 、 * クライアントネットワークゲートウェイ * 、および * クライアントネットワーク MTU * を入力します。
- DHCP を選択した場合は、 * クライアントネットワーク IP * 、 * クライアントネットワークマスク * 、および * クライアントネットワークゲートウェイ * が自動的に割り当てられます。

8. 仮想マシンの設定を確認し、必要な変更を行います。
9. 完了する準備ができたら、 [ 完了 ] を選択して仮想マシンのアップロードを開始します。
10. [[step_recovery_storage] - リカバリ処理の一環としてこのノードを導入し、フルノードリカバリではない場合は、導入の完了後に次の手順を実行します。

a. 仮想マシンを右クリックし、 * 設定の編集 * を選択します。

b. ストレージに指定されている各デフォルト仮想ハードディスクを選択し、 * 削除 * を選択します。

c. データリカバリの状況に応じて、ストレージ要件に従って新しい仮想ディスクを追加し、以前に削除した障害グリッドノードから保存した仮想ハードディスクを再接続するか、またはその両方を実行します。

次の重要なガイドラインに注意してください。

- 新しいディスクを追加する場合は、ノードのリカバリ前に使用していたものと同じタイプのストレージデバイスを使用する必要があります。
- ストレージノードの .ovf ファイルは、ストレージ用の複数の VMDK を定義します。これらの VMDK がストレージ要件を満たしていない場合は、ノードの電源を入れる前に、それらの VMDK を削除し、ストレージに適切な VMDK または RDM を割り当てる必要があります。VMware 環境で一般に使用され、管理も容易であるのは VMDK ですが、大きなオブジェクトサイズ（たとえば 100MB 超）を使用するワークロードのパフォーマンスは RDM の方が高くなります。

11. このノードで使用されるポートを再マッピングする必要がある場合は、次の手順を実行します。

ポートの再マッピングが必要となるのは、 StorageGRID で使用される 1 つ以上のポートへのアクセスがエンタープライズネットワークポリシーによって制限される場合です。StorageGRID で使用するポートのネットワークガイドラインを参照してください。

"ネットワークのガイドライン"

ロードバランサエンドポイントで使用されるポートは再マッピングしないでください。

a. 新しい VM を選択します。

b. [ 構成 ] タブで、 [ * 設定 * > * vApp オプション * ] を選択します。

> vapp Options * の場所は、 vCenter のバージョンによって異なります。

c. プロパティ * テーブルで、 PORT_REMAP_INBOUND および PORT_REMAP を確認します。

d. ポートのインバウンド通信とアウトバウンド通信の両方を対称的にマッピングするには、 * PORT_REMAP * を選択します。

> PORT_REMAP のみを設定すると、インバウンド通信とアウトバウンド通信の両方で環境 を指定したマッピングが適用されます。PORT_REMAP_INBOUND を併せて指定した場合は、 PORT_REMAP がアウトバウンド通信のみに適用されます。

i. 表の一番上までスクロールし、 * Edit * を選択します。

ii. [ タイプ ] タブで、 [ ユーザー設定可能 *] を選択し、 [ 保存 *] を選択します。

iii. 「 * 値の設定 * 」を選択します。

iv. ポートマッピングを入力します。

```
<network type>/<protocol>/<default port used by grid node>/<new port>
```

`<network type>` は、grid、admin、client、およびです `<protocol>` は、tcpまたはudpです。

たとえば、 ssh トラフィックをポート 22 からポート 3022 に再マッピングするには、次のように入力します。

```
client/tcp/22/3022
```

i. 「 * OK 」を選択します。

e. ノードへのインバウンド通信に使用するポートを指定するには、 * port_remap_inbound * を選択します。

> PORT_REMAP_INBOUND を指定して PORT_REMAP に値を指定しなかった場合は、ポートのアウトバウンド通信が変更されません。

i. 表の一番上までスクロールし、 * Edit * を選択します。

ii. [ タイプ ] タブで、 [ ユーザー設定可能 *] を選択し、 [ 保存 *] を選択します。

iii. 「 * 値の設定 * 」を選択します。

iv. ポートマッピングを入力します。

```
<network type>/<protocol>/<remapped inbound port>/<default inbound port used by grid node>
```

`<network type>` は、grid、admin、client、およびです `<protocol>` は、tcpまたはudpです。

たとえば、ポート 3022 に送信されるインバウンドの SSH トラフィックを再マッピングしてグリッドノードがポート 22 で受信するようにするには、次のように入力します。

```
client/tcp/3022/22
```

i. 「 * OK 」を選択します

12. ノードの CPU またはメモリをデフォルトの設定から増やす場合は、次の手順を実行します。
    a. 仮想マシンを右クリックし、 * 設定の編集 * を選択します。
    b. CPU の数またはメモリの容量を必要に応じて変更します。

       [ メモリ予約 * ] を、仮想マシンに割り当てられた * メモリ * と同じサイズに設定します。

    c. 「 * OK 」を選択します。
13. 仮想マシンの電源をオンにします。

完了後

このノードを拡張またはリカバリ用手順 の一部として導入した場合は、その手順に戻って手順 を完了します。

## グリッドの設定とインストールの完了

## プライマリ管理ノード上のグリッドマネージャからStorageGRID システムを設定すると、インストールが完了します。

- "Grid Managerに移動します"
- "StorageGRID ライセンス情報の指定"
- "サイトの追加"
- "グリッドネットワークのサブネットの指定"
- "保留中のグリッドノードを承認します"
- "Network Time Protocolサーバ情報の指定"
- "Domain Name Systemサーバ情報の指定"
- "StorageGRID システムのパスワードの指定"
- "設定を確認し、インストールを完了します"
- "インストール後のガイドライン"

**Grid Manager**に移動します

## StorageGRID システムの設定に必要なすべての情報については、グリッドマネージャを使用して定義します。

必要なもの

プライマリ管理ノードが導入され、最初の起動シーケンスが完了している必要があります。

手順

1. Web ブラウザを開き、次のいずれかのアドレスに移動します。

   `https://primary_admin_node_ip`

   `client_network_ip`

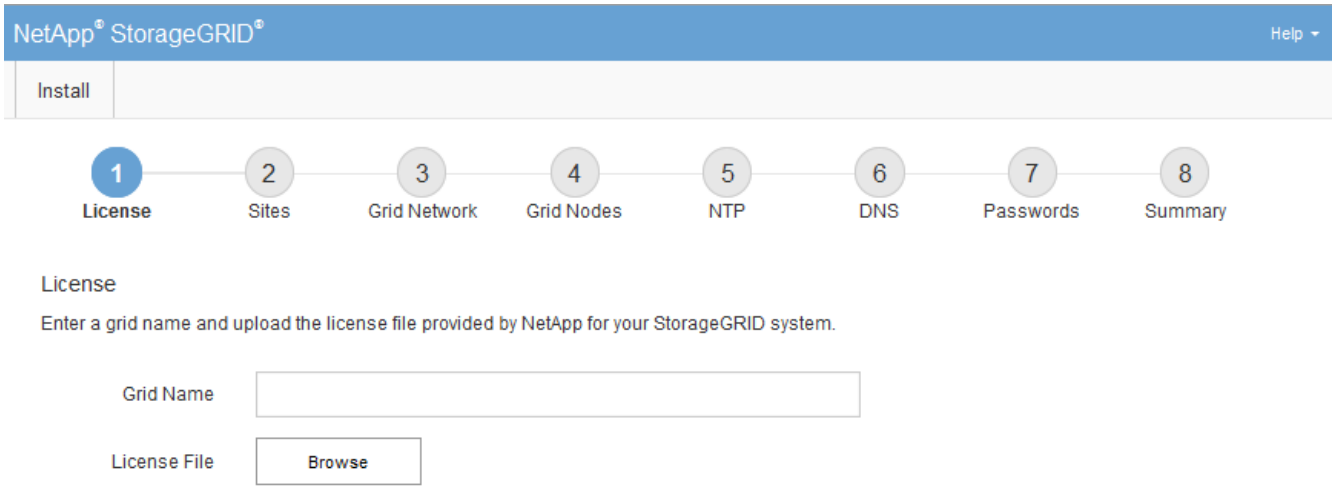
   ポート 8443 でグリッドマネージャにアクセスすることもできます。

   `https://primary_admin_node_ip:8443`

   ネットワーク設定に応じて、グリッドネットワーク上または管理ネットワーク上のプライマリ管理ノード IP の IP アドレスを使用できます。

2. StorageGRID システムのインストール * をクリックします。

   StorageGRID グリッドを設定するためのページが表示されます。




**StorageGRID** ライセンス情報の指定

## StorageGRID システムの名前を指定し、ネットアップから提供されたライセンスファイルをアップロードする必要があります。

手順

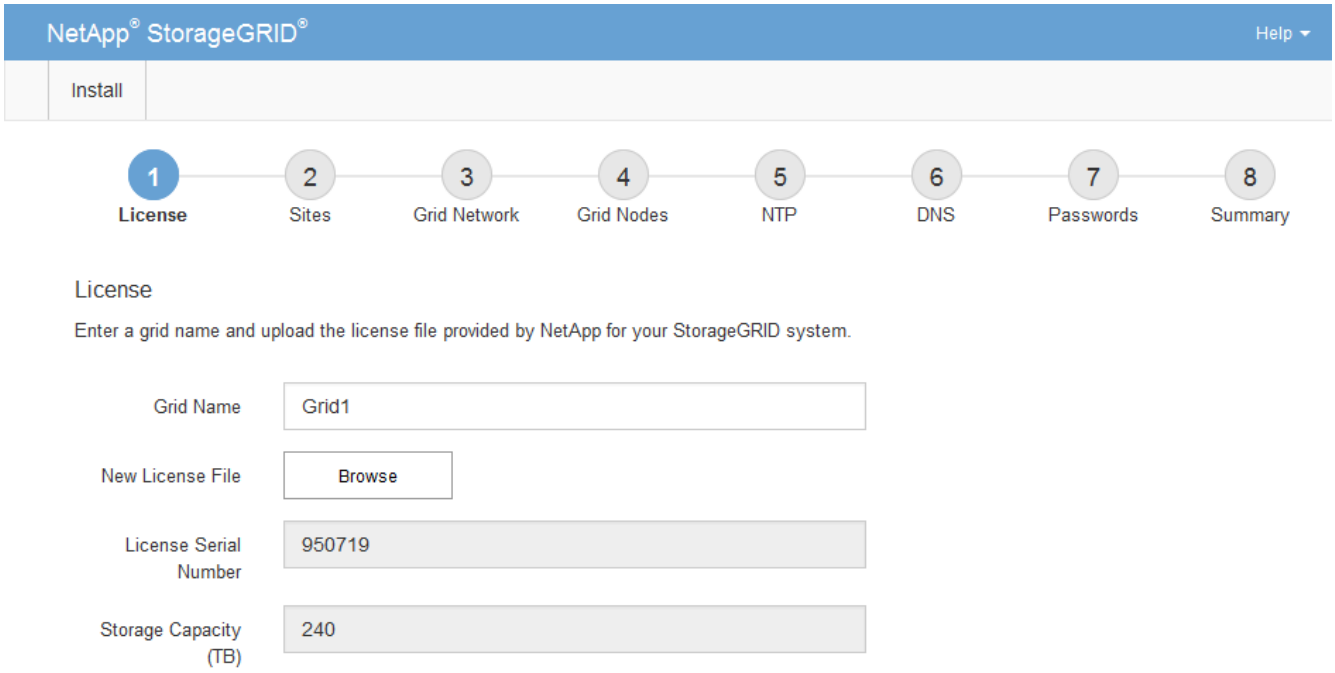
1. [ ライセンス ] ページで、 StorageGRID システムの名前として「 * グリッド名 * 」を入力します。

   インストール後、ノードメニューの上部に名前が表示されます。

2. [* Browse]をクリックして、ネットアップライセンスファイルを探します (`NLFunique_id.txt`）をクリックし、*開く*をクリックします。

   ライセンスファイルが検証され、シリアル番号とライセンスされたストレージ容量が表示されます。

   StorageGRID インストールアーカイブには、製品サポートのない無償ライセンスが含まれています。インストール後に、サポートを提供するライセンスに更新できます。




3. 「 * 次へ * 」をクリックします。

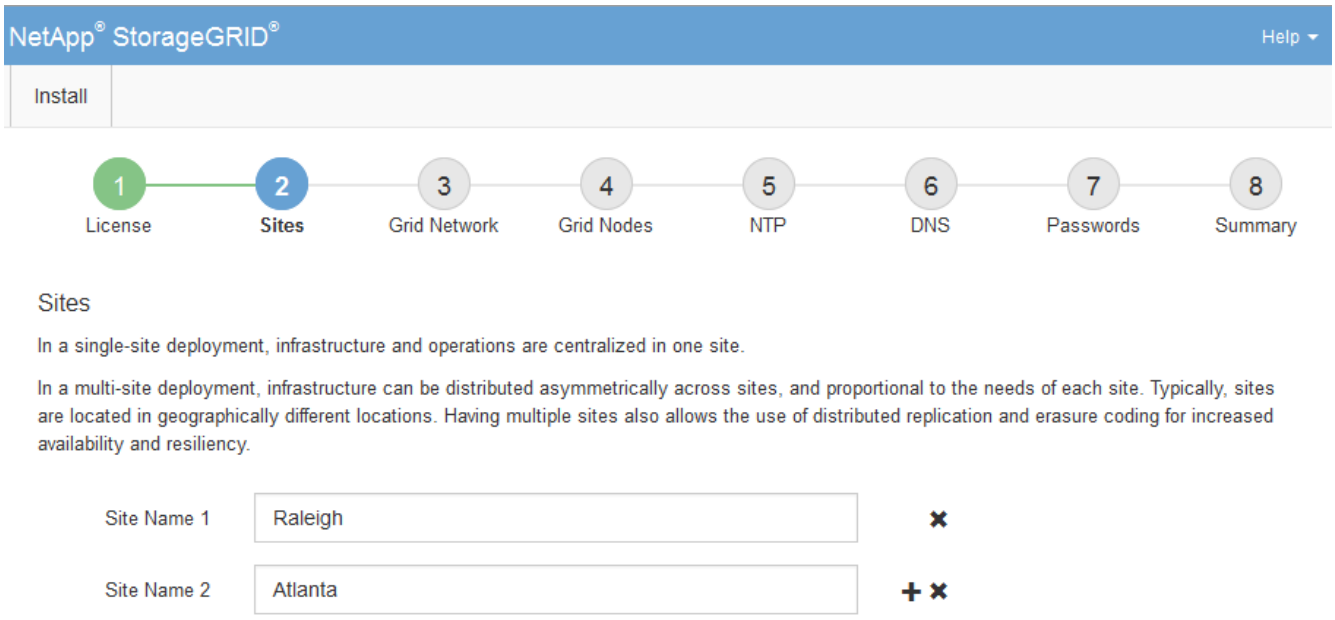
サイトの追加

## StorageGRID をインストールするときに、サイトを少なくとも 1 つ作成する必要があります。StorageGRID システムの信頼性を高め、ストレージ容量を増やすために、追加のサイトを作成することができます。

手順

1. [ サイト ] ページで、 * サイト名 * を入力します。
2. サイトを追加するには、最後のサイトエントリの横にあるプラス記号をクリックし、新しい * サイト名 * テキストボックスに名前を入力します。

   グリッドトポロジに必要な数のサイトを追加します。サイトは最大 16 個まで追加できます。




3. 「 * 次へ * 」をクリックします。

グリッドネットワークのサブネットの指定

## グリッドネットワークで使用されるサブネットを指定する必要があります。

このタスクについて

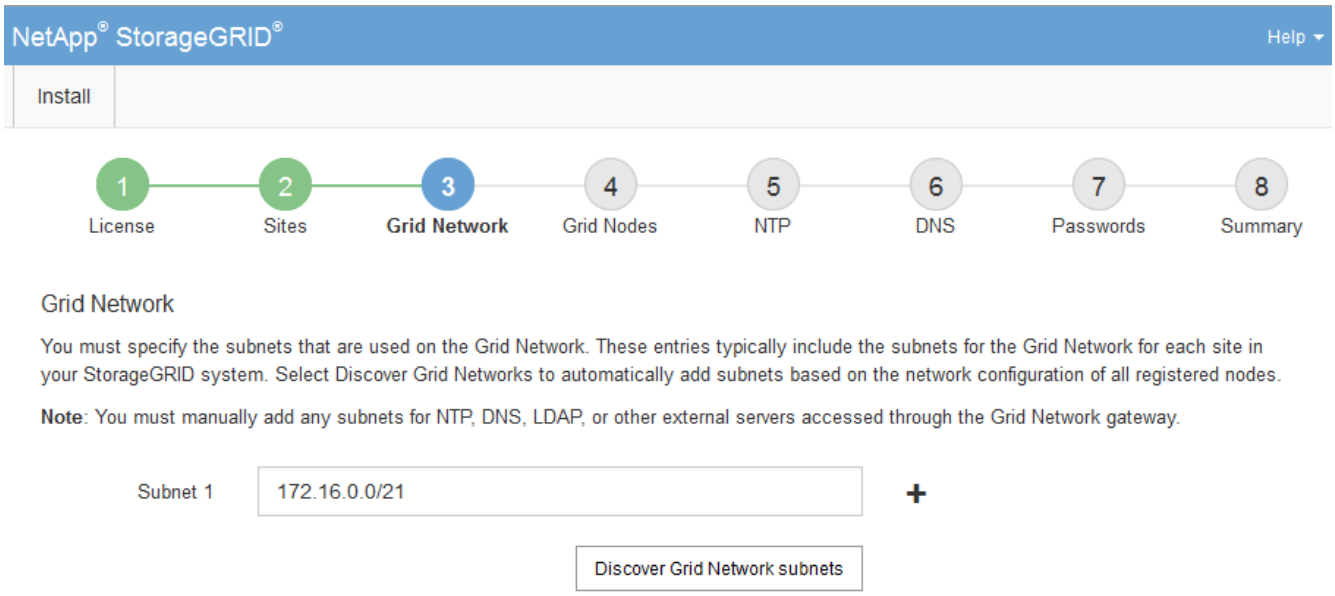
サブネットエントリには、 StorageGRID システム内の各サイトのグリッドネットワークのサブネット、およびグリッドネットワーク経由でアクセスできる必要があるサブネットが含まれます。

グリッドサブネットが複数ある場合は、グリッドネットワークゲートウェイが必要です。指定するすべてのグリッドサブネットが、このゲートウェイ経由でアクセス可能であることが必要です。

手順

1. [* サブネット 1*] テキストボックスで、少なくとも 1 つのグリッドネットワークの CIDR ネットワークアドレスを指定します。
2. 最後のエントリの横にあるプラス記号をクリックして、追加のネットワークエントリを追加します。

   少なくとも 1 つのノードがすでに導入されている場合は、 * グリッドネットワークのサブネットの検出 * をクリックすると、 Grid Manager に登録されているグリッドノードから報告されたサブネットが Grid ネットワークサブネットリストに自動的に追加されます。




3. 「 * 次へ * 」をクリックします。

保留中のグリッドノードを承認します

## 各グリッドノードは、 StorageGRID システムに追加する前に承認する必要があります。

必要なもの

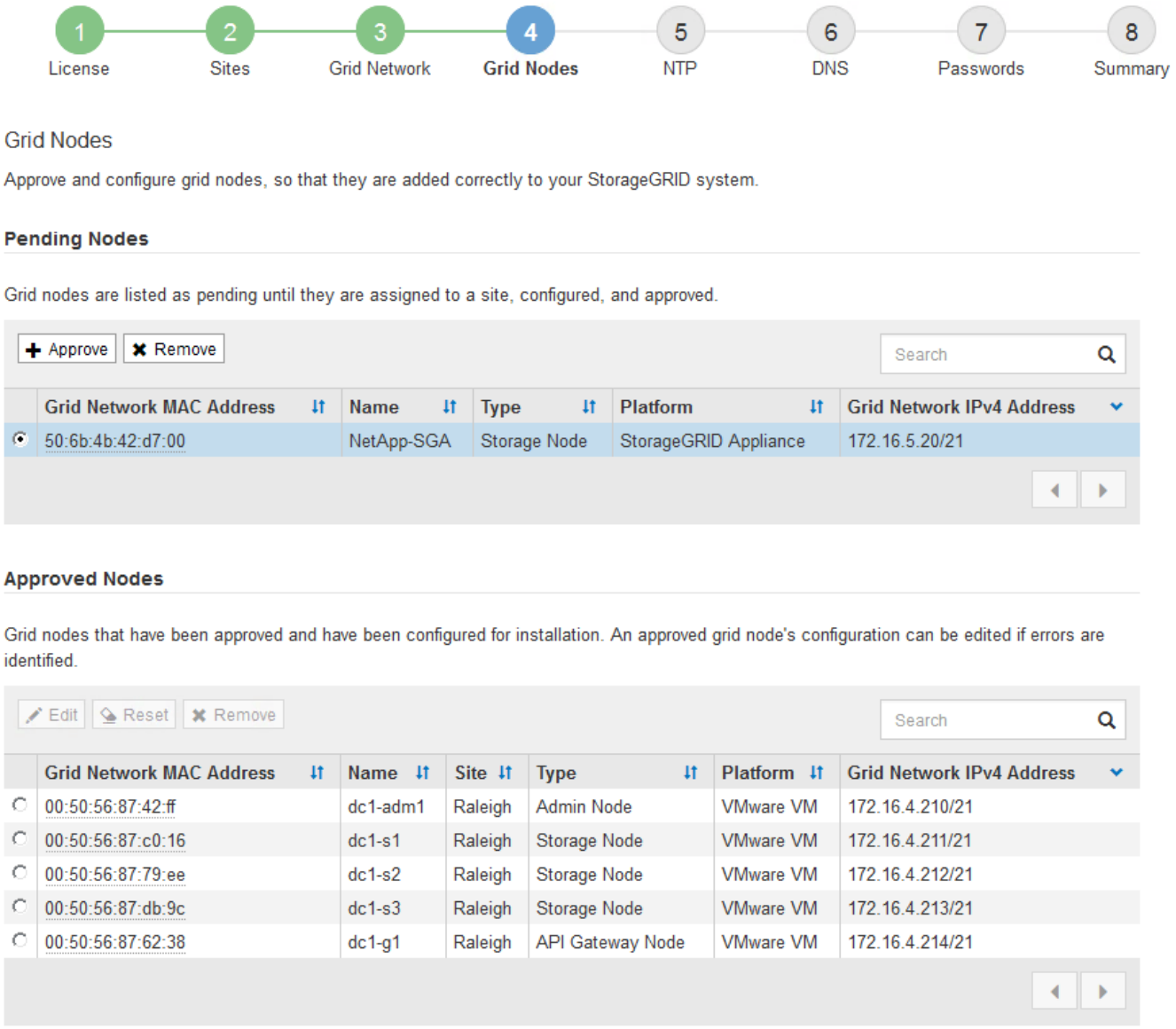
仮想アプライアンスおよびStorageGRID アプライアンスのグリッドノードをすべて導入しておく必要があります。

手順

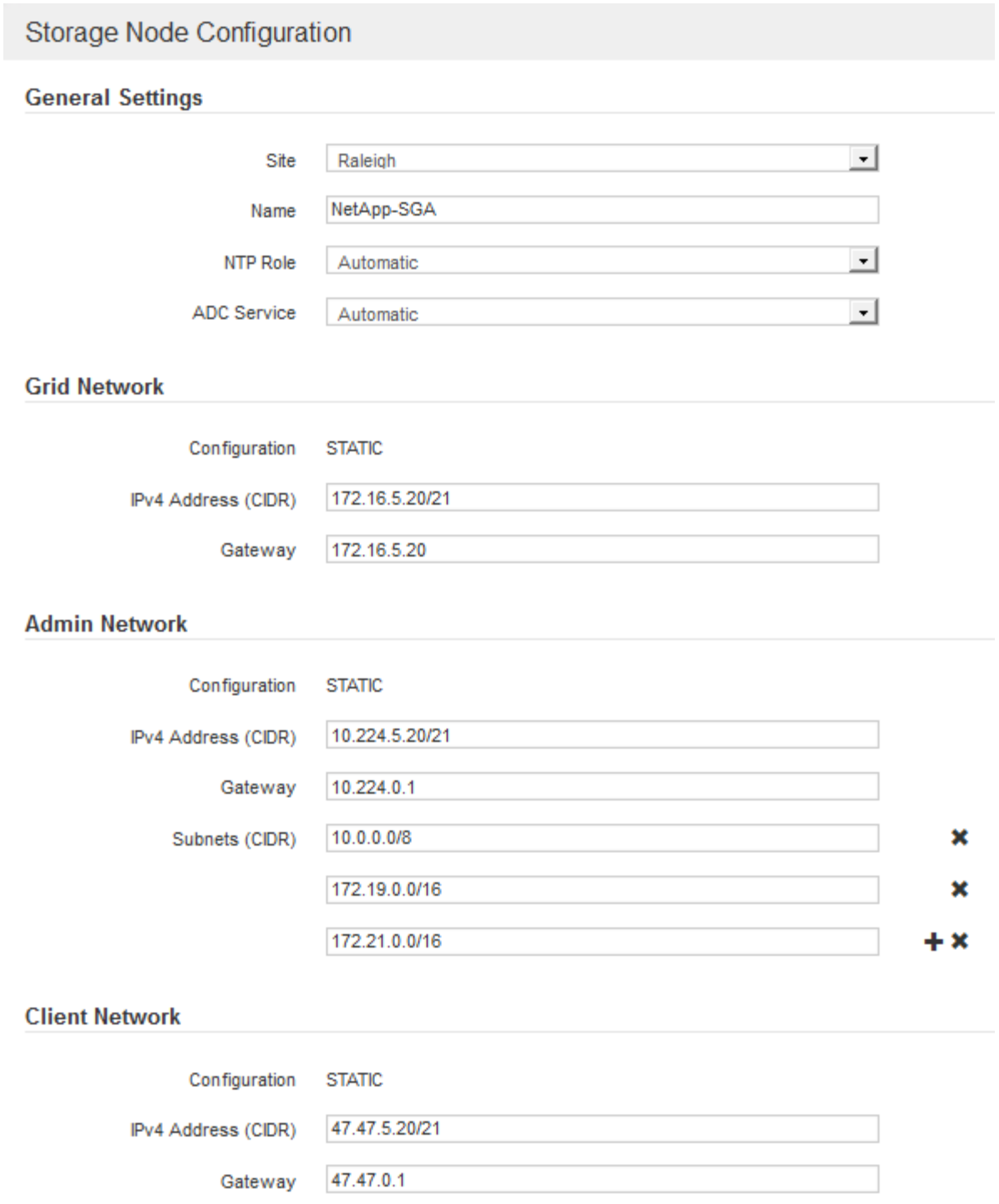
1. Pending 状態のノードのリストを確認し、導入したすべてのグリッドノードが表示されていることを確認します。

   見つからないグリッドノードがある場合は、正常に導入されたことを確認します。

2. 承認する保留中のノードの横にあるラジオボタンを選択します。




3. [ 承認（ Approve ） ] をクリックします
4. [ 一般設定 ] で、必要に応じて次のプロパティの設定を変更します。




◦ * Site * ：このグリッドノードが関連付けられるサイトの名前。

◦ * 名前 * ：ノードに割り当てられる名前。 Grid Manager に表示される名前。デフォルトでは、ノードの設定時に指定した名前が付けられます。インストールプロセスのこのステップでは、必要に応じて名前を変更できます。

インストールの完了後にノードの名前を変更することはできません。

VMware ノードの場合はここで名前を変更できますが、 vSphere で仮想マシンの名前は変更されません。

- * NTP Role * ：グリッドノードのネットワークタイムプロトコル（ NTP ）ロール。オプションは * Automatic * 、 * Primary * 、 * Client * です。「 * 自動」を選択すると、管理ノード、 ADC サービスを採用するストレージノード、ゲートウェイノード、および静的な IP アドレスでないグリッドノードにプライマリロールが割り当てられます。他のすべてのグリッドノードにはクライアントロールが割り当てられます。

  > 各サイトの少なくとも 2 つのノードが、少なくとも 4 つの外部 NTP ソースにアクセスできることを確認します。NTP ソースにアクセスできるノードがサイトに 1 つしかないと、そのノードがダウンした場合にタイミングの問題が生じます。また、各サイトで 2 つのノードをプライマリ NTP ソースとして指定することにより、サイトがグリッドの他の部分から分離されても、正確なタイミングが保証されます。

- * ADC service * （ストレージノードのみ）：「 * Automatic * 」を選択して、ノードに Administrative Domain Controller （ ADC ）サービスが必要かどうかをシステムに通知します。ADC サービスは、グリッドサービスの場所と可用性を追跡します。各サイトで少なくとも 3 つのストレージノードに ADC サービスが含まれている必要があります。導入後のノードに ADC サービスを追加することはできません。

5. グリッドネットワークで、必要に応じて次のプロパティの設定を変更します。

   - * IPv4 Address （ CIDR ） * ：グリッドネットワークインターフェイス（コンテナ内の eth0 ）の CIDR ネットワークアドレス。例： 192.168.1.234/21
   - * ゲートウェイ * ：グリッドネットワークゲートウェイ。例： 192.168.0.1

     > グリッドサブネットが複数ある場合は、ゲートウェイが必要です。

   > グリッドネットワーク設定で DHCP を選択した場合は、ここで値を変更すると、新しい値がノード上の静的アドレスとして設定されます。設定された IP アドレスが DHCP アドレスプールにないことを確認する必要があります。

6. グリッドノードの管理ネットワークを設定する場合は、必要に応じて管理ネットワークセクションで設定を追加または更新します。

   サブネット（ CIDR ） * テキストボックスに、このインターフェイスから発信されるルートの宛先サブネットを入力します。管理サブネットが複数ある場合は、管理ゲートウェイが必要です。

   > 管理ネットワーク設定で DHCP を選択した場合は、ここで値を変更すると、新しい値がノード上の静的アドレスとして設定されます。設定された IP アドレスが DHCP アドレスプールにないことを確認する必要があります。

   - アプライアンス： StorageGRID アプライアンスでは、 StorageGRID アプライアンスインストーラを使用した初回インストール時に管理ネットワークが設定されなかった場合、このグリッドマネージャのダイアログボックスで管理ネットワークを設定することはできません。代わりに、次の手順を実行する必要があります。

     a. アプライアンスをリブートします。アプライアンスインストーラで、 * Advanced * > * Reboot * を選択します。

        リブートには数分かかることがあります。

     b. [Configure Networking*] > [**Link Configuration**] を選択し、適切なネットワークを有効にします。

c. [Configure Networking*]>[**IP Configuration**] を選択し、有効なネットワークを設定します。

d. ホームページに戻り、「インストールの開始」をクリックします。

e. Grid Manager で、ノードが承認済みノード（ Approved Nodes ）テーブルにリストされている場合は、ノードをリセットします。

f. Pending Nodes テーブルからノードを削除します。

g. ノードが Pending Nodes リストに再表示されるまで待ちます。

h. 適切なネットワークを設定できることを確認します。IP Configuration ページで指定した情報があらかじめ入力されている必要があります。

追加情報 の場合は、使用しているアプライアンスモデルのインストールとメンテナンスの手順を参照してください。

7. グリッドノードのクライアントネットワークを設定する場合は、必要に応じてクライアントネットワークセクションで設定を追加または更新します。クライアントネットワークを設定する場合はゲートウェイが必要になります。これは、インストール後にノードのデフォルトゲートウェイになります。

クライアントネットワーク設定で DHCP を選択した場合は、ここで値を変更すると、新しい値がノード上の静的アドレスとして設定されます。設定された IP アドレスが DHCP アドレスプールにないことを確認する必要があります。

◦ アプライアンス： StorageGRID アプライアンスでは、 StorageGRID アプライアンスインストーラを使用した初回インストール時にクライアントネットワークが設定されなかった場合、このグリッドマネージャのダイアログボックスでクライアントネットワークを設定することはできません。代わりに、次の手順を実行する必要があります。

a. アプライアンスをリブートします。アプライアンスインストーラで、 * Advanced * > * Reboot * を選択します。

リブートには数分かかることがあります。

b. [Configure Networking*] > [**Link Configuration**] を選択し、適切なネットワークを有効にします。

c. [Configure Networking*]>[**IP Configuration**] を選択し、有効なネットワークを設定します。

d. ホームページに戻り、「インストールの開始」をクリックします。

e. Grid Manager で、ノードが承認済みノード（ Approved Nodes ）テーブルにリストされている場合は、ノードをリセットします。

f. Pending Nodes テーブルからノードを削除します。

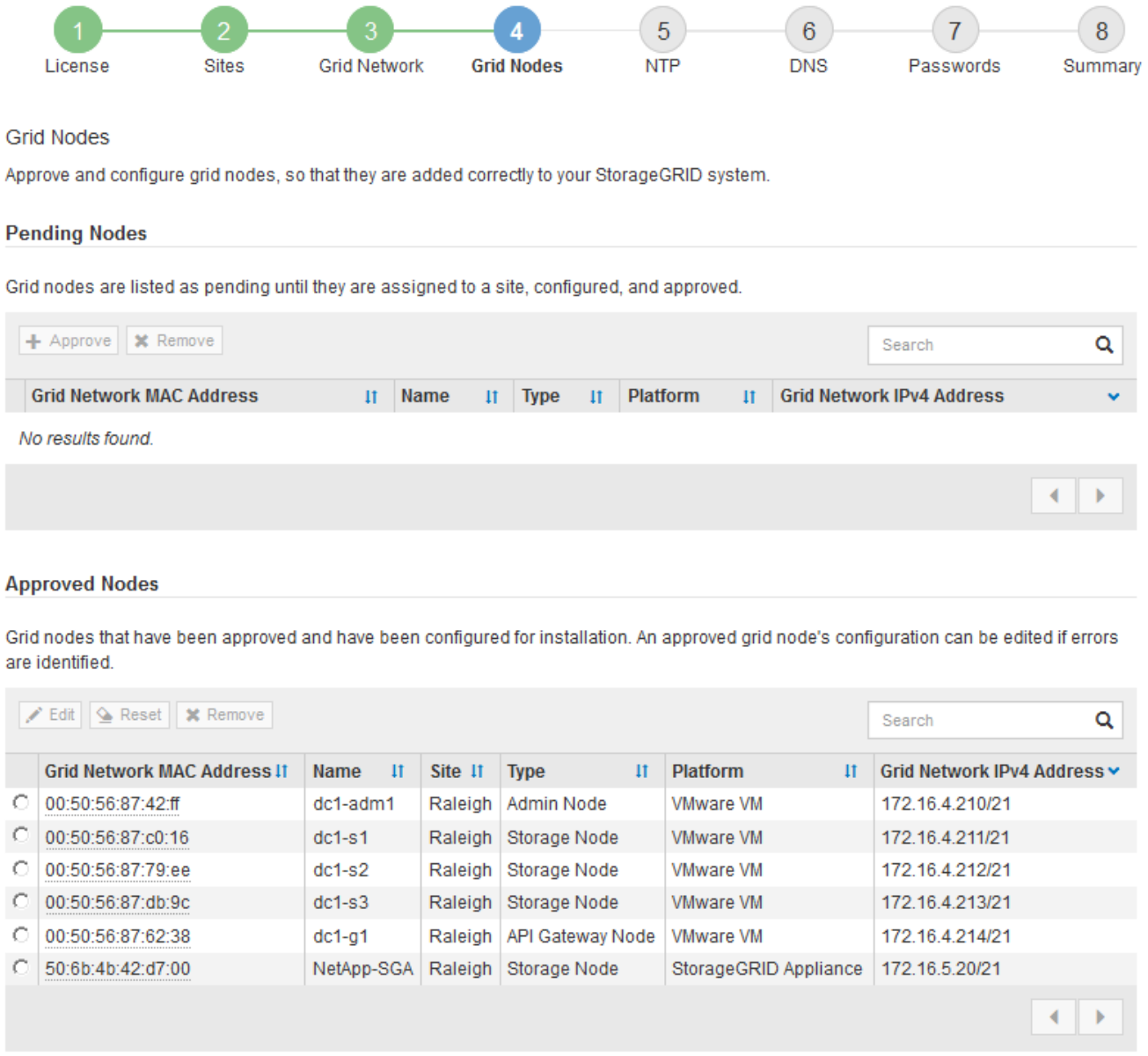
g. ノードが Pending Nodes リストに再表示されるまで待ちます。

h. 適切なネットワークを設定できることを確認します。IP Configuration ページで指定した情報があらかじめ入力されている必要があります。

追加情報 の場合は、使用しているアプライアンスのインストールとメンテナンスの手順を参照してください。

8. [ 保存（ Save ） ] をクリックします。

グリッドノードエントリが [ 承認済みノード（ Approved Nodes ） ] リストに移動します。




9. 承認する保留中のグリッドノードごとに、上記の手順を繰り返します。

   グリッドに必要なすべてのノードを承認する必要があります。ただし、サマリページで * インストール * をクリックする前に、いつでもこのページに戻ることができます。承認済みグリッドノードのプロパティを変更するには、ラジオボタンを選択し、 * 編集 * をクリックします。

10. グリッドノードの承認が完了したら、 * 次へ * をクリックします。

### Network Time Protocolサーバ情報の指定

別々のサーバで実行された処理を常に同期された状態にするには、 StorageGRID システムの NTP 設定情報を指定する必要があります。

このタスクについて

NTP サーバの IPv4 アドレスを指定する必要があります。

外部 NTP サーバを指定する必要があります。指定した NTP サーバで NTP プロトコルが使用されている必要

があります。

時間のずれに伴う問題を防ぐには、 Stratum 3 またはそれより上位の NTP サーバ参照を 4 つ指定する必要があります。

> 本番レベルの StorageGRID インストール環境で外部 NTP ソースを指定する場合は、 Windows Server 2016 より前のバージョンの Windows で Windows Time （ W32Time ）サービスを使用しないでください。以前のバージョンの Windows のタイムサービスは精度が十分でないため、 StorageGRID などの高精度環境での使用は Microsoft でサポートされていません。

"高精度環境用に Windows タイムサービスを構成するためのサポート境界"

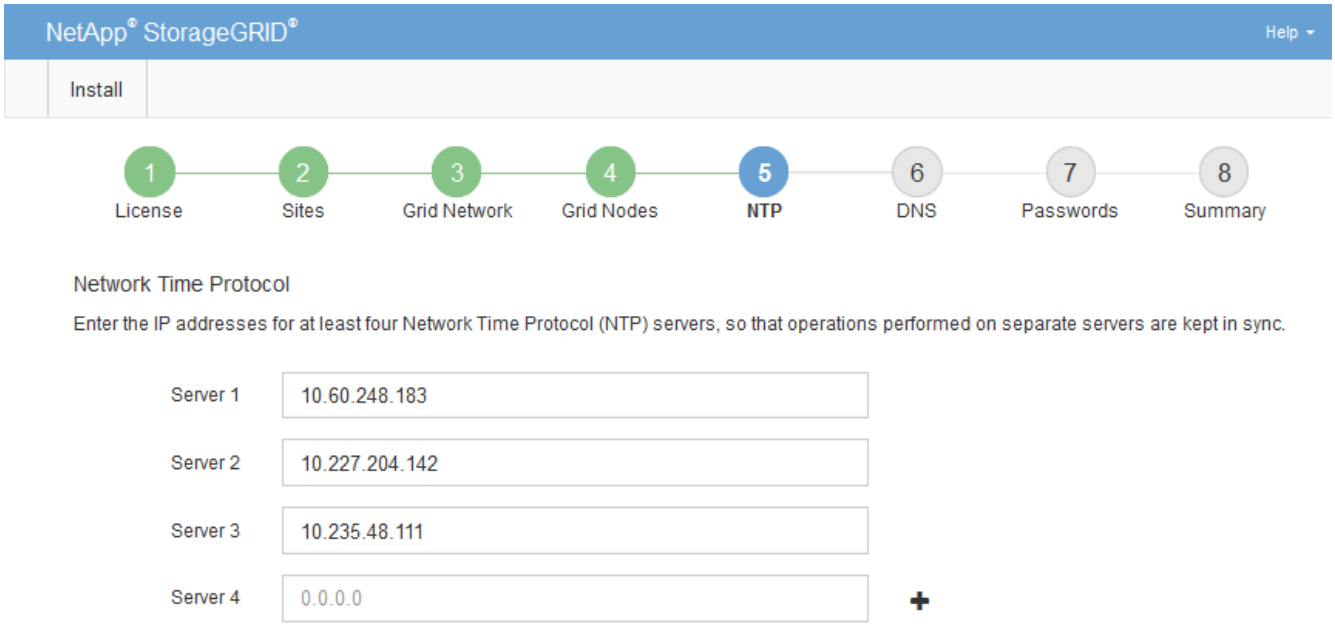
外部 NTP サーバは、以前にプライマリ NTP ロールを割り当てていたノードによって使用されます。

> 各サイトの少なくとも 2 つのノードが、少なくとも 4 つの外部 NTP ソースにアクセスできることを確認します。NTP ソースにアクセスできるノードがサイトに 1 つしかないと、そのノードがダウンした場合にタイミングの問題が生じます。また、各サイトで 2 つのノードをプライマリ NTP ソースとして指定することにより、サイトがグリッドの他の部分から分離されても、正確なタイミングが保証されます。

VMware に関する追加のチェックを実行します。たとえば、ハイパーバイザーが仮想マシンと同じ NTP ソースを使用していることを確認したり、 VMTools を使用してハイパーバイザーと StorageGRID 仮想マシン間の時刻同期を無効にしたりします。

手順

1. [* サーバー 1 * から * サーバー 4 * ] テキストボックスに、少なくとも 4 つの NTP サーバーの IPv4 アドレスを指定します。
2. 必要に応じて、最後のエントリの横にあるプラス記号を選択して、サーバエントリを追加します。




3. 「 * 次へ * 」を選択します。

**Domain Name System**サーバ情報の指定

# IP アドレスの代わりにホスト名を使用して外部サーバにアクセスできるようにするには、 StorageGRID システムの DNS 情報を指定する必要があります。

このタスクについて

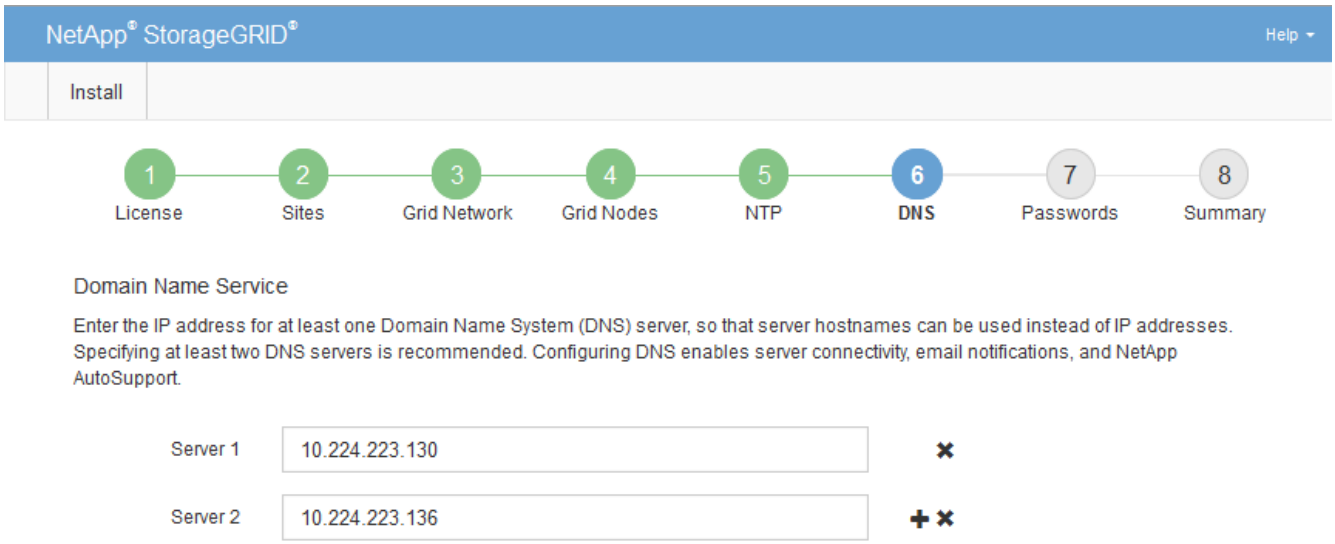
DNS サーバ情報を指定すると、 E メール通知や AutoSupport に、 IP アドレスではなく Fully Qualified Domain Name （ FQDN ；完全修飾ドメイン名）ホスト名を使用できます。DNS サーバは少なくとも 2 つ指定することを推奨します。

> DNS サーバの IPv4 アドレスは 2~6 個指定します。ネットワーク分離が発生した場合に各サイトがローカルにアクセスできる DNS サーバを選択する必要があります。これにより、分離されたサイトは引き続き DNS サービスにアクセスできます。グリッド全体の DNS サーバリストを設定したあとに、ノードごとに DNS サーバリストをカスタマイズできます。詳細については、リカバリおよびメンテナンスの手順にある DNS 設定の変更に関する情報を参照してください。

DNS サーバ情報を省略したり誤って設定したりすると、各グリッドノードの SSM サービスで DNST アラームがトリガーされます。このアラームは、 DNS が正しく設定され、新しいサーバ情報がすべてのグリッドノードに配信された時点で解除されます。

手順

1. 「 * サーバー 1 * 」テキストボックスで、少なくとも 1 つの DNS サーバーの IPv4 アドレスを指定します。
2. 必要に応じて、最後のエントリの横にあるプラス記号を選択して、サーバエントリを追加します。




少なくとも 2 つの DNS サーバを指定することを推奨します。DNS サーバは 6 つまで指定できます。

3. 「 * 次へ * 」を選択します。

関連情報

""

**StorageGRID** システムのパスワードの指定

# StorageGRID システムのインストールの一環として、システムの保護とメンテナンス作業に使用するパスワードを入力する必要があります。

このタスクについて

Install Passwords ページを使用して、プロビジョニングパスフレーズとグリッド管理 root ユーザのパスワードを指定します。

- プロビジョニングパスフレーズは暗号化キーとして使用され、 StorageGRID システムでは格納されません。
- リカバリパッケージのダウンロードなど、インストール、拡張、メンテナンスの手順用のプロビジョニングパスフレーズが必要です。そのため、プロビジョニングパスフレーズは安全な場所に保存しておくことが重要です。
- 現在のプロビジョニングパスフレーズがある場合は、 Grid Manager からプロビジョニングパスフレーズを変更できます。
- Grid 管理 root ユーザのパスワードは Grid Manager を使用して変更できる。
- ランダムに生成されたコマンドラインコンソールおよびSSHパスワードは、に格納されます `Passwords.txt` リカバリパッケージ内のファイル。

手順

1. 「 * プロビジョニングパスフレーズ * 」に、 StorageGRID システムのグリッドトポロジを変更するために必要なプロビジョニングパスフレーズを入力します。

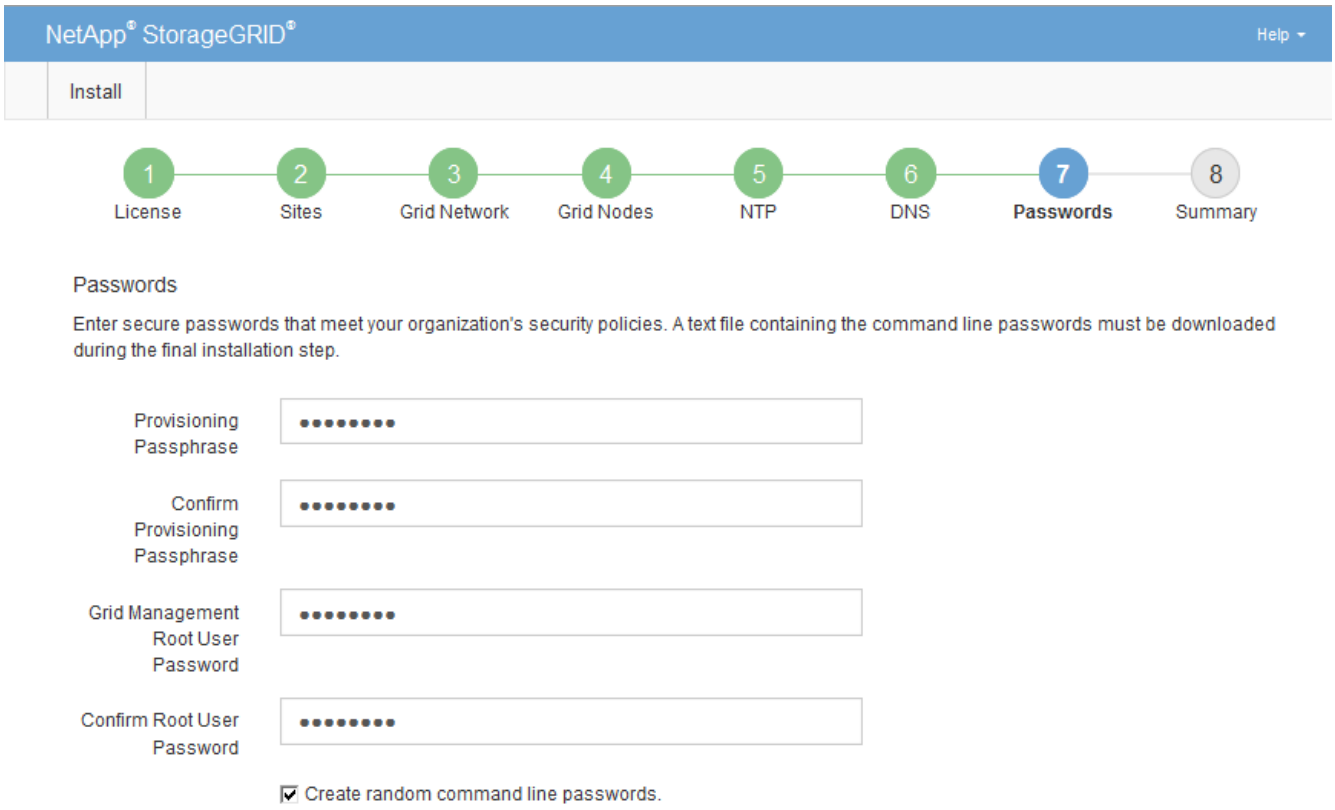
   プロビジョニングパスフレーズは安全な場所に保存してください。

   > インストールの完了後にプロビジョニングパスフレーズを変更する場合は、 Grid Manager を使用してください。[構成（Configuration ）]>[*アクセス制御（* Access Control ）]>[ Gridパスワード*（* Grid

2. [Confirm Provisioning Passphrase* （プロビジョニングパスフレーズの確認） ] にプロビジョニングパスフレーズを再入力して確定します。
3. * Grid Management Root User Password * に、 Grid Manager に「 root 」ユーザとしてアクセスするために使用するパスワードを入力します。

   パスワードは安全な場所に保管してください。

4. Confirm Root User Password * で、 Grid Manager のパスワードを再入力して確認します。




5. コンセプトの実証やデモを目的としてグリッドをインストールする場合は、必要に応じて、 * ランダムなコマンドラインパスワードの作成 * チェックボックスの選択を解除します。

   本番環境では、セキュリティ上の理由から常にランダムパスワードを使用する必要があります。デフォルトのパスワードを使用してコマンドラインから "root" または "admin" アカウントを使用してグリッドノードにアクセスする場合は、デモ用グリッドの * ランダムなコマンドラインパスワードの作成 * のみを選択解除します。

   リカバリパッケージファイルをダウンロードするように求められます (`sgws-recovery-package-id-revision.zip`)サマリページで*Install*をクリックした後。インストールを完了するには、このファイルをダウンロードする必要があります。システムへのアクセスに必要なパスワードは、に保存されています `Passwords.txt` リカバリパッケージファイルに含まれているファイル。

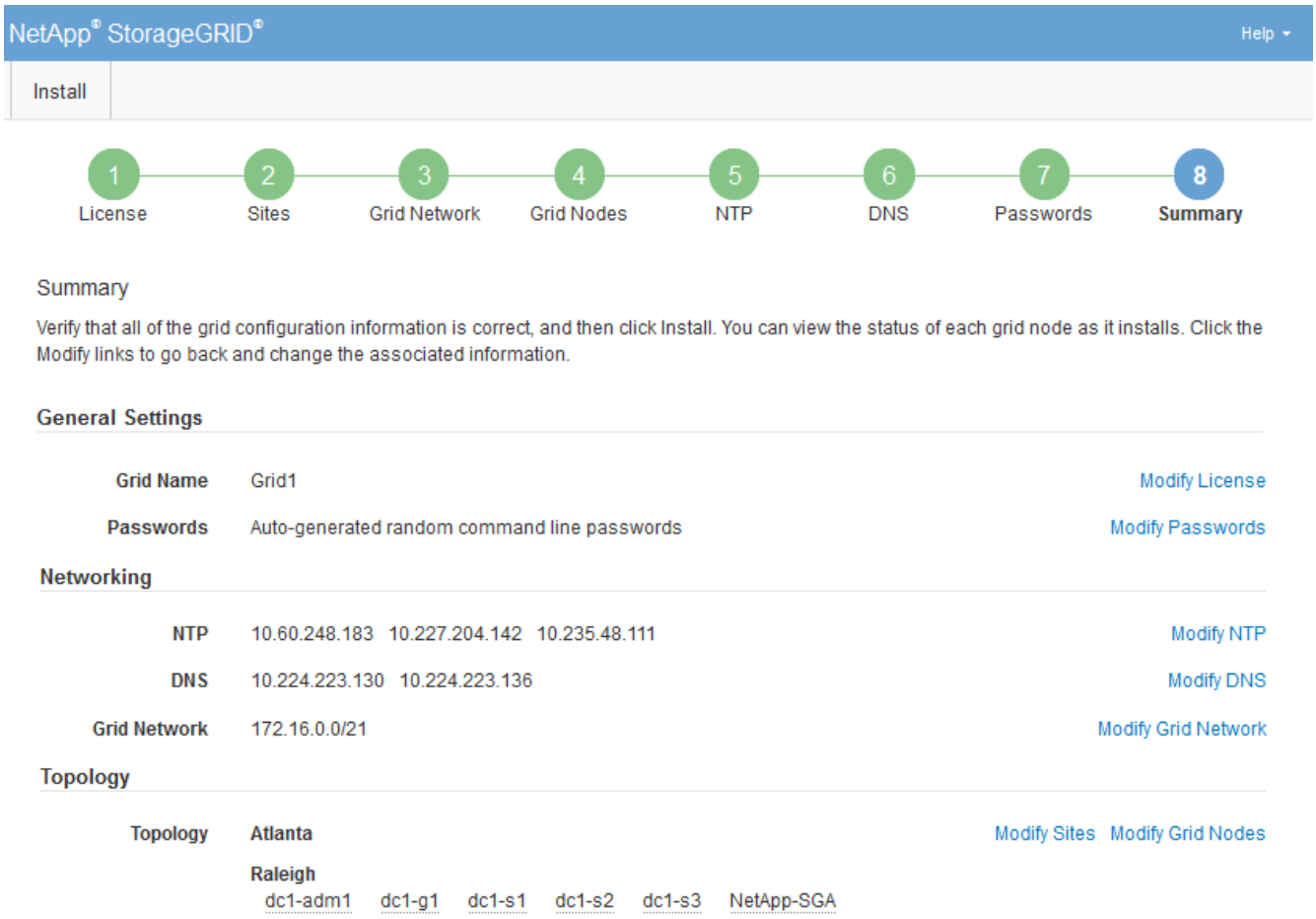
6. 「 * 次へ * 」をクリックします。

設定を確認し、インストールを完了します

インストールを正常に完了するために、入力した設定情報をよく確認する必要があります。

手順

1. 「 * 概要 * 」ページを表示します。




2. グリッドの設定情報がすべて正しいことを確認します。Summary （サマリ）ページの Modify （変更）リンクを使用して、戻ってエラーを修正します。
3. 「 * Install * 」をクリックします。

> クライアントネットワークを使用するようにノードが設定されている場合、 * Install * をクリックすると、そのノードのデフォルトゲートウェイがグリッドネットワークからクライアントネットワークに切り替わります。接続を失った場合は、アクセス可能なサブネット経由でプライマリ管理ノードにアクセスしていることを確認する必要があります。を参照してください "ネットワークのガイドライン" を参照してください。

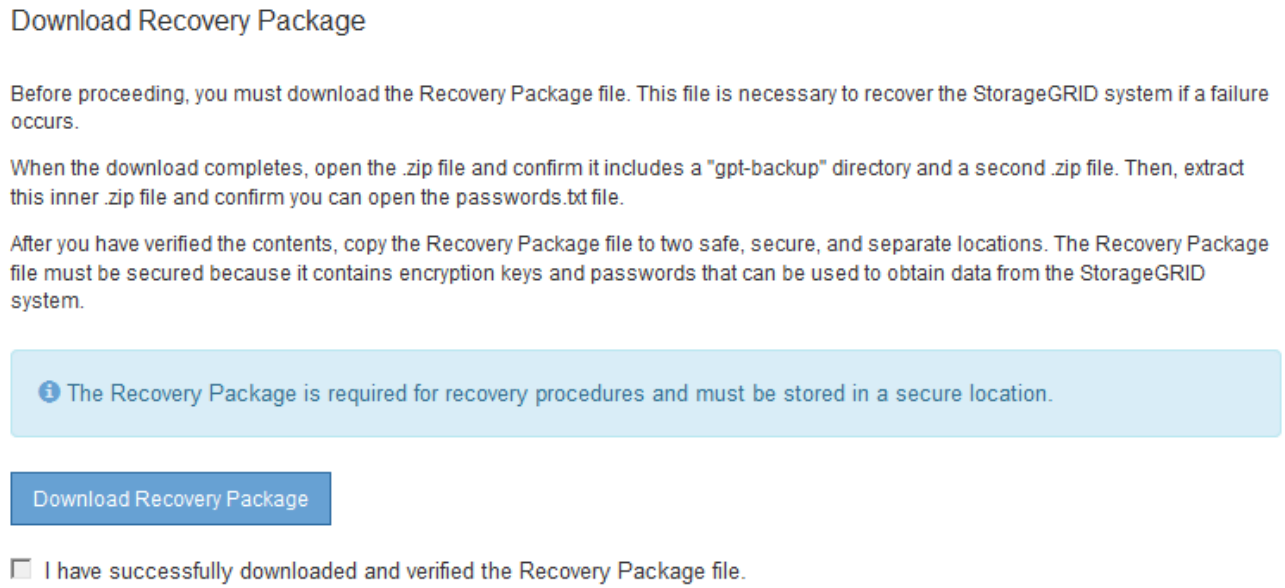
4. [ リカバリパッケージのダウンロード ] をクリックします。

   グリッドトポロジを定義するポイントまでインストールが進むと、リカバリパッケージファイルをダウンロードするように求められます (`.zip`) をクリックし、このファイルの内容に正常にアクセスできることを確認します。リカバリパッケージファイルのダウンロードが必要となるのは、グリッドノードで障害が発生した場合に StorageGRID システムをリカバリできるようにするためです。インストールはバックグラウンドで続行されますが、このファイルをダウンロードして検証するまでは、インストールを完了して StorageGRID システムにアクセスすることができません。

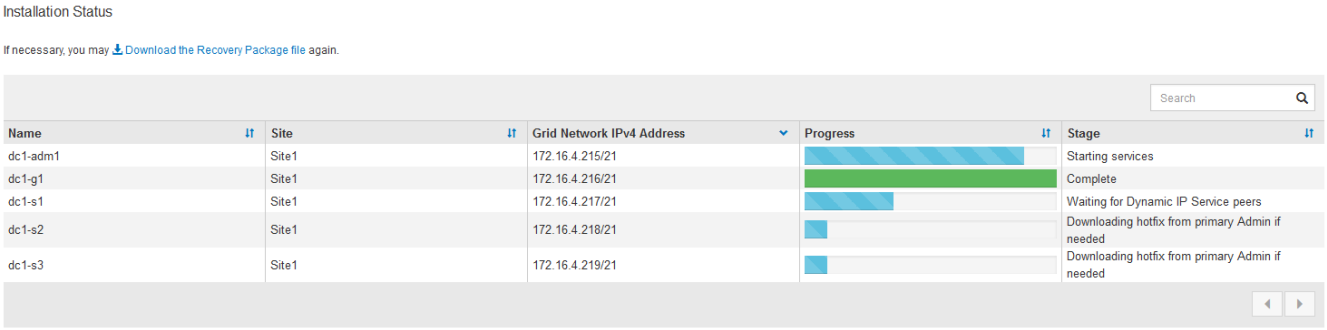
5. の内容を展開できることを確認します `.zip` ファイルを作成し、安全で安全な2つの場所に保存します。

> リカバリパッケージファイルには StorageGRID システムからデータを取得するための暗号キーとパスワードが含まれているため、安全に保管する必要があります。

6. [I have successfully downloaded and verified the Recovery Package file*] チェックボックスをオンにし、 [ 次へ ] をクリックします。




インストールがまだ進行中の場合は、ステータスページが表示されます。このページには、グリッドノードごとのインストールの進捗状況が表示されます。




すべてのグリッドノードが完了ステージに到達すると、 Grid Manager のサインインページが表示されます。

7. 「 root 」ユーザとインストール時に指定したパスワードを使用して Grid Manager にサインインします。

インストール後のガイドライン

## グリッドノードの導入と設定が完了したら、 DHCP アドレスおよびネットワーク設定の変更について、次のガイドラインに従ってください。

- DHCP を使用して IP アドレスを割り当てた場合は、使用しているネットワーク上の各 IP アドレスに対して DHCP 予約を設定します。

  DHCP は導入フェーズでのみ設定できます。設定時に DHCP を設定することはできません。

  IP アドレスが変わるとノードがリブートします。 DHCP アドレスの変更が同時に複数のノードに影響を及ぼす場合、原因 が停止する可能性があります。

- グリッドノードの IP アドレス、サブネットマスク、およびデフォルトゲートウェイを変更する場合は、IP 変更手順を使用する必要があります。リカバリとメンテナンスの手順のIPアドレスの設定に関する情報を参照してください。
- ルーティングやゲートウェイの変更など、ネットワーク設定を変更すると、プライマリ管理ノードおよびその他のグリッドノードへのクライアント接続が失われる可能性があります。ネットワークの変更内容によっては、接続の再確立が必要になる場合があります。

## インストールの自動化

### VMware仮想グリッドノードの導入、グリッドノードの設定、およびStorageGRID アプライアンスの設定を自動化することができます。

- "VMware vSphereへのグリッドノード導入の自動化"
- "StorageGRID の設定の自動化"

#### **VMware vSphere**へのグリッドノード導入の自動化

### VMware vSphereへのStorageGRID グリッドノードの導入を自動化することができます。

必要なもの

- Bash 3.2 以降が搭載された Linux / UNIX システムにアクセスできるようにしておきます。
- VMware OVF Tool 4.1 をインストールし、正しく設定しておきます。
- OVF Tool を使用して VMware vSphere にアクセスするために必要なユーザ名とパスワードを確認しておきます。
- StorageGRID 仮想マシンを導入する vSphere 内の場所の仮想インフラ（ VI ） URL を確認しておきます。この URL は通常、 vApp またはリソースプールです。例：
  `vi://vcenter.example.com/vi/sgws`

  VMwareを使用できます `ovftool` この値を決定するユーティリティ（を参照） `ovftool` 詳細についてはドキュメントを参照してください）。

  vApp に導入する場合、初回は仮想マシンが自動的に起動されないため、手動で電源をオンにする必要があります。

- 構成ファイルに必要なすべての情報を収集しておきます。を参照してください "導入環境に関する情報を収集" を参照してください。
- VMware 用インストールアーカイブに含まれている次のファイルに StorageGRID からアクセスできるようにしておきます。

| ファイル名 | 説明 |
| --- | --- |
| NetApp-SG-version-sha.vmdk | グリッドノード仮想マシンを作成するためのテンプレートとして使用される仮想マシンディスクファイル。<br><br>*注意：*このファイルはと同じフォルダになければなりません `.ovf` および `.mf` ファイル。 |
| vsphere-primary-admin.ovf vsphere-primary-admin.mf | Open Virtualization Formatテンプレートファイル (`.ovf`)とマニフェストファイル (`.mf`）を使用してください。 |
| vsphere-non-primary-admin.ovf vsphere-non-primary-admin.mf | テンプレートファイル (`.ovf`)とマニフェストファイル (`.mf`）。非プライマリ管理ノードを導入する場合に使用します。 |
| vsphere-archive.ovf vsphere-archive.mf | テンプレートファイル (`.ovf`)とマニフェストファイル (`.mf`）を使用してアーカイブノードを導入します。 |
| vsphere-gateway.ovf vsphere-gateway.mf | テンプレートファイル (`.ovf`)とマニフェストファイル (`.mf`）を選択します。 |
| vsphere-storage.ovf vsphere-storage.mf | テンプレートファイル (`.ovf`)とマニフェストファイル (`.mf`）を選択します。 |
| deploy-vsphere-ovftool.sh | 仮想グリッドノードの導入を自動化するための Bash シェルスクリプト。 |
| deploy-vsphere-ovftool-sample.ini | で使用するサンプル構成ファイル `deploy-vsphere-ovftool.sh` スクリプト： |

導入用の構成ファイルを定義しています

StorageGRID の仮想グリッドノードを導入するために必要な情報を構成ファイルで指定します。このファイルは、で使用されます `deploy-vsphere-ovftool.sh` bashスクリプト。サンプル構成ファイルを変更して、ファイルをゼロから作成する必要がないようにすることができます。

手順

1. サンプル構成ファイルのコピーを作成します (`deploy-vsphere-ovftool.sample.ini`）。新しいファイルをという名前で保存します `deploy-vsphere-ovftool.ini` と同じディレクトリ内にあります `deploy-vsphere-ovftool.sh`。
2. を開きます `deploy-vsphere-ovftool.ini`。
3. VMware 仮想グリッドノードを導入するために必要なすべての情報を入力します。

を参照してください "構成ファイルの設定" を参照してください。

4. 必要な情報をすべて入力して確認したら、ファイルを保存して閉じます。

構成ファイルの設定

## 。 deploy-vsphere-ovftool.ini 構成ファイルには、仮想グリッドノードを導入するために必要な設定が含まれています。

構成ファイルでは、最初にグローバルパラメータがリストされ、そのあとにノード名で定義されるセクションにノード固有のパラメータがリストされます。ファイルの使用状況：

- *Global parameters* は、すべてのグリッドノードに適用されます。
- _Node-specific parameters_override グローバルパラメータ。

グローバルパラメータ

グローバルパラメータは、個々のセクションの設定で上書きされないかぎり、すべてのグリッドノードに適用されます。複数のノードに適用するパラメータをグローバルパラメータセクションに配置し、個々のノードのセクションで必要に応じてこれらの設定を上書きします。

- * OVFTOOL_ARGUMENTS * ： OVFTOOL_ARGUMENTS をグローバル設定として指定するか、または特定のノードに個別に引数を適用できます。例：

```
OVFTOOL_ARGUMENTS = --powerOn --noSSLVerify --diskMode=thin
--datastore='<em>datastore_name</em>'
```

  を使用できます `--powerOffTarget` および `--overwrite` 既存の仮想マシンをシャットダウンおよび交換するオプション。

  ⓘ ノードを別々のデータストアに導入し、 OVFTOOL_ARGUMENTS をグローバルに指定するのではなくノードごとに指定する必要があります。

- * source *：StorageGRID 仮想マシン・テンプレートへのパス (`.vmdk`)ファイルと `.ovf` および `.mf` 個々のグリッドノードのファイル。デフォルトでは現在のディレクトリに設定されます。

```
SOURCE = /downloads/StorageGRID-Webscale-<em>version</em>/vsphere
```

- * target * ： StorageGRID の導入先となる VMware vSphere 仮想インフラ（ vi ）の URL 。例：

```
TARGET = vi://vcenter.example.com/vm/sgws
```

- * GRID_NETWORK_CONFIG * ：静的または DHCP のいずれかの IP アドレスの取得に使用される方法。デフォルトは「 STATIC 」です。全ノードまたはほとんどのノードが IP アドレスの取得に同じ方法を使用する場合は、ここでその方法を指定できます。その後、個々のノードで別々の設定を指定してグローバル設定を上書きできます。例：

```
GRID_NETWORK_CONFIG = DHCP
```

- * GRID_NETWORK_TARGET * ：グリッドネットワークに使用される既存の VMware ネットワークの名前。全ノードまたはほとんどのノードが同じネットワーク名を使用する場合は、ここでその名前を指定できます。その後、個々のノードで別々の設定を指定してグローバル設定を上書きできます。例：

```
GRID_NETWORK_TARGET = SG-Admin-Network
```

- * GRID_NETWORK_MASK * ：グリッドネットワークのネットワークマスク。全ノードまたはほとんどのノードが同じネットワークマスクを使用する場合は、ここでそのネットワークマスクを指定できます。その後、個々のノードで別々の設定を指定してグローバル設定を上書きできます。例：

```
GRID_NETWORK_MASK = 255.255.255.0
```

- * GRID_NETWORK_GATEWAY * ：グリッドネットワークのネットワークゲートウェイ。全ノードまたはほとんどのノードが同じネットワークゲートウェイを使用する場合は、ここでそのネットワークゲートウェイを指定できます。その後、個々のノードで別々の設定を指定してグローバル設定を上書きできます。例：

```
GRID_NETWORK_GATEWAY = 10.1.0.1
```

- * GRID_NETWORK_MTU * ：オプション。グリッドネットワークでの最大伝送ユニット（ MTU ）です。この値を指定する場合、 1280 ～ 9216 の範囲で指定する必要があります。例：

```
GRID_NETWORK_MTU = 8192
```

省略すると 1400 に設定されます。

ジャンボフレームを使用する場合は、 MTU を 9000 などのジャンボフレームに適した値に設定します。それ以外の場合は、デフォルト値のままにします。

> ネットワークの MTU 値は、ノードが接続されているスイッチポートに設定されている値と同じである必要があります。そうしないと、ネットワークパフォーマンスの問題やパケット損失が発生する可能性があります。

> ネットワークのパフォーマンスを最大限に高めるには、すべてのノードのグリッドネットワークインターフェイスで MTU 値がほぼ同じになるように設定する必要があります。個々のノードのグリッドネットワークの MTU 設定に大きな違いがある場合は、 * Grid Network MTU mismatch * アラートがトリガーされます。MTU 値はすべてのネットワークタイプで同じである必要はありません。

- * ADMIN_NETWORK_CONFIG * ： IP アドレスの取得に使用された方法。無効、静的、または DHCP のいずれかです。デフォルトは disabled です。全ノードまたはほとんどのノードが IP アドレスの取得に同じ方法を使用する場合は、ここでその方法を指定できます。その後、個々のノードで別々の設定を指定し

てグローバル設定を上書きできます。例：

```
ADMIN_NETWORK_CONFIG = STATIC
```

- * ADMIN_NETWORK_TARGET * ：管理ネットワークに使用する既存の VMware ネットワークの名前。この設定は、管理ネットワークが無効になっていない場合に必要となります。全ノードまたはほとんどのノードが同じネットワーク名を使用する場合は、ここでその名前を指定できます。その後、個々のノードで別々の設定を指定してグローバル設定を上書きできます。例：

```
ADMIN_NETWORK_TARGET = SG-Admin-Network
```

- * ADMIN_NETWORK_MASK * ：管理ネットワークのネットワークマスク。この設定は、静的 IP アドレスを使用する場合に必要となります。全ノードまたはほとんどのノードが同じネットワークマスクを使用する場合は、ここでそのネットワークマスクを指定できます。その後、個々のノードで別々の設定を指定してグローバル設定を上書きできます。例：

```
ADMIN_NETWORK_MASK = 255.255.255.0
```

- * ADMIN_NETWORK_GATEWAY * ：管理ネットワークのネットワークゲートウェイ。この設定は、 IP アドレスを静的に指定し、かつ ADMIN_NETWORK_ESL 設定で外部サブネットを指定する場合に必要となります（ ADMIN_NETWORK_ESL が空の場合は不要です）。 全ノードまたはほとんどのノードが同じネットワークゲートウェイを使用する場合は、ここでそのネットワークゲートウェイを指定できます。その後、個々のノードで別々の設定を指定してグローバル設定を上書きできます。例：

```
ADMIN_NETWORK_GATEWAY = 10.3.0.1
```

- * ADMIN_NETWORK_ESL * ：管理ネットワークの外部サブネットリスト（ルート）。 CIDR ルートのデスティネーションをカンマで区切ったリストとして指定します。全ノードまたはほとんどのノードが同じ外部サブネットリストを使用する場合は、ここでそのリストを指定できます。その後、個々のノードで別々の設定を指定してグローバル設定を上書きできます。例：

```
ADMIN_NETWORK_ESL = 172.16.0.0/21,172.17.0.0/21
```

- * ADMIN_NETWORK_MTU * ：オプション。管理ネットワークでの最大伝送ユニット（ MTU ）です。ADMIN_NETWORK_CONFIG = DHCP の場合は指定しないでください。この値を指定する場合、 1280 ～ 9216 の範囲で指定する必要があります。省略すると 1400 に設定されます。ジャンボフレームを使用する場合は、 MTU を 9000 などのジャンボフレームに適した値に設定します。それ以外の場合は、デフォルト値のままにします。全ノードまたはほとんどのノードが管理ネットワークに同じ MTU を使用する場合は、ここでその MTU を指定できます。その後、個々のノードで別々の設定を指定してグローバル設定を上書きできます。例：

```
ADMIN_NETWORK_MTU = 8192
```

- * CLIENT_NETWORK_CONFIG * ： IP アドレスの取得に使用する方法。無効、静的、または DHCP のいずれかになります。デフォルトは disabled です。全ノードまたはほとんどのノードが IP アドレスの取得に同じ方法を使用する場合は、ここでその方法を指定できます。その後、個々のノードで別々の設定を指定してグローバル設定を上書きできます。例：

```
CLIENT_NETWORK_CONFIG = STATIC
```

- * client_network_target * ：クライアントネットワークに使用する既存の VMware ネットワークの名前。この設定は、クライアントネットワークが無効になっていない場合に必要となります。全ノードまたはほとんどのノードが同じネットワーク名を使用する場合は、ここでその名前を指定できます。その後、個々のノードで別々の設定を指定してグローバル設定を上書きできます。例：

```
CLIENT_NETWORK_TARGET = SG-Client-Network
```

- * CLIENT_NETWORK_MASK * ：クライアントネットワークのネットワークマスク。この設定は、静的 IP アドレスを使用する場合に必要となります。全ノードまたはほとんどのノードが同じネットワークマスクを使用する場合は、ここでそのネットワークマスクを指定できます。その後、個々のノードで別々の設定を指定してグローバル設定を上書きできます。例：

```
CLIENT_NETWORK_MASK = 255.255.255.0
```

- * client_network_gateway * ：クライアントネットワークのネットワークゲートウェイ。この設定は、静的 IP アドレスを使用する場合に必要となります。全ノードまたはほとんどのノードが同じネットワークゲートウェイを使用する場合は、ここでそのネットワークゲートウェイを指定できます。その後、個々のノードで別々の設定を指定してグローバル設定を上書きできます。例：

```
CLIENT_NETWORK_GATEWAY = 10.4.0.1
```

- * CLIENT_NETWORK_MTU * ：オプション。クライアントネットワークでの最大伝送ユニット（ MTU ）です。CLIENT_NETWORK_CONFIG = DHCP の場合は指定しないでください。この値を指定する場合、 1280 ～ 9216 の範囲で指定する必要があります。省略すると 1400 に設定されます。ジャンボフレームを使用する場合は、 MTU を 9000 などのジャンボフレームに適した値に設定します。それ以外の場合は、デフォルト値のままにします。全ノードまたはほとんどのノードがクライアントネットワークに同じ MTU を使用する場合は、ここでその MTU を指定できます。その後、個々のノードで別々の設定を指定してグローバル設定を上書きできます。例：

```
CLIENT_NETWORK_MTU = 8192
```

- * PORT_REMAP * ：ノードが内部でのグリッドノードの通信または外部との通信に使用するポートを再マッピングします。StorageGRID で使用される 1 つ以上のポートがエンタープライズネットワークポリシーによって制限される場合は、ポートの再マッピングが必要です。StorageGRID で使用されるポートのリストについては、で内部でのグリッドノードの通信および外部との通信を参照してください "ネットワークのガイドライン"。

ロードバランサエンドポイントの設定に使用する予定のポートは再マッピングしないでください。

PORT_REMAP のみを設定すると、指定したマッピングがインバウンド通信とアウトバウンド通信の両方に使用されます。PORT_REMAP_INBOUND を併せて指定した場合は、PORT_REMAP がアウトバウンド通信のみに適用されます。

使用される形式は次のとおりです。 `*network type*/*protocol*/*_default port used by grid node*/*new port*`network typeはgrid、admin、clientのいずれかで、protocolはTCPまたはUDPです。

例：

```
PORT_REMAP = client/tcp/18082/443
```

この例の設定だけを使用した場合は、グリッドノードのインバウンド通信とアウトバウンド通信の両方が、ポート 18082 からポート 443 へと対称的にマッピングされます。この例の設定を PORT_REMAP_INBOUND とともに使用した場合は、アウトバウンド通信がポート 18082 からポート 443 にマッピングされます。

- * port_remap_inbound * ：指定したポートのインバウンド通信を再マッピングします。PORT_REMAP_INBOUND を指定して PORT_REMAP に値を指定しなかった場合は、ポートのアウトバウンド通信が変更されません。

ロードバランサエンドポイントの設定に使用する予定のポートは再マッピングしないでください。

使用される形式は次のとおりです。 `*network type*/*protocol*/*_default port used by grid node*/*new port*`network typeはgrid、admin、clientのいずれかで、protocolはTCPまたはUDPです。

例：

```
PORT_REMAP_INBOUND = client/tcp/443/18082
```

次の例は、ポート 443 に送信されたトラフィックを内部ファイアウォールを通過させ、グリッドノードが S3 要求をリスンしているポート 18082 に転送します。

ノード固有のパラメータ

構成ファイルには、各ノード専用のセクションがあります。各ノードには次の設定が必要です。

- セクションヘッドでは、 Grid Manager に表示されるノード名を定義します。この値を無視するには、ノードに対してオプションの node_name パラメータを指定します。
- * node_name * ： VM_Admin_Node 、 VM_Storage_Node 、 VM_Archive_Node 、 VM_API_Gateway_Node のいずれか
- * GRID_NETWORK_IP * ：グリッドネットワークでのノードの IP アドレス。
- * ADMIN_NETWORK_IP * ：管理ネットワークでのノードの IP アドレス。ノードが管理ネットワークに

接続され、かつ ADMIN_NETWORK_CONFIG が STATIC に設定されている場合にのみ必要です。

- * client_network_ip * ：クライアントネットワーク上のノードの IP アドレス。ノードがクライアントネットワークに接続され、かつノードの CLIENT_NETWORK_CONFIG が STATIC に設定されている場合にのみ必要です。
- * ADMIN_IP * ：グリッドネットワークでのプライマリ管理ノードの IP アドレス。プライマリ管理ノードの GRID_NETWORK_IP で指定した値を使用します。このパラメータを省略すると、ノードは mDNS を使用してプライマリ管理ノードの IP を検出しようとします。詳細については、を参照してください "グリッドノードによるプライマリ管理ノードの検出"。

  プライマリ管理ノードでは ADMIN_IP パラメータが無視されます。

- グローバルに設定されていないすべてのパラメータ。たとえば、ノードが管理ネットワークに接続されていて、 ADMIN_NETWORK_NETWORK パラメータをグローバルに指定していない場合は、ノードに対してそれらのパラメータを指定する必要があります。

プライマリ管理ノード

プライマリ管理ノードには次の設定を追加する必要があります。

- * node_type * ： VM_Admin_Node
- * Admin_role * ：プライマリ

次のエントリ例は、プライマリ管理ノードが 3 つのネットワークすべてに接続される場合を示しています。

```
[DC1-ADM1]
  ADMIN_ROLE = Primary
  NODE_TYPE = VM_Admin_Node

  GRID_NETWORK_IP = 10.1.0.2
  ADMIN_NETWORK_IP = 10.3.0.2
  CLIENT_NETWORK_IP = 10.4.0.2
```

プライマリ管理ノードにオプションで追加できる設定は次のとおりです。

- * DISK * ：デフォルトでは、管理ノードに対して監査用とデータベース用の 2 つの 200GB ハードディスクが追加で割り当てられます。DISK パラメータを使用して、この容量を増やすことができます。例：

```
DISK = INSTANCES=2, CAPACITY=300
```

管理ノードの場合は、 INSTANCES を必ず 2 にする必要があります。

ストレージノード

ストレージノードには次の設定を追加する必要があります。

- * node_name * ： VM_Storage_Node

  次のエントリ例は、ストレージノードがグリッドネットワークと管理ネットワークに接続され、クライアントネットワークに接続されない場合を示しています。このノードでは、 ADMIN_IP 設定を使用してグリッドネットワークでのプライマリ管理ノードの IP アドレスを指定しています。

```
[DC1-S1]
  NODE_TYPE = VM_Storage_Node

  GRID_NETWORK_IP = 10.1.0.3
  ADMIN_NETWORK_IP = 10.3.0.3

  ADMIN_IP = 10.1.0.2
```

  2 番目のエントリ例は、ストレージノードがクライアントネットワークに接続される場合を示しています。ここでは、 S3 クライアントアプリケーションがストレージノードへのアクセスに使用できるポートが、ユーザのエンタープライズネットワークポリシーによって 80 または 443 に制限されています。この例の構成ファイルでは、 PORT_REMAP を使用して、ストレージノードがポート 443 で S3 メッセージを送受信できるようにしています。

```
[DC2-S1]
  NODE_TYPE = VM_Storage_Node

  GRID_NETWORK_IP = 10.1.1.3
  CLIENT_NETWORK_IP = 10.4.1.3
  PORT_REMAP = client/tcp/18082/443

  ADMIN_IP = 10.1.0.2
```

  最後の例では、 ssh トラフィックに対してポート 22 からポート 3022 への対称的な再マッピングが作成されますが、インバウンドとアウトバウンドの両方のトラフィックに明示的に値が設定されます。

```
[DC1-S3]
  NODE_TYPE = VM_Storage_Node

  GRID_NETWORK_IP = 10.1.1.3

  PORT_REMAP = grid/tcp/22/3022
  PORT_REMAP_INBOUND = grid/tcp/3022/22

  ADMIN_IP = 10.1.0.2
```

ストレージノードにオプションで追加できる設定は次のとおりです。

- * DISK * ：デフォルトでは、ストレージノードに対して RangeDB 用に 3 つの 4TB ディスクが割り当てられます。DISK パラメータを使用して、この容量を増やすことができます。例：

```
DISK = INSTANCES=16, CAPACITY=4096
```

アーカイブノード

アーカイブノードには次の設定を追加する必要があります。

- * node_name * ： VM_Archive_Node

次のエントリ例は、アーカイブノードがグリッドネットワークと管理ネットワークに接続され、クライアントネットワークに接続されない場合を示しています。

```
[DC1-ARC1]
  NODE_TYPE = VM_Archive_Node

  GRID_NETWORK_IP = 10.1.0.4
  ADMIN_NETWORK_IP = 10.3.0.4

  ADMIN_IP = 10.1.0.2
```

ゲートウェイノード

ゲートウェイノードには次の設定を追加する必要があります。

- * node_name * ： VM_API_Gateway

次のエントリ例は、ゲートウェイノードが 3 つのネットワークすべてに接続される場合を示しています。この例では、構成ファイルのグローバルセクションでクライアントネットワークのパラメータが指定されていないため、ノードに対してそれらのパラメータを指定する必要があります。

```
[DC1-G1]
  NODE_TYPE = VM_API_Gateway

  GRID_NETWORK_IP = 10.1.0.5
  ADMIN_NETWORK_IP = 10.3.0.5

  CLIENT_NETWORK_CONFIG = STATIC
  CLIENT_NETWORK_TARGET = SG-Client-Network
  CLIENT_NETWORK_MASK = 255.255.255.0
  CLIENT_NETWORK_GATEWAY = 10.4.0.1
  CLIENT_NETWORK_IP = 10.4.0.5

  ADMIN_IP = 10.1.0.2
```

非プライマリ管理ノード

非プライマリ管理ノードには次の設定を追加する必要があります。

- * node_type * ： VM_Admin_Node
- * Admin_role * ：非プライマリ

次のエントリ例は、非プライマリ管理ノードがクライアントネットワークに接続されない場合を示しています。

```
[DC2-ADM1]
  ADMIN_ROLE = Non-Primary
  NODE_TYPE = VM_Admin_Node

  GRID_NETWORK_TARGET = SG-Grid-Network
  GRID_NETWORK_IP = 10.1.0.6
  ADMIN_NETWORK_IP = 10.3.0.6

  ADMIN_IP = 10.1.0.2
```

非プライマリ管理ノードにオプションで追加できる設定は次のとおりです。

- * DISK * ：デフォルトでは、管理ノードに対して監査用とデータベース用の 2 つの 200GB ハードディスクが追加で割り当てられます。DISK パラメータを使用して、この容量を増やすことができます。例：

  ```
  DISK = INSTANCES=2, CAPACITY=300
  ```

  管理ノードの場合は、 INSTANCES を必ず 2 にする必要があります。

関連情報

"グリッドノードによるプライマリ管理ノードの検出"

"ネットワークのガイドライン"

**Bash**スクリプトの実行

## を使用できます `deploy-vsphere-ovftool.sh` VMware vSphereへのStorageGRID グリッドノードの導入を自動化するために変更したBashスクリプトおよびdeploy-vsphere-ovftool.ini構成ファイル。

必要なもの

- 環境に対応した deploy-vsphere-ovftool.ini 構成ファイルを作成しておきます。

Bashスクリプトのヘルプを参照するには、ヘルプコマンドを入力します (`-h/--help`）。例：

```
./deploy-vsphere-ovftool.sh -h
```

または

```
./deploy-vsphere-ovftool.sh --help
```

手順

1. Bash スクリプトの実行に使用する Linux マシンにログインします。
2. インストールアーカイブを展開したディレクトリに移動します。

   例：

   ```
   cd StorageGRID-Webscale-version/vsphere
   ```

3. グリッドノードをすべて導入する場合は、使用する環境に適したオプションを指定して Bash スクリプトを実行します。

   例：

   ```
   ./deploy-vsphere-ovftool.sh --username=user --password=pwd ./deploy-vsphere-ovftool.ini
   ```

4. エラーのために導入できなかったグリッドノードがある場合は、エラーを解決し、そのノードだけを対象に Bash スクリプトを再実行します。

   例：

```
./deploy-vsphere-ovftool.sh --username=user --password=pwd --single
-node="DC1-S3" ./deploy-vsphere-ovftool.ini
```

各ノードのステータスが Passed になると ' 配備は完了します

```
Deployment Summary
+------------------------------+----------+----------------------+
| node                         | attempts | status               |
+------------------------------+----------+----------------------+
| DC1-ADM1                     |        1 | Passed               |
| DC1-G1                       |        1 | Passed               |
| DC1-S1                       |        1 | Passed               |
| DC1-S2                       |        1 | Passed               |
| DC1-S3                       |        1 | Passed               |
+------------------------------+----------+----------------------+
```

**StorageGRID** の設定の自動化

## グリッドノードを導入したら、 StorageGRID システムの設定を自動化できます。

必要なもの

- インストールアーカイブにある次のファイルの場所を確認しておきます。

| ファイル名 | 説明 |
| --- | --- |
| configure-storagegrid.py | 設定を自動化するための Python スクリプト |
| storagegrid-sample.json を設定します | スクリプトで使用するサンプル構成ファイル |
| storagegrid-bank.json を設定する | スクリプトで使用する空の構成ファイルです |

- を作成しておきます `configure-storagegrid.json` 構成ファイルこのファイルを作成するには、サンプル構成ファイルを変更します (`configure-storagegrid.sample.json`)または空の構成ファイル (`configure-storagegrid.blank.json`) 。

を使用できます `configure-storagegrid.py` Pythonスクリプトおよび `configure-storagegrid.json` StorageGRID システムの設定を自動化するための構成ファイル。

また、 Grid Manager またはインストール API を使用してシステムを設定することもできます。

手順

1. Python スクリプトを実行するために使用する Linux マシンにログインします。

2. インストールアーカイブを展開したディレクトリに移動します。

   例：

   ```
   cd StorageGRID-Webscale-version/platform
   ```

   ここで、 `platform` は、debs、RPM、またはvSphereです。

3. Python スクリプトを実行し、作成した構成ファイルを使用します。

   例：

   ```
   ./configure-storagegrid.py ./configure-storagegrid.json --start-install
   ```

結果

設定プロセスでリカバリパッケージの .zip ファイルが生成され、インストールと設定を実行するディレクトリにダウンロードされます。グリッドノードで障害が発生した場合に StorageGRID システムをリカバリできるようにするために、リカバリパッケージファイルをバックアップする必要があります。たとえば、バックアップされたセキュアなネットワーク上の場所や、安全なクラウドストレージ上の場所にコピーします。

> リカバリパッケージファイルには StorageGRID システムからデータを取得するための暗号キーとパスワードが含まれているため、安全に保管する必要があります。

ランダムパスワードを生成するように指定した場合は、 Passwords.txt ファイルを展開し、 StorageGRID システムへのアクセスに必要なパスワードを探す必要があります。

```
######################################################################
##### The StorageGRID "recovery package" has been downloaded as: #####
#####           ./sgws-recovery-package-994078-rev1.zip          #####
#####   Safeguard this file as it will be needed in case of a    #####
#####                 StorageGRID node recovery.                 #####
######################################################################
```

StorageGRID システムがインストールおよび設定されると、確認メッセージが表示されます。

```
StorageGRID has been configured and installed.
```

関連情報

"Grid Managerに移動します"

"インストール REST API の概要"

# インストール **REST API** の概要

## StorageGRID には、インストールタスクを実行するための StorageGRID インストール API が用意されています。

API のドキュメントは、 Swagger オープンソース API プラットフォームで提供されています。Swagger では、ユーザインターフェイスを使用してパラメータやオプションを変更した場合の API の動作を確認しながら、 API の開発を進めることができます。このドキュメントは、標準的な Web テクノロジと JavaScript Object Notation （ JSON ）データ形式について十分理解していることを前提としています。

> API Docs Web ページを使用して実行する API 処理はすべてその場で実行されます。設定データやその他のデータを誤って作成、更新、または削除しないように注意してください。

各 REST API コマンドは、 API の URL 、 HTTP アクション、必須またはオプションの URL パラメータ、および想定される API 応答で構成されます。

### **StorageGRID** インストール **API**

StorageGRID インストール API は、 StorageGRID システムを最初に設定するとき、およびプライマリ管理ノードのリカバリを実行する必要がある場合にのみ使用できます。インストール API には、 Grid Manager から HTTPS 経由でアクセスできます。

API のドキュメントにアクセスするには、プライマリ管理ノードのインストール用 Web ページに移動し、メニューバーから * Help * > * API Documentation * を選択します。

StorageGRID インストール API には次のセクションがあります。

- *config *-- API の製品リリースとバージョンに関連する操作。製品リリースバージョンおよびそのリリースでサポートされる API のメジャーバージョンを一覧表示できます。
- * grid * — グリッドレベルの設定操作。グリッドの詳細、グリッドネットワークのサブネット、グリッドパスワード、 NTP および DNS サーバの IP アドレスなど、グリッド設定を取得および更新できます。
- *nodes * — ノードレベルの設定操作。グリッドノードのリストを取得できるほか、グリッドノードの削除、設定、表示、およびグリッドノードの設定のリセットを行うことができます。
- *provision * — プロビジョニング操作。プロビジョニング処理を開始し、プロビジョニング処理のステータスを表示できます。
- * recovery * - プライマリ管理ノードのリカバリ処理。情報のリセット、リカバリパッケージのアップロード、リカバリの開始、およびリカバリ処理のステータスの表示を行うことができます。
- * recovery-package * — リカバリパッケージをダウンロードする処理。
- *sites * — サイトレベルの設定操作。サイトを作成、表示、削除、および変更できます。

## 次の手順

## インストールが完了したら、統合と設定のための一連の手順を実行する必要があります。手順には必須のものとオプションのものがあります。

必要な作業

- VMware vSphere ハイパーバイザーで自動再起動を設定する。

  サーバの再起動時に仮想マシンを再起動するようにハイパーバイザーを設定する必要があります。自動再起動を有効にしないと、サーバが再起動したあとも仮想マシンとグリッドノードがシャットダウンされたままになります。詳細については、 VMware vSphere ハイパーバイザーのドキュメントを参照してください。

- StorageGRID システムにオブジェクトを格納するために使用されるクライアントプロトコル（ Swift または S3 ）ごとに、テナントアカウントを作成します。
- グループとユーザアカウントを設定してシステムアクセスを制御します。管理者グループおよびユーザをインポートできるように、必要に応じて、フェデレーテッドアイデンティティソース（ Active Directory や OpenLDAP など）を設定できます。または、ローカルグループやユーザを作成することもできます。
- StorageGRID システムにオブジェクトをアップロードするために使用する S3 または Swift API クライアントアプリケーションを統合し、テストします。
- 準備ができたら、オブジェクトデータの保護に使用する情報ライフサイクル管理（ ILM ）ルールと ILM ポリシーを設定します。

  StorageGRID をインストールすると、デフォルトの ILM ポリシーである Baseline 2 Copies Policy がアクティブになります。このポリシーには組み込みの ILM ルール（ Make 2 Copies ）が含まれており、他のポリシーがアクティブ化されていない場合に適用されます。

- インストール環境にアプライアンスストレージノードが含まれている場合は、 SANtricity ソフトウェアを使用して次の作業を実行します。
  - 各 StorageGRID アプライアンスに接続します。
  - AutoSupport データの受信を確認します。
- StorageGRID システムにアーカイブノードが含まれている場合は、アーカイブノードからターゲットの外部アーカイブストレージシステムへの接続を設定します。

  アーカイブノードが Tivoli Storage Manager を外部アーカイブストレージシステムとして使用する場合は、 Tivoli Storage Manager を設定する必要もあります。

- StorageGRID システムのセキュリティ設定ガイドラインに従ってセキュリティリスクを排除します。
- システムアラートの E メール通知を設定します。

任意のタスク

- （レガシー）アラームシステムから通知を受信するには、アラーム用のメーリングリストおよび E メール通知を設定します。
- 導入を計画し、リカバリパッケージを生成したあとにグリッドノードの IP アドレスが変わった場合は、それらの IP アドレスを更新します。リカバリとメンテナンスの手順の IP アドレスの変更に関する情報を参照してください。
- 必要に応じて、ストレージ暗号化を設定します。
- 必要に応じて、ストレージの圧縮を設定し、格納されているオブジェクトのサイズを削減します。

- 監査クライアントアクセスを設定します。NFS または CIFS ファイル共有を通じて、監査を目的としたシステムへのアクセスを設定できます。StorageGRID の管理手順を参照してください。

> CIFS / Samba を使用した監査エクスポートは廃止されており、 StorageGRID の今後のリリースで削除される予定です。

# インストールに関する問題のトラブルシューティング

## StorageGRID システムのインストール中に問題が発生した場合は、インストールログファイルにアクセスできます。

次のファイルは、テクニカルサポートが問題の解決に必要とする場合があるメインのインストールログファイルです。

- `/var/local/log/install.log` （すべてのグリッドノードに存在）
- `/var/local/log/gdu-server.log` （プライマリ管理ノードに存在）

ログファイルへのアクセス方法については、 StorageGRID の監視とトラブルシューティングの手順を参照してください。アプライアンスの設置に関する問題のトラブルシューティングについては、使用しているアプライアンスの設置とメンテナンスの手順を参照してください。その他のサポートが必要な場合は、テクニカルサポートにお問い合わせください。

関連情報

"トラブルシューティングを監視します"

"SG100 SG1000サービスアプライアンス"

"SG6000 ストレージアプライアンス"

"SG5700 ストレージアプライアンス"

"SG5600 ストレージアプライアンス"

"ネットアップサポート"

### 仮想マシンのリソースリザベーションの調整が必要です

## OVF ファイルでは、各グリッドノードが十分な RAM と CPU を確保して効率よく動作できるようにするためのリソースリザベーションが設定されています。VMware で OVF ファイルを導入して仮想マシンを作成する場合、事前に定義された数のリソースを使用できないと、仮想マシンは起動されません。

このタスクについて

VM ホストに各グリッドノード用の十分なリソースがあることがわかっている場合は、各仮想マシンに割り当てられているリソースを手動で調整し、仮想マシンの起動を試みます。

手順

1. VMware vSphere ハイパーバイザーのクライアントツリーで、起動されていない仮想マシンを選択します。

2. 仮想マシンを右クリックし、 * 設定の編集 * を選択します。
3. [ 仮想マシンのプロパティ ] ウィンドウで、 [ * リソース * ] タブを選択します。
4. 仮想マシンに割り当てられているリソースを調整します。
   a. [**CPU**] を選択し、 [ 予約 ] スライダを使用して、この仮想マシン用に予約されている MHz を調整します。
   b. [* Memory] を選択し、 [Reservation （予約） ] スライダを使用してこの仮想マシン用に予約されている MB を調整します。
5. [OK] をクリックします。
6. 必要に応じて、同じ VM ホストでホストされている他の仮想マシンに対して同じ手順を繰り返します。

# ソフトウェアをアップグレードする

StorageGRID システムを新しいリリースにアップグレードする方法について説明します。

- "StorageGRID 11.5について"
- "アップグレードの計画と準備"
- "アップグレードを実行する"
- "アップグレードの問題のトラブルシューティング"

## StorageGRID 11.5について

アップグレードを開始する前に、このセクションを一目で確認して、StorageGRID 11.5の新機能と機能強化について把握し、廃止または削除された機能がないかを確認してください。また、StorageGRID APIに対する変更も確認してください。

- "StorageGRID 11.5の新機能"
- "削除または廃止された機能"
- "Grid 管理 API に対する変更"
- "テナント管理 API に変更が加えられました"

### StorageGRID 11.5の新機能

StorageGRID 11.5では、S3オブジェクトロック、データのKMIP暗号化のサポート、ILMの操作性の向上、Tenant Managerユーザインターフェイスの再設計、StorageGRID サイトの運用停止のサポート、およびアプライアンスノードのクローン手順 が導入されています。

#### S3オブジェクトロックで準拠データをロック

StorageGRID 11.5のS3オブジェクトロック機能は、Amazon Simple Storage Service（Amazon S3）のS3オブジェクトロックに相当するオブジェクト保護解決策 です。StorageGRID システムに対してグローバルな S3 オブジェクトロック設定を有効にすると、 S3 テナントアカウントで S3 オブジェクトのロックを有効にした

状態でバケットを作成できるようになります。テナントは、S3クライアントアプリケーションを使用して、必要に応じてバケット内のオブジェクトの保持設定とリーガルホールド設定を指定できます。

S3オブジェクトロックを使用すると、テナントユーザは、一定期間、または無期限に特定のオブジェクトを保持することを求める規制に準拠できます。

詳細はこちら。

- "ILM を使用してオブジェクトを管理する"
- "S3 を使用する"
- "テナントアカウントを使用する"

#### KMS暗号化キー管理

Grid Managerで1つ以上の外部キー管理サーバ（KMS）を設定して、StorageGRID サービスとストレージアプライアンスに暗号化キーを提供できるようになりました。KMS や KMS の各クラスタは、 Key Management Interoperability Protocol （ KMIP ）を使用して、関連する StorageGRID サイトにあるアプライアンスノードに暗号化キーを提供します。アプライアンスのボリュームを暗号化すると、ノードが KMS と通信できないかぎり、アプライアンスのデータにアクセスすることはできません。

暗号化キー管理を使用する場合は、アプライアンスをグリッドに追加する前に、StorageGRID アプライアンスインストーラを使用してアプライアンスのノード暗号化*設定を有効にする必要があります。

詳細はこちら。

- "StorageGRID の管理"

#### 情報ライフサイクル管理（ILM）のユーザビリティ向上

- ストレージプールの合計容量と使用済みスペースおよび空きスペースを表示できるようになりました。また、ストレージプールに含まれているノード、およびストレージプールを使用しているILMルールとイレイジャーコーディングプロファイルも確認できます。
- 複数のテナントアカウントに適用されるILMルールを設計できるようになりました。
- イレイジャーコーディング用のILMルールを作成する際に、非常に小さなオブジェクトがイレイジャーコーディングされないように、高度なフィルタ「オブジェクトサイズ（MB）」を0.2より大きい値に設定するように求められます。
- これで、デフォルトのILMルールが、別のルールに一致しないオブジェクトに常に使用されるようになりました。StorageGRID 11.5以降では、デフォルトルールで基本または高度なフィルタを使用することはできず、自動的にポリシーの最後のルールとして配置されます。

  現在のILMポリシーが新しい要件に準拠していない場合は、StorageGRID 11.5へのアップグレード後もそのまま使用できます。ただし、アップグレード後に非準拠ポリシーをクローニングする場合は、フィルタを含まないデフォルトルールを選択するように求められ、デフォルトルールをポリシーの末尾に配置する必要があります。

- 新しいILMルールまたは新しいイレイジャーコーディングプロファイルを作成するときに、組み込みのAll Storage Nodesストレージプールがデフォルトで選択されなくなりました。また、どのルールでも使用されていないかぎり、All Storage Nodesストレージプールを削除できるようになりました。

All Storage Nodesストレージプールにはすべてのサイトが含まれているため、このストレージプールを使用することは推奨されません。複数のサイトを含むStorageGRID システムでこのストレージプールを使用する場合は、オブジェクトの複数のコピーが同じサイトに配置されることがあります。

- アクティブポリシーまたはドラフトポリシーで使用されていないかぎり、組み込みのMake 2 Copiesルール（All Storage Nodesストレージプールを使用）を削除できるようになりました。
- クラウドストレージプールに格納されているオブジェクトをただちに削除できるようになりました（同期削除）。

詳細はこちら。

- "ILM を使用してオブジェクトを管理する"

**Grid Managerの機能が強化されています**

- 再設計されたTenant Accountsページでは、テナントアカウントの使用状況を簡単に確認できます。テナントの概要テーブルに、使用済みスペース、クォータ利用率、クォータ、オブジェクト数の列が表示されるようになりました。新しい* View Details *ボタンをクリックすると、各テナントの概要に加え、アカウントのS3バケットまたはSwiftコンテナの詳細情報にアクセスできます。さらに、2つのをエクスポートできるようになりました `.csv` テナントで使用するファイル：すべてのテナントの使用量の値とテナントのバケットまたはコンテナの詳細を含むファイル。

  この変更に関連して、テナントアカウントの使用状況を追跡するために次の3つの新しいPrometheus指標が追加されました。

  - `storagegrid_tenant_usage_data_bytes`
  - `storagegrid_tenant_usage_object_count`
  - `storagegrid_tenant_usage_quota_bytes`

- Admin Groupsページの新しい* Access Mode フィールド（ Configuration > Access Control *）では、グループの管理権限を読み取り/書き込み（デフォルト）と読み取り専用のどちらにするかを指定できます。読み取り/書き込みアクセスモードのグループに属しているユーザは、Grid Managerおよびグリッド管理APIで設定を変更して処理を実行できます。読み取り専用アクセスモードのグループに属しているユーザは、グループに対して選択されている設定と機能のみを表示できます。

  StorageGRID 11.5にアップグレードすると、既存のすべての管理者グループに対して読み取り/書き込みアクセスモードオプションが選択されます。

- AutoSupport のユーザインターフェイスが再設計されました。グリッドマネージャの1つのページから、イベントトリガー型、ユーザトリガー型、および週次のAutoSupport メッセージを設定できるようになりました。AutoSupport メッセージの追加の送信先を設定することもできます。

  AutoSupport が有効になっていない場合は、Grid ManagerDashboardにリマインダメッセージが表示されます。

- Nodesページで* Storage Used - Object Data グラフを表示したときに、レプリケートされたオブジェクトデータの量と、グリッド、サイト、またはストレージノード（ Nodes ***>*grid/site / Storage Node***>* Storage *）上のイレイジャーコーディングデータの量の推定値が表示されるようになりました。
- Grid Managerのメニューオプションが再編成され、オプションが簡単に見つかりました。たとえば、新し

い*ネットワーク設定*サブメニューが*環境設定*メニューに追加され、*メンテナンス*および*サポート*メニューのオプションがアルファベット順に表示されるようになりました。

詳細はこちら。

- "StorageGRID の管理"

#### Tenant Managerの機能拡張

- Tenant Managerのユーザインターフェイスの外観と構成は、ユーザエクスペリエンスを向上させるために完全に再設計されています。
- 新しいTenant Managerダッシュボードには各アカウントの概要が表示されます。バケットの詳細と、バケットまたはコンテナ、グループ、ユーザ、プラットフォームサービスのエンドポイント（設定されている場合）の数が表示されます。

詳細はこちら。

- "テナントアカウントを使用する"

#### Prometheus指標エクスポート用のクライアント証明書

クライアント証明書（* Configuration > Access Control > Client Certificates *）をアップロードまたは生成できるようになりました。この証明書を使用して、StorageGRID Prometheusデータベースへのセキュアで認証されたアクセスを提供できます。たとえば、Grafanaを使用して外部からStorageGRID を監視する必要がある場合、クライアント証明書を使用できます。

詳細はこちら。

- "StorageGRID の管理"

#### ロードバランサの機能拡張

- サイトでルーティング要求を処理する際に、ロードバランササービスでロード対応ルーティングが実行されるようになりました。これにより、同じサイトにあるストレージノードのCPUの可用性が考慮されます。CPU の可用性に関する情報が、ロードバランササービスが配置されているサイトに制限されている場合があります。

> CPUアウェアネスは、サイトのストレージノードの3分の2以上がStorageGRID 11.5にアップグレードされてCPU統計がレポートされるまで有効になりません。

- セキュリティを強化するために、ロードバランサエンドポイントごとにバインディングモードを指定できるようになりました。エンドポイントのピン接続を使用すると、各エンドポイントのアクセス性を特定のハイアベイラビリティグループまたはノードインターフェイスに制限できます。

詳細はこちら。

- "StorageGRID の管理"

#### オブジェクトのメタデータが変更される

- 新しい実際のリザーブスペース指標：各ストレージノードでのオブジェクトメタデータのスペース使用量を把握および監視するために、ストレージノードのStorage Used - Object Metadataグラフ（* Nodes ***>*Storage Node***>* Storage *）に新しいPrometheus指標が表示されます。

```
storagegrid_storage_utilization_metadata_reserved
```

Actual Reserved Space *指標は、特定のストレージノードでオブジェクトメタデータ用にStorageGRIDがリザーブしているスペースの量を示します。

- 大容量のストレージノードを使用した環境でのメタデータスペースの増加：次のように、128GB以上のRAMを搭載したストレージノードを含むStorageGRID システムでは、システム全体のMetadata Reserved Space設定が拡張されています。
  - 注：新規インストールの場合は8TB *：StorageGRID 11.5システムをインストールし、グリッド内の各ストレージノードに128GB以上のRAMがある場合、システム全体のMetadata Reserved Space設定は、3TBではなく8TBに設定されます。
  - *アップグレード用に4TB *：StorageGRID 11.5にアップグレードする際、いずれかのサイトの各ストレージノードに128GB以上のRAMが搭載されている場合、システム全体のMetadata Reserved Space設定が3TBではなく4TBに設定されています。

    Metadata Reserved Space設定の新しい値によって、これらの大容量ストレージノードで使用できるメタデータスペースが最大2.64TB増加し、将来のハードウェアとソフトウェアのバージョン用に十分なメタデータスペースがリザーブされるようになりました。

    ストレージノードに十分なRAMがあり、ボリューム0に十分なスペースがある場合は、アップグレード後にMetadata Reserved Space設定を手動で8TBに増やすことができます。StorageGRID 11.5へのアップグレード後にメタデータスペースをリザーブすると、以降のハードウェアおよびソフトウェアのアップグレードが簡単になります。

    "Metadata Reserved Space設定を拡張しています"

    +

    StorageGRID システムで任意のストレージノードに2.64TBを超えるメタデータを格納（または格納する予定がある場合）がある場合、許可されるメタデータスペースが増加することがあります。各ストレージノードのストレージボリューム0に空きスペースがあり、128GBを超えるRAMが搭載されている場合は、ネットアップのアカウント担当者にお問い合わせください。要件を確認し、可能であれば各ストレージノードで許可されているメタデータスペースを増やします。

- 削除されたメタデータの自動クリーンアップ：ストレージノードに格納されているメタデータの20%以上を削除する準備ができた場合（対応するオブジェクトが削除されたため）、StorageGRID はそのストレージノードに対して自動コンパクションを実行できるようになりました。このバックグラウンドプロセスは、システムの負荷が低い場合にのみ実行されます。つまり、使用可能なCPU、ディスクスペース、メモリがある場合にのみ実行されます。新しいコンパクションプロセスでは、以前のリリースよりも前に削除されたオブジェクトのメタデータが削除されるため、新しいオブジェクトを格納するためのスペースを解放できます。

詳細はこちら。

- "StorageGRID の管理"

#### S3 REST API のサポートに関する変更点

- S3 REST APIを使用して指定できるようになりました S3 オブジェクトのロック 設定：
  - S3オブジェクトロックを有効にしてバケットを作成するには、でPUT Bucket要求を使用します `x-amz-bucket-object-lock-enabled` ヘッダー。
  - バケットでS3オブジェクトロックが有効になっているかどうかを確認するには、GET Object Lock Configuration要求を使用します。
  - S3オブジェクトのロックが有効になっているバケットにオブジェクトのバージョンを追加する場合は、次の要求ヘッダーを使用して保持設定とリーガルホールド設定を指定します。 `x-amz-object-lock-mode`、 `x-amz-object-lock-retain-until-date`および `x-amz-object-lock-legal-hold`。
- バージョン管理が有効になったバケットでDELETE Multiple Objectsを使用できるようになりました。
- PUT、GET、DELETE Bucket encryption要求を使用して、既存のS3バケットの暗号化を管理できるようになりました。
- のフィールド名が若干変更されました `Expiration` パラメータこのパラメータは、ライフサイクル設定環境 内の有効期限ルールが特定のオブジェクトである場合に、PUT Object、HEAD Object、またはGET Object要求への応答に含まれます。照合された有効期限ルールを示すフィールドは、以前に名前が付けられていました `rule_id`。このフィールドの名前がに変更されました `rule-id` AWSの実装に合わせて調整できます。
- デフォルトでは、S3 GET Storage Usage要求は、strong-global整合性を使用して、テナントアカウントとそのバケットで使用されているストレージの取得を試みます。strong-global整合性を保証できない場合、StorageGRID は、strong-site整合性を保証して使用状況の情報を取得します。
- 。 `Content-MD5` 要求ヘッダーが正しくサポートされるようになりました。

詳細はこちら。

- "S3 を使用する"

#### CloudMirrorオブジェクトの最大サイズが5TBに拡張されました

CloudMirrorレプリケーションサービスでデスティネーションバケットにレプリケートできるオブジェクトの最大サイズが5TBに拡張されました。これはStorageGRID でサポートされる最大オブジェクトサイズです。

詳細はこちら。

- "S3 を使用する"
- "Swift を使用します"

#### 新しいアラートが追加されました

StorageGRID 11.5で追加された新しいアラートは次のとおりです。

- アプライアンスの BMC 通信エラー
- アプライアンスのファイバ・チャネル障害が検出されました
- アプライアンスのファイバ・チャネル HBA ポート障害
- アプライアンスの LACP ポートがありません
- Cassandra 自動コンパクターエラーです

- Cassandra 自動コンパクターメトリックが古くなっています
- Cassandra の圧縮処理が過負荷です
- ディスク I/O が非常に遅い
- KMS CA 証明書の有効期限
- KMS クライアント証明書の有効期限
- KMS の設定をロードできませんでした
- KMS 接続エラー
- KMS 暗号化キー名が見つかりません
- KMS 暗号化キーのローテーションに失敗しました
- KMS は設定されていません
- KMS キーでアプライアンスボリュームを復号化できませんでした
- KMS サーバ証明書の有効期限
- ストレージプールの空き容量が不足しています
- ノードネットワーク受信フレームエラー
- サービスアプライアンスストレージの接続がデグレードされました
- ストレージアプライアンスストレージ接続のデグレード（以前の名称はアプライアンスストレージ接続デグレード）
- テナントクォータの使用率が高い
- 予期しないノードのリブートです

詳細はこちら。

- "トラブルシューティングを監視します"

#### SNMPトラップのTCPサポート

SNMPトラップの送信先のプロトコルとしてTransmission Control Protocol（TCP；伝送制御プロトコル）を選択できるようになりました。以前は、User Datagram Protocol（UDP）プロトコルだけがサポートされていました。

詳細はこちら。

- "トラブルシューティングを監視します"

#### インストールとネットワークの機能拡張

- * MACアドレス・クローニング*：MACアドレス・クローニングを使用して、特定の環境のセキュリティを強化できるようになりました。MACアドレスクローニングを使用すると、グリッドネットワーク、管理ネットワーク、およびクライアントネットワークに専用の仮想NICを使用できます。Dockerコンテナでホスト上の専用NICのMACアドレスを使用すると、プロミスキャスモードのネットワーク設定を回避できます。Linuxベース（ベアメタル）ノードのノード構成ファイルに3つの新しいMACアドレスクローニングキーが追加されました。
- * DNSおよびNTPホストルートの自動検出*:これまでは、クライアントネットワーク上にすべてのNTPおよびDNSサーバを配置できなかったという要件など、NTPおよびDNSサーバが接続する必要のあるネットワークに制限がありました。現在、これらの制限は削除されています。

詳細はこちら。

- "Red Hat Enterprise Linux または CentOS をインストールします"
- "Ubuntu または Debian をインストールします"

ストレージノードの拡張後のイレイジャーコーディング（**EC**）データのリバランシングをサポート

EC Rebalance手順 は、新しいストレージノードを追加したあとに必要になる可能性があるコマンドラインスクリプトです。手順 を実行すると、StorageGRID によって、サイトの既存および新しく拡張したストレージノードにイレイジャーコーディングフラグメントが再配分されます。

ECのリバランシング手順 は、限られた場合にのみ実行してください。たとえば、推奨数のストレージノードを追加して拡張できない場合は、ECのリバランシング手順 を使用してイレイジャーコーディングされたオブジェクトを追加で格納できます。

詳細はこちら。

- "グリッドを展開します"

新規および改訂されたメンテナンス手順

- サイトの運用停止：StorageGRID システムから運用サイトを削除できるようになりました。接続されたサイトの運用停止手順 は、運用サイトを削除し、データを保持します。新しいDecommission Siteウィザードの指示に従って、次のプロセスを実行できます（* Maintenance **>** Decommission **>** Decommission Site *）。
- アプライアンスノードのクローニング：既存のアプライアンスノードをクローニングして、ノードを新しいアプライアンスモデルにアップグレードできるようになりました。たとえば、容量の小さいアプライアンスノードを容量の大きいアプライアンスにクローニングできます。また、アプライアンスノードをクローニングして、KMS暗号化に必要な新しい* Node Encryption *設定などの新機能を実装することもできます。
- プロビジョニングパスフレーズの変更：プロビジョニングパスフレーズ（* Configuration **>** Access Control **>** Grid Passwords *）を変更できるようになりました。パスフレーズは、リカバリ、拡張、およびメンテナンスの手順で必要になります。
- 拡張**SSH**パスワードの動作：StorageGRID アプライアンスのセキュリティを強化するため、アプライアンスを保守モードにしてもSSHパスワードは変更されません。また、ノードをStorageGRID 11.5にアップグレードすると、新しいSSHホスト証明書とホストキーが生成されます。

StorageGRID 11.5へのアップグレード後にSSHを使用してノードにログインすると、ホストキーが変更されたことを示す警告が表示されます。この動作は想定される動作であり、新しいキーを安全に承認することができます。

詳細はこちら。

- ""

**StorageGRID** アプライアンスに対する変更

- ストレージアプライアンス用の**SANtricity** システムマネージャへの直接アクセス：StorageGRID アプライアンスインストーラおよびグリッドマネージャからEシリーズSANtricity システムマネージャのユーザインターフェイスにアクセスできるようになりました。これらの新しい方法を使用すると、アプライアンスの管理ポートを使用せずにSANtricity System Managerにアクセスできます。グリッドマネージャからSANtricity システムマネージャにアクセスする必要があるユーザには、新しいストレージアプライアン

ス管理者権限が必要です。

- ノード暗号化:新しいKMS暗号化機能の一部として、StorageGRID アプライアンスインストーラに新しい*ノード暗号化*設定が追加されました。暗号化キー管理を使用してアプライアンスのデータを保護する場合は、アプライアンスのハードウェア構成ステージでこの設定を有効にする必要があります。
- * UDPポート接続*：StorageGRID アプライアンスとUDPポート間のネットワーク接続をテストできるようになりました。たとえば、外部NFSサーバやDNSサーバに使用されるポートなどです。StorageGRID アプライアンスインストーラから、**Configure Networking *>** Port Connectivity Test (nmap)*を選択します。
- インストールと設定の自動化：StorageGRID アプライアンスインストーラに新しいJSON構成のアップロードページが追加されました（* Advanced **>** Update Appliance Configuration *）。このページでは、1つのファイルを使用して大規模なグリッド内に複数のアプライアンスを設定できます。また、も参照してください `configure-sga.py` StorageGRID アプライアンスインストーラの機能に合わせてPythonスクリプトが更新されました。

詳細はこちら。

- "SG100 SG1000サービスアプライアンス"
- "SG6000 ストレージアプライアンス"
- "SG5700 ストレージアプライアンス"
- "SG5600 ストレージアプライアンス"

監査メッセージに対する変更

- 上書きされたオブジェクトの自動クリーンアップ：以前は、特定のケースで上書きされたオブジェクトがディスクから削除されず、結果として追加のスペースが消費されていました。上書きされたこれらのオブジェクトはユーザがアクセスできなくなり、ストレージスペースを節約するために自動的に削除されるようになりました。詳細については、LCU監査メッセージを参照してください。
- * S3オブジェクトロック*用の新しい監査コード：SPUT監査メッセージに4つの新しい監査コードが追加されました S3 オブジェクトのロック 要求ヘッダー：
  - LKEN：オブジェクトロックが有効です
  - LKLH：オブジェクトロックリーガルホールド
  - LKMD：オブジェクトロック保持モード
  - LKRU：オブジェクトロックまで保持日
- 最終変更時刻と前のオブジェクトサイズの新しいフィールド:オブジェクトが上書きされた日時と元のオブジェクトサイズを追跡できるようになりました。
  - MTME（Last Modified Time）フィールドが次の監査メッセージに追加されました。
    - SDEL（S3 DELETE）
    - SPUT（S3 PUT）
    - WDEL（Swift DELETE）
    - WPUT（Swift PUT）
  - CSIZ（Previous Object Size）フィールドがOVWR（Object Overwrite）監査メッセージに追加されました。

詳細はこちら。

- "監査ログを確認します"

新しい**nms.requestlog**ファイル

新しいログファイル、 `/var/local/log/nms.requestlog`は、すべての管理ノードで管理されます。このファイルには、管理APIから内部StorageGRID サービスへの発信接続に関する情報が格納されます。

詳細はこちら。

- "トラブルシューティングを監視します"

**StorageGRID** のマニュアルの変更点

- ネットワーク情報と要件を見つけやすくし、環境 StorageGRID アプライアンスノードに関する情報も明確にするために、ネットワーク関連のドキュメントはソフトウェアベースのインストールガイド（Red Hat Enterprise Linux/CentOS、Ubuntu / Debian、VMware）から新しいネットワークガイドに移動されました。

  "ネットワークガイドライン"

- ILM関連の手順や例を簡単に見つけることができるように、情報ライフサイクル管理を含むオブジェクトを管理するためのドキュメントを、_管理者ガイド_から新しいILMガイドに移動しました。

  "ILM を使用してオブジェクトを管理する"

- 新しいFabricPool ガイドでは、StorageGRID をNetApp FabricPool クラウド階層として設定する方法の概要を示し、ILMおよびFabricPool ワークロードのその他のStorageGRID オプションを設定するためのベストプラクティスについて説明します。

  "StorageGRID for FabricPool を設定します"

- グリッドマネージャからいくつかの手順ビデオにアクセスできるようになりました。最新のビデオでは、アラート、カスタムアラート、ILMルール、ILMポリシーを管理する手順について説明しています。

削除または廃止された機能

## 一部の機能は、StorageGRID 11.5で削除または廃止されました。以下の項目を確認して、アップグレードの前にクライアントアプリケーションの更新や設定の変更が必要かどうかを把握してください。

整合性制御が脆弱になりました

StorageGRID 11.5では、弱い整合性制御が削除されました。アップグレード後は、次の動作が適用されます。

- S3バケットまたはSwiftコンテナに弱い整合性を設定する要求は成功しますが、実際には整合性レベルはavailableに設定されます。
- 整合性に脆弱性を使用する既存のバケットとコンテナは、整合性を使用するようにサイレントに更新されます。
- 整合性制御ヘッダーが脆弱な要求では、実際には使用可能な整合性が使用されます（該当する場合）。

使用可能な整合性制御は「read-after-new-write」整合性レベルと同じ動作をしますが、HEAD処理については

結果整合性のみを提供します。ストレージ・ノードが使用できない場合' Availableコンシステンシ・コントロールは'リードアフター・ニュー・ライトよりもヘッド・オペレーションの可用性が高くなります

#### Grid健全性のアラームが廃止されました

。 `/grid/health/topology` active_alarms_onノードをチェックするAPIは廃止されました。その代わりに、新しい `/grid/node-health` エンドポイントが追加されました。このAPIは、active_alerts_onノードを確認することで各ノードの現在のステータスを返します。

#### コンプライアンス機能は廃止されました

StorageGRID 11.5のS3オブジェクトロック機能は、以前のバージョンのStorageGRID で使用できた準拠機能に代わる機能です。新しいS3オブジェクトロック機能はAmazon S3の要件に準拠しているため、「従来のコンプライアンス」と呼ばれる独自のStorageGRID 準拠機能は廃止されています。

グローバル準拠設定を有効にしている場合は、StorageGRID 11.5にアップグレードすると、新しいグローバルS3オブジェクトロック設定が自動的に有効になります。テナントユーザは、StorageGRID で準拠を有効にした新しいバケットを作成できなくなります。ただし、必要に応じて、テナントユーザは既存の従来の準拠バケットを引き続き使用および管理できます。

Tenant Managerの盾アイコン 従来の準拠バケットを示します。従来の準拠バケットには保留バッジが付いている場合もあります バケットがリーガルホールドの対象であることを示します。

"KB：StorageGRID 11.5で従来の準拠バケットを管理する方法"

"ILM を使用してオブジェクトを管理する"

#### 「S3マルチパートのパートが小さすぎます」というアラートが削除されました

S3マルチパートのパートが小さすぎる*アラートは削除されました。以前は、S3クライアントがAmazon S3のサイズ制限を満たしていないパーツでマルチパートアップロードを完了しようとしたときに、このアラートがトリガーされていました。StorageGRID 11.5へのアップグレード後に、次のサイズの制限を満たしていないマルチパートアップロード要求が失敗します。

- マルチパートアップロードの各パートのサイズは 5MiB （ 5 、 242 、 880 バイト）と 5GiB （ 5 、 368 、 709 、 120 バイト）の間にする必要があります。
- 最後の部分は 5MiB （ 5,242,880 バイト）より小さくできます。
- 一般に、パーツサイズはできるだけ大きくする必要があります。たとえば、 100GiB オブジェクトの場合、 5GB のパートサイズを使用します。各パートは固有のオブジェクトとみなされるため、大きなパートサイズを使用すると、 StorageGRID のメタデータのオーバーヘッドが軽減されます。
- 5GB 未満のオブジェクトでは、マルチパートではないアップロードの使用を検討してください。

#### 「Appliance link down on Grid Network」アラートが削除されました

次のアラートが削除されました。グリッドネットワークが停止している場合、これらのアラートをトリガーする指標にはアクセスできません。

- サービスアプライアンスはグリッドネットワーク上でリンクダウン状態になります
- グリッドネットワーク上のストレージアプライアンスのリンクが停止しています

### SNMP設定から削除された完全修飾ドメイン名のサポート

SG6000、SG100、またはSG1000のベースボード管理コントローラ（BMC）でSNMPサーバを設定するときに、完全修飾ドメイン名の代わりにIPアドレスを指定する必要があります。完全修飾ドメイン名がすでに設定されている場合は、StorageGRID 11.5にアップグレードする前にIPアドレスに変更します。

### レガシー属性が削除されました

次のレガシー属性が削除されました。該当する場合、Prometheus指標は同等の情報を提供します。

| レガシー属性 | 同等の**Prometheus**指標 |
| --- | --- |
| BREC | storagegrid_service_network_received_bytes |
| BTRA | storagegrid_service_network_transmitted バイト数 |
| CQST | storagegrid_meta_query_average _latency _milliseconds |
| はい | storagegrid_http_session_ining_attempted 」というメッセージが表示されます |
| HCCS | storagegrid_http_session_ining_currently established |
| Heis | storagegrid_http_session_ining_failed |
| HISCのように | storagegrid_http_session_ining_successful |
| LHAC | _ なし _ |
| NREC | _ なし _ |
| NTSO（選択された時間ソースオフセット） | storagegrid_ntp_Chosen_time_source_offset_milliseconds |
| NTRA | _ なし _ |
| SLOD | storagegrid_service_load |
| SMEM | storagegrid_service_memory_usage_bytes |
| SUTM | storagegrid_service_cpu_seconds で指定します |
| SVUT | storagegrid_service_uptime</1> を指定します |
| TRBS（受信1秒あたりの合計ビット数） | _ なし _ |

| レガシー属性 | 同等の**Prometheus**指標 |
| --- | --- |
| TRXB | storagegrid_network_received_bytes |
| TTBS（送信1秒あたりの合計ビット数） | _ なし _ |
| TTXB | storagegrid_network_transmitted _bytes |

次の関連する変更も行われました。

- 。 `network_received_bytes` および `network_transmitted_bytes` Prometheus指標はゲージからカウンタに変更されました。これらの指標の値は増加するだけです。Prometheusクエリでこれらの指標を現在使用している場合は、の使用を開始します `increase()` クエリ内の関数です。
- StorageGRID サービスの[リソース]タブから、[ネットワークリソース]テーブルが削除されました。（* Support **>** Tools **>** Grid Topology を選択します。次に、***Node***>**service*>* Resources *を選択します。）
- ストレージノードのHTTP Sessionsページが削除されました。以前は、このページにアクセスするには、* Support **>** Tools **>** Grid Topology を選択し、***Storage Node***>* LDR **>** HTTP *を選択します。
- HCCS（現在確立されている着信セッション）アラームが削除されました。
- NTSO（Chosen Time Source Offset）アラームが削除されました。

**Grid** 管理 **API** に対する変更

## StorageGRID 11.5はグリッド管理APIのバージョン3を使用します。バージョン 3 はバージョン 2 に代わるものですが、バージョン 1 とバージョン 2 も引き続きサポートされます。

> バージョン1とバージョン2の管理APIはStorageGRID 11.5で引き続き使用できますが、これらのバージョンのAPIのサポートはStorageGRID の今後のリリースで終了する予定です。StorageGRID 11.5にアップグレードしたあとに、でv1およびv2 APIを非アクティブ化できます `PUT /grid/config/management` API

新しいクライアント証明書セクション

新しいセクション、 `/grid/client-certificates`を使用すると、クライアント証明書を設定して、StorageGRID Prometheusデータベースへのセキュアで認証されたアクセスを提供できます。たとえば、Grafanaを使用してStorageGRID を外部から監視できます。

従来のコンプライアンスエンドポイントは、新しい**s3 - object-lock**セクションに移動されました

StorageGRID S3オブジェクトのロックが導入され、グリッドの従来の準拠設定の管理に使用していたAPIが、Swaggerユーザインターフェイスの新しいセクションに移動されました。s3 - object-lock *セクションには2つのセクションがあります `/grid/compliance-global` APIエンドポイント。グローバルなS3オブジェクトのロック設定を制御します。エンドポイントURIは、既存のアプリケーションとの互換性を維持するために変更されません。

#### **Swift-admin-password**アカウントエンドポイントが削除されました

StorageGRID 10.4で廃止された次のアカウントAPIエンドポイントが削除されました。

```
https://<IP-Address>/api/v1/grid/accounts/<AccountID>/swift-admin-password
```

#### 新しい**Grid**パスワードセクション

「* grid-password*」セクションでは、グリッドパスワード管理の処理を使用できます。このセクションには、2つのが含まれ `/grid/change-provisioning-passphrase` APIエンドポイント。エンドポイントを使用すると、ユーザはStorageGRID プロビジョニングパスフレーズを変更して、パスフレーズの変更のステータスを取得できます。

#### **Storageadmin**権限がグループ**API**に追加されました

。 `/grid/groups` APIにstorageadmin権限が追加されました。

#### **Storage Usage API**の新しいパラメータ

。 `GET /grid/accounts/{id}/usage` APIにが追加されました `strictConsistency` パラメータストレージノード間でストレージ使用状況情報を取得するときにstrong-global整合性を適用するには、このパラメータをに設定します `true`。このパラメータがに設定されている場合 `false` （デフォルト）StorageGRID は、strong-global整合性を使用して使用状況の情報を取得しますが、strong-global整合性が保証されていない場合はstrong-site整合性にフォールバックします。

#### 新しいノード健全性**API**

新しい `/grid/node-health` エンドポイントが追加されました。このAPIは、ノードでactive_alerts_onを確認することで各ノードの現在のステータスを返します。。 `/grid/health/topology` active_alarms_onノードをチェックするAPIは廃止されました。

#### 「**Appliance StorageShellvesPowerSupplyDegraded**」アラートルール**ID**に変更します

アラートルールID「Appliance StorageShellvesPowerSupplyDegraded」の名前が「Appliance StorageShellvesDegraded」に変更され、アラートの実際の動作がより正確に反映されました。

関連情報

"StorageGRID の管理"

### テナント管理 **API** に変更が加えられました

StorageGRID 11.5は、バージョン3のテナント管理APIを使用します。バージョン 3 はバージョン 2 に代わるものですが、バージョン 1 とバージョン 2 も引き続きサポートされます。

> バージョン1とバージョン2の管理APIはStorageGRID 11.5で引き続き使用できますが、これらのバージョンのAPIのサポートはStorageGRID の今後のリリースで終了する予定です。StorageGRID 11.5にアップグレードしたあとに、でv1およびv2 APIを非アクティブ化できます `PUT /grid/config/management` API

テナントストレージ使用状況**API**の新しいパラメータ

。 `GET /org/usage` APIにが追加されました `strictConsistency` パラメータストレージノード間でストレージ使用状況情報を取得するときにstrong-global整合性を適用するには、このパラメータをに設定します `true`。このパラメータがに設定されている場合 `false` （デフォルト）StorageGRID は、strong-global整合性を使用して使用状況の情報を取得しますが、strong-global整合性が保証されていない場合はstrong-site整合性にフォールバックします。

関連情報

"S3 を使用する"

"テナントアカウントを使用する"

# アップグレードの計画と準備

StorageGRID システムのアップグレードを計画して、システムをアップグレードする準備ができていること、および最小限の中断でアップグレードを完了できることを確認する必要があります。

手順

1. "アップグレード所要時間の見積もり"
2. "アップグレード中にシステムが受ける影響"
3. "アップグレードによるグループおよびユーザアカウントへの影響"
4. "インストールされているStorageGRID のバージョンを確認しています"
5. "ソフトウェアアップグレードの前提要件の確認"
6. "StorageGRID アップグレードファイルをダウンロードします"
7. "リカバリパッケージをダウンロードしています"
8. "ソフトウェアのアップグレード前のシステム状態の確認"

## アップグレード所要時間の見積もり

StorageGRID 11.5へのアップグレードを計画するときは、アップグレードにかかる時間に応じて、いつ実行するかを考慮する必要があります。また、アップグレードの各ステージ中に実行できる処理と実行できない処理についても把握しておく必要があります。

### このタスクについて

StorageGRID のアップグレード完了までに必要な時間は、クライアントの負荷やハードウェアのパフォーマンスなどのさまざまな要因によって異なります。

次の表に、アップグレードの主なタスクをまとめ、各タスクに必要なおおよその時間を示します。表に続いて、システムのアップグレード時間を見積もる手順を記載します。

StorageGRID 11.4から11.5にアップグレードすると、ストレージノード上のCassandraデータベーステーブルがアップグレードされます。データベースのアップグレード*タスクはバックグラウンドで実行されますが、完了までにかなりの時間がかかることがあります。データベースのアップグレード中も、新しい機能の使用、ホットフィックスの適用、ノードのリカバリ処理を安全に実行できます。ただし、他のメンテナンス手順を実行できない場合があります。

拡張が緊急に必要な場合は、11.5にアップグレードする前に拡張を実行します。

| アップグレードタスク | 説明 | おおよその所要時間です | このタスクの実行中です |
| --- | --- | --- | --- |
| アップグレードサービスを開始します | アップグレードの事前確認が実行され、ソフトウェアファイルが配布されて、アップグレードサービスが開始されます。 | 検証エラーが報告されないかぎり、グリッドノードあたり 3 分 | 必要に応じて、スケジュールされたアップグレードのメンテナンス時間の前に、アップグレードの事前確認を手動で実行できます。 |
| Grid ノード（プライマリ管理ノード）をアップグレード | プライマリ管理ノードが停止されてアップグレードされ、再起動されます。 | 最大30分 | プライマリ管理ノードにはアクセスできません。接続エラーが報告されますが、無視してかまいません。 |
| Grid ノード（他のすべてのノード）をアップグレード | 他のすべてのグリッドノードのソフトウェアが、ノードを承認した順序でアップグレードされます。システムの各ノードが一度に 1 つずつ数分間停止されます。 | ノードあたり15~45分、アプライアンスストレージノードで最も時間が必要です<br>• 注： * アプライアンスノードの場合、StorageGRID アプライアンスインストーラは自動的に最新リリースに更新されます。 | • グリッド設定は変更しないでください。<br>• 監査レベルの設定は変更しないでください。<br>• ILM 設定を更新しないでください。<br>• ホットフィックス、運用停止、拡張など、別のメンテナンス手順 は実行しないでください。<br>*注：リカバリ手順 を実行する必要がある場合は、テクニカル・サポートにお問い合わせください。 |

| アップグレードタスク | 説明 | おおよその所要時間です | このタスクの実行中です |
| --- | --- | --- | --- |
| 機能を有効にします | 新しいバージョンの新機能が有効になります。 | 5 分未満 | • グリッド設定は変更しないでください。<br>• 監査レベルの設定は変更しないでください。<br>• ILM 設定を更新しないでください。<br>• 別のメンテナンス手順 は実行しないでください。 |
| データベースをアップグレードします | すべてのストレージノードに存在するCassandraデータベーステーブルがアップグレードされている。 | システム内のメタデータの量に応じて、数時間から数日を指定します | データベースのアップグレードタスク中は、アップグレード済みのグリッドは正常に動作しますが、アップグレードは進行中です。このタスクでは、次の操作を実行できます。<br>• 新しいStorageGRIDバージョンの新機能を使用します。<br>• 監査レベル設定の変更<br>• ILM設定の更新<br>• ホットフィックスを適用します。<br>• ノードをリカバリ<br>*注：*最終アップグレード手順*が完了するまで、手順 の運用停止や拡張は実行できません。 |
| 最終アップグレード手順 | 一時ファイルが削除され、新しいリリースへのアップグレードが完了します。 | 5 分 | [* 最終アップグレードステップ * ] タスクが完了すると、すべてのメンテナンス手順を実行できます。 |

手順

1. すべてのグリッドノードのアップグレードに必要な推定時間を見積もります（データベースのアップグレード*を除くすべてのアップグレードタスクを考慮）。
   a. StorageGRID システムのノード数に30分（平均）を掛けます。

b. この時間に1時間を追加して、をダウンロードするために必要な時間を考慮してください `.upgrade` ファイルを選択し、事前確認検証を実行して、最終アップグレード手順を完了します。

2. Linux ノードがある場合は、 RPM パッケージまたは DEB パッケージをダウンロードしてインストールするために必要な時間として、各ノードに 15 分を追加します。

3. データベースのアップグレードに必要な推定時間。

   a. Grid Managerから* Nodes *を選択します。

   b. ツリーの最初のエントリ（グリッド全体）を選択し、*ストレージ*タブを選択します。

   c. 「* Storage Used - Object Metadata *」グラフにカーソルを合わせ、「Used *」の値を探します。これは、グリッド上にあるオブジェクトメタデータのバイト数を示します。

   d. Used *値を1日あたり1.5TBで割り、データベースのアップグレードに必要な日数を決定します。

4. 手順1、2、3の結果を追加して、アップグレードの合計推定時間を計算します。

例：**StorageGRID 11.4**から**11.5**へのアップグレード時間の見積もり

システムにグリッドノードが 14 個あり、そのうち 8 個が Linux ノードであるとします。また、オブジェクトメタデータの* used *の値が6TBであるとします。

1. 14に30分を掛け、1時間を足します。すべてのノードのアップグレードにかかる推定時間は8時間です。

2. LinuxノードにRPMパッケージまたはDEBパッケージをインストールする時間として、8~15分/ノードが複数必要です。この手順の推定時間は 2 時間です。

3. 6を1.5 TB/日で割ります。データベースのアップグレード*タスクの推定日数は4日です。

   > データベースのアップグレード*タスクの実行中は、新しい機能の使用、ホットフィックスの適用、ノードのリカバリ処理を安全に実行できます。

4. 値をまとめて追加します。システムのStorageGRID 11.5.0へのアップグレードを完了するまでに5日かかります。

アップグレード中にシステムが受ける影響

## アップグレード中に StorageGRID システムがどのような影響を受けるかを理解しておく必要があります。

**StorageGRID** のアップグレードは無停止で実行されます

StorageGRID システムは、アップグレードプロセス中もクライアントアプリケーションからデータを取り込み、読み出すことができます。アップグレード中に一度に 1 つずつグリッドノードが停止されるため、すべてのグリッドノードが使用できなくなることはありません。

継続的な可用性を確保するには、オブジェクトが適切な ILM ポリシーを使用して冗長に格納されていることを確認する必要があります。また、次のいずれかに要求を送信するようにすべての外部の S3 または Swift クライアントを設定する必要があります。

- ハイアベイラビリティ（ HA ）グループとして設定された StorageGRID エンドポイント
- 高可用性のサードパーティ製ロードバランサ
- 各クライアントに複数のゲートウェイノードが必要

- クライアントごとに複数のストレージノード

アプライアンスファームウェアがアップグレードされている

StorageGRID 11.5へのアップグレード中：

- すべてのStorageGRID アプライアンスノードは、StorageGRID アプライアンスインストーラファームウェアバージョン3.5に自動的にアップグレードされます。
- SG6060とSGF6024アプライアンスは、BIOSファームウェアバージョン3B03.EXおよびBMCファームウェアバージョンBMC 3.90.07に自動的にアップグレードされます。
- SG100およびSG1000アプライアンスは、自動的にBIOSファームウェアバージョン3B08.ECおよびBMCファームウェアバージョン4.64.07にアップグレードされます。

アラートがトリガーされる可能性があります

アラートは、サービスの開始と停止、および StorageGRID システムを複数バージョンが混在した環境で使用している場合（一部のグリッドノードで以前のバージョンを実行し、その他のノードはより新しいバージョンにアップグレードしている場合）にトリガーされることがあります。たとえば、サービスが停止しているときに「ノードと通信できません」というアラートが表示されたり、一部のノードがStorageGRID 11.5にアップグレードされても、他のノードでStorageGRID 11.4が実行されているときに「Cassandra communication error *」アラートが表示されることがあります。

通常、これらのアラートはアップグレードが完了するとクリアされます。

アップグレードが完了したら、Grid Managerのダッシュボードで「Recently Resolved alerts」を選択して、アップグレード関連のアラートを確認できます。

StorageGRID 11.5へのアップグレード中に、ストレージノードが停止したときに「ILM placement unAchievable *」アラートがトリガーされることがあります。このアラートは、アップグレードが正常に完了してから1日後も継続する場合があります。

多数の **SNMP** 通知が生成されます

アップグレード中にグリッドノードが停止および再起動されると、多数の SNMP 通知が生成される場合があります。過剰な通知を避けるには、[* SNMPエージェント通知を有効にする*]チェックボックス（* Configuration > Monitoring > SNMP Agent *）をオフにして、アップグレードを開始する前にSNMP通知を無効にします。その後、アップグレードの完了後に通知を再度有効にします。

設定の変更は制限されています

[ 新しい機能を有効にする *] タスクが完了するまで :

- グリッドの設定は変更しないでください。
- 監査レベルの設定は変更しないでください。
- 新しい機能を有効または無効にしないでください。
- ILM 設定を更新しないでください。ILM の動作が不安定になり、正常に動作しない場合があります。
- ホットフィックスの適用やグリッドノードのリカバリは行わないでください。

[* Final Upgrade Steps * （最終アップグレード手順 * ） ] タスクが完了するまで：

- 拡張手順 は実行しないでください。
- 手順 の運用停止は実行しないでください。

アップグレードによるグループおよびユーザアカウントへの影響

## アップグレードの完了後にグループとユーザアカウントを適切に更新できるよう、StorageGRID アップグレードの影響を理解しておく必要があります。

グループの権限とオプションが変更されました

StorageGRID 11.5にアップグレードしたあと、必要に応じて、次の新しい権限とオプションを選択します（* Configuration > Access Control > Admin Groups *）。

| 権限またはオプション | 説明 |
| --- | --- |
| ストレージアプライアンス管理者 | Grid ManagerからSANtricity System Managerのユーザインターフェイスにアクセスするために必要です。 |
| アクセスモード | グループを管理するときに、この新しいオプションに対して「読み取り専用」を選択すると、ユーザーがグループに対して選択した設定や機能を変更できなくなります。読み取り専用アクセスモードのグループ内のユーザは設定を表示できますが、変更することはできません。 |

関連情報

"StorageGRID の管理"

インストールされている**StorageGRID** のバージョンを確認しています

## アップグレードを開始する前に、利用可能な最新のホットフィックスを適用して以前のバージョンの StorageGRID が現在インストールされていることを確認する必要があります。

手順

1. サポートされているブラウザを使用してGrid Managerにサインインします。
2. 「ヘルプ>*バージョン情報*」を選択します。
3. バージョン*が11.4であることを確認します。_x y _。

   StorageGRID 11.4の_x.y_version番号で、次の手順を実行します。

   - メジャーリリースの_x_valueは0（11.4.0）です。
   - マイナーリリースが存在する場合、0以外の_x_valueが存在します（例：11.4.1）。
   - ホットフィックスがある場合は、_y_valueが含まれています（例：11.11.1.0.1）。

   以前のバージョンのStorageGRID を使用している場合は、StorageGRID 11.5にアップグレードする前に、すべてのバージョン11.4にアップグレードする必要があります。StorageGRID 11.5にアップグレードするには、11.4マイナーバージョンのリリースが最も高い必要はありません。

4. StorageGRID 11.4バージョンを使用していない場合は、各リリースの手順に従って、一度に1つのリリースをバージョン11.4にアップグレードする必要があります。

   また、StorageGRID の各バージョンに最新のホットフィックスを適用してから、次のレベルにアップグレードする必要があります。

   使用可能なアップグレードパスの例を次に示します。

5. StorageGRID 11.4が表示されたら、StorageGRID のネットアップのダウンロードページにアクセスし、StorageGRID 11.4._x_versionに利用可能なホットフィックスがあるかどうかを確認します。

   "ネットアップのダウンロード： StorageGRID"

6. StorageGRID 11.4._x_versionに最新のホットフィックスが適用されていることを確認します。
7. 必要に応じて、最新のStorageGRID 11.4._x.y_hotfixをダウンロードしてStorageGRID 11.4._x_versionに適用します。

   ホットフィックスの適用については、リカバリとメンテナンスの手順を参照してください。

例：バージョン**11.3.0.8**から**StorageGRID 11.5**にアップグレードする準備

次の例は、StorageGRID バージョン11.3.0.8からバージョン11.5へのアップグレード準備のためのアップグレード手順を示しています。StorageGRID 11.5にアップグレードするには、システムにStorageGRID 11.4バージョンがインストールされていて、最新のホットフィックスがインストールされている必要があります。

次の順序でソフトウェアをダウンロードしてインストールし、システムをアップグレードする準備をします。

1. 最新の StorageGRID 11.3.0 ._y_hotfix を適用します。
2. StorageGRID 11.4.0 メジャーリリースにアップグレードします。（11.4._x_minorリリースをインストールする必要はありません）。
3. 最新の StorageGRID 11.11.0._y_hotfix を適用します。

関連情報

"StorageGRID の管理"

""

ソフトウェアアップグレードの前提要件の確認

ソフトウェアのアップグレードを開始する前に、アップグレードを正常に完了できるよう、必要なファイル、機器、情報をすべて揃えておく必要があります。

| 項目 | 注： |
| --- | --- |
| StorageGRID アップグレードファイル | 必要なファイルをサービスラップトップにダウンロードする必要があります。<br>• すべてのプラットフォーム： `.upgrade` ファイル。<br>• * Red Hat Enterprise LinuxまたはCentOS *上の任意のノード： `.upgrade` ファイルおよびRPMファイル (`.zip` または `.tgz`)<br>• * UbuntuまたはDebian上の任意のノード*： `.upgrade` ファイルとDEBファイル (`.zip` または `.tgz`) |
| サービスラップトップ | サービスラップトップには次のものが必要です。<br>• ネットワークポート<br>• SSH クライアント（ PuTTY など） |
| サポートされている Web ブラウザ | サービスラップトップのWebブラウザがStorageGRID 11.5でサポートされていることを確認する必要があります。<br>"Web ブラウザの要件"<br>*注：StorageGRID 11.5ではブラウザサポートが変更されています。サポート対象のバージョンを使用していることを確認してください。 |
| リカバリパッケージ (`.zip`)ファイル | アップグレード前に、アップグレード中に問題が発生した場合に備えて、最新のリカバリパッケージファイルをダウンロードする必要があります。<br>プライマリ管理ノードをアップグレードしたら、リカバリパッケージファイルの新しいコピーをダウンロードして安全な場所に保存する必要があります。更新されたリカバリパッケージファイルは、障害発生時のシステムのリストアに使用できます。<br>"リカバリパッケージをダウンロードしています" |
| `Passwords.txt` ファイル。 | このファイルは、リカバリパッケージの一部であるSAIDパッケージに含まれています `.zip` ファイル。最新バージョンのリカバリパッケージを入手する必要があります。 |
| プロビジョニングパスフレーズ | このパスフレーズは、 StorageGRID システムが最初にインストールされるときに作成されて文書化されます。プロビジョニングパスフレーズは、に表示されません `Passwords.txt` ファイル。 |

| 項目 | 注： |
| --- | --- |
| 関連ドキュメント | • StorageGRID 11.5リリースノートアップグレードを開始する前に、このドキュメントに記載されている情報をよくお読みください。<br>• StorageGRID の管理手順<br>• Linux環境をアップグレードする場合は、使用しているLinuxプラットフォーム用のStorageGRID インストール手順<br>• 必要に応じて、その他の StorageGRID ドキュメント |

関連情報

"Web ブラウザの要件"

"StorageGRID の管理"

"Red Hat Enterprise Linux または CentOS をインストールします"

"Ubuntu または Debian をインストールします"

"VMware をインストールする"

"StorageGRID アップグレードファイルをダウンロードします"

"リカバリパッケージをダウンロードしています"

"リリースノート"

**Web** ブラウザの要件

サポートされている Web ブラウザを使用する必要があります。

| **Web** ブラウザ | サポートされる最小バージョン |
| --- | --- |
| Google Chrome | 87 |
| Microsoft Edge の場合 | 87 |
| Mozilla Firefox | 84 |

ブラウザウィンドウの幅を推奨される値に設定してください。

| ブラウザの幅 | ピクセル |
| --- | --- |
| 最小（ Minimum ） | 1024 |
| 最適 | 1280 |

**StorageGRID** アップグレードファイルをダウンロードします

# StorageGRID システムをアップグレードする前に、必要なファイルをサービスラップトップにダウンロードする必要があります。

必要なもの

アップグレードするStorageGRID ソフトウェアのバージョンに必要な修正プログラムをすべてインストールしておく必要があります。リカバリとメンテナンスの手順のホットフィックス手順 を参照してください。

このタスクについて

をダウンロードする必要があります `.upgrade` あらゆるプラットフォームに対応したアーカイブ。Linuxホストに導入されているノードがある場合は、アップグレードを開始する前にインストールするRPMアーカイブまたはDEBアーカイブもダウンロードする必要があります。

手順

1. ネットアップの StorageGRID ダウンロードページにアクセスします。

   "ネットアップのダウンロード： StorageGRID"

2. 最新のリリースをダウンロードするボタンを選択するか、ドロップダウンメニューから別のバージョンを選択して、「 * Go * 」を選択します。

   StorageGRID ソフトウェアのバージョンの形式は、 11.*x.y*. です。StorageGRID ホットフィックスの形式は、 11._x.y.z _ です。

3. ネットアップアカウントのユーザ名とパスワードを使用してサインインします。
4. 「注意 / 必ずお読みください」という記述が表示されたら、それを読んでチェックボックスを選択してください。

   このステートメントは、リリースに必要なホットフィックスがある場合に表示されます。

5. エンドユーザライセンス契約を読み、チェックボックスをオンにして、「 * 同意して続行 * 」を選択します。

   選択したバージョンのダウンロードページが表示されます。このページには 3 つの列があります。

   - StorageGRID をインストールします
   - StorageGRID をアップグレードします
   - StorageGRID アプライアンスのサポートファイル

6. [* Upgrade StorageGRID （アップグレードファイル）]列で、を選択してダウンロードします `.upgrade` Archiveサービスの略。

   どのプラットフォームにもが必要です `.upgrade` Archiveサービスの略。

7. Linuxホストに導入されているノードがある場合は、RPMアーカイブまたはDEBアーカイブもダウンロードします `.tgz` または `.zip` の形式で入力し

   アップグレードを開始する前に、すべてのLinuxノードにRPMアーカイブまたはDEBアーカイブをインストールする必要があります。

SG100 または SG1000 では追加のファイルは必要ありません。

を選択します `.zip` ファイルサービスラップトップでWindowsを実行している場合。

- Red Hat Enterprise LinuxまたはCentOS
  `StorageGRID-Webscale-version-RPM-uniqueID.zip` [+]
  `StorageGRID-Webscale-version-RPM-uniqueID.tgz`
- UbuntuまたはDebian+
  `StorageGRID-Webscale-version-DEB-uniqueID.zip` [+]
  `StorageGRID-Webscale-version-DEB-uniqueID.tgz`

関連情報

"Linux：すべてのホストにRPMパッケージまたはDEBパッケージをインストールします"

""

リカバリパッケージをダウンロードしています

## リカバリパッケージファイルを使用すると、障害発生時に StorageGRID システムをリストアできます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- プロビジョニングパスフレーズが必要です。
- 特定のアクセス権限が必要です。

このタスクについて

StorageGRID システムでグリッドトポロジの変更を行う前、またはソフトウェアをアップグレードする前に、現在のリカバリパッケージファイルをダウンロードしてください。グリッドトポロジを変更するかソフトウェアをアップグレードしたあとに、リカバリパッケージの新しいコピーをダウンロードします。

手順

1. [* Maintenance * （メンテナンス） ] > [* System * （システム * ） ] > [* Recovery Package] （リカバリパッケージ * ）
2. プロビジョニングパスフレーズを入力し、 * ダウンロードの開始 * を選択します。

   ダウンロードがすぐに開始されます。

3. ダウンロードが完了したら、次の手順を実行
   a. を開きます `.zip` ファイル。
   b. が含まれていることを確認します `gpt-backup` ディレクトリと内部 `.zip` ファイル。
   c. 内側を引き出します `.zip` ファイル。
   d. を開くことができることを確認します `Passwords.txt` ファイル。
4. ダウンロードしたリカバリパッケージファイルをコピーします (`.zip`)を2箇所に安全に、安全に、そして

別々の場所に移動します。

リカバリパッケージファイルには StorageGRID システムからデータを取得するための暗号キーとパスワードが含まれているため、安全に保管する必要があります。

関連情報

"StorageGRID の管理"

ソフトウェアをアップグレードする前に、システムの状態を確認します

StorageGRID システムをアップグレードする前に、システムがアップグレードできる状態にあることを確認する必要があります。システムが正常に稼働し、すべてのグリッドノードが動作している必要があります。

手順

1. サポートされているブラウザを使用してGrid Managerにサインインします。
2. アクティブなアラートがないかを確認し、ある場合は解決します。

   特定のアラートの詳細については、監視とトラブルシューティングの手順を参照してください。

3. 競合するグリッドタスクがアクティブまたは保留中でないことを確認します。
   a. Support > Tools > Grid Topology *を選択します。
   b. *site* * > * *_primary Admin Node** > * CMN * > * Grid Tasks * > * Configuration * を選択します。

      情報ライフサイクル管理評価（ ILME ）タスクは、ソフトウェアのアップグレードと同時に実行できる唯一のグリッドタスクです。

   c. 他のグリッドタスクがアクティブまたは保留中の場合は、それらが終了するまで、またはロックが解放されるまで待ちます。

      タスクが終了しない、またはロックが解放されない場合は、テクニカルサポートにお問い合わせください。

4. アップグレード前に、11.5バージョンのネットワークガイドラインで内部ポートと外部ポートのリストを参照し、必要なすべてのポートが開いていることを確認します。

   カスタムのファイアウォールポートが開いている場合は、アップグレードの事前確認中に通知されます。アップグレードを続行する前に、テクニカルサポートに連絡する必要があります。

関連情報

"トラブルシューティングを監視します"

"StorageGRID の管理"

""

"ネットワークガイドライン"

## アップグレードを実行する

### Software Upgradeページの指示に従って、必要なファイルをアップロードし、StorageGRID システム内のすべてのグリッドノードをアップグレードします。

必要なもの

次の点に注意してください。

- Grid Managerを使用して、プライマリ管理ノードからすべてのデータセンターサイトのすべてのグリッドノードをアップグレードする必要があります。
- 問題を検出して解決するために、実際のアップグレードを開始する前にアップグレードの事前確認を手動で実行できます。アップグレードを開始した場合も、同じ事前確認が実行されます。事前確認が失敗すると、アップグレードプロセスが停止し、解決のためにテクニカルサポートの支援が必要になる場合があります。
- アップグレードを開始すると、プライマリ管理ノードが自動的にアップグレードされます。
- プライマリ管理ノードのアップグレードが完了したら、次にアップグレードするグリッドノードを選択できます。
- アップグレードを完了するには、StorageGRID システムですべてのグリッドノードをアップグレードする必要がありますが、個 々 のグリッドノードは任意の順序でアップグレードしてかまいません。個 々 のグリッドノード、グリッドノードのグループ、またはすべてのグリッドノードを選択できます。グリッドノードの選択プロセスを必要な回数だけ繰り返し、すべてのサイトのすべてのグリッドノードをアップグレードします。
- グリッドノードでアップグレードを開始すると、そのノードのサービスは停止します。グリッドノードはあとでリブートされます。グリッドノードを停止およびリブートして問題ないことを確認するまでは、そのノードのアップグレードを承認しないでください。
- すべてのグリッドノードがアップグレードされると、新しい機能が有効になり、運用を再開できます。ただし、バックグラウンドの*アップグレードデータベース*タスクおよび*最終アップグレード手順*タスクが完了するまでは、運用停止または拡張手順 の実行を待つ必要があります。
- アップグレードを開始したハイパーバイザープラットフォームでアップグレードを完了する必要があります。

手順

1. "Linux：すべてのホストにRPMパッケージまたはDEBパッケージをインストールします"
2. "アップグレードを開始する"
3. "グリッドノードのアップグレードとアップグレードの完了"
4. "Metadata Reserved Space設定を拡張しています"

関連情報

"StorageGRID の管理"

"アップグレード所要時間の見積もり"

**Linux**：すべてのホストに**RPM**パッケージまたは**DEB**パッケージをインストールします

# Linux ホストに StorageGRID ノードが導入されている場合は、アップグレードを開始する前に、これらの各ホストに追加の RPM パッケージまたは DEB パッケージをインストールする必要があります。

必要なもの

次のいずれかをダウンロードしておく必要があります `.tgz` または `.zip` ネットアップのStorageGRID ダウンロードページにあるファイル。

> を使用します `.zip` ファイルサービスラップトップでWindowsを実行している場合。

| **Linux** プラットフォーム | 追加ファイル（ **1** つ選択） |
| --- | --- |
| Red Hat Enterprise Linux または CentOS | • `StorageGRID-Webscale-version-RPM-uniqueID.zip`<br>• `StorageGRID-Webscale-version-RPM-uniqueID.tgz` |
| Ubuntu または Debian | • `StorageGRID-Webscale-version-DEB-uniqueID.zip`<br>• `StorageGRID-Webscale-version-DEB-uniqueID.tgz` |

手順

1. インストールファイルから RPM パッケージまたは DEB パッケージを展開します。
2. すべての Linux ホストに RPM パッケージまたは DEB パッケージをインストールします。

   使用している Linux プラットフォーム用のインストール手順の StorageGRID ホストサービスのインストール手順を参照してください。

   "Red Hat Enterprise Linux または CentOS をインストールします"

   "Ubuntu または Debian をインストールします"

   新しいパッケージは追加のパッケージとしてインストールされます。既存のパッケージは削除しないでください。

アップグレードを開始する

# アップグレードを実行する準備ができたら、ダウンロードしたファイルを選択してプロビジョニングパスフレーズを入力します。オプションとして、実際のアップグレードを実行する前にアップグレードの事前確認を実行することもできます。

必要なもの

のすべての考慮事項を確認し、のすべての手順を完了しておきます "アップグレードの計画と準備"。

手順

1. サポートされているブラウザを使用してGrid Managerにサインインします。

2. [* Maintenance * （メンテナンス） ] > [* System * （ * システム * ） ] > [* Software Update * （ソフトウェア・アップデート

   Software Update ページが表示されます。

3. StorageGRID アップグレード * を選択します。

   StorageGRID のアップグレードページが表示されます。このページには、アップグレードの実行後にプライマリ管理ノードがリブートされた場合や管理APIが再起動された場合を除き、最後に完了したアップグレードの日時が表示されます。

4. を選択します `.upgrade` ダウンロードしたファイル。

   a. [ * 参照 * ] を選択します。

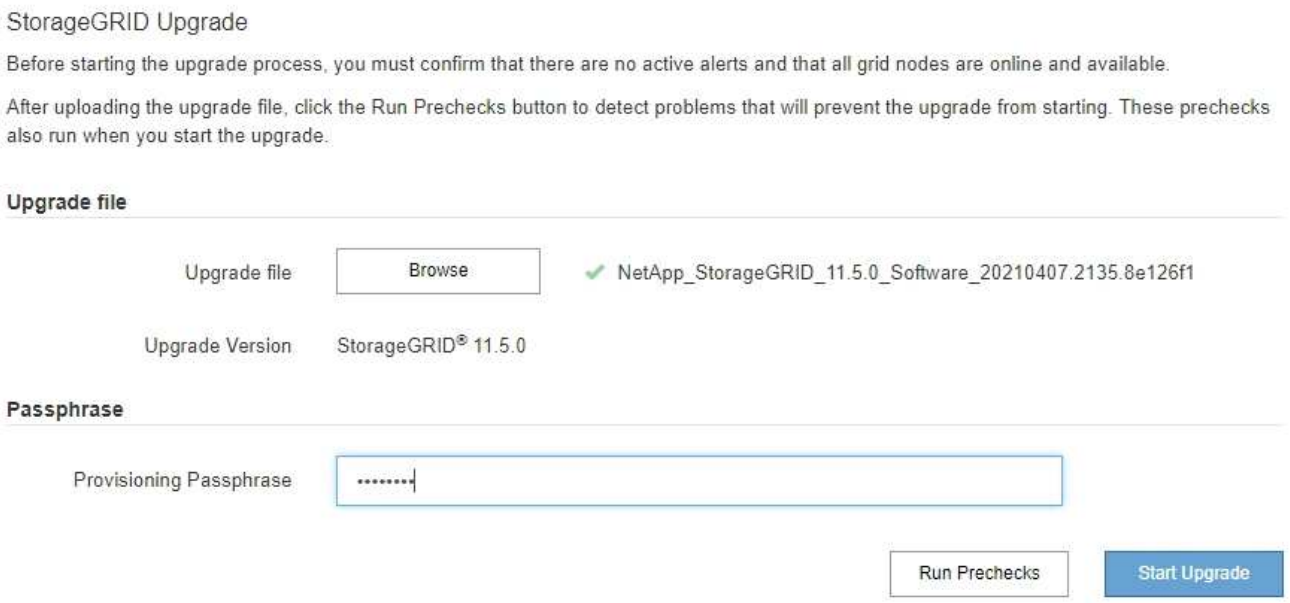
   b. 次のファイルを探して選択します。
   `NetApp_StorageGRID_version_Software_uniqueID.upgrade`

   c. 「 * 開く * 」を選択します。

      ファイルがアップロードされて検証されます。検証プロセスが完了したら、アップグレードファイル名の横に緑のチェックマークが表示されます。

5. プロビジョニングパスフレーズをテキストボックスに入力します。

   Run PreChecks * ボタンと * Start Upgrade * ボタンが有効になります。



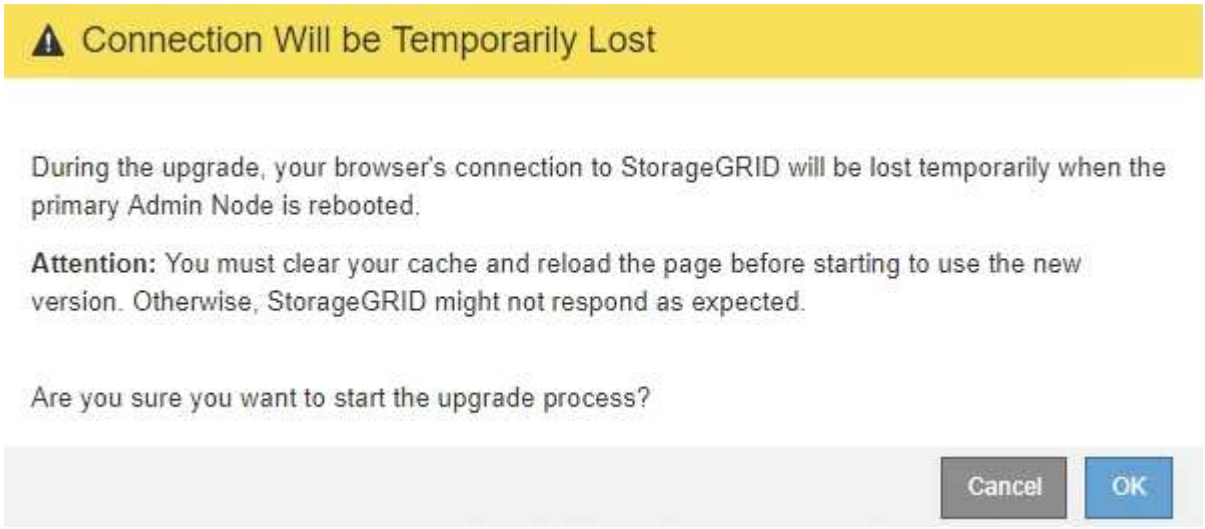

6. 実際のアップグレードを開始する前にシステムの状態を検証する場合は、*事前チェックを実行*を選択します。その後、事前確認で報告されたエラーを解決します。

   カスタムのファイアウォールポートが開いている場合は、事前確認の実行中に通知されます。アップグレードを続行する前に、テクニカルサポートに連絡する必要があります。

アップグレードの開始*を選択した場合も、同じ事前確認が実行されます。[Run Prechecks]を選択すると、アップグレードを開始する前に問題を検出して解決できます。

7. アップグレードを実行する準備ができたら、 * アップグレードを開始 * を選択します。

   プライマリ管理ノードのリブート時にブラウザの接続が失われることを通知する警告が表示されます。プライマリ管理ノードが再び使用できるようになったら、WebブラウザのキャッシュをクリアしてSoftware Upgradeページをリロードする必要があります。




8. 警告を確認してアップグレードプロセスを開始するには、「 * OK 」を選択します。

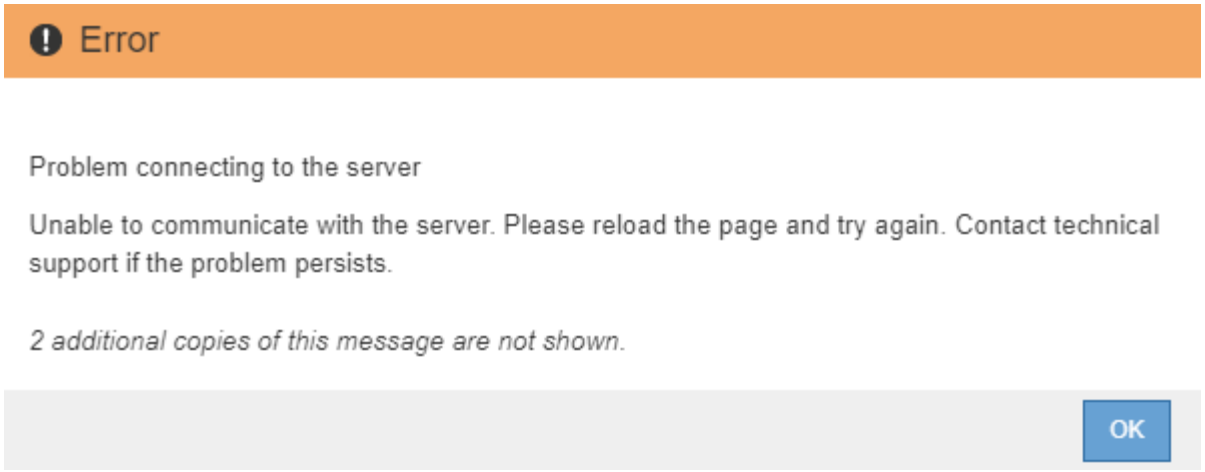
   アップグレードを開始すると、次の処理が

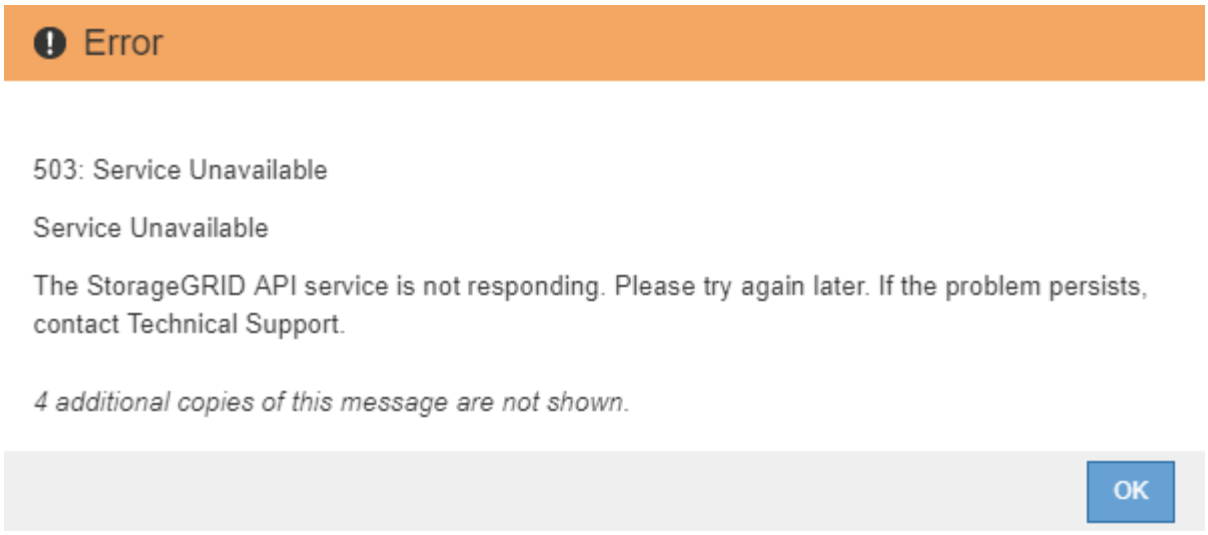
   a. アップグレードの事前確認が実行されます。

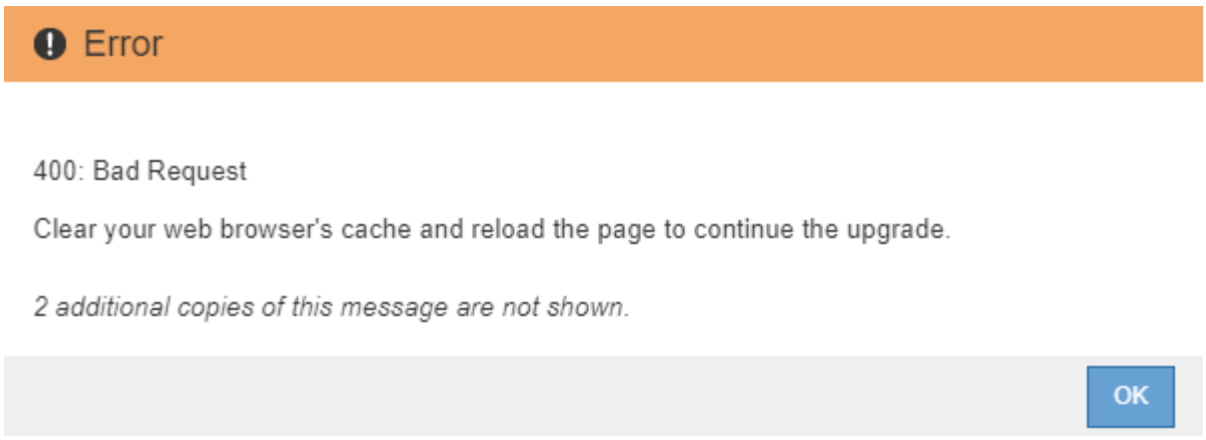
      事前確認のエラーが報告された場合は、それらを解決し、 * アップグレードの開始 * を再度選択します。

   b. プライマリ管理ノードがアップグレードされます。これには、サービスの停止、ソフトウェアのアップグレード、サービスの再開が含まれます。プライマリ管理ノードのアップグレード中はGrid Managerにアクセスできません。監査ログも使用できなくなります。このアップグレードには最大 30 分かかることがあります。

      プライマリ管理ノードのアップグレード中に、次のエラーメッセージが繰り返し表示されますが、このエラーは無視してかまいません。




9. プライマリ管理ノードのアップグレードが完了したら、Webブラウザのキャッシュをクリアし、再度サインインして、ソフトウェアのアップグレードページをリロードします。

   手順については、 Web ブラウザのドキュメントを参照してください。

   Web ブラウザのキャッシュをクリアするのは、前のバージョンのソフトウェアで使用していた古いリソースを削除するためです。

関連情報

"アップグレードの計画と準備"

グリッドノードのアップグレードとアップグレードの完了

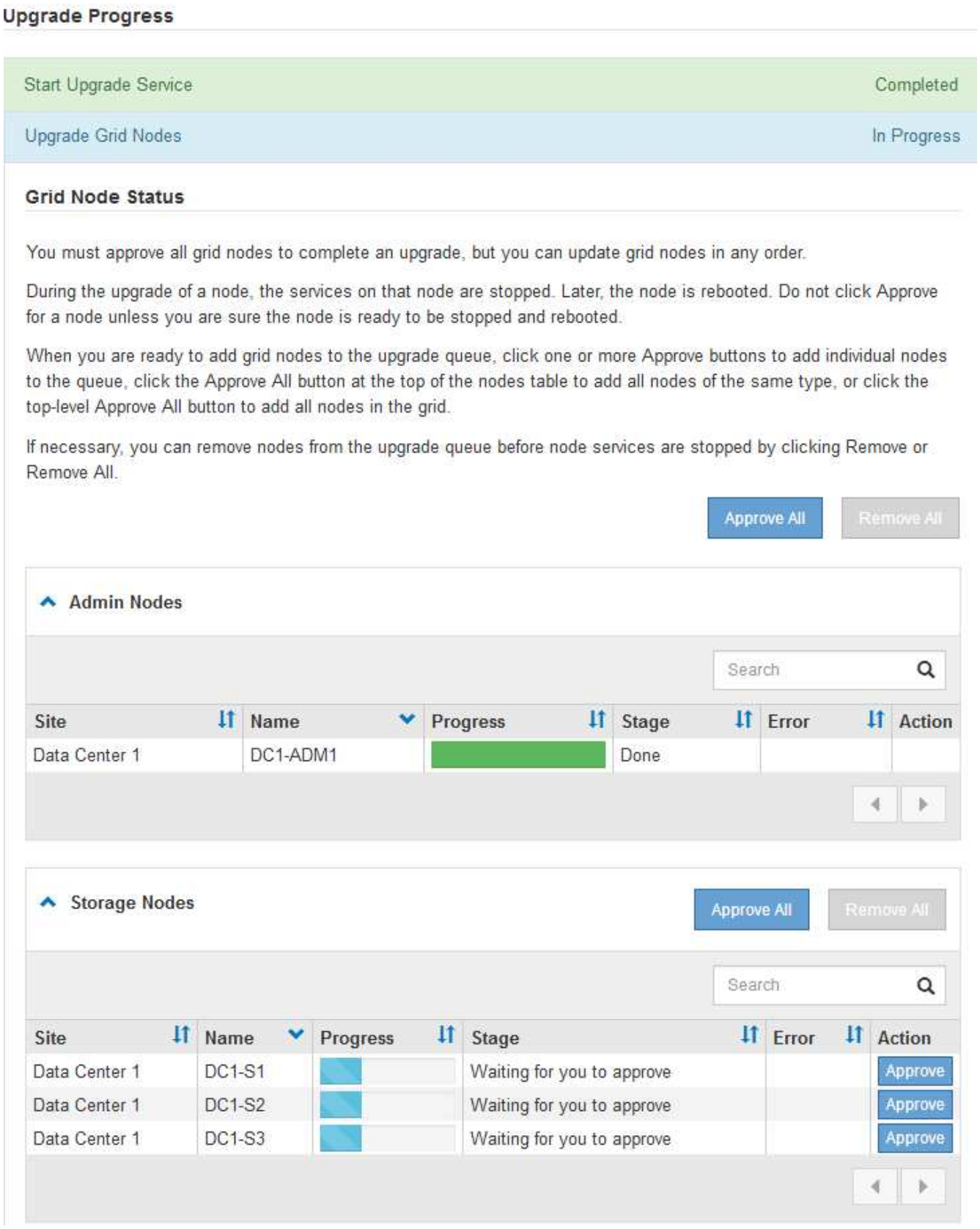
プライマリ管理ノードをアップグレードしたあと、StorageGRID システムに含まれる他のグリッドノードをすべてアップグレードする必要があります。個 々 のグリッドノード、グリッドノードのグループ、またはすべてのグリッドノードを選択して、アップグレードの順序をカスタマイズできます。

手順

1. Software UpgradeページのUpgrade Progressセクションを確認します。このセクションには、各メジャーアップグレードタスクに関する情報が記載されています。
   a. * アップグレード・サービスの開始 * が最初のアップグレード・タスクですこのタスクでは、ソフトウェアファイルがグリッドノードに配信され、アップグレードサービスが開始されます。
   b. * Start Upgrade Service * タスクが完了すると、 * Upgrade Grid Nodes * タスクが開始されます。
   c. * Upgrade Grid Nodes * タスクの実行中は、 Grid Node Status テーブルが表示され、システム内の各グリッドノードのアップグレードステージが示されます。
2. グリッドノードがグリッドノードステータステーブルに表示されたあと、グリッドノードを承認する前に、リカバリパッケージの新しいコピーをダウンロードします。

   プライマリ管理ノードでソフトウェアバージョンをアップグレードしたあとで、リカバリパッケージファイルの新しいコピーをダウンロードする必要があります。リカバリパッケージファイルは、障害が発生した場合にシステムをリストアするために使用します。

3. Grid Node Status テーブルの情報を確認します。グリッドノードは、管理ノード、 API ゲートウェイノード、ストレージノード、およびアーカイブノードの各セクションに分類されています。




このページが最初に表示されたとき、グリッドノードは次のいずれかの段階にあります。

- Done （プライマリ管理ノードのみ）
- アップグレードを準備中

- ソフトウェアのダウンロードがキューに登録され
- ダウンロード中です
- 承認待ちです

4. アップグレードキューに追加する準備ができたグリッドノードを承認します。同じタイプの承認済みノードが一度に 1 つずつアップグレードされます。

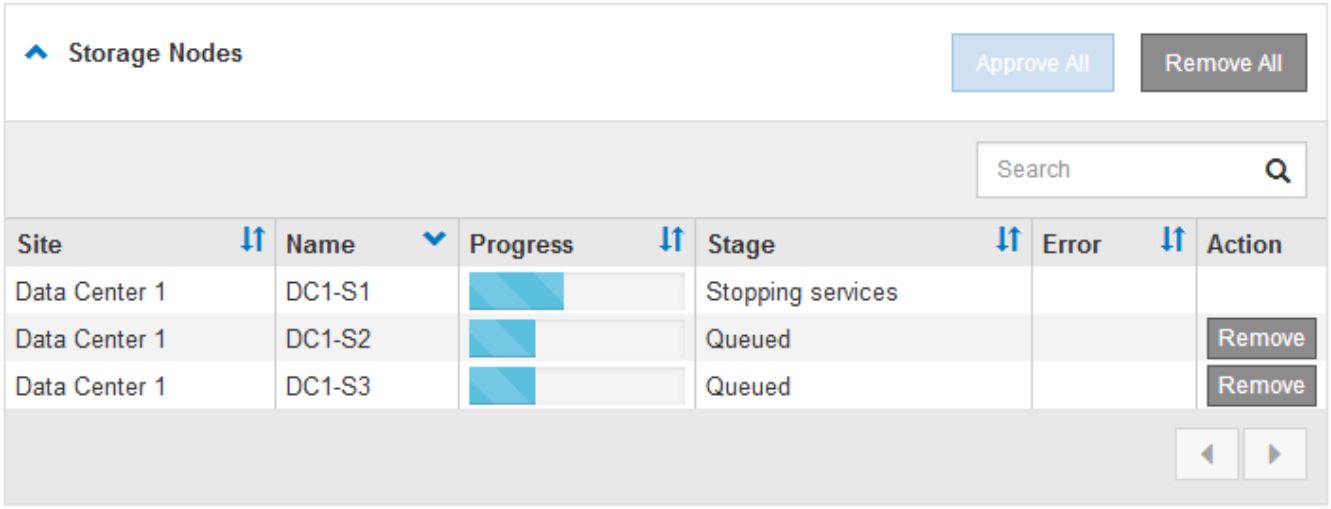
   ノードのアップグレード順序が重要な場合は、ノードまたはノードグループを 1 つずつ承認し、各ノードでアップグレードが完了するまで待ってから、次のノードまたはノードグループを承認します。

   > グリッドノードでアップグレードを開始すると、そのノードのサービスは停止します。グリッドノードはあとでリブートされます。このような処理を実行すると、ノードと通信しているクライアントで原因 サービスが中断する可能性があります。ノードを停止およびリブートして問題ないことを確認するまでは、そのノードのアップグレードを承認しないでください。

   - 1 つまたは複数の * 承認 * ボタンを選択して、アップグレードキューに 1 つまたは複数のノードを追加します。
   - 各セクション内の * すべて承認 * ボタンを選択して、同じタイプのすべてのノードをアップグレードキューに追加します。
   - グリッド内のすべてのノードをアップグレードキューに追加するには、最上位の * すべて承認 * ボタンを選択します。

5. アップグレードキューからノードまたはすべてのノードを削除する必要がある場合は、「* Remove 」または「 Remove All *」を選択します。

   例に示すように、Stageが* Stopping services に達すると、 Remove *ボタンが非表示になり、ノードを削除できなくなります。




6. 各ノードのアップグレード段階の処理が終わるまで待機します。各段階には、Queued、Stopping services、Stopping container、Cleaning up Docker images、Upgrading base OS packages、Rebaling 、and Starting servicesがあります。

アプライアンスノードの Upgrading base OS packages ステージに達すると、アプライアンス上の StorageGRID アプライアンスインストーラソフトウェアが更新されます。この自動プロセスにより、 StorageGRID アプライアンスインストーラのバージョンが StorageGRID ソフトウェアのバージョンと常に同期された状態になります。

すべてのグリッドノードをアップグレードすると、「Upgrade Grid Nodes *」タスクが完了と表示されます。残りのアップグレードタスクは自動的にバックグラウンドで実行されます。

7. 機能の有効化*タスクが完了すると（すぐに実行されます）、アップグレードされたStorageGRID バージョンの新機能の使用を開始できます。

   たとえば、StorageGRID 11.5にアップグレードするときに、S3オブジェクトロックを有効にするか、キー管理サーバを設定するか、Metadata Reserved Space設定を拡張できます。

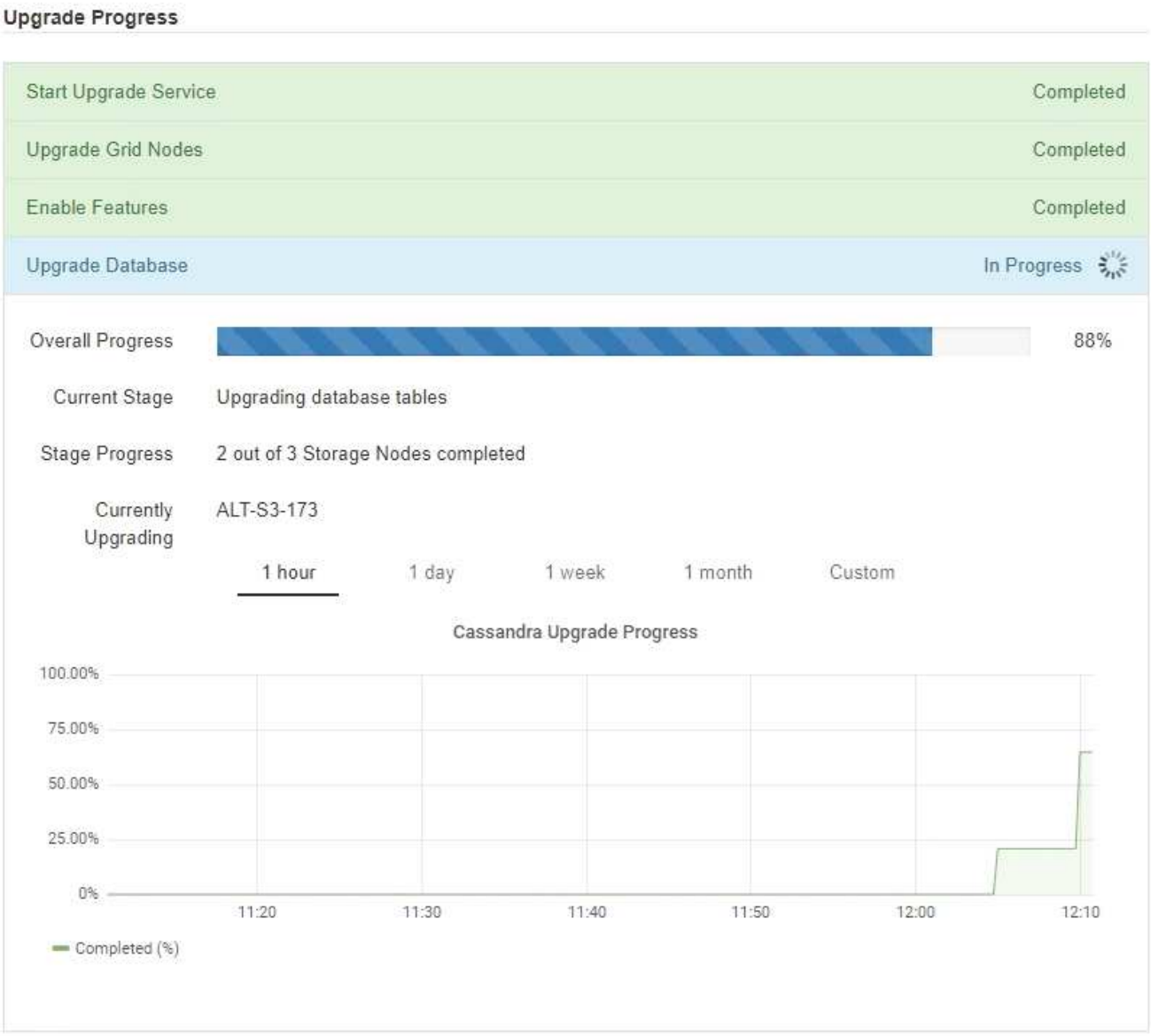
   "Metadata Reserved Space設定を拡張しています"

8. *データベースのアップグレード*タスクの進捗状況を定期的に監視します。

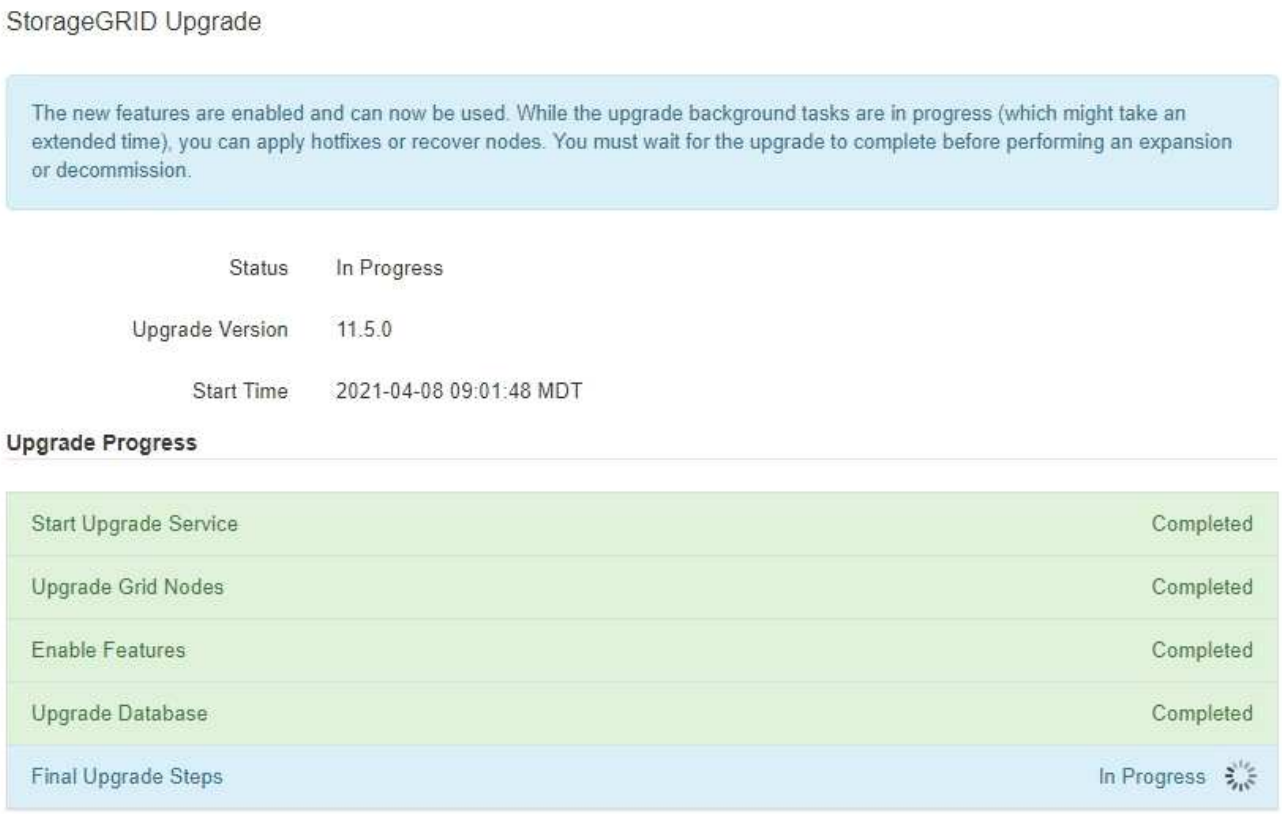
   このタスクの実行中、各ストレージノード上のCassandraデータベースがアップグレードされます。

   データベースのアップグレード*タスクが完了するまでに数日かかることがあります。このバックグラウンドタスクの実行時に、ホットフィックスの適用やノードのリカバリが可能です。ただし、最終アップグレード手順*タスクが完了するまで待ってから、拡張または手順 の運用停止を実行する必要があります。

   このグラフを確認して、各ストレージノードの進捗状況を監視できます。

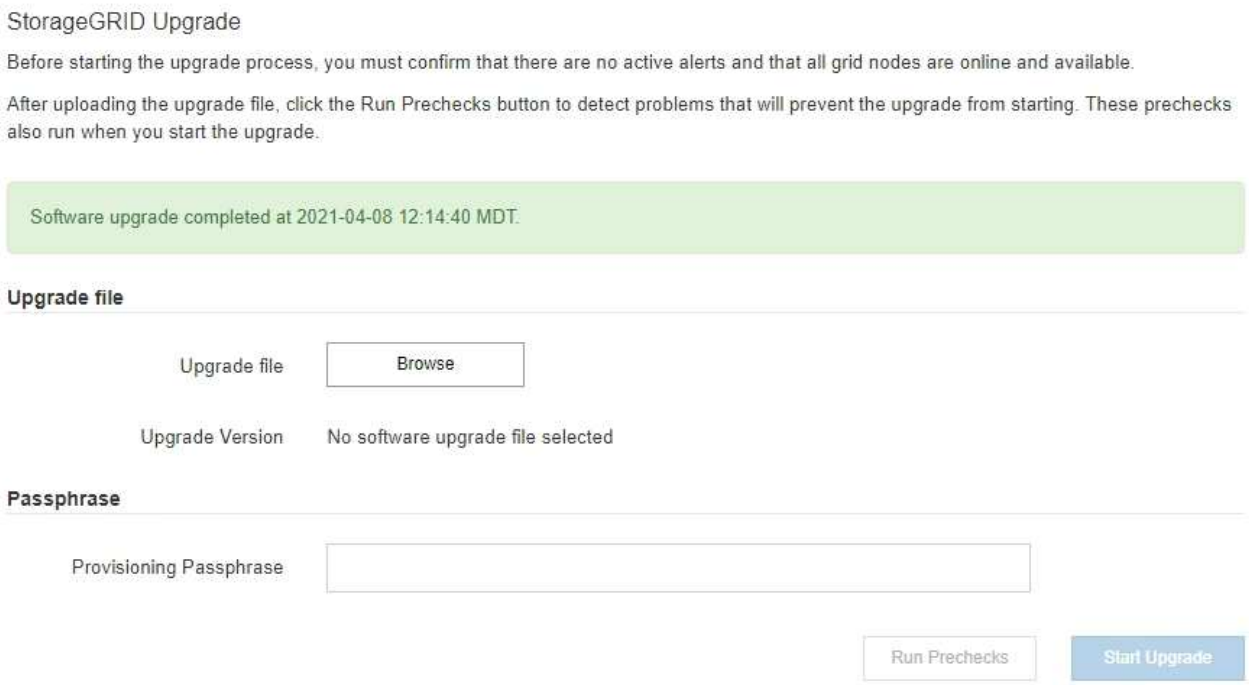



9. データベースのアップグレード * タスクが完了したら、 * 最終アップグレード手順 * タスクが完了するまで数分待ちます。




最終アップグレード手順タスクが完了すると、アップグレードが完了します。

10. アップグレードが正常に完了したことを確認します。
    a. サポートされているブラウザを使用してGrid Managerにサインインします。
    b. 「ヘルプ>*バージョン情報*」を選択します。
    c. 表示されたバージョンが想定どおりであることを確認します。
    d. [* Maintenance * （メンテナンス） ] > [* System * （ * システム * ） ] > [* Software Update * （ソフトウェア・アップデート次に、* StorageGRID アップグレード*を選択します。
    e. 緑のバナーが表示されていて、ソフトウェアのアップグレードが予定の日時に完了していることを確認します。




11. グリッドの動作が正常に戻っていることを確認します。
    a. サービスが正常に動作していること、および予期しないアラートが発生していないことを確認してください。
    b. StorageGRID システムへのクライアント接続が想定どおり動作していることを確認する。
12. ネットアップのダウンロードページでStorageGRID を確認し、インストールしたStorageGRID バージョンに対応したホットフィックスがないかどうかを確認します。

    "ネットアップのダウンロード： StorageGRID"

    StorageGRID 11.5._x.y_version の番号で、次の手順を実行します。

    - メジャーリリースの_x_valueは0（11.5.0）です。
    - マイナーリリースがある場合、0以外の値（11.5.1など）が_x_valueになっています。
    - ホットフィックスがある場合は、_y_value（例：11.5.0.1）です。
13. 該当する場合は、最新のホットフィックスをダウンロードしてStorageGRID バージョンに適用します。

    ホットフィックスの適用については、リカバリとメンテナンスの手順を参照してください。

関連情報

"リカバリパッケージをダウンロードしています"

""

**Metadata Reserved Space**設定を拡張しています

StorageGRID 11.5にアップグレードしたあとに、ストレージノードがRAMおよび使用可能なスペースの特定の要件を満たしている場合は、Metadata Reserved Spaceシステム

設定を拡張できることがあります。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限または Grid Topology Page Configuration 権限と Other Grid Configuration 権限が必要です。
- StorageGRID 11.5へのアップグレードが開始され、「新機能を有効にする」*アップグレードタスクが完了しました。

このタスクについて

StorageGRID 11.5へのアップグレード後に、システム全体のMetadata Reserved Space設定を8TBに手動で拡張できることがあります。11.5へのアップグレード後にメタデータスペースをリザーブすると、以降のハードウェアおよびソフトウェアのアップグレードが簡単になります。

次の両方に該当する場合にのみ、「 Metadata Reserved Space 」設定の値を増やすことができます。

- システムの任意のサイトのストレージノードには、それぞれ 128GB 以上の RAM が搭載されています。
- システムの任意のサイトのストレージノードには、ストレージボリューム 0 上に十分な利用可能スペースがあります。

この設定を大きくすると、すべてのストレージノードのストレージボリューム 0 でオブジェクトストレージに使用できるスペースが同時に減少することに注意してください。そのため、想定されるオブジェクトメタデータの要件に基づいて、 Metadata Reserved Space を 8TB 未満の値に設定することを推奨します。

> 一般的には、より低い値ではなく、より高い値を使用することをお勧めします。Metadata Reserved Space 設定が大きすぎる場合は、あとで設定を縮小できます。一方、値をあとで大きくした場合は、オブジェクトデータを移動してスペースを解放しなければならないことがあります。

Metadata Reserved Space設定が、特定のストレージノードでオブジェクトメタデータストレージに使用できるスペースにどのように影響するかについての詳細な説明は、StorageGRID の管理手順を参照して「オブジェクトメタデータストレージの管理」を検索してください。

"StorageGRID の管理"

手順

1. サポートされているブラウザを使用してGrid Managerにサインインします。
2. 現在の Metadata Reserved Space 設定を確認します。
   a. * Configuration > System Settings > Storage Options *を選択します。
   b. 「ストレージウォーターマーク」セクションで、「 * Metadata Reserved Space * 」の値を確認します。
3. この値を増やすには、各ストレージノードのストレージボリューム 0 に十分な利用可能スペースがあることを確認してください。
   a. [ノード（ Nodes）]を選択し
   b. グリッドの最初のストレージノードを選択します。
   c. Storage （ストレージ）タブを選択します。

d. Volumes セクションで、 * /var/local/rangedb/0 * エントリを探します。

e. 使用可能な値が、使用する新しい値と現在の Metadata Reserved Space 値の差以上であることを確認します。

   たとえば、 Metadata Reserved Space 設定が現在 4TB の場合に、 6TB に拡張するには、使用可能な値を 2TB 以上にする必要があります。

f. すべてのストレージノードに対して上記の手順を繰り返します。

   - 1 つ以上のストレージノードに十分な利用可能スペースがない場合は、 Metadata Reserved Space の値を増やすことはできません。この手順を続行しないでください。
   - 各ストレージノードのボリューム 0 に十分な利用可能スペースがある場合は、次の手順に進みます。

4. 各ストレージノードに 128GB 以上の RAM があることを確認してください。

   a. [ノード（ Nodes）]を選択し

   b. グリッドの最初のストレージノードを選択します。

   c. [* ハードウェア * ] タブを選択します。

   d. メモリ使用状況グラフにカーソルを合わせます。合計メモリ * が 128 GB 以上であることを確認します。

   e. すべてのストレージノードに対して上記の手順を繰り返します。

      - 1 つ以上のストレージノードに使用可能な合計メモリが十分にない場合は、 Metadata Reserved Space の値を増やすことはできません。この手順を続行しないでください。
      - 各ストレージノードの合計メモリが 128GB 以上の場合は、次の手順に進みます。

5. Metadata Reserved Space 設定を更新します。

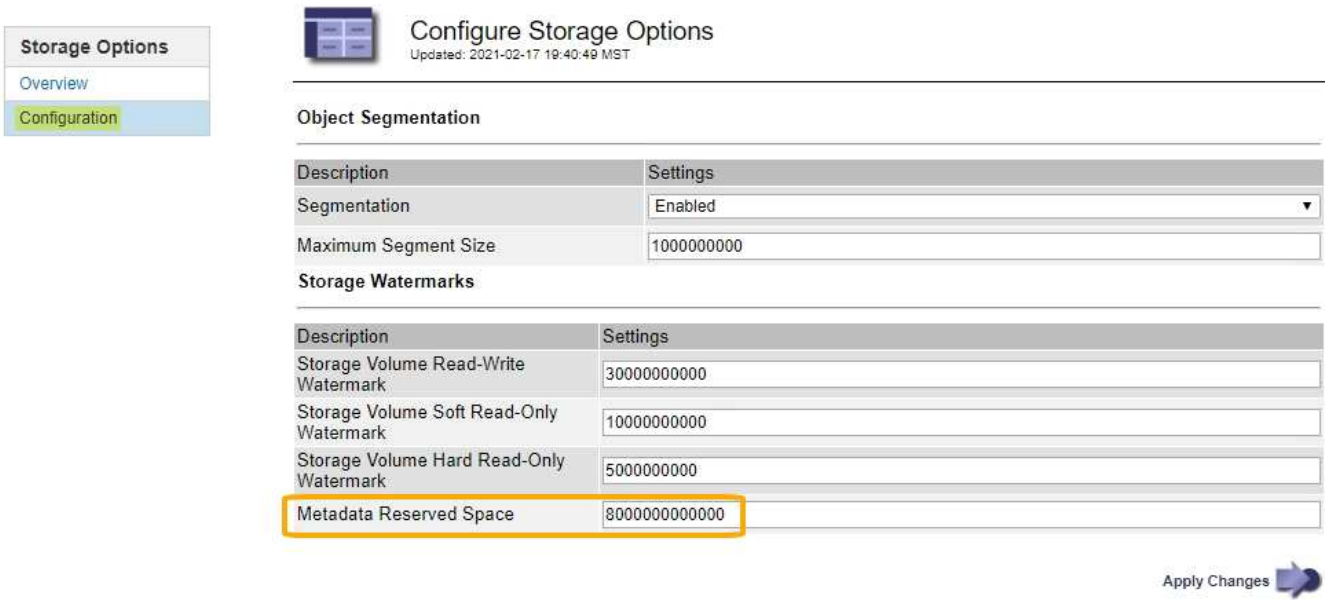
   a. * Configuration **>** System Settings **>** Storage Options *を選択します。

   b. [ 構成 ] タブを選択します。

   c. [ 記憶域の透かし ] セクションで、 [ * Metadata Reserved Space * ] を選択します。

   d. 新しい値を入力します。

      たとえば、サポートされている最大値である 8TB を入力するには、「 * 8000000000000 * （ 8 、 0 が 12 個）」と入力します。




a. 「 * 変更を適用する * 」を選択します。

## アップグレードの問題のトラブルシューティング

アップグレードが正常に完了しない場合は、問題 を自分で解決できることがあります。問題 を解決できない場合は、テクニカルサポートに連絡する前に、必要な情報を収集する必要があります。

次のセクションでは、アップグレードが部分的に失敗した場合のリカバリ方法について説明します。アップグレード問題 を解決できない場合は、テクニカルサポートにお問い合わせください。

### アップグレードの事前確認エラー

問題を検出して解決するために、実際のアップグレードを開始する前にアップグレードの事前確認を手動で実行できます。事前確認で報告されるほとんどのエラーには、問題 の解決方法が表示されます。サポートが必要な場合は、テクニカルサポートにお問い合わせください。

### プロビジョニングに失敗しました

自動プロビジョニングプロセスが失敗する場合は、テクニカルサポートにお問い合わせください。

### グリッドノードがクラッシュするか起動しない

アップグレードプロセス中にグリッドノードがクラッシュする、またはアップグレードの終了後に正常に起動しない場合は、テクニカルサポートに調査を依頼して、根本的な問題を修正してください。

### データの取り込みまたは読み出しが中断される

グリッドノードをアップグレードしていないときにデータの取り込みまたは読み出しが突然中断する場合は、テクニカルサポートにお問い合わせください。

データベースのアップグレードエラーです

データベースのアップグレードがエラーで失敗した場合は、アップグレードを再試行します。それでも失敗する場合は、テクニカルサポートにお問い合わせください。

関連情報

"ソフトウェアのアップグレード前のシステム状態の確認"

ユーザインターフェイスの問題のトラブルシューティング

## StorageGRID ソフトウェアを新しいバージョンにアップグレードしたあとに、 Grid Manager またはテナントマネージャで問題が発生することがある。

**Web** インターフェイスが想定どおりに応答しません

StorageGRID ソフトウェアのアップグレード後に Grid Manager またはテナントマネージャが想定どおりに応答しない場合がある。

Web インターフェイスで問題が発生した場合：

- サポートされているブラウザを使用していることを確認します。

  StorageGRID 11.5 でサポートされるブラウザが変更になりました。サポート対象のバージョンを使用していることを確認してください。

- Web ブラウザのキャッシュをクリアします。

  キャッシュをクリアすると、以前のバージョンの StorageGRID ソフトウェアで使用されていた古いリソースが削除され、ユーザインターフェイスが再び正しく動作するようになります。手順については、 Web ブラウザのドキュメントを参照してください。

関連情報

"Web ブラウザの要件"

「 **Docker image availability check** 」というエラーメッセージが表示される

## アップグレードプロセスを開始しようとすると、「 The following issues were identified by the Docker image availability check validation suite 」というエラーメッセージが表示される場合があります。 アップグレードを完了する前に、すべての問題を解決しておく必要があります。

見つかった問題の解決に必要な変更内容がわからない場合は、テクニカルサポートにお問い合わせください。

| メッセージ | 原因 | 解決策 |
| --- | --- | --- |
| アップグレードバージョンを特定できません。バージョン情報ファイルをアップグレードします `{file_path}` 想定される形式と一致しませんでした。 | アップグレードパッケージが破損しています。 | アップグレードパッケージを再度アップロードしてやり直してください。問題が解決しない場合は、テクニカルサポートにお問い合わせください。 |
| バージョン情報ファイルをアップグレードします `{file_path}` が見つかりませんでした。アップグレードバージョンを特定できません。 | アップグレードパッケージが破損しています。 | アップグレードパッケージを再度アップロードしてやり直してください。問題が解決しない場合は、テクニカルサポートにお問い合わせください。 |
| に現在インストールされているリリースバージョンを確認できません `{node_name}`。 | ノード上の重要なファイルが破損しています。 | テクニカルサポートにお問い合わせください。 |
| のバージョンを表示しようとしているときに接続エラーが発生しました `{node_name}` | ノードがオフラインであるか、接続が中断されました。 | すべてのノードがオンラインで、プライマリ管理ノードからアクセスできることを確認して、操作をやり直します。 |
| ノードのホスト `{node_name}` にはStorageGRID がありません `{upgrade_version}` イメージがロードされましたアップグレードを続行するには、イメージとサービスがホストにインストールされている必要があります。 | ノードを実行しているホストにアップグレード用の RPM パッケージまたは DEB パッケージがインストールされていないか、イメージのインポートがまだ終了していません。<br>• 注：このエラーは、 Linux でコンテナとして実行されている環境 ノードのみに該当します。 | RPM パッケージまたは DEB パッケージが、ノードが実行されているすべての Linux ホストにインストールされていることを確認します。サービスとイメージファイルの両方について、バージョンが正しいことを確認します。数分待ってから再試行してください。<br>詳細については、使用しているLinuxプラットフォーム用のインストール手順を参照してください。 |
| ノードの確認中にエラーが発生しました `{node_name}` | 予期しないエラーが発生しました。 | 数分待ってから再試行してください。 |
| 事前確認の実行時に不明なエラーが発生する。 `{error_string}` | 予期しないエラーが発生しました。 | 数分待ってから再試行してください。 |

関連情報

"Red Hat Enterprise Linux または CentOS をインストールします"

"Ubuntu または Debian をインストールします"

# ハードウェアを設置して保守する

## SG6000 ストレージアプライアンス

StorageGRID SG6060とSGF6024アプライアンスの設置とメンテナンスの方法について説明します。

- "SG6000アプライアンスの概要"
- "インストールと導入の概要"
- "設置を準備しています"
- "ハードウェアを設置"
- "ハードウェアの設定"
- "アプライアンスストレージノードの導入"
- "ストレージアプライアンスのインストールの監視"
- "アプライアンスのインストールと設定の自動化"
- "インストール REST API の概要"
- "ハードウェアの設置のトラブルシューティング"
- "SG6000アプライアンスのメンテナンス"

### SG6000アプライアンスの概要

StorageGRID DSG6000アプライアンスは、StorageGRID システムにおいてストレージノードとして機能する、ストレージとコンピューティングを統合したプラットフォームです。これらのアプライアンスは、アプライアンスストレージノードと仮想（ソフトウェアベース）ストレージノードを組み合わせたハイブリッドグリッド環境で使用できます。

SG6000 アプライアンスには次の機能があります。

- 次の 2 つのモデルがあります。
  - SG6060 には 60 本のドライブが含まれ、拡張シェルフをサポートします。
  - SGF6024 は、 24 本のソリッドステートドライブ（ SSD ）を提供します。
- StorageGRID ストレージノードのストレージ要素とコンピューティング要素を統合します。
- ストレージノードの導入と設定を簡易化するために、 StorageGRID アプライアンスインストーラが搭載されています。
- ストレージコントローラとドライブを管理および監視するための SANtricity System Manager が搭載されています。
- コンピューティングコントローラのハードウェアを監視および診断するためのベースボード管理コントローラ（ BMC ）が搭載されています。
- StorageGRID のグリッドネットワークとクライアントネットワークとの 10GbE または 25GbE 接続を最

大 4 つサポートします。

- 連邦情報処理標準（ FIPS ）ドライブに対応しています。これらのドライブを SANtricity System Manager のドライブセキュリティ機能と併用すると、データへの不正アクセスを防止できます。

### SG6060 の概要

StorageGRID DSG6060アプライアンスには、コンピューティングコントローラと、2台のストレージコントローラと60本のドライブを搭載したストレージコントローラシェルフが含まれています。必要に応じて、 60 ドライブ拡張シェルフも追加できます。

#### SG6060 のコンポーネント

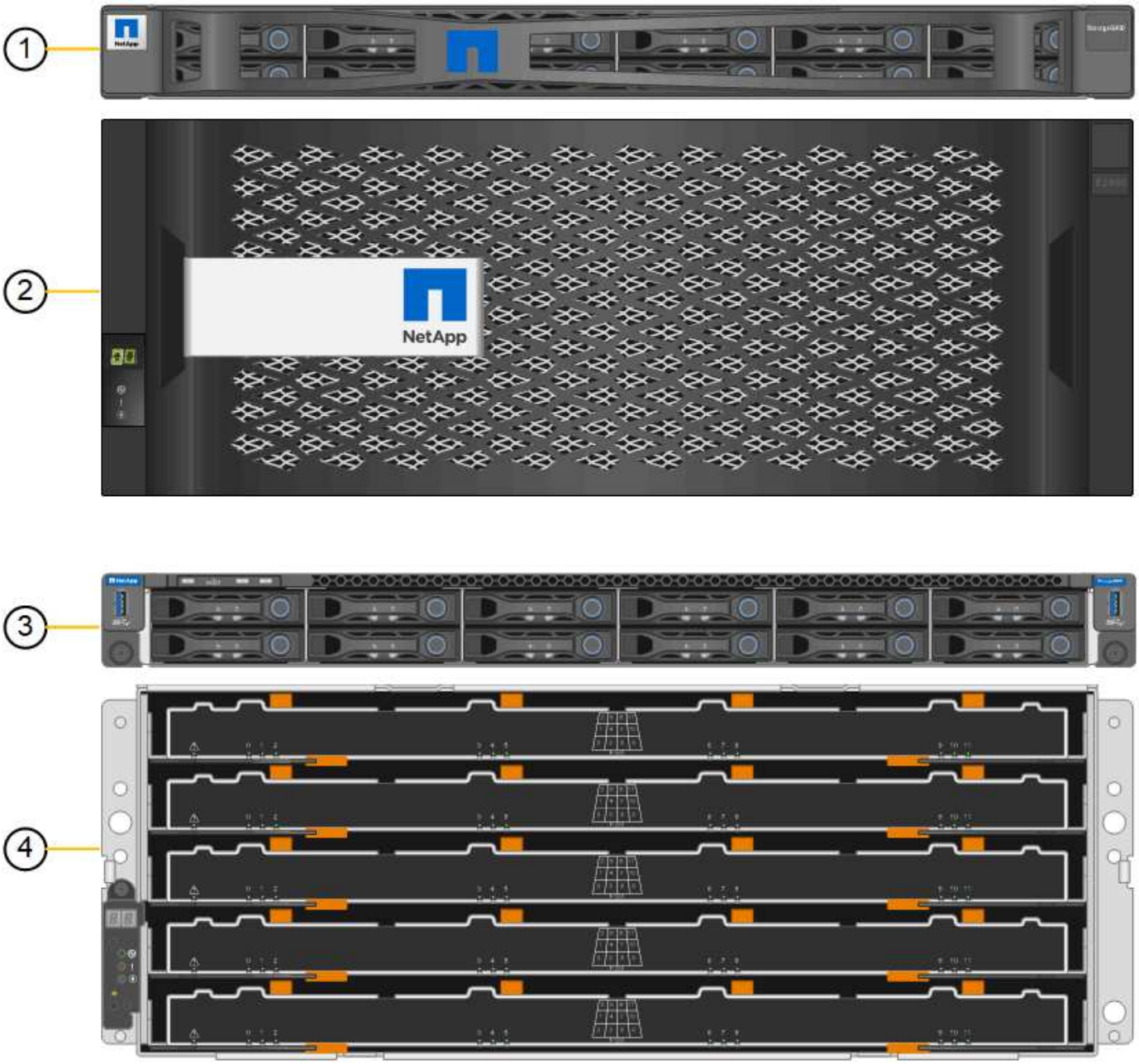
SG6060 アプライアンスには、次のコンポーネントが含まれています。

| コンポーネント | 説明 |
| --- | --- |
| コンピューティングコントローラ | SG6000-CN コントローラ、 1 ラックユニット（ 1U ）サーバ。次のものが搭載されています。<br>• 40 コア（ 80 スレッド）<br>• 192GB の RAM<br>• 25Gbps アグリゲートイーサネット帯域幅 × 最大 4<br>• 16Gbps Fibre Channel （ FC ）インターコネクト × 4<br>• ベースボード管理コントローラ（ BMC ） - ハードウェア管理を簡素化します<br>• 冗長電源装置 |
| ストレージコントローラシェルフ | E シリーズ E2860 コントローラシェルフ（ストレージアレイ）。 4U シェルフの 1 つで、構成は次のとおりです。<br>• E シリーズ E2800 コントローラ × 2 （デュプレックス構成） - ストレージコントローラのフェイルオーバーをサポートします<br>• 5 ドロワードライブシェルフ - 3.5 インチドライブを 60 本（ SSD × 2 、 NL-SAS ドライブ × 58 ）収容<br>• 冗長電源装置とファン |

| コンポーネント | 説明 |
| --- | --- |
| オプション：ストレージ拡張シェルフ<br><br>• 注：拡張シェルフは、初期導入時に設置することも、あとで追加することもできます。 | E シリーズ DE460C エンクロージャ： 4U シェルフで、以下を構成：<br><br>• 入出力モジュール（ IOM ） × 2<br>• それぞれに 12 本の NL-SAS ドライブを搭載し、合計 60 本のドライブを搭載したドロワー × 5<br>• 冗長電源装置とファン<br><br>各 SG6060 アプライアンスには、合計 180 本のドライブを搭載できる拡張シェルフを 1 台または 2 台設置できます。 |

#### SG6060 の図

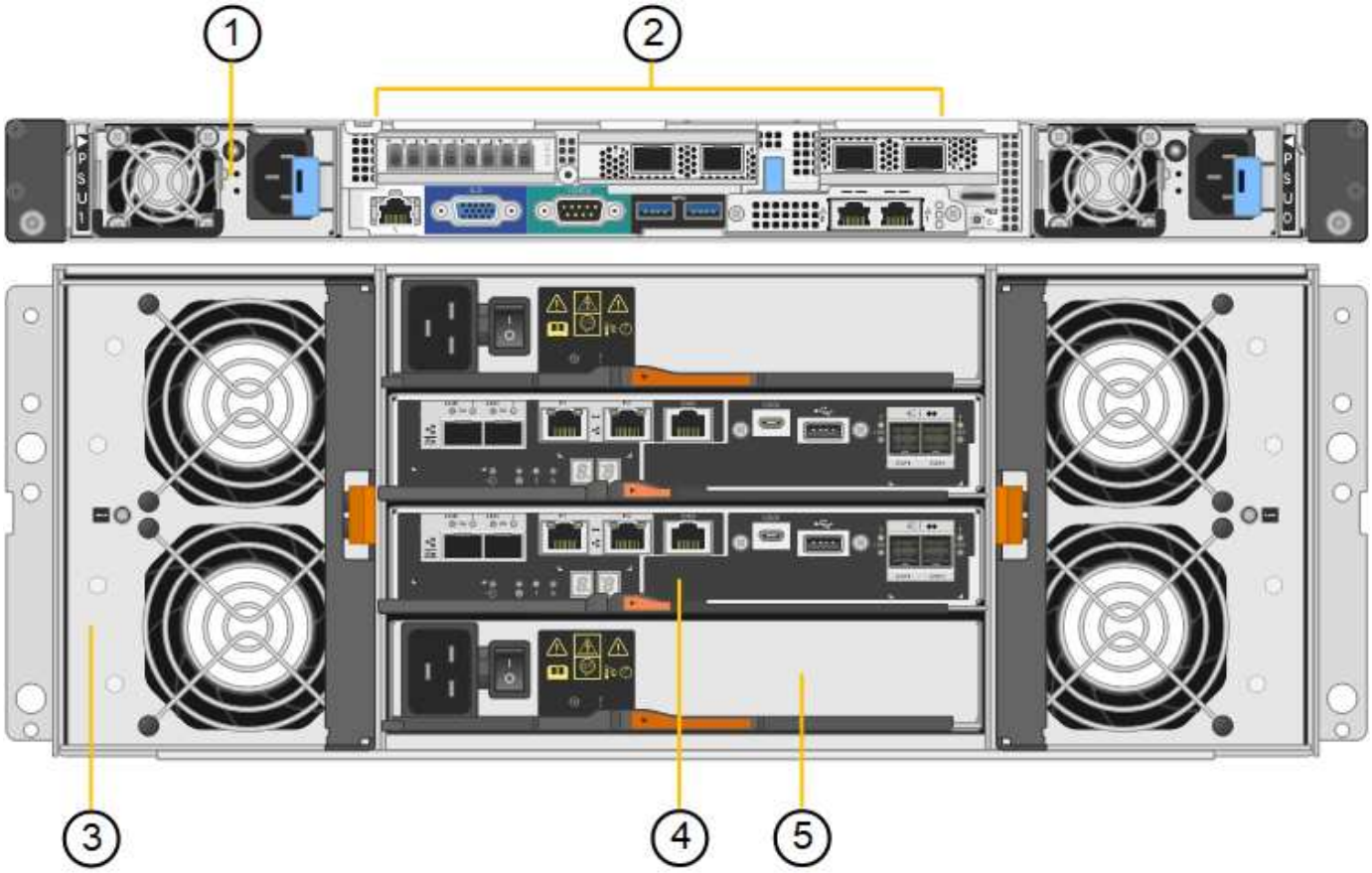
次の図は、 1U コンピューティングコントローラ 1 台、 2 台のストレージコントローラと 5 つのドライブドロワーに 60 本のドライブを搭載した 4U シェルフ 1 台で構成される SG6060 の前面を示しています。




| | 説明 |
|---|---|
| 1. | 前面ベゼルを取り付けた SG6000-CN コンピューティングコントローラ |
| 2. | 前面ベゼルを取り付けたE2860コントローラシェルフ（オプションの拡張シェルフの外観も同じ） |
| 3. | 前面ベゼルを取り外した SG6000-CN のコンピューティングコントローラ |
| 4. | 前面ベゼルを取り外したE2860コントローラシェルフ（オプションの拡張シェルフの外観も同じ） |

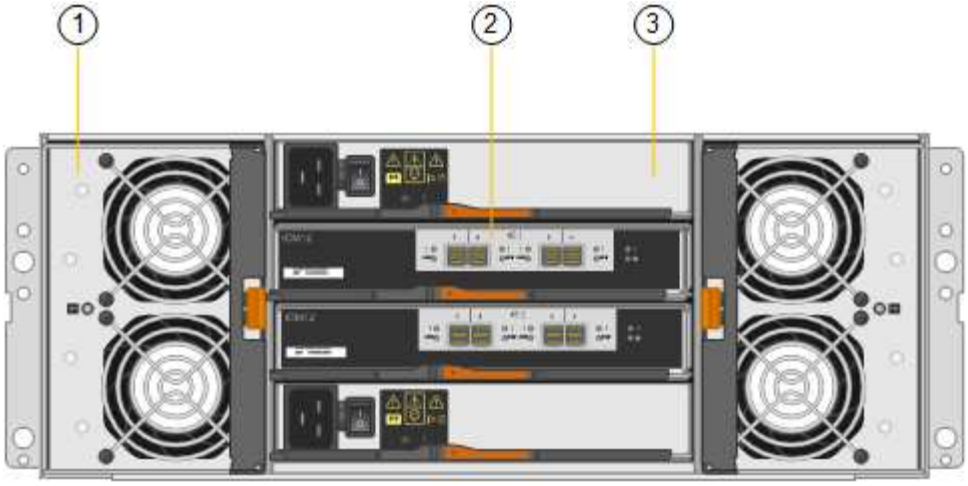
この図は、コンピューティングコントローラ、ストレージコントローラ、ファン、電源装置を含む SG6060

の背面を示しています。




| | 説明 |
|---|---|
| 1. | SG6000-CN コンピューティングコントローラの電源装置（ × 2 ） |
| 2. | SG6000-CN コンピューティングコントローラのコネクタ |
| 3. | E2860 コントローラシェルフのファン（ × 2 ） |
| 4. | E シリーズ E2800 ストレージコントローラ（ × 2 ）とコネクタ |
| 5. | E2860 コントローラシェルフの電源装置（ × 2 ） |

次の図は、 SG6060 のオプションの拡張シェルフの背面です。これには、入出力モジュール（ IOM ）、ファン、電源装置が含まれます。各 SG6060 には、初期設置に含めることもあとで追加することもできる拡張シェルフを 1 台または 2 台設置することもできます。




| | 説明 |
|---|---|
| 1. | 拡張シェルフのファン（ × 2 ） |
| 2. | 拡張シェルフの IOM （ × 2 ） |
| 3. | 拡張シェルフの電源装置（ × 2 ） |

**SGF6024** の概要

## StorageGRIDWebscale 6024 には、コンピューティングコントローラ、およびソリッドステートドライブを 24 本収容できるストレージコントローラシェルフが含まれています。

**SGF6024** コンポーネント

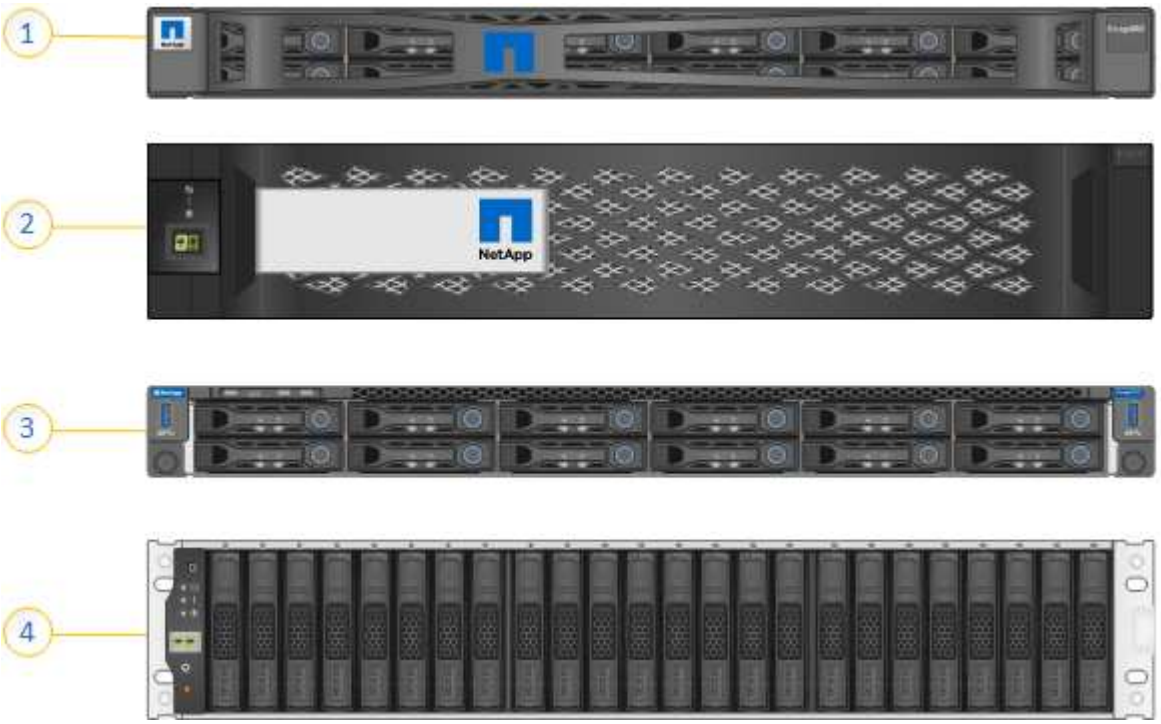
SGF6024 アプライアンスには、次のコンポーネントが含まれています。

| コンポーネント | 説明 |
|---|---|
| コンピューティングコントローラ | SG6000-CN コントローラ、 1 ラックユニット（ 1U ）サーバ。次のものが搭載されています。<br>• 40 コア（ 80 スレッド）<br>• 192GB の RAM<br>• 25Gbps アグリゲートイーサネット帯域幅 × 最大 4<br>• 16Gbps Fibre Channel （ FC ）インターコネクト × 4<br>• ベースボード管理コントローラ（ BMC ） - ハードウェア管理を簡素化します<br>• 冗長電源装置 |

| コンポーネント | 説明 |
| --- | --- |
| フラッシュアレイ（コントローラシェルフ） | E シリーズ EF570 フラッシュアレイ（コントローラシェルフとも呼ばれます）。 2U シェルフで、構成は次のとおりです。<br>• E シリーズの EF570 コントローラ × 2 （デュプレックス構成） - ストレージコントローラのフェイルオーバーをサポートします<br>• ソリッドステートドライブ（ SSD またはフラッシュドライブとも呼ばれます） × 24<br>• 冗長電源装置とファン |

**SGF6024** の図

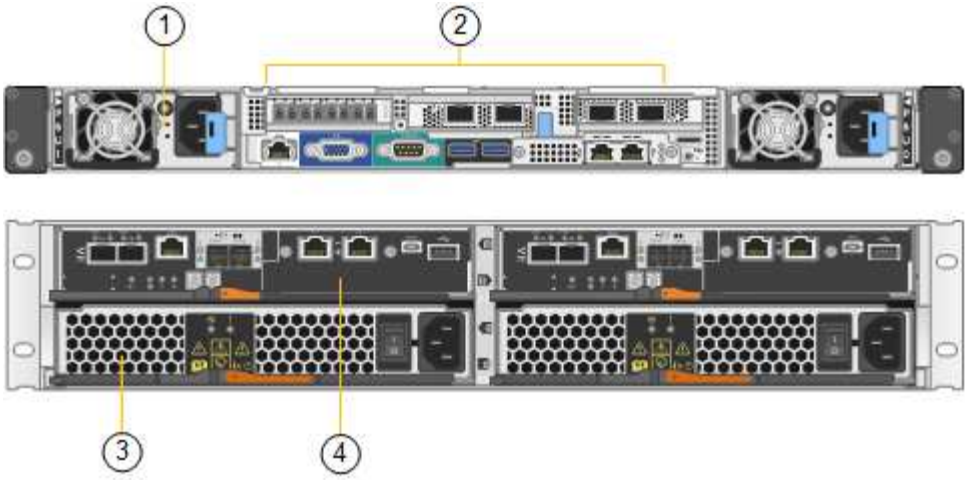
次の図は、 SGF6024 の前面です。この SGF6024 には、 1U コンピューティングコントローラ 1 台、 2 台のストレージコントローラと 24 本のフラッシュドライブを搭載した 2U エンクロージャ 1 台が含まれています。




| | 説明 |
| --- | --- |
| 1. | 前面ベゼルを取り付けた SG6000-CN コンピューティングコントローラ |
| 2. | EF570 フラッシュアレイ、前面ベゼル |
| 3. | 前面ベゼルを取り外した SG6000-CN のコンピューティングコントローラ |
| 4. | 前面ベゼルを取り外した EF570 フラッシュアレイ |

この図は、コンピューティングコントローラ、ストレージコントローラ、ファン、電源装置を含む SGF6024

の背面を示しています。




| | 説明 |
|---|---|
| 1. | SG6000-CN コンピューティングコントローラの電源装置（ × 2 ） |
| 2. | SG6000-CN コンピューティングコントローラのコネクタ |
| 3. | EF570 フラッシュアレイの電源装置（ × 2 ） |
| 4. | E シリーズ EF570 ストレージコントローラ（ × 2 ）とコネクタ |

**SG6000**アプライアンスのコントローラ

StorageGRID DSG6000アプライアンスの各モデルには、1UエンクロージャにSG6000-CNコンピューティングコントローラが1台、2Uまたは4UエンクロージャにEシリーズストレージコントローラが2台搭載されています。各タイプのコントローラの詳細については、次の図を確認してください。

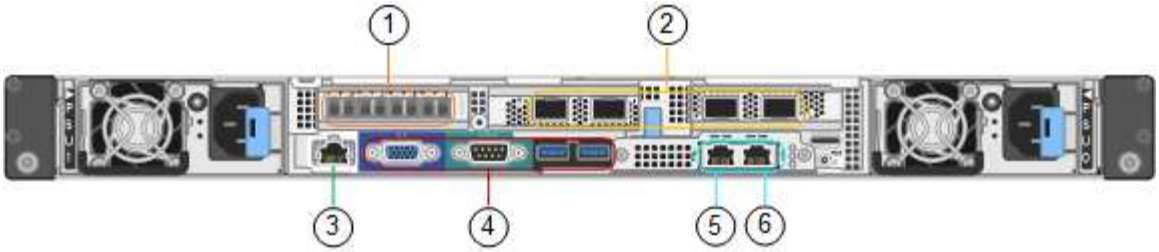
すべてのアプライアンス： **SG6000-CN** コンピューティングコントローラ

- アプライアンスのコンピューティングリソースを提供します。
- StorageGRID アプライアンスインストーラが搭載されています。

> StorageGRID ソフトウェアは、アプライアンスにプリインストールされていません。このソフトウェアは、アプライアンスの導入時に管理ノードから取得されます。

- グリッドネットワーク、管理ネットワーク、クライアントネットワークを含む、 3 つの StorageGRID ネットワークすべてに接続できます。
- E シリーズストレージコントローラに接続し、イニシエータとして機能します。

次の図は、 SG6000-CN の背面にあるコネクタを示しています。



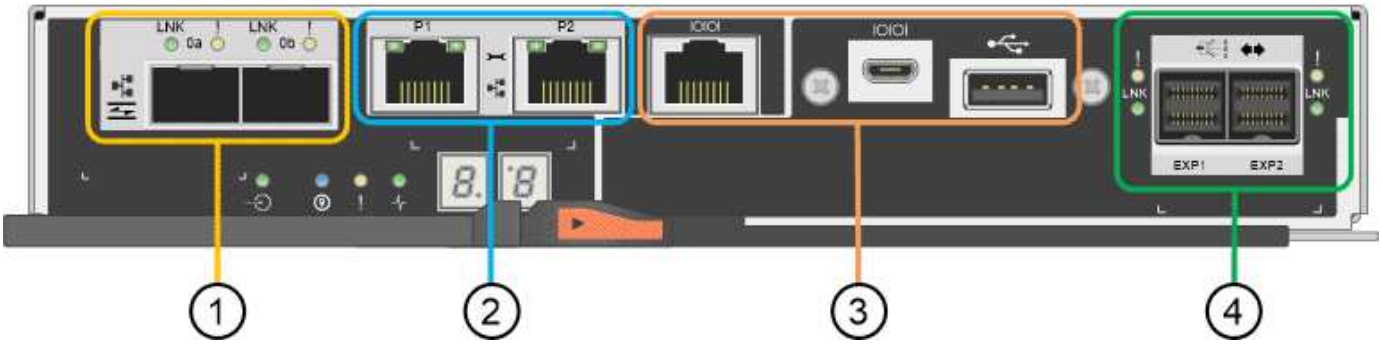

| | ポート | を入力します | 使用 |
|---|---|---|---|
| 1. | インターコネクトポート 1~4 | 16Gb/s Fibre Channel （ FC ）、光ファイバ内蔵 | SG6000-CN コントローラを E2800 コントローラに接続（各 E2800 に 2 つの接続）します。 |
| 2. | ネットワークポート 1~4 | 10GbE または 25GbE 。ケーブルまたは SFP トランシーバタイプ、スイッチ速度、および設定されたリンク速度に基づきます | StorageGRID のグリッドネットワークおよびクライアントネットワークに接続します。 |
| 3. | BMC 管理ポート | 1GbE （ RJ-45 ） | SG6000-CN のベースボード管理コントローラに接続します。 |
| 4. | 診断とサポート用のポート | • VGA<br>• シリアル、 115200 8-N-1<br>• USB | テクニカルサポート専用です。 |
| 5. | 管理ネットワークポート 1 | 1GbE （ RJ-45 ） | SG6000-CN を StorageGRID の管理ネットワークに接続します。 |

| | ポート | を入力します | 使用 |
| --- | --- | --- | --- |
| 6. | 管理ネットワークポート 2 | 1GbE （ RJ-45 ） | オプション：<br>• StorageGRID の管理ネットワークへの冗長接続を確保するには、管理ポート 1 とボンディングします。<br>• 一時的なローカルアクセス用（ IP 169.254.0.1 ）に空けておくことができます。<br>• DHCP によって割り当てられた IP アドレスを使用できない場合は、設置時の IP 設定にポート 2 を使用します。 |

**SG6060 ： E2800** ストレージコントローラ

- 2 台のコントローラでフェイルオーバーに対応。
- ドライブ上のデータを格納。
- デュプレックス構成では標準の E シリーズコントローラとして機能。
- SANtricity OS ソフトウェア（コントローラファームウェア）を搭載。
- ストレージハードウェアの監視やアラートの管理、 AutoSupport 機能、ドライブセキュリティ機能に対応した SANtricity System Manager が搭載されています。
- SG6000-CN コントローラに接続して、ストレージへのアクセスを提供します。

次の図は、各 E2800 コントローラ背面のコネクタを示しています。

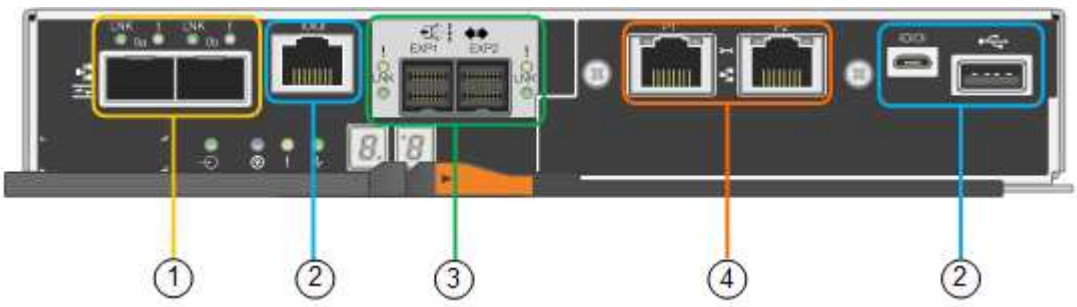


| | ポート | を入力します | 使用 |
|---|---|---|---|
| 1. | インターコネクトポート 1 と 2 | 16Gb/s FC 光ファイバ SFPA | 各 E2800 コントローラを SG6000-CN コントローラに接続します。SG6000-CN コントローラへの接続は 4 つ（各 E2800 に 2 つ）あります。 |
| 2. | 管理ポート 1 と 2 | 1Gb （ RJ-45 ）イーサネット | • ポート 1 は、ブラウザから SANtricity System Manager にアクセスするネットワークに接続します。<br>• ポート 2 はテクニカルサポート専用です。 |
| 3. | 診断とサポート用のポート | • RJ-45 シリアルポート<br>• マイクロ USB シリアルポート<br>• USB ポート | テクニカルサポート専用です。 |
| 4. | ドライブ拡張ポート 1 と 2 | 12Gb/ 秒 SAS の場合 | 拡張シェルフの IOM のドライブ拡張ポートに接続します。 |

**SGF6024 ： EF570** ストレージコントローラ

- 2 台のコントローラでフェイルオーバーに対応。
- ドライブ上のデータを格納。
- デュプレックス構成では標準の E シリーズコントローラとして機能。
- SANtricity OS ソフトウェア（コントローラファームウェア）を搭載。
- ストレージハードウェアの監視やアラートの管理、 AutoSupport 機能、ドライブセキュリティ機能に対応した SANtricity System Manager が搭載されています。
- SG6000-CN コントローラに接続して、フラッシュストレージへのアクセスを提供します。

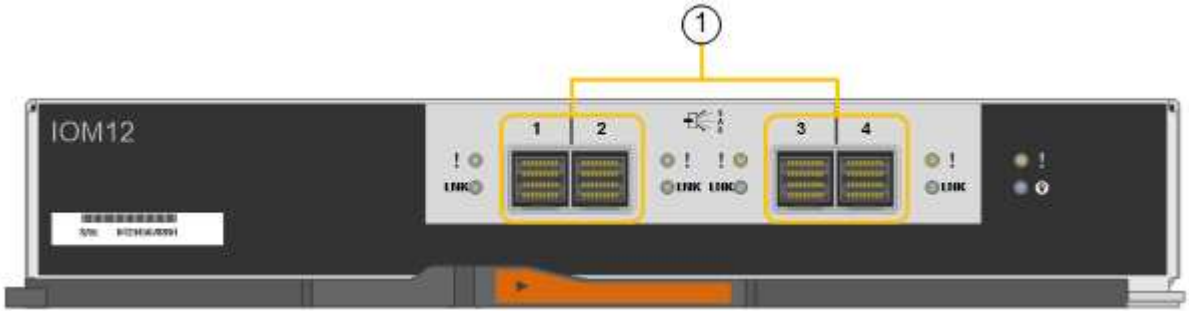
次の図は、各 EF570 コントローラ背面のコネクタを示しています。



| | ポート | を入力します | 使用 |
| --- | --- | --- | --- |
| 1. | インターコネクトポート 1 と 2 | 16Gb/s FC 光ファイバ SFPA | 各 EF570 コントローラを SG6000-CN コントローラに接続します。SG6000-CN コントローラへの接続は 4 つ（各 EF570 から 2 つ）あります。 |
| 2. | 診断とサポート用のポート | • RJ-45 シリアルポート<br>• マイクロ USB シリアルポート<br>• USB ポート | テクニカルサポート専用です。 |
| 3. | ドライブ拡張ポート | 12Gb/ 秒 SAS の場合 | 使用されません。SGF6024 アプライアンスでは、拡張ドライブシェルフはサポートされません。 |
| 4. | 管理ポート 1 と 2 | 1Gb （ RJ-45 ）イーサネット | • ポート 1 は、ブラウザから SANtricity System Manager にアクセスするネットワークに接続します。<br>• ポート 2 はテクニカルサポート専用です。 |

**SG6060** ：オプションの拡張シェルフの入力 / 出力モジュール

拡張シェルフには、ストレージコントローラまたはその他の拡張シェルフに接続する入出力モジュール（ IOM ）が 2 台搭載されています。




| | ポート | を入力します | 使用 |
| --- | --- | --- | --- |
| 1. | ドライブ拡張ポート 1~4 | 12Gb/ 秒 SAS の場合 | 各ポートをストレージコントローラまたは追加の拡張シェルフ（ある場合）に接続します。 |

# インストールと導入の概要

StorageGRID ストレージアプライアンスは StorageGRID の初回導入時に設置することも、後日拡張の一環として追加することもできます。リカバリ処理の一環としてアプライアンスストレージノードの設置が必要となる場合もあります。

必要なもの

StorageGRID システムが、必要なバージョンの StorageGRID ソフトウェアを使用している。

| アプライアンス | 必要な **StorageGRID** のバージョン |
| --- | --- |
| SG6060 に拡張シェルフがない | 11.1.1 以降 |
| 拡張シェルフを備えた SG6060 （ 1 台または 2 台） | 11.3 以降<br>• 注： * 初期導入後に拡張シェルフを追加する場合は、バージョン 11.4 以降を使用する必要があります。 |
| SGF6024 | 11.3 以降 |

インストールと導入のタスク

StorageGRID システムに StorageGRID ストレージアプライアンスを追加するには、主に次の 4 つの手順を実行します。

1. 設置の準備：
   - 設置場所の準備
   - 開梱と内容の確認
   - 追加機器および工具の入手方法
   - IP アドレスとネットワーク情報を収集しています
   - オプション：すべてのアプライアンスデータを暗号化する場合は、外部キー管理サーバ（ KMS ）を設定します。外部キー管理の詳細については、 StorageGRID の管理手順を参照してください。
2. ハードウェアの設置
   - ハードウェアの登録
   - キャビネットまたはラックへのアプライアンスの設置
   - ドライブを取り付けます
   - オプションの拡張シェルフの設置（モデル SG6060 のみ、最大 2 台の拡張シェルフ）
   - アプライアンスのケーブル接続
   - 電源コードの接続と電源の投入
   - ブート時のステータスコードの確認
3. ハードウェアの設定

- SANtricity System Manager にアクセスして、 SANtricity システムマネージャを設定します
- StorageGRID アプライアンスインストーラへのアクセス、ストレージコントローラの管理ポート 1 の静的 IP アドレスの設定、および StorageGRID ネットワークへの接続に必要なリンクとネットワーク IP の設定を行います
- SG6000-CN コントローラのベースボード管理コントローラ（ BMC ）インターフェイスへのアクセス
- オプション：外部 KMS を使用してアプライアンスデータを暗号化する場合は、ノード暗号化を有効にします。
- オプション： RAID モードを変更する

4. アプライアンスをストレージノードとして導入する：

| タスク | 手順 |
| --- | --- |
| 新しい StorageGRID システムにアプライアンスストレージノードを導入する | "アプライアンスストレージノードの導入" |
| 既存の StorageGRID システムへのアプライアンスストレージノードの追加 | StorageGRID システムの拡張手順 |
| ストレージノードのリカバリ処理の一環としてアプライアンスストレージノードを導入する | リカバリとメンテナンスの手順 |

関連情報

"設置を準備しています"

"ハードウェアを設置"

"ハードウェアの設定"

"グリッドを展開します"

""

"StorageGRID の管理"

## 設置を準備しています

StorageGRID アプライアンスを設置するための準備では、設置場所を準備し、必要なすべてのハードウェア、ケーブル、工具を揃えます。また、 IP アドレスとネットワーク情報を収集する必要があります。

手順

- "サイトの準備（SG6000）"
- "開梱（SG6000）"
- "追加の機器と工具の入手（SG6000）"
- "Web ブラウザの要件"

- "アプライアンスのネットワーク接続を確認します"
- "設置情報（SG6000）の収集"

サイトの準備（**SG6000**）

## アプライアンスを設置する前に、設置場所および使用するキャビネットやラックが StorageGRID アプライアンスの仕様を満たしていることを確認する必要があります。

手順

1. 設置場所の温度、湿度、高度範囲、通気、熱放散の要件を満たしていることを確認します。 配線、電源、およびアース。詳細については、 NetApp Hardware Universe を参照してください。
2. 設置場所に SGF6024 の SG6060 または 120V AC 電源が 240V になっていることを確認します。
3. 次のサイズのシェルフ（ケーブルなし）が収まる 48.3cm （ 19 インチ）のキャビネットまたはラックを用意します。

| シェルフのタイプ | 高さ | 幅 | 奥行き | 最大重量 |
|---|---|---|---|---|
| • SG6060 の E2860 コントローラシェルフ * | 6.87 インチ （ 17.46 cm ） | 17.66 インチ （ 44.86 cm ） | 38.25 インチ （ 97.16 cm ） | 250 ポンド （ 113 kg ） |
| • SG6060 のオプションの拡張シェルフ * （ 1 台または 2 台） | 6.87 インチ （ 17.46 cm ） | 17.66 インチ （ 44.86 cm ） | 38.25 インチ （ 97.16 cm ） | 250 ポンド （ 113 kg ） |
| • EF570 コントローラシェルフ * SGF6024 | 3.35 インチ （ 8.50 cm ） | 17.66 インチ （ 44.86 cm ） | 19.00 インチ （ 48.26cm ） | 51.74 ポンド （ 23.47 kg ） |
| • 各アプライアンスの SG6000-CN コントローラ * | 1.70 インチ （ 4.32 cm ） | 17.32 インチ （ 44.0 cm ） | 32.0 インチ （ 81.3 cm ） | 39 ポンド （ 17.7 kg ） |

4. アプライアンスの設置場所を決定します。

E2860 コントローラシェルフまたはオプションの拡張シェルフを設置する場合は、機器の転倒を防ぐために、ラックまたはキャビネットの一番下から順にハードウェアを設置してください。最も重い機器をキャビネットまたはラックの一番下に設置するには、 E2860 コントローラシェルフおよび拡張シェルフの上に SG6000-CN コントローラを設置します。

設置作業を行う前に、アプライアンスに付属の 0.5m 光ケーブル、または用意したケーブルの長さが、計画したレイアウトに十分であることを確認してください。

関連情報

"NetApp Hardware Universe の略"

"NetApp Interoperability Matrix Tool で確認できます"

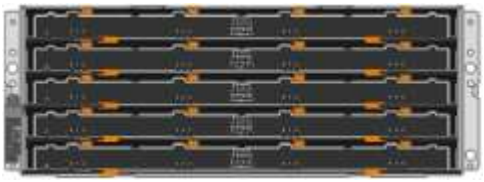
開梱（**SG6000**）

StorageGRID アプライアンスを設置する前にすべて開梱し、内容物を納品書の項目と比較します。

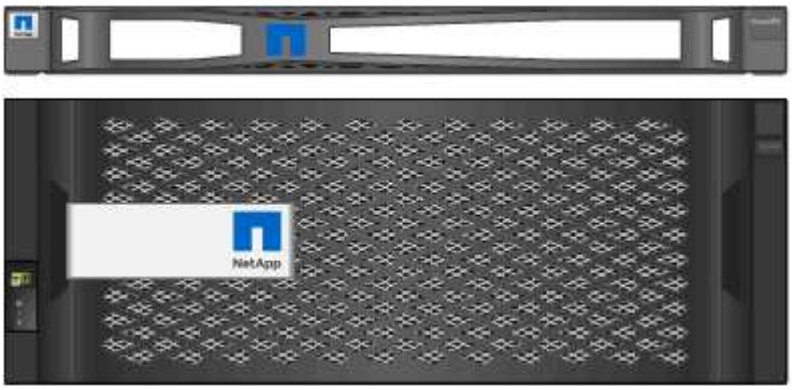
**SG6060** の設計

- * SG6000-CN コントローラ *

- * ドライブを取り付けていない E2860 コントローラシェルフ *

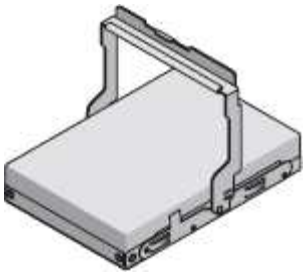


- ※前面ベゼル × 2

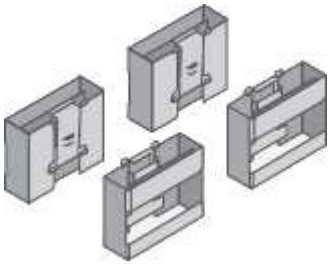



- * レールキット 2 個、取扱説明書付き *

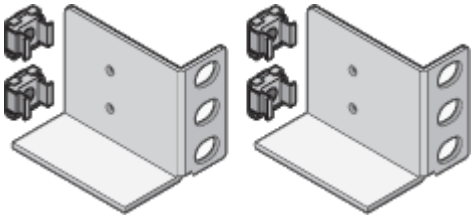
- * ドライブ 60 台（ SSD 2 台、 NL-SAS 58 台） *



- * ハンドル 4 個 *

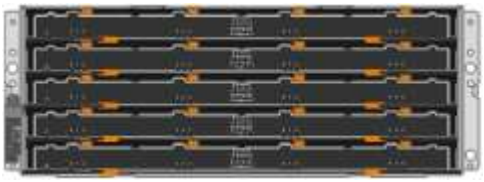


- * 角穴ラック取り付け用のバックブラケットとケージナット *



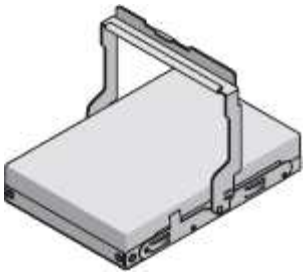
**SG6060** 拡張シェルフ

- * ドライブを取り付けていない拡張シェルフ *



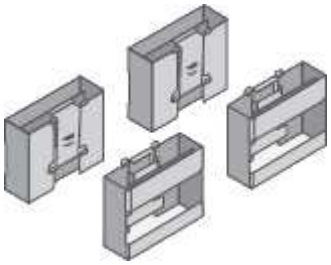
- * フロントベゼル *

- *60 NL-SAS ドライブ *

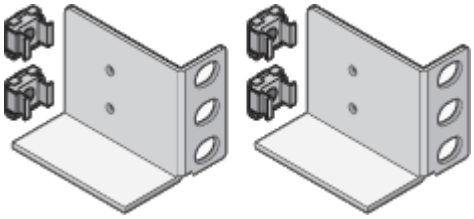


- * レールキット 1 個、取扱説明書付き *

- * ハンドル 4 個 *



- * 角穴ラック取り付け用のバックブラケットとケージナット *



**SGF6024**

- * SG6000-CN コントローラ *

- * 24 本のソリッドステート（フラッシュ）ドライブを搭載した EF570 フラッシュアレイ *

- ※前面ベゼル × 2

- * レールキット 2 個、取扱説明書付き *

- * シェルフエンドキャップ *

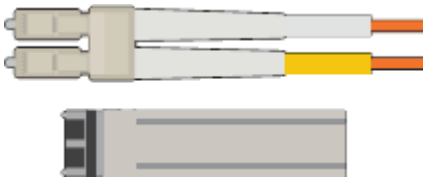
ケーブルとコネクタ

StorageGRID アプライアンスには、出荷時に次のケーブルとコネクタが付属しています。

- * お住まいの国に対応した電源コード 4 本 *

キャビネットによっては、アプライアンスに付属している電源コードではなく特別な電源コードを使用する場合があります。

- * 光ケーブルと SFP トランシーバ *



FC インターコネクトポート用の光ケーブル × 4

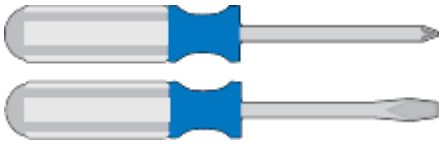
16Gb/s FC 対応の SFP+ トランシーバ × 4

- * オプション： 1 台の SG6060 拡張シェルフ接続用 SAS ケーブル 2 本 *

# StorageGRID アプライアンスを設置する前に、必要な追加機器や工具がすべて揃っていることを確認します。

ハードウェアの設置と設定を行うには、次の追加機器が必要です。

- * ドライバ *

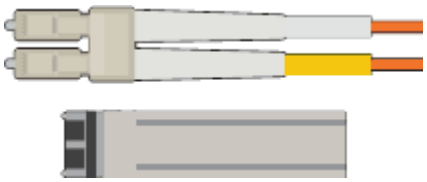


フィリップス番号2 本のドライバ

中型マイナスドライバ

- * 静電気防止用リストストラップ *

- * 光ケーブルと SFP トランシーバ *



次のいずれかを用意する必要があります。

  - SG6000-CN コントローラで使用する 10 / 25GbE ポート用に TwinAx ケーブルまたは光ケーブルを 1~4 本
  - 光ケーブルを 10GbE のリンク速度で使用する場合は、 10 / 25GbE ポート用に SFP+ トランシーバを 1~4 個
  - 光ケーブルを 25GbE のリンク速度で使用する場合は、 10 / 25GbE ポート用に SFP28 トランシーバを 1~4 個

- * RJ-45 （ Cat5 / Cat5e / Cat6 ）イーサネットケーブル *

- * サービスラップトップ *

サポートされている Web ブラウザ

1GbE （ RJ-45 ）ポート

- * オプションのツール *

ヘッドビット付き電源ドリル

懐中電灯

60 ドライブシェルフのリフト機を使用します

**Web** ブラウザの要件

サポートされている Web ブラウザを使用する必要があります。

| **Web** ブラウザ | サポートされる最小バージョン |
| --- | --- |
| Google Chrome | 87 |
| Microsoft Edge の場合 | 87 |
| Mozilla Firefox | 84 |

ブラウザウィンドウの幅を推奨される値に設定してください。

| ブラウザの幅 | ピクセル |
| --- | --- |
| 最小（ Minimum ） | 1024 |
| 最適 | 1280 |

アプライアンスのネットワーク接続を確認します

## StorageGRID アプライアンスを設置する前に、アプライアンスに接続できるネットワークを確認しておく必要があります。

StorageGRID アプライアンスを StorageGRID システムのストレージノードとして導入する場合は、次のネットワークに接続できます。

- * StorageGRID のグリッドネットワーク * ：グリッドネットワークは、すべての内部 StorageGRID トラフィックに使用されます。このネットワークによって、グリッド内のすべてのノードが、すべてのサイトおよびサブネットにわたって相互に接続されます。グリッドネットワークは必須です。
- * StorageGRID の管理ネットワーク * ：管理ネットワークは、システムの管理とメンテナンスに使用するクローズドネットワークです。管理ネットワークは通常はプライベートネットワークであり、サイト間でルーティング可能にする必要はありません。管理ネットワークはオプションです。
- * StorageGRID のクライアントネットワーク： * クライアントネットワークは、 S3 や Swift などのクライアントアプリケーションへのアクセスを可能にするオープンネットワークです。クライアントネットワークはグリッドへのクライアントプロトコルアクセスを提供するため、グリッドネットワークを分離してセキュリティを確保できます。クライアントネットワークはオプションです。
- * SANtricity システム・マネージャ用管理ネットワーク*：このネットワークは、ストレージ・コントローラ上のSANtricity システム・マネージャへのアクセスを提供し、ストレージ・コントローラ・シェルフ内のハードウェア・コンポーネントの監視と管理を可能にします。この管理ネットワークは、 StorageGRID の管理ネットワークと同じにすることも、独立した管理ネットワークにすることもできます。
- * SG6000-CNコントローラのBMC管理ネットワーク：*このネットワークはSG6000-CN内のベースボード管理コントローラへのアクセスを提供し、SG6000-CNコントローラのハードウェアコンポーネントの監視と管理を可能にします。この管理ネットワークは、 StorageGRID の管理ネットワークと同じにすることも、独立した管理ネットワークにすることもできます。

StorageGRID ネットワークの詳細については、 _ グリッド入門 _ を参照してください。

関連情報

"設置情報（SG6000）の収集"

"アプライアンスのケーブル接続（SG6000）"

"SG6000-CNコントローラのポートボンディングモード"

"ネットワークガイドライン"

**SG6000-CN**コントローラのポートボンディングモード

## SG6000-CN のネットワークリンクを設定する場合は、グリッドネットワークとオプションのクライアントネットワークに接続する 10 / 25GbE ポート、およびオプションの管

理ネットワークに接続する 1GbE 管理ポートに対してポートボンディングを使用できます。ポートボンディングを使用すると、 StorageGRID ネットワークとアプライアンスの間のパスが冗長化されるため、データの保護に役立ちます。

関連情報

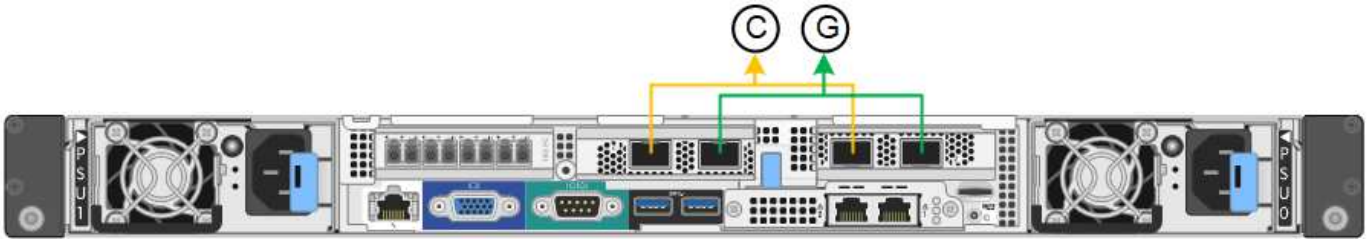
"ネットワークリンクの設定（SG6000）"

**10 / 25GbE**ポートのネットワークボンディングモード

SG6000-CN コントローラの 10 / 25GbE ネットワークポートは、グリッドネットワークおよびクライアントネットワーク接続用に、 Fixed または Aggregate のポートボンディングモードをサポートします。

**Fixed** ポートボンディングモード

固定モードは、 10 / 25GbE ネットワークポートのデフォルトの設定です。




| | ボンディングされるポート |
|---|---|
| C | このネットワークを使用する場合、ポート 1 とポート 3 がクライアントネットワーク用にボンディングされます。 |
| G | ポート 2 とポート 4 がグリッドネットワーク用にボンディングされます。 |

Fixed ポートボンディングモードを使用する場合は、 Active-Backup モードまたは Link Aggregation Control Protocol （ LACP ）（ 802.3ad ）モードを使用してポートをボンディングできます。

- Active-Backup モード（デフォルト）では、一度に 1 つのポートのみがアクティブになります。アクティブポートで障害が発生すると、バックアップポートが自動的にフェイルオーバーして接続が継続されます。ポート 4 がポート 2 のバックアップパスとなり（グリッドネットワーク）、ポート 3 がポート 1 のバックアップパスとなります（クライアントネットワーク）。
- LACP モードでは、各ポートペアでコントローラとネットワークの間の論理チャネルが形成され、スループットが向上します。一方のポートで障害が発生しても、もう一方のポートは引き続きチャネルを提供します。スループットは低下しますが、接続に影響はありません。

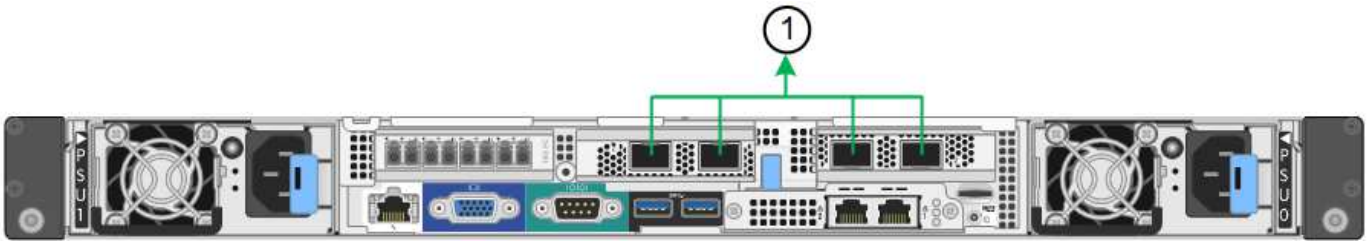
> 冗長な接続が不要な場合は、各ネットワークで使用できるポートは 1 つだけです。ただし、 StorageGRID のインストール後に Grid Manager でアラートがトリガーされてリンクが停止したことが通知される。このポートは切断されているため、このアラートは安全に無効にすることができます。

Grid Manager から * Alert * > * Rules * を選択し、ルールを選択して * Edit rule * をクリックします。次に、

[**enabled**] チェックボックスをオフにします。

**Aggregate** ポートボンディングモード

アグリゲートポートボンディングモードを使用すると、各 StorageGRID ネットワークのスループットが大幅に向上し、追加のフェイルオーバーパスも確保されます。




| | ボンディングされるポート |
|---|---|
| 1. | 接続されたすべてのポートを 1 つの LACP ボンドにグループ化して、すべてのポートをグリッドネットワークとクライアントネットワークのトラフィックに使用できるようにします。 |

アグリゲートポートボンディングモードを使用する場合は、次の点に注意してください。

- LACP ネットワークボンディングモードを使用する必要があります。
- 各ネットワークに一意の VLAN タグを指定する必要があります。この VLAN タグが各ネットワークパケットに追加され、ネットワークトラフィックが正しいネットワークにルーティングされます。
- VLAN と LACP をサポートするスイッチにポートを接続する必要があります。複数のスイッチを LACP ボンドに加える場合は、対象のスイッチが Multi-Chassis Link Aggregation （ MLAG ）グループまたは同等の機能をサポートしていることが必要です。
- VLAN 、 LACP 、 MLAG などを使用するようにスイッチを設定する方法について理解しておく必要があります。

4 つの 10 / 25GbE ポートをすべて使用する必要がない場合、使用するポートの数は 1~3 のいくつでもかまいません。複数のポートを使用すると、 10 / 25GbE ポートの 1 つに障害が発生した場合でも、ネットワーク接続を確保できる可能性が高くなります。

> 4 つのポート全部を使用しない場合は、 StorageGRID をインストールしたあとにケーブルが取り外されていることを通知するアラームがグリッドマネージャで生成されるので注意してください。このアラームは確認後に解除してかまいません。

**1GbE**管理ポートのネットワークボンディングモード

## SG6000-CN コントローラの 2 つの 1GbE 管理ポートでは、独立したネットワークボンディングモードまたは Active-Backup ネットワークボンディングモードを選択してオプションの管理ネットワークに接続できます。

Independent モードでは、左側の管理ポートだけが管理ネットワークに接続されます。このモードではパスは冗長化されません。右側の管理ポートは接続されず、一時的なローカル接続（ IP アドレス 169.254.0.1 ）に使用できます。

Active-Backup モードでは、両方の管理ポートが管理ネットワークに接続されます。一度に 1 つのポートのみがアクティブになります。アクティブポートで障害が発生すると、バックアップポートが自動的にフェイルオーバーして接続が継続されます。これら 2 つの物理ポートを 1 つの論理管理ポートにボンディングすることで、管理ネットワークへのパスが冗長化されます。

> 1GbE 管理ポートが Active-Backup モードに設定されている場合に SG6000-CN コントローラへの一時的なローカル接続が必要となった場合は、両方の管理ポートからケーブルを取り外し、一時的なケーブルを右側の管理ポートに接続し、 IP アドレス 169.254.0.1 を使用してアプライアンスにアクセスしてください。

| | ネットワークボンディングモード |
|---|---|
| A | 両方の管理ポートが、管理ネットワークに接続された 1 つの論理管理ポートにボンディングされます。 |
| 私 | 左側のポートが管理ネットワークに接続されます。右側のポートは一時的なローカル接続（ IP アドレス 169.254.0.1 ）に使用できます。 |

設置情報（**SG6000**）の収集

## StorageGRID アプライアンスを設置および設定する際に、イーサネットスイッチポート、 IP アドレス、およびポートとネットワークのボンディングモードについて決定し、関連情報を収集する必要があります。

このタスクについて

次の表を使用して、アプライアンスに接続する各ネットワークの必要な情報を記録できます。これらの値は、ハードウェアの設置と設定に必要です。

ストレージコントローラの**SANtricity System Manager**に接続するために必要な情報

アプライアンスの両方のストレージコントローラ（ E2800 コントローラまたは EF570 コントローラ）を、 SANtricity System Manager で使用する管理ネットワークに接続する必要があります。コントローラは次のように各アプライアンスに配置されています。

- SG6060 ：コントローラ A は上部にあり、コントローラ B は下部に配置されています。
- SGF6024 ：コントローラ A が左側、コントローラ B が右側にあります。

| 必要な情報 | コントローラ **A** の値 | コントローラ **B** の値 |
|---|---|---|
| 管理ポート 1 （コントローラの P1 ポート）に接続するイーサネットスイッチポート | | |

| 必要な情報 | コントローラ **A** の値 | コントローラ **B** の値 |
| --- | --- | --- |
| 管理ポート 1 の MAC アドレス（ポート P1 のラベルに記載） | | |
| DHCP によって管理ポート 1 に割り当てられた IP アドレス（電源投入後に使用可能な場合）<br>• 注： * ストレージコントローラに接続するネットワークに DHCP サーバがある場合、ネットワーク管理者は MAC アドレスを使用して DHCP サーバによって割り当てられた IP アドレスを特定できます。 | | |
| 管理ネットワークでアプライアンスに使用する静的 IP アドレス | IPv4 の場合：<br>• IPv4 アドレス：<br>• サブネットマスク：<br>• ゲートウェイ<br>IPv6 の場合：<br>• IPv6 アドレス：<br>• ルーティング可能な IP アドレス：<br>• ストレージコントローラルータの IP アドレス： | IPv4 の場合：<br>• IPv4 アドレス：<br>• サブネットマスク：<br>• ゲートウェイ<br>IPv6 の場合：<br>• IPv6 アドレス：<br>• ルーティング可能な IP アドレス：<br>• ストレージコントローラルータの IP アドレス： |
| IP アドレスの形式 | 1 つ選択してください：<br>• IPv4<br>• IPv6 | 1 つ選択してください：<br>• IPv4<br>• IPv6 |
| 速度と二重モード<br>• 注： SANtricity システムマネージャ管理ネットワークのイーサネットスイッチが自動ネゴシエーションに設定されていることを確認してください。 | 次の値でなければなりません<br>• Autonegotiate （デフォルト） | 次の値でなければなりません<br>• Autonegotiate （デフォルト） |

**SG6000-CN**コントローラを管理ネットワークに接続するために必要な情報

StorageGRID の管理ネットワークは、システムの管理とメンテナンスに使用するオプションのネットワークです。アプライアンスは、 SG6000-CN コントローラの次の 1GbE 管理ポートを使用して管理ネットワーク

に接続します。

| 必要な情報 | あなたの価値 |
| --- | --- |
| 管理ネットワークが有効になりました | 1 つ選択してください：<br>• いいえ<br>• ○（デフォルト） |
| ネットワークボンディングモード | 1 つ選択してください：<br>• Independent （デフォルト）<br>• アクティブ / バックアップ |
| 図の赤い丸で示された左側のポートのスイッチポート（ Independent ネットワークボンディングモードのデフォルトのアクティブポート） | |
| 図の赤い丸で示されている右側のポートのスイッチポート（ Active-Backup ネットワークボンディングモードの場合のみ） | |
| 管理ネットワークポートの MAC アドレス<br>• 注： SG6000-CN コントローラの前面にある MAC アドレスラベルには、 BMC 管理ポートの MAC アドレスが記載されています。管理ネットワークポートの MAC アドレスを特定するには、ラベルに記載された 16 進数に * 2 * を追加する必要があります。たとえば、ラベルに記載されている MAC アドレスの末尾が * 09 * の場合、管理ポートの MAC アドレスの末尾は * 0B * となります。ラベルに記載された MAC アドレスの末尾が * （ *y* ） FF* の場合、管理ポートの MAC アドレスの末尾は * （ *y*+1 ） 01 * となります。この計算を簡単に行うには、 Windows で Calculator を開き、 Programmer モードに設定して Hex を選択し、 MAC アドレスを入力してから、 **+2=** と入力します。 | |
| DHCP によって割り当てられた管理ネットワークポートの IP アドレス（電源投入後に使用可能な場合）<br>• 注： * DHCP によって割り当てられた IP アドレスは、 MAC アドレスを使用して特定できます。 | • IPv4 アドレス（ CIDR ）：<br>• ゲートウェイ |

| 必要な情報 | あなたの価値 |
| --- | --- |
| 管理ネットワークでアプライアンスストレージノードに使用する静的 IP アドレス<br>• 注： * ネットワークにゲートウェイがない場合は、同じ静的 IPv4 アドレスをゲートウェイに指定してください。 | • IPv4 アドレス（ CIDR ）：<br>• ゲートウェイ |
| 管理ネットワークのサブネット（ CIDR ） | |

**SG6000-CN**コントローラの**10 / 25GbE**ポートの接続と設定に必要な情報

SG6000-CN コントローラの 4 つの 10 / 25GbE ポートは、 StorageGRID のグリッドネットワーク、およびオプションのクライアントネットワークに接続します。

| 必要な情報 | あなたの価値 |
| --- | --- |
| リンク速度 | 1 つ選択してください：<br>• auto （デフォルト）<br>• 10GbE の場合<br>• 25GbE |
| ポートボンディングモード | 1 つ選択してください：<br>• Fixed （デフォルト）<br>• アグリゲート |
| ポート 1 のスイッチポート（固定モードのクライアントネットワーク） | |
| ポート 2 のスイッチポート（ Fixed モードのグリッドネットワーク） | |
| ポート 3 のスイッチポート（固定モードのクライアントネットワーク） | |
| ポート 4 のスイッチポート（ Fixed モードのグリッドネットワーク） | |

**SG6000-CN**コントローラをグリッドネットワークに接続するために必要な情報

StorageGRID のグリッドネットワークは、内部のすべての StorageGRID トラフィックに使用される必須のネットワークです。アプライアンスは、 SG6000-CN コントローラの 10 / 25GbE ポートを使用してグリッドネットワークに接続します。

| 必要な情報 | あなたの価値 |
| --- | --- |
| ネットワークボンディングモード | 1 つ選択してください：<br>• Active-Backup （デフォルト）<br>• LACP （ 802.3ad ） |
| VLAN タギングが有効です | 1 つ選択してください：<br>• いいえ（デフォルト）<br>• はい。 |
| VLAN タグ（ VLAN タギングが有効な場合） | 0~4095 の値を入力してください： |
| 電源投入後に使用可能な場合、 DHCP によってグリッドネットワークに割り当てられた IP アドレス | • IPv4 アドレス（ CIDR ）：<br>• ゲートウェイ |
| グリッドネットワークでアプライアンスストレージノードに使用する静的 IP アドレス<br>• 注： * ネットワークにゲートウェイがない場合は、同じ静的 IPv4 アドレスをゲートウェイに指定してください。 | • IPv4 アドレス（ CIDR ）：<br>• ゲートウェイ |
| グリッドネットワークのサブネット（ CIDRs ） | |

**SG6000-CN**コントローラをクライアントネットワークに接続するために必要な情報

StorageGRID のクライアントネットワークは、一般にグリッドへのクライアントプロトコルアクセスを可能にするために使用する、オプションのネットワークです。アプライアンスは、 SG6000-CN コントローラの 10 / 25GbE ポートを使用してクライアントネットワークに接続します。

| 必要な情報 | あなたの価値 |
| --- | --- |
| クライアントネットワークが有効になりました | 1 つ選択してください：<br>• いいえ（デフォルト）<br>• はい。 |
| ネットワークボンディングモード | 1 つ選択してください：<br>• Active-Backup （デフォルト）<br>• LACP （ 802.3ad ） |

| 必要な情報 | あなたの価値 |
| --- | --- |
| VLAN タギングが有効です | 1 つ選択してください：<br>• いいえ（デフォルト）<br>• はい。 |
| VLAN タグ（ VLAN タギングが有効な場合） | 0~4095 の値を入力してください： |
| 電源投入後に DHCP によってクライアントネットワークに割り当てられた IP アドレスがある場合は | • IPv4 アドレス（ CIDR ）：<br>• ゲートウェイ |
| クライアントネットワークでアプライアンスストレージノードに使用する静的 IP アドレス<br>• 注：＊クライアントネットワークが有効になっている場合、コントローラのデフォルトルートではここで指定したゲートウェイが使用されます。 | • IPv4 アドレス（ CIDR ）：<br>• ゲートウェイ |

**SG6000-CN**コントローラを**BMC**管理ネットワークに接続するために必要な情報

SG6000-CN コントローラの BMC インターフェイスには、次の 1GbE 管理ポートを使用してアクセスできます。このポートは、 Intelligent Platform Management Interface （ IPMI ）標準を使用した、イーサネット経由でのコントローラハードウェアのリモート管理をサポートします。

| 必要な情報 | あなたの価値 |
| --- | --- |
| BMC 管理ポートに接続するイーサネットスイッチポート（赤枠内） | |
| 電源投入後に DHCP によって BMC 管理ネットワークに割り当てられた IP アドレスがある場合は | • IPv4 アドレス（ CIDR ）：<br>• ゲートウェイ |
| BMC 管理ポートに使用する静的 IP アドレス | • IPv4 アドレス（ CIDR ）：<br>• ゲートウェイ |

関連情報

"SG6000アプライアンスのコントローラ"

"アプライアンスのネットワーク接続を確認します"

"SG6000-CNコントローラのポートボンディングモード"

"アプライアンスのケーブル接続（SG6000）"

"StorageGRID IPアドレスを設定しています"

## ハードウェアを設置

ハードウェアの設置作業では、 SG6000-CN コントローラとストレージコントローラシェルフをキャビネットまたはラックに設置し、ケーブルを接続し、電源を投入します。

手順

- "ハードウェアの登録"
- "SG6060：キャビネットまたはラックへの60ドライブシェルフの設置"
- "SG6060：ドライブの取り付け"
- "SGF6024：キャビネットまたはラックへの24ドライブシェルフの設置"
- "SG6000-CN：キャビネットまたはラックへの設置"
- "アプライアンスのケーブル接続（SG6000）"
- "SG6060：オプションの拡張シェルフのケーブル接続"
- "電源コードの接続と電源の投入（SG6000）"
- "SG6000-CNコントローラのステータスインジケータとボタンの表示"
- "SG6000ストレージコントローラのブート時のステータスコードを確認する"

### ハードウェアの登録

アプライアンスハードウェアを登録するとサポートを受けられるようになります。

手順

1. ストレージコントローラシェルフのシャーシのシリアル番号を確認します。

   この番号は、納品書や確認用 E メールで確認できるほか、開梱したアプライアンスにも記載されています。

   ストレージアプライアンスには複数のシリアル番号があります。ストレージコントローラシェルフのシリアル番号は、アプライアンスのサービスまたはサポートを受けるために登録して使用する必要がある番号です。

2. NetApp Support Siteにアクセスします "mysupport.netapp.com"。
3. ハードウェアの登録が必要かどうかを確認します。

| ユーザのタイプとアクセス方法 | 実行する手順 |
| --- | --- |
| ネットアップの既存のお客様 | a. ユーザ名とパスワードを使用してサインインします。<br>b. [ 製品 **>*My Products** ] を選択します。<br>c. 新しいシリアル番号が表示されていることを確認します。<br>d. 表示されていない場合は、ネットアップの新規のお客様向けの手順に従ってください。 |
| ネットアップの新規のお客様 | a. [ 今すぐ登録 ] をクリックしてアカウントを作成します。<br>b. [**Products**>*Register Products*] を選択します。<br>c. 製品のシリアル番号と要求された詳細情報を入力します。<br>登録が承認されると、必要なソフトウェアをダウンロードできます。承認プロセスには最大 24 時間かかる場合があります。 |

**SG6060**：キャビネットまたはラックへの**60**ドライブシェルフの設置

## キャビネットまたはラックに E2860 コントローラシェルフ用のレール一式を取り付け、レールにコントローラシェルフをスライドさせます。60 ドライブ拡張シェルフを設置する場合は、同じ手順 が適用されます。

必要なもの

- 同梱されている安全上の注意に関するドキュメントを確認し、ハードウェアの移動と設置に関する注意事項を理解しておきます。
- レールキットに手順書が同梱されていることを確認します。

ドライブが取り付けられていない状態の 60 ドライブシェルフの重量は、約 60kg （ 132 ポンド ）です。シェルフを安全に移動するには、 4 名の人員または電動リフトが必要です。

ハードウェアの損傷を避けるため、ドライブを取り付けた状態でシェルフを移動しないでください。シェルフを移動する前に、ドライブをすべて取り外す必要があります。

E2860 コントローラシェルフまたはオプションの拡張シェルフを設置する場合は、機器の転倒を防ぐために、ラックまたはキャビネットの一番下から順にハードウェアを設置してください。最も重い機器をキャビネットまたはラックの一番下に設置するには、 E2860 コントローラシェルフおよび拡張シェルフの上に SG6000-CN コントローラを設置します。

設置作業を行う前に、アプライアンスに付属の 0.5m 光ケーブル、または用意したケーブルの長さが、計画したレイアウトに十分であることを確認してください。

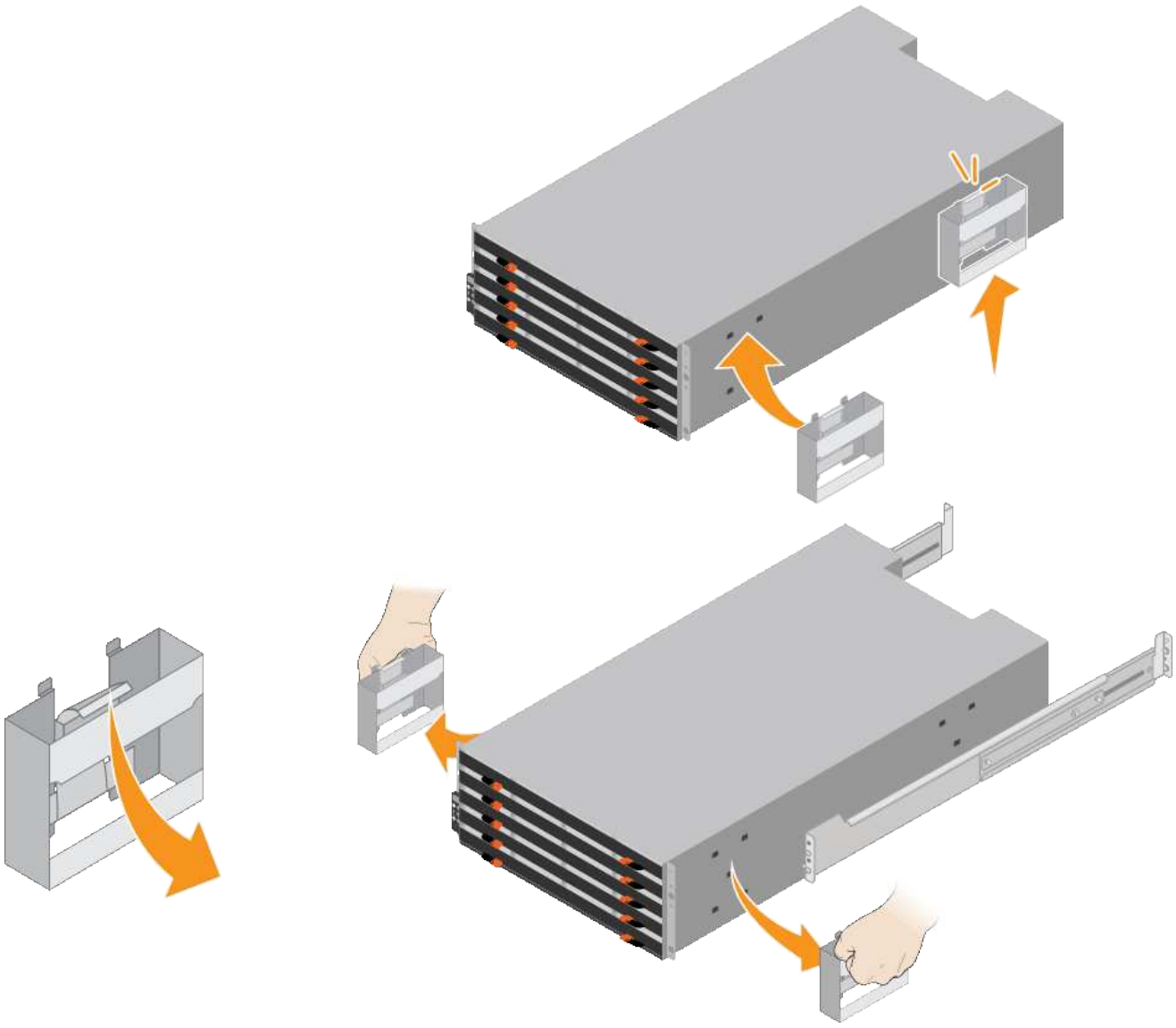
手順

1. キャビネットまたはラックにレールを取り付ける際には、レールキットの手順書に慎重に従ってください。

   角穴キャビネットの場合は、最初に付属のケージナットを取り付けて、シェルフの前面と背面をネジで固定する必要があります。

2. アプライアンスの外箱を取り外します。次に、内側のボックスのフラップを折りたたみます。
3. アプライアンスを手で持ち上げる場合は、シャーシの側面に 4 つのハンドルを取り付けます。

   各ハンドルをカチッと所定の位置に収まるまで押し上げます。



4. シェルフの背面（コネクタ側）をレールに配置します。
5. シェルフを底から支えながら、キャビネットにスライドさせます。ハンドルを使用している場合は、サムラッチを使用して、シェルフをスライドさせながら一度に 1 つずつハンドルを外します。

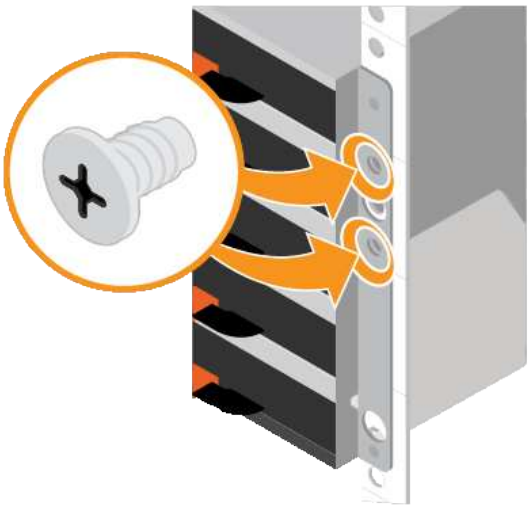
   ハンドルを取り外すには、リリースラッチを後方に引き、押し下げてシェルフから引き出します。

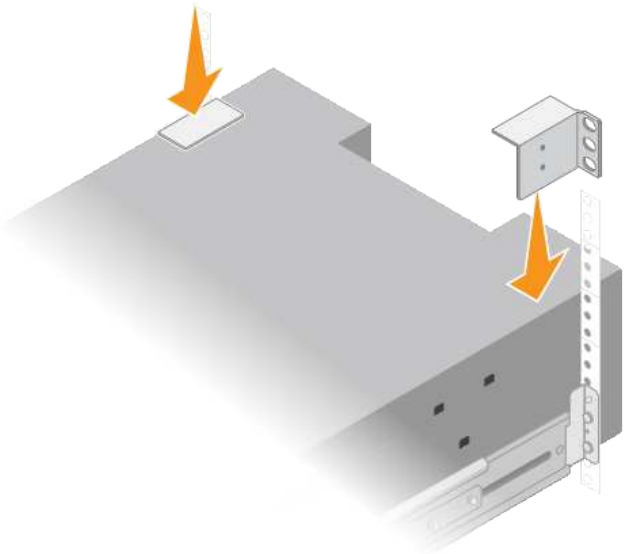
6. シェルフをキャビネットの前面に固定します。

   シェルフの両側の上部から 1 番目と 3 番目の穴にネジを差し込みます。

7. シェルフをキャビネットの背面に固定します。

   シェルフの背面上部の両側に 2 つの後部ブラケットを配置します。各ブラケットの 1 番目と 3 番目の穴にネジを差し込みます。





8. すべての拡張シェルフについて、上記の手順を繰り返します。

**SG6060**：ドライブの取り付け

## 60 ドライブシェルフをキャビネットまたはラックに設置したら、シェルフに 60 本のドライブをすべて取り付ける必要があります。E2860 コントローラシェルフには SSD ドライブが 2 本同梱されており、これらをコントローラシェルフ上段のドロワーに取り付ける必要があります。オプションの拡張シェルフには HDD ドライブが 60 本同梱されていますが、 SSD ドライブは同梱され

必要なもの

E2860 コントローラシェルフまたはオプションの拡張シェルフ（ 1 台または 2 台）をキャビネットまたはラックに設置しておきます。

ハードウェアの損傷を避けるため、ドライブを取り付けた状態でシェルフを移動しないでください。シェルフを移動する前に、ドライブをすべて取り外す必要があります。

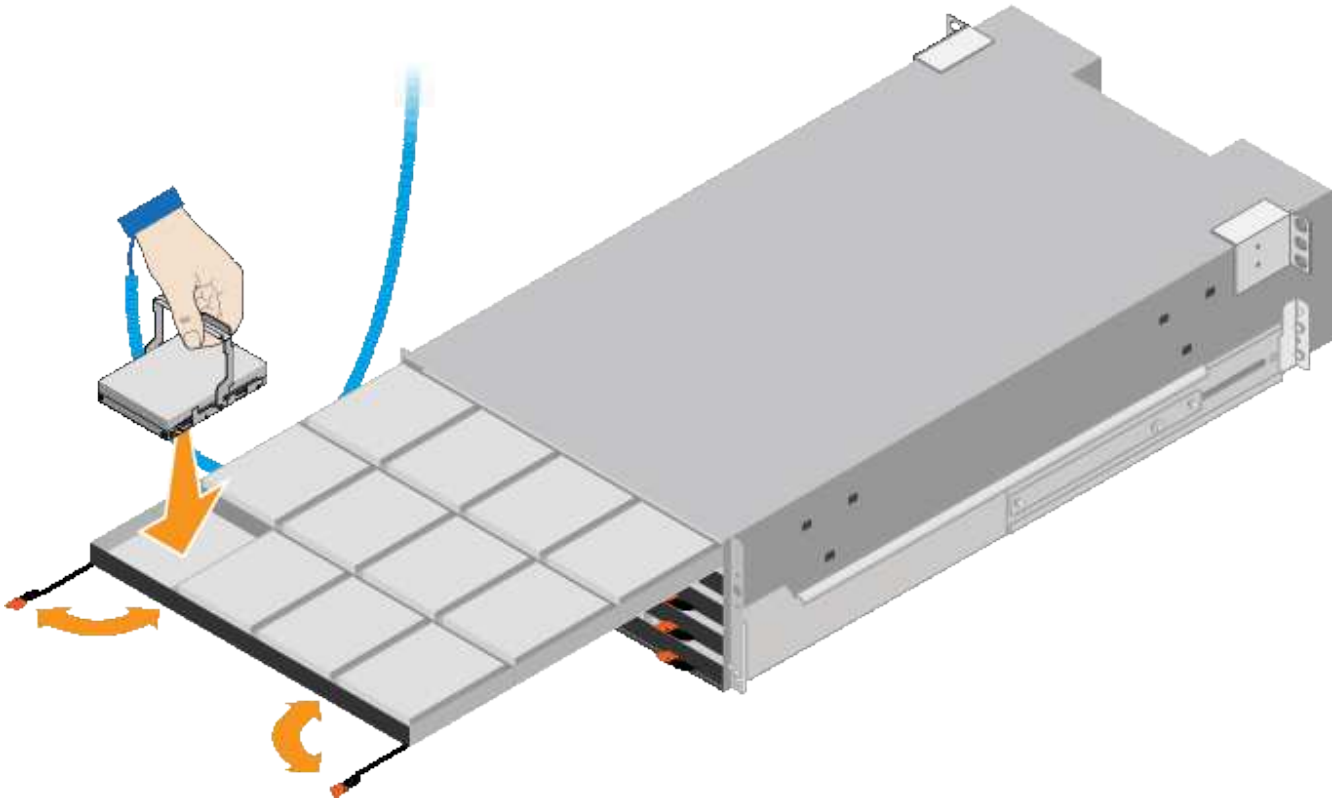
手順

1. ESD リストバンドのストラップの端を手首に巻き付け、静電気の放電を防ぐためにクリップの端をメタルアースに固定します。
2. ドライブをパッケージから取り出します。
3. 上部ドライブドロワーのレバーを解放し、レバーを使用してドロワーを引き出します。

4. 2 本の SSD ドライブを確認します。

   拡張シェルフでは SSD ドライブを使用しません。

5. 各ドライブのハンドルを垂直な位置まで持ち上げます。
6. 2 本の SSD ドライブをスロット 0 と 1 （ドロワーの左側にある最初の 2 つのスロット）に取り付けます。
7. 各ドライブをスロットに慎重に配置し、持ち上げたドライブのハンドルをカチッと所定の位置に収まるまで下げます。



8. 10 本の HDD ドライブを上段のドロワーに取り付けます。
9. ドロワーの中央を押し、両方のレバーを静かに閉じてドロワーを元の位置に戻します。

   しっかりはまったら、ドロワーを押すのを止めます。ドロワーの前面にあるリリースレバーを使ってドロワーを引き出します。次に、ドロワーを慎重にスロットに挿入し直します。

10. 残りの 4 つのドロワーに HDD ドライブを取り付ける場合は、上記の手順を繰り返します。

    正しく動作させるためには、 60 本のドライブをすべて取り付ける必要があります。

11. 前面ベゼルをシェルフに取り付けます。
12. 拡張シェルフを使用する場合は、上記の手順を繰り返して、それぞれの拡張シェルフの各ドロワーに HDD ドライブを 12 本取り付けます。
13. キャビネットまたはラックに SG6000-CN を設置する手順に進みます。

# EF570 コントローラシェルフ用のレールをキャビネットまたはラックに取り付け、レールにアレイをスライドさせます。

必要なもの

- 同梱されている安全上の注意に関するドキュメントを確認し、ハードウェアの移動と設置に関する注意事項を理解しておきます。
- レールキットに手順書が同梱されていることを確認します。

手順

1. キャビネットまたはラックにレールを取り付ける際には、レールキットの手順書に慎重に従ってください。

   角穴キャビネットの場合は、最初に付属のケージナットを取り付けて、シェルフの前面と背面をネジで固定する必要があります。

2. アプライアンスの外箱を取り外します。次に、内側のボックスのフラップを折りたたみます。
3. シェルフの背面（コネクタ側）をレールに配置します。

   フル装備のシェルフの重量は、約 24kg （ 52 ポンド）です。エンクロージャを安全に移動するには、 2 名で運搬する必要があります。

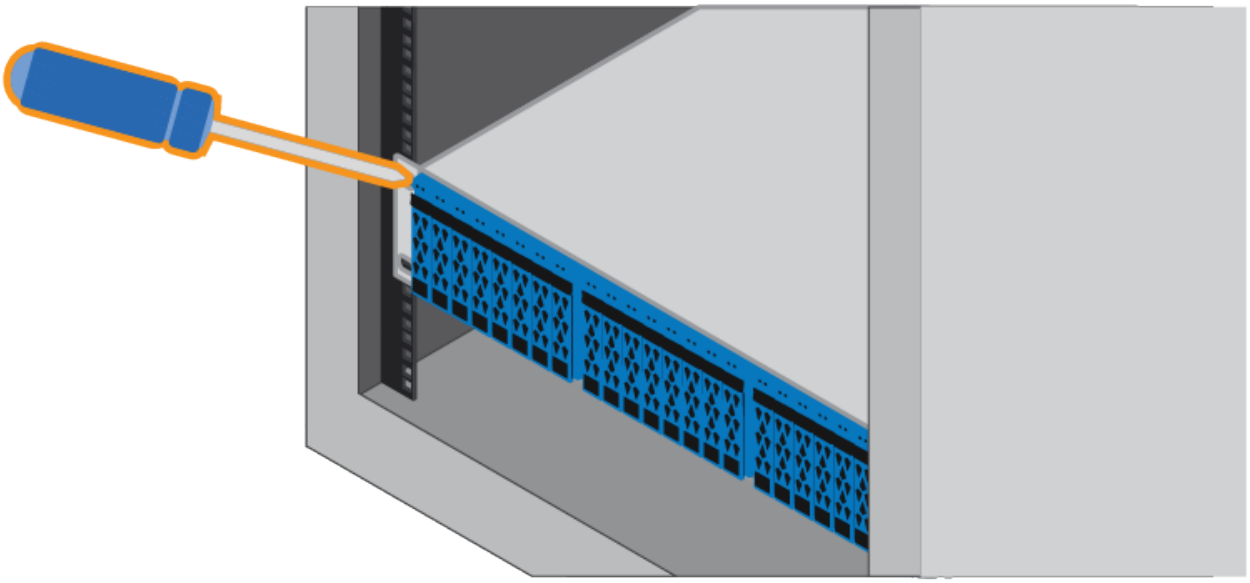
4. シェルフを慎重にレールにスライドさせて、奥まで押し込みます。

   シェルフを奥まで入るよう、レールの調整が必要になる場合があります。

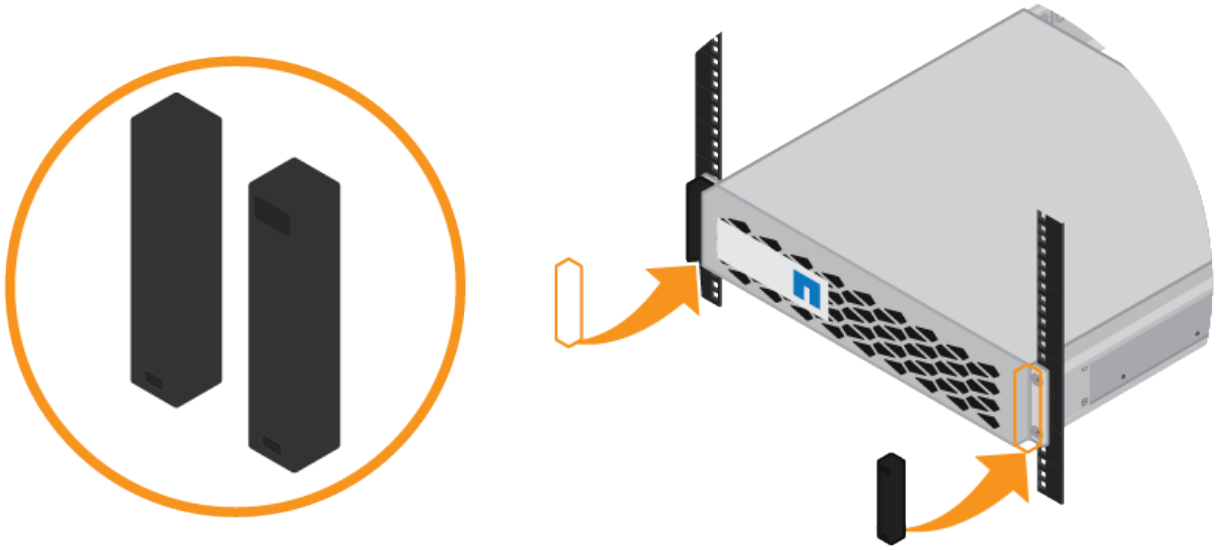
   シェルフの設置が完了したあとにレールにその他の機器を置かないでください。レールはシェルフ以外の機器の重量を支えるようには設計されていません。

   必要に応じて、シェルフのエンドキャップやシステムベゼルを取り外してエンクロージャをラックポストに固定しなければならない場合があります。その場合は、作業が終わったらエンドキャップやベゼルを交換する必要があります。

5. 取り付け用ブラケット（エンクロージャ前面の両側に取り付け済み）、ラックまたはシステムキャビネットの穴、およびレール前面の穴に 2 本の M5 ネジを通し、エンクロージャをキャビネットまたはラックとレールの前面に固定します。



6. シェルフのブラケットとレールキットブラケットに 2 本の M5 ネジを通して、エンクロージャをレールの背面に固定します。
7. 必要に応じて、シェルフのエンドキャップまたはシステムベゼルを交換します。



**SG6000-CN**：キャビネットまたはラックへの設置

## キャビネットまたはラックに SG6000-CN コントローラのレールを 1 組取り付け、レールにコントローラをスライドさせます。

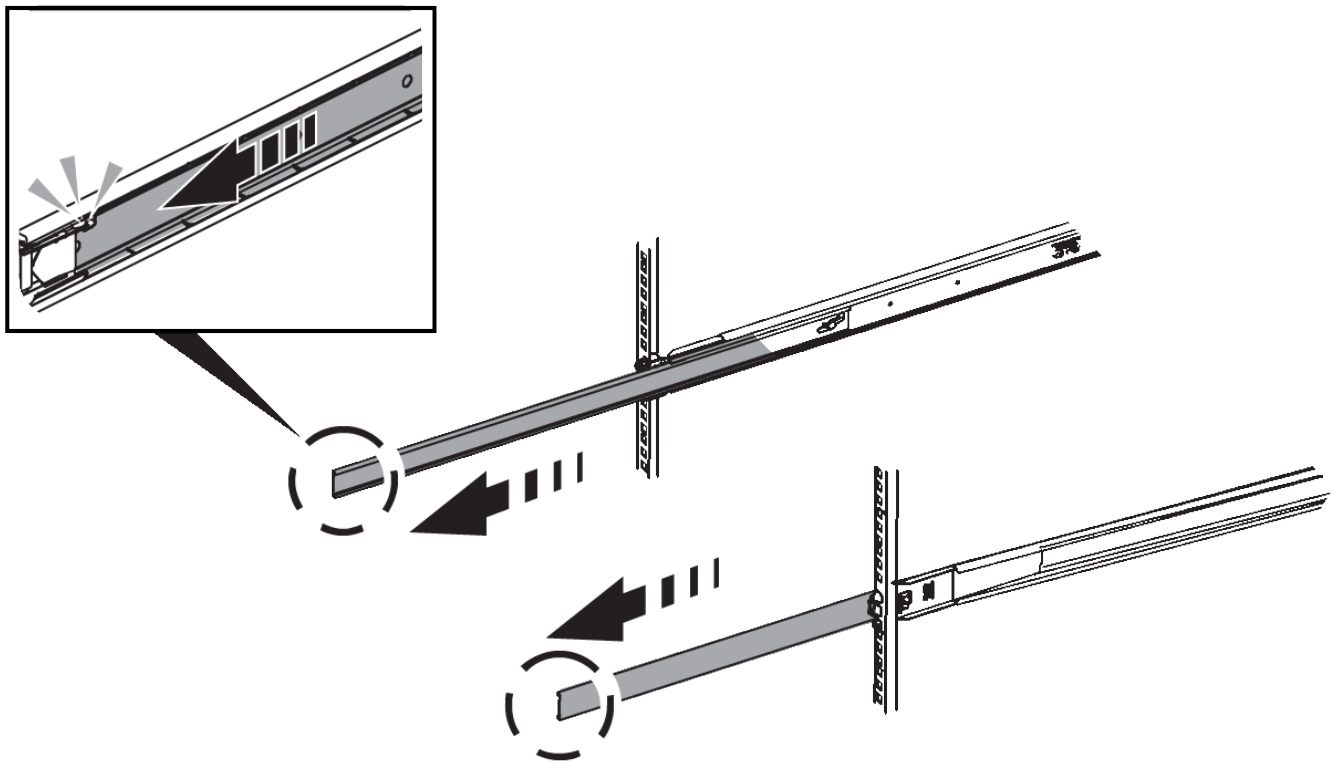
必要なもの

- 同梱されている安全上の注意に関するドキュメントを確認し、ハードウェアの移動と設置に関する注意事項を理解しておきます。

- レールキットに手順書が同梱されていることを確認します。
- E2860 コントローラシェルフとドライブまたは EF570 コントローラシェルフを取り付けておきます。

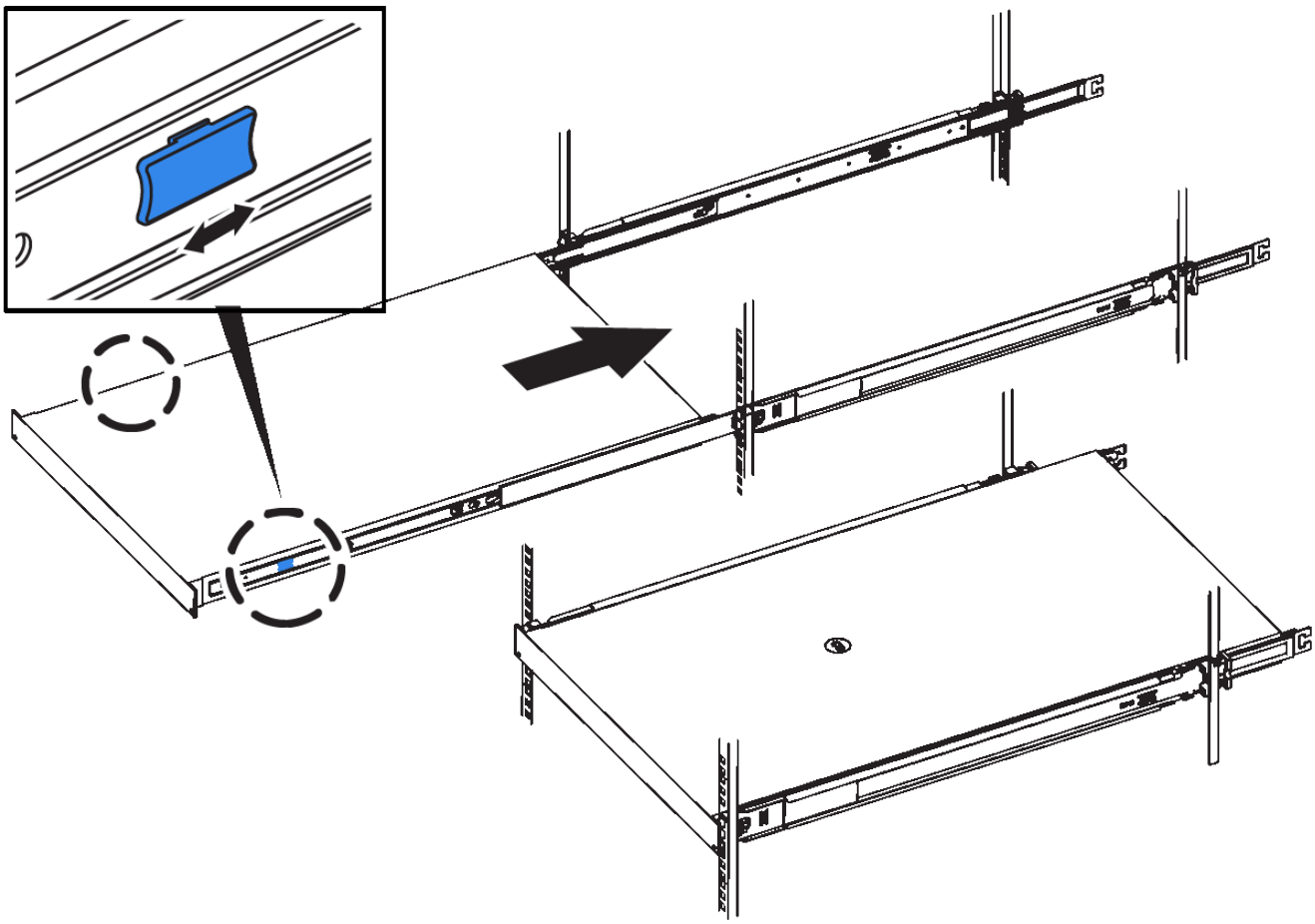
手順

1. キャビネットまたはラックにレールを取り付ける際には、レールキットの手順書に慎重に従ってください。
2. キャビネットまたはラックに取り付けた 2 本のレールで、カチッという音がするまでレールの可動部分を伸ばします。



3. SG6000-CN コントローラをレールに挿入します。
4. コントローラをキャビネットまたはラックにスライドさせます。

   コントローラが途中でひっかかる場合は、シャーシの両側にある青いラッチを引いて、コントローラを奥までスライドさせます。



コントローラの電源を入れるまでは、前面ベゼルを取り付けないでください。

5. コントローラの前面パネルの非脱落型ネジを締めて、コントローラをラックに固定します。

アプライアンスのケーブル接続（**SG6000**）

## ストレージコントローラを SG6000-CN コントローラに接続し、 3 台すべてのコントローラの管理ポートを接続して、 SG6000-CN コントローラのネットワークポートを StorageGRID のグリッドネットワークとオプションのクライアントネットワークに接続する必要があります。

必要なもの

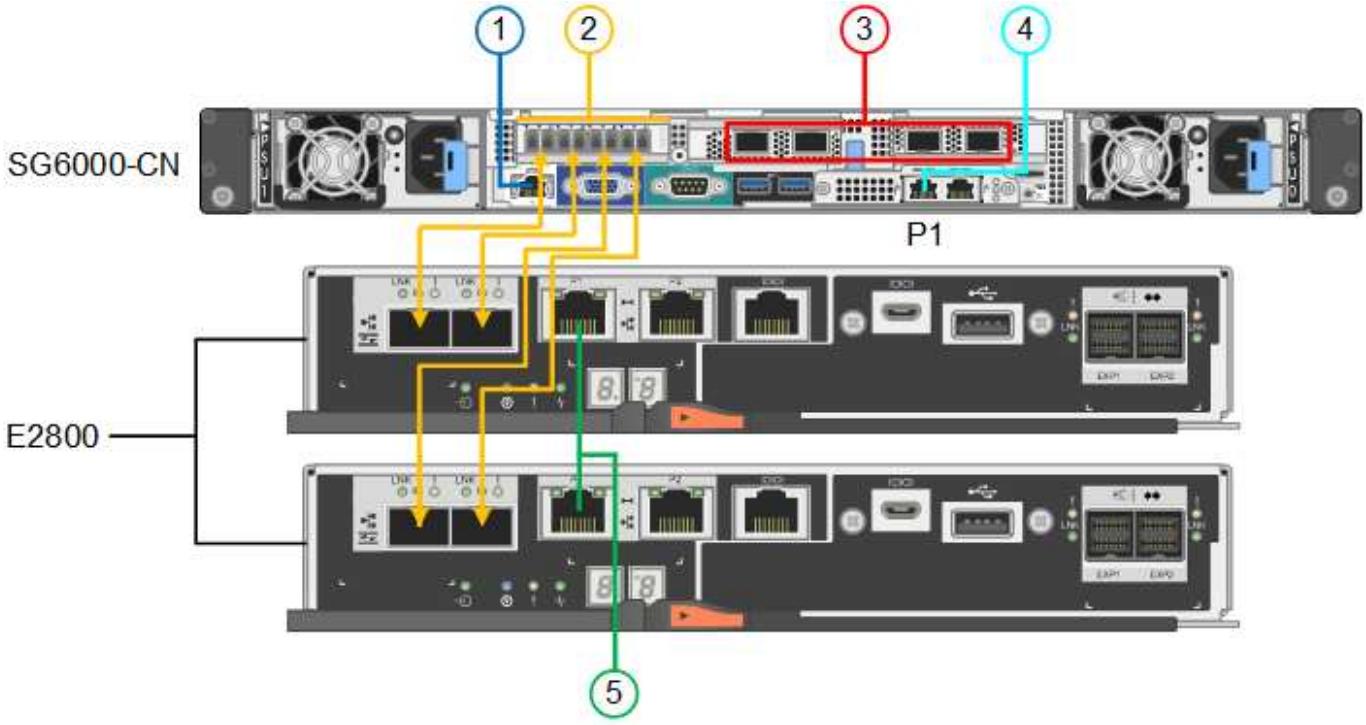
- アプライアンスに付属する 4 本の光ケーブルを使用して、 2 台のストレージコントローラを SG6000-CN コントローラに接続します。
- 管理ポートを接続するための RJ-45 イーサネットケーブルを最低 4 本用意しておきます。
- ネットワークポートに次のいずれかを設定しておきます。これらはアプライアンスには付属していません。

- 4 つのネットワークポートを接続するための TwinAx ケーブルを 1~4 本。
- ポートに光ケーブルを使用する場合は、 SFP+ または SFP28 トランシーバを 1~4 個。

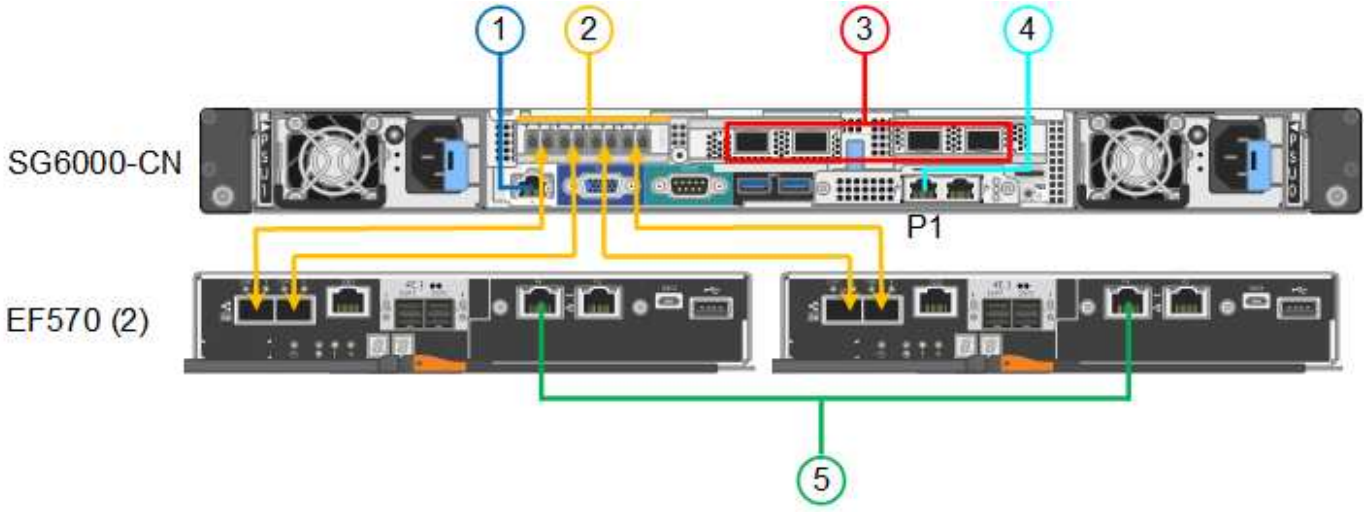
> * レーザー被ばくの危険性 * — SFP トランシーバを分解したり部品を取り外したりしないでください。レーザー被ばくのおそれがあります。

このタスクについて

次の図は、 SG6060 アプライアンスの 3 台のコントローラ、 SG6000-CN コンピューティングコントローラが上に、 E2800 ストレージコントローラが下にそれぞれ配置された状態を示しています。




次の図は、 SGF6024 アプライアンスの 3 台のコントローラを示しています。 SG6000-CN コンピューティングコントローラが上部に、 2 台の EF570 ストレージコントローラがコンピューティングコントローラの下側にそれぞれ配置されています。



| | ポート | ポートのタイプ | 機能 |
|---|---|---|---|
| 1. | SG6000-CN コントローラの BMC 管理ポート | 1GbE （ RJ-45 ） | BMC インターフェイスにアクセスするネットワークに接続します。 |
| 2. | FC 接続ポート：<br>• SG6000-CN コントローラで 4 つ<br>• 各ストレージコントローラに 2 つ | 16Gb/s FC 光ファイバ SFP+ | 各ストレージコントローラを SG6000-CN コントローラに接続します。 |
| 3. | SG6000-CN コントローラの 4 つのネットワークポート | 10 / 25GbE | StorageGRID のグリッドネットワークおよびクライアントネットワークに接続します。 |
| 4. | SG6000-CN コントローラの管理ネットワークポート（図の P1 ） | 1GbE （ RJ-45 ）<br>• 重要： * このポートは 1000BASE-T / 全二重でのみ動作し、 10 メガビットまたは 100 メガビットの速度はサポートしません。 | SG6000-CN コントローラを StorageGRID の管理ネットワークに接続します。 |
| 4. | SG6000-CN コントローラの右端の RJ-45 ポート | 1GbE （ RJ-45 ）<br>• 重要： * このポートは 1000BASE-T / 全二重でのみ動作し、 10 メガビットまたは 100 メガビットの速度はサポートしません。 | • 管理ネットワークへの冗長接続が必要な場合は、管理ポート 1 とボンディングできます。<br>• 一時的なローカルアクセス用（ IP 169.254.0.1 ）に空けておくことができます。<br>• DHCP によって割り当てられた IP アドレスを使用できない場合は、設置時に SG6000-CN コントローラをサービスラップトップに接続するためにを使用できます。 |

| | ポート | ポートのタイプ | 機能 |
|---|---|---|---|
| 5. | 各ストレージコントローラの管理ポート 1 | 1GbE （ RJ-45 ） | SANtricity System Manager にアクセスするネットワークに接続します。 |
| 5. | 各ストレージコントローラの管理ポート 2 | 1GbE （ RJ-45 ） | テクニカルサポート専用です。 |

手順

1. イーサネットケーブルを使用して、 SG6000-CN コントローラの BMC 管理ポートを管理ネットワークに接続します。

   この接続はオプションですが、サポート用に接続することを推奨します。

2. ストレージコントローラの 4 本の光ケーブルと 4 個の SFP+ トランシーバを使用して、各ストレージコントローラの 2 つの FC ポートを SG6000-CN コントローラの FC ポートに接続します。
3. SG6000-CN コントローラのネットワークポートを、 TwinAx ケーブル、または光ケーブルと SFP+ または SFP28 トランシーバを使用して、適切なネットワークスイッチに接続します。

   4 つのネットワークポートで同じリンク速度を使用する必要があります。10GbE のリンク速度を使用する場合は、 SFP+ トランシーバを取り付けます。25GbE のリンク速度を使用する場合は、 SFP28 トランシーバを取り付けます。

   - 固定ポートボンディングモード（デフォルト）を使用する場合は、次の表のように各ポートを StorageGRID のグリッドネットワークまたはクライアントネットワークに接続します。

     | ポート | 接続先 |
     |---|---|
     | ポート 1 | クライアントネットワーク（オプション） |
     | ポート 2 | Grid ネットワーク |
     | ポート 3 | クライアントネットワーク（オプション） |
     | ポート 4. | Grid ネットワーク |

   - アグリゲートポートボンディングモードを使用する場合は、 1 つ以上のネットワークポートを 1 つ以上のスイッチに接続します。単一点障害を回避するために、 4 つのポートのうち少なくとも 2 つを接続する必要があります。1 つの LACP ボンドに複数のスイッチを使用する場合は、スイッチが MLAG または同等の機能をサポートしている必要があります。
4. StorageGRID の管理ネットワークを使用する場合は、 SG6000-CN コントローラの管理ネットワークポートをイーサネットケーブルで管理ネットワークに接続します。
5. 各ストレージコントローラの管理ポート1（P1、左側のRJ-45ポート）を、イーサネットケーブルでSANtricity System Managerの管理ネットワークに接続します。

ストレージコントローラの管理ポート 2 （ P2 、右側の RJ-45 ポート）は使用しないでください。このポートはテクニカルサポート専用です。

関連情報

"SG6000-CNコントローラのポートボンディングモード"

"キャビネットまたはラックへのSG6000-CNコントローラの再取り付け"

**SG6060**：オプションの拡張シェルフのケーブル接続

拡張シェルフを使用する場合は、 E2860 コントローラシェルフに拡張シェルフを接続する必要があります。SG6060 アプライアンスには、最大 2 台の拡張シェルフを用意できます。

必要なもの

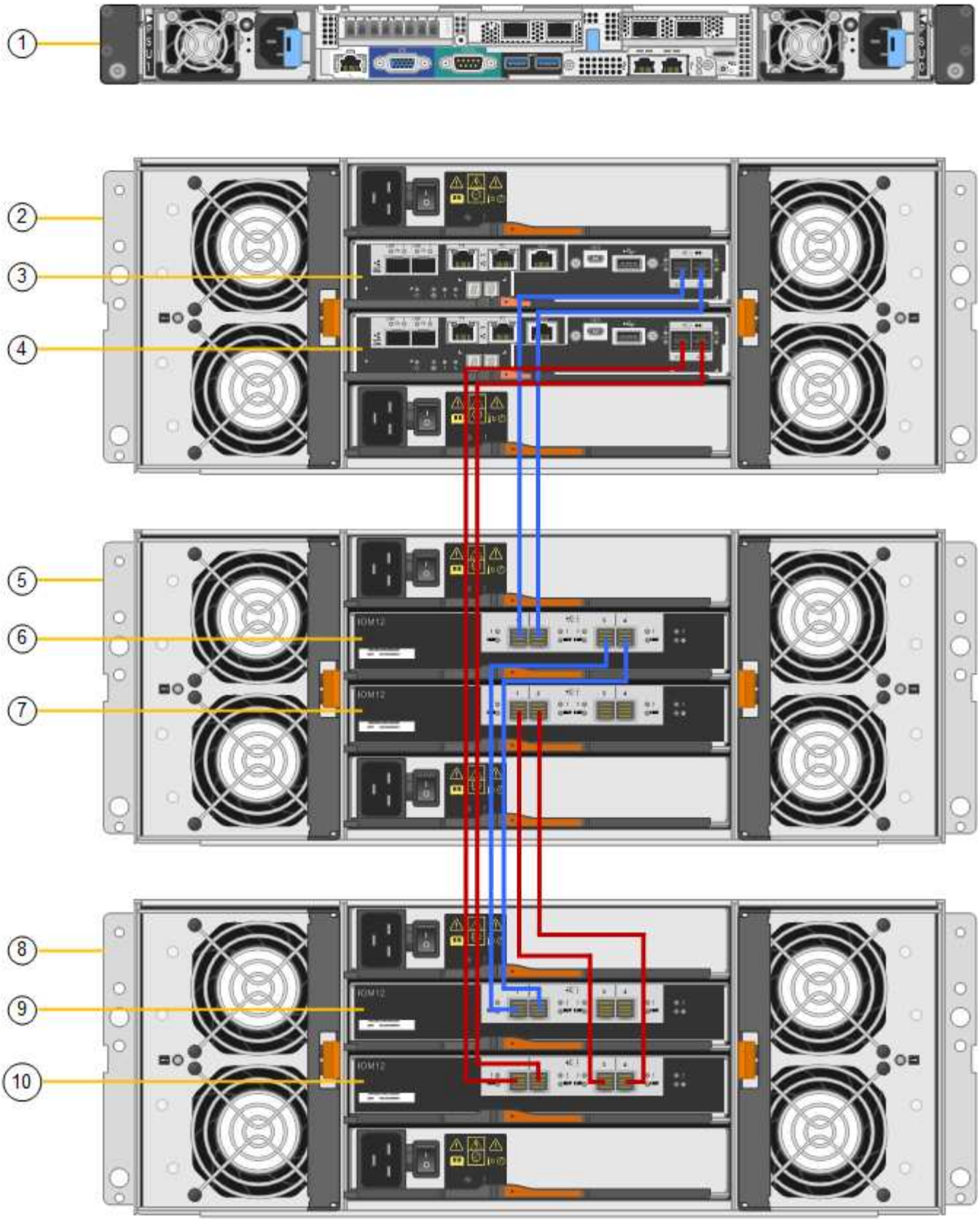
- それぞれの拡張シェルフに付属の 2 本の SAS ケーブルを用意しておきます。
- E2860 コントローラシェルフが搭載されたキャビネットまたはラックに拡張シェルフを設置しておきます。

  "SG6060：キャビネットまたはラックへの60ドライブシェルフの設置"

ステップ

次の図に示すように、各拡張シェルフを E2860 コントローラシェルフに接続します。

この図は、 2 台の拡張シェルフを示しています。IOM A のみをコントローラ A に接続し、 IOM B をコントローラ B に接続します




| | 説明 |
|---|---|
| 1. | SG6000-CN の情報 |

| | 説明 |
|---|---|
| 2. | E2860 コントローラシェルフです |
| 3. | コントローラ A |
| 4. | コントローラ B |
| 5. | 拡張シェルフ 1 |
| 6. | 拡張シェルフ 1 の IOM A |
| 7. | 拡張シェルフ 1 の IOM B |
| 8. | 拡張シェルフ 2 |
| 9. | 拡張シェルフ 2 の IOM A |
| 10. | 拡張シェルフ 2 の IOM B |

電源コードの接続と電源の投入（**SG6000**）

## ネットワークケーブルを接続したら、 SG6000-CN コントローラと 2 台のストレージコントローラまたはオプションの拡張シェルフの電源を入れることができます。

手順

1. ストレージコントローラシェルフの両方のコントローラがオフになっていることを確認します。

> * 感電の危険性 * — 電源コードを接続する前に、 2 台の各ストレージコントローラの電源スイッチがオフになっていることを確認してください。

2. 拡張シェルフがある場合は、両方の IOM の電源スイッチがオフになっていることを確認します。

> * 感電の危険性 * — 電源コードを接続する前に、各拡張シェルフの 2 つの電源スイッチがオフになっていることを確認してください。

3. SG6000-CN コントローラの 2 つ電源装置のそれぞれに電源コードを接続します。
4. これらの 2 本の電源コードを、キャビネットまたはラック内の別々の配電ユニット（ PDU ）に接続します。
5. ストレージコントローラシェルフの 2 つ電源装置のそれぞれに電源コードを接続します。
6. 拡張シェルフがある場合は、各拡張シェルフの 2 つ電源装置のそれぞれに電源コードを接続します。
7. 各ストレージシェルフ（オプションの拡張シェルフを含む）の 2 本の電源コードを、キャビネットまたはラック内の別々の PDU に接続します。
8. SG6000-CN コントローラの前面にある電源ボタンが青色に点灯していない場合は、ボタンを押してコン

トローラの電源をオンにします。

電源投入プロセス中は、電源ボタンを再度押さないでください。

9. ストレージコントローラシェルフの背面にある 2 つの電源スイッチをオンにします。拡張シェルフがある場合は、各シェルフの 2 つの電源スイッチをオンにします。
   - 電源投入プロセスの実行中は電源スイッチをオフにしないでください。
   - ストレージコントローラシェルフとオプションの拡張シェルフのファンは、初回起動時に大きな音を立てることがあります。起動時に大きな音がしても問題はありません。
10. コンポーネントが起動したら、ステータスを確認します。
    - 各ストレージコントローラの背面のデジタル表示ディスプレイを確認します。詳細については、起動時のステータスコードの表示に関する記事を参照してください。
    - SG6000-CN コントローラの前面にある電源ボタンが点灯していることを確認します。
11. エラーが発生した場合は、問題を修正します。
12. 前面ベゼルをSG6000-CNコントローラに接続します。

関連情報

"SG6000ストレージコントローラのブート時のステータスコードを確認する"

"SG6000-CNコントローラのステータスインジケータとボタンの表示"

"キャビネットまたはラックへのSG6000-CNコントローラの再取り付け"

**SG6000-CN**コントローラのステータスインジケータとボタンの表示

SG6000-CN コントローラには、次のインジケータやボタンなど、コントローラのステータスの確認に役立つインジケータが搭載されています。

| | 表示 | 説明 |
|---|---|---|
| 1. | 電源ボタン | • 青色：コントローラの電源がオンになっています。<br>• off ：コントローラの電源がオフになっています。 |
| 2. | リセットボタン | _ インジケータなし _<br><br>このボタンを使用して、コントローラのハードリセットを実行します。 |

| | 表示 | 説明 |
|---|---|---|
| 3. | 識別ボタン | • 点滅または青で点灯：キャビネットまたはラック内のコントローラを示します。<br>• 消灯：キャビネットやラック内のコントローラを目視で識別できません。<br><br>このボタンは、点滅、点灯、または消灯に設定できます。 |
| 4. | アラーム LED | • アンバー：エラーが発生しました。<br>• 注：＊ブート時のコードとエラーコードを確認するには、BMC インターフェイスにアクセスする必要があります。<br>• 消灯：エラーはありません。 |

一般的なブートコード

SG6000-CN コントローラのブート時またはハードリセット後、次の処理が実行されます。

1. ベースボード管理コントローラ（ BMC ）が、ブート処理のコード（発生したエラーを含む）を記録します。
2. 電源ボタンが点灯します。
3. ブート中にエラーが発生した場合は、アラーム LED が点灯します。

   ブート時のコードとエラーコードを表示するには、 BMC インターフェイスにアクセスする必要があります。

関連情報

"ハードウェアの設置のトラブルシューティング"

"BMCインターフェイスを設定しています"

"SG6000-CNコントローラの電源をオンにして処理を確認します"

**SG6000**ストレージコントローラのブート時のステータスコードを確認する

各ストレージコントローラにはデジタル表示ディスプレイがあり、電源投入時にステータスコードが表示されます。ステータスコードは、 E2800 コントローラと EF570 コントローラで同じです。

このタスクについて

これらのコードの説明については、使用しているストレージコントローラタイプの E シリーズシステムの監視に関する情報を参照してください。

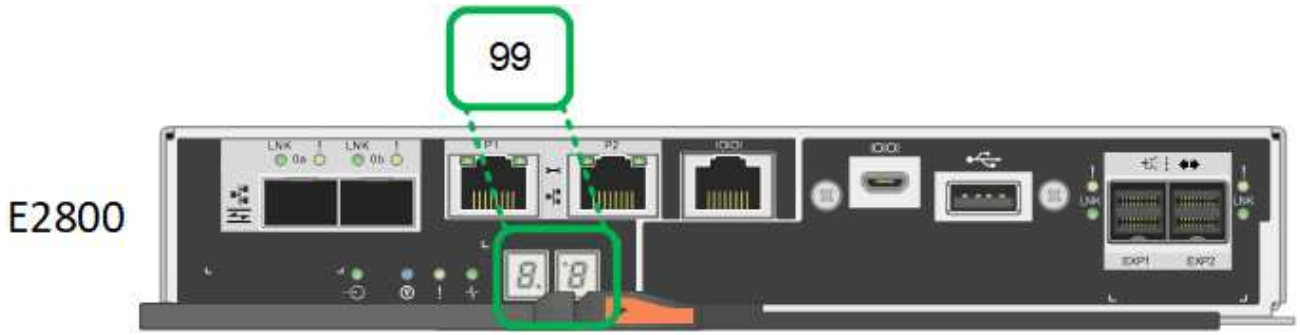
手順

1. ブート時に、各ストレージコントローラのデジタル表示ディスプレイに表示されるコードを確認して進行状況を監視します。

   各ストレージコントローラのデジタル表示ディスプレイに、* OS 、 SD 、 ***blank*** コントローラが一日の開始処理を実行中であることを示します。

2. コントローラがブートすると、各ストレージコントローラに E シリーズコントローラシェルフのデフォルト ID である 99 が表示されます。

   この値が両方のストレージコントローラに表示されていることを確認してください。以下は E2800 コントローラの例です。




3. 一方または両方のコントローラに別の値が表示される場合は、ハードウェアの設置に関するトラブルシューティング情報を参照し、設置手順が正しく完了していることを確認してください。問題を解決できない場合は、テクニカルサポートにお問い合わせください。

関連情報

"E5700 and E2800 System Monitoring Guide"

"ハードウェアの設置のトラブルシューティング"

"ネットアップサポート"

"SG6000-CNコントローラの電源をオンにして処理を確認します"

## ハードウェアの設定

アプライアンスの電源を入れたら、 StorageGRID で使用するネットワーク接続を設定する必要があります。SANtricity System Manager を設定する必要があります。これは、コントローラシェルフのストレージコントローラとその他のハードウェアを監視するためのソフトウェアです。また、 SG6000-CN コントローラの BMC インターフェイスにアクセスできることを確認する必要もあります。

手順

- "StorageGRID 接続を設定しています"
- "SANtricity システムマネージャにアクセスして設定します"
- "BMCインターフェイスを設定しています"
- "オプション：ノード暗号化を有効にする"

- "オプション：RAIDモードの変更（SG6000のみ）"
- "オプション：アプライアンスに対するネットワークポートの再マッピング"

**StorageGRID** 接続を設定しています

StorageGRID アプライアンスをストレージノードとして StorageGRID システムに導入するには、アプライアンスと使用するネットワークの間の接続を設定する必要があります。ネットワークを設定するには、 SG6000-CN コントローラ（コンピューティングコントローラ）に事前にインストールされている StorageGRID アプライアンスインストーラにアクセスします。

手順

- "StorageGRID アプライアンスインストーラへのアクセス"
- "StorageGRID アプライアンスインストーラのバージョンの確認とアップグレード"
- "ネットワークリンクの設定（SG6000）"
- "StorageGRID IPアドレスを設定しています"
- "ネットワーク接続の確認"
- "ポートレベルのネットワーク接続の確認"

**StorageGRID** アプライアンスインストーラへのアクセス

インストーラのバージョンを確認し、アプライアンスと 3 つの StorageGRID ネットワーク（グリッドネットワーク、管理ネットワーク（オプション）、クライアントネットワーク（オプション））の間の接続を設定するには、 StorageGRID アプライアンスインストーラにアクセスする必要があります。

必要なもの

- StorageGRID 管理ネットワークに接続できる管理クライアントを使用しているか、サービスラップトップを使用している必要があります。
- クライアントまたはサービスラップトップに、サポートされている Web ブラウザをインストールしておきます。
- SG6000-CN コントローラは、使用するすべての StorageGRID ネットワークに接続されています。
- これらのネットワーク上の SG6000-CN コントローラの IP アドレス、ゲートウェイ、およびサブネットを確認しておきます。
- 使用するネットワークスイッチを設定しておきます。

このタスクについて

StorageGRID アプライアンスインストーラに最初にアクセスするには、 DHCP によって SG6000-CN コントローラの管理ネットワークポートに割り当てられた IP アドレスを使用するか（コントローラが管理ネットワークに接続されている場合）、サービスラップトップを SG6000-CN コントローラに直接接続します。

手順

1. 可能であれば、 SG6000-CN コントローラの管理ネットワークポートの DHCP アドレスを使用して StorageGRID アプライアンスインストーラにアクセスします。

a. SG6000-CN コントローラの前面にある MAC アドレスラベルを確認し、管理ネットワークポートの MAC アドレスを特定します。

   MAC アドレスラベルには、 BMC 管理ポートの MAC アドレスが記載されています。

   管理ネットワークポートの MAC アドレスを特定するには、ラベルに記載された 16 進数に * 2 * を追加する必要があります。たとえば、ラベルに記載されている MAC アドレスの末尾が * 09 * の場合、管理ポートの MAC アドレスの末尾は * 0B * となります。ラベルに記載された MAC アドレスの末尾が * （ *y* ） FF* の場合、管理ポートの MAC アドレスの末尾は * （ *y*+1 ） 01 * となります。この計算を簡単に行うには、 Windows で Calculator を開き、 Programmer モードに設定して Hex を選択し、 MAC アドレスを入力してから、 **+2=** と入力します。

b. MAC アドレスをネットワーク管理者に伝え、管理者が管理ネットワークでのアプライアンスの DHCP アドレスを確認できるようにします。

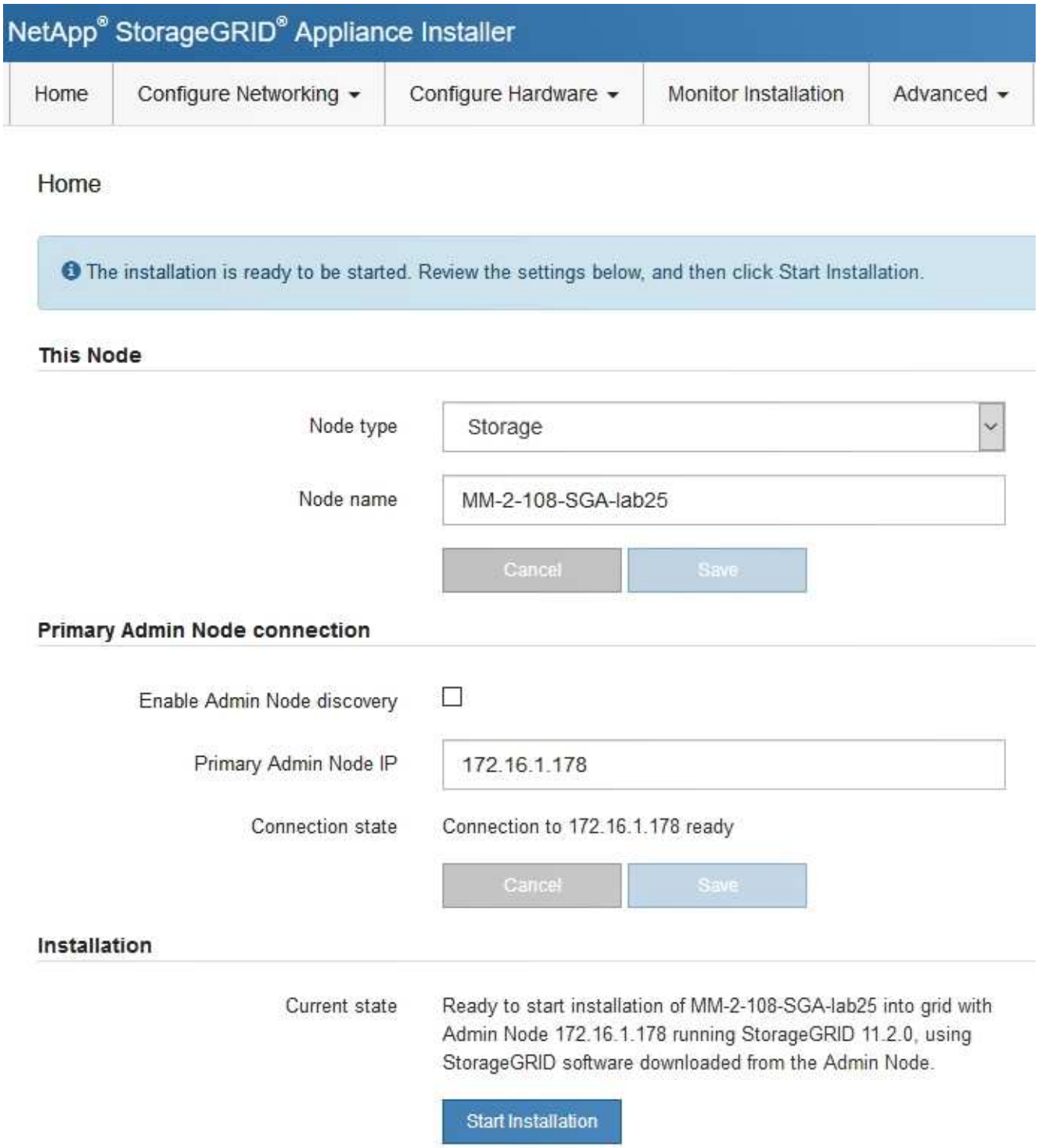
c. クライアントから、StorageGRID アプライアンスインストーラのURLとして「+」を入力します **`https://Appliance_Controller_IP:8443`**

   の場合 `*SG6000-CN_Controller_IP*`DHCPアドレスを使用してください。

d. セキュリティアラートが表示された場合は、ブラウザのインストールウィザードを使用して証明書を表示およびインストールします。

   次回この URL にアクセスしたときに、アラートは表示されません。

   StorageGRID アプライアンスインストーラのホームページが表示されます。このページに最初にアクセスしたときに表示される情報とメッセージは、アプライアンスと StorageGRID ネットワークの現在の接続状況によって異なります。エラーメッセージが表示された場合は、以降の手順で解決されます。




2. DHCP を使用して IP アドレスを取得できない場合は、リンクローカル接続を使用できます。

   a. イーサネットケーブルを使用して、サービスラップトップを SG6000-CN コントローラの右端の RJ-45 ポートに直接接続します。

   b. サービスラップトップで Web ブラウザを開きます。

c. StorageGRID アプライアンスインストーラのURLに+を入力します
**`https://169.254.0.1:8443`**

StorageGRID アプライアンスインストーラのホームページが表示されます。このページに最初にアクセスしたときに表示される情報とメッセージは、アプライアンスの現在の接続状況によって異なります。

リンクローカル接続でホームページにアクセスできない場合は、サービスラップトップのIPアドレスをに設定します `169.254.0.2`をクリックして、もう一度やり直してください。

完了後

StorageGRID アプライアンスインストーラにアクセスしたあとに、次の手順を実行

- アプライアンスの StorageGRID アプライアンスインストーラのバージョンが StorageGRID システムにインストールされているソフトウェアのバージョンと一致していることを確認します。必要に応じて、StorageGRID アプライアンスインストーラをアップグレードします。

  "StorageGRID アプライアンスインストーラのバージョンの確認とアップグレード"

- StorageGRID アプライアンスインストーラのホームページに表示されるメッセージを確認し、必要に応じてリンク設定と IP 設定を行います。

関連情報

"Web ブラウザの要件"

**StorageGRID** アプライアンスインストーラのバージョンの確認とアップグレード

# StorageGRID のすべての機能がサポートされるようにするには、アプライアンスの StorageGRID アプライアンスインストーラのバージョンと StorageGRID システムにインストールされているソフトウェアのバージョンが一致している必要があります。

必要なもの

StorageGRID アプライアンスインストーラにアクセスしておきます。

このタスクについて

StorageGRID アプライアンスは、 StorageGRID アプライアンスインストーラがプリインストールされた状態で出荷されます。最近アップグレードした StorageGRID システムにアプライアンスを追加する場合は、そのアプライアンスを新しいノードとしてインストールする前に、 StorageGRID アプライアンスインストーラの手動アップグレードが必要になることがあります。

新しい StorageGRID バージョンにアップグレードすると、 StorageGRID アプライアンスインストーラが自動的にアップグレードされます。インストールされているアプライアンスノードでは、 StorageGRID アプライアンスインストーラをアップグレードする必要はありません。この手順 が必要になるのは、以前のバージョンの StorageGRID アプライアンスインストーラを搭載したアプライアンスをインストールする場合のみです。

手順

1. StorageGRID アプライアンス・インストーラから、 * アドバンスト * > * アップグレード・ファームウェア * を選択します。

2. 現在のファームウェアバージョンとStorageGRID システムにインストールされているソフトウェアバージョンを比較します（Grid Managerから* Help > About *を選択します）。

   2 つのバージョンの 2 桁目の数字が一致している必要があります。たとえば、StorageGRID システムでバージョン11.* 5 。***x*.y_y__**を実行している場合、**StorageGRID** アプライアンスインストーラのバージョンは**3.** 5 *._z_にする必要があります。

3. アプライアンスに StorageGRID アプライアンスインストーラの下位バージョンがインストールされている場合は、 StorageGRID のネットアップのダウンロードページにアクセスします。

   "ネットアップのダウンロード： StorageGRID"

   ネットアップアカウントのユーザ名とパスワードを使用してサインインします。

4. StorageGRID アプライアンス * 対応するバージョンのサポート・ファイルと対応するチェックサム・ファイルをダウンロードします。

   StorageGRID アプライアンスファイルのサポートファイルは、です `.zip` すべてのStorageGRID アプライアンスモデルの最新および以前のファームウェアバージョンを、各コントローラタイプのサブディレクトリに格納してアーカイブする。

   StorageGRID アプライアンスファイルのサポートファイルをダウンロードしたら、を展開します `.zip` StorageGRID アプライアンスインストーラのインストールに関する重要な情報については、READMEファイルをアーカイブして参照してください。

5. StorageGRID アプライアンスインストーラのファームウェアのアップグレードページの手順に従って、次の手順を実行します。

   a. コントローラタイプとチェックサムファイルに適したサポートファイル（ファームウェアイメージ）をアップロードします。

   b. 非アクティブなパーティションをアップグレードします。

   c. パーティションを再起動してスワップします。

   d. 2番目のパーティションをアップグレードします。

関連情報

"StorageGRID アプライアンスインストーラへのアクセス"

ネットワークリンクの設定（**SG6000**）

# アプライアンスをグリッドネットワーク、クライアントネットワーク、および管理ネットワークに接続するために使用するポートのネットワークリンクを設定できます。リンク速度およびポートボンディングモードとネットワークボンディングモードを設定できます。

必要なもの

アプライアンスノードをクローニングする場合は、ソースアプライアンスノードで使用されるすべてのリンクについて、ターゲットアプライアンスのネットワークリンクを設定します。

25GbE のリンク速度を使用する場合は、次の要件があります。

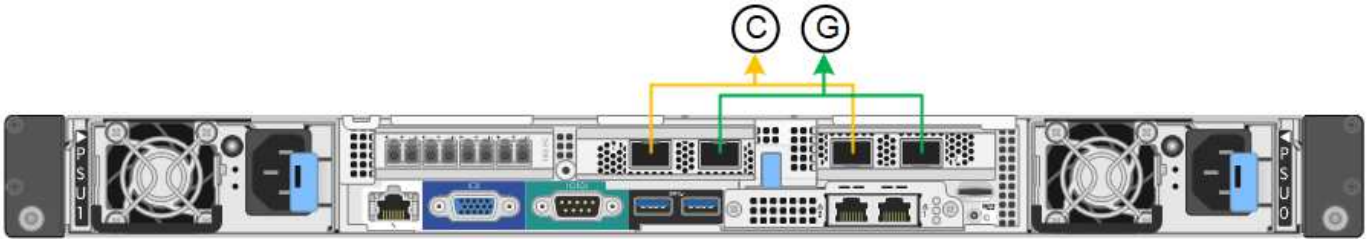
- SFP28 TwinAx ケーブルを使用するか、使用するネットワークポートに SFP28 トランシーバを取り付けておきます。
- この速度をサポートするスイッチにネットワークポートを接続しておきます。
- この速度を使用するようにスイッチを設定する方法を理解しておきます。

アグリゲートポートボンディングモード、 LACP ネットワークボンディングモード、または VLAN タギングを使用する場合

- アプライアンスのネットワークポートを、 VLAN と LACP をサポートするスイッチに接続しておきます。
- 複数のスイッチを LACP ボンドに加える場合は、 Multi-Chassis Link Aggregation （ MLAG ）グループまたは同等の機能をサポートするスイッチを使用します。
- VLAN 、 LACP 、 MLAG などを使用するようにスイッチを設定する方法について理解しておく必要があります。
- 各ネットワークに使用する一意の VLAN タグを確認しておきます。この VLAN タグが各ネットワークパケットに追加され、ネットワークトラフィックが正しいネットワークにルーティングされます。

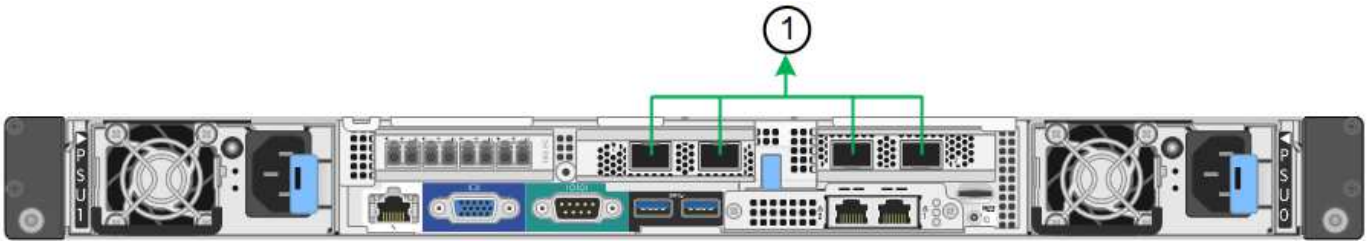
このタスクについて

次の図では、 4 つのネットワークポートが Fixed ポートボンディングモードでボンディングされています（デフォルトの構成）。




| | ボンディングされるポート |
|---|---|
| C | このネットワークを使用する場合、ポート 1 とポート 3 がクライアントネットワーク用にボンディングされます。 |
| G | ポート 2 とポート 4 がグリッドネットワーク用にボンディングされます。 |

次の図では、 4 つのネットワークポートが Aggregate ポートボンディングモードでボンディングされています。



| | ボンディングされるポート |
|---|---|
| 1. | 4 つのポートすべてを 1 つの LACP ボンドにグループ化して、すべてのポートをグリッドネットワークとクライアントネットワークのトラフィックに使用できるようにします。 |

次の表に、 4 つのネットワークポートを設定するためのオプションをまとめます。デフォルトの設定は太字で示しています。デフォルト以外の設定を使用する場合にのみ、 Link Configuration ページで設定を行う必要があります。

- * 固定（デフォルト）ポートボンディングモード *

| ネットワークボンディングモード | クライアントネットワークが無効な場合（デフォルト） | クライアントネットワークが有効になりました |
|---|---|---|
| アクティブ/バックアップ（デフォルト） | • ポート 2 と 4 がグリッドネットワークにアクティブ / バックアップボンドを使用します。<br>• ポート 1 と 3 は使用されません。<br>• VLAN タグはオプションです。 | • ポート 2 と 4 がグリッドネットワークにアクティブ / バックアップボンドを使用します。<br>• ポート 1 と 3 がクライアントネットワークに Active-Backup ボンドを使用します。<br>• ネットワーク管理者用に、両方のネットワークに VLAN タグを指定できます。 |
| LACP （ 802.3ad ） | • ポート 2 と 4 がグリッドネットワークに LACP ボンドを使用します。<br>• ポート 1 と 3 は使用されません。<br>• VLAN タグはオプションです。 | • ポート 2 と 4 がグリッドネットワークに LACP ボンドを使用します。<br>• ポート 1 と 3 がクライアントネットワークに LACP ボンドを使用します。<br>• ネットワーク管理者用に、両方のネットワークに VLAN タグを指定できます。 |

- * アグリゲートポートボンディングモード *

| ネットワークボンディングモード | クライアントネットワークが無効な場合（デフォルト） | クライアントネットワークが有効になりました |
|---|---|---|
| LACP （ 802.3ad ）のみ | • ポート 1~4 がグリッドネットワークに単一の LACP ボンドを使用します。<br>• 単一の VLAN タグでグリッドネットワークのパケットが識別されます。 | • ポート 1~4 がグリッドネットワークとクライアントネットワークに単一の LACP ボンドを使用します。<br>• 2 つの VLAN タグで、グリッドネットワークのパケットとクライアントネットワークのパケットを分離できます。 |

ポートボンディングモードとネットワークボンディングモードの詳細については、「SG6000-CNコントローラのネットワークポート接続」を参照してください。

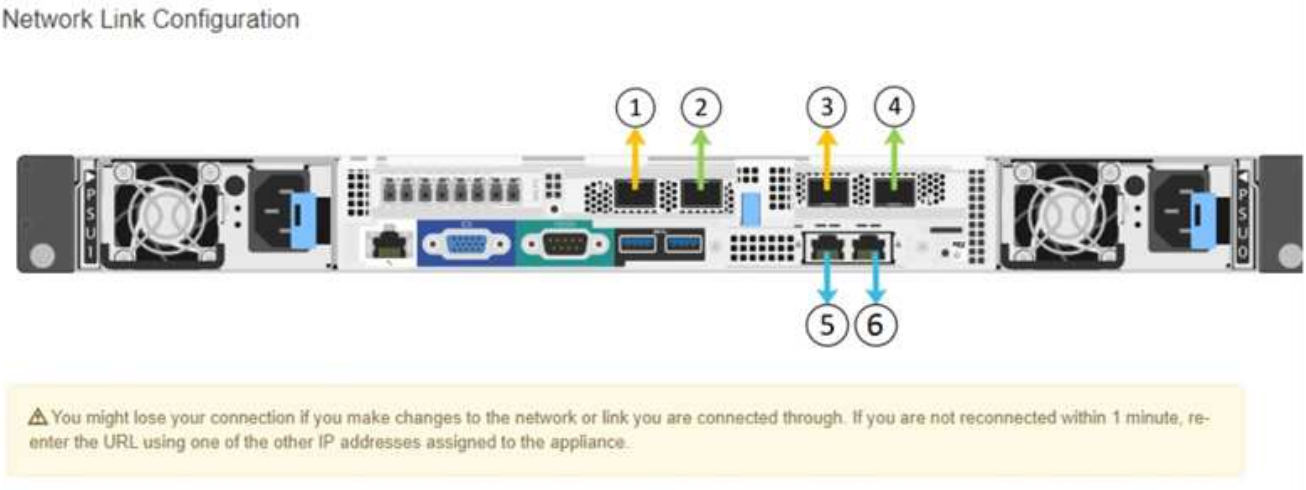
次の図では、 SG6000-CN コントローラの 2 つの 1GbE 管理ポートが管理ネットワーク用に Active-Backup

ネットワークボンディングモードでボンディングされています。

手順

1. StorageGRID アプライアンスインストーラから、 **Configure Networking *>*Link Configuration** をクリックします。

   Network Link Configuration ページには、アプライアンスの図と、ネットワークポートおよび管理ポートの番号が表示されます。




   Link Status テーブルには、番号が付けられたポートのリンクステート（アップ / ダウン）と速度（ 1/10/25 / 40/100Gbps ）が表示されます。

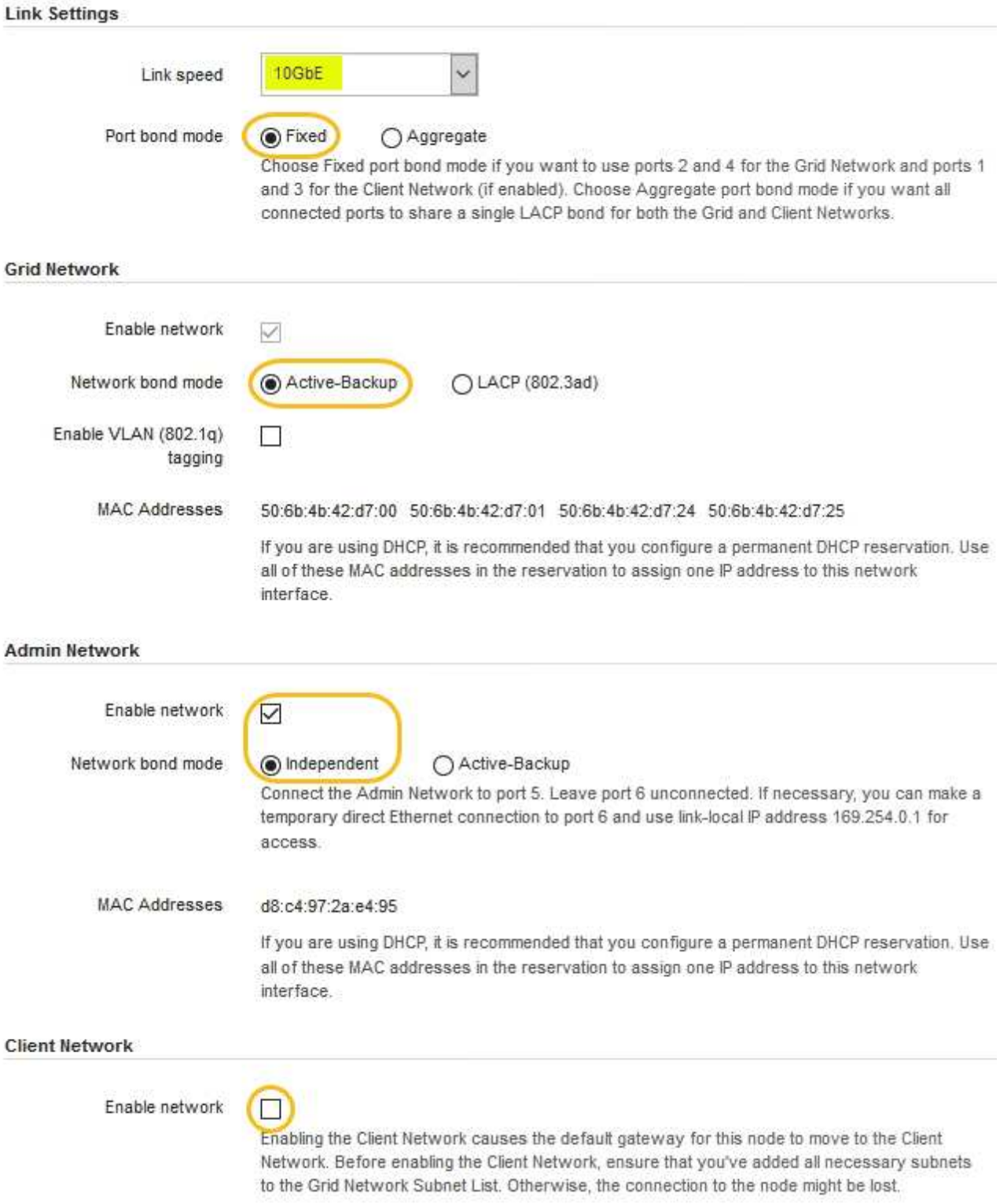
**Link Status**

| Link | State | Speed (Gbps) |
|---|---|---|
| 1 | Up | 10 |
| 2 | Up | 10 |
| 3 | Down | N/A |
| 4 | Down | N/A |
| 5 | Up | 1 |
| 6 | Up | 1 |

   このページに初めてアクセスしたときの動作は次のとおりです。

   ◦ * リンク速度 * は * 10GbE * に設定されています。

- * ポートボンディングモード * は「 * Fixed 」に設定されます。
- * グリッドネットワークの場合、ネットワークボンディングモード * が「アクティブ / バックアップ」に設定されます。
- 管理ネットワーク * が有効になっており、ネットワークボンディングモードが * Independent * に設定されています。
- クライアントネットワーク * が無効になっています。



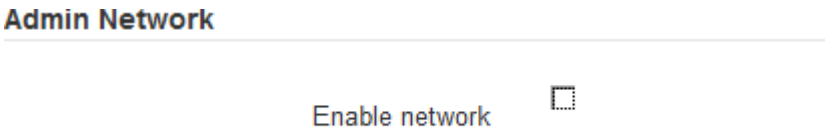
2. ネットワークポートに25GbEのリンク速度を使用する場合は、Link speed（リンク速度）ドロップダウンリストから* 25GbE *を選択します。

   グリッドネットワークとクライアントネットワークに使用するネットワークスイッチも、この速度をサポートし、この速度に対応するように設定する必要があります。また、 SFP28 TwinAx ケーブル、または光ケーブルと SFP28 トランシーバを使用する必要があります。

3. 使用する StorageGRID ネットワークを有効または無効にします。

   グリッドネットワークは必須です。このネットワークは無効にできません。

   a. アプライアンスが管理ネットワークに接続されていない場合は、管理ネットワークの * ネットワークを有効にする * チェックボックスの選択を解除します。

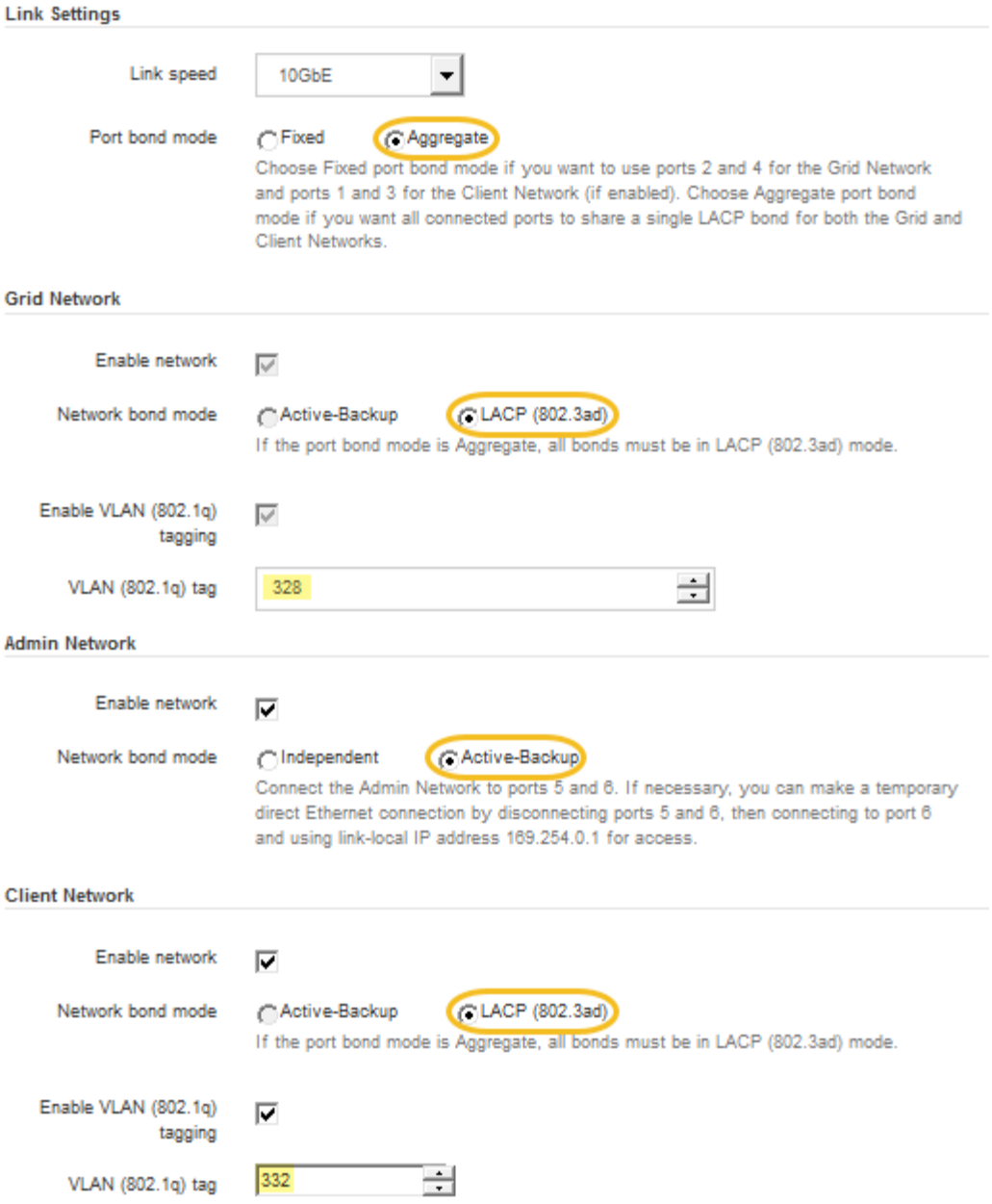
   b. アプライアンスがクライアントネットワークに接続されている場合は、クライアントネットワークの * ネットワークを有効にする * チェックボックスをオンにします。

      これで、ネットワークポートでのクライアントネットワークの設定が表示されます。

4. 表を参照して、ポートボンディングモードとネットワークボンディングモードを設定します。

   次の例では、次のよう

   - * グリッドネットワークとクライアントネットワークでアグリゲート * と * LACP * が選択されました。各ネットワークに一意の VLAN タグを指定する必要があります。値は 0~4095 の間で選択できます。
   - * 管理ネットワーク用に選択されたアクティブ / バックアップ * 。




5. 選択に問題がなければ、 * 保存 * をクリックします。

> 接続しているネットワークまたはリンクを変更すると、接続が失われる可能性があります。1分以内に再接続されない場合は、アプライアンスに割り当てられている他のIPアドレスのいずれかを使用してStorageGRID アプライアンスインストーラのURLを再入力します：+
> **`https://SG6000-CN_Controller_IP:8443`**

関連情報

"SG6000-CNコントローラのポートボンディングモード"

"StorageGRID IPアドレスを設定しています"

# StorageGRID アプライアンスインストーラを使用して、 StorageGRID のグリッドネットワーク、管理ネットワーク、クライアントネットワークでアプライアンスストレージノードに使用される IP アドレスとルーティング情報を設定します。

このタスクについて

接続された各ネットワークでアプライアンスの静的 IP を割り当てるか、 DHCP サーバでアドレスの永久リースを割り当てる必要があります。

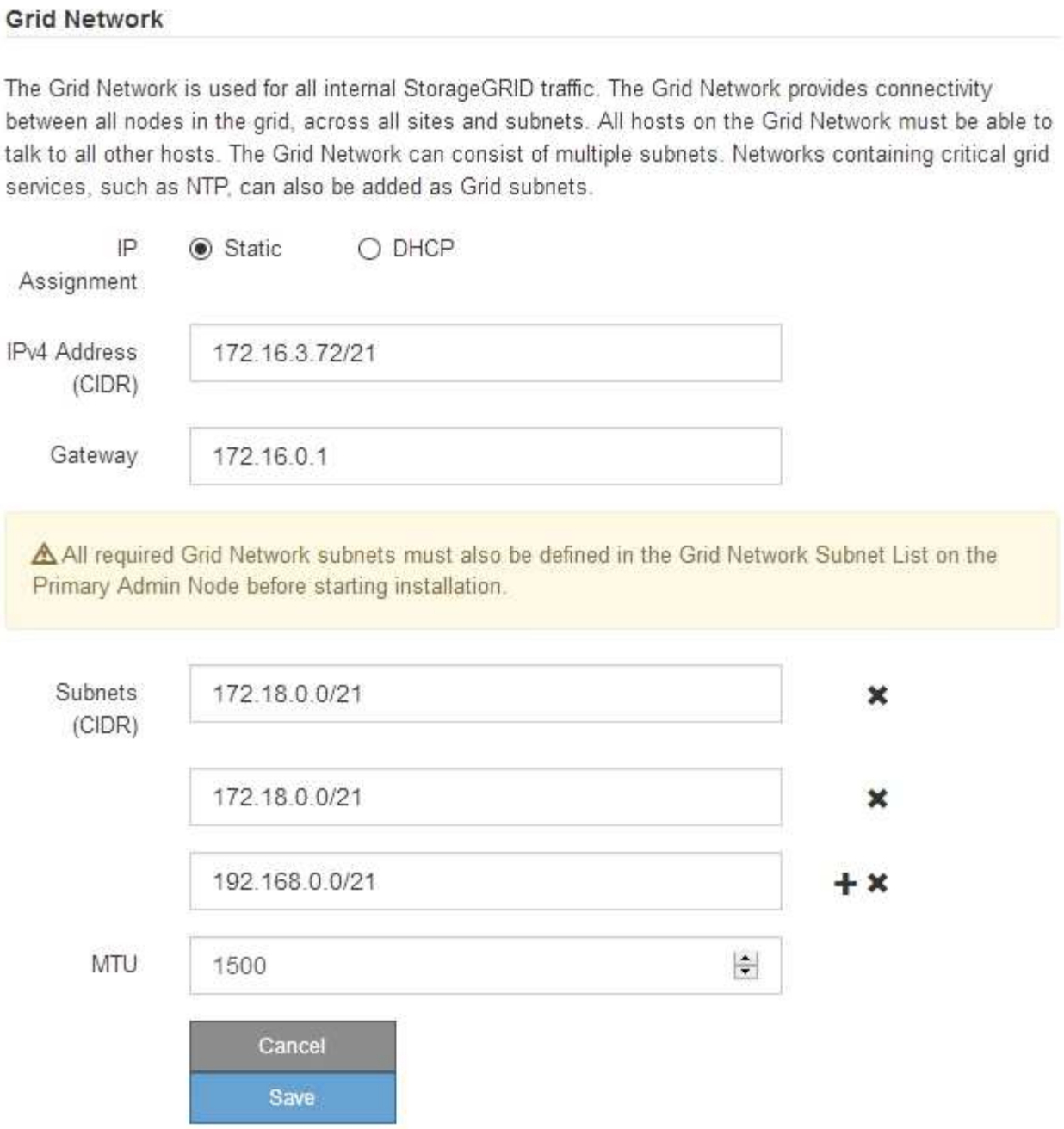
リンク設定を変更する場合は、SG6000-CNコントローラのリンク設定を変更する手順を参照してください。

手順

1. StorageGRID アプライアンスインストーラで、 * ネットワークの設定 * > * IP 構成 * を選択します。

   [IP Configuration] ページが表示されます。

2. グリッドネットワークを設定するには、ページの * グリッドネットワーク * セクションで * 静的 * または * DHCP * のいずれかを選択します。




3. 「 * Static * 」を選択した場合は、次の手順に従ってグリッドネットワークを設定します。
   a. CIDR 表記を使用して静的 IPv4 アドレスを入力します。
   b. ゲートウェイを入力します。

      ネットワークにゲートウェイがない場合は、同じ静的 IPv4 アドレスを再入力します。

   c. ジャンボフレームを使用する場合は、 MTU フィールドを 9000 などのジャンボフレームに適した値に変更します。それ以外の場合は、デフォルト値 1500 のままにします。

      ネットワークの MTU 値は、ノードが接続されているスイッチポートに設定されている値と同じである必要があります。そうしないと、ネットワークパフォーマンスの問題やパケット損失が発生する可能性があります。

ネットワークのパフォーマンスを最大限に高めるには、すべてのノードのグリッドネットワークインターフェイスで MTU 値がほぼ同じになるように設定する必要があります。個々のノードのグリッドネットワークの MTU 設定に大きな違いがある場合は、 * Grid Network MTU mismatch * アラートがトリガーされます。MTU 値はすべてのネットワークタイプで同じである必要はありません。

d. [ 保存（ Save ） ] をクリックします。

IP アドレスを変更すると、ゲートウェイとサブネットのリストも変更される可能性があります。

StorageGRID アプライアンスインストーラへの接続が失われた場合は、割り当てた新しい静的 IP アドレスを使用して URL を再入力します。たとえば、「+」と入力します
`https://services_appliance_IP:8443`

e. グリッドネットワークのサブネットのリストが正しいことを確認します。

グリッドサブネットがある場合は、グリッドネットワークゲートウェイが必要です。指定するすべてのグリッドサブネットが、このゲートウェイ経由でアクセス可能であることが必要です。StorageGRID のインストールを開始するときに、プライマリ管理ノードのグリッドネットワークサブネットリストでこれらのサブネットも定義する必要があります。

デフォルトルートはリストされません。クライアントネットワークが有効になっていない場合は、デフォルトルートがグリッドネットワークゲートウェイを使用します。

- サブネットを追加するには、挿入アイコンをクリックします ➕ アイコン"] をクリックします。
- 使用されていないサブネットを削除するには、削除アイコンをクリックします ✖。

f. [ 保存（ Save ） ] をクリックします。

4. 「 * DHCP * 」を選択した場合は、次の手順に従ってグリッドネットワークを設定します。

a. [**DHCP**] ラジオボタンを選択した後、 [**Save**] をクリックします。

[* IPv4 アドレス * ] 、 [ * ゲートウェイ * ] 、および [ * サブネット * ] フィールドには、自動的に値が入力されます。DHCP サーバが MTU 値を割り当てるように設定されている場合は、 **MTU** フィールドにその値が入力され、フィールドは読み取り専用になります。

Web ブラウザは、 StorageGRID アプライアンスインストーラの新しい IP アドレスに自動的にリダイレクトされます。

b. グリッドネットワークのサブネットのリストが正しいことを確認します。

グリッドサブネットがある場合は、グリッドネットワークゲートウェイが必要です。指定するすべてのグリッドサブネットが、このゲートウェイ経由でアクセス可能であることが必要です。StorageGRID のインストールを開始するときに、プライマリ管理ノードのグリッドネットワークサブネットリストでこれらのサブネットも定義する必要があります。

デフォルトルートはリストされません。クライアントネットワークが有効になっていない場合は、デフォルトルートがグリッドネットワークゲートウェイを使用します。

- サブネットを追加するには、挿入アイコンをクリックします ➕ アイコン"] をクリックします。

- 使用されていないサブネットを削除するには、削除アイコンをクリックします ✖。

c. ジャンボフレームを使用する場合は、 MTU フィールドを 9000 などのジャンボフレームに適した値に変更します。それ以外の場合は、デフォルト値 1500 のままにします。

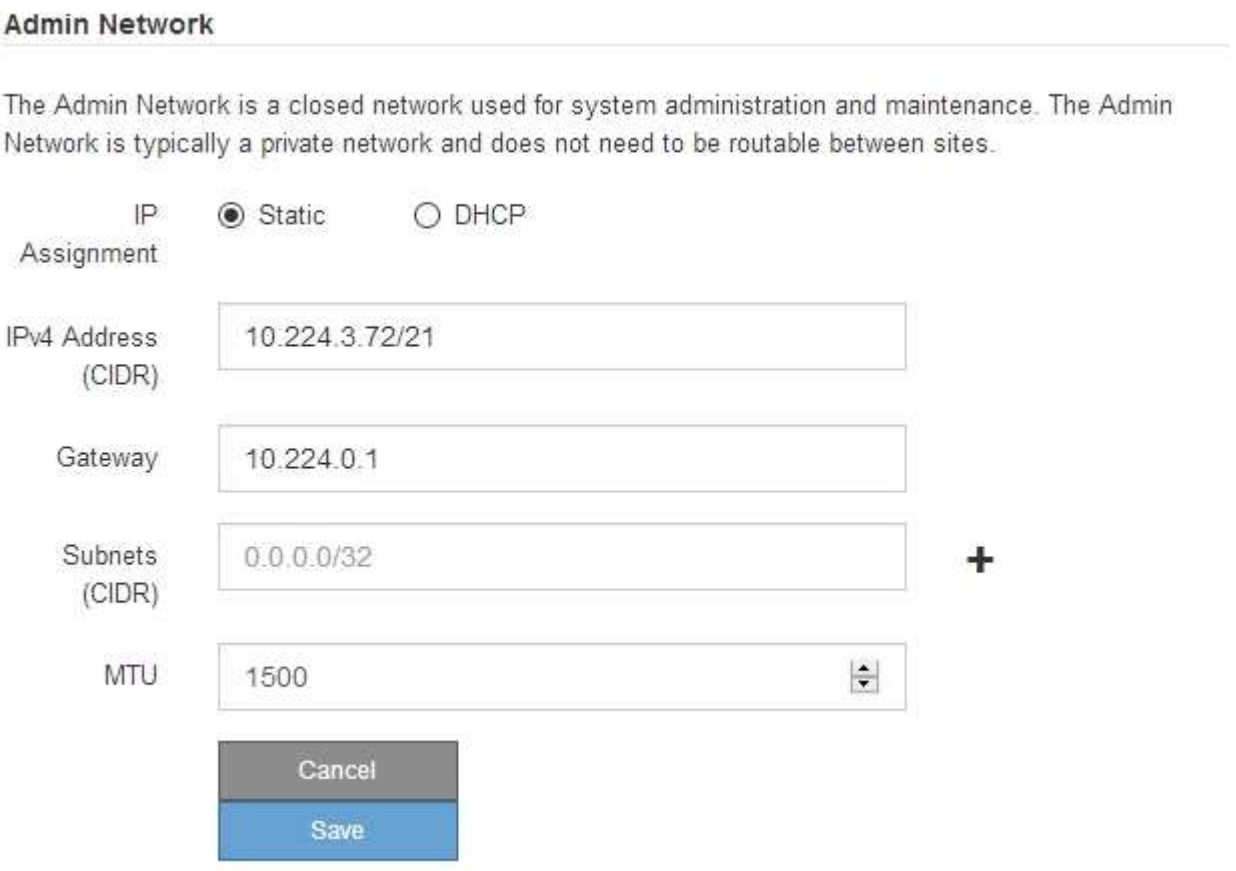
ネットワークの MTU 値は、ノードが接続されているスイッチポートに設定されている値と同じである必要があります。そうしないと、ネットワークパフォーマンスの問題やパケット損失が発生する可能性があります。

ネットワークのパフォーマンスを最大限に高めるには、すべてのノードのグリッドネットワークインターフェイスで MTU 値がほぼ同じになるように設定する必要があります。個々のノードのグリッドネットワークの MTU 設定に大きな違いがある場合は、 * Grid Network MTU mismatch * アラートがトリガーされます。MTU 値はすべてのネットワークタイプで同じである必要はありません。

a. [ 保存（ Save ） ] をクリックします。

5. 管理ネットワークを設定するには、ページの * 管理ネットワーク * セクションで * 静的 * または * DHCP * のいずれかを選択します。

管理ネットワークを設定するには、 Link Configuration ページで管理ネットワークを有効にする必要があります。




6. 「 * Static * 」を選択した場合は、次の手順に従って管理ネットワークを設定します。

a. アプライアンスの管理ポート 1 に対して、 CIDR 表記を使用して静的 IPv4 アドレスを入力します。

管理ポート 1 は、アプライアンス右端にある 2 つの 1GbE RJ45 ポートのうち、左側のポートです。

b. ゲートウェイを入力します。

ネットワークにゲートウェイがない場合は、同じ静的 IPv4 アドレスを再入力します。

c. ジャンボフレームを使用する場合は、 MTU フィールドを 9000 などのジャンボフレームに適した値に変更します。それ以外の場合は、デフォルト値 1500 のままにします。

ネットワークの MTU 値は、ノードが接続されているスイッチポートに設定されている値と同じである必要があります。そうしないと、ネットワークパフォーマンスの問題やパケット損失が発生する可能性があります。

d. [ 保存（ Save ） ] をクリックします。

IP アドレスを変更すると、ゲートウェイとサブネットのリストも変更される可能性があります。

StorageGRID アプライアンスインストーラへの接続が失われた場合は、割り当てた新しい静的 IP アドレスを使用して URL を再入力します。たとえば、「+」と入力します
**`https://services_appliance:8443`**

e. 管理ネットワークのサブネットのリストが正しいことを確認します。

指定したゲートウェイを使用してすべてのサブネットにアクセスできることを確認する必要があります。

管理ネットワークゲートウェイを使用するデフォルトルートは作成できません。

- サブネットを追加するには、挿入アイコンをクリックします ➕ アイコン"] をクリックします。
- 使用されていないサブネットを削除するには、削除アイコンをクリックします ✖。

f. [ 保存（ Save ） ] をクリックします。

7. [**DHCP**] を選択した場合は、次の手順に従って管理ネットワークを設定します。

a. [**DHCP**] ラジオボタンを選択した後、 [**Save**] をクリックします。

[* IPv4 アドレス * ] 、 [ * ゲートウェイ * ] 、および [ * サブネット * ] フィールドには、自動的に値が入力されます。DHCP サーバが MTU 値を割り当てるように設定されている場合は、 **MTU** フィールドにその値が入力され、フィールドは読み取り専用になります。

Web ブラウザは、 StorageGRID アプライアンスインストーラの新しい IP アドレスに自動的にリダイレクトされます。

b. 管理ネットワークのサブネットのリストが正しいことを確認します。

指定したゲートウェイを使用してすべてのサブネットにアクセスできることを確認する必要があります。

管理ネットワークゲートウェイを使用するデフォルトルートは作成できません。

- サブネットを追加するには、挿入アイコンをクリックします ➕ アイコン"] をクリックします。

- 使用されていないサブネットを削除するには、削除アイコンをクリックします ✖。

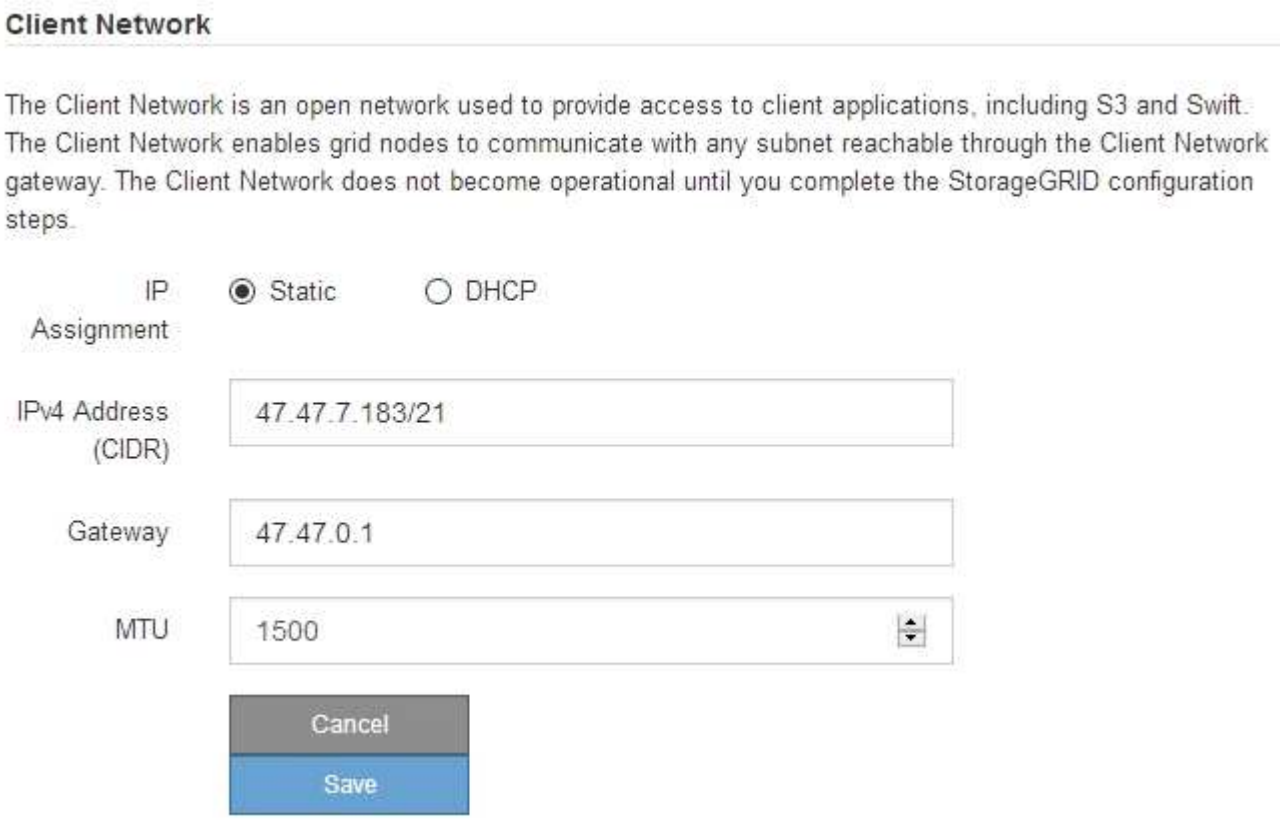
c. ジャンボフレームを使用する場合は、 MTU フィールドを 9000 などのジャンボフレームに適した値に変更します。それ以外の場合は、デフォルト値 1500 のままにします。

> ネットワークの MTU 値は、ノードが接続されているスイッチポートに設定されている値と同じである必要があります。そうしないと、ネットワークパフォーマンスの問題やパケット損失が発生する可能性があります。

d. [ 保存（ Save ） ] をクリックします。

8. クライアントネットワークを設定するには、ページの * クライアントネットワーク * セクションで * 静的 * または * DHCP * のいずれかを選択します。

> クライアントネットワークを設定するには、 Link Configuration ページで Client Network を有効にする必要があります。




9. * Static * を選択した場合は、次の手順に従ってクライアントネットワークを設定します。

a. CIDR 表記を使用して静的 IPv4 アドレスを入力します。

b. [ 保存（ Save ） ] をクリックします。

c. クライアントネットワークゲートウェイの IP アドレスが正しいことを確認します。

> クライアントネットワークが有効になっている場合は、デフォルトルートが表示されます。デフォルトルートはクライアントネットワークゲートウェイを使用し、クライアントネットワークが有効になっている間は別のインターフェイスに移動できません。

d. ジャンボフレームを使用する場合は、 MTU フィールドを 9000 などのジャンボフレームに適した値に変更します。それ以外の場合は、デフォルト値 1500 のままにします。

> ネットワークの MTU 値は、ノードが接続されているスイッチポートに設定されている値と同じである必要があります。そうしないと、ネットワークパフォーマンスの問題やパケット損失が発生する可能性があります。

e. [ 保存（ Save ） ] をクリックします。

10. [**DHCP**] を選択した場合は、次の手順に従ってクライアントネットワークを設定します。

a. [**DHCP**] ラジオボタンを選択した後、 [**Save**] をクリックします。

[**IPv4 Address**] フィールドと [**Gateway**] フィールドが自動的に入力されます。DHCP サーバが MTU 値を割り当てるように設定されている場合は、 **MTU** フィールドにその値が入力され、フィールドは読み取り専用になります。

Web ブラウザは、 StorageGRID アプライアンスインストーラの新しい IP アドレスに自動的にリダイレクトされます。

a. ゲートウェイが正しいことを確認します。

> クライアントネットワークが有効になっている場合は、デフォルトルートが表示されます。デフォルトルートはクライアントネットワークゲートウェイを使用し、クライアントネットワークが有効になっている間は別のインターフェイスに移動できません。

b. ジャンボフレームを使用する場合は、 MTU フィールドを 9000 などのジャンボフレームに適した値に変更します。それ以外の場合は、デフォルト値 1500 のままにします。

> ネットワークの MTU 値は、ノードが接続されているスイッチポートに設定されている値と同じである必要があります。そうしないと、ネットワークパフォーマンスの問題やパケット損失が発生する可能性があります。

関連情報

"SG6000-CNコントローラのリンク設定を変更する"

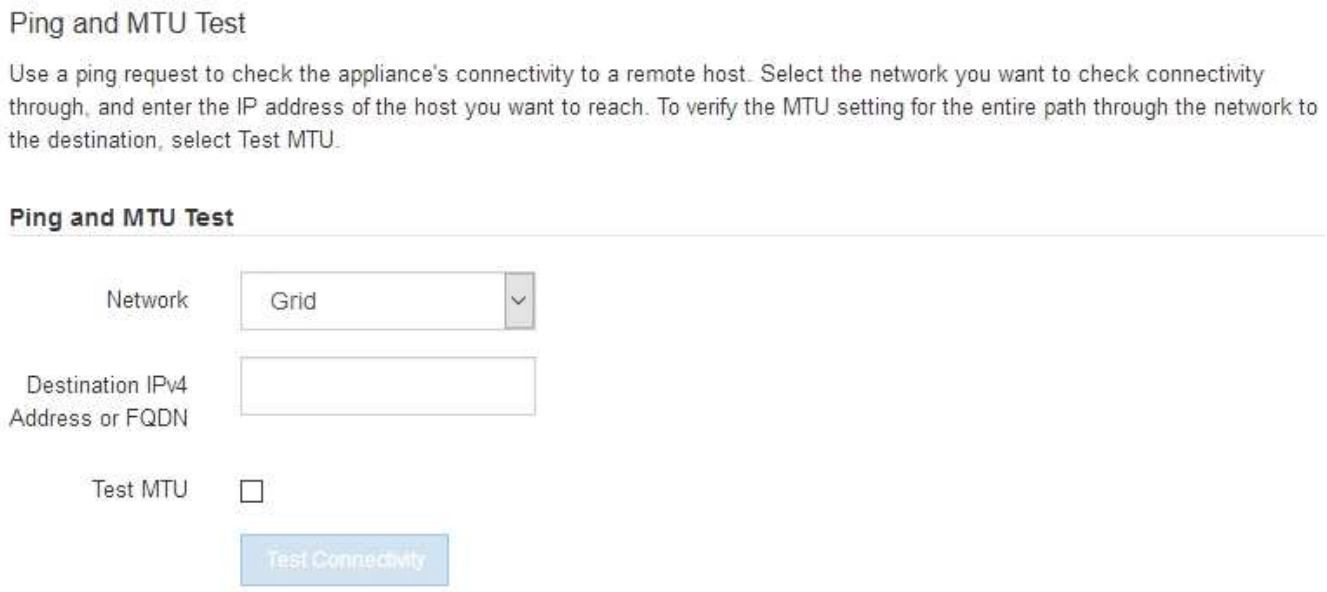
ネットワーク接続の確認

使用する StorageGRID ネットワークに、アプライアンスからアクセスできることを確認する必要があります。ネットワークゲートウェイ経由のルーティングを検証するには、StorageGRID アプライアンスインストーラと異なるサブネット上の IP アドレスとの接続をテストする必要があります。MTU 設定を確認することもできます。

手順

1. StorageGRID アプライアンスインストーラのメニューバーから、 *Configure Networking *>*Ping and MTU Test * をクリックします。

[Ping and MTU Test] ページが表示されます。




2. [* ネットワーク *] ドロップダウンボックスから、テストするネットワークを選択します。グリッド、管理、またはクライアント。
3. そのネットワーク上のホストの IPv4 アドレスまたは完全修飾ドメイン名（ FQDN ）を入力します。

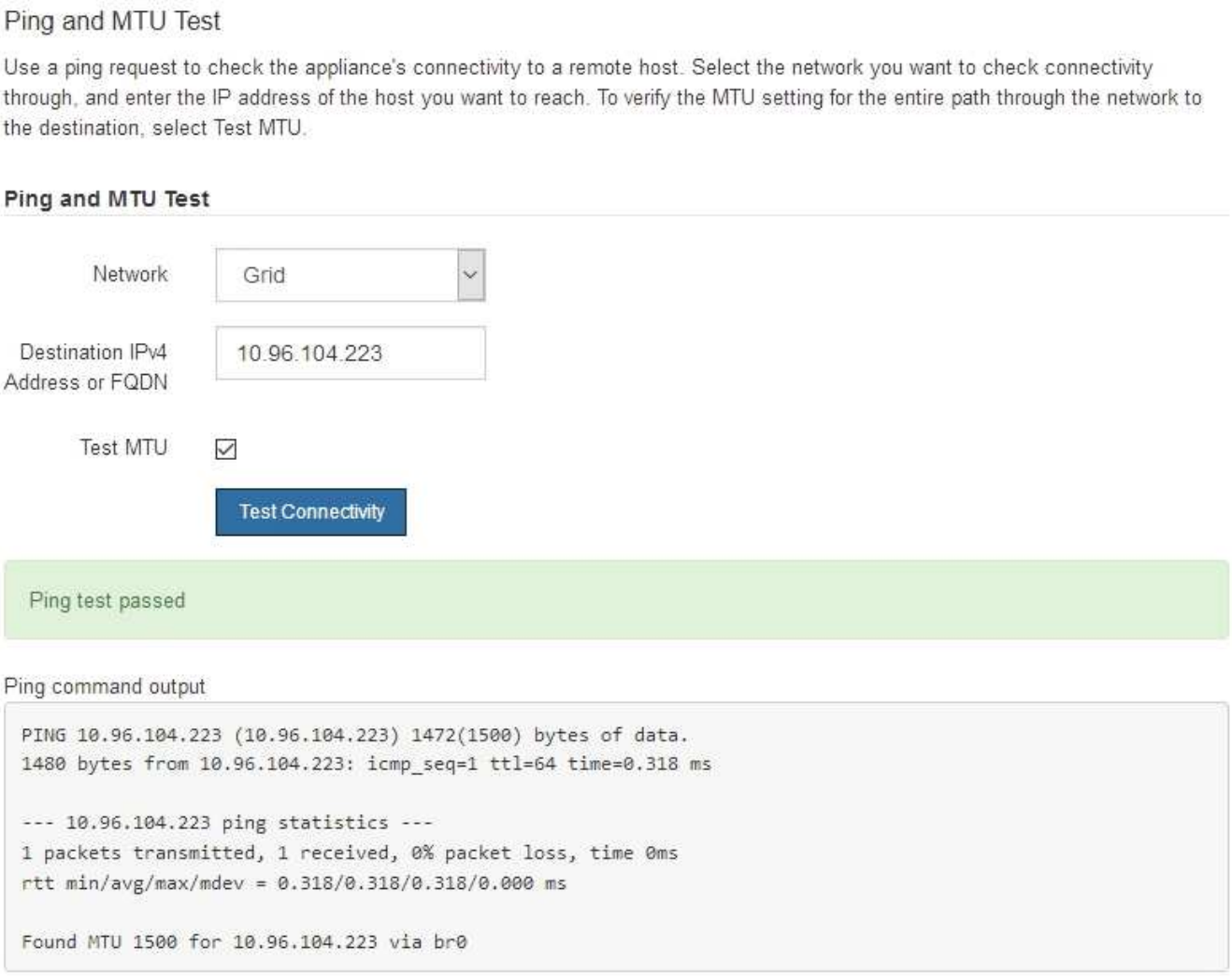
   たとえば、ネットワーク上のゲートウェイやプライマリ管理ノードに ping を送信できます。

4. 必要に応じて、 * Test MTU * チェックボックスをオンにして、ネットワーク経由でデスティネーションへのパス全体の MTU 設定を確認します。

   たとえば、アプライアンスノードと別のサイトのノードの間のパスをテストできます。

5. [ 接続のテスト * ] をクリックします。

   ネットワーク接続が有効な場合は、「 Ping test passed 」メッセージと ping コマンドの出力が表示されます。




関連情報

"ネットワークリンクの設定（SG6000）"

"MTU設定を変更します"

ポートレベルのネットワーク接続の確認

## StorageGRID アプライアンスインストーラとその他のノードの間のアクセスがファイアウォールの妨げにならないように、 StorageGRID アプライアンスインストーラが指定した IP アドレスまたはアドレス範囲にある特定の TCP ポートまたはポートセットに接続できることを確認します。

このタスクについて

StorageGRID アプライアンスインストーラに付属のポートのリストを使用して、アプライアンスとグリッドネットワーク内の他のノードの間の接続をテストできます。

また、外部 NFS サーバや DNS サーバで使用されるポートなど、管理ネットワークとクライアントネットワーク、および UDP ポートで接続をテストすることもできます。これらのポートの一覧については、StorageGRID ネットワークのガイドラインにあるポートリファレンスを参照してください。

ポート接続テーブルに表示されているグリッドネットワークポートは、StorageGRID バージョン11.5.0に対してのみ有効です。各ノードタイプに適したポートを確認するには、使用している StorageGRID のバージョンに対応したネットワークガイドラインを確認する必要があります。

手順

1. StorageGRID アプライアンスインストーラから、 **Configure Networking *>** Port Connectivity Test (nmap)* をクリックします。

   Port Connectivity Test ページが表示されます。

   ポート接続テーブルには、グリッドネットワークでの TCP 接続を必要とするノードタイプが表示されます。各ノードタイプについて、アプライアンスにアクセスできる必要があるグリッドネットワークのポートがテーブルに表示されます。

   The following node types require TCP connectivity on the Grid Network.

| Node Type | Grid Network Ports |
|---|---|
| Admin Node | 22,80,443,1504,1505,1506,1508,7443,9999 |
| Storage Node without ADC | 22,1139,1502,1506,1511,7001,9042,9999,18002,18017,18019,18082,18083,18200 |
| Storage Node with ADC | 22,1139,1501,1502,1506,1511,7001,9042,9999,18000,18001,18002,18003,18017,18019,18082,18083,18200,19000 |
| API Gateway | 22,1506,1507,9999 |
| Archive Node | 22,1506,1509,9999,11139 |

   表に記載されたアプライアンスポートとグリッドネットワーク内のその他のノードの間の接続をテストできます。

2. [* ネットワーク *] ドロップダウンから、テストするネットワークを選択します。 * グリッド * 、 * 管理者 * 、または * クライアント * 。
3. そのネットワーク上のホストの IPv4 アドレスの範囲を指定します。

   たとえば、ネットワーク上のゲートウェイやプライマリ管理ノードをプローブできます。

   次の例に示すように、ハイフンを使用して範囲を指定します。

4. TCP ポート番号、カンマで区切ったポートのリスト、またはポートの範囲を入力します。

The following node types require TCP connectivity on the Grid Network.

| Node Type | Grid Network Ports |
| --- | --- |
| Admin Node | 22,80,443,1504,1505,1506,1508,7443,9999 |
| Storage Node without ADC | 22,1139,1502,1506,1511,7001,9042,9999,18002,18017,18019,18082,18083,18200 |
| Storage Node with ADC | 22,1139,1501,1502,1506,1511,7001,9042,9999,18000,18001,18002,18003,18017,18019,18082,18083,18200,19000 |
| API Gateway | 22,1506,1507,9999 |
| Archive Node | 22,1506,1509,9999,11139 |

**Port Connectivity Test**

Network: Grid

IPv4 Address Ranges: 10.224.6.160-161

Port Ranges: 22,2022

Protocol: TCP UDP

Test Connectivity

5. [ 接続のテスト * ] をクリックします。

   ◦ 選択したポートレベルのネットワーク接続が有効な場合は、「 Port connectivity test passed 」というメッセージが緑色のバナーに表示されます。nmap コマンドの出力は、バナーの下に表示されます。

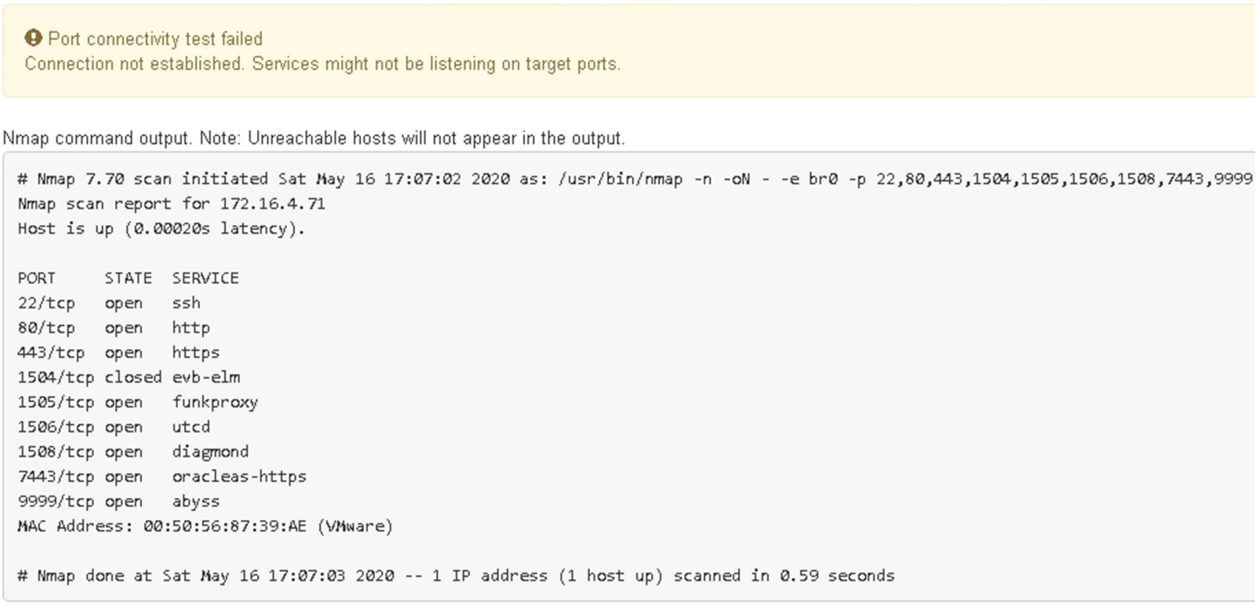
   Port connectivity test passed

   Nmap command output. Note: Unreachable hosts will not appear in the output.

```
# Nmap 7.70 scan initiated Fri Nov 13 18:32:03 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,2022 10.224.6.160-161
Nmap scan report for 10.224.6.160
Host is up (0.00072s latency).

PORT     STATE SERVICE
22/tcp   open  ssh
2022/tcp open  down

Nmap scan report for 10.224.6.161
Host is up (0.00060s latency).

PORT     STATE SERVICE
22/tcp   open  ssh
2022/tcp open  down

# Nmap done at Fri Nov 13 18:32:04 2020 -- 2 IP addresses (2 hosts up) scanned in 0.55 seconds
```

   ◦ ポートレベルのネットワーク接続がリモートホストに確立されても ' ホストが選択したポートの 1 つ以上をリッスンしていない場合は ' ポート接続テストに失敗しましたというメッセージが黄色のバナーに表示されますnmap コマンドの出力は、バナーの下に表示されます。

   ホストがリッスンしていないリモート・ポートの状態はすべて「 closed 」です。 たとえば、接続しようとしているノードがインストール済みの状態で、 StorageGRID NMS サービスがまだ実行されていない場合に、黄色のバナーが表示されることがあります。




- 選択した 1 つ以上のポートに対してポートレベルのネットワーク接続を確立できない場合は、「 Port connectivity test failed 」というメッセージが赤いバナーに表示されます。nmap コマンドの出力は、バナーの下に表示されます。

  赤いバナーは、リモートホストのポートへの TCP 接続試行が行われたが、送信者には何も返されなかったことを示します。応答が返されない場合、ポートの状態は「 filtered 」となり、ファイアウォールによってブロックされている可能性があります。

  「閉」のポートも一覧表示されます。

関連情報

"ネットワークガイドライン"

## SANtricity システムマネージャにアクセスして設定します

SANtricity System Manager を使用して、ストレージコントローラシェルフのストレージコントローラ、ストレージディスク、その他のハードウェアコンポーネントのステータスを監視できます。E シリーズ AutoSupport のプロキシを設定することもできます。管理ポートを使用せずにアプライアンスから AutoSupport メッセージを送信できます。

手順

- "『Setting Up and Accessing SANtricity System Manager』を参照してください"
- "SANtricity システムマネージャでハードウェアステータスを確認します"
- "StorageGRID アプライアンスインストーラを使用してストレージコントローラのIPアドレスを設定します"

### 『Setting Up and Accessing SANtricity System Manager』を参照してください

ストレージコントローラシェルフのハードウェアを監視したり、 E シリーズ AutoSupport を設定したりするために、ストレージコントローラの SANtricity System Manager へのアクセスが必要になる場合があります。

必要なもの

- サポートされているWebブラウザを使用します。
- グリッドマネージャから SANtricity システムマネージャにアクセスするには、 StorageGRID をインストールし、ストレージアプライアンスの管理者権限またはルートアクセス権限が必要です。
- StorageGRID アプライアンスインストーラを使用して SANtricity System Manager にアクセスするには、 SANtricity System Manager 管理者のユーザ名とパスワードが必要です。
- Web ブラウザを使用して SANtricity System Manager に直接アクセスするには、 SANtricity System Manager 管理者のユーザ名とパスワードが必要です。

> グリッドマネージャまたは StorageGRID アプライアンスインストーラを使用して SANtricity System Manager にアクセスするには、 SANtricity ファームウェア 8.70 以降が必要です。StorageGRID アプライアンス・インストーラを使用してファームウェアのバージョンを確認し、 * Help * > * About * を選択します。

> グリッドマネージャまたはアプライアンスインストーラから SANtricity システムマネージャにアクセスする方法は、通常、ハードウェアを監視して E シリーズ AutoSupport を設定することだけを目的としています。ファームウェアのアップグレードなど、 SANtricity System Manager 内の多くの機能や操作は、 StorageGRID アプライアンスの監視には適用されません。問題を回避するには、アプライアンスのハードウェアの設置とメンテナンスの手順に必ず従ってください。

このタスクについて

SANtricity System Manager にアクセスする方法は 3 種類あり、その方法はインストールおよび設定のどの段階にあるかによって異なります。

- アプライアンスが StorageGRID システムにノードとして導入されていない場合は、 StorageGRID アプライアンスインストーラの Advanced タブを使用します。

導入されたノードは、 StorageGRID アプライアンスインストーラを使用して SANtricity システムマネージャにアクセスできなくなります。

- アプライアンスを StorageGRID システムにノードとして導入している場合は、グリッドマネージャのノードページにある SANtricity システムマネージャタブを使用します。
- StorageGRID アプライアンスインストーラまたはグリッドマネージャを使用できない場合は、管理ポートに接続された Web ブラウザを使用して SANtricity System Manager に直接アクセスできます。

この手順 には、 SANtricity システムマネージャに最初にアクセスする手順が含まれています。SANtricity System Manager をすでにセットアップしている場合は、に進みます ハードウェアアラートを設定します ステップ。

グリッドマネージャまたは StorageGRID アプライアンスインストーラを使用すると、アプライアンスの管理ポートを設定または接続しなくても SANtricity System Manager にアクセスできます。

SANtricity System Manager を使用して次の項目を監視します。

- ストレージアレイレベルのパフォーマンス、 I/O レイテンシ、 CPU 利用率、スループットなどのパフォーマンスデータ
- ハードウェアコンポーネントのステータス
- 診断データの表示などの機能をサポートします

SANtricity System Manager を使用して、次の設定を行うことができます。

- ストレージコントローラシェルフのコンポーネントの E メールアラート、 SNMP アラート、または syslog アラート
- ストレージコントローラシェルフのコンポーネントの E シリーズ AutoSupport の設定。

  E シリーズ AutoSupport の詳細については、 E シリーズドキュメントセンターを参照してください。

  "NetApp E シリーズシステムのドキュメントのサイト"

- セキュリティ保護されたドライブのロックを解除するために必要なドライブセキュリティキー（ドライブセキュリティ機能が有効になっている場合はロックの解除が必要）
- SANtricity システムマネージャにアクセスするための管理者パスワード

手順

1. 次のいずれかを実行します。
   - StorageGRID アプライアンス・インストーラを使用して、 * アドバンスト * > * SANtricity システム・マネージャ * を選択します
   - Grid Managerを使用して* Nodes >を選択します ***appliance Storage Node*** >* SANtricity システム・マネージャ*

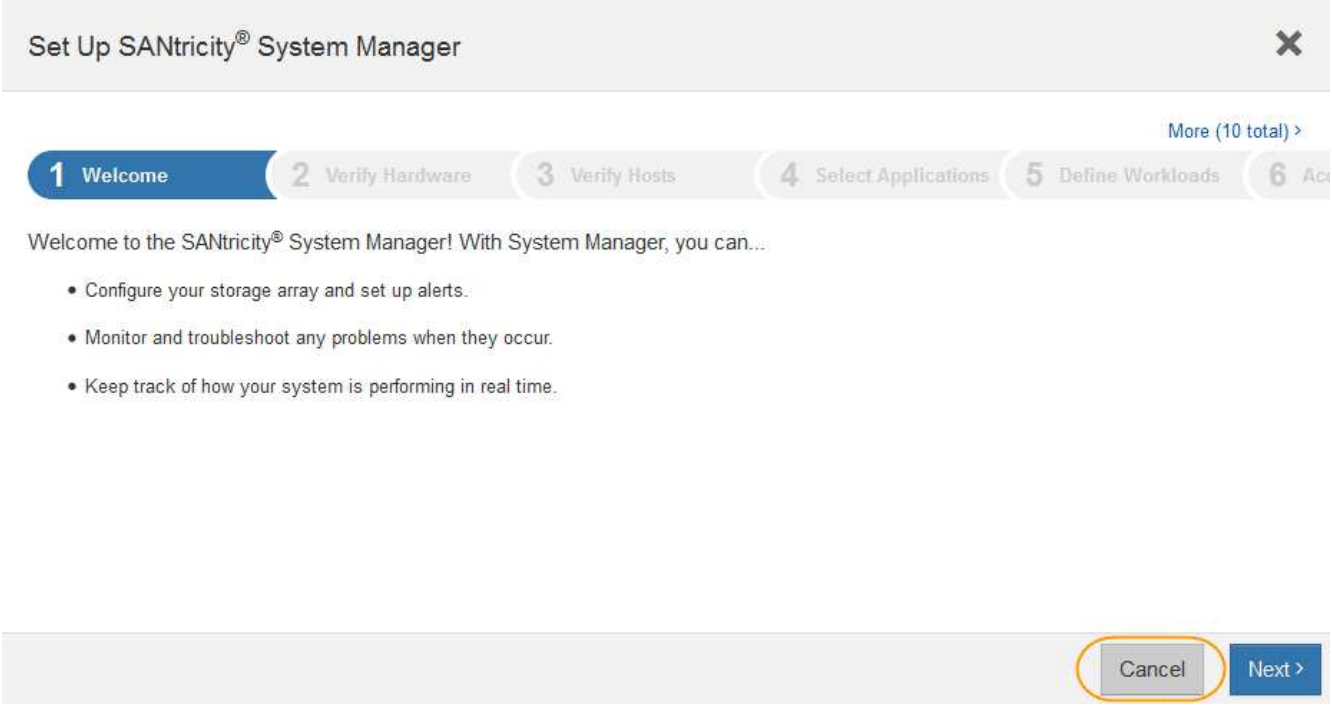
これらのオプションを使用できない場合やログインページが表示されない場合は、ストレージコントローラの IP アドレスを使用する必要があります。SANtricity System Managerにアクセスするには、ストレージコントローラのIP：+にアクセスします `https://Storage_Controller_IP`

SANtricity System Manager のログインページが表示されます。

2. 管理者パスワードを設定または入力します。

SANtricity System Manager では、すべてのユーザで共有する管理者パスワードを 1 つ使用します。

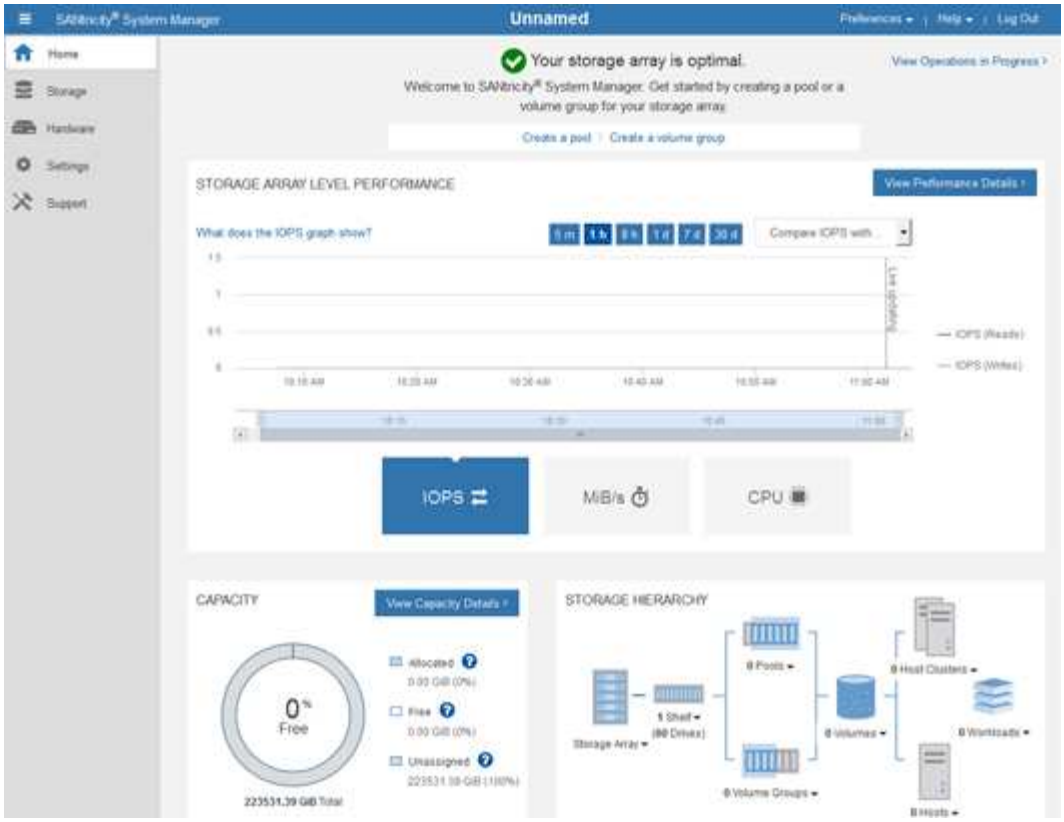
セットアップウィザードが表示されます。




3. 「 * キャンセル * 」を選択してウィザードを閉じます。

StorageGRID アプライアンスにはセットアップ・ウィザードを実行しないでください。

SANtricity の System Manager ホームページが表示されます。




1. ハードウェアアラートを設定します。
   a. SANtricity System Manager のオンラインヘルプにアクセスするには、 * Help * を選択します。
   b. オンラインヘルプの「 * Settings * > * Alerts * 」（ * 設定 * > * アラート * ）セクションを使用して、アラートについて学習します。
   c. How To の指示に従って ' メール・アラート 'SNMP アラート ' または syslog アラートを設定します
2. ストレージコントローラシェルフのコンポーネントの AutoSupport を管理します。
   a. SANtricity System Manager のオンラインヘルプにアクセスするには、 * Help * を選択します。
   b. オンラインヘルプの「* Support > Support Center *」セクションで、AutoSupport 機能について学習します。
   c. 「 How To 」の指示に従って、 AutoSupport を管理します。

      管理ポートを使用せずに E シリーズ AutoSupport メッセージを送信するための StorageGRID プロキシを設定する手順については、 StorageGRID の管理手順および「 E シリーズ AutoSupport のプロキシ設定」を参照してください。

   "StorageGRID の管理"
3. アプライアンスでドライブセキュリティ機能が有効になっている場合は、セキュリティキーを作成して管理します。
   a. SANtricity System Manager のオンラインヘルプにアクセスするには、 * Help * を選択します。
   b. オンラインヘルプの「 * Settings * > * System * > * Security key management * 」セクションでドライブセキュリティについて学習します。
   c. 「 How To 」の指示に従って、セキュリティキーを作成および管理します。

4. 必要に応じて、管理者パスワードを変更します。
   a. SANtricity System Manager のオンラインヘルプにアクセスするには、 * Help * を選択します。
   b. オンラインヘルプの * Home * > * Storage array administration * セクションで、管理者パスワードを確認してください。
   c. 「 How To 」の指示に従ってパスワードを変更します。

関連情報

"Web ブラウザの要件"

"StorageGRID アプライアンスインストーラを使用してストレージコントローラのIPアドレスを設定します"

**SANtricity** システムマネージャでハードウェアステータスを確認します

## SANtricity System Manager を使用して、ストレージコントローラシェルフの個々のハードウェアコンポーネントを監視および管理したり、コンポーネントの温度やドライブに関連する問題など、ハードウェア診断および環境に関する情報を確認したりできます。

必要なもの

- サポートされているWebブラウザを使用します。
- グリッドマネージャを介して SANtricity システムマネージャにアクセスするには、ストレージアプライアンス管理者の権限またはルートアクセス権限が必要です。
- StorageGRID アプライアンスインストーラを使用して SANtricity System Manager にアクセスするには、SANtricity System Manager 管理者のユーザ名とパスワードが必要です。
- Web ブラウザを使用して SANtricity System Manager に直接アクセスするには、 SANtricity System Manager 管理者のユーザ名とパスワードが必要です。

> グリッドマネージャまたは StorageGRID アプライアンスインストーラを使用して SANtricity System Manager にアクセスするには、 SANtricity ファームウェア 8.70 以降が必要です。

> グリッドマネージャまたはアプライアンスインストーラから SANtricity システムマネージャにアクセスする方法は、通常、ハードウェアを監視して E シリーズ AutoSupport を設定することだけを目的としています。ファームウェアのアップグレードなど、 SANtricity System Manager 内の多くの機能や操作は、 StorageGRID アプライアンスの監視には適用されません。問題を回避するには、アプライアンスのハードウェアの設置とメンテナンスの手順に必ず従ってください。

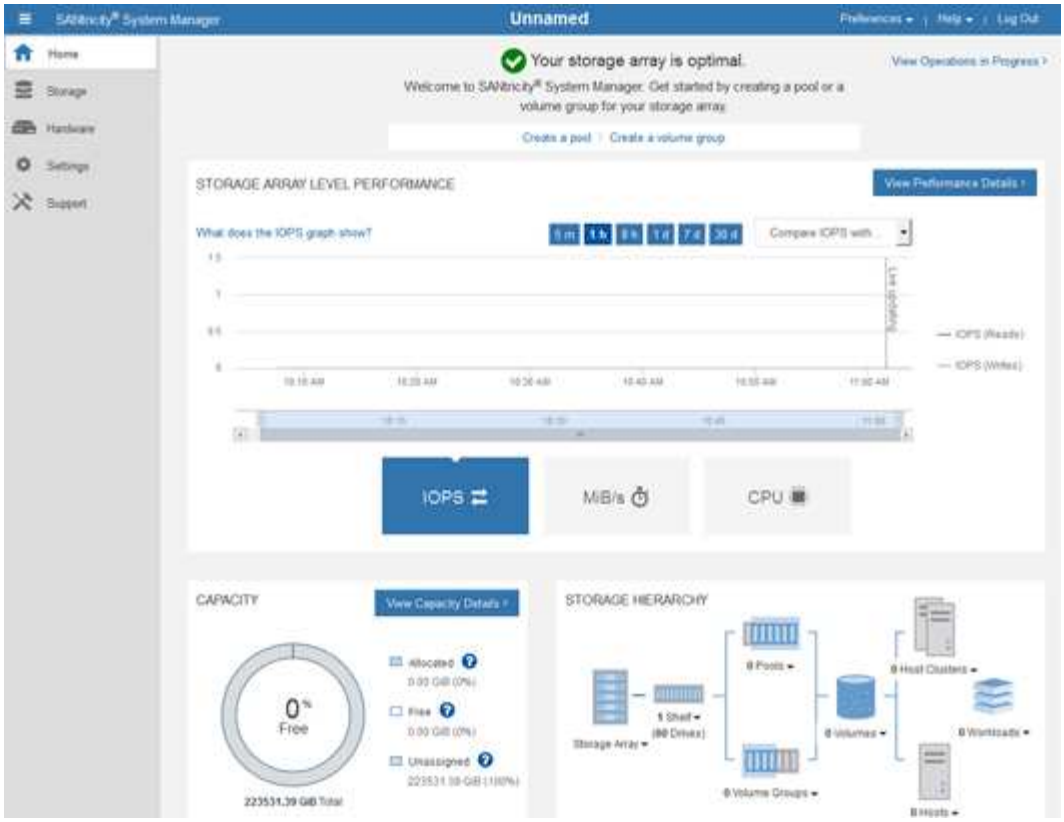
手順

1. SANtricity システムマネージャにアクセスします。

   "『Setting Up and Accessing SANtricity System Manager』を参照してください"

2. 必要に応じて、管理者のユーザ名とパスワードを入力します。
3. セットアップウィザードを閉じて SANtricity システムマネージャのホームページを表示するには、 * Cancel * をクリックします。

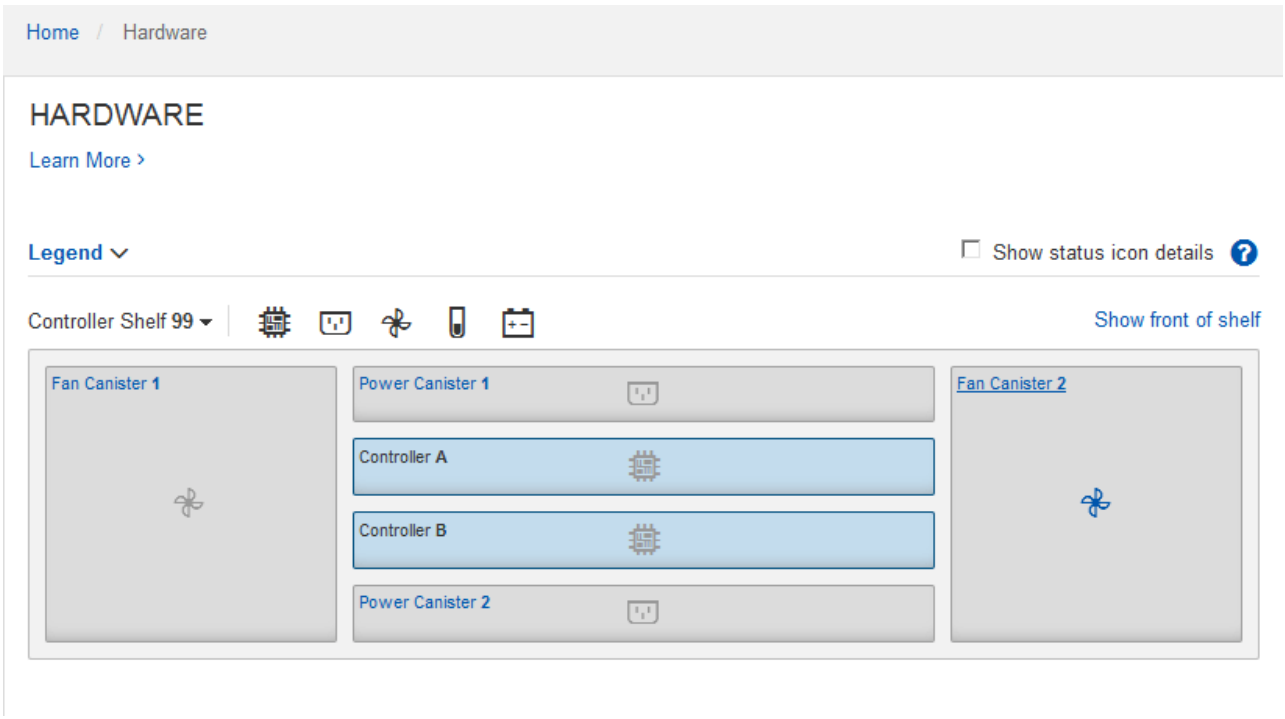
   SANtricity の System Manager ホームページが表示されます。SANtricity System Manager では、コントローラシェルフがストレージアレイと表示されます。




4. アプライアンスハードウェアについて表示された情報を確認し、すべてのハードウェアコンポーネントのステータスが「 Optimal 」であることを確認します。

   a. [* ハードウェア * ] タブをクリックします。

   b. Show back of shelf* （シェルフの背面を表示）をクリックします。




シェルフの背面から、両方のストレージコントローラ、各ストレージコントローラのバッテリ、電源キャ

ニスター 2 台、ファンキャニスター 2 台、および拡張シェルフ（ある場合）を確認できます。構成部品の温度を表示することもできます。

a. 各ストレージコントローラの設定を表示するには、コントローラを選択し、コンテキストメニューから * 設定の表示 * を選択します。

b. シェルフの背面にある他のコンポーネントの設定を確認するには、対象となるコンポーネントを選択します。

c. [Show front of shelf* （シェルフの前面を表示） ] をクリックし、表示するコンポーネントを選択します。

   シェルフの前面からは、ストレージコントローラシェルフまたは拡張シェルフ（ある場合）のドライブとドライブドロワーを確認できます。

ステータスが「 Needs Attention 」になっているコンポーネントがある場合は、 Recovery Guru に示される手順に従って問題 を解決するか、テクニカルサポートに連絡してください。

**StorageGRID** アプライアンスインストーラを使用してストレージコントローラの**IP**アドレスを設定します

## 各ストレージコントローラの管理ポート 1 を使用して、アプライアンスを SANtricity System Manager の管理ネットワークに接続します。StorageGRID アプライアンスインストーラから SANtricity System Manager にアクセスできない場合は、各ストレージコントローラの静的 IP アドレスを設定して、コントローラシェルフのハードウェアおよびコントローラファームウェアへの管理接続が失われないようにする必要があります。

必要なもの

- StorageGRID 管理ネットワークに接続できる管理クライアントを使用しているか、サービスラップトップを使用している必要があります。
- クライアントまたはサービスラップトップに、サポートされている Web ブラウザをインストールしておきます。

このタスクについて

DHCP によって割り当てられたアドレスは、いつ変更されるかわかりません。一貫したアクセスを確保するために、コントローラには静的 IP アドレスを割り当ててください。

> この手順 は、StorageGRID アプライアンスインストーラ（アドバンスト>* SANtricity システムマネージャ*）またはグリッドマネージャ（ノード>* SANtricity システムマネージャ*）からSANtricity システムマネージャにアクセスできない場合にのみ使用してください。

手順

1. クライアントから、StorageGRID アプライアンスインストーラのURLを入力します：+
   **`https://Appliance_Controller_IP:8443`**

   の場合 `*Appliance_Controller_IP*`には、任意のStorageGRID ネットワーク上のアプライアンスのIPアドレスを使用します。

   StorageGRID アプライアンスインストーラのホームページが表示されます。

2. Configure Hardware * > * Storage Controller Network Configuration * を選択します。

Storage Controller Network Configuration ページが表示されます。

3. ネットワーク構成に応じて、 IPv4 、 IPv6 、またはその両方で * Enabled * を選択します。
4. 自動的に表示される IPv4 アドレスを書き留めます。

   ストレージコントローラの管理ポートに IP アドレスを割り当てるためのデフォルトの方法は、 DHCP です。

   DHCP 値が表示されるまでに数分かかる場合があります。

5. 必要に応じて、ストレージコントローラの管理ポートに静的 IP アドレスを設定します。

   管理ポートに静的 IP を割り当てるか、 DHCP サーバでアドレスの永久リースを割り当てる必要があります。

   a. 「 * Static * 」を選択します。
   b. CIDR 表記を使用して IPv4 アドレスを入力します。
   c. デフォルトゲートウェイを入力します。

   d. [ 保存（ Save ） ] をクリックします。

      変更が適用されるまで数分かかる場合があります。

SANtricity System Managerに接続するときは、新しい静的IPアドレスをURL：+として使用します
`https://Storage_Controller_IP`

**BMC**インターフェイスを設定しています

SG6000-CN コントローラのベースボード管理コントローラ（ BMC ）のユーザインターフェイスは、ハードウェアに関するステータス情報を提供し、 SG6000-CN コントローラの SNMP 設定やその他のオプションを設定できます。

手順

- "BMCインターフェイスのrootパスワードを変更しています"
- "BMC管理ポートのIPアドレスを設定します"
- "BMCインターフェイスへのアクセス"
- "SG6000-CNコントローラのSNMP設定"
- "アラート用のEメール通知の設定"

**BMC**インターフェイスの**root**パスワードを変更しています

## セキュリティを確保するために、 BMC の root ユーザのパスワードを変更する必要があります。

必要なもの

- 管理クライアントがサポートされているWebブラウザを使用している必要があります。

このタスクについて

初めてアプライアンスをインストールするとき、BMCではrootユーザのデフォルトパスワードが使用されます(`root/calvin`）。システムを保護するために、 root ユーザのパスワードを変更する必要があります。

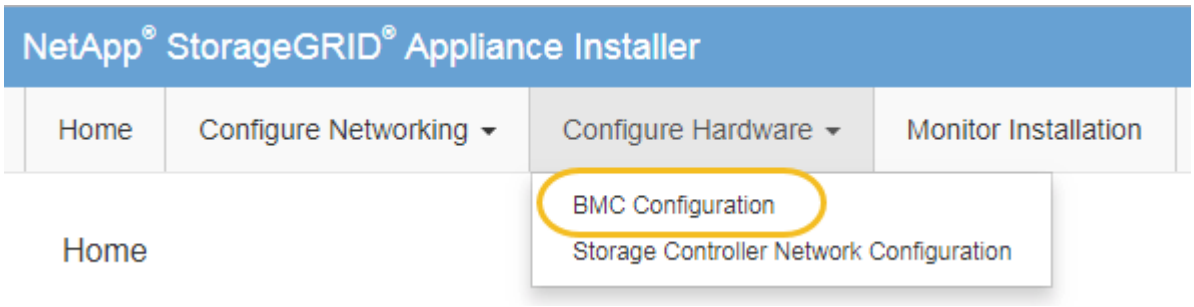
手順

1. クライアントから、StorageGRID アプライアンスインストーラのURLを入力します：+ **`https://Appliance_Controller_IP:8443`**

   の場合 `*Appliance_Controller_IP*`には、任意のStorageGRID ネットワーク上のアプライアンスのIPアドレスを使用します。

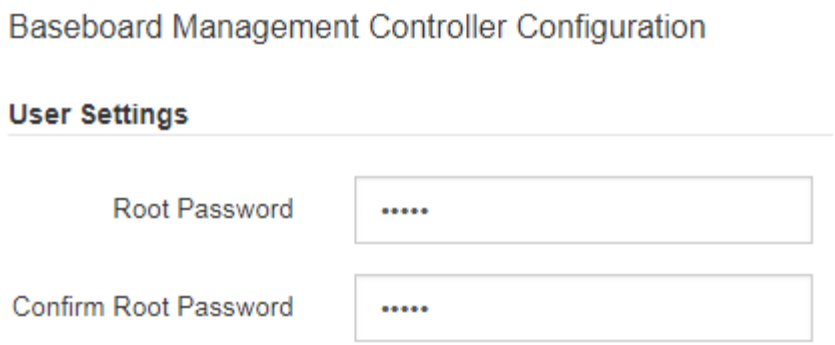
   StorageGRID アプライアンスインストーラのホームページが表示されます。

2. [ ハードウェアの設定 *>*BMC 構成 *] を選択します。




   [Baseboard Management Controller Configuration] ページが表示されます。

3. root アカウントの新しいパスワードを 2 つのフィールドに入力します。




4. [ 保存（ Save ） ] をクリックします。

**BMC**管理ポートの**IP**アドレスを設定します

## BMC インターフェイスにアクセスするには、 SG6000-CN コントローラの BMC 管理ポートの IP アドレスを設定する必要があります。

必要なもの

- 管理クライアントがサポートされているWebブラウザを使用している必要があります。
- StorageGRID ネットワークに接続できる管理クライアントを使用している必要があります。
- BMC 管理ポートが、使用する管理ネットワークに接続されている必要があります。

このタスクについて

BMC 管理ポートでは、サポート目的で下位レベルのハードウェアアクセスが許可されます。

> このポートは、信頼されているセキュアな内部管理ネットワークにのみ接続してください。該当するネットワークがない場合は、テクニカルサポートから BMC 接続の要請があった場合を除き、 BMC ポートを接続しないか、またはブロックしたままにしてください。

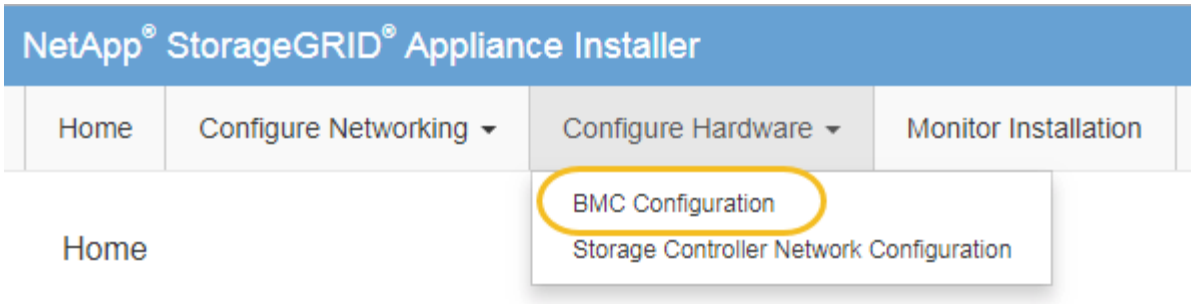
手順

1. クライアントから、StorageGRID アプライアンスインストーラのURLを入力します：+ **`https://SG6000-CN_Controller_IP:8443`**

   の場合 `SG6000-CN_Controller_IP`には、任意のStorageGRID ネットワーク上のアプライアンスのIPアドレスを使用します。

   StorageGRID アプライアンスインストーラのホームページが表示されます。

2. [ ハードウェアの設定 *>*BMC 構成 *] を選択します。

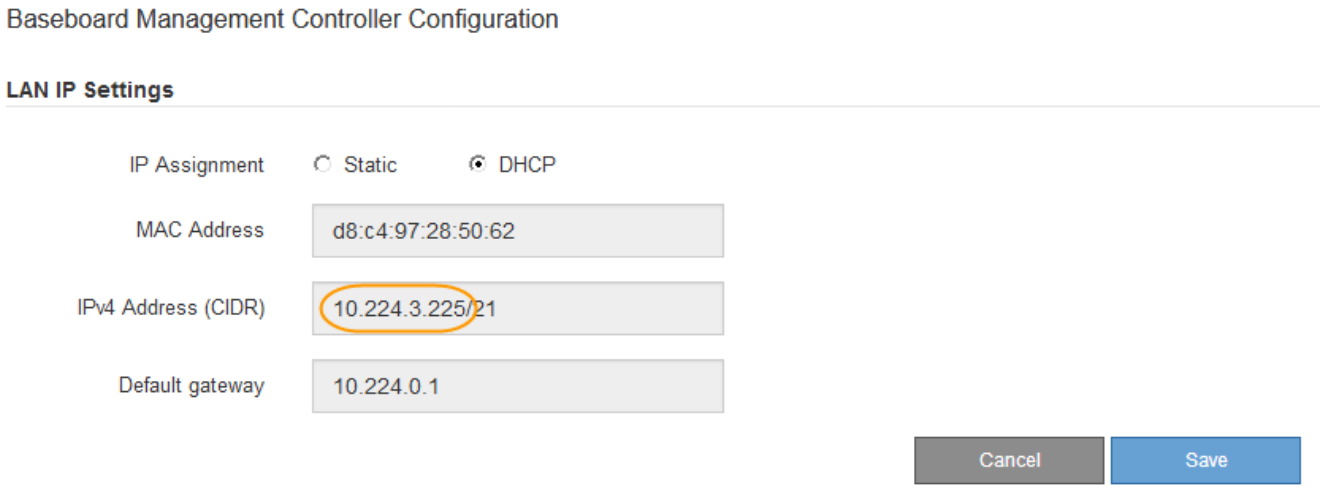



[Baseboard Management Controller Configuration] ページが表示されます。

3. 自動的に表示される IPv4 アドレスを書き留めます。

   このポートに IP アドレスを割り当てるためのデフォルトの方法は、 DHCP です。

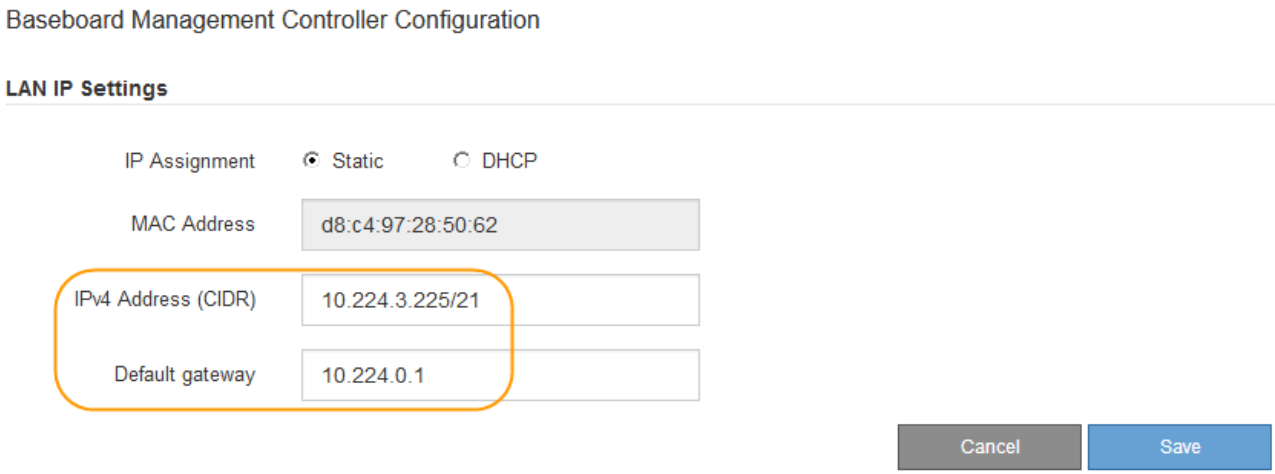
   DHCP 値が表示されるまでに数分かかる場合があります。




4. 必要に応じて、 BMC 管理ポートに静的 IP アドレスを設定します。

   BMC 管理ポートに静的 IP を割り当てるか、 DHCP サーバでアドレスの永久リースを割り当てる必要があります。

   a. 「 * Static * 」を選択します。
   b. CIDR 表記を使用して IPv4 アドレスを入力します。
   c. デフォルトゲートウェイを入力します。




d. [ 保存（ Save ） ] をクリックします。

変更が適用されるまで数分かかる場合があります。

**BMC**インターフェイスへのアクセス

## BMC 管理ポートの DHCP または静的 IP アドレスを使用して、 SG6000-CN コントローラの BMC インターフェイスにアクセスできます。

必要なもの

- SG6000-CN コントローラの BMC 管理ポートが、使用する管理ネットワークに接続されている。

- 管理クライアントがサポートされているWebブラウザを使用している必要があります。

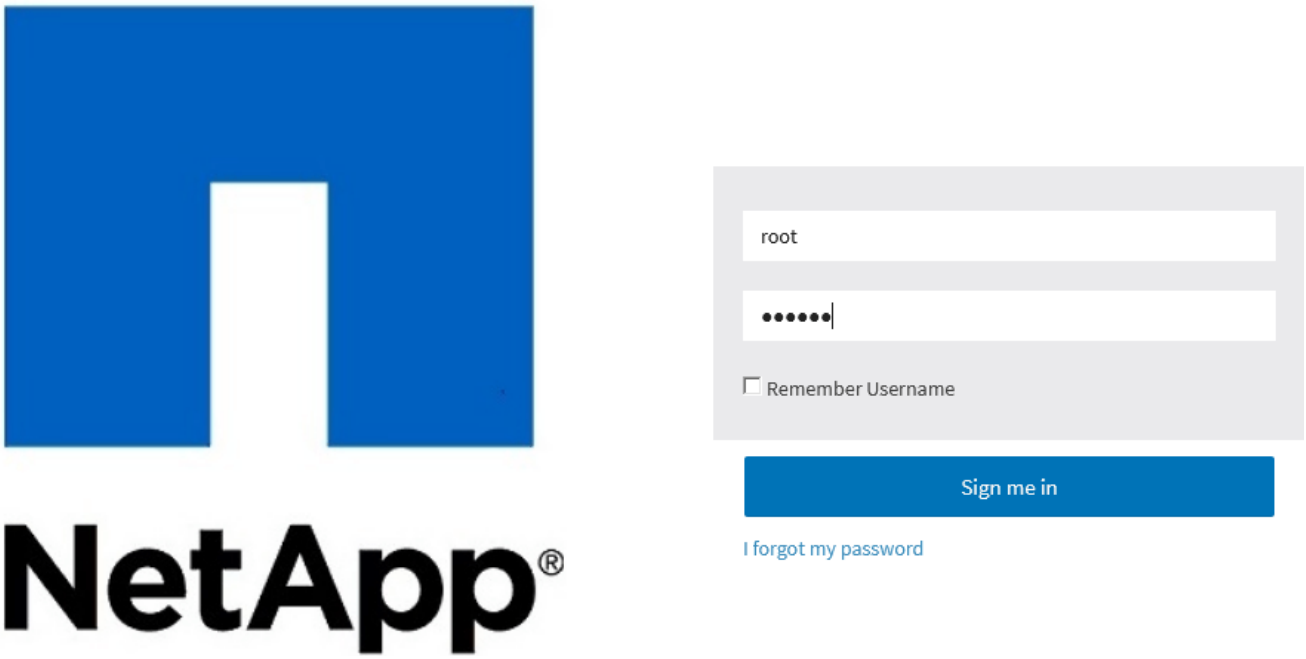
手順

1. BMCインターフェイスのURLとして「+」を入力します
**`https://BMC_Port_IP`**

の場合 `*BMC_Port_IP*`BMC管理ポートのDHCPまたは静的IPアドレスを使用します。

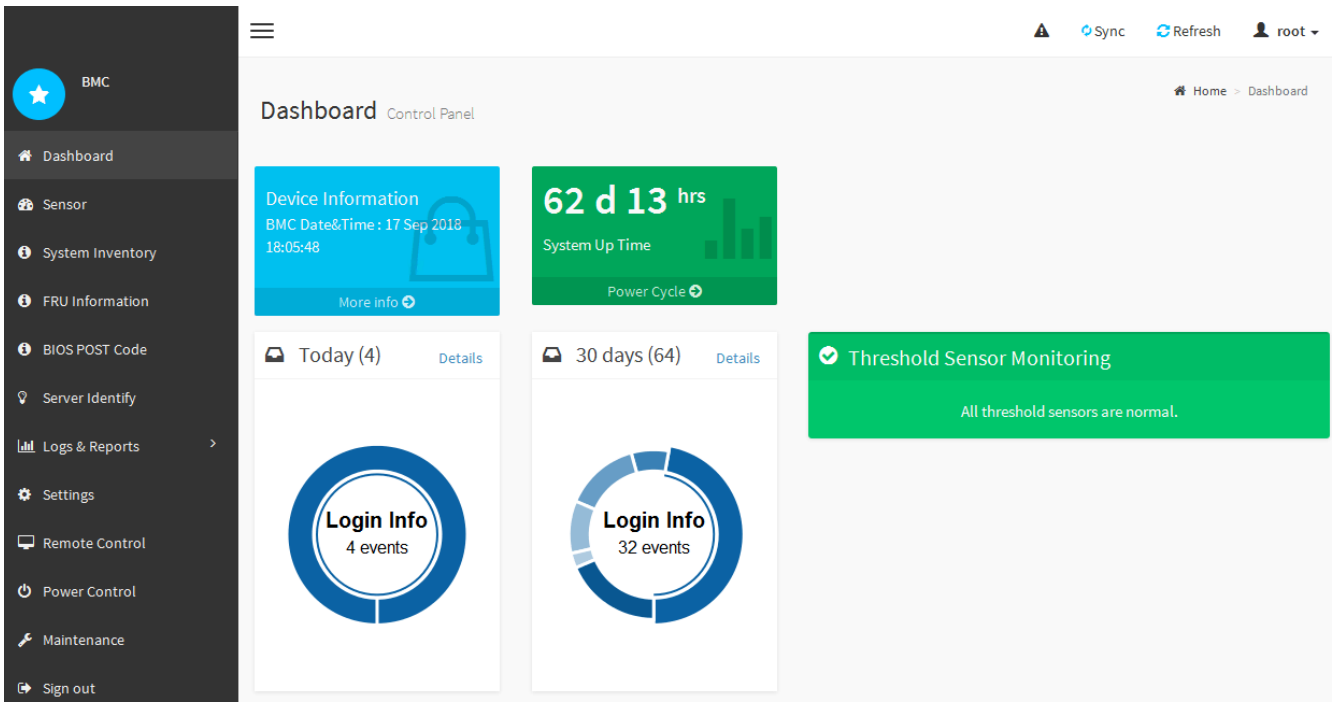
BMC のサインインページが表示されます。

2. rootのユーザ名とパスワードを入力します。デフォルトのrootパスワード+を変更したときに設定したパスワードを使用します
**`root`** [+]
***`password`***




3. 「 * サインイン * 」を選択します。

   BMC ダッシュボードが表示されます。




4. 必要に応じて、 **Settings**>*User Management* を選択し、「 disabled 」ユーザをクリックして、追加のユーザを作成します。

   ユーザが初めてサインインすると、セキュリティを強化するためにパスワードの変更を求められる場合があります。

関連情報

"BMCインターフェイスのrootパスワードを変更しています"

### SG6000-CNコントローラのSNMP設定

ハードウェアの SNMP の設定に精通している場合は、 BMC インターフェイスを使用して SG6000-CN コントローラの SNMP 設定を行うことができます。セキュリティで保護されたコミュニティストリングを指定し、 SNMP トラップを有効にし、 SNMP の送信先を最大 5 つ指定できます。

必要なもの

- BMC ダッシュボードへのアクセス方法を確認しておく必要があります。
- SNMPv1-v2c 機器の SNMP 設定経験が必要です。

手順

1. BMC ダッシュボードで、 * Settings * > * SNMP Settings * を選択します。
2. SNMP 設定ページで、 * SNMP V1/V2* を有効にするを選択し、読み取り専用コミュニティストリングと読み取り / 書き込みコミュニティストリングを指定します。

   読み取り専用コミュニティストリングは、ユーザ ID やパスワードのようなものです。侵入者がネットワーク設定に関する情報を取得できないようにするには、この値を変更する必要があります。読み取り / 書き込みコミュニティストリングは、不正な変更からデバイスを保護します。

3. 必要に応じて、 * トラップを有効にする * を選択し、必要な情報を入力します。

   IP アドレスを使用して、各 SNMP トラップの送信先 IP を入力します。完全修飾ドメイン名はサポートされません。

   SG6000-CN コントローラが異常な状態になったときに SNMP コンソールにすぐに通知を送信するには、トラップを有効にします。トラップは、さまざまなコンポーネントや温度のしきい値のハードウェア障害を示している場合があります。

4. 必要に応じて、 [ テストトラップの送信 ] をクリックして設定をテストします。
5. 設定が正しい場合は、 * 保存 * をクリックします。

### アラート用のEメール通知の設定

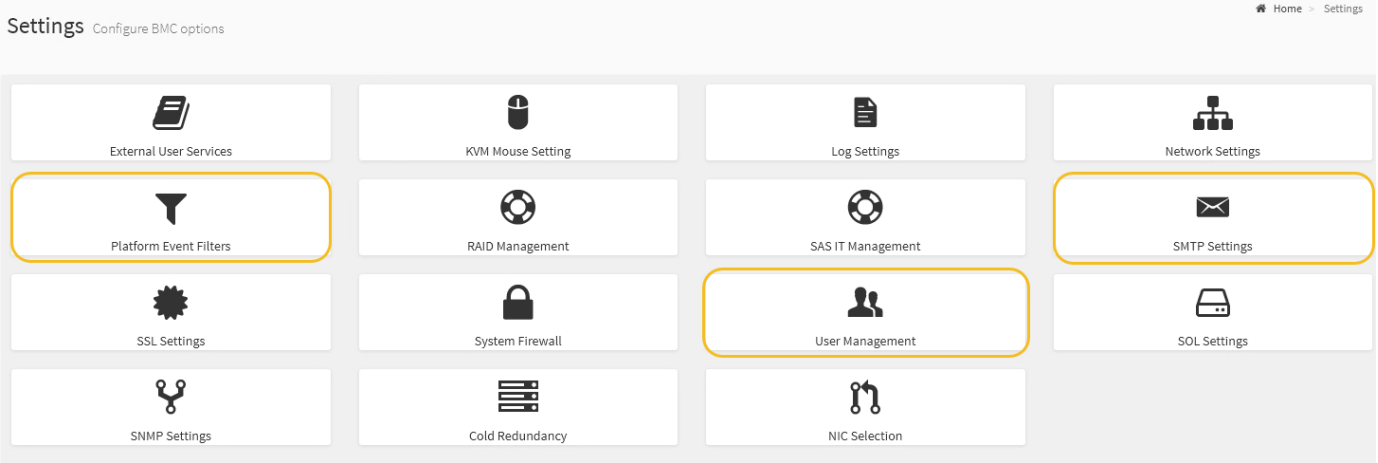
アラート発生時に E メール通知が送信されるようにするには、 BMC インターフェイスを使用して SMTP 設定、ユーザ、 LAN 宛先、アラートポリシー、およびイベントフィルタを設定する必要があります。

必要なもの

BMC ダッシュボードへのアクセス方法を確認しておく必要があります。

このタスクについて

BMC インターフェイスでは、 [ 設定 ] ページの *SMTP 設定 * 、 * ユーザー管理 * 、および * プラットフォーム・イベント・フィルタ * オプションを使用して、電子メール通知を設定します。




手順

1. SMTP を設定します。
   a. [ * 設定 * > * SMTP 設定 * ] を選択します。
   b. [ 送信者電子メール ID] に、有効な電子メールアドレスを入力します。

      この E メールアドレスは、 BMC が E メールを送信したときの送信元アドレスとして提供されます。

2. アラートを受信するようにユーザを設定します。
   a. BMC ダッシュボードで、 * Settings * > * User Management * を選択します。
   b. アラート通知を受信するユーザを少なくとも 1 人追加してください。

      ユーザに設定する E メールアドレスは、 BMC がアラート通知の送信先アドレスです。たとえば、「 notification-user 」などの一般的なユーザーを追加し、テクニカルサポートチームの Email宛先リストの電子メールアドレスを使用できます。

3. LAN 宛先にアラートを設定します。
   a. [ * 設定 * > * プラットフォーム・イベント・フィルタ * > * LAN 宛先 * ] を選択します。
   b. LAN 宛先を少なくとも 1 つ設定します。
      - [ 宛先の種類 ] で [**Email**] を選択します。
      - BMC Username には、前に追加したユーザ名を選択します。
      - 複数のユーザを追加し、すべてのユーザが通知メールを受信できるようにするには、ユーザごとに LAN 宛先を追加する必要があります。
   c. テストアラートを送信します。
4. アラートポリシーを設定して、 BMC がアラートを送信するタイミングと場所を定義できるようにします。
   a. [ * 設定 * > * プラットフォーム・イベント・フィルタ * > * アラート・ポリシー * ] を選択します。
   b. LAN 宛先ごとに少なくとも 1 つのアラートポリシーを設定します。
      - [ ポリシーグループ番号（ Policy Group Number ） ] で、 * 1 * を選択します。
      - ［ ポリシーアクション ］ で、 ［ * 常にこの宛先にアラートを送信する * ］ を選択します。
      - LAN チャンネルの場合、 * 1 * を選択します。

- [Destination Selector] で、ポリシーの LAN 宛先を選択します。

5. イベントフィルタを設定して、さまざまなイベントタイプのアラートを適切なユーザに送信します。
   a. [ * 設定 * > * プラットフォーム・イベント・フィルタ * > * イベント・フィルタ * ] を選択します。
   b. Alert Policy Group Number （アラートポリシーグループ番号）に * 1 * を入力します。
   c. アラートポリシーグループに通知するイベントごとにフィルタを作成します。
      - 電源アクション、特定のセンサーイベント、またはすべてのイベントのイベントフィルタを作成できます。
      - 監視するイベントが不明な場合は、センサーの種類として「 * すべてのセンサー * 」を選択し、イベントオプションとして「すべてのイベント * 」を選択します。不要な通知を受け取った場合は、選択内容をあとで変更できます。

オプション：ノード暗号化を有効にする

ノードの暗号化を有効にすると、アプライアンス内のディスクを安全なキー管理サーバ（ KMS ）暗号化によってサイト内での物理的な損失やデータの削除から保護することができます。アプライアンスのインストール時にノード暗号化を選択して有効にする必要があります。また、 KMS 暗号化プロセスが開始されると、ノード暗号化の選択を解除できません。

必要なもの

StorageGRID の管理手順の KMS に関する情報を確認します。

このタスクについて

ノード暗号化が有効になっているアプライアンスは、 StorageGRID サイト用に設定されている外部キー管理サーバ（ KMS ）に接続します。各 KMS （または KMS クラスタ）は、サイトにあるすべてのアプライアンスノードの暗号化キーを管理します。これらのキーは、ノード暗号化が有効なアプライアンスで、各ディスク上のデータを暗号化および復号化します。

Grid Manager StorageGRID では、アプライアンスのインストール前またはインストール後に KMS を設定できます。詳細については、 StorageGRID の管理手順の KMS とアプライアンスの設定に関する情報を参照してください。

- アプライアンスをインストールする前に KMS を設定すると、 KMS で制御される暗号化が開始されます。この暗号化は、アプライアンスでノード暗号化を有効にし、 KMS が設定されている StorageGRID サイトに追加します。
- アプライアンスをインストールする前に KMS が設定されていない場合は、 KMS が設定され、アプライアンスノードを含むサイトで利用可能になった時点で、ノード暗号化が有効になっている各アプライアンスで KMS 制御された暗号化が実行されます。

> ノード暗号化が有効になっているアプライアンスより前に存在するデータは、設定されたKMSに接続する前に、セキュアでない一時キーで暗号化されます。キーが KMS から提供される値に設定されるまで、アプライアンスの取り外しや盗難は防止されません。

ディスクの復号化に KMS キーが必要な場合を除いて、アプライアンス上のデータを取得することはできず、データが実質的に失われます。これは、 KMS から復号化キーを取得できない場合に発生します。顧客が KMS 設定をクリアするか、 KMS キーの有効期限が切れるか、 KMS への接続が失われるか、 KMS キーがインストールされている StorageGRID システムからアプライアンスが削除されると、キーにアクセスできなく

なります。

手順

1. ブラウザを開き、アプライアンスのコンピューティングコントローラの IP アドレスのいずれかを入力します。

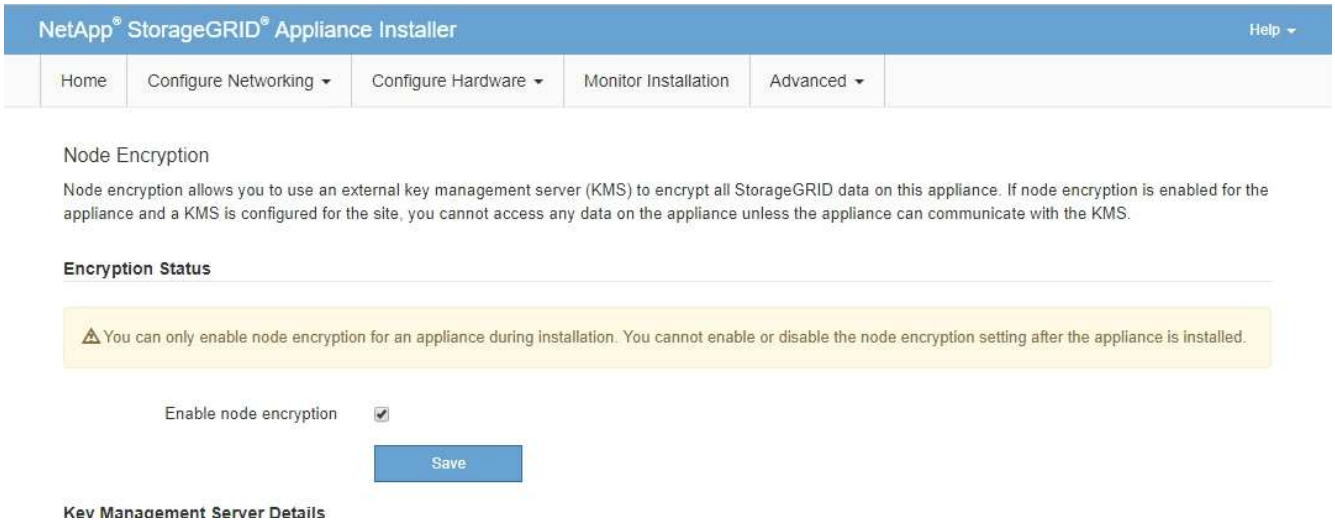
   **`https://Controller_IP:8443`**

   *`Controller_IP`* は、3つのStorageGRID ネットワークのいずれかでのコンピューティングコントローラ（ストレージコントローラではない）のIPアドレスです。

   StorageGRID アプライアンスインストーラのホームページが表示されます。

   > アプライアンスを KMS キーで暗号化すると、アプライアンスディスクを復号化する際に同じ KMS キーを使用する必要がなくなります。

2. Configure Hardware * > * Node Encryption * を選択します。




3. [ ノード暗号化を有効にする *] を選択します。

   保存を選択し、アプライアンスノードがStorageGRID システム内のKMS暗号化キーにアクセスしてディスク暗号化を開始するまでは、「ノード暗号化を有効にする」を選択解除してデータ損失のリスクを回避できます。アプライアンスのインストール後、ノード暗号化を無効にすることはできません。

   > KMS を含む StorageGRID サイトにノード暗号化が有効になっているアプライアンスを追加すると、そのノードで KMS 暗号化を使用するのを停止することはできません。

4. [ 保存（ Save ） ] を選択します。

5. アプライアンスを StorageGRID システムのノードとして導入します。

   KMS で制御される暗号化は、アプライアンスが StorageGRID サイト用に設定されている KMS キーにアクセスすると開始されます。KMS 暗号化プロセス中にインストーラによって進捗状況のメッセージが表示されます。この処理には、アプライアンス内のディスクボリュームの数によっては数分かかることがあります。

アプライアンスは、最初に各ディスクボリュームにランダムな KMS 以外の暗号化キーを割り当てて構成します。ディスクはこの一時的な暗号化キーを使用して暗号化されます。このキーは、ノード暗号化が有効になっているアプライアンスが StorageGRID サイト用に設定されている KMS キーにアクセスするまではセキュリティ保護されません。

完了後

アプライアンスノードがメンテナンスモードのときに使用されているノード暗号化ステータス、 KMS の詳細、および証明書を確認できます。

関連情報

"StorageGRID の管理"

"メンテナンスモードでのノード暗号化の監視"

オプション：**RAID**モードの変更（**SG6000**のみ）

アプライアンスでは、ストレージとリカバリの要件に応じて別の RAID モードに変更できます。モードを変更できるのは、アプライアンスストレージノードを導入する前だけです。

必要なもの

- StorageGRID に接続できるクライアントを使用している必要があります。
- クライアントにサポートされているWebブラウザをインストールしておきます。

このタスクについて

アプライアンスをストレージノードとして導入する前に、次のいずれかのボリューム設定オプションを選択できます。

- * DDP * ：データドライブ 8 本につきパリティドライブを 2 本使用します。すべてのアプライアンスに推奨されるデフォルトのモードです。RAID6 よりもシステムパフォーマンスに優れ、ドライブ障害が発生したあとのリビルド時間も短く、管理も簡単です。また、 60 ドライブアプライアンスをドロワー損失から保護します。
- * DDP16 * ：このモードはデータドライブ 16 本につきパリティドライブを 2 本使用するため、 DDP よりもストレージ効率が高くなります。RAID6 よりもシステムパフォーマンスに優れ、ドライブ障害が発生したあとのリビルド時間も短く、管理も簡単です。ストレージ効率は RAID6 と同等です。DDP16 モードを使用するには、構成にドライブが 20 本以上含まれている必要があります。ドロワー損失からの保護は提供しません。
- *RAID6 *: このモードは 16 台以上のデータドライブごとに 2 本のパリティドライブを使用します。RAID 6 モードを使用するには、構成にドライブが 20 本以上含まれている必要があります。DDP よりもアプライアンスのストレージ効率を上げることができますが、ほとんどの StorageGRID 環境では推奨されません。

ボリュームがすでに構成されている場合や StorageGRID が事前にインストールされている場合に RAID モードを変更すると、ボリュームが削除されて置き換えられます。対象となったボリュームのデータはすべて失われます。

手順

1. ブラウザを開き、アプライアンスのコンピューティングコントローラの IP アドレスのいずれかを入力します。

   **https://*Controller_IP*:8443**

   *Controller_IP* は、3つのStorageGRID ネットワークのいずれかでのコンピューティングコントローラ（ストレージコントローラではない）のIPアドレスです。

   StorageGRID アプライアンスインストーラのホームページが表示されます。

2. 「 * アドバンスト * 」 > 「 * RAID モード * 」の順に選択します。
3. [Configure RAID Mode*] ページで、 [Mode] ドロップダウンリストから目的の RAID モードを選択します。
4. [ 保存（ Save ） ] をクリックします。

関連情報

"NetApp E シリーズシステムのドキュメントのサイト"

オプション：アプライアンスに対するネットワークポートの再マッピング

アプライアンスストレージノードの内部ポートを別の外部ポートに再マッピングすることが必要になる場合があります。たとえば、ファイアウォールの問題 が原因でポートの再マッピングが必要になることがあります。

必要なもの

- 以前に StorageGRID アプライアンスインストーラにアクセスしていた場合。
- ロードバランサエンドポイントを設定しておらず、設定する予定もない状態である必要があります。

> ポートを再マッピングする場合、同じポートを使用してロードバランサエンドポイントを設定することはできません。ポートを再マッピング済みの場合にロードバランサエンドポイントを設定するには、リカバリとメンテナンスの手順に従ってポートの再マッピングを削除してください。

手順

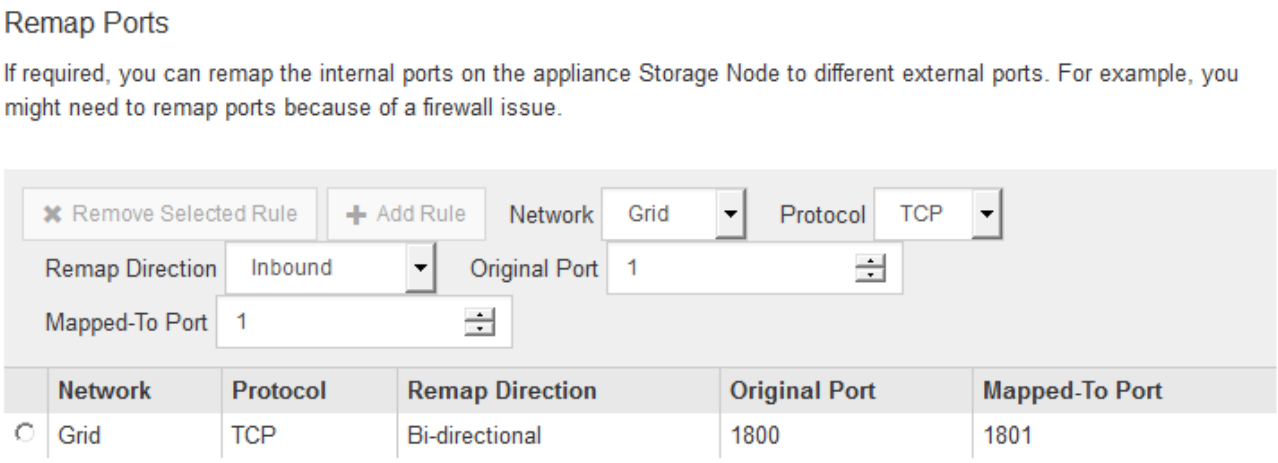
1. StorageGRID アプライアンスインストーラから、 **Configure Networking *>** Remap Port* をクリックします。

   Remap Port ページが表示されます。

2. Network * ドロップダウンボックスから、再マッピングするポートのネットワーク（ Grid 、 Admin 、または Client ）を選択します。
3. [**Protocol**] ドロップダウンボックスから、 IP プロトコルとして [TCP] または [UDP] を選択します。
4. [* Remap Direction] * ドロップダウンボックスから、このポートに再マッピングするトラフィック方向（インバウンド、アウトバウンド、または双方向）を選択します。
5. 「 * Original Port * 」に、再マッピングするポートの番号を入力します。
6. 「 * mapped-to Port * 」には、代わりに使用するポートの番号を入力します。

7. [ * ルールの追加 * ] をクリックします。

   新しいポートマッピングがテーブルに追加され、新しいマッピングがただちに有効になります。




8. ポートマッピングを削除するには、削除するルールのオプションボタンを選択し、 * 選択したルールの削除 * をクリックします。

## アプライアンスストレージノードの導入

ストレージアプライアンスを設置して設定したら、 StorageGRID システムにストレージノードとして導入できます。アプライアンスをストレージノードとして導入する場合は、アプライアンスに搭載されている StorageGRID アプライアンスインストーラを使用します。

必要なもの

- アプライアンスノードのクローンを作成する場合は、リカバリとメンテナンスの手順を続行します。

  ""

- アプライアンスをラックまたはキャビネットに設置し、ネットワークに接続し、電源を投入しておきます。
- StorageGRID アプライアンスインストーラを使用して、アプライアンスのネットワークリンク、 IP アドレス、ポートの再マッピング（必要な場合）を設定しておきます。
- アプライアンスのコンピューティングコントローラに割り当てられている IP アドレスのいずれかを確認しておきます。接続されているどの StorageGRID ネットワークの IP アドレスでも使用できます。
- StorageGRID システムのプライマリ管理ノードを導入しておきます。
- StorageGRID アプライアンスインストーラの IP 設定ページに表示されるすべてのグリッドネットワークサブネットが、プライマリ管理ノードのグリッドネットワークサブネットリストで定義されている。
- サポートされている Web ブラウザがインストールされたサービスラップトップを用意しておきます。

このタスクについて

各ストレージアプライアンスは単一のストレージノードとして機能します。すべてのアプライアンスは、グリッドネットワーク、管理ネットワーク、およびクライアントネットワークに接続できます

StorageGRID システムにアプライアンスストレージノードを導入するには、 StorageGRID アプライアンスインストーラにアクセスして次の手順を実行します。

- プライマリ管理ノードの IP アドレスおよびストレージノードの名前を指定または確認します。
- 導入を開始し、ボリュームの設定とソフトウェアのインストールが完了するまで待機します。
- アプライアンスインストールタスクの途中でインストールが一時停止した場合は、 Grid Manager にサインインしてすべてのグリッドノードを承認し、 StorageGRID のインストールプロセスと導入プロセスを完了すると、インストールを再開できます。

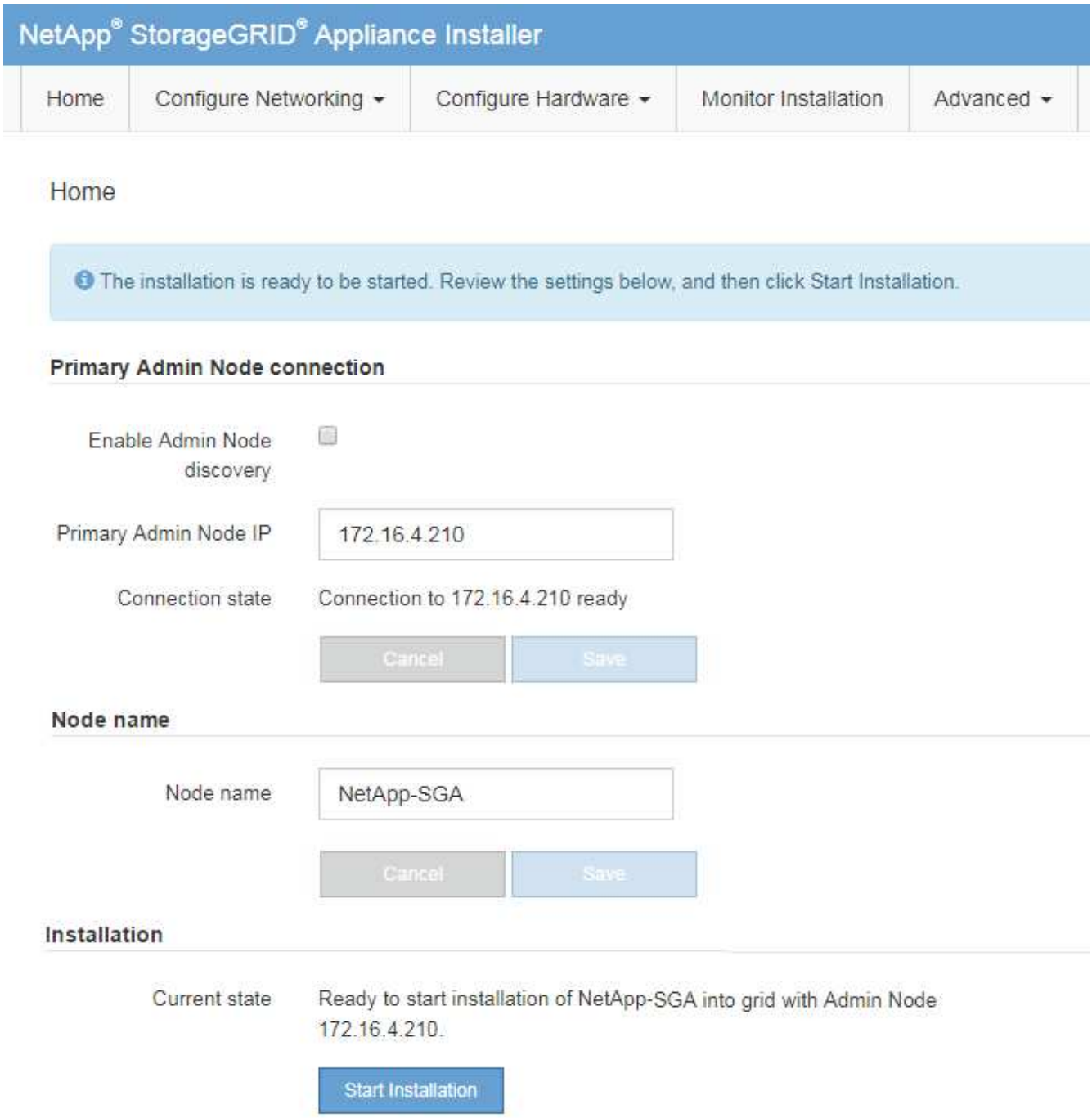
> 一度に複数のアプライアンスノードを導入する必要がある場合は、を使用してインストールプロセスを自動化できます `configure-sga.py` アプライアンスインストールスクリプト。

- 拡張またはリカバリ処理を実行する場合は、該当する手順に従います。
  - 既存の StorageGRID システムにアプライアンスストレージノードを追加する場合は、 StorageGRID システムの拡張手順を参照してください。
  - リカバリ処理の一環としてアプライアンスストレージノードを導入する場合は、リカバリとメンテナンスの手順を参照してください。

手順

1. ブラウザを開き、アプライアンスのコンピューティングコントローラの IP アドレスのいずれかを入力します。[+]
   **`https://Controller_IP:8443`**

   StorageGRID アプライアンスインストーラのホームページが表示されます。




2. 「 * プライマリ管理ノード接続 * 」セクションで、プライマリ管理ノードの IP アドレスを指定する必要があるかどうかを判断します。

   このデータセンターに他のノードがすでにインストールされている場合は、プライマリ管理ノードまたは ADMIN_IP が設定された少なくとも 1 つのグリッドノードが同じサブネットにあるという想定で、StorageGRID アプライアンスインストーラがこの IP アドレスを自動的に検出します。

3. この IP アドレスが表示されない場合や変更する必要がある場合は、アドレスを指定します。

| オプション | 説明 |
| --- | --- |
| IP を手動で入力します | a. Enable Admin Node discovery * チェックボックスの選択を解除します。<br>b. IP アドレスを手動で入力します。<br>c. [ 保存（ Save ） ] をクリックします。<br>d. 新しい IP アドレスの接続状態が READY になるまで待ちます。 |
| 接続されたすべてのプライマリ管理ノードの自動検出 | a. Enable Admin Node discovery * チェックボックスを選択します。<br>b. 検出された IP アドレスのリストが表示されるまで待ちます。<br>c. このアプライアンスストレージノードを導入するグリッドのプライマリ管理ノードを選択します。<br>d. [ 保存（ Save ） ] をクリックします。<br>e. 新しい IP アドレスの接続状態が READY になるまで待ちます。 |

4. [* Node name* （ノード名 * ） ] フィールドに、このアプライアンスノードに使用する名前を入力し、 [ * Save * （保存） ] をクリックします。

   このノード名は、 StorageGRID システムでこのアプライアンスノードに割り当てられ、このタブは、 Grid Manager のノードページ（概要タブ）に表示されます。ノードを承認するときに、必要に応じて、この名前を変更できます。

5. [インストール]セクションで、現在の状態が「のインストール開始準備完了」であることを確認します *node name* をプライマリ管理ノードでグリッドに追加します *admin_ip* "*インストールの開始*ボタンが有効になっていることを確認します。

   [Start Installation* （インストールの開始） ] ボタンが有効になっていない場合は、ネットワーク設定またはポート設定の変更が必要になることがあります。手順については、使用しているアプライアンスのインストールとメンテナンスの手順を参照してください。

   ストレージノードアプライアンスをノードクローニングターゲットとして導入する場合は、ここで導入プロセスを停止して、リカバリとメンテナンスのためにノードクローニング手順 を継続します。[+]""

6. StorageGRID アプライアンスインストーラのホームページで、 * インストールの開始 * をクリックします。

   現在の状態が「 Installation is in progress 」に変わり、「 Monitor Installation 」ページが表示されます。

   モニタのインストールページに手動でアクセスする必要がある場合は、 * モニタのインストール * をクリックします。

7. グリッドに複数のアプライアンスストレージノードがある場合は、アプライアンスごとに上記の手順を繰り返します。

> 一度に複数のアプライアンスストレージノードを導入する必要がある場合は、を使用してインストールプロセスを自動化できます `configure-sga.py` アプライアンスインストールスクリプト。このスクリプトはストレージノードにのみ適用されます。

関連情報

"グリッドを展開します"

""

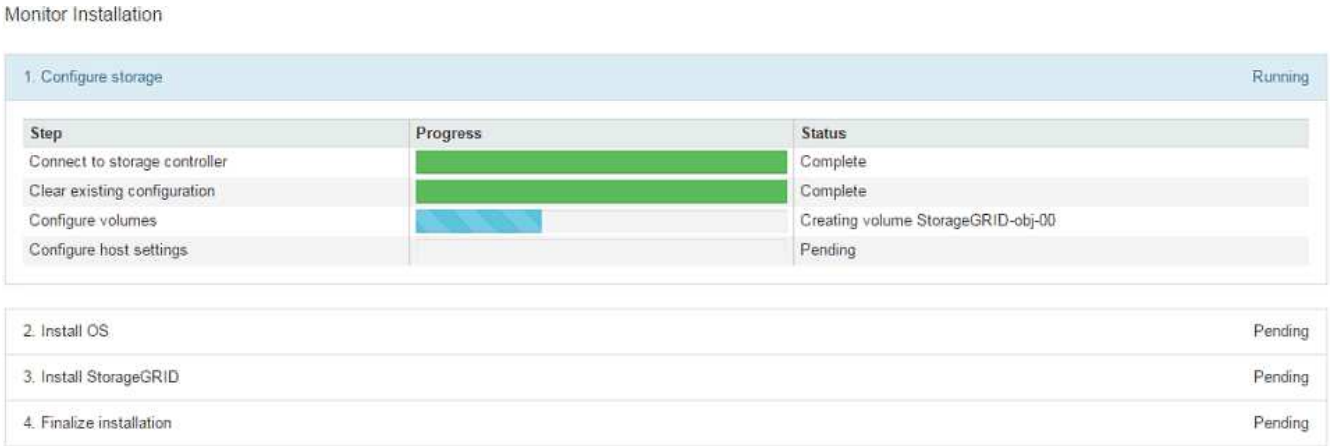
## ストレージアプライアンスのインストールの監視

StorageGRID アプライアンスインストーラでは、インストールが完了するまでステータスが提供されます。ソフトウェアのインストールが完了すると、アプライアンスがリブートされます。

手順

1. インストールの進行状況を監視するには、 * インストールの監視 * をクリックします。

   Monitor Installation ページにインストールの進行状況が表示されます。




   青色のステータスバーは、現在進行中のタスクを示します。緑のステータスバーは、正常に完了したタスクを示します。

> インストーラは、以前のインストールで完了したタスクが再実行されないようにします。インストールを再実行している場合 ' 再実行する必要のないタスクは ' 緑色のステータスバーとステータスが [ スキップ済み ] と表示されます

2. インストールの最初の 2 つのステージの進行状況を確認します。

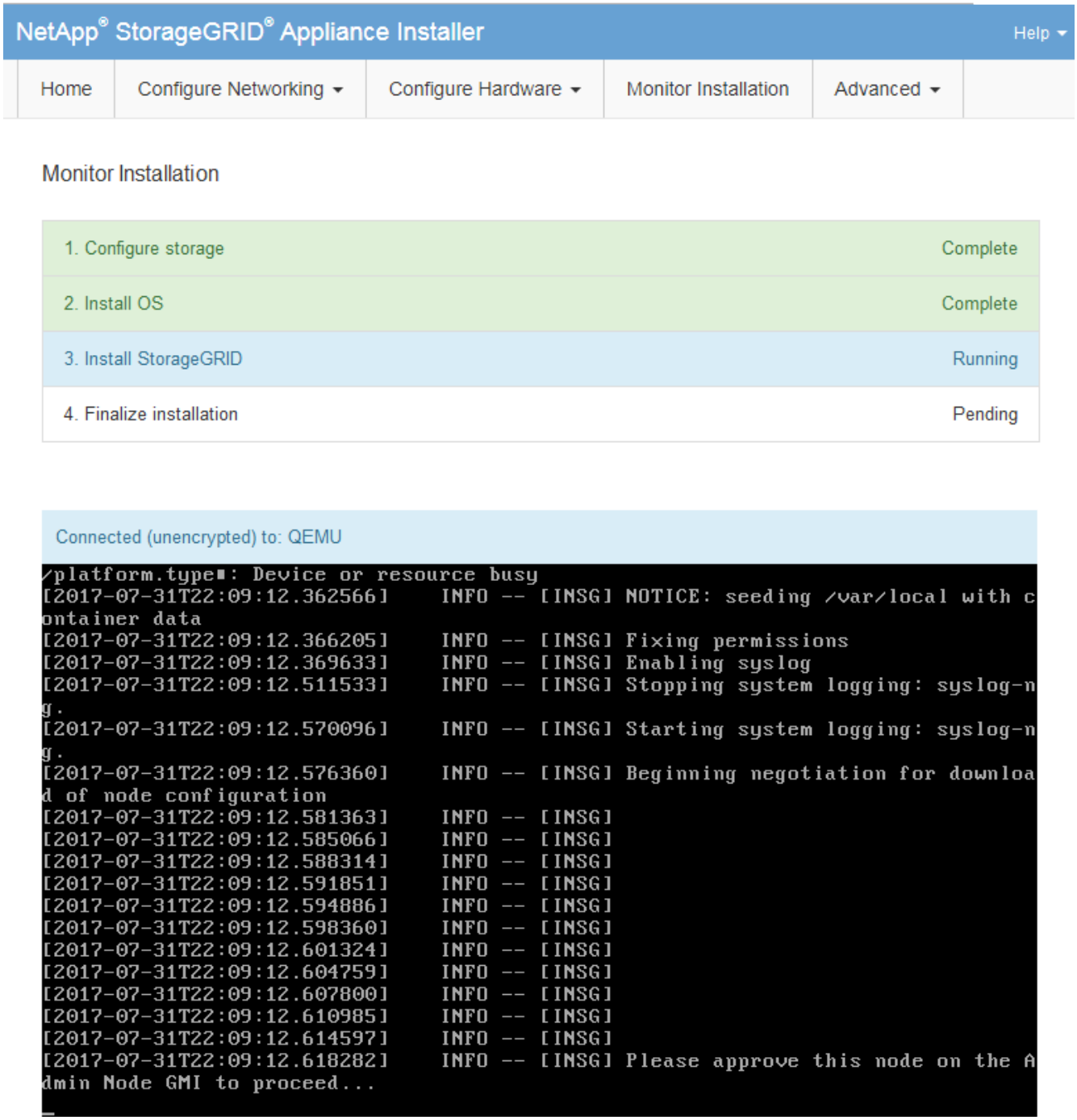
   ◦ 1 。ストレージの構成 *

   インストーラがストレージコントローラに接続し、既存の設定があれば消去し、 SANtricity ソフトウェアと通信してボリュームを設定し、ホストを設定します。

※ 2OS * をインストールします

インストーラが StorageGRID のベースとなるオペレーティングシステムイメージをアプライアンスにコピーします。

3. インストールの進行状況の監視を継続して、組み込みコンソールに「 Install StorageGRID * 」ステージが一時停止し、グリッドマネージャを使用して管理ノードでこのノードを承認するように求めるメッセージが表示されるまで続けます。次の手順に進みます。




4. グリッドマネージャに移動し、保留中のストレージノードを承認して、StorageGRID のインストールプロセスを完了します。

Grid Manager から * Install * をクリックすると、ステージ 3 が完了し、ステージ 4 * Finalize Installation *

が開始されます。ステージ 4 が完了すると、コントローラがリブートされます。

## アプライアンスのインストールと設定の自動化

### アプライアンスのインストールと設定、および StorageGRID システム全体の設定を自動化することができます。

このタスクについて

インストールと設定を自動化すると、複数の StorageGRID インスタンス、または大規模で複雑な StorageGRID インスタンスを 1 つ導入する場合に便利です。

インストールと設定を自動化するには、次のオプションを 1 つ以上使用します。

- アプライアンスの構成設定を指定した JSON ファイルを作成します。StorageGRID アプライアンスインストーラを使用して JSON ファイルをアップロードします。

  同じファイルを使用して、複数のアプライアンスを設定できます。

- StorageGRID を使用します`configure-sga.py` アプライアンスの設定を自動化するPythonスクリプト。
- 追加の Python スクリプトを使用して、 StorageGRID システム全体の他のコンポーネント（「グリッド」）を設定します。

Python スクリプトを StorageGRID 自動化で直接使用することも、 StorageGRID インストール REST API を独自に開発するグリッド導入および設定ツールで使用する例として使用することもできます。リカバリとメンテナンスの手順のStorageGRID インストールファイルのダウンロードと展開に関する情報を参照してください。

**StorageGRID** アプライアンスインストーラを使用したアプライアンス設定の自動化

### 設定情報を含む JSON ファイルを使用して、アプライアンスの設定を自動化することができます。ファイルは StorageGRID アプライアンスインストーラを使用してアップロードします。

必要なもの

- アプライアンスは、 StorageGRID 11.5 以降と互換性のある最新のファームウェアを使用している必要があります。
- 設定するアプライアンスのStorageGRID アプライアンスインストーラに、サポートされているブラウザを使用して接続する必要があります。

このタスクについて

次の設定など、アプライアンスの設定作業を自動化することができます。

- グリッドネットワーク、管理ネットワーク、およびクライアントネットワークの IP アドレス
- BMC インターフェイス
- ネットワークリンク
  - ポートボンディングモード

- ネットワークボンディングモード
- リンク速度

アップロードした JSON ファイルを使用してアプライアンスを設定する方が、 StorageGRID アプライアンスインストーラの複数のページを使用して手動で設定を行うよりも効率的です。特に、多数のノードを設定する必要がある場合は効果的です。構成ファイルはノードごとに 1 つずつ適用する必要があります。

> アプライアンスのインストールと設定の両方を自動化したいと考えている経験豊富なユーザが、を使用できます `configure-sga.py` スクリプト：[+]"configure-sga.pyスクリプトを使用して、アプライアンスノードのインストールと設定を自動化する"

手順

1. 次のいずれかの方法で JSON ファイルを生成します。
   - ConfigBuilder アプリケーション

     "ConfigBuilder.netapp.com"

   - 。 `configure-sga.py` アプライアンス設定スクリプト。スクリプトは、 StorageGRID アプライアンスインストーラ（ * Help * > * アプライアンス構成スクリプト * ）からダウンロードできます。configure-sga.py スクリプトを使用して設定を自動化する手順を参照してください。

     "configure-sga.pyスクリプトを使用して、アプライアンスノードのインストールと設定を自動化する"

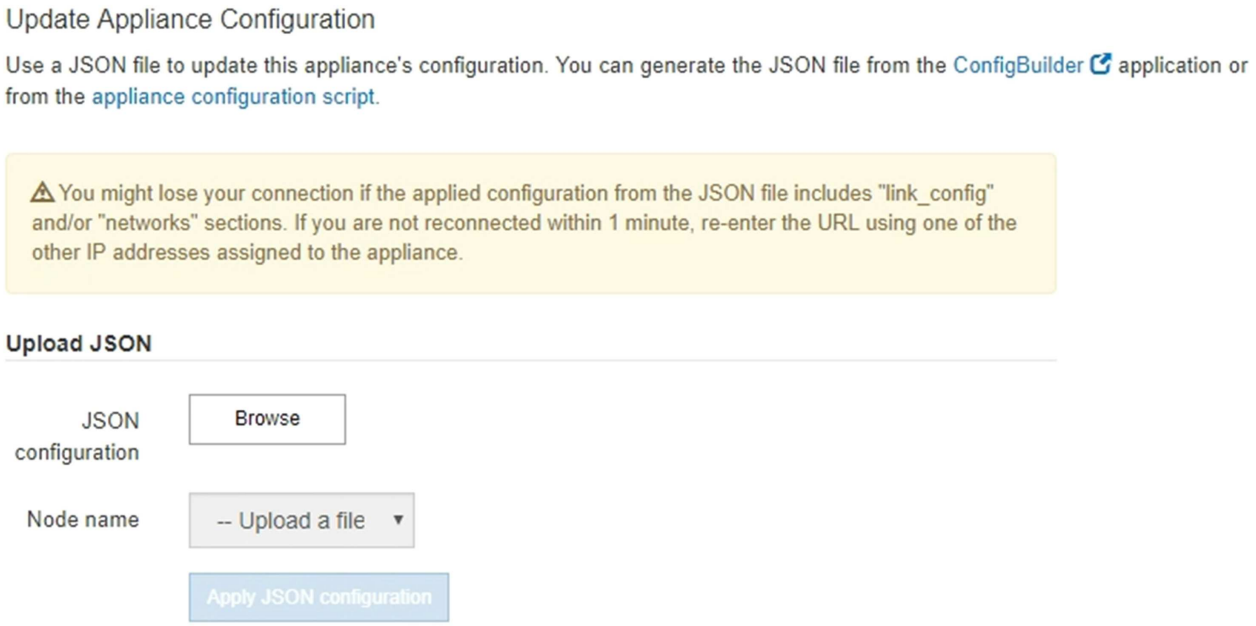
     JSON ファイル内のノード名は、次の要件に従う必要があります。

   - 1 文字以上 32 文字以下の有効なホスト名を指定する必要があります
   - アルファベット、数字、およびハイフンを使用できます
   - 1文字目または最後の文字をハイフンにすることはできません。また、数字だけを使用すること

     > JSON ファイル内のノード名（最上位の名前）が一意であることを確認してください。一意でないと、 JSON ファイルを使用して複数のノードを設定できません。

2. 「 * Advanced * > * Update Appliance Configuration * 」を選択します。

   [Update Appliance Configuration] ページが表示されます。




3. アップロードする設定の JSON ファイルを選択します。

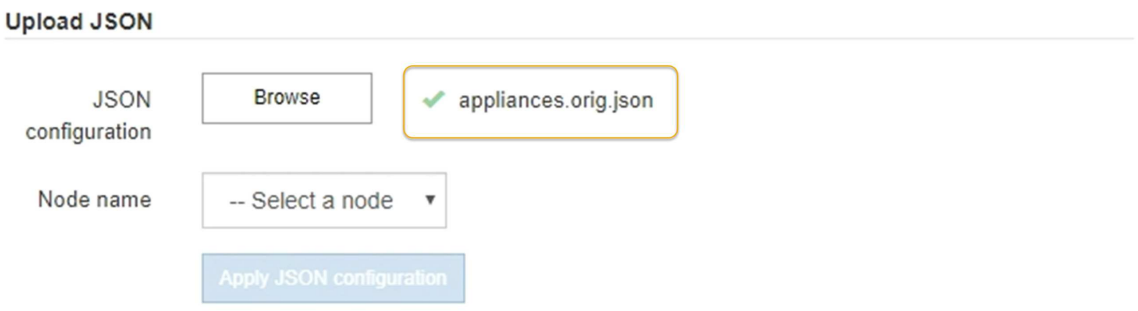
   a. [ * 参照 * ] を選択します。

   b. ファイルを探して選択します。

   c. 「 * 開く * 」を選択します。

   ファイルがアップロードされて検証されます。検証プロセスが完了すると、ファイル名が緑色のチェックマークの横に表示されます。

   > JSON ファイルの構成に「 link_config 」、「 networks 」、またはその両方のセクションが含まれている場合は、アプライアンスへの接続が失われる可能性があります。1 分以内に再接続されない場合は、アプライアンスに割り当てられている他の IP アドレスのいずれかを使用して、アプライアンスの URL を再入力します。

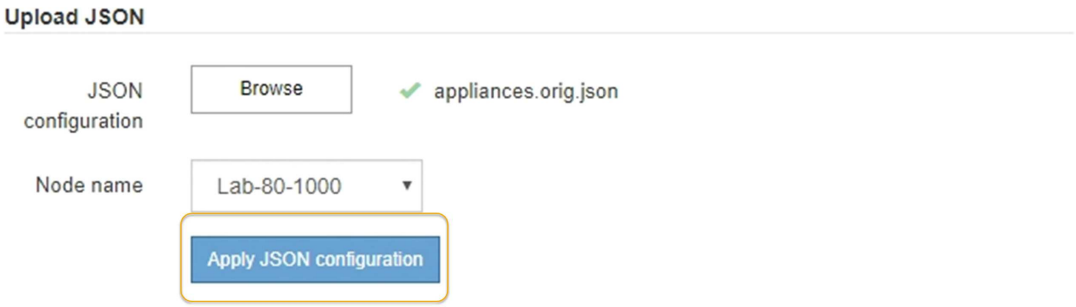



   ノード名 * ドロップダウンには、 JSON ファイルで定義された最上位のノード名が表示されます。

ファイルが有効でない場合、ファイル名は赤色で表示され、黄色のバナーにエラーメッセージが表示されます。無効なファイルはアプライアンスに適用されません。ConfigBuilder を使用して、有効な JSON ファイルを作成できます。

4. ノード名 * ドロップダウンのリストからノードを選択します。

   Apply JSON configuration * ボタンが有効になっている。




5. Apply JSON configuration * を選択します。

   選択したノードに構成が適用されます。

**configure-sga.py**スクリプトを使用して、アプライアンスノードのインストールと設定を自動化する

を使用できます `configure-sga.py` プライマリ管理ノードのインストールや設定など、StorageGRID アプライアンスノードのインストールタスクや設定タスクの多くを自動化するスクリプトです。このスクリプトは、設定するアプライアンスが多数ある場合に役立ちます。スクリプトを使用して、アプライアンスの設定情報を含む JSON ファイルを生成することもできます。

必要なもの

- アプライアンスをラックに設置し、ネットワークに接続し、電源を投入しておきます。
- StorageGRID アプライアンスインストーラを使用してプライマリ管理ノードのネットワークリンクと IP アドレスを設定しておきます。
- プライマリ管理ノードをインストールする場合は、その IP アドレスを確認しておきます。
- 他のノードをインストールして設定する場合は、プライマリ管理ノードが導入され、その IP アドレスを確認しておきます。
- プライマリ管理ノード以外のすべてのノードについて、 StorageGRID アプライアンスインストーラの IP 設定ページに表示されるすべてのグリッドネットワークサブネットが、プライマリ管理ノードのグリッドネットワークサブネットリストで定義されている。
- をダウンロードしておきます `configure-sga.py` ファイル。このファイルはインストール・アーカイブに含まれています。または、 StorageGRID アプライアンス・インストーラの * Help * > * Appliance Installation Script * をクリックしてアクセスできます。

この手順 は、コマンドラインインターフェイスを使用した経験のある上級ユーザを対象としています。また、 StorageGRID アプライアンスインストーラを使用して設定を自動化することもできます。[+]"StorageGRID アプライアンスインストーラを使用したアプライアンス設定の自動化"

手順

1. Python スクリプトを実行するために使用する Linux マシンにログインします。
2. スクリプト構文に関する一般的なヘルプおよび使用可能なパラメータの一覧を表示するには、次のように入力します。

```
configure-sga.py --help
```

   。 `configure-sga.py` スクリプトでは、次の5つのサブコマンド

   - `advanced` BMCの設定、アプライアンスの現在の設定を含むJSONファイルの作成など、StorageGRID アプライアンスの高度な操作用
   - `configure` RAIDモード、ノード名、およびネットワークパラメータを設定するために使用します
   - `install` StorageGRID のインストールを開始する場合に使用します
   - `monitor` StorageGRID インストールの監視用です
   - `reboot` アプライアンスのリブート用です

   サブコマンド（advanced、configure、install、monitor、またはreboot）引数のあとにを入力すると `--help` オプションを指定すると、そのサブコマンド内で使用可能なオプションの詳細を示すヘルプテキストが表示されます
   `configure-sga.py` *`subcommand`* `--help`

3. アプライアンスノードの現在の設定を確認するには、以下のコマンドをどこに入力するかを確認します *`SGA-install-ip`* には、アプライアンスノードのいずれかのIPアドレスを指定します。+
   `configure-sga.py configure` *`SGA-INSTALL-IP`*

   この結果には、プライマリ管理ノードの IP アドレスや管理、グリッド、クライアントネットワークに関する情報など、アプライアンスの現在の IP 情報が表示されます。

```
Connecting to +https://10.224.2.30:8443+ (Checking version and
connectivity.)
2021/02/25 16:25:11: Performing GET on /api/versions... Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/system-info... Received
200
2021/02/25 16:25:11: Performing GET on /api/v2/admin-connection...
Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/link-config... Received
200
2021/02/25 16:25:11: Performing GET on /api/v2/networks... Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/system-config... Received
200
```

```
StorageGRID Appliance
  Name:        LAB-SGA-2-30
  Node type:   storage

StorageGRID primary Admin Node
  IP:        172.16.1.170
  State:     unknown
  Message:   Initializing...
  Version:   Unknown

Network Link Configuration
  Link Status
        Link      State      Speed (Gbps)
        ----      -----      -----
        1         Up         10
        2         Up         10
        3         Up         10
        4         Up         10
        5         Up         1
        6         Down       N/A

  Link Settings
      Port bond mode:      FIXED
      Link speed:          10GBE

      Grid Network:        ENABLED
          Bonding mode:    active-backup
          VLAN:            novlan
          MAC Addresses:   00:a0:98:59:8e:8a  00:a0:98:59:8e:82

      Admin Network:       ENABLED
          Bonding mode:    no-bond
          MAC Addresses:   00:80:e5:29:70:f4

      Client Network:      ENABLED
          Bonding mode:    active-backup
          VLAN:            novlan
          MAC Addresses:   00:a0:98:59:8e:89  00:a0:98:59:8e:81

Grid Network
  CIDR:      172.16.2.30/21 (Static)
  MAC:       00:A0:98:59:8E:8A
  Gateway:   172.16.0.1
  Subnets:   172.17.0.0/21
             172.18.0.0/21
```

```
                192.168.0.0/21
    MTU:        1500

  Admin Network
    CIDR:       10.224.2.30/21 (Static)
    MAC:        00:80:E5:29:70:F4
    Gateway:    10.224.0.1
    Subnets:    10.0.0.0/8
                172.19.0.0/16
                172.21.0.0/16
    MTU:        1500

  Client Network
    CIDR:       47.47.2.30/21 (Static)
    MAC:        00:A0:98:59:8E:89
    Gateway:    47.47.0.1
    MTU:        2000

#####################################################################
#####   If you are satisfied with this configuration,    #####
##### execute the script with the "install" sub-command. #####
#####################################################################
```

4. 現在の設定のいずれかの値を変更する必要がある場合は、を使用します `configure` サブコマンドを使用して更新します。たとえば、アプライアンスがプライマリ管理ノードへの接続に使用するIPアドレスをに変更する場合などです `172.16.2.99`をクリックし、「+」と入力します
`configure-sga.py configure --admin-ip 172.16.2.99 SGA-INSTALL-IP`
5. アプライアンスの設定をJSONファイルにバックアップする場合は、を使用します `advanced` および `backup-file` サブコマンド。たとえば、IPアドレスを持つアプライアンスの設定をバックアップする場合などです *SGA-INSTALL-IP* を指定します `appliance-SG1000.json`をクリックし、「+」と入力します
`configure-sga.py advanced --backup-file appliance-SG1000.json SGA-INSTALL-IP`

   設定情報が格納された JSON ファイルは、スクリプトの実行元と同じディレクトリに書き込まれます。

   > 生成された JSON ファイルの最上位のノード名がアプライアンス名と一致していることを確認します。経験豊富なユーザで StorageGRID API について十分な知識がある場合を除き、このファイルに変更を加えないでください。

6. アプライアンスの設定に問題がなければ、を使用します `install` および `monitor` アプライアンスをインストールするためのサブコマンド：+
`configure-sga.py install --monitor SGA-INSTALL-IP`
7. アプライアンスをリブートする場合は、「+」を入力します
`configure-sga.py reboot SGA-INSTALL-IP`

# グリッドノードを導入したら、 StorageGRID システムの設定を自動化できます。

必要なもの

- インストールアーカイブにある次のファイルの場所を確認しておきます。

| ファイル名 | 説明 |
| --- | --- |
| `configure-storagegrid.py` | 設定を自動化するための Python スクリプト |
| `configure-storagegrid.sample.json` | スクリプトで使用するサンプル構成ファイル |
| `configure-storagegrid.blank.json` | スクリプトで使用する空の構成ファイルです |

- を作成しておきます `configure-storagegrid.json` 構成ファイルこのファイルを作成するには、サンプル構成ファイルを変更します (`configure-storagegrid.sample.json`)または空の構成ファイル (`configure-storagegrid.blank.json`) 。

このタスクについて

を使用できます `configure-storagegrid.py` Pythonスクリプトおよび `configure-storagegrid.json` StorageGRID システムの設定を自動化するための構成ファイル。

また、 Grid Manager またはインストール API を使用してシステムを設定することもできます。

手順

1. Python スクリプトを実行するために使用する Linux マシンにログインします。
2. インストールアーカイブを展開したディレクトリに移動します。

   たとえば、「+」と入力します
   `cd StorageGRID-Webscale-version/platform`

   ここで、 *platform* はです `debs`、 `rpms`または `vsphere`。

3. Python スクリプトを実行し、作成した構成ファイルを使用します。

   例：

```
./configure-storagegrid.py ./configure-storagegrid.json --start-install
```

完了後

リカバリパッケージ `.zip` 設定プロセスでファイルが生成され、インストールと設定を実行するディレクトリにダウンロードされます。グリッドノードで障害が発生した場合に StorageGRID システムをリカバリできるようにするために、リカバリパッケージファイルをバックアップする必要があります。たとえば、バックアップされたセキュアなネットワーク上の場所や、安全なクラウドストレージ上の場所にコピーします。

リカバリパッケージファイルには StorageGRID システムからデータを取得するための暗号キーとパスワードが含まれているため、安全に保管する必要があります。

ランダムパスワードを生成するように指定した場合は、を展開する必要があります `Passwords.txt` ファイルを開き、StorageGRID システムへのアクセスに必要なパスワードを探します。

```
######################################################################
##### The StorageGRID "recovery package" has been downloaded as: #####
#####           ./sgws-recovery-package-994078-rev1.zip          #####
#####   Safeguard this file as it will be needed in case of a    #####
#####                 StorageGRID node recovery.                 #####
######################################################################
```

StorageGRID システムがインストールおよび設定されると、確認メッセージが表示されます。

```
StorageGRID has been configured and installed.
```

## インストール **REST API** の概要

StorageGRID には、インストールタスクを実行するための REST API として、StorageGRID インストール API と StorageGRID アプライアンスインストーラ API の 2 つが用意されています。

どちらの API も、 Swagger オープンソース API プラットフォームを使用して API のドキュメントを提供しています。Swagger では、ユーザインターフェイスを使用してパラメータやオプションを変更した場合の API の動作を確認しながら、 API の開発を進めることができます。このドキュメントは、標準的な Web テクノロジと JavaScript Object Notation （ JSON ）データ形式について十分理解していることを前提としています。

API Docs Web ページを使用して実行する API 処理はすべてその場で実行されます。設定データやその他のデータを誤って作成、更新、または削除しないように注意してください。

各 REST API コマンドは、 API の URL 、 HTTP アクション、必須またはオプションの URL パラメータ、および想定される API 応答で構成されます。

### **StorageGRID** インストール **API**

StorageGRID インストール API は、 StorageGRID システムを最初に設定するとき、およびプライマリ管理ノードのリカバリを実行する必要がある場合にのみ使用できます。インストール API には、 Grid Manager から HTTPS 経由でアクセスできます。

API のドキュメントにアクセスするには、プライマリ管理ノードのインストール用 Web ページに移動し、メニューバーから * Help * > * API Documentation * を選択します。

StorageGRID インストール API には次のセクションがあります。

- *config *-- API の製品リリースとバージョンに関連する操作。製品リリースバージョンおよびそのリリースでサポートされる API のメジャーバージョンを一覧表示できます。

- * grid * — グリッドレベルの設定操作。グリッドの詳細、グリッドネットワークのサブネット、グリッドパスワード、 NTP および DNS サーバの IP アドレスなど、グリッド設定を取得および更新できます。
- *nodes * — ノードレベルの設定操作。グリッドノードのリストを取得できるほか、グリッドノードの削除、設定、表示、およびグリッドノードの設定のリセットを行うことができます。
- *provision * — プロビジョニング操作。プロビジョニング処理を開始し、プロビジョニング処理のステータスを表示できます。
- * recovery * - プライマリ管理ノードのリカバリ処理。情報のリセット、リカバリパッケージのアップロード、リカバリの開始、およびリカバリ処理のステータスの表示を行うことができます。
- * recovery-package * — リカバリパッケージをダウンロードする処理。
- *sites * — サイトレベルの設定操作。サイトを作成、表示、削除、および変更できます。

**StorageGRID** アプライアンスインストーラ **API**

StorageGRID アプライアンスインストーラAPIには、からHTTPS経由でアクセスできます `Controller_IP:8443`。

API ドキュメントにアクセスするには、アプライアンスの StorageGRID アプライアンスインストーラのメニューバーから * Help * > * API Docs * を選択します。

StorageGRID アプライアンスインストーラ API には、次のセクションがあります。

- * clone * — ノードのクローニングを構成および制御するための処理。
- *encryption * — 暗号化を管理し、暗号化ステータスを表示するための処理。
- * ハードウェア構成 * — 接続されたハードウェアでシステム設定を構成するための操作。
- *installation * ：アプライアンスのインストールを開始し、インストール・ステータスを監視するための処理。
- * networking * — StorageGRID アプライアンスのグリッドネットワーク、管理ネットワーク、クライアントネットワークの設定、およびアプライアンスのポート設定に関連する処理です。
- * setup * - システムに関する情報の取得やプライマリ管理ノード IP の更新要求など、アプライアンスの初期インストール設定に役立つ処理。
- *support *--コントローラのリブートとログ取得のための処理。
- * upgrade * ：アプライアンス・ファームウェアのアップグレードに関連する操作
- **uploadsg** — StorageGRID インストールファイルをアップロードするための操作。

## ハードウェアの設置のトラブルシューティング

設置作業で問題が発生した場合は、ハードウェアのセットアップや接続の問題に関するトラブルシューティング情報を確認すると役立つことがあります。

関連情報

"ハードウェアのセットアップがハングしたように見えます"

"接続の問題のトラブルシューティング"

**SG6000-CN**コントローラのブート時のコードを確認する

# アプライアンスの電源を入れると、 BMC は SG6000-CN コントローラの一連のブート時のコードを記録します。これらのコードはいくつかの方法で確認できます。

必要なもの

- BMC ダッシュボードへのアクセス方法を確認しておく必要があります。
- Kernel-based Virtual Machine（KVM）を使用する場合は、KVMアプリケーションの導入および使用経験が必要です。
- Serial-Over-LAN （ SOL ）を使用する場合は、 IPMI SOL コンソールアプリケーションの使用経験が必要です。

手順

1. アプライアンスコントローラのブート時のコードを確認するための方法を選択し、必要な機器を揃えます。

| メソッド | 必要な機器 |
| --- | --- |
| VGA コンソール | • VGA 対応モニタ<br>• VGA ケーブル |
| KVM の略 | • KVMアプリケーション<br>• RJ-45 ケーブル |
| シリアルポート | • DB-9 シリアルケーブル<br>• 仮想シリアルターミナル |
| ソル | • 仮想シリアルターミナル |

2. VGA コンソールを使用する場合は、次の手順を実行します。
   a. VGA 対応モニタをアプライアンス背面の VGA ポートに接続します。
   b. モニタに表示されるコードを確認します。
3. BMC KVM を使用する場合は、次の手順を実行します。
   a. BMC 管理ポートに接続し、 BMC の Web インターフェイスにログインします。
   b. 「 * リモートコントロール * 」を選択します。
   c. KVM を起動します。
   d. 仮想モニタのコードを確認します。
4. シリアルポートと端末を使用している場合は、次の手順を実行します。
   a. アプライアンス背面の DB-9 シリアルポートに接続します。
   b. 設定を使用します `115200 8-N-1`。
   c. シリアルターミナルに印刷されているコードを確認します。

5. SOL を使用する場合は、次の手順を実行します。
   a. BMC の IP アドレスとログインクレデンシャルを使用して IPMI SOL に接続します。

      ```
      ipmitool -I lanplus -H 10.224.3.91 -U root -P calvin sol activate
      ```

   b. 仮想シリアルターミナルのコードを確認します。
6. 次の表を使用して、アプライアンスのコードを確認します。

| コード | を示します |
| --- | --- |
| こんにちは | マスターブートスクリプトが開始されました。 |
| HP | ネットワークインターフェイスカード（ NIC ）の更新が必要かどうかをシステムがチェックしています。 |
| 朝食付き | ファームウェアの更新の適用が完了し、システムがリブートしています。 |
| FP | ハードウェアサブシステムのファームウェアの更新の確認が完了しました。コントローラ間の通信サービスが開始されています。 |
| 彼 | アプライアンスストレージノードの場合のみ：<br><br>システムがストレージコントローラとの接続待ちで、 SANtricity オペレーティングシステムと同期しています。<br><br>• 注：この段階でブート手順 が進行しない場合は、次の手順を実行します。<br>a. SG6000-CN コントローラと 2 台のストレージコントローラの間の 4 本のインターコネクトケーブルがしっかり接続されていることを確認します。<br>b. 必要に応じて、 1 本以上のケーブルを交換し、再試行します。<br>c. この方法で問題 が解決しない場合は、テクニカルサポートにお問い合わせください。 |
| HC | 既存の StorageGRID のインストールデータがチェックされています。 |
| HO | StorageGRID アプライアンスインストーラが実行されている。 |
| 高可用性 | StorageGRID が実行されています。 |

**SG6000-CN**コントローラのエラーコードの確認

SG6000-CN コントローラのブート時にハードウェアエラーが発生すると、 BMC にエラーコードが記録されます。必要に応じて BMC インターフェイスを使用してこれらのエラーコードを確認し、テクニカルサポートと協力して問題 を解決できます。

必要なもの

- BMC ダッシュボードへのアクセス方法を確認しておく必要があります。

手順

1. BMC ダッシュボードで、 * BIOS POST Code * を選択します。
2. 現在のコードと前のコードについて表示された情報を確認します。

   次のいずれかのエラーコードが表示された場合は、テクニカルサポートに連絡して問題 を解決してください。

| コード | を示します |
| --- | --- |
| 0x0E | マイクロコードが見つかりません |
| 0x0F | マイクロコードがロードされません |
| 0x50 | メモリの初期化エラー。メモリタイプが無効か、メモリ速度に互換性がありません。 |
| 0x51 | メモリの初期化エラー。SPD の読み取りに失敗しました。 |
| 0x52 | メモリの初期化エラー。メモリサイズが無効か、メモリモジュールが一致しません。 |
| 0x53 | メモリの初期化エラー。使用可能なメモリが検出されませんでし |
| 0x54 | 不明なメモリ初期化エラー |
| 0x55 | メモリが取り付けられていません |
| 0x56 | CPU のタイプまたは速度が無効です |
| 0x57 | CPU が一致しません |
| 0x58 | CPU セルフテストに失敗したか、 CPU キャッシュエラーの可能性があります |

| コード | を示します |
| --- | --- |
| 0x59 | CPU マイクロコードが見つからないか、マイクロコードの更新に失敗しました |
| 0x5A | 内部 CPU エラー |
| 0x5B | リセット PPI が使用できません |
| 0x5C | PEI フェーズの BMC セルフテストに失敗しました |
| 0xD0 | CPU の初期化エラー |
| 0xD1 | ノースブリッジの初期化エラー |
| 0xD2 | サウスブリッジの初期化エラー |
| 0xd3 | 一部のアーキテクチャプロトコルが使用できません |
| 0xD4 | PCI リソースの割り当てエラー。リソース不足です。 |
| 0xD5 | レガシーオプション ROM 用のスペースがありません |
| 0xD6 | コンソール出力デバイスが見つかりません |
| 0xD7 | コンソール入力デバイスが見つかりません |
| 0xD8 | パスワードが無効です |
| 0xD9 | ブートオプションのロードエラー（ LoadImage がエラーを返しました） |
| 0xda | ブートオプションが失敗しました（ StartImage がエラーを返しました）。 |
| 0xDB | フラッシュの更新に失敗しました |
| 0xDC | リセットプロトコルは使用できません |
| 0xDD | DXE フェーズの BMC セルフテストに失敗しました |
| 0xE8 | MRC ： ERR_NO_MEMORY |

| コード | を示します |
| --- | --- |
| 0xE9 | MRC ： ERR_LT_LOCK |
| 0xEA | MRC ： ERR_DDR_INIT |
| 0xEB | MRC ： ERR_MEM_TEST |
| 0xEC | MRC ： ERR_VENDER_Specific |
| 0xED | MRC ： ERR_DIMM_COMPAT |
| 0xEE | MRC ： ERR_MRC_compatibility |
| 0xef | MRC ： ERR_MRC_STRUCT |
| 0xF0 | MRC ： ERR_SET_VDD |
| 0xf1 | MRC ： ERR_IOT_MEM_BUFFER |
| 0xF2 | MRC ： ERR_RC_INTERNAL |
| 0xF3 | MRC ： ERR_INVALL_REG_ACCESS |
| 0xF4 | MRC ： ERR_SET_MC_Freq |
| 0xf5 | MRC ： ERR_READ_MC_Freq |
| 0x70 | MRC ： ERR_DIMM_CHANNEL |
| 0x74 | MRC ： ERR_BIST チェック |
| 0xF6 | MRC ： ERR_SMBus |
| 0xF7 | MRC ： ERR_PCU |
| 0xf8 | MRC ： ERR_NGN |
| 0xF9 | MRC ： ERR_interleave_failure |

ハードウェアのセットアップがハングしたように見えます

## ハードウェア障害やケーブル接続エラーによってストレージコントローラまたは

## SG6000-CN コントローラのブート処理が完了しなかった場合は、 StorageGRID アプライアンスインストーラを使用できなくなることがあります。

手順

1. ストレージコントローラの場合は、デジタル表示ディスプレイのコードを監視します。

   電源投入時にハードウェアが初期化される際に、 2 つのデジタル表示ディスプレイに一連のコードが表示されます。ハードウェアが正常にブートすると、デジタル表示ディスプレイが両方に表示されます `99`。

2. SG6000-CN コントローラの LED と、 BMC に表示されたブート時のコードとエラーコードを確認します。
3. 問題 の解決にサポートが必要な場合は、テクニカルサポートにお問い合わせください。

関連情報

"SG6000ストレージコントローラのブート時のステータスコードを確認する"

"E5700 and E2800 System Monitoring Guide"

"SG6000-CNコントローラのステータスインジケータとボタンの表示"

"SG6000-CNコントローラのブート時のコードを確認する"

"SG6000-CNコントローラのエラーコードの確認"

接続の問題のトラブルシューティング

## StorageGRID アプライアンスのインストール時に接続の問題が発生した場合は、以下に記載する対処策を実施する必要があります。

アプライアンスに接続できません

## アプライアンスに接続できない場合は、ネットワーク問題 があるか、またはハードウェアの設置が正常に完了していない可能性があります。

手順

1. SANtricity システムマネージャに接続できない場合は、次の手順を実行します。
   a. SANtricity システムマネージャの管理ネットワークで、どちらかのストレージコントローラのIPアドレスを使用してアプライアンスにpingを送信します。+
      **`ping Storage_Controller_IP`**
   b. ping からの応答がない場合は、正しい IP アドレスを使用していることを確認します。

      どちらかのストレージコントローラの管理ポート 1 の IP アドレスを使用してください。

   c. IP アドレスが正しい場合は、アプライアンスのケーブル接続とネットワークのセットアップを確認します。

      この手順で問題 が解決しない場合は、テクニカルサポートにお問い合わせください。

   d. ping が成功した場合は、 Web ブラウザを開きます。

e. SANtricity システムマネージャのURLとして「+」を入力します
**https://*Storage_Controller_IP***

SANtricity System Manager のログインページが表示されます。

2. SG6000-CN コントローラに接続できない場合は、次の手順を実行します。

a. SG6000-CNコントローラのIPアドレス+を使用してアプライアンスにpingを送信します
**ping *SG6000-CN_Controller_IP***

b. ping からの応答がない場合は、正しい IP アドレスを使用していることを確認します。

グリッドネットワーク、管理ネットワーク、またはクライアントネットワークでのアプライアンスの IP アドレスを使用できます。

c. IP アドレスが正しい場合は、アプライアンスのケーブル接続、 SFP トランシーバ、およびネットワークのセットアップを確認します。

この手順で問題 が解決しない場合は、テクニカルサポートにお問い合わせください。

d. ping が成功した場合は、 Web ブラウザを開きます。

e. StorageGRID アプライアンスインストーラのURLとして「+」を入力します
**https://*SG6000-CN_Controller_IP*:8443**

ホームページが表示されます。

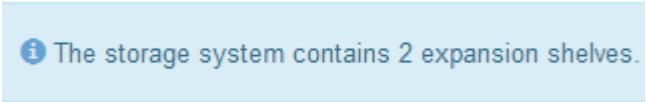
拡張シェルフはアプライアンスインストーラに表示されません

## SG6060 に拡張シェルフが設置されていて、 StorageGRID アプライアンスインストーラに表示されない場合は、シェルフの設置が完了していて、電源がオンになっていることを確認する必要があります。

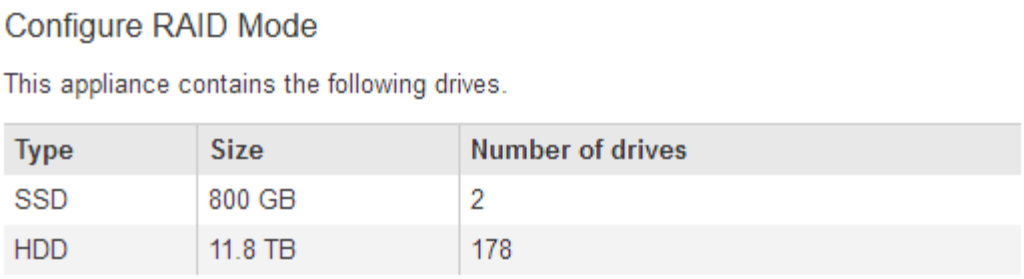
このタスクについて

拡張シェルフがアプライアンスに接続されていることを確認するには、 StorageGRID アプライアンスインストーラで次の情報を表示します。

- ホーム * ページには、拡張シェルフに関するメッセージが表示されます。




- Advanced * > * RAID Mode * ページには、アプライアンスに拡張シェルフが含まれているかどうかをドライブ数で示します。たとえば、以下のスクリーンショットでは、 2 本の SSD と 178 本の HDD が表示されています。2 台の拡張シェルフを備えた SG6060 には、合計 180 本のドライブが搭載されてい




拡張シェルフが存在しないことが StorageGRID アプライアンスインストーラのページに示された場合は、次の手順 を実行します。

手順

1. 必要なすべてのケーブルがしっかりと接続されていることを確認します。
2. 拡張シェルフの電源がオンになっていることを確認します。
3. 問題 の解決にサポートが必要な場合は、テクニカルサポートにお問い合わせください。

関連情報

"SG6060：オプションの拡張シェルフのケーブル接続"

"電源コードの接続と電源の投入（SG6000）"

### **StorageGRID** アプライアンスインストーラの実行中に**SG6000-CN**コントローラをリブートする

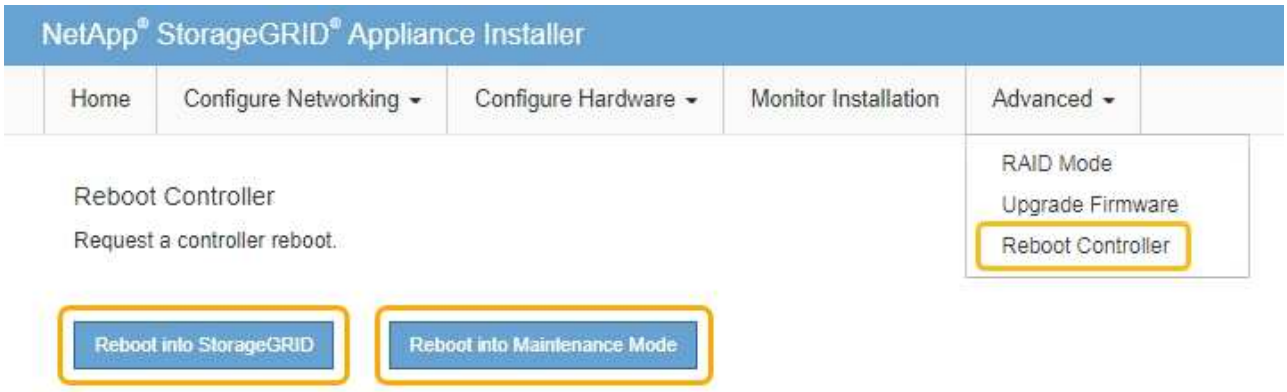
StorageGRID アプライアンスインストーラの実行中に、 SG6000-CN コントローラのリブートが必要になることがあります。たとえば、インストールが失敗した場合は、コントローラのリブートが必要になることがあります。

このタスクについて

この手順 は、 SG6000-CN コントローラで StorageGRID アプライアンスインストーラが実行されている場合にのみ該当します。インストールが完了すると、 StorageGRID アプライアンスインストーラが使用できなくなるため、この手順は機能しなくなります。

手順

1. StorageGRID アプライアンス・インストーラで、 [**Advanced**>*Reboot Controller*] をクリックし、次のいずれかのオプションを選択します。
   - Reboot into StorageGRID * を選択し、ノードをグリッドに再追加してコントローラをリブートします。メンテナンスモードで作業を完了し、ノードを通常動作に戻す準備ができている場合は、このオプションを選択します。
   - メンテナンスモードを維持したままコントローラをリブートするには、 * Reboot into Maintenance Mode * を選択します。このオプションは、グリッドに再追加する前にノードで追加のメンテナンス処理を実行する必要がある場合に選択します。




SG6000-CN コントローラがリブートされます。

## SG6000アプライアンスのメンテナンス

SG6000 アプライアンスでメンテナンス手順を実行する必要がある場合があります。このセクションの手順は、アプライアンスが StorageGRID システムにストレージノードとしてすでに導入されていることを前提としています。

手順

- "アプライアンスをメンテナンスモードにします"
- "ストレージコントローラのSANtricity OSをアップグレードします"
- "SANtricity System Managerを使用してドライブファームウェアをアップグレードする"
- "導入済みのSG6060への拡張シェルフの追加"
- "コントローラ識別LEDのオンとオフの切り替え"
- "コントローラのデータセンターへの配置"
- "ストレージコントローラの交換"
- "ストレージコントローラシェルフのハードウェアコンポーネントの交換"
- "オプションの60ドライブ拡張シェルフのハードウェアコンポーネントの交換"
- "SG6000-CNコントローラをシャットダウンします"
- "SG6000-CNコントローラの電源をオンにして処理を確認します"
- "SG6000-CNコントローラの交換"
- "SG6000-CNコントローラの電源装置の交換"
- "キャビネットまたはラックからのSG6000-CNコントローラの取り外し"
- "キャビネットまたはラックへのSG6000-CNコントローラの再取り付け"
- "SG6000-CNコントローラのカバーの取り外し"
- "SG6000-CNコントローラカバーの再取り付け"
- "SG6000-CNコントローラのFibre Channel HBAの交換"

- "SG6000-CNコントローラのリンク設定を変更する"
- "MTU設定を変更します"
- "DNSサーバの設定を確認しています"
- "メンテナンスモードでのノード暗号化の監視"

アプライアンスをメンテナンスモードにします

## 特定のメンテナンス手順を実行する前に、アプライアンスをメンテナンスモードにする必要があります。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Maintenance または Root Access 権限が必要です。詳細については、 StorageGRID の管理手順を参照してください。

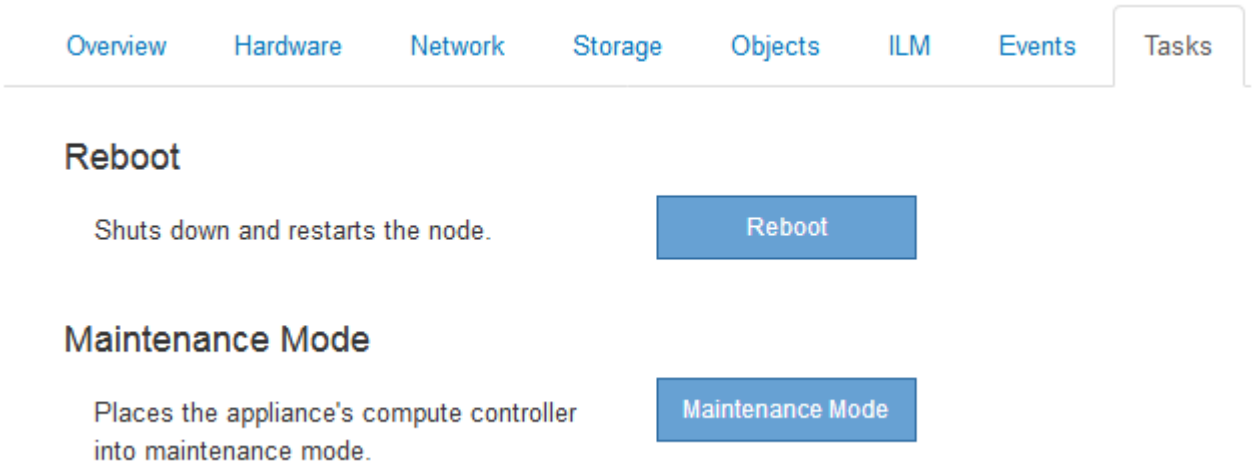
このタスクについて

StorageGRID アプライアンスをメンテナンスモードにすると、アプライアンスにリモートアクセスできなくなることがあります。

保守モードのStorageGRID アプライアンスのパスワードおよびホスト・キーは、アプライアンスが稼働していたときと同じままです。

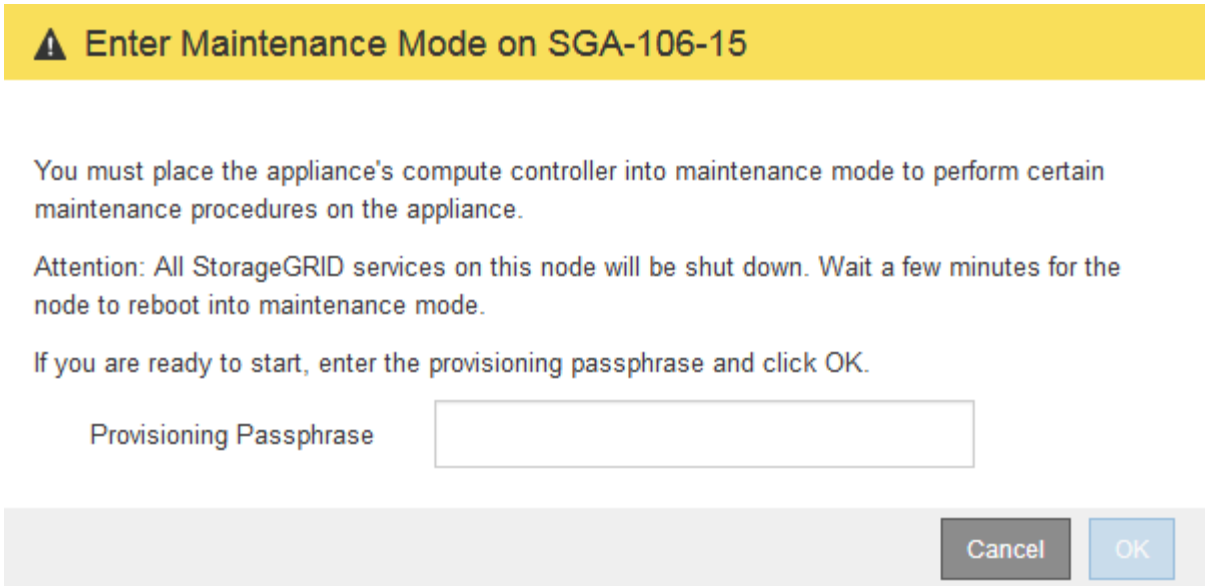
手順

1. Grid Managerから* Nodes *を選択します。
2. Nodes ページのツリービューで、アプライアンスストレージノードを選択します。
3. [ タスク ] を選択します。



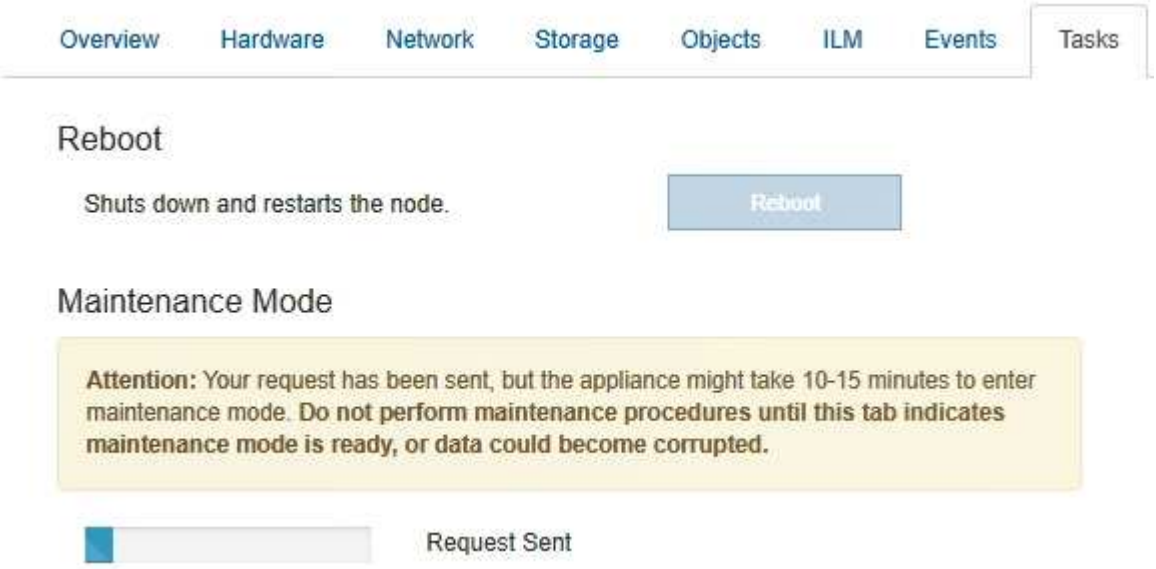

4. [* Maintenance Mode]*を選択します。

   確認のダイアログボックスが表示されます。

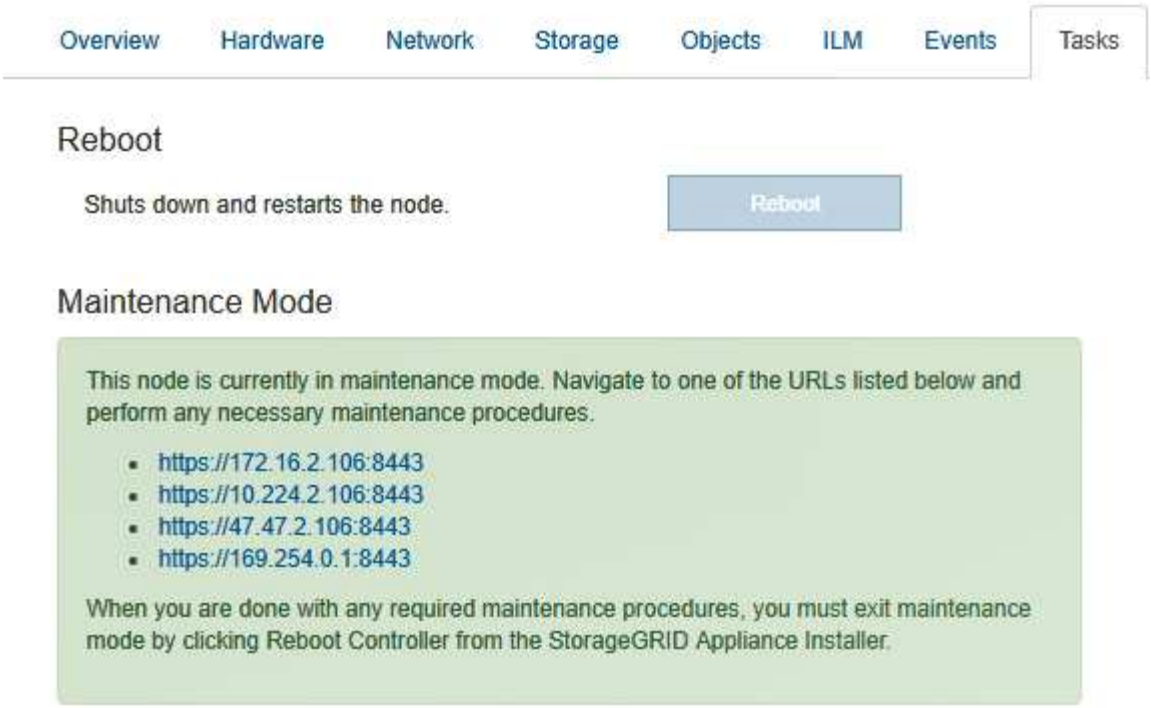



5. プロビジョニングパスフレーズを入力し、「 * OK 」を選択します。

進捗状況バーと一連のメッセージ（「 Request Sent 」、「 Stopping StorageGRID 」、「 Rebaling 」など）は、アプライアンスがメンテナンスモードに入るための手順を完了していることを示しています。




アプライアンスがメンテナンスモードになっている場合は、 StorageGRID アプライアンスインストーラへのアクセスに使用できる URL が確認メッセージに表示されます。



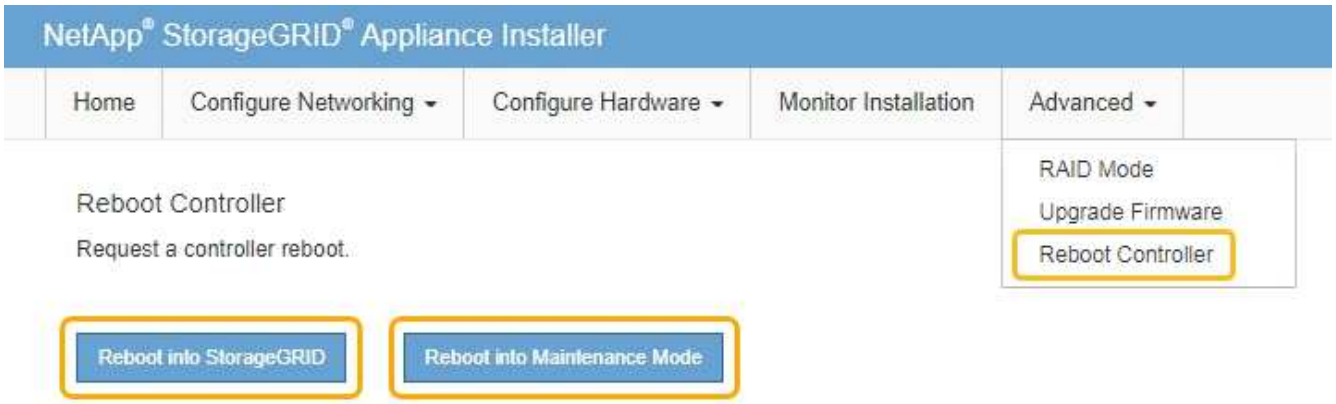

6. StorageGRID アプライアンスインストーラにアクセスするには、表示されたいずれかの URL にアクセスします。

   可能であれば、アプライアンスの管理ネットワークポートの IP アドレスを含む URL を使用します。

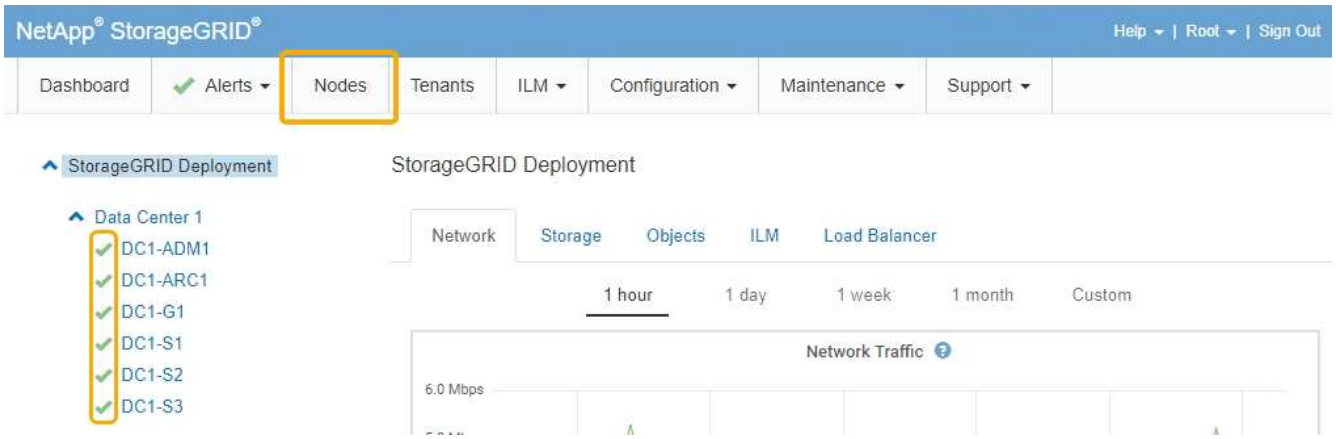
   > へのアクセス `https://169.254.0.1:8443` ローカル管理ポートに直接接続する必要があります。

7. StorageGRID アプライアンスインストーラで、アプライアンスがメンテナンスモードになっていることを確認します。

8. 必要なメンテナンスタスクを実行します。
9. メンテナンス作業が完了したら、メンテナンスモードを終了して通常のノードの運用を再開します。StorageGRID アプライアンス・インストーラから、 **Advanced**>* Reboot Controller* を選択し、 * Reboot into StorageGRID * を選択します。




アプライアンスがリブートしてグリッドに再参加するまでに最大 20 分かかることがあります。リブートが完了し、ノードが再びグリッドに参加したことを確認するには、 Grid Manager に戻ります。[ノード*（Nodes *）]タブには、通常のステータスが表示されます ✔ アクティブなアラートがなく、ノードがグリッドに接続されていることを示す、アプライアンスノードの場合。




ストレージコントローラの**SANtricity OS**をアップグレードします

ストレージコントローラが最適に機能するようにするには、 StorageGRID アプライアンスに対応した最新の SANtricity OS メンテナンスリリースにアップグレードする必要があります。使用するバージョンを確認するには、 NetApp Interoperability Matrix Tool （ IMT ）を参照してください。サポートが必要な場合は、テクニカルサポートにお問い合わせください。

現在インストールされている SANtricity OS のバージョンに応じて、次のいずれかの手順を実行します。

- ストレージコントローラで SANtricity OS 08.42.20.00 （ 11.42 ）以降を使用している場合、 Grid Manager を使用してアップグレードを実行します。

  "グリッドマネージャを使用してストレージコントローラのSANtricity OSをアップグレードします"

- ストレージコントローラで 08.42.20.00 （ 11.42 ）より前のバージョンの SANtricity OS を使用している場合、メンテナンスモードを使用してアップグレードを実行します。

"ストレージコントローラのSANtricity OSをメンテナンスモードでアップグレードします"

ストレージアプライアンスの SANtricity OS をアップグレードするときは、 StorageGRID のドキュメントに記載されている手順に従う必要があります。他の手順を使用すると、アプライアンスが動作しなくなる可能性があります。

関連情報

"NetApp Interoperability Matrix Tool で確認できます"

"ネットアップのダウンロード： SANtricity OS"

"トラブルシューティングを監視します"

グリッドマネージャを使用してストレージコントローラの**SANtricity OS**をアップグレードします

## 現在 SANtricity OS 08.42.20.00 （ 11.42 ）以降を使用しているストレージコントローラの場合、 Grid Manager を使用してアップグレードを適用する必要があります。

必要なもの

- NetApp Interoperability Matrix Tool （ IMT ）を参照して、アップグレードに使用する SANtricity OS のバージョンがお使いのアプライアンスと互換性があることを確認してください。
- Maintenance権限が必要です。
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- プロビジョニングパスフレーズが必要です。
- SANtricity OSに関するネットアップのダウンロードページを利用する必要があります。

このタスクについて

SANtricity OS のアップグレードプロセスが完了するまで、他のソフトウェアの更新（ StorageGRID ソフトウェアのアップグレードまたはホットフィックス）は実行できません。SANtricity OS のアップグレードプロセスが完了する前にホットフィックスや StorageGRID ソフトウェアのアップグレードを開始しようとすると、SANtricity OS のアップグレードページが表示されます。

該当するすべてのノードにSANtricity OSのアップグレードが正常に適用されるまで、手順 は完了しません。各ノードにSANtricity OSがロードされ、各StorageGRID ストレージアプライアンスがリブートされるまでに30分以上かかることがあります。

次の手順は、 Grid Manager を使用してアップグレードを実行する場合にのみ実行できます。08.42.20.00（11.42）より前のSANtricity OSを使用しているコントローラの場合、SG6000シリーズアプライアンスのストレージコントローラをGrid Managerを使用してアップグレードすることはできません。

この手順 は、 SANtricity OS のアップグレードに関連付けられた最新バージョンに NVSRAM を自動的にアップグレードします。個別の NVSRAM アップグレードファイルを適用する必要はありません。

手順

1. サービスラップトップから、NetApp Support Site から新しいSANtricity OSソフトウェアファイルをダウ

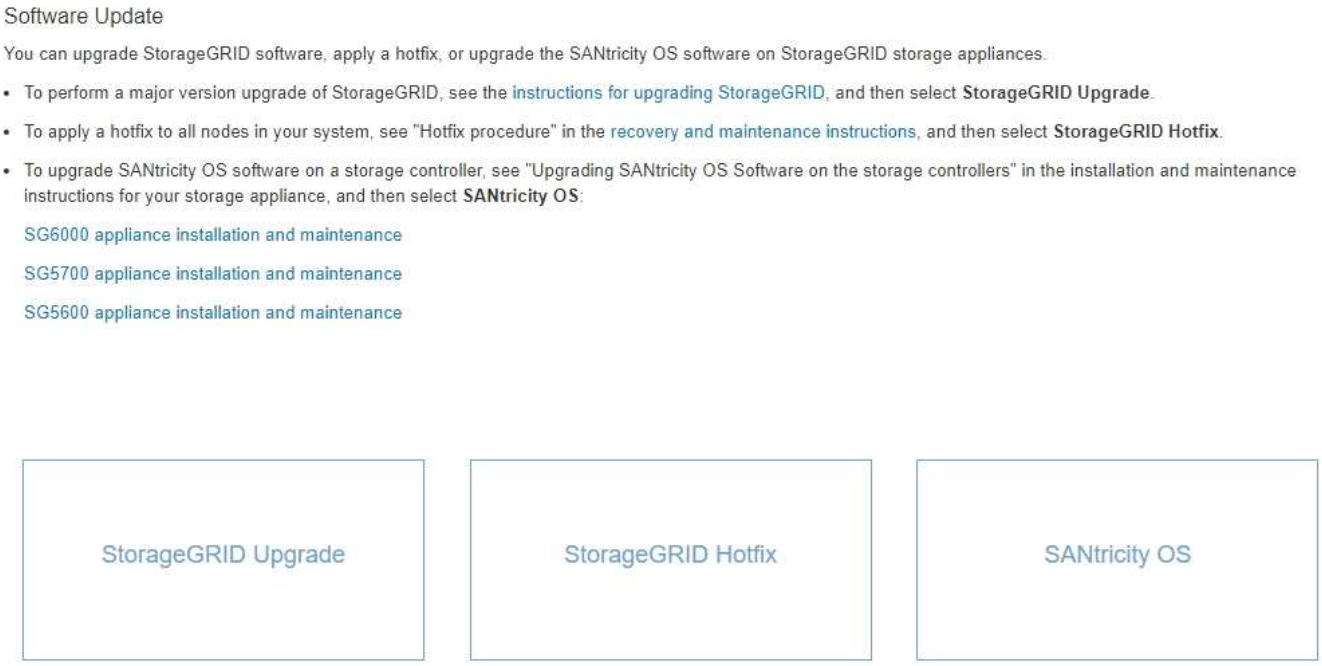
ンロードします。

アプライアンス内のストレージコントローラに対応する正しいバージョンのSANtricity OSを選択してください。SG6060ではE2800コントローラを、SGF6024ではEF570コントローラを使用します。

"ネットアップのダウンロード： SANtricity OS"

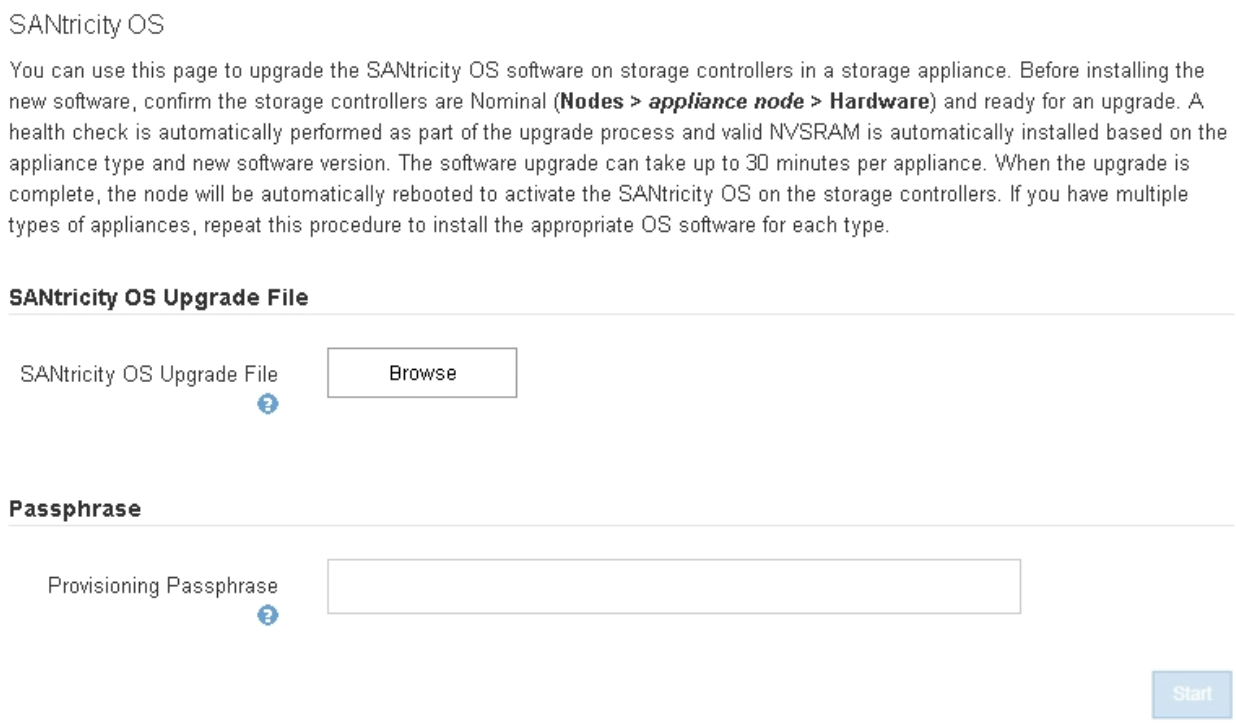
2. サポートされているブラウザを使用してGrid Managerにサインインします。
3. [* Maintenance（メンテナンス）]を選択します次に、メニューの[システム]セクションで、[ソフトウェア・アップデート]を選択します。

   Software Update ページが表示されます。




4. SANtricity OS *をクリックします。

   SANtricity OSページが表示されます。




5. NetApp Support Siteからダウンロードした SANtricity OS アップグレードファイルを選択します。

   a. [* 参照 ] をクリックします。

   b. ファイルを探して選択します。

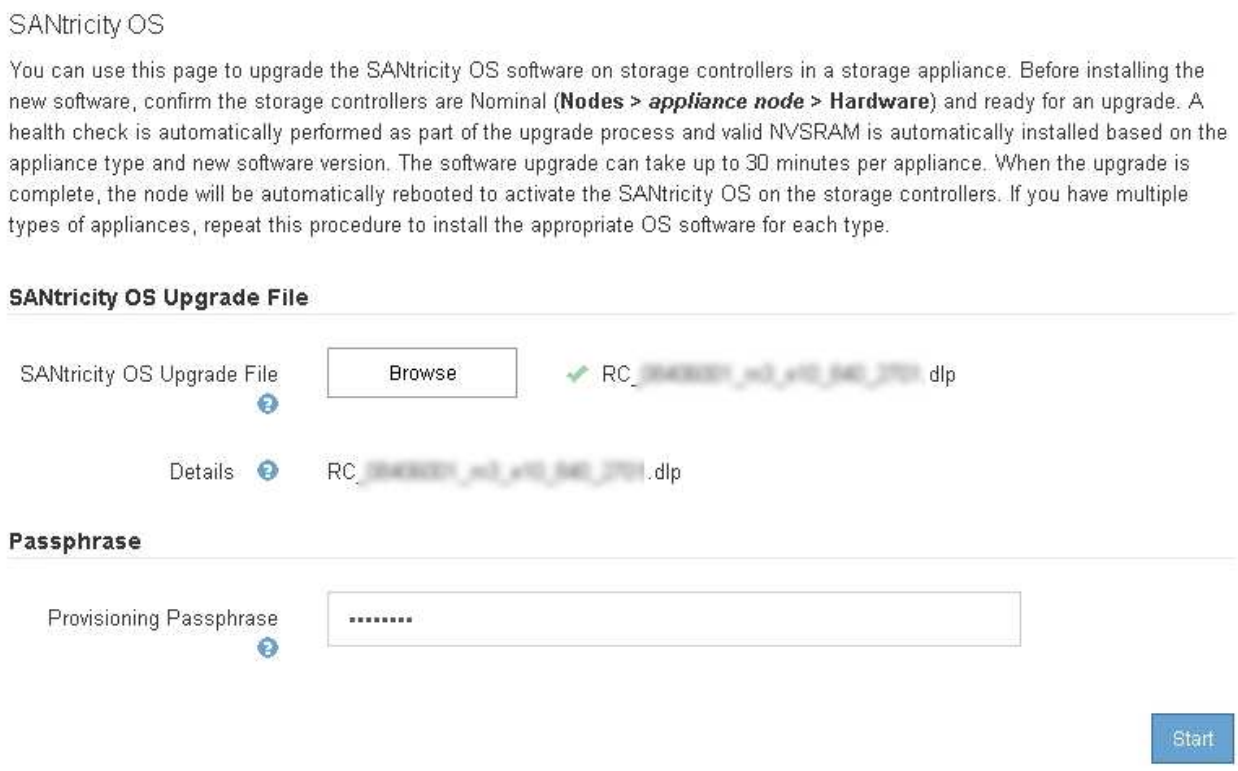
   c. * 開く * をクリックします。

   ファイルがアップロードされて検証されます。検証プロセスが完了すると、[詳細]フィールドにファイル名が表示されます。

   ファイル名は検証プロセスで指定されるため変更しないでください。

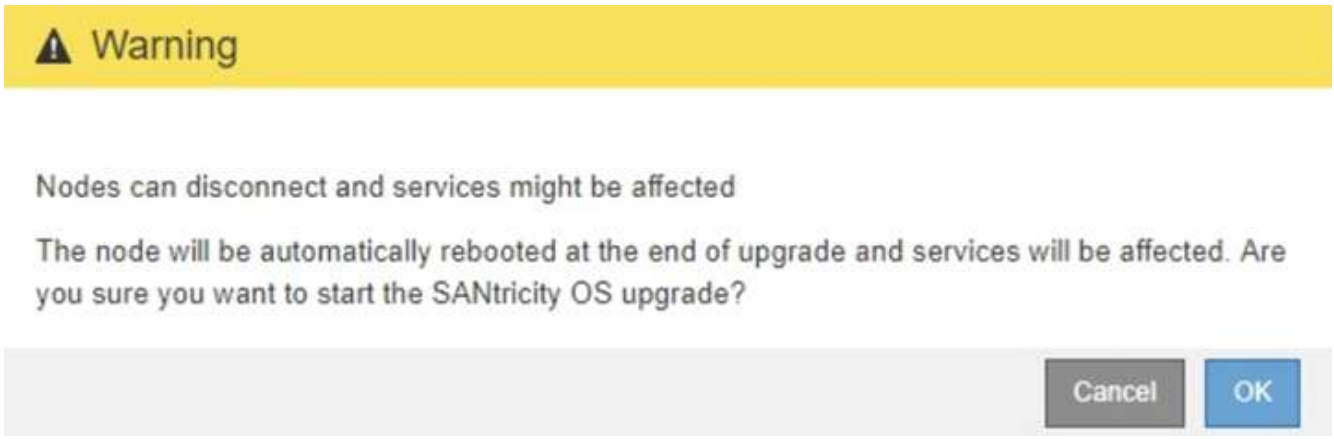
6. プロビジョニングパスフレーズを入力します。

「 * Start * （スタート * ）」ボタンが有効になります。



7. [ スタート ] ボタンをクリックします。

   アップグレードされたノードのサービスを再起動するとブラウザの接続が一時的に失われる可能性があることを示す警告ボックスが表示されます。




8. OK *をクリックして、SANtricity OSアップグレードファイルをプライマリ管理ノードにステージングします。

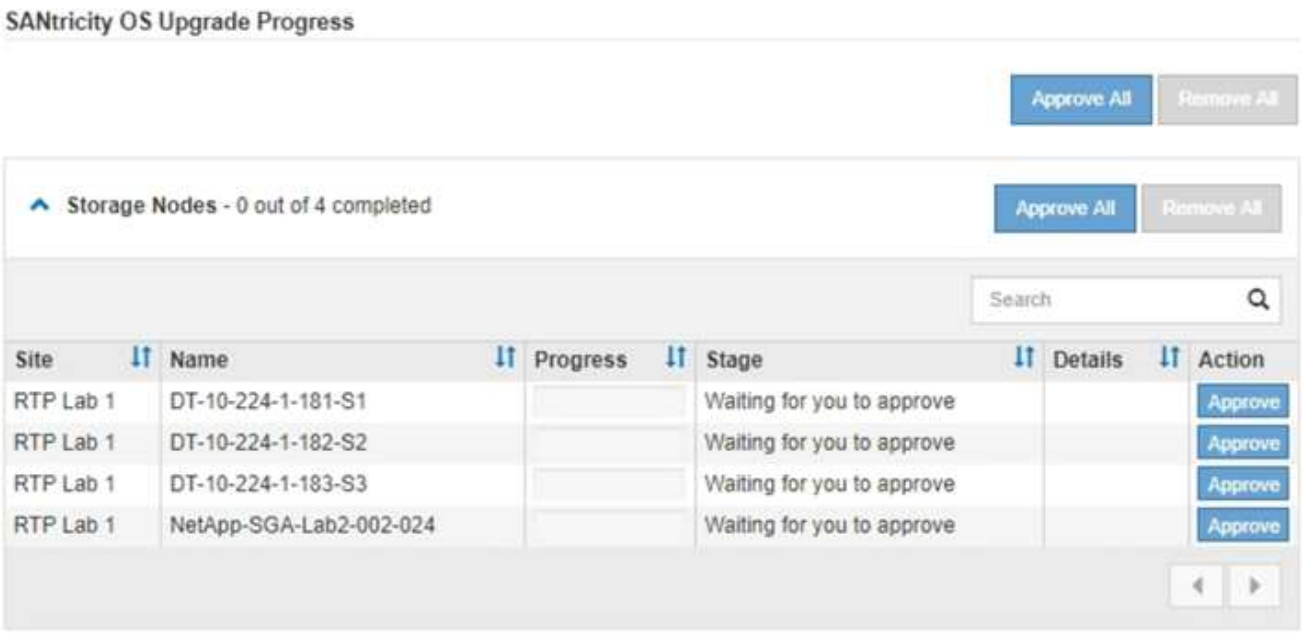
   SANtricity OS のアップグレードを開始すると、次の処理が行わ

   a. 健全性チェックが実行されます。このプロセスにより、ステータスが「 Needs Attention 」になっているノードがないかどうかが確認されます。

      エラーが報告された場合は、エラーを解決してから、*開始*をもう一度クリックします。

   b. SANtricity OS Upgrade Progress テーブルが表示されます。この表には、グリッド内のすべてのストレージノードと、各ノードのアップグレードの現在のステージが表示されます。

      ソフトウェアベースのストレージノードを含むすべてのストレージノードが表示されます。SANtricity OSのアップグレードがソフトウェアベースのストレージノードに影響しない場合でも、すべてのストレージノードのアップグレードを承認する必要があります。ソフトウェア・ベースのストレージ・ノードに対して返されたアップグレード・メッセージは「SANtricity OS upgrade is not applicable to this node.」です。




9. 必要に応じて、ノードのリストを* Site 、 Name 、 Progress 、 Stage 、または Details *で昇順または降順にソートします。または、 * 検索 * ボックスに用語を入力して特定のノードを検索します。

   ノードのリストをスクロールするには、セクションの右下隅にある左右の矢印を使用します。

10. アップグレードキューに追加する準備ができたグリッドノードを承認します。同じタイプの承認済みノードが一度に 1 つずつアップグレードされます。

    アプライアンスストレージノードのSANtricity OSアップグレードは、ノードを停止およびリブートする準備ができているかどうかが確認されないかぎり承認しないでください。ノードでSANtricity OSのアップグレードが承認されると、そのノードのサービスが停止します。あとでノードをアップグレードすると、アプライアンスノードがリブートされます。このような処理を実行すると、ノードと通信しているクライアントで原因 サービスが中断する可能性があります。

    - すべてのストレージノードをSANtricity OSアップグレードキューに追加するには、いずれかの*すべて承認ボタンをクリックします。

      ノードのアップグレード順序が重要な場合は、ノードまたはノードグループを 1 つずつ承認し、各ノードでアップグレードが完了するまで待ってから、次のノードを承認します。

    - 1つ以上の*承認*ボタンをクリックして、SANtricity OSアップグレードキューに1つ以上のノードを追加します。

      ノードへのSANtricity OSのアップグレードの適用は遅延できますが、リストされているすべてのストレージノードでSANtricity OSのアップグレードを承認するまで、SANtricity OSのアップグレードプロセスは完了しません。

    [* Approve *（承認）]をクリックすると、アップグレードプロセスによってノードをアップグレードできるかどうかが決定されます。ノードをアップグレード可能な場合は、アップグレードキューに追加されます。[+]

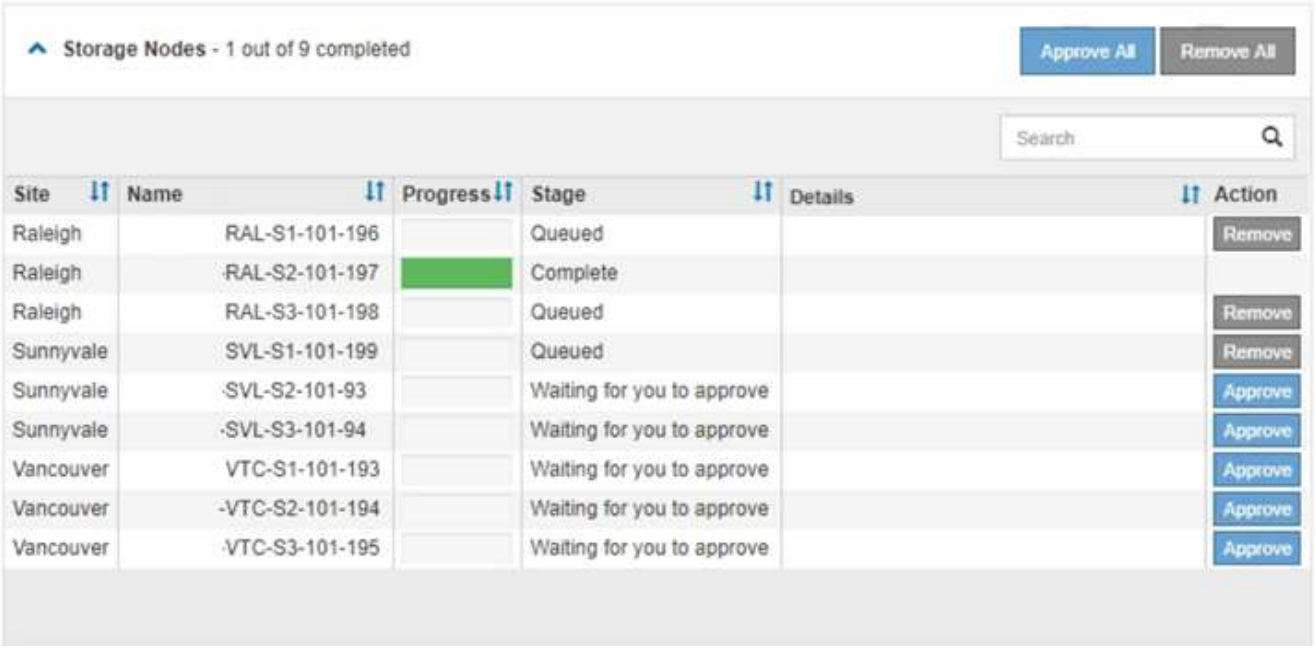
ノードによっては、選択したアップグレードファイルが意図的に適用されていないため、これらのノードをアップグレードせずにアップグレードプロセスを完了することができます。ノードが意図的にアップグレードされていない場合、プロセスの「Complete」列に次のいずれかのメッセージが表示されます。

- ストレージノードはすでにアップグレードされています。
- このノードではSANtricity OSのアップグレードは実行できません。
- SANtricity OSファイルがこのノードに対応していません。

「SANtricity OS upgrade is not applicable to this node」というメッセージは、ノードにStorageGRID システムで管理可能なストレージ・コントローラがないことを示します。このメッセージは、非アプライアンスストレージノードに対して表示されます。このメッセージが表示されているノードをアップグレードせずに、SANtricity OSのアップグレードプロセスを完了できます。+「SANtricity OS file is not compatible with this node」というメッセージは、ノードに、インストールしようとしているプロセスとは異なるSANtricity OSファイルが必要であることを示しています。現在のSANtricity OSのアップグレードが完了したら、そのノードに適したSANtricity OSをダウンロードして、アップグレードプロセスを繰り返します。

11. SANtricity OSアップグレードキューからノードまたはすべてのノードを削除する必要がある場合は、* Remove または Remove All *をクリックします。

例に示すように、ステージがQueuedを超えて進むと、* Remove *ボタンが非表示になり、SANtricity OSアップグレード処理からノードを削除できなくなります。




12. 承認された各グリッドノードに SANtricity OS のアップグレードが適用されるまで待ちます。

SANtricity OSのアップグレードの適用中にいずれかのノードでエラーステージが表示される場合、そのノードのアップグレードは失敗しています。障害からリカバリするために、アプライアンスをメンテナンスモードに切り替える必要がある場合があります。続行する前にテクニカルサポートにお問い合わせください。

ノード上のファームウェアが古すぎて Grid Manager でアップグレードできない場合、そのノードは Error をステージに表示します。 "` このノードで SANtricity OS をアップグレードするには、保守モードを使用

する必要があります。使用しているアプライアンスのインストールとメンテナンスの手順を参照してください。アップグレード後は ' このユーティリティを将来のアップグレードに使用できます エラーを解決するには、次の手順を実行します。

a. メンテナンスモードを使用して、「エラー」のステージが表示されるノードの SANtricity OS をアップグレードします。

b. Grid Managerを使用してSANtricity OSのアップグレードを再開し、完了します。

   承認されたすべてのノードで SANtricity OS のアップグレードが完了すると、 SANtricity OS アップグレードの進捗状況テーブルが閉じ、緑のバナーに SANtricity OS のアップグレードが完了した日時が表示されます。

13. 別の SANtricity OS アップグレードファイルが必要な、完了段階のノードすべてについて、このアップグレード手順 を繰り返します。

ステータスが「 Needs Attention 」のノードがある場合は、メンテナンスモードを使用してアップグレードを実行します。

関連情報

"NetApp Interoperability Matrix Tool で確認できます"

"ストレージコントローラのSANtricity OSをメンテナンスモードでアップグレードします"

ストレージコントローラの**SANtricity OS**をメンテナンスモードでアップグレードします

## 08.42.20.00 （ 11.42 ）より前の SANtricity OS を使用しているストレージコントローラの場合、メンテナンスモード手順 を使用してアップグレードを適用する必要があります。

必要なもの

- NetApp Interoperability Matrix Tool （ IMT ）を参照して、アップグレードに使用する SANtricity OS のバージョンがお使いのアプライアンスと互換性があることを確認してください。
- StorageGRID アプライアンスを StorageGRID システムで実行中の場合は、 SG6000-CN コントローラがメンテナンスモードになります。

保守モードでは、ストレージコントローラへの接続が中断されます。

"アプライアンスをメンテナンスモードにします"

このタスクについて

一度に複数の StorageGRID アプライアンスで E シリーズコントローラの SANtricity OS または NVSRAM をアップグレードしないでください。

> 一度に複数の StorageGRID アプライアンスをアップグレードすると、導入モデルや ILM ポリシーによっては、原因 データを使用できなくなる可能性があります。

手順

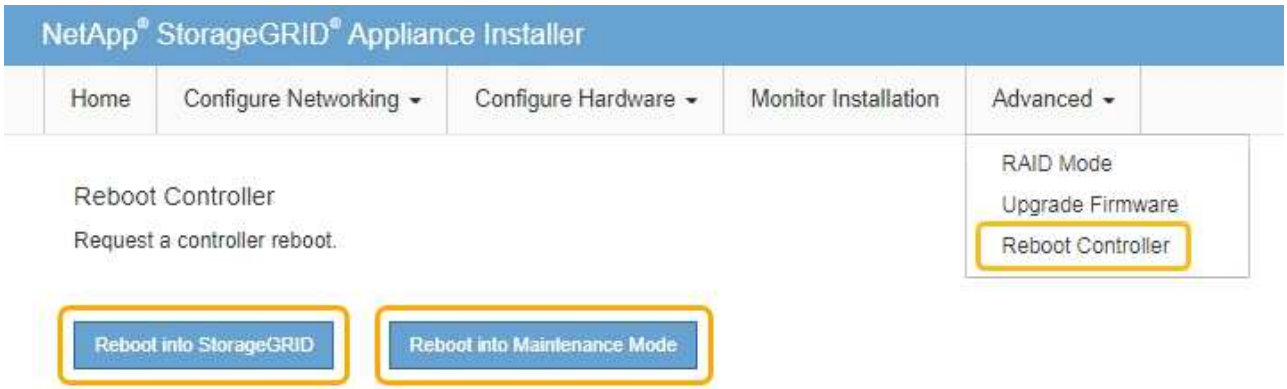
1. サービスラップトップから、 SANtricity System Manager にアクセスしてサインインします。
2. 新しい SANtricity OS ソフトウェアファイルと NVSRAM ファイルを管理クライアントにダウンロードします。

> NVSRAM は、 StorageGRID アプライアンスに固有です。標準の NVSRAM ダウンロードを使用しないでください。

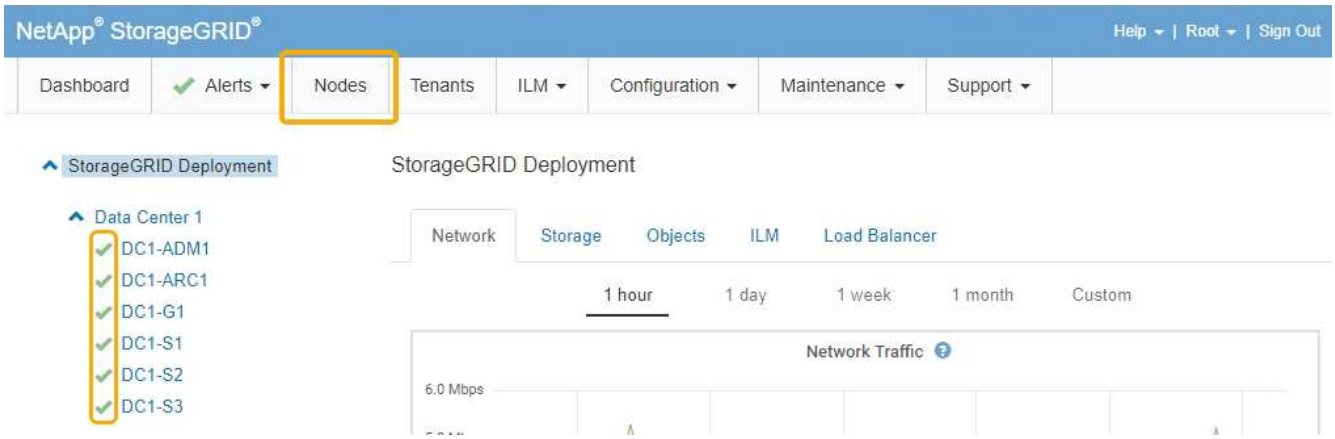
3. SANtricity OS_guide または SANtricity System Manager のオンラインヘルプの指示に従って、ファームウェアと NVSRAM をアップグレードします。

> アップグレードファイルはただちにアクティブ化する必要があります。アクティブ化を先延ばしにしないでください。

4. アップグレード処理が完了したら、ノードをリブートします。StorageGRID アプライアンス・インストーラから、 **Advanced**>*Reboot Controller* を選択し、次のいずれかのオプションを選択します。
   - Reboot into StorageGRID * を選択し、ノードをグリッドに再追加してコントローラをリブートします。メンテナンスモードで作業を完了し、ノードを通常動作に戻す準備ができている場合は、このオプションを選択します。
   - メンテナンスモードを維持したままコントローラをリブートするには、 * Reboot into Maintenance Mode * を選択します。このオプションは、グリッドに再追加する前にノードで追加のメンテナンス処理を実行する必要がある場合に選択します。




アプライアンスがリブートしてグリッドに再参加するまでに最大 20 分かかることがあります。リブートが完了し、ノードが再びグリッドに参加したことを確認するには、 Grid Manager に戻ります。[ノード*（Nodes *）]タブには、通常のステータスが表示されます ✔ アクティブなアラートがなく、ノードがグリッドに接続されていることを示す、アプライアンスノードの場合。




関連情報

"NetApp Interoperability Matrix Tool で確認できます"

"グリッドマネージャを使用してストレージコントローラのSANtricity OSをアップグレードします"

**SANtricity System Manager**を使用してドライブファームウェアをアップグレードする

ドライブファームウェアをアップグレードして、最新の機能とバグ修正をすべて適用します。

必要なもの

- ストレージアプライアンスのステータスが「最適」であることを確認します。
- すべてのドライブのステータスが最適な状態である必要があります
- 最新バージョンの SANtricity System Manager がインストールされていて、 StorageGRID のバージョンと互換性があることを確認します。
- StorageGRID アプライアンスをメンテナンスモードにしておきます。

  "アプライアンスをメンテナンスモードにします"

> 保守モードでは、ストレージコントローラへの接続が中断され、すべての I/O アクティビティが停止されて、すべてのドライブがオフラインになります。

> 一度に複数の StorageGRID アプライアンスでドライブファームウェアをアップグレードしないでください。お使いの導入モデルや ILM ポリシーによっては、原因 データを使用できなくなる場合があります。

手順

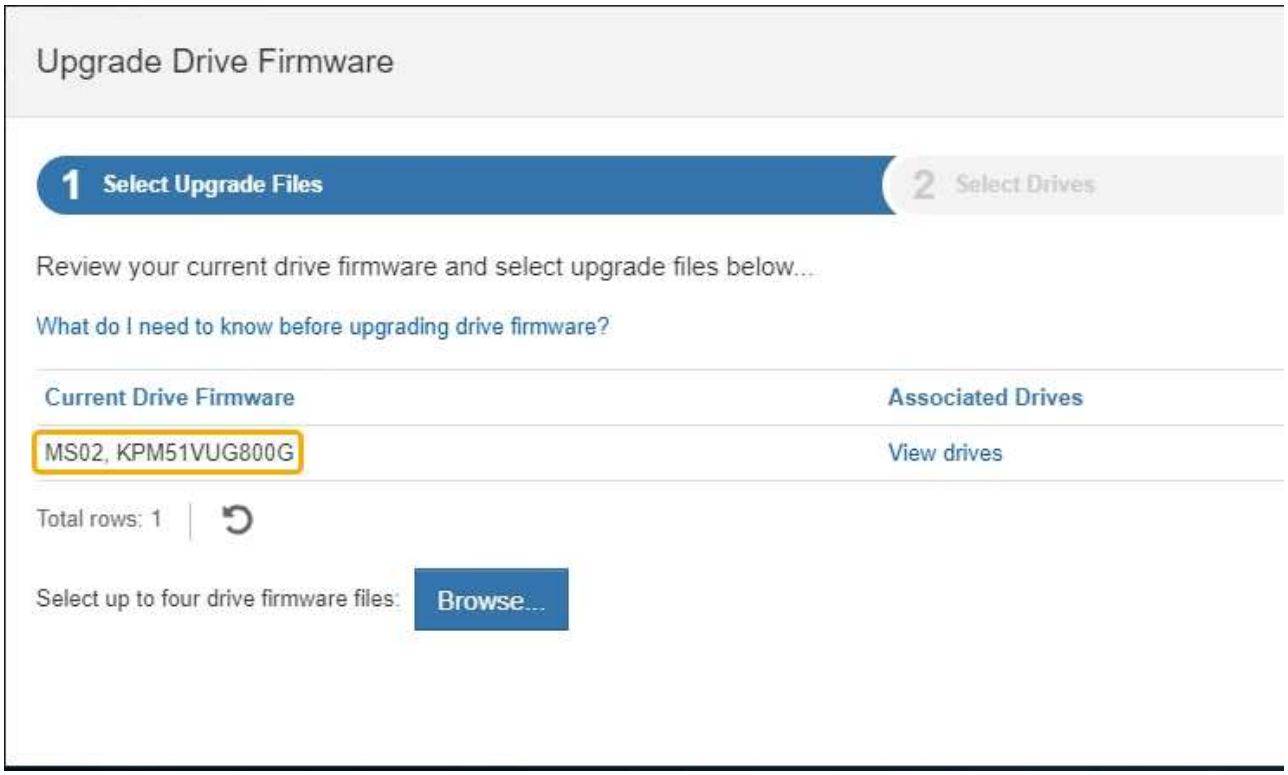
1. 次のいずれかの方法で SANtricity System Manager にアクセスします。
   - StorageGRID アプライアンス・インストーラを使用して、 * アドバンスト * > * SANtricity システム・マネージャ * を選択します
   - Grid Managerを使用して* Nodes >を選択します ***appliance Storage Node*** >* SANtricity システム・マネージャ*

これらのオプションが表示されない場合や、SANtricity System Managerのログインページが表示されない場合は、ストレージコントローラのIP：+にアクセスしてSANtricity System Managerにアクセスします
**https://*Storage_Controller_IP***

2. 必要に応じて、 SANtricity System Manager 管理者のユーザ名とパスワードを入力します。
3. ストレージアプライアンスに現在インストールされているドライブファームウェアのバージョンを確認します。
   a. SANtricity システムマネージャで、* Support > Upgrade Center *を選択します。
   b. ドライブファームウェアのアップグレードで、 * アップグレードの開始 * を選択します。

      ドライブファームウェアのアップグレードに、現在インストールされているドライブファームウェアファイルが表示されます。

   c. 現在のドライブファームウェア列に表示されているドライブファームウェアのリビジョンとドライブ ID をメモします。




次の例では、

- ドライブファームウェアのリビジョンは * MS02 * です。
- ドライブ識別子は **KPM51VUG800G** です。

Associated Drives 列で「 * View drives 」を選択して、ストレージアプライアンス内のドライブがどこに取り付けられているかを表示します。

   a. ドライブファームウェアのアップグレードウィンドウを閉じます。

4. 使用可能なドライブファームウェアのアップグレードをダウンロードして準備します。

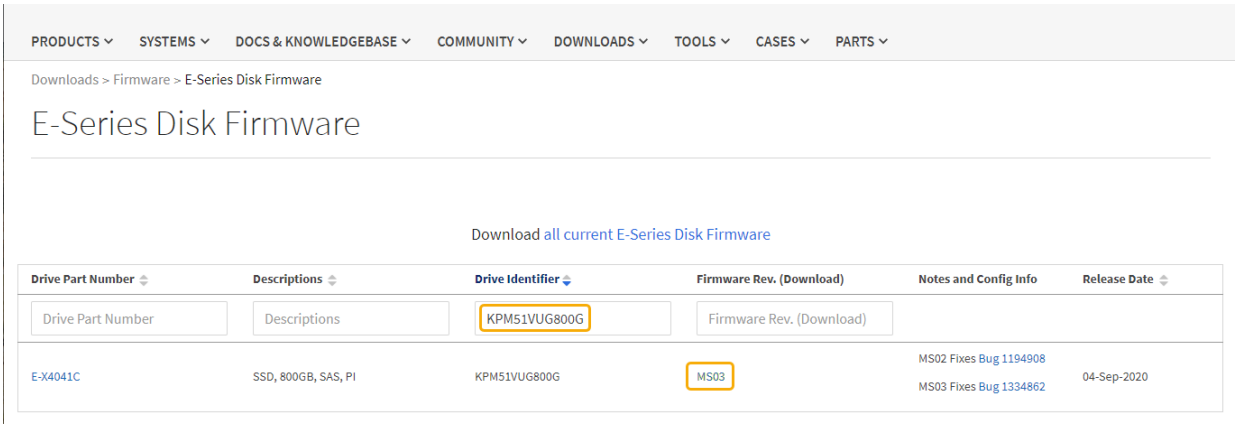
a. ドライブファームウェアのアップグレードで、 * ネットアップサポート * を選択します。

b. ネットアップサポート Web サイトで、「 * Downloads * 」タブを選択し、「 * E-Series Disk Drive Firmware * 」を選択します。

   E-Series Disk Firmware ページが表示されます。

c. ストレージアプライアンスにインストールされているドライブ識別子 * をそれぞれ検索し、各ドライブ識別子に最新のファームウェアリビジョンが適用されていることを確認します。

   - ファームウェアリビジョンがリンクでない場合、このドライブ識別子には最新のファームウェアリビジョンが含まれます。
   - ドライブ識別子が記載されたドライブのパーツ番号が 1 つ以上であれば、それらのドライブでファームウェアのアップグレードを実行できます。任意のリンクを選択してファームウェアファイルをダウンロードできま
     す。




d. 新しいファームウェアリビジョンがリストされている場合は、ファームウェアリビジョンのリンクを選択します（ダウンロード）列をクリックしてをダウンロードします `.zip` ファームウェアファイルを含むアーカイブ。

e. サポートサイトからダウンロードしたドライブファームウェアのアーカイブファイルを展開（解凍）します。

5. ドライブファームウェアのアップグレードをインストールします。

a. SANtricity システムマネージャのドライブファームウェアアップグレードで、 * アップグレードの開始 * を選択します。

b. [* Browse] を選択し、サポートサイトからダウンロードした新しいドライブファームウェアファイルを選択します。

   ドライブファームウェアファイルの名前は、+のようになります `D_HUC101212CSS600_30602291_MS01_2800_0002.dlp`。

   ドライブファームウェアファイルは一度に 1 つずつ、最大 4 つまで選択できます。同じドライブに複数のドライブファームウェアファイルが対応している場合は、ファイル競合エラーが発生します。アップグレードに使用するドライブファームウェアファイルを決定し、それ以外のファイルは削除します。

c. 「 * 次へ * 」を選択します。

   - ドライブの選択 * には、選択したファームウェアファイルでアップグレードできるドライブがリストされています。

対応しているドライブのみが表示されます。

選択したドライブのファームウェアが * 推奨ファームウェア * に表示されます。このファームウェアを変更する必要がある場合は、 * 戻る * を選択します。

d. 「オフライン（パラレル） * アップグレード」を選択します。

オフラインアップグレード方式を使用できるのは、アプライアンスがメンテナンスモードで、すべてのドライブとすべてのボリュームの I/O アクティビティが停止されているためです。

e. テーブルの最初の列で、アップグレードするドライブを選択します。

ベストプラクティスとして、同じモデルのドライブをすべて同じファームウェアリビジョンにアップグレードすることを推奨します。

f. [ スタート ] ボタンをクリックし、アップグレードを実行することを確認します。

アップグレードを停止する必要がある場合は、 * 停止 * を選択します。実行中のファームウェアのダウンロードは完了します。開始されていないファームウェアのダウンロードはキャンセルされます。

ドライブファームウェアのアップグレードを停止すると、データが失われたり、ドライブを使用できなくなったりする可能性があります。

g. （オプション）アップグレードされた内容のリストを表示するには、 * ログを保存 * を選択します。

ログファイルは、ブラウザのダウンロードフォルダにという名前で保存されます `latest-upgrade-log-timestamp.txt`。

手順のアップグレード中に次のいずれかのエラーが発生した場合は、推奨される対処方法を実行してください。

- * 割り当て済みドライブの障害 *

  エラーの理由の 1 つとして、ドライブに適切な署名がない可能性があります。該当するドライブが認定済みのドライブであることを確認します。詳細については、テクニカルサポートにお問い合わせください。

ドライブを交換する場合は、交換用ドライブの容量が交換する障害ドライブと同じかそれよりも大きいことを確認してください。

障害が発生したドライブの交換は、ストレージアレイで I/O を受信中に実行できます

- * ストレージアレイを確認してください *
  - 各コントローラに IP アドレスが割り当てられていることを確認します。
  - コントローラに接続されているすべてのケーブルが破損していないことを確認します。
  - すべてのケーブルがしっかりと接続されていることを確認します。
- * 内蔵ホットスペアドライブ *

ファームウェアをアップグレードする前に、このエラーを修正する必要があります。

- * 不完全なボリュームグループ *

  1 つ以上のボリュームグループまたはディスクプールが不完全な場合は、ファームウェアをアップグレードする前に、このエラーを修正する必要があります。

- * すべてのボリュームグループで実行中の排他的な処理（バックグラウンドメディア / パリティスキャン以外） *

  1 つ以上の排他的な処理を実行中の場合は、その処理を完了してからファームウェアをアップグレードする必要があります。System Manager で処理の進捗状況を監視します。

- * 見つからないボリューム *

  ファームウェアをアップグレードする前に、ボリュームが見つからない状態を修正する必要があります。

- * いずれかのコントローラが最適以外の状態 *

  いずれかのストレージアレイコントローラを確認する必要があります。ファームウェアをアップグレードする前に、この状態を修正する必要があります。

- * コントローラオブジェクトグラフ間でストレージパーティション情報が一致しません *

  コントローラ上のデータの検証中にエラーが発生しました。この問題を解決するには、テクニカルサポートにお問い合わせください。

- * SPM によるデータベースコントローラの検証が失敗します *

  コントローラでストレージパーティションマッピングデータベースのエラーが発生しました。この問題を解決するには、テクニカルサポートにお問い合わせください。

- * 構成データベースの検証（ストレージアレイのコントローラのバージョンでサポートされている場合） *

  コントローラで構成データベースのエラーが発生しました。この問題を解決するには、テクニカルサポートにお問い合わせください。

- * MEL 関連のチェック *

  この問題を解決するには、テクニカルサポートにお問い合わせください。

- * 過去 7 日間に 10 個を超える DDE 情報または重大 MEL イベントが報告されました *

  この問題を解決するには、テクニカルサポートにお問い合わせください。

- * 過去 7 日間に 2 ページ 2C 重大 MEL イベントが報告されました *

  この問題を解決するには、テクニカルサポートにお問い合わせください。

- * 過去 7 日間に 2 個以上の低下したドライブチャネル重大 MEL イベントが報告されました *

  この問題を解決するには、テクニカルサポートにお問い合わせください。

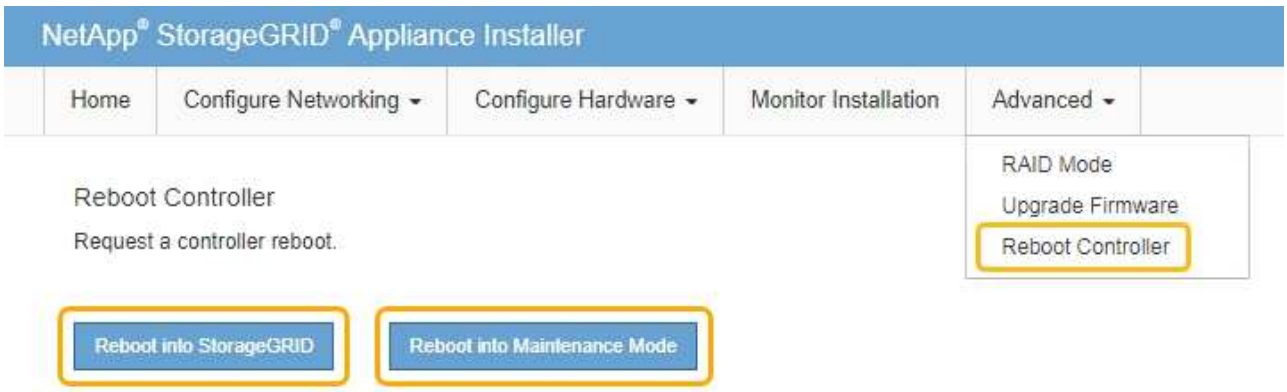
◦ * 過去 7 日間に 4 個を超える重大 MEL エントリがあります *

この問題を解決するには、テクニカルサポートにお問い合わせください。

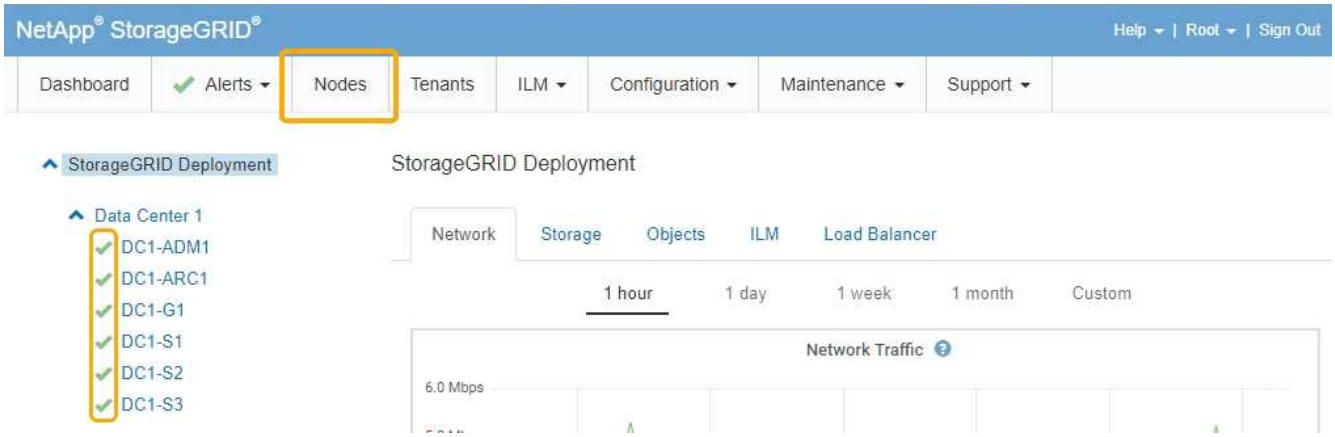
6. アップグレード処理が完了したら、アプライアンスをリブートします。StorageGRID アプライアンス・インストーラから、 **Advanced**>*Reboot Controller* を選択し、次のいずれかのオプションを選択します。

◦ Reboot into StorageGRID * を選択し、ノードをグリッドに再追加してコントローラをリブートします。メンテナンスモードで作業を完了し、ノードを通常動作に戻す準備ができている場合は、このオプションを選択します。

◦ メンテナンスモードを維持したままコントローラをリブートするには、 * Reboot into Maintenance Mode * を選択します。このオプションは、グリッドに再追加する前にノードで追加のメンテナンス処理を実行する必要がある場合に選択しま
す。




アプライアンスがリブートしてグリッドに再参加するまでに最大 20 分かかることがあります。リブートが完了し、ノードが再びグリッドに参加したことを確認するには、 Grid Manager に戻ります。[ノード*（Nodes *）]タブには、通常のステータスが表示されます ✔ アクティブなアラートがなく、ノードがグリッドに接続されていることを示す、アプライアンスノードの場合。




関連情報

"ストレージコントローラのSANtricity OSをアップグレードします"

導入済みの**SG6060**への拡張シェルフの追加

# ストレージ容量を増やすには、 StorageGRID システムに導入されている SG6060 に拡張シェルフを 1 台または 2 台追加します。

必要なもの

- プロビジョニングパスフレーズが必要です。
- StorageGRID 11.4 以降が実行されている必要があります。
- 拡張シェルフごとに、拡張シェルフと SAS ケーブルを 2 本用意します。
- データセンターに拡張シェルフを追加するストレージアプライアンスを物理的に配置しておきます。

  "コントローラのデータセンターへの配置"

このタスクについて

拡張シェルフを追加するには、次の手順を実行します。

- キャビネットまたはラックにハードウェアを設置します。
- SG6060 をメンテナンスモードにします。
- 拡張シェルフを E2860 コントローラシェルフまたは別の拡張シェルフに接続します。
- StorageGRID アプライアンスインストーラを使用して拡張を開始します
- 新しいボリュームが設定されるまで待ちます。

拡張シェルフ 1 台または 2 台の手順 を完了するには、アプライアンスノードあたり 1 時間以内に作業を行う必要があります。ダウンタイムを最小限に抑えるために、次の手順では、 SG6060 をメンテナンスモードにする前に新しい拡張シェルフとドライブを設置するように指示します。残りの手順には、アプライアンスノード 1 台あたり 20~30 分かかります。

手順

1. 60 ドライブシェルフをキャビネットまたはラックに設置する手順に従います。

   "SG6060：キャビネットまたはラックへの60ドライブシェルフの設置"

2. ドライブの取り付け手順に従います。

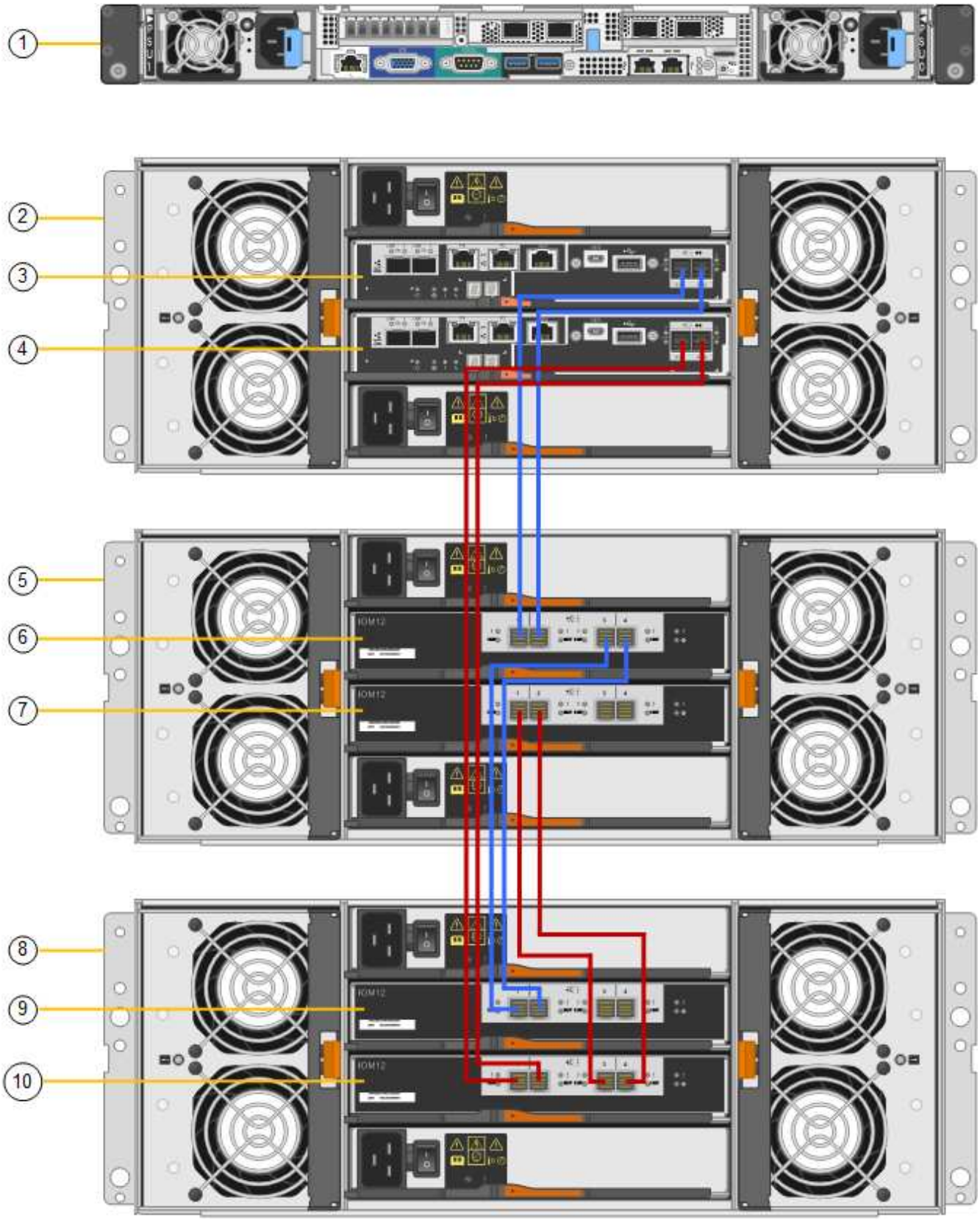
   "SG6060：ドライブの取り付け"

3. Grid Managerから、SG6000-CNコントローラをメンテナンスモードにします。

   "アプライアンスをメンテナンスモードにします"

4. 次の図に示すように、各拡張シェルフを E2860 コントローラシェルフに接続します。

   この図は、 2 台の拡張シェルフを示しています。IOM A のみをコントローラ A に接続し、 IOM B をコントローラ B に接続します




| | 説明 |
|---|---|
| 1. | SG6000-CN の情報 |

| | 説明 |
|---|---|
| 2. | E2860 コントローラシェルフです |
| 3. | コントローラ A |
| 4. | コントローラ B |
| 5. | 拡張シェルフ 1 |
| 6. | 拡張シェルフ 1 の IOM A |
| 7. | 拡張シェルフ 1 の IOM B |
| 8. | 拡張シェルフ 2 |
| 9. | 拡張シェルフ 2 の IOM A |
| 10. | 拡張シェルフ 2 の IOM B |

5. 電源コードを接続し、拡張シェルフに電源を投入
   a. 各拡張シェルフの 2 つ電源装置のそれぞれに電源コードを接続します。
   b. 各拡張シェルフの 2 本の電源コードを、キャビネットまたはラック内の別々の PDU に接続します。
   c. 拡張シェルフごとに 2 つの電源スイッチをオンにします。
      - 電源投入プロセスの実行中は電源スイッチをオフにしないでください。
      - 拡張シェルフのファンは、初回起動時に大きな音を立てることがあります。起動時に大きな音がしても問題はありません。
6. StorageGRID アプライアンスインストーラのホームページを監視します。

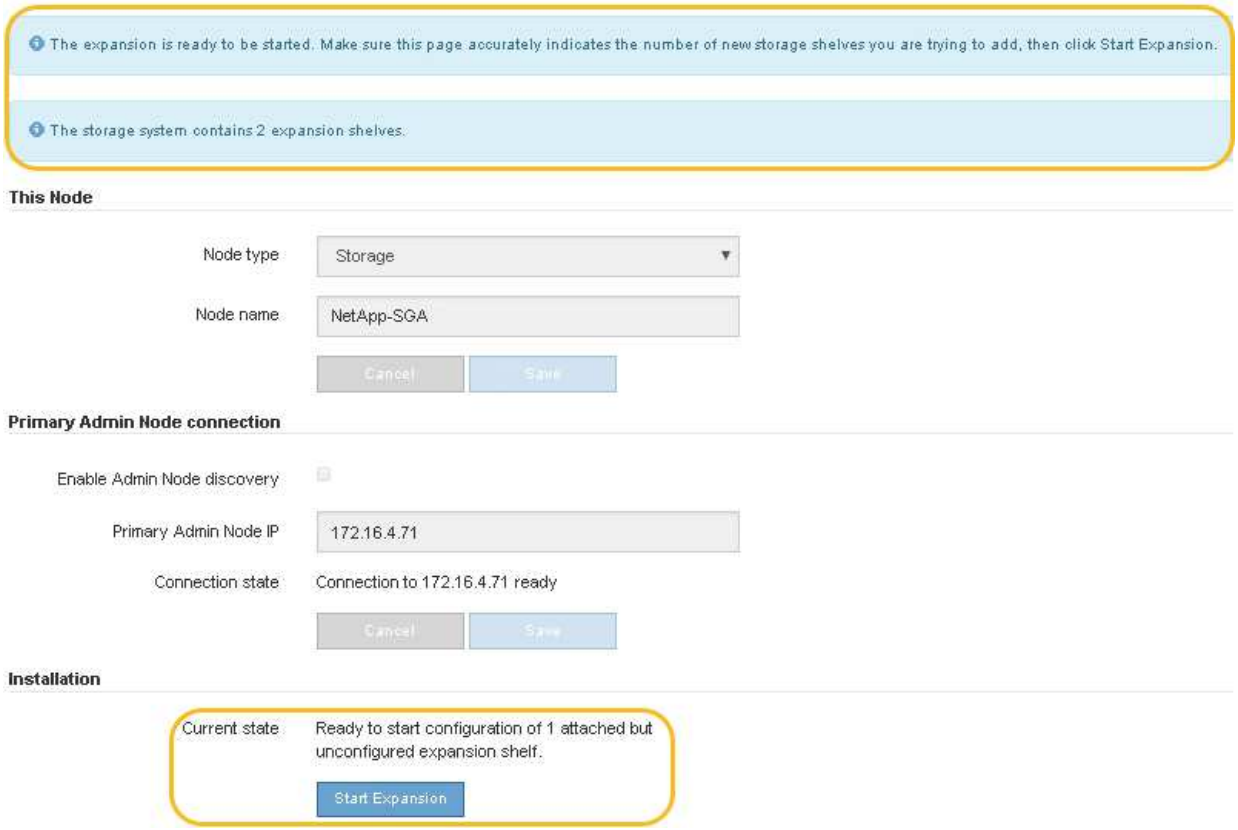
   拡張シェルフの電源投入が完了してシステムで検出されるまでに約 5 分かかります。ホームページに、検出された新しい拡張シェルフの数と、拡張の開始ボタンが有効になっていることが表示されます。

   次のスクリーンショットは、既存または新規の拡張シェルフの数に応じて、ホームページに表示されるメッセージの例を示しています。

   - ページ上部の丸で囲まれたバナーには、検出された拡張シェルフの総数が表示されます。
     - バナーには拡張シェルフの総数が表示され、シェルフの構成と導入が完了しているか、新規および未設定のいずれであるかが示されます。
     - 拡張シェルフが検出されなかった場合は、バナーは表示されません。
   - ページ下部の丸で囲まれたメッセージは、拡張を開始する準備ができていることを示します。
     - メッセージには、 StorageGRID が検出した新しい拡張シェルフの数が示されます。「 Attached 」は、シェルフが検出されたことを示します。"`Unconfigureed" は、シェルフが新規であり、 StorageGRID アプライアンス・インストーラを使用してまだ構成されていないことを示します。

すでに導入されている拡張シェルフはこのメッセージに含まれません。これらの値は、ページ上部のバナーの数に含まれています。

- このメッセージは、新しい拡張シェルフが検出されない場合は表示されません。




7. 必要に応じて、ホームページのメッセージに記載されている問題を解決します。

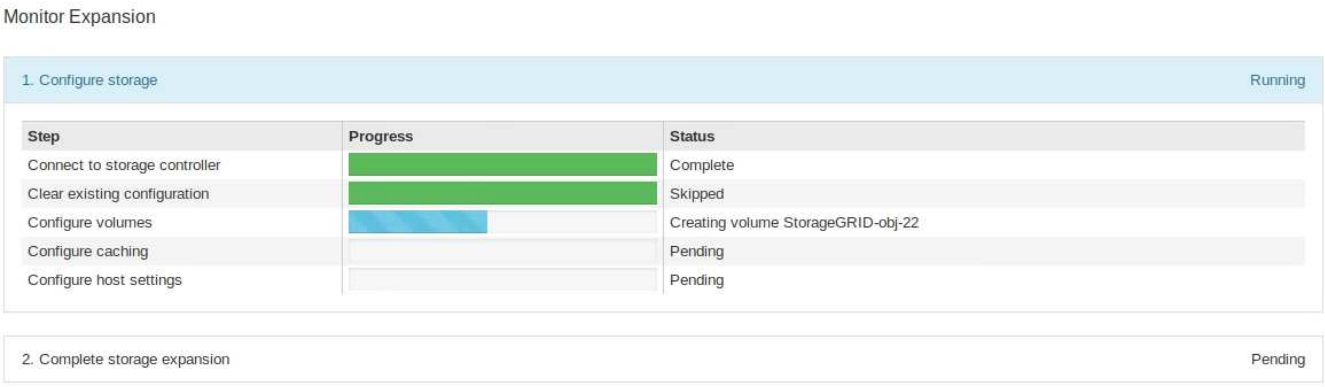
   たとえば、ストレージハードウェアの問題を解決するには、 SANtricity System Manager を使用します。

8. ホームページに表示される拡張シェルフの数が、追加する拡張シェルフの数と一致していることを確認します。

   新しい拡張シェルフが検出されていない場合は、適切にケーブル接続され、電源がオンになっていることを確認します。

9. 拡張の開始*をクリックして拡張シェルフを設定し、オブジェクトストレージで使用できるようにします。
10. 拡張シェルフ構成の進捗状況を監視します。

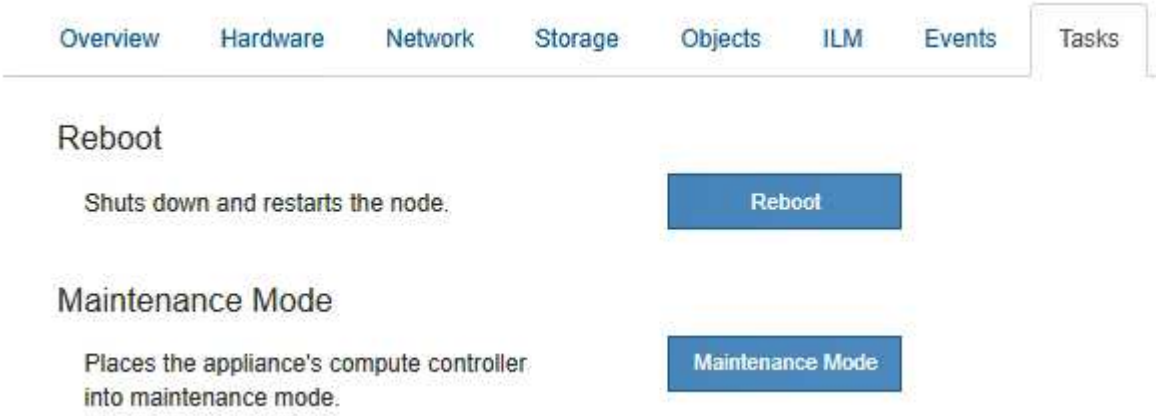
    初期インストール時と同様に、進行状況バーが Web ページに表示されます。




設定が完了すると、アプライアンスが自動的にリブートしてメンテナンスモードを終了し、グリッドに再参加します。この処理には最大 20 分かかることがあります。

アプライアンスがグリッドに再参加しない場合は、StorageGRID アプライアンスインストーラのホームページに移動し、アドバンスト>*コントローラのリブート*を選択して、*メンテナンスモードでリブート*を選択します。

リブートが完了すると、 * Tasks * タブは次のスクリーンショットのようになります。




11. アプライアンスストレージノードおよび新しい拡張シェルフのステータスを確認します。
    a. Grid Managerで* Nodes *を選択し、アプライアンスストレージノードのチェックマークが緑色になっていることを確認します。

       緑のチェックマークアイコンは、アクティブなアラートがなく、ノードがグリッドに接続されていることを示します。ノードアイコンの概要 については、 StorageGRID の監視とトラブルシューティングの手順を参照してください。

    b. 「 * Storage * 」タブを選択し、追加した各拡張シェルフのオブジェクトストレージテーブルに 16 個の新しいオブジェクトストアが表示されていることを確認します。

    c. 新しい各拡張シェルフのシェルフステータスが Nominal であり、構成ステータスが Configured になっていることを確認します。

Storage Shelves

| Shelf Chassis Serial Number | Shelf ID | Shelf Status | IOM Status | Power Supply Status | Drawer Status | Fan Status | Drive Slots | Data Drives | Data Drive Size | Cache Drives | Cache Drive Size | Configuration Status |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 721924500063 | 99 | Nominal | N/A | Nominal | Nominal | Nominal | 60 | 58 | 9.80 TB | 2 | 800.17 GB | Configured (in use) |
| 721929500038 | 0 | Nominal | Nominal | Nominal | Nominal | Nominal | 60 | 60 | 9.80 TB | 0 | 0 bytes | Configured (in use) |
| 721929500039 | 1 | Nominal | Nominal | Nominal | Nominal | Nominal | 60 | 60 | 9.80 TB | 0 | 0 bytes | Configured (in use) |

関連情報

"開梱（SG6000）"

"SG6060：キャビネットまたはラックへの60ドライブシェルフの設置"

"SG6060：ドライブの取り付け"

"トラブルシューティングを監視します"

コントローラ識別**LED**のオンとオフの切り替え

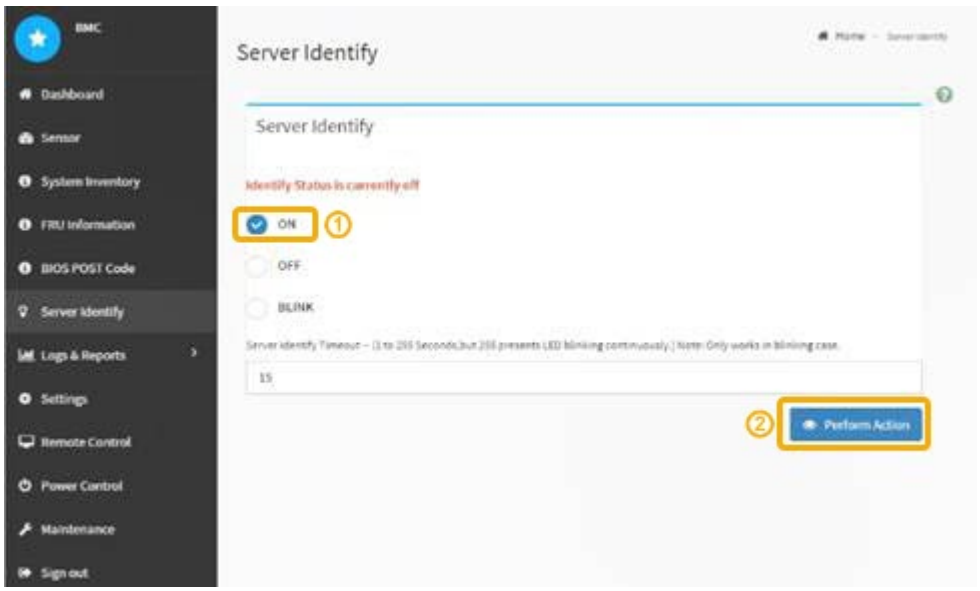
## コントローラの前面と背面にある青色の識別 LED は、データセンターでアプライアンスを特定するのに役立ちます。

必要なもの

識別するコントローラの BMC IP アドレスが必要です。

手順

1. コントローラの BMC インターフェイスにアクセスします。
2. 「 * サーバー識別 * 」を選択します。
3. 「 * オン * 」を選択し、「 * アクションの実行 * 」を選択します。




結果

青色の識別 LED は、コントローラの前面（図）と背面（図）に点灯します。

コントローラにベゼルが取り付けられている場合、前面の識別 LED が見えにくいことがあります。

完了後

コントローラ識別 LED を消灯するには、次の手順を実行します。

- コントローラの前面パネルにある識別 LED スイッチを押します。
- コントローラの BMC インターフェイスから、 * Server identify * を選択し、 * off * を選択して、 * Perform Action * を選択します。

コントローラの前面と背面の青色の識別 LED が消灯します。

関連情報

"交換するファイバチャネルHBAの確認"

"コントローラのデータセンターへの配置"

"BMCインターフェイスへのアクセス"

コントローラのデータセンターへの配置

## ハードウェアのメンテナンスやアップグレードを実行できるように、コントローラを特定します。

必要なもの

- メンテナンスが必要なコントローラを特定しておきます。

  （オプション）データセンター内のコントローラの位置を確認するには、青色の識別 LED をオンにします。

  "コントローラ識別LEDのオンとオフの切り替え"

手順

1. データセンターでメンテナンスが必要なコントローラを特定します。
   - コントローラの前面または背面の LED が青色に点灯していることを確認します。

     前面の識別 LED はコントローラの前面ベゼルの背面にあり、ベゼルが取り付けられているかどうかを確認するのが困難な場合があります。

   - 各コントローラの前面にあるタグで、一致するパーツ番号を確認します。
2. コントローラの前面ベゼルが取り付けられている場合は、前面パネルのコントロールとインジケータにアクセスするために取り外します。
3. オプション：コントローラの場所を確認するために使用した場合は、青色の識別 LED を消灯します。
   - コントローラの前面パネルにある識別 LED スイッチを押します。
   - コントローラの BMC インターフェイスを使用します。

     "コントローラ識別LEDのオンとオフの切り替え"

関連情報

"Fibre Channel HBAの取り外し"

"キャビネットまたはラックからのSG6000-CNコントローラの取り外し"

"SG6000-CNコントローラをシャットダウンします"

ストレージコントローラの交換

## E2800 コントローラまたは EF570 コントローラが適切に機能しない場合や障害が発生

した場合は、交換が必要となることがあります。

必要なもの

- 交換するコントローラと同じパーツ番号の交換用コントローラを用意しておきます。
- コントローラに接続する各ケーブルを識別するためのラベルを用意しておきます。
- ESD リストバンドを装着するか、静電気防止処置を施しておきます。
- No.1 プラスドライバを用意しておきます。
- デュプレックス構成のコントローラを交換するための E シリーズの手順書を用意しておきます。

> E シリーズの手順書は、指示された場合、または特定の手順の詳細を知る必要がある場合にのみ参照してください。StorageGRID アプライアンスのコントローラを交換する際は、E シリーズの手順書を参考にしないでください。手順が異なります。

- データセンター内のコントローラを交換するストレージアプライアンスの物理的な場所を確認しておきます。

  "コントローラのデータセンターへの配置"

このタスクについて

コントローラに障害が発生したかどうかは、次の 2 つの方法で確認できます。

- SANtricity System Manager の Recovery Guru から、コントローラを交換するように指示されます。
- コントローラの黄色の警告 LED が点灯して、コントローラに障害が発生したことが通知されます。

> シェルフ内の両方のコントローラの警告 LED が点灯している場合は、テクニカルサポートに連絡してください。

ストレージコントローラシェルフにはストレージコントローラが 2 台搭載されているため、次の条件を満たしていれば、アプライアンスの電源がオンで読み取り / 書き込み処理が行われている間に片方のコントローラを交換できます。

- シェルフのもう一方のコントローラのステータスが「最適」である。
- SANtricity System Manager の Recovery Guru の詳細領域にある「 ok to remove 」フィールドに「 Yes 」と表示され、このコンポーネントを安全に削除できることを示します。

> シェルフの 2 台目のコントローラキャニスターのステータスが「最適」でない場合や、Recovery Guru にコントローラキャニスターを取り外すことができないことが示された場合は、テクニカルサポートにお問い合わせください。

コントローラを交換するときは、元のコントローラからバッテリを取り外し、交換用コントローラに取り付ける必要があります。

> アプライアンスのストレージコントローラには、ホストインターフェイスカード（HIC）は搭載されていません。

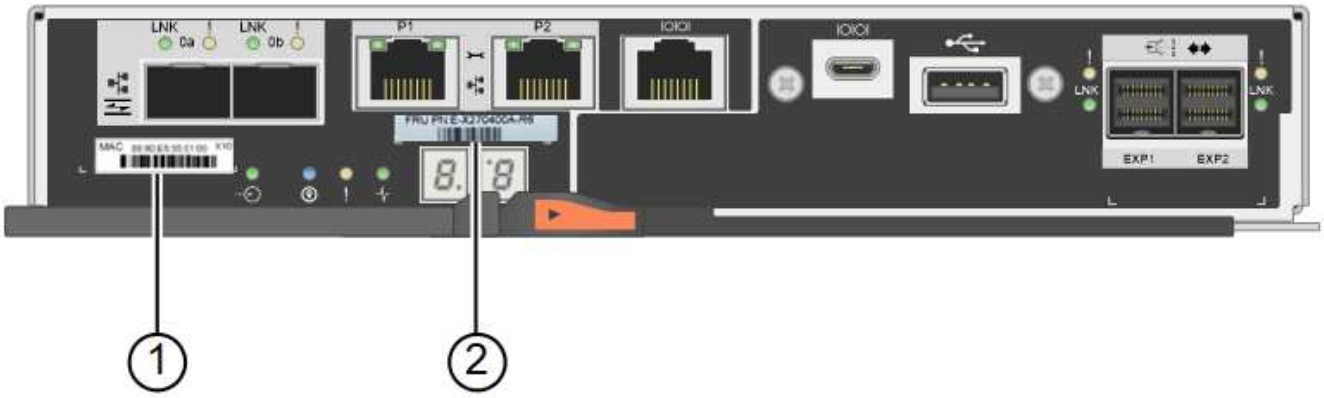
手順

1. 新しいコントローラを開封し、静電気防止処置を施した平らな場所に置きます。

   梱包材は、障害が発生したコントローラを発送するときのために保管しておいてください。

2. 交換用コントローラの背面にある MAC アドレスと FRU パーツ番号のラベルを確認します。

   この図は E2800 コントローラを示しています。EF570 コントローラの交換手順 は同じです。




| ラベル | ラベル | 説明 |
| --- | --- | --- |
| 1. | MAC アドレス | 管理ポート 1 （「P1 」）の MAC アドレス。元のコントローラの IP アドレスが DHCP を使用して取得したアドレスである場合は、新しいコントローラに接続する際にこのアドレスが必要になります。 |
| 2. | FRU パーツ番号 | FRU パーツ番号。この番号は、現在取り付けられているコントローラの交換パーツ番号と一致している必要があります。 |

3. コントローラを取り外す準備をします。

   これらの手順を実行するには、 SANtricity System Manager を使用します。詳細については、ストレージコントローラの交換に関する E シリーズの手順書を参照してください。

   a. 障害が発生したコントローラの交換パーツ番号が交換用コントローラの FRU パーツ番号と同じであることを確認します。

      コントローラに障害が発生しているため交換が必要な場合は、 Recovery Guru の詳細領域に交換パーツ番号が表示されます。この番号を手動で確認する必要がある場合は、コントローラの * Base * タブを参照してください。

      * データアクセスが失われる可能性 — * 2 つのパーツ番号が同じでない場合は、この手順 を試みないでください。

   a. 構成データベースをバックアップします。

コントローラを取り外すときに問題が発生した場合は、保存したファイルを使用して構成をリストアできます。

b. アプライアンスのサポートデータを収集します。

> コンポーネントを交換する前後にサポートデータを収集しておけば、交換しても問題が解決しない場合に、テクニカルサポートにすべてのログを送信できます。

c. 交換するコントローラをオフラインにします。

4. コントローラをアプライアンスから取り外します。

a. ESD リストバンドを装着するか、静電気防止処置を施します。

b. ケーブルにラベルを付け、ケーブルと SFP を外します。

> パフォーマンスの低下を防ぐために、ケーブルをねじったり、折り曲げたり、はさんだり、踏みつけたりしないでください。

c. カムハンドルのラッチを押してコントローラをアプライアンスから外し、カムハンドルを右側に開きます。

d. 両手でカムハンドルをつかみ、コントローラをスライドしてアプライアンスから引き出します。

> コントローラは重いので、必ず両手で支えながら作業してください。

e. 取り外し可能なカバーを上にして、静電気防止処置を施した平らな場所にコントローラを置きます。

f. カバーをボタンを押し下げながらスライドして取り外します。

5. 障害が発生したコントローラからバッテリを取り外し、交換用コントローラに取り付けます。

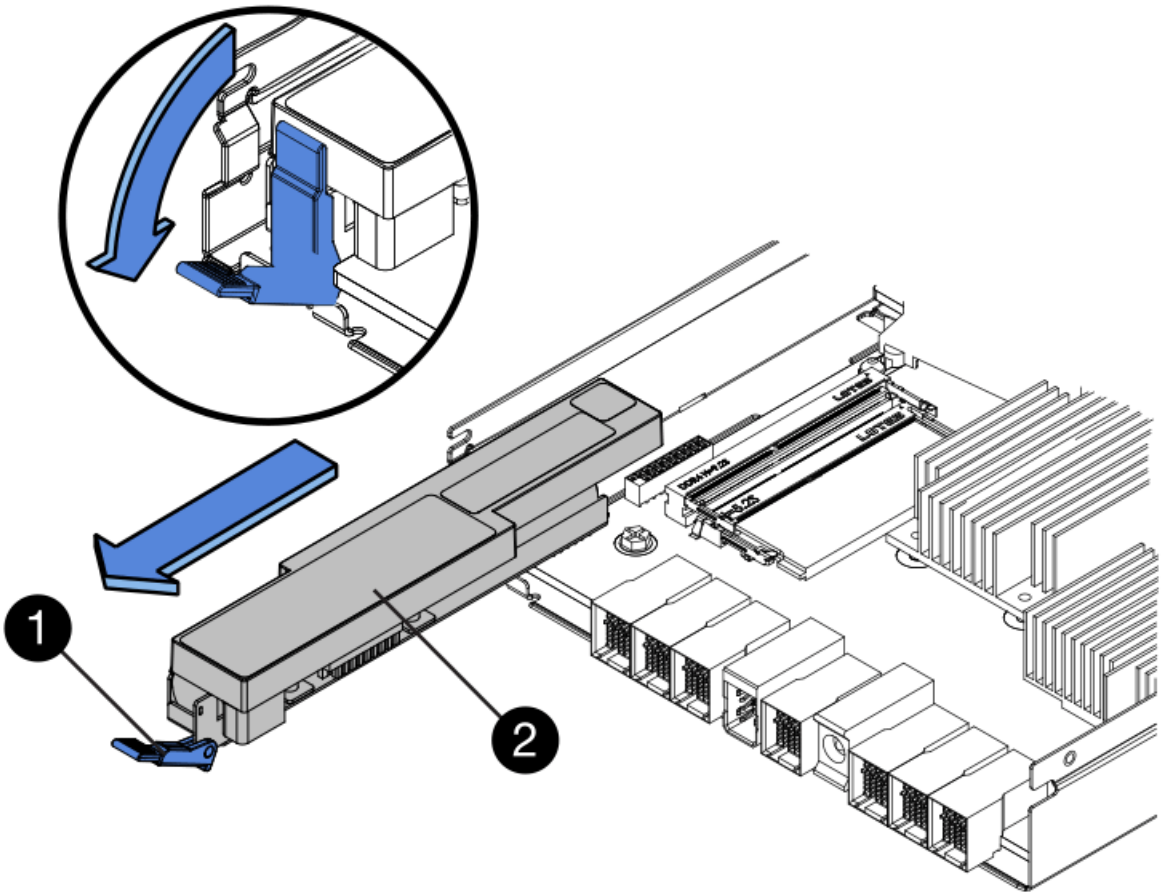
a. コントローラ内部（バッテリと DIMM の間）の緑の LED が消灯していることを確認します。

この緑の LED が点灯している場合は、コントローラがまだバッテリ電源を使用しています。この LED が消灯するのを待ってから、コンポーネントを取り外す必要があります。

| 項目 | 説明 |
| --- | --- |
| 1 | 内部キャッシュアクティブ LED |
| 2 | バッテリー |

b. バッテリの青色のリリースラッチの位置を確認します。

c. バッテリをリリースラッチを押し下げながら引き出し、コントローラから外します。




| 項目 | 説明 |
| --- | --- |
| | バッテリのリリースラッチ |
| | バッテリー |

d. バッテリを持ち上げながらスライドし、コントローラから引き出します。

e. 交換用コントローラのカバーを取り外します。

f. バッテリのスロットが手前になるよう交換用コントローラの向きを変えます。

g. バッテリを少し下に傾けながらコントローラに挿入します。

   バッテリ前部の金属製のフランジをコントローラ下部のスロットに挿入し、バッテリの上部がコントローラの左側にある小さな位置決めピンの下にくるまでスライドする必要があります。

h. バッテリラッチを上に動かしてバッテリを固定します。

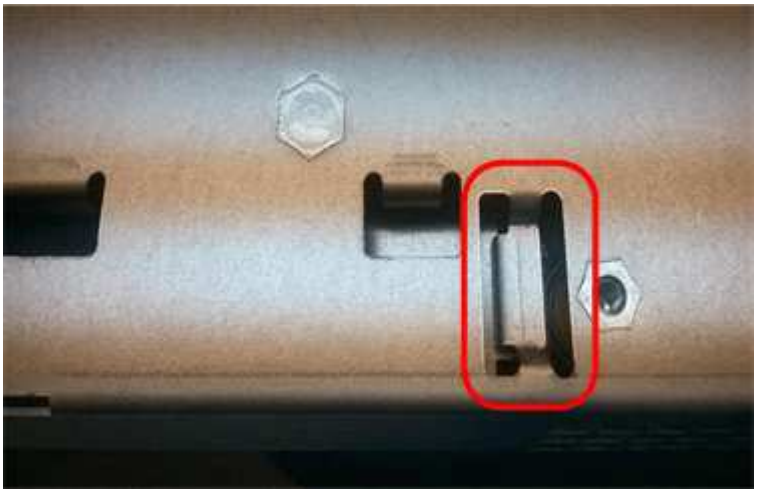
   カチッという音がしてラッチが固定されると、ラッチの下部がシャーシの金属製のスロットに収まります。

i. コントローラを裏返し、バッテリが正しく取り付けられていることを確認します。

> * ハードウェアの破損の可能性 * - バッテリ前部の金属製のフランジがコントローラのスロットにしっかりと挿入されている必要があります（ 1 つ目の図）。バッテリが正しく取り付けられていないと（ 2 つ目の図）、金属製のフランジがコントローラボードに接触し、破損の原因となる可能性があります。

- * 正解 — バッテリの金属製のフランジがコントローラのスロットに完全に挿入されています *

- * 不正解 — バッテリの金属製のフランジがコントローラのスロットに挿入されていません *



j. コントローラカバーを取り付けます。

6. 交換用コントローラをアプライアンスに取り付けます。
   a. 取り外し可能なカバーが下になるようにコントローラを裏返します。
   b. カムハンドルを開いた状態でコントローラをスライドし、アプライアンスに最後まで挿入します。
   c. カムハンドルを左側に動かして、コントローラを所定の位置にロックします。
   d. ケーブルと SFP を交換します。
   e. 元のコントローラの IP アドレスが DHCP を使用して取得したアドレスである場合は、交換用コントローラの背面のラベルに記載された MAC アドレスを確認します。取り外したコントローラの DNS / ネットワークおよび IP アドレスを交換用コントローラの MAC アドレスと関連付けるよう、ネットワ

ーク管理者に依頼します。

元のコントローラの IP アドレスが DHCP を使用して取得したアドレスでなければ、取り外したコントローラの IP アドレスが新しいコントローラで使用されます。

7. SANtricity System Manager を使用して、コントローラをオンラインにします。
   a. 「 * ハードウェア * 」を選択します。
   b. 図にドライブが表示されている場合は、 * シェルフの背面を表示 * を選択します。
   c. オンラインに切り替えるコントローラを選択します。
   d. コンテキストメニューから * オンラインに配置 * を選択し、操作を確定します。
   e. デジタル表示ディスプレイの状態がになっていることを確認します `99`。
8. 新しいコントローラのステータスが「 Optimal 」であることを確認し、サポートデータを収集します。

関連情報

"NetApp E シリーズシステムのドキュメントのサイト"

ストレージコントローラシェルフのハードウェアコンポーネントの交換

# ハードウェアの問題が発生した場合は、ストレージコントローラシェルフのコンポーネントの交換が必要となることがあります。

必要なもの

- E シリーズハードウェアの交換用手順 を用意しておきます。
- データセンターでストレージシェルフのハードウェアコンポーネントを交換するストレージアプライアンスを物理的に配置しておきます。

  "コントローラのデータセンターへの配置"

このタスクについて

ストレージコントローラのバッテリを交換するには、ストレージコントローラの交換手順の説明を参照してください。これらの手順では、アプライアンスからのコントローラの取り外し、コントローラからのバッテリの取り外し、バッテリの取り付け、およびコントローラの交換の方法について説明します。

コントローラシェルフの他の Field Replaceable Unit （ FRU ；フィールド交換可能ユニット）に関する手順については、システムメンテナンスに関する E シリーズの手順書を参照してください。

| FRU | 手順を参照してください |
| --- | --- |
| バッテリー | StorageGRID （以下の手順）：ストレージコントローラの交換 |

| FRU | 手順を参照してください |
| --- | --- |
| ドライブ | E シリーズ：<br>• ドライブの交換（ 60 ドライブ）<br>• ドライブの交換（ 12 ドライブまたは 24 ドライブ） |
| 電源キャニスター | E シリーズ<br>• 電源キャニスターの交換（ 60 ドライブ）<br>• 電源装置の交換（ 12 ドライブまたは 24 ドライブ） |
| ファンキャニスター（ 60 ドライブシェルフのみ） | E シリーズ：ファンキャニスターの交換（ 60 ドライブ） |
| ドライブドロワー（ 60 ドライブシェルフのみ） | E シリーズ：ドライブドロワーの交換（ 60 ドライブ） |

関連情報

"NetApp E シリーズシステムのドキュメントのサイト"

"ストレージコントローラの交換"

オプションの**60**ドライブ拡張シェルフのハードウェアコンポーネントの交換

## 拡張シェルフの入出力モジュール、電源装置、またはファンの交換が必要になることがあります。

必要なもの

- E シリーズハードウェアの交換用手順 を用意しておきます。
- データセンターの拡張シェルフのハードウェアコンポーネントを交換するストレージアプライアンスが物理的に配置されている。

  "コントローラのデータセンターへの配置"

このタスクについて

60 ドライブ拡張シェルフの入出力モジュール（ IOM ）を交換するには、ストレージコントローラの交換手順の説明を参照してください。

60 ドライブ拡張シェルフの電源装置またはファンを交換するには、 60 ドライブハードウェアのメンテナンスに関する E シリーズの手順書を参照してください。

| FRU | については、 E<br>シリーズの手順書を参照してください |
| --- | --- |
| 入出力モジュール（ IOM ） | IOM の交換 |
| 電源キャニスター | 電源キャニスターの交換（ 60 ドライブ） |
| ファンキャニスター | ファンキャニスターの交換（ 60 ドライブ） |

**SG6000-CN**コントローラをシャットダウンします

# ハードウェアのメンテナンスを実行するには、 SG6000-CN コントローラをシャットダウンします。

必要なもの

- データセンターでのメンテナンスが必要な SG6000-CN コントローラの物理的な場所を確認しておきます。

  "コントローラのデータセンターへの配置"

- アプライアンスのメンテナンスモードが開始されました。

  "アプライアンスをメンテナンスモードにします"

このタスクについて

サービスの中断を回避するには、通常はサービスの停止が想定される時間帯に、スケジュールされたメンテナンス期間中にコントローラをシャットダウンする前に、他のすべてのストレージノードがグリッドに接続されていることを確認してください。情報ライフサイクル管理を使用してオブジェクトを管理する手順のノード接続状態の確認に関する情報を参照してください。

> オブジェクトのコピーを 1 つだけ作成する ILM ルールを使用したことがある場合は、スケジュールされたメンテナンス時間中にコントローラをシャットダウンする必要があります。そうしないと、この手順 中にオブジェクトへのアクセスが一時的に失われる可能性があります。+ 情報ライフサイクル管理を使用したオブジェクトの管理に関する情報を参照してください

手順

1. アプライアンスをメンテナンスモードにしたら、 SG6000-CN コントローラをシャットダウンします。

   > 以下に示すコマンドを入力して、コントローラの制御シャットダウンを実行する必要があります。電源スイッチを使用してコントローラをシャットダウンすると、データが失われます。

   a. PuTTY または別の SSH クライアントを使用して、グリッドノードにログインします。
      i. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
      ii. に記載されているパスワードを入力します `Passwords.txt` ファイル。
      iii. 次のコマンドを入力してrootに切り替えます。 `su -`

iv. に記載されているパスワードを入力します `Passwords.txt` ファイル。

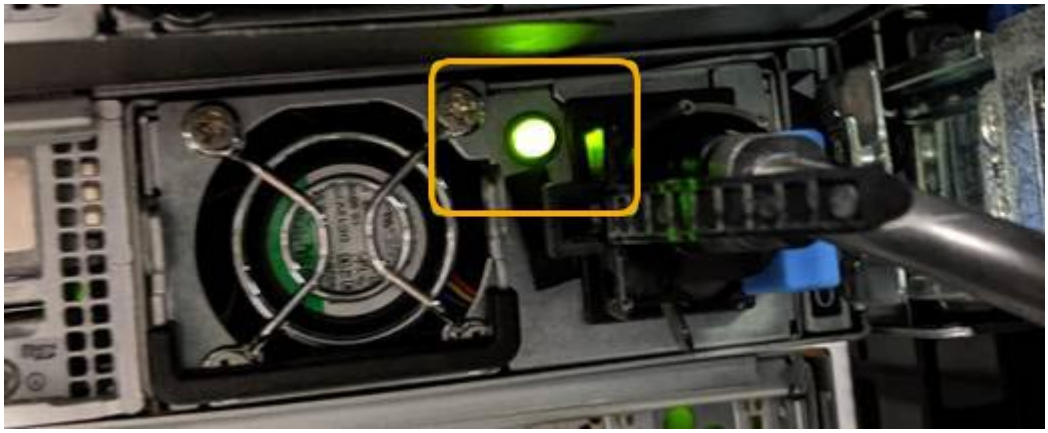
rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

b. SG6000-CNコントローラをシャットダウンします。+
**`shutdown -h now`**

このコマンドの実行には 10 分程度かかる場合があります。

2. 次のいずれかの方法を使用して、 SG6000-CN コントローラの電源がオフになっていることを確認します。
   - コントローラ前面の青色の電源 LED が消灯していることを確認します。

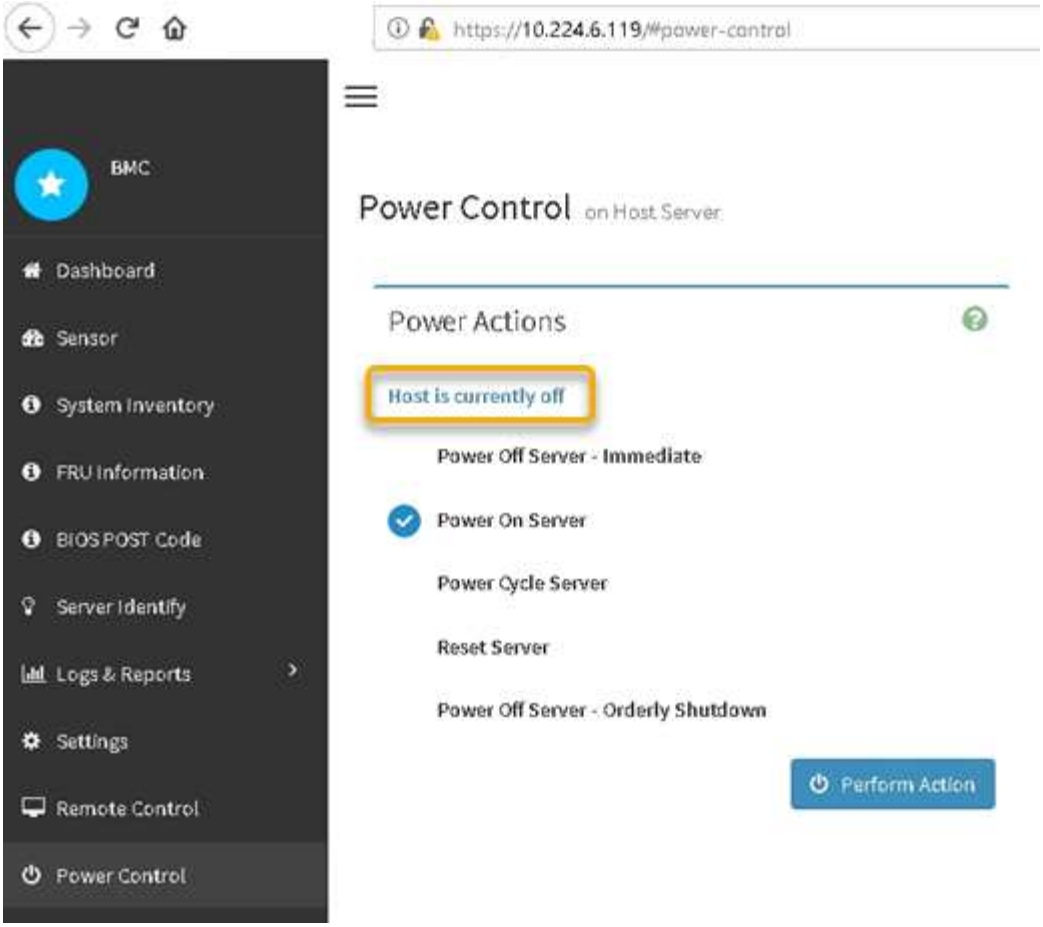
   - コントローラ背面の両方の電源装置の緑の LED を確認し、一定の速度で点滅することを確認します（ 1 秒あたり約 1 回点滅）。



   - コントローラの BMC インターフェイスを使用します。
     i. コントローラの BMC インターフェイスにアクセスします。

     "BMCインターフェイスへのアクセス"

     ii. 「 * 電源制御 * 」を選択します。
     iii. 電源操作でホストが現在オフになっていることを確認します。




関連情報

"キャビネットまたはラックからのSG6000-CNコントローラの取り外し"

**SG6000-CN**コントローラの電源をオンにして処理を確認します

## メンテナンスが完了したら、コントローラの電源をオンにします。

必要なもの

- コントローラをキャビネットまたはラックに設置し、データケーブルと電源ケーブルを接続しておきます。

  "キャビネットまたはラックへのSG6000-CNコントローラの再取り付け"

- コントローラをデータセンターに物理的に配置しておきます。

  "コントローラのデータセンターへの配置"

手順

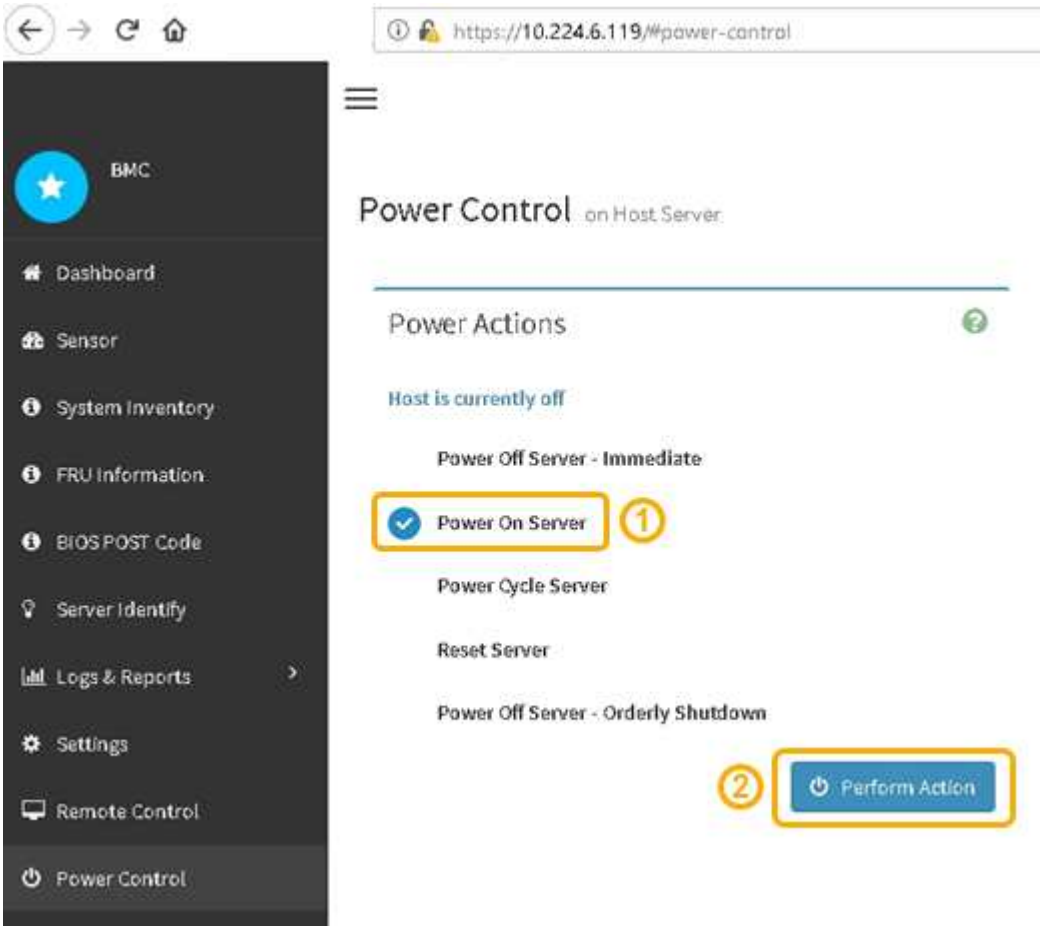
1. SG6000-CN コントローラの電源をオンにし、次のいずれかの方法でコントローラの LED とブート時のコードを監視します。

   - コントローラ前面の電源スイッチを押します。

- コントローラの BMC インターフェイスを使用します。
  i. コントローラの BMC インターフェイスにアクセスします。

     "BMCインターフェイスへのアクセス"

  ii. 「 * 電源制御 * 」を選択します。
  iii. [ サーバーの電源をオンにする *] を選択し、 [ アクションの実行 *] を選択します。




BMC インターフェイスを使用して、起動ステータスを監視します。

2. アプライアンスコントローラが Grid Manager に表示され、アラートがないことを確認します。

コントローラが Grid Manager に表示されるまでに最大 20 分かかることがあります。

3. 新しい SG6000-CN コントローラが完全に動作していることを確認します。

   a. PuTTY または別の SSH クライアントを使用して、グリッドノードにログインします。

      i. 次のコマンドを入力します。 `ssh admin@grid_node_IP`

      ii. に記載されているパスワードを入力します `Passwords.txt` ファイル。

      iii. 次のコマンドを入力してrootに切り替えます。 `su -`

      iv. に記載されているパスワードを入力します `Passwords.txt` ファイル。

      rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

   b. 次のコマンドを入力して、想定される出力が返されることを確認します。+
   `cat /sys/class/fc_host/*/port_state`

   想定される出力：

   ```
   Online
   Online
   Online
   ```

   想定する出力が返されない場合は、テクニカルサポートにお問い合わせください。

   c. 次のコマンドを入力して、想定される出力が返されることを確認します。+
   `cat /sys/class/fc_host/*/speed`

   想定される出力：

```
16 Gbit
16 Gbit
16 Gbit16 Gbit
16 Gbit
```

+
想定する出力が返されない場合は、テクニカルサポートにお問い合わせください。

   a. Grid Manager のノードページで、アプライアンスノードがグリッドに接続されていてアラートがないことを確認する。

   > このアプライアンスに緑のアイコンが表示されていないかぎり、別のアプライアンスノードをオフラインにしないでください。

4. オプション：前面ベゼルが取り外されている場合は、取り付けます。

関連情報

"SG6000-CNコントローラのステータスインジケータとボタンの表示"

"SG6000ストレージコントローラのブート時のステータスコードを確認する"

**SG6000-CN**コントローラの交換

## SG6000-CN コントローラが適切に機能しない場合や障害が発生した場合は、交換が必要となることがあります。

必要なもの

- 交換するコントローラと同じパーツ番号の交換用コントローラを用意しておきます。
- コントローラに接続する各ケーブルを識別するためのラベルを用意しておきます。
- データセンター内で交換するコントローラの物理的な場所を確認しておきます。

  "コントローラのデータセンターへの配置"

このタスクについて

SG6000-CN コントローラを交換すると、アプライアンスストレージノードにアクセスできなくなります。SG6000-CN コントローラが十分に機能している場合は、この手順 の開始時に通常の方法でシャットダウンを実行できます。

> StorageGRID ソフトウェアをインストールする前にコントローラを交換すると、この手順 の完了後すぐに StorageGRID アプライアンスインストーラにアクセスできない場合があります。アプライアンスと同じサブネット上の他のホストから StorageGRID アプライアンスインストーラにアクセスすることはできますが、他のサブネット上のホストからはアクセスできません。この状態は 15 分以内に（元のコントローラのいずれかの ARP キャッシュエントリがタイムアウトした時点で）自動的に解消されます。あるいは、古い ARP キャッシュエントリをローカルルータまたはゲートウェイから手動でパージすれば、すぐにこの状態を解消できます。

手順

1. SG6000-CN コントローラが動作していて通常の方法でシャットダウンできる場合は、 SG6000-CN コントローラをシャットダウンします。

   "SG6000-CNコントローラをシャットダウンします"

   キャッシュされたデータをドライブに書き込む必要がある場合は、 E2800 コントローラの背面にある緑のキャッシュアクティブ LED が点灯します。この LED が消灯するまで待つ必要があります。

2. 次のどちらかの方法を使用して、 SG6000-CN コントローラの電源がオフになっていることを確認します。
   - コントローラ前面の電源 LED が消灯している。
   - BMC インターフェイスの電源制御ページに、コントローラがオフになっていることが示されます。
3. コントローラに接続されている StorageGRID ネットワークが DHCP サーバを使用している場合は、 DNS / ネットワークと IP アドレスの設定を更新します。

   a. SG6000-CN コントローラの前面にある MAC アドレスラベルを確認し、管理ネットワークポートの MAC アドレスを特定します。

MAC アドレスラベルには、 BMC 管理ポートの MAC アドレスが記載されています。+ 管理ネットワークポートの MAC アドレスを特定するには、ラベルに記載された 16 進数に * 2 * を追加する必要があります。たとえば、ラベルに記載されている MAC アドレスの末尾が * 09 * の場合、管理ポートの MAC アドレスの末尾は * 0B * となります。ラベルに記載された MAC アドレスの末尾が * （ *y* ） FF* の場合、管理ポートの MAC アドレスの末尾は * （ *y*+1 ） 01 * となります。この計算を簡単に行うには、 Windows で Calculator を開き、 Programmer モードに設定して Hex を選択し、 MAC アドレスを入力してから、 **+2=** と入力します。

b. 取り外したコントローラの DNS / ネットワークおよび IP アドレスを交換用コントローラの MAC アドレスと関連付けるよう、ネットワーク管理者に依頼します。

交換用コントローラに電源を投入する前に、元のコントローラのすべての IP アドレスが更新されたことを確認する必要があります。そうしないと、コントローラのブート時に新しい DHCP IP アドレスが取得されて、 StorageGRID に再接続できなくなることがあります。この手順では、コントローラに接続されているすべての StorageGRID ネットワークを環境 接続します。

元のコントローラが静的 IP アドレスを使用していた場合は、取り外したコントローラの IP アドレスが自動的に新しいコントローラで使用されます。

4. SG6000-CN コントローラを取り外して交換します。

a. ケーブルにラベルを付けてから、ケーブルと SFP+ または SFP28 トランシーバを取り外します。

パフォーマンスの低下を防ぐために、ケーブルをねじったり、折り曲げたり、はさんだり、踏みつけたりしないでください。

b. 障害が発生したコントローラをキャビネットまたはラックから取り外します。

c. 交換用コントローラをキャビネットまたはラックに取り付けます。

d. ケーブルと SFP+ または SFP28 トランシーバを交換します。

e. コントローラの電源を入れ、コントローラの LED とブート時のコードを監視します。

5. アプライアンスストレージノードが Grid Manager に表示され、アラームが表示されていないことを確認します。

6. Grid Managerで* Nodes *を選択し、ノードコントローラのBMC IPアドレスが正しいことを確認します。

ノードコントローラの IP アドレスが無効であるか、想定範囲に含まれていない場合は、リカバリおよびメンテナンスの手順に従って IP アドレスを再設定します。

""

関連情報

"SG6000-CN：キャビネットまたはラックへの設置"

"SG6000-CNコントローラのステータスインジケータとボタンの表示"

"SG6000-CNコントローラのブート時のコードを確認する"

**SG6000-CN**コントローラの電源装置の交換

SG6000-CN コントローラには、冗長性を確保するために電源装置が 2 つあります。いずれかの電源装置で障害が発生した場合は、コンピューティングコントローラの電源の冗長性を維持するために、できるだけ早く交換する必要があります。

必要なもの

- 交換用電源装置を開封しておきます。
- データセンターの電源装置を交換するコントローラを物理的に配置しておきます。

  "コントローラのデータセンターへの配置"

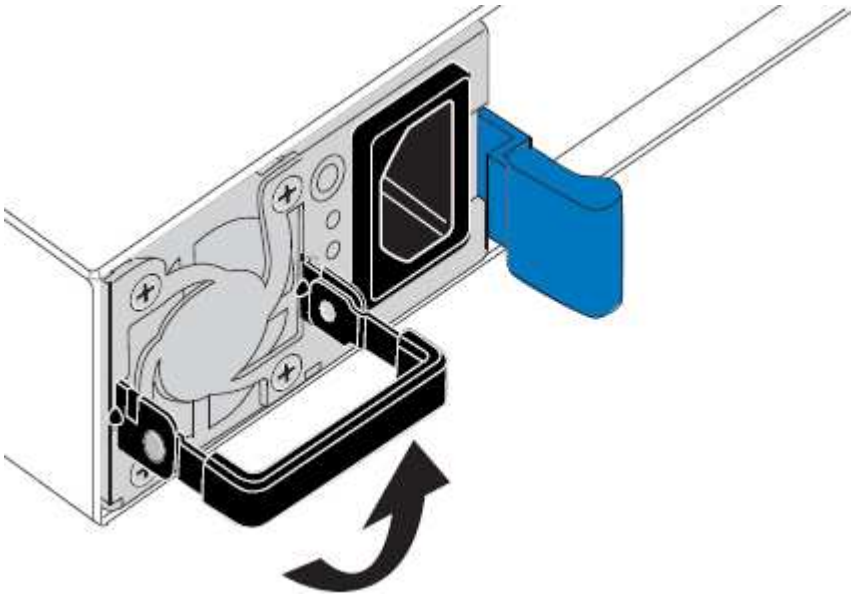
- もう 1 つの電源装置が搭載され、動作していることを確認しておきます。

このタスクについて

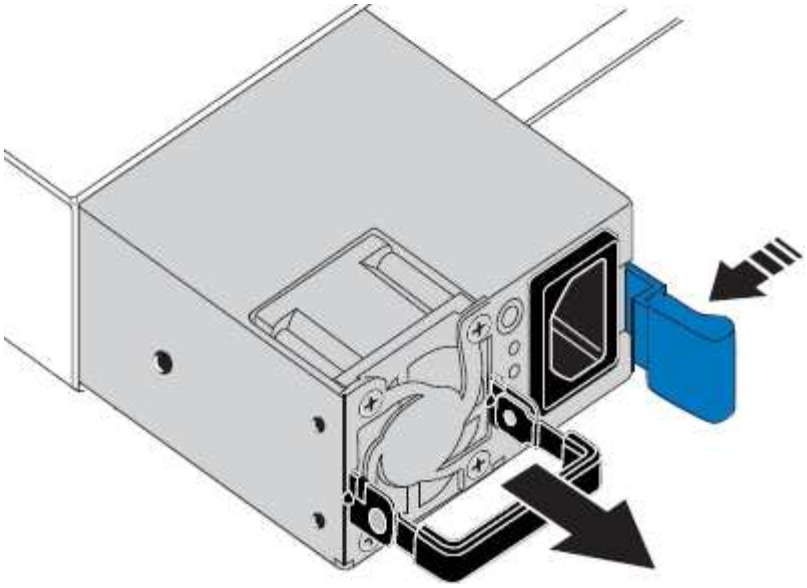
次の図は、 SG6000-CN コントローラの 2 つの電源装置を示しています。これらの装置には、コントローラの背面からアクセスできます。

手順

1. 電源装置から電源コードを抜きます。
2. カムハンドルを持ち上げます。

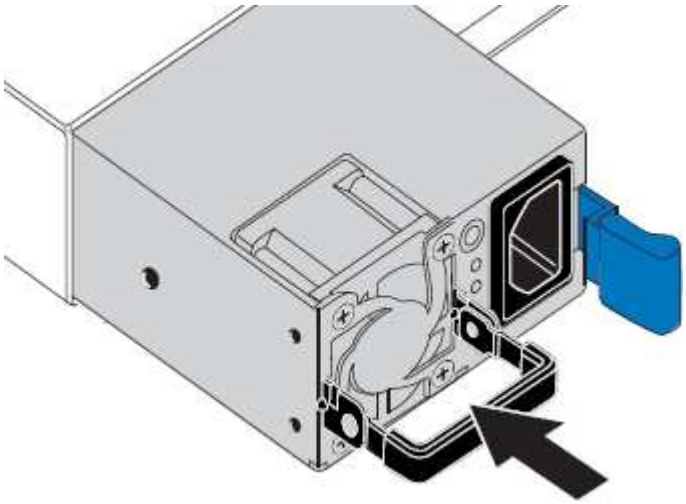


3. 青色のラッチを押し、電源装置を引き出します。



4. 交換用電源装置をシャーシにスライドさせて挿入します。

   ユニットをスライドさせて挿入するときは、青色のラッチが右側にあることを確認してください。



5. カムハンドルを下に押して、電源装置を固定します。
6. 電源コードを電源装置に接続し、緑色の LED が点灯することを確認します。

キャビネットまたはラックからの**SG6000-CN**コントローラの取り外し

## キャビネットまたはラックから SG6000-CN コントローラを取り外して上部カバーにアクセスしたり、コントローラを別の場所に移動したりします。

必要なもの

- SG6000-CN コントローラに接続する各ケーブルを識別するためのラベルを用意しておきます。
- データセンターでメンテナンスを実行する SG6000-CN コントローラを物理的に配置しておきます。

  "コントローラのデータセンターへの配置"

- SG6000-CN コントローラをシャットダウンしておきます。

  "SG6000-CNコントローラをシャットダウンします"

  電源スイッチを使用してコントローラをシャットダウンしないでください。

手順

1. コントローラの電源ケーブルにラベルを付けてから外します。
2. ESD リストバンドのストラップの端を手首に巻き付け、静電気の放電を防ぐためにクリップの端をメタルアースに固定します。
3. コントローラのデータケーブルと SFP+ または SFP28 トランシーバにラベルを付けてから外します。

   パフォーマンスの低下を防ぐために、ケーブルをねじったり、折り曲げたり、はさんだり、踏みつけたりしないでください。

4. コントローラの前面パネルにある 2 本の非脱落型ネジを緩めます。

5. 取り付けレールが完全に引き出されて両側のラッチがカチッという音がするまで、 SG6000-CN コントローラをラックから前方にスライドします。

   コントローラの上部カバーに手が届くようになっています。

6. オプション：キャビネットまたはラックからコントローラを完全に取り外す場合は、レールキットの手順に従ってレールからコントローラを取り外します。

関連情報

"SG6000-CNコントローラのカバーの取り外し"

キャビネットまたはラックへの**SG6000-CN**コントローラの再取り付け

## ハードウェアのメンテナンスが完了したら、コントローラをキャビネットまたはラックに再度取り付けます。

必要なもの

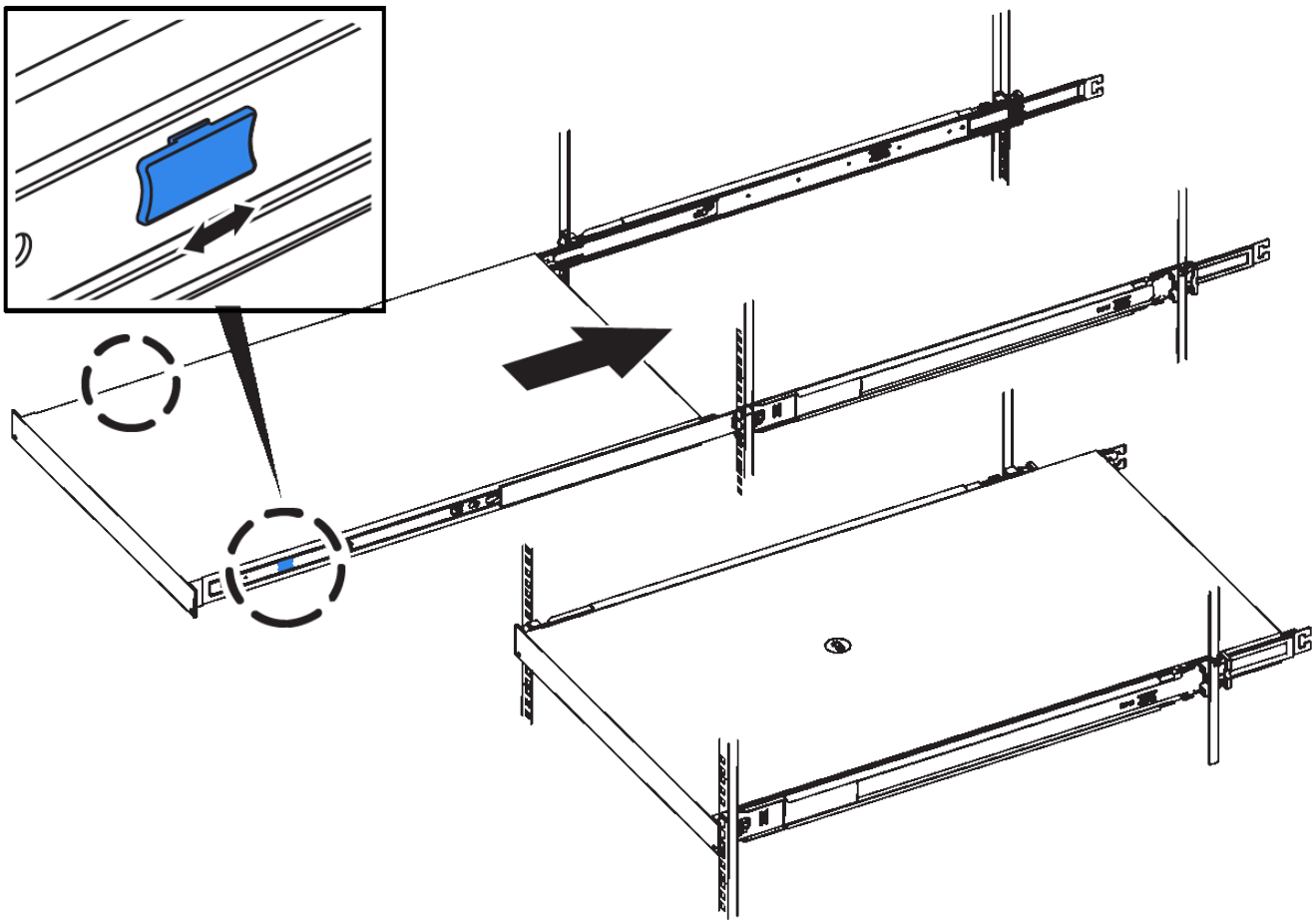
コントローラカバーを再度取り付けておきます。

"SG6000-CNコントローラカバーの再取り付け"

手順

1. 青色のレールを同時に押して両方のラックレールを外し、 SG6000-CN コントローラをラックに完全に挿入するまでスライドします。

   コントローラが途中でひっかかる場合は、シャーシの両側にある青いラッチを引いて、コントローラを奥までスライドさせます。



コントローラの電源を入れるまでは、前面ベゼルを取り付けないでください。

2. コントローラの前面パネルの非脱落型ネジを締めて、コントローラをラックに固定します。

3. ESD リストバンドのストラップの端を手首に巻き付け、静電気の放電を防ぐためにクリップの端をメタルアースに固定します。
4. コントローラのデータケーブルと SFP+ または SFP28 トランシーバを再接続します。

パフォーマンスの低下を防ぐために、ケーブルをねじったり、折り曲げたり、はさんだり、踏みつけたりしないでください。

"アプライアンスのケーブル接続（SG6000）"

5. コントローラの電源ケーブルを再接続します。

"電源コードの接続と電源の投入（SG6000）"

完了後

コントローラは再起動可能です。

"SG6000-CNコントローラの電源をオンにして処理を確認します"

**SG6000-CN**コントローラのカバーの取り外し

## メンテナンスのために内部コンポーネントにアクセスするために、コントローラカバーを取り外します。

必要なもの

コントローラをキャビネットまたはラックから取り外して、上部カバーにアクセスします。

"キャビネットまたはラックからのSG6000-CNコントローラの取り外し"

手順

1. SG6000-CN コントローラのカバーラッチがロックされていないことを確認します。必要に応じて、ラッチロックに表示されているように、プラスチック製ラッチロックの青色の 4 分の 1 回転をアンロック方向に回します。
2. ラッチを SG6000-CN コントローラシャーシの背面方向に回して止まるまで回し、シャーシから慎重にカバーを持ち上げて脇に置きます。

ESD リストバンドのストラップの端を手首に巻き付け、 SG6000-CN コントローラの内部で静電気の放電を防ぐためにクリップの端をメタルアースに固定します。

関連情報

"Fibre Channel HBAの取り外し"

**SG6000-CN**コントローラカバーの再取り付け

## 内蔵ハードウェアのメンテナンスが完了したら、コントローラカバーを再度取り付けます。

必要なもの

コントローラ内部のすべてのメンテナンス手順を完了しておきます。

手順

1. カバーラッチを開いた状態で、シャーシの上にあるカバーを持ち、上部カバーラッチの穴をシャーシのピンに合わせます。カバーの位置が合ったら、シャーシに下ろします。

2. カバーラッチが止まるまで前後に回し、カバーをシャーシに完全に固定します。カバーの前端に隙間がないことを確認します。

   カバーが完全に装着されていないと、 SG6000-CN コントローラをラックにスライドして挿入できないことがあります。

3. オプション：ラッチロックに表示されているように、青色のプラスチックラッチロックを 1 / 4 回転させてロック方向に回します。

完了後

コントローラをキャビネットまたはラックに再度取り付けます。

"キャビネットまたはラックへのSG6000-CNコントローラの再取り付け"

### **SG6000-CN**コントローラの**Fibre Channel HBA**の交換

SG6000-CN コントローラが適切に機能しない場合や障害が発生した場合は、 SG6000-CN コントローラの Fibre Channel Host Bus Adapter （ HBA ；ホストバスアダプタ）の交換が必要となることがあります。

#### 交換するファイバチャネル**HBA**の確認

交換する Fibre Channel Host Bus Adapter （ HBA ；ホストバスアダプタ）が不明な場合は、この手順 を確認してください。

必要なもの

- Fibre Channel HBA を交換する必要があるストレージアプライアンスまたは SG6000-CN コントローラのシリアル番号を確認しておきます。

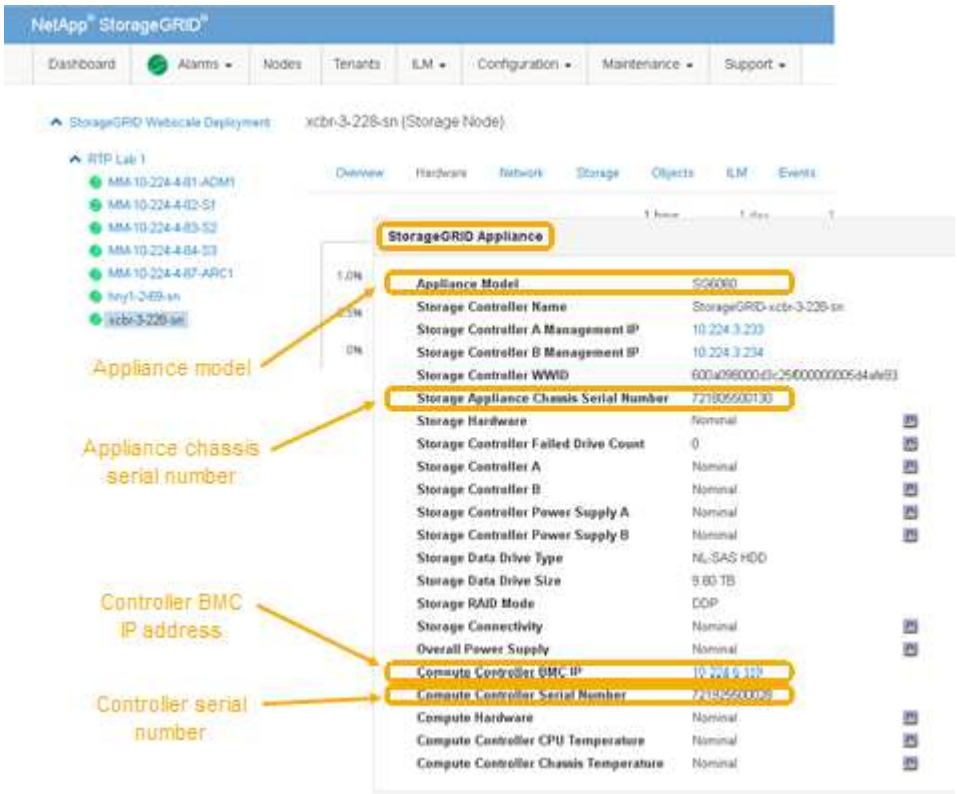
交換するファイバチャネル HBA を搭載したストレージアプライアンスのシリアル番号が先頭の文字が Q である場合、 Grid Manager には表示されません。データセンター内の各 SG6000-CN コントローラの前面に接続されているタグが一致するまで確認しておく必要があります。

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

手順

1. Grid Managerから* Nodes *を選択します。
2. ノードページのツリービューで、アプライアンスストレージノードを選択します。
3. [* ハードウェア * ] タブを選択します。

   StorageGRID アプライアンスのセクションで、ストレージアプライアンスのシャーシのシリアル番号とコンピューティングコントローラのシリアル番号を調べて、これらのシリアル番号のいずれかが、ファイバチャネルHBAを交換するストレージアプライアンスのシリアル番号と一致しているかどうかを確認します。いずれかのシリアル番号が一致していれば、正しいアプライアンスが見つかりました。




   - StorageGRID アプライアンスのセクションが表示されない場合、選択したノードは StorageGRID アプライアンスではありません。ツリービューから別のノードを選択する。
   - アプライアンスモデルが SG6060 でない場合は、ツリービューから別のノードを選択します。
   - シリアル番号が一致しない場合は、ツリービューから別のノードを選択します。
4. ファイバチャネルHBAを交換する必要があるノードの場所を確認したら、StorageGRID アプライアンスセクションに記載されているコンピューティングコントローラのBMC IPアドレスを書き留めます。

   この IP アドレスを使用すると、コンピューティングコントローラの識別 LED をオンにして、データセンターでアプライアンスを探す際に役立ちます。

"コントローラ識別LEDのオンとオフの切り替え"

関連情報

"Fibre Channel HBAの取り外し"

**Fibre Channel HBA**の取り外し

# SG6000-CN コントローラが適切に機能しない場合や障害が発生した場合は、 SG6000-CN コントローラの Fibre Channel Host Bus Adapter （ HBA ；ホストバスアダプタ）の交換が必要となることがあります。

必要なもの

- 正しい交換用の Fibre Channel HBA を用意しておきます。
- 交換する Fibre Channel HBA が搭載されている SG6000-CN コントローラを特定します。

  "交換するファイバチャネルHBAの確認"

- データセンター内の Fibre Channel HBA を交換する SG6000-CN コントローラを物理的に配置しておきます。

  "コントローラのデータセンターへの配置"

- コントローラのカバーを取り外しておきます。

  "SG6000-CNコントローラのカバーの取り外し"

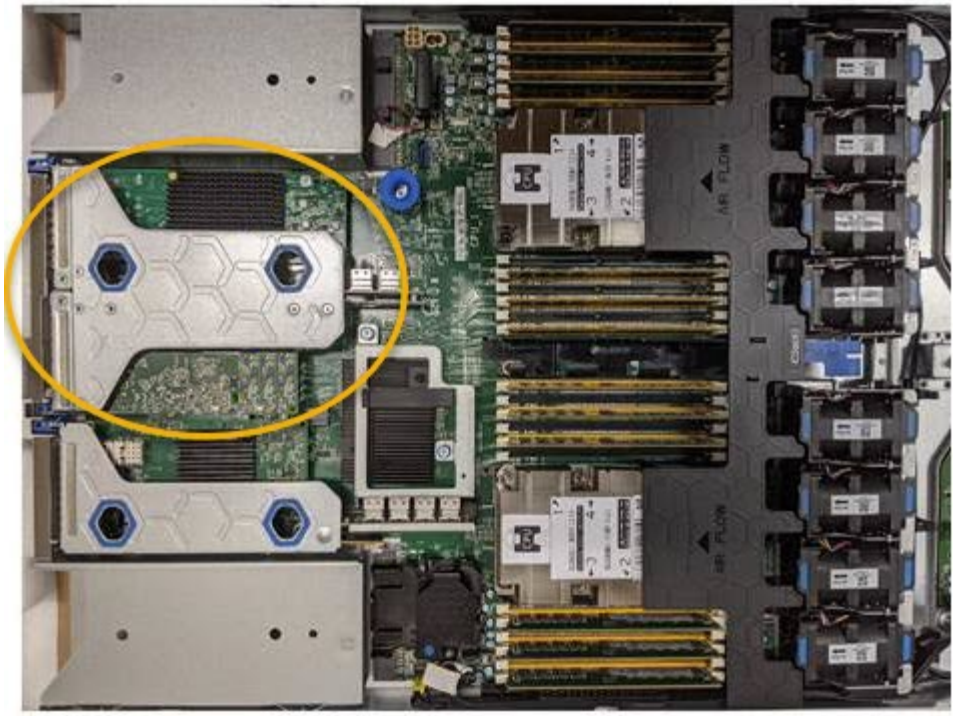
このタスクについて

サービスの中断を回避するには、 Fibre Channel HBA の交換を開始する前に他のすべてのストレージノードがグリッドに接続されていることを確認するか、定期的なメンテナンスの実行中にサービスの中断が通常どおりに発生するようにアダプタを交換してください。情報ライフサイクル管理を使用してオブジェクトを管理する手順のノード接続状態の確認に関する情報を参照してください。

オブジェクトのコピーを 1 つだけ作成する ILM ルールを使用したことがある場合は、スケジュールされたメンテナンス期間中に Fibre Channel HBA を交換する必要があります。そうしないと、この手順 中にオブジェクトへのアクセスが一時的に失われる可能性があります。+ 情報ライフサイクル管理を使用したオブジェクトの管理に関する情報を参照してください

手順

1. ESD リストバンドのストラップの端を手首に巻き付け、静電気の放電を防ぐためにクリップの端をメタルアースに固定します。
2. ファイバーチャネル HBA を搭載したコントローラの背面にあるライザーアセンブリを探します。



3. 青いマークの付いた穴を通してライザーアセンブリをつかみ、慎重に持ち上げます。取り付けられているアダプタの外部コネクタがシャーシから外れるように、ライザーアセンブリをシャーシの前面方向に持ち上げます。
4. 金属製フレーム側を下にしてライザーカードを静電気防止用の平らな場所に置き、アダプタにアクセスします。

ライザーアセンブリには、ファイバチャネル HBA とイーサネットネットワークアダプタの 2 つのアダプタがあります。この図では Fibre Channel HBA を示しています。

5. 青色のアダプタラッチ（丸で囲んだ部分）を開き、ファイバチャネル HBA をライザーアセンブリから慎重に取り外します。アダプタをわずかにロックして、アダプタをコネクタから取り外します。力を入れすぎないように注意してください。
6. アダプタを静電気防止処置を施した平らな場所に置きます。

完了後

交換用の Fibre Channel HBA を取り付けます。

"Fibre Channel HBAの再取り付け"

関連情報

"Fibre Channel HBAの再取り付け"

"StorageGRID の管理"

"トラブルシューティングを監視します"

"ILM を使用してオブジェクトを管理する"

**Fibre Channel HBA**の再取り付け

# 交換用のファイバチャネル HBA は、取り外した HBA と同じ場所に取り付けます。

必要なもの

- 正しい交換用の Fibre Channel HBA を用意しておきます。
- 既存の Fibre Channel HBA を削除しておきます。

  "Fibre Channel HBAの取り外し"

手順

1. ESD リストバンドのストラップの端を手首に巻き付け、静電気の放電を防ぐためにクリップの端をメタルアースに固定します。
2. 交換用の Fibre Channel HBA をパッケージから取り出します。
3. 青色のアダプタラッチを開いた状態で、ファイバチャネル HBA をライザーアセンブリのコネクタに合わせ、アダプタが完全に装着されるまで慎重にコネクタに押し込みます。

   ライザーアセンブリには、ファイバチャネル HBA とイーサネットネットワークアダプタの 2 つのアダプタがあります。この図では Fibre Channel HBA を示しています。

4. ライザーアセンブリの位置合わせ穴（丸で囲んだ箇所）を見つけます。この穴は、システム基板のガイドピンに合わせて配置されており、ライザーアセンブリの位置が正しいことを確認します。

5. ライザーアセンブリをシャーシに配置し、システム基板のコネクタとガイドピンの位置が合っていることを確認してから、ライザーアセンブリを挿入します。
6. ライザーアセンブリが完全に装着されるまで、青いマークの付いた穴の横にある中心線に沿って慎重に押し込みます。
7. ケーブルを再取り付けするファイバチャネル HBA ポートから保護キャップを取り外します。

完了後

コントローラで他のメンテナンス手順を実行する必要がない場合は、コントローラカバーを再度取り付けます。

"SG6000-CNコントローラカバーの再取り付け"

**SG6000-CN**コントローラのリンク設定を変更する

SG6000-CN コントローラのイーサネットリンク設定を変更することができます。ポートボンディングモード、ネットワークボンディングモード、およびリンク速度を変更できます。

必要なもの

アプライアンスのメンテナンスモードが開始されました。

"アプライアンスをメンテナンスモードにします"

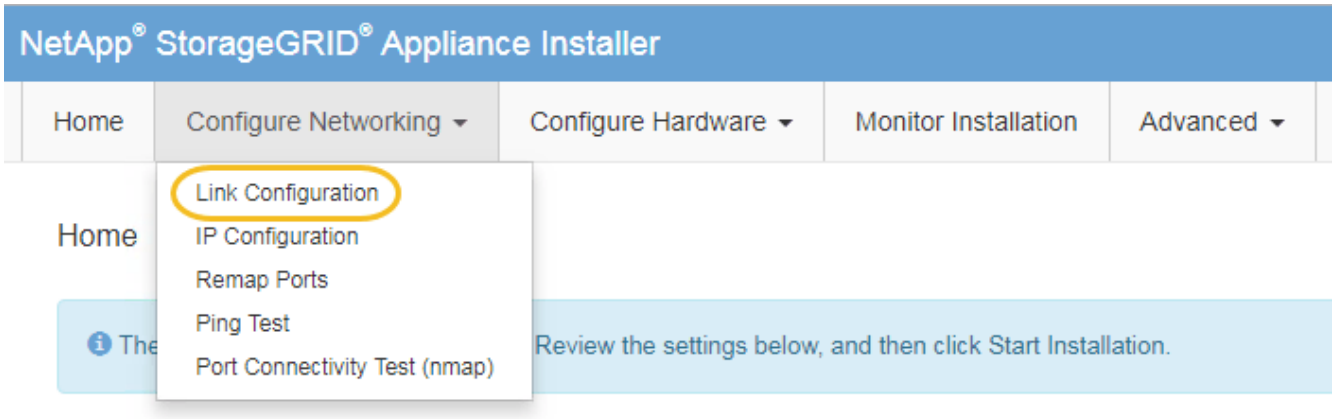
このタスクについて

SG6000-CN コントローラのイーサネットリンク設定を変更するオプションには、次のものがあります。

- ポートボンディングモード * を「 Fixed 」から「 Aggregate 」または「 Aggregate 」から「 Fixed 」に変更します
- ネットワークボンディングモード * を Active-Backup から LACP に、または LACP から Active-Backup に変更
- VLAN タグを有効または無効にするか、 VLAN タグの値を変更します
- リンク速度を変更する。

手順

1. StorageGRID アプライアンスインストーラから、 **Configure Networking**>*Link Configuration* を選択します。




1. リンク設定に必要な変更を加えます。

   オプションの詳細については、を参照してください "ネットワークリンクの設定（SG6000）"。

2. 選択に問題がなければ、 * 保存 * をクリックします。

   接続しているネットワークまたはリンクを変更すると、接続が失われる可能性があります。1分以内に再接続されない場合は、アプライアンスに割り当てられている他のIPアドレスのいずれかを使用してStorageGRID アプライアンスインストーラのURLを再入力します：+
   **`https://Appliance_Controller_IP:8443`**

   VLAN 設定を変更した場合は、アプライアンスのサブネットが変更されている可能性があります。アプライアンスのIPアドレスを変更する必要がある場合は、IPアドレスの設定手順に従います。

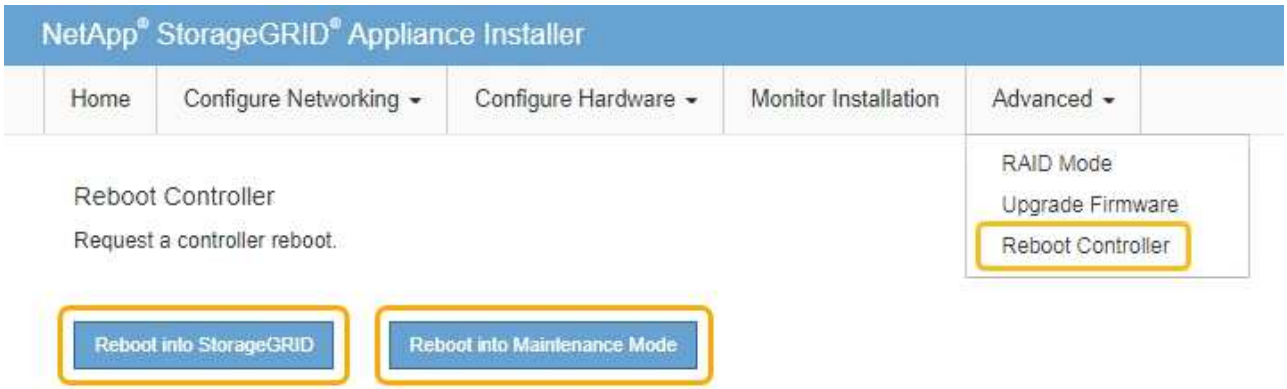
   "StorageGRID IPアドレスを設定しています"

3. メニューから [ ネットワークの設定 *>*Ping テスト *] を選択します。
4. ping テストツールを使用して、で行ったリンク設定の変更によって影響を受けた可能性のあるネットワーク上の IP アドレスへの接続を確認します リンク設定の変更 ステップ。

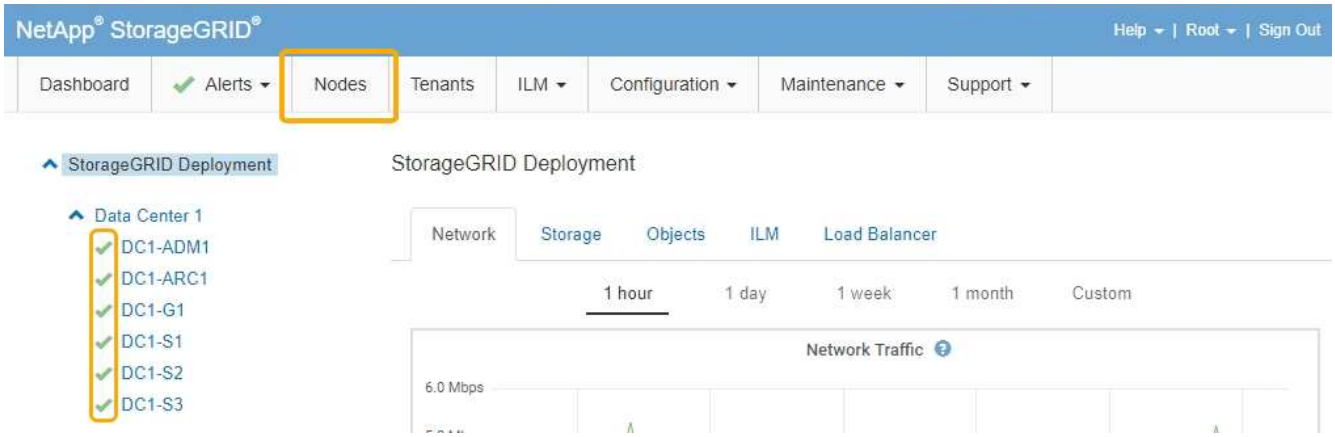
   最低でもプライマリ管理ノードのグリッドネットワーク IP アドレスと、 1 つ以上の他のストレージノードのグリッドネットワーク IP アドレスについて、 ping が通ることを確認します。必要に応じて、に戻ります リンク設定の変更 リンク設定の問題があれば手順を実行して修正します。

5. リンク設定の変更が問題なく機能していることを確認したら、ノードをリブートします。StorageGRID アプライアンス・インストーラから、 **Advanced**>*Reboot Controller* を選択し、次のいずれかのオプションを選択します。

   - Reboot into StorageGRID * を選択し、ノードをグリッドに再追加してコントローラをリブートします。メンテナンスモードで作業を完了し、ノードを通常動作に戻す準備ができている場合は、このオプションを選択します。
   - メンテナンスモードを維持したままコントローラをリブートするには、 * Reboot into Maintenance Mode * を選択します。このオプションは、グリッドに再追加する前にノードで追加のメンテナンス処理を実行する必要がある場合に選択しま
     す。




アプライアンスがリブートしてグリッドに再参加するまでに最大 20 分かかることがあります。リブートが完了し、ノードが再びグリッドに参加したことを確認するには、 Grid Manager に戻ります。[ノード*（Nodes *）]タブには、通常のステータスが表示されます ✔ アクティブなアラートがなく、ノードがグリッドに接続されていることを示す、アプライアンスノードの場合。




**MTU**設定を変更します

## アプライアンスノードの IP アドレスを設定するときに割り当てた MTU 設定を変更できます。

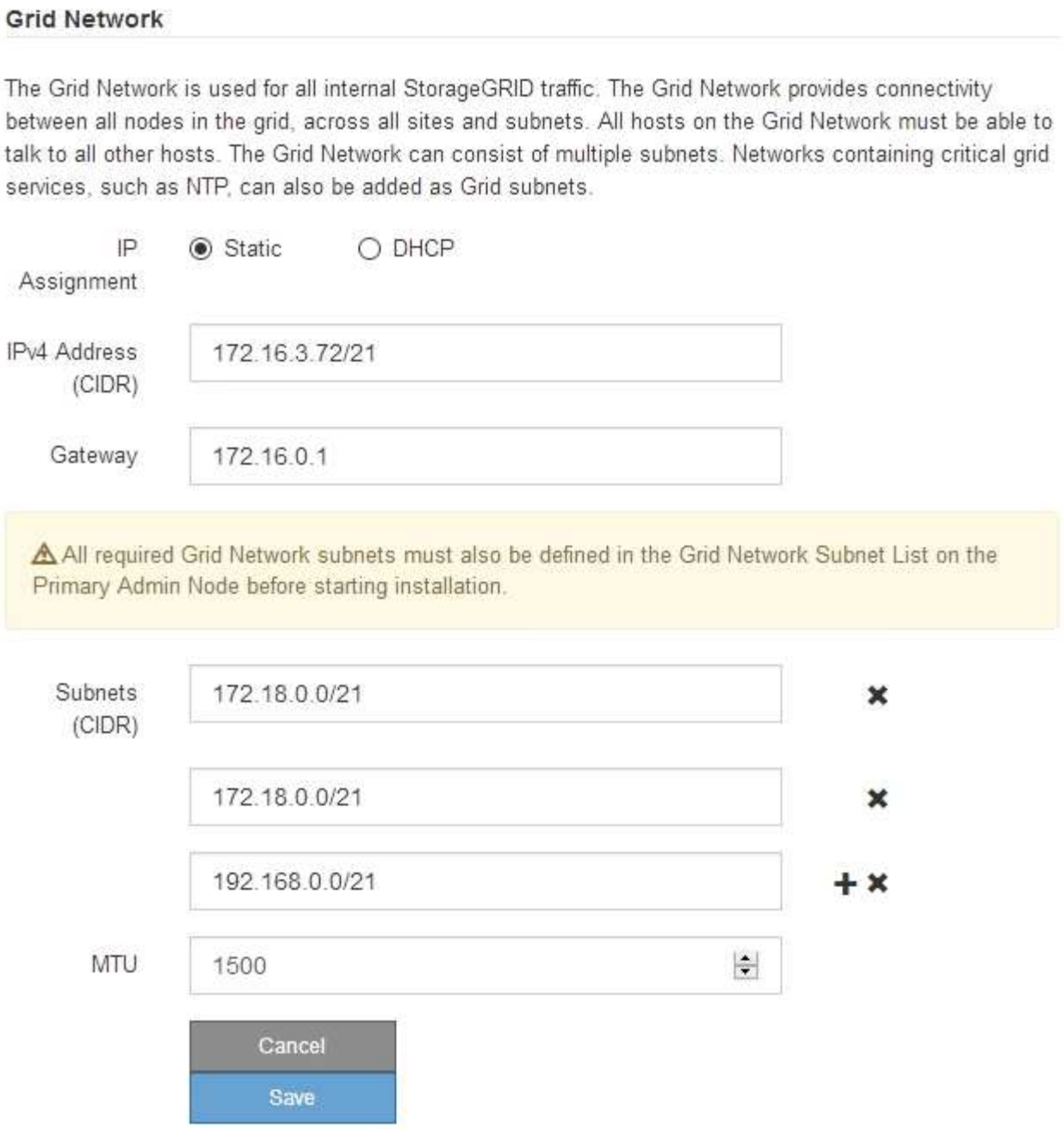
必要なもの

アプライアンスのメンテナンスモードが開始されました。

"アプライアンスをメンテナンスモードにします"

手順

1. StorageGRID アプライアンスインストーラから、 **Configure Networking**>*IP Configuration* を選択します。
2. グリッドネットワーク、管理ネットワーク、およびクライアントネットワークの MTU 設定に必要な変更を加えます。



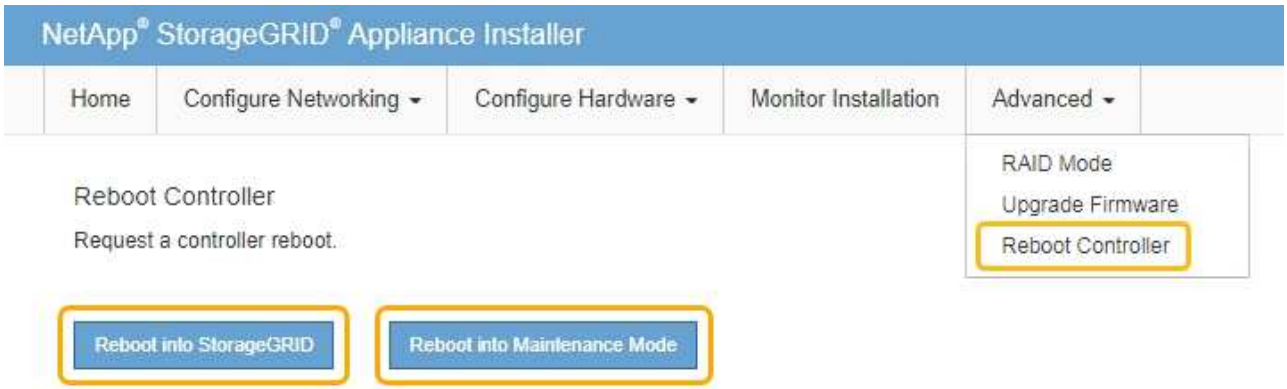

ネットワークの MTU 値は、ノードが接続されているスイッチポートに設定されている値と同じである必要があります。そうしないと、ネットワークパフォーマンスの問題やパケット損失が発生する可能性があります。

ネットワークのパフォーマンスを最大限に高めるには、すべてのノードのグリッドネットワークインターフェイスで MTU 値がほぼ同じになるように設定する必要があります。個々のノードのグリッドネットワークの MTU 設定に大きな違いがある場合は、 * Grid Network MTU mismatch * アラートがトリガーされます。MTU 値はすべてのネットワークタイプで同じである必要はありません。

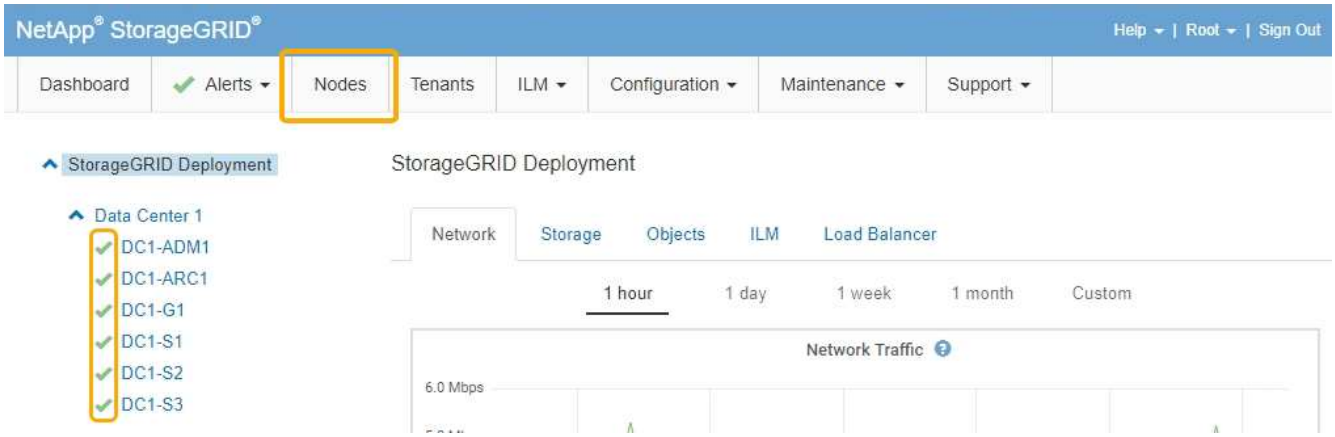
3. 設定に問題がなければ、「 * 保存 * 」を選択します。
4. ノードをリブートします。StorageGRID アプライアンス・インストーラから、 **Advanced**>*Reboot

Controller* を選択し、次のいずれかのオプションを選択します。

- Reboot into StorageGRID * を選択し、ノードをグリッドに再追加してコントローラをリブートします。メンテナンスモードで作業を完了し、ノードを通常動作に戻す準備ができている場合は、このオプションを選択します。
- メンテナンスモードを維持したままコントローラをリブートするには、 * Reboot into Maintenance Mode * を選択します。このオプションは、グリッドに再追加する前にノードで追加のメンテナンス処理を実行する必要がある場合に選択しま
す。




アプライアンスがリブートしてグリッドに再参加するまでに最大 20 分かかることがあります。リブートが完了し、ノードが再びグリッドに参加したことを確認するには、 Grid Manager に戻ります。[ノード*（Nodes *）]タブには、通常のステータスが表示されます ✔ アクティブなアラートがなく、ノードがグリッドに接続されていることを示す、アプライアンスノードの場合。




関連情報

"StorageGRID の管理"

**DNS**サーバの設定を確認しています

このアプライアンスノードで現在使用されているドメインネームシステム（ DNS ）サーバを確認し、一時的に変更することができます。

必要なもの

アプライアンスのメンテナンスモードが開始されました。

"アプライアンスをメンテナンスモードにします"

このタスクについて

KMS のホスト名は IP アドレスではなくドメイン名として指定されているため、暗号化されたアプライアンスがキー管理サーバ（ KMS ）または KMS クラスタに接続できない場合は、 DNS サーバ設定の変更が必要になることがあります。アプライアンスの DNS 設定に加えた変更は一時的なものであり、メンテナンスモードを終了すると失われます。これらの変更を永続的に行うには、Grid ManagerでDNSサーバを指定します（* Maintenance > Network > DNS Servers *）。

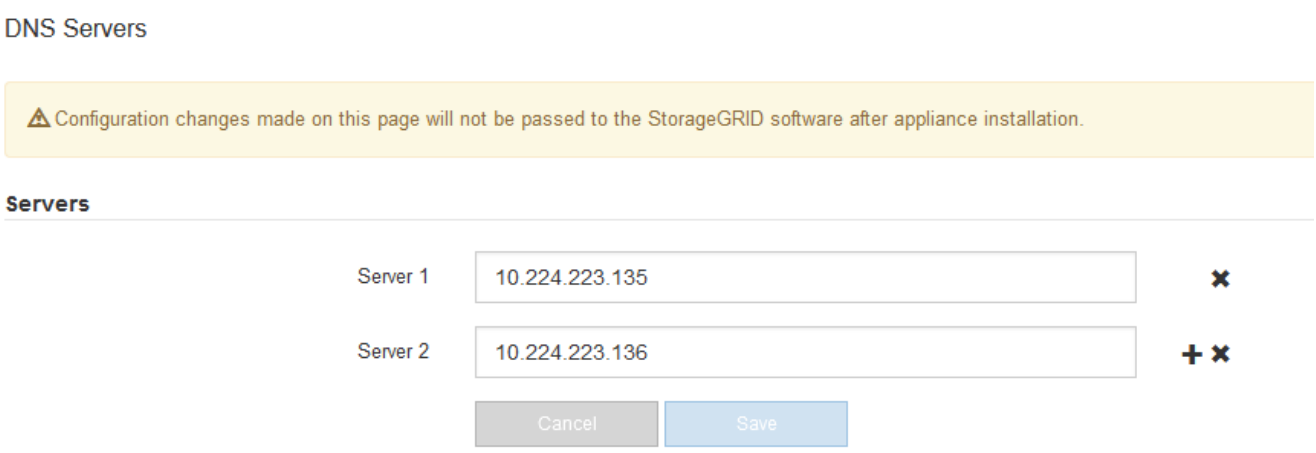
- DNS 設定の一時的な変更が必要になるのは、ホスト名に IP アドレスではなく完全修飾ドメイン名を使用して KMS サーバが定義されているノード暗号化アプライアンスのみです。
- ノード暗号化アプライアンスをドメイン名を使用して KMS に接続する場合は、グリッド用に定義されている DNS サーバの 1 つに接続する必要があります。これらの DNS サーバの 1 つが、ドメイン名を IP アドレスに変換します。
- ノードがグリッドの DNS サーバにアクセスできない場合、またはノード暗号化アプライアンスノードがオフラインのときにグリッド全体の DNS 設定を変更した場合は、ノードは KMS に接続できません。アプライアンス上の暗号化されたデータは、 DNS 問題 が解決されるまで復号化できません。

KMS 接続を回避する DNS 問題 を解決するには、 StorageGRID アプライアンスインストーラで 1 つ以上の DNS サーバの IP アドレスを指定します。この一時的な DNS 設定により、アプライアンスは KMS に接続してノード上のデータを復号化することができます。

たとえば、暗号化されたノードがオフラインのときにグリッドの DNS サーバが変更された場合、ノードは以前の DNS 値をまだ使用しているため、オンラインに戻った時点で KMS にアクセスできなくなります。StorageGRID アプライアンスインストーラで新しい DNS サーバの IP アドレスを入力すると、 KMS 接続を使用してノードのデータを復号化できます。

手順

1. StorageGRID アプライアンスインストーラから、 **Configure Networking *>*DNS Configuration** を選択します。
2. 指定した DNS サーバが正しいことを確認してください。




3. 必要に応じて、 DNS サーバを変更します。

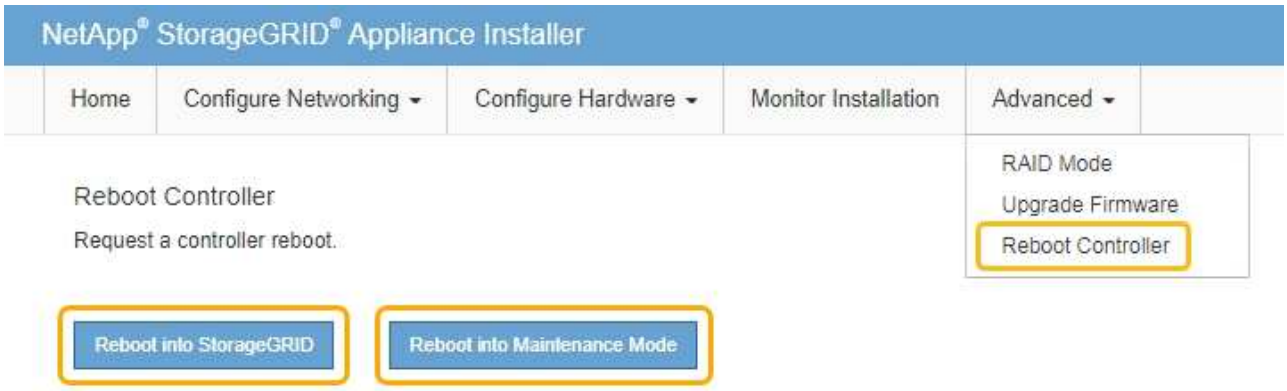
DNS 設定に対する変更は一時的なものであり、メンテナンスモードを終了すると失われます。

4. 一時的な DNS 設定に問題がなければ、 * 保存 * を選択します。

   ノードは、このページで指定されている DNS サーバ設定を使用して KMS に再接続し、ノード上のデータを復号化できるようにします。

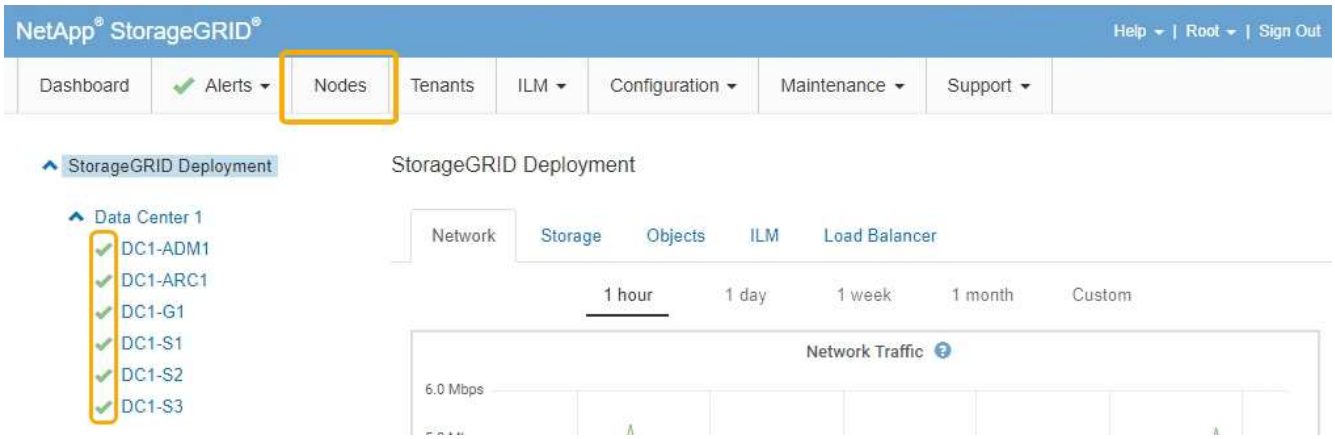
5. ノードデータが復号化されたら、ノードをリブートします。StorageGRID アプライアンス・インストーラから、 **Advanced**>*Reboot Controller* を選択し、次のいずれかのオプションを選択します。

   - Reboot into StorageGRID * を選択し、ノードをグリッドに再追加してコントローラをリブートします。メンテナンスモードで作業を完了し、ノードを通常動作に戻す準備ができている場合は、このオプションを選択します。
   - メンテナンスモードを維持したままコントローラをリブートするには、 * Reboot into Maintenance Mode * を選択します。このオプションは、グリッドに再追加する前にノードで追加のメンテナンス処理を実行する必要がある場合に選択します。




ノードがリブートしてグリッドに再び参加すると、 Grid Manager にリストされているシステム全体の DNS サーバが使用されます。グリッドに再追加したあとは、アプライアンスがメンテナンスモードのときに、 StorageGRID アプライアンスインストーラで指定された一時的な DNS サーバがアプライアンスで使用されなくなります。

アプライアンスがリブートしてグリッドに再参加するまでに最大 20 分かかることがあります。リブートが完了し、ノードが再びグリッドに参加したことを確認するには、 Grid Manager に戻ります。[ノード*（Nodes *）]タブには、通常のステータスが表示されます アクティブなアラートがなく、ノードがグリッドに接続されていることを示す、アプライアンスノードの場合。




メンテナンスモードでのノード暗号化の監視

# インストール中にアプライアンスのノード暗号化を有効にした場合は、ノード暗号化の状態やキー管理サーバ（ KMS ）の詳細など、各アプライアンスノードのノード暗号化ステータスを監視できます。

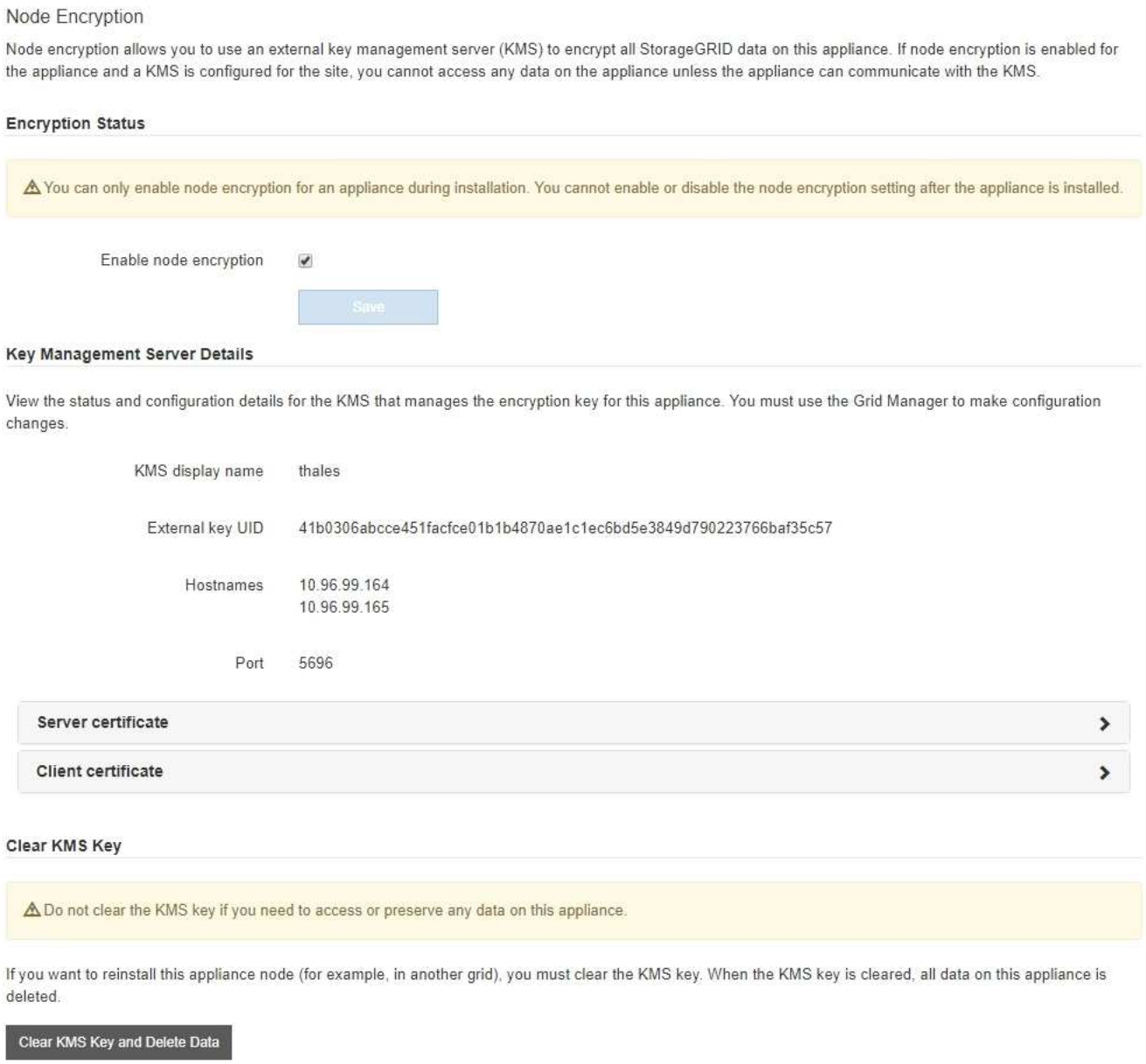
必要なもの

- インストール時にアプライアンスのノード暗号化を有効にしておく必要があります。アプライアンスのインストール後にノード暗号化を有効にすることはできません。
- アプライアンスはメンテナンスモードになりました。

  "アプライアンスをメンテナンスモードにします"

手順

1. StorageGRID アプライアンスインストーラから、 * ハードウェアの設定 * > * ノード暗号化 * を選択します。




Node Encryption のページには次の 3 つのセクションがあります。

- Encryption Status には、アプライアンスでノード暗号化が有効か無効かが表示されます。
- キー管理サーバの詳細には、アプライアンスの暗号化に使用されている KMS に関する情報が表示されます。サーバおよびクライアント証明書のセクションを展開すると、証明書の詳細およびステータスを表示できます。
  - 期限切れの証明書の更新など、証明書自体に関する問題に対処するには、 StorageGRID の管理手順の KMS に関する情報を参照してください。
  - KMS ホストへの接続で予期しない問題が発生する場合は、ドメインネームシステム（ DNS ）サーバが正しいこと、およびアプライアンスのネットワークが正しく設定されていることを確認してください。

    "DNSサーバの設定を確認しています"

  - 証明書の問題を解決できない場合は、テクニカルサポートにお問い合わせください。

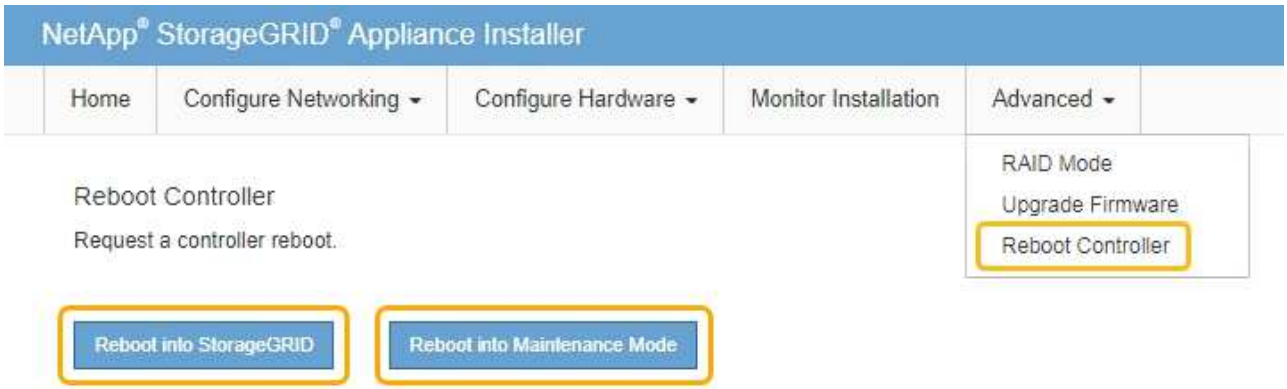
- KMS Key をクリアすると、アプライアンスのノード暗号化が無効になり、 StorageGRID サイト用に設定されているアプライアンスとキー管理サーバの間の関連付けが解除され、アプライアンスのすべてのデータが削除されます。別の StorageGRID システムにアプライアンスをインストールする前に、KMS キーをクリアする必要があります。

  "キー管理サーバ設定のクリア"

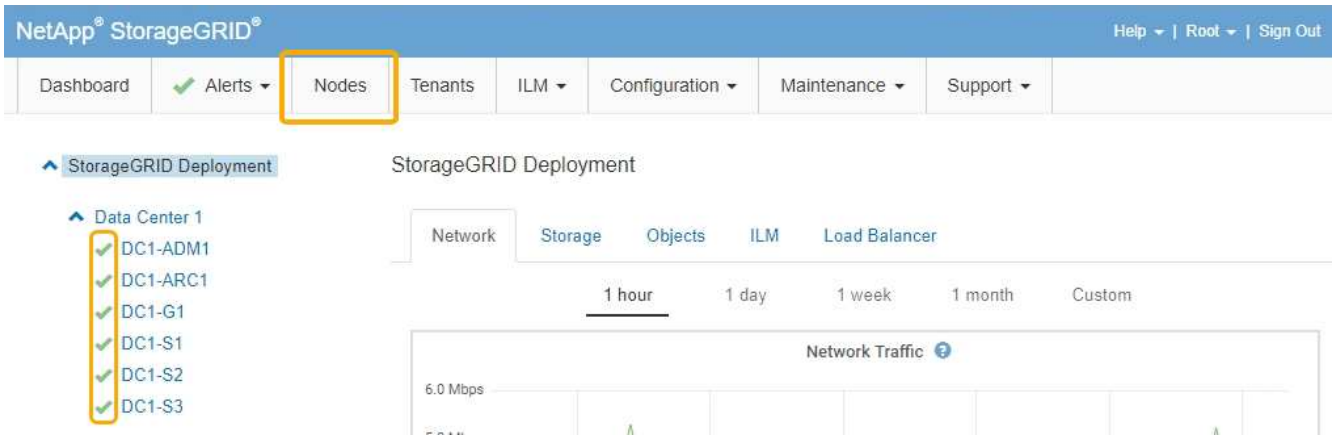
  KMS の設定をクリアすると、アプライアンスからデータが削除され、永久にアクセスできなくなります。このデータはリカバリできません。

2. ノード暗号化ステータスの確認が完了したら、ノードをリブートします。StorageGRID アプライアンス・インストーラから、 **Advanced**>*Reboot Controller* を選択し、次のいずれかのオプションを選択します。

   - Reboot into StorageGRID * を選択し、ノードをグリッドに再追加してコントローラをリブートします。メンテナンスモードで作業を完了し、ノードを通常動作に戻す準備ができている場合は、このオプションを選択します。
   - メンテナンスモードを維持したままコントローラをリブートするには、 * Reboot into Maintenance Mode * を選択します。このオプションは、グリッドに再追加する前にノードで追加のメンテナンス処理を実行する必要がある場合に選択します。




アプライアンスがリブートしてグリッドに再参加するまでに最大 20 分かかることがあります。リブートが完了し、ノードが再びグリッドに参加したことを確認するには、 Grid Manager に戻ります。[ノード*（Nodes *）]タブには、通常のステータスが表示されます ✔ アクティブなアラートがなく、ノードがグリッドに接続されていることを示す、アプライアンスノードの場合。




関連情報

"StorageGRID の管理"

キー管理サーバ設定のクリア

# キー管理サーバ（ KMS ）の設定をクリアすると、アプライアンスでノード暗号化が無効になります。KMS の設定をクリアすると、アプライアンスのデータは完全に削除され、アクセスできなくなります。このデータはリカバリできません。

必要なもの

アプライアンス上のデータを保持する必要がある場合は、KMSの設定をクリアする前に、ノードの運用停止手順 を実行する必要があります。

KMS をクリアすると、アプライアンスのデータが完全に削除され、アクセスできなくなります。このデータはリカバリできません。

ノードを運用停止して、格納されているデータをStorageGRID 内の他のノードに移動します。グリッドノードの運用停止手順については、リカバリとメンテナンスの手順を参照してください。

このタスクについて

アプライアンス KMS の設定をクリアすると、ノード暗号化が無効になり、アプライアンスノードと StorageGRID サイトの KMS の設定との間の関連付けが解除されます。その後、アプライアンスのデータが削除され、アプライアンスはインストール前の状態のままになります。このプロセスを元に戻すことはできません。

KMS の設定をクリアする必要があります。

- アプライアンスを別の StorageGRID システムにインストールする前に、 KMS を使用しない、または別の KMS を使用する前に、

  同じ KMS キーを使用する StorageGRID システムにアプライアンスノードを再インストールする場合は、 KMS の設定をクリアしないでください。

- KMS 設定が失われて KMS キーをリカバリおよび再インストールできないノードをリカバリする前に、 KMS キーをリカバリできません。
- お客様のサイトで以前使用していたアプライアンスを返却する前に、

- ノード暗号化が有効になっているアプライアンスの運用を停止したあと。

> KMS をクリアして StorageGRID システム内の他のノードにデータを移動する前に、アプライアンスの運用を停止します。アプライアンスの運用を停止する前に KMS をクリアすると、データが失われるため、アプライアンスが動作しなくなる可能性があります。

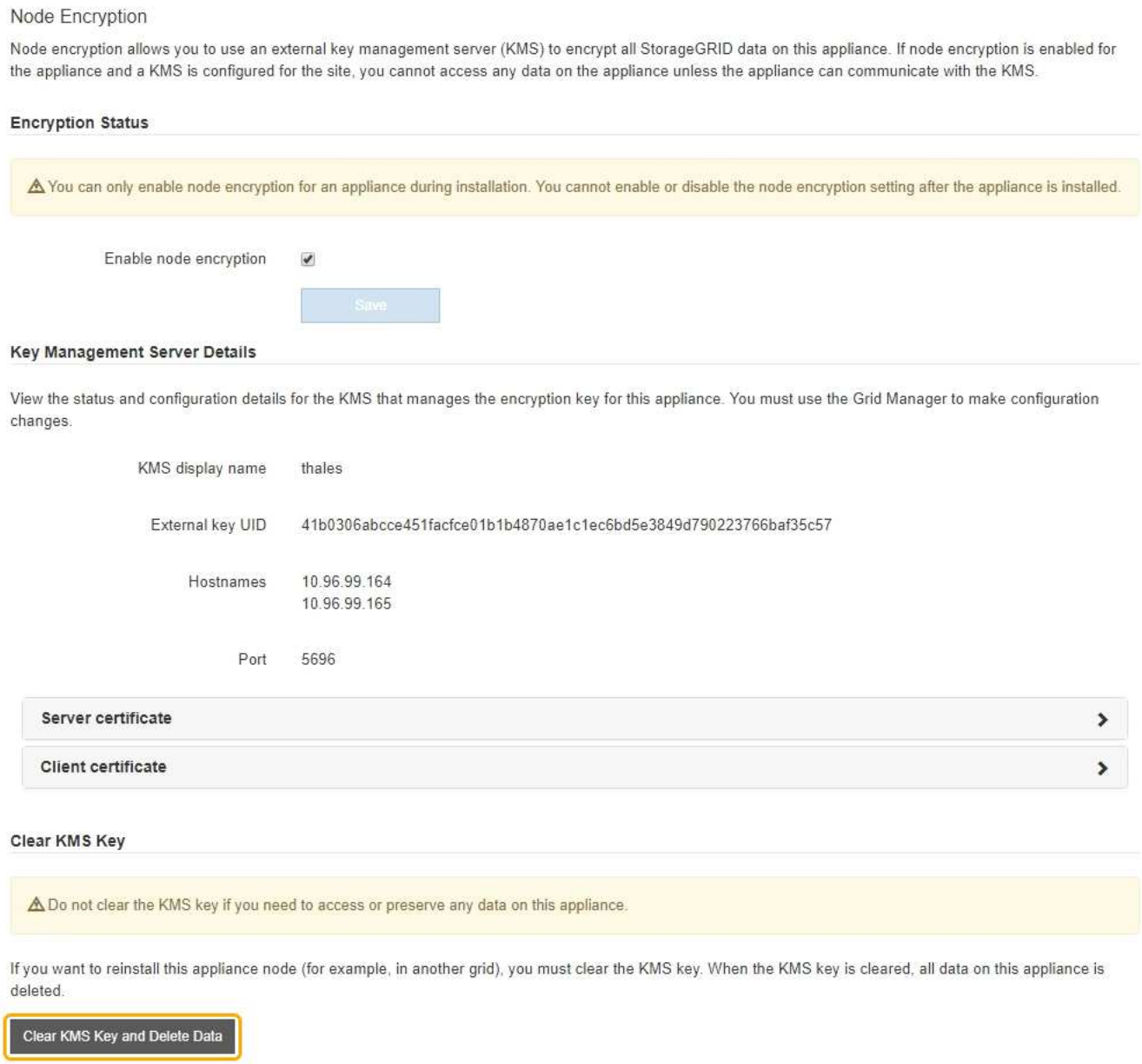
手順

1. ブラウザを開き、アプライアンスのコンピューティングコントローラの IP アドレスのいずれかを入力します。[+]
   **`https://Controller_IP:8443`**

   *`Controller_IP`* は、3つのStorageGRID ネットワークのいずれかでのコンピューティングコントローラ（ストレージコントローラではない）のIPアドレスです。

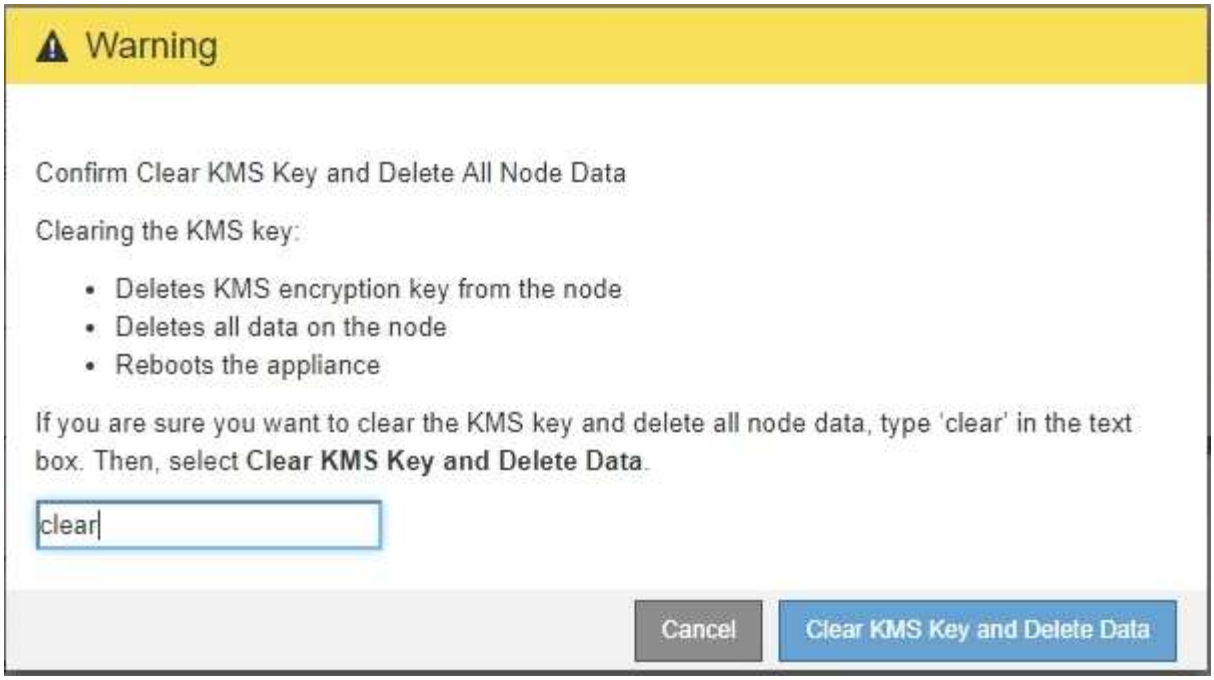
   StorageGRID アプライアンスインストーラのホームページが表示されます。

2. Configure Hardware * > * Node Encryption * を選択します。




KMS の設定をクリアすると、アプライアンス上のデータが完全に削除されます。このデータはリカバリできません。

3. ウィンドウの下部で、 * KMS キーをクリアしてデータを削除 * を選択します。
4. KMSの設定をクリアしても問題がない場合は、「+」と入力します **`clear`** +を押して、「* KMSキーを消去してデータを削除*」を選択します。




KMS 暗号化キーとすべてのデータがノードから削除され、アプライアンスがリブートします。この処理には 20 分程度かかる場合があります。

5. ブラウザを開き、アプライアンスのコンピューティングコントローラの IP アドレスのいずれかを入力します。[+]
**`https://Controller_IP:8443`**

   *`Controller_IP`* は、3つのStorageGRID ネットワークのいずれかでのコンピューティングコントローラ（ストレージコントローラではない）のIPアドレスです。

   StorageGRID アプライアンスインストーラのホームページが表示されます。

6. Configure Hardware * > * Node Encryption * を選択します。
7. ノードの暗号化が無効になっていること、および * キー管理サーバの詳細 * および * KMS キーと削除 * のコントロールでキーと証明書の情報がウィンドウから削除されていることを確認します。

   アプライアンスでのノード暗号化の再インストールまでは、グリッドでのノード暗号化を再度有効にすることはできません。

完了後

アプライアンスがリブートし、 KMS がクリアされてインストール前の状態になっていることを確認したら、StorageGRID システムからアプライアンスを物理的に取り外すことができます。再インストールのためのアプライアンスの準備については、リカバリおよびメンテナンスの手順を参照してください。

関連情報

"StorageGRID の管理"

""

# SG5700 ストレージアプライアンス

StorageGRID SG5712とSG5760アプライアンスの設置とメンテナンスの方法について説明します。

- "StorageGRID アプライアンスの概要"
- "インストールと導入の概要"
- "設置を準備しています"
- "ハードウェアを設置"
- "ハードウェアの設定"
- "アプライアンスストレージノードの導入"
- "ストレージアプライアンスのインストールの監視"
- "アプライアンスのインストールと設定の自動化"
- "インストール REST API の概要"
- "ハードウェアの設置のトラブルシューティング"
- "SG5700アプライアンスのメンテナンス"

## StorageGRID アプライアンスの概要

SG5700 StorageGRID アプライアンスは、 StorageGRID グリッドにおいてストレージノードとして機能する、ストレージとコンピューティングを統合したプラットフォームです。アプライアンスは、アプライアンスストレージノードと仮想（ソフトウェアベース）ストレージノードを組み合わせたハイブリッドグリッド環境で使用できます。

StorageGRID SG5700 アプライアンスには次のような特長があります。

- StorageGRID ストレージノードのストレージ要素とコンピューティング要素を統合します。
- ストレージノードの導入と設定を簡易化する StorageGRID アプライアンスインストーラが搭載されています。
- ハードウェアの管理と監視に使用する E シリーズ SANtricity System Manager が搭載されています。
- StorageGRID のグリッドネットワークとクライアントネットワークとの 10GbE または 25GbE 接続を最大 4 つサポートします。
- Full Disk Encryption （ FDE ）ドライブまたは連邦情報処理標準（ FIPS ）ドライブに対応しています。これらのドライブを SANtricity System Manager のドライブセキュリティ機能と併用すると、データへの不正アクセスを防止できます。

SG5700 アプライアンスには SG5712 と SG5760 の 2 つのモデルがあります。どちらのモデルにも次のコンポーネントが含まれています。

| コンポーネント | **SG5712** | **SG5760** |
| --- | --- | --- |
| コンピューティングコントローラ | E5700SG コントローラのものです | E5700SG コントローラのものです |

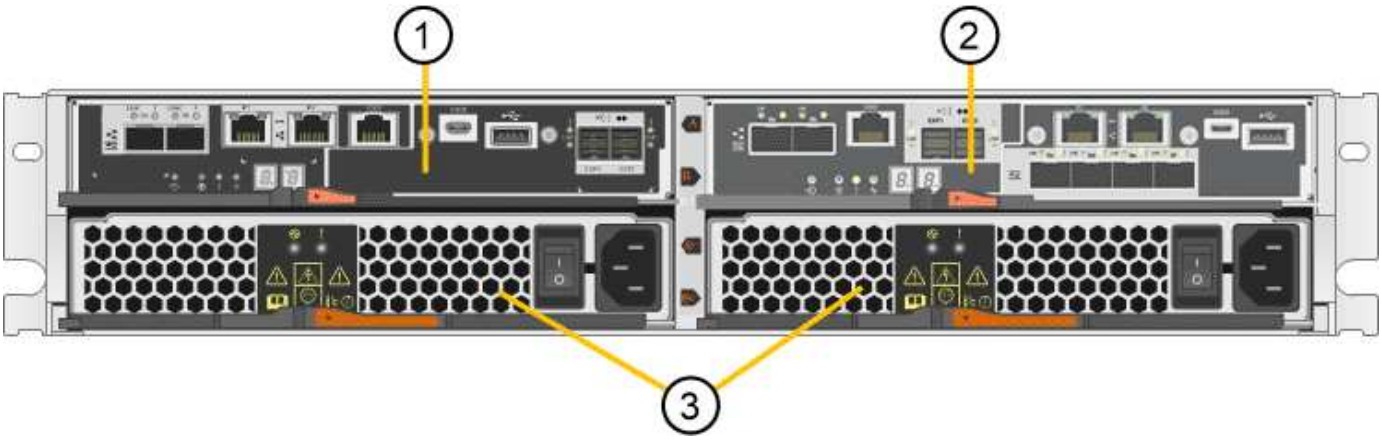
| コンポーネント | **SG5712** | **SG5760** |
| --- | --- | --- |
| ストレージコントローラ | E シリーズ E2800 コントローラ | E シリーズ E2800 コントローラ |
| シャーシ | E シリーズ DE212C エンクロージャ： 2 ラックユニット（ 2U ）エンクロージャ | E シリーズ DE460C エンクロージャ： 4 台のラックユニット（ 4U ）エンクロージャ |
| ドライブ | 12 本の NL-SAS ドライブ（ 3.5 インチ） | 60 本の NL-SAS ドライブ（ 3.5 インチ） |
| 冗長電源装置とファン | 電源 / ファンキャニスター × 2 | 2 つの電源キャニスターと 2 つのファンキャニスター |

StorageGRID アプライアンスで使用可能な最大物理ストレージは、各エンクロージャ内のドライブの数に応じて決まっています。ドライブを増設したシェルフを追加してストレージを拡張することはできません。

### モデル **SG5712**

この図は SG5712 モデルの前面と背面を示しています。 SG5712 モデルは、 12 本のドライブを搭載した 2U エンクロージャです。

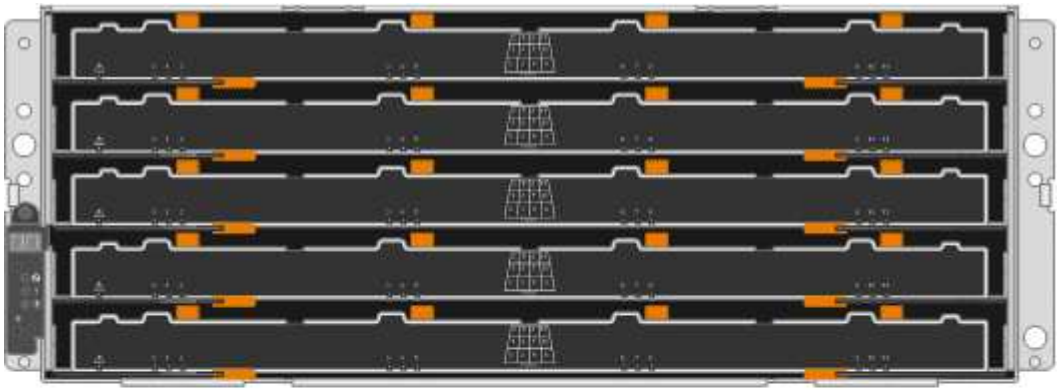
SG5712 には、 2 台のコントローラと 2 つの電源 / ファンキャニスターが含まれています。



| | 説明 |
|---|---|
| 1. | E2800 コントローラ（ストレージコントローラ） |
| 2. | E5700SG コントローラ（コンピューティングコントローラ） |
| 3. | 電源 / ファンキャニスター |

**SG5760** モデル

この図は、 SG5760 モデルの前面と背面を示しています。このモデルは、 4U エンクロージャで、 5 つのドライブドロワーに 60 本のドライブを搭載します。



SG5760 には、コントローラ 2 台、ファンキャニスター 2 台、電源キャニスター 2 台が搭載されています。

| | 説明 |
|---|---|
| 1. | E2800 コントローラ（ストレージコントローラ） |
| 2. | E5700SG コントローラ（コンピューティングコントローラ） |
| 3. | ファンキャニスター（ 2 つのうちの 1 つ） |
| 4. | 電源キャニスター（ 2 つのうちの 1 つ） |

関連情報

"NetApp E シリーズシステムのドキュメントのサイト"

**StorageGRID** アプライアンスのコントローラ

StorageGRID アプライアンス SG5712 と SG5760 の両モデルには、 E5700SG コントローラと E2800 コントローラが含まれています。次の図で、コントローラの違いを確認してください。

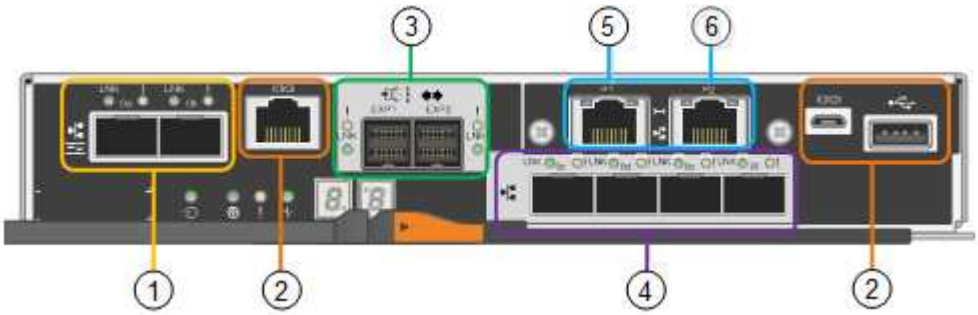
**E5700SG** コントローラのものです

- アプライアンスのコンピューティングサーバとして機能します。
- StorageGRID アプライアンスインストーラが搭載されています。

> StorageGRID ソフトウェアは、アプライアンスにプリインストールされていません。このソフトウェアには、アプライアンスの導入時に管理ノードからアクセスします。

- グリッドネットワーク、管理ネットワーク、クライアントネットワークを含む、 3 つの StorageGRID ネットワークすべてに接続できます。
- E2800 コントローラに接続し、イニシエータとして機能します。

この図は、 E5700SG コントローラの背面のコネクタを示しています。



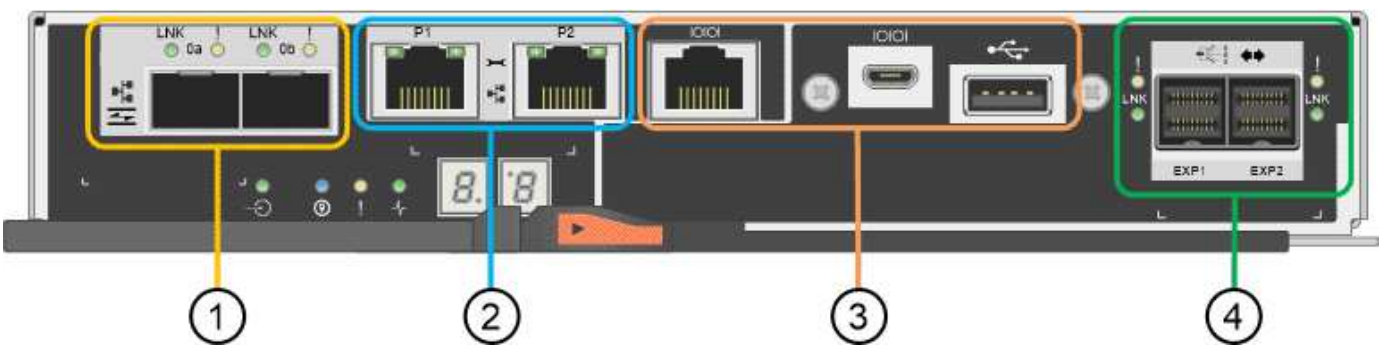

| | ポート | を入力します | 使用 |
|---|---|---|---|
| 1. | インターコネクトポート 1 と 2 | 16Gb/s Fibre Channel （ FC ）、光ファイバ SFPA | E5700SG コントローラを E2800 コントローラに接続してください。 |
| 2. | 診断とサポート用のポート | • RJ-45 シリアルポート<br>• マイクロ USB シリアルポート<br>• USB ポート | テクニカルサポート専用です。 |
| 3. | ドライブ拡張ポート | 12Gb/ 秒 SAS の場合 | 使用されません。StorageGRID アプライアンスでは、拡張ドライブシェルフはサポートされません。 |

| | ポート | を入力します | 使用 |
|---|---|---|---|
| 4. | ネットワークポート 1~4 | SFP トランシーバのタイプ、スイッチの速度、設定されたリンク速度に基づく 10GbE または 25GbE | StorageGRID のグリッドネットワークおよびクライアントネットワークに接続します。 |
| 5. | 管理ポート 1 | 1Gb （ RJ-45 ）イーサネット | StorageGRID の管理ネットワークに接続します。 |
| 6. | 管理ポート 2. | 1Gb （ RJ-45 ）イーサネット | オプション：<br>• StorageGRID の管理ネットワークへの冗長接続を確保するには、管理ポート 1 とボンディングします。<br>• 一時的なローカルアクセス用（ IP 169.254.0.1 ）に空けておくことができます。<br>• DHCP によって割り当てられた IP アドレスを使用できない場合は、設置時の IP 設定にポート 2 を使用します。 |

**E2800** コントローラ

- アプライアンスのストレージコントローラとして機能します。
- ドライブ上のデータストレージを管理します。
- シンプレックスモードでは標準の E シリーズコントローラとして機能します。
- SANtricity OS ソフトウェア（コントローラファームウェア）を搭載しています。
- アプライアンスハードウェアの監視、アラートの管理、 AutoSupport 機能、ドライブセキュリティ機能を実行するための SANtricity System Manager が搭載されています。
- E5700SG コントローラに接続してターゲットとして機能します。

次の図は、 E2800 コントローラ背面のコネクタを示しています。



| | ポート | を入力します | 使用 |
|---|---|---|---|
| 1. | インターコネクトポート 1 と 2 | 16Gb/s FC 光ファイバ SFPA | E2800 コントローラを E5700SG コントローラに接続します。 |
| 2. | 管理ポート 1 と 2 | 1Gb （ RJ-45 ）イーサネット | • ポート 1 は、ブラウザから SANtricity System Manager にアクセスするネットワークに接続します。<br>• ポート 2 はテクニカルサポート専用です。 |
| 3. | 診断とサポート用のポート | • RJ-45 シリアルポート<br>• マイクロ USB シリアルポート<br>• USB ポート | テクニカルサポート専用です。 |
| 4. | ドライブ拡張ポート | 12Gb/ 秒 SAS の場合 | 使用されません。StorageGRID アプライアンスでは、拡張ドライブシェルフはサポートされません。 |

## インストールと導入の概要

StorageGRID アプライアンスは StorageGRID の初回導入時に設置することも、後日拡張の一環として追加することもできます。リカバリ処理の一環としてアプライアンスストレージノードの設置が必要となる場合もあります。

StorageGRID システムに StorageGRID ストレージアプライアンスを追加するには、主に次の 4 つの手順を実行します。

1. 設置の準備：
    - 設置場所の準備
    - 開梱と内容の確認
    - 追加機器および工具の入手方法
    - IP アドレスとネットワーク情報を収集しています
    - オプション：すべてのアプライアンスデータを暗号化する場合は、外部キー管理サーバ（ KMS ）を設定します。外部キー管理の詳細については、 StorageGRID の管理手順を参照してください。
2. ハードウェアの設置
    - ハードウェアの登録
    - キャビネットまたはラックへのアプライアンスの設置
    - ドライブの取り付け（ SG5760 のみ）
    - アプライアンスのケーブル接続

- 電源コードの接続と電源の投入
- ブート時のステータスコードの確認

3. ハードウェアの設定
   - SANtricity System Manager へのアクセス、 E2800 コントローラの管理ポート 1 の静的 IP アドレスの設定、および SANtricity System Manager の設定
   - StorageGRID アプライアンスインストーラへのアクセス、および StorageGRID ネットワークへの接続に必要なリンクとネットワーク IP の設定
   - オプション：外部 KMS を使用してアプライアンスデータを暗号化する場合は、ノード暗号化を有効にします。
   - オプション： RAID モードを変更する
4. アプライアンスをストレージノードとして導入する：

| タスク | 手順 |
| --- | --- |
| 新しい StorageGRID システムにアプライアンスストレージノードを導入する | "アプライアンスストレージノードの導入" |
| 既存の StorageGRID システムへのアプライアンスストレージノードの追加 | StorageGRID システムの拡張手順 |
| ストレージノードのリカバリ処理の一環としてアプライアンスストレージノードを導入する | リカバリとメンテナンスの手順 |

関連情報

"設置を準備しています"

"ハードウェアを設置"

"ハードウェアの設定"

"VMware をインストールする"

"Red Hat Enterprise Linux または CentOS をインストールします"

"Ubuntu または Debian をインストールします"

"SG100 SG1000サービスアプライアンス"

"グリッドを展開します"

""

"StorageGRID の管理"

## 設置を準備しています

StorageGRID アプライアンスを設置するための準備では、設置場所を準備し、必要なす

べてのハードウェア、ケーブル、工具を揃えます。また、 IP アドレスとネットワーク情報を収集する必要があります。

手順

- "サイトの準備（SG5700）"
- "開梱（SG5700）"
- "追加の機器や工具の入手（SG5700）"
- "Web ブラウザの要件"
- "アプライアンスのネットワーク接続を確認します"
- "設置情報の収集（SG5700）"

### サイトの準備（**SG5700**）

アプライアンスを設置する前に、設置場所および使用するキャビネットやラックが StorageGRID アプライアンスの仕様を満たしていることを確認する必要があります。

手順

1. 設置場所の温度、湿度、高度範囲、通気、熱放散の要件を満たしていることを確認します。 配線、電源、およびアース。詳細については、 NetApp Hardware Universe を参照してください。
2. SG5760 モデルを設置する場合は、設置場所が 240 ボルトの AC 電源を備えていることを確認してください。
3. 次のサイズのシェルフ（ケーブルなし）が収まる 48.3cm （ 19 インチ）のキャビネットまたはラックを用意します。

| アプライアンスのモデル | 高さ | 幅 | 奥行き | 最大重量 |
|---|---|---|---|---|
| SG5712<br>（ 12 ドライブ） | 3.41 インチ<br>（ 8.68 cm ） | 17.6 インチ<br>（ 44.7 cm ） | 21.1 インチ<br>（ 53.6 cm ） | 63.9 ポンド<br>（ 29.0 kg ） |
| SG5760<br>（ 60 ドライブ） | 6.87 インチ<br>（ 17.46 cm ） | 17.66 インチ<br>（ 44.86 cm ） | 38.25 インチ<br>（ 97.16 cm ） | 250 ポンド<br>（ 113 kg ） |

4. 必要なネットワークスイッチを取り付けます。互換性の情報については、 NetApp Interoperability Matrix Tool を参照してください。

関連情報

"NetApp Hardware Universe の略"

"NetApp Interoperability Matrix Tool で確認できます"

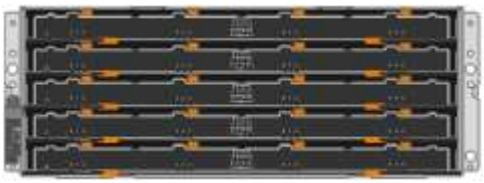
### 開梱（**SG5700**）

StorageGRID アプライアンスを設置する前にすべて開梱し、内容物を納品書の項目と比

較します。

- * SG5712 アプライアンス、 12 ドライブ搭載 *

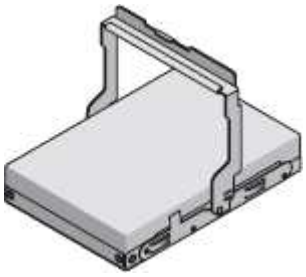
- * ドライブを取り付けていない SG5760 アプライアンス *



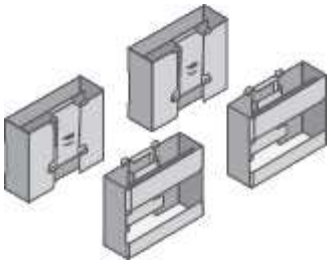
- * アプライアンスの前面ベゼル *

- * 取扱説明書付きレールキット *

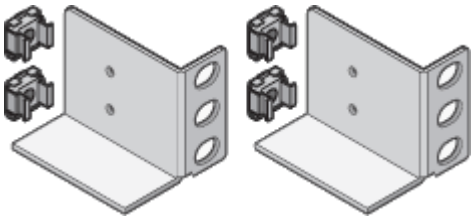
- * SG5760 ： 60 ドライブ *



- * SG5760 ：取っ手 *



- * SG5760 ：角穴ラックに設置するための後部ブラケットとケージナット *



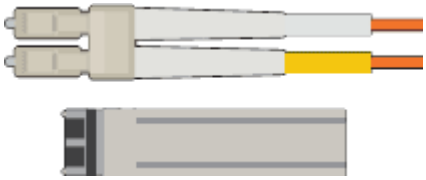
ケーブルとコネクタ

StorageGRID アプライアンスには、出荷時に次のケーブルとコネクタが付属しています。

- * お住まいの国に対応した電源コード 2 本 *

キャビネットによっては、アプライアンスに付属している電源コードではなく特別な電源コードを使用する場合があります。

- * 光ケーブルと SFP トランシーバ *



FC インターコネクトポート用の光ケーブル × 2

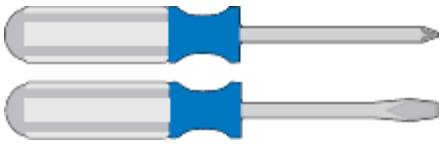
4 つの 16Gb/s FC インターコネクトポートおよび 4 つの 10GbE ネットワークポートの両方に対応した、8 つの SFP+ トランシーバ

追加の機器や工具の入手（**SG5700**）

## StorageGRID アプライアンスを設置する前に、必要な追加機器や工具がすべて揃っていることを確認します。

ハードウェアの設置と設定を行うには、次の追加機器が必要です。

- * ドライバ *

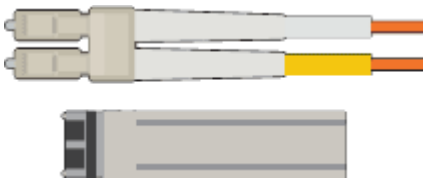


フィリップス番号2 本のドライバ

中型マイナスドライバ

- * 静電気防止用リストストラップ *

- * 光ケーブルと SFP トランシーバ *



使用する 10 / 25GbE ポート用の光ケーブル

オプション： 25GbE のリンク速度を使用する場合は、 SFP28 トランシーバを搭載します

- * イーサネットケーブル *

- * サービスラップトップ *

サポートされている Web ブラウザ

PuTTY などの SSH クライアント

1Gb （ RJ-45 ）イーサネットポート

- * オプションのツール *

ヘッドビット付き電源ドリル

懐中電灯

SG5760 のリフト機械化

**Web** ブラウザの要件

サポートされている Web ブラウザを使用する必要があります。

| **Web** ブラウザ | サポートされる最小バージョン |
| --- | --- |
| Google Chrome | 87 |
| Microsoft Edge の場合 | 87 |
| Mozilla Firefox | 84 |

ブラウザウィンドウの幅を推奨される値に設定してください。

| ブラウザの幅 | ピクセル |
| --- | --- |
| 最小（ Minimum ） | 1024 |
| 最適 | 1280 |

アプライアンスのネットワーク接続を確認します

StorageGRID アプライアンスを設置する前に、アプライアンスに接続できるネットワークを確認し、各コントローラのポートがどのように使用されるかを把握する必要があります。

**StorageGRID** アプライアンスのネットワーク

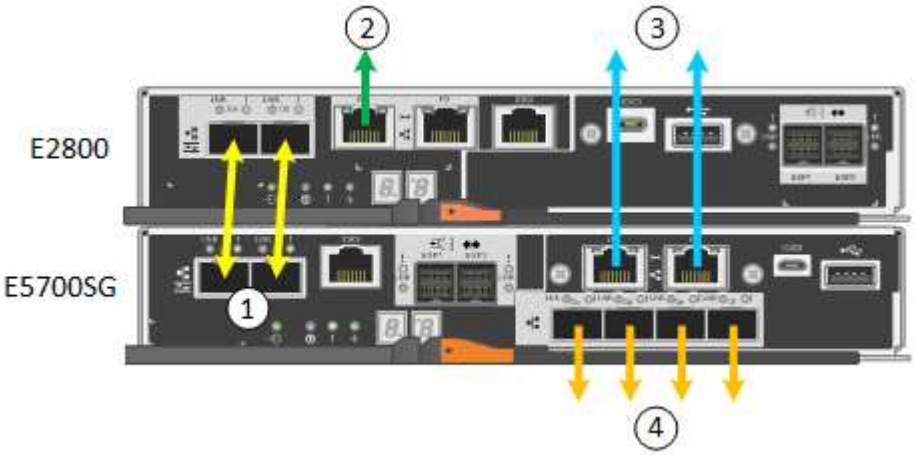
StorageGRID アプライアンスを StorageGRID グリッドのストレージノードとして導入する場合は、次のネットワークに接続できます。

- * StorageGRID のグリッドネットワーク * ：グリッドネットワークは、すべての内部 StorageGRID トラフィックに使用されます。このネットワークによって、グリッド内のすべてのノードが、すべてのサイトおよびサブネットにわたって相互に接続されます。グリッドネットワークは必須です。
- * StorageGRID の管理ネットワーク * ：管理ネットワークは、システムの管理とメンテナンスに使用するクローズドネットワークです。管理ネットワークは通常はプライベートネットワークであり、サイト間でルーティング可能にする必要はありません。管理ネットワークはオプションです。
- * StorageGRID のクライアントネットワーク： * クライアントネットワークは、 S3 や Swift などのクライアントアプリケーションへのアクセスを可能にするオープンネットワークです。クライアントネットワークはグリッドへのクライアントプロトコルアクセスを提供するため、グリッドネットワークを分離してセキュリティを確保できます。クライアントネットワークはオプションです。
- * SANtricity System Manager用管理ネットワーク*：このネットワークは、E2800コントローラのSANtricity システムマネージャへのアクセスを提供することで、アプライアンス内のハードウェアコンポーネントの監視と管理を可能にします。この管理ネットワークは、 StorageGRID の管理ネットワークと同じにすることも、独立した管理ネットワークにすることもできます。

StorageGRID ネットワークの詳細については、 _ グリッド入門 _ を参照してください。

**StorageGRID** アプライアンスの接続

StorageGRID アプライアンスを設置するときは、 2 台のコントローラを相互に接続するとともに、必要なネットワークに接続する必要があります。この図では、 SG5760 の 2 台のコントローラと、 E2800 コントローラを上部に、 E5700SG コントローラを下部に示しています。SG5712 では、 E2800 コントローラは E5700SG コントローラの左側にあります。




| | ポート | ポートのタイプ | 機能 |
|---|---|---|---|
| 1. | 各コントローラの 2 つのインターコネクトポート | 16Gb/s FC 光ファイバ SFP+ | 2 台のコントローラを相互に接続します。 |

| | ポート | ポートのタイプ | 機能 |
|---|---|---|---|
| 2. | E2800 コントローラの管理ポート 1 | 1GbE （ RJ-45 ） | SANtricity System Manager にアクセスするネットワークに接続します。StorageGRID の管理ネットワークまたは独立した管理ネットワークを使用できます。 |
| 2. | E2800 コントローラの管理ポート 2 | 1GbE （ RJ-45 ） | テクニカルサポート専用です。 |
| 3. | E5700SG コントローラの管理ポート 1 | 1GbE （ RJ-45 ） | E5700SG コントローラを StorageGRID の管理ネットワークに接続しています。 |
| 3. | E5700SG コントローラの管理ポート 2 | 1GbE （ RJ-45 ） | • 管理ネットワークへの冗長接続が必要な場合は、管理ポート 1 とボンディングできます。<br>• 一時的なローカルアクセス用（ IP 169.254.0.1 ）に空けておくことができます。<br>• DHCP によって割り当てられた IP アドレスを使用できない場合、設置時に E5700SG コントローラをサービスラップトップに接続するために使用できます。 |
| 4. | E5700SG コントローラの 10 / 25GbE ポート 1~4 | 10GbE または 25GbE<br>• 注：アプライアンス付属の SFP+ トランシーバは、 10GbE のリンク速度をサポートしています。4 つのネットワークポートで 25GbE のリンク速度を使用する場合は、 SFP28 トランシーバを取り付ける必要があります。 | StorageGRID のグリッドネットワークおよびクライアントネットワークに接続します。E5700SG コントローラでの 10 / 25GbE ポート接続を参照してください |

関連情報

"設置情報の収集（SG5700）"

"アプライアンスのケーブル接続（SG5700）"

"E5700SG コントローラポートのポートボンディングモード"

"ネットワークガイドライン"

"VMware をインストールする"

"Red Hat Enterprise Linux または CentOS をインストールします"

"Ubuntu または Debian をインストールします"

#### E5700SG コントローラポートのポートボンディングモード

E5700SG コントローラポートのネットワークリンクを設定する場合は、グリッドネットワークとオプションのクライアントネットワークに接続する 10 / 25GbE ポート、およびオプションの管理ネットワークに接続する 1GbE 管理ポートに対してポートボンディングを使用できます。ポートボンディングを使用すると、 StorageGRID ネットワークとアプライアンスの間のパスが冗長化されるため、データの保護に役立ちます。

関連情報

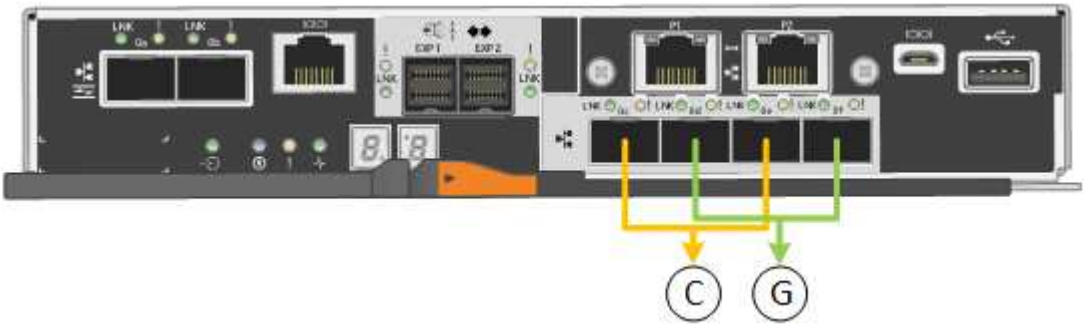
"ネットワークリンクの設定（SG5700）"

#### 10 / 25GbEポートのネットワークボンディングモード

E5700SG コントローラの 10 / 25GbE ネットワークポートは、グリッドネットワークおよびクライアントネットワーク接続用に、 Fixed または Aggregate のポートボンディングモードをサポートしています。

**Fixed** ポートボンディングモード

固定モードは、 10 / 25GbE ネットワークポートのデフォルトの設定です。




| | ボンディングされるポート |
|---|---|
| C | このネットワークを使用する場合、ポート 1 とポート 3 がクライアントネットワーク用にボンディングされます。 |
| G | ポート 2 とポート 4 がグリッドネットワーク用にボンディングされます。 |

Fixed ポートボンディングモードを使用する場合は、 Active-Backup または Link Aggregation Control Protocol （ LACP ）のいずれかのネットワークボンディングモードを使用できます。

- Active-Backup モード（デフォルト）では、一度に 1 つのポートのみがアクティブになります。アクティブポートで障害が発生すると、バックアップポートが自動的にフェイルオーバーして接続が継続されま

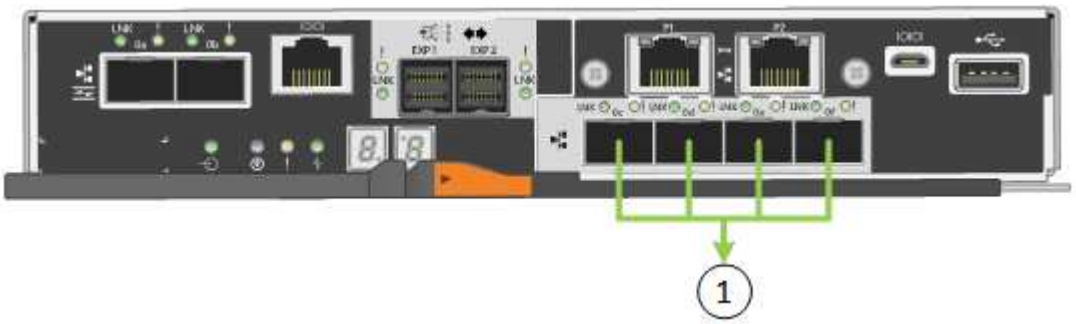
す。ポート 4 がポート 2 のバックアップパスとなり（グリッドネットワーク）、ポート 3 がポート 1 のバックアップパスとなります（クライアントネットワーク）。

- LACP モードでは、各ポートペアでコントローラとネットワークの間の論理チャネルが形成され、スループットが向上します。一方のポートで障害が発生しても、もう一方のポートは引き続きチャネルを提供します。スループットは低下しますが、接続に影響はありません。

> 冗長な接続が不要な場合は、各ネットワークで使用できるポートは 1 つだけです。ただし、StorageGRID をインストールしたあとにグリッドマネージャでアラームが生成され、ケーブルが取り外されていることが通知されます。このアラームは確認後に解除してかまいません。

**Aggregate** ポートボンディングモード

アグリゲートポートボンディングモードを使用すると、各 StorageGRID ネットワークのスループットが大幅に向上し、追加のフェイルオーバーパスも確保されます。




| | ボンディングされるポート |
|---|---|
| 1. | 接続されたすべてのポートを 1 つの LACP ボンドにグループ化して、すべてのポートをグリッドネットワークとクライアントネットワークのトラフィックに使用できるようにします。 |

Aggregate ポートボンディングモードを使用する場合は、次の点に注意してください。

- LACP ネットワークボンディングモードを使用する必要があります。
- 各ネットワークに一意の VLAN タグを指定する必要があります。この VLAN タグが各ネットワークパケットに追加され、ネットワークトラフィックが正しいネットワークにルーティングされます。
- VLAN と LACP をサポートするスイッチにポートを接続する必要があります。複数のスイッチを LACP ボンドに加える場合は、対象のスイッチが Multi-Chassis Link Aggregation （ MLAG ）グループまたは同等の機能をサポートしていることが必要です。
- VLAN 、 LACP 、 MLAG などを使用するようにスイッチを設定する方法について理解しておく必要があります。

4 つの 10 / 25GbE ポートをすべて使用する必要がない場合、使用するポートの数は 1~3 のいくつでもかまいません。複数のポートを使用すると、 10 / 25GbE ポートの 1 つに障害が発生した場合でも、ネットワーク接続を確保できる可能性が高くなります。

> 4 つのポート全部を使用しない場合は、 StorageGRID をインストールしたあとにケーブルが取り外されていることを通知するアラームがグリッドマネージャで生成されるので注意してください。このアラームは確認後に解除してかまいません。

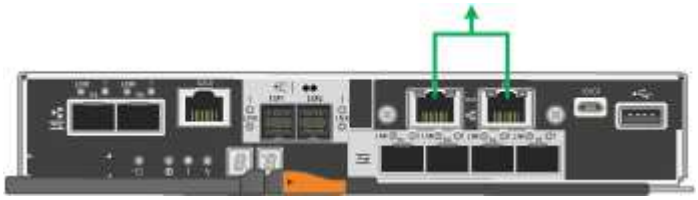
### 1GbE管理ポートのネットワークボンディングモード

## E5700SG コントローラの 2 つの 1GbE 管理ポートでは、 Independent ネットワークボンディングモードまたは Active-Backup ネットワークボンディングモードを選択してオプションの管理ネットワークに接続できます。

Independent モードでは、管理ポート 1 だけが管理ネットワークに接続されます。このモードではパスは冗長化されません。管理ポート 2 は、一時的なローカル接続（ IP アドレス 169.254.0.1 ）用に確保されます。

Active-Backup モードでは、管理ポート 1 と 2 の両方が管理ネットワークに接続されます。一度に 1 つのポートのみがアクティブになります。アクティブポートで障害が発生すると、バックアップポートが自動的にフェイルオーバーして接続が継続されます。これら 2 つの物理ポートを 1 つの論理管理ポートにボンディングすることで、管理ネットワークへのパスが冗長化されます。

> 1GbE 管理ポートが Active-Backup モードに設定されている場合に E5700SG コントローラへの一時的なローカル接続が必要な場合は、両方の管理ポートからケーブルを取り外し、一時的なケーブルを管理ポート 2 に接続し、 IP アドレス 169.254.0.1 を使用してアプライアンスにアクセスしてください。



### 設置情報の収集（SG5700）

## StorageGRID アプライアンスを設置および設定する際に、イーサネットスイッチポート、 IP アドレス、およびポートとネットワークのボンディングモードについて決定し、関連情報を収集する必要があります。

このタスクについて

次の表を使用して、アプライアンスに接続する各ネットワークの必要な情報を記録できます。これらの値は、ハードウェアの設置と設定に必要です。

#### E2800コントローラのSANtricity System Managerに接続するために必要な情報

E2800 コントローラは、 SANtricity System Manager で使用する管理ネットワークに接続する必要があります。

| 必要な情報 | あなたの価値 |
| --- | --- |
| 管理ポート 1 に接続するイーサネットスイッチポート | |
| 管理ポート 1 の MAC アドレス（ポート P1 のラベルに記載） | |

| 必要な情報 | あなたの価値 |
| --- | --- |
| DHCP によって管理ポート 1 に割り当てられた IP アドレス（電源投入後に使用可能な場合）<br><br>• 注： * E2800 コントローラに接続するネットワークに DHCP サーバがある場合、ネットワーク管理者は MAC アドレスを使用して DHCP サーバによって割り当てられた IP アドレスを特定できます。 | |
| 速度と二重モード<br><br>• 注： SANtricity システムマネージャ管理ネットワークのイーサネットスイッチが自動ネゴシエーションに設定されていることを確認してください。 | 次の値でなければなりません<br><br>• Autonegotiate （デフォルト） |
| IP アドレスの形式 | 1 つ選択してください：<br><br>• IPv4<br>• IPv6 |
| 管理ネットワークでアプライアンスに使用する静的 IP アドレス | IPv4 の場合：<br><br>• IPv4 アドレス：<br>• サブネットマスク：<br>• ゲートウェイ<br><br>IPv6 の場合：<br><br>• IPv6 アドレス：<br>• ルーティング可能な IP アドレス：<br>• E2800 コントローラのルータ IP アドレス： |

**E5700SG**コントローラを管理ネットワークに接続するために必要な情報

StorageGRID の管理ネットワークは、システムの管理とメンテナンスに使用するオプションのネットワークです。アプライアンスは、 E5700SG コントローラの 1GbE 管理ポートを使用して管理ネットワークに接続しています。

| 必要な情報 | あなたの価値 |
| --- | --- |
| 管理ネットワークが有効になりました | 1 つ選択してください：<br><br>• いいえ<br>• ○（デフォルト） |

| 必要な情報 | あなたの価値 |
| --- | --- |
| ネットワークボンディングモード | 1 つ選択してください：<br>• 独立<br>• アクティブ / バックアップ |
| ポート 1 のスイッチポートを指定します | |
| ポート 2 のスイッチポート（アクティブ / バックアップネットワークボンディングモードのみ） | |
| DHCP によって管理ポート 1 に割り当てられた IP アドレス（電源投入後に使用可能な場合）<br>• 注：管理ネットワークに DHCP サーバが含まれている場合、 E5700SG コントローラのブート後のデジタル表示ディスプレイに、 DHCP によって割り当てられた IP アドレスが表示されます。DHCP によって割り当てられた IP アドレスは、 MAC アドレスを使用して IP アドレスを調べる方法でも確認できます。 | • IPv4 アドレス（ CIDR ）：<br>• ゲートウェイ |
| 管理ネットワークでアプライアンスストレージノードに使用する静的 IP アドレス<br>• 注： * ネットワークにゲートウェイがない場合は、同じ静的 IPv4 アドレスをゲートウェイに指定してください。 | • IPv4 アドレス（ CIDR ）：<br>• ゲートウェイ |
| 管理ネットワークのサブネット（ CIDR ） | |

**E5700SG**コントローラの**10 / 25GbE**ポートの接続と設定に必要な情報

E5700SG コントローラの 4 つの 10 / 25GbE ポートは、 StorageGRID のグリッドネットワークおよびクライアントネットワークに接続しています。

これらのポートのオプションの詳細については、 E5700SG コントローラでの 10 / 25GbE ポート接続を参照してください。

| 必要な情報 | あなたの価値 |
| --- | --- |
| リンク速度<br>• 注： 25GbE を選択した場合は、 SPF28 トランシーバを取り付ける必要があります。自動ネゴシエーションはサポートされないため、 25GbE 用のポートおよび接続されたスイッチも設定する必要があります。 | 1 つ選択してください：<br>• 10GbE （デフォルト）<br>• 25GbE |
| ポートボンディングモード | 1 つ選択してください：<br>• Fixed （デフォルト）<br>• アグリゲート |
| ポート 1 のスイッチポート（クライアントネットワーク） | |
| ポート 2 のスイッチポート（グリッドネットワーク） | |
| ポート 3 のスイッチポート（クライアントネットワーク） | |
| ポート 4 のスイッチポート（グリッドネットワーク） | |

**E5700SG**コントローラをグリッドネットワークに接続するために必要な情報

StorageGRID のグリッドネットワークは、内部のすべての StorageGRID トラフィックに使用される必須のネットワークです。アプライアンスは、 E5700SG コントローラの 10 / 25GbE ポートを使用してグリッドネットワークに接続しています。

これらのポートのオプションの詳細については、 E5700SG コントローラでの 10 / 25GbE ポート接続を参照してください。

| 必要な情報 | あなたの価値 |
| --- | --- |
| ネットワークボンディングモード | 1 つ選択してください：<br>• Active-Backup （デフォルト）<br>• LACP （ 802.3ad ） |
| VLAN タギングが有効です | 1 つ選択してください：<br>• いいえ（デフォルト）<br>• はい。 |

| 必要な情報 | あなたの価値 |
| --- | --- |
| VLAN タグ（ VLAN タギングが有効な場合） | 0~4095 の値を入力してください： |
| 電源投入後に使用可能な場合、 DHCP によってグリッドネットワークに割り当てられた IP アドレス<br>• 注： * グリッドネットワークに DHCP サーバがある場合、 E5700SG コントローラのブート後のデジタル表示ディスプレイに、 DHCP によって割り当てられたグリッドネットワークの IP アドレスが表示されます。 | • IPv4 アドレス（ CIDR ）：<br>• ゲートウェイ |
| グリッドネットワークでアプライアンスストレージノードに使用する静的 IP アドレス<br>• 注： * ネットワークにゲートウェイがない場合は、同じ静的 IPv4 アドレスをゲートウェイに指定してください。 | • IPv4 アドレス（ CIDR ）：<br>• ゲートウェイ |
| グリッドネットワークのサブネット（ CIDR ）<br>• 注： * クライアントネットワークが有効になっていない場合、コントローラのデフォルトルートではここで指定したゲートウェイが使用されます。 | |

**E5700SG**コントローラをクライアントネットワークに接続するために必要な情報

StorageGRID のクライアントネットワークは、一般にグリッドへのクライアントプロトコルアクセスを可能にするために使用する、オプションのネットワークです。アプライアンスは、 E5700SG コントローラの 10 / 25GbE ポートを使用してクライアントネットワークに接続しています。

これらのポートのオプションの詳細については、 E5700SG コントローラでの 10 / 25GbE ポート接続を参照してください。

| 必要な情報 | あなたの価値 |
| --- | --- |
| クライアントネットワークが有効になりました | 1 つ選択してください：<br>• いいえ（デフォルト）<br>• はい。 |
| ネットワークボンディングモード | 1 つ選択してください：<br>• Active-Backup （デフォルト）<br>• LACP （ 802.3ad ） |

| 必要な情報 | あなたの価値 |
| --- | --- |
| VLAN タギングが有効です | 1 つ選択してください：<br>• いいえ（デフォルト）<br>• はい。 |
| VLAN タグ<br>（ VLAN タギングが有効な場合） | 0~4095 の値を入力してください： |
| 電源投入後に DHCP によってクライアントネットワークに割り当てられた IP アドレスがある場合は | • IPv4 アドレス（ CIDR ）：<br>• ゲートウェイ |
| クライアントネットワークでアプライアンスストレージノードに使用する静的 IP アドレス<br>• 注：* クライアントネットワークが有効になっている場合、コントローラのデフォルトルートではここで指定したゲートウェイが使用されます。 | • IPv4 アドレス（ CIDR ）：<br>• ゲートウェイ |

関連情報

"アプライアンスのネットワーク接続を確認します"

"E5700SG コントローラポートのポートボンディングモード"

"ハードウェアの設定"

## ハードウェアを設置

ハードウェアの設置作業では、アプライアンスをキャビネットまたはラックに設置し、ケーブルを接続し、電源を投入します。

手順

- "ハードウェアの登録"
- "キャビネットまたはラックへのアプライアンスの設置（SG5700）"
- "アプライアンスのケーブル接続（SG5700）"
- "電源コードの接続と電源の投入（SG5700）"
- "SG5700ブート時のステータスコードの表示"

ハードウェアの登録

アプライアンスハードウェアを登録するとサポートを受けられるようになります。

手順

1. シャーシのシリアル番号を確認します。

   この番号は、納品書や確認用 E メールで確認できるほか、開梱したアプライアンスにも記載されています。

2. NetApp Support Siteにアクセスします "mysupport.netapp.com"。
3. ハードウェアの登録が必要かどうかを確認します。

| ユーザのタイプとアクセス方法 | 実行する手順 |
| --- | --- |
| ネットアップの既存のお客様 | a. ユーザ名とパスワードを使用してサインインします。<br>b. [ 製品 **>*My Products** ] を選択します。<br>c. 新しいシリアル番号が表示されていることを確認します。<br>d. 表示されていない場合は、ネットアップの新規のお客様向けの手順に従ってください。 |
| ネットアップの新規のお客様 | a. [ 今すぐ登録 ] をクリックしてアカウントを作成します。<br>b. [**Products**>*Register Products*] を選択します。<br>c. 製品のシリアル番号と要求された詳細情報を入力します。<br>登録が承認されると、必要なソフトウェアをダウンロードできます。承認プロセスには最大 24 時間かかる場合があります。 |

キャビネットまたはラックへのアプライアンスの設置（**SG5700**）

## キャビネットまたはラックにレールを取り付け、レールにアプライアンスをスライドさせます。SG5760 を使用している場合は、アプライアンスの設置後にドライブも取り付ける必要があります。

必要なもの

- 同梱されている安全上の注意に関するドキュメントを確認し、ハードウェアの移動と設置に関する注意事項を理解しておきます。
- レールキットに手順書が同梱されていることを確認します。
- アプライアンスにインストールおよびセットアップ手順 _ が付属していることを確認します。

機器の転倒を防ぐために、ラックまたはキャビネットの一番下から順にハードウェアを設置してください。

SG5712 の重量は、ドライブが完全に搭載された状態のときの約 29kg （ 64 ポンド）です。SG5712 を安全に移動するには、 2 人で行うか電動リフトを使用する必要があります。

ドライブが取り付けられていない状態の SG5760 の重量は、約 60kg （ 132 ポンド）です。空の SG5760 を安全に移動するには、 4 人で行うかリフト機を使用する必要があります。

ハードウェアの損傷を避けるため、ドライブを取り付けている場合は SG5760 を移動しないでください。シェルフを移動する前に、ドライブをすべて取り外す必要があります。

手順

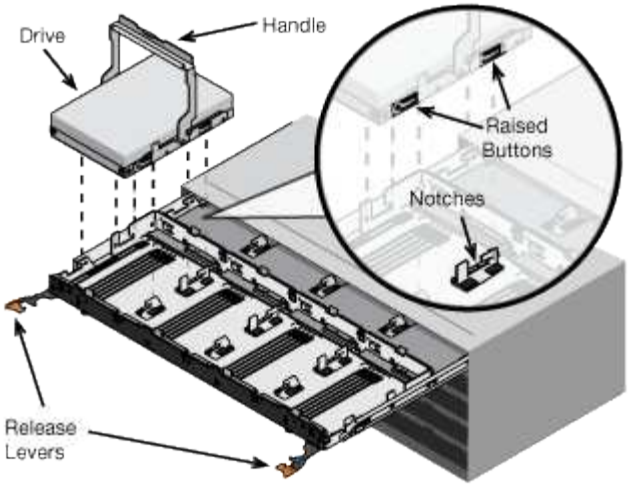
1. キャビネットまたはラックにレールを取り付ける際には、レールキットの手順書に慎重に従ってください。
2. SG5760 を使用している場合は、次の手順に従ってアプライアンスを移動する準備をしてください。
   a. 包装箱を取り除きます。次に、内側のボックスのフラップを折りたたみます。
   b. SG5760 を手で持ち上げる場合は、シャーシの側面に 4 つのハンドルを取り付けます。

      この取っ手は、アプライアンスをレールにスライドさせて挿入するときに取り外します。
3. 設置およびセットアップ手順を参照しながら、アプライアンスをキャビネットまたはラックにスライドさせます。
4. 設置およびセットアップ手順を参照し、アプライアンスをキャビネットまたはラックに固定します。

   SG5760 を使用する場合は、後部ブラケットを使用してアプライアンスをラックまたはキャビネットの背面に固定します。ラックまたはキャビネットに角穴がある場合は、ケージナットを使用します。
5. SG5760 を使用している場合は、 5 つのドライブドロワーに 12 本ずつドライブを取り付けます。

   正しく動作させるためには、 60 本のドライブをすべて取り付ける必要があります。

   a. ESD リストバンドを装着し、パッケージからドライブを取り出します。
   b. 上部ドライブドロワーのレバーを解放し、レバーを使用してドロワーを引き出します。
   c. ドライブのハンドルを垂直に持ち上げ、ドライブのボタンをドロワーのノッチに合わせます。




d. ドライブの上部を軽く押し、ドライブが完全に固定されるまでドライブのハンドルを下に回転させます。

e. 最初の 12 本のドライブを取り付けたら、ドロワーの中央を押し、両方のレバーを静かに閉じてドロワーを元の位置に戻します。

f. 残りの 4 つのドロワーで同じ手順を繰り返します。

6. 前面ベゼルを取り付けます。

アプライアンスのケーブル接続（**SG5700**）

## E5700SG コントローラの 2 台のコントローラを相互に接続して、各コントローラの管理ポートを接続し、 E5700SG コントローラの 10 / 25GbE ポートを StorageGRID のグリッドネットワークとオプションのクライアントネットワークに接続する必要があります。

必要なもの

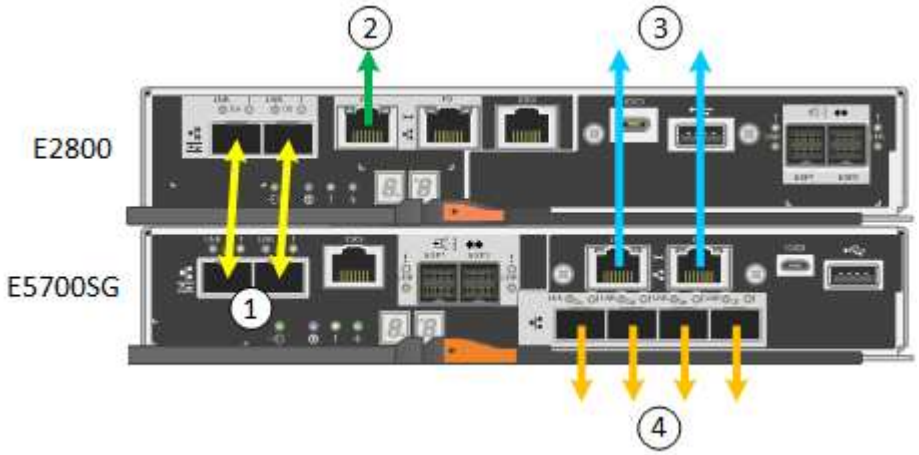
- アプライアンスの箱を開封し、次のものを取り出しておきます。
  - 電源コード × 2 。
  - コントローラの FC インターコネクトポート用の光ケーブル × 2 。
  - 10GbE または 16Gbps FC をサポートする SFP+ トランシーバ × 8 。ネットワークポートで 10GbE のリンク速度を使用する場合は、両方のコントローラの 2 つのインターコネクトポートと E5700SG コントローラの 4 つの 10 / 25GbE ネットワークポートでトランシーバを使用できます。
- アプライアンスに付属していない次のものを入手しておきます。
  - 使用する 10 / 25GbE ポート用の光ケーブルを 1~4 本。
  - 25GbE のリンク速度を使用する場合は、 SFP28 トランシーバを 1~4 個。
  - 管理ポートを接続するためのイーサネットケーブル。

* レーザー被ばくの危険性 * — SFP トランシーバを分解したり部品を取り外したりしないでください。レーザー被ばくのおそれがあります。

このタスクについて

この図では、 SG5760 の 2 台のコントローラと、 E2800 コントローラを上部に、 E5700SG コントローラを

下部に示しています。SG5712 では、 E2800 コントローラは背面から見て E5700SG コントローラの左側にあります。




| | ポート | ポートのタイプ | 機能 |
|---|---|---|---|
| 1. | 各コントローラの 2 つのインターコネクトポート | 16Gb/s FC 光ファイバ SFP+ | 2 台のコントローラを相互に接続します。 |
| 2. | E2800 コントローラの管理ポート 1 | 1GbE （ RJ-45 ） | SANtricity System Manager にアクセスするネットワークに接続します。StorageGRID の管理ネットワークまたは独立した管理ネットワークを使用できます。 |
| 2. | E2800 コントローラの管理ポート 2 | 1GbE （ RJ-45 ） | テクニカルサポート専用です。 |
| 3. | E5700SG コントローラの管理ポート 1 | 1GbE （ RJ-45 ） | E5700SG コントローラを StorageGRID の管理ネットワークに接続しています。 |

| | ポート | ポートのタイプ | 機能 |
|---|---|---|---|
| 3. | E5700SG コントローラの管理ポート 2 | 1GbE （ RJ-45 ） | • 管理ネットワークへの冗長接続が必要な場合は、管理ポート 1 とボンディングできます。<br>• 一時的なローカルアクセス用（ IP 169.254.0.1 ）に空けておくことができます。<br>• DHCP によって割り当てられた IP アドレスを使用できない場合、設置時に E5700SG コントローラをサービスラップトップに接続するために使用できます。 |
| 4. | E5700SG コントローラの 10 / 25GbE ポート 1~4 | 10GbE または 25GbE<br>• 注：アプライアンス付属の SFP+ トランシーバは、 10GbE のリンク速度をサポートしています。4 つのネットワークポートで 25GbE のリンク速度を使用する場合は、 SFP28 トランシーバを取り付ける必要があります。 | StorageGRID のグリッドネットワークおよびクライアントネットワークに接続します。E5700SG コントローラでの 10 / 25GbE ポート接続を参照してください |

手順

1. 2 本の光ケーブルと 8 つのうち 4 つの SFP+ トランシーバを使用して、 E2800 コントローラを E5700SG コントローラに接続します。

| 接続するポート | 接続先のポート |
|---|---|
| E2800 コントローラのインターコネクトポート 1 | E5700SG コントローラのインターコネクトポート 1 |
| E2800 コントローラのインターコネクトポート 2 | E5700SG コントローラのインターコネクトポート 2 |

2. E2800コントローラの管理ポート1（P1、左側のRJ-45ポート）を、イーサネットケーブルでSANtricity System Managerの管理ネットワークに接続します。

E2800 コントローラの管理ポート 2 （ P2 、右側の RJ-45 ポート）は使用しないでください。このポートはテクニカルサポート専用です。

3. StorageGRID の管理ネットワークを使用する場合は、 E5700SG コントローラの管理ポート 1 （ P1 、左側の RJ-45 ポート）をイーサネットケーブルで管理ネットワークに接続してください。

   管理ネットワークにアクティブ / バックアップネットワークボンディングモードを使用する場合は、 E5700SG コントローラの管理ポート 2 （右側の RJ-45 ポート）をイーサネットケーブルで管理ネットワークに接続してください。

4. E5700SG コントローラの 10 / 25GbE ポートを、光ケーブルと SFP+ または SFP28 トランシーバを使用して適切なネットワークスイッチに接続します。

   すべてのポートで同じリンク速度を使用する必要があります。10GbE のリンク速度を使用する場合は、 SFP+ トランシーバを取り付けます。25GbE のリンク速度を使用する場合は、 SFP28 トランシーバを取り付けます。

   - 固定ポートボンディングモード（デフォルト）を使用する場合は、次の表のように各ポートを StorageGRID のグリッドネットワークまたはクライアントネットワークに接続します。

| ポート | 接続先 |
| --- | --- |
| ポート 1 | クライアントネットワーク（オプション） |
| ポート 2 | Grid ネットワーク |
| ポート 3 | クライアントネットワーク（オプション） |
| ポート 4. | Grid ネットワーク |

   - アグリゲートポートボンディングモードを使用する場合は、 1 つ以上のネットワークポートを 1 つ以上のスイッチに接続します。単一点障害を回避するために、 4 つのポートのうち少なくとも 2 つを接続する必要があります。1 つの LACP ボンドに複数のスイッチを使用する場合は、スイッチが MLAG または同等の機能をサポートしている必要があります。

関連情報

"StorageGRID アプライアンスインストーラへのアクセス"

"E5700SG コントローラポートのポートボンディングモード"

電源コードの接続と電源の投入（**SG5700**）

## アプライアンスの電源を入れると、両方のコントローラがブートされます。

必要なもの

両方のアプライアンスの電源スイッチをオフにしてから、電源を接続する必要があります。

* 感電の危険性 * — 電源コードを接続する前に、アプライアンスの 2 つの電源スイッチがオフになっていることを確認してください。

手順

1. アプライアンスの 2 つの電源スイッチがオフになっていることを確認します。
2. アプライアンスに 2 本の電源コードを接続します。
3. 2 本の電源コードを、キャビネットまたはラック内の別々の配電ユニットに接続します。
4. アプライアンスの 2 つの電源スイッチをオンにします。
   - 電源投入プロセスの実行中は電源スイッチをオフにしないでください。
   - ファンは初回起動時に大きな音を立てます。起動時に大きな音がしても問題はありません。
5. コントローラがブートしたら、コントローラのデジタル表示ディスプレイを確認します。

**SG5700**ブート時のステータスコードの表示

## アプライアンスの電源をオンにすると、各コントローラのデジタル表示ディスプレイにステータスコードとエラーコードが表示されます。

このタスクについて

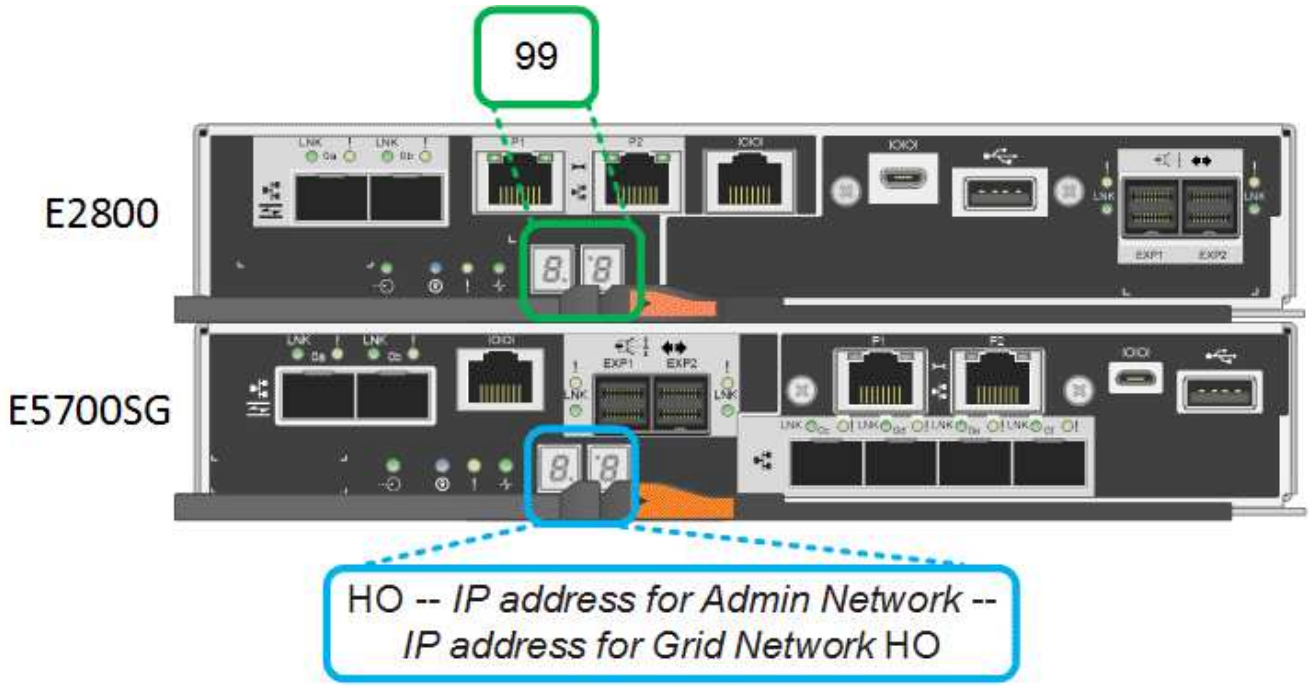
E2800 コントローラと E5700SG コントローラでは、さまざまなステータスとエラーコードが表示されています。

これらのコードの意味については、次のリソースを参照してください。

| コントローラ | 参照 |
| --- | --- |
| E2800 コントローラ | E5700 and E2800 System Monitoring Guide<br>• 注： * E シリーズ E5700 コントローラに関するコードの一覧は、アプライアンスの E5700SG コントローラには適用されません。 |
| E5700SG コントローラのものです | E5700SG コントローラのステータス・インジケータ |

手順

1. ブート時に、デジタル表示ディスプレイに表示されるコードを確認して進行状況を監視します。
   - E2800コントローラのデジタル表示ディスプレイに、* OS 、 SD 、 ***blank*** 一日の開始処理を実行中であることを示します。
   - E5700SG コントローラのデジタル表示ディスプレイには、 * AA * と * FF * で終わる一連のコードが表示されています。
2. コントローラがブートしたら、デジタル表示ディスプレイに次のコードが表示されることを確認します。




| コントローラ | デジタル表示ディスプレイ |
| --- | --- |
| E2800 コントローラ | E シリーズコントローラシェルフのデフォルト ID である 99 が表示されます。 |
| E5700SG コントローラのものです | HO * が表示され、続いて 2 つの数字が順番に表示されます。<br><br>`HO -- IP address for Admin Network -- IP address for Grid Network HO`<br><br>最初に表示される数字は、コントローラの管理ポート 1 に対して DHCP によって割り当てられた IP アドレスです。このアドレスは、コントローラを StorageGRID の管理ネットワークに接続するときに使用されます。2 番目に表示される数字は、StorageGRID のグリッドネットワークにアプライアンスを接続するときに使用される DHCP によって割り当てられた IP アドレスです。<br><br>• 注： * DHCP を使用して IP アドレスを割り当てることができなかった場合は、 0.0.0.0 と表示されます。 |

3. その他の値がデジタル表示ディスプレイに表示される場合は、「ハードウェアの設置に関するトラブルシューティング」を参照し、インストール手順が正しく完了したことを確認してください。問題を解決できない場合は、テクニカルサポートにお問い合わせください。

関連情報

"E5700SG コントローラのステータスインジケータ"

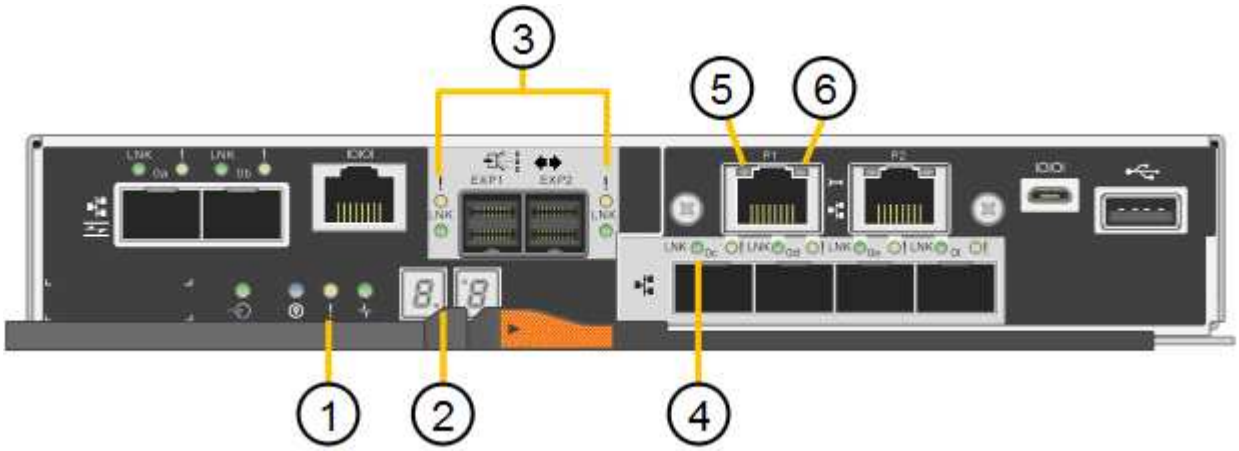
"ハードウェアの設置のトラブルシューティング"

"E5700 and E2800 System Monitoring Guide"

**E5700SG** コントローラのステータスインジケータ

アプライアンスの電源投入やハードウェアの初期化の実行中、 E5700SG コントローラのデジタル表示ディスプレイと LED にステータスコードとエラーコードが表示されます。これらの画面を使用して、ステータスを確認したり、エラーのトラブルシューティングを行ったりできます。

StorageGRID アプライアンスインストーラが開始されたら、 E5700SG コントローラのステータスインジケータを定期的に確認してください。




| | 表示 | 説明 |
|---|---|---|
| 1. | 警告 LED | 黄色：コントローラに障害が発生してオペレータによる対応が必要であるか、インストールスクリプトが見つかりませんでした。<br><br>off ：コントローラは正常に動作しています。 |
| 2. | デジタル表示ディスプレイ | 診断コードを表示します<br><br>デジタル表示ディスプレイの数字から、アプライアンスのエラーと動作状態を確認できます。 |
| 3. | 拡張ポート警告 LED | オレンジ：アプライアンスでは拡張ポートが使用されないため、これらの LED は常に黄色（リンクが確立されていない状態）です。 |
| 4. | ホストポートリンクステータス LED | グリーン：リンクがアップ状態です。<br><br>消灯：リンクがダウン状態です。 |

| | 表示 | 説明 |
|---|---|---|
| 5. | イーサネットリンク状態 LED | 緑：リンクが確立されています。<br><br>消灯：リンクが確立されていません。 |
| 6. | イーサネットアクティビティ LED | グリーン：管理ポートと接続されているデバイス（イーサネットスイッチなど）の間のリンクが稼働しています。<br><br>消灯：コントローラと接続されているデバイスの間にリンクがありません。<br><br>緑色の点滅：イーサネットアクティビティがあります。 |

一般的なブートコード

アプライアンスのブート時やハードリセット後に、次の処理が実行されます。

1. E5700SG コントローラのデジタル表示ディスプレイには、コントローラ固有ではない一連の一般的なコードが表示されています。全般的な連続コードは、 AA と FF で終わります。
2. E5700SG コントローラ固有のブート時のコードが表示されます。

**E5700SG** コントローラのブート時のコードです

アプライアンスが正常にブートされているときは、 E5700SG コントローラのデジタル表示ディスプレイに次のコードが記載された順序で表示されています。

| コード | を示します |
|---|---|
| こんにちは | マスターブートスクリプトが開始されました。 |
| PP （ PP ） | FPGA の更新が必要かどうかがチェックされています。 |
| HP | 10 / 25GbE コントローラファームウェアの更新が必要かどうかがチェックされています。 |
| 朝食付き | ファームウェアの更新の適用が完了し、システムがリブートしています。 |
| FP | ハードウェアサブシステムのファームウェアの更新の確認が完了しました。コントローラ間の通信サービスが開始されています。 |
| 彼 | システムが E2800 コントローラとの接続待ちで、 SANtricity オペレーティングシステムと同期しています。<br><br>• 注：このブート手順 がこの段階から進まない場合は、 2 台のコントローラ間の接続を確認してください。 |

| コード | を示します |
| --- | --- |
| HC | 既存の StorageGRID のインストールデータがチェックされています。 |
| HO | StorageGRID アプライアンスインストーラが実行されている。 |
| 高可用性 | StorageGRID が実行されています。 |

**E5700SG** コントローラのエラーコードです

これらのコードは、 E5700SG コントローラのブート時に表示されるエラー状態を表しています。特定の下位レベルのハードウェアエラーが発生した場合は、 2 桁の 16 進数コードが追加で表示されます。これらのいずれかのコードが数秒にわたって表示され、規定のトラブルシューティング手順を実行してもエラーを解決できない場合は、テクニカルサポートにお問い合わせください。

| コード | を示します |
| --- | --- |
| 22 | どのブートデバイスにもマスターブートレコードが見つかりません。 |
| 23 | 内蔵フラッシュディスクが接続されていません。 |
| 2A 、 2B | スタックバスにより、 DIMM SPD データを読み取れません。 |
| 40 | DIMM が無効です。 |
| 41. | DIMM が無効です。 |
| 42 | メモリテストに失敗しました。 |
| 51 | SPD の読み取りに失敗しました。 |
| 92 ~ 96 | PCI バスの初期化中です。 |
| A0 から A3 | SATA ドライブの初期化中です。 |
| AB | 代替ブートコードです。 |
| AE | OS のブート中です。 |
| EA | DDR4 トレーニングに失敗しました。 |
| E8. | メモリが取り付けられていません。 |
| 欧州連合（ EU | インストールスクリプトが見つかりませんでした。 |

| コード | を示します |
| --- | --- |
| EP | E2800 コントローラとのインストールまたは通信に失敗しました。 |

関連情報

"ハードウェアの設置のトラブルシューティング"

"ネットアップサポート"

## ハードウェアの設定

アプライアンスの電源を入れたら、ハードウェアの監視に使用するソフトウェアである SANtricity System Manager を設定する必要があります。また、 StorageGRID で使用されるネットワーク接続も設定する必要があります。

手順

- "StorageGRID 接続を設定しています"
- "SANtricity システムマネージャにアクセスして設定します"
- "オプション：ノード暗号化を有効にする"
- "オプション：RAIDモードの変更（SG5760のみ）"
- "オプション：アプライアンスに対するネットワークポートの再マッピング"

### StorageGRID 接続を設定しています

StorageGRID アプライアンスをストレージノードとして StorageGRID グリッドに導入するには、アプライアンスと使用するネットワークの間の接続を設定する必要があります。ネットワークを設定するには、 E5700SG コントローラ（アプライアンスのコンピューティングコントローラ）に搭載されている StorageGRID アプライアンスインストーラを参照してください。

手順

- "StorageGRID アプライアンスインストーラへのアクセス"
- "StorageGRID アプライアンスインストーラのバージョンの確認とアップグレード"
- "ネットワークリンクの設定（SG5700）"
- "IPの設定"
- "ネットワーク接続の確認"
- "ポートレベルのネットワーク接続の確認"

#### StorageGRID アプライアンスインストーラへのアクセス

アプライアンスと 3 つの StorageGRID ネットワーク（グリッドネットワーク、管理ネットワーク（オプション）、クライアントネットワーク（オプション））間の接続を設定するには、 StorageGRID アプライアンスインストーラにアクセスする必要がありま

す。

必要なもの

- サポートされているWebブラウザを使用します。
- 使用するすべての StorageGRID ネットワークにアプライアンスを接続しておきます。
- これらのネットワークでのアプライアンスの IP アドレス、ゲートウェイ、およびサブネットを確認しておきます。
- 使用するネットワークスイッチを設定しておきます。

このタスクについて

StorageGRID アプライアンスインストーラに初めてアクセスするときは、 DHCP によって割り当てられた管理ネットワークの IP アドレス（アプライアンスが管理ネットワークに接続されている場合）または DHCP によって割り当てられたグリッドネットワークの IP アドレスを使用できます。管理ネットワークの IP アドレスを使用することを推奨します。グリッドネットワークの DHCP アドレスを使用して StorageGRID アプライアンスインストーラにアクセスすると、リンク設定を変更した場合や静的な IP アドレスを入力した場合に StorageGRID アプライアンスインストーラとの接続が失われる可能性があります。

手順

1. 管理ネットワークが接続されている場合は、管理ネットワークでのアプライアンスの DHCP アドレスを取得し、管理ネットワークが接続されていない場合はグリッドネットワークの DHCP アドレスを取得します。

   次のいずれかを実行できます。

   - E5700SG コントローラのデジタル表示ディスプレイを参照してください。E5700SG コントローラの管理ポート 1 および 10 / 25GbE ポート 2 と 4 を DHCP サーバがあるネットワークに接続している場合は、エンクロージャの電源投入時に動的に割り当てられた IP アドレスの取得が試行されます。コントローラの電源投入プロセスが完了すると、デジタル表示ディスプレイに * HO * と表示され、続いて 2 つの数字が順番に表示されます。

     ```
     HO -- IP address for Admin Network -- IP address for Grid Network HO
     ```

     次の順序で実行します。

     - 最初に表示される数字は、管理ネットワークに接続されているアプライアンスストレージノードの DHCP アドレスです。この IP アドレスは、 E5700SG コントローラの管理ポート 1 に割り当てられています。
     - 2 番目に表示される数字は、グリッドネットワーク上のアプライアンスストレージノードの DHCP アドレスです。この IP アドレスは、アプライアンスに最初に電源を投入するときに、 10 / 25GbE ポート 2 と 4 に割り当てられます。

       DHCP を使用して IP アドレスを割り当てることができなかった場合は、 0.0.0.0 と表示されます。

   - 管理ポート 1 の MAC アドレスをネットワーク管理者に伝え、管理者が管理ネットワークでのこのポートの DHCP アドレスを確認できるようにします。MAC アドレスは、 E5700SG コントローラのポートの横のラベルに記載されています。

2. いずれかの DHCP アドレスを取得できた場合は、次の手順を実行します。

   a. サービスラップトップで Web ブラウザを開きます。

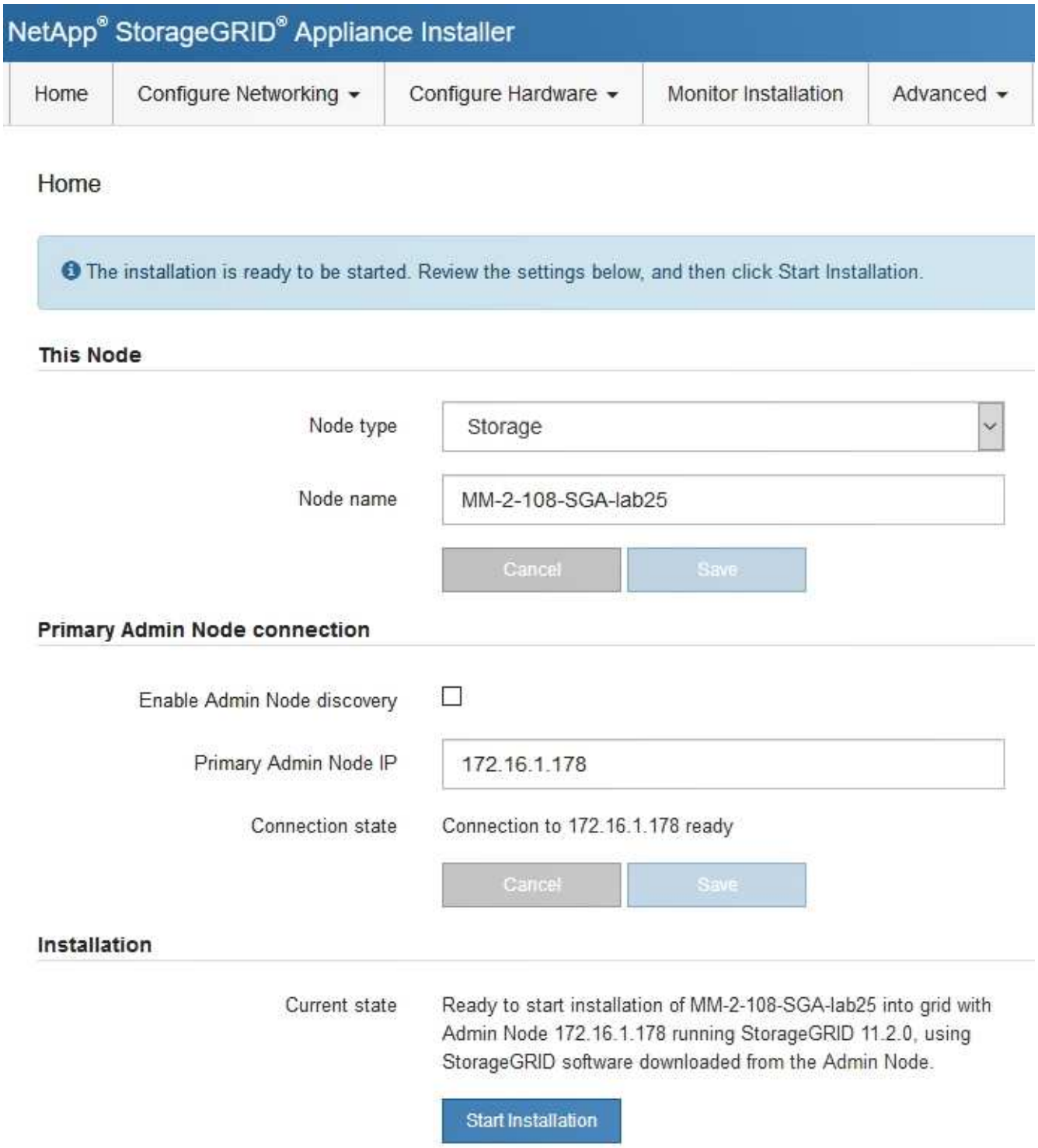
   b. StorageGRID アプライアンスインストーラのURLに+を入力します
   **`https://E5700SG_Controller_IP:8443`**

      の場合 `E5700SG_Controller_IP`を使用して、コントローラのDHCPアドレスを指定します（管理ネットワークを使用する場合はそのIPアドレスを使用）。

   c. セキュリティアラートが表示された場合は、ブラウザのインストールウィザードを使用して証明書を表示およびインストールします。

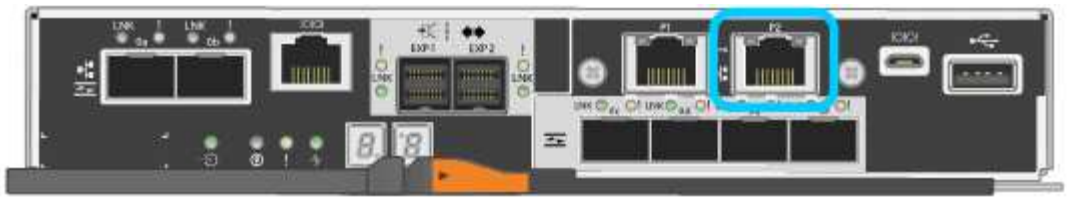
      次回この URL にアクセスしたときに、アラートは表示されません。

      StorageGRID アプライアンスインストーラのホームページが表示されます。このページに最初にアクセスしたときに表示される情報とメッセージは、アプライアンスと StorageGRID ネットワークの現在の接続状況によって異なります。エラーメッセージが表示された場合は、以降の手順で解決されます。




3. E5700SG コントローラで DHCP を使用して IP アドレスを取得できなかった場合：

   a. イーサネットケーブルを使用して、 E5700SG コントローラの管理ポート 2 にサービスラップトップを接続してください。



b. サービスラップトップで Web ブラウザを開きます。

c. StorageGRID アプライアンスインストーラのURLに+を入力します
**`https://169.254.0.1:8443`**

StorageGRID アプライアンスインストーラのホームページが表示されます。このページに最初にアクセスしたときに表示される情報とメッセージは、アプライアンスの現在の接続状況によって異なります。

リンクローカル接続でホームページにアクセスできない場合は、サービスラップトップのIPアドレスをに設定します `169.254.0.2`をクリックして、もう一度やり直してください。

4. ホームページに表示されたメッセージを確認し、必要に応じてリンク設定と IP 設定を行います。

関連情報

"Web ブラウザの要件"

**StorageGRID** アプライアンスインストーラのバージョンの確認とアップグレード

# StorageGRID のすべての機能がサポートされるようにするには、アプライアンスの StorageGRID アプライアンスインストーラのバージョンと StorageGRID システムにインストールされているソフトウェアのバージョンが一致している必要があります。

必要なもの

StorageGRID アプライアンスインストーラにアクセスしておきます。

このタスクについて

StorageGRID アプライアンスは、 StorageGRID アプライアンスインストーラがプリインストールされた状態で出荷されます。最近アップグレードした StorageGRID システムにアプライアンスを追加する場合は、そのアプライアンスを新しいノードとしてインストールする前に、 StorageGRID アプライアンスインストーラの手動アップグレードが必要になることがあります。

新しい StorageGRID バージョンにアップグレードすると、 StorageGRID アプライアンスインストーラが自動的にアップグレードされます。インストールされているアプライアンスノードでは、 StorageGRID アプライアンスインストーラをアップグレードする必要はありません。この手順 が必要になるのは、以前のバージョンの StorageGRID アプライアンスインストーラを搭載したアプライアンスをインストールする場合のみです。

手順

1. StorageGRID アプライアンス・インストーラから、 * アドバンスト * > * アップグレード・ファームウェア * を選択します。
2. 現在のファームウェアバージョンとStorageGRID システムにインストールされているソフトウェアバージョンを比較します（Grid Managerから* Help > About *を選択します）。

2 つのバージョンの 2 桁目の数字が一致している必要があります。たとえば、StorageGRID システムでバージョン11.* 5 。***x*.y_y__**を実行している場合、**StorageGRID** アプライアンスインストーラのバージョンは**3.** 5 *._z_にする必要があります。

3. アプライアンスに StorageGRID アプライアンスインストーラの下位バージョンがインストールされている場合は、 StorageGRID のネットアップのダウンロードページにアクセスします。

   "ネットアップのダウンロード： StorageGRID"

   ネットアップアカウントのユーザ名とパスワードを使用してサインインします。

4. StorageGRID アプライアンス * 対応するバージョンのサポート・ファイルと対応するチェックサム・ファイルをダウンロードします。

   StorageGRID アプライアンスファイルのサポートファイルは、です `.zip` すべてのStorageGRID アプライアンスモデルの最新および以前のファームウェアバージョンを、各コントローラタイプのサブディレクトリに格納してアーカイブする。

   StorageGRID アプライアンスファイルのサポートファイルをダウンロードしたら、を展開します `.zip` StorageGRID アプライアンスインストーラのインストールに関する重要な情報については、READMEファイルをアーカイブして参照してください。

5. StorageGRID アプライアンスインストーラのファームウェアのアップグレードページの手順に従って、次の手順を実行します。
   a. コントローラタイプとチェックサムファイルに適したサポートファイル（ファームウェアイメージ）をアップロードします。
   b. 非アクティブなパーティションをアップグレードします。
   c. パーティションを再起動してスワップします。
   d. 2番目のパーティションをアップグレードします。

関連情報

"StorageGRID アプライアンスインストーラへのアクセス"

ネットワークリンクの設定（**SG5700**）

# アプライアンスをグリッドネットワーク、クライアントネットワーク、および管理ネットワークに接続するために使用するポートのネットワークリンクを設定できます。リンク速度およびポートボンディングモードとネットワークボンディングモードを設定できます。

必要なもの

10 / 25GbE ポートに 25GbE のリンク速度を使用する場合は、次の要件があります。

- 使用するポートに SFP28 トランシーバを取り付けておきます。
- この速度をサポートするスイッチにポートを接続しておきます。
- この速度を使用するようにスイッチを設定する方法を理解しておきます。

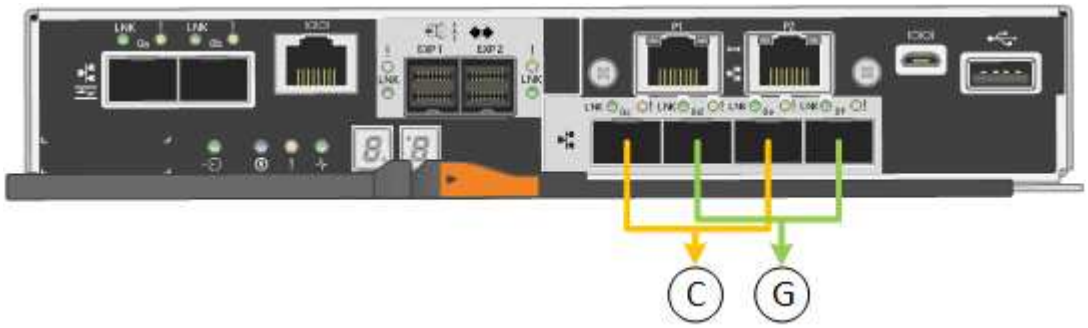
10 / 25GbE ポートにアグリゲートポートボンディングモード、 LACP ネットワークボンディングモード、ま

たは VLAN タギングを使用する場合は、次の要件があります。

- アプライアンスのポートを、 VLAN と LACP をサポートするスイッチに接続しておきます。
- 複数のスイッチを LACP ボンドに加える場合は、 Multi-Chassis Link Aggregation （ MLAG ）グループまたは同等の機能をサポートするスイッチを使用します。
- VLAN 、 LACP 、 MLAG などを使用するようにスイッチを設定する方法について理解しておく必要があります。
- 各ネットワークに使用する一意の VLAN タグを確認しておきます。この VLAN タグが各ネットワークパケットに追加され、ネットワークトラフィックが正しいネットワークにルーティングされます。
- 管理ネットワークにアクティブ / バックアップモードを使用する場合は、コントローラの両方の管理ポートにイーサネットケーブルを接続しておきます。

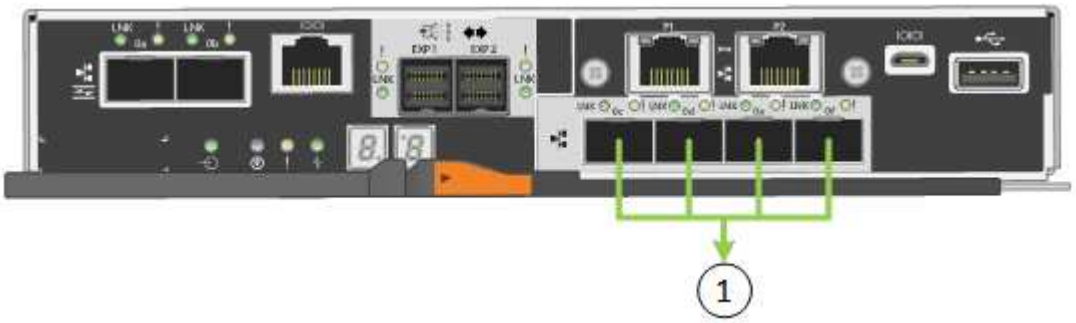
このタスクについて

次の図では、 4 つの 10 / 25GbE ポートが Fixed ポートボンディングモードでボンディングされています（デフォルトの構成）。




| | ボンディングされるポート |
|---|---|
| C | このネットワークを使用する場合、ポート 1 とポート 3 がクライアントネットワーク用にボンディングされます。 |
| G | ポート 2 とポート 4 がグリッドネットワーク用にボンディングされます。 |

次の図では、 4 つの 10 / 25GbE ポートがアグリゲートポートボンディングモードでボンディングされています。



| | ボンディングされるポート |
|---|---|
| 1. | 4 つのポートすべてを 1 つの LACP ボンドにグループ化して、すべてのポートをグリッドネットワークとクライアントネットワークのトラフィックに使用できるようにします。 |

次の表に、 4 つの 10 / 25GbE ポートを設定するためのオプションをまとめます。デフォルトの設定は太字で示しています。デフォルト以外の設定を使用する場合にのみ、 Link Configuration ページで設定を行う必要があります。

- * 固定（デフォルト）ポートボンディングモード *

| ネットワークボンディングモード | クライアントネットワークが無効な場合（デフォルト） | クライアントネットワークが有効になりました |
|---|---|---|
| アクティブ/バックアップ（デフォルト） | • ポート 2 と 4 がグリッドネットワークにアクティブ / バックアップボンドを使用します。<br>• ポート 1 と 3 は使用されません。<br>• VLAN タグはオプションです。 | • ポート 2 と 4 がグリッドネットワークにアクティブ / バックアップボンドを使用します。<br>• ポート 1 と 3 がクライアントネットワークに Active-Backup ボンドを使用します。<br>• ネットワーク管理者用に、両方のネットワークに VLAN タグを指定できます。 |
| LACP （ 802.3ad ） | • ポート 2 と 4 がグリッドネットワークに LACP ボンドを使用します。<br>• ポート 1 と 3 は使用されません。<br>• VLAN タグはオプションです。 | • ポート 2 と 4 がグリッドネットワークに LACP ボンドを使用します。<br>• ポート 1 と 3 がクライアントネットワークに LACP ボンドを使用します。<br>• ネットワーク管理者用に、両方のネットワークに VLAN タグを指定できます。 |

- * アグリゲートポートボンディングモード *

| ネットワークボンディングモード | クライアントネットワークが無効な場合（デフォルト） | クライアントネットワークが有効になりました |
|---|---|---|
| LACP （ 802.3ad ）のみ | • ポート 1~4 がグリッドネットワークに単一の LACP ボンドを使用します。<br>• 単一の VLAN タグでグリッドネットワークのパケットが識別されます。 | • ポート 1~4 がグリッドネットワークとクライアントネットワークに単一の LACP ボンドを使用します。<br>• 2 つの VLAN タグで、グリッドネットワークのパケットとクライアントネットワークのパケットを分離できます。 |

ポートボンディングモードとネットワークボンディングモードの詳細については、 E5700SG コントローラでの 10 / 25GbE ポートの接続に関する情報を参照してください。

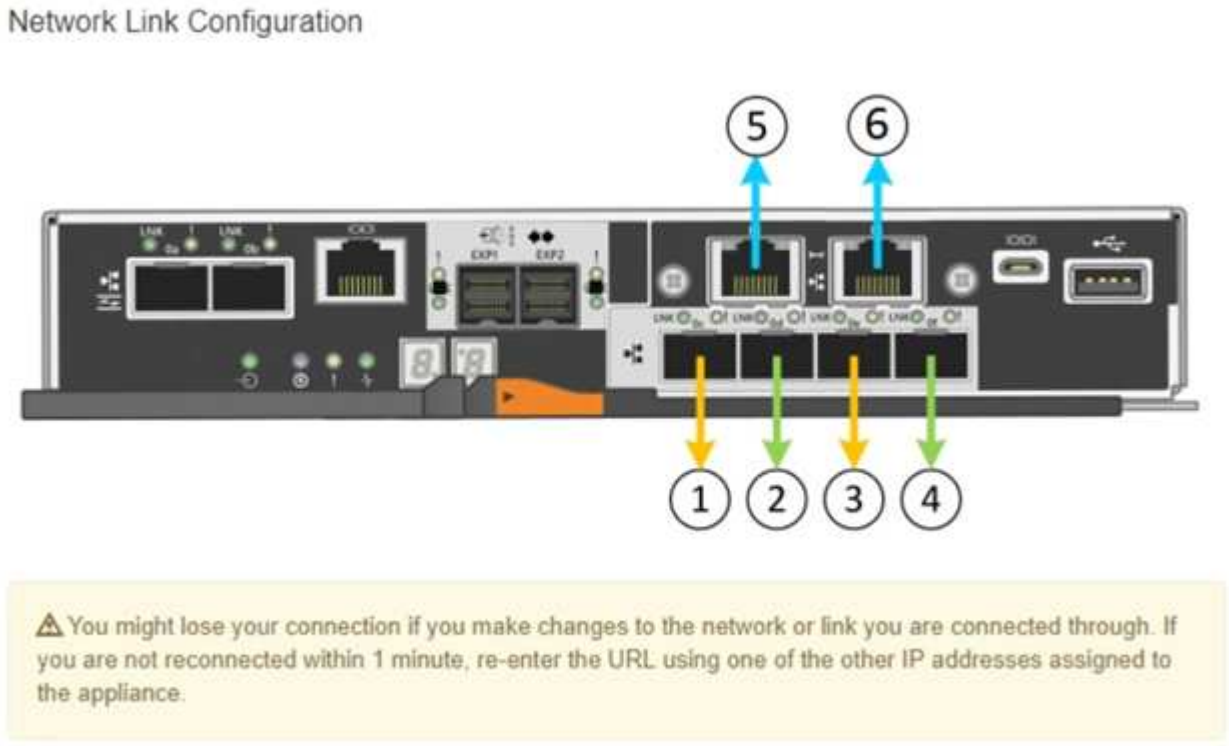
この図では、 E5700SG コントローラの 2 つの 1GbE 管理ポートが管理ネットワーク用に Active-Backup ネッ

トワークボンディングモードでボンディングされています。

手順

1. StorageGRID アプライアンスインストーラのメニューバーから、 *Configure Networking *>*Link Configuration * をクリックします。

   Network Link Configuration ページには、アプライアンスの図と、ネットワークポートおよび管理ポートの番号が表示されます。



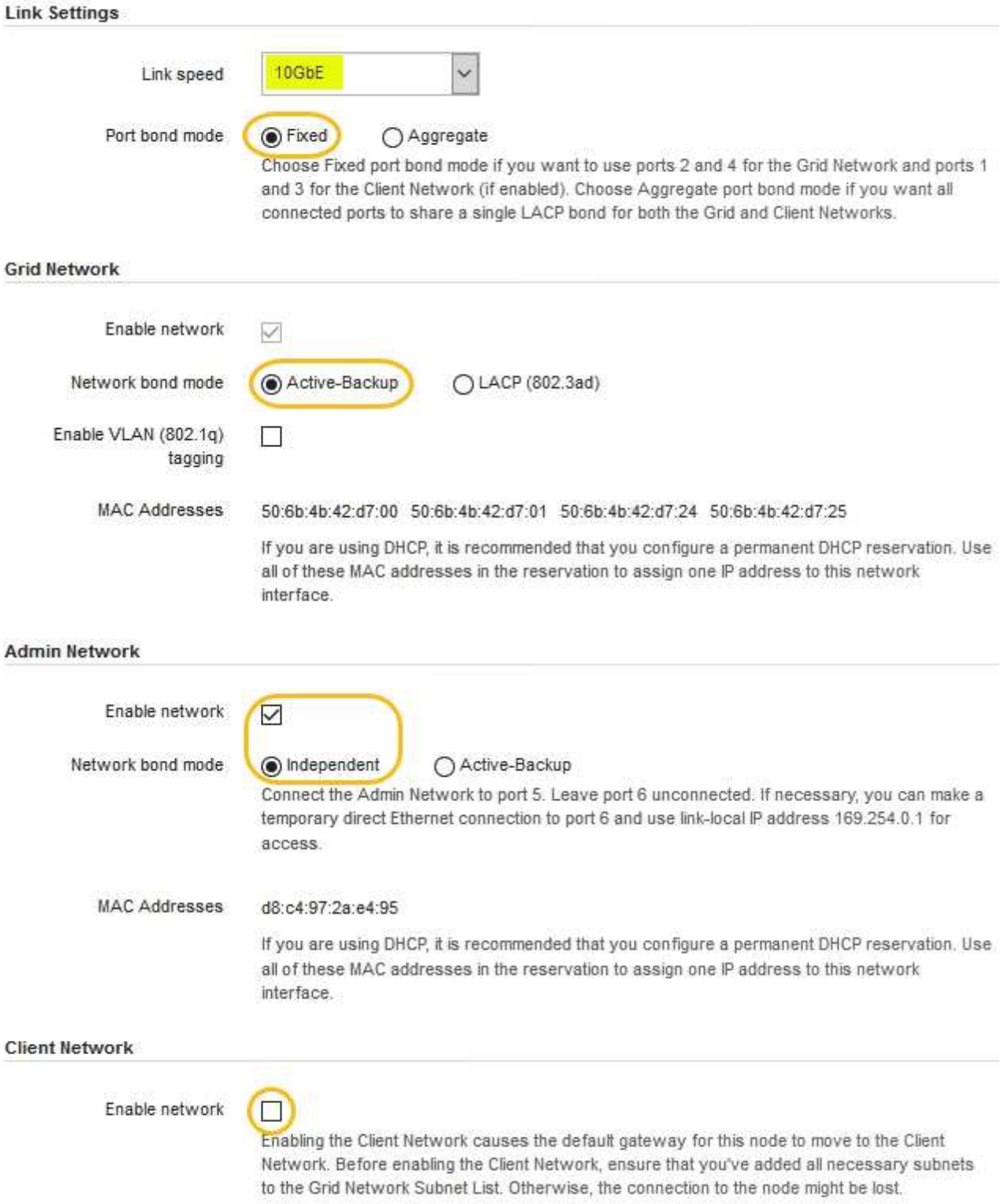

   Link Status テーブルには、番号が付けられたポートのリンクステート（アップ / ダウン）と速度（ 1/10/25 / 40/100Gbps ）が表示されます。

**Link Status**

| Link | State | Speed (Gbps) |
|---|---|---|
| 1 | Up | 25 |
| 2 | Up | 25 |
| 3 | Up | 25 |
| 4 | Up | 25 |
| 5 | Up | 1 |
| 6 | Up | 1 |

このページに初めてアクセスしたときの動作は次のとおりです。

- * リンク速度 * は * 10GbE * に設定されています。
- * ポートボンディングモード * は「 * Fixed 」に設定されます。
- * グリッドネットワークのネットワークボンディングモード * が「アクティブ / バックアップ」に設定されています。
- 管理ネットワーク * が有効になっており、ネットワークボンディングモードが * Independent * に設定されています。
- クライアントネットワーク * が無効になっています。



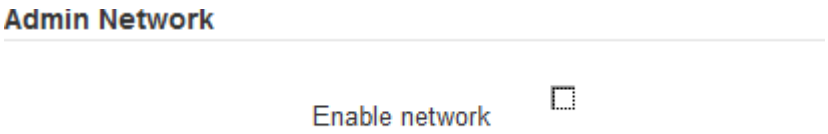

2. 10 / 25GbE ポートに 25GbE のリンク速度を使用する場合は、リンク速度のドロップダウンリストから * 25GbE * を選択します。

   グリッドネットワークとクライアントネットワークに使用するネットワークスイッチも、この速度をサポートし、この速度に対応するように設定する必要があります。ポートに SFP28 トランシーバを取り付ける必要があります。

3. 使用する StorageGRID ネットワークを有効または無効にします。

   グリッドネットワークは必須です。このネットワークは無効にできません。

   a. アプライアンスが管理ネットワークに接続されていない場合は、管理ネットワークの * ネットワークを有効にする * チェックボックスの選択を解除します。

   b. アプライアンスがクライアントネットワークに接続されている場合は、クライアントネットワークの * ネットワークを有効にする * チェックボックスをオンにします。

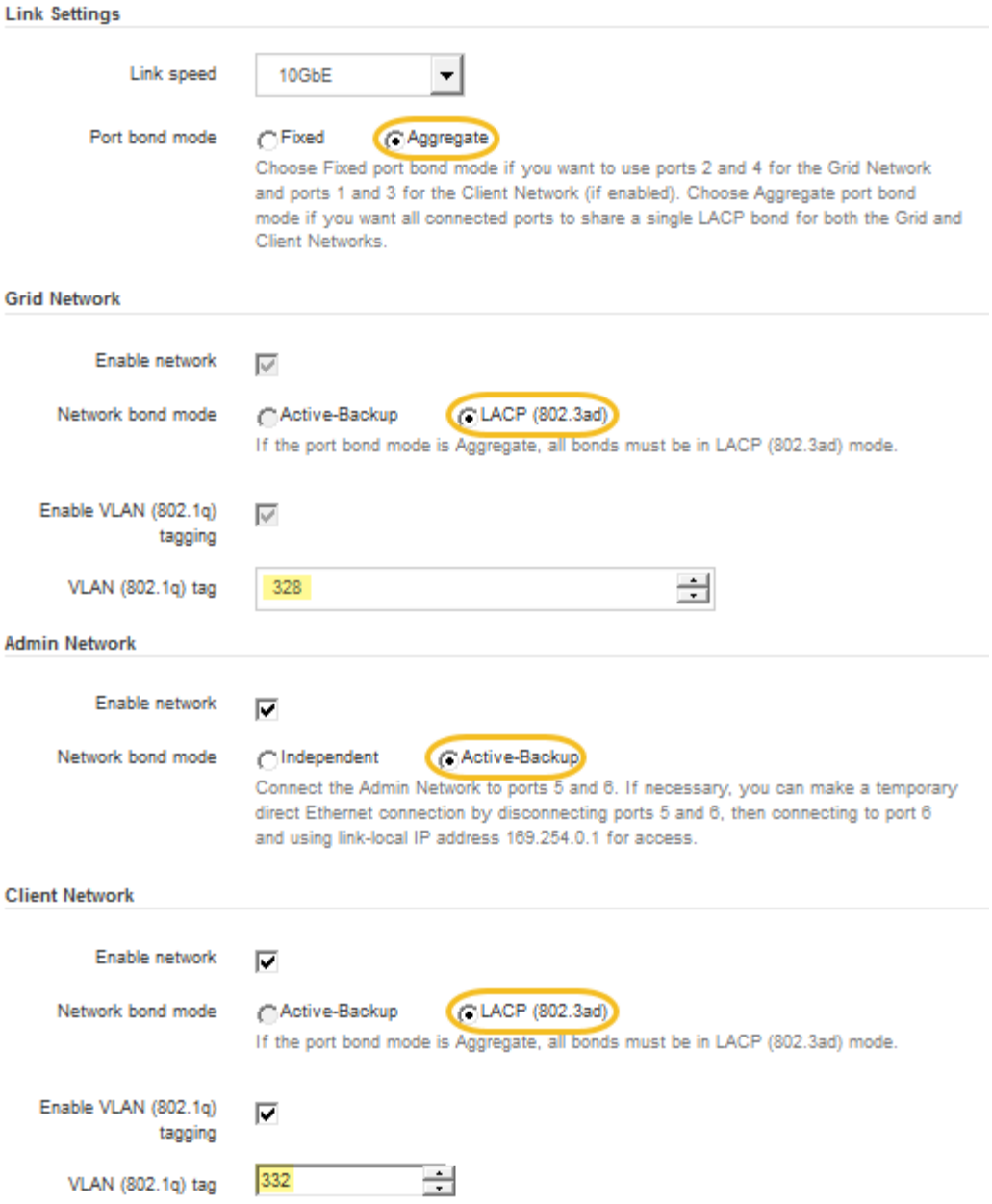
      これで、 10 / 25GbE ポートでのクライアントネットワークの設定が表示されます。

4. 表を参照して、ポートボンディングモードとネットワークボンディングモードを設定します。

   この例では、次のように

   ◦ * グリッドネットワークとクライアントネットワークでアグリゲート * と * LACP * が選択されました。各ネットワークに一意の VLAN タグを指定する必要があります。値は 0~4095 の間で選択できます。

   ◦ * 管理ネットワーク用に選択されたアクティブ / バックアップ * 。




5. 選択に問題がなければ、 * 保存 * をクリックします。

> 接続しているネットワークまたはリンクを変更すると、接続が失われる可能性があります。1分以内に再接続されない場合は、アプライアンスに割り当てられている他のIPアドレスのいずれかを使用してStorageGRID アプライアンスインストーラのURLを再入力します：+
> **`https://E5700SG_Controller_IP:8443`**

関連情報

"E5700SG コントローラポートのポートボンディングモード"

**IP**の設定

## StorageGRID アプライアンスインストーラを使用して、 StorageGRID のグリッドネッ

# トワーク、管理ネットワーク、クライアントネットワークでアプライアンスストレージノードに使用される IP アドレスとルーティング情報を設定します。

このタスクについて

接続された各ネットワークでアプライアンスの静的 IP を割り当てるか、 DHCP サーバでアドレスの永久リースを割り当てる必要があります。

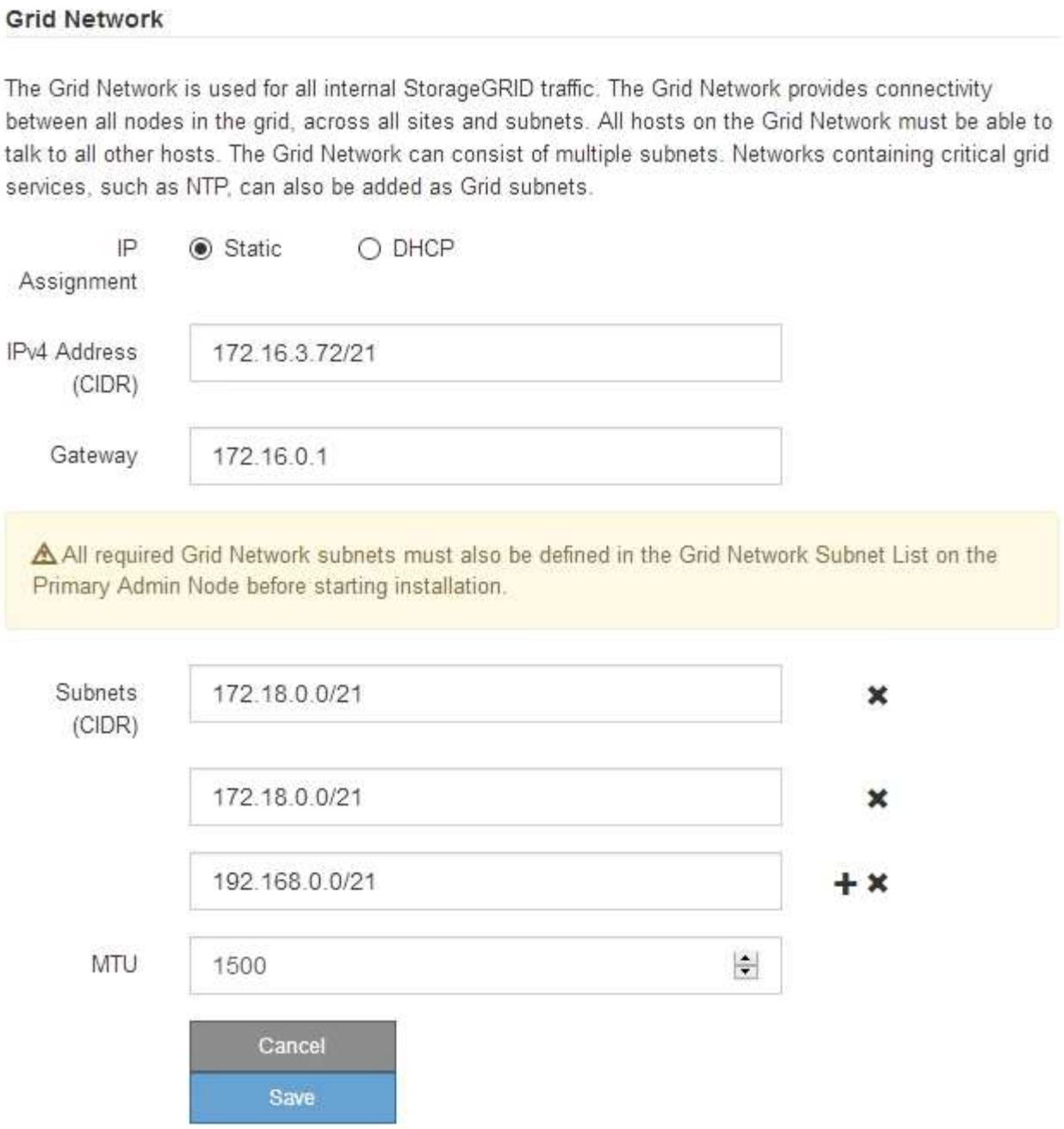
リンク設定を変更する場合は、 E5700SG コントローラのリンク設定の変更手順を参照してください。

手順

1. StorageGRID アプライアンスインストーラで、 * ネットワークの設定 * > * IP 構成 * を選択します。

   [IP Configuration] ページが表示されます。

2. グリッドネットワークを設定するには、ページの * グリッドネットワーク * セクションで * 静的 * または * DHCP * のいずれかを選択します。




3. 「 * Static * 」を選択した場合は、次の手順に従ってグリッドネットワークを設定します。
   a. CIDR 表記を使用して静的 IPv4 アドレスを入力します。
   b. ゲートウェイを入力します。

      ネットワークにゲートウェイがない場合は、同じ静的 IPv4 アドレスを再入力します。

   c. ジャンボフレームを使用する場合は、 MTU フィールドを 9000 などのジャンボフレームに適した値に変更します。それ以外の場合は、デフォルト値 1500 のままにします。

      ネットワークの MTU 値は、ノードが接続されているスイッチポートに設定されている値と同じである必要があります。そうしないと、ネットワークパフォーマンスの問題やパケット損失が発生する可能性があります。

ネットワークのパフォーマンスを最大限に高めるには、すべてのノードのグリッドネットワークインターフェイスで MTU 値がほぼ同じになるように設定する必要があります。個々のノードのグリッドネットワークの MTU 設定に大きな違いがある場合は、 * Grid Network MTU mismatch * アラートがトリガーされます。MTU 値はすべてのネットワークタイプで同じである必要はありません。

d. [ 保存（ Save ） ] をクリックします。

IP アドレスを変更すると、ゲートウェイとサブネットのリストも変更される可能性があります。

StorageGRID アプライアンスインストーラへの接続が失われた場合は、割り当てた新しい静的 IP アドレスを使用して URL を再入力します。たとえば、「+」と入力します
`https://services_appliance_IP:8443`

e. グリッドネットワークのサブネットのリストが正しいことを確認します。

グリッドサブネットがある場合は、グリッドネットワークゲートウェイが必要です。指定するすべてのグリッドサブネットが、このゲートウェイ経由でアクセス可能であることが必要です。StorageGRID のインストールを開始するときに、プライマリ管理ノードのグリッドネットワークサブネットリストでこれらのサブネットも定義する必要があります。

デフォルトルートはリストされません。クライアントネットワークが有効になっていない場合は、デフォルトルートがグリッドネットワークゲートウェイを使用します。

- サブネットを追加するには、挿入アイコンをクリックします ➕ アイコン"] をクリックします。
- 使用されていないサブネットを削除するには、削除アイコンをクリックします ✖。

f. [ 保存（ Save ） ] をクリックします。

4. 「 * DHCP * 」を選択した場合は、次の手順に従ってグリッドネットワークを設定します。

a. [**DHCP**] ラジオボタンを選択した後、 [**Save**] をクリックします。

[* IPv4 アドレス * ] 、 [ * ゲートウェイ * ] 、および [ * サブネット * ] フィールドには、自動的に値が入力されます。DHCP サーバが MTU 値を割り当てるように設定されている場合は、 **MTU** フィールドにその値が入力され、フィールドは読み取り専用になります。

Web ブラウザは、 StorageGRID アプライアンスインストーラの新しい IP アドレスに自動的にリダイレクトされます。

b. グリッドネットワークのサブネットのリストが正しいことを確認します。

グリッドサブネットがある場合は、グリッドネットワークゲートウェイが必要です。指定するすべてのグリッドサブネットが、このゲートウェイ経由でアクセス可能であることが必要です。StorageGRID のインストールを開始するときに、プライマリ管理ノードのグリッドネットワークサブネットリストでこれらのサブネットも定義する必要があります。

デフォルトルートはリストされません。クライアントネットワークが有効になっていない場合は、デフォルトルートがグリッドネットワークゲートウェイを使用します。

- サブネットを追加するには、挿入アイコンをクリックします ➕ アイコン"] をクリックします。

- 使用されていないサブネットを削除するには、削除アイコンをクリックします ✖。

c. ジャンボフレームを使用する場合は、 MTU フィールドを 9000 などのジャンボフレームに適した値に変更します。それ以外の場合は、デフォルト値 1500 のままにします。

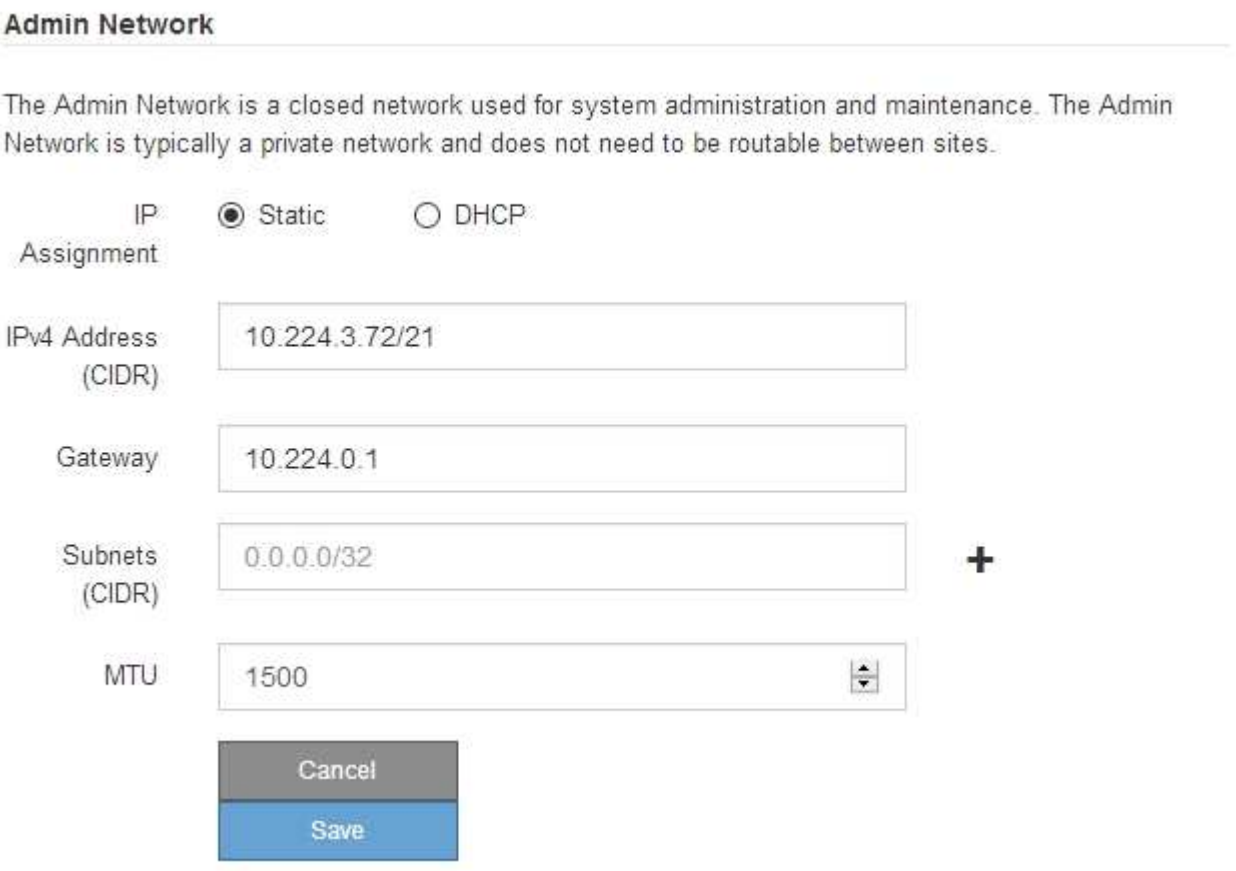
ネットワークの MTU 値は、ノードが接続されているスイッチポートに設定されている値と同じである必要があります。そうしないと、ネットワークパフォーマンスの問題やパケット損失が発生する可能性があります。

ネットワークのパフォーマンスを最大限に高めるには、すべてのノードのグリッドネットワークインターフェイスで MTU 値がほぼ同じになるように設定する必要があります。個々のノードのグリッドネットワークの MTU 設定に大きな違いがある場合は、 * Grid Network MTU mismatch * アラートがトリガーされます。MTU 値はすべてのネットワークタイプで同じである必要はありません。

a. [ 保存（ Save ） ] をクリックします。

5. 管理ネットワークを設定するには、ページの管理ネットワークセクションで * 静的 * または * DHCP * のいずれかを選択します。

管理ネットワークを設定するには、 Link Configuration ページで管理ネットワークを有効にする必要があります。




6. 「 * Static * 」を選択した場合は、次の手順に従って管理ネットワークを設定します。

a. アプライアンスの管理ポート 1 に対して、 CIDR 表記を使用して静的 IPv4 アドレスを入力します。

管理ポート 1 は、アプライアンス右端にある 2 つの 1GbE RJ45 ポートのうち、左側のポートです。

b. ゲートウェイを入力します。

ネットワークにゲートウェイがない場合は、同じ静的 IPv4 アドレスを再入力します。

c. ジャンボフレームを使用する場合は、 MTU フィールドを 9000 などのジャンボフレームに適した値に変更します。それ以外の場合は、デフォルト値 1500 のままにします。

ネットワークの MTU 値は、ノードが接続されているスイッチポートに設定されている値と同じである必要があります。そうしないと、ネットワークパフォーマンスの問題やパケット損失が発生する可能性があります。

d. [ 保存（ Save ） ] をクリックします。

IP アドレスを変更すると、ゲートウェイとサブネットのリストも変更される可能性があります。

StorageGRID アプライアンスインストーラへの接続が失われた場合は、割り当てた新しい静的 IP アドレスを使用して URL を再入力します。たとえば、「+」と入力します
**`https://services_appliance:8443`**

e. 管理ネットワークのサブネットのリストが正しいことを確認します。

指定したゲートウェイを使用してすべてのサブネットにアクセスできることを確認する必要があります。

管理ネットワークゲートウェイを使用するデフォルトルートは作成できません。

- サブネットを追加するには、挿入アイコンをクリックします ➕ アイコン"] をクリックします。
- 使用されていないサブネットを削除するには、削除アイコンをクリックします ✖。

f. [ 保存（ Save ） ] をクリックします。

7. [**DHCP**] を選択した場合は、次の手順に従って管理ネットワークを設定します。

a. [**DHCP**] ラジオボタンを選択した後、 [**Save**] をクリックします。

[* IPv4 アドレス * ] 、 [ * ゲートウェイ * ] 、および [ * サブネット * ] フィールドには、自動的に値が入力されます。DHCP サーバが MTU 値を割り当てるように設定されている場合は、 **MTU** フィールドにその値が入力され、フィールドは読み取り専用になります。

Web ブラウザは、 StorageGRID アプライアンスインストーラの新しい IP アドレスに自動的にリダイレクトされます。

b. 管理ネットワークのサブネットのリストが正しいことを確認します。

指定したゲートウェイを使用してすべてのサブネットにアクセスできることを確認する必要があります。

管理ネットワークゲートウェイを使用するデフォルトルートは作成できません。

- サブネットを追加するには、挿入アイコンをクリックします ➕ アイコン"] をクリックします。

- 使用されていないサブネットを削除するには、削除アイコンをクリックします ✖。

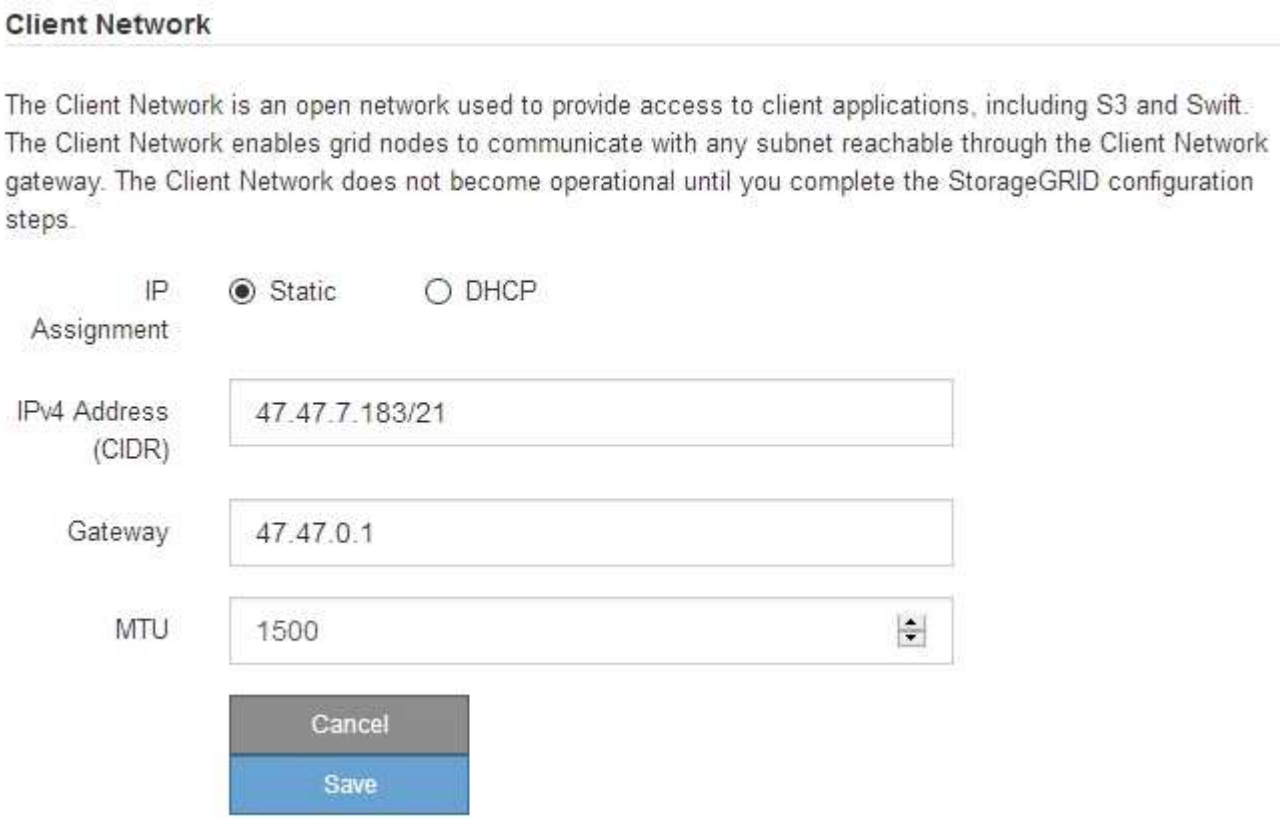
c. ジャンボフレームを使用する場合は、 MTU フィールドを 9000 などのジャンボフレームに適した値に変更します。それ以外の場合は、デフォルト値 1500 のままにします。

> ネットワークの MTU 値は、ノードが接続されているスイッチポートに設定されている値と同じである必要があります。そうしないと、ネットワークパフォーマンスの問題やパケット損失が発生する可能性があります。

d. [ 保存（ Save ） ] をクリックします。

8. クライアントネットワークを設定するには、ページの * クライアントネットワーク * セクションで * 静的 * または * DHCP * のいずれかを選択します。

> クライアントネットワークを設定するには、 Link Configuration ページで Client Network を有効にする必要があります。




9. * Static * を選択した場合は、次の手順に従ってクライアントネットワークを設定します。

a. CIDR 表記を使用して静的 IPv4 アドレスを入力します。

b. [ 保存（ Save ） ] をクリックします。

c. クライアントネットワークゲートウェイの IP アドレスが正しいことを確認します。

> クライアントネットワークが有効になっている場合は、デフォルトルートが表示されます。デフォルトルートはクライアントネットワークゲートウェイを使用し、クライアントネットワークが有効になっている間は別のインターフェイスに移動できません。

d. ジャンボフレームを使用する場合は、 MTU フィールドを 9000 などのジャンボフレームに適した値に変更します。それ以外の場合は、デフォルト値 1500 のままにします。

> ネットワークの MTU 値は、ノードが接続されているスイッチポートに設定されている値と同じである必要があります。そうしないと、ネットワークパフォーマンスの問題やパケット損失が発生する可能性があります。

e. [ 保存（ Save ） ] をクリックします。

10. **[DHCP]** を選択した場合は、次の手順に従ってクライアントネットワークを設定します。

a. **[DHCP]** ラジオボタンを選択した後、 **[Save]** をクリックします。

**[IPv4 Address]** フィールドと **[Gateway]** フィールドが自動的に入力されます。DHCP サーバが MTU 値を割り当てるように設定されている場合は、 **MTU** フィールドにその値が入力され、フィールドは読み取り専用になります。

Web ブラウザは、 StorageGRID アプライアンスインストーラの新しい IP アドレスに自動的にリダイレクトされます。

a. ゲートウェイが正しいことを確認します。

> クライアントネットワークが有効になっている場合は、デフォルトルートが表示されます。デフォルトルートはクライアントネットワークゲートウェイを使用し、クライアントネットワークが有効になっている間は別のインターフェイスに移動できません。

b. ジャンボフレームを使用する場合は、 MTU フィールドを 9000 などのジャンボフレームに適した値に変更します。それ以外の場合は、デフォルト値 1500 のままにします。

> ネットワークの MTU 値は、ノードが接続されているスイッチポートに設定されている値と同じである必要があります。そうしないと、ネットワークパフォーマンスの問題やパケット損失が発生する可能性があります。

関連情報

"E5700SGコントローラのリンク設定の変更"

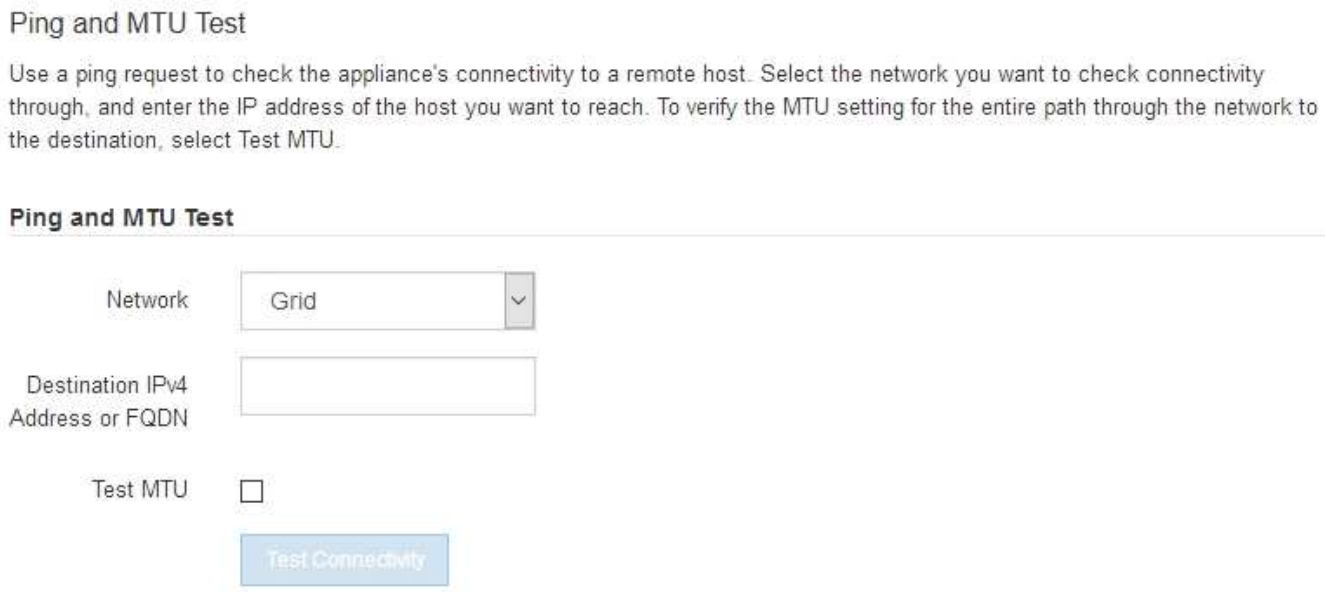
ネットワーク接続の確認

使用する StorageGRID ネットワークに、アプライアンスからアクセスできることを確認する必要があります。ネットワークゲートウェイ経由のルーティングを検証するには、StorageGRID アプライアンスインストーラと異なるサブネット上の IP アドレスとの接続をテストする必要があります。MTU 設定を確認することもできます。

手順

1. StorageGRID アプライアンスインストーラのメニューバーから、 *Configure Networking *>*Ping and MTU Test * をクリックします。

[Ping and MTU Test] ページが表示されます。




2. [* ネットワーク *] ドロップダウンボックスから、テストするネットワークを選択します。グリッド、管理、またはクライアント。
3. そのネットワーク上のホストの IPv4 アドレスまたは完全修飾ドメイン名（ FQDN ）を入力します。

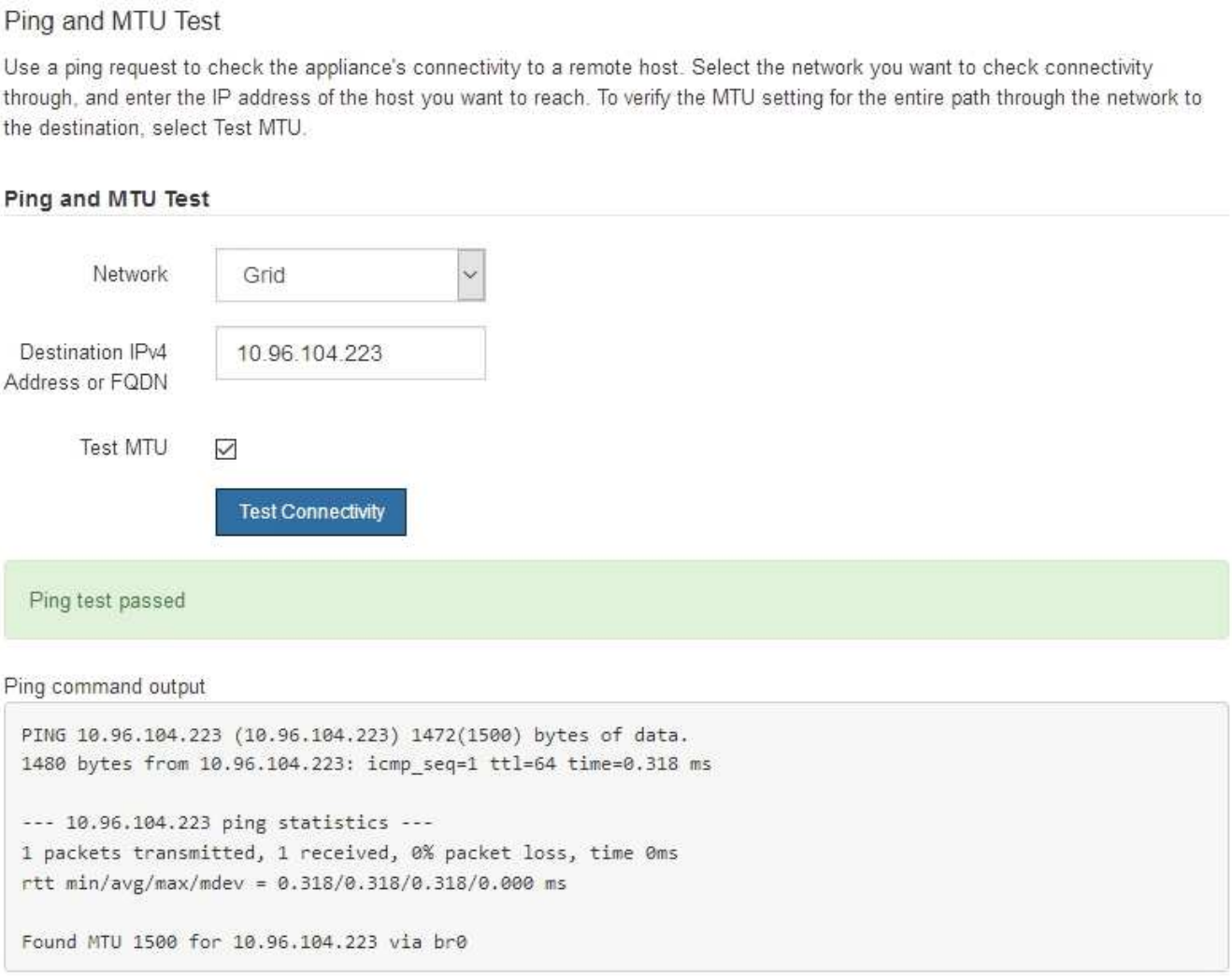
   たとえば、ネットワーク上のゲートウェイやプライマリ管理ノードに ping を送信できます。

4. 必要に応じて、 * Test MTU * チェックボックスをオンにして、ネットワーク経由でデスティネーションへのパス全体の MTU 設定を確認します。

   たとえば、アプライアンスノードと別のサイトのノードの間のパスをテストできます。

5. [ 接続のテスト * ] をクリックします。

   ネットワーク接続が有効な場合は、「 Ping test passed 」メッセージと ping コマンドの出力が表示されます。




関連情報

"ネットワークリンクの設定（SG5700）"

"MTU設定を変更します"

ポートレベルのネットワーク接続の確認

## StorageGRID アプライアンスインストーラとその他のノードの間のアクセスがファイアウォールの妨げにならないように、 StorageGRID アプライアンスインストーラが指定した IP アドレスまたはアドレス範囲にある特定の TCP ポートまたはポートセットに接続できることを確認します。

このタスクについて

StorageGRID アプライアンスインストーラに付属のポートのリストを使用して、アプライアンスとグリッドネットワーク内の他のノードの間の接続をテストできます。

また、外部 NFS サーバや DNS サーバで使用されるポートなど、管理ネットワークとクライアントネットワーク、および UDP ポートで接続をテストすることもできます。これらのポートの一覧については、StorageGRID ネットワークのガイドラインにあるポートリファレンスを参照してください。

ポート接続テーブルに表示されているグリッドネットワークポートは、StorageGRID バージョン11.5.0に対してのみ有効です。各ノードタイプに適したポートを確認するには、使用している StorageGRID のバージョンに対応したネットワークガイドラインを確認する必要があります。

手順

1. StorageGRID アプライアンスインストーラから、 **Configure Networking *>** Port Connectivity Test (nmap)* をクリックします。

   Port Connectivity Test ページが表示されます。

   ポート接続テーブルには、グリッドネットワークでの TCP 接続を必要とするノードタイプが表示されます。各ノードタイプについて、アプライアンスにアクセスできる必要があるグリッドネットワークのポートがテーブルに表示されます。

   The following node types require TCP connectivity on the Grid Network.

| Node Type | Grid Network Ports |
|---|---|
| Admin Node | 22,80,443,1504,1505,1506,1508,7443,9999 |
| Storage Node without ADC | 22,1139,1502,1506,1511,7001,9042,9999,18002,18017,18019,18082,18083,18200 |
| Storage Node with ADC | 22,1139,1501,1502,1506,1511,7001,9042,9999,18000,18001,18002,18003,18017,18019,18082,18083,18200,19000 |
| API Gateway | 22,1506,1507,9999 |
| Archive Node | 22,1506,1509,9999,11139 |

   表に記載されたアプライアンスポートとグリッドネットワーク内のその他のノードの間の接続をテストできます。

2. [* ネットワーク *] ドロップダウンから、テストするネットワークを選択します。 * グリッド * 、 * 管理者 * 、または * クライアント * 。
3. そのネットワーク上のホストの IPv4 アドレスの範囲を指定します。

   たとえば、ネットワーク上のゲートウェイやプライマリ管理ノードをプローブできます。

   次の例に示すように、ハイフンを使用して範囲を指定します。

4. TCP ポート番号、カンマで区切ったポートのリスト、またはポートの範囲を入力します。

The following node types require TCP connectivity on the Grid Network.

| Node Type | Grid Network Ports |
| --- | --- |
| Admin Node | 22,80,443,1504,1505,1506,1508,7443,9999 |
| Storage Node without ADC | 22,1139,1502,1506,1511,7001,9042,9999,18002,18017,18019,18082,18083,18200 |
| Storage Node with ADC | 22,1139,1501,1502,1506,1511,7001,9042,9999,18000,18001,18002,18003,18017,18019,18082,18083,18200,19000 |
| API Gateway | 22,1506,1507,9999 |
| Archive Node | 22,1506,1509,9999,11139 |

**Port Connectivity Test**

Network: Grid

IPv4 Address Ranges: 10.224.6.160-161

Port Ranges: 22,2022

Protocol: TCP UDP

Test Connectivity

5. [ 接続のテスト * ] をクリックします。

   ◦ 選択したポートレベルのネットワーク接続が有効な場合は、「 Port connectivity test passed 」というメッセージが緑色のバナーに表示されます。nmap コマンドの出力は、バナーの下に表示されます。

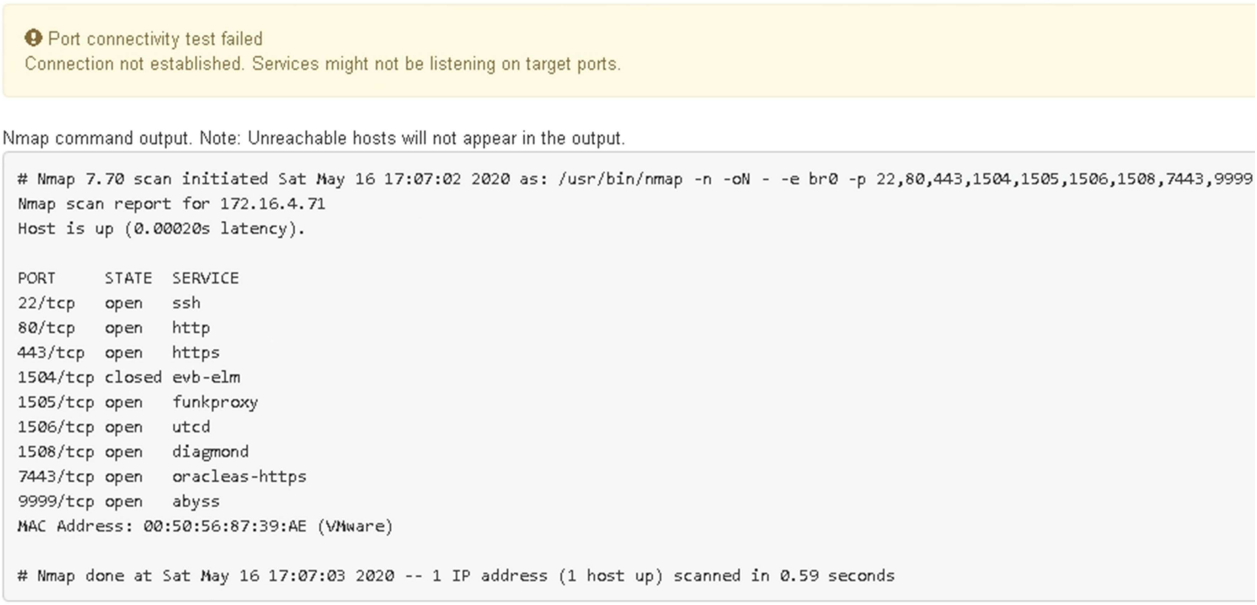
   Port connectivity test passed

   Nmap command output. Note: Unreachable hosts will not appear in the output.

```
# Nmap 7.70 scan initiated Fri Nov 13 18:32:03 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,2022 10.224.6.160-161
Nmap scan report for 10.224.6.160
Host is up (0.00072s latency).

PORT     STATE SERVICE
22/tcp   open  ssh
2022/tcp open  down

Nmap scan report for 10.224.6.161
Host is up (0.00060s latency).

PORT     STATE SERVICE
22/tcp   open  ssh
2022/tcp open  down

# Nmap done at Fri Nov 13 18:32:04 2020 -- 2 IP addresses (2 hosts up) scanned in 0.55 seconds
```

   ◦ ポートレベルのネットワーク接続がリモートホストに確立されても ' ホストが選択したポートの 1 つ以上をリッスンしていない場合は ' ポート接続テストに失敗しましたというメッセージが黄色のバナーに表示されますnmap コマンドの出力は、バナーの下に表示されます。

   ホストがリッスンしていないリモート・ポートの状態はすべて「 closed 」です。 たとえば、接続しようとしているノードがインストール済みの状態で、 StorageGRID NMS サービスがまだ実行されていない場合に、黄色のバナーが表示されることがあります。




- 選択した 1 つ以上のポートに対してポートレベルのネットワーク接続を確立できない場合は、「 Port connectivity test failed 」というメッセージが赤いバナーに表示されます。nmap コマンドの出力は、バナーの下に表示されます。

  赤いバナーは、リモートホストのポートへの TCP 接続試行が行われたが、送信者には何も返されなかったことを示します。応答が返されない場合、ポートの状態は「 filtered 」となり、ファイアウォールによってブロックされている可能性があります。

  「閉」のポートも一覧表示されます。

関連情報

"ネットワークガイドライン"

**SANtricity** システムマネージャにアクセスして設定します

SANtricity System Manager を使用して、ストレージコントローラシェルフのストレージコントローラ、ストレージディスク、その他のハードウェアコンポーネントのステータスを監視できます。E シリーズ AutoSupport のプロキシを設定することもできます。管理ポートを使用せずにアプライアンスから AutoSupport メッセージを送信できます。

『**Setting Up and Accessing SANtricity System Manager**』を参照してください

ストレージコントローラシェルフのハードウェアを監視したり、 E シリーズ AutoSupport を設定したりするために、ストレージコントローラの SANtricity System Manager へのアクセスが必要になる場合があります。

必要なもの

- サポートされているWebブラウザを使用します。
- グリッドマネージャから SANtricity システムマネージャにアクセスするには、 StorageGRID をインストールし、ストレージアプライアンスの管理者権限またはルートアクセス権限が必要です。
- StorageGRID アプライアンスインストーラを使用して SANtricity System Manager にアクセスするには、 SANtricity System Manager 管理者のユーザ名とパスワードが必要です。
- Web ブラウザを使用して SANtricity System Manager に直接アクセスするには、 SANtricity System Manager 管理者のユーザ名とパスワードが必要です。

> グリッドマネージャまたは StorageGRID アプライアンスインストーラを使用して SANtricity System Manager にアクセスするには、 SANtricity ファームウェア 8.70 以降が必要です。StorageGRID アプライアンス・インストーラを使用してファームウェアのバージョンを確認し、 * Help * > * About * を選択します。

> グリッドマネージャまたはアプライアンスインストーラから SANtricity システムマネージャにアクセスする方法は、通常、ハードウェアを監視して E シリーズ AutoSupport を設定することだけを目的としています。ファームウェアのアップグレードなど、 SANtricity System Manager 内の多くの機能や操作は、 StorageGRID アプライアンスの監視には適用されません。問題を回避するには、アプライアンスのハードウェアの設置とメンテナンスの手順に必ず従ってください。

このタスクについて

SANtricity System Manager にアクセスする方法は 3 種類あり、その方法はインストールおよび設定のどの段階にあるかによって異なります。

- アプライアンスが StorageGRID システムにノードとして導入されていない場合は、 StorageGRID アプライアンスインストーラの Advanced タブを使用します。

  > 導入されたノードは、 StorageGRID アプライアンスインストーラを使用して SANtricity システムマネージャにアクセスできなくなります。

- アプライアンスを StorageGRID システムにノードとして導入している場合は、グリッドマネージャのノードページにある SANtricity システムマネージャタブを使用します。
- StorageGRID アプライアンスインストーラまたはグリッドマネージャを使用できない場合は、管理ポート

に接続された Web ブラウザを使用して SANtricity System Manager に直接アクセスできます。

この手順 には、 SANtricity システムマネージャに最初にアクセスする手順が含まれています。SANtricity System Manager をすでにセットアップしている場合は、に進みます ハードウェアアラートを設定します ステップ。

> グリッドマネージャまたは StorageGRID アプライアンスインストーラを使用すると、アプライアンスの管理ポートを設定または接続しなくても SANtricity System Manager にアクセスできます。

SANtricity System Manager を使用して次の項目を監視します。

- ストレージアレイレベルのパフォーマンス、 I/O レイテンシ、 CPU 利用率、スループットなどのパフォーマンスデータ
- ハードウェアコンポーネントのステータス
- 診断データの表示などの機能をサポートします

SANtricity System Manager を使用して、次の設定を行うことができます。

- ストレージコントローラシェルフのコンポーネントの E メールアラート、 SNMP アラート、または syslog アラート
- ストレージコントローラシェルフのコンポーネントの E シリーズ AutoSupport の設定。

  E シリーズ AutoSupport の詳細については、 E シリーズドキュメントセンターを参照してください。

  "NetApp E シリーズシステムのドキュメントのサイト"

- セキュリティ保護されたドライブのロックを解除するために必要なドライブセキュリティキー（ドライブセキュリティ機能が有効になっている場合はロックの解除が必要）
- SANtricity システムマネージャにアクセスするための管理者パスワード

手順

1. 次のいずれかを実行します。

   - StorageGRID アプライアンス・インストーラを使用して、 * アドバンスト * > * SANtricity システム・マネージャ * を選択します
   - Grid Managerを使用して* Nodes >を選択します ***appliance Storage Node*** >* SANtricity システム・マネージャ*

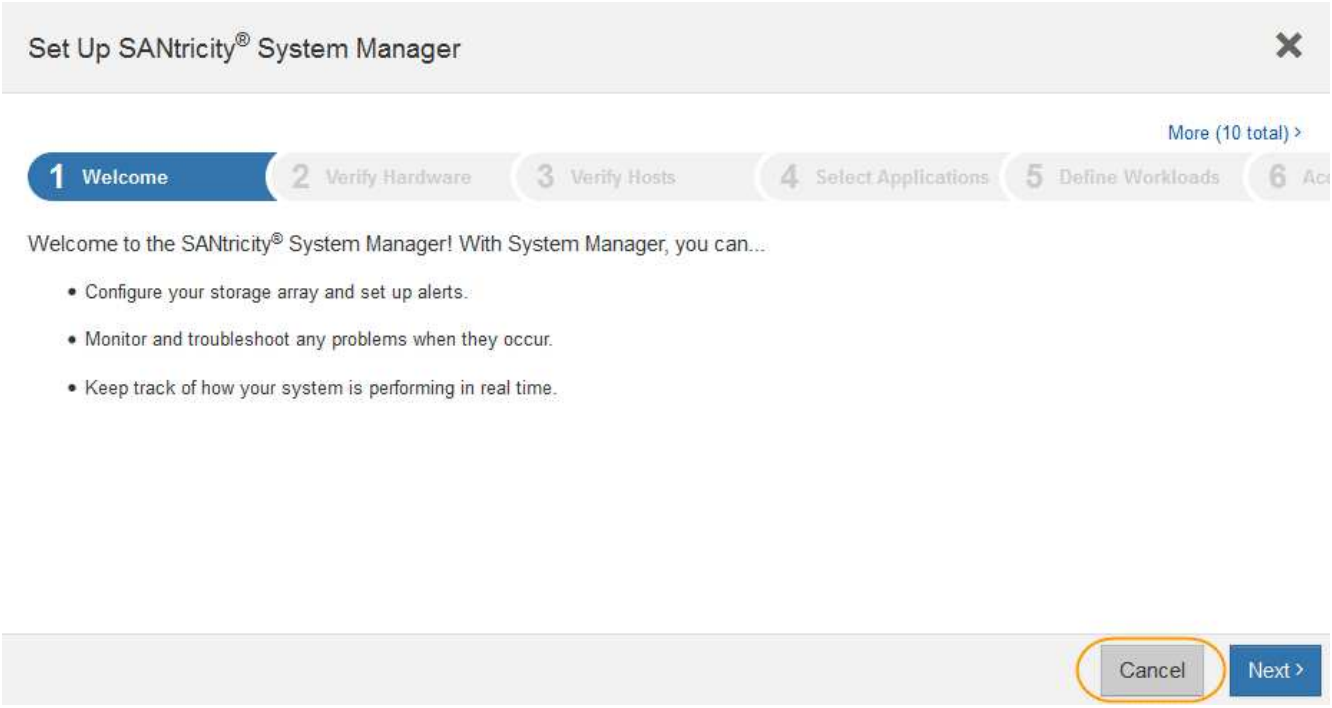
   > これらのオプションを使用できない場合やログインページが表示されない場合は、ストレージコントローラの IP アドレスを使用する必要があります。SANtricity System Managerにアクセスするには、ストレージコントローラのIP：+にアクセスします **https://*Storage_Controller_IP***

   SANtricity System Manager のログインページが表示されます。

2. 管理者パスワードを設定または入力します。

SANtricity System Manager では、すべてのユーザで共有する管理者パスワードを 1 つ使用します。

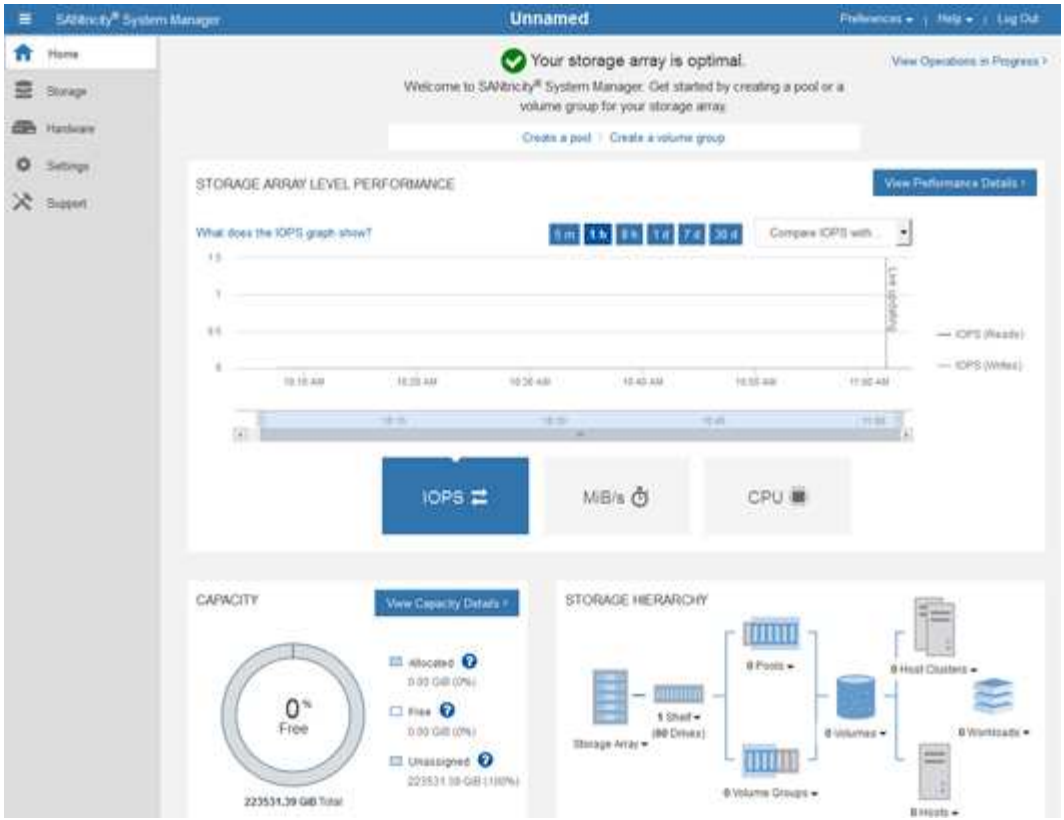
セットアップウィザードが表示されます。




3. 「 * キャンセル * 」を選択してウィザードを閉じます。

StorageGRID アプライアンスにはセットアップ・ウィザードを実行しないでください。

SANtricity の System Manager ホームページが表示されます。




1. ハードウェアアラートを設定します。
   a. SANtricity System Manager のオンラインヘルプにアクセスするには、 * Help * を選択します。
   b. オンラインヘルプの「 * Settings * > * Alerts * 」（ * 設定 * > * アラート * ）セクションを使用して、アラートについて学習します。
   c. How To の指示に従って ' メール・アラート 'SNMP アラート ' または syslog アラートを設定します
2. ストレージコントローラシェルフのコンポーネントの AutoSupport を管理します。
   a. SANtricity System Manager のオンラインヘルプにアクセスするには、 * Help * を選択します。
   b. オンラインヘルプの「* Support > Support Center *」セクションで、AutoSupport 機能について学習します。
   c. 「 How To 」の指示に従って、 AutoSupport を管理します。

      管理ポートを使用せずに E シリーズ AutoSupport メッセージを送信するための StorageGRID プロキシを設定する手順については、 StorageGRID の管理手順および「 E シリーズ AutoSupport のプロキシ設定」を参照してください。

   "StorageGRID の管理"
3. アプライアンスでドライブセキュリティ機能が有効になっている場合は、セキュリティキーを作成して管理します。
   a. SANtricity System Manager のオンラインヘルプにアクセスするには、 * Help * を選択します。
   b. オンラインヘルプの「 * Settings * > * System * > * Security key management * 」セクションでドライブセキュリティについて学習します。
   c. 「 How To 」の指示に従って、セキュリティキーを作成および管理します。

4. 必要に応じて、管理者パスワードを変更します。
   a. SANtricity System Manager のオンラインヘルプにアクセスするには、 * Help * を選択します。
   b. オンラインヘルプの * Home * > * Storage array administration * セクションで、管理者パスワードを確認してください。
   c. 「 How To 」の指示に従って、パスワードを変更します。

**SANtricity** システムマネージャでハードウェアステータスを確認します

## SANtricity System Manager を使用して、ストレージコントローラシェルフの個々のハードウェアコンポーネントを監視および管理したり、コンポーネントの温度やドライブに関連する問題など、ハードウェア診断および環境に関する情報を確認したりできます。

必要なもの

- サポートされているWebブラウザを使用します。
- グリッドマネージャを介して SANtricity システムマネージャにアクセスするには、ストレージアプライアンス管理者の権限またはルートアクセス権限が必要です。
- StorageGRID アプライアンスインストーラを使用して SANtricity System Manager にアクセスするには、 SANtricity System Manager 管理者のユーザ名とパスワードが必要です。
- Web ブラウザを使用して SANtricity System Manager に直接アクセスするには、 SANtricity System Manager 管理者のユーザ名とパスワードが必要です。

> グリッドマネージャまたは StorageGRID アプライアンスインストーラを使用して SANtricity System Manager にアクセスするには、 SANtricity ファームウェア 8.70 以降が必要です。

> グリッドマネージャまたはアプライアンスインストーラから SANtricity システムマネージャにアクセスする方法は、通常、ハードウェアを監視して E シリーズ AutoSupport を設定することだけを目的としています。ファームウェアのアップグレードなど、 SANtricity System Manager 内の多くの機能や操作は、 StorageGRID アプライアンスの監視には適用されません。問題を回避するには、アプライアンスのハードウェアの設置とメンテナンスの手順に必ず従ってください。

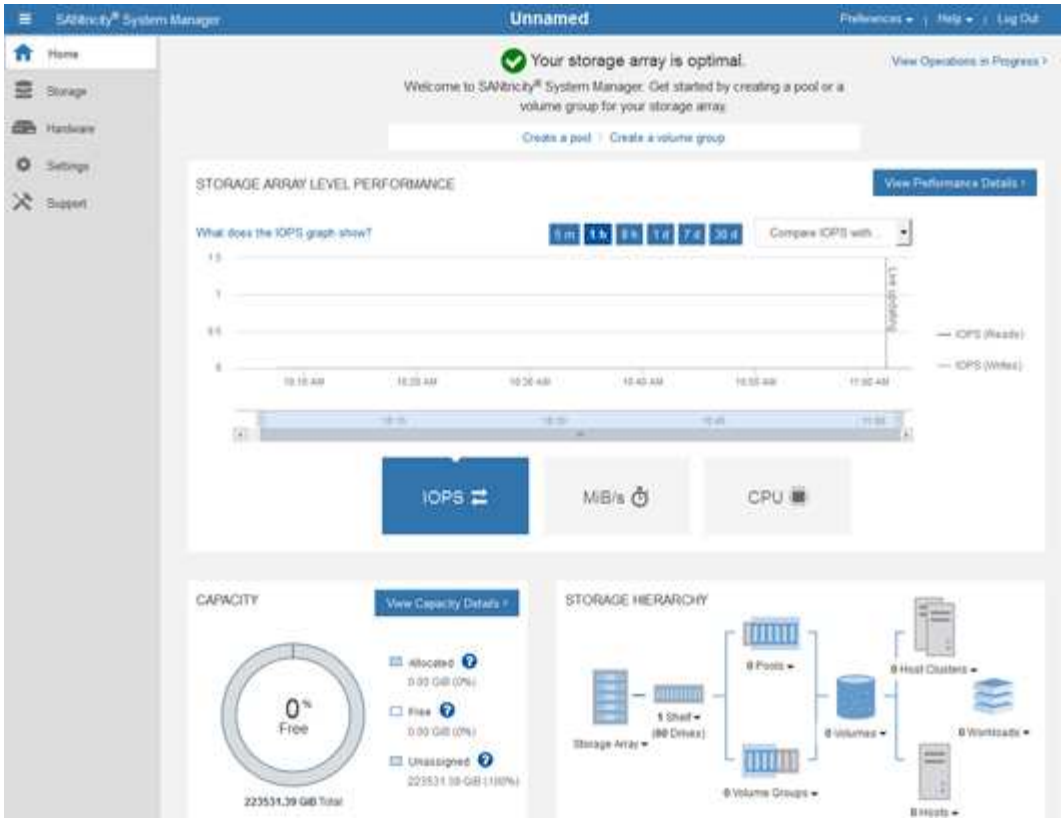
手順

1. SANtricity システムマネージャにアクセスします。

   "『Setting Up and Accessing SANtricity System Manager』を参照してください"

2. 必要に応じて、管理者のユーザ名とパスワードを入力します。
3. セットアップウィザードを閉じて SANtricity システムマネージャのホームページを表示するには、 * Cancel * をクリックします。

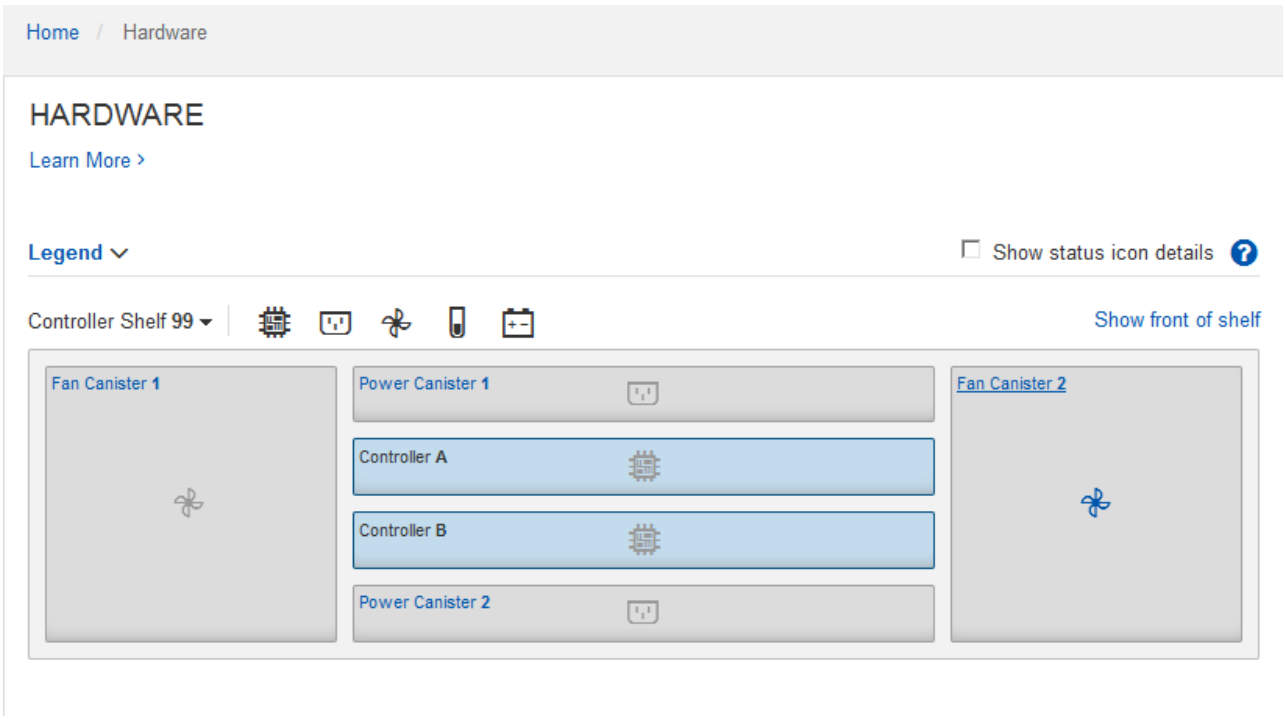
   SANtricity の System Manager ホームページが表示されます。SANtricity System Manager では、コントローラシェルフがストレージアレイと表示されます。




4. アプライアンスハードウェアについて表示された情報を確認し、すべてのハードウェアコンポーネントのステータスが「 Optimal 」であることを確認します。

   a. [* ハードウェア * ] タブをクリックします。

   b. Show back of shelf* （シェルフの背面を表示）をクリックします。




シェルフの背面から、両方のストレージコントローラ、各ストレージコントローラのバッテリ、電源キャ

ニスター 2 台、ファンキャニスター 2 台、および拡張シェルフ（ある場合）を確認できます。構成部品の温度を表示することもできます。

a. 各ストレージコントローラの設定を表示するには、コントローラを選択し、コンテキストメニューから * 設定の表示 * を選択します。

b. シェルフの背面にある他のコンポーネントの設定を確認するには、対象となるコンポーネントを選択します。

c. [Show front of shelf* （シェルフの前面を表示） ] をクリックし、表示するコンポーネントを選択します。

   シェルフの前面からは、ストレージコントローラシェルフまたは拡張シェルフ（ある場合）のドライブとドライブドロワーを確認できます。

ステータスが「 Needs Attention 」になっているコンポーネントがある場合は、 Recovery Guru に示される手順に従って問題 を解決するか、テクニカルサポートに連絡してください。

**StorageGRID** アプライアンスインストーラを使用してストレージコントローラの**IP**アドレスを設定します

各ストレージコントローラの管理ポート 1 を使用して、アプライアンスを SANtricity System Manager の管理ネットワークに接続します。StorageGRID アプライアンスインストーラから SANtricity System Manager にアクセスできない場合は、各ストレージコントローラの静的 IP アドレスを設定して、コントローラシェルフのハードウェアおよびコントローラファームウェアへの管理接続が失われないようにする必要があります。

必要なもの

- StorageGRID 管理ネットワークに接続できる管理クライアントを使用しているか、サービスラップトップを使用している必要があります。
- クライアントまたはサービスラップトップに、サポートされている Web ブラウザをインストールしておきます。

このタスクについて

DHCP によって割り当てられたアドレスは、いつ変更されるかわかりません。一貫したアクセスを確保するために、コントローラには静的 IP アドレスを割り当ててください。

> この手順 は、StorageGRID アプライアンスインストーラ（アドバンスト>* SANtricity システムマネージャ*）またはグリッドマネージャ（ノード>* SANtricity システムマネージャ*）からSANtricity システムマネージャにアクセスできない場合にのみ使用してください。

手順

1. クライアントから、StorageGRID アプライアンスインストーラのURLを入力します：+
   **`https://Appliance_Controller_IP:8443`**

   の場合 `*Appliance_Controller_IP*`には、任意のStorageGRID ネットワーク上のアプライアンスのIPアドレスを使用します。

   StorageGRID アプライアンスインストーラのホームページが表示されます。

2. Configure Hardware * > * Storage Controller Network Configuration * を選択します。

Storage Controller Network Configuration ページが表示されます。

3. ネットワーク構成に応じて、 IPv4 、 IPv6 、またはその両方で * Enabled * を選択します。
4. 自動的に表示される IPv4 アドレスを書き留めます。

   ストレージコントローラの管理ポートに IP アドレスを割り当てるためのデフォルトの方法は、 DHCP です。

   DHCP 値が表示されるまでに数分かかる場合があります。

5. 必要に応じて、ストレージコントローラの管理ポートに静的 IP アドレスを設定します。

   管理ポートに静的 IP を割り当てるか、 DHCP サーバでアドレスの永久リースを割り当てる必要があります。

   a. 「 * Static * 」を選択します。
   b. CIDR 表記を使用して IPv4 アドレスを入力します。
   c. デフォルトゲートウェイを入力します。

   d. [ 保存（ Save ） ] をクリックします。

      変更が適用されるまで数分かかる場合があります。

   SANtricity System Managerに接続するときは、新しい静的IPアドレスをURL：+として使用します `https://Storage_Controller_IP`

オプション：ノード暗号化を有効にする

ノードの暗号化を有効にすると、アプライアンス内のディスクを安全なキー管理サーバ（ KMS ）暗号化によってサイト内での物理的な損失やデータの削除から保護することができます。アプライアンスのインストール時にノード暗号化を選択して有効にする必要があります。また、 KMS 暗号化プロセスが開始されると、ノード暗号化の選択を解

除できません。

必要なもの

StorageGRID の管理手順の KMS に関する情報を確認します。

このタスクについて

ノード暗号化が有効になっているアプライアンスは、 StorageGRID サイト用に設定されている外部キー管理サーバ（ KMS ）に接続します。各 KMS （または KMS クラスタ）は、サイトにあるすべてのアプライアンスノードの暗号化キーを管理します。これらのキーは、ノード暗号化が有効なアプライアンスで、各ディスク上のデータを暗号化および復号化します。

Grid Manager StorageGRID では、アプライアンスのインストール前またはインストール後に KMS を設定できます。詳細については、 StorageGRID の管理手順の KMS とアプライアンスの設定に関する情報を参照してください。

- アプライアンスをインストールする前に KMS を設定すると、 KMS で制御される暗号化が開始されます。この暗号化は、アプライアンスでノード暗号化を有効にし、 KMS が設定されている StorageGRID サイトに追加します。
- アプライアンスをインストールする前に KMS が設定されていない場合は、 KMS が設定され、アプライアンスノードを含むサイトで利用可能になった時点で、ノード暗号化が有効になっている各アプライアンスで KMS 制御された暗号化が実行されます。

ノード暗号化が有効になっているアプライアンスより前に存在するデータは、設定されたKMSに接続する前に、セキュアでない一時キーで暗号化されます。キーが KMS から提供される値に設定されるまで、アプライアンスの取り外しや盗難は防止されません。

ディスクの復号化に KMS キーが必要な場合を除いて、アプライアンス上のデータを取得することはできず、データが実質的に失われます。これは、 KMS から復号化キーを取得できない場合に発生します。顧客が KMS 設定をクリアするか、 KMS キーの有効期限が切れるか、 KMS への接続が失われるか、 KMS キーがインストールされている StorageGRID システムからアプライアンスが削除されると、キーにアクセスできなくなります。

手順

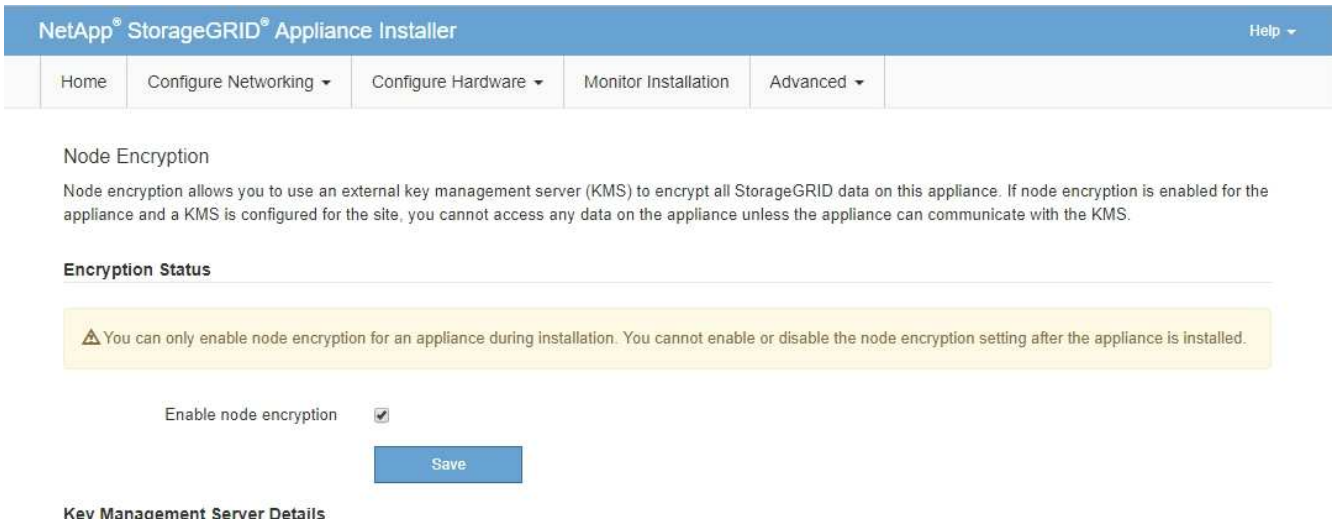
1. ブラウザを開き、アプライアンスのコンピューティングコントローラの IP アドレスのいずれかを入力します。[+]
**`https://Controller_IP:8443`**

   *`Controller_IP`* は、3つのStorageGRID ネットワークのいずれかでのコンピューティングコントローラ（ストレージコントローラではない）のIPアドレスです。

   StorageGRID アプライアンスインストーラのホームページが表示されます。

   アプライアンスを KMS キーで暗号化すると、アプライアンスディスクを復号化する際に同じ KMS キーを使用する必要がなくなります。

2. Configure Hardware * > * Node Encryption * を選択します。




3. [ ノード暗号化を有効にする *] を選択します。

   保存を選択し、アプライアンスノードがStorageGRID システム内のKMS暗号化キーにアクセスしてディスク暗号化を開始するまでは、「ノード暗号化を有効にする」を選択解除してデータ損失のリスクを回避できます。アプライアンスのインストール後、ノード暗号化を無効にすることはできません。

   KMS を含む StorageGRID サイトにノード暗号化が有効になっているアプライアンスを追加すると、そのノードで KMS 暗号化を使用するのを停止することはできません。

4. [ 保存（ Save ） ] を選択します。
5. アプライアンスを StorageGRID システムのノードとして導入します。

   KMS で制御される暗号化は、アプライアンスが StorageGRID サイト用に設定されている KMS キーにアクセスすると開始されます。KMS 暗号化プロセス中にインストーラによって進捗状況のメッセージが表示されます。この処理には、アプライアンス内のディスクボリュームの数によっては数分かかることがあります。

   アプライアンスは、最初に各ディスクボリュームにランダムな KMS 以外の暗号化キーを割り当てて構成します。ディスクはこの一時的な暗号化キーを使用して暗号化されます。このキーは、ノード暗号化が有効になっているアプライアンスが StorageGRID サイト用に設定されている KMS キーにアクセスするまではセキュリティ保護されません。

完了後

アプライアンスノードがメンテナンスモードのときに使用されているノード暗号化ステータス、 KMS の詳細、および証明書を確認できます。

関連情報

"StorageGRID の管理"

"メンテナンスモードでのノード暗号化の監視"

オプション：**RAID**モードの変更（**SG5760**のみ）

60 本のドライブを搭載した SG5760 では、ストレージとリカバリの要件に対応するため

に、別の RAID モードに変更できます。モードを変更できるのは、 StorageGRID アプライアンスストレージノードを導入する前だけです。

必要なもの

- SG5760 を使用します。SG5712 がある場合は、 DDP モードを使用する必要があります。
- StorageGRID に接続できるクライアントを使用している必要があります。
- クライアントにサポートされているWebブラウザをインストールしておきます。

このタスクについて

SG5760 アプライアンスをストレージノードとして導入する前に、次のいずれかのボリューム構成オプションを選択できます。

- * DDP * ：データドライブ 8 本につきパリティドライブを 2 本使用します。すべてのアプライアンスに推奨されるデフォルトのモードです。RAID6 よりもシステムパフォーマンスに優れ、ドライブ障害が発生したあとのリビルド時間も短く、管理も簡単です。また、 60 ドライブアプライアンスをドロワー損失から保護します。
- * DDP16 * ：このモードはデータドライブ 16 本につきパリティドライブを 2 本使用するため、 DDP よりもストレージ効率が高くなります。RAID6 よりもシステムパフォーマンスに優れ、ドライブ障害が発生したあとのリビルド時間も短く、管理も簡単です。ストレージ効率は RAID6 と同等です。DDP16 モードを使用するには、構成にドライブが 20 本以上含まれている必要があります。ドロワー損失からの保護は提供しません。
- *RAID6 *: このモードは 16 台以上のデータドライブごとに 2 本のパリティドライブを使用します。RAID 6 モードを使用するには、構成にドライブが 20 本以上含まれている必要があります。DDP よりもアプライアンスのストレージ効率を上げることができますが、ほとんどの StorageGRID 環境では推奨されません。

> ボリュームがすでに構成されている場合や StorageGRID が事前にインストールされている場合に RAID モードを変更すると、ボリュームが削除されて置き換えられます。対象となったボリュームのデータはすべて失われます。

手順

1. サービスラップトップでWebブラウザを開き、StorageGRID アプライアンスインストーラの+にアクセスします
   **`https://E5700SG_Controller_IP:8443`**

   ここで *`E5700SG_Controller_IP`* E5700SGコントローラのいずれかのIPアドレスです。

2. 「 * アドバンスト * 」 > 「 * RAID モード * 」の順に選択します。
3. [Configure RAID Mode*] ページで、 [Mode] ドロップダウンリストから目的の RAID モードを選択します。
4. [ 保存（ Save ） ] をクリックします。

関連情報

"NetApp E シリーズシステムのドキュメントのサイト"

# アプライアンスストレージノードの内部ポートを別の外部ポートに再マッピングすることが必要になる場合があります。たとえば、ファイアウォールの問題 が原因でポートの再マッピングが必要になることがあります。

必要なもの

- 以前に StorageGRID アプライアンスインストーラにアクセスしていた場合。
- ロードバランサエンドポイントを設定しておらず、設定する予定もない状態である必要があります。

> ポートを再マッピングする場合、同じポートを使用してロードバランサエンドポイントを設定することはできません。ポートを再マッピング済みの場合にロードバランサエンドポイントを設定するには、リカバリとメンテナンスの手順に従ってポートの再マッピングを削除してください。

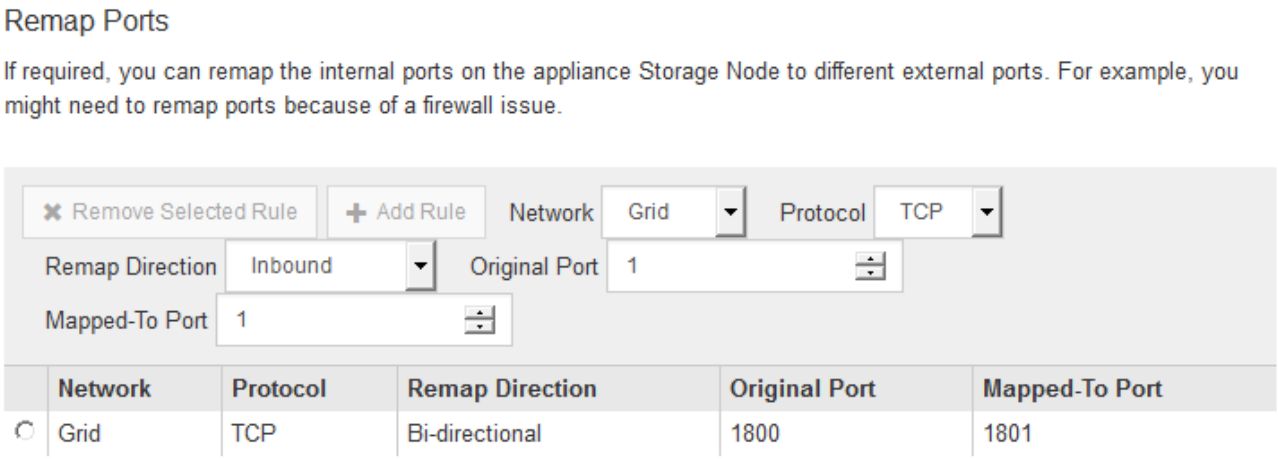
手順

1. StorageGRID アプライアンスインストーラのメニューバーから、 **Configure Networking *>*Remap Port** をクリックします。

   Remap Port ページが表示されます。

2. Network * ドロップダウンボックスから、再マッピングするポートのネットワーク（ Grid 、 Admin 、または Client ）を選択します。
3. [**Protocol**] ドロップダウンボックスから、 IP プロトコルとして [TCP] または [UDP] を選択します。
4. [* Remap Direction] * ドロップダウンボックスから、このポートに再マッピングするトラフィック方向（インバウンド、アウトバウンド、または双方向）を選択します。
5. 「 * Original Port * 」に、再マッピングするポートの番号を入力します。
6. 「 * mapped-to Port * 」には、代わりに使用するポートの番号を入力します。
7. [ * ルールの追加 * ] をクリックします。

   新しいポートマッピングがテーブルに追加され、新しいマッピングがただちに有効になります。



8. ポートマッピングを削除するには、削除するルールのオプションボタンを選択し、 * 選択したルールの削除 * をクリックします。

## アプライアンスストレージノードの導入

ストレージアプライアンスを設置して設定したら、 StorageGRID システムにストレージノードとして導入できます。アプライアンスをストレージノードとして導入する場合は、アプライアンスに搭載されている StorageGRID アプライアンスインストーラを使用します。

必要なもの

- アプライアンスノードのクローンを作成する場合は、リカバリとメンテナンスの手順を続行します。

  ""

- アプライアンスをラックまたはキャビネットに設置し、ネットワークに接続し、電源を投入しておきます。
- StorageGRID アプライアンスインストーラを使用して、アプライアンスのネットワークリンク、 IP アドレス、ポートの再マッピング（必要な場合）を設定しておきます。
- アプライアンスのコンピューティングコントローラに割り当てられている IP アドレスのいずれかを確認しておきます。接続されているどの StorageGRID ネットワークの IP アドレスでも使用できます。
- StorageGRID システムのプライマリ管理ノードを導入しておきます。
- StorageGRID アプライアンスインストーラの IP 設定ページに表示されるすべてのグリッドネットワークサブネットが、プライマリ管理ノードのグリッドネットワークサブネットリストで定義されている。
- サポートされている Web ブラウザがインストールされたサービスラップトップを用意しておきます。

このタスクについて

各ストレージアプライアンスは単一のストレージノードとして機能します。すべてのアプライアンスは、グリッドネットワーク、管理ネットワーク、およびクライアントネットワークに接続できます

StorageGRID システムにアプライアンスストレージノードを導入するには、 StorageGRID アプライアンスインストーラにアクセスして次の手順を実行します。

- プライマリ管理ノードの IP アドレスおよびストレージノードの名前を指定または確認します。
- 導入を開始し、ボリュームの設定とソフトウェアのインストールが完了するまで待機します。
- アプライアンスインストールタスクの途中でインストールが一時停止した場合は、 Grid Manager にサインインしてすべてのグリッドノードを承認し、 StorageGRID のインストールプロセスと導入プロセスを完了すると、インストールを再開できます。

> 一度に複数のアプライアンスノードを導入する必要がある場合は、を使用してインストールプロセスを自動化できます `configure-sga.py` アプライアンスインストールスクリプト。

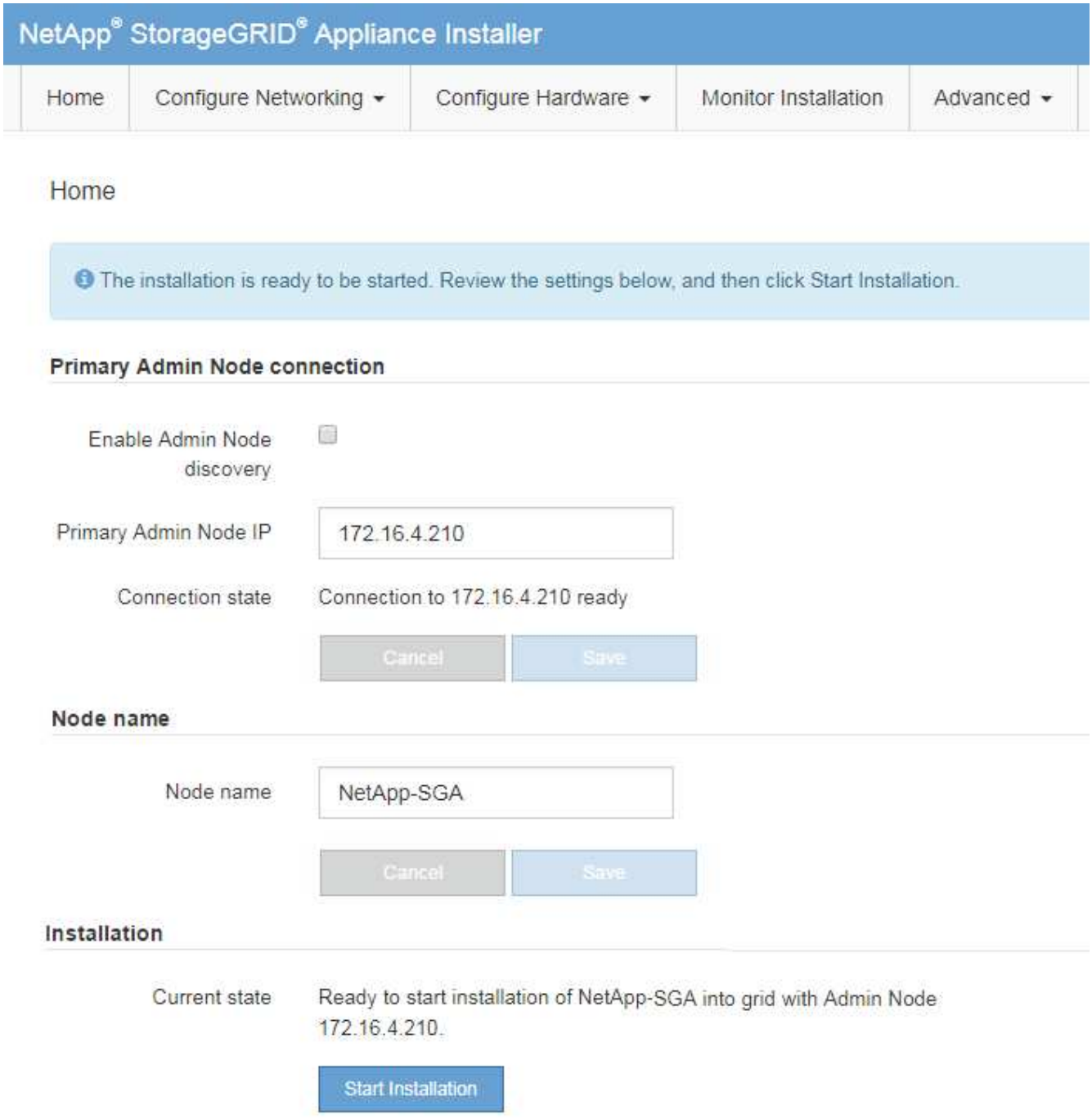
- 拡張またはリカバリ処理を実行する場合は、該当する手順に従います。
  - 既存の StorageGRID システムにアプライアンスストレージノードを追加する場合は、 StorageGRID システムの拡張手順を参照してください。
  - リカバリ処理の一環としてアプライアンスストレージノードを導入する場合は、リカバリとメンテナ

ンスの手順を参照してください。

手順

1. ブラウザを開き、アプライアンスのコンピューティングコントローラの IP アドレスのいずれかを入力します。[+]
**`https://Controller_IP:8443`**

   StorageGRID アプライアンスインストーラのホームページが表示されます。




2. 「 * プライマリ管理ノード接続 * 」セクションで、プライマリ管理ノードの IP アドレスを指定する必要があるかどうかを判断します。

   このデータセンターに他のノードがすでにインストールされている場合は、プライマリ管理ノードまたは

ADMIN_IP が設定された少なくとも 1 つのグリッドノードが同じサブネットにあるという想定で、StorageGRID アプライアンスインストーラがこの IP アドレスを自動的に検出します。

3. この IP アドレスが表示されない場合や変更する必要がある場合は、アドレスを指定します。

| オプション | 説明 |
| --- | --- |
| IP を手動で入力します | a. Enable Admin Node discovery * チェックボックスの選択を解除します。<br>b. IP アドレスを手動で入力します。<br>c. [ 保存（ Save ） ] をクリックします。<br>d. 新しい IP アドレスの接続状態が READY になるまで待ちます。 |
| 接続されたすべてのプライマリ管理ノードの自動検出 | a. Enable Admin Node discovery * チェックボックスを選択します。<br>b. 検出された IP アドレスのリストが表示されるまで待ちます。<br>c. このアプライアンスストレージノードを導入するグリッドのプライマリ管理ノードを選択します。<br>d. [ 保存（ Save ） ] をクリックします。<br>e. 新しい IP アドレスの接続状態が READY になるまで待ちます。 |

4. [* Node name* （ノード名 * ） ] フィールドに、このアプライアンスノードに使用する名前を入力し、 [ * Save * （保存） ] をクリックします。

   このノード名は、 StorageGRID システムでこのアプライアンスノードに割り当てられ、このタブは、Grid Manager のノードページ（概要タブ）に表示されます。ノードを承認するときに、必要に応じて、この名前を変更できます。

5. [インストール]セクションで、現在の状態が「のインストール開始準備完了」であることを確認します *node name* をプライマリ管理ノードでグリッドに追加します *admin_ip* "*インストールの開始*ボタンが有効になっていることを確認します。

   [Start Installation* （インストールの開始） ] ボタンが有効になっていない場合は、ネットワーク設定またはポート設定の変更が必要になることがあります。手順については、使用しているアプライアンスのインストールとメンテナンスの手順を参照してください。

   ストレージノードアプライアンスをノードクローニングターゲットとして導入する場合は、ここで導入プロセスを停止して、のノードクローニング手順 を続行してください ""。

6. StorageGRID アプライアンスインストーラのホームページで、 * インストールの開始 * をクリックします。

   現在の状態が「 Installation is in progress 」に変わり、「 Monitor Installation 」ページが表示されます。

   モニタのインストールページに手動でアクセスする必要がある場合は、 * モニタのインストール * をクリックします。

7. グリッドに複数のアプライアンスストレージノードがある場合は、アプライアンスごとに上記の手順を繰り返します。

一度に複数のアプライアンスストレージノードを導入する必要がある場合は、を使用してインストールプロセスを自動化できます `configure-sga.py` アプライアンスインストールスクリプト。このスクリプトはストレージノードにのみ適用されます。

関連情報

"グリッドを展開します"

""

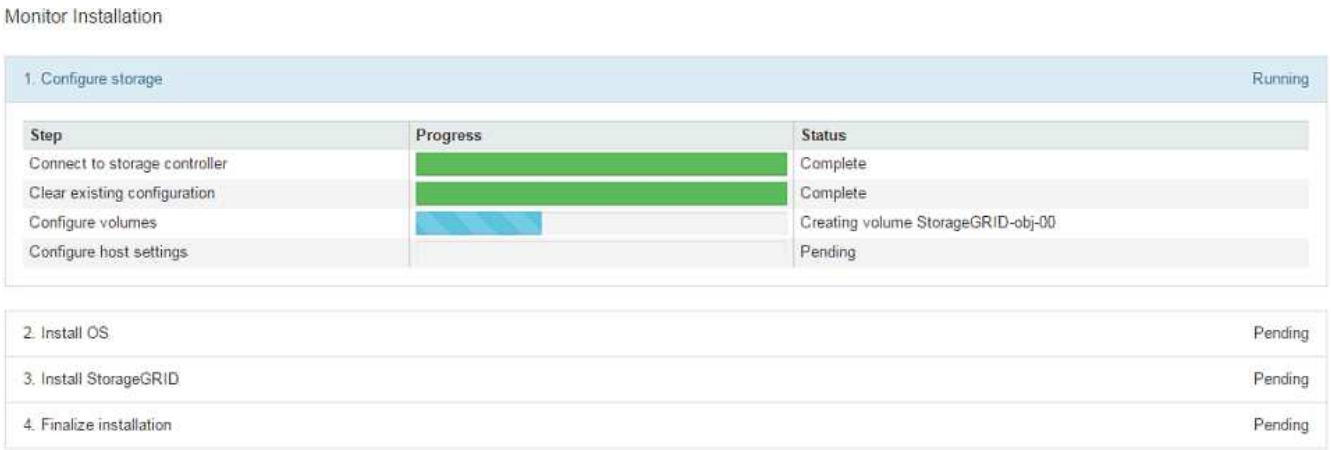
## ストレージアプライアンスのインストールの監視

StorageGRID アプライアンスインストーラでは、インストールが完了するまでステータスが提供されます。ソフトウェアのインストールが完了すると、アプライアンスがリブートされます。

手順

1. インストールの進行状況を監視するには、 * インストールの監視 * をクリックします。

   Monitor Installation ページにインストールの進行状況が表示されます。




   青色のステータスバーは、現在進行中のタスクを示します。緑のステータスバーは、正常に完了したタスクを示します。

   インストーラは、以前のインストールで完了したタスクが再実行されないようにします。インストールを再実行している場合 ' 再実行する必要のないタスクは ' 緑色のステータスバーとステータスが [ スキップ済み ] と表示されます

2. インストールの最初の 2 つのステージの進行状況を確認します。

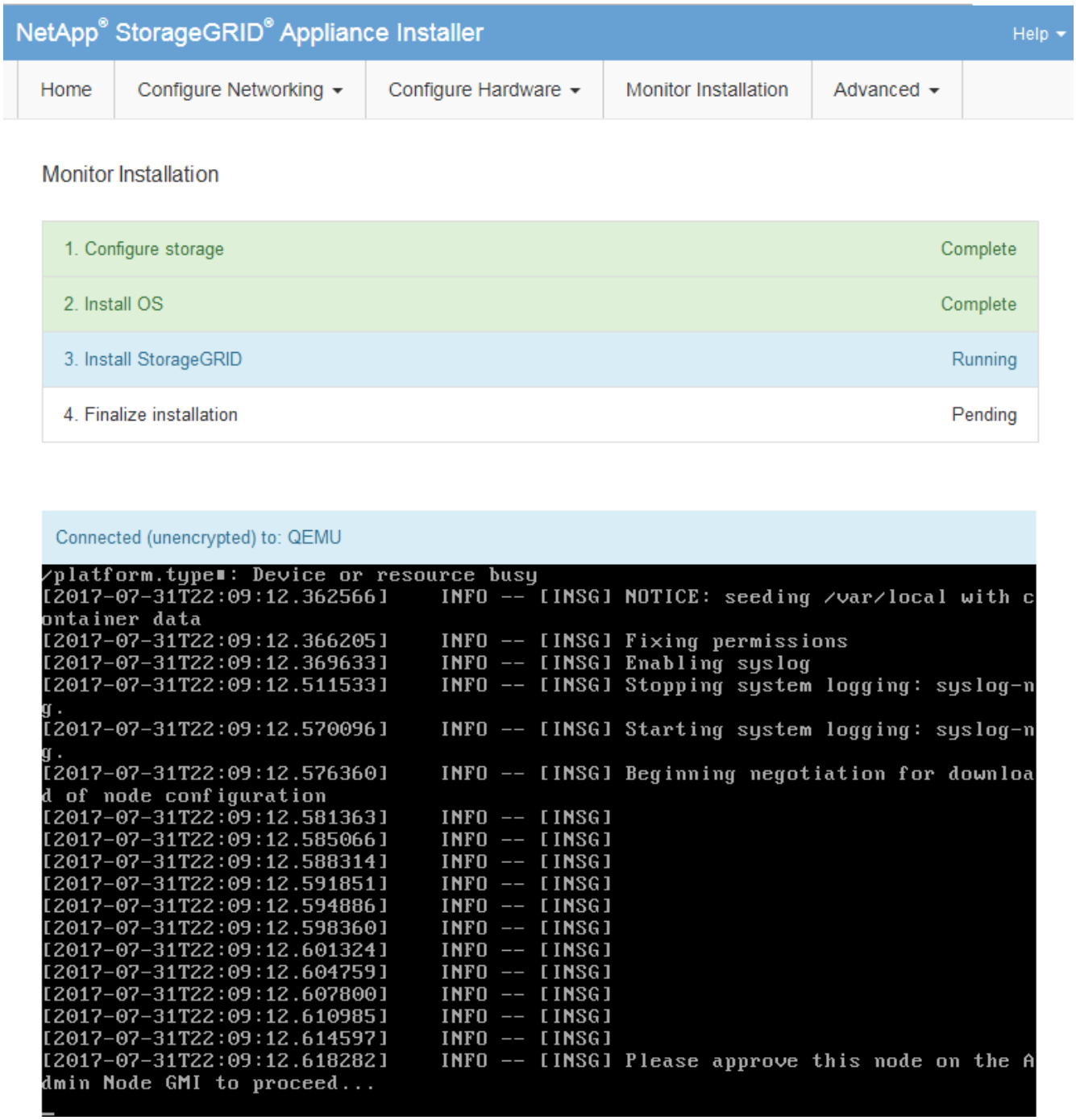
   ◦ 1 。ストレージの構成 *

   インストーラがストレージコントローラに接続し、既存の設定があれば消去し、 SANtricity ソフトウェアと通信してボリュームを設定し、ホストを設定します。

   ※ 2OS * をインストールします

インストーラが StorageGRID のベースとなるオペレーティングシステムイメージをアプライアンスにコピーします。

3. インストールの進行状況の監視を継続して、組み込みコンソールに「 Install StorageGRID * 」ステージが一時停止し、グリッドマネージャを使用して管理ノードでこのノードを承認するように求めるメッセージが表示されるまで続けます。次の手順に進みます。




4. グリッドマネージャに移動し、保留中のストレージノードを承認して、StorageGRID のインストールプロセスを完了します。

Grid Manager から * Install * をクリックすると、ステージ 3 が完了し、ステージ 4 * Finalize Installation * が開始されます。ステージ 4 が完了すると、コントローラがリブートされます。

# アプライアンスのインストールと設定の自動化

## アプライアンスのインストールと設定、および StorageGRID システム全体の設定を自動化することができます。

このタスクについて

インストールと設定を自動化すると、複数の StorageGRID インスタンス、または大規模で複雑な StorageGRID インスタンスを 1 つ導入する場合に便利です。

インストールと設定を自動化するには、次のオプションを 1 つ以上使用します。

- アプライアンスの構成設定を指定した JSON ファイルを作成します。StorageGRID アプライアンスインストーラを使用して JSON ファイルをアップロードします。

  同じファイルを使用して、複数のアプライアンスを設定できます。

- StorageGRID を使用します`configure-sga.py` アプライアンスの設定を自動化するPythonスクリプト。
- 追加の Python スクリプトを使用して、 StorageGRID システム全体の他のコンポーネント（「グリッド」）を設定します。

Python スクリプトを StorageGRID 自動化で直接使用することも、 StorageGRID インストール REST API を独自に開発するグリッド導入および設定ツールで使用する例として使用することもできます。リカバリとメンテナンスの手順のStorageGRID インストールファイルのダウンロードと展開に関する情報を参照してください。

**StorageGRID** アプライアンスインストーラを使用したアプライアンス設定の自動化

## 設定情報を含む JSON ファイルを使用して、アプライアンスの設定を自動化することができます。ファイルは StorageGRID アプライアンスインストーラを使用してアップロードします。

必要なもの

- アプライアンスは、 StorageGRID 11.5 以降と互換性のある最新のファームウェアを使用している必要があります。
- 設定するアプライアンスのStorageGRID アプライアンスインストーラに、サポートされているブラウザを使用して接続する必要があります。

このタスクについて

次の設定など、アプライアンスの設定作業を自動化することができます。

- グリッドネットワーク、管理ネットワーク、およびクライアントネットワークの IP アドレス
- BMC インターフェイス
- ネットワークリンク
  - ポートボンディングモード
  - ネットワークボンディングモード

- リンク速度

アップロードした JSON ファイルを使用してアプライアンスを設定する方が、 StorageGRID アプライアンスインストーラの複数のページを使用して手動で設定を行うよりも効率的です。特に、多数のノードを設定する必要がある場合は効果的です。構成ファイルはノードごとに 1 つずつ適用する必要があります。

> アプライアンスのインストールと設定の両方を自動化したいと考えている経験豊富なユーザが、を使用できます `configure-sga.py` スクリプト：[+]"configure-sga.pyスクリプトを使用して、アプライアンスノードのインストールと設定を自動化する"

手順

1. 次のいずれかの方法で JSON ファイルを生成します。
   - ConfigBuilder アプリケーション

     "ConfigBuilder.netapp.com"

   - 。 `configure-sga.py` アプライアンス設定スクリプト。スクリプトは、 StorageGRID アプライアンスインストーラ（ * Help * > * アプライアンス構成スクリプト * ）からダウンロードできます。configure-sga.py スクリプトを使用して設定を自動化する手順を参照してください。

     "configure-sga.pyスクリプトを使用して、アプライアンスノードのインストールと設定を自動化する"

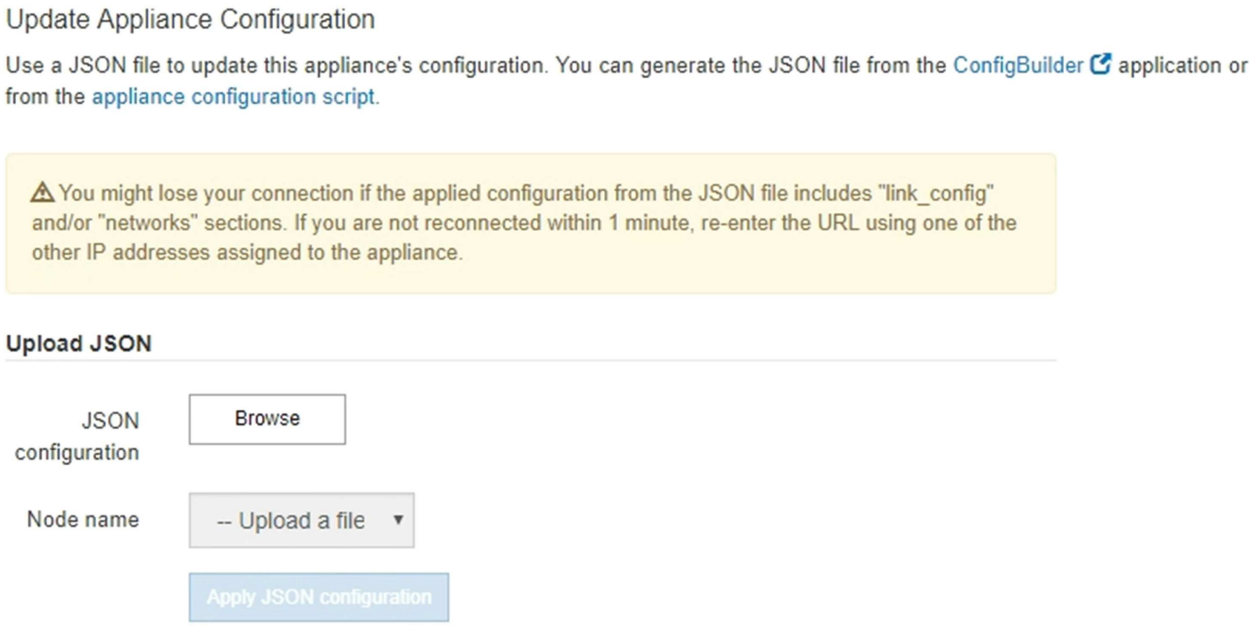
     JSON ファイル内のノード名は、次の要件に従う必要があります。

     - 1 文字以上 32 文字以下の有効なホスト名を指定する必要があります
     - アルファベット、数字、およびハイフンを使用できます
     - 1文字目または最後の文字をハイフンにすることはできません。また、数字だけを使用すること

       > JSON ファイル内のノード名（最上位の名前）が一意であることを確認してください。一意でないと、 JSON ファイルを使用して複数のノードを設定できません。

2. 「 * Advanced * > * Update Appliance Configuration * 」を選択します。

   [Update Appliance Configuration] ページが表示されます。




3. アップロードする設定の JSON ファイルを選択します。

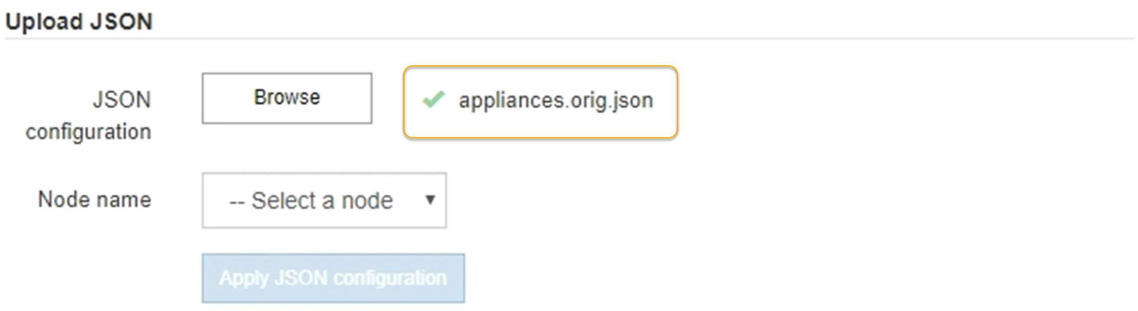
   a. [ * 参照 * ] を選択します。

   b. ファイルを探して選択します。

   c. 「 * 開く * 」を選択します。

   ファイルがアップロードされて検証されます。検証プロセスが完了すると、ファイル名が緑色のチェックマークの横に表示されます。

   > JSON ファイルの構成に「 link_config 」、「 networks 」、またはその両方のセクションが含まれている場合は、アプライアンスへの接続が失われる可能性があります。1 分以内に再接続されない場合は、アプライアンスに割り当てられている他の IP アドレスのいずれかを使用して、アプライアンスの URL を再入力します。

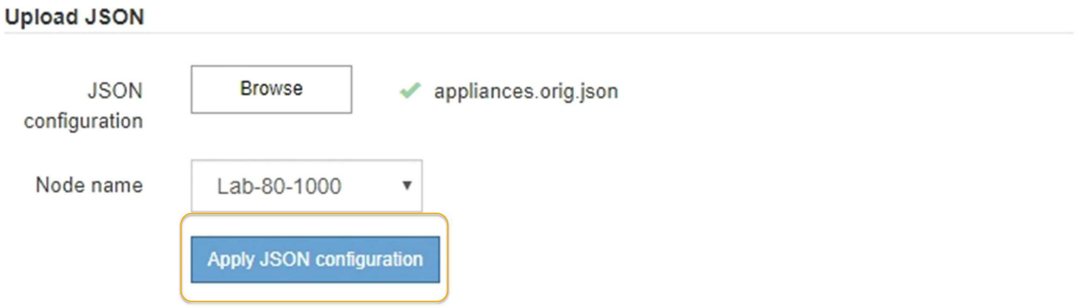



   ノード名 * ドロップダウンには、 JSON ファイルで定義された最上位のノード名が表示されます。

ファイルが有効でない場合、ファイル名は赤色で表示され、黄色のバナーにエラーメッセージが表示されます。無効なファイルはアプライアンスに適用されません。ConfigBuilder を使用して、有効な JSON ファイルを作成できます。

4. ノード名 * ドロップダウンのリストからノードを選択します。

   Apply JSON configuration * ボタンが有効になっている。




5. Apply JSON configuration * を選択します。

   選択したノードに構成が適用されます。

**configure-sga.py**スクリプトを使用して、アプライアンスノードのインストールと設定を自動化する

を使用できます `configure-sga.py` プライマリ管理ノードのインストールや設定など、StorageGRID アプライアンスノードのインストールタスクや設定タスクの多くを自動化するスクリプトです。このスクリプトは、設定するアプライアンスが多数ある場合に役立ちます。スクリプトを使用して、アプライアンスの設定情報を含む JSON ファイルを生成することもできます。

このタスクについて

- アプライアンスをラックに設置し、ネットワークに接続し、電源を投入しておきます。
- StorageGRID アプライアンスインストーラを使用してプライマリ管理ノードのネットワークリンクと IP アドレスを設定しておきます。
- プライマリ管理ノードをインストールする場合は、その IP アドレスを確認しておきます。
- 他のノードをインストールして設定する場合は、プライマリ管理ノードが導入され、その IP アドレスを確認しておきます。
- プライマリ管理ノード以外のすべてのノードについて、 StorageGRID アプライアンスインストーラの IP 設定ページに表示されるすべてのグリッドネットワークサブネットが、プライマリ管理ノードのグリッドネットワークサブネットリストで定義されている。
- をダウンロードしておきます `configure-sga.py` ファイル。このファイルはインストール・アーカイブに含まれています。または、 StorageGRID アプライアンス・インストーラの * Help * > * Appliance Installation Script * をクリックしてアクセスできます。

この手順 は、コマンドラインインターフェイスを使用した経験のある上級ユーザを対象としています。また、 StorageGRID アプライアンスインストーラを使用して設定を自動化することもできます。[+]"StorageGRID アプライアンスインストーラを使用したアプライアンス設定の自動化"

手順

1. Python スクリプトを実行するために使用する Linux マシンにログインします。
2. スクリプト構文に関する一般的なヘルプおよび使用可能なパラメータの一覧を表示するには、次のように入力します。

```
configure-sga.py --help
```

   。 `configure-sga.py` スクリプトでは、次の5つのサブコマンド

   - `advanced` BMCの設定、アプライアンスの現在の設定を含むJSONファイルの作成など、StorageGRID アプライアンスの高度な操作用
   - `configure` RAIDモード、ノード名、およびネットワークパラメータを設定するために使用します
   - `install` StorageGRID のインストールを開始する場合に使用します
   - `monitor` StorageGRID インストールの監視用です
   - `reboot` アプライアンスのリブート用です

   サブコマンド（advanced、configure、install、monitor、またはreboot）引数のあとにを入力すると `--help` オプションを指定すると、そのサブコマンド内で使用可能なオプションの詳細を示すヘルプテキストが表示されます
   `configure-sga.py` *`subcommand`* `--help`

3. アプライアンスノードの現在の設定を確認するには、以下のコマンドをどこに入力するかを確認します *`SGA-install-ip`* には、アプライアンスノードのいずれかのIPアドレスを指定します。+
   `configure-sga.py configure` *`SGA-INSTALL-IP`*

   この結果には、プライマリ管理ノードの IP アドレスや管理、グリッド、クライアントネットワークに関する情報など、アプライアンスの現在の IP 情報が表示されます。

```
Connecting to +https://10.224.2.30:8443+ (Checking version and
connectivity.)
2021/02/25 16:25:11: Performing GET on /api/versions... Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/system-info... Received
200
2021/02/25 16:25:11: Performing GET on /api/v2/admin-connection...
Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/link-config... Received
200
2021/02/25 16:25:11: Performing GET on /api/v2/networks... Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/system-config... Received
200
```

```
StorageGRID Appliance
  Name:        LAB-SGA-2-30
  Node type:   storage

StorageGRID primary Admin Node
  IP:        172.16.1.170
  State:     unknown
  Message:   Initializing...
  Version:   Unknown

Network Link Configuration
  Link Status
        Link      State      Speed (Gbps)
        ----      -----      -----
        1         Up         10
        2         Up         10
        3         Up         10
        4         Up         10
        5         Up         1
        6         Down       N/A

  Link Settings
      Port bond mode:      FIXED
      Link speed:          10GBE

      Grid Network:        ENABLED
          Bonding mode:    active-backup
          VLAN:            novlan
          MAC Addresses:   00:a0:98:59:8e:8a  00:a0:98:59:8e:82

      Admin Network:       ENABLED
          Bonding mode:    no-bond
          MAC Addresses:   00:80:e5:29:70:f4

      Client Network:      ENABLED
          Bonding mode:    active-backup
          VLAN:            novlan
          MAC Addresses:   00:a0:98:59:8e:89  00:a0:98:59:8e:81

Grid Network
  CIDR:      172.16.2.30/21 (Static)
  MAC:       00:A0:98:59:8E:8A
  Gateway:   172.16.0.1
  Subnets:   172.17.0.0/21
             172.18.0.0/21
```

```
                192.168.0.0/21
    MTU:        1500

  Admin Network
    CIDR:       10.224.2.30/21 (Static)
    MAC:        00:80:E5:29:70:F4
    Gateway:    10.224.0.1
    Subnets:    10.0.0.0/8
                172.19.0.0/16
                172.21.0.0/16
    MTU:        1500

  Client Network
    CIDR:       47.47.2.30/21 (Static)
    MAC:        00:A0:98:59:8E:89
    Gateway:    47.47.0.1
    MTU:        2000

######################################################################
#####   If you are satisfied with this configuration,    #####
##### execute the script with the "install" sub-command. #####
######################################################################
```

4. 現在の設定のいずれかの値を変更する必要がある場合は、を使用します `configure` サブコマンドを使用して更新します。たとえば、アプライアンスがプライマリ管理ノードへの接続に使用するIPアドレスをに変更する場合などです `172.16.2.99`をクリックし、「+」と入力します
`configure-sga.py configure --admin-ip 172.16.2.99 SGA-INSTALL-IP`
5. アプライアンスの設定をJSONファイルにバックアップする場合は、を使用します `advanced` および `backup-file` サブコマンド。たとえば、IPアドレスを持つアプライアンスの設定をバックアップする場合などです *SGA-INSTALL-IP* を指定します `appliance-SG1000.json`をクリックし、「+」と入力します
`configure-sga.py advanced --backup-file appliance-SG1000.json SGA-INSTALL-IP`

   設定情報が格納された JSON ファイルは、スクリプトの実行元と同じディレクトリに書き込まれます。

   > 生成された JSON ファイルの最上位のノード名がアプライアンス名と一致していることを確認します。経験豊富なユーザで StorageGRID API について十分な知識がある場合を除き、このファイルに変更を加えないでください。

6. アプライアンスの設定に問題がなければ、を使用します `install` および `monitor` アプライアンスをインストールするためのサブコマンド：+
`configure-sga.py install --monitor SGA-INSTALL-IP`
7. アプライアンスをリブートする場合は、「+」を入力します
`configure-sga.py reboot SGA-INSTALL-IP`

# グリッドノードを導入したら、 StorageGRID システムの設定を自動化できます。

必要なもの

- インストールアーカイブにある次のファイルの場所を確認しておきます。

| ファイル名 | 説明 |
| --- | --- |
| `configure-storagegrid.py` | 設定を自動化するための Python スクリプト |
| `configure-storagegrid.sample.json` | スクリプトで使用するサンプル構成ファイル |
| `configure-storagegrid.blank.json` | スクリプトで使用する空の構成ファイルです |

- を作成しておきます `configure-storagegrid.json` 構成ファイルこのファイルを作成するには、サンプル構成ファイルを変更します (`configure-storagegrid.sample.json`)または空の構成ファイル (`configure-storagegrid.blank.json`) 。

このタスクについて

を使用できます `configure-storagegrid.py` Pythonスクリプトおよび `configure-storagegrid.json` StorageGRID システムの設定を自動化するための構成ファイル。

また、 Grid Manager またはインストール API を使用してシステムを設定することもできます。

手順

1. Python スクリプトを実行するために使用する Linux マシンにログインします。
2. インストールアーカイブを展開したディレクトリに移動します。

   たとえば、「+」と入力します
   `cd StorageGRID-Webscale-version/platform`

   ここで、 *platform* はです `debs`、 `rpms`または `vsphere`。

3. Python スクリプトを実行し、作成した構成ファイルを使用します。

   例：

```
./configure-storagegrid.py ./configure-storagegrid.json --start-install
```

完了後

リカバリパッケージ `.zip` 設定プロセスでファイルが生成され、インストールと設定を実行するディレクトリにダウンロードされます。グリッドノードで障害が発生した場合に StorageGRID システムをリカバリできるようにするために、リカバリパッケージファイルをバックアップする必要があります。たとえば、バックアップされたセキュアなネットワーク上の場所や、安全なクラウドストレージ上の場所にコピーします。

リカバリパッケージファイルには StorageGRID システムからデータを取得するための暗号キーとパスワードが含まれているため、安全に保管する必要があります。

ランダムパスワードを生成するように指定した場合は、を展開する必要があります `Passwords.txt` ファイルを開き、StorageGRID システムへのアクセスに必要なパスワードを探します。

```
######################################################################
##### The StorageGRID "recovery package" has been downloaded as: #####
#####           ./sgws-recovery-package-994078-rev1.zip          #####
#####   Safeguard this file as it will be needed in case of a    #####
#####                 StorageGRID node recovery.                 #####
######################################################################
```

StorageGRID システムがインストールおよび設定されると、確認メッセージが表示されます。

```
StorageGRID has been configured and installed.
```

## インストール **REST API** の概要

StorageGRID には、インストールタスクを実行するための REST API として、StorageGRID インストール API と StorageGRID アプライアンスインストーラ API の 2 つが用意されています。

どちらの API も、 Swagger オープンソース API プラットフォームを使用して API のドキュメントを提供しています。Swagger では、ユーザインターフェイスを使用してパラメータやオプションを変更した場合の API の動作を確認しながら、 API の開発を進めることができます。このドキュメントは、標準的な Web テクノロジと JavaScript Object Notation （ JSON ）データ形式について十分理解していることを前提としています。

API Docs Web ページを使用して実行する API 処理はすべてその場で実行されます。設定データやその他のデータを誤って作成、更新、または削除しないように注意してください。

各 REST API コマンドは、 API の URL 、 HTTP アクション、必須またはオプションの URL パラメータ、および想定される API 応答で構成されます。

### **StorageGRID** インストール **API**

StorageGRID インストール API は、 StorageGRID システムを最初に設定するとき、およびプライマリ管理ノードのリカバリを実行する必要がある場合にのみ使用できます。インストール API には、 Grid Manager から HTTPS 経由でアクセスできます。

API のドキュメントにアクセスするには、プライマリ管理ノードのインストール用 Web ページに移動し、メニューバーから * Help * > * API Documentation * を選択します。

StorageGRID インストール API には次のセクションがあります。

- *config *-- API の製品リリースとバージョンに関連する操作。製品リリースバージョンおよびそのリリースでサポートされる API のメジャーバージョンを一覧表示できます。

- * grid * — グリッドレベルの設定操作。グリッドの詳細、グリッドネットワークのサブネット、グリッドパスワード、 NTP および DNS サーバの IP アドレスなど、グリッド設定を取得および更新できます。
- *nodes * — ノードレベルの設定操作。グリッドノードのリストを取得できるほか、グリッドノードの削除、設定、表示、およびグリッドノードの設定のリセットを行うことができます。
- *provision * — プロビジョニング操作。プロビジョニング処理を開始し、プロビジョニング処理のステータスを表示できます。
- * recovery * - プライマリ管理ノードのリカバリ処理。情報のリセット、リカバリパッケージのアップロード、リカバリの開始、およびリカバリ処理のステータスの表示を行うことができます。
- * recovery-package * — リカバリパッケージをダウンロードする処理。
- *sites * — サイトレベルの設定操作。サイトを作成、表示、削除、および変更できます。

**StorageGRID** アプライアンスインストーラ **API**

StorageGRID アプライアンスインストーラAPIには、からHTTPS経由でアクセスできます `Controller_IP:8443`。

API ドキュメントにアクセスするには、アプライアンスの StorageGRID アプライアンスインストーラのメニューバーから * Help * > * API Docs * を選択します。

StorageGRID アプライアンスインストーラ API には、次のセクションがあります。

- * clone * — ノードのクローニングを構成および制御するための処理。
- *encryption * — 暗号化を管理し、暗号化ステータスを表示するための処理。
- * ハードウェア構成 * — 接続されたハードウェアでシステム設定を構成するための操作。
- *installation * ：アプライアンスのインストールを開始し、インストール・ステータスを監視するための処理。
- * networking * — StorageGRID アプライアンスのグリッドネットワーク、管理ネットワーク、クライアントネットワークの設定、およびアプライアンスのポート設定に関連する処理です。
- * setup * - システムに関する情報の取得やプライマリ管理ノード IP の更新要求など、アプライアンスの初期インストール設定に役立つ処理。
- *support *--コントローラのリブートとログ取得のための処理。
- * upgrade * ：アプライアンス・ファームウェアのアップグレードに関連する操作
- **uploadsg** — StorageGRID インストールファイルをアップロードするための操作。

## ハードウェアの設置のトラブルシューティング

設置作業で問題が発生した場合は、ハードウェアのセットアップや接続の問題に関するトラブルシューティング情報を確認すると役立つことがあります。

関連情報

"ハードウェアのセットアップがハングしたように見えます"

"接続の問題のトラブルシューティング"

# ハードウェア障害やケーブル接続エラーによって E5700SG コントローラのブート処理が完了しなかった場合、 StorageGRID アプライアンスインストーラを使用できないことがあります。

手順

1. デジタル表示ディスプレイのコードを監視します。

   電源投入時にハードウェアが初期化される際に、 2 つのデジタル表示ディスプレイに一連のコードが表示されます。ハードウェアが正常にブートされると、各コントローラのデジタル表示ディスプレイに異なるコードが表示されます。

2. E5700SG コントローラのデジタル表示ディスプレイのコードを確認してください。

   インストールとプロビジョニングには時間がかかります。フェーズによっては、StorageGRID アプライアンスインストーラの更新が数分間報告されないこともあります。

   エラーが発生すると、デジタル表示ディスプレイに HE などの一連のコードが点滅します。

3. これらのコードの意味については、次のリソースを参照してください。

| コントローラ | 参照 |
| --- | --- |
| E5700SG コントローラのものです | • E5700SG コントローラのステータス・インジケータ<br>• “he error:Error synchronizing with SANtricity OS Software” （エラー： OS ソフトウェアとの同期エラー） |
| E2800 コントローラ | E5700 and E2800 System Monitoring Guide<br>• 注： * E シリーズ E5700 コントローラに関するコードは、アプライアンスの E5700SG コントローラには適用されません。 |

4. この方法で問題 が解決しない場合は、テクニカルサポートにお問い合わせください。

関連情報

"E5700SG コントローラのステータスインジケータ"

"HE エラー： SANtricity OS ソフトウェアとの同期エラー"

"NetApp E シリーズシステムのドキュメントのサイト"

**HE** エラー： **SANtricity OS** ソフトウェアとの同期エラー

# StorageGRID アプライアンスインストーラが SANtricity OS ソフトウェアと同期できない場合は、コンピューティングコントローラのデジタル表示ディスプレイに HE エラー

コードが表示されます。

このタスクについて

HE エラーコードが表示された場合は、次の対処策を実施します。

手順

1. 2 台のコントローラ間の 2 本のインターコネクトケーブルを調べて、ケーブルと SFP+ トランシーバがしっかりと接続されていることを確認します。
2. 必要に応じて、一方または両方のケーブルまたは SFP+ トランシーバを交換し、再試行します。
3. この方法で問題 が解決しない場合は、テクニカルサポートにお問い合わせください。

接続の問題のトラブルシューティング

## StorageGRID アプライアンスのインストール時に接続の問題が発生した場合は、以下に記載する対処策を実施する必要があります。

アプライアンスに接続できません

## アプライアンスに接続できない場合は、ネットワーク問題 があるか、またはハードウェアの設置が正常に完了していない可能性があります。

手順

1. SANtricity システムマネージャに接続できない場合は、次の手順を実行します。
   a. SANtricity System Managerの管理ネットワークで、E2800コントローラのIPアドレスを使用してアプライアンスにpingを送信します：+
   **`ping E2800_Controller_IP`**
   b. ping からの応答がない場合は、正しい IP アドレスを使用していることを確認します。

      E2800 コントローラの管理ポート 1 の IP アドレスを使用します。

   c. IP アドレスが正しい場合は、アプライアンスのケーブル接続とネットワークのセットアップを確認します。

      この手順で問題 が解決しない場合は、テクニカルサポートにお問い合わせください。

   d. ping が成功した場合は、 Web ブラウザを開きます。
   e. SANtricity システムマネージャのURLとして「+」を入力します
   **`https://E2800_Controller_IP`**

      SANtricity System Manager のログインページが表示されます。

2. E5700SG コントローラに接続できない場合は、次の手順を実行してください。
   a. E5700SGコントローラのIPアドレス+を使用してアプライアンスにpingを送信してください
   **`ping E5700SG_Controller_IP`**
   b. ping からの応答がない場合は、正しい IP アドレスを使用していることを確認します。

      グリッドネットワーク、管理ネットワーク、またはクライアントネットワークでのアプライアンスの

IP アドレスを使用できます。

c. IP アドレスが正しい場合は、アプライアンスのケーブル接続、 SFP トランシーバ、およびネットワークのセットアップを確認します。

この手順で問題 が解決しない場合は、テクニカルサポートにお問い合わせください。

d. ping が成功した場合は、 Web ブラウザを開きます。

e. StorageGRID アプライアンスインストーラのURLとして「+」を入力します
**`https://E5700SG_Controller_IP:8443`**

ホームページが表示されます。

**StorageGRID** アプライアンスインストーラの実行中にコントローラをリブートします

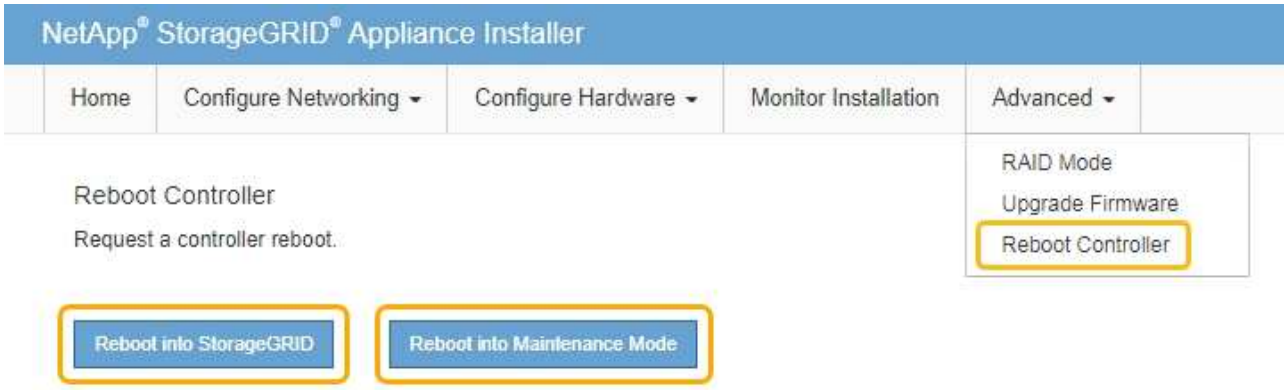
## StorageGRID アプライアンスインストーラの実行中にコンピューティングコントローラのリブートが必要になる場合があります。たとえば、インストールが失敗した場合は、コントローラのリブートが必要になることがあります。

このタスクについて

この手順 は、コンピューティングコントローラで StorageGRID アプライアンスインストーラが実行されている場合にのみ適用されます。インストールが完了すると、 StorageGRID アプライアンスインストーラが使用できなくなるため、この手順は機能しなくなります。

手順

1. StorageGRID アプライアンス・インストーラで、 [**Advanced**>*Reboot Controller*] をクリックし、次のいずれかのオプションを選択します。
   - Reboot into StorageGRID * を選択し、ノードをグリッドに再追加してコントローラをリブートします。メンテナンスモードで作業を完了し、ノードを通常動作に戻す準備ができている場合は、このオプションを選択します。
   - メンテナンスモードを維持したままコントローラをリブートするには、 * Reboot into Maintenance Mode * を選択します。このオプションは、グリッドに再追加する前にノードで追加のメンテナンス処理を実行する必要がある場合に選択しま
   す。




SG6000-CN コントローラがリブートされます。

# SG5700アプライアンスのメンテナンス

E2800 コントローラでの SANtricity OS ソフトウェアのアップグレード、 E5700SG コントローラのイーサネットリンク設定の変更、 E2800 コントローラまたは E5700SG コントローラの交換、または特定のコンポーネントの交換が必要になることがあります。このセクションの手順は、アプライアンスが StorageGRID システムにストレージノードとしてすでに導入されていることを前提としています。

手順

- "アプライアンスをメンテナンスモードにします"
- "ストレージコントローラのSANtricity OSをアップグレードしています"
- "SANtricity System Managerを使用してドライブファームウェアをアップグレードする"
- "E2800コントローラの交換"
- "E5700SGコントローラの交換"
- "その他のハードウェアコンポーネントの交換"
- "E5700SGコントローラのリンク設定の変更"
- "MTU設定を変更します"
- "DNSサーバの設定を確認しています"
- "メンテナンスモードでのノード暗号化の監視"

## アプライアンスをメンテナンスモードにします

特定のメンテナンス手順を実行する前に、アプライアンスをメンテナンスモードにする必要があります。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Maintenance または Root Access 権限が必要です。詳細については、 StorageGRID の管理手順を参照してください。

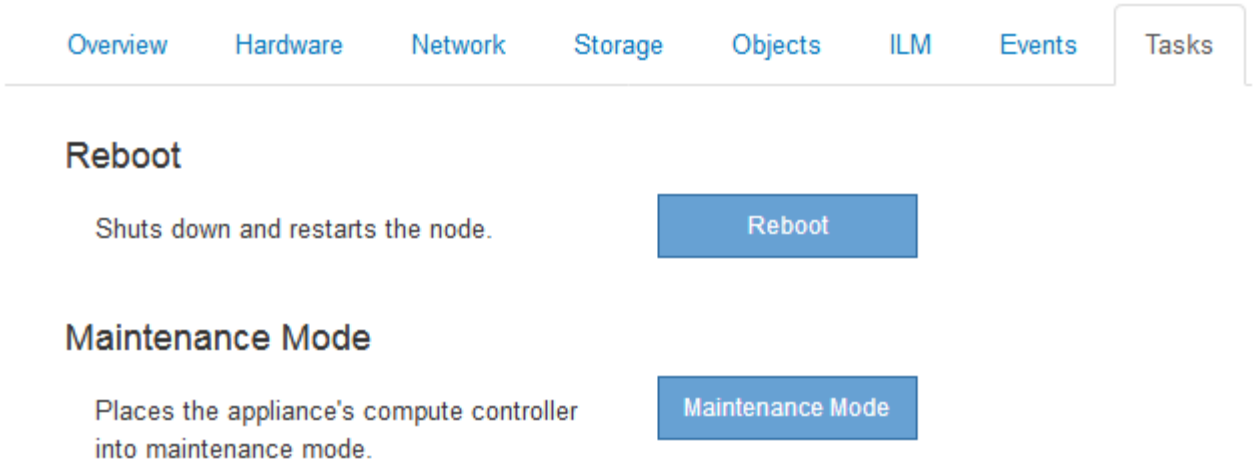
このタスクについて

StorageGRID アプライアンスをメンテナンスモードにすると、アプライアンスにリモートアクセスできなくなることがあります。

> 保守モードのStorageGRID アプライアンスのパスワードおよびホスト・キーは、アプライアンスが稼働していたときと同じままです。

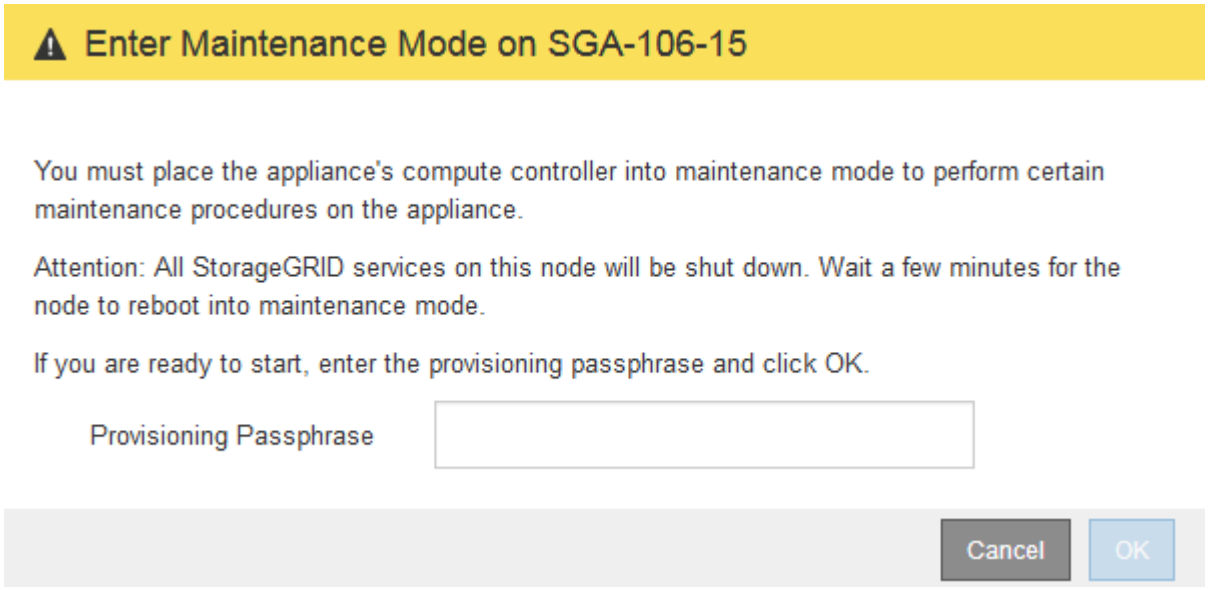
手順

1. Grid Managerから* Nodes *を選択します。
2. Nodes ページのツリービューで、アプライアンスストレージノードを選択します。
3. [ タスク ] を選択します。



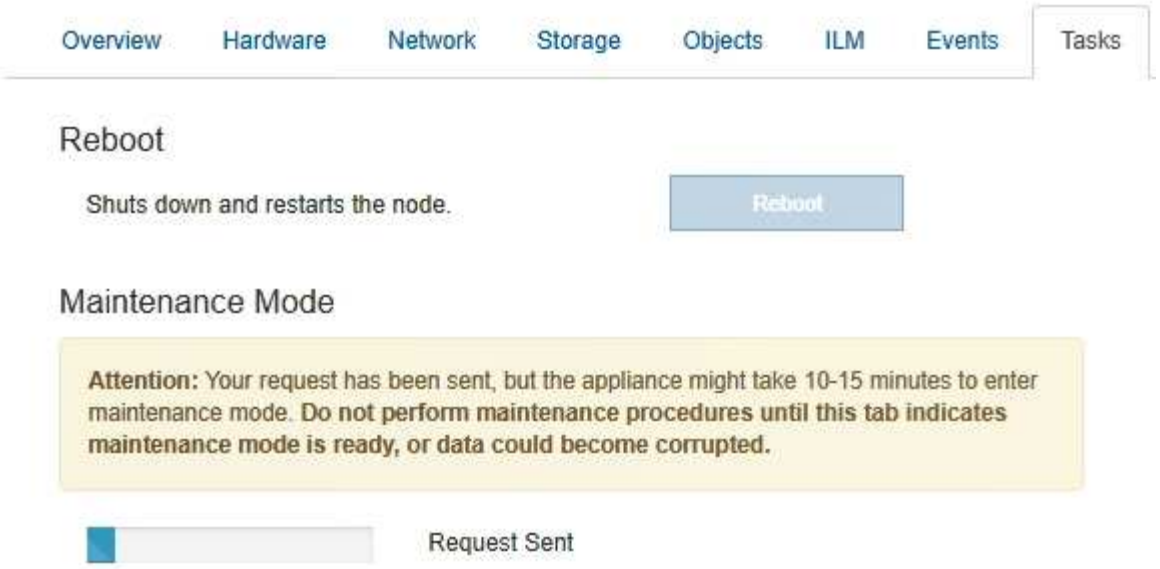

4. [* Maintenance Mode]*を選択します。

   確認のダイアログボックスが表示されます。

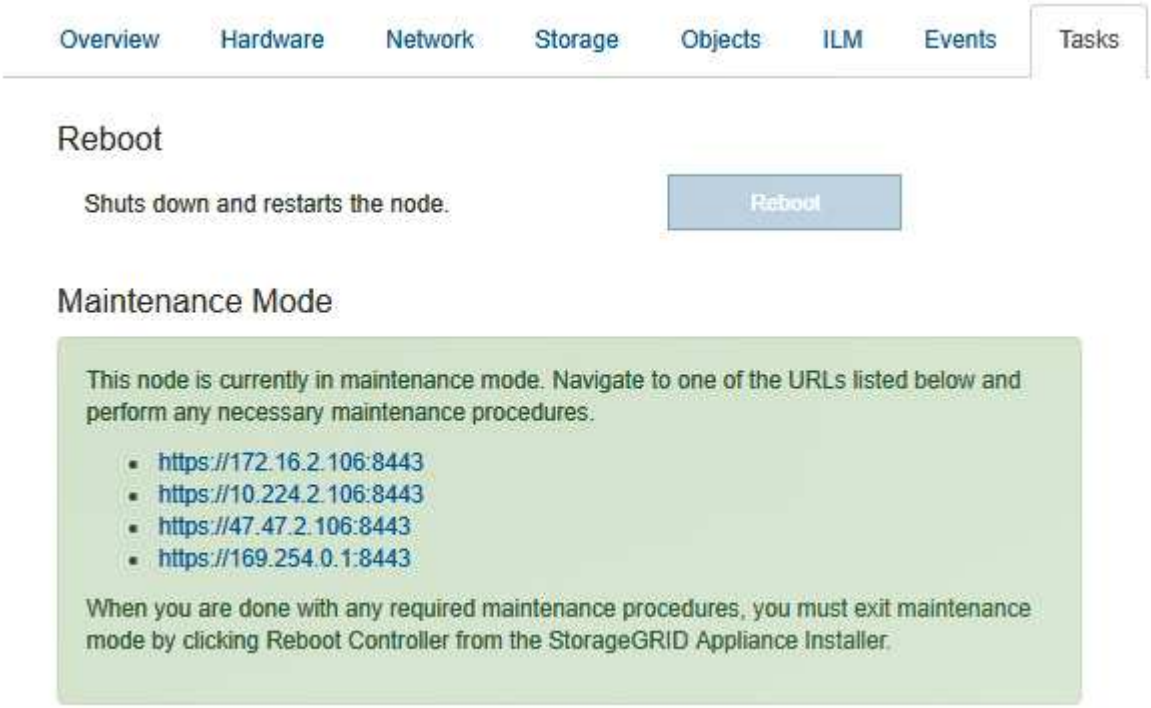



5. プロビジョニングパスフレーズを入力し、「 * OK 」を選択します。

   進捗状況バーと一連のメッセージ（「 Request Sent 」、「 Stopping StorageGRID 」、「 Rebaling 」など）は、アプライアンスがメンテナンスモードに移行するための手順を完了していることを示しています。




アプライアンスがメンテナンスモードになっている場合は、 StorageGRID アプライアンスインストーラへのアクセスに使用できる URL が確認メッセージに表示されます。




6. StorageGRID アプライアンスインストーラにアクセスするには、表示されたいずれかの URL にアクセスします。

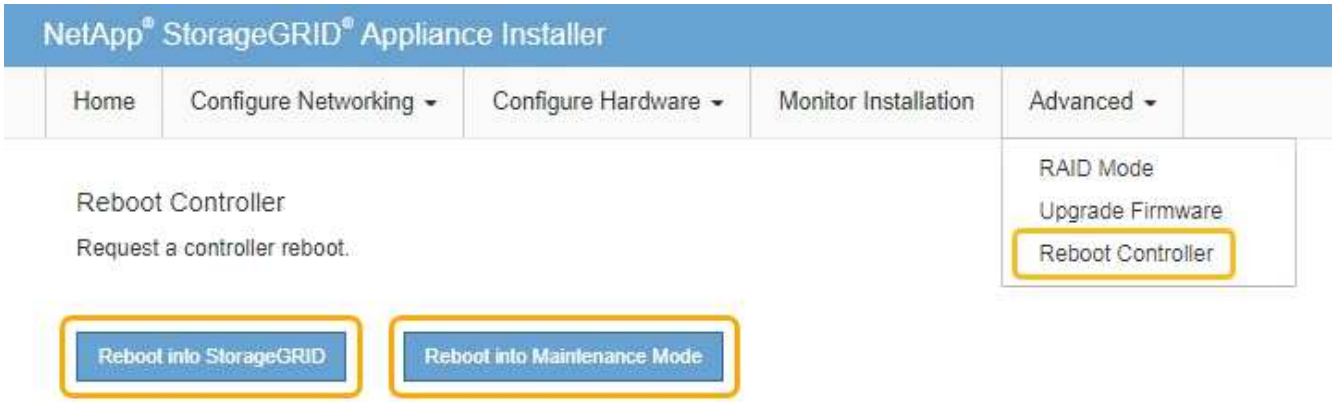
   可能であれば、アプライアンスの管理ネットワークポートの IP アドレスを含む URL を使用します。

   > へのアクセス `https://169.254.0.1:8443` ローカル管理ポートに直接接続する必要があります。

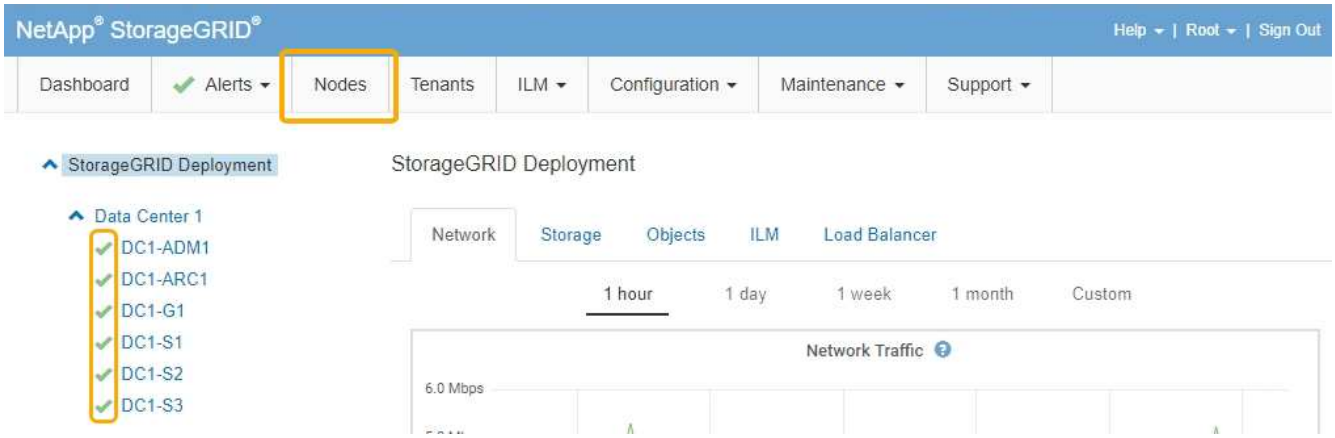
7. StorageGRID アプライアンスインストーラで、アプライアンスがメンテナンスモードになっていることを

確認します。

8. 必要なメンテナンスタスクを実行します。
9. メンテナンス作業が完了したら、メンテナンスモードを終了して通常のノードの運用を再開します。StorageGRID アプライアンス・インストーラから、 **Advanced**>* Reboot Controller* を選択し、 * Reboot into StorageGRID * を選択します。




アプライアンスがリブートしてグリッドに再参加するまでに最大 20 分かかることがあります。リブートが完了し、ノードが再びグリッドに参加したことを確認するには、 Grid Manager に戻ります。[ノード*（Nodes *）]タブには、通常のステータスが表示されます ✔ アクティブなアラートがなく、ノードがグリッドに接続されていることを示す、アプライアンスノードの場合。




ストレージコントローラの**SANtricity OS**をアップグレードしています

ストレージコントローラが最適に機能するようにするには、 StorageGRID アプライアンスに対応した最新の SANtricity OS メンテナンスリリースにアップグレードする必要があります。使用するバージョンを確認するには、 NetApp Interoperability Matrix Tool （ IMT ）を参照してください。サポートが必要な場合は、テクニカルサポートにお問い合

わせください。

- ストレージコントローラで SANtricity OS 08.42.20.00 （ 11.42 ）以降を使用している場合、 Grid Manager を使用してアップグレードを実行します。

  "グリッドマネージャを使用してストレージコントローラのSANtricity OSをアップグレードします"

- ストレージコントローラで 08.42.20.00 （ 11.42 ）より前のバージョンの SANtricity OS を使用している場合、メンテナンスモードを使用してアップグレードを実行します。

  "メンテナンスモードを使用したE2800コントローラでのSANtricity OSのアップグレード"

関連情報

"NetApp Interoperability Matrix Tool で確認できます"

"ネットアップのダウンロード： SANtricity OS"

"トラブルシューティングを監視します"

グリッドマネージャを使用してストレージコントローラの**SANtricity OS**をアップグレードします

## 現在 SANtricity OS 08.42.20.00 （ 11.42 ）以降を使用しているストレージコントローラの場合、 Grid Manager を使用してアップグレードを適用する必要があります。

必要なもの

- NetApp Interoperability Matrix Tool （ IMT ）を参照して、アップグレードに使用する SANtricity OS のバージョンがお使いのアプライアンスと互換性があることを確認してください。
- Maintenance権限が必要です。
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- プロビジョニングパスフレーズが必要です。
- SANtricity OSに関するネットアップのダウンロードページを利用する必要があります。

このタスクについて

SANtricity OS のアップグレードプロセスが完了するまで、他のソフトウェアの更新（ StorageGRID ソフトウェアのアップグレードまたはホットフィックス）は実行できません。SANtricity OS のアップグレードプロセスが完了する前にホットフィックスや StorageGRID ソフトウェアのアップグレードを開始しようとすると、SANtricity OS のアップグレードページが表示されます。

該当するすべてのノードにSANtricity OSのアップグレードが正常に適用されるまで、手順 は完了しません。各ノードにSANtricity OSがロードされ、各StorageGRID ストレージアプライアンスがリブートされるまでに30分以上かかることがあります。

次の手順は、 Grid Manager を使用してアップグレードを実行する場合にのみ実行できます。SG5700シリーズアプライアンスのストレージコントローラは、コントローラで08.42.20.00（11.42）より前のSANtricity OSを使用している場合、Grid Managerを使用してアップグレードできません。

この手順 は、 SANtricity OS のアップグレードに関連付けられた最新バージョンに NVSRAM を自動的にアップグレードします。個別の NVSRAM アップグレードファイルを適用する必要はありません。

手順

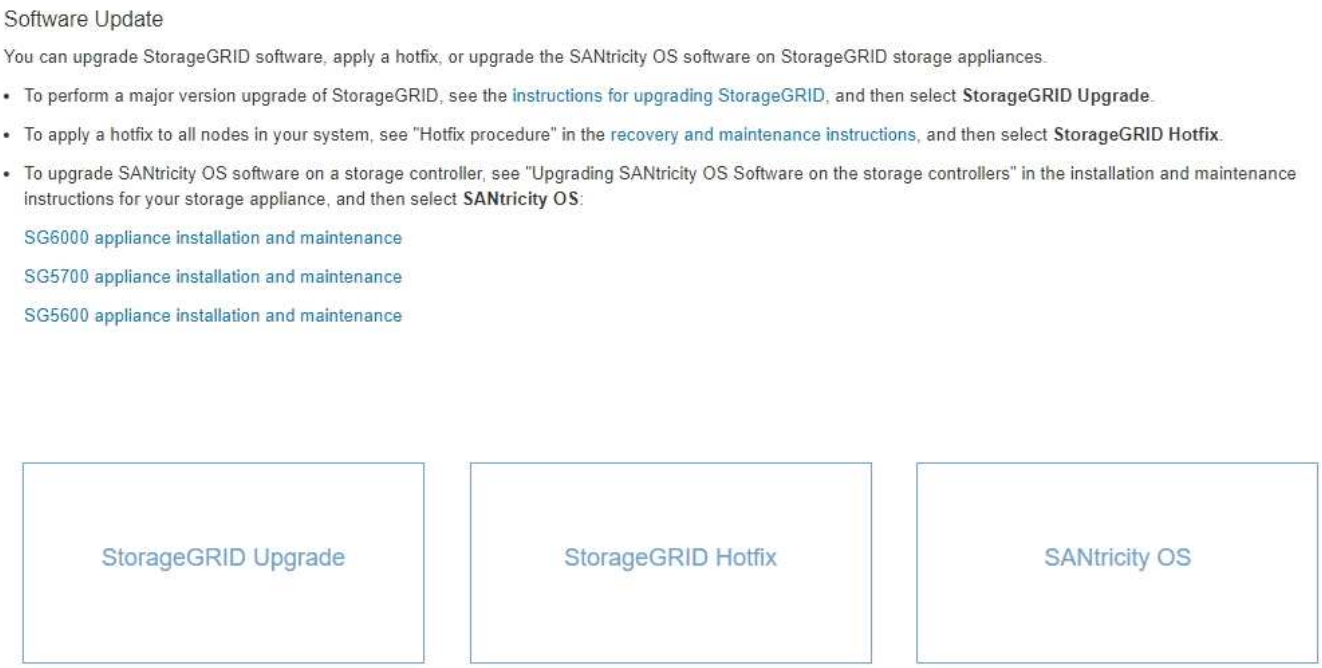
1. サービスラップトップから、NetApp Support Site から新しいSANtricity OSソフトウェアファイルをダウンロードします。

   必ずE2800ストレージコントローラのSANtricity OSバージョンを選択してください。

   "ネットアップのダウンロード： SANtricity OS"

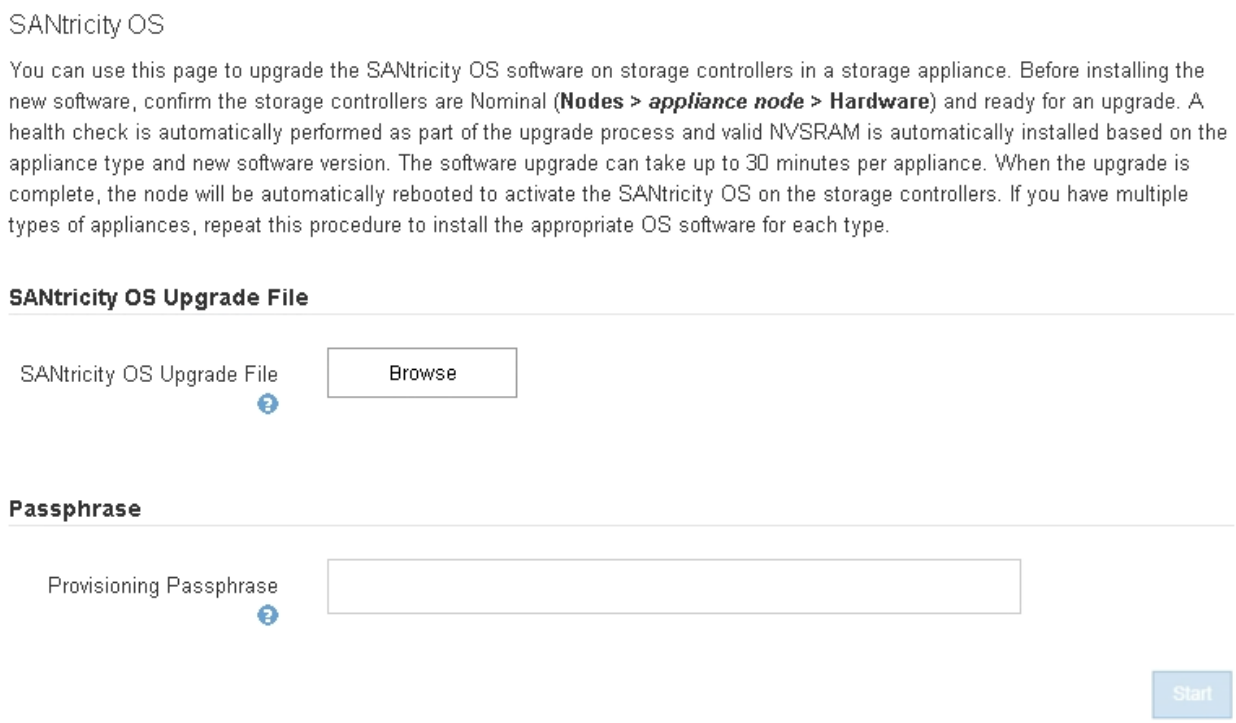
2. サポートされているブラウザを使用してGrid Managerにサインインします。
3. [* Maintenance（メンテナンス）]を選択します次に、メニューの[システム]セクションで、[ソフトウェア・アップデート]を選択します。

   Software Update ページが表示されます。




4. SANtricity OS *をクリックします。

   SANtricity OSページが表示されます。




5. NetApp Support Siteからダウンロードした SANtricity OS アップグレードファイルを選択します。

   a. [* 参照 ] をクリックします。

   b. ファイルを探して選択します。

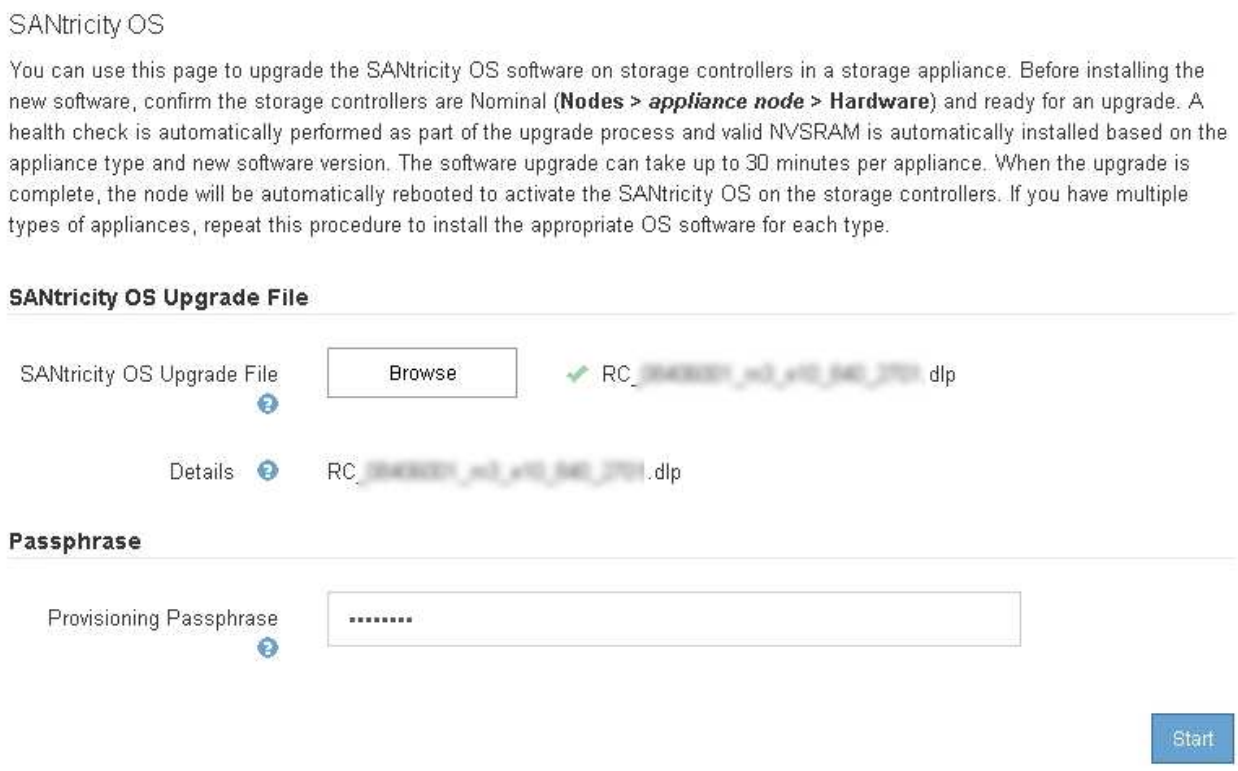
   c. * 開く * をクリックします。

   ファイルがアップロードされて検証されます。検証プロセスが完了すると、[詳細]フィールドにファイル名が表示されます。

   ファイル名は検証プロセスで指定されるため変更しないでください。

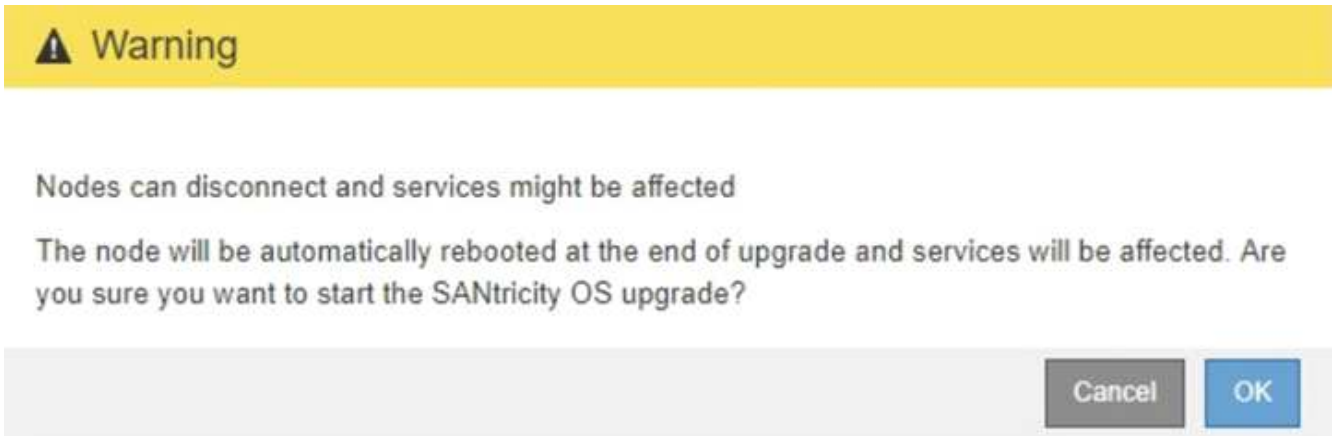
6. プロビジョニングパスフレーズを入力します。

「* Start *（スタート *）」ボタンが有効になります。



7. [ スタート ] ボタンをクリックします。

   アップグレードされたノードのサービスを再起動するとブラウザの接続が一時的に失われる可能性があることを示す警告ボックスが表示されます。




8. OK *をクリックして、SANtricity OSアップグレードファイルをプライマリ管理ノードにステージングします。

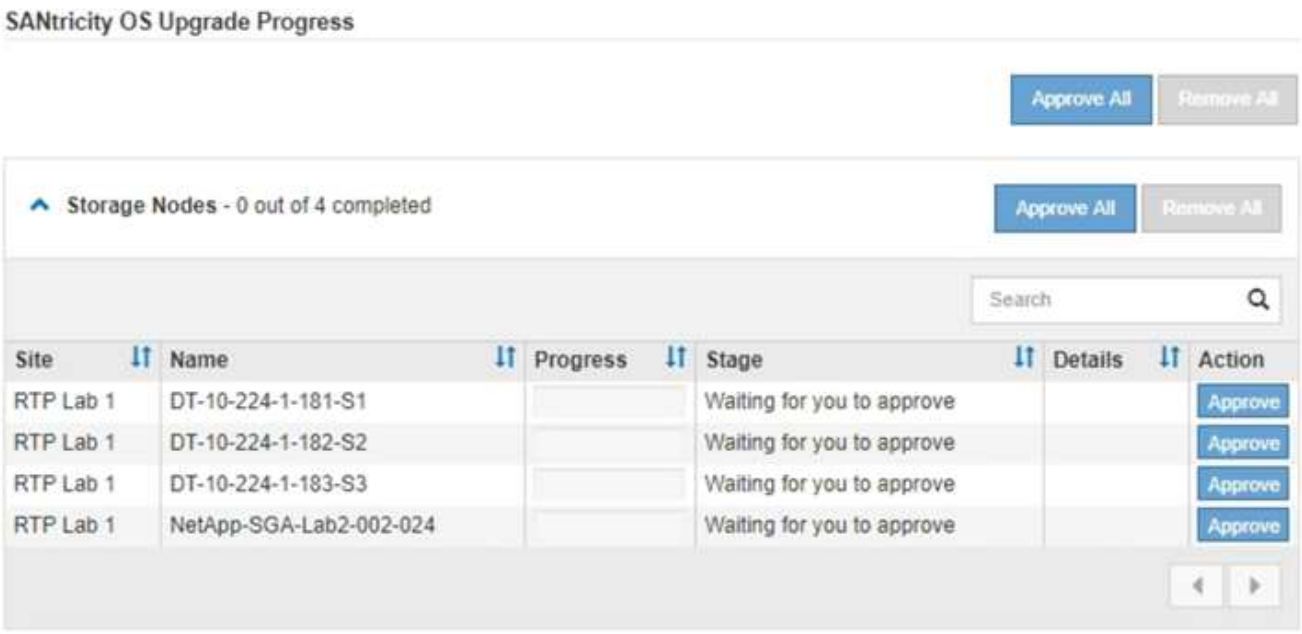
   SANtricity OS のアップグレードを開始すると、次の処理が行わ

   a. 健全性チェックが実行されます。このプロセスにより、ステータスが「 Needs Attention 」になっているノードがないかどうかが確認されます。

      エラーが報告された場合は、エラーを解決してから、*開始*をもう一度クリックします。

   b. SANtricity OS Upgrade Progress テーブルが表示されます。この表には、グリッド内のすべてのストレージノードと、各ノードのアップグレードの現在のステージが表示されます。

      ソフトウェアベースのストレージノードを含むすべてのストレージノードが表示されます。SANtricity OSのアップグレードがソフトウェアベースのストレージノードに影響しない場合でも、すべてのストレージノードのアップグレードを承認する必要があります。ソフトウェア・ベースのストレージ・ノードに対して返されたアップグレード・メッセージは「SANtricity OS upgrade is not applicable to this node.」です。




9. 必要に応じて、ノードのリストを* Site 、 Name 、 Progress 、 Stage 、または Details *で昇順または降順にソートします。または、 * 検索 * ボックスに用語を入力して特定のノードを検索します。

   ノードのリストをスクロールするには、セクションの右下隅にある左右の矢印を使用します。

10. アップグレードキューに追加する準備ができたグリッドノードを承認します。同じタイプの承認済みノードが一度に 1 つずつアップグレードされます。

    アプライアンスストレージノードのSANtricity OSアップグレードは、ノードを停止およびリブートする準備ができているかどうかが確認されないかぎり承認しないでください。ノードでSANtricity OSのアップグレードが承認されると、そのノードのサービスが停止します。あとでノードをアップグレードすると、アプライアンスノードがリブートされます。このような処理を実行すると、ノードと通信しているクライアントで原因 サービスが中断する可能性があります。

    - すべてのストレージノードをSANtricity OSアップグレードキューに追加するには、いずれかの*すべて承認ボタンをクリックします。

      ノードのアップグレード順序が重要な場合は、ノードまたはノードグループを 1 つずつ承認し、各ノードでアップグレードが完了するまで待ってから、次のノードを承認します。

    - 1つ以上の*承認*ボタンをクリックして、SANtricity OSアップグレードキューに1つ以上のノードを追加します。

      ノードへのSANtricity OSのアップグレードの適用は遅延できますが、リストされているすべてのストレージノードでSANtricity OSのアップグレードを承認するまで、SANtricity OSのアップグレードプロセスは完了しません。

    [* Approve *（承認）]をクリックすると、アップグレードプロセスによってノードをアップグレードできるかどうかが決定されます。ノードをアップグレード可能な場合は、アップグレードキューに追加されます。[+]

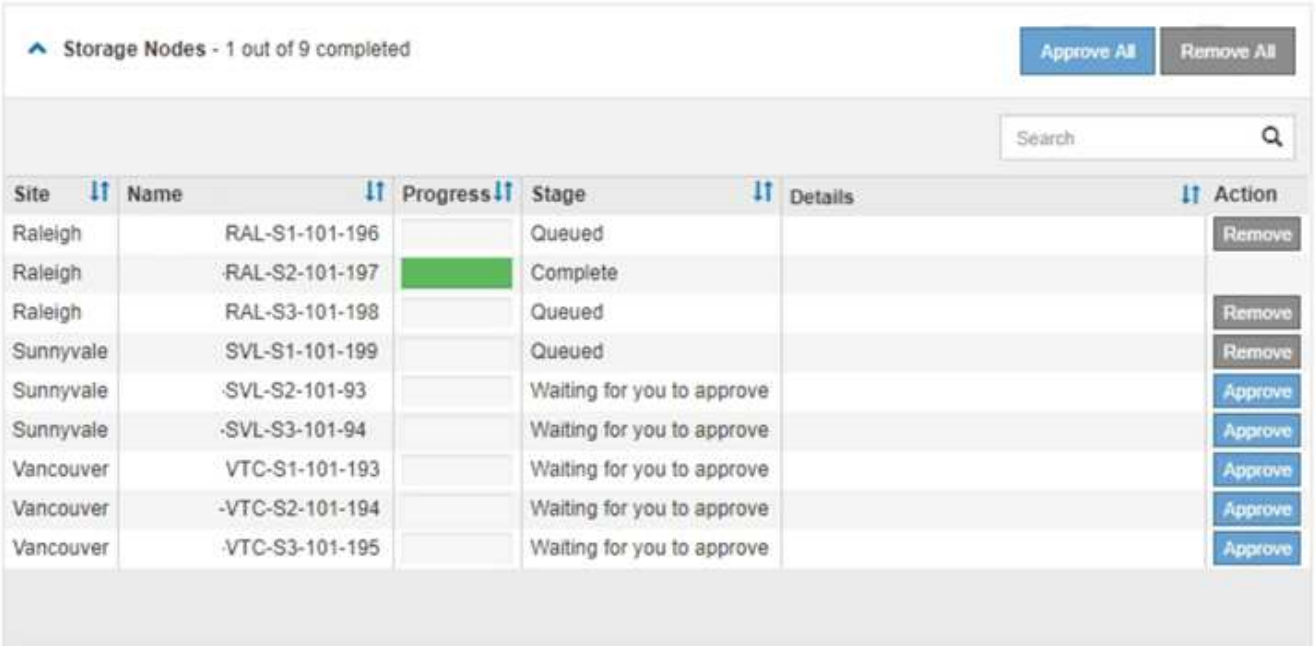
ノードによっては、選択したアップグレードファイルが意図的に適用されていないため、これらのノードをアップグレードせずにアップグレードプロセスを完了することができます。ノードが意図的にアップグレードされていない場合、プロセスの「Complete」列に次のいずれかのメッセージが表示されます。

- ストレージノードはすでにアップグレードされています。
- このノードではSANtricity OSのアップグレードは実行できません。
- SANtricity OSファイルがこのノードに対応していません。

「SANtricity OS upgrade is not applicable to this node」というメッセージは、ノードにStorageGRID システムで管理可能なストレージ・コントローラがないことを示します。このメッセージは、非アプライアンスストレージノードに対して表示されます。このメッセージが表示されているノードをアップグレードせずに、SANtricity OSのアップグレードプロセスを完了できます。+「SANtricity OS file is not compatible with this node」というメッセージは、ノードに、インストールしようとしているプロセスとは異なるSANtricity OSファイルが必要であることを示しています。現在のSANtricity OSのアップグレードが完了したら、そのノードに適したSANtricity OSをダウンロードして、アップグレードプロセスを繰り返します。

11. SANtricity OSアップグレードキューからノードまたはすべてのノードを削除する必要がある場合は、* Remove または Remove All *をクリックします。

例に示すように、ステージがQueuedを超えて進むと、* Remove *ボタンが非表示になり、SANtricity OSアップグレード処理からノードを削除できなくなります。




12. 承認された各グリッドノードに SANtricity OS のアップグレードが適用されるまで待ちます。

SANtricity OSのアップグレードの適用中にいずれかのノードでエラーステージが表示される場合、そのノードのアップグレードは失敗しています。障害からリカバリするために、アプライアンスをメンテナンスモードに切り替える必要がある場合があります。続行する前にテクニカルサポートにお問い合わせください。

ノード上のファームウェアが古すぎて Grid Manager でアップグレードできない場合、そのノードは Error をステージに表示します。 "` このノードで SANtricity OS をアップグレードするには、保守モードを使用

する必要があります。使用しているアプライアンスのインストールとメンテナンスの手順を参照してください。アップグレード後は ' このユーティリティを将来のアップグレードに使用できます エラーを解決するには、次の手順を実行します。

a. メンテナンスモードを使用して、「エラー」のステージが表示されるノードの SANtricity OS をアップグレードします。

b. Grid Managerを使用してSANtricity OSのアップグレードを再開し、完了します。

   承認されたすべてのノードで SANtricity OS のアップグレードが完了すると、 SANtricity OS アップグレードの進捗状況テーブルが閉じ、緑のバナーに SANtricity OS のアップグレードが完了した日時が表示されます。

13. 別の SANtricity OS アップグレードファイルが必要な、完了段階のノードすべてについて、このアップグレード手順 を繰り返します。

ステータスが「 Needs Attention 」のノードがある場合は、メンテナンスモードを使用してアップグレードを実行します。

関連情報

"メンテナンスモードを使用したE2800コントローラでのSANtricity OSのアップグレード"

メンテナンスモードを使用した**E2800**コントローラでの**SANtricity OS**のアップグレード

## 08.42.20.00 （ 11.42 ）より前の SANtricity OS を使用しているストレージコントローラの場合、メンテナンスモード手順 を使用してアップグレードを適用する必要があります。

必要なもの

- NetApp Interoperability Matrix Tool （ IMT ）を参照して、アップグレードに使用する SANtricity OS のバージョンがお使いのアプライアンスと互換性があることを確認してください。
- E5700SG コントローラをメンテナンスモードにして、 E2800 コントローラへの接続を中断する必要があります。StorageGRID アプライアンスをメンテナンスモードにすると、アプライアンスにリモートアクセスできなくなることがあります。

  "アプライアンスをメンテナンスモードにします"

このタスクについて

一度に複数の StorageGRID アプライアンスで E シリーズコントローラの SANtricity OS または NVSRAM を

アップグレードしないでください。

> 一度に複数の StorageGRID アプライアンスをアップグレードすると、導入モデルや ILM ポリシーによっては、原因 データを使用できなくなる可能性があります。

手順

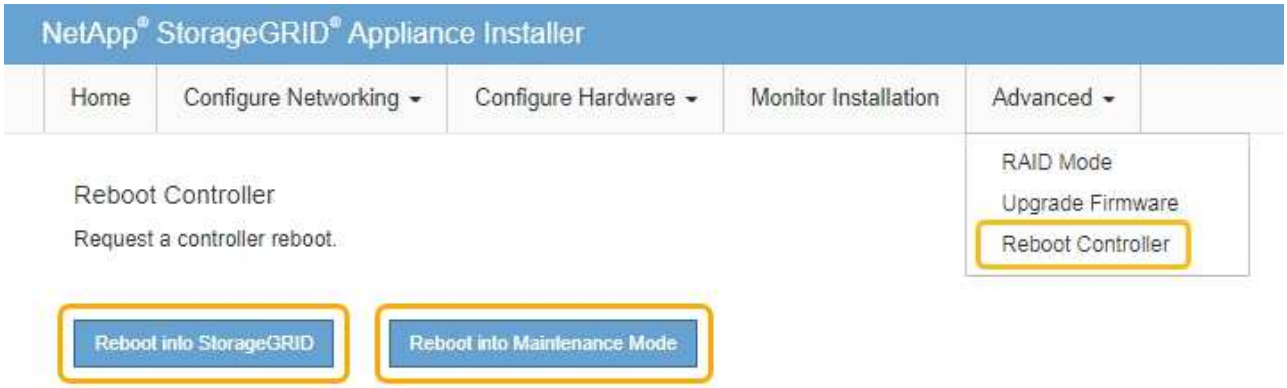
1. サービスラップトップから、 SANtricity System Manager にアクセスしてサインインします。
2. 新しい SANtricity OS ソフトウェアファイルと NVSRAM ファイルを管理クライアントにダウンロードします。

> NVSRAM は、 StorageGRID アプライアンスに固有です。標準の NVSRAM ダウンロードを使用しないでください。

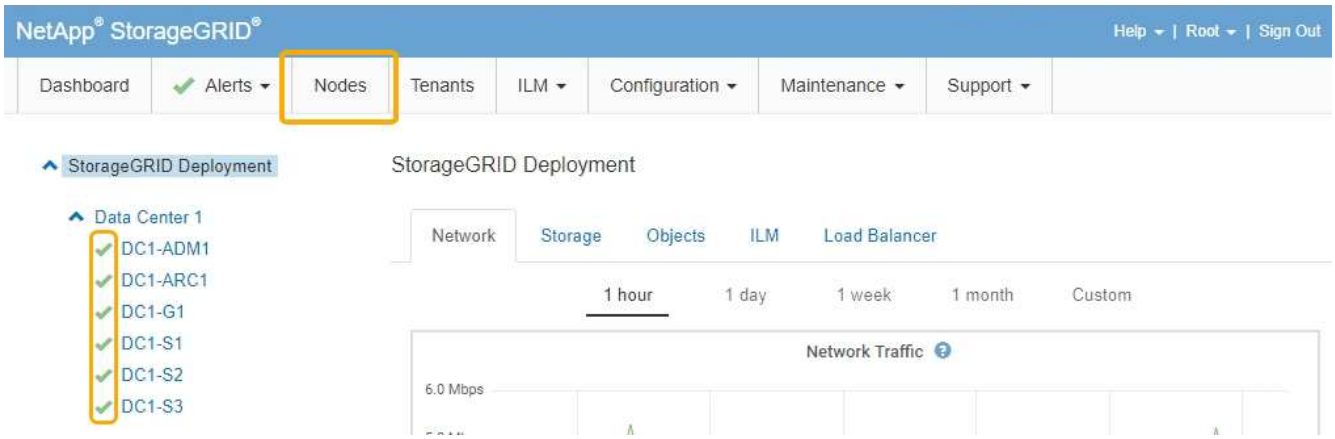
3. E2800 and E5700 SANtricity Software and Firmware Upgrade Guide または SANtricity System Manager のオンラインヘルプに記載されている手順に従って、 E2800 コントローラのファームウェアと NVSRAM をアップグレードします。

> アップグレードファイルはただちにアクティブ化する必要があります。アクティブ化を先延ばしにしないでください。

4. アップグレード処理が完了したら、ノードをリブートします。StorageGRID アプライアンス・インストーラから、 **Advanced**>*Reboot Controller* を選択し、次のいずれかのオプションを選択します。
   - Reboot into StorageGRID * を選択し、ノードをグリッドに再追加してコントローラをリブートします。メンテナンスモードで作業を完了し、ノードを通常動作に戻す準備ができている場合は、このオプションを選択します。
   - メンテナンスモードを維持したままコントローラをリブートするには、 * Reboot into Maintenance Mode * を選択します。このオプションは、グリッドに再追加する前にノードで追加のメンテナンス処理を実行する必要がある場合に選択します。




アプライアンスがリブートしてグリッドに再参加するまでに最大 20 分かかることがあります。リブートが完了し、ノードが再びグリッドに参加したことを確認するには、 Grid Manager に戻ります。[ノード*（Nodes *）]タブには、通常のステータスが表示されます ✔ アクティブなアラートがなく、ノードがグリッドに接続されていることを示す、アプライアンスノードの場合。




関連情報

"グリッドマネージャを使用してストレージコントローラのSANtricity OSをアップグレードします"

**SANtricity System Manager**を使用してドライブファームウェアをアップグレードする

## ドライブファームウェアをアップグレードして、最新の機能とバグ修正をすべて適用します。

必要なもの

- ストレージアプライアンスのステータスが「最適」であることを確認します。
- すべてのドライブのステータスが最適な状態である必要があります
- 最新バージョンの SANtricity System Manager がインストールされていて、 StorageGRID のバージョンと互換性があることを確認します。
- StorageGRID アプライアンスをメンテナンスモードにしておきます。

  "アプライアンスをメンテナンスモードにします"

> 保守モードでは、ストレージコントローラへの接続が中断され、すべての I/O アクティビティが停止されて、すべてのドライブがオフラインになります。

> 一度に複数の StorageGRID アプライアンスでドライブファームウェアをアップグレードしないでください。お使いの導入モデルや ILM ポリシーによっては、原因 データを使用できなくなる場合があります。

手順

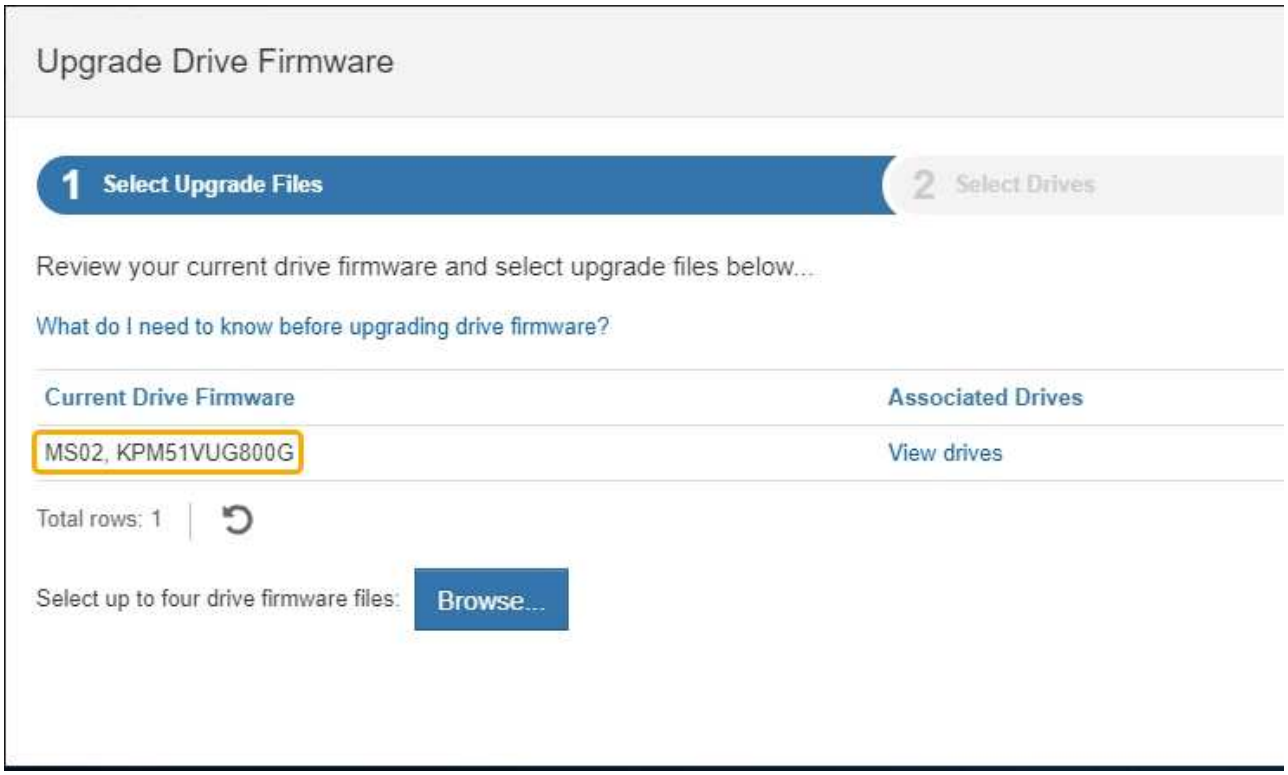
1. 次のいずれかの方法で SANtricity System Manager にアクセスします。
   - StorageGRID アプライアンス・インストーラを使用して、 * アドバンスト * > * SANtricity システム・マネージャ * を選択します
   - Grid Managerを使用して* Nodes >を選択します ***appliance Storage Node*** >* SANtricity システム・マネージャ*

これらのオプションが表示されない場合や、SANtricity System Managerのログインページが表示されない場合は、ストレージコントローラのIP：+にアクセスしてSANtricity System Managerにアクセスします
**https://*Storage_Controller_IP***

2. 必要に応じて、 SANtricity System Manager 管理者のユーザ名とパスワードを入力します。
3. ストレージアプライアンスに現在インストールされているドライブファームウェアのバージョンを確認します。
   a. SANtricity システムマネージャで、* Support > Upgrade Center *を選択します。
   b. ドライブファームウェアのアップグレードで、 * アップグレードの開始 * を選択します。

      ドライブファームウェアのアップグレードに、現在インストールされているドライブファームウェアファイルが表示されます。

   c. 現在のドライブファームウェア列に表示されているドライブファームウェアのリビジョンとドライブ ID をメモします。




次の例では、

- ドライブファームウェアのリビジョンは * MS02 * です。
- ドライブ識別子は **KPM51VUG800G** です。

Associated Drives 列で「 * View drives 」を選択して、ストレージアプライアンス内のドライブがどこに取り付けられているかを表示します。

   a. ドライブファームウェアのアップグレードウィンドウを閉じます。

4. 使用可能なドライブファームウェアのアップグレードをダウンロードして準備します。

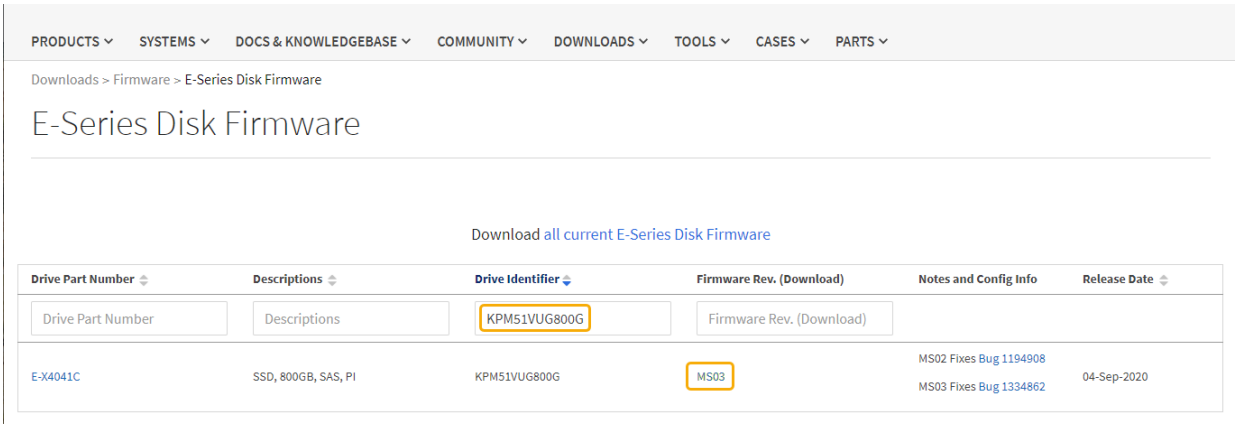
a. ドライブファームウェアのアップグレードで、 * ネットアップサポート * を選択します。

b. ネットアップサポート Web サイトで、「 * Downloads * 」タブを選択し、「 * E-Series Disk Drive Firmware * 」を選択します。

   E-Series Disk Firmware ページが表示されます。

c. ストレージアプライアンスにインストールされているドライブ識別子 * をそれぞれ検索し、各ドライブ識別子に最新のファームウェアリビジョンが適用されていることを確認します。

   - ファームウェアリビジョンがリンクでない場合、このドライブ識別子には最新のファームウェアリビジョンが含まれます。
   - ドライブ識別子が記載されたドライブのパーツ番号が 1 つ以上であれば、それらのドライブでファームウェアのアップグレードを実行できます。任意のリンクを選択してファームウェアファイルをダウンロードできま
     す。




d. 新しいファームウェアリビジョンがリストされている場合は、ファームウェアリビジョンのリンクを選択します（ダウンロード）列をクリックしてをダウンロードします `.zip` ファームウェアファイルを含むアーカイブ。

e. サポートサイトからダウンロードしたドライブファームウェアのアーカイブファイルを展開（解凍）します。

5. ドライブファームウェアのアップグレードをインストールします。

a. SANtricity システムマネージャのドライブファームウェアアップグレードで、 * アップグレードの開始 * を選択します。

b. [* Browse] を選択し、サポートサイトからダウンロードした新しいドライブファームウェアファイルを選択します。

   ドライブファームウェアファイルの名前は、+のようになります
   `D_HUC101212CSS600_30602291_MS01_2800_0002.dlp`

   ドライブファームウェアファイルは一度に 1 つずつ、最大 4 つまで選択できます。同じドライブに複数のドライブファームウェアファイルが対応している場合は、ファイル競合エラーが発生します。アップグレードに使用するドライブファームウェアファイルを決定し、それ以外のファイルは削除します。

c. 「 * 次へ * 」を選択します。

   - ドライブの選択 * には、選択したファームウェアファイルでアップグレードできるドライブがリストされています。

対応しているドライブのみが表示されます。

選択したドライブのファームウェアが * 推奨ファームウェア * に表示されます。このファームウェアを変更する必要がある場合は、 * 戻る * を選択します。

d. 「オフライン（パラレル） * アップグレード」を選択します。

オフラインアップグレード方式を使用できるのは、アプライアンスがメンテナンスモードで、すべてのドライブとすべてのボリュームの I/O アクティビティが停止されているためです。

e. テーブルの最初の列で、アップグレードするドライブを選択します。

ベストプラクティスとして、同じモデルのドライブをすべて同じファームウェアリビジョンにアップグレードすることを推奨します。

f. [ スタート ] ボタンをクリックし、アップグレードを実行することを確認します。

アップグレードを停止する必要がある場合は、 * 停止 * を選択します。実行中のファームウェアのダウンロードは完了します。開始されていないファームウェアのダウンロードはキャンセルされます。

ドライブファームウェアのアップグレードを停止すると、データが失われたり、ドライブを使用できなくなったりする可能性があります。

g. （オプション）アップグレードされた内容のリストを表示するには、 * ログを保存 * を選択します。

ログファイルは、ブラウザのダウンロードフォルダにという名前で保存されます `latest-upgrade-log-timestamp.txt`。

手順のアップグレード中に次のいずれかのエラーが発生した場合は、推奨される対処方法を実行してください。

- * 割り当て済みドライブの障害 *

  エラーの理由の 1 つとして、ドライブに適切な署名がない可能性があります。該当するドライブが認定済みのドライブであることを確認します。詳細については、テクニカルサポートにお問い合わせください。

ドライブを交換する場合は、交換用ドライブの容量が交換する障害ドライブと同じかそれよりも大きいことを確認してください。

障害が発生したドライブの交換は、ストレージアレイで I/O を受信中に実行できます

- * ストレージアレイを確認してください *
  - 各コントローラに IP アドレスが割り当てられていることを確認します。
  - コントローラに接続されているすべてのケーブルが破損していないことを確認します。
  - すべてのケーブルがしっかりと接続されていることを確認します。
- * 内蔵ホットスペアドライブ *

ファームウェアをアップグレードする前に、このエラーを修正する必要があります。

- * 不完全なボリュームグループ *

  1 つ以上のボリュームグループまたはディスクプールが不完全な場合は、ファームウェアをアップグレードする前に、このエラーを修正する必要があります。

- * すべてのボリュームグループで実行中の排他的な処理（バックグラウンドメディア / パリティスキャン以外） *

  1 つ以上の排他的な処理を実行中の場合は、その処理を完了してからファームウェアをアップグレードする必要があります。System Manager で処理の進捗状況を監視します。

- * 見つからないボリューム *

  ファームウェアをアップグレードする前に、ボリュームが見つからない状態を修正する必要があります。

- * いずれかのコントローラが最適以外の状態 *

  いずれかのストレージアレイコントローラを確認する必要があります。ファームウェアをアップグレードする前に、この状態を修正する必要があります。

- * コントローラオブジェクトグラフ間でストレージパーティション情報が一致しません *

  コントローラ上のデータの検証中にエラーが発生しました。この問題を解決するには、テクニカルサポートにお問い合わせください。

- * SPM によるデータベースコントローラの検証が失敗します *

  コントローラでストレージパーティションマッピングデータベースのエラーが発生しました。この問題を解決するには、テクニカルサポートにお問い合わせください。

- * 構成データベースの検証（ストレージアレイのコントローラのバージョンでサポートされている場合） *

  コントローラで構成データベースのエラーが発生しました。この問題を解決するには、テクニカルサポートにお問い合わせください。

- * MEL 関連のチェック *

  この問題を解決するには、テクニカルサポートにお問い合わせください。

- * 過去 7 日間に 10 個を超える DDE 情報または重大 MEL イベントが報告されました *

  この問題を解決するには、テクニカルサポートにお問い合わせください。

- * 過去 7 日間に 2 ページ 2C 重大 MEL イベントが報告されました *

  この問題を解決するには、テクニカルサポートにお問い合わせください。

- * 過去 7 日間に 2 個以上の低下したドライブチャネル重大 MEL イベントが報告されました *

  この問題を解決するには、テクニカルサポートにお問い合わせください。

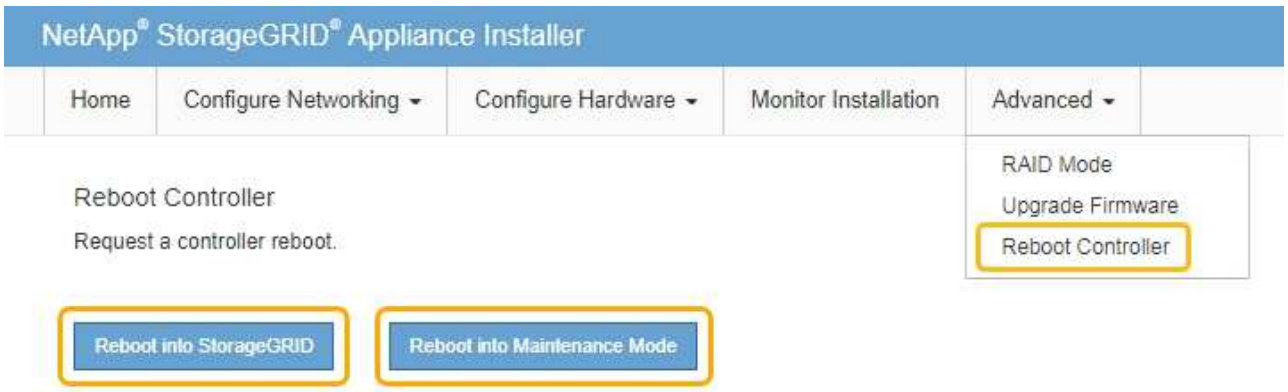
◦ * 過去 7 日間に 4 個を超える重大 MEL エントリがあります *

この問題を解決するには、テクニカルサポートにお問い合わせください。

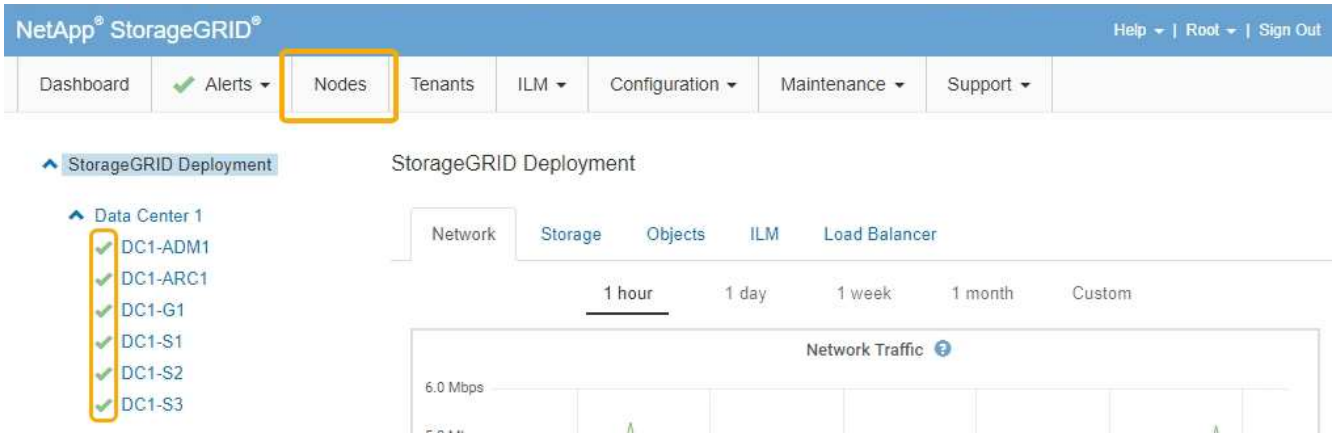
6. アップグレード処理が完了したら、アプライアンスをリブートします。StorageGRID アプライアンス・インストーラから、 **Advanced**>*Reboot Controller* を選択し、次のいずれかのオプションを選択します。

◦ Reboot into StorageGRID * を選択し、ノードをグリッドに再追加してコントローラをリブートします。メンテナンスモードで作業を完了し、ノードを通常動作に戻す準備ができている場合は、このオプションを選択します。

◦ メンテナンスモードを維持したままコントローラをリブートするには、 * Reboot into Maintenance Mode * を選択します。このオプションは、グリッドに再追加する前にノードで追加のメンテナンス処理を実行する必要がある場合に選択しま
す。




アプライアンスがリブートしてグリッドに再参加するまでに最大 20 分かかることがあります。リブートが完了し、ノードが再びグリッドに参加したことを確認するには、 Grid Manager に戻ります。[ノード*（Nodes *）]タブには、通常のステータスが表示されます ✔ アクティブなアラートがなく、ノードがグリッドに接続されていることを示す、アプライアンスノードの場合。




関連情報

"ストレージコントローラのSANtricity OSをアップグレードしています"

# E2800 コントローラが適切に機能しない場合や障害が発生した場合は、交換が必要となることがあります。

このタスクについて

- 交換するコントローラと同じパーツ番号の交換用コントローラを用意しておきます。
- 障害が発生した E2800 コントローラキャニスターのシンプレックス構成を交換するための手順書をダウンロードしておきます。

> E シリーズの手順書は、指示された場合、または特定の手順の詳細を知る必要がある場合にのみ参照してください。StorageGRID アプライアンスのコントローラを交換する際は、E シリーズの手順書を参考にしないでください。手順が異なります。

- コントローラに接続する各ケーブルを識別するためのラベルを用意しておきます。
- すべてのドライブがセキュリティ保護されている場合は、シンプレックス E2800 コントローラ交換手順の手順を確認します。これには、NetApp Support Siteから E シリーズ SANtricity Storage Manager をダウンロードしてインストールし、コントローラの交換後に Enterprise Management Window （ EMW ）を使用してセキュリティ保護されたドライブのロックを解除する作業が含まれます。

> 保存されたキーでドライブのロックを解除するまでは、アプライアンスを使用できません。

- 特定のアクセス権限が必要です。
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

このタスクについて

コントローラキャニスターに障害が発生したかどうかは、次の 2 つの方法で確認できます。

- SANtricity System Manager の Recovery Guru から、コントローラを交換するように指示されます。
- コントローラの黄色の警告 LED が点灯して、コントローラに障害が発生したことが通知されます。

コントローラを交換すると、アプライアンスストレージノードにアクセスできなくなります。E2800コントローラが動作している場合は、E5700SGコントローラをメンテナンスモードにすることができます。

"アプライアンスをメンテナンスモードにします"

コントローラを交換するときは、元のコントローラからバッテリを取り外し、交換用コントローラに取り付ける必要があります。

> アプライアンス内の E2800 コントローラには、ホストインターフェイスカード（ HIC ）は搭載されていません。

手順

1. E2800 コントローラの交換用手順 の手順に従って、コントローラを取り外す準備をします。

   これらの手順を実行するには、 SANtricity System Manager を使用します。

a. コントローラに現在インストールされている SANtricity OS ソフトウェアのバージョンを書き留めます。

b. 現在インストールされている NVSRAM のバージョンを書き留めます。

c. ドライブセキュリティ機能が有効になっている場合は、保存されたキーが存在すること、およびそのインストールに必要なパスフレーズを確認しておきます。

> * データ・アクセスが失われる可能性 - * アプライアンスのすべてのドライブでセキュリティが有効になっている場合、 SANtricity ストレージ・マネージャの [ エンタープライズ管理 ] ウィンドウを使用してセキュリティ保護されたドライブのロックを解除するまで、新しいコントローラはアプライアンスにアクセスできません。

d. 構成データベースをバックアップします。

コントローラを取り外すときに問題が発生した場合は、保存したファイルを使用して構成をリストアできます。

e. アプライアンスのサポートデータを収集します。

> コンポーネントを交換する前後にサポートデータを収集しておけば、交換しても問題が解決しない場合に、テクニカルサポートにすべてのログを送信できます。

2. StorageGRID アプライアンスをStorageGRID システムで実行している場合は、E5700SGコントローラをメンテナンスモードにしてください。

"アプライアンスをメンテナンスモードにします"

3. E2800 コントローラが動作していて通常の方法でシャットダウンできる場合は、すべての処理が完了していることを確認します。

a. SANtricity システムマネージャのホームページで、「 * 進行中の処理を表示」を選択します。

b. すべての処理が完了したことを確認します。

4. コントローラをアプライアンスから取り外します。

a. ESD リストバンドを装着するか、静電気防止処置を施します。

b. ケーブルにラベルを付け、ケーブルと SFP を外します。

> パフォーマンスの低下を防ぐために、ケーブルをねじったり、折り曲げたり、はさんだり、踏みつけたりしないでください。

c. カムハンドルのラッチを押してコントローラをアプライアンスから外し、カムハンドルを右側に開きます。

d. 両手でカムハンドルをつかみ、コントローラをスライドしてアプライアンスから引き出します。

> コントローラは重いので、必ず両手で支えながら作業してください。

e. 取り外し可能なカバーを上にして、静電気防止処置を施した平らな場所にコントローラを置きます。

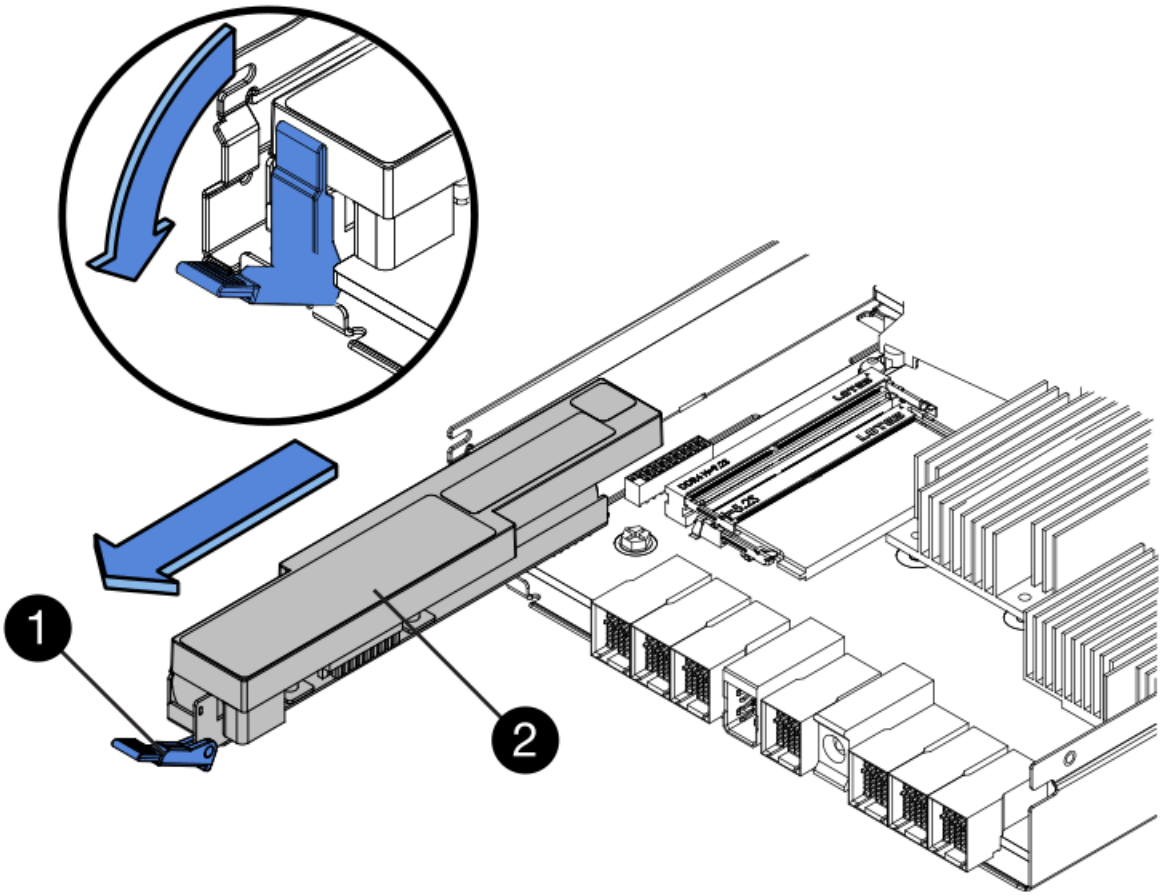
f. カバーをボタンを押し下げながらスライドして取り外します。

5. 障害が発生したコントローラからバッテリを取り外し、交換用コントローラに取り付けます。
   a. コントローラ内部（バッテリと DIMM の間）の緑の LED が消灯していることを確認します。

      この緑の LED が点灯している場合は、コントローラがまだバッテリ電源を使用しています。この LED が消灯するのを待ってから、コンポーネントを取り外す必要があります。

| 項目 | 説明 |
| --- | --- |
| | 内部キャッシュアクティブ LED |
| | バッテリー |

   b. バッテリの青色のリリースラッチの位置を確認します。
   c. バッテリをリリースラッチを押し下げながら引き出し、コントローラから外します。




| 項目 | 説明 |
| --- | --- |
| | バッテリのリリースラッチ |
| | バッテリー |

d. バッテリを持ち上げながらスライドし、コントローラから引き出します。

e. 交換用コントローラのカバーを取り外します。

f. バッテリのスロットが手前になるよう交換用コントローラの向きを変えます。

g. バッテリを少し下に傾けながらコントローラに挿入します。

   バッテリ前部の金属製のフランジをコントローラ下部のスロットに挿入し、バッテリの上部がコントローラの左側にある小さな位置決めピンの下にくるまでスライドする必要があります。

h. バッテリラッチを上に動かしてバッテリを固定します。

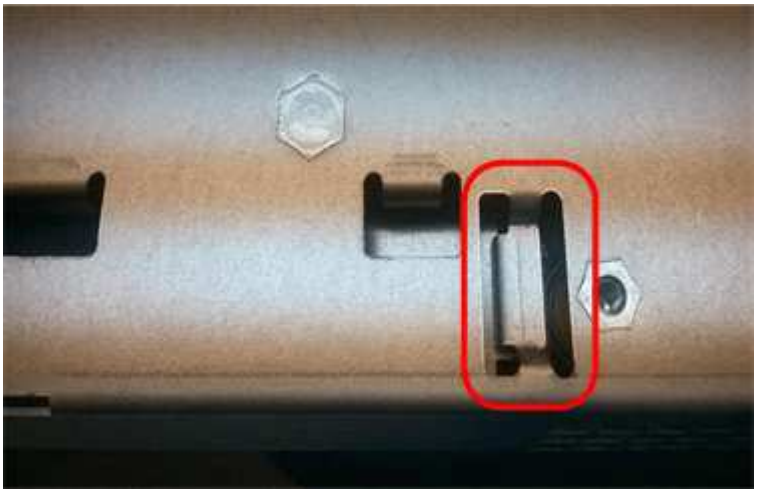
   カチッという音がしてラッチが固定されると、ラッチの下部がシャーシの金属製のスロットに収まります。

i. コントローラを裏返し、バッテリが正しく取り付けられていることを確認します。

> * ハードウェアの破損の可能性 * - バッテリ前部の金属製のフランジがコントローラのスロットにしっかりと挿入されている必要があります（ 1 つ目の図）。バッテリが正しく取り付けられていないと（ 2 つ目の図）、金属製のフランジがコントローラボードに接触し、破損の原因となる可能性があります。

- * 正解 — バッテリの金属製のフランジがコントローラのスロットに完全に挿入されています *

- * 不正解 — バッテリの金属製のフランジがコントローラのスロットに挿入されていません *



j. コントローラカバーを取り付けます。

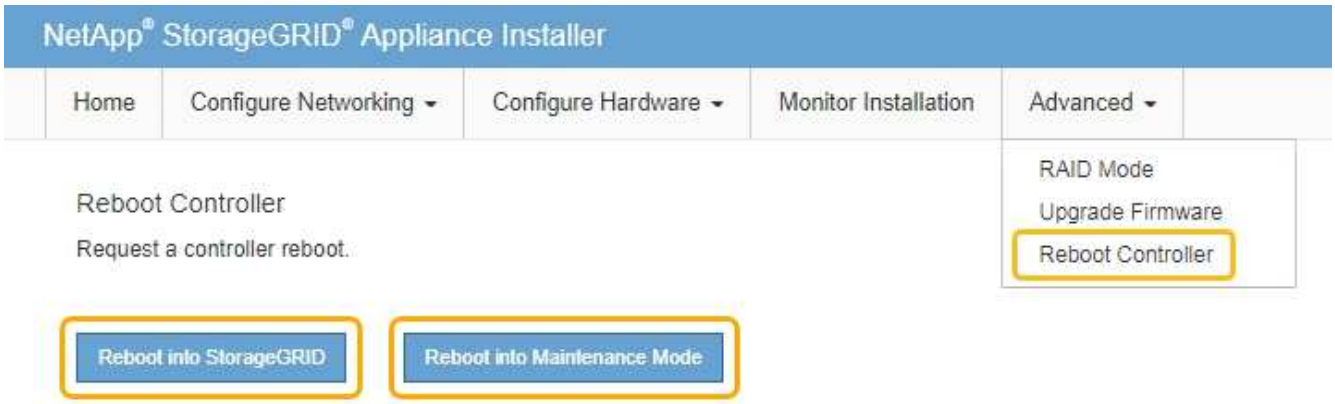
6. 交換用コントローラをアプライアンスに取り付けます。
   a. 取り外し可能なカバーが下になるようにコントローラを裏返します。
   b. カムハンドルを開いた状態でコントローラをスライドし、アプライアンスに最後まで挿入します。
   c. カムハンドルを左側に動かして、コントローラを所定の位置にロックします。
   d. ケーブルと SFP を交換します。
   e. E2800 コントローラがリブートするまで待ちます。デジタル表示ディスプレイの状態がになっていることを確認します `99`。

f. 交換用コントローラに IP アドレスを割り当てる方法を決定します。

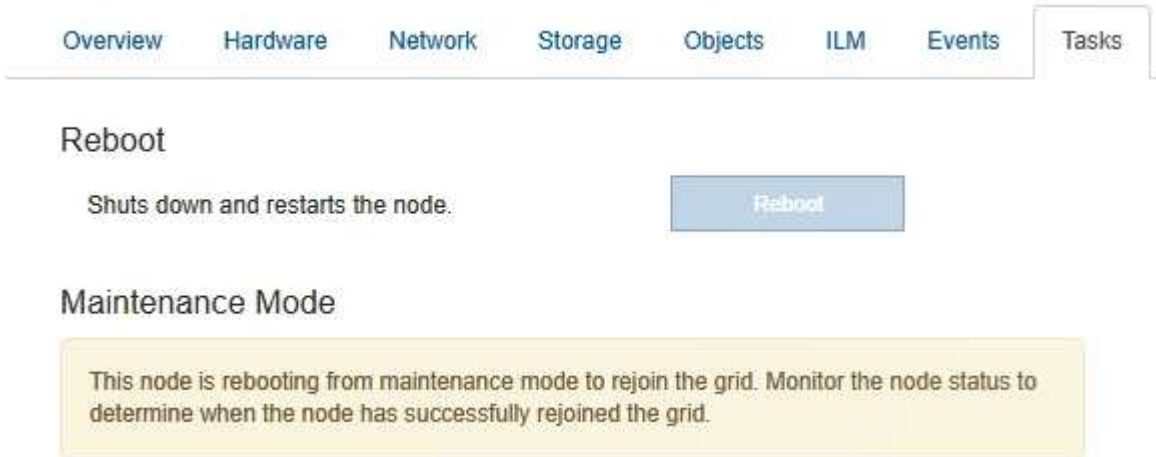
交換用コントローラに IP アドレスを割り当てる手順は、管理ポート 1 を接続したネットワークに DHCP サーバがあるかどうか、またすべてのドライブがセキュリティ保護されているかどうかによって異なります。

- 管理ポート 1 が DHCP サーバがあるネットワークに接続されている場合は、新しいコントローラの IP アドレスが DHCP サーバから取得されます。この値は、元のコントローラの IP アドレスと異なる場合があります。
- すべてのドライブがセキュリティ保護されている場合は、 SANtricity Storage Manager の Enterprise Management Window （ EMW ）を使用して、セキュリティ保護されたドライブのロックを解除する必要があります。保存されたキーでドライブのロックを解除するまでは、新しいコントローラにアクセスできません。シンプレックス E2800 コントローラの交換については、 E シリーズの手順書を参照してください。

7. アプライアンスで使用されるドライブがセキュリティ保護されている場合は、 E2800 コントローラの交換用手順 の手順に従ってドライブセキュリティキーをインポートします。
8. アプライアンスを通常の動作モードに戻します。StorageGRID アプライアンス・インストーラから、**Advanced**>* Reboot Controller* を選択し、 * Reboot into StorageGRID * を選択します。

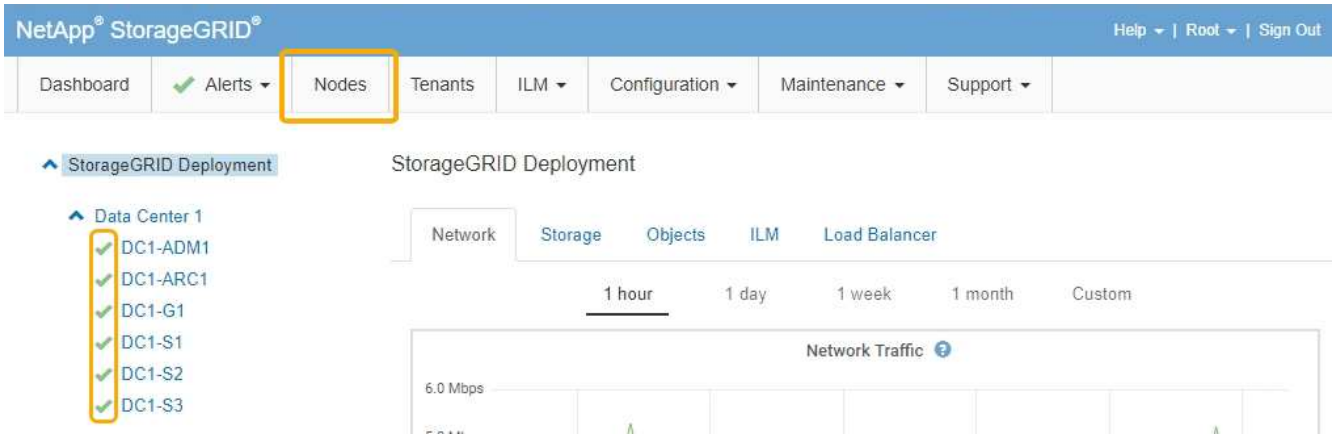



リブート中、次の画面が表示されます。



アプライアンスがリブートし、グリッドに再度参加します。この処理には最大 20 分かかることがあります。

9. リブートが完了し、ノードが再びグリッドに参加したことを確認します。Grid Managerで、* Nodes *タブに正常なステータスが表示されることを確認します ✔ アクティブなアラートがなく、ノードがグリッドに接続されていることを示す、アプライアンスノードの場合。




10. SANtricity System Manager で、新しいコントローラのステータスが「 Optimal 」であることを確認し、サポートデータを収集します。

関連情報

"NetApp E シリーズシステムのドキュメントのサイト"

**E5700SG**コントローラの交換

## E5700SG コントローラが適切に機能しない場合や障害が発生した場合は、交換が必要となることがあります。

必要なもの

- 交換するコントローラと同じパーツ番号の交換用コントローラを用意しておきます。
- 障害が発生した E5700 コントローラを交換するための E シリーズの手順書をダウンロードしておきます。

> E シリーズの手順書は、特定の手順の詳細を知る必要がある場合のみ参照してください。StorageGRID アプライアンスのコントローラを交換する際は、 E シリーズの手順書を参考にしないでください。手順が異なります。たとえば、 E5700 コントローラ向けの E シリーズの手順書では、障害が発生したコントローラからバッテリとホストインターフェイスカード（ HIC ）を取り外して交換用コントローラに取り付ける方法が説明されています。以下の手順は E5700SG コントローラには適用されません。

- コントローラに接続する各ケーブルを識別するためのラベルを用意しておきます。
- アプライアンスのメンテナンスモードが開始されました。

  "アプライアンスをメンテナンスモードにします"

このタスクについて

コントローラを交換すると、アプライアンスストレージノードにアクセスできなくなります。E5700SG コン

トローラが動作している場合は、この手順 の起動時に通常の方法でシャットダウンを実行してください。

> StorageGRID ソフトウェアをインストールする前にコントローラを交換すると、この手順 の完了後すぐに StorageGRID アプライアンスインストーラにアクセスできない場合があります。アプライアンスと同じサブネット上の他のホストから StorageGRID アプライアンスインストーラにアクセスすることはできますが、他のサブネット上のホストからはアクセスできません。この状態は 15 分以内に（元のコントローラのいずれかの ARP キャッシュエントリがタイムアウトした時点で）自動的に解消されます。あるいは、古い ARP キャッシュエントリをローカルルータまたはゲートウェイから手動でパージすれば、すぐにこの状態を解消できます。

手順

1. アプライアンスをメンテナンスモードにしたら、 E5700SG コントローラをシャットダウンしてください。
   a. グリッドノードにログインします。
      i. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
      ii. に記載されているパスワードを入力します `Passwords.txt` ファイル。
      iii. 次のコマンドを入力してrootに切り替えます。 `su -`
      iv. に記載されているパスワードを入力します `Passwords.txt` ファイル。

      rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。
   b. E5700SGコントローラのをシャットダウンしてください：+
      **`shutdown -h now`**
   c. キャッシュメモリ内のデータがドライブに書き込まれるまで待ちます。

      キャッシュされたデータをドライブに書き込む必要がある場合は、 E2800 コントローラの背面にある緑のキャッシュアクティブ LED が点灯します。この LED が消灯するまで待つ必要があります。
2. 電源をオフにします。
   a. SANtricity システムマネージャのホームページで、「 * 進行中の処理を表示」を選択します。
   b. すべての処理が完了したことを確認します。
   c. アプライアンスの両方の電源スイッチをオフにします。
   d. すべての LED が消灯するまで待ちます。
3. コントローラに接続されている StorageGRID ネットワークが DHCP サーバを使用している場合は、次の作業を行い
   a. 交換用コントローラのポートの MAC アドレス（コントローラのラベルに記載）を書き留めます。
   b. ネットワーク管理者に元のコントローラの IP アドレス設定を更新するよう依頼して、交換用コントローラの MAC アドレスを反映させます。

> 交換用コントローラに電源を投入する前に、元のコントローラの IP アドレスが更新されたことを確認する必要があります。そうしないと、コントローラのブート時に新しい DHCP IP アドレスが取得されて、 StorageGRID に再接続できなくなることがあります。この手順では、コントローラに接続されているすべての StorageGRID ネットワークを環境 接続します。

4. コントローラをアプライアンスから取り外します。
   a. ESD リストバンドを装着するか、静電気防止処置を施します。
   b. ケーブルにラベルを付け、ケーブルと SFP を外します。

      パフォーマンスの低下を防ぐために、ケーブルをねじったり、折り曲げたり、はさんだり、踏みつけたりしないでください。

   c. カムハンドルのラッチを押してコントローラをアプライアンスから外し、カムハンドルを右側に開きます。
   d. 両手でカムハンドルをつかみ、コントローラをスライドしてアプライアンスから引き出します。

      コントローラは重いので、必ず両手で支えながら作業してください。

5. 交換用コントローラをアプライアンスに取り付けます。
   a. 取り外し可能なカバーが下になるようにコントローラを裏返します。
   b. カムハンドルを開いた状態でコントローラをスライドし、アプライアンスに最後まで挿入します。
   c. カムハンドルを左側に動かして、コントローラを所定の位置にロックします。
   d. ケーブルと SFP を交換します。
6. アプライアンスの電源を入れ、コントローラの LED とデジタル表示ディスプレイを監視します。

   コントローラが正常にブートされると、デジタル表示ディスプレイに次のコードが表示されます。

   - E2800 コントローラ：

     最後の状態はです `99`。

   - E5700SG コントローラ：

     最後の状態はです `HA`。

7. アプライアンスストレージノードが Grid Manager に表示され、アラームが表示されていないことを確認します。

関連情報

"NetApp E シリーズシステムのドキュメントのサイト"

その他のハードウェアコンポーネントの交換

## StorageGRID アプライアンスのコントローラバッテリ、ドライブ、ファン、または電源装置の交換が必要になることがあります。

必要なもの

- E シリーズハードウェアの交換用手順 を用意しておきます。
- コンポーネントの交換用手順 でアプライアンスをシャットダウンする必要がある場合は、アプライアンスをメンテナンスモードにしておきます。

"アプライアンスをメンテナンスモードにします"

このタスクについて

E2800 コントローラのバッテリを交換する場合は、 E2800 コントローラの交換手順の説明を参照してください。これらの手順では、アプライアンスからのコントローラの取り外し、コントローラからのバッテリの取り外し、バッテリの取り付け、およびコントローラの交換の方法について説明します。

アプライアンスのドライブ、電源 / ファンキャニスター、ファンキャニスター、電源キャニスター、またはドライブドロワーを交換する場合は、 E2800 ハードウェアのメンテナンスに関する E シリーズの手順書を参照してください。

**SG5712** コンポーネントの交換手順

| **FRU** | については、 **E** シリーズの手順書を参照してください |
|---|---|
| ドライブ | E2800 12 ドライブまたは 24 ドライブシェルフのドライブの交換 |
| 電源 / ファンキャニスター | E2800 シェルフの電源 / ファンキャニスターの交換 |

**SG5760** のコンポーネントの交換手順

| **FRU** | については、 **E** シリーズの手順書を参照してください |
|---|---|
| ドライブ | E2860 シェルフのドライブの交換 |
| 電源キャニスター | E2860 シェルフの電源キャニスターの交換 |
| ファンキャニスター | E2860 シェルフのファンキャニスターの交換 |
| ドライブドロワー | E2860 シェルフのドライブドロワーの交換 |

関連情報

"E2800コントローラの交換"

"NetApp E シリーズシステムのドキュメントのサイト"

**E5700SG**コントローラのリンク設定の変更

E5700SG コントローラのイーサネットリンク設定を変更できます。ポートボンディングモード、ネットワークボンディングモード、およびリンク速度を変更できます。

必要なもの

E5700SGコントローラをメンテナンスモードにする必要があります。StorageGRID アプライアンスをメンテナンスモードにすると、アプライアンスにリモートアクセスできなくなることがあります。

"アプライアンスをメンテナンスモードにします"

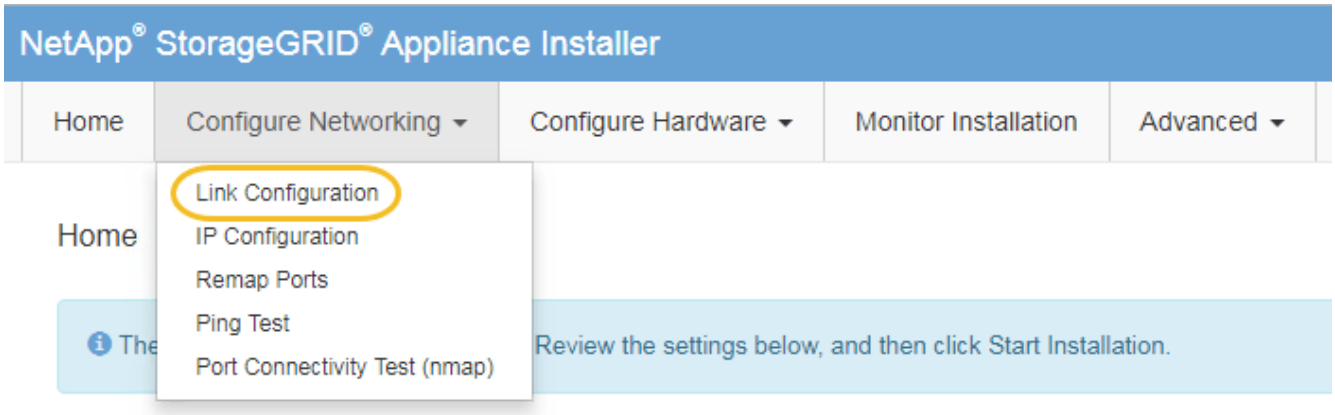
このタスクについて

E5700SG コントローラのイーサネットリンク設定を変更するためのオプションは次のとおりです。

- ポートボンディングモード * を「 Fixed 」から「 Aggregate 」または「 Aggregate 」から「 Fixed 」に変更します
- ネットワークボンディングモード * を Active-Backup から LACP に、または LACP から Active-Backup に変更
- VLAN タグを有効または無効にするか、 VLAN タグの値を変更します
- リンク速度を 10GbE から 25GbE に、または 25GbE から 10GbE に変更する

手順

1. メニューから * Configure Networking * > * Link Configuration * を選択します。




1. リンク設定に必要な変更を加えます。

   オプションの詳細については、「ネットワークリンクの設定」を参照してください。

2. 選択に問題がなければ、 * 保存 * をクリックします。

   接続しているネットワークまたはリンクを変更すると、接続が失われる可能性があります。1分以内に再接続されない場合は、アプライアンスに割り当てられている他のIPアドレスのいずれかを使用してStorageGRID アプライアンスインストーラのURLを再入力します：+
   **`https://E5700SG_Controller_IP:8443`**

   VLAN 設定を変更した場合は、アプライアンスのサブネットが変更されている可能性があります。アプライアンスのIPアドレスを変更する必要がある場合は、IPアドレスの設定手順に従います。

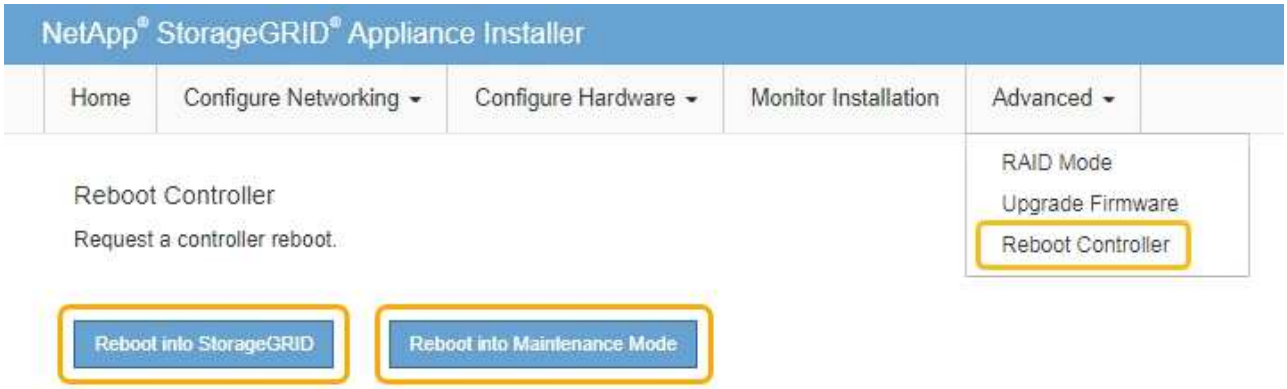
   "IPの設定"

3. StorageGRID アプライアンスインストーラから、 **Configure Networking**>*Ping Test* を選択します。
4. ping テストツールを使用して、で行ったリンク設定の変更によって影響を受けた可能性のあるネットワーク上の IP アドレスへの接続を確認します リンク設定を変更します ステップ。

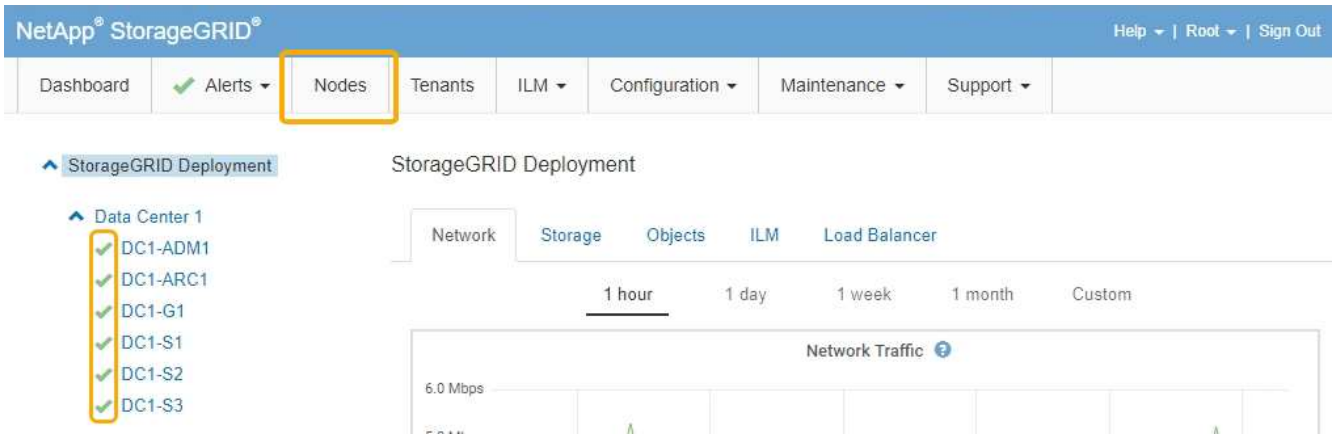
最低でもプライマリ管理ノードのグリッド IP アドレスと、 1 つ以上の他のストレージノードのグリッド IP アドレスについて、 ping が通ることを確認します。必要に応じて、リンク設定の問題を修正します。

5. リンク設定の変更が問題なく機能していることを確認したら、ノードをリブートします。StorageGRID アプライアンス・インストーラから、 **Advanced**>*Reboot Controller* を選択し、次のいずれかのオプションを選択します。

   - Reboot into StorageGRID * を選択し、ノードをグリッドに再追加してコントローラをリブートします。メンテナンスモードで作業を完了し、ノードを通常動作に戻す準備ができている場合は、このオプションを選択します。
   - メンテナンスモードを維持したままコントローラをリブートするには、 * Reboot into Maintenance Mode * を選択します。このオプションは、グリッドに再追加する前にノードで追加のメンテナンス処理を実行する必要がある場合に選択しま
     す。




   アプライアンスがリブートしてグリッドに再参加するまでに最大 20 分かかることがあります。リブートが完了し、ノードが再びグリッドに参加したことを確認するには、 Grid Manager に戻ります。[ノード*（Nodes *）]タブには、通常のステータスが表示されます ✔ アクティブなアラートがなく、ノードがグリッドに接続されていることを示す、アプライアンスノードの場合。




関連情報

"ネットワークリンクの設定（SG5700）"

**MTU**設定を変更します

# アプライアンスノードの IP アドレスを設定するときに割り当てた MTU 設定を変更できます。

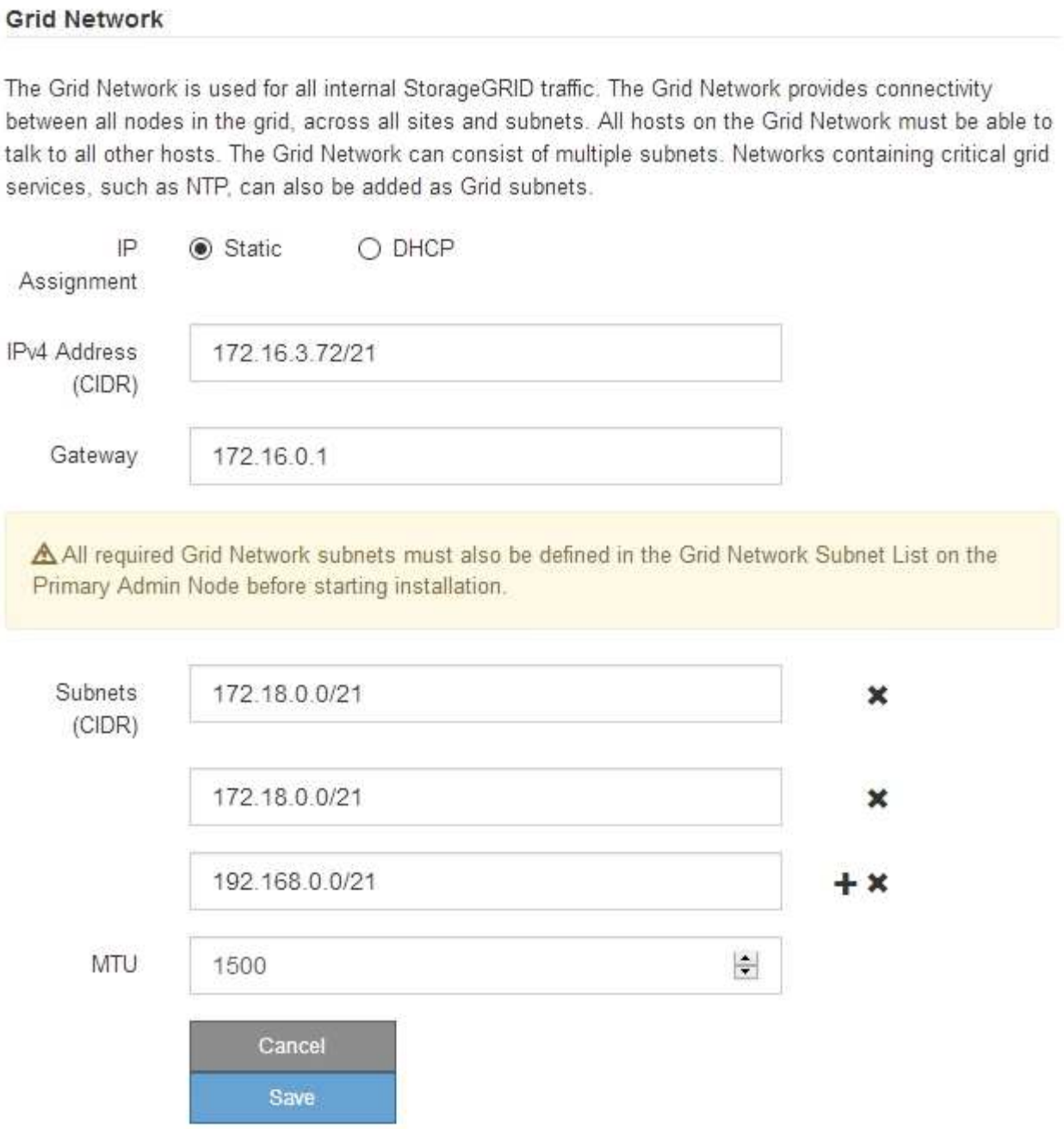
必要なもの

アプライアンスのメンテナンスモードが開始されました。

"アプライアンスをメンテナンスモードにします"

手順

1. StorageGRID アプライアンスインストーラから、 **Configure Networking**>*IP Configuration* を選択します。
2. グリッドネットワーク、管理ネットワーク、およびクライアントネットワークの MTU 設定に必要な変更を加えます。



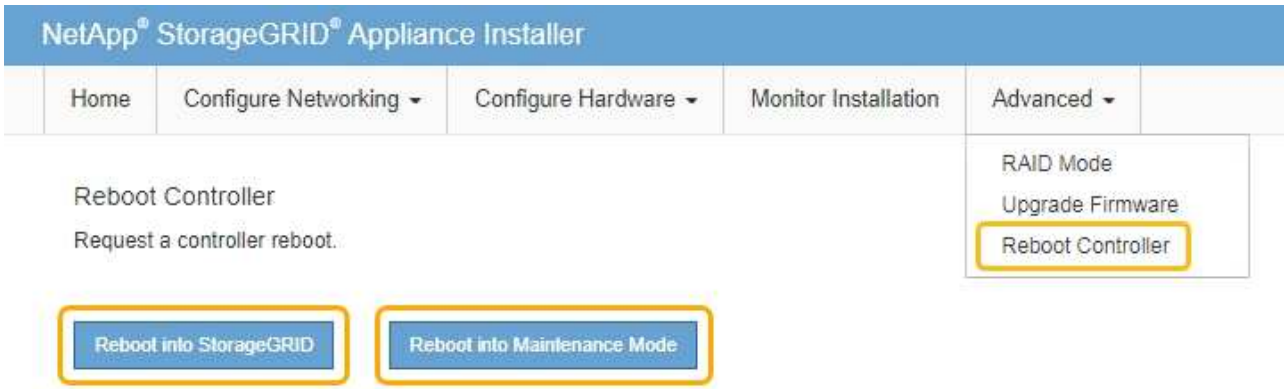

ネットワークの MTU 値は、ノードが接続されているスイッチポートに設定されている値と同じである必要があります。そうしないと、ネットワークパフォーマンスの問題やパケット損失が発生する可能性があります。

ネットワークのパフォーマンスを最大限に高めるには、すべてのノードのグリッドネットワークインターフェイスで MTU 値がほぼ同じになるように設定する必要があります。個々のノードのグリッドネットワークの MTU 設定に大きな違いがある場合は、 * Grid Network MTU mismatch * アラートがトリガーされます。MTU 値はすべてのネットワークタイプで同じである必要はありません。

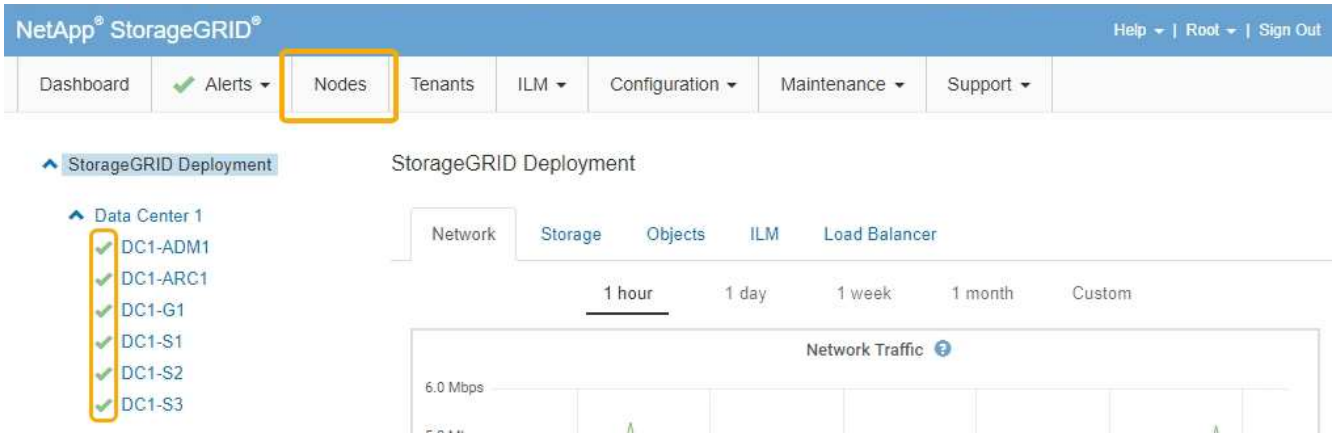
3. 設定に問題がなければ、「 * 保存 * 」を選択します。
4. ノードをリブートします。StorageGRID アプライアンス・インストーラから、 **Advanced**>*Reboot

Controller* を選択し、次のいずれかのオプションを選択します。

- Reboot into StorageGRID * を選択し、ノードをグリッドに再追加してコントローラをリブートします。メンテナンスモードで作業を完了し、ノードを通常動作に戻す準備ができている場合は、このオプションを選択します。
- メンテナンスモードを維持したままコントローラをリブートするには、 * Reboot into Maintenance Mode * を選択します。このオプションは、グリッドに再追加する前にノードで追加のメンテナンス処理を実行する必要がある場合に選択しま
す。




アプライアンスがリブートしてグリッドに再参加するまでに最大 20 分かかることがあります。リブートが完了し、ノードが再びグリッドに参加したことを確認するには、 Grid Manager に戻ります。[ノード*（Nodes *）]タブには、通常のステータスが表示されます ✔ アクティブなアラートがなく、ノードがグリッドに接続されていることを示す、アプライアンスノードの場合。




関連情報

"StorageGRID の管理"

**DNS**サーバの設定を確認しています

## このアプライアンスノードで現在使用されているドメインネームシステム（ DNS ）サーバを確認し、一時的に変更することができます。

必要なもの

アプライアンスのメンテナンスモードが開始されました。

"アプライアンスをメンテナンスモードにします"

このタスクについて

KMS のホスト名は IP アドレスではなくドメイン名として指定されているため、暗号化されたアプライアンスがキー管理サーバ（ KMS ）または KMS クラスタに接続できない場合は、 DNS サーバ設定の変更が必要になることがあります。アプライアンスの DNS 設定に加えた変更は一時的なものであり、メンテナンスモードを終了すると失われます。これらの変更を永続的に行うには、Grid ManagerでDNSサーバを指定します（* Maintenance > Network > DNS Servers *）。

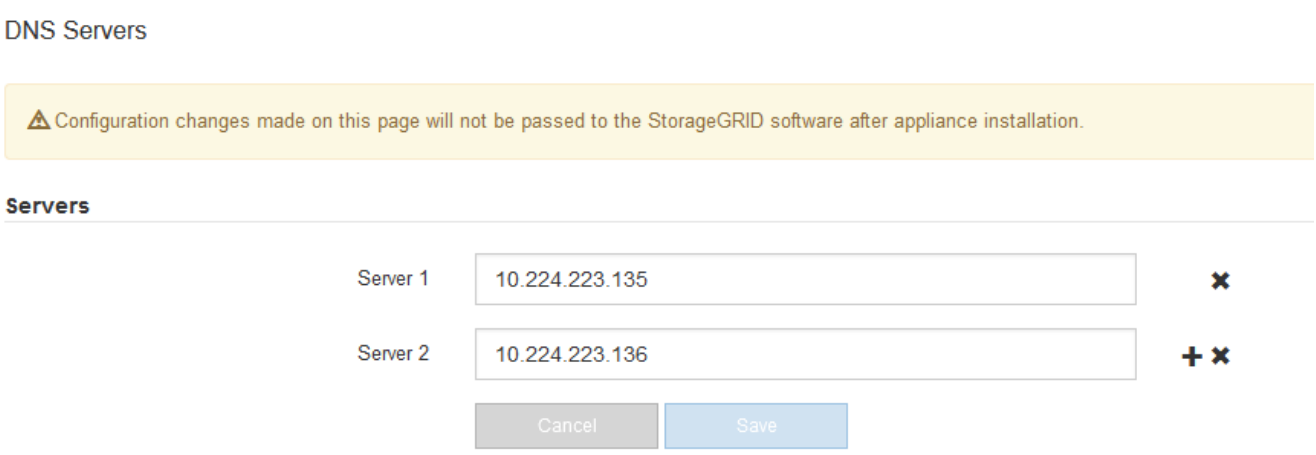
- DNS 設定の一時的な変更が必要になるのは、ホスト名に IP アドレスではなく完全修飾ドメイン名を使用して KMS サーバが定義されているノード暗号化アプライアンスのみです。
- ノード暗号化アプライアンスをドメイン名を使用して KMS に接続する場合は、グリッド用に定義されている DNS サーバの 1 つに接続する必要があります。これらの DNS サーバの 1 つが、ドメイン名を IP アドレスに変換します。
- ノードがグリッドの DNS サーバにアクセスできない場合、またはノード暗号化アプライアンスノードがオフラインのときにグリッド全体の DNS 設定を変更した場合は、ノードは KMS に接続できません。アプライアンス上の暗号化されたデータは、 DNS 問題 が解決されるまで復号化できません。

KMS 接続を回避する DNS 問題 を解決するには、 StorageGRID アプライアンスインストーラで 1 つ以上の DNS サーバの IP アドレスを指定します。この一時的な DNS 設定により、アプライアンスは KMS に接続してノード上のデータを復号化することができます。

たとえば、暗号化されたノードがオフラインのときにグリッドの DNS サーバが変更された場合、ノードは以前の DNS 値をまだ使用しているため、オンラインに戻った時点で KMS にアクセスできなくなります。StorageGRID アプライアンスインストーラで新しい DNS サーバの IP アドレスを入力すると、 KMS 接続を使用してノードのデータを復号化できます。

手順

1. StorageGRID アプライアンスインストーラから、 **Configure Networking *>*DNS Configuration** を選択します。
2. 指定した DNS サーバが正しいことを確認してください。




3. 必要に応じて、 DNS サーバを変更します。

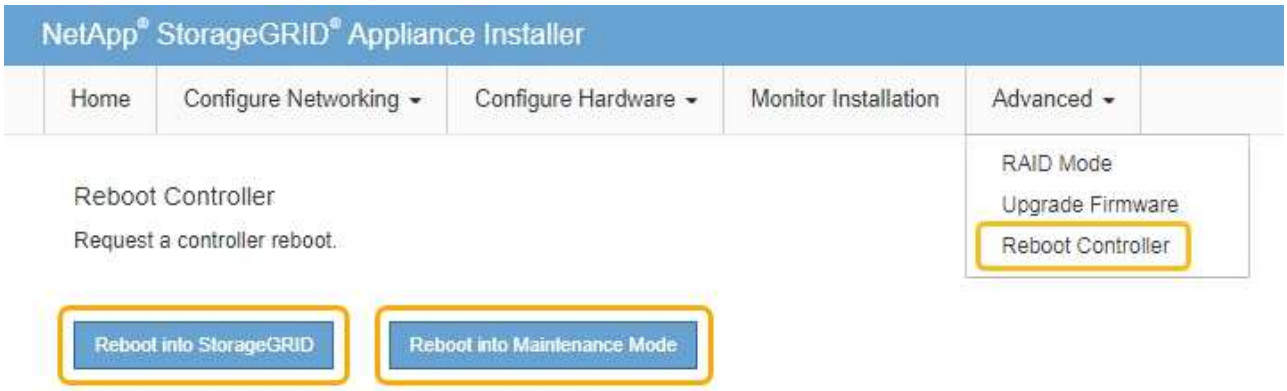
DNS 設定に対する変更は一時的なものであり、メンテナンスモードを終了すると失われます。

4. 一時的な DNS 設定に問題がなければ、 * 保存 * を選択します。

   ノードは、このページで指定されている DNS サーバ設定を使用して KMS に再接続し、ノード上のデータを復号化できるようにします。

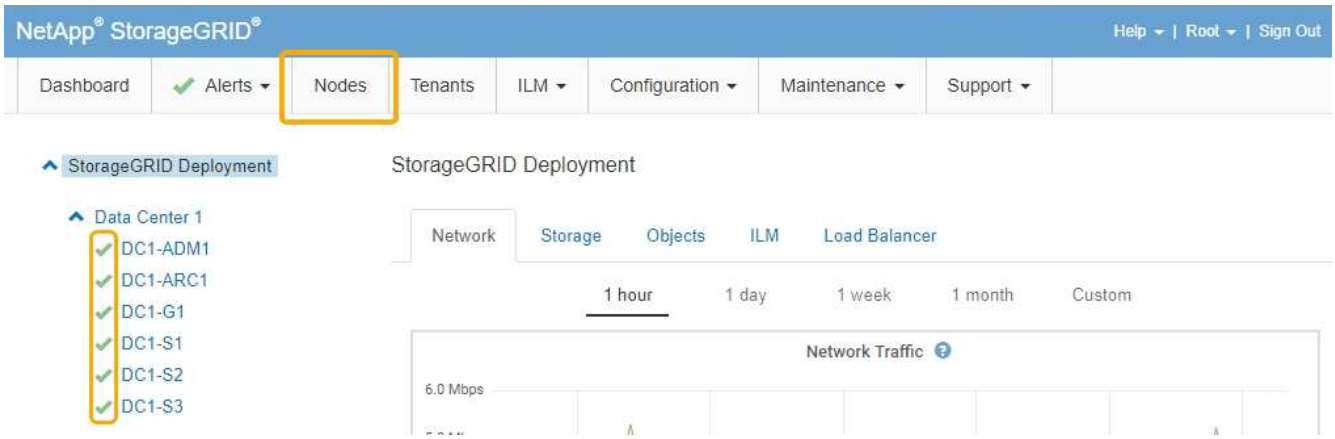
5. ノードデータが復号化されたら、ノードをリブートします。StorageGRID アプライアンス・インストーラから、 **Advanced**>*Reboot Controller* を選択し、次のいずれかのオプションを選択します。

   - Reboot into StorageGRID * を選択し、ノードをグリッドに再追加してコントローラをリブートします。メンテナンスモードで作業を完了し、ノードを通常動作に戻す準備ができている場合は、このオプションを選択します。
   - メンテナンスモードを維持したままコントローラをリブートするには、 * Reboot into Maintenance Mode * を選択します。このオプションは、グリッドに再追加する前にノードで追加のメンテナンス処理を実行する必要がある場合に選択します。




ノードがリブートしてグリッドに再び参加すると、 Grid Manager にリストされているシステム全体の DNS サーバが使用されます。グリッドに再追加したあとは、アプライアンスがメンテナンスモードのときに、 StorageGRID アプライアンスインストーラで指定された一時的な DNS サーバがアプライアンスで使用されなくなります。

アプライアンスがリブートしてグリッドに再参加するまでに最大 20 分かかることがあります。リブートが完了し、ノードが再びグリッドに参加したことを確認するには、 Grid Manager に戻ります。[ノード*（Nodes *）]タブには、通常のステータスが表示されます アクティブなアラートがなく、ノードがグリッドに接続されていることを示す、アプライアンスノードの場合。




メンテナンスモードでのノード暗号化の監視

# インストール中にアプライアンスのノード暗号化を有効にした場合は、ノード暗号化の状態やキー管理サーバ（ KMS ）の詳細など、各アプライアンスノードのノード暗号化ステータスを監視できます。

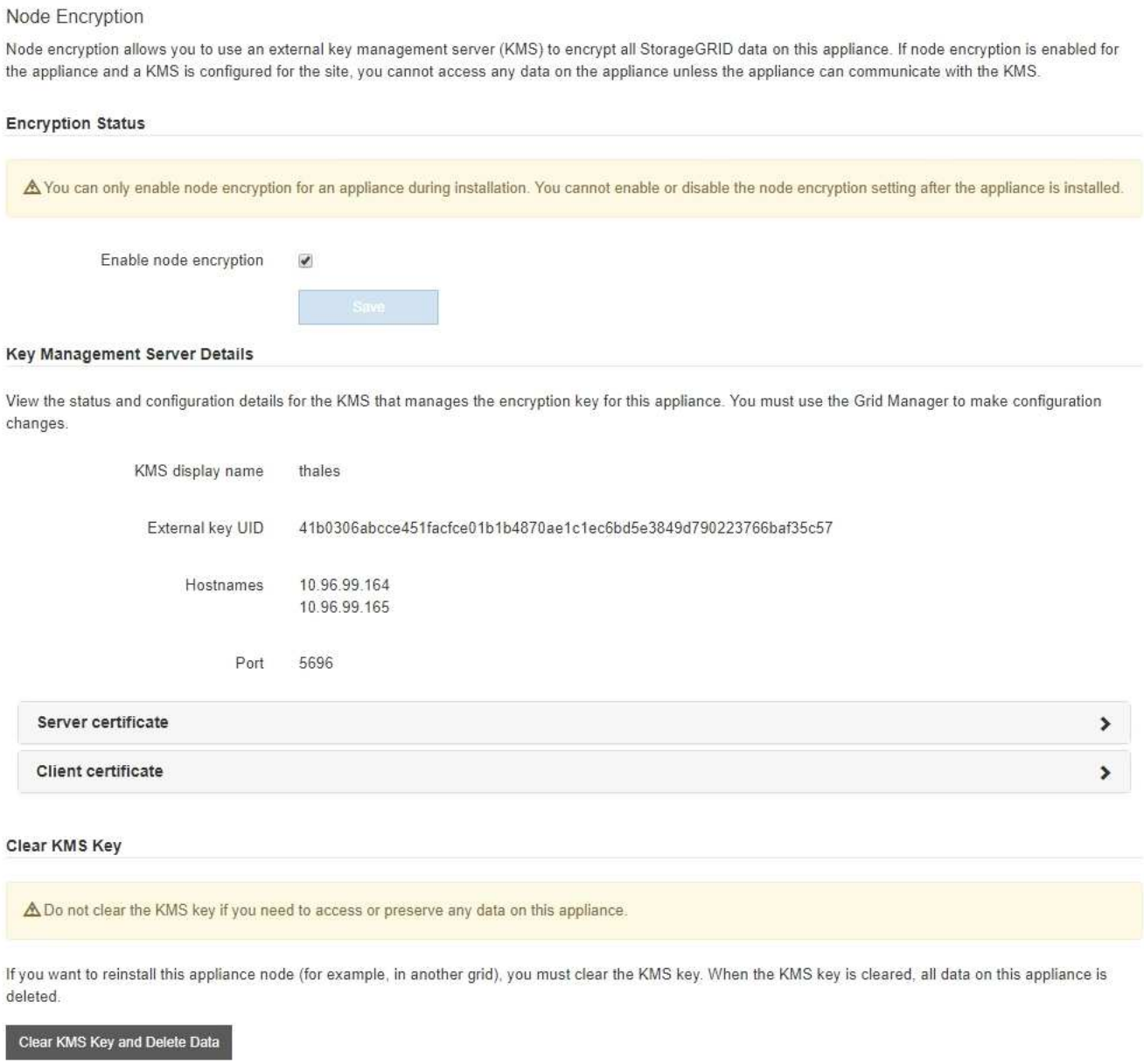
必要なもの

- インストール時にアプライアンスのノード暗号化を有効にしておく必要があります。アプライアンスのインストール後にノード暗号化を有効にすることはできません。
- アプライアンスはメンテナンスモードになりました。

  "アプライアンスをメンテナンスモードにします"

手順

1. StorageGRID アプライアンスインストーラから、 * ハードウェアの設定 * > * ノード暗号化 * を選択します。




Node Encryption のページには次の 3 つのセクションがあります。

- Encryption Status には、アプライアンスでノード暗号化が有効か無効かが表示されます。
- キー管理サーバの詳細には、アプライアンスの暗号化に使用されている KMS に関する情報が表示されます。サーバおよびクライアント証明書のセクションを展開すると、証明書の詳細およびステータスを表示できます。
  - 期限切れの証明書の更新など、証明書自体に関する問題に対処するには、 StorageGRID の管理手順の KMS に関する情報を参照してください。
  - KMS ホストへの接続で予期しない問題が発生する場合は、ドメインネームシステム（ DNS ）サーバが正しいこと、およびアプライアンスのネットワークが正しく設定されていることを確認してください。

    "DNSサーバの設定を確認しています"

  - 証明書の問題を解決できない場合は、テクニカルサポートにお問い合わせください。

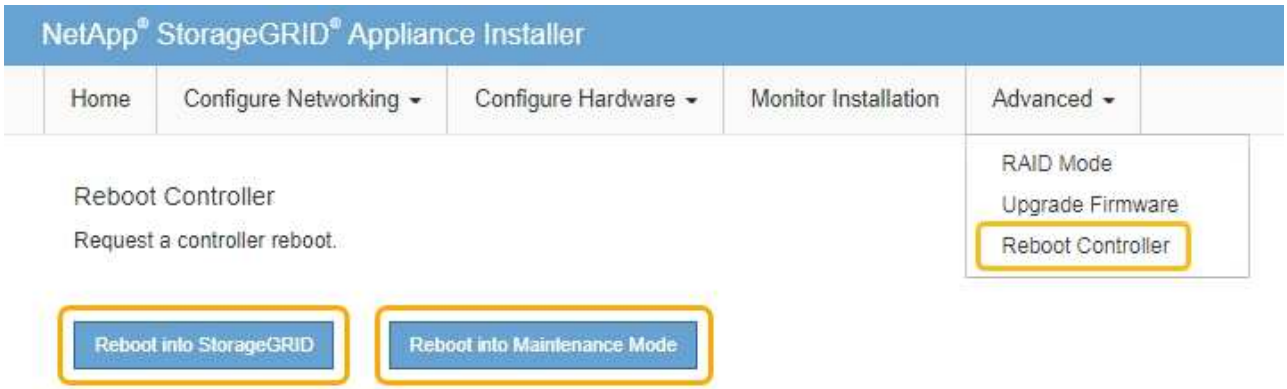
- KMS Key をクリアすると、アプライアンスのノード暗号化が無効になり、 StorageGRID サイト用に設定されているアプライアンスとキー管理サーバの間の関連付けが解除され、アプライアンスのすべてのデータが削除されます。別の StorageGRID システムにアプライアンスをインストールする前に、KMS キーをクリアする必要があります。

  "キー管理サーバ設定のクリア"

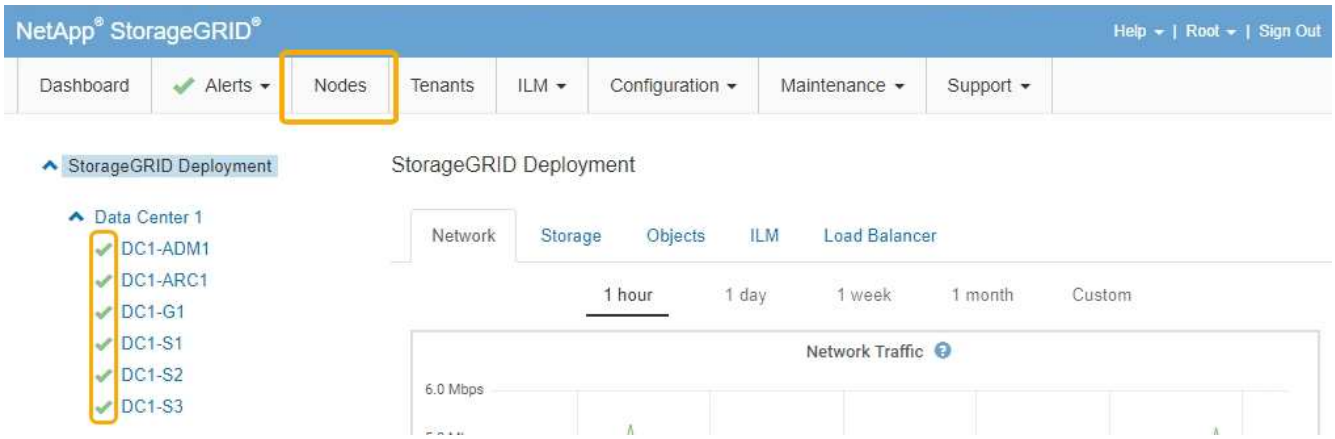
  KMS の設定をクリアすると、アプライアンスからデータが削除され、永久にアクセスできなくなります。このデータはリカバリできません。

2. ノード暗号化ステータスの確認が完了したら、ノードをリブートします。StorageGRID アプライアンス・インストーラから、 **Advanced**>*Reboot Controller* を選択し、次のいずれかのオプションを選択します。

   - Reboot into StorageGRID * を選択し、ノードをグリッドに再追加してコントローラをリブートします。メンテナンスモードで作業を完了し、ノードを通常動作に戻す準備ができている場合は、このオプションを選択します。
   - メンテナンスモードを維持したままコントローラをリブートするには、 * Reboot into Maintenance Mode * を選択します。このオプションは、グリッドに再追加する前にノードで追加のメンテナンス処理を実行する必要がある場合に選択します。




アプライアンスがリブートしてグリッドに再参加するまでに最大 20 分かかることがあります。リブートが完了し、ノードが再びグリッドに参加したことを確認するには、 Grid Manager に戻ります。[ノード*（Nodes *）]タブには、通常のステータスが表示されます ✔ アクティブなアラートがなく、ノードがグリッドに接続されていることを示す、アプライアンスノードの場合。




関連情報

"StorageGRID の管理"

キー管理サーバ設定のクリア

# キー管理サーバ（ KMS ）の設定をクリアすると、アプライアンスでノード暗号化が無効になります。KMS の設定をクリアすると、アプライアンスのデータは完全に削除され、アクセスできなくなります。このデータはリカバリできません。

必要なもの

アプライアンス上のデータを保持する必要がある場合は、KMSの設定をクリアする前に、ノードの運用停止手順 を実行する必要があります。

KMS をクリアすると、アプライアンスのデータが完全に削除され、アクセスできなくなります。このデータはリカバリできません。

ノードを運用停止して、格納されているデータをStorageGRID 内の他のノードに移動します。グリッドノードの運用停止手順については、リカバリとメンテナンスの手順を参照してください。

このタスクについて

アプライアンス KMS の設定をクリアすると、ノード暗号化が無効になり、アプライアンスノードと StorageGRID サイトの KMS の設定との間の関連付けが解除されます。その後、アプライアンスのデータが削除され、アプライアンスはインストール前の状態のままになります。このプロセスを元に戻すことはできません。

KMS の設定をクリアする必要があります。

- アプライアンスを別の StorageGRID システムにインストールする前に、 KMS を使用しない、または別の KMS を使用する前に、

  同じ KMS キーを使用する StorageGRID システムにアプライアンスノードを再インストールする場合は、 KMS の設定をクリアしないでください。

- KMS 設定が失われて KMS キーをリカバリおよび再インストールできないノードをリカバリする前に、 KMS キーをリカバリできません。
- お客様のサイトで以前使用していたアプライアンスを返却する前に、

- ノード暗号化が有効になっているアプライアンスの運用を停止したあと。

> KMS をクリアして StorageGRID システム内の他のノードにデータを移動する前に、アプライアンスの運用を停止します。アプライアンスの運用を停止する前に KMS をクリアすると、データが失われるため、アプライアンスが動作しなくなる可能性があります。

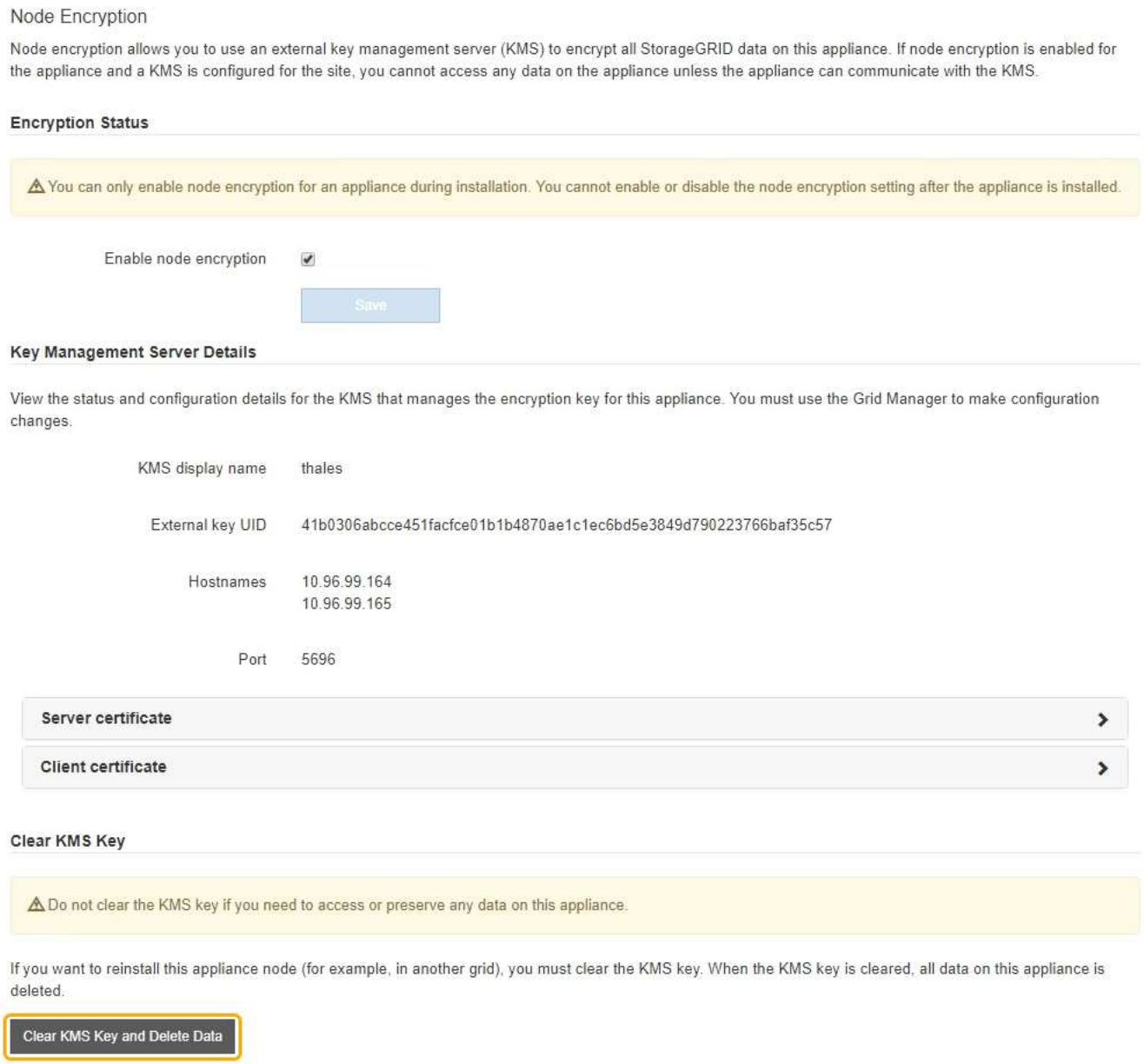
手順

1. ブラウザを開き、アプライアンスのコンピューティングコントローラの IP アドレスのいずれかを入力します。[+]
   **`https://Controller_IP:8443`**

   *`Controller_IP`* は、3つのStorageGRID ネットワークのいずれかでのコンピューティングコントローラ（ストレージコントローラではない）のIPアドレスです。

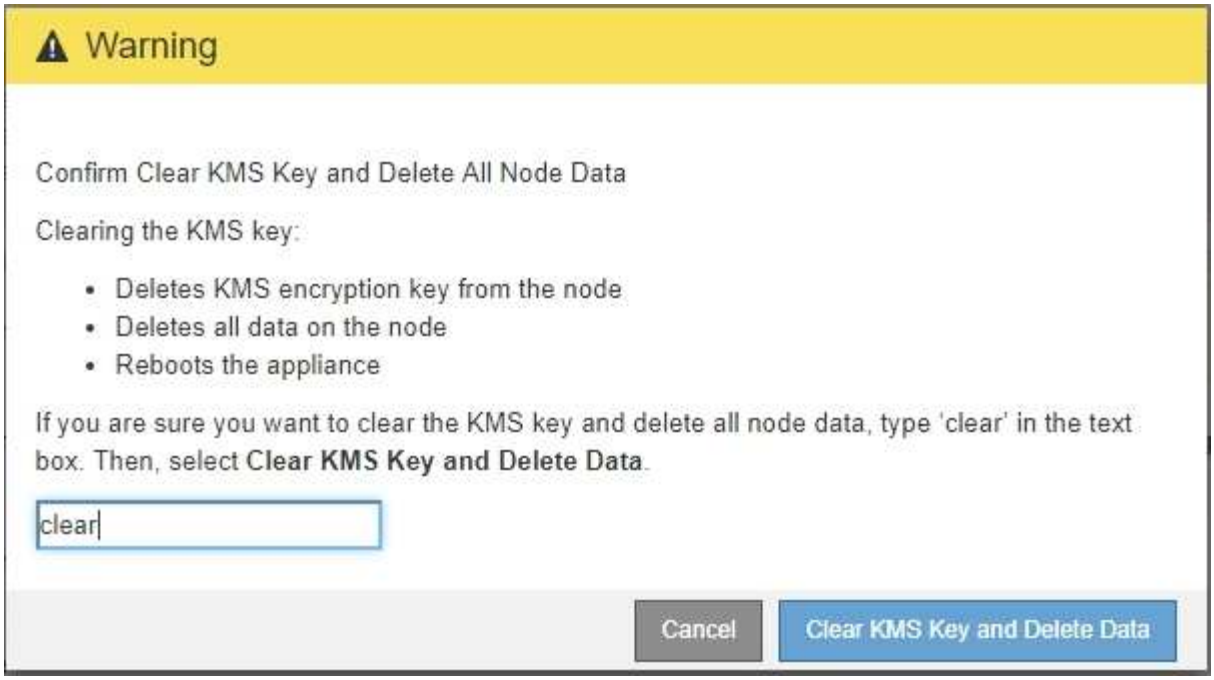
   StorageGRID アプライアンスインストーラのホームページが表示されます。

2. Configure Hardware * > * Node Encryption * を選択します。




KMS の設定をクリアすると、アプライアンス上のデータが完全に削除されます。このデータはリカバリできません。

3. ウィンドウの下部で、 * KMS キーをクリアしてデータを削除 * を選択します。
4. KMSの設定をクリアしても問題がない場合は、「+」と入力します **`clear`** +を押して、「* KMSキーを消去してデータを削除*」を選択します。




KMS 暗号化キーとすべてのデータがノードから削除され、アプライアンスがリブートします。この処理には 20 分程度かかる場合があります。

5. ブラウザを開き、アプライアンスのコンピューティングコントローラの IP アドレスのいずれかを入力します。[+]
**`https://Controller_IP:8443`**

   *`Controller_IP`* は、3つのStorageGRID ネットワークのいずれかでのコンピューティングコントローラ（ストレージコントローラではない）のIPアドレスです。

   StorageGRID アプライアンスインストーラのホームページが表示されます。

6. Configure Hardware * > * Node Encryption * を選択します。
7. ノードの暗号化が無効になっていること、および * キー管理サーバの詳細 * および * KMS キーと削除 * のコントロールでキーと証明書の情報がウィンドウから削除されていることを確認します。

   アプライアンスでのノード暗号化の再インストールまでは、グリッドでのノード暗号化を再度有効にすることはできません。

完了後

アプライアンスがリブートし、 KMS がクリアされてインストール前の状態になっていることを確認したら、StorageGRID システムからアプライアンスを物理的に取り外すことができます。再インストールのためのアプライアンスの準備については、リカバリおよびメンテナンスの手順を参照してください。

関連情報

"StorageGRID の管理"

""

# SG5600 ストレージアプライアンス

StorageGRID SG5612とSG5660アプライアンスをインストールおよび保守する方法について説明します。

- "StorageGRID アプライアンスの概要"
- "インストールと導入の概要"
- "設置を準備しています"
- "ハードウェアを設置"
- "ハードウェアの設定"
- "アプライアンスストレージノードの導入"
- "ストレージアプライアンスのインストールの監視"
- "アプライアンスのインストールと設定の自動化"
- "インストール REST API の概要"
- "ハードウェアの設置のトラブルシューティング"
- "SG5600アプライアンスのメンテナンス"

## StorageGRID アプライアンスの概要

StorageGRID SG5600 アプライアンスは、 StorageGRID グリッドにおいてストレージノードとして機能する、ストレージとコンピューティングを統合したプラットフォームです。

StorageGRID SG5600 アプライアンスには、次のコンポーネントが含まれています。

| コンポーネント | 説明 |
| --- | --- |
| E5600SG コントローラ | コンピューティングサーバ E5600SG コントローラは Linux オペレーティングシステムと StorageGRID ソフトウェアを実行します。<br><br>このコントローラは次のものに接続されています。<br><br>• StorageGRID システムの管理、グリッド、クライアントネットワーク<br>• E2700 コントローラ。 E5600SG コントローラがイニシエータとして動作しているデュアル SAS パス（アクティブ / アクティブ）を使用します |

| コンポーネント | 説明 |
| --- | --- |
| E2700 コントローラ | ストレージコントローラ E2700 コントローラは、シンプレックスモードで標準の E シリーズストレージアレイとして動作し、 SANtricity オペレーティングシステム（コントローラファームウェア）を実行します。<br><br>このコントローラは次のものに接続されています。<br><br>• SANtricity Storage Manager がインストールされている管理ネットワーク<br>• E5600SG コントローラは、 E2700 コントローラがターゲットとして動作しているデュアル SAS パス（アクティブ / アクティブ）を使用する |

SG5600 アプライアンスには、モデルに応じて次のコンポーネントも含まれています。

| コンポーネント | モデル **SG5612** | モデル **SG5660** |
| --- | --- | --- |
| ドライブ | 12 本の NL-SAS ドライブ | NL-SAS ドライブ × 60 |
| エンクロージャ | DE1600 エンクロージャ：ドライブとコントローラを収容する 2 ラックユニット（ 2U ）シャーシ | DE6600 エンクロージャは、ドライブとコントローラを収納する 4 ラックユニット（ 4U ）シャーシです |
| 電源装置とファン | 電源 / ファンキャニスター × 2 | 電源装置 × 2 、ファン × 2 |

E5600SG コントローラは、 StorageGRID アプライアンスで使用するために高度にカスタマイズされています。それ以外のコンポーネントは、それぞれの手順に記載されている点を除いて、 E シリーズのドキュメントで説明されているとおりに動作します。

各 StorageGRID アプライアンスストレージノードで使用可能な最大物理容量は固定であり、アプライアンスのモデルと構成に基づいて決まります。ドライブを増設したシェルフを追加してストレージを拡張することはできません。

**StorageGRID** アプライアンスの特長

## StorageGRID SG5600 アプライアンスは、 StorageGRID システムの新規作成や既存システムの容量の拡張に使用できる統合ストレージ解決策 です。

StorageGRID アプライアンスには次のような特長があります。

- StorageGRID ストレージノードのコンピューティング要素とストレージ要素を 1 つに統合した効率的な解決策 です
- 必要なプロセスのほとんどを自動化できるため、ストレージノードのインストールと設定を簡単に行えます

- 2U と 4U の 2 種類のエンクロージャが用意された高密度なストレージ解決策 を提供します
- FC や iSCSI などの中間ストレージインターフェイスを使用せずに、 10GbE の IP インターフェイスでストレージノードに直接接続します
- は、 StorageGRID アプライアンスと仮想（ソフトウェアベース）のストレージノードを使用するハイブリッドなグリッド環境で使用できます
- 構成済みのストレージと StorageGRID アプライアンスインストーラが搭載されており（ E5600SG コントローラ）、すぐにソフトウェアの導入と統合を実行できます

ハードウェアの構成図

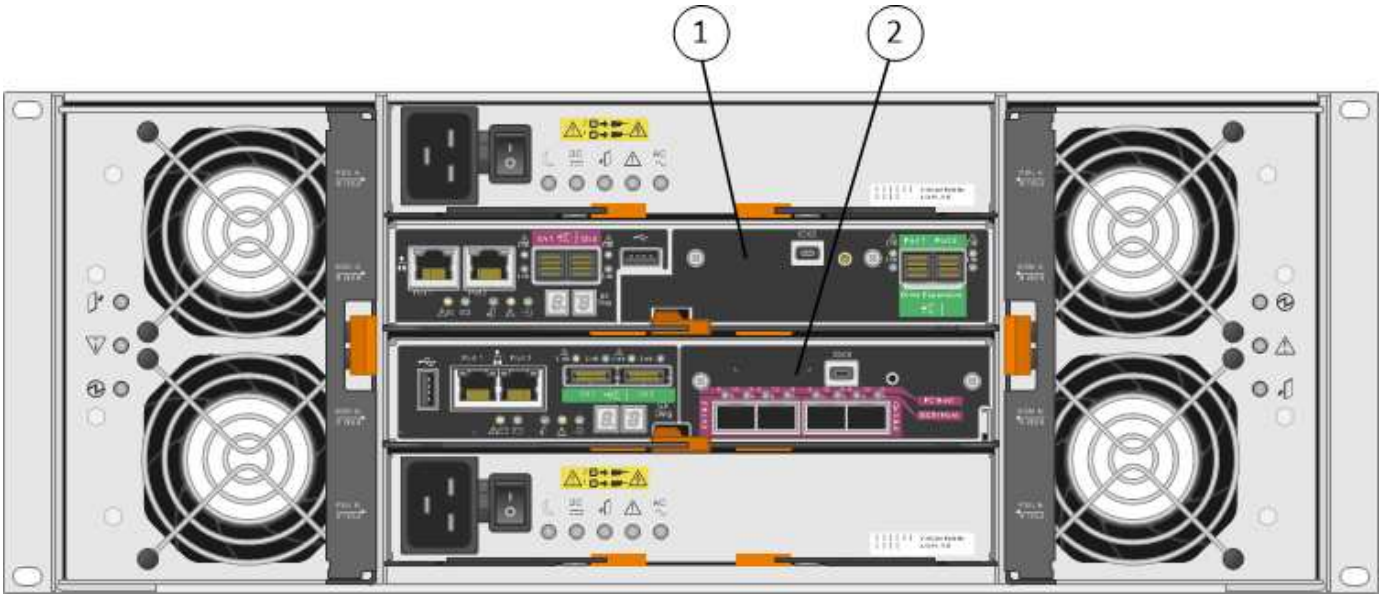
## StorageGRID アプライアンス SG5612 と SG5660 の両モデルには、 E2700 コントローラと E5600SG コントローラが含まれています。次の図で、モデルとコントローラの違いを確認してください。

モデル**SG5612 2U**：**E2700**コントローラと**E5600SG**コントローラの背面

| | 説明 |
|---|---|
| 1. | E2700 コントローラ |
| 2. | E5600SG コントローラ |

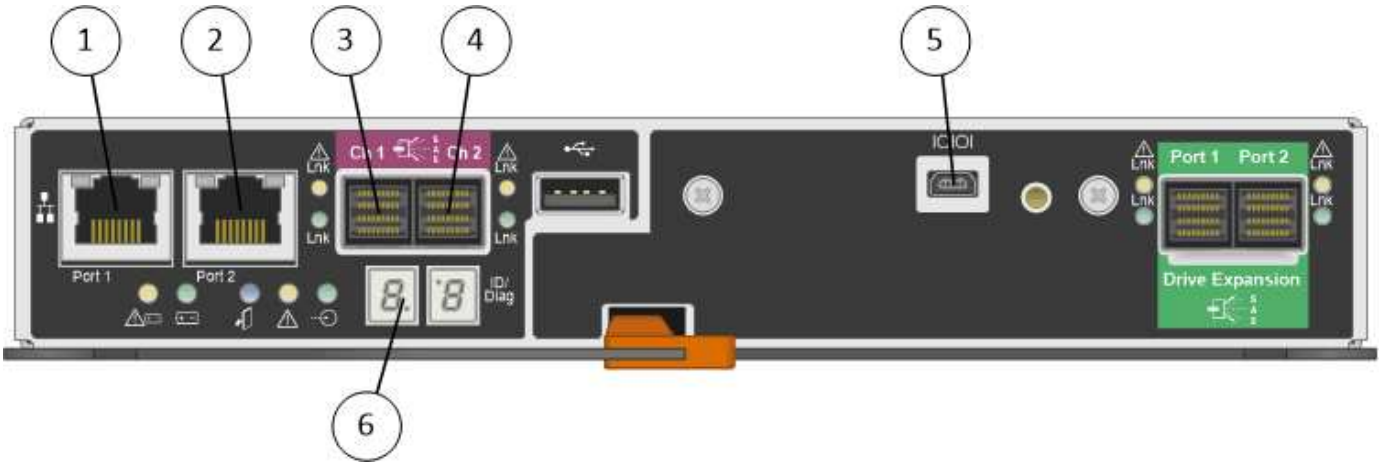
モデル**SG5660 4U**：**E2700**コントローラと**E5600SG**コントローラの背面図

E2700 コントローラは E5600SG コントローラの上にあります。




| | 説明 |
|---|---|
| 1. | E2700 コントローラ |
| 2. | E5600SG コントローラ |

**E2700**コントローラの背面

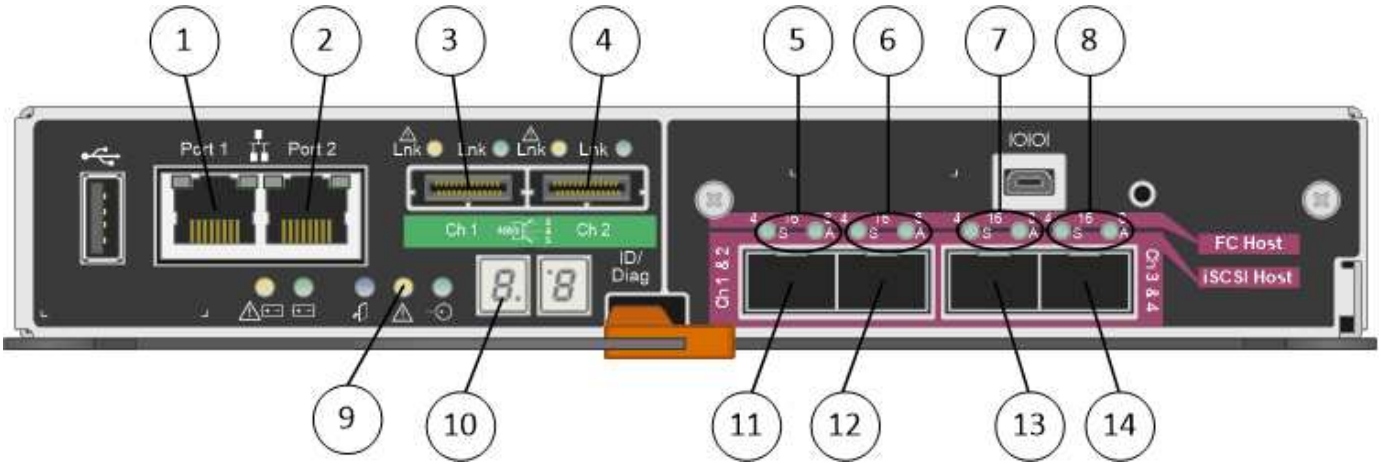



| | 説明 |
|---|---|
| 1. | 管理ポート 1 （ SANtricity Storage Manager がインストールされているネットワークに接続） |
| 2. | 管理ポート 2 （設置作業でラップトップへの接続に使用） |
| 3. | SAS インターコネクトポート 1 |
| 4. | SAS インターコネクトポート 2 |

| | 説明 |
|---|---|
| 5. | シリアル接続ポート |
| 6. | デジタル表示ディスプレイ |

E2700 コントローラの背面にある「 Drive Expansion 」というラベルが付いた 2 つの SAS ポートは使用しません。StorageGRID アプライアンスでは拡張ドライブシェルフはサポートされません。

**E5600SG**コントローラの背面




| | 説明 |
|---|---|
| 1. | 管理ポート1（StorageGRID の管理ネットワークに接続） |
| 2. | 管理ポート 2 のオプション：<br>• StorageGRID の管理ネットワークへの冗長接続を確保するには、管理ポート 1 とボンディングします。<br>• 一時的なローカルアクセス用（ IP 169.254.0.1 ）に空けておくことができます。<br>• DHCP によって割り当てられた IP アドレスを使用できない場合は、設置時の IP 設定に使用します。 |
| 3. | SAS インターコネクトポート 1 |
| 4. | SAS インターコネクトポート 2 |
| 5. | 10GbE ネットワークポート 1 の障害 LED とアクティブ LED |
| 6. | 10GbE ネットワークポート 2 の障害 LED とアクティブ LED |
| 7. | 10GbE ネットワークポート 3 の障害 LED とアクティブ LED |

| | 説明 |
|---|---|
| 8. | 10GbE ネットワークポート 4 の障害 LED とアクティブ LED |
| 9. | 警告 LED が必要です |
| 10. | デジタル表示ディスプレイ |
| 11. | 10GbE ネットワークポート 1 |
| 12. | 10GbE ネットワークポート 2 |
| 13 | 10GbE ネットワークポート 3 |
| 14 | 10GbE ネットワークポート 4 |

StorageGRID アプライアンス E5600SG コントローラのホストインターフェイスカード（ HIC ）では、 10Gb のイーサネット接続のみがサポートされます。iSCSI 接続には使用できません。

## インストールと導入の概要

### StorageGRID アプライアンスは StorageGRID の初回導入時に設置することも、後日拡張の一環として追加することもできます。リカバリ処理の一環としてアプライアンスストレージノードの設置が必要となる場合もあります。

StorageGRID システムに StorageGRID ストレージアプライアンスを追加するには、主に次の 4 つの手順を実行します。

1. 設置の準備：
    - 設置場所の準備
    - 開梱と内容の確認
    - 追加機器および工具の入手方法
    - IP アドレスとネットワーク情報を収集しています
    - オプション：すべてのアプライアンスデータを暗号化する場合は、外部キー管理サーバ（ KMS ）を設定します。外部キー管理の詳細については、 StorageGRID の管理手順を参照してください。
2. ハードウェアの設置
    - ハードウェアの登録
    - キャビネットまたはラックへのアプライアンスの設置
    - ドライブの取り付け（ SG5660 のみ）
    - アプライアンスのケーブル接続
    - 電源コードの接続と電源の投入

- ブート時のステータスコードの確認

3. ハードウェアの設定
   - SANtricity Storage Manager へのアクセス、 E2700 コントローラの管理ポート 1 の静的 IP アドレスの設定、および SANtricity Storage Manager の設定
   - StorageGRID アプライアンスインストーラへのアクセス、および StorageGRID ネットワークへの接続に必要なリンクとネットワーク IP の設定
   - オプション：外部 KMS を使用してアプライアンスデータを暗号化する場合は、ノード暗号化を有効にします。
   - オプション： RAID モードを変更する
4. アプライアンスをストレージノードとして導入する：

| タスク | を参照してください |
| --- | --- |
| 新しい StorageGRID システムにアプライアンスストレージノードを導入する | "アプライアンスストレージノードの導入" |
| 既存の StorageGRID システムへのアプライアンスストレージノードの追加 | StorageGRID システムの拡張手順 |
| ストレージノードのリカバリ処理の一環としてアプライアンスストレージノードを導入する | リカバリとメンテナンスの手順 |

関連情報

"設置を準備しています"

"ハードウェアを設置"

"ハードウェアの設定"

"グリッドを展開します"

""

"StorageGRID の管理"

## 設置を準備しています

StorageGRID アプライアンスを設置するための準備では、設置場所を準備し、必要なすべてのハードウェア、ケーブル、工具を揃えます。また、 IP アドレスとネットワーク情報を収集する必要があります。

手順

- "サイトの準備（SG5600）"
- "開梱（SG5600）"
- "追加の機器と工具の入手（SG5600）"

- "サービスラップトップの要件"
- "Web ブラウザの要件"
- "アプライアンスのネットワーク接続を確認します"
- "設置情報の収集（SG5600）"

サイトの準備（**SG5600**）

## アプライアンスを設置する前に、設置場所および使用するキャビネットやラックが StorageGRID アプライアンスの仕様を満たしていることを確認する必要があります。

手順

1. 設置場所の温度、湿度、高度範囲、通気、熱放散の要件を満たしていることを確認します。 配線、電源、およびアース。詳細については、 NetApp Hardware Universe を参照してください。
2. 次のサイズのシェルフ（ケーブルなし）が収まる 48.3cm （ 19 インチ）のキャビネットまたはラックを用意します。

| アプライアンスのモデル | 高さ | 幅 | 奥行き | 最大重量 |
|---|---|---|---|---|
| SG5612<br>（ 12 ドライブ） | 3.40 インチ<br>（ 8.64 cm ） | 48.3cm<br>（ 48.26cm ） | 21.75 インチ<br>（ 55.25 cm ） | 59.5 ポンド<br>（ 27 kg ） |
| SG5660<br>（ 60 ドライブ） | 7.00 インチ<br>（ 17.78 cm ） | 17.75 インチ<br>（ 45.08 cm ） | 32.50 インチ<br>（ 82.55 cm ） | 236.2 ポンド<br>（ 107.1 kg ） |

3. 必要なネットワークスイッチを取り付けます。互換性の情報については、 NetApp Interoperability Matrix Tool を参照してください。

関連情報

"NetApp Hardware Universe の略"

"ネットアップの相互運用性"

開梱（**SG5600**）

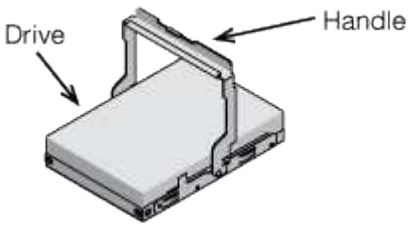
## StorageGRID アプライアンスを設置する前にすべて開梱し、内容物を納品書の項目と比較します。

- * 60 ドライブを搭載した 4U シャーシ * SG5660 エンクロージャ

- * SG5612 エンクロージャは 12 ドライブ * の 2U シャーシ

- *4U ベゼルまたは 2U エンドキャップ *

- * NL-SAS ドライブ *



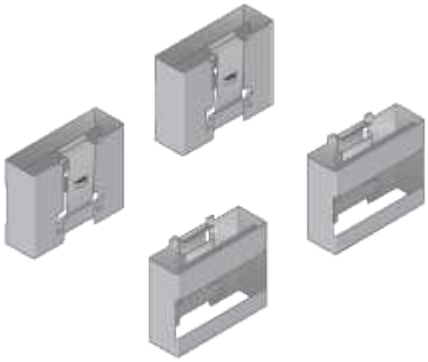

2U SG5612 にはドライブがあらかじめ取り付けられていますが、安全性を確保するために SG5660 は 4U には取り付けません。

- * E5600SG コントローラ *

- * E2700 コントローラ *

- * 取り付けレールとネジ *

- * エンクロージャハンドル（ 4U エンクロージャのみ） *



ケーブルとコネクタ

StorageGRID アプライアンスには、出荷時に次のケーブルとコネクタが付属しています。

- * お住まいの国の電源コード *

  コンセントなどの外部電源に接続するための AC 電源コードが 2 本付属しています。キャビネットによっては、アプライアンスに付属している電源コードではなく特別な電源コードを使用する場合があります。

- * SAS インターコネクトケーブル *

mini-SAS-HD コネクタと mini-SAS コネクタが付いた 0.5m の SAS インターコネクトケーブル 2 本。

正方形のコネクタは E2700 コントローラに、長方形のコネクタは E5600SG コントローラに接続します。

追加の機器と工具の入手（**SG5600**）

## SG5600 アプライアンスを設置する前に、必要な追加機器や工具がすべて揃っていることを確認します。

- * ドライバ *

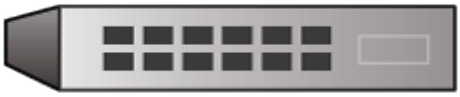
フィリップス番号2 本のドライバ

中型マイナスドライバ

- * 静電気防止用リストストラップ *

- * イーサネットケーブル *

- * イーサネットスイッチ *



- * サービスラップトップ *

サービスラップトップの要件

## StorageGRID アプライアンスハードウェアを設置する前に、サービスラップトップが最小限必要なリソースを備えているかどうかを確認する必要があります。

ハードウェアの設置に必要なサービスラップトップは、次の要件を満たしている必要があります。

- Microsoft Windows オペレーティングシステム
- ネットワークポート
- サポートされている Web ブラウザ
- ネットアップ SANtricity ストレージマネージャバージョン 11.40 以降
- SSH クライアント（ PuTTY など）

関連情報

"Web ブラウザの要件"

"ネットアップのマニュアル： SANtricity Storage Manager"

**Web** ブラウザの要件

## サポートされている Web ブラウザを使用する必要があります。

| Web ブラウザ | サポートされる最小バージョン |
| --- | --- |
| Google Chrome | 87 |
| Microsoft Edge の場合 | 87 |
| Mozilla Firefox | 84 |

ブラウザウィンドウの幅を推奨される値に設定してください。

| ブラウザの幅 | ピクセル |
| --- | --- |
| 最小（ Minimum ） | 1024 |
| 最適 | 1280 |

アプライアンスのネットワーク接続を確認します

## StorageGRID アプライアンスを設置する前に、アプライアンスに接続できるネットワークを確認し、各コントローラのポートがどのように使用されるかを把握する必要があります。

**StorageGRID** アプライアンスのネットワーク

StorageGRID アプライアンスをストレージノードとして導入する場合は、次のネットワークに接続できます。

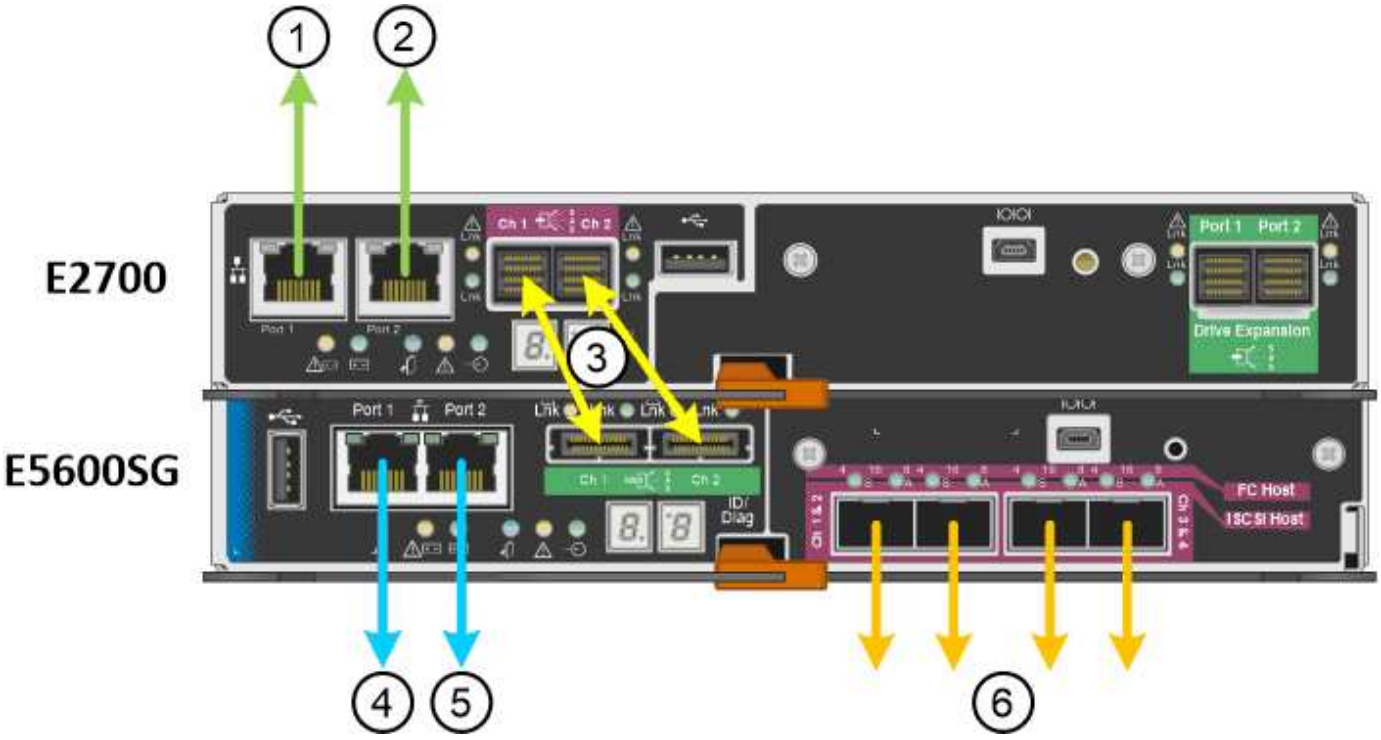
- * StorageGRID のグリッドネットワーク * ：グリッドネットワークは、すべての内部 StorageGRID トラフィックに使用されます。このネットワークによって、グリッド内のすべてのノードが、すべてのサイトおよびサブネットにわたって相互に接続されます。グリッドネットワークは必須です。
- * StorageGRID の管理ネットワーク * ：管理ネットワークは、システムの管理とメンテナンスに使用するクローズドネットワークです。管理ネットワークは通常はプライベートネットワークであり、サイト間でルーティング可能にする必要はありません。管理ネットワークはオプションです。
- * StorageGRIDのクライアントネットワーク*：クライアントネットワークは、S3やSwiftなどのクライアントアプリケーションへのアクセスを可能にするオープンネットワークです。クライアントネットワークはグリッドへのクライアントプロトコルアクセスを提供するため、グリッドネットワークを分離してセキュリティを確保できます。クライアントネットワークはオプションです。
- * SANtricity Storage Manager用管理ネットワーク*：E2700コントローラは、SANtricity Storage Managerがインストールされている管理ネットワークに接続し、アプライアンス内のハードウェアコンポーネントの監視と管理を行うことができます。この管理ネットワークは、 StorageGRID の管理ネットワークと同じにすることも、独立した管理ネットワークにすることもできます。

StorageGRID ネットワークの詳細については、 _ グリッド入門 _ を参照してください。

**StorageGRID** アプライアンスの接続

StorageGRID アプライアンスを設置するときは、 2 台のコントローラを相互に接続するとともに、必要なネ

ットワークに接続する必要があります。この図は、 E2700 コントローラを上部に、 E5600SG コントローラを下部に配置した SG5660 の 2 台のコントローラを示しています。SG5612 では、 E2700 コントローラは E5600SG コントローラの左側にある。




| 項目 | ポート | ポートのタイプ | 機能 |
|---|---|---|---|
| 1. | E2700 コントローラの管理ポート 1 | 1Gb （ RJ-45 ）イーサネット | E2700 コントローラを、 SANtricity Storage Manager がインストールされているネットワークに接続します。 |
| 2. | E2700 コントローラの管理ポート 2 | 1Gb （ RJ-45 ）イーサネット | 設置時に E2700 コントローラをサービスラップトップに接続します。 |
| 3. | 各コントローラの 2 つの SAS インターコネクトポート、 Ch 1 および Ch 2 | E2700 コントローラ： Mini-SAS - HD<br><br>E5600SG コントローラ： Mini-SAS | 2 台のコントローラを相互に接続します。 |
| 4. | E5600SG コントローラの管理ポート 1 | 1Gb （ RJ-45 ）イーサネット | E5600SG コントローラを StorageGRID の管理ネットワークに接続します。 |

| 項目 | ポート | ポートのタイプ | 機能 |
| --- | --- | --- | --- |
| 5. | E5600SG コントローラの管理ポート 2 | 1Gb （ RJ-45 ）イーサネット | • 管理ネットワークへの冗長接続が必要な場合は、管理ポート 1 とボンディングできます。<br>• 一時的なローカルアクセス用（ IP 169.254.0.1 ）に空けておくことができます。<br>• DHCP によって割り当てられた IP アドレスを使用できない場合、設置時に E5600SG コントローラをサービスラップトップに接続するために使用できます。 |
| 6. | E5600SG コントローラの 4 つのネットワークポート | 10GbE （光ファイバ） | StorageGRID のグリッドネットワークおよびクライアントネットワークに接続します。「 E5600SG コントローラでの 10 GbE ポート接続」を参照してください。 |

関連情報

"E5600SG コントローラポートのポートボンディングモード"

"設置情報の収集（SG5600）"

"アプライアンスのケーブル接続（SG5600）"

"ネットワークガイドライン"

"VMware をインストールする"

"Red Hat Enterprise Linux または CentOS をインストールします"

"Ubuntu または Debian をインストールします"

**E5600SG** コントローラポートのポートボンディングモード

E5600SG コントローラポートにネットワークリンクを設定する場合は、グリッドネットワークとオプションのクライアントネットワークに接続する 10GbE ポート、およびオプションの管理ネットワークに接続する 1GbE 管理ポートに対してポートボンディングを使用できます。ポートボンディングを使用すると、 StorageGRID ネットワークとアプ

ライアンスの間のパスが冗長化されるため、データの保護に役立ちます。

関連情報

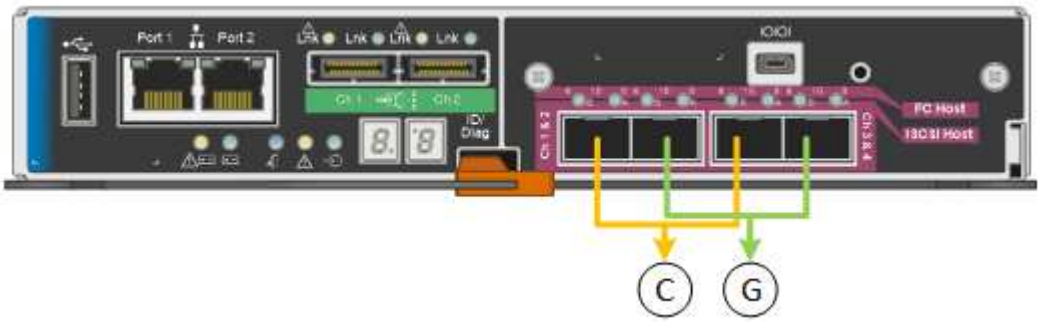
"ネットワークリンクの設定（SG5600）"

**10GbE**ポートのネットワークボンディングモード

## E5600SG コントローラの 10GbE ネットワークポートは、グリッドネットワークおよびクライアントネットワーク接続用に、 Fixed または Aggregate のポートボンディングモードをサポートします。

**Fixed** ポートボンディングモード

Fixed モードは、 10GbE ネットワークポートのデフォルトの設定です。




| | ボンディングされるポート |
|---|---|
| C | このネットワークを使用する場合、ポート 1 とポート 3 がクライアントネットワーク用にボンディングされます。 |
| G | ポート 2 とポート 4 がグリッドネットワーク用にボンディングされます。 |

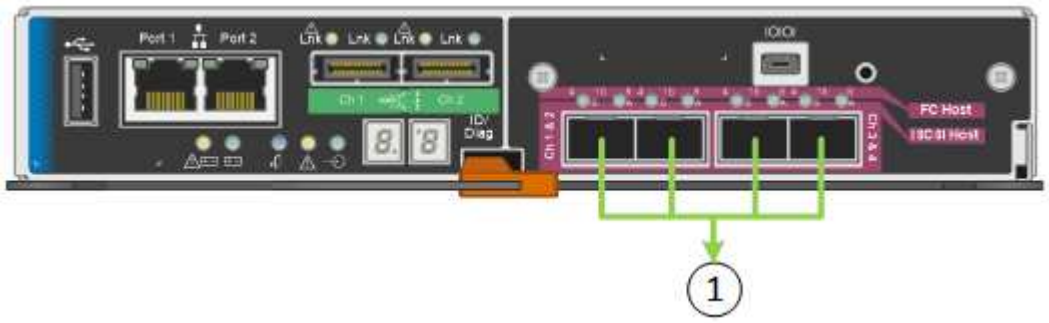
Fixed ポートボンディングモードを使用する場合は、 Active-Backup モードまたは Link Aggregation Control Protocol （ LACP ）（ 802.3ad ）モードを使用してポートをボンディングできます。

- Active-Backup モード（デフォルト）では、一度に 1 つのポートのみがアクティブになります。アクティブポートで障害が発生すると、バックアップポートが自動的にフェイルオーバーして接続が継続されます。ポート 4 がポート 2 のバックアップパスとなり（グリッドネットワーク）、ポート 3 がポート 1 のバックアップパスとなります（クライアントネットワーク）。
- LACP モードでは、各ポートペアでコントローラとネットワークの間の論理チャネルが形成され、スループットが向上します。一方のポートで障害が発生しても、もう一方のポートは引き続きチャネルを提供します。スループットは低下しますが、接続に影響はありません。

冗長な接続が不要な場合は、各ネットワークで使用できるポートは 1 つだけです。ただし、StorageGRID をインストールしたあとにグリッドマネージャでアラームが生成され、ケーブルが取り外されていることが通知されます。このアラームは確認後に解除してかまいません。

**Aggregate** ポートボンディングモード

アグリゲートポートボンディングモードを使用すると、各 StorageGRID ネットワークのスループットが大幅に向上し、追加のフェイルオーバーパスも確保されます。




| | ボンディングされるポート |
|---|---|
| 1. | 接続されたすべてのポートを 1 つの LACP ボンドにグループ化して、すべてのポートをグリッドネットワークとクライアントネットワークのトラフィックに使用できるようにします。 |

Aggregate ポートボンディングモードを使用する場合は、次の点に注意してください。

- LACP ネットワークボンディングモードを使用する必要があります。
- 各ネットワークに一意の VLAN タグを指定する必要があります。この VLAN タグが各ネットワークパケットに追加され、ネットワークトラフィックが正しいネットワークにルーティングされます。
- VLAN と LACP をサポートするスイッチにポートを接続する必要があります。複数のスイッチを LACP ボンドに加える場合は、対象のスイッチが Multi-Chassis Link Aggregation （ MLAG ）グループまたは同等の機能をサポートしていることが必要です。
- VLAN 、 LACP 、 MLAG などを使用するようにスイッチを設定する方法について理解しておく必要があります。

4 つの 10GbE ポートをすべて使用する必要がない場合、使用するポートの数は 1~3 のいくつでもかまいません。複数のポートを使用すると、 10GbE ポートの 1 つに障害が発生した場合でも、ネットワーク接続を確保できる可能性が高くなります。

> 4 つのポート全部を使用しない場合は、 StorageGRID をインストールしたあとにケーブルが取り外されていることを通知するアラームがグリッドマネージャで生成されるので注意してください。このアラームは確認後に解除してかまいません。

**1GbE**管理ポートのネットワークボンディングモード

## E5600SG コントローラの 2 つの 1GbE 管理ポートでは、オプションの管理ネットワークに接続するために、独立したネットワークボンディングモードまたは Active-Backup ネットワークボンディングモードを選択できます。

Independent モードでは、管理ポート 1 だけが管理ネットワークに接続されます。このモードではパスは冗長化されません。管理ポート 2 は、一時的なローカル接続（ IP アドレス 169.254.0.1 ）用に確保されます。

Active-Backup モードでは、管理ポート 1 と 2 の両方が管理ネットワークに接続されます。一度に 1 つのポートのみがアクティブになります。アクティブポートで障害が発生すると、バックアップポートが自動的にフェイルオーバーして接続が継続されます。これら 2 つの物理ポートを 1 つの論理管理ポートにボンディングすることで、管理ネットワークへのパスが冗長化されます。

> 1GbE 管理ポートが Active-Backup モードに設定されている場合に E5600SG コントローラへの一時的なローカル接続が必要となった場合は、両方の管理ポートからケーブルを取り外し、一時的なケーブルを管理ポート 2 に接続し、 IP アドレス 169.254.0.1 を使用してアプライアンスにアクセスしてください。

設置情報の収集（**SG5600**）

## StorageGRID アプライアンスを設置および設定する際に、イーサネットスイッチポート、 IP アドレス、およびポートとネットワークのボンディングモードについて決定し、関連情報を収集する必要があります。

このタスクについて

次の表を使用して、アプライアンスに接続する各ネットワークの情報を記録できます。これらの値は、ハードウェアの設置と設定に必要です。

**E2700**コントローラを**SANtricity Storage Manager**に接続するために必要な情報

SANtricity Storage Manager で使用する管理ネットワークに E2700 コントローラを接続する必要があります。

| 必要な情報 | あなたの価値 |
| --- | --- |
| 管理ポート 1 に接続するイーサネットスイッチポート | |
| 管理ポート 1 の MAC アドレス（ポート P1 のラベルに記載） | |
| DHCP によって管理ポート 1 に割り当てられた IP アドレス（電源投入後に使用可能な場合）<br><br>• 注： * E2700 コントローラに接続するネットワークに DHCP サーバがある場合、ネットワーク管理者は、 MAC アドレスを使用して DHCP サーバによって割り当てられた IP アドレスを特定できます。 | |

| 必要な情報 | あなたの価値 |
| --- | --- |
| 速度と二重モード<br>• 注： SANtricity Storage Manager 管理ネットワークのイーサネットスイッチが自動ネゴシエーションに設定されていることを確認する必要があります。 | 次の値でなければなりません<br>• Autonegotiate （デフォルト） |
| IP アドレスの形式 | 1 つ選択してください：<br>• IPv4<br>• IPv6 |
| 管理ネットワークでアプライアンスに使用する静的 IP アドレス | IPv4 の場合：<br>• IPv4 アドレス：<br>• サブネットマスク：<br>• ゲートウェイ<br>IPv6 の場合：<br>• IPv6 アドレス：<br>• ルーティング可能な IP アドレス：<br>• E2700 コントローラルータの IP アドレス： |

**E5600SG**コントローラを管理ネットワークに接続するために必要な情報

StorageGRID の管理ネットワークは、システムの管理とメンテナンスに使用するオプションのネットワークです。アプライアンスは、 E5600SG コントローラの 1GbE 管理ポートを使用して管理ネットワークに接続します。

| 必要な情報 | あなたの価値 |
| --- | --- |
| 管理ネットワークが有効になりました | 1 つ選択してください：<br>• いいえ<br>• ○（デフォルト） |
| ネットワークボンディングモード | 1 つ選択してください：<br>• 独立<br>• アクティブ / バックアップ |
| 管理ポート 1 （ P1 ）のスイッチポート | |

| 必要な情報 | あなたの価値 |
| --- | --- |
| 管理ポート 2 のスイッチポート（ P2 、アクティブ / バックアップネットワークボンディングモードのみ） | |
| 管理ポート 1 の MAC アドレス（ポート P1 のラベルに記載） | |
| DHCP によって管理ポート 1 に割り当てられた IP アドレス（電源投入後に使用可能な場合）<br>• 注： * 管理ネットワークに DHCP サーバが含まれている場合、 E5600SG コントローラのブート後はデジタル表示ディスプレイに DHCP によって割り当てられた IP アドレスが表示されます。DHCP によって割り当てられた IP アドレスは、 MAC アドレスを使用して IP アドレスを調べる方法でも確認できます。 | • IPv4 アドレス（ CIDR ）：<br>• ゲートウェイ |
| 管理ネットワークでアプライアンスストレージノードに使用する静的 IP アドレス<br>• 注： * ネットワークにゲートウェイがない場合は、同じ静的 IPv4 アドレスをゲートウェイに指定してください。 | • IPv4 アドレス（ CIDR ）：<br>• ゲートウェイ |
| 管理ネットワークのサブネット（ CIDR ） | |

**E5600SG**コントローラで**10GbE**ポートの接続と設定に必要な情報

E5600SG コントローラの 4 つの 10GbE ポートは、 StorageGRID のグリッドネットワークとクライアントネットワークに接続します。

これらのポートのオプションの詳細については、「 E5600SG コントローラでの 10GbE ポート接続」を参照してください。

| 必要な情報 | あなたの価値 |
| --- | --- |
| ポートボンディングモード | 1 つ選択してください：<br>• Fixed （デフォルト）<br>• アグリゲート |
| ポート 1 のスイッチポート（固定モードのクライアントネットワーク） | |

| 必要な情報 | あなたの価値 |
| --- | --- |
| ポート 2 のスイッチポート（ Fixed モードのグリッドネットワーク） | |
| ポート 3 のスイッチポート（固定モードのクライアントネットワーク） | |
| ポート 4 のスイッチポート（ Fixed モードのグリッドネットワーク） | |

**E5600SG**コントローラをグリッドネットワークに接続するために必要な情報

StorageGRID のグリッドネットワークは、内部のすべての StorageGRID トラフィックに使用される必須のネットワークです。アプライアンスは、 E5600SG コントローラの 10GbE ポートを使用してグリッドネットワークに接続します。

これらのポートのオプションの詳細については、「 E5600SG コントローラでの 10GbE ポート接続」を参照してください。

| 必要な情報 | あなたの価値 |
| --- | --- |
| ネットワークボンディングモード | 1 つ選択してください：<br>• Active-Backup （デフォルト）<br>• LACP （ 802.3ad ） |
| VLAN タギングが有効です | 1 つ選択してください：<br>• いいえ（デフォルト）<br>• はい。 |
| VLAN タグ（ VLAN タギングが有効な場合） | 0~4095 の値を入力してください： |
| 電源投入後に使用可能な場合、 DHCP によってグリッドネットワークに割り当てられた IP アドレス<br>• 注： * グリッドネットワークに DHCP サーバが含まれている場合、 E5600SG コントローラのブート後にデジタル表示ディスプレイにグリッドネットワークに対して DHCP によって割り当てられた IP アドレスが表示されます。 | • IPv4 アドレス（ CIDR ）：<br>• ゲートウェイ |

| 必要な情報 | あなたの価値 |
| --- | --- |
| グリッドネットワークでアプライアンスストレージノードに使用する静的 IP アドレス<br>• 注： * ネットワークにゲートウェイがない場合は、同じ静的 IPv4 アドレスをゲートウェイに指定してください。 | • IPv4 アドレス（ CIDR ）：<br>• ゲートウェイ |
| グリッドネットワークのサブネット（ CIDR ）<br>• 注： * クライアントネットワークが有効になっていない場合、コントローラのデフォルトルートではここで指定したゲートウェイが使用されます。 | |

**E5600SG**コントローラをクライアントネットワークに接続するために必要な情報

StorageGRID のクライアントネットワークは、グリッドへのクライアントプロトコルアクセスを可能にするオプションのネットワークです。アプライアンスは、 E5600SG コントローラの 10GbE ポートを使用してクライアントネットワークに接続します。

これらのポートのオプションの詳細については、「 E5600SG コントローラでの 10GbE ポート接続」を参照してください。

| 必要な情報 | あなたの価値 |
| --- | --- |
| クライアントネットワークが有効になりました | 1 つ選択してください：<br>• いいえ（デフォルト）<br>• はい。 |
| ネットワークボンディングモード | 1 つ選択してください：<br>• Active-Backup （デフォルト）<br>• LACP （ 802.3ad ） |
| VLAN タギングが有効です | 1 つ選択してください：<br>• いいえ（デフォルト）<br>• はい。 |
| VLAN タグ（ VLAN タギングが有効な場合） | 0~4095 の値を入力してください： |
| 電源投入後に DHCP によってクライアントネットワークに割り当てられた IP アドレスがある場合は | • IPv4 アドレス（ CIDR ）：<br>• ゲートウェイ |

| 必要な情報 | あなたの価値 |
| --- | --- |
| クライアントネットワークでアプライアンスストレージノードに使用する静的 IP アドレス<br>• 注：* クライアントネットワークが有効になっている場合、コントローラのデフォルトルートではここで指定したゲートウェイが使用されます。 | • IPv4 アドレス（ CIDR ）：<br>• ゲートウェイ |

関連情報

"アプライアンスのネットワーク接続を確認します"

"ハードウェアの設定"

"E5600SG コントローラポートのポートボンディングモード"

## ハードウェアを設置

ハードウェアの設置では、ハードウェアコンポーネントを設置し、それらのコンポーネントをケーブルで接続し、ポートを設定することが主な作業となります。

手順

- "ハードウェアの登録"
- "キャビネットまたはラックへのアプライアンスの設置（SG5600）"
- "アプライアンスのケーブル接続（SG5600）"
- "AC電源コードの接続（SG5600）"
- "電源のオン（SG5600）"
- "SG5600コントローラのブート時のステータスコードとエラーコードの確認"

### ハードウェアの登録

アプライアンスハードウェアを登録するとサポートを受けられるようになります。

手順

1. シャーシのシリアル番号を確認します。

   この番号は、納品書や確認用 E メールで確認できるほか、開梱したアプライアンスにも記載されています。

2. NetApp Support Siteにアクセスします "mysupport.netapp.com"。
3. ハードウェアの登録が必要かどうかを確認します。

| ユーザのタイプとアクセス方法 | 実行する手順 |
| --- | --- |
| ネットアップの既存のお客様 | a. ユーザ名とパスワードを使用してサインインします。<br>b. [ 製品 **>*My Products** ] を選択します。<br>c. 新しいシリアル番号が表示されていることを確認します。<br>d. 表示されていない場合は、ネットアップの新規のお客様向けの手順に従ってください。 |
| ネットアップの新規のお客様 | a. [ 今すぐ登録 ] をクリックしてアカウントを作成します。<br>b. [**Products**>*Register Products*] を選択します。<br>c. 製品のシリアル番号と要求された詳細情報を入力します。<br>登録が承認されると、必要なソフトウェアをダウンロードできます。承認プロセスには最大 24 時間かかる場合があります。 |

キャビネットまたはラックへのアプライアンスの設置（**SG5600**）

# キャビネットまたはラックにレールを取り付け、レールにアプライアンスをスライドさせます。SG5660 を使用している場合は、アプライアンスを設置したあとにもドライブを設置する必要があります。

必要なもの

- 同梱されている安全上の注意に関するドキュメントを確認し、ハードウェアの移動と設置に関する注意事項を理解しておきます。
- ハードウェアに E シリーズのインストール手順が付属していることを確認します。

機器の転倒を防ぐために、ラックまたはキャビネットの一番下から順にハードウェアを設置してください。

ドライブがすべて取り付けられた状態の SG5612 の重量は、約 27kg （ 60 ポンド）です。SG5612 を安全に移動するには、 2 人の人員または電動リフトが必要です。

ドライブが取り付けられていない状態の SG5660 の重量は、約 60kg （ 132 ポンド）です。空の SG5660 を安全に移動するには、 4 人で行うかリフト機を使用する必要があります。

ハードウェアの損傷を避けるため、ドライブを取り付ける場合は SG5660 を移動しないでください。アプライアンスを移動する前に、ドライブをすべて取り外す必要があります。

このタスクについて

キャビネットまたはラックに SG5660 アプライアンスを設置するには、次の作業を実行します。

- * マウントレール * を取り付けます

  キャビネットまたはラックにマウントレールを取り付けます。

  E2700 または E5600 用の E シリーズインストール手順を参照してください。

- * キャビネットまたはラックにアプライアンスを設置します。 *

  アプライアンスをキャビネットまたはラックにスライドさせて挿入し、固定します。

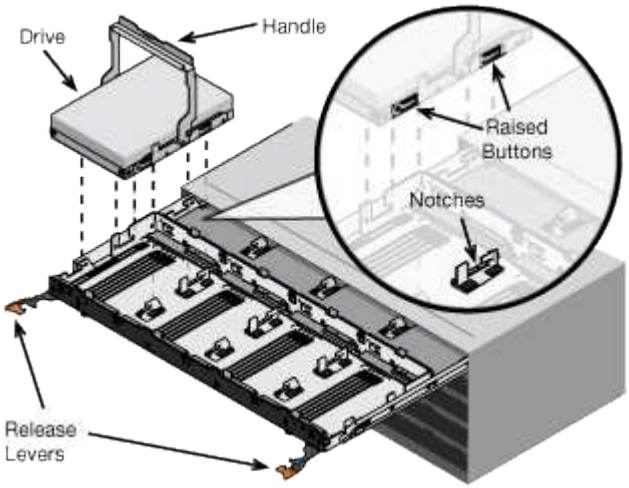
  SG5660 を手で持ち上げる場合は、シャーシの側面に 4 つのハンドルを取り付けます。この取っ手は、アプライアンスをレールにスライドさせて挿入するときに取り外します。

- * ドライブを取り付けます *

  SG5660 を使用する場合は、 5 つの各ドライブドロワーに 12 本のドライブを設置します。

  正しく動作させるためには、 60 本のドライブをすべて取り付ける必要があります。

  a. ESD リストバンドを装着し、パッケージからドライブを取り出します。
  b. 上部ドライブドロワーのレバーを解放し、レバーを使用してドロワーを引き出します。
  c. ドライブのハンドルを垂直に持ち上げ、ドライブのボタンをドロワーのノッチに合わせます。




  d. ドライブの上部を軽く押し、ドライブが完全に固定されるまでドライブのハンドルを下に回転させます。
  e. 最初の 12 本のドライブを取り付けたら、ドロワーの中央を押し、両方のレバーを静かに閉じてドロワーを元の位置に戻します。
  f. 残りの 4 つのドロワーで同じ手順を繰り返します。

- * フロントベゼルを取り付けます *
- SG5612 * ：左右のエンドキャップを前面に取り付けます。
- SG5660 * ：ベゼルを前面に取り付けます。

関連情報

"E2700 コントローラドライブトレイおよび関連ドライブトレイ設置ガイド"

"E5600 コントローラドライブトレイおよび関連ドライブトレイ設置ガイド"

アプライアンスのケーブル接続（**SG5600**）

SAS インターコネクトケーブルを使用して、 2 台のコントローラを相互に接続し、管理ポートを適切な管理ネットワークに接続して、 E5600SG コントローラの 10GbE ポートを StorageGRID のグリッドネットワークとオプションのクライアントネットワークに接続する必要があります。

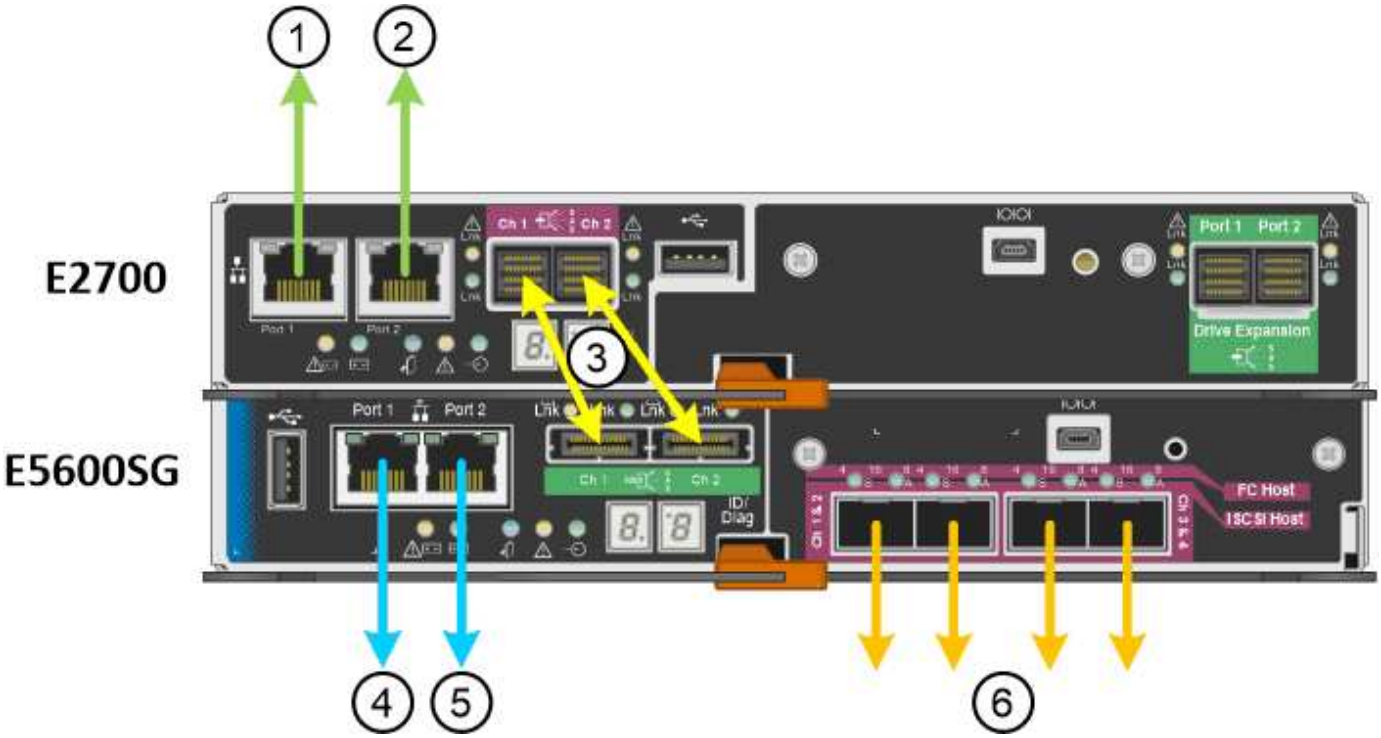
必要なもの

- 管理ポートを接続するためのイーサネットケーブルを用意しておきます。
- 4 つの 10GbE ポートを接続するための光ケーブルを用意しておきます（アプライアンスには付属していません）。

> * レーザー被ばくの危険性 * — SFP トランシーバを分解したり部品を取り外したりしないでください。レーザー被ばくのおそれがあります。

このタスクについて

ケーブルを接続するときは、次の図を参照してください。上の E2700 コントローラと下の E5600SG コントローラが示されています。この図は SG5660 モデルを示しています。 SG5612 モデルのコントローラは、スタックされずに並列に配置されています。



| 項目 | ポート | ポートのタイプ | 機能 |
| --- | --- | --- | --- |
| 1. | E2700 コントローラの管理ポート 1 | 1Gb （ RJ-45 ）イーサネット | E2700 コントローラを、 SANtricity Storage Manager がインストールされているネットワークに接続します。 |
| 2. | E2700 コントローラの管理ポート 2 | 1Gb （ RJ-45 ）イーサネット | 設置時に E2700 コントローラをサービスラップトップに接続します。 |
| 3. | 各コントローラの 2 つの SAS インターコネクトポート、 Ch 1 および Ch 2 | E2700 コントローラ： Mini-SAS - HD<br><br>E5600SG コントローラ： Mini-SAS | 2 台のコントローラを相互に接続します。 |
| 4. | E5600SG コントローラの管理ポート 1 | 1Gb （ RJ-45 ）イーサネット | E5600SG コントローラを StorageGRID の管理ネットワークに接続します。 |
| 5. | E5600SG コントローラの管理ポート 2 | 1Gb （ RJ-45 ）イーサネット | • 管理ネットワークへの冗長接続が必要な場合は、管理ポート 1 とボンディングできます。<br>• 一時的なローカルアクセス用（ IP 169.254.0.1 ）に空けておくことができます。<br>• DHCP によって割り当てられた IP アドレスを使用できない場合、インストール時に E5600SG コントローラをサービスラップトップに接続するために使用できます。 |

| 項目 | ポート | ポートのタイプ | 機能 |
| --- | --- | --- | --- |
| 6. | E5600SG コントローラの 4 つのネットワークポート | 10GbE （光ファイバ） | E5600SG コントローラを StorageGRID のグリッドネットワークとクライアントネットワーク（使用している場合）に接続します。ポートをボンディングしてコントローラへの冗長パスを構成できます。 |

手順

1. 2 本の SAS インターコネクトケーブルを使用して、 E2700 コントローラを E5600SG コントローラに接続します。

| 接続するポート | 接続先のポート |
| --- | --- |
| E2700 コントローラの SAS インターコネクトポート 1 （ Ch 1 | E5600SG コントローラの SAS インターコネクトポート 1 （ Ch 1 |
| E2700 コントローラの SAS インターコネクトポート 2 （ Ch 2 | E5600SG コントローラの SAS インターコネクトポート 2 （ Ch 2 |

E2700 コントローラには四角形のコネクタ（ Mini-SAS HD ）を使用し、 E5600SG コントローラには長方形のコネクタ（ Mini-SAS ）を使用します。

SAS コネクタのプルタブを下にし、各コネクタをカチッと音がして所定の位置に収まるまで慎重に挿入します。抵抗がある場合は、コネクタを押さないでください。プルタブの位置を確認してから続行してください。

2. イーサネットケーブルを使用して、 SANtricity Storage Manager ソフトウェアがインストールされている管理ネットワークに E2700 コントローラを接続します。

| 接続するポート | 接続先のポート |
| --- | --- |
| E2700 コントローラのポート 1 （左側の RJ-45 ポート） | SANtricity Storage Manager に使用する管理ネットワークのスイッチポートを指定します |
| E2700 コントローラのポート 2 | DHCP を使用していない場合は、サービスラップトップを使用します |

3. StorageGRID で管理ネットワークを使用する場合は、イーサネットケーブルを使用して E5600SG コントローラを接続します。

| 接続するポート | 接続先のポート |
| --- | --- |
| E5600SG コントローラのポート 1 （左側の RJ-45 ポート） | StorageGRID の管理ネットワークのスイッチポート |
| E5600SG コントローラのポート 2 | DHCP を使用していない場合は、サービスラップトップを使用します |

4. E5600SG コントローラの 10GbE ポートを、光ケーブルと SFP+ トランシーバを使用して適切なネットワークスイッチに接続します。
   - 固定ポートボンディングモード（デフォルト）を使用する場合は、次の表のように各ポートを StorageGRID のグリッドネットワークまたはクライアントネットワークに接続します。

| ポート | 接続先 |
| --- | --- |
| ポート 1 | クライアントネットワーク（オプション） |
| ポート 2 | Grid ネットワーク |
| ポート 3 | クライアントネットワーク（オプション） |
| ポート 4. | Grid ネットワーク |

   - アグリゲートポートボンディングモードを使用する場合は、 1 つ以上のネットワークポートを 1 つ以上のスイッチに接続します。単一点障害を回避するために、 4 つのポートのうち少なくとも 2 つを接続する必要があります。1 つの LACP ボンドに複数のスイッチを使用する場合は、スイッチが MLAG または同等の機能をサポートしている必要があります。

関連情報

"E5600SG コントローラポートのポートボンディングモード"

"StorageGRID アプライアンスインストーラへのアクセス"

### **AC**電源コードの接続（**SG5600**）

AC 電源コードを外部電源と各コントローラの AC 電源コネクタに接続する必要があります。電源コードを接続したら、電源をオンにできます。

必要なもの

両方のアプライアンスの電源スイッチをオフにしてから、電源を接続する必要があります。

> * 感電の危険性 * — 電源コードを接続する前に、アプライアンスの 2 つの電源スイッチがオフになっていることを確認してください。

このタスクについて

- 電源装置ごとに別々の電源を使用する必要があります。

独立した電源に接続することで、電力の冗長性が維持されます

- コントローラに付属の電源コードは、無停電電源装置（ UPS ）の壁面コンセントなど、それぞれの国で使用される一般的なコンセントで使用できます。

  ただし、 EIA 準拠のほとんどのキャビネットには対応していないことに注意してください。

手順

1. エンクロージャまたはシャーシの電源スイッチをオフにします。
2. コントローラの電源スイッチをオフにします。
3. 主電源コードをキャビネットから外部電源に接続します。
4. 各コントローラの AC 電源コネクタに電源コードを接続します。

電源のオン（**SG5600**）

## エンクロージャの電源を入れると、両方のコントローラの電源がオンになります。

手順

1. エンクロージャの背面にある 2 つの電源スイッチをオンにします。

   電源が投入されている間、コントローラの LED が断続的に点灯または消灯します。

   電源投入プロセスが完了するまでに最大 10 分かかることがあります。最初の起動時にコントローラが数回リブートすると、ファンの速度が低下し、 LED が点滅します。

2. 各コントローラの電源 LED とホストリンクアクティブ LED で、電源がオンになっていることを確認します。
3. すべてのドライブが緑の永続的 LED で点灯し、オンラインになったことが示されるまで待ちます。
4. エンクロージャの前面と背面に緑の LED があることを確認します。

   オレンジ色の LED がある場合は、その場所をメモします。

5. E5600SG コントローラのデジタル表示ディスプレイを確認します。

   このディスプレイには * HO * が表示され、続いて 2 桁の数字が順番に表示されます。

   ```
   HO -- IP address for Admin Network -- IP address for Grid Network HO
   ```

   最初に表示される数字は、コントローラの管理ポート 1 に対して DHCP によって割り当てられた IP アドレスです。このアドレスは、コントローラを StorageGRID の管理ネットワークに接続するときに使用されます。2 番目に表示される数字は、 StorageGRID のグリッドネットワークにアプライアンスを接続するときに使用される DHCP によって割り当てられた IP アドレスです。

   DHCP を使用して IP アドレスを割り当てることができなかった場合は、 0.0.0.0 と表示されます。

## SG5600コントローラのブート時のステータスコードとエラーコードの確認

アプライアンスの電源投入やハードウェアの初期化の実行時、ハードウェアで障害が発生して初期化を取り消す必要がある場合など、各コントローラのデジタル表示ディスプレイにステータスコードとエラーコードが表示されます。進行状況の監視やトラブルシューティングの際は、表示される順番に一連のコードを確認する必要があります。

### このタスクについて

E5600SG コントローラのステータスコードとエラーコードは、 E2700 コントローラのものとは異なります。

### 手順

1. ブート時の進行状況を監視するには、デジタル表示ディスプレイに表示されるコードを確認します。
2. E5600SG コントローラのエラーコードについては、デジタル表示ディスプレイのステータスとエラーコードの情報を参照してください。
3. E2700 コントローラのエラーコードについては、サポートサイトの E2700 コントローラのドキュメントを参照してください。

### 関連情報

"E5600SG コントローラのデジタル表示ディスプレイのコード"

"ネットアップのマニュアル： E2700 シリーズ"

## E5600SG コントローラのデジタル表示ディスプレイのコード

アプライアンスの電源投入やハードウェアの初期化の実行時、 E5600SG コントローラのデジタル表示ディスプレイにステータスコードとエラーコードが表示されます。これらのコードからステータスを確認し、エラーのトラブルシューティングを行うことができます。

E5600SG コントローラのステータスコードとエラーコードを確認するときは、次の種類のコードを確認する必要があります。

- * 一般的な起動コード *

  標準のブートイベントを表します。

- * 通常の起動コード *

  アプライアンスで発生する正常なブートイベントを表します。

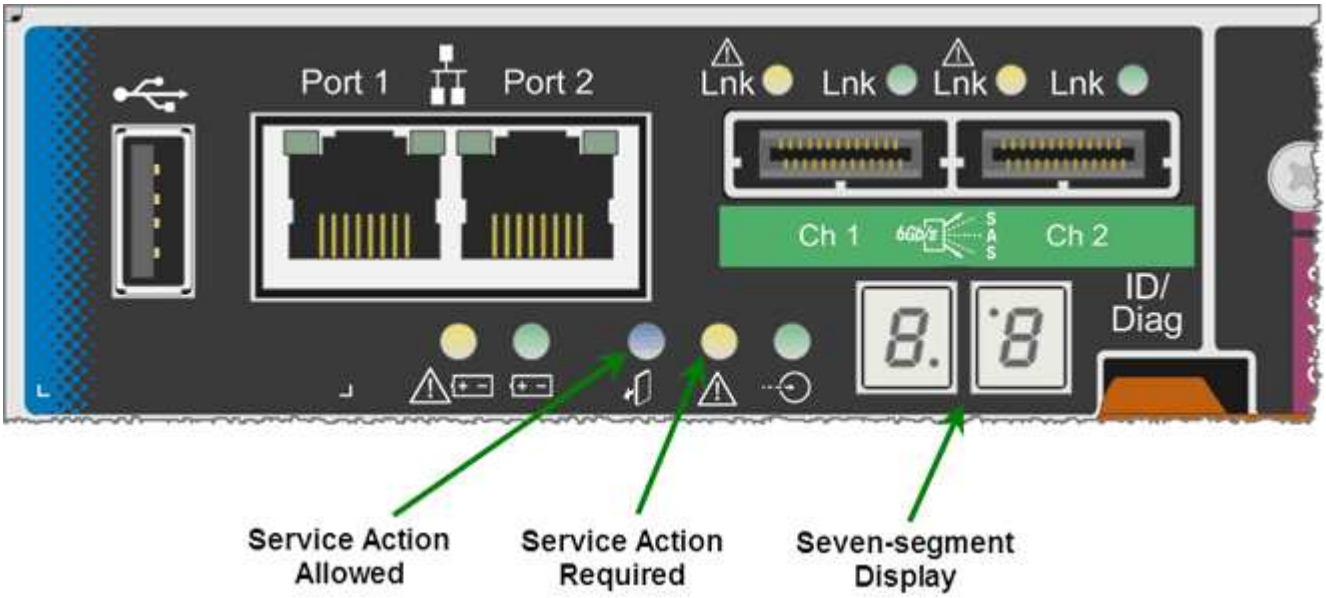
- * エラーコード *

  ブートイベント中に問題が発生したことを示します。

StorageGRID は、 StorageGRID アプライアンスインストーラが起動されるまで、 E5600SG コントローラの次の LED のみを制御します。

- 保守操作可能

- 保守操作要
- デジタル表示ディスプレイ




デジタル表示ディスプレイの小数点は、 StorageGRID アプライアンスでは使用されません。

- 小さい方の桁の上に表示される小数点はプラットフォーム診断 LED です。

  この機能は、ハードウェアのリセット時および初期設定時にオンになります。それ以外の場合はオフになります。

- 大きい方の桁の下に表示される小数点はオフになります。

その他の問題を診断するには、必要に応じて次のリソースを参照してください。

- ハードウェアや環境のその他すべての診断情報を確認するには、 E シリーズオペレーティングシステムのハードウェア診断を参照してください。

  これには、電源、温度、ディスクドライブなどのハードウェアの問題が含まれます。このアプライアンスでは、 E シリーズオペレーティングシステムを使用して、プラットフォームのすべての環境ステータスを監視します。

- ファームウェアとドライバの問題を確認するには、 SAS ポートとネットワークポートのリンク LED を確認します。

  詳細については、 E シリーズ E5600 のドキュメントを参照してください。

一般的なブートコード

ハードウェアのブート時やハードリセット後、ハードウェアの初期化中は、保守操作可能と保守操作要を示す LED が点灯します。デジタル表示ディスプレイには、 E シリーズハードウェアと E5600SG コントローラに固有のコードではなく、同じコードが表示されます。

ブート時に、 Field Programmable Gate Array （ FPGA ）でハードウェアの機能と初期化が制御されます。

| コード | 表示 |
| --- | --- |
| 19 | FPGA の初期化。 |
| 68 | FPGA の初期化。 |
| … | FPGA の初期化。コードが連続して表示されます。 |
| AA | プラットフォームの BIOS ブートを実行中です。 |
| FF | BIOS のブートが完了しました。これは、 E5600SG コントローラが LED を初期化してステータスを管理する前の中間状態です。 |

AA と FF のコードが表示されたあと、正常なブートコードかエラーコードのいずれかが表示されます。また、保守操作可能と保守操作要を示す LED が消灯します。

正常なブートコード

これらのコードは、アプライアンスで発生する正常なブートイベントを時間順に表します。

| コード | 表示 |
| --- | --- |
| こんにちは | マスターブートスクリプトが開始されました。 |
| PP （ PP ） | プラットフォームの FPGA ファームウェアが更新をチェックしています。 |
| HP | ホストインターフェイスカード（ HIC ）の更新を確認しています。 |
| 朝食付き | ファームウェアの更新後、必要に応じてシステムをリブートします。 |
| FP | ファームウェアの更新の確認が完了しました。E2700 コントローラと通信して管理するためのプロセス（ utmagent ）を開始しています。このプロセスにより、アプライアンスのプロビジョニングが容易になります。 |
| 彼 | システムを E シリーズオペレーティングシステムと同期しています。 |
| HC | StorageGRID のインストールを確認しています。 |

| コード | 表示 |
| --- | --- |
| HO | インストールの管理とアクティブな接続を実行中です。 |
| 高可用性 | Linux オペレーティングシステムと StorageGRID が実行されている。 |

**E5600SG** コントローラのエラーコード

これらのコードは、アプライアンスのブート時に E5600SG コントローラで表示される可能性があるエラー状態を表しています。特定の下位レベルのハードウェアエラーが発生した場合は、 2 桁の 16 進数コードが追加で表示されます。これらのいずれかのコードが数秒にわたって表示され、規定のトラブルシューティング手順を実行してもエラーを解決できない場合は、テクニカルサポートにお問い合わせください。

| コード | 表示 |
| --- | --- |
| 22 | どのブートデバイスにもマスターブートレコードが見つかりません。 |
| 23 | SATA ドライブが取り付けられていません。 |
| 2A 、 2B | スタックバスにより、 DIMM SPD データを読み取れません。 |
| 40 | DIMM が無効です。 |
| 41. | DIMM が無効です。 |
| 42 | メモリテストに失敗しました。 |
| 51 | SPD の読み取りに失敗しました。 |
| 92 ~ 96 | PCI バスの初期化中です。 |
| A0 から A3 | SATA ドライブの初期化中です。 |
| AB | 代替ブートコードです。 |
| AE | OS のブート中です。 |
| EA | DDR3 トレーニングに失敗しました。 |
| E8. | メモリが取り付けられていません。 |

| コード | 表示 |
| --- | --- |
| 欧州連合（ EU | インストールスクリプトが見つかりませんでした。 |
| EP | 「 ManageSGA 」コードは、 E2700 コントローラとのグリッド構成前の通信に失敗したことを示します。 |

関連情報

"ハードウェアの設置のトラブルシューティング"

"ネットアップサポート"

## ハードウェアの設定

アプライアンスの電源を入れたら、ハードウェアの監視に使用するソフトウェアである SANtricity Storage Manager を設定する必要があります。また、 StorageGRID で使用されるネットワーク接続も設定する必要があります。

手順

- "StorageGRID 接続を設定しています"
- "SANtricity Storage Managerを設定しています"
- "オプション：ノード暗号化を有効にする"
- "オプション：RAID 6モードへの変更（SG5660のみ）"
- "オプション：アプライアンスに対するネットワークポートの再マッピング"

### StorageGRID 接続を設定しています

StorageGRID アプライアンスをストレージノードとして StorageGRID グリッドに導入するには、アプライアンスと使用するネットワークの間の接続を設定する必要があります。ネットワークを設定するには、 StorageGRID アプライアンスインストーラを使用します。インストーラは、 E5600SG コントローラ（アプライアンスのコンピューティングコントローラ）に搭載されています。

手順

- "StorageGRID アプライアンスインストーラへのアクセス"
- "StorageGRID アプライアンスインストーラのバージョンの確認とアップグレード"
- "ネットワークリンクの設定（SG5600）"
- "IPの設定"
- "ネットワーク接続の確認"
- "ポートレベルのネットワーク接続の確認"

# アプライアンスと 3 つの StorageGRID ネットワーク（グリッドネットワーク、管理ネットワーク（オプション）、クライアントネットワーク（オプション））間の接続を設定するには、 StorageGRID アプライアンスインストーラにアクセスする必要があります。

必要なもの

- サポートされているWebブラウザを使用します。
- 使用するすべての StorageGRID ネットワークにアプライアンスを接続しておきます。
- これらのネットワークでのアプライアンスの IP アドレス、ゲートウェイ、およびサブネットを確認しておきます。
- 使用するネットワークスイッチを設定しておきます。

このタスクについて

StorageGRID アプライアンスインストーラに初めてアクセスするときは、 DHCP によって割り当てられた管理ネットワークの IP アドレス（アプライアンスが管理ネットワークに接続されている場合）または DHCP によって割り当てられたグリッドネットワークの IP アドレスを使用できます。管理ネットワークの IP アドレスを使用することを推奨します。グリッドネットワークの DHCP アドレスを使用して StorageGRID アプライアンスインストーラにアクセスすると、リンク設定を変更した場合や静的な IP アドレスを入力した場合に StorageGRID アプライアンスインストーラとの接続が失われる可能性があります。

手順

1. 管理ネットワークが接続されている場合は、管理ネットワークでのアプライアンスの DHCP アドレスを取得し、管理ネットワークが接続されていない場合はグリッドネットワークの DHCP アドレスを取得します。

   次のいずれかを実行できます。

   - 管理ポート 1 の MAC アドレスをネットワーク管理者に伝え、管理者が管理ネットワークでのこのポートの DHCP アドレスを確認できるようにします。MAC アドレスは、ポートの横の E5600SG コントローラのラベルに記載されています。
   - E5600SG コントローラのデジタル表示ディスプレイを確認します。E5600SG コントローラの管理ポート 1 と 10GbE ポート 2 と 4 を DHCP サーバがあるネットワークに接続している場合は、エンクロージャの電源投入時に動的に割り当てられた IP アドレスをコントローラが取得しようとします。コントローラの電源投入プロセスが完了すると、デジタル表示ディスプレイに * HO * と表示され、続いて 2 つの数字が順番に表示されます。

     ```
     HO -- IP address for Admin Network -- IP address for Grid Network HO
     ```

     次の順序で実行します。

     - 最初に表示される数字は、管理ネットワークに接続されているアプライアンスストレージノードの DHCP アドレスです。この IP アドレスは、 E5600SG コントローラの管理ポート 1 に割り当てられています。
     - 2 番目に表示される数字は、グリッドネットワーク上のアプライアンスストレージノードの DHCP アドレスです。この IP アドレスは、アプライアンスに最初に電源を投入するときに、 10GbE ポ

ート 2 と 4 に割り当てられます。

DHCP を使用して IP アドレスを割り当てることができなかった場合は、 0.0.0.0 と表示されます。

2. いずれかの DHCP アドレスを取得できた場合は、次の手順を実行します。

   a. サービスラップトップで Web ブラウザを開きます。

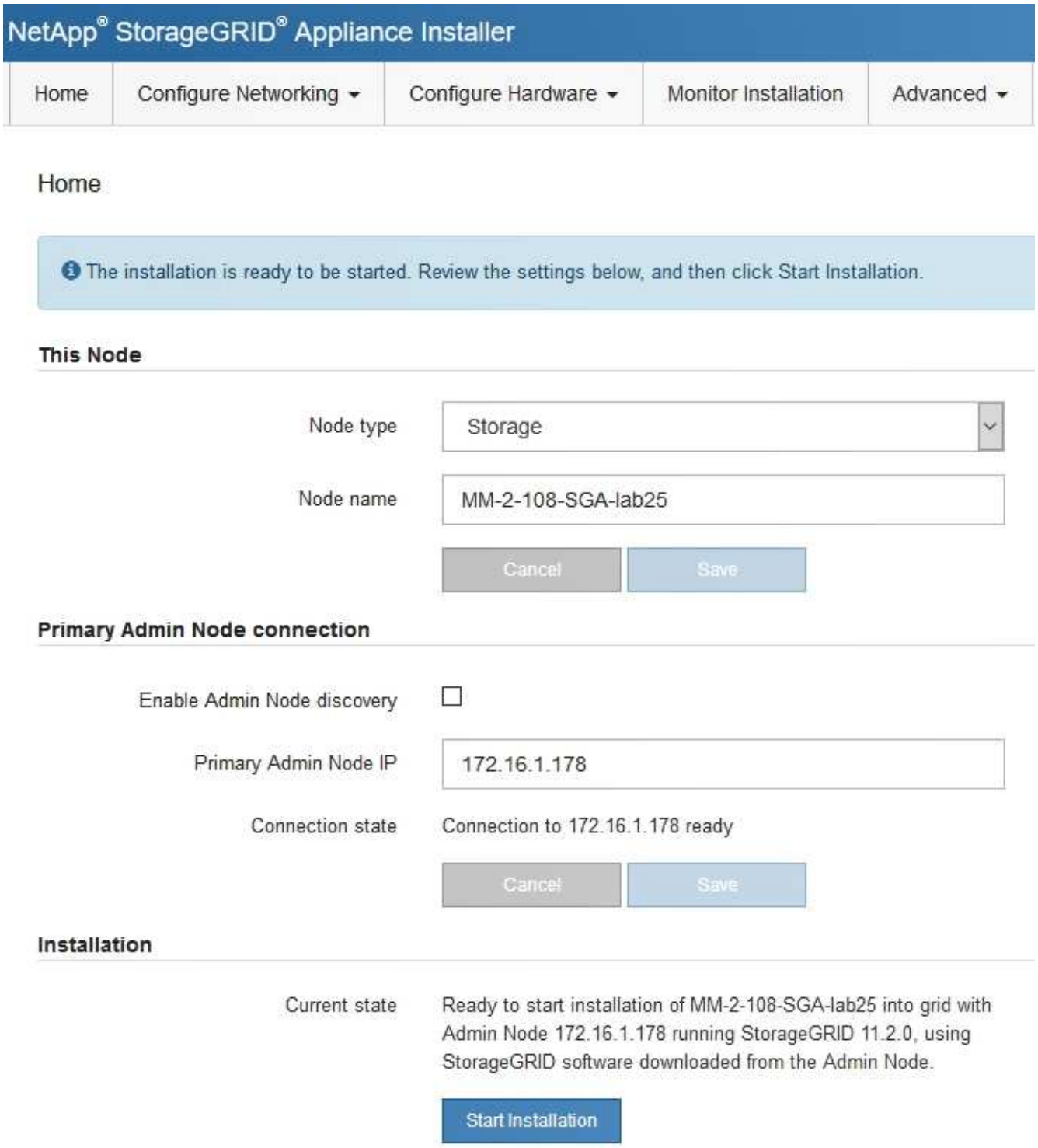
   b. StorageGRID アプライアンスインストーラのURLに+を入力します
   **`https://E5600SG_Controller_IP:8443`**

   の場合 `*E5600SG_Controller_IP*`を使用して、コントローラのDHCPアドレスを指定します（管理ネットワークを使用する場合はそのIPアドレスを使用）。

   c. セキュリティアラートが表示された場合は、ブラウザのインストールウィザードを使用して証明書を表示およびインストールします。

   次回この URL にアクセスしたときに、アラートは表示されません。

   StorageGRID アプライアンスインストーラのホームページが表示されます。このページに最初にアクセスしたときに表示される情報とメッセージは、アプライアンスと StorageGRID ネットワークの現在の接続状況によって異なります。エラーメッセージが表示された場合は、以降の手順で解決されます。




3. E5600SG コントローラが DHCP を使用して IP アドレスを取得できなかった場合は、次の手順を実行します。

   a. イーサネットケーブルを使用して、サービスラップトップを E5600SG コントローラの管理ポート 2 に接続します。

b. サービスラップトップで Web ブラウザを開きます。

c. StorageGRID アプライアンスインストーラのURLに+を入力します
**`https://169.254.0.1:8443`**

StorageGRID アプライアンスインストーラのホームページが表示されます。このページに最初にアクセスしたときに表示される情報とメッセージは、アプライアンスの現在の接続状況によって異なります。

> リンクローカル接続でホームページにアクセスできない場合は、サービスラップトップのIPアドレスをに設定します `169.254.0.2`をクリックして、もう一度やり直してください。

4. ホームページに表示されたメッセージを確認し、必要に応じてリンク設定と IP 設定を行います。

関連情報

"Web ブラウザの要件"

**StorageGRID** アプライアンスインストーラのバージョンの確認とアップグレード

## StorageGRID のすべての機能がサポートされるようにするには、アプライアンスの StorageGRID アプライアンスインストーラのバージョンと StorageGRID システムにインストールされているソフトウェアのバージョンが一致している必要があります。

必要なもの

StorageGRID アプライアンスインストーラにアクセスしておきます。

StorageGRID アプライアンスは、 StorageGRID アプライアンスインストーラがプリインストールされた状態で出荷されます。最近アップグレードした StorageGRID システムにアプライアンスを追加する場合は、そのアプライアンスを新しいノードとしてインストールする前に、 StorageGRID アプライアンスインストーラの手動アップグレードが必要になることがあります。

新しい StorageGRID バージョンにアップグレードすると、 StorageGRID アプライアンスインストーラが自動的にアップグレードされます。インストールされているアプライアンスノードでは、 StorageGRID アプライアンスインストーラをアップグレードする必要はありません。この手順 が必要になるのは、以前のバージョンの StorageGRID アプライアンスインストーラを搭載したアプライアンスをインストールする場合のみです。

手順

1. StorageGRID アプライアンス・インストーラから、 * アドバンスト * > * アップグレード・ファームウェア * を選択します。
2. 現在のファームウェアバージョンとStorageGRID システムにインストールされているソフトウェアバージョンを比較します（Grid Managerから* Help > About *を選択します）。

2 つのバージョンの 2 桁目の数字が一致している必要があります。たとえば、StorageGRID システムでバージョン11.* 5 。***x*.y_y__**を実行している場合、**StorageGRID** アプライアンスインストーラのバージョンは**3.** 5 *._z_にする必要があります。

3. アプライアンスに StorageGRID アプライアンスインストーラの下位バージョンがインストールされている場合は、 StorageGRID のネットアップのダウンロードページにアクセスします。

   "ネットアップのダウンロード： StorageGRID"

   ネットアップアカウントのユーザ名とパスワードを使用してサインインします。

4. StorageGRID アプライアンス * 対応するバージョンのサポート・ファイルと対応するチェックサム・ファイルをダウンロードします。

   StorageGRID アプライアンスファイルのサポートファイルは、です `.zip` すべてのStorageGRID アプライアンスモデルの最新および以前のファームウェアバージョンを、各コントローラタイプのサブディレクトリに格納してアーカイブする。

   StorageGRID アプライアンスファイルのサポートファイルをダウンロードしたら、を展開します `.zip` StorageGRID アプライアンスインストーラのインストールに関する重要な情報については、READMEファイルをアーカイブして参照してください。

5. StorageGRID アプライアンスインストーラのファームウェアのアップグレードページの手順に従って、次の手順を実行します。

   a. コントローラタイプとチェックサムファイルに適したサポートファイル（ファームウェアイメージ）をアップロードします。

   b. 非アクティブなパーティションをアップグレードします。

   c. パーティションを再起動してスワップします。

   d. 2番目のパーティションをアップグレードします。

関連情報

"StorageGRID アプライアンスインストーラへのアクセス"

ネットワークリンクの設定（**SG5600**）

# アプライアンスをグリッドネットワーク、クライアントネットワーク、および管理ネットワークに接続するために使用するポートのネットワークリンクを設定できます。リンク速度およびポートボンディングモードとネットワークボンディングモードを設定できます。

必要なもの

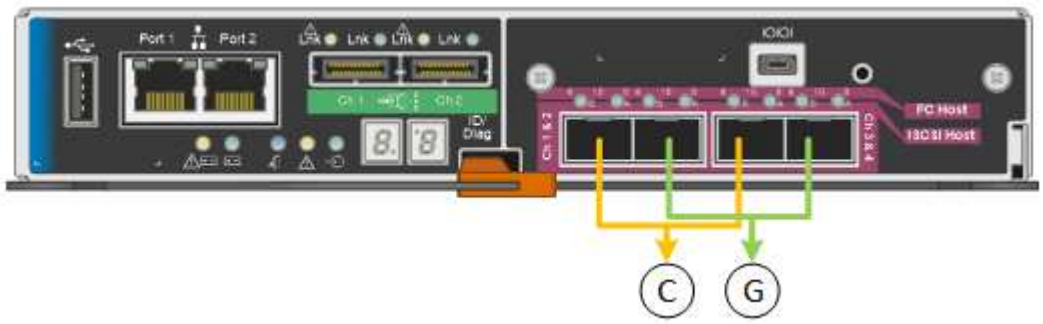
アグリゲートポートボンディングモード、 LACP ネットワークボンディングモード、または VLAN タギングを使用する場合

- アプライアンスの 10GbE ポートを、 VLAN と LACP をサポートするスイッチに接続しておきます。
- 複数のスイッチを LACP ボンドに加える場合は、 Multi-Chassis Link Aggregation （ MLAG ）グループまたは同等の機能をサポートするスイッチを使用します。
- VLAN 、 LACP 、 MLAG などを使用するようにスイッチを設定する方法について理解しておく必要があります。

- 各ネットワークに使用する一意の VLAN タグを確認しておきます。この VLAN タグが各ネットワークパケットに追加され、ネットワークトラフィックが正しいネットワークにルーティングされます。

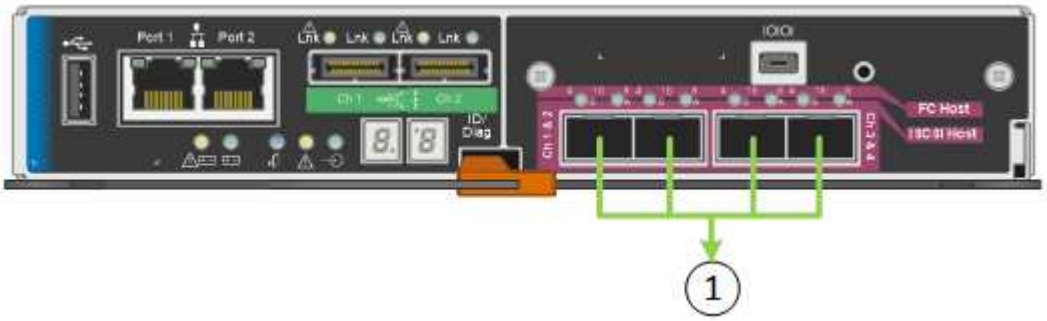
このタスクについて

次の図では、 4 つの 10GbE ポートが固定ポートボンディングモードでボンディングされています（デフォルトの構成）。




| | ボンディングされるポート |
|---|---|
| C | このネットワークを使用する場合、ポート 1 とポート 3 がクライアントネットワーク用にボンディングされます。 |
| G | ポート 2 とポート 4 がグリッドネットワーク用にボンディングされます。 |

次の図では、 4 つの 10GbE ポートがアグリゲートポートボンディングモードでボンディングされています。




| | ボンディングされるポート |
|---|---|
| 1. | 4 つのポートすべてを 1 つの LACP ボンドにグループ化して、すべてのポートをグリッドネットワークとクライアントネットワークのトラフィックに使用できるようにします。 |

次の表に、 4 つの 10GbE ポートを設定するためのオプションをまとめます。デフォルト以外の設定を使用する場合にのみ、 Link Configuration ページで設定を行う必要があります。

- * 固定（デフォルト）ポートボンディングモード *

| ネットワークボンディングモード | クライアントネットワークが無効な場合（デフォルト） | クライアントネットワークが有効になりました |
| --- | --- | --- |
| アクティブ/バックアップ（デフォルト） | • ポート 2 と 4 がグリッドネットワークにアクティブ / バックアップボンドを使用します。<br>• ポート 1 と 3 は使用されません。<br>• VLAN タグはオプションです。 | • ポート 2 と 4 がグリッドネットワークにアクティブ / バックアップボンドを使用します。<br>• ポート 1 と 3 がクライアントネットワークに Active-Backup ボンドを使用します。<br>• ネットワーク管理者用に、両方のネットワークに VLAN タグを指定できます。 |
| LACP （ 802.3ad ） | • ポート 2 と 4 がグリッドネットワークに LACP ボンドを使用します。<br>• ポート 1 と 3 は使用されません。<br>• VLAN タグはオプションです。 | • ポート 2 と 4 がグリッドネットワークに LACP ボンドを使用します。<br>• ポート 1 と 3 がクライアントネットワークに LACP ボンドを使用します。<br>• ネットワーク管理者用に、両方のネットワークに VLAN タグを指定できます。 |

- * アグリゲートポートボンディングモード *

| ネットワークボンディングモード | クライアントネットワークが無効な場合（デフォルト） | クライアントネットワークが有効になりました |
| --- | --- | --- |
| LACP （ 802.3ad ）のみ | • ポート 1~4 がグリッドネットワークに単一の LACP ボンドを使用します。<br>• 単一の VLAN タグでグリッドネットワークのパケットが識別されます。 | • ポート 1~4 がグリッドネットワークとクライアントネットワークに単一の LACP ボンドを使用します。<br>• 2 つの VLAN タグで、グリッドネットワークのパケットとクライアントネットワークのパケットを分離できます。 |

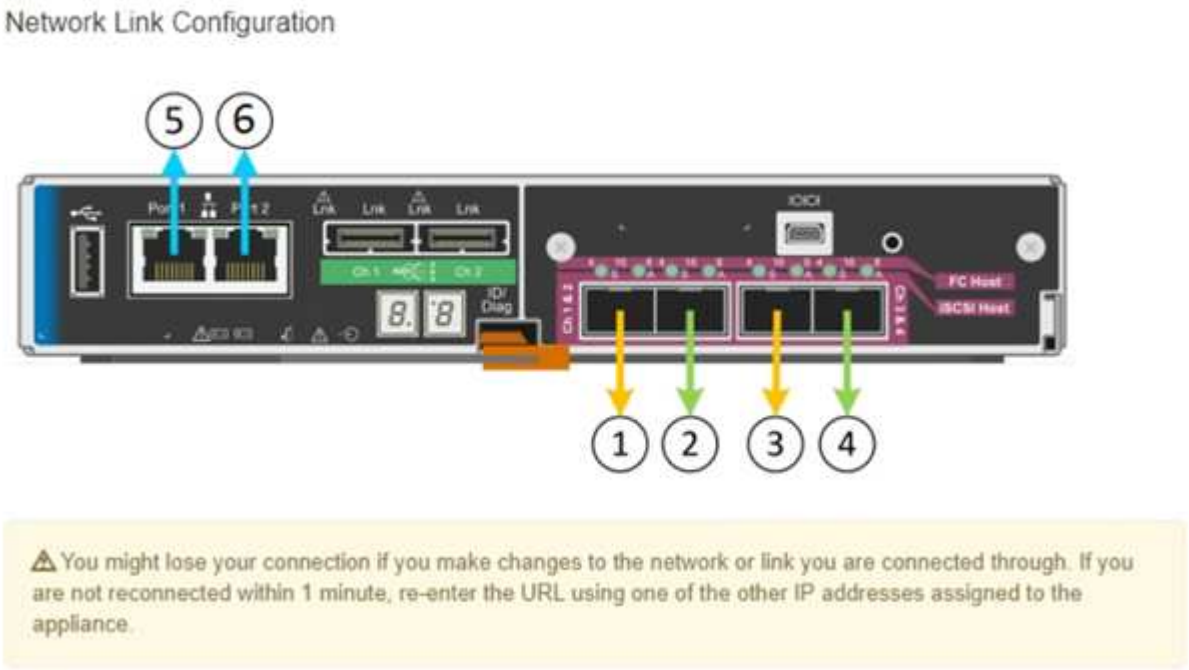
ポートボンディングモードとネットワークボンディングモードの詳細については、「 E5600SG コントローラでの 10 GbE ポート接続」を参照してください。

次の図では、 E5600SG コントローラの 2 つの 1GbE 管理ポートが管理ネットワーク用に Active-Backup ネットワークボンディングモードでボンディングされています。

手順

1. StorageGRID アプライアンスインストーラのメニューバーから、 *Configure Networking *>*Link Configuration * をクリックします。

Network Link Configuration ページには、アプライアンスの図と、ネットワークポートおよび管理ポートの番号が表示されます。




Link Status テーブルには、番号が付けられたポートのリンクステート（アップ / ダウン）と速度（ 1/10/25 / 40/100Gbps ）が表示されます。

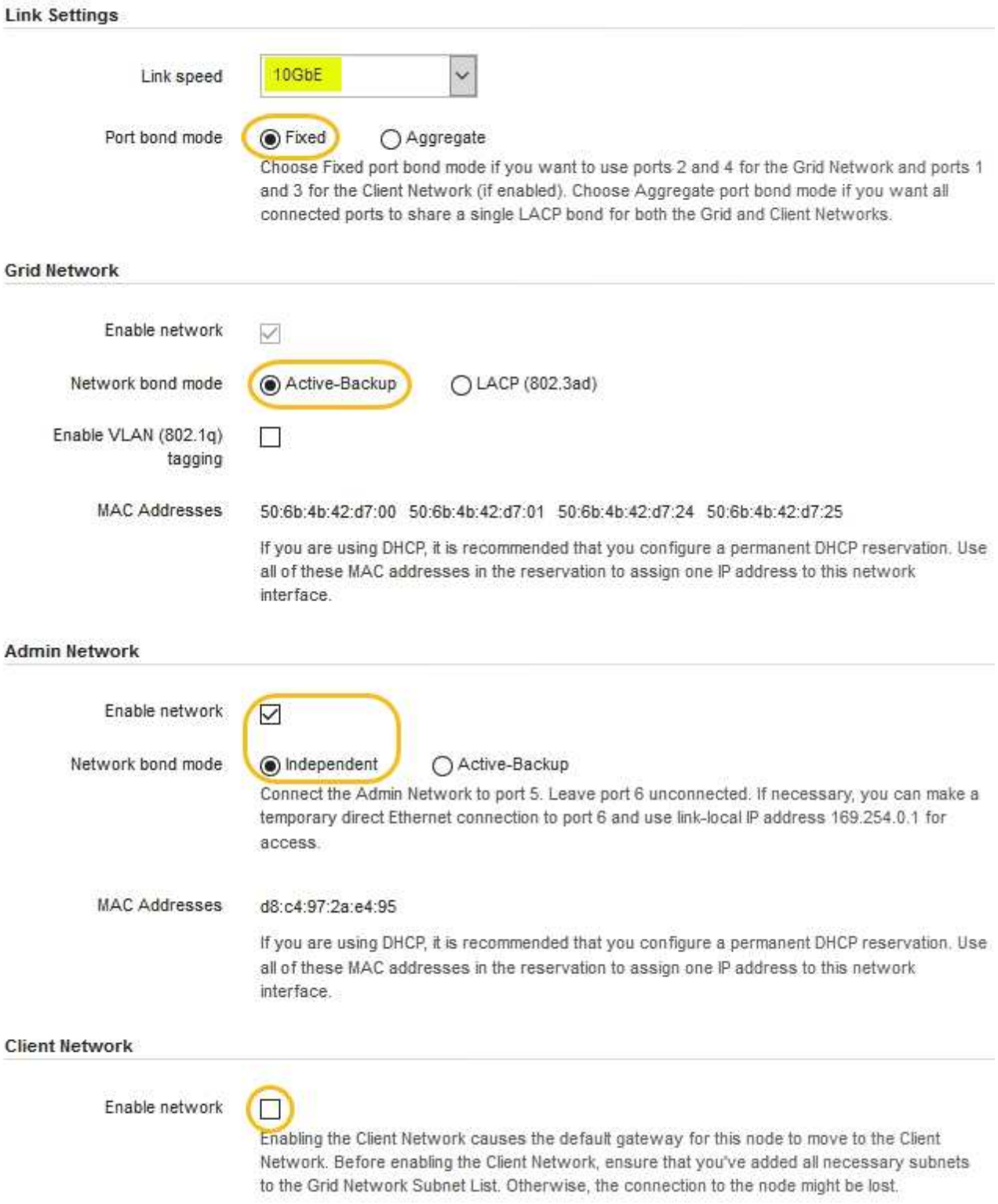
**Link Status**

| Link | State | Speed (Gbps) |
|---|---|---|
| 1 | Down | N/A |
| 2 | Up | 10 |
| 3 | Up | 10 |
| 4 | Down | N/A |
| 5 | Up | 1 |
| 6 | Up | 1 |

このページに初めてアクセスしたときの動作は次のとおりです。

- * リンク速度 * は * 10GbE * に設定されています。これは、 E5600SG コントローラで使用できる唯一のリンク速度です。
- * ポートボンディングモード * は「 * Fixed 」に設定されます。
- * グリッドネットワークのネットワークボンディングモード * が「アクティブ / バックアップ」に設定されています。

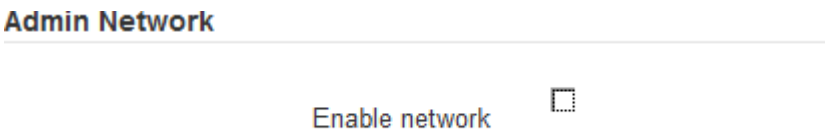
- 管理ネットワーク * が有効になっており、ネットワークボンディングモードが * Independent * に設定されています。
- クライアントネットワーク * が無効になっています。




2. 使用する StorageGRID ネットワークを有効または無効にします。

   グリッドネットワークは必須です。このネットワークは無効にできません。

a. アプライアンスが管理ネットワークに接続されていない場合は、管理ネットワークの * ネットワークを有効にする * チェックボックスの選択を解除します。



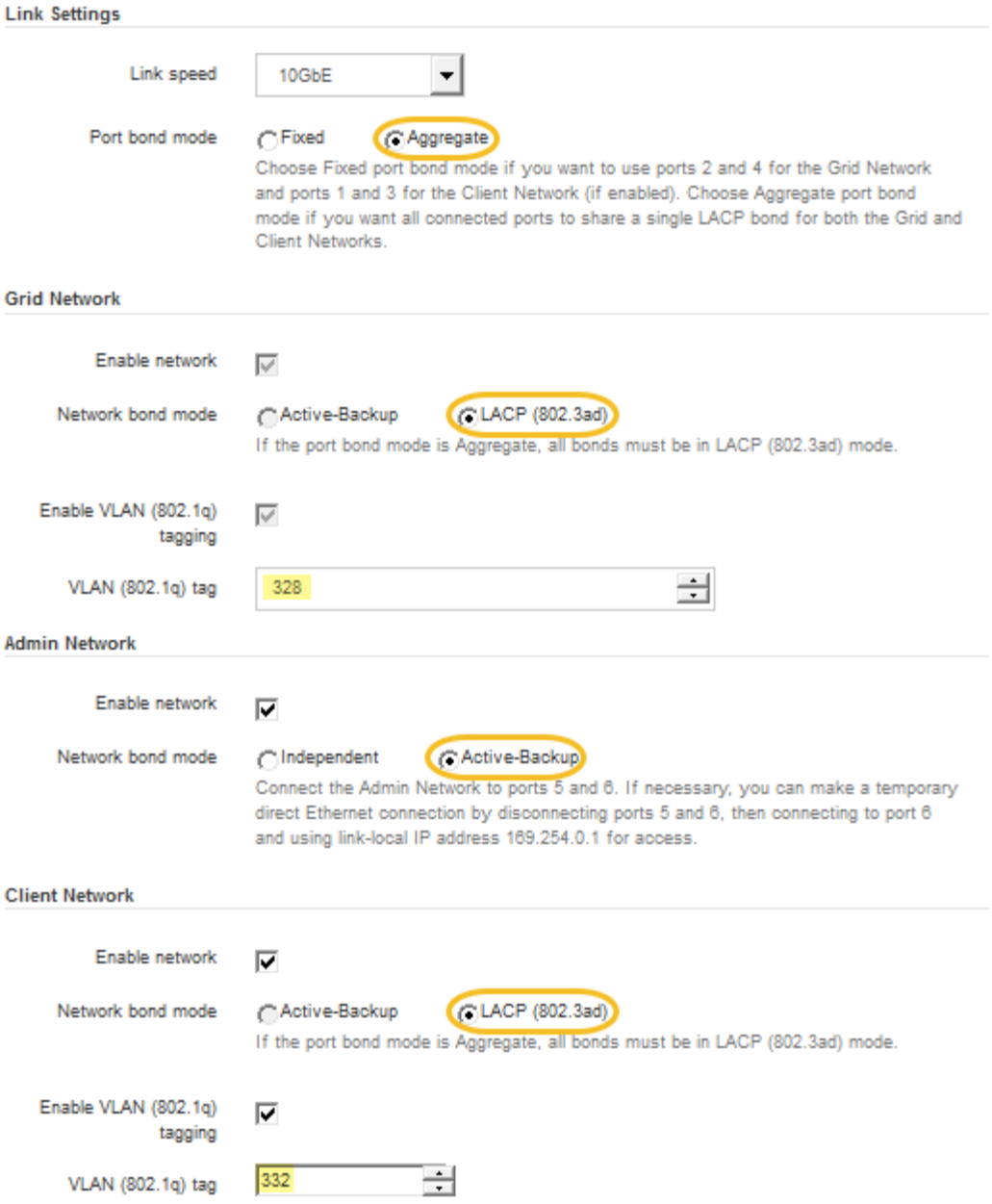

b. アプライアンスがクライアントネットワークに接続されている場合は、クライアントネットワークの * ネットワークを有効にする * チェックボックスをオンにします。

これで、 10GbE ポートでのクライアントネットワークの設定が表示されます。

3. 表を参照して、ポートボンディングモードとネットワークボンディングモードを設定します。

この例では、次のように

- * グリッドネットワークとクライアントネットワークでアグリゲート * と * LACP * が選択されました。各ネットワークに一意の VLAN タグを指定する必要があります。値は 0~4095 の間で選択できます。
- * 管理ネットワーク用に選択されたアクティブ / バックアップ * 。




4. 選択に問題がなければ、 * 保存 * をクリックします。

> 接続しているネットワークまたはリンクを変更すると、接続が失われる可能性があります。1分以内に再接続されない場合は、アプライアンスに割り当てられている他のIPアドレスのいずれかを使用してStorageGRID アプライアンスインストーラのURLを再入力します：+
> **`https://E5600SG_Controller_IP:8443`**

関連情報

"E5600SG コントローラポートのポートボンディングモード"

**IP**の設定

## StorageGRID アプライアンスインストーラを使用して、 StorageGRID のグリッドネッ

# トワーク、管理ネットワーク、クライアントネットワークでアプライアンスストレージノードに使用される IP アドレスとルーティング情報を設定します。

このタスクについて

接続された各ネットワークでアプライアンスの静的 IP を割り当てるか、 DHCP サーバでアドレスの永久リースを割り当てる必要があります。

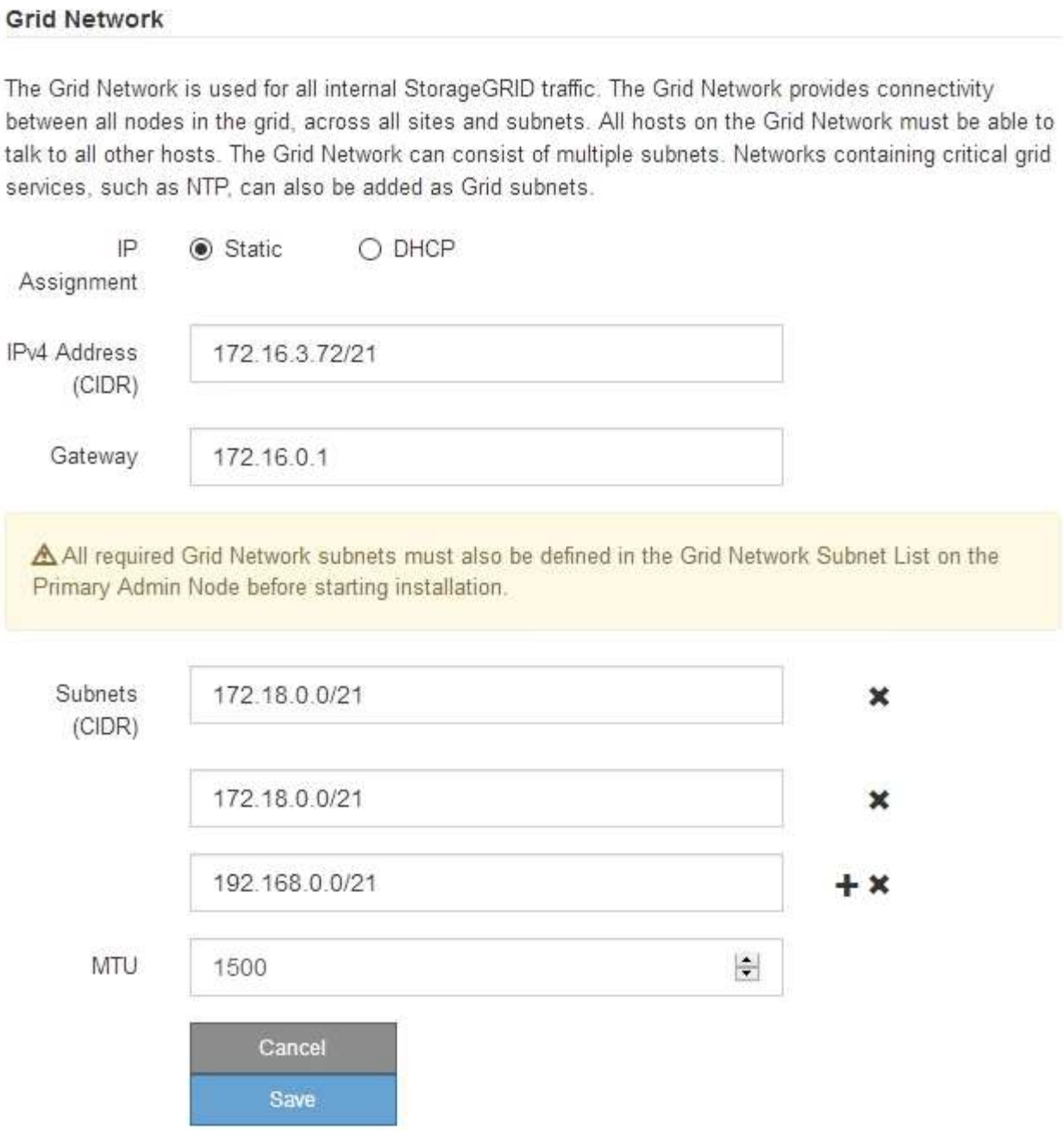
リンク設定を変更する場合は、 E5600SG コントローラのリンク設定の変更手順を参照してください。

手順

1. StorageGRID アプライアンスインストーラで、 * ネットワークの設定 * > * IP 構成 * を選択します。

   [IP Configuration] ページが表示されます。

2. グリッドネットワークを設定するには、ページの * グリッドネットワーク * セクションで * 静的 * または * DHCP * のいずれかを選択します。




3. 「 * Static * 」を選択した場合は、次の手順に従ってグリッドネットワークを設定します。
   a. CIDR 表記を使用して静的 IPv4 アドレスを入力します。
   b. ゲートウェイを入力します。

      ネットワークにゲートウェイがない場合は、同じ静的 IPv4 アドレスを再入力します。

   c. ジャンボフレームを使用する場合は、 MTU フィールドを 9000 などのジャンボフレームに適した値に変更します。それ以外の場合は、デフォルト値 1500 のままにします。

      ネットワークの MTU 値は、ノードが接続されているスイッチポートに設定されている値と同じである必要があります。そうしないと、ネットワークパフォーマンスの問題やパケット損失が発生する可能性があります。

ネットワークのパフォーマンスを最大限に高めるには、すべてのノードのグリッドネットワークインターフェイスで MTU 値がほぼ同じになるように設定する必要があります。個々のノードのグリッドネットワークの MTU 設定に大きな違いがある場合は、 * Grid Network MTU mismatch * アラートがトリガーされます。MTU 値はすべてのネットワークタイプで同じである必要はありません。

d. [ 保存（ Save ） ] をクリックします。

IP アドレスを変更すると、ゲートウェイとサブネットのリストも変更される可能性があります。

StorageGRID アプライアンスインストーラへの接続が失われた場合は、割り当てた新しい静的 IP アドレスを使用して URL を再入力します。たとえば、「+」と入力します
`https://services_appliance_IP:8443`

e. グリッドネットワークのサブネットのリストが正しいことを確認します。

グリッドサブネットがある場合は、グリッドネットワークゲートウェイが必要です。指定するすべてのグリッドサブネットが、このゲートウェイ経由でアクセス可能であることが必要です。StorageGRID のインストールを開始するときに、プライマリ管理ノードのグリッドネットワークサブネットリストでこれらのサブネットも定義する必要があります。

デフォルトルートはリストされません。クライアントネットワークが有効になっていない場合は、デフォルトルートがグリッドネットワークゲートウェイを使用します。

- サブネットを追加するには、挿入アイコンをクリックします ➕ アイコン"] をクリックします。
- 使用されていないサブネットを削除するには、削除アイコンをクリックします ✖。

f. [ 保存（ Save ） ] をクリックします。

4. 「 * DHCP * 」を選択した場合は、次の手順に従ってグリッドネットワークを設定します。

a. [**DHCP**] ラジオボタンを選択した後、 [**Save**] をクリックします。

[* IPv4 アドレス * ] 、 [ * ゲートウェイ * ] 、および [ * サブネット * ] フィールドには、自動的に値が入力されます。DHCP サーバが MTU 値を割り当てるように設定されている場合は、 **MTU** フィールドにその値が入力され、フィールドは読み取り専用になります。

Web ブラウザは、 StorageGRID アプライアンスインストーラの新しい IP アドレスに自動的にリダイレクトされます。

b. グリッドネットワークのサブネットのリストが正しいことを確認します。

グリッドサブネットがある場合は、グリッドネットワークゲートウェイが必要です。指定するすべてのグリッドサブネットが、このゲートウェイ経由でアクセス可能であることが必要です。StorageGRID のインストールを開始するときに、プライマリ管理ノードのグリッドネットワークサブネットリストでこれらのサブネットも定義する必要があります。

デフォルトルートはリストされません。クライアントネットワークが有効になっていない場合は、デフォルトルートがグリッドネットワークゲートウェイを使用します。

- サブネットを追加するには、挿入アイコンをクリックします ➕ アイコン"] をクリックします。

- 使用されていないサブネットを削除するには、削除アイコンをクリックします ✖。

c. ジャンボフレームを使用する場合は、 MTU フィールドを 9000 などのジャンボフレームに適した値に変更します。それ以外の場合は、デフォルト値 1500 のままにします。

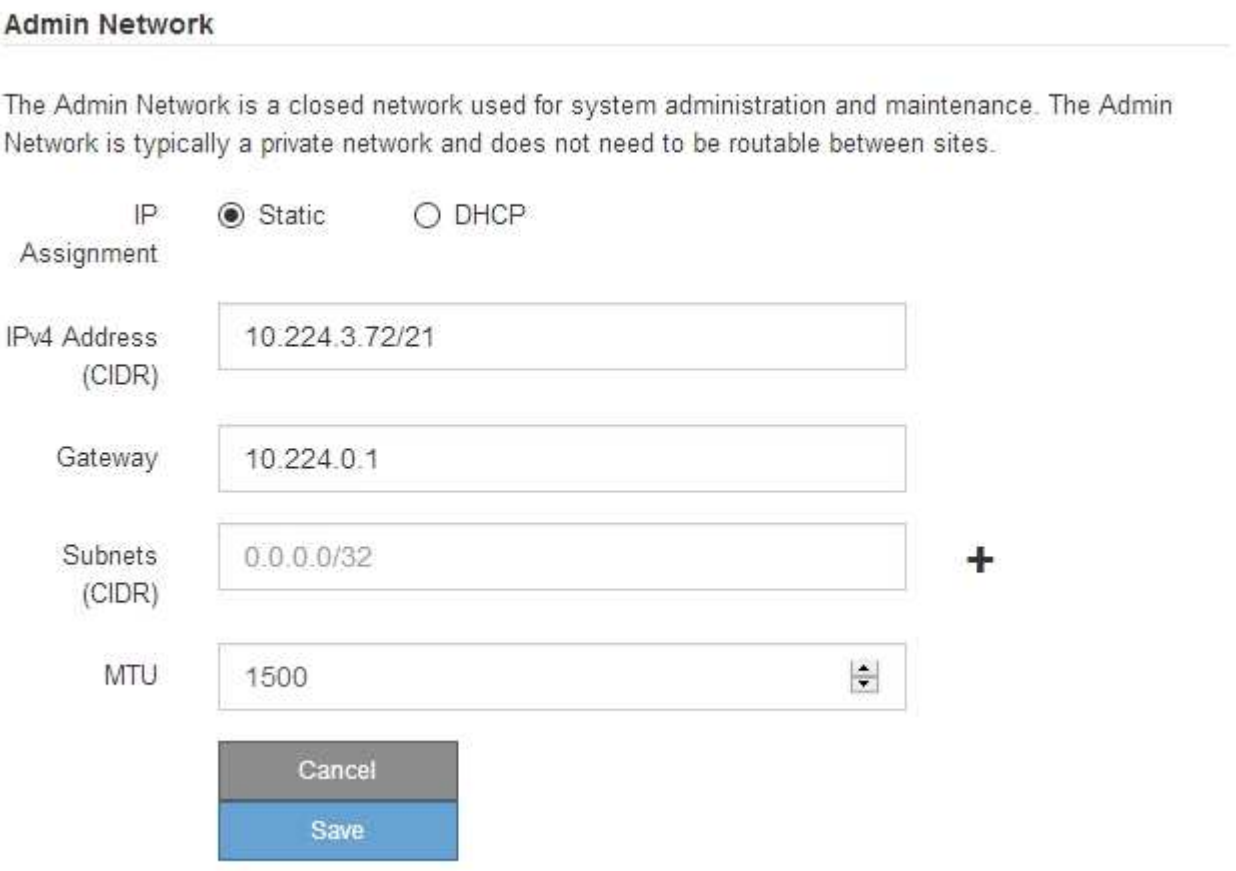
ネットワークの MTU 値は、ノードが接続されているスイッチポートに設定されている値と同じである必要があります。そうしないと、ネットワークパフォーマンスの問題やパケット損失が発生する可能性があります。

ネットワークのパフォーマンスを最大限に高めるには、すべてのノードのグリッドネットワークインターフェイスで MTU 値がほぼ同じになるように設定する必要があります。個々のノードのグリッドネットワークの MTU 設定に大きな違いがある場合は、 * Grid Network MTU mismatch * アラートがトリガーされます。MTU 値はすべてのネットワークタイプで同じである必要はありません。

a. [ 保存（ Save ） ] をクリックします。

5. 管理ネットワークを設定するには、ページの管理ネットワークセクションで * 静的 * または * DHCP * のいずれかを選択します。

管理ネットワークを設定するには、 Link Configuration ページで管理ネットワークを有効にする必要があります。




6. 「 * Static * 」を選択した場合は、次の手順に従って管理ネットワークを設定します。

a. アプライアンスの管理ポート 1 に対して、 CIDR 表記を使用して静的 IPv4 アドレスを入力します。

管理ポート 1 は、アプライアンス右端にある 2 つの 1GbE RJ45 ポートのうち、左側のポートです。

b. ゲートウェイを入力します。

ネットワークにゲートウェイがない場合は、同じ静的 IPv4 アドレスを再入力します。

c. ジャンボフレームを使用する場合は、 MTU フィールドを 9000 などのジャンボフレームに適した値に変更します。それ以外の場合は、デフォルト値 1500 のままにします。

ネットワークの MTU 値は、ノードが接続されているスイッチポートに設定されている値と同じである必要があります。そうしないと、ネットワークパフォーマンスの問題やパケット損失が発生する可能性があります。

d. [ 保存（ Save ） ] をクリックします。

IP アドレスを変更すると、ゲートウェイとサブネットのリストも変更される可能性があります。

StorageGRID アプライアンスインストーラへの接続が失われた場合は、割り当てた新しい静的 IP アドレスを使用して URL を再入力します。たとえば、「+」と入力します
**`https://services_appliance:8443`**

e. 管理ネットワークのサブネットのリストが正しいことを確認します。

指定したゲートウェイを使用してすべてのサブネットにアクセスできることを確認する必要があります。

管理ネットワークゲートウェイを使用するデフォルトルートは作成できません。

- サブネットを追加するには、挿入アイコンをクリックします ➕ アイコン"] をクリックします。
- 使用されていないサブネットを削除するには、削除アイコンをクリックします ✖。

f. [ 保存（ Save ） ] をクリックします。

7. [**DHCP**] を選択した場合は、次の手順に従って管理ネットワークを設定します。

a. [**DHCP**] ラジオボタンを選択した後、 [**Save**] をクリックします。

[* IPv4 アドレス * ] 、 [ * ゲートウェイ * ] 、および [ * サブネット * ] フィールドには、自動的に値が入力されます。DHCP サーバが MTU 値を割り当てるように設定されている場合は、 **MTU** フィールドにその値が入力され、フィールドは読み取り専用になります。

Web ブラウザは、 StorageGRID アプライアンスインストーラの新しい IP アドレスに自動的にリダイレクトされます。

b. 管理ネットワークのサブネットのリストが正しいことを確認します。

指定したゲートウェイを使用してすべてのサブネットにアクセスできることを確認する必要があります。

管理ネットワークゲートウェイを使用するデフォルトルートは作成できません。

- サブネットを追加するには、挿入アイコンをクリックします ➕ アイコン"] をクリックします。

- 使用されていないサブネットを削除するには、削除アイコンをクリックします ✖。

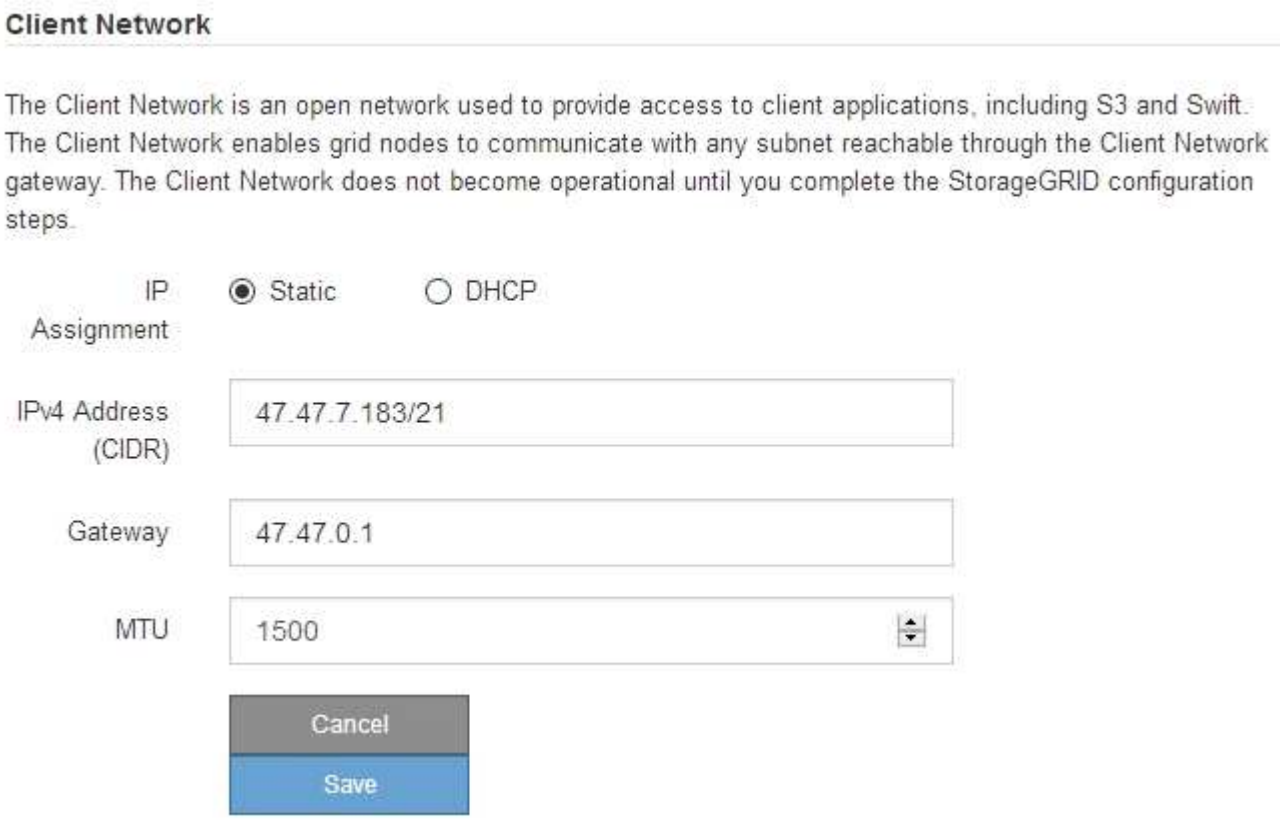
c. ジャンボフレームを使用する場合は、 MTU フィールドを 9000 などのジャンボフレームに適した値に変更します。それ以外の場合は、デフォルト値 1500 のままにします。

> ネットワークの MTU 値は、ノードが接続されているスイッチポートに設定されている値と同じである必要があります。そうしないと、ネットワークパフォーマンスの問題やパケット損失が発生する可能性があります。

d. [ 保存（ Save ） ] をクリックします。

8. クライアントネットワークを設定するには、ページの * クライアントネットワーク * セクションで * 静的 * または * DHCP * のいずれかを選択します。

> クライアントネットワークを設定するには、 Link Configuration ページで Client Network を有効にする必要があります。




9. * Static * を選択した場合は、次の手順に従ってクライアントネットワークを設定します。

a. CIDR 表記を使用して静的 IPv4 アドレスを入力します。

b. [ 保存（ Save ） ] をクリックします。

c. クライアントネットワークゲートウェイの IP アドレスが正しいことを確認します。

> クライアントネットワークが有効になっている場合は、デフォルトルートが表示されます。デフォルトルートはクライアントネットワークゲートウェイを使用し、クライアントネットワークが有効になっている間は別のインターフェイスに移動できません。

d. ジャンボフレームを使用する場合は、 MTU フィールドを 9000 などのジャンボフレームに適した値に変更します。それ以外の場合は、デフォルト値 1500 のままにします。

> ネットワークの MTU 値は、ノードが接続されているスイッチポートに設定されている値と同じである必要があります。そうしないと、ネットワークパフォーマンスの問題やパケット損失が発生する可能性があります。

e. [ 保存（ Save ） ] をクリックします。

10. **[DHCP]** を選択した場合は、次の手順に従ってクライアントネットワークを設定します。

a. **[DHCP]** ラジオボタンを選択した後、 **[Save]** をクリックします。

**[IPv4 Address]** フィールドと **[Gateway]** フィールドが自動的に入力されます。DHCP サーバが MTU 値を割り当てるように設定されている場合は、 **MTU** フィールドにその値が入力され、フィールドは読み取り専用になります。

Web ブラウザは、 StorageGRID アプライアンスインストーラの新しい IP アドレスに自動的にリダイレクトされます。

a. ゲートウェイが正しいことを確認します。

> クライアントネットワークが有効になっている場合は、デフォルトルートが表示されます。デフォルトルートはクライアントネットワークゲートウェイを使用し、クライアントネットワークが有効になっている間は別のインターフェイスに移動できません。

b. ジャンボフレームを使用する場合は、 MTU フィールドを 9000 などのジャンボフレームに適した値に変更します。それ以外の場合は、デフォルト値 1500 のままにします。

> ネットワークの MTU 値は、ノードが接続されているスイッチポートに設定されている値と同じである必要があります。そうしないと、ネットワークパフォーマンスの問題やパケット損失が発生する可能性があります。

関連情報

"E5600SGコントローラのリンク設定の変更"

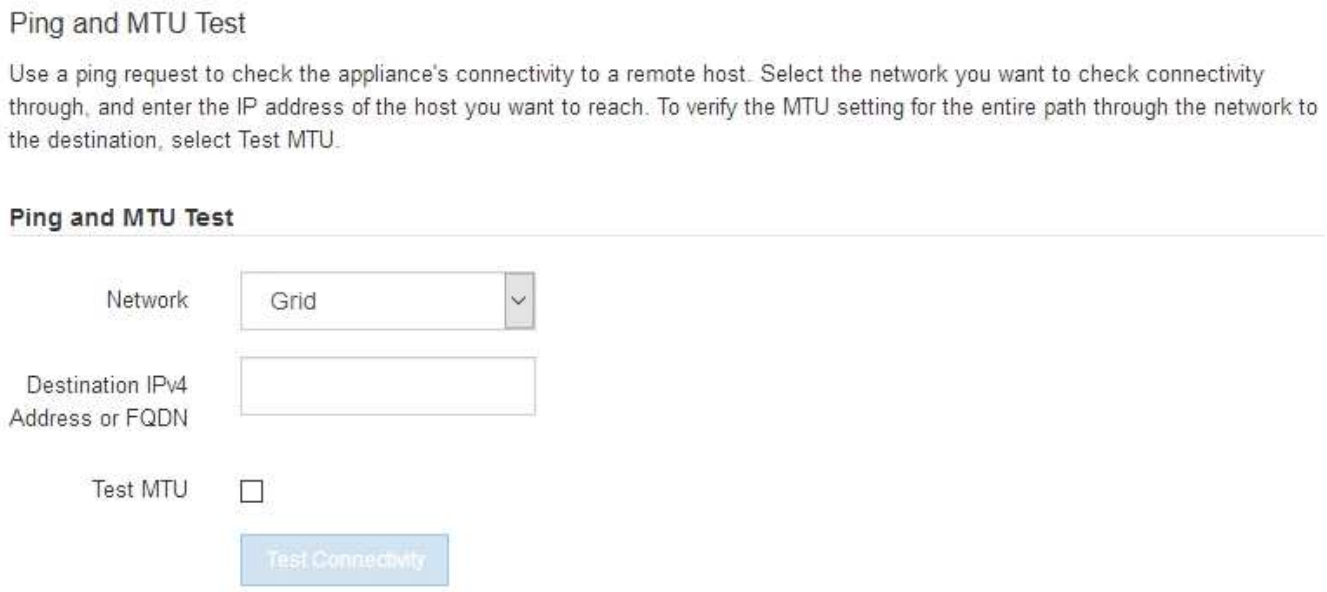
ネットワーク接続の確認

使用する StorageGRID ネットワークに、アプライアンスからアクセスできることを確認する必要があります。ネットワークゲートウェイ経由のルーティングを検証するには、StorageGRID アプライアンスインストーラと異なるサブネット上の IP アドレスとの接続をテストする必要があります。MTU 設定を確認することもできます。

手順

1. StorageGRID アプライアンスインストーラのメニューバーから、 *Configure Networking *>*Ping and MTU Test * をクリックします。

[Ping and MTU Test] ページが表示されます。




2. [* ネットワーク *] ドロップダウンボックスから、テストするネットワークを選択します。グリッド、管理、またはクライアント。
3. そのネットワーク上のホストの IPv4 アドレスまたは完全修飾ドメイン名（ FQDN ）を入力します。

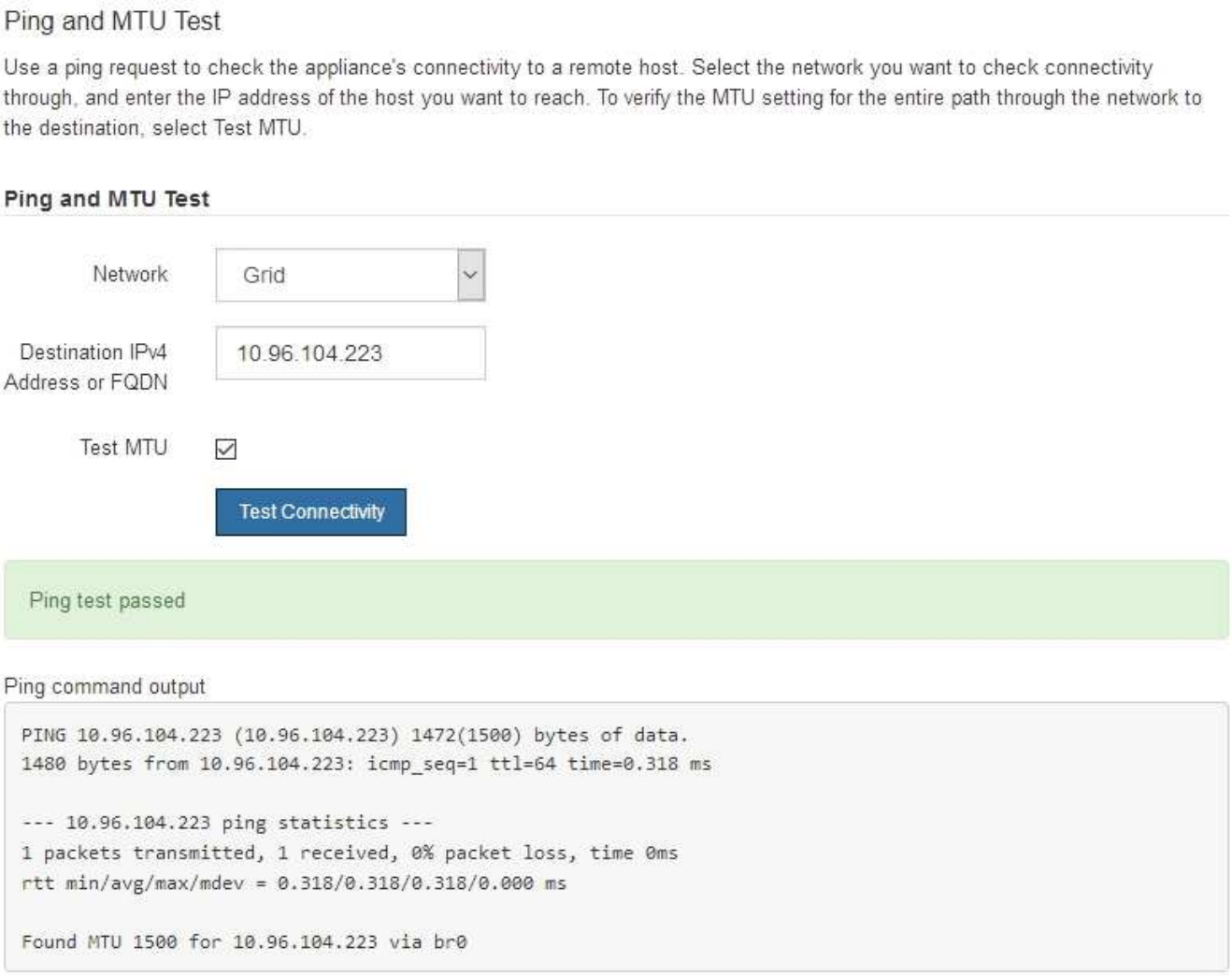
   たとえば、ネットワーク上のゲートウェイやプライマリ管理ノードに ping を送信できます。

4. 必要に応じて、 * Test MTU * チェックボックスをオンにして、ネットワーク経由でデスティネーションへのパス全体の MTU 設定を確認します。

   たとえば、アプライアンスノードと別のサイトのノードの間のパスをテストできます。

5. [ 接続のテスト * ] をクリックします。

   ネットワーク接続が有効な場合は、「 Ping test passed 」メッセージと ping コマンドの出力が表示されます。




関連情報

"ネットワークリンクの設定（SG5600）"

"MTU設定を変更します"

ポートレベルのネットワーク接続の確認

# StorageGRID アプライアンスインストーラとその他のノードの間のアクセスがファイアウォールの妨げにならないように、 StorageGRID アプライアンスインストーラが指定した IP アドレスまたはアドレス範囲にある特定の TCP ポートまたはポートセットに接続できることを確認します。

このタスクについて

StorageGRID アプライアンスインストーラに付属のポートのリストを使用して、アプライアンスとグリッドネットワーク内の他のノードの間の接続をテストできます。

また、外部 NFS サーバや DNS サーバで使用されるポートなど、管理ネットワークとクライアントネットワーク、および UDP ポートで接続をテストすることもできます。これらのポートの一覧については、StorageGRID ネットワークのガイドラインにあるポートリファレンスを参照してください。

ポート接続テーブルに表示されているグリッドネットワークポートは、StorageGRID バージョン11.5.0に対してのみ有効です。各ノードタイプに適したポートを確認するには、使用している StorageGRID のバージョンに対応したネットワークガイドラインを確認する必要があります。

手順

1. StorageGRID アプライアンスインストーラから、 **Configure Networking *>** Port Connectivity Test (nmap)* をクリックします。

   Port Connectivity Test ページが表示されます。

   ポート接続テーブルには、グリッドネットワークでの TCP 接続を必要とするノードタイプが表示されます。各ノードタイプについて、アプライアンスにアクセスできる必要があるグリッドネットワークのポートがテーブルに表示されます。

   The following node types require TCP connectivity on the Grid Network.

| Node Type | Grid Network Ports |
|---|---|
| Admin Node | 22,80,443,1504,1505,1506,1508,7443,9999 |
| Storage Node without ADC | 22,1139,1502,1506,1511,7001,9042,9999,18002,18017,18019,18082,18083,18200 |
| Storage Node with ADC | 22,1139,1501,1502,1506,1511,7001,9042,9999,18000,18001,18002,18003,18017,18019,18082,18083,18200,19000 |
| API Gateway | 22,1506,1507,9999 |
| Archive Node | 22,1506,1509,9999,11139 |

   表に記載されたアプライアンスポートとグリッドネットワーク内のその他のノードの間の接続をテストできます。

2. [* ネットワーク *] ドロップダウンから、テストするネットワークを選択します。 * グリッド * 、 * 管理者 * 、または * クライアント * 。
3. そのネットワーク上のホストの IPv4 アドレスの範囲を指定します。

   たとえば、ネットワーク上のゲートウェイやプライマリ管理ノードをプローブできます。

   次の例に示すように、ハイフンを使用して範囲を指定します。

4. TCP ポート番号、カンマで区切ったポートのリスト、またはポートの範囲を入力します。

The following node types require TCP connectivity on the Grid Network.

| Node Type | Grid Network Ports |
| --- | --- |
| Admin Node | 22,80,443,1504,1505,1506,1508,7443,9999 |
| Storage Node without ADC | 22,1139,1502,1506,1511,7001,9042,9999,18002,18017,18019,18082,18083,18200 |
| Storage Node with ADC | 22,1139,1501,1502,1506,1511,7001,9042,9999,18000,18001,18002,18003,18017,18019,18082,18083,18200,19000 |
| API Gateway | 22,1506,1507,9999 |
| Archive Node | 22,1506,1509,9999,11139 |

**Port Connectivity Test**

Network: Grid

IPv4 Address Ranges: 10.224.6.160-161

Port Ranges: 22,2022

Protocol: TCP UDP

Test Connectivity

5. [ 接続のテスト * ] をクリックします。

   ◦ 選択したポートレベルのネットワーク接続が有効な場合は、「 Port connectivity test passed 」というメッセージが緑色のバナーに表示されます。nmap コマンドの出力は、バナーの下に表示されます。

   Port connectivity test passed

   Nmap command output. Note: Unreachable hosts will not appear in the output.

```
# Nmap 7.70 scan initiated Fri Nov 13 18:32:03 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,2022 10.224.6.160-161
Nmap scan report for 10.224.6.160
Host is up (0.00072s latency).

PORT     STATE SERVICE
22/tcp   open  ssh
2022/tcp open  down

Nmap scan report for 10.224.6.161
Host is up (0.00060s latency).

PORT     STATE SERVICE
22/tcp   open  ssh
2022/tcp open  down

# Nmap done at Fri Nov 13 18:32:04 2020 -- 2 IP addresses (2 hosts up) scanned in 0.55 seconds
```

   ◦ ポートレベルのネットワーク接続がリモートホストに確立されても ' ホストが選択したポートの 1 つ以上をリッスンしていない場合は ' ポート接続テストに失敗しましたというメッセージが黄色のバナーに表示されますnmap コマンドの出力は、バナーの下に表示されます。

   ホストがリッスンしていないリモート・ポートの状態はすべて「 closed 」です。 たとえば、接続しようとしているノードがインストール済みの状態で、 StorageGRID NMS サービスがまだ実行されていない場合に、黄色のバナーが表示されることがあります。

Nmap command output. Note: Unreachable hosts will not appear in the output.

```
# Nmap 7.70 scan initiated Sat May 16 17:07:02 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,80,443,1504,1505,1506,1508,7443,9999
Nmap scan report for 172.16.4.71
Host is up (0.00020s latency).

PORT     STATE  SERVICE
22/tcp   open   ssh
80/tcp   open   http
443/tcp  open   https
1504/tcp closed evb-elm
1505/tcp open   funkproxy
1506/tcp open   utcd
1508/tcp open   diagmond
7443/tcp open   oracleas-https
9999/tcp open   abyss
MAC Address: 00:50:56:87:39:AE (VMware)

# Nmap done at Sat May 16 17:07:03 2020 -- 1 IP address (1 host up) scanned in 0.59 seconds
```

- 選択した 1 つ以上のポートに対してポートレベルのネットワーク接続を確立できない場合は、「 Port connectivity test failed 」というメッセージが赤いバナーに表示されます。nmap コマンドの出力は、バナーの下に表示されます。

  赤いバナーは、リモートホストのポートへの TCP 接続試行が行われたが、送信者には何も返されなかったことを示します。応答が返されない場合、ポートの状態は「 filtered 」となり、ファイアウォールによってブロックされている可能性があります。

  「閉」のポートも一覧表示されます。

Nmap command output. Note: Unreachable hosts will not appear in the output.

```
# Nmap 7.70 scan initiated Sat May 16 17:11:01 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,79,80,443,1504,1505,1506,1508,7443,9999 172.16.4.71
Nmap scan report for 172.16.4.71
Host is up (0.00029s latency).

PORT     STATE    SERVICE
22/tcp   open     ssh
79/tcp   filtered finger
80/tcp   open     http
443/tcp  open     https
1504/tcp closed   evb-elm
1505/tcp open     funkproxy
1506/tcp open     utcd
1508/tcp open     diagmond
7443/tcp open     oracleas-https
9999/tcp open     abyss
MAC Address: 00:50:56:87:39:AE (VMware)

# Nmap done at Sat May 16 17:11:02 2020 -- 1 IP address (1 host up) scanned in 1.60 seconds
```

関連情報

"ネットワークガイドライン"

### SANtricity Storage Managerを設定しています

SANtricity Storage Manager を使用して、 StorageGRID アプライアンスのストレージディスクおよびハードウェアコンポーネントのステータスを監視できます。このソフトウェアにアクセスするには、 E2700 コントローラ（アプライアンスのストレージコントローラ）の管理ポート 1 の IP アドレスが必要です。

手順

- "E2700コントローラのIPアドレスを設定します"
- "SANtricity ストレージ・マネージャへのアプライアンスの追加"
- "SANtricity Storage Managerをセットアップしています"

#### E2700コントローラのIPアドレスを設定します

E2700 コントローラの管理ポート 1 を使用して、アプライアンスを SANtricity Storage Manager の管理ネットワークに接続します。StorageGRID アプライアンスのハードウェアおよびコントローラファームウェアとの管理接続が失われないように、 E2700 コントローラの静的 IP アドレスを設定する必要があります。

必要なもの

サポートされているWebブラウザを使用します。

このタスクについて

DHCP によって割り当てられたアドレスは、いつ変更されるかわかりません。一貫したアクセスを確保するために、コントローラに静的 IP アドレスを割り当ててください。

手順

1. クライアントから、StorageGRID アプライアンスインストーラのURLを入力します：+ **`https://E5600SG_Controller_IP:8443`**

   の場合 `E5600SG_Controller_IP` には、任意のStorageGRID ネットワーク上のアプライアンスのIPアドレスを使用します。

   StorageGRID アプライアンスインストーラのホームページが表示されます。

2. ハードウェア構成 * > * ストレージ・コントローラ・ネットワーク構成 * を選択します。

   Storage Controller Network Configuration ページが表示されます。

3. ネットワーク構成に応じて、 IPv4 、 IPv6 、またはその両方で * Enabled * を選択します。
4. 自動的に表示される IPv4 アドレスを書き留めます。

   このポートに IP アドレスを割り当てるためのデフォルトの方法は、 DHCP です。

   DHCP 値が表示されるまでに数分かかる場合があります。

5. 必要に応じて、 E2700 コントローラ管理ポートの静的 IP アドレスを設定します。

   管理ポートに静的 IP を割り当てるか、 DHCP サーバでアドレスの永久リースを割り当てる必要があります。

   a. 「 * Static * 」を選択します。
   b. CIDR 表記を使用して IPv4 アドレスを入力します。
   c. デフォルトゲートウェイを入力します。

   d. [ 保存（ Save ） ] をクリックします。

      変更が適用されるまで数分かかる場合があります。

SANtricity Storage Managerに接続するときは、新しい静的IPアドレスをURL：+として使用します **`https://E2700_Controller_IP`**

関連情報

"ネットアップのマニュアル： SANtricity Storage Manager"

**SANtricity** ストレージ・マネージャへのアプライアンスの追加

## アプライアンス内の E2700 コントローラを SANtricity Storage Manager に接続し、アプライアンスをストレージアレイとして追加します。

必要なもの

サポートされているWebブラウザを使用します。

このタスクについて

詳しい手順については、 SANtricity Storage Manager のドキュメントを参照してください。

手順

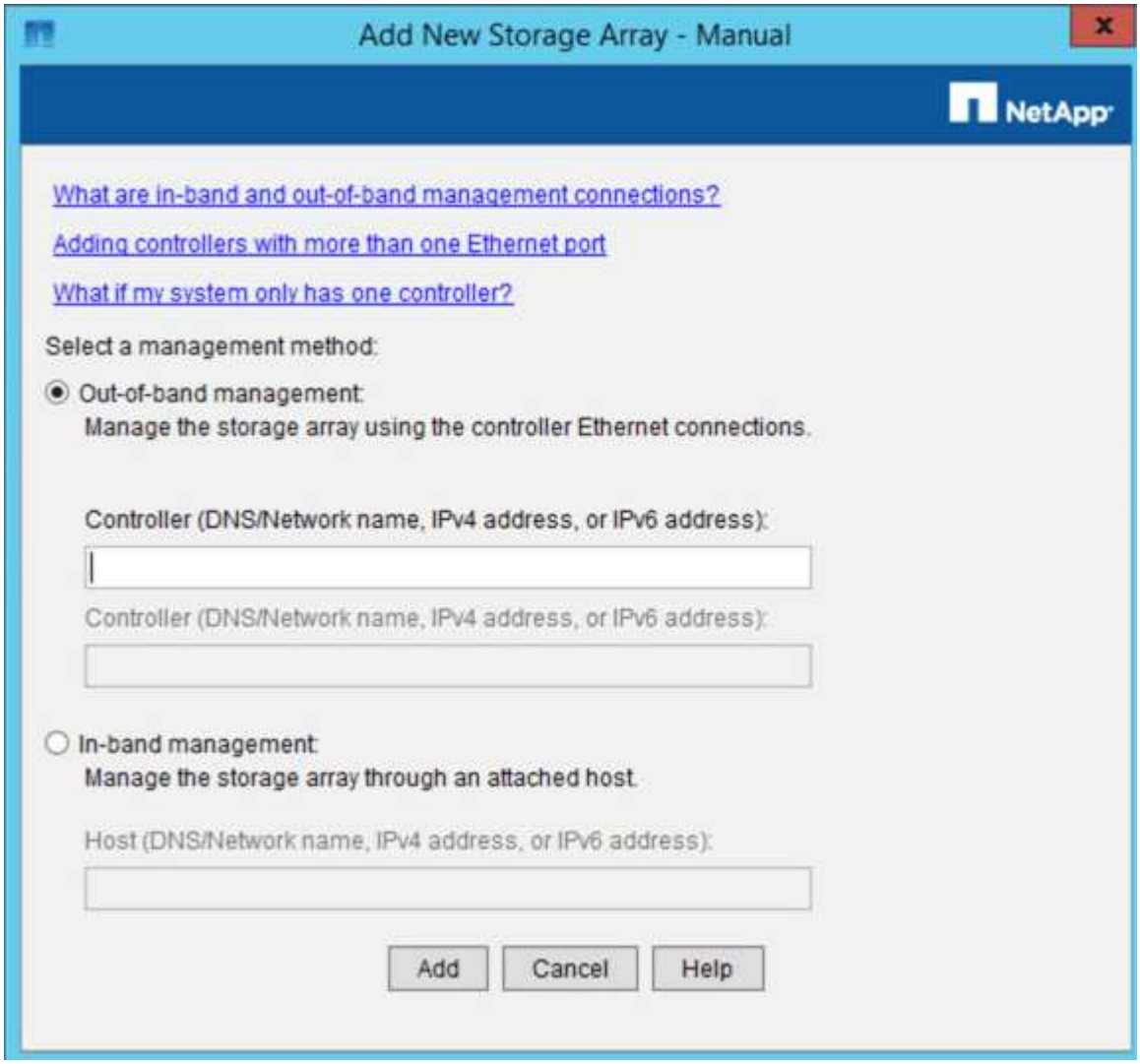
1. Webブラウザを開き、SANtricity Storage ManagerのURLにIPアドレスを入力します：+

`https://E2700_Controller_IP`

SANtricity Storage Manager のログインページが表示されます。

2. [ 追加方法の選択 ] ページで、 **[*Manual]** を選択し、 [OK] をクリックします。
3. 「 * 編集 * > * ストレージアレイの追加 * 」を選択します。

Add New Storage Array - Manual ページが表示されます。




4. [ 帯域外管理 * ] ボックスに、次のいずれかの値を入力します。
   - * DHCP を使用： * E2700 コントローラ上の管理ポート 1 に対して DHCP サーバによって割り当てられた IP アドレス
   - * DHCPを使用しない：* `192.168.128.101`

   SANtricity Storage Manager に接続されるのはアプライアンスの一方のコントローラだけなので、 IP アドレスは 1 つだけで済みます。

5. [ 追加（ Add ） ] をクリックします。

関連情報

"ネットアップのマニュアル： SANtricity Storage Manager"

**SANtricity Storage Manager**をセットアップしています

## SANtricity Storage Manager にアクセスしたあと、ハードウェアを設定する際にそのマネージャを使用できます。通常、この設定はアプライアンスを StorageGRID システムのストレージノードとして導入する前に行います。

手順

- "AutoSupport を設定しています"
- "AutoSupport の受信確認"
- "EメールおよびSNMPトラップのアラート通知の設定"
- "SANtricity Storage Managerのパスワードを設定しています"

**AutoSupport** を設定しています

## AutoSupport ツールは、アプライアンスからカスタマーサポートバンドルのデータを収集し、テクニカルサポートに自動的に送信します。AutoSupport を設定すると、トラブルシューティングや問題の分析をテクニカルサポートがリモートから行えるようになります。

必要なもの

- AutoSupport 機能をアクティブ化し、アプライアンスで有効にする必要があります。

  AutoSupport 機能のアクティブ化と非アクティブ化は、ストレージ管理ステーションでグローバルに設定します。

- Storage Manager Event Monitor は、アプライアンスにアクセスできる 1 台以上のマシン上で実行する必要があります。できれば、複数のマシン上で実行することはできません。

このタスクについて

すべてのデータが単一のアーカイブファイル（ .7z 形式）に圧縮されて、指定した場所に格納されます。

AutoSupport には、次の種類のメッセージが用意されています。

| メッセージタイプ | 説明 |
| --- | --- |
| イベントメッセージ | • 管理対象アプライアンスでサポートイベントが発生したときに送信されます<br>• システム構成と診断情報が含まれます |
| 毎日のメッセージ | • アプライアンスのローカル時間にユーザが設定可能な時間間隔で、 1 日に 1 回送信されます<br>• 現在のシステムイベントログとパフォーマンスデータが含まれます |

| メッセージタイプ | 説明 |
| --- | --- |
| 週次メッセージ | • アプライアンスのローカル時間内にユーザが設定可能な時間間隔で、毎週 1 回送信されます<br>• 構成とシステムの状態の情報が含まれます |

手順

1. SANtricity ストレージ・マネージャの [ エンタープライズ管理 ] ウィンドウで '[ デバイス ] タブを選択し '[* 検出されたストレージ・アレイ * ] を選択します
2. [ ツール（ Tools ） ] [ * （ * ） ] [ ツール（ * AutoSupport ） ] [ * 構成（ * Configuration ） ]
3. SANtricity Storage Manager のオンラインヘルプを必要に応じて参照しながら、タスクを完了します。

関連情報

"ネットアップのマニュアル： SANtricity Storage Manager"

**AutoSupport** の受信確認

テクニカルサポートに AutoSupport メッセージが届いていることを確認する必要があります。システムの AutoSupport のステータスは、 Active IQ ポータルで確認できます。これらのメッセージがテクニカルサポートに届いていれば、支援が必要な場合にはその情報を利用できます。

このタスクについて

AutoSupport のステータスは次のいずれかになります。

- * オン *

  オンのステータスは、テクニカルサポートが現在システムから AutoSupport メッセージを受信していることを示します。

- * オフ *

  テクニカルサポートにシステムの週単位のログが 15 日以上届いておらず、 AutoSupport が無効になっている可能性があります。または環境や構成に変更があった可能性などが考えられます。

- * 拒否 *

  拒否ステータスは、 AutoSupport を有効にしないことをテクニカルサポートに通知済みであることを示します。

システムの週単位のログをテクニカルサポートが受信すると、 AutoSupport のステータスが ON に変わります。

手順

1. NetApp Support Siteにアクセスします "mysupport.netapp.com"をクリックし、 Active IQ ポータルにサインインします。
2. AutoSupport のステータスが誤って OFF になっている場合は、次の手順を実行します。

a. システム構成をチェックして、 AutoSupport がオンになっていることを確認します。

b. ネットワーク環境と構成をチェックして、システムからテクニカルサポートにメッセージを送信できることを確認します。

**E**メールおよび**SNMP**トラップのアラート通知の設定

SANtricity Storage Manager では、アプライアンスのステータスまたはいずれかのコンポーネントが変わったときに通知を受け取ることができます。これはアラート通知と呼ばれます。アラート通知は、 E メールと SNMP トラップの 2 つの方法で受信できます。受信するアラート通知を設定する必要があります。

手順

1. SANtricity Storage Manager の Enterprise Management ウィンドウで、 * Devices * タブを選択し、ノードを選択します。
2. * Edit * > * Configure Alerts * を選択します。
3. [**Email**] タブを選択して、電子メールアラート通知を設定します。
4. SNMP トラップのアラート通知を設定するには、 [**SNMP**] タブを選択します。
5. SANtricity Storage Manager のオンラインヘルプを必要に応じて参照しながら、タスクを完了します。

**SANtricity Storage Manager**のパスワードを設定しています

SANtricity Storage Manager でアプライアンスに使用するパスワードを設定できます。パスワードを設定することでシステムのセキュリティが維持され

手順

1. SANtricity Storage Manager の Enterprise Management Window で、コントローラをダブルクリックします。
2. Array Management Window で、 * Storage Array * メニューを選択し、 * Security * > * Set Password * を選択します。
3. パスワードを設定します。
4. SANtricity Storage Manager のオンラインヘルプを必要に応じて参照しながら、タスクを完了します。

オプション：ノード暗号化を有効にする

ノードの暗号化を有効にすると、アプライアンス内のディスクを安全なキー管理サーバ（ KMS ）暗号化によってサイト内での物理的な損失やデータの削除から保護することができます。アプライアンスのインストール時にノード暗号化を選択して有効にする必要があります。また、 KMS 暗号化プロセスが開始されると、ノード暗号化の選択を解除できません。

必要なもの

StorageGRID の管理手順の KMS に関する情報を確認します。

このタスクについて

ノード暗号化が有効になっているアプライアンスは、 StorageGRID サイト用に設定されている外部キー管理サーバ（ KMS ）に接続します。各 KMS （または KMS クラスタ）は、サイトにあるすべてのアプライアンスノードの暗号化キーを管理します。これらのキーは、ノード暗号化が有効なアプライアンスで、各ディスク上のデータを暗号化および復号化します。

Grid Manager StorageGRID では、アプライアンスのインストール前またはインストール後に KMS を設定できます。詳細については、 StorageGRID の管理手順の KMS とアプライアンスの設定に関する情報を参照してください。

- アプライアンスをインストールする前に KMS を設定すると、 KMS で制御される暗号化が開始されます。この暗号化は、アプライアンスでノード暗号化を有効にし、 KMS が設定されている StorageGRID サイトに追加します。
- アプライアンスをインストールする前に KMS が設定されていない場合は、 KMS が設定され、アプライアンスノードを含むサイトで利用可能になった時点で、ノード暗号化が有効になっている各アプライアンスで KMS 制御された暗号化が実行されます。

> ノード暗号化が有効になっているアプライアンスより前に存在するデータは、設定されたKMSに接続する前に、セキュアでない一時キーで暗号化されます。キーが KMS から提供される値に設定されるまで、アプライアンスの取り外しや盗難は防止されません。

ディスクの復号化に KMS キーが必要な場合を除いて、アプライアンス上のデータを取得することはできず、データが実質的に失われます。これは、 KMS から復号化キーを取得できない場合に発生します。顧客が KMS 設定をクリアするか、 KMS キーの有効期限が切れるか、 KMS への接続が失われるか、 KMS キーがインストールされている StorageGRID システムからアプライアンスが削除されると、キーにアクセスできなくなります。

手順

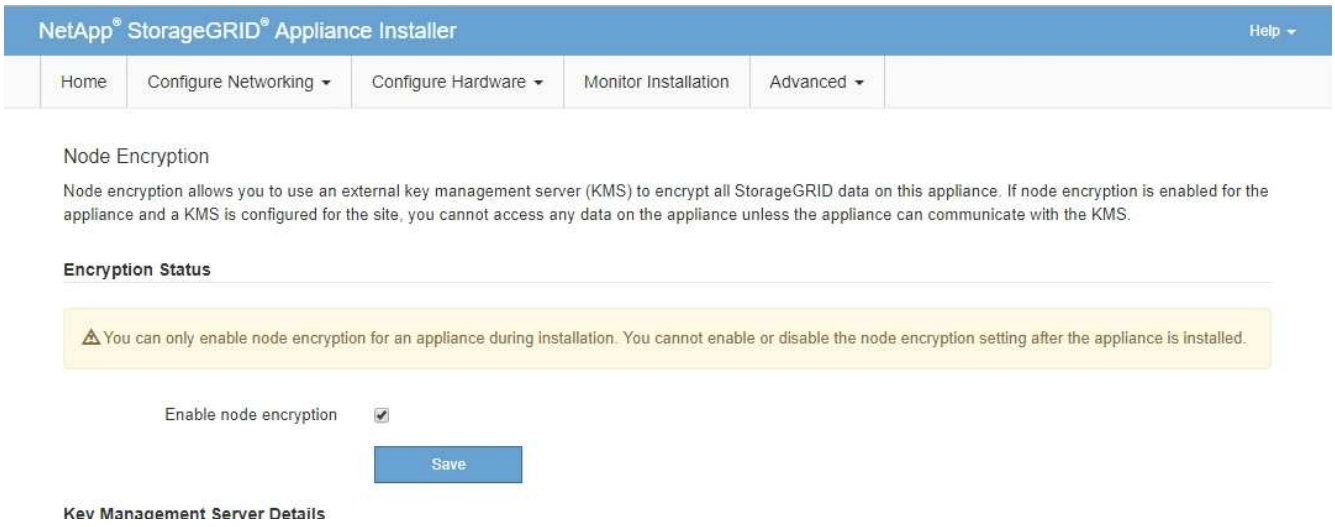
1. ブラウザを開き、アプライアンスのコンピューティングコントローラの IP アドレスのいずれかを入力します。[+]
   **`https://Controller_IP:8443`**

   *`Controller_IP`* は、3つのStorageGRID ネットワークのいずれかでのコンピューティングコントローラ（ストレージコントローラではない）のIPアドレスです。

   StorageGRID アプライアンスインストーラのホームページが表示されます。

   > アプライアンスを KMS キーで暗号化すると、アプライアンスディスクを復号化する際に同じ KMS キーを使用する必要がなくなります。

2. Configure Hardware * > * Node Encryption * を選択します。




3. [ ノード暗号化を有効にする *] を選択します。

   保存を選択し、アプライアンスノードがStorageGRID システム内のKMS暗号化キーにアクセスしてディスク暗号化を開始するまでは、「ノード暗号化を有効にする」を選択解除してデータ損失のリスクを回避できます。アプライアンスのインストール後、ノード暗号化を無効にすることはできません。

   KMS を含む StorageGRID サイトにノード暗号化が有効になっているアプライアンスを追加すると、そのノードで KMS 暗号化を使用するのを停止することはできません。

4. [ 保存（ Save ） ] を選択します。
5. アプライアンスを StorageGRID システムのノードとして導入します。

   KMS で制御される暗号化は、アプライアンスが StorageGRID サイト用に設定されている KMS キーにアクセスすると開始されます。KMS 暗号化プロセス中にインストーラによって進捗状況のメッセージが表示されます。この処理には、アプライアンス内のディスクボリュームの数によっては数分かかることがあります。

   アプライアンスは、最初に各ディスクボリュームにランダムな KMS 以外の暗号化キーを割り当てて構成します。ディスクはこの一時的な暗号化キーを使用して暗号化されます。このキーは、ノード暗号化が有効になっているアプライアンスが StorageGRID サイト用に設定されている KMS キーにアクセスするまではセキュリティ保護されません。

完了後

アプライアンスノードがメンテナンスモードのときに使用されているノード暗号化ステータス、 KMS の詳細、および証明書を確認できます。

関連情報

"StorageGRID の管理"

"メンテナンスモードでのノード暗号化の監視"

オプション：**RAID 6**モードへの変更（**SG5660**のみ）

60 ドライブを搭載した SG5660 を使用する場合は、ボリューム構成をデフォルトかつ推

奨される設定である Dynamic Disk Pools （ DDP ）から RAID 6 に変更できます。モードを変更できるのは、 StorageGRID アプライアンスストレージノードを導入する前だけです。

必要なもの

- SG5660 を使用している。SG5612 は RAID 6 をサポートしていない。SG5612 を使用している場合は、DDP モードを使用する必要があります。

> ボリュームがすでに構成されている場合や StorageGRID が事前にインストールされている場合に RAID モードを変更すると、ボリュームが削除されて置き換えられます。対象となったボリュームのデータはすべて失われます。

このタスクについて

StorageGRID アプライアンスストレージノードを導入する前に、ボリューム構成オプションを次の 2 つから選択できます。

- * Dynamic Disk Pools （ DDP ） * - 推奨されるデフォルトの設定です。DDP は、システムのパフォーマンスに優れた高度なハードウェアデータ保護方式です。ドライブ障害が発生したあとのリビルド時間を短縮することができ、管理も簡単です。
- *RAID6 * — 各ディスクでパリティストライプを使用するハードウェア保護方式で、データが失われる前に RAID セット内の 2 つのディスク障害に対応します。

> ほとんどの StorageGRID 環境では、 RAID 6 の使用が推奨されません。RAID 6 を使用するとストレージ効率が 88% まで向上しますが（ DDP では 80% ）、ドライブ障害からのリカバリの効率は DDP モードの方が優れています。

手順

1. サービスラップトップでWebブラウザを開き、StorageGRID アプライアンスインストーラの+にアクセスします
   **`https://E5600SG_Controller_IP:8443`**

   ここで *`E5600SG_Controller_IP`* は、E5600SGコントローラのいずれかのIPアドレスです。

2. メニューバーから * アドバンスト * > * RAID モード * を選択します。
3. RAID モードの設定 * ページで、モードドロップダウンリストから *RAID6 * を選択します。
4. [ 保存（ Save ） ] をクリックします。

オプション：アプライアンスに対するネットワークポートの再マッピング

アプライアンスストレージノードの内部ポートを別の外部ポートに再マッピングすることが必要になる場合があります。たとえば、ファイアウォールの問題 が原因でポートの再マッピングが必要になることがあります。

必要なもの

- 以前に StorageGRID アプライアンスインストーラにアクセスしていた場合。
- ロードバランサエンドポイントを設定しておらず、設定する予定もない状態である必要があります。

ポートを再マッピングする場合、同じポートを使用してロードバランサエンドポイントを設定することはできません。ポートを再マッピング済みの場合にロードバランサエンドポイントを設定するには、リカバリとメンテナンスの手順に従ってポートの再マッピングを削除してください。

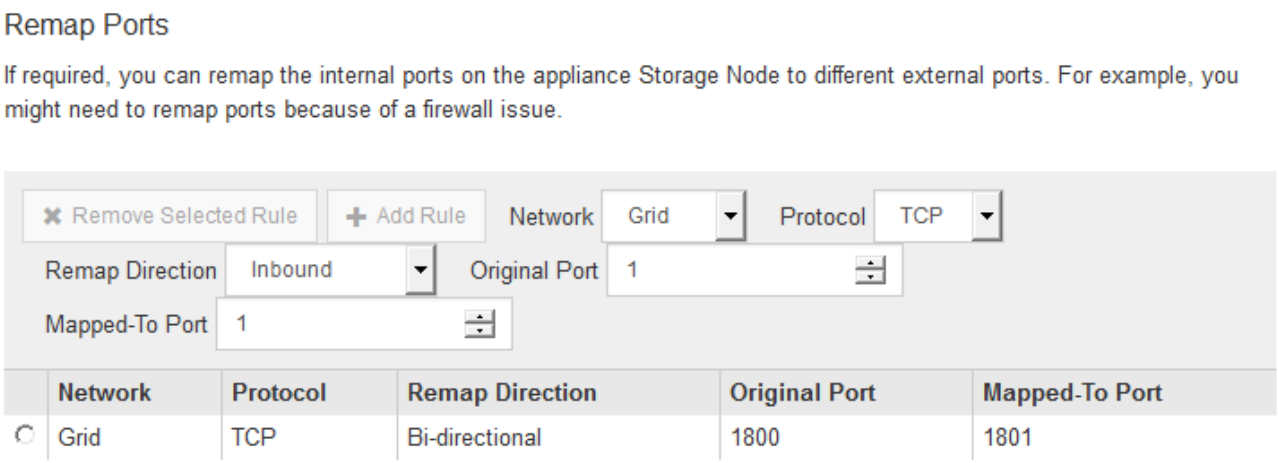
手順

1. StorageGRID アプライアンスインストーラのメニューバーから、 **Configure Networking *>*Remap Port** をクリックします。

   Remap Port ページが表示されます。

2. Network * ドロップダウンボックスから、再マッピングするポートのネットワーク（ Grid 、 Admin 、または Client ）を選択します。
3. [**Protocol**] ドロップダウンボックスから、 IP プロトコルとして [TCP] または [UDP] を選択します。
4. [* Remap Direction] * ドロップダウンボックスから、このポートに再マッピングするトラフィック方向（インバウンド、アウトバウンド、または双方向）を選択します。
5. 「 * Original Port * 」に、再マッピングするポートの番号を入力します。
6. 「 * mapped-to Port * 」には、代わりに使用するポートの番号を入力します。
7. [ * ルールの追加 * ] をクリックします。

   新しいポートマッピングがテーブルに追加され、新しいマッピングがただちに有効になります。




8. ポートマッピングを削除するには、削除するルールのオプションボタンを選択し、 * 選択したルールの削除 * をクリックします。

関連情報

""

## アプライアンスストレージノードの導入

ストレージアプライアンスを設置して設定したら、 StorageGRID システムにストレージノードとして導入できます。アプライアンスをストレージノードとして導入する場合は、アプライアンスに搭載されている StorageGRID アプライアンスインストーラを使用

します。

必要なもの

- アプライアンスノードのクローンを作成する場合は、リカバリとメンテナンスの手順を続行します。

  ""

- アプライアンスをラックまたはキャビネットに設置し、ネットワークに接続し、電源を投入しておきます。
- StorageGRID アプライアンスインストーラを使用して、アプライアンスのネットワークリンク、 IP アドレス、ポートの再マッピング（必要な場合）を設定しておきます。
- アプライアンスのコンピューティングコントローラに割り当てられている IP アドレスのいずれかを確認しておきます。接続されているどの StorageGRID ネットワークの IP アドレスでも使用できます。
- StorageGRID システムのプライマリ管理ノードを導入しておきます。
- StorageGRID アプライアンスインストーラの IP 設定ページに表示されるすべてのグリッドネットワークサブネットが、プライマリ管理ノードのグリッドネットワークサブネットリストで定義されている。
- サポートされている Web ブラウザがインストールされたサービスラップトップを用意しておきます。

このタスクについて

各ストレージアプライアンスは単一のストレージノードとして機能します。すべてのアプライアンスは、グリッドネットワーク、管理ネットワーク、およびクライアントネットワークに接続できます

StorageGRID システムにアプライアンスストレージノードを導入するには、 StorageGRID アプライアンスインストーラにアクセスして次の手順を実行します。

- プライマリ管理ノードの IP アドレスおよびストレージノードの名前を指定または確認します。
- 導入を開始し、ボリュームの設定とソフトウェアのインストールが完了するまで待機します。
- アプライアンスインストールタスクの途中でインストールが一時停止した場合は、 Grid Manager にサインインしてすべてのグリッドノードを承認し、 StorageGRID のインストールプロセスと導入プロセスを完了すると、インストールを再開できます。

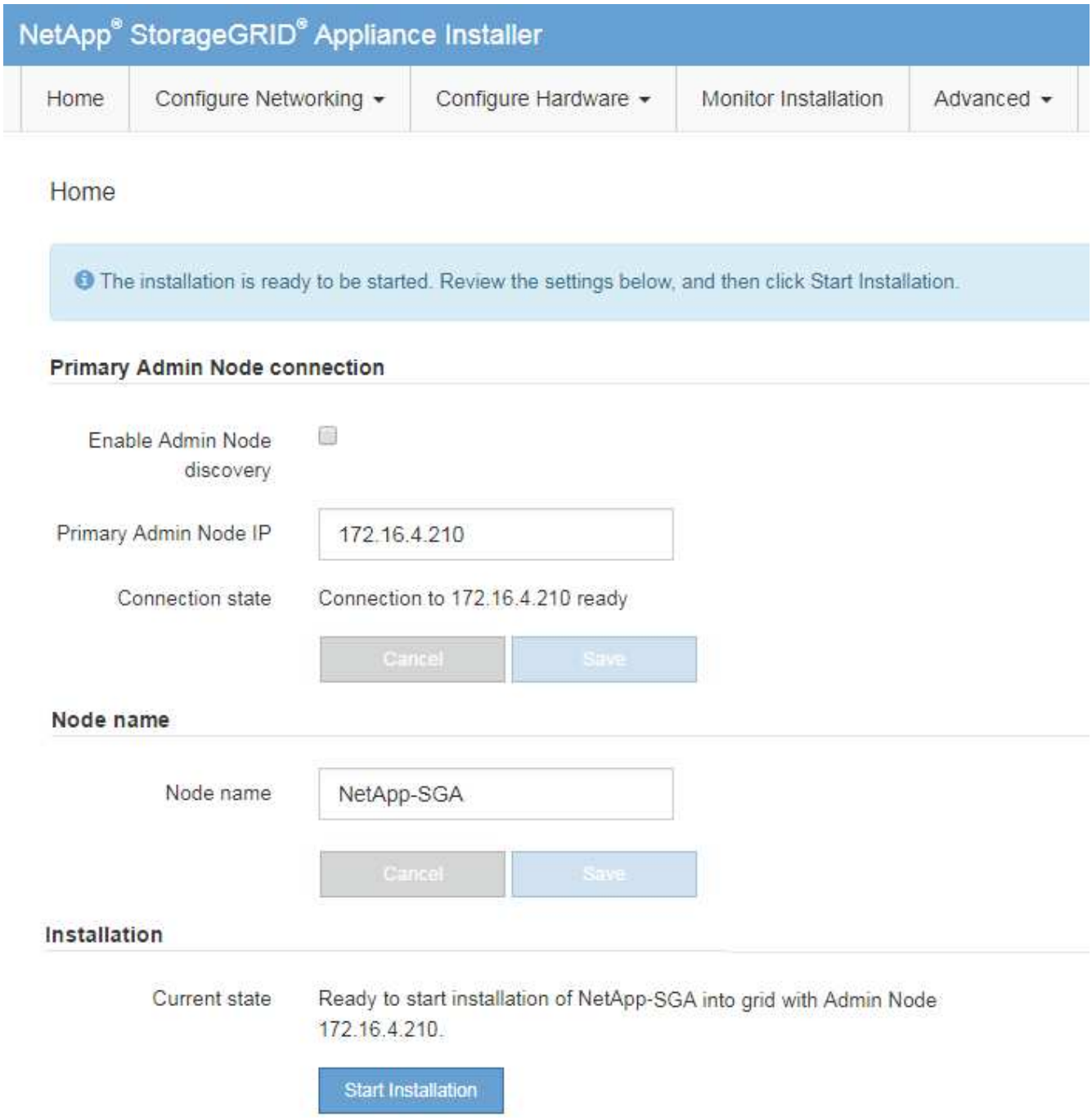
> 一度に複数のアプライアンスノードを導入する必要がある場合は、を使用してインストールプロセスを自動化できます `configure-sga.py` アプライアンスインストールスクリプト。

- 拡張またはリカバリ処理を実行する場合は、該当する手順に従います。
  - 既存の StorageGRID システムにアプライアンスストレージノードを追加する場合は、 StorageGRID システムの拡張手順を参照してください。
  - リカバリ処理の一環としてアプライアンスストレージノードを導入する場合は、リカバリとメンテナンスの手順を参照してください。

手順

1. ブラウザを開き、アプライアンスのコンピューティングコントローラの IP アドレスのいずれかを入力します。[+]
   **`https://Controller_IP:8443`**

   StorageGRID アプライアンスインストーラのホームページが表示されます。




2. 「 * プライマリ管理ノード * 接続」セクションで、プライマリ管理ノードの IP アドレスを指定する必要があるかどうかを確認します。

   このデータセンターに他のノードがすでにインストールされている場合は、プライマリ管理ノードまたは ADMIN_IP が設定された少なくとも 1 つのグリッドノードが同じサブネットにあるという想定で、StorageGRID アプライアンスインストーラがこの IP アドレスを自動的に検出します。

3. この IP アドレスが表示されない場合や変更する必要がある場合は、アドレスを指定します。

| オプション | 説明 |
| --- | --- |
| IP を手動で入力します | a. Enable Admin Node discovery * チェックボックスの選択を解除します。<br>b. IP アドレスを手動で入力します。<br>c. [ 保存（ Save ） ] をクリックします。<br>d. 新しい IP アドレスの接続状態が READY になるまで待ちます。 |
| 接続されたすべてのプライマリ管理ノードの自動検出 | a. Enable Admin Node discovery * チェックボックスを選択します。<br>b. 検出された IP アドレスのリストが表示されるまで待ちます。<br>c. このアプライアンスストレージノードを導入するグリッドのプライマリ管理ノードを選択します。<br>d. [ 保存（ Save ） ] をクリックします。<br>e. 新しい IP アドレスの接続状態が READY になるまで待ちます。 |

4. [* Node name* （ノード名 * ） ] フィールドに、このアプライアンスノードに使用する名前を入力し、 [ * Save * （保存） ] をクリックします。

   このノード名は、 StorageGRID システムでこのアプライアンスノードに割り当てられ、このタブは、 Grid Manager のノードページ（概要タブ）に表示されます。ノードを承認するときに、必要に応じて、この名前を変更できます。

5. Installation（インストール）セクションで、現在の状態がのインストール開始準備完了（Ready to start installation）であることを確認します `node name` をプライマリ管理ノードでグリッドに追加します `admin_ip` "*インストールの開始*ボタンが有効になっていることを確認します。

   [Start Installation* （インストールの開始） ] ボタンが有効になっていない場合は、ネットワーク設定またはポート設定の変更が必要になることがあります。手順については、使用しているアプライアンスのインストールとメンテナンスの手順を参照してください。

   ストレージノードアプライアンスをノードクローニングターゲットとして導入する場合は、ここで導入プロセスを停止して、リカバリとメンテナンスのためにノードクローニング手順 を継続します。

   ""

6. StorageGRID アプライアンスインストーラのホームページで、 * インストールの開始 * をクリックします。

   現在の状態が「 Installation is in progress 」に変わり、「 Monitor Installation 」ページが表示されます。

モニタのインストールページに手動でアクセスする必要がある場合は、 * モニタのインストール * をクリックします。

7. グリッドに複数のアプライアンスストレージノードがある場合は、アプライアンスごとに上記の手順を繰り返します。

一度に複数のアプライアンスストレージノードを導入する必要がある場合は、を使用してインストールプロセスを自動化できます `configure-sga.py` アプライアンスインストールスクリプト。このスクリプトはストレージノードにのみ適用されます。

関連情報

"グリッドを展開します"

""

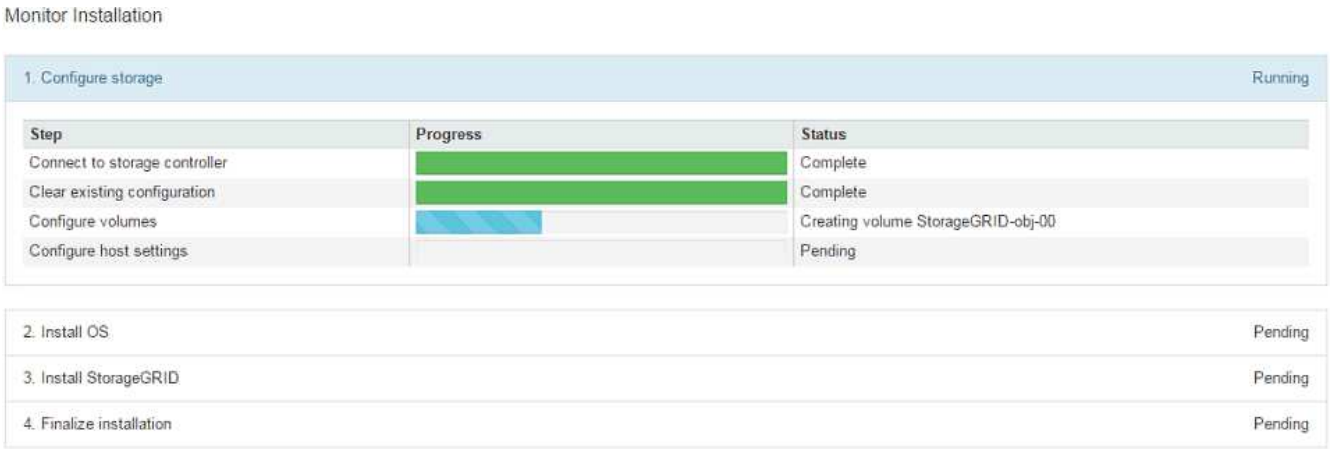
## ストレージアプライアンスのインストールの監視

StorageGRID アプライアンスインストーラでは、インストールが完了するまでステータスが提供されます。ソフトウェアのインストールが完了すると、アプライアンスがリブートされます。

手順

1. インストールの進行状況を監視するには、 * インストールの監視 * をクリックします。

   Monitor Installation ページにインストールの進行状況が表示されます。




   青色のステータスバーは、現在進行中のタスクを示します。緑のステータスバーは、正常に完了したタスクを示します。

インストーラは、以前のインストールで完了したタスクが再実行されないようにします。インストールを再実行している場合 ' 再実行する必要のないタスクは ' 緑色のステータスバーとステータスが [ スキップ済み ] と表示されます

2. インストールの最初の 2 つのステージの進行状況を確認します。

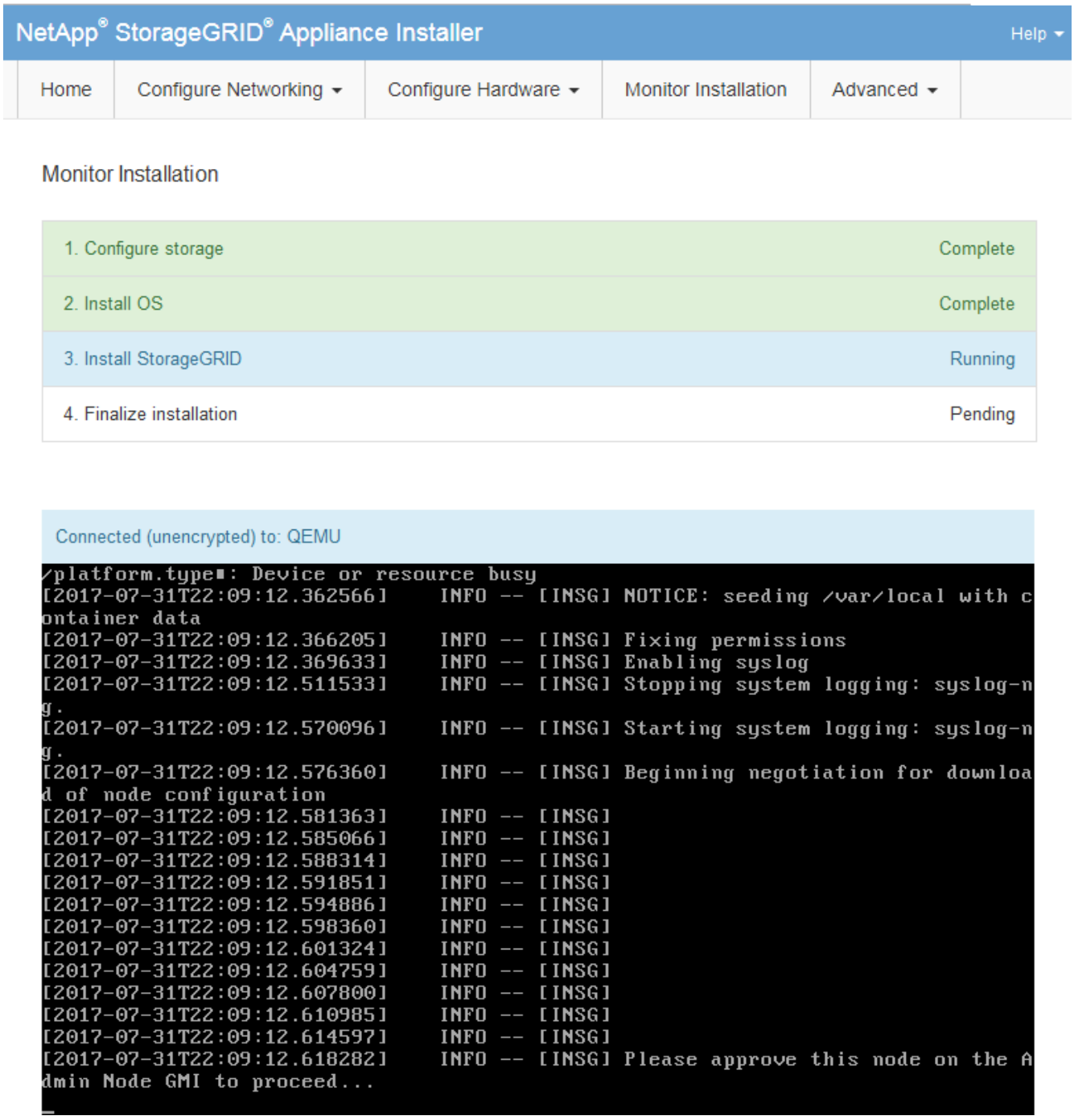
   ◦ 1 。ストレージの構成 *

インストーラがストレージコントローラに接続し、既存の設定があれば消去し、 SANtricity ソフトウェアと通信してボリュームを設定し、ホストを設定します。

※ 2OS * をインストールします

インストーラが StorageGRID のベースとなるオペレーティングシステムイメージをアプライアンスにコピーします。

3. インストールの進行状況の監視を継続して、組み込みコンソールに「 Install StorageGRID * 」ステージが一時停止し、グリッドマネージャを使用して管理ノードでこのノードを承認するように求めるメッセージが表示されるまで続けます。次の手順に進みます。




4. グリッドマネージャに移動し、保留中のストレージノードを承認して、StorageGRID のインストールプロ

セスを完了します。

Grid Manager から * Install * をクリックすると、ステージ 3 が完了し、ステージ 4 * Finalize Installation * が開始されます。ステージ 4 が完了すると、コントローラがリブートされます。

## アプライアンスのインストールと設定の自動化

### アプライアンスのインストールと設定、および StorageGRID システム全体の設定を自動化することができます。

このタスクについて

インストールと設定を自動化すると、複数の StorageGRID インスタンス、または大規模で複雑な StorageGRID インスタンスを 1 つ導入する場合に便利です。

インストールと設定を自動化するには、次のオプションを 1 つ以上使用します。

- アプライアンスの構成設定を指定した JSON ファイルを作成します。StorageGRID アプライアンスインストーラを使用して JSON ファイルをアップロードします。

  同じファイルを使用して、複数のアプライアンスを設定できます。

- StorageGRID を使用します`configure-sga.py` アプライアンスの設定を自動化するPythonスクリプト。
- 追加の Python スクリプトを使用して、 StorageGRID システム全体の他のコンポーネント（「グリッド」）を設定します。

Python スクリプトを StorageGRID 自動化で直接使用することも、 StorageGRID インストール REST API を独自に開発するグリッド導入および設定ツールで使用する例として使用することもできます。リカバリとメンテナンスの手順のStorageGRID インストールファイルのダウンロードと展開に関する情報を参照してください。

**StorageGRID** アプライアンスインストーラを使用したアプライアンス設定の自動化

### 設定情報を含む JSON ファイルを使用して、アプライアンスの設定を自動化することができます。ファイルは StorageGRID アプライアンスインストーラを使用してアップロードします。

必要なもの

- アプライアンスは、 StorageGRID 11.5 以降と互換性のある最新のファームウェアを使用している必要があります。
- 設定するアプライアンスのStorageGRID アプライアンスインストーラに、サポートされているブラウザを使用して接続する必要があります。

このタスクについて

次の設定など、アプライアンスの設定作業を自動化することができます。

- グリッドネットワーク、管理ネットワーク、およびクライアントネットワークの IP アドレス
- BMC インターフェイス

- ネットワークリンク
  - ポートボンディングモード
  - ネットワークボンディングモード
  - リンク速度

アップロードした JSON ファイルを使用してアプライアンスを設定する方が、 StorageGRID アプライアンスインストーラの複数のページを使用して手動で設定を行うよりも効率的です。特に、多数のノードを設定する必要がある場合は効果的です。構成ファイルはノードごとに 1 つずつ適用する必要があります。

アプライアンスのインストールと設定の両方を自動化したいと考えている経験豊富なユーザが、を使用できます `configure-sga.py` スクリプト：[+]"configure-sga.pyスクリプトを使用して、アプライアンスノードのインストールと設定を自動化する"

手順

1. 次のいずれかの方法で JSON ファイルを生成します。
   - ConfigBuilder アプリケーション

     "ConfigBuilder.netapp.com"

   - 。 `configure-sga.py` アプライアンス設定スクリプト。スクリプトは、 StorageGRID アプライアンスインストーラ（ * Help * > * アプライアンス構成スクリプト * ）からダウンロードできます。configure-sga.py スクリプトを使用して設定を自動化する手順を参照してください。

     "configure-sga.pyスクリプトを使用して、アプライアンスノードのインストールと設定を自動化する"

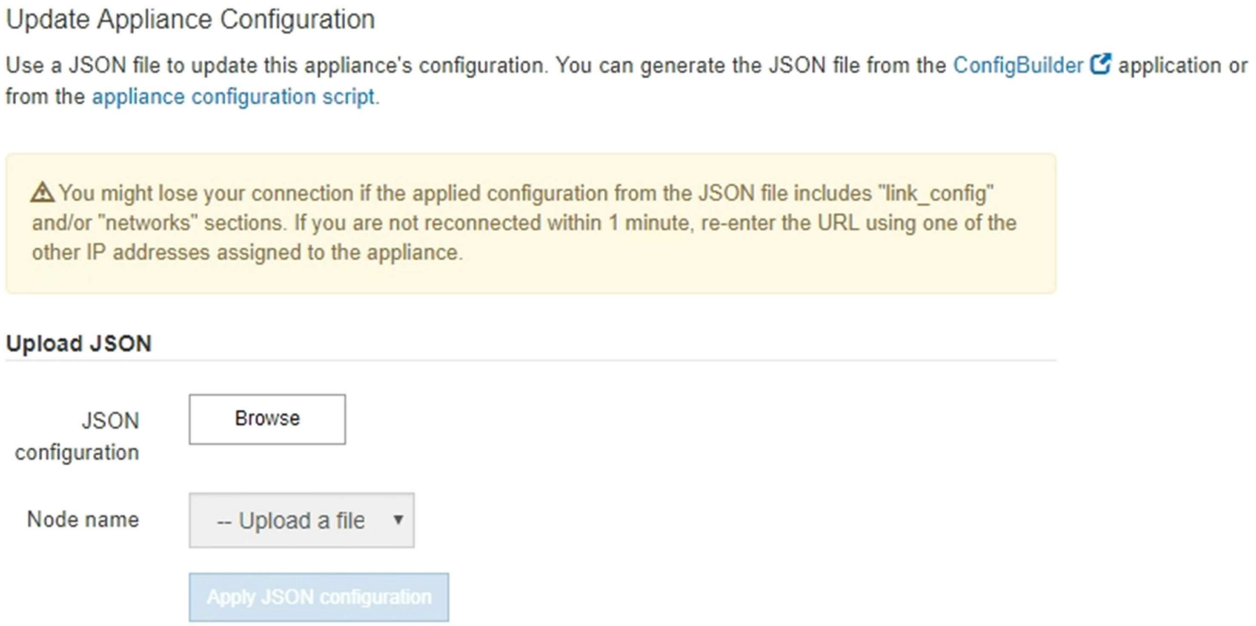
     JSON ファイル内のノード名は、次の要件に従う必要があります。

     - 1 文字以上 32 文字以下の有効なホスト名を指定する必要があります
     - アルファベット、数字、およびハイフンを使用できます
     - 1文字目または最後の文字をハイフンにすることはできません。また、数字だけを使用すること

       JSON ファイル内のノード名（最上位の名前）が一意であることを確認してください。一意でないと、 JSON ファイルを使用して複数のノードを設定できません。

2. 「 * Advanced * > * Update Appliance Configuration * 」を選択します。

   [Update Appliance Configuration] ページが表示されます。




3. アップロードする設定の JSON ファイルを選択します。

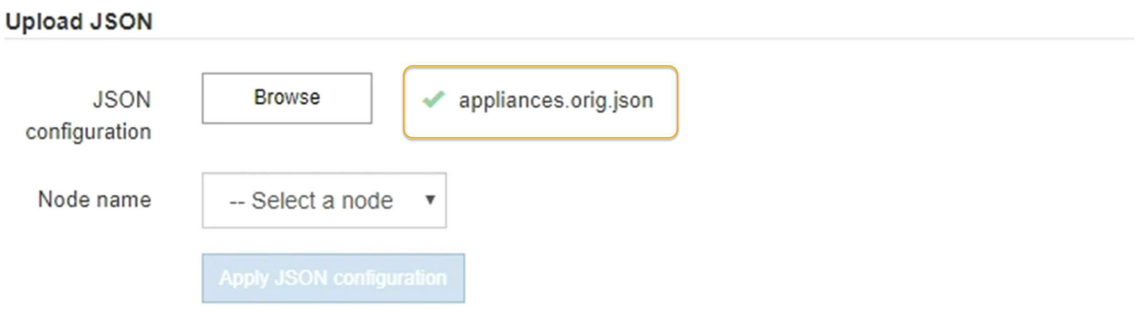
   a. [ * 参照 * ] を選択します。

   b. ファイルを探して選択します。

   c. 「 * 開く * 」を選択します。

   ファイルがアップロードされて検証されます。検証プロセスが完了すると、ファイル名が緑色のチェックマークの横に表示されます。

   > JSON ファイルの構成に「 link_config 」、「 networks 」、またはその両方のセクションが含まれている場合は、アプライアンスへの接続が失われる可能性があります。1 分以内に再接続されない場合は、アプライアンスに割り当てられている他の IP アドレスのいずれかを使用して、アプライアンスの URL を再入力します。

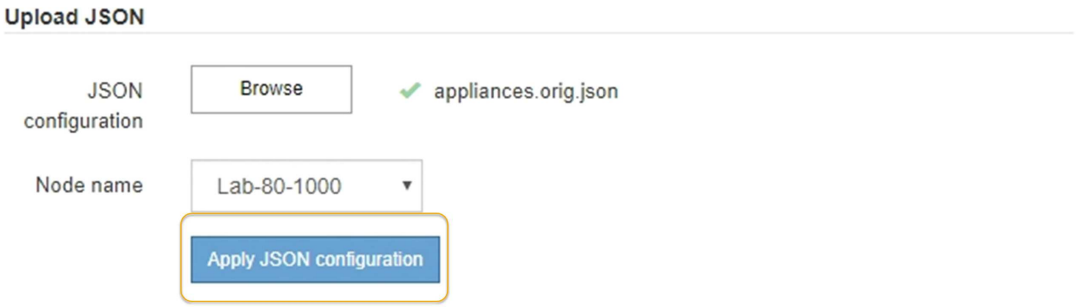



   ノード名 * ドロップダウンには、 JSON ファイルで定義された最上位のノード名が表示されます。

ファイルが有効でない場合、ファイル名は赤色で表示され、黄色のバナーにエラーメッセージが表示されます。無効なファイルはアプライアンスに適用されません。ConfigBuilder を使用して、有効な JSON ファイルを作成できます。

4. ノード名 * ドロップダウンのリストからノードを選択します。

   Apply JSON configuration * ボタンが有効になっている。




5. Apply JSON configuration * を選択します。

   選択したノードに構成が適用されます。

**configure-sga.py**スクリプトを使用して、アプライアンスノードのインストールと設定を自動化する

を使用できます `configure-sga.py` プライマリ管理ノードのインストールや設定など、StorageGRID アプライアンスノードのインストールタスクや設定タスクの多くを自動化するスクリプトです。このスクリプトは、設定するアプライアンスが多数ある場合に役立ちます。スクリプトを使用して、アプライアンスの設定情報を含む JSON ファイルを生成することもできます。

必要なもの

- アプライアンスをラックに設置し、ネットワークに接続し、電源を投入しておきます。
- StorageGRID アプライアンスインストーラを使用してプライマリ管理ノードのネットワークリンクと IP アドレスを設定しておきます。
- プライマリ管理ノードをインストールする場合は、その IP アドレスを確認しておきます。
- 他のノードをインストールして設定する場合は、プライマリ管理ノードが導入され、その IP アドレスを確認しておきます。
- プライマリ管理ノード以外のすべてのノードについて、 StorageGRID アプライアンスインストーラの IP 設定ページに表示されるすべてのグリッドネットワークサブネットが、プライマリ管理ノードのグリッドネットワークサブネットリストで定義されている。
- をダウンロードしておきます `configure-sga.py` ファイル。このファイルはインストール・アーカイブに含まれています。または、 StorageGRID アプライアンス・インストーラの * Help * > * Appliance Installation Script * をクリックしてアクセスできます。

この手順 は、コマンドラインインターフェイスを使用した経験のある上級ユーザを対象としています。また、 StorageGRID アプライアンスインストーラを使用して設定を自動化することもできます。[+]"StorageGRID アプライアンスインストーラを使用したアプライアンス設定の自動化"

手順

1. Python スクリプトを実行するために使用する Linux マシンにログインします。
2. スクリプト構文に関する一般的なヘルプおよび使用可能なパラメータの一覧を表示するには、次のように入力します。

```
configure-sga.py --help
```

   。 `configure-sga.py` スクリプトでは、次の5つのサブコマンド

   ◦ `advanced` BMCの設定、アプライアンスの現在の設定を含むJSONファイルの作成など、StorageGRID アプライアンスの高度な操作用

   ◦ `configure` RAIDモード、ノード名、およびネットワークパラメータを設定するために使用します

   ◦ `install` StorageGRID のインストールを開始する場合に使用します

   ◦ `monitor` StorageGRID インストールの監視用です

   ◦ `reboot` アプライアンスのリブート用です

   サブコマンド（advanced、configure、install、monitor、またはreboot）引数のあとにを入力すると `--help` オプションを指定すると、そのサブコマンド内で使用可能なオプションの詳細を示すヘルプテキストが表示されます
   `configure-sga.py` *`subcommand`* `--help`

3. アプライアンスノードの現在の設定を確認するには、以下のコマンドをどこに入力するかを確認します *`SGA-install-ip`* には、アプライアンスノードのいずれかのIPアドレスを指定します。+
   `configure-sga.py configure` *`SGA-INSTALL-IP`*

   この結果には、プライマリ管理ノードの IP アドレスや管理、グリッド、クライアントネットワークに関する情報など、アプライアンスの現在の IP 情報が表示されます。

```
Connecting to +https://10.224.2.30:8443+ (Checking version and
connectivity.)
2021/02/25 16:25:11: Performing GET on /api/versions... Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/system-info... Received
200
2021/02/25 16:25:11: Performing GET on /api/v2/admin-connection...
Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/link-config... Received
200
2021/02/25 16:25:11: Performing GET on /api/v2/networks... Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/system-config... Received
200
```

```
StorageGRID Appliance
  Name:        LAB-SGA-2-30
  Node type:   storage

StorageGRID primary Admin Node
  IP:        172.16.1.170
  State:     unknown
  Message:   Initializing...
  Version:   Unknown

Network Link Configuration
  Link Status
        Link      State      Speed (Gbps)
        ----      -----      -----
        1         Up         10
        2         Up         10
        3         Up         10
        4         Up         10
        5         Up         1
        6         Down       N/A

  Link Settings
      Port bond mode:      FIXED
      Link speed:          10GBE

      Grid Network:        ENABLED
          Bonding mode:    active-backup
          VLAN:            novlan
          MAC Addresses:   00:a0:98:59:8e:8a  00:a0:98:59:8e:82

      Admin Network:       ENABLED
          Bonding mode:    no-bond
          MAC Addresses:   00:80:e5:29:70:f4

      Client Network:      ENABLED
          Bonding mode:    active-backup
          VLAN:            novlan
          MAC Addresses:   00:a0:98:59:8e:89  00:a0:98:59:8e:81

Grid Network
  CIDR:      172.16.2.30/21 (Static)
  MAC:       00:A0:98:59:8E:8A
  Gateway:   172.16.0.1
  Subnets:   172.17.0.0/21
             172.18.0.0/21
```

```
                192.168.0.0/21
    MTU:        1500

  Admin Network
    CIDR:       10.224.2.30/21 (Static)
    MAC:        00:80:E5:29:70:F4
    Gateway:    10.224.0.1
    Subnets:    10.0.0.0/8
                172.19.0.0/16
                172.21.0.0/16
    MTU:        1500

  Client Network
    CIDR:       47.47.2.30/21 (Static)
    MAC:        00:A0:98:59:8E:89
    Gateway:    47.47.0.1
    MTU:        2000

#################################################################
#####   If you are satisfied with this configuration,    #####
##### execute the script with the "install" sub-command. #####
#################################################################
```

4. 現在の設定のいずれかの値を変更する必要がある場合は、を使用します `configure` サブコマンドを使用して更新します。たとえば、アプライアンスがプライマリ管理ノードへの接続に使用するIPアドレスをに変更する場合などです `172.16.2.99`をクリックし、「+」と入力します
`configure-sga.py configure --admin-ip 172.16.2.99 SGA-INSTALL-IP`
5. アプライアンスの設定をJSONファイルにバックアップする場合は、を使用します `advanced` および `backup-file` サブコマンド。たとえば、IPアドレスを持つアプライアンスの設定をバックアップする場合などです *SGA-INSTALL-IP* を指定します `appliance-SG1000.json`をクリックし、「+」と入力します
`configure-sga.py advanced --backup-file appliance-SG1000.json SGA-INSTALL-IP`

   設定情報が格納された JSON ファイルは、スクリプトの実行元と同じディレクトリに書き込まれます。

   > 生成された JSON ファイルの最上位のノード名がアプライアンス名と一致していることを確認します。経験豊富なユーザで StorageGRID API について十分な知識がある場合を除き、このファイルに変更を加えないでください。

6. アプライアンスの設定に問題がなければ、を使用します `install` および `monitor` アプライアンスをインストールするためのサブコマンド：+
`configure-sga.py install --monitor SGA-INSTALL-IP`
7. アプライアンスをリブートする場合は、「+」を入力します
`configure-sga.py reboot SGA-INSTALL-IP`

# グリッドノードを導入したら、 StorageGRID システムの設定を自動化できます。

必要なもの

- インストールアーカイブにある次のファイルの場所を確認しておきます。

| ファイル名 | 説明 |
| --- | --- |
| `configure-storagegrid.py` | 設定を自動化するための Python スクリプト |
| `configure-storagegrid.sample.json` | スクリプトで使用するサンプル構成ファイル |
| `configure-storagegrid.blank.json` | スクリプトで使用する空の構成ファイルです |

- を作成しておきます `configure-storagegrid.json` 構成ファイルこのファイルを作成するには、サンプル構成ファイルを変更します (`configure-storagegrid.sample.json`)または空の構成ファイル (`configure-storagegrid.blank.json`) 。

このタスクについて

を使用できます `configure-storagegrid.py` Pythonスクリプトおよび `configure-storagegrid.json` StorageGRID システムの設定を自動化するための構成ファイル。

また、 Grid Manager またはインストール API を使用してシステムを設定することもできます。

手順

1. Python スクリプトを実行するために使用する Linux マシンにログインします。
2. インストールアーカイブを展開したディレクトリに移動します。

   たとえば、「+」と入力します
   `cd StorageGRID-Webscale-version/platform`

   ここで、 *platform* はです `debs`、 `rpms`または `vsphere`。

3. Python スクリプトを実行し、作成した構成ファイルを使用します。

   例：

```
./configure-storagegrid.py ./configure-storagegrid.json --start-install
```

完了後

リカバリパッケージ `.zip` 設定プロセスでファイルが生成され、インストールと設定を実行するディレクトリにダウンロードされます。グリッドノードで障害が発生した場合に StorageGRID システムをリカバリできるようにするために、リカバリパッケージファイルをバックアップする必要があります。たとえば、バックアップされたセキュアなネットワーク上の場所や、安全なクラウドストレージ上の場所にコピーします。

リカバリパッケージファイルには StorageGRID システムからデータを取得するための暗号キーとパスワードが含まれているため、安全に保管する必要があります。

ランダムパスワードを生成するように指定した場合は、を展開する必要があります `Passwords.txt` ファイルを開き、StorageGRID システムへのアクセスに必要なパスワードを探します。

```
######################################################################
##### The StorageGRID "recovery package" has been downloaded as: #####
#####           ./sgws-recovery-package-994078-rev1.zip          #####
#####   Safeguard this file as it will be needed in case of a    #####
#####                 StorageGRID node recovery.                 #####
######################################################################
```

StorageGRID システムがインストールおよび設定されると、確認メッセージが表示されます。

```
StorageGRID has been configured and installed.
```

## インストール **REST API** の概要

StorageGRID には、インストールタスクを実行するための REST API として、StorageGRID インストール API と StorageGRID アプライアンスインストーラ API の 2 つが用意されています。

どちらの API も、 Swagger オープンソース API プラットフォームを使用して API のドキュメントを提供しています。Swagger では、ユーザインターフェイスを使用してパラメータやオプションを変更した場合の API の動作を確認しながら、 API の開発を進めることができます。このドキュメントは、標準的な Web テクノロジと JavaScript Object Notation （ JSON ）データ形式について十分理解していることを前提としています。

API Docs Web ページを使用して実行する API 処理はすべてその場で実行されます。設定データやその他のデータを誤って作成、更新、または削除しないように注意してください。

各 REST API コマンドは、 API の URL 、 HTTP アクション、必須またはオプションの URL パラメータ、および想定される API 応答で構成されます。

### **StorageGRID** インストール **API**

StorageGRID インストール API は、 StorageGRID システムを最初に設定するとき、およびプライマリ管理ノードのリカバリを実行する必要がある場合にのみ使用できます。インストール API には、 Grid Manager から HTTPS 経由でアクセスできます。

API のドキュメントにアクセスするには、プライマリ管理ノードのインストール用 Web ページに移動し、メニューバーから * Help * > * API Documentation * を選択します。

StorageGRID インストール API には次のセクションがあります。

- *config *-- API の製品リリースとバージョンに関連する操作。製品リリースバージョンおよびそのリリースでサポートされる API のメジャーバージョンを一覧表示できます。

- * grid * — グリッドレベルの設定操作。グリッドの詳細、グリッドネットワークのサブネット、グリッドパスワード、 NTP および DNS サーバの IP アドレスなど、グリッド設定を取得および更新できます。
- *nodes * — ノードレベルの設定操作。グリッドノードのリストを取得できるほか、グリッドノードの削除、設定、表示、およびグリッドノードの設定のリセットを行うことができます。
- *provision * — プロビジョニング操作。プロビジョニング処理を開始し、プロビジョニング処理のステータスを表示できます。
- * recovery * - プライマリ管理ノードのリカバリ処理。情報のリセット、リカバリパッケージのアップロード、リカバリの開始、およびリカバリ処理のステータスの表示を行うことができます。
- * recovery-package * — リカバリパッケージをダウンロードする処理。
- *sites * — サイトレベルの設定操作。サイトを作成、表示、削除、および変更できます。

**StorageGRID** アプライアンスインストーラ **API**

StorageGRID アプライアンスインストーラAPIには、からHTTPS経由でアクセスできます `Controller_IP:8443`。

API ドキュメントにアクセスするには、アプライアンスの StorageGRID アプライアンスインストーラのメニューバーから * Help * > * API Docs * を選択します。

StorageGRID アプライアンスインストーラ API には、次のセクションがあります。

- * clone * — ノードのクローニングを構成および制御するための処理。
- *encryption * — 暗号化を管理し、暗号化ステータスを表示するための処理。
- * ハードウェア構成 * — 接続されたハードウェアでシステム設定を構成するための操作。
- *installation * ：アプライアンスのインストールを開始し、インストール・ステータスを監視するための処理。
- * networking * — StorageGRID アプライアンスのグリッドネットワーク、管理ネットワーク、クライアントネットワークの設定、およびアプライアンスのポート設定に関連する処理です。
- * setup * - システムに関する情報の取得やプライマリ管理ノード IP の更新要求など、アプライアンスの初期インストール設定に役立つ処理。
- *support *--コントローラのリブートとログ取得のための処理。
- * upgrade * ：アプライアンス・ファームウェアのアップグレードに関連する操作
- **uploadsg** — StorageGRID インストールファイルをアップロードするための操作。

## ハードウェアの設置のトラブルシューティング

設置作業で問題が発生した場合は、ハードウェアのセットアップや接続の問題に関するトラブルシューティング情報を確認すると役立つことがあります。

関連情報

"ハードウェアのセットアップがハングしたように見えます"

"接続の問題のトラブルシューティング"

# ハードウェア障害やケーブル接続エラーによって E5600SG コントローラのブート処理が完了しなかった場合は、 StorageGRID アプライアンスインストーラを使用できないことがあります。

手順

1. いずれかのコントローラの警告 LED を確認し、点滅しているエラーコードを探します。

   電源投入時は、ハードウェアの初期化が完了するまで、保守操作可能を示す LED と保守操作要を示す LED が点灯した状態になります。また、 *diagnostic LED* という名前の下の桁の上の小数点も点灯します。デジタル表示ディスプレイには、両方のコントローラに共通のコードが順番に表示されます。これは正常な状態であり、エラーを示すものではありません。ハードウェアのブートが完了すると、保守操作の LED は消灯し、ディスプレイの制御がファームウェアに切り替わります。

2. E5600SG コントローラのデジタル表示ディスプレイのコードを確認します。

   インストールとプロビジョニングには時間がかかります。フェーズによっては、StorageGRID アプライアンスインストーラの更新が数分間報告されないこともあります。

   エラーが発生すると、デジタル表示ディスプレイに HE などの一連のコードが点滅します。

3. これらのコードの意味については、次のリソースを参照してください。

| コントローラ | 参照 |
| --- | --- |
| E5600SG コントローラ | • “he error:Error synchronizing with SANtricity OS Software” （エラー： OS ソフトウェアとの同期エラー）<br>• "E5600SG コントローラのデジタル表示ディスプレイ・コード " |
| E2700 コントローラ | E シリーズのドキュメント<br>• 注： * E シリーズ E5600 コントローラに関するコードは、アプライアンスの E5600SG コントローラには適用されません。 |

4. この方法で問題 が解決しない場合は、テクニカルサポートにお問い合わせください。

関連情報

"E5600SG コントローラのデジタル表示ディスプレイのコード"

"HE エラー： SANtricity OS ソフトウェアとの同期エラー"

"E2700 コントローラドライブトレイおよび関連ドライブトレイ設置ガイド"

"ネットアップのマニュアル： E2700 シリーズ"

**HE** エラー： **SANtricity OS** ソフトウェアとの同期エラー

# StorageGRID アプライアンスインストーラが SANtricity OS ソフトウェアと同期できない場合は、コンピューティングコントローラのデジタル表示ディスプレイに HE エラーコードが表示されます。

このタスクについて

HE エラーコードが表示された場合は、次の対処策を実施します。

手順

1. 2 本の SAS インターコネクトケーブルの整合性をチェックし、しっかりと接続されていることを確認します。
2. 必要に応じて、一方または両方のケーブルを交換し、再試行します。
3. この方法で問題 が解決しない場合は、テクニカルサポートにお問い合わせください。

接続の問題のトラブルシューティング

# StorageGRID アプライアンスのインストール時に接続の問題が発生した場合は、以下に記載する対処策を実施する必要があります。

**StorageGRID** アプライアンスにネットワーク経由で接続できません

# アプライアンスに接続できない場合は、ネットワーク問題 があるか、またはハードウェアの設置が正常に完了していない可能性があります。

- * 問題 *

  アプライアンスに接続できません。

- * 原因 *

  この問題は、ネットワーク問題 が存在する場合、またはハードウェアの設置が正常に完了しなかった場合に発生することがあります。

- * 是正措置 *

  a. アプライアンスにpingを送信します。+
  **`ping E5600_controller_IP`**

  b. ブラウザを開いて次のように入力し、StorageGRID アプライアンスインストーラにアクセスします。+
  **`https://Management_Port_IP:8443`**

  Management_Port_IP には、 E5600SG コントローラ（物理インストールでプロビジョニングされた）の管理ポート 1 の IP アドレスを入力します。

  c. [ 管理ネットワークの設定 *] をクリックし、 IP を確認します。

  d. ping からの応答を受信したら、ファイアウォールでポート 8443 が開いていることを確認します。

  e. アプライアンスをリブートします。

f. インストール用 Web ページをリフレッシュします。

g. この方法で接続問題 が解決しない場合は、NetApp Support Siteからテクニカルサポートにお問い合わせください "mysupport.netapp.com"。

関連情報

"E5600SG コントローラのデジタル表示ディスプレイのコード"

**StorageGRID** アプライアンスインストーラの実行中にコントローラをリブートします

## StorageGRID アプライアンスインストーラの実行中にコンピューティングコントローラのリブートが必要になる場合があります。たとえば、インストールが失敗した場合は、コントローラのリブートが必要になることがあります。

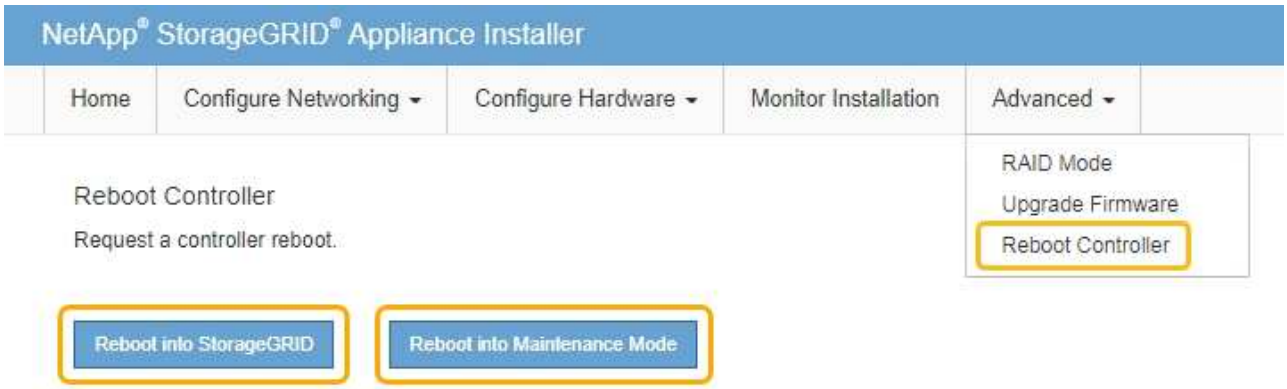
このタスクについて

この手順 は、コンピューティングコントローラで StorageGRID アプライアンスインストーラが実行されている場合にのみ適用されます。インストールが完了すると、 StorageGRID アプライアンスインストーラが使用できなくなるため、この手順は機能しなくなります。

手順

1. StorageGRID アプライアンス・インストーラで、 [**Advanced**>*Reboot Controller*] をクリックし、次のいずれかのオプションを選択します。

   - Reboot into StorageGRID * を選択し、ノードをグリッドに再追加してコントローラをリブートします。メンテナンスモードで作業を完了し、ノードを通常動作に戻す準備ができている場合は、このオプションを選択します。
   - メンテナンスモードを維持したままコントローラをリブートするには、 * Reboot into Maintenance Mode * を選択します。このオプションは、グリッドに再追加する前にノードで追加のメンテナンス処理を実行する必要がある場合に選択しま
     す。




SG6000-CN コントローラがリブートされます。

# SG5600アプライアンスのメンテナンス

## E2700 コントローラ上の SANtricity OS ソフトウェアのアップグレード、 E2700 コント

ローラまたは E5600SG コントローラの交換、または特定のコンポーネントの交換が必要となる場合があります。このセクションの手順は、アプライアンスが StorageGRID システムにストレージノードとしてすでに導入されていることを前提としています。

手順

- "アプライアンスをメンテナンスモードにします"
- "グリッドマネージャを使用してストレージコントローラのSANtricity OSをアップグレードします"
- "E2700コントローラでのSANtricity OSのメンテナンスモードを使用したアップグレード"
- "SANtricity Storage Managerを使用してドライブファームウェアをアップグレードしています"
- "E2700コントローラの交換"
- "E5600SGコントローラの交換"
- "その他のハードウェアコンポーネントの交換"
- "E5600SGコントローラのリンク設定の変更"
- "MTU設定を変更します"
- "DNSサーバの設定を確認しています"
- "メンテナンスモードでのノード暗号化の監視"

アプライアンスをメンテナンスモードにします

## 特定のメンテナンス手順を実行する前に、アプライアンスをメンテナンスモードにする必要があります。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Maintenance または Root Access 権限が必要です。詳細については、 StorageGRID の管理手順を参照してください。

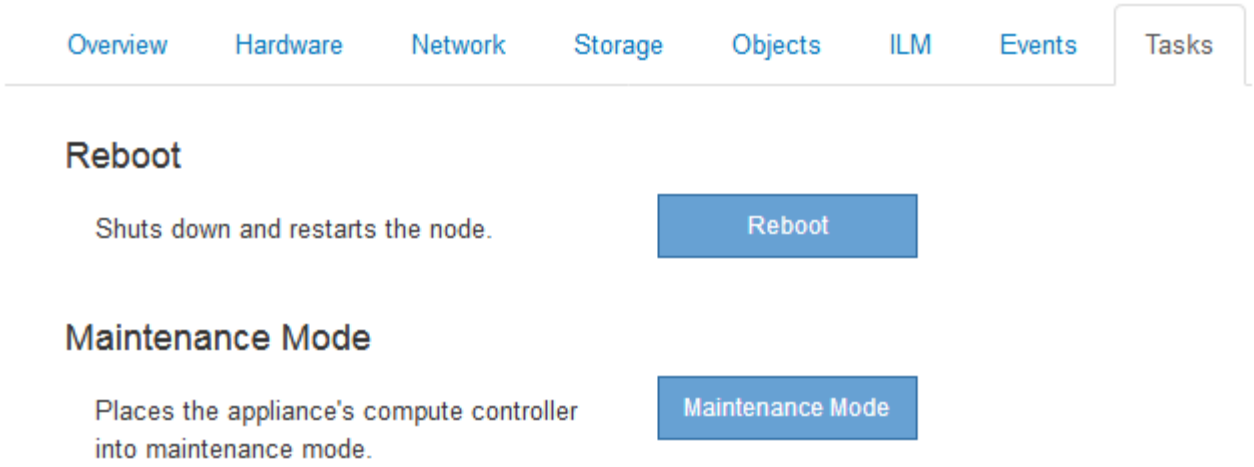
このタスクについて

StorageGRID アプライアンスをメンテナンスモードにすると、アプライアンスにリモートアクセスできなくなることがあります。

保守モードのStorageGRID アプライアンスのパスワードおよびホスト・キーは、アプライアンスが稼働していたときと同じままです。

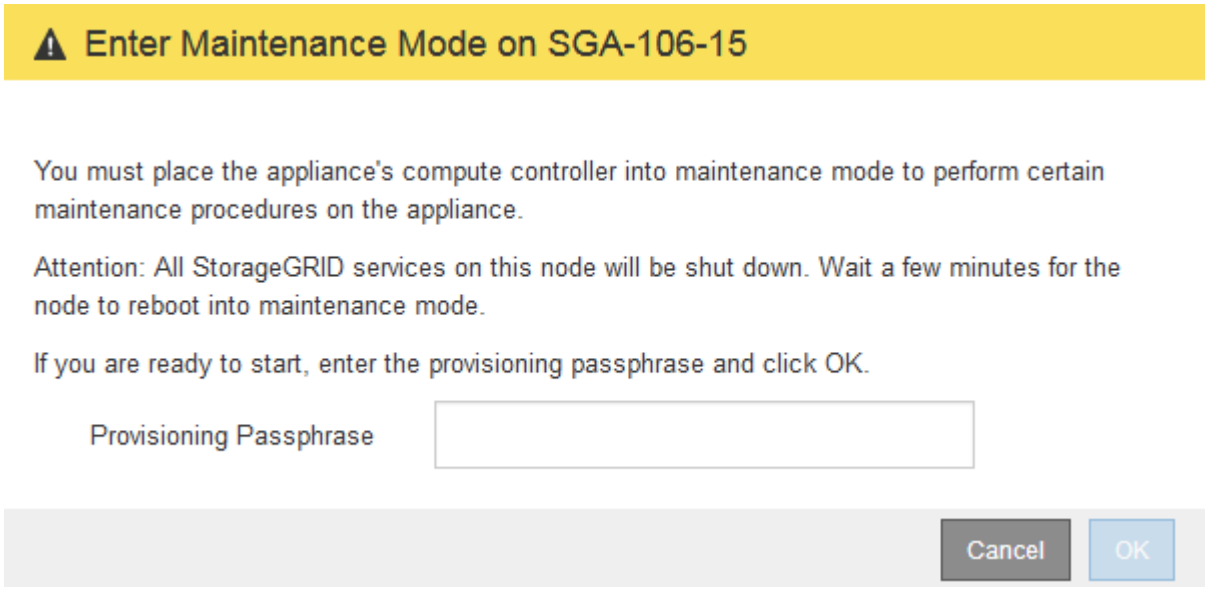
手順

1. Grid Managerから* Nodes *を選択します。
2. Nodes ページのツリービューで、アプライアンスストレージノードを選択します。
3. [ タスク ] を選択します。



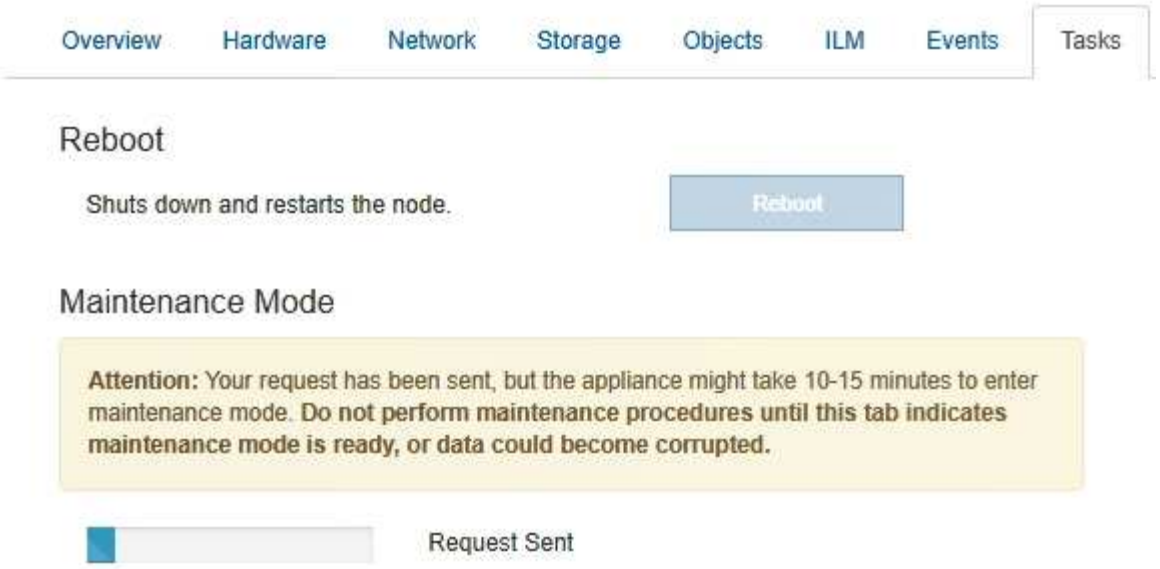

4. [* Maintenance Mode]*を選択します。

   確認のダイアログボックスが表示されます。

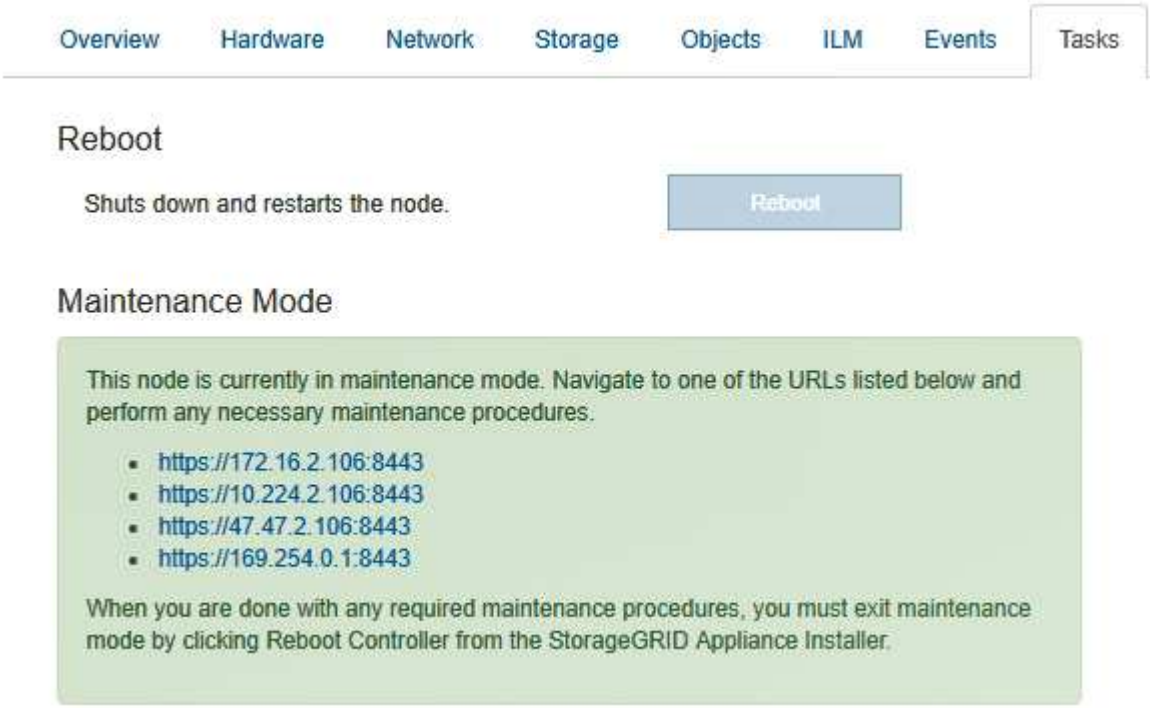



5. プロビジョニングパスフレーズを入力し、「 * OK 」を選択します。

   進捗状況バーと一連のメッセージ（「 Request Sent 」、「 Stopping StorageGRID 」、「 Rebaling 」など）は、アプライアンスがメンテナンスモードに移行するための手順を完了していることを示しています。




アプライアンスがメンテナンスモードになっている場合は、 StorageGRID アプライアンスインストーラへのアクセスに使用できる URL が確認メッセージに表示されます。




6. StorageGRID アプライアンスインストーラにアクセスするには、表示されたいずれかの URL にアクセスします。

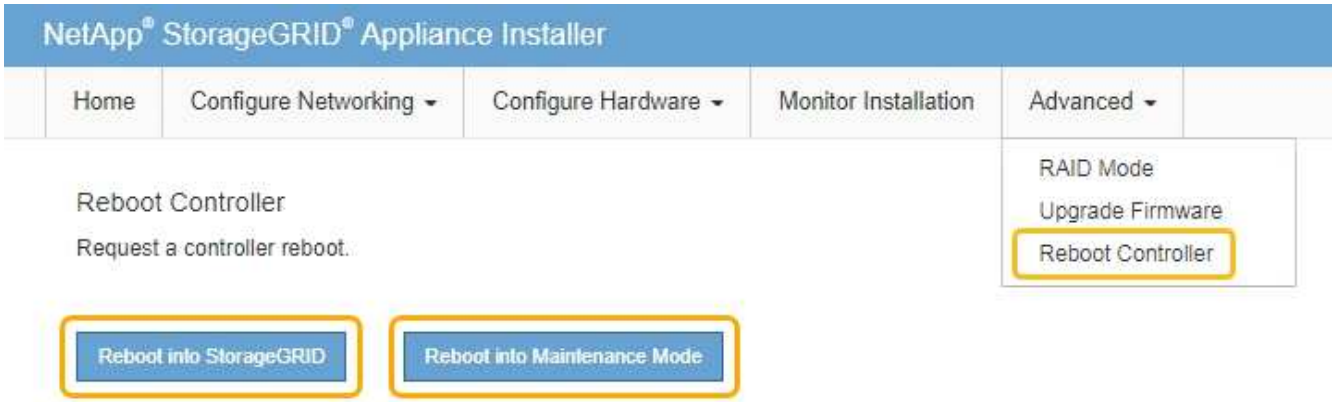
   可能であれば、アプライアンスの管理ネットワークポートの IP アドレスを含む URL を使用します。

   > へのアクセス `https://169.254.0.1:8443` ローカル管理ポートに直接接続する必要があります。

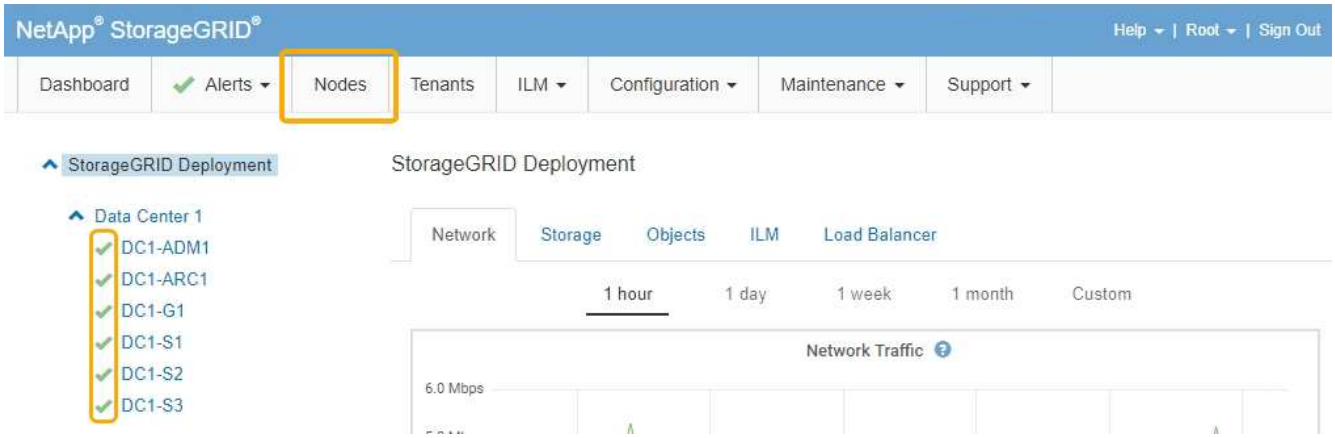
7. StorageGRID アプライアンスインストーラで、アプライアンスがメンテナンスモードになっていることを

確認します。

8. 必要なメンテナンスタスクを実行します。
9. メンテナンス作業が完了したら、メンテナンスモードを終了して通常のノードの運用を再開します。StorageGRID アプライアンス・インストーラから、 **Advanced**>* Reboot Controller* を選択し、 * Reboot into StorageGRID * を選択します。




アプライアンスがリブートしてグリッドに再参加するまでに最大 20 分かかることがあります。リブートが完了し、ノードが再びグリッドに参加したことを確認するには、 Grid Manager に戻ります。[ノード*（Nodes *）]タブには、通常のステータスが表示されます ✔ アクティブなアラートがなく、ノードがグリッドに接続されていることを示す、アプライアンスノードの場合。




グリッドマネージャを使用してストレージコントローラの**SANtricity OS**をアップグレードします

## Grid Managerを使用してSANtricity OSのアップグレードを適用

必要なもの

- NetApp Interoperability Matrix Tool （ IMT ）を参照して、アップグレードに使用する SANtricity OS のバージョンがお使いのアプライアンスと互換性があることを確認してください。

- Maintenance権限が必要です。
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- プロビジョニングパスフレーズが必要です。
- SANtricity OSに関するネットアップのダウンロードページを利用する必要があります。

このタスクについて

SANtricity OS のアップグレードプロセスが完了するまで、他のソフトウェアの更新（ StorageGRID ソフトウェアのアップグレードまたはホットフィックス）は実行できません。SANtricity OS のアップグレードプロセスが完了する前にホットフィックスや StorageGRID ソフトウェアのアップグレードを開始しようとすると、SANtricity OS のアップグレードページが表示されます。

該当するすべてのノードにSANtricity OSのアップグレードが正常に適用されるまで、手順 は完了しません。各ノードにSANtricity OSがロードされ、各StorageGRID ストレージアプライアンスがリブートされるまでに30分以上かかることがあります。

次の手順は、 Grid Manager を使用してアップグレードを実行する場合にのみ実行できます。

この手順 は、 SANtricity OS のアップグレードに関連付けられた最新バージョンに NVSRAM を自動的にアップグレードします。個別の NVSRAM アップグレードファイルを適用する必要はありません。

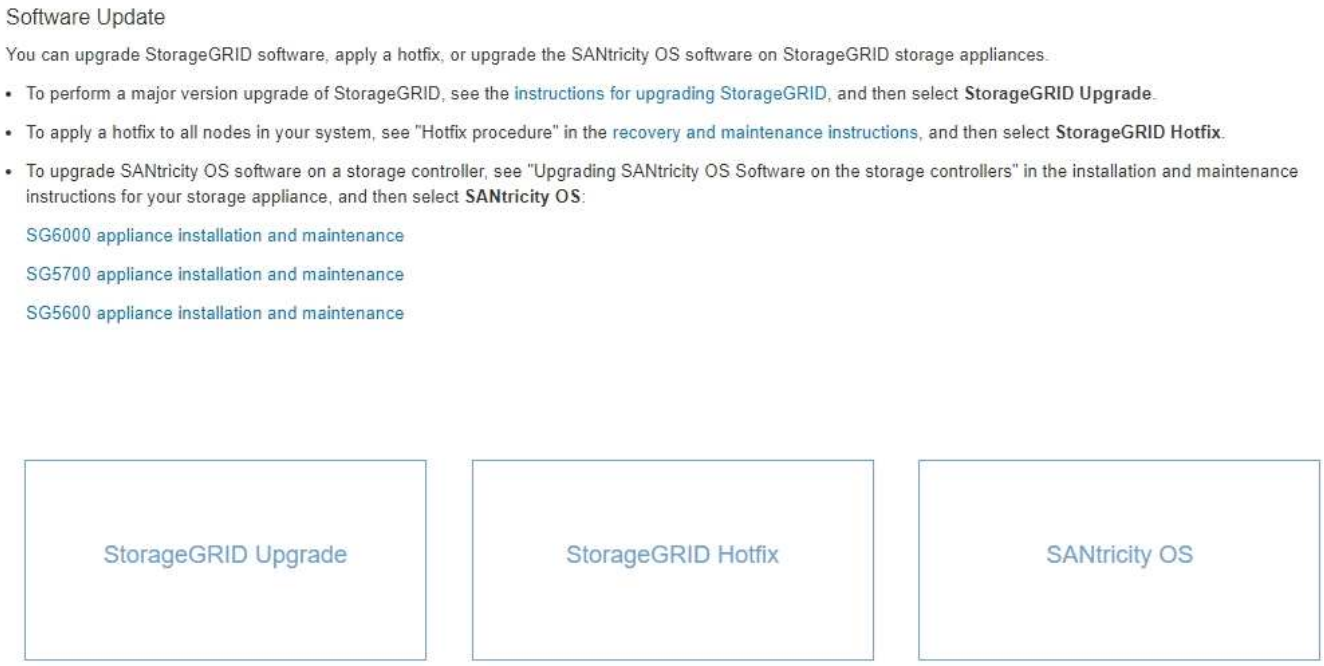
手順

1. サービスラップトップから、NetApp Support Site から新しいSANtricity OSファイルをダウンロードします。

   E2700ストレージコントローラのSANtricity OSバージョンを選択してください。

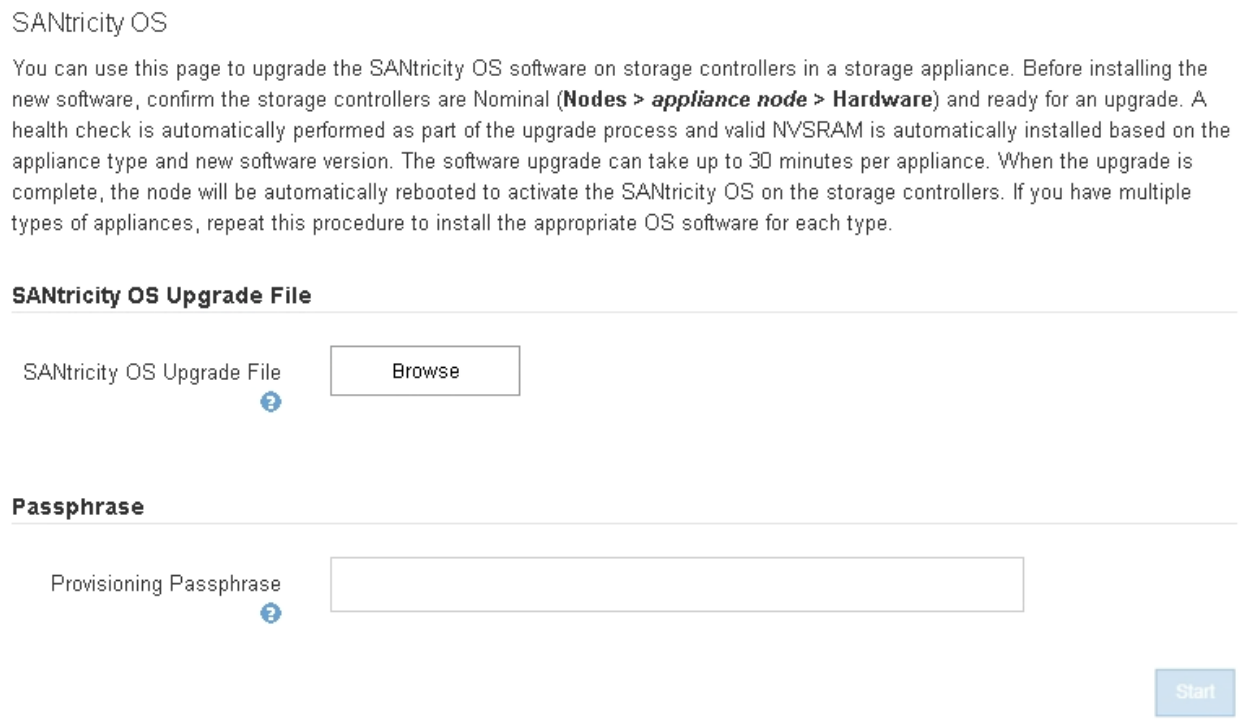
2. サポートされているブラウザを使用してGrid Managerにサインインします。
3. [* Maintenance（メンテナンス）]を選択します次に、メニューの[システム]セクションで、[ソフトウェア・アップデート]を選択します。

   Software Update ページが表示されます。




4. SANtricity OS *をクリックします。

   SANtricity OSページが表示されます。




5. NetApp Support Siteからダウンロードした SANtricity OS アップグレードファイルを選択します。

   a. [* 参照 ] をクリックします。

   b. ファイルを探して選択します。

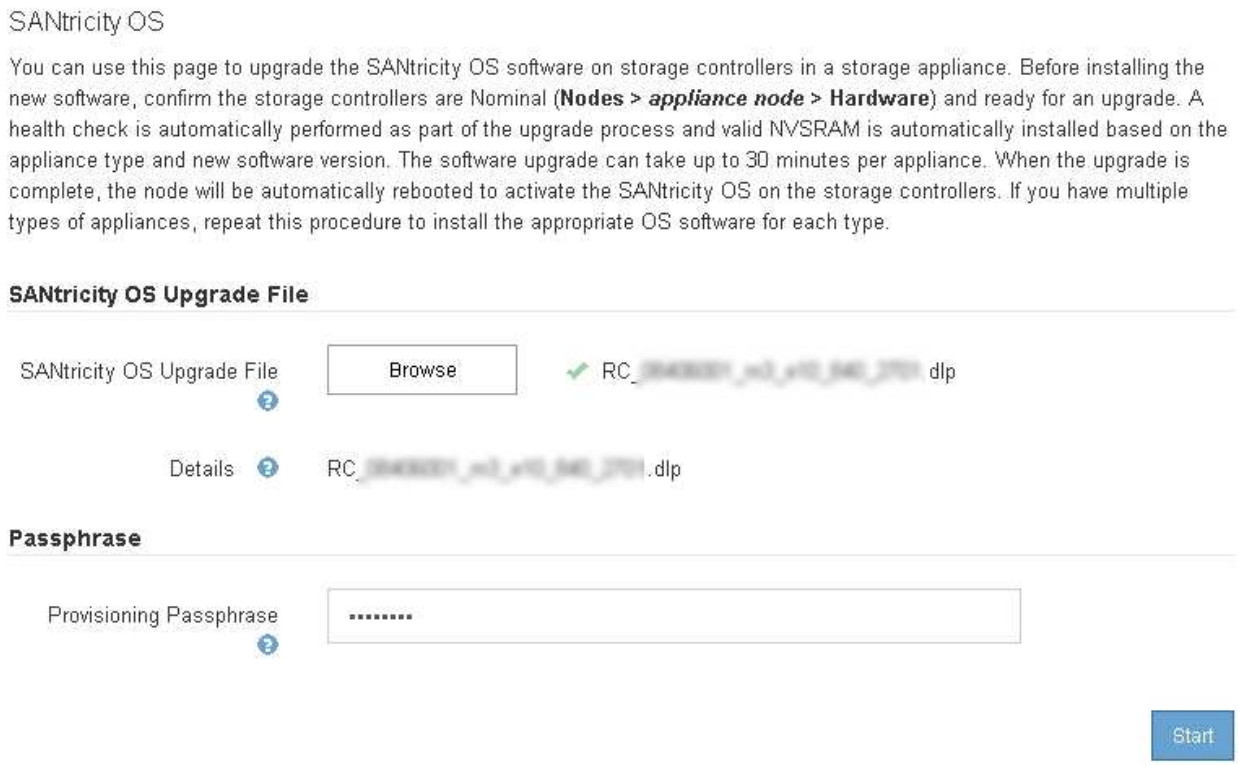
c. * 開く * をクリックします。

ファイルがアップロードされて検証されます。検証プロセスが完了すると、[詳細]フィールドにファイル名が表示されます。

ファイル名は検証プロセスで指定されるため変更しないでください。

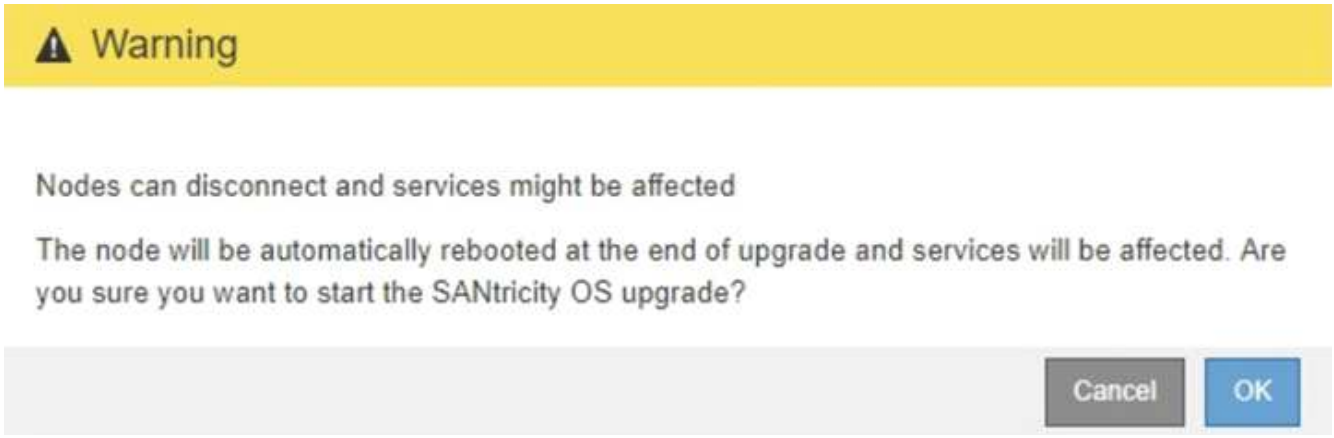
6. プロビジョニングパスフレーズを入力します。

「 * Start * （スタート * ）」ボタンが有効になります。




7. [ スタート ] ボタンをクリックします。

   アップグレードされたノードのサービスを再起動するとブラウザの接続が一時的に失われる可能性があることを示す警告ボックスが表示されます。




8. OK *をクリックして、SANtricity OSアップグレードファイルをプライマリ管理ノードにステージングします。

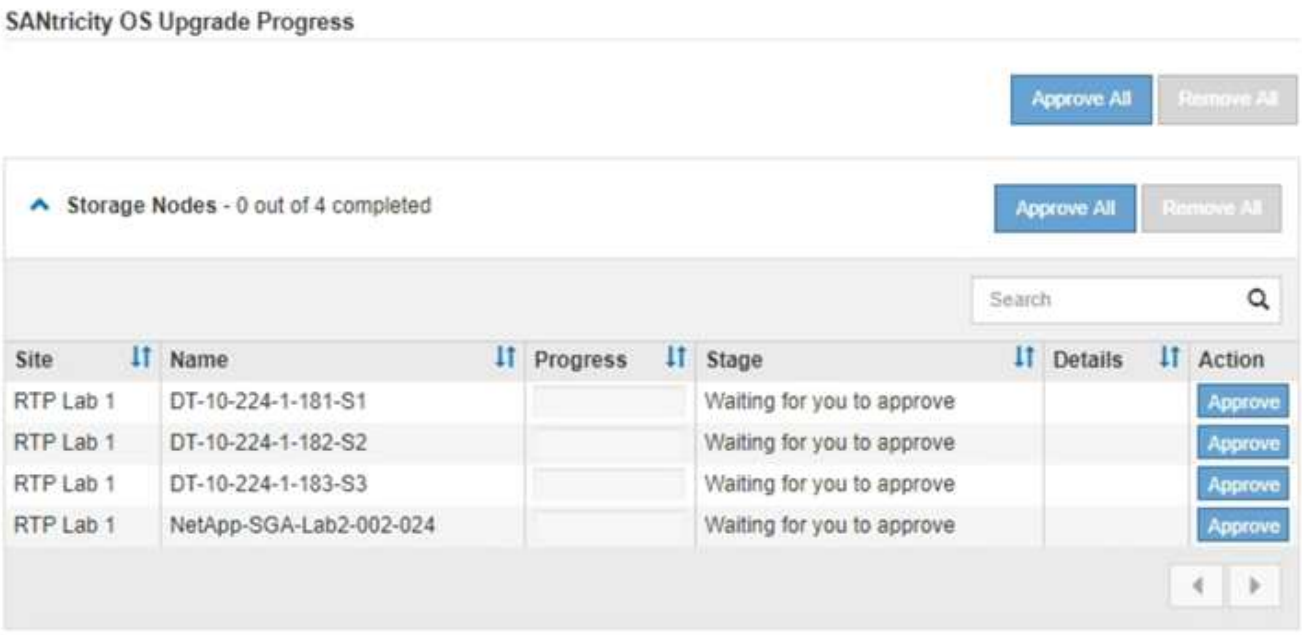
   SANtricity OS のアップグレードを開始すると、次の処理が行わ

   a. 健全性チェックが実行されます。このプロセスにより、ステータスが「 Needs Attention 」になっているノードがないかどうかが確認されます。

      エラーが報告された場合は、エラーを解決してから、*開始*をもう一度クリックします。

b. SANtricity OS Upgrade Progress テーブルが表示されます。この表には、グリッド内のすべてのストレージノードと、各ノードのアップグレードの現在のステージが表示されます。

ソフトウェアベースのストレージノードを含むすべてのストレージノードが表示されます。SANtricity OSのアップグレードがソフトウェアベースのストレージノードに影響しない場合でも、すべてのストレージノードのアップグレードを承認する必要があります。ソフトウェア・ベースのストレージ・ノードに対して返されたアップグレード・メッセージは「SANtricity OS upgrade is not applicable to this node.」です。




9. 必要に応じて、ノードのリストを* Site 、 Name 、 Progress 、 Stage 、または Details *で昇順または降順にソートします。または、 * 検索 * ボックスに用語を入力して特定のノードを検索します。

ノードのリストをスクロールするには、セクションの右下隅にある左右の矢印を使用します。

10. アップグレードキューに追加する準備ができたグリッドノードを承認します。同じタイプの承認済みノードが一度に 1 つずつアップグレードされます。

アプライアンスストレージノードのSANtricity OSアップグレードは、ノードを停止およびリブートする準備ができているかどうかが確認されないかぎり承認しないでください。ノードでSANtricity OSのアップグレードが承認されると、そのノードのサービスが停止します。あとでノードをアップグレードすると、アプライアンスノードがリブートされます。このような処理を実行すると、ノードと通信しているクライアントで原因 サービスが中断する可能性があります。

- すべてのストレージノードをSANtricity OSアップグレードキューに追加するには、いずれかの*すべて承認ボタンをクリックします。

ノードのアップグレード順序が重要な場合は、ノードまたはノードグループを 1 つずつ承認し、各ノードでアップグレードが完了するまで待ってから、次のノードを承認します。

- 1つ以上の*承認*ボタンをクリックして、SANtricity OSアップグレードキューに1つ以上のノードを追

加します。

> ノードへのSANtricity OSのアップグレードの適用は遅延できますが、リストされているすべてのストレージノードでSANtricity OSのアップグレードを承認するまで、SANtricity OSのアップグレードプロセスは完了しません。

[* Approve *（承認）]をクリックすると、アップグレードプロセスによってノードをアップグレードできるかどうかが決定されます。ノードをアップグレード可能な場合は、アップグレードキューに追加されます。[+]

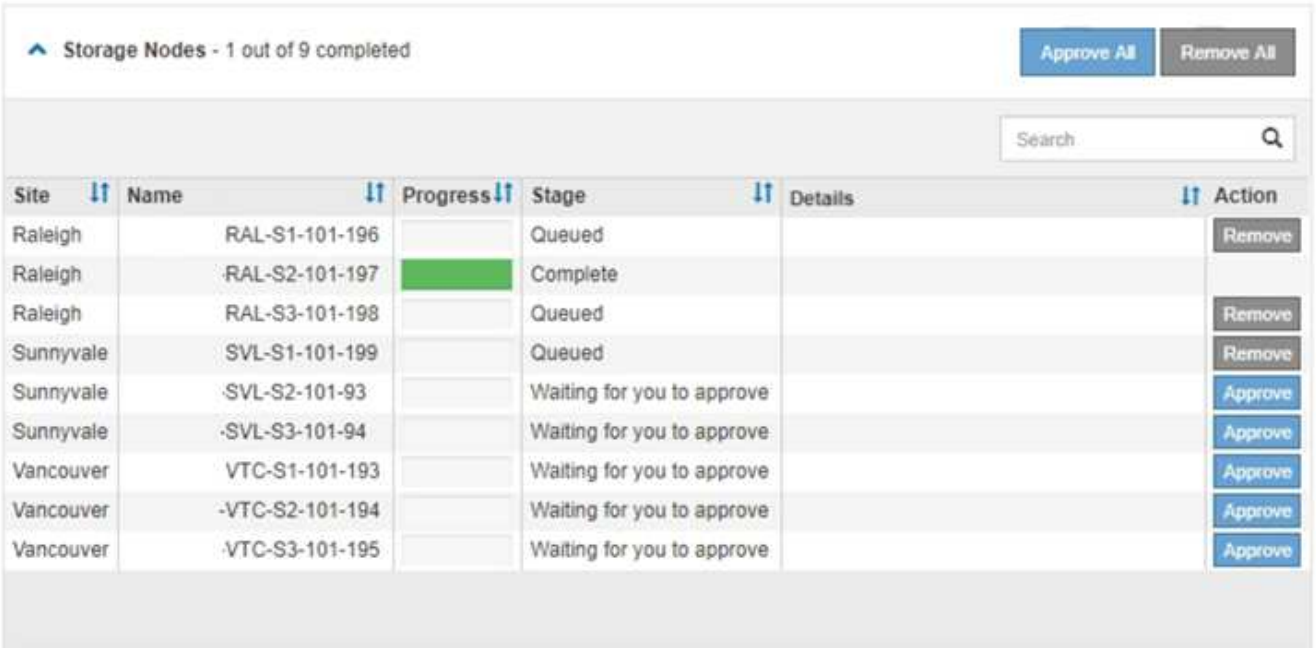
ノードによっては、選択したアップグレードファイルが意図的に適用されていないため、これらのノードをアップグレードせずにアップグレードプロセスを完了することができます。ノードが意図的にアップグレードされていない場合、プロセスの「Complete」ステージが表示され、「Details」列に次のいずれかのメッセージが表示されます：+

- ストレージノードはすでにアップグレードされています。
- このノードではSANtricity OSのアップグレードは実行できません。
- SANtricity OSファイルがこのノードに対応していません。

「SANtricity OS upgrade is not applicable to this node」というメッセージは、ノードにStorageGRID システムで管理可能なストレージ・コントローラがないことを示します。このメッセージは、非アプライアンスストレージノードに対して表示されます。このメッセージが表示されているノードをアップグレードせずに、SANtricity OSのアップグレードプロセスを完了できます。+「SANtricity OS file is not compatible with this node」というメッセージは、ノードに、インストールしようとしているプロセスとは異なるSANtricity OSファイルが必要であることを示しています。現在のSANtricity OSのアップグレードが完了したら、そのノードに適したSANtricity OSをダウンロードして、アップグレードプロセスを繰り返します。

11. SANtricity OSアップグレードキューからノードまたはすべてのノードを削除する必要がある場合は、* Remove または Remove All *をクリックします。

例に示すように、ステージがQueuedを超えて進むと、* Remove *ボタンが非表示になり、SANtricity OSアップグレード処理からノードを削除できなくなります。



12. 承認された各グリッドノードに SANtricity OS のアップグレードが適用されるまで待ちます。

> SANtricity OSのアップグレードの適用中にいずれかのノードでエラーステージが表示される場合、そのノードのアップグレードは失敗しています。障害からリカバリするために、アプライアンスをメンテナンスモードに切り替える必要がある場合があります。続行する前にテクニカルサポートにお問い合わせください。

ノード上のファームウェアが古すぎて Grid Manager でアップグレードできない場合、そのノードは Error をステージに表示します。 "` このノードで SANtricity OS をアップグレードするには、保守モードを使用する必要があります。使用しているアプライアンスのインストールとメンテナンスの手順を参照してください。アップグレード後は ' このユーティリティを将来のアップグレードに使用できます エラーを解決するには、次の手順を実行します。

a. メンテナンスモードを使用して、「エラー」のステージが表示されるノードの SANtricity OS をアップグレードします。

b. Grid Managerを使用してSANtricity OSのアップグレードを再開し、完了します。

   承認されたすべてのノードで SANtricity OS のアップグレードが完了すると、 SANtricity OS アップグレードの進捗状況テーブルが閉じ、緑のバナーに SANtricity OS のアップグレードが完了した日時が表示されます。

13. 別の SANtricity OS アップグレードファイルが必要な、完了段階のノードすべてについて、このアップグレード手順 を繰り返します。

> ステータスが「 Needs Attention 」のノードがある場合は、メンテナンスモードを使用してアップグレードを実行します。

関連情報

"E2700コントローラでのSANtricity OSのメンテナンスモードを使用したアップグレード"

**E2700**コントローラでの**SANtricity OS**のメンテナンスモードを使用したアップグレード

## グリッドマネージャを使用して SANtricity OS ソフトウェアをアップグレードできない場合は、メンテナンスモードの手順 を使用してアップグレードを適用します。

必要なもの

- NetApp Interoperability Matrix Tool （ IMT ）を参照して、アップグレードに使用する SANtricity OS のバージョンがお使いのアプライアンスと互換性があることを確認してください。

- グリッドマネージャを使用しない場合は、 E5600SG コントローラをメンテナンスモードにする必要があります。コントローラをメンテナンスモードにすると、 E2700 コントローラへの接続が中断されます。リンク設定を変更する前に、E5600SGコントローラをメンテナンスモードにする必要があります。StorageGRID アプライアンスをメンテナンスモードにすると、アプライアンスにリモートアクセスできなくなることがあります。

  "アプライアンスをメンテナンスモードにします"

このタスクについて

一度に複数の StorageGRID アプライアンスで E シリーズコントローラの SANtricity OS または NVSRAM をアップグレードしないでください。

> 一度に複数の StorageGRID アプライアンスをアップグレードすると、導入モデルや ILM ポリシーによっては、原因 データを使用できなくなる可能性があります。

手順

1. サービスラップトップから、 SANtricity ストレージマネージャにアクセスしてサインインします。
2. 新しい SANtricity OS ソフトウェアファイルと NVSRAM ファイルを管理クライアントにダウンロードします。

   > NVSRAM は、 StorageGRID アプライアンスに固有です。標準の NVSRAM ダウンロードを使用しないでください。

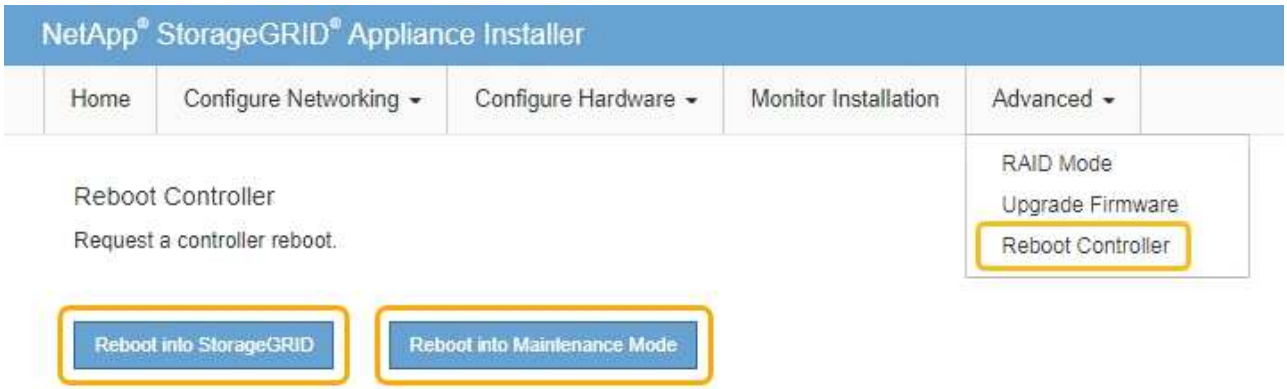
3. E2700 および E5600 SANtricity ソフトウェアとファームウェアのアップグレード手順 _ または SANtricity Storage Manager のオンラインヘルプに記載されている手順に従って、 E2700 コントローラのファームウェア、 NVSRAM 、またはその両方をアップグレードします。

   > E2700 コントローラの NVSRAM をアップグレードする必要がある場合は、ダウンロードした SANtricity OS ファイルが StorageGRID アプライアンスと互換性があると明記されていることを確認する必要があります。

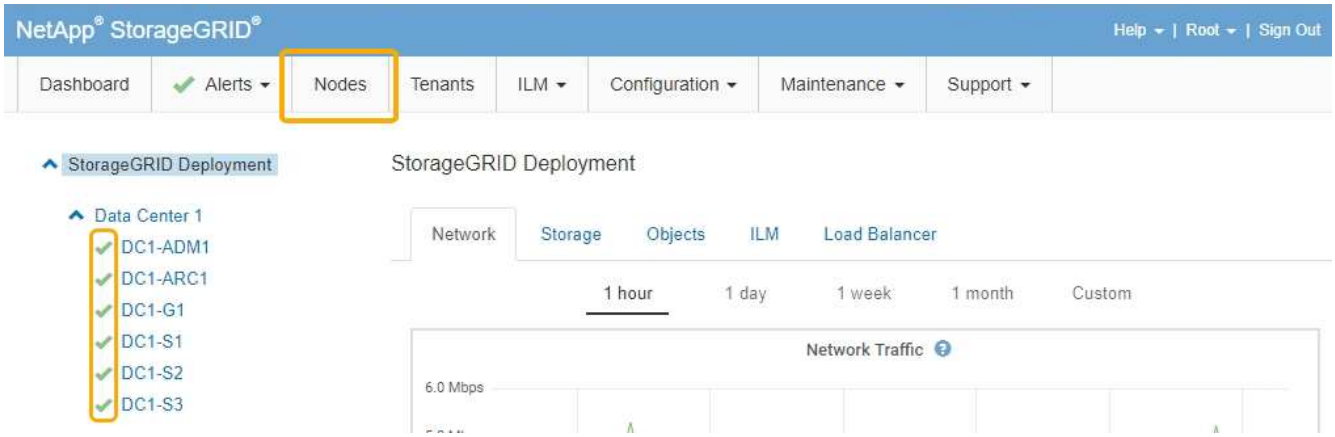
   > アップグレードファイルはただちにアクティブ化する必要があります。アクティブ化を先延ばしにしないでください。

4. アップグレード処理が完了したら、ノードをリブートします。StorageGRID アプライアンス・インストーラから、 **Advanced**>*Reboot Controller* を選択し、次のいずれかのオプションを選択します。

   - Reboot into StorageGRID * を選択し、ノードをグリッドに再追加してコントローラをリブートします。メンテナンスモードで作業を完了し、ノードを通常動作に戻す準備ができている場合は、このオプションを選択します。
   - メンテナンスモードを維持したままコントローラをリブートするには、 * Reboot into Maintenance Mode * を選択します。このオプションは、グリッドに再追加する前にノードで追加のメンテナンス処理を実行する必要がある場合に選択します。




アプライアンスがリブートしてグリッドに再参加するまでに最大 20 分かかることがあります。リブートが完了し、ノードが再びグリッドに参加したことを確認するには、 Grid Manager に戻ります。[ノード*（Nodes *）]タブには、通常のステータスが表示されます ✔ アクティブなアラートがなく、ノードがグリッドに接続されていることを示す、アプライアンスノードの場合。




**SANtricity Storage Manager**を使用してドライブファームウェアをアップグレードしています

## ドライブファームウェアをアップグレードして、最新の機能とバグ修正をすべて適用します。

必要なもの

- ストレージアプライアンスのステータスが「最適」であることを確認します。
- すべてのドライブのステータスが最適な状態である必要があります
- 最新バージョンの SANtricity Storage Manager がインストールされていて、 StorageGRID のバージョンと互換性があることを確認しておきます。

  "グリッドマネージャを使用してストレージコントローラのSANtricity OSをアップグレードします"

  "E2700コントローラでのSANtricity OSのメンテナンスモードを使用したアップグレード"

- StorageGRID アプライアンスをメンテナンスモードにしておきます。

  "アプライアンスをメンテナンスモードにします"

保守モードでは、ストレージコントローラへの接続が中断され、すべての I/O アクティビティが停止されて、すべてのドライブがオフラインになります。

一度に複数の StorageGRID アプライアンスでドライブファームウェアをアップグレードしないでください。お使いの導入モデルや ILM ポリシーによっては、原因 データを使用できなくなる場合があります。

手順

1. Webブラウザを開き、SANtricity Storage ManagerのURLにIPアドレスを入力します：+ `https://E2700_Controller_IP`
2. 必要に応じて、 SANtricity Storage Manager 管理者のユーザ名とパスワードを入力します。
3. SANtricity エンタープライズ管理で、 * デバイス * タブを選択します。

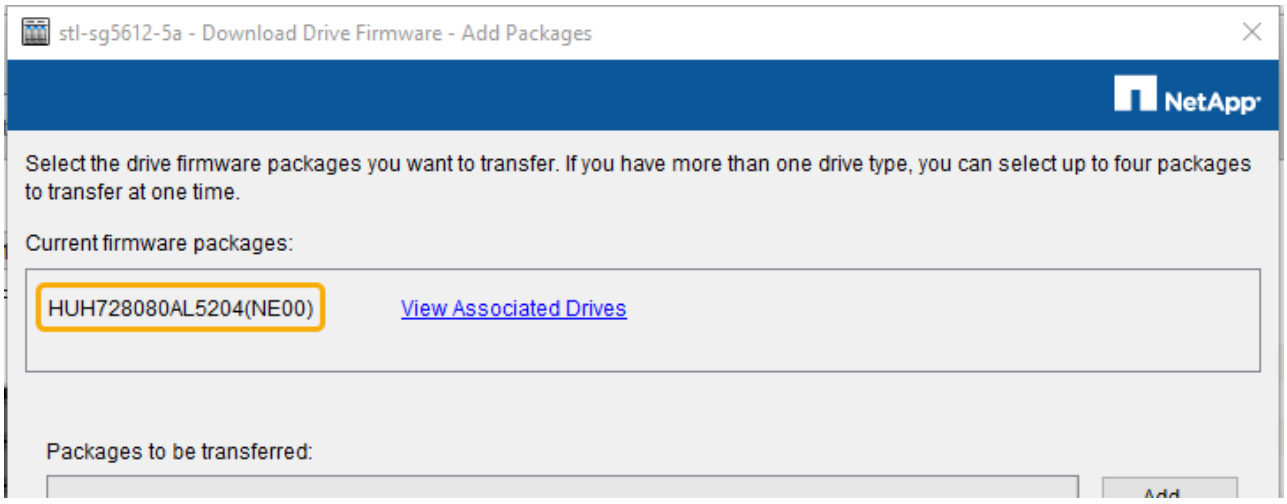
   SANtricity Array Management （アレイ管理）ウィンドウが開きます。

4. SANtricity アレイ管理で、アップグレードするドライブが格納されているストレージアレイをダブルクリックします。
5. ストレージアレイとドライブの両方のステータスが最適であることを確認します。
6. ストレージアプライアンスに現在インストールされているドライブファームウェアのバージョンを確認します。

   a. SANtricity Enterprise Management から、 * Upgrade * > * Drive Firmware * を選択します。

      Download Drive Firmware - Add Packages （ドライブファームウェアのダウンロード - パッケージの追加）ウィンドウに、現在使用中のドライブファームウェアファイルが表示されます。

   b. 現在のファームウェアパッケージに含まれているドライブファームウェアのリビジョンとドライブ ID をメモします。




   次の例では、

   - ドライブファームウェアのリビジョンは * NE00 * です。
   - ドライブ識別子は * HUH7280AL5204 * です。

View associated Drives * を選択して、ストレージアプライアンス内のドライブの位置を表示します。

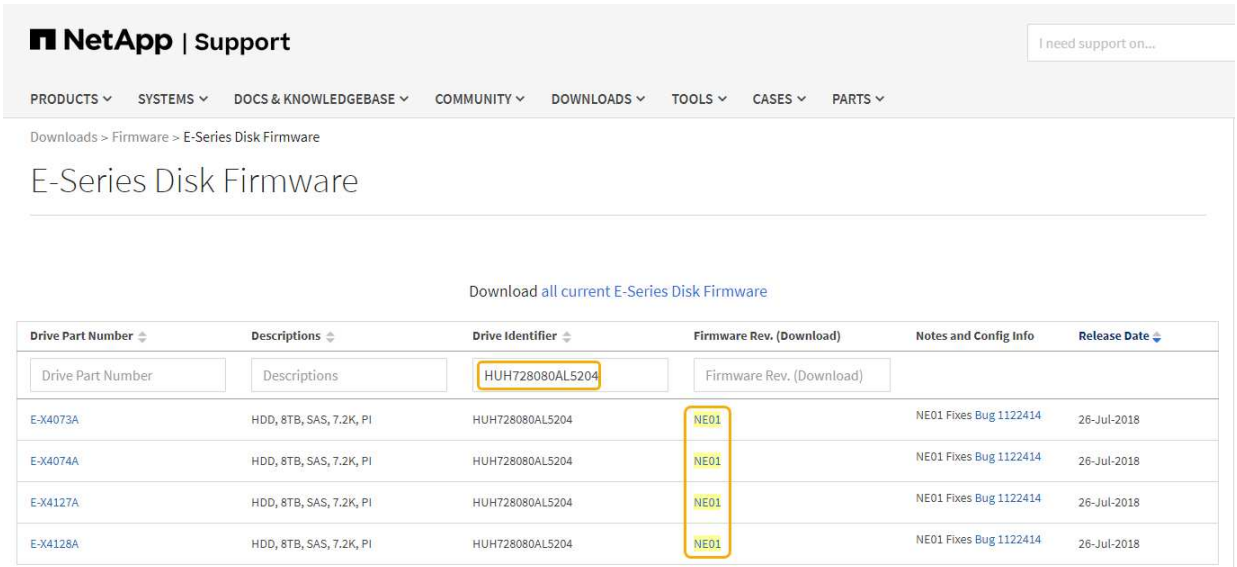
7. 使用可能なドライブファームウェアのアップグレードをダウンロードして準備します。
   a. Web ブラウザを開き、ネットアップサポート Web サイトにアクセスして、 ID とパスワードを使用してログインします。

      "ネットアップサポート"

   b. ネットアップサポート Web サイトで、「 * Downloads * 」タブを選択し、「 * E-Series Disk Drive Firmware * 」を選択します。

      E-Series Disk Firmware ページが表示されます。

   c. ストレージアプライアンスにインストールされているドライブ識別子 * をそれぞれ検索し、各ドライブ識別子に最新のファームウェアリビジョンが適用されていることを確認します。
      - ファームウェアリビジョンがリンクでない場合、このドライブ識別子には最新のファームウェアリビジョンが含まれます。
      - ドライブ識別子が記載されたドライブのパーツ番号が 1 つ以上であれば、それらのドライブでファームウェアのアップグレードを実行できます。任意のリンクを選択してファームウェアファイルをダウンロードできま
      す。




   d. 新しいファームウェアリビジョンがリストされている場合は、ファームウェアリビジョンのリンクを選択します（ダウンロード）列をクリックしてをダウンロードします `.zip` ファームウェアファイルを含むアーカイブ。

   e. サポートサイトからダウンロードしたドライブファームウェアのアーカイブファイルを展開（解凍）します。

8. ドライブファームウェアのアップグレードをインストールします。
   a. SANtricity ストレージ・マネージャの [ ドライブ・ファームウェアのダウンロード - パッケージの追加 ] ウィンドウで '[* 追加 ] を選択します

   b. ファームウェアファイルが保存されているディレクトリに移動し、最大 4 つのファームウェアファイルを選択します。

ドライブファームウェアファイルの名前は、+のようになります
`D_HUC101212CSS600_30602291_MS01_2800_0002.dlp`

複数のファームウェアファイルを選択して同じドライブのファームウェアをアップグレードすると、ファイルの競合エラーが発生することがあります。ファイルの競合エラーが発生した場合は、エラーダイアログが表示されます。このエラーを解決するには、 [OK] を選択し、ドライブのファームウェアのアップグレードに使用する以外のファームウェアファイルをすべて削除します。ファームウェアファイルを削除するには、転送するパッケージ情報領域でファームウェアファイルを選択し、 * 削除 * を選択します。また、一度に選択できるドライブファームウェアパッケージは最大 4 つです。

c. 「 * OK 」を選択します。

選択したファームウェアファイルで転送されるパッケージがアップデートされ、情報領域が更新されます。

d. 「 * 次へ * 」を選択します。

[Download Drive Firmware - Select Drives] ウィンドウが開きます。

- アプライアンス内のすべてのドライブで、設定情報とアップグレードの可否がスキャンされます。
- 選択したファームウェアでアップグレード可能な互換性があるドライブ（ストレージアレイのドライブの種類によって異なる）が表示されます。デフォルトでは、オンライン処理としてアップグレード可能なドライブが表示されます。
- ドライブに対して選択したファームウェアが、推奨されるファームウェア情報領域に表示されます。ファームウェアを変更する必要がある場合は、前のダイアログに戻るには、「 * 戻る」を選択します。

e. ドライブアップグレード機能から、 * パラレル * ダウンロード操作または * すべて * を選択します。

アプライアンスがメンテナンスモードになっていて、すべてのドライブとすべてのボリュームの I/O アクティビティが停止されているため、これらのアップグレード方式のいずれかを使用できます。

f. 互換性のあるドライブで、選択したファームウェアファイルをアップグレードするドライブを選択します。

- ドライブを 1 つ以上アップグレードする場合は、各ドライブを選択します。
- 互換性のあるすべてのドライブについて、 * すべて選択 * を選択します。

ベストプラクティスとして、同じモデルのドライブをすべて同じファームウェアリビジョンにアップグレードすることを推奨します。

g. 「完了」を選択し、と入力します `yes` 「 * OK 」を選択します。

- ドライブファームウェアのダウンロードとアップグレードが開始され、すべてのドライブのファームウェア転送のステータスが Download Drive Firmware - Progress で示されます。
- アップグレードに参加している各ドライブのステータスが、更新されたデバイスの転送の進行状況列に表示されます。

24 ドライブのシステムですべてのドライブがアップグレードされている場合は、ドライブファームウェアの並行アップグレード処理が完了するまでに最大 90 秒かかることがあります。大規模なシステムでは、実行時間が少し長くなります。

h. ファームウェアのアップグレードプロセスでは、 + を実行できます

- [* Stop] を選択して、進行中のファームウェアのアップグレードを停止します。実行中のファームウェアのアップグレードが完了します。ファームウェアアップグレードを試行したドライブには、それぞれのステータスが表示されます。残りのドライブのステータスが「 Not Attempted 」と表示されます。

> ドライブファームウェアのアップグレードプロセスを停止すると、データが失われたり、ドライブを使用できなくなったりする可能性があります。

- [ 名前を付けて保存 ] を選択して、ファームウェアアップグレードの進行状況の概要に関するテキストレポートを保存します。レポートは、デフォルトの .log ファイル拡張子で保存されます。ファイル拡張子またはディレクトリを変更する場合は、 [Save Drive Download Log] でパラメータを変更します。

i. ドライブファームウェアのダウンロード - 進捗状況を監視します。ドライブの更新領域には、ファームウェアのアップグレードが予定されているドライブのリストと、各ドライブのダウンロードおよびアップグレードの転送ステータスが表示されます。

アップグレードに参加している各ドライブの進捗状況とステータスが Transfer Progress 列に表示されます。アップグレード中にエラーが発生した場合は、推奨される対処方法を実行します。

- * 保留中 *

  スケジュールされているがまだ開始されていないオンラインファームウェアダウンロード処理の場合は、このステータスが表示されます。

- * 実行中 *

  ファームウェアをドライブに転送しています。

- * 再構成を実行中 *

  このステータスは、ドライブの高速再構築中にボリューム転送が実行された場合に表示されます。コントローラのリセットまたは障害が原因で、コントローラ所有者がボリュームを転送している場合が一般的です。

ドライブの完全な再構築が開始されます。

◦ * 失敗 - 一部 *

問題が発生して残りのファイルを転送できなくなるまで、ファームウェアはドライブに一部だけ転送されました。

◦ * 失敗 - 無効な状態 *

ファームウェアが無効です。

◦ * 失敗 - その他 *

ドライブの物理的な問題が原因で、ファームウェアをダウンロードできませんでした。

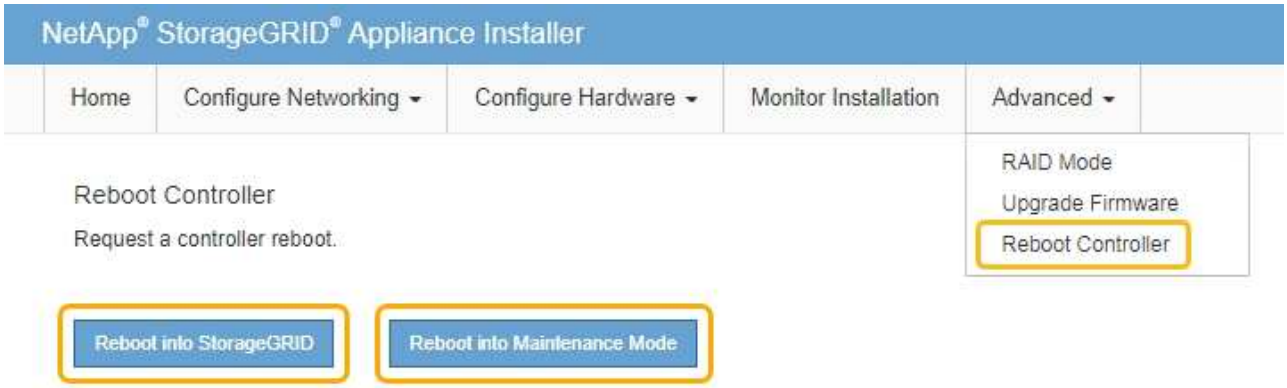
◦ * 未試行 *

ファームウェアがダウンロードされませんでした。ダウンロードが停止してからアップグレードを実行できなかった、ドライブがアップグレードの対象にならなかった、エラーが原因でダウンロードができなかったなどのさまざまな理由が原因である可能性があります。

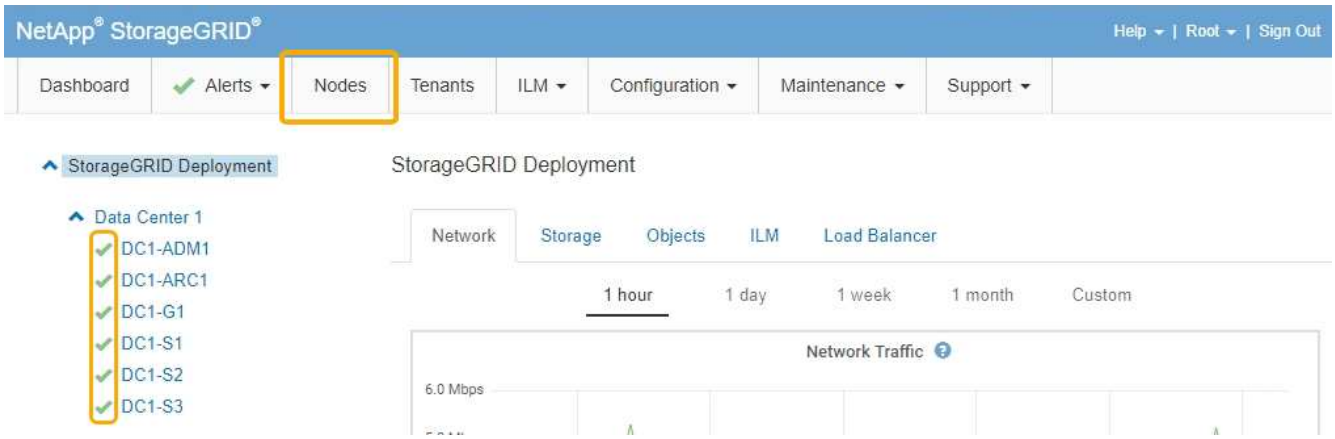
- * 成功 *

  ファームウェアが正常にダウンロードされました。

9. ドライブファームウェアのアップグレードが完了したら、次の手順を実行
   - ドライブファームウェアダウンロードウィザードを閉じるには、 * 閉じる * を選択します。
   - ウィザードを再開するには、 * 転送詳細 * を選択します。
10. アップグレード処理が完了したら、アプライアンスをリブートします。StorageGRID アプライアンス・インストーラから、 **Advanced**>*Reboot Controller* を選択し、次のいずれかのオプションを選択します。
    - Reboot into StorageGRID * を選択し、ノードをグリッドに再追加してコントローラをリブートします。メンテナンスモードで作業を完了し、ノードを通常動作に戻す準備ができている場合は、このオプションを選択します。
    - メンテナンスモードを維持したままコントローラをリブートするには、 * Reboot into Maintenance Mode * を選択します。このオプションは、グリッドに再追加する前にノードで追加のメンテナンス処理を実行する必要がある場合に選択しま
      す。




アプライアンスがリブートしてグリッドに再参加するまでに最大 20 分かかることがあります。リブートが完了し、ノードが再びグリッドに参加したことを確認するには、 Grid Manager に戻ります。[ノード*（Nodes *）]タブには、通常のステータスが表示されます ✔ アクティブなアラートがなく、ノードがグリッドに接続されていることを示す、アプライアンスノードの場合。




**E2700**コントローラの交換

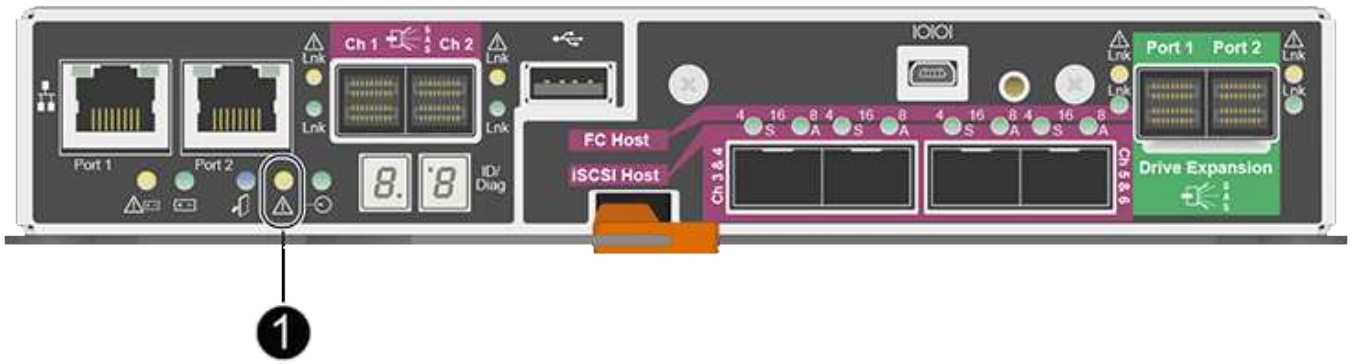
## E2700 コントローラが適切に機能しない場合や障害が発生した場合は、交換が必要となることがあります。

必要なもの

- 交換するコントローラと同じパーツ番号の交換用コントローラを用意しておきます。
- コントローラに接続する各ケーブルを識別するためのラベルを用意しておきます。
- 静電気防止処置が必要です。
- Maintenance または Root Access 権限が必要です。詳細については、 StorageGRID の管理手順を参照してください。

このタスクについて

コントローラの保守操作要を示す黄色の LED （図中の 1 ）を見ると、コントローラに障害が発生したかどうかを確認できます。この LED が点灯している場合は、コントローラを交換する必要があります。




コントローラを交換すると、アプライアンスストレージノードにアクセスできなくなります。E2700 コントローラが動作している場合は、 E5600SG コントローラをメンテナンスモードにすることができます。

コントローラを交換するときは、元のコントローラからバッテリを取り外し、交換用コントローラに取り付ける必要があります。

手順

1. コントローラを取り外す準備をします。

   これらの手順を実行するには、 SANtricity Storage Manager を使用します。

   a. コントローラに現在インストールされている SANtricity OS ソフトウェアのバージョンを書き留めます。

   b. 現在インストールされている NVSRAM のバージョンを書き留めます。

   c. ドライブセキュリティ機能が有効になっている場合は、保存されたキーが存在すること、およびそのインストールに必要なパスフレーズを確認しておきます。

      * データ・アクセスが失われる可能性 - * アプライアンスのすべてのドライブでセキュリティが有効になっている場合、 SANtricity ストレージ・マネージャの [ エンタープライズ管理 ] ウィンドウを使用してセキュリティ保護されたドライブのロックを解除するまで、新しいコントローラはアプライアンスにアクセスできません。

   d. 構成データベースをバックアップします。

      コントローラを取り外すときに問題が発生した場合は、保存したファイルを使用して構成をリストアできます。

   e. アプライアンスのサポートデータを収集します。

      コンポーネントを交換する前後にサポートデータを収集しておけば、交換しても問題が解決しない場合に、テクニカルサポートにすべてのログを送信できます。

2. StorageGRID アプライアンスをStorageGRID システムで実行中の場合は、E5600SGコントローラをメンテナンスモードにします。

   "アプライアンスをメンテナンスモードにします"

3. E2700 コントローラが動作していて通常の方法でシャットダウンできる場合は、すべての処理が完了していることを確認します。

   a. Array Management Window のタイトルバーから、 **Monitor**>*Reports*>*Operations In Progress * を選択します。

   b. すべての処理が完了したことを確認します。

4. シンプレックス E2700 コントローラの交換用手順 に記載されている手順に従って、次の手順を実行します。

   a. ケーブルにラベルを付け、ケーブルを外します。

      パフォーマンスの低下を防ぐために、ケーブルをねじったり、折り曲げたり、はさんだり、踏みつけたりしないでください。

   b. 障害が発生したコントローラをアプライアンスから取り外します。

   c. コントローラのカバーを取り外します。

   d. 取り付けネジを外して、障害が発生したコントローラからバッテリを取り外します。

   e. 交換用コントローラにバッテリを取り付け、コントローラカバーを元の位置に戻します。

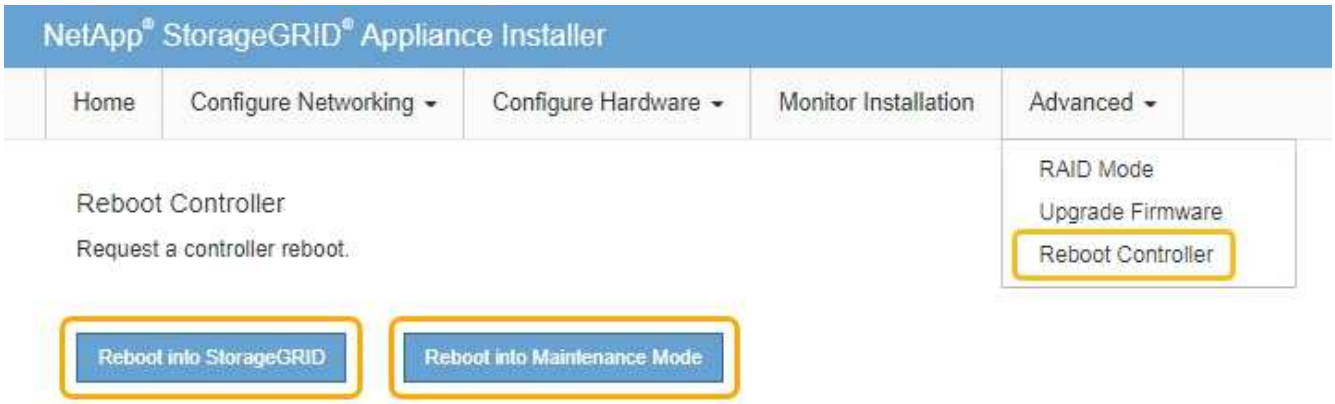
f. 交換用コントローラをアプライアンスに取り付けます。

g. ケーブルを交換します。

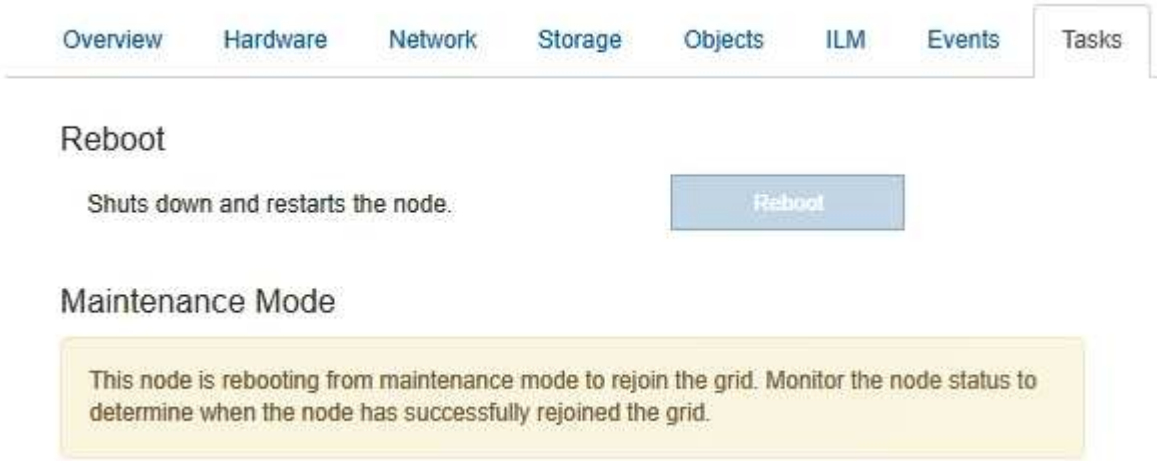
h. E2700 コントローラがリブートするまで待ちます。デジタル表示ディスプレイの状態がになっていることを確認します `99`。

5. アプライアンスでセキュリティ保護されたドライブを使用する場合は、ドライブのセキュリティキーをインポートします。

6. アプライアンスを通常の動作モードに戻します。StorageGRID アプライアンス・インストーラから、**Advanced**>* Reboot Controller* を選択し、 * Reboot into StorageGRID * を選択します。

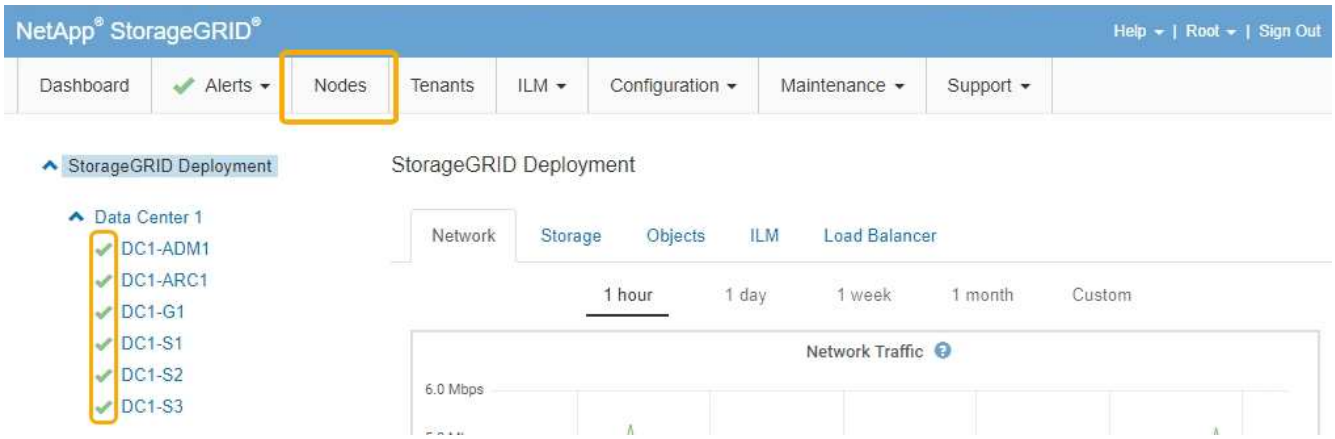



リブート中、次の画面が表示されます。




アプライアンスがリブートし、グリッドに再度参加します。この処理には最大 20 分かかることがあります。

7. リブートが完了し、ノードが再びグリッドに参加したことを確認します。Grid Managerで、* Nodes *タブに正常なステータスが表示されることを確認します ✔ アクティブなアラートがなく、ノードがグリッドに接続されていることを示す、アプライアンスノードの場合。




8. SANtricity Storage Manager で、新しいコントローラのステータスが「 Optimal 」であることを確認し、サポートデータを収集します。

関連情報

"NetApp E シリーズおよび EF シリーズでのハードウェアの交換手順"

"ネットアップのマニュアル： E2700 シリーズ"

**E5600SG**コントローラの交換

## E5600SG コントローラの交換が必要となる場合があります。

必要なもの

次のリソースにアクセスできる必要があります。

- NetApp Support Site at + に掲載のE シリーズハードウェアの交換に関する情報http://mysupport.netapp.com/["mysupport.netapp.com"^]
- E5600 に関するサポートサイトのドキュメント
- アプライアンスのメンテナンスモードが開始されました。

  "アプライアンスをメンテナンスモードにします"

このタスクについて

両方のコントローラが動作していて通常の方法でシャットダウンできる場合は、まず E5600SG コントローラをシャットダウンして E2700 コントローラへの接続を中断できます。

> StorageGRID ソフトウェアをインストールする前にコントローラを交換すると、この手順 の完了後すぐに StorageGRID アプライアンスインストーラにアクセスできない場合があります。アプライアンスと同じサブネット上の他のホストから StorageGRID アプライアンスインストーラにアクセスすることはできますが、他のサブネット上のホストからはアクセスできません。この状態は 15 分以内に（元のコントローラのいずれかの ARP キャッシュエントリがタイムアウトした時点で）自動的に解消されます。あるいは、古い ARP キャッシュエントリをローカルルータまたはゲートウェイから手動でパージすれば、すぐにこの状態を解消できます。

手順

1. 静電気防止処置を施します。

2. 再接続するときにわかるように、 E5600SG コントローラに接続されている各ケーブルにラベルを付けます。

> パフォーマンスの低下を防ぐために、ケーブルをねじったり、折り曲げたり、はさんだり、踏みつけたりしないでください。ケーブルを曲げないでください。半径が 5cm 以上になるようにしてください。

3. アプライアンスがメンテナンスモードになったら、 E5600SG コントローラをシャットダウンします。
   a. グリッドノードにログインします。
      i. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
      ii. に記載されているパスワードを入力します `Passwords.txt` ファイル。
      iii. 次のコマンドを入力してrootに切り替えます。 `su -`
      iv. に記載されているパスワードを入力します `Passwords.txt` ファイル。

      rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

   b. E5600SGコントローラをシャットダウンします。+
      **`shutdown -h now`**
4. エンクロージャの電源をオフにし、コントローラの背面にあるすべての LED とデジタル表示ディスプレイの動作が停止するまで待ちます。
5. ケーブルを取り外します。
6. E5600SG コントローラのドキュメントの説明に従って、コントローラを取り外します。
7. E5600SG コントローラのドキュメントの説明に従って、新しいコントローラを挿入します。
8. すべてのケーブルを交換します。
9. エンクロージャの電源を再度オンにします。
10. デジタル表示のコードを監視します。
    - E2700 コントローラ：

      最後のLEDの状態はです `99`。

    - E5600SG コントローラ：

      最後のLEDの状態はです `HA`。

11. Grid Manager で、アプライアンスストレージノードのステータスを監視します。

    アプライアンスストレージノードが想定されるステータスに戻ったことを確認します。

関連情報

"NetApp E シリーズおよび EF シリーズでのハードウェアの交換手順"

"ネットアップのマニュアル： E5600 シリーズ"

# StorageGRID アプライアンスのドライブ、ファン、電源装置、またはバッテリの交換が必要になることがあります。

必要なもの

- E シリーズハードウェアの交換用手順 を用意しておきます。
- コンポーネントの交換用手順 でアプライアンスをシャットダウンする必要がある場合は、アプライアンスをメンテナンスモードにしておきます。

  "アプライアンスをメンテナンスモードにします"

このタスクについて

ドライブ、電源 / ファンキャニスター、ファンキャニスター、電源キャニスター、バッテリを交換する方法またはドライブドロワーについては、 E2700 および E5600 ストレージアレイでの標準的な手順を参照してください。ハードウェア自体の取り外しや交換についてのステップバイステップの手順をよくお読みください。SANtricity Storage Manager の手順の多くは、アプライアンスには当てはまりません。

**SG5612** コンポーネントの交換手順

| **FRU** | を参照してください |
|---|---|
| ドライブ | E2600 、 E2700 、 E5400 、 E5500 、 E5600 、 12 ドライブまたは 24 ドライブトレイのドライブを交換する場合は、 E シリーズの手順に従ってください。 |
| 電源 / ファンキャニスター | E シリーズの手順に従い、 E5612 または E5624 コントローラドライブトレイの電源 / ファンキャニスターで障害が発生した場合は交換します |
| E2700 コントローラのバッテリ（コントローラの取り外しが必要） | の手順に従います "E2700コントローラの交換"をクリックします。ただし、既存のコントローラに新しいバッテリを取り付けます。 |

**SG5660** コンポーネントの交換手順

| **FRU** | を参照してください |
|---|---|
| ドライブ | E シリーズの手順に従って、 E2660 、 E2760 、 E5460 、 E5560 、または E5660 トレイのドライブを交換します。 |
| 電源キャニスター | E シリーズの手順に従って、 E5660 コントローラドライブトレイの電源キャニスターに障害が発生した場合の交換を行ってください |

| FRU | を参照してください |
| --- | --- |
| ファンキャニスター | E シリーズの手順に従って、 E5660 コントローラドライブトレイのファンキャニスターで障害が発生した場合の交換を行ってください |
| E2700 コントローラのバッテリ（コントローラの取り外しが必要） | の手順に従います "E2700コントローラの交換"をクリックします。ただし、既存のコントローラに新しいバッテリを取り付けます。 |

関連情報

"NetApp E シリーズおよび EF シリーズでのハードウェアの交換手順"

"ネットアップのマニュアル： E2700 シリーズ"

"ネットアップのマニュアル： E5600 シリーズ"

**E5600SG**コントローラのリンク設定の変更

## E5600SG コントローラのイーサネットリンク設定を変更できます。ポートボンディングモード、ネットワークボンディングモード、およびリンク速度を変更できます。

必要なもの

- E5600SGコントローラをメンテナンスモードにする必要があります。コントローラをメンテナンスモードにすると、 E2700 コントローラへの接続が中断されます。StorageGRID アプライアンスをメンテナンスモードにすると、アプライアンスにリモートアクセスできなくなることがあります。

  "アプライアンスをメンテナンスモードにします"

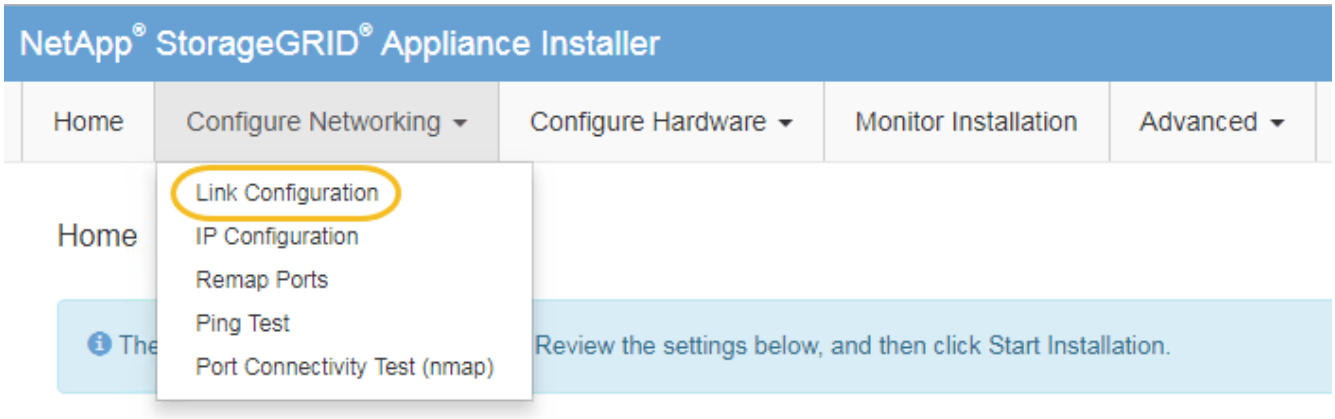
このタスクについて

E5600SG コントローラのイーサネットリンク設定を変更するオプションは次のとおりです。

- ポートボンディングモード * を「 Fixed 」から「 Aggregate 」または「 Aggregate 」から「 Fixed 」に変更します
- ネットワークボンディングモード * を Active-Backup から LACP に、または LACP から Active-Backup に変更
- VLAN タグを有効または無効にするか、 VLAN タグの値を変更します
- リンク速度を 10GbE から 25GbE に、または 25GbE から 10GbE に変更する

手順

1. メニューから * Configure Networking * > * Link Configuration * を選択します。




1. リンク設定に必要な変更を加えます。

   オプションの詳細については、「ネットワークリンクの設定」を参照してください。

2. 選択に問題がなければ、 * 保存 * をクリックします。

   > 接続しているネットワークまたはリンクを変更すると、接続が失われる可能性があります。1分以内に再接続されない場合は、アプライアンスに割り当てられている他のIPアドレスのいずれかを使用してStorageGRID アプライアンスインストーラのURLを再入力します：+
   > **`https://E5600SG_Controller_IP:8443`**

   VLAN 設定を変更した場合は、アプライアンスのサブネットが変更されている可能性があります。アプライアンスのIPアドレスを変更する必要がある場合は、IPアドレスの設定手順に従います。

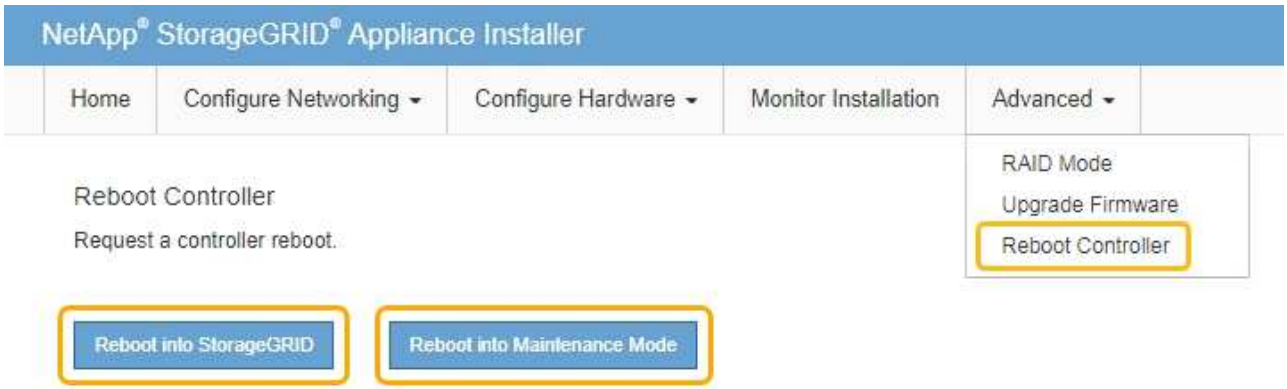
   "IPの設定"

3. StorageGRID アプライアンスインストーラから、 **Configure Networking**>*Ping Test* を選択します。
4. Ping Test ツールを使用して、で行ったリンク設定の変更によって影響を受けた可能性のあるネットワーク上の IP アドレスへの接続を確認します リンク設定を変更します ステップ。

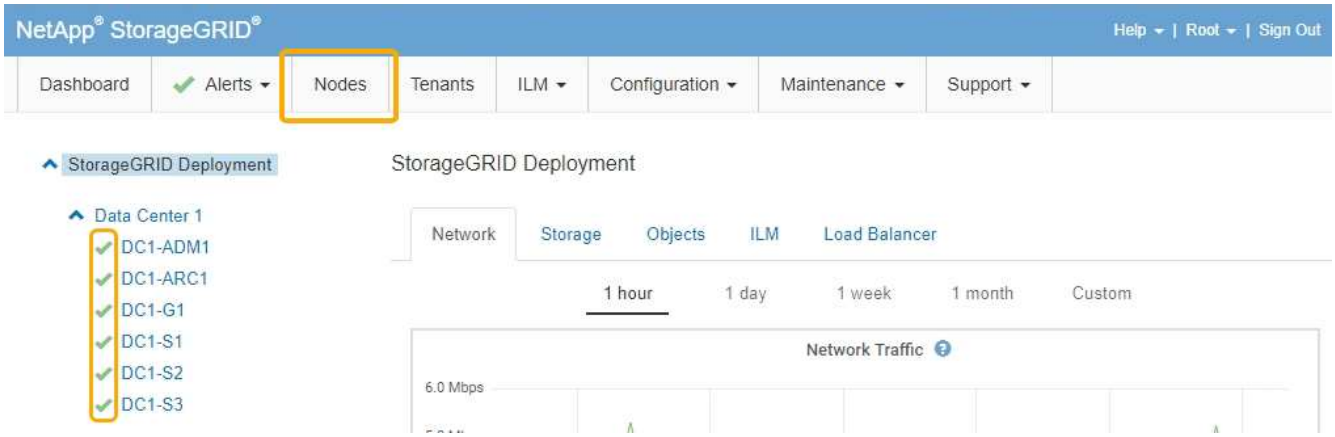
   最低でもプライマリ管理ノードのグリッド IP アドレスと、 1 つ以上の他のストレージノードのグリッド IP アドレスについて、 ping が通ることを確認します。必要に応じて、リンク設定の問題を修正します。

5. リンク設定の変更が問題なく機能していることを確認したら、ノードをリブートします。StorageGRID アプライアンス・インストーラから、 **Advanced**>*Reboot Controller* を選択し、次のいずれかのオプションを選択します。

   - Reboot into StorageGRID * を選択し、ノードをグリッドに再追加してコントローラをリブートします。メンテナンスモードで作業を完了し、ノードを通常動作に戻す準備ができている場合は、このオプションを選択します。
   - メンテナンスモードを維持したままコントローラをリブートするには、 * Reboot into Maintenance Mode * を選択します。このオプションは、グリッドに再追加する前にノードで追加のメンテナンス処理を実行する必要がある場合に選択しま
     す。




アプライアンスがリブートしてグリッドに再参加するまでに最大 20 分かかることがあります。リブートが完了し、ノードが再びグリッドに参加したことを確認するには、 Grid Manager に戻ります。[ノード*（Nodes *）]タブには、通常のステータスが表示されます ✔ アクティブなアラートがなく、ノードがグリッドに接続されていることを示す、アプライアンスノードの場合。




関連情報

"ネットワークリンクの設定（SG5600）"

**MTU**設定を変更します

アプライアンスノードの IP アドレスを設定するときに割り当てた MTU 設定を変更できます。

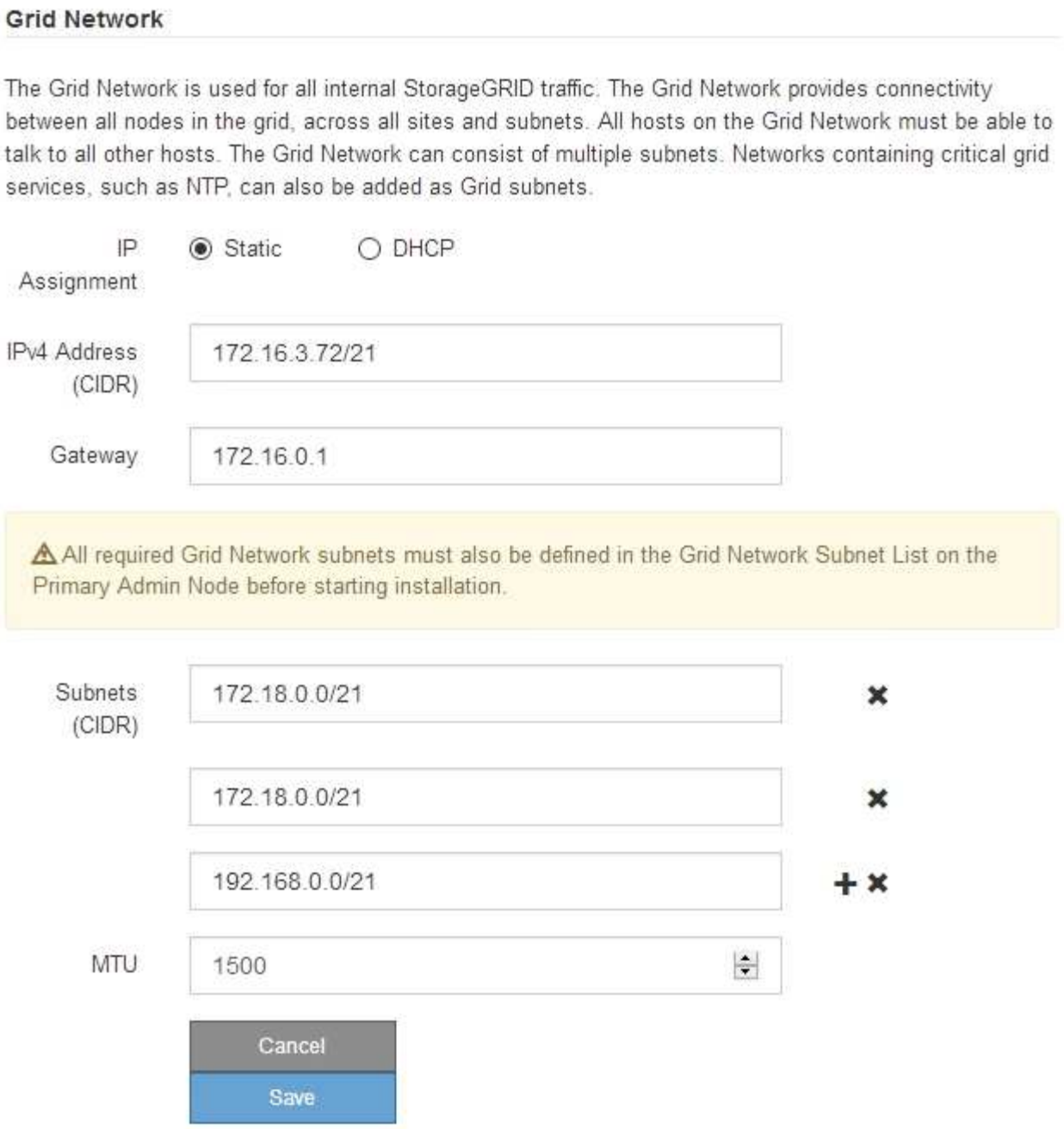
必要なもの

アプライアンスのメンテナンスモードが開始されました。

"アプライアンスをメンテナンスモードにします"

手順

1. StorageGRID アプライアンスインストーラから、 **Configure Networking**>*IP Configuration* を選択します。
2. グリッドネットワーク、管理ネットワーク、およびクライアントネットワークの MTU 設定に必要な変更を加えます。



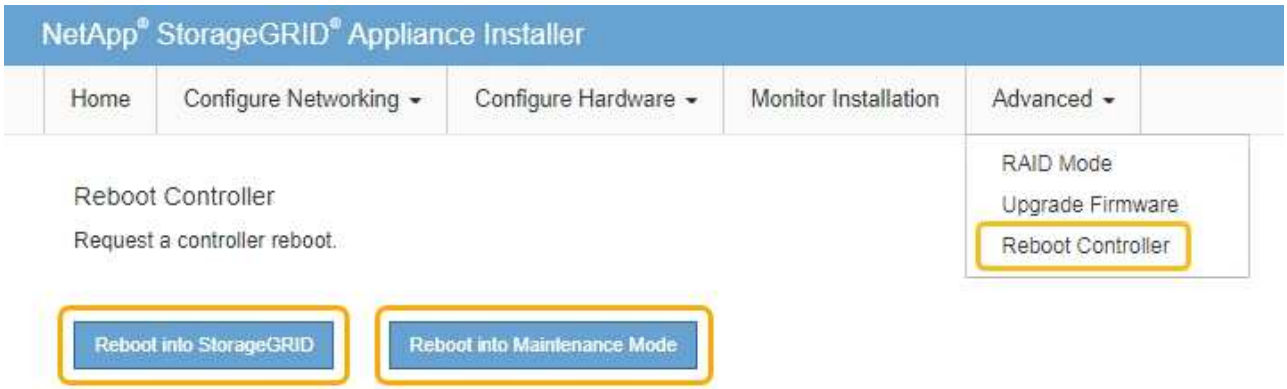

ネットワークの MTU 値は、ノードが接続されているスイッチポートに設定されている値と同じである必要があります。そうしないと、ネットワークパフォーマンスの問題やパケット損失が発生する可能性があります。

ネットワークのパフォーマンスを最大限に高めるには、すべてのノードのグリッドネットワークインターフェイスで MTU 値がほぼ同じになるように設定する必要があります。個々のノードのグリッドネットワークの MTU 設定に大きな違いがある場合は、 * Grid Network MTU mismatch * アラートがトリガーされます。MTU 値はすべてのネットワークタイプで同じである必要はありません。

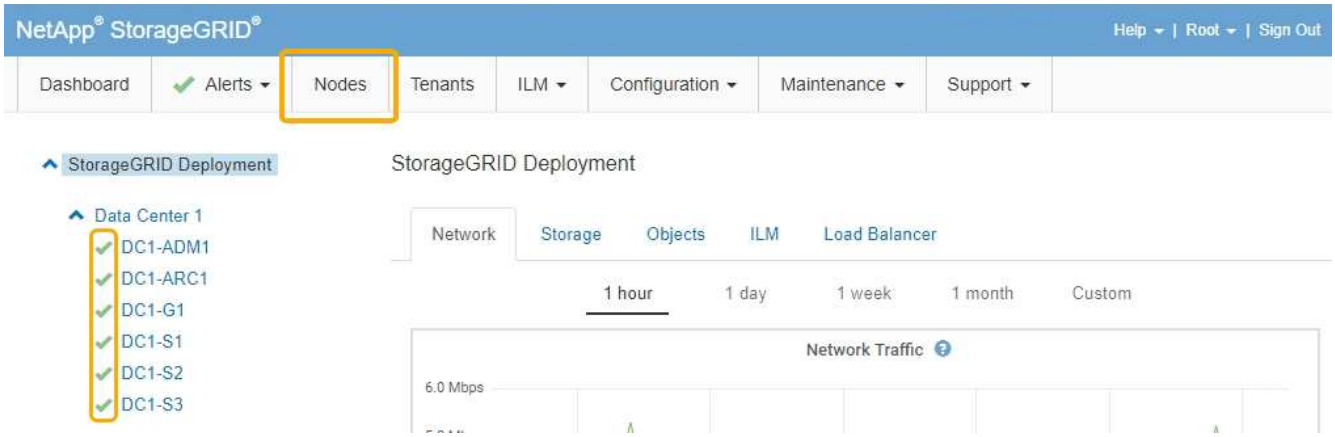
3. 設定に問題がなければ、「 * 保存 * 」を選択します。
4. ノードをリブートします。StorageGRID アプライアンス・インストーラから、 **Advanced**>*Reboot

Controller* を選択し、次のいずれかのオプションを選択します。

- Reboot into StorageGRID * を選択し、ノードをグリッドに再追加してコントローラをリブートします。メンテナンスモードで作業を完了し、ノードを通常動作に戻す準備ができている場合は、このオプションを選択します。
- メンテナンスモードを維持したままコントローラをリブートするには、 * Reboot into Maintenance Mode * を選択します。このオプションは、グリッドに再追加する前にノードで追加のメンテナンス処理を実行する必要がある場合に選択しま
す。




アプライアンスがリブートしてグリッドに再参加するまでに最大 20 分かかることがあります。リブートが完了し、ノードが再びグリッドに参加したことを確認するには、 Grid Manager に戻ります。[ノード*（Nodes *）]タブには、通常のステータスが表示されます ✔ アクティブなアラートがなく、ノードがグリッドに接続されていることを示す、アプライアンスノードの場合。




関連情報

"StorageGRID の管理"

**DNS**サーバの設定を確認しています

このアプライアンスノードで現在使用されているドメインネームシステム（ DNS ）サーバを確認し、一時的に変更することができます。

必要なもの

アプライアンスのメンテナンスモードが開始されました。

"アプライアンスをメンテナンスモードにします"

このタスクについて

KMS のホスト名は IP アドレスではなくドメイン名として指定されているため、暗号化されたアプライアンスがキー管理サーバ（ KMS ）または KMS クラスタに接続できない場合は、 DNS サーバ設定の変更が必要になることがあります。アプライアンスの DNS 設定に加えた変更は一時的なものであり、メンテナンスモードを終了すると失われます。これらの変更を永続的に行うには、Grid ManagerでDNSサーバを指定します（* Maintenance > Network > DNS Servers *）。

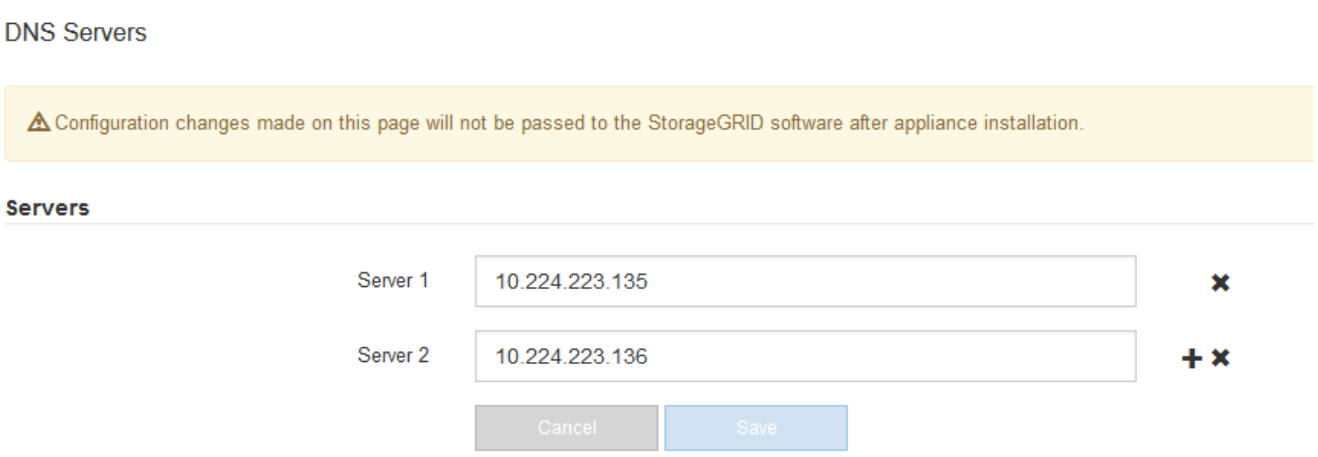
- DNS 設定の一時的な変更が必要になるのは、ホスト名に IP アドレスではなく完全修飾ドメイン名を使用して KMS サーバが定義されているノード暗号化アプライアンスのみです。
- ノード暗号化アプライアンスをドメイン名を使用して KMS に接続する場合は、グリッド用に定義されている DNS サーバの 1 つに接続する必要があります。これらの DNS サーバの 1 つが、ドメイン名を IP アドレスに変換します。
- ノードがグリッドの DNS サーバにアクセスできない場合、またはノード暗号化アプライアンスノードがオフラインのときにグリッド全体の DNS 設定を変更した場合は、ノードは KMS に接続できません。アプライアンス上の暗号化されたデータは、 DNS 問題 が解決されるまで復号化できません。

KMS 接続を回避する DNS 問題 を解決するには、 StorageGRID アプライアンスインストーラで 1 つ以上の DNS サーバの IP アドレスを指定します。この一時的な DNS 設定により、アプライアンスは KMS に接続してノード上のデータを復号化することができます。

たとえば、暗号化されたノードがオフラインのときにグリッドの DNS サーバが変更された場合、ノードは以前の DNS 値をまだ使用しているため、オンラインに戻った時点で KMS にアクセスできなくなります。StorageGRID アプライアンスインストーラで新しい DNS サーバの IP アドレスを入力すると、 KMS 接続を使用してノードのデータを復号化できます。

手順

1. StorageGRID アプライアンスインストーラから、 **Configure Networking *>*DNS Configuration** を選択します。
2. 指定した DNS サーバが正しいことを確認してください。




3. 必要に応じて、 DNS サーバを変更します。

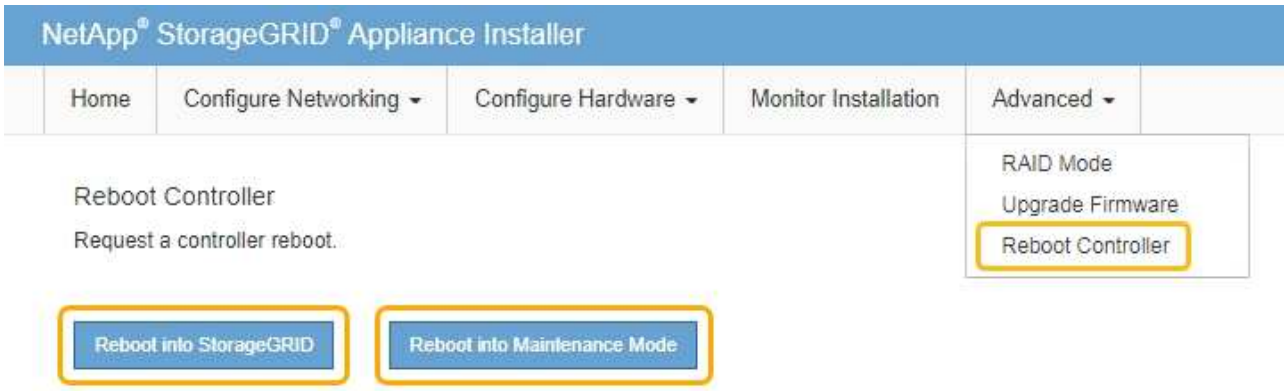
DNS 設定に対する変更は一時的なものであり、メンテナンスモードを終了すると失われます。

4. 一時的な DNS 設定に問題がなければ、 * 保存 * を選択します。

   ノードは、このページで指定されている DNS サーバ設定を使用して KMS に再接続し、ノード上のデータを復号化できるようにします。

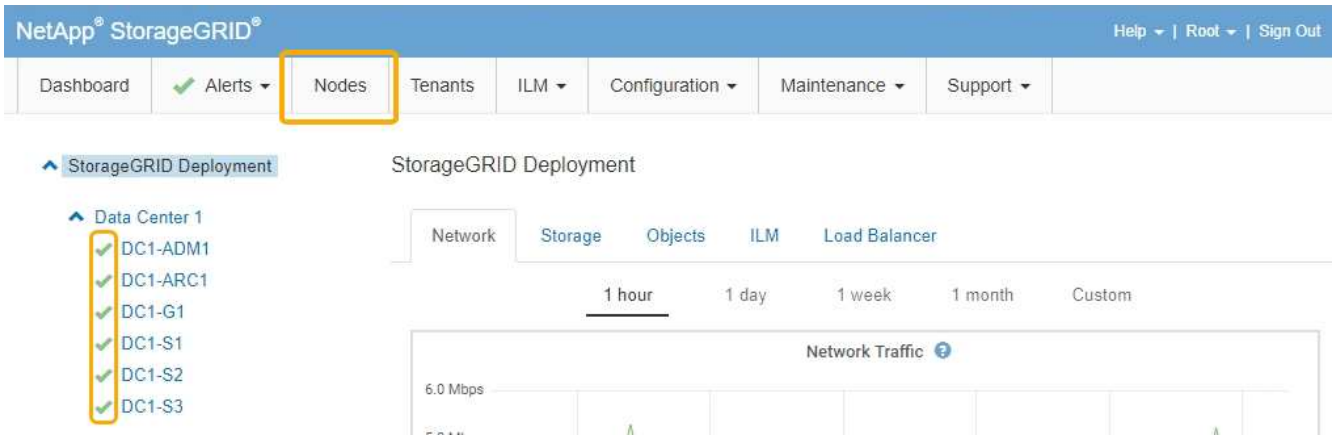
5. ノードデータが復号化されたら、ノードをリブートします。StorageGRID アプライアンス・インストーラから、 **Advanced**>*Reboot Controller* を選択し、次のいずれかのオプションを選択します。

   - Reboot into StorageGRID * を選択し、ノードをグリッドに再追加してコントローラをリブートします。メンテナンスモードで作業を完了し、ノードを通常動作に戻す準備ができている場合は、このオプションを選択します。
   - メンテナンスモードを維持したままコントローラをリブートするには、 * Reboot into Maintenance Mode * を選択します。このオプションは、グリッドに再追加する前にノードで追加のメンテナンス処理を実行する必要がある場合に選択します。




ノードがリブートしてグリッドに再び参加すると、 Grid Manager にリストされているシステム全体の DNS サーバが使用されます。グリッドに再追加したあとは、アプライアンスがメンテナンスモードのときに、 StorageGRID アプライアンスインストーラで指定された一時的な DNS サーバがアプライアンスで使用されなくなります。

アプライアンスがリブートしてグリッドに再参加するまでに最大 20 分かかることがあります。リブートが完了し、ノードが再びグリッドに参加したことを確認するには、 Grid Manager に戻ります。[ノード*（Nodes *）]タブには、通常のステータスが表示されます アクティブなアラートがなく、ノードがグリッドに接続されていることを示す、アプライアンスノードの場合。




メンテナンスモードでのノード暗号化の監視

# インストール中にアプライアンスのノード暗号化を有効にした場合は、ノード暗号化の状態やキー管理サーバ（ KMS ）の詳細など、各アプライアンスノードのノード暗号化ステータスを監視できます。

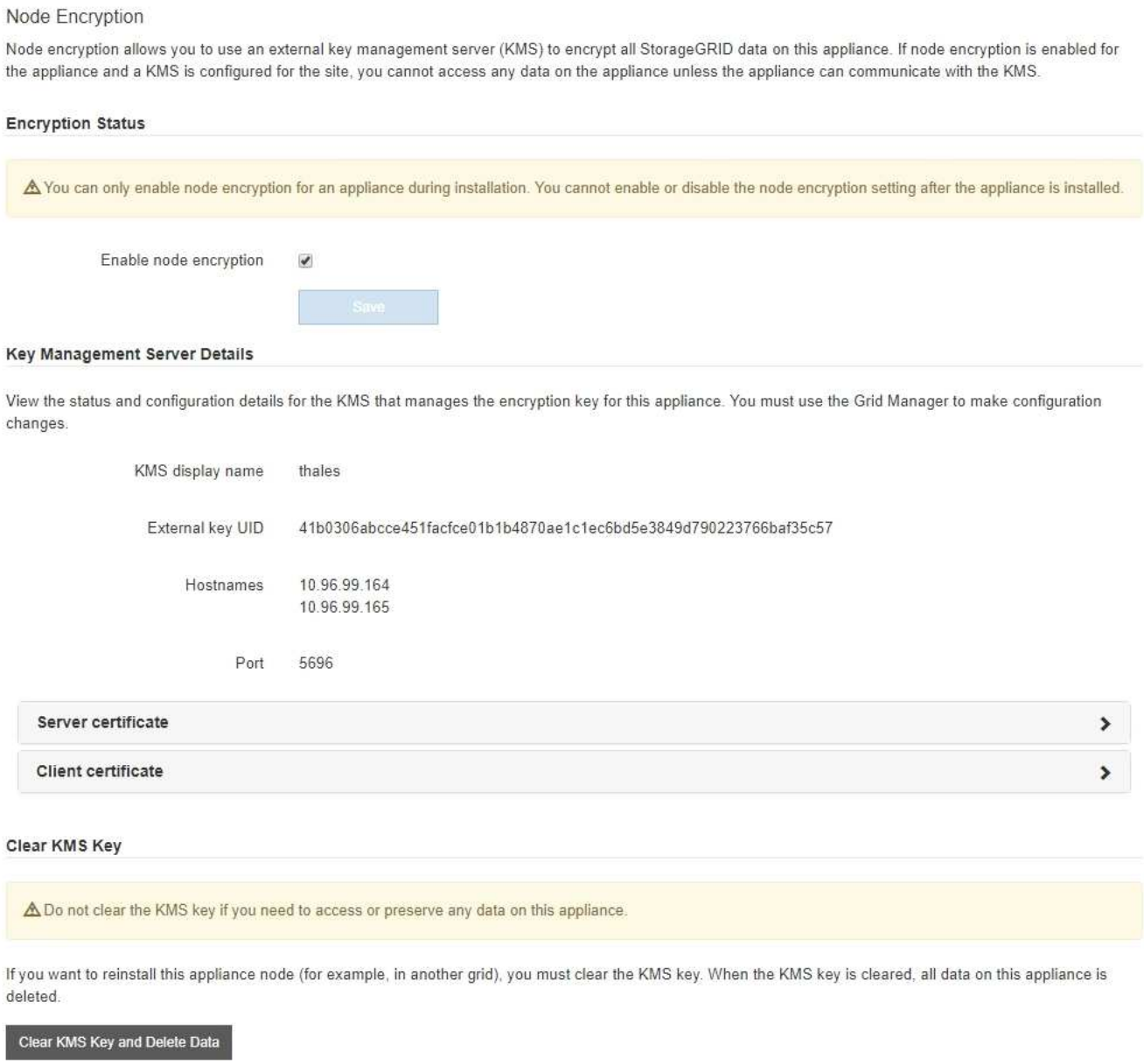
必要なもの

- インストール時にアプライアンスのノード暗号化を有効にしておく必要があります。アプライアンスのインストール後にノード暗号化を有効にすることはできません。
- アプライアンスはメンテナンスモードになりました。

  "アプライアンスをメンテナンスモードにします"

手順

1. StorageGRID アプライアンスインストーラから、 * ハードウェアの設定 * > * ノード暗号化 * を選択します。




Node Encryption のページには次の 3 つのセクションがあります。

- Encryption Status には、アプライアンスでノード暗号化が有効か無効かが表示されます。
- キー管理サーバの詳細には、アプライアンスの暗号化に使用されている KMS に関する情報が表示されます。サーバおよびクライアント証明書のセクションを展開すると、証明書の詳細およびステータスを表示できます。
  - 期限切れの証明書の更新など、証明書自体に関する問題に対処するには、 StorageGRID の管理手順の KMS に関する情報を参照してください。
  - KMS ホストへの接続で予期しない問題が発生する場合は、ドメインネームシステム（ DNS ）サーバが正しいこと、およびアプライアンスのネットワークが正しく設定されていることを確認してください。

    "DNSサーバの設定を確認しています"

  - 証明書の問題を解決できない場合は、テクニカルサポートにお問い合わせください。

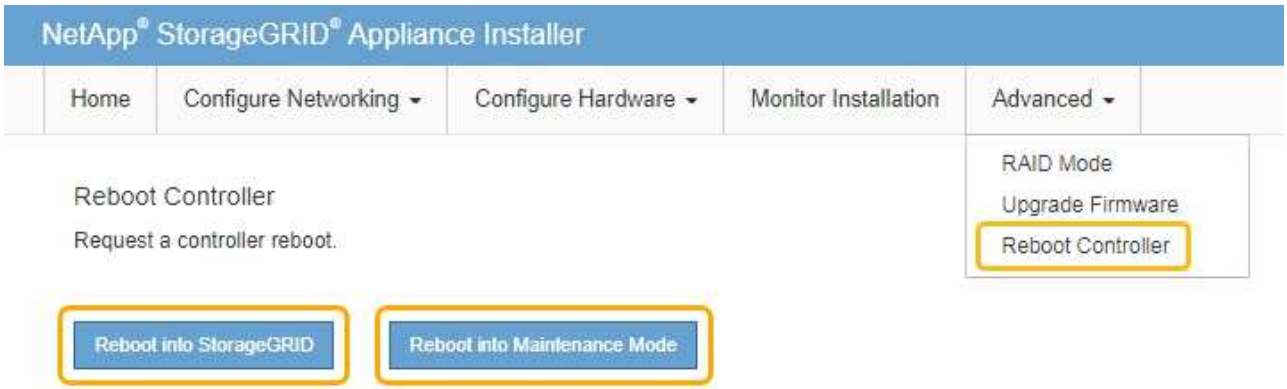
- KMS Key をクリアすると、アプライアンスのノード暗号化が無効になり、 StorageGRID サイト用に設定されているアプライアンスとキー管理サーバの間の関連付けが解除され、アプライアンスのすべてのデータが削除されます。別の StorageGRID システムにアプライアンスをインストールする前に、KMS キーをクリアする必要があります。

  "キー管理サーバ設定のクリア"

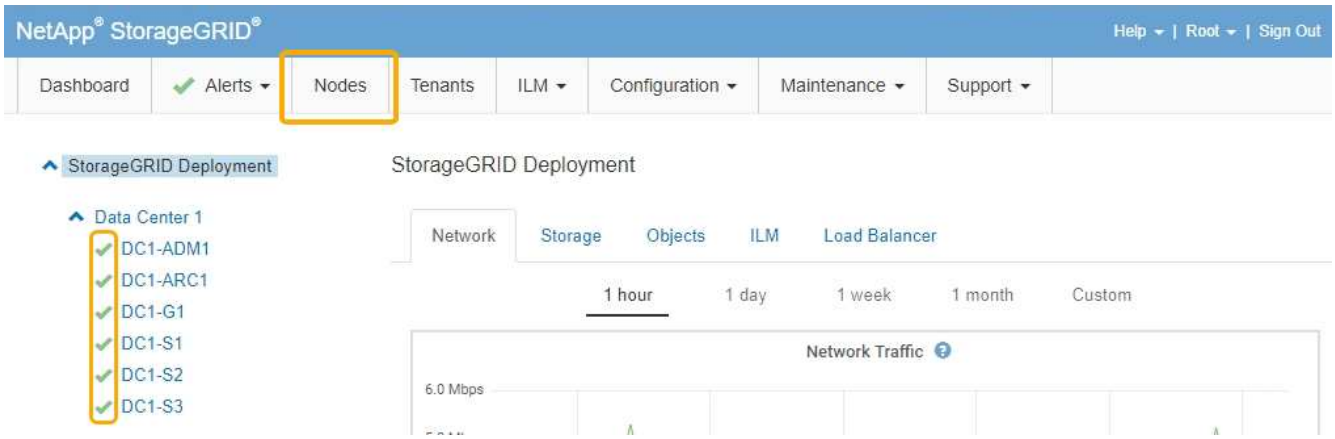
  KMS の設定をクリアすると、アプライアンスからデータが削除され、永久にアクセスできなくなります。このデータはリカバリできません。

2. ノード暗号化ステータスの確認が完了したら、ノードをリブートします。StorageGRID アプライアンス・インストーラから、 **Advanced**>*Reboot Controller* を選択し、次のいずれかのオプションを選択します。

   - Reboot into StorageGRID * を選択し、ノードをグリッドに再追加してコントローラをリブートします。メンテナンスモードで作業を完了し、ノードを通常動作に戻す準備ができている場合は、このオプションを選択します。
   - メンテナンスモードを維持したままコントローラをリブートするには、 * Reboot into Maintenance Mode * を選択します。このオプションは、グリッドに再追加する前にノードで追加のメンテナンス処理を実行する必要がある場合に選択します。




アプライアンスがリブートしてグリッドに再参加するまでに最大 20 分かかることがあります。リブートが完了し、ノードが再びグリッドに参加したことを確認するには、 Grid Manager に戻ります。[ノード*（Nodes *）]タブには、通常のステータスが表示されます ✔ アクティブなアラートがなく、ノードがグリッドに接続されていることを示す、アプライアンスノードの場合。




関連情報

"StorageGRID の管理"

キー管理サーバ設定のクリア

# キー管理サーバ（ KMS ）の設定をクリアすると、アプライアンスでノード暗号化が無効になります。KMS の設定をクリアすると、アプライアンスのデータは完全に削除され、アクセスできなくなります。このデータはリカバリできません。

必要なもの

アプライアンス上のデータを保持する必要がある場合は、KMSの設定をクリアする前に、ノードの運用停止手順 を実行する必要があります。

> KMS をクリアすると、アプライアンスのデータが完全に削除され、アクセスできなくなります。このデータはリカバリできません。

ノードを運用停止して、格納されているデータをStorageGRID 内の他のノードに移動します。グリッドノードの運用停止手順については、リカバリとメンテナンスの手順を参照してください。

このタスクについて

アプライアンス KMS の設定をクリアすると、ノード暗号化が無効になり、アプライアンスノードと StorageGRID サイトの KMS の設定との間の関連付けが解除されます。その後、アプライアンスのデータが削除され、アプライアンスはインストール前の状態のままになります。このプロセスを元に戻すことはできません。

KMS の設定をクリアする必要があります。

- アプライアンスを別の StorageGRID システムにインストールする前に、 KMS を使用しない、または別の KMS を使用する前に、

> 同じ KMS キーを使用する StorageGRID システムにアプライアンスノードを再インストールする場合は、 KMS の設定をクリアしないでください。

- KMS 設定が失われて KMS キーをリカバリおよび再インストールできないノードをリカバリする前に、 KMS キーをリカバリできません。
- お客様のサイトで以前使用していたアプライアンスを返却する前に、

- ノード暗号化が有効になっているアプライアンスの運用を停止したあと。

> KMS をクリアして StorageGRID システム内の他のノードにデータを移動する前に、アプライアンスの運用を停止します。アプライアンスの運用を停止する前に KMS をクリアすると、データが失われるため、アプライアンスが動作しなくなる可能性があります。

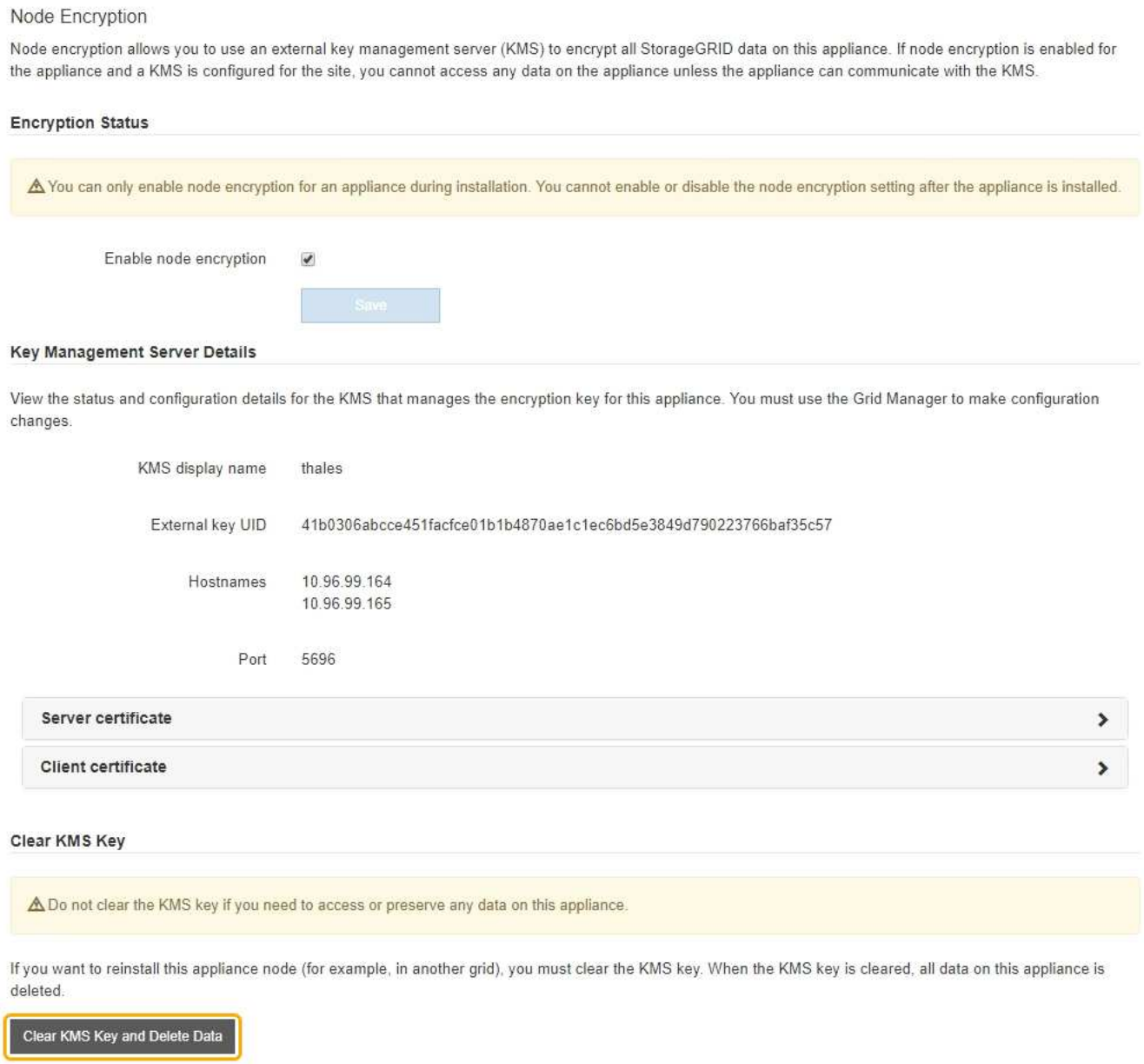
手順

1. ブラウザを開き、アプライアンスのコンピューティングコントローラの IP アドレスのいずれかを入力します。[+]
   **`https://Controller_IP:8443`**

   *`Controller_IP`* は、3つのStorageGRID ネットワークのいずれかでのコンピューティングコントローラ（ストレージコントローラではない）のIPアドレスです。

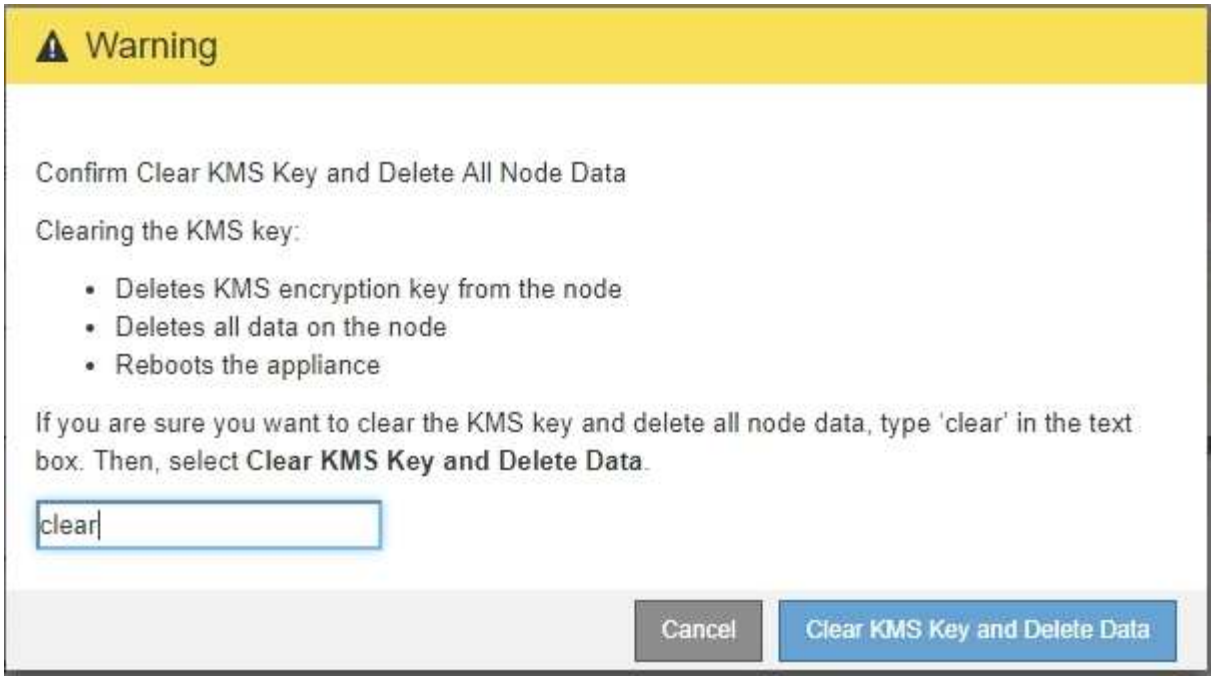
   StorageGRID アプライアンスインストーラのホームページが表示されます。

2. Configure Hardware * > * Node Encryption * を選択します。




KMS の設定をクリアすると、アプライアンス上のデータが完全に削除されます。このデータはリカバリできません。

3. ウィンドウの下部で、 * KMS キーをクリアしてデータを削除 * を選択します。
4. KMSの設定をクリアしても問題がない場合は、「+」と入力します **`clear`** +を押して、「* KMSキーを消去してデータを削除*」を選択します。




KMS 暗号化キーとすべてのデータがノードから削除され、アプライアンスがリブートします。この処理には 20 分程度かかる場合があります。

5. ブラウザを開き、アプライアンスのコンピューティングコントローラの IP アドレスのいずれかを入力します。[+]
**`https://Controller_IP:8443`**

   *`Controller_IP`* は、3つのStorageGRID ネットワークのいずれかでのコンピューティングコントローラ（ストレージコントローラではない）のIPアドレスです。

   StorageGRID アプライアンスインストーラのホームページが表示されます。

6. Configure Hardware * > * Node Encryption * を選択します。
7. ノードの暗号化が無効になっていること、および * キー管理サーバの詳細 * および * KMS キーと削除 * のコントロールでキーと証明書の情報がウィンドウから削除されていることを確認します。

   アプライアンスでのノード暗号化の再インストールまでは、グリッドでのノード暗号化を再度有効にすることはできません。

完了後

アプライアンスがリブートし、 KMS がクリアされてインストール前の状態になっていることを確認したら、StorageGRID システムからアプライアンスを物理的に取り外すことができます。再インストールのためのアプライアンスの準備については、リカバリおよびメンテナンスの手順を参照してください。

関連情報

"StorageGRID の管理"

""

# SG100およびSG1000サービスアプライアンス

StorageGRID SG100およびSG1000アプライアンスの設置とメンテナンスの方法について説明します。

- "SG100 および SG1000 アプライアンスの概要"
- "SG100 および SG1000 アプリケーション"
- "インストールと導入の概要"
- "設置を準備しています"
- "ハードウェアを設置"
- "StorageGRID 接続を設定しています"
- "BMCインターフェイスを設定しています"
- "オプション：ノード暗号化を有効にする"
- "サービスアプライアンスノードの導入"
- "ハードウェアの設置のトラブルシューティング"
- "アプライアンスのメンテナンス"

## SG100 および SG1000 アプライアンスの概要

StorageGRID SG100 サービスアプライアンスと SG1000 サービスアプライアンスはゲートウェイノードおよび管理ノードとして動作して、 StorageGRID システムで高可用性のロードバランシングサービスを提供できます。両方のアプライアンスをゲートウェイノードとして使用し、管理ノード（プライマリノードまたは非プライマリノード）を同時に使用できます。

### アプライアンスの特長

サービスアプライアンスのどちらのモデルにも次の機能があります。

- ゲートウェイノードまたは管理ノードは StorageGRID システムで機能します。
- ノードの導入と設定を簡易化する StorageGRID アプライアンスインストーラ。
- 導入後、は既存の管理ノードから、またはローカルドライブにダウンロードしたソフトウェアから StorageGRID ソフトウェアにアクセスできます。導入プロセスをさらに簡易化するために、アプライアンスには最新バージョンのソフトウェアがプリロードされています。
- 一部のアプライアンスハードウェアを監視および診断するためのベースボード管理コントローラ（ BMC ）。
- グリッドネットワーク、管理ネットワーク、クライアントネットワークを含む 3 つの StorageGRID ネットワークすべてに接続できること。
  - SG100 は、グリッドネットワークとクライアントネットワークとの 10GbE または 25GbE 接続を最大 4 つサポートします。
  - SG1000 では、グリッドネットワークとクライアントネットワークとの 10GbE 、 25GbE 、 40GbE 、または 100GbE 接続が最大 4 つサポートされています。

### SG100 と SG1000 の図

この図は、 SG100 の前面とベゼルを取り外した SG1000 の前面を示しています。

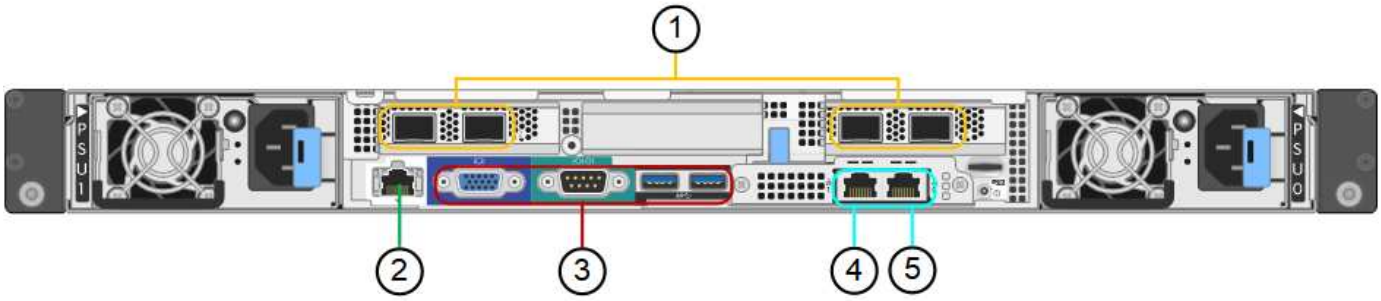
前面からは、ベゼル上の製品名以外の 2 つのアプライアンスは同じです。

オレンジの枠で囲まれた 2 本のソリッドステートドライブ（ SSD ）は、 StorageGRID オペレーティングシステムの格納に使用され、冗長性を確保するために RAID 1 を使用してミラーリングされます。SG100 または SG1000 サービスアプライアンスが管理ノードとして設定されている場合は、これらのドライブに監査ログ、指標、およびデータベーステーブルが格納されます。

残りのドライブスロットは空です。

### SG100 の背面にあるコネクタ

この図は、 SG100 の背面にあるコネクタを示しています。

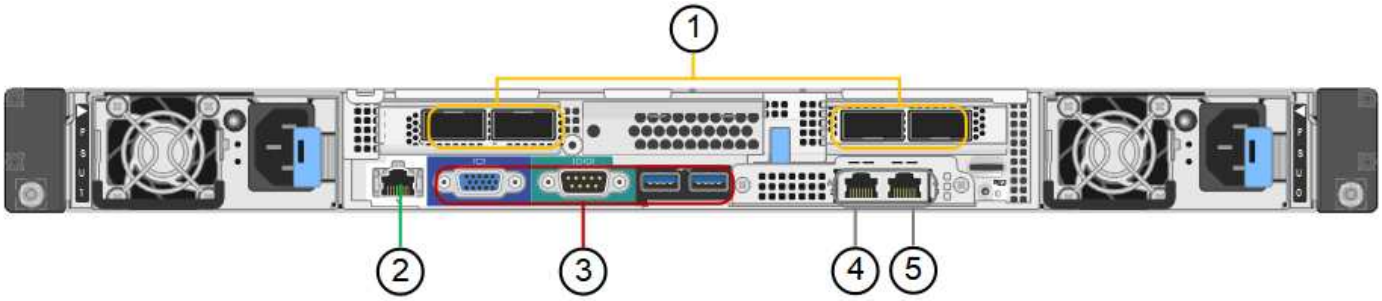



| | ポート | を入力します | 使用 |
|---|---|---|---|
| 1. | ネットワークポート 1~4 | ケーブルまたは SFP トランシーバタイプ（ SFP28 および SFP+ モジュールをサポート ）、スイッチ速度、設定されたリンク速度に基づく 10 / 25GbE | StorageGRID のグリッドネットワークおよびクライアントネットワークに接続します。 |
| 2. | BMC 管理ポート | 1GbE （ RJ-45 ） | アプライアンスのベースボード管理コントローラに接続します。 |
| 3. | 診断とサポート用のポート | • VGA<br>• シリアル、 115200 8-N-1<br>• USB | テクニカルサポート専用です。 |
| 4. | 管理ネットワークポート 1 | 1GbE （ RJ-45 ） | アプライアンスを StorageGRID の管理ネットワークに接続します。 |

| | ポート | を入力します | 使用 |
|---|---|---|---|
| 5. | 管理ネットワークポート 2 | 1GbE （ RJ-45 ） | オプション：<br>• StorageGRID の管理ネットワークへの冗長接続を確保するには、管理ポート 1 とボンディングします。<br>• 一時的なローカルアクセス用（ IP 169.254.0.1 ）に空けておくことができます。<br>• DHCP によって割り当てられた IP アドレスを使用できない場合は、設置時の IP 設定にポート 2 を使用します。 |

**SG1000** の背面のコネクタ

この図は、 SG1000 の背面にあるコネクタを示しています。




| | ポート | を入力します | 使用 |
|---|---|---|---|
| 1. | ネットワークポート 1~4 | ケーブルまたはトランシーバのタイプ、スイッチ速度、設定されたリンク速度に基づく 10 / 25 / 40 / 100GbE 。QSFP28 と QSFP+ （ 40/100GbE ）はネイティブでサポートされており、 SFP28 / SFP+ トランシーバを QSA （別売）と併用して 10 / 25GbE の速度を使用できます。 | StorageGRID のグリッドネットワークおよびクライアントネットワークに接続します。 |
| 2. | BMC 管理ポート | 1GbE （ RJ-45 ） | アプライアンスのベースボード管理コントローラに接続します。 |
| 3. | 診断とサポート用のポート | • VGA<br>• シリアル、 115200 8-N-1<br>• USB | テクニカルサポート専用です。 |

| | ポート | を入力します | 使用 |
|---|---|---|---|
| 4. | 管理ネットワークポート 1 | 1GbE （ RJ-45 ） | アプライアンスを StorageGRID の管理ネットワークに接続します。 |
| 5. | 管理ネットワークポート 2 | 1GbE （ RJ-45 ） | オプション：<br>• StorageGRID の管理ネットワークへの冗長接続を確保するには、管理ポート 1 とボンディングします。<br>• 一時的なローカルアクセス用（ IP 169.254.0.1 ）に空けておくことができます。<br>• DHCP によって割り当てられた IP アドレスを使用できない場合は、設置時の IP 設定にポート 2 を使用します。 |

## SG100 および SG1000 アプリケーション

StorageGRID サービスアプライアンスは、ゲートウェイサービスおよび一部のグリッド管理サービスの冗長性を提供するためにさまざまな方法で設定できます。

アプライアンスは、次の方法で導入できます。

- ゲートウェイノードとして新規または既存のグリッドに追加します
- プライマリまたは非プライマリ管理ノードとして新しいグリッドに追加するか、非プライマリ管理ノードとして既存のグリッドに追加します
- ゲートウェイノードと管理ノード（プライマリまたは非プライマリ）として同時に動作します

アプライアンスでは、 S3 または Swift データパス接続に対し、ハイアベイラビリティ（ HA ）グループとインテリジェントなロードバランシングを実装できます。

次に、アプライアンスの機能を最大限に活用する例を示します。

- 2 台の SG1000 アプライアンスをゲートウェイノードとして設定して、ゲートウェイサービスを提供するには、 2 台の SG100 または 2 台の SG1000 アプライアンスを使用します。

> SG100 と SG1000 サービスアプライアンスは同じサイトに導入しないでください。パフォーマンスが予測不能になる可能性があります

- 一部のグリッド管理サービスの冗長性を確保するには、 2 台の SG100 または 2 台の SG1000 アプライアンスを使用します。そのためには、各アプライアンスを管理ノードとして設定します。
- 2 台の SG1000 アプライアンスを使用して、 1 つ以上の仮想 IP アドレス経由でアクセスする可用性の高いロードバランシングサービスとトラフィックシェーピングサービスを提供します。そのためには、アプライアンスを管理ノードまたはゲートウェイノードの任意の組み合わせとして設定し、両方のノードを同じ HA グループに追加します。

同じ HA グループ内の管理ノードとゲートウェイノードを使用する場合、 CLB （ Connection Load Balancer ）ポートと管理ノードのみのポートはフェイルオーバーされません。HA グループを設定する手順については、 StorageGRID の管理手順を参照してください。

CLB サービスは廃止されました。

StorageGRID ストレージアプライアンスとともに使用すると、 SG100 と SG1000 サービスアプライアンスの両方で、外部のハイパーバイザーやコンピューティングハードウェアに依存しないアプライアンスのみのグリッドを導入できます。

関連情報

"StorageGRID の管理"

## インストールと導入の概要

### StorageGRID サービスアプライアンスは StorageGRID の初回導入時に設置することも、後日拡張の一環としてサービスアプライアンスノードを追加することもできます。

必要なもの

StorageGRID システムが、必要なバージョンの StorageGRID ソフトウェアを使用している。

| アプライアンス | 必要な **StorageGRID** のバージョン |
| --- | --- |
| SG100 | 11.4 以降（最新のホットフィックスを推奨） |
| SG1000 からのアクセス | 11.3 以降（最新のホットフィックスを推奨） |

インストールと導入のタスク

StorageGRID アプライアンスの準備とグリッドへの追加は、主に 4 つの手順で行います。

1. 設置の準備：
   - 設置場所の準備
   - 開梱と内容の確認
   - 追加機器および工具の入手方法
   - ネットワーク構成を検証しています
   - オプション：すべてのアプライアンスデータを暗号化する場合は、外部キー管理サーバ（ KMS ）を設定します。外部キー管理の詳細については、 StorageGRID の管理手順を参照してください。
2. ハードウェアの設置
   - ハードウェアの登録
   - キャビネットまたはラックへのアプライアンスの設置
   - アプライアンスのケーブル接続

- 電源コードの接続と電源の投入
- ブート時のステータスコードの確認

3. ハードウェアの設定
   - StorageGRID アプライアンスインストーラへのアクセス、および StorageGRID ネットワークへの接続に必要なリンクとネットワーク IP の設定
   - アプライアンスのベースボード管理コントローラ（ BMC ）インターフェイスへのアクセス
   - オプション：外部 KMS を使用してアプライアンスデータを暗号化する場合は、ノード暗号化を有効にします。
4. アプライアンスのゲートウェイノードまたは管理ノードを導入する

   アプライアンスハードウェアの設置と設定が完了したら、アプライアンスをゲートウェイノードおよび管理ノードとして StorageGRID システムに導入できます。SG100 と SG1000 アプライアンスは、両方ともゲートウェイノードと管理ノード（プライマリノードと非プライマリノード）として同時に動作できます。

| タスク | 手順 |
| --- | --- |
| 新しい StorageGRID システムにアプライアンスのゲートウェイノードまたは管理ノードを導入する | "サービスアプライアンスノードの導入" |
| 既存の StorageGRID システムにアプライアンスのゲートウェイノードまたは管理ノードを追加する | "StorageGRID システムの拡張手順" |
| ノードのリカバリ処理の一環としてアプライアンスのゲートウェイノードまたは管理ノードを導入する | "リカバリとメンテナンスの手順" |

関連情報

"設置を準備しています"

"ハードウェアを設置"

"StorageGRID 接続を設定しています"

"グリッドを展開します"

""

"StorageGRID の管理"

## 設置を準備しています

StorageGRID アプライアンスを設置するための準備では、設置場所を準備し、必要なすべてのハードウェア、ケーブル、工具を揃えます。また、 IP アドレスとネットワーク情報を収集する必要があります。

手順

- "サイトの準備（SG100およびSG1000）"
- "アプライアンスの開梱（SG100およびSG1000）"
- "追加の機器と工具の入手（SG100およびSG1000）"
- "Web ブラウザの要件"
- "アプライアンスのネットワーク接続を確認します"
- "設置情報の収集（SG100およびSG1000）"

サイトの準備（**SG100**および**SG1000**）

## アプライアンスを設置する前に、設置場所および使用するキャビネットやラックが StorageGRID アプライアンスの仕様を満たしていることを確認する必要があります。

手順

1. 設置場所の温度、湿度、高度範囲、通気、熱放散の要件を満たしていることを確認します。 配線、電源、およびアース。詳細については、 NetApp Hardware Universe を参照してください。
2. 設置場所が AC 電源の正しい電圧を供給していることを確認します（ AC 120 ～ 240 ボルトの範囲）。
3. 次のサイズのシェルフ（ケーブルなし）が収まる 48.3cm （ 19 インチ）のキャビネットまたはラックを用意します。

| 高さ | 幅 | 奥行き | 最大重量 |
|---|---|---|---|
| 1.70 インチ<br>（ 4.32 cm ） | 17.32 インチ<br>（ 44.0 cm ） | 32.0 インチ<br>（ 81.3 cm ） | 39 ポンド<br>（ 17.7 kg ） |

4. アプライアンスの設置場所を決定します。

関連情報

"NetApp Hardware Universe の略"

"NetApp Interoperability Matrix Tool で確認できます"

アプライアンスの開梱（**SG100**および**SG1000**）

## StorageGRID アプライアンスを設置する前にすべて開梱し、内容物を納品書の項目と比較します。

アプライアンスハードウェア

- * SG100 または SG1000 *

- * 取扱説明書付きレールキット *

電源コード

StorageGRID アプライアンスには、次の電源コードが付属しています。

- * お住まいの国に対応した電源コード 2 本 *

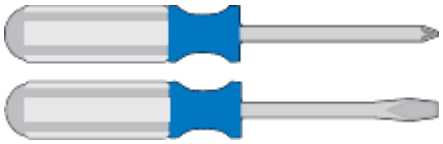
キャビネットによっては、アプライアンスに付属している電源コードではなく特別な電源コードを使用する場合があります。

追加の機器と工具の入手（**SG100**および**SG1000**）

## StorageGRID アプライアンスを設置する前に、必要な追加機器や工具がすべて揃っていることを確認します。

ハードウェアの設置と設定を行うには、次の追加機器が必要です。

- * ドライバ *

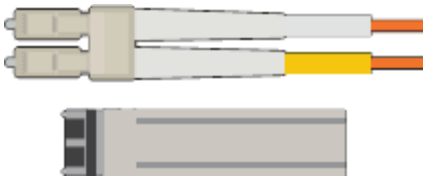


フィリップス番号2 本のドライバ

中型マイナスドライバ

- * 静電気防止用リストストラップ *

- * 光ケーブルとトランシーバ *



◦ ケーブル

▪ TwinAx / 銅線（ 1~4 本）

または

▪ ファイバ / 光（ 1~4 本）

◦ リンク速度に基づいて、各トランシーバ / アダプタの 1 ～ 4 （速度の混在はサポートされていません）

▪ SG100 ：

| リンク速度（ **GbE** ） | 必要な機器 |
|---|---|
| 10. | SFP+ トランシーバ |
| 25 | SFP28 トランシーバ |

▪ SG1000 ：

| リンク速度（ **GbE** ） | 必要な機器 |
|---|---|
| 10. | QSFP-SFP アダプタ（ QSA ）および SFP+ トランシーバ |
| 25 | QSFP-SFP アダプタ（ QSA ）および SFP28 トランシーバです |
| 40 | QSFP+ トランシーバ |
| 100 | QFSP28 トランシーバ |

- * RJ-45 （ Cat5 / Cat5e / Cat6 / Cat6A ）イーサネットケーブル *

- * サービスラップトップ *

サポートされている Web ブラウザ

1GbE （ RJ-45 ）ポート

一部のポートでは 10/100 イーサネット速度がサポートされない場合があります。

- * オプションのツール *

ヘッドビット付き電源ドリル

懐中電灯

**Web** ブラウザの要件

## サポートされている Web ブラウザを使用する必要があります。

| **Web** ブラウザ | サポートされる最小バージョン |
|---|---|
| Google Chrome | 87 |
| Microsoft Edge の場合 | 87 |
| Mozilla Firefox | 84 |

ブラウザウィンドウの幅を推奨される値に設定してください。

| ブラウザの幅 | ピクセル |
|---|---|
| 最小（ Minimum ） | 1024 |

| ブラウザの幅 | ピクセル |
| --- | --- |
| 最適 | 1280 |

アプライアンスのネットワーク接続を確認します

## StorageGRID アプライアンスを設置する前に、アプライアンスに接続できるネットワークを確認しておく必要があります。

StorageGRID アプライアンスを StorageGRID システムのノードとして導入する場合は、次のネットワークに接続できます。

- * StorageGRID のグリッドネットワーク * ：グリッドネットワークは、すべての内部 StorageGRID トラフィックに使用されます。このネットワークによって、グリッド内のすべてのノードが、すべてのサイトおよびサブネットにわたって相互に接続されます。グリッドネットワークは必須です。
- * StorageGRID の管理ネットワーク * ：管理ネットワークは、システムの管理とメンテナンスに使用するクローズドネットワークです。管理ネットワークは通常はプライベートネットワークであり、サイト間でルーティング可能にする必要はありません。管理ネットワークはオプションです。
- * StorageGRID のクライアントネットワーク： * クライアントネットワークは、 S3 や Swift などのクライアントアプリケーションへのアクセスを可能にするオープンネットワークです。クライアントネットワークはグリッドへのクライアントプロトコルアクセスを提供するため、グリッドネットワークを分離してセキュリティを確保できます。開くことを選択したポートだけを使用してこのネットワーク経由でアプライアンスにアクセスできるよう、クライアントネットワークを設定できます。クライアントネットワークはオプションです。
- *サービスアプライアンス用のBMC管理ネットワーク：このネットワークは、SG100およびSG1000のベースボード管理コントローラへのアクセスを提供し、アプライアンス内のハードウェアコンポーネントの監視と管理を可能にします。この管理ネットワークは、 StorageGRID の管理ネットワークと同じにすることも、独立した管理ネットワークにすることもできます。

関連情報

"設置情報の収集（SG100およびSG1000）"

"アプライアンスSG100およびSG1000のケーブル接続"

"ネットワークガイドライン"

"グリッド入門"

**SG100** および **SG1000** アプライアンスのポートボンディングモード

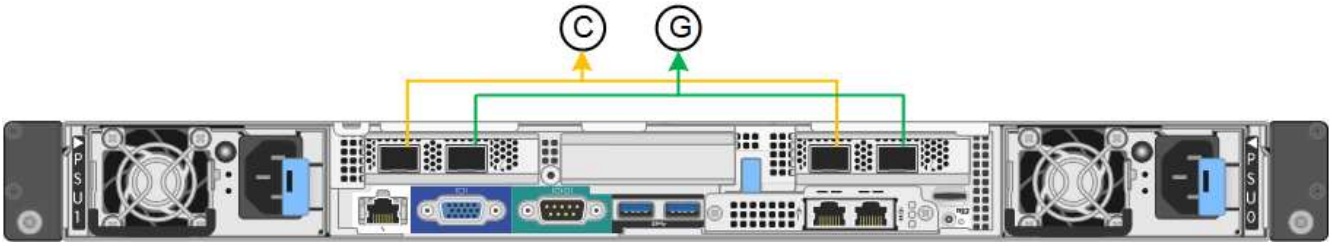
## SG100 および SG1000 アプライアンスのネットワークリンクを設定する場合は、グリッドネットワークとオプションのクライアントネットワークに接続するポート、およびオプションの管理ネットワークに接続する 1GbE 管理ポートに対してポートボンディングを使用できます。ポートボンディングを使用すると、 StorageGRID ネットワークとアプライアンスの間のパスが冗長化されるため、データの保護に役立ちます。

# サービスアプライアンスのネットワークポートは、グリッドネットワークおよびクライアントネットワーク接続用に、 Fixed または Aggregate のポートボンディングモードをサポートします。

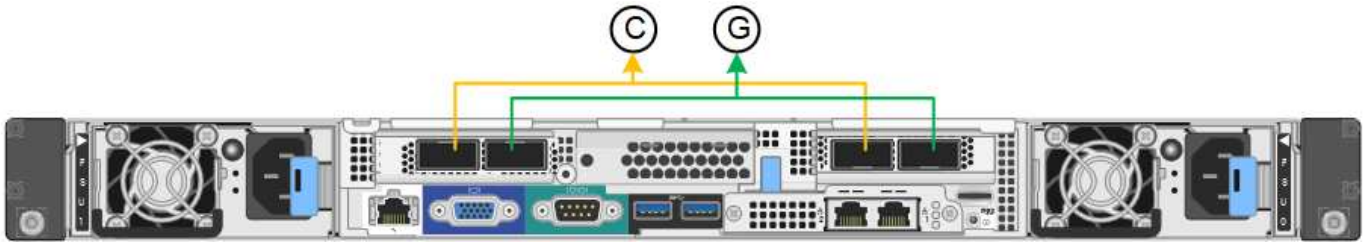
## **Fixed** ポートボンディングモード

Fixed ポートボンディングモードは、ネットワークポートのデフォルトの設定です。

- SG100 固定ポートボンディングモード *




- SG1000 の固定ポートボンディングモード *




| | ボンディングされるポート |
|---|---|
| C | このネットワークを使用する場合、ポート 1 とポート 3 がクライアントネットワーク用にボンディングされます。 |
| G | ポート 2 とポート 4 がグリッドネットワーク用にボンディングされます。 |

Fixed ポートボンディングモードを使用する場合は、 Active-Backup モードまたは Link Aggregation Control Protocol （ LACP ）（ 802.3ad ）モードを使用してポートをボンディングできます。

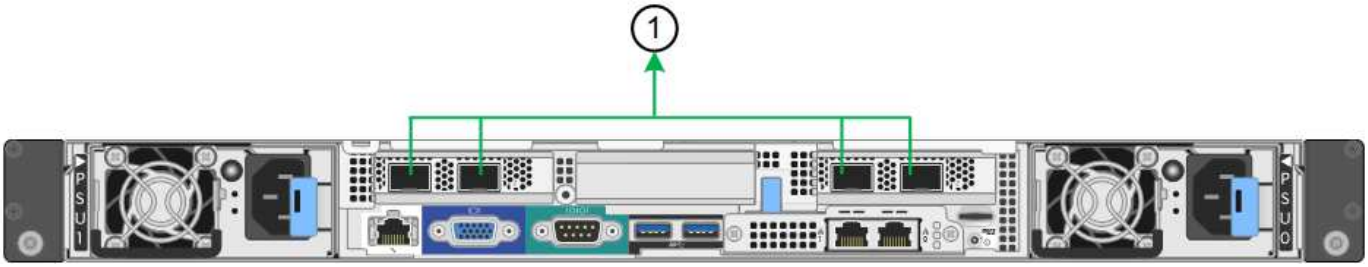
- Active-Backup モード（デフォルト）では、一度に 1 つのポートのみがアクティブになります。アクティブポートで障害が発生すると、バックアップポートが自動的にフェイルオーバーして接続が継続されます。ポート 4 がポート 2 のバックアップパスとなり（グリッドネットワーク）、ポート 3 がポート 1 のバックアップパスとなります（クライアントネットワーク）。
- LACP モードでは、各ポートペアでサービスアプライアンスとネットワークの間の論理チャネルが形成され、スループットが向上します。一方のポートで障害が発生しても、もう一方のポートは引き続きチャネルを提供します。スループットは低下しますが、接続に影響はありません。

冗長な接続が不要な場合は、各ネットワークで使用できるポートは 1 つだけです。ただし、StorageGRID をインストールしたあとに、ケーブルが取り外されていることを示す * サービスアプライアンスリンク停止 * アラートがグリッドマネージャでトリガーされることがあります。このアラートルールは安全に無効にすることができます。

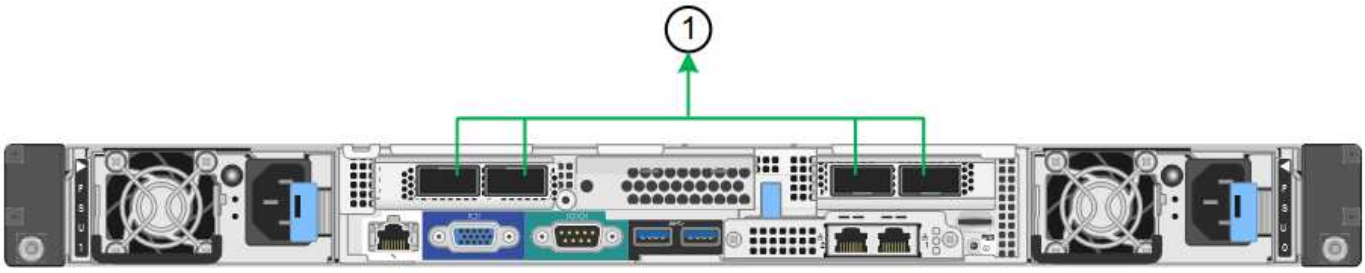
### Aggregate ポートボンディングモード

アグリゲートポートボンディングモードを使用すると、各 StorageGRID ネットワークのスループットが大幅に向上し、追加のフェイルオーバーパスも確保されます。

- SG100 アグリゲートポートボンディングモード *




- SG1000 Aggregate ポートボンディングモード *




| | ボンディングされるポート |
|---|---|
| 1. | 接続されたすべてのポートを 1 つの LACP ボンドにグループ化して、すべてのポートをグリッドネットワークとクライアントネットワークのトラフィックに使用できるようにします。 |

アグリゲートポートボンディングモードを使用する場合は、次の点に注意してください。

- LACP ネットワークボンディングモードを使用する必要があります。
- 各ネットワークに一意の VLAN タグを指定する必要があります。この VLAN タグが各ネットワークパケットに追加され、ネットワークトラフィックが正しいネットワークにルーティングされます。
- VLAN と LACP をサポートするスイッチにポートを接続する必要があります。複数のスイッチを LACP ボンドに加える場合は、対象のスイッチが Multi-Chassis Link Aggregation （ MLAG ）グループまたは同等の機能をサポートしていることが必要です。
- VLAN 、 LACP 、 MLAG などを使用するようにスイッチを設定する方法について理解しておく必要があります。

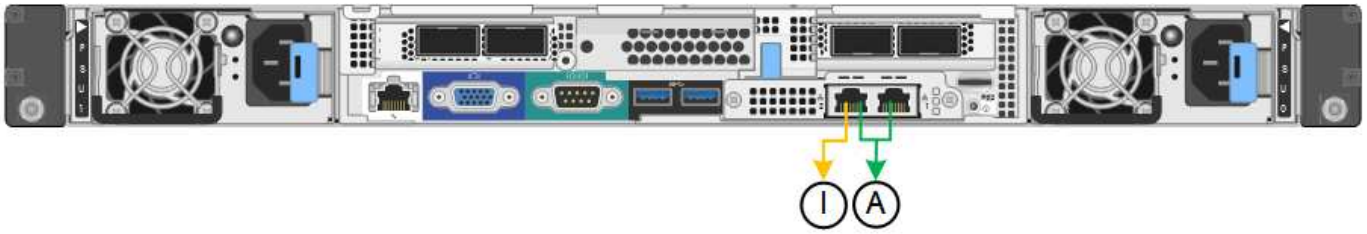
4 つのポートをすべて使用する必要がない場合は、使用するポートの数を 1~3 のいくつでも指定できます。複数のポートを使用すると、ポートの 1 つに障害が発生した場合でも、ネットワーク接続を確保できる可能性が高くなります。

ネットワークポートを 4 つ未満にすると、アプライアンスノードをインストールしたあとに、ケーブルが取り外されていることを示す * サービスアプライアンスリンク停止 * アラートが Grid Manager でトリガーされる場合があることに注意してください。トリガーされたアラートに対してこのアラートルールを安全に無効にすることができます。

サービスアプライアンス上の 2 つの 1GbE 管理ポートでは、オプションの管理ネットワークに接続するためのネットワークボンディングモードとして、 Independent または Active-Backup を選択できます。

- SG100 ネットワーク管理ポート *

- SG1000 ネットワーク管理ポート *




Independent モードでは、左側の管理ポートだけが管理ネットワークに接続されます。このモードではパスは冗長化されません。右側の管理ポートは接続されず、一時的なローカル接続（ IP アドレス 169.254.0.1 ）に使用できます。

Active-Backup モードでは、両方の管理ポートが管理ネットワークに接続されます。一度に 1 つのポートのみがアクティブになります。アクティブポートで障害が発生すると、バックアップポートが自動的にフェイルオーバーして接続が継続されます。これら 2 つの物理ポートを 1 つの論理管理ポートにボンディングすることで、管理ネットワークへのパスが冗長化されます。

1GbE 管理ポートが Active-Backup モードに設定されている場合にサービスアプライアンスへの一時的なローカル接続が必要となった場合は、両方の管理ポートからケーブルを取り外し、一時的なケーブルを右側の管理ポートに接続し、 IP アドレス 169.254.0.1 を使用してアプライアンスにアクセスしてください。

| | ネットワークボンディングモード |
|---|---|
| A | アクティブ / バックアップモード：両方の管理ポートが、管理ネットワークに接続された 1 つの論理管理ポートにボンディングされます。 |
| 私 | Independent モード。左側のポートが管理ネットワークに接続されます。右側のポートは一時的なローカル接続（ IP アドレス 169.254.0.1 ）に使用できます。 |

設置情報の収集（**SG100**および**SG1000**）

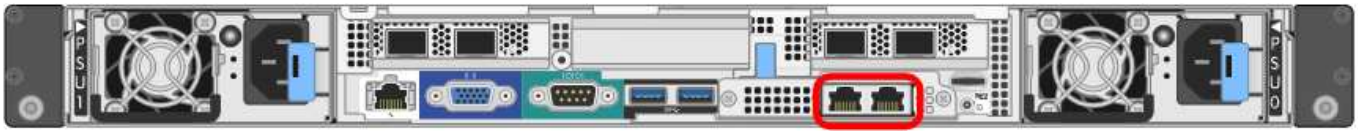
StorageGRID アプライアンスを設置および設定する際に、イーサネットスイッチポー

ト、 IP アドレス、およびポートとネットワークのボンディングモードについて決定し、関連情報を収集する必要があります。アプライアンスに接続する各ネットワークの必要な情報を記録します。これらの値は、ハードウェアの設置と設定に必要です。

管理ポートとメンテナンスポート

StorageGRID の管理ネットワークは、システムの管理とメンテナンスに使用するオプションのネットワークです。アプライアンスは、アプライアンス上の次の 1GbE 管理ポートを使用して管理ネットワークに接続します。

- SG100 RJ-45 ポート *



- SG1000 RJ-45 ポート *

- 管理および保守接続 *

| 必要な情報 | あなたの価値 |
| --- | --- |
| 管理ネットワークが有効になりました | 1 つ選択してください：<br>• いいえ<br>• ○（デフォルト） |
| ネットワークボンディングモード | 1 つ選択してください：<br>• Independent （デフォルト）<br>• アクティブ / バックアップ |
| 図の赤枠内左側のポートのスイッチポート（ Independent ネットワークボンディングモードのデフォルトのアクティブポート） | |
| 図の赤枠内右側のポートのスイッチポート（ Active-Backup ネットワークボンディングモードの場合のみ） | |

| 必要な情報 | あなたの価値 |
| --- | --- |
| 管理ネットワークポートの MAC アドレス<br>• 注： * アプライアンス前面の MAC アドレス・ラベルには、 BMC 管理ポートの MAC アドレスが記載されています。管理ネットワークポートの MAC アドレスを特定するには、ラベルに記載された 16 進数に * 2 * を追加する必要があります。たとえば、ラベルに記載されている MAC アドレスの末尾が * 09 * の場合、管理ポートの MAC アドレスの末尾は * 0B * となります。ラベルに記載された MAC アドレスの末尾が * （ *y* ） FF* の場合、管理ポートの MAC アドレスの末尾は * （ *y*+1 ） 01 * となります。この計算を簡単に行うには、 Windows で Calculator を開き、 Programmer モードに設定して Hex を選択し、 MAC アドレスを入力してから、 **+2=** と入力します。 | |
| DHCP によって割り当てられた管理ネットワークポートの IP アドレス（電源投入後に使用可能な場合）<br>• 注： * DHCP によって割り当てられた IP アドレスは、 MAC アドレスを使用して特定できます。 | • IPv4 アドレス（ CIDR ）：<br>• ゲートウェイ |
| 管理ネットワークでアプライアンスノードに使用する静的 IP アドレス<br>• 注： * ネットワークにゲートウェイがない場合は、同じ静的 IPv4 アドレスをゲートウェイに指定してください。 | • IPv4 アドレス（ CIDR ）：<br>• ゲートウェイ |
| 管理ネットワークのサブネット（ CIDR ） | |

ネットワークポート

アプライアンスの 4 つのネットワークポートは、 StorageGRID のグリッドネットワーク、およびオプションのクライアントネットワークに接続します。

• ネットワーク接続 *

| 必要な情報 | あなたの価値 |
| --- | --- |
| リンク速度 | SG100 の場合は、次のいずれかを選択します。<br>• auto （デフォルト）<br>• 10GbE の場合<br>• 25GbE<br>SG1000 の場合は、次のいずれかを選択します。<br>• auto （デフォルト）<br>• 10GbE の場合<br>• 25GbE<br>• 40GbE<br>• 100GbE<br>• 注： SG1000 の場合、 10GbE および 25GbE の速度には QSA アダプタが必要です。 |
| ポートボンディングモード | 1 つ選択してください：<br>• Fixed （デフォルト）<br>• アグリゲート |
| ポート 1 のスイッチポート（固定モードのクライアントネットワーク） | |
| ポート 2 のスイッチポート（ Fixed モードのグリッドネットワーク） | |
| ポート 3 のスイッチポート（固定モードのクライアントネットワーク） | |
| ポート 4 のスイッチポート（ Fixed モードのグリッドネットワーク） | |

**Grid** ネットワークポート

StorageGRID のグリッドネットワークは、内部のすべての StorageGRID トラフィックに使用される必須のネットワークです。アプライアンスは、 4 つのネットワークポートを使用してグリッドネットワークに接続します。

- グリッドネットワーク接続 *

| 必要な情報 | あなたの価値 |
| --- | --- |
| ネットワークボンディングモード | 1 つ選択してください：<br>• Active-Backup （デフォルト）<br>• LACP （ 802.3ad ） |
| VLAN タギングが有効です | 1 つ選択してください：<br>• いいえ（デフォルト）<br>• はい。 |
| VLAN タグ（ VLAN タギングが有効な場合） | 0~4095 の値を入力してください： |
| 電源投入後に使用可能な場合、 DHCP によってグリッドネットワークに割り当てられた IP アドレス | • IPv4 アドレス（ CIDR ）：<br>• ゲートウェイ |
| グリッドネットワークでアプライアンスノードに使用する静的 IP アドレス<br>• 注： * ネットワークにゲートウェイがない場合は、同じ静的 IPv4 アドレスをゲートウェイに指定してください。 | • IPv4 アドレス（ CIDR ）：<br>• ゲートウェイ |
| グリッドネットワークのサブネット（ CIDRs ） | |
| Maximum Transmission Unit （ MTU ；最大転送単位）設定（オプション）：デフォルト値の 1500 を使用するか、 9000 などのジャンボフレームに適した値に MTU を設定できます。 | |

クライアントネットワークポート

StorageGRID のクライアントネットワークは、一般にグリッドへのクライアントプロトコルアクセスを可能にするために使用する、オプションのネットワークです。アプライアンスは、 4 つのネットワーク・ポートを使用してクライアント・ネットワークに接続します。

• クライアントネットワーク接続 *

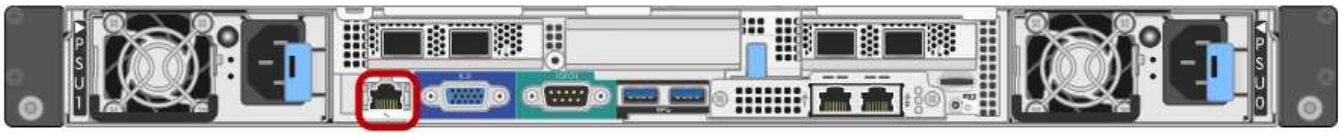
| 必要な情報 | あなたの価値 |
| --- | --- |
| クライアントネットワークが有効になりました | 1 つ選択してください：<br>• いいえ（デフォルト）<br>• はい。 |

| 必要な情報 | あなたの価値 |
| --- | --- |
| ネットワークボンディングモード | 1 つ選択してください：<br>• Active-Backup （デフォルト）<br>• LACP （ 802.3ad ） |
| VLAN タギングが有効です | 1 つ選択してください：<br>• いいえ（デフォルト）<br>• はい。 |
| VLAN タグ（ VLAN タギングが有効な場合） | 0~4095 の値を入力してください： |
| 電源投入後に DHCP によってクライアントネットワークに割り当てられた IP アドレスがある場合は | • IPv4 アドレス（ CIDR ）：<br>• ゲートウェイ |
| クライアントネットワークでアプライアンスノードに使用する静的 IP アドレス<br>• 注： * クライアントネットワークが有効な場合、アプライアンスのデフォルトルートにはここで指定したゲートウェイが使用されます。 | • IPv4 アドレス（ CIDR ）：<br>• ゲートウェイ |

**BMC** 管理ネットワークポート

サービスアプライアンスの BMC インターフェイスには、図の赤枠内にある 1GbE 管理ポートを使用してアクセスできます。このポートは、 Intelligent Platform Management Interface （ IPMI ）標準を使用した、イーサネット経由でのコントローラハードウェアのリモート管理をサポートします。

• SG100 BMC 管理ポート *



• SG1000 BMC 管理ポート *

• BMC 管理ネットワーク接続 *

| 必要な情報 | あなたの価値 |
| --- | --- |
| BMC 管理ポートに接続するイーサネットスイッチポート（赤枠内） | |
| 電源投入後に DHCP によって BMC 管理ネットワークに割り当てられた IP アドレスがある場合は | • IPv4 アドレス（ CIDR ）：<br>• ゲートウェイ |
| BMC 管理ポートに使用する静的 IP アドレス | • IPv4 アドレス（ CIDR ）：<br>• ゲートウェイ |

関連情報

"SG100 および SG1000 アプライアンスの概要"

"アプライアンスSG100およびSG1000のケーブル接続"

"StorageGRID IPアドレスを設定しています"

## ハードウェアを設置

ハードウェアの設置作業では、アプライアンスをキャビネットまたはラックに設置し、ケーブルを接続し、電源を投入します。

手順

- "ハードウェアの登録"
- "キャビネットまたはラックへのアプライアンスの設置（SG100およびSG1000）"
- "アプライアンスSG100およびSG1000のケーブル接続"
- "電源コードの接続と電源の投入（SG100およびSG1000）"
- "SG100およびSG1000アプライアンスのステータスインジケータの表示"

ハードウェアの登録

アプライアンスハードウェアを登録するとサポートを受けられるようになります。

手順

1. アプライアンスのシャーシのシリアル番号を確認します。

   この番号は、納品書や確認用 E メールで確認できるほか、開梱したアプライアンスにも記載されています。

2. NetApp Support Siteにアクセスします "mysupport.netapp.com"。
3. ハードウェアの登録が必要かどうかを確認します。

| ユーザのタイプとアクセス方法 | 実行する手順 |
| --- | --- |
| ネットアップの既存のお客様 | a. ユーザ名とパスワードを使用してサインインします。<br>b. [ 製品 **>*My Products** ] を選択します。<br>c. 新しいシリアル番号が表示されていることを確認します。<br>d. 表示されていない場合は、ネットアップの新規のお客様向けの手順に従ってください。 |
| ネットアップの新規のお客様 | a. [ 今すぐ登録 ] をクリックしてアカウントを作成します。<br>b. [**Products**>*Register Products*] を選択します。<br>c. 製品のシリアル番号と要求された詳細情報を入力します。<br>登録が承認されると、必要なソフトウェアをダウンロードできます。承認プロセスには最大 24 時間かかる場合があります。 |

キャビネットまたはラックへのアプライアンスの設置（**SG100**および**SG1000**）

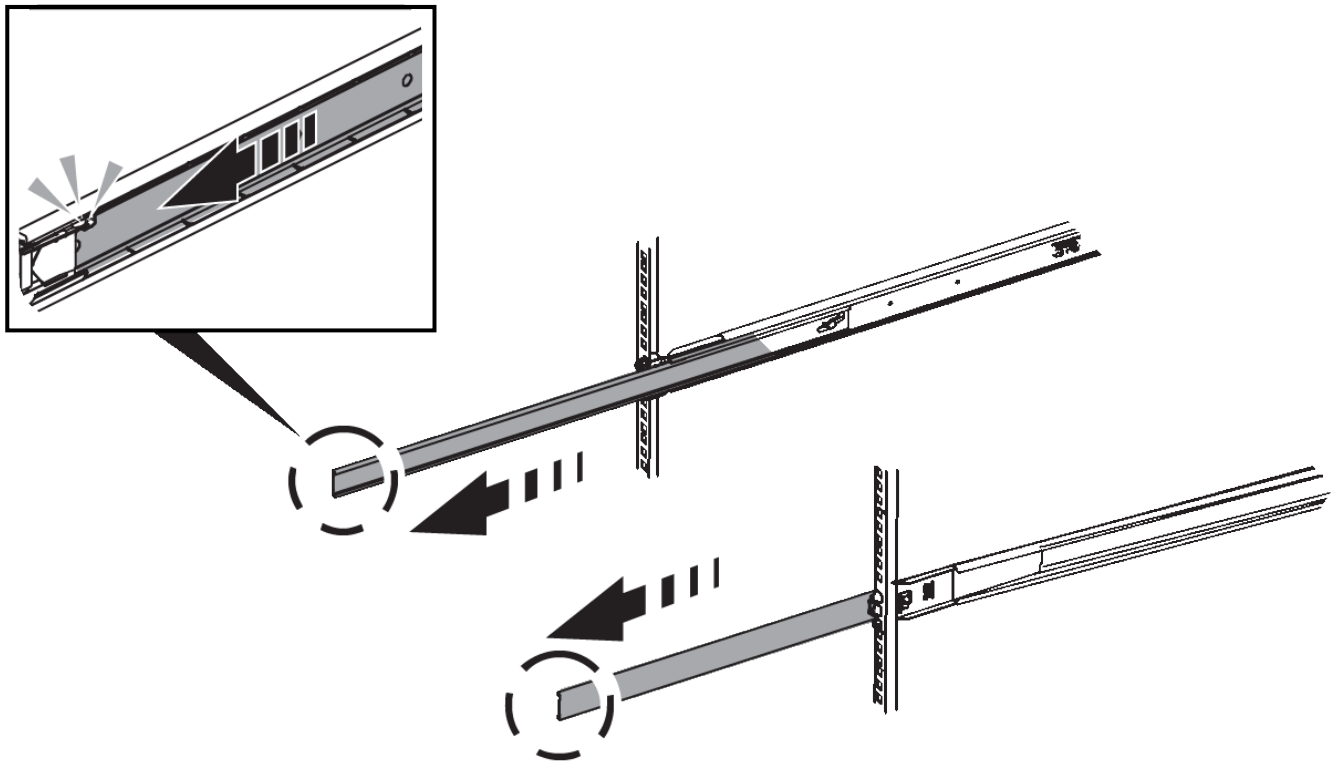
## キャビネットまたはラックにアプライアンス用のレール 1 組を取り付け、レール上にアプライアンスをスライドさせます。

必要なもの

- 同梱されている安全上の注意に関するドキュメントを確認し、ハードウェアの移動と設置に関する注意事項を理解しておきます。
- レールキットに手順書が同梱されていることを確認します。

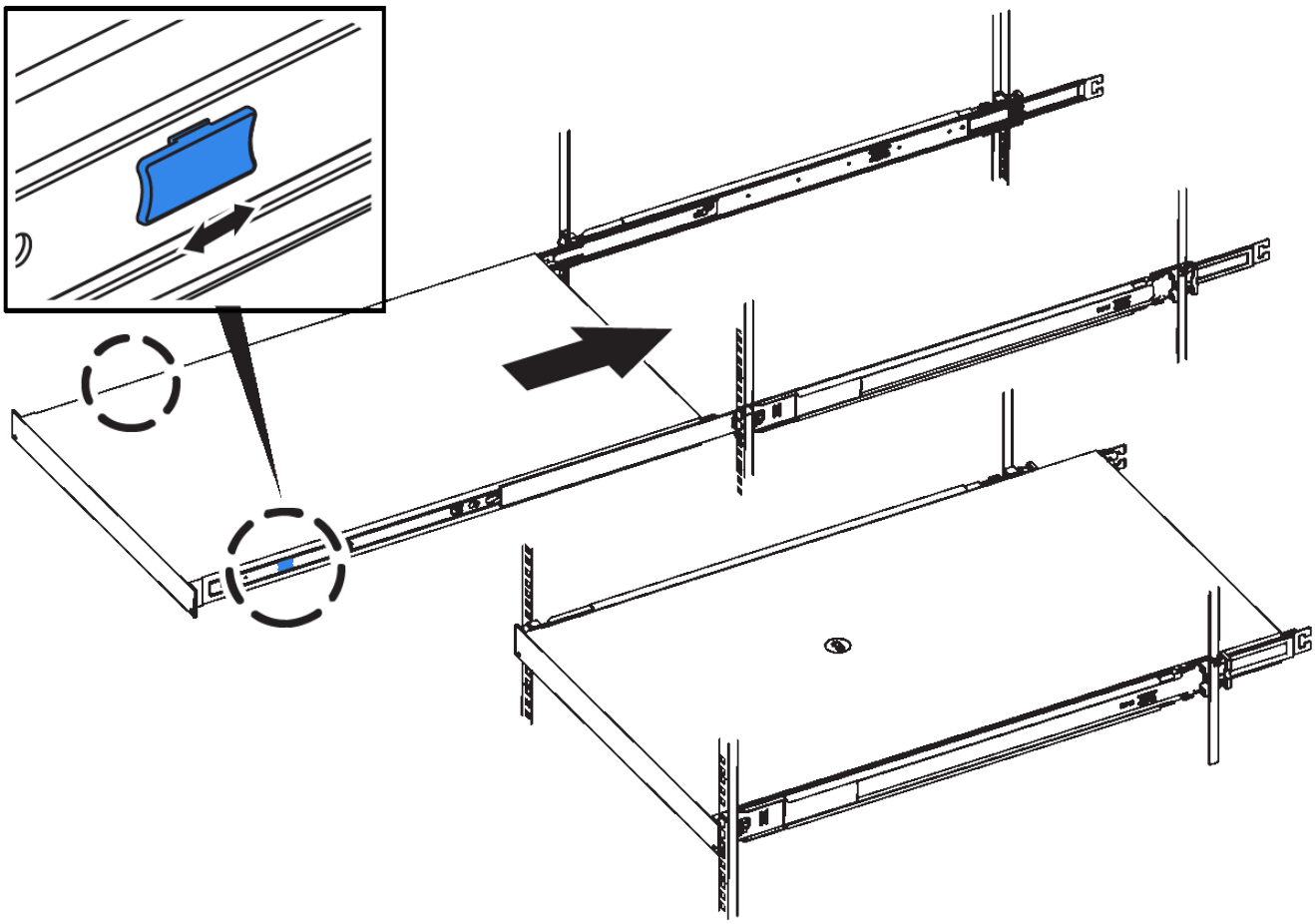
手順

1. キャビネットまたはラックにレールを取り付ける際には、レールキットの手順書に慎重に従ってください。
2. キャビネットまたはラックに取り付けた 2 本のレールで、カチッという音がするまでレールの可動部分を伸ばします。



3. アプライアンスをレールに挿入します。
4. キャビネットまたはラックにアプライアンスをスライドさせます。

   アプライアンスをこれ以上動かすことができない場合は、シャーシの両側にある青いラッチを引いて、アプライアンスを奥までスライドさせます。



アプライアンスの電源を入れるまでは、前面ベゼルを取り付けないでください。

アプライアンス**SG100**および**SG1000**のケーブル接続

## アプライアンスの管理ポートをサービスラップトップに接続し、アプライアンスのネットワークポートを、 StorageGRID のグリッドネットワークとオプションのクライアントネットワークに接続する必要があります。

必要なもの

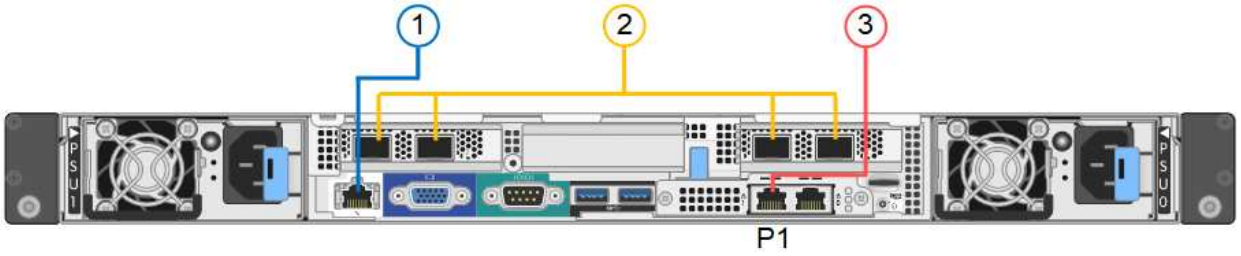
- 管理ポートを接続するための RJ-45 イーサネットケーブルを用意しておきます。
- ネットワークポートに次のいずれかを設定しておきます。これらはアプライアンスには付属していません。
  - 4 つのネットワークポートを接続するための TwinAx ケーブルを 1~4 本。
  - ポートに光ケーブルを使用する場合は、 SG100 用に SFP+ または SFP28 トランシーバを 1~4 個。
  - SG1000 のポートに光ケーブルを使用する場合は、 QSFP+ または QSFP28 トランシーバを 1~4 個。

* レーザー被ばくのリスク * - SFP または QSFP トランシーバを分解したり、部品を取り外したりしないでください。レーザー被ばくのおそれがあります。

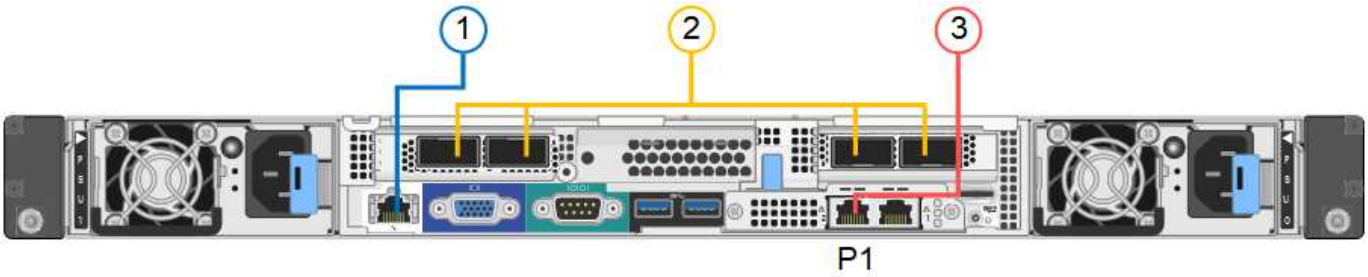
このタスクについて

次の図は、アプライアンス背面のポートを示しています。

- SG100 ポート接続 *




- SG1000 ポートの接続 *




| | ポート | ポートのタイプ | 機能 |
|---|---|---|---|
| 1. | アプライアンスの BMC 管理ポート | 1GbE （ RJ-45 ） | BMC インターフェイスにアクセスするネットワークに接続します。 |
| 2. | アプライアンスの 4 つのネットワーク・ポート | • SG100 ： 10 / 25GbE<br>• SG1000 の場合： 10 / 25 / 40 / 100GbE | StorageGRID のグリッドネットワークおよびクライアントネットワークに接続します。 |
| 3. | アプライアンスの管理ネットワーク・ポート（図の P1 ） | 1GbE （ RJ-45 ）<br>• 重要： * このポートは 1000BASE-T / 全二重でのみ動作し、 10 メガビットまたは 100 メガビットの速度はサポートしません。 | アプライアンスを StorageGRID の管理ネットワークに接続します。 |

| | ポート | ポートのタイプ | 機能 |
|---|---|---|---|
| 3. | アプライアンスの右端の RJ-45 ポート | 1GbE （ RJ-45 ）<br>• 重要： * このポートは 1000BASE-T / 全二重でのみ動作し、 10 メガビットまたは 100 メガビットの速度はサポートしません。 | • 管理ネットワークへの冗長接続が必要な場合は、管理ポート 1 とボンディングできます。<br>• 一時的なローカルアクセス用（ IP 169.254.0.1 ）に空けておくことができます。<br>• DHCP によって割り当てられた IP アドレスを使用できない場合は、設置時にアプライアンスをサービスラップトップに接続するためにを使用できます。 |

手順

1. イーサネットケーブルを使用して、アプライアンスの BMC 管理ポートを管理ネットワークに接続します。

   この接続はオプションですが、サポート用に接続することを推奨します。

2. アプライアンスのネットワークポートを、 TwinAx ケーブル、または光ケーブルとトランシーバを使用して、適切なネットワークスイッチに接続します。

   4 つのネットワークポートで同じリンク速度を使用する必要があります。ハードウェアおよびリンク速度に応じた必要な機器については、次の表を参照してください。

| **SG100** リンク速度（ **GbE** ） | 必要な機器 |
|---|---|
| 10. | SFP+ トランシーバ |
| 25 | SFP28 トランシーバ |
| SG1000 リンク速度（ GbE ） | 必要な機器 |
| 10. | QSA および SFP+ トランシーバ |
| 25 | QSA および SFP28 トランシーバ |
| 40 | QSFP+ トランシーバ |
| 100 | QFSP28 トランシーバ |

   ◦ 固定ポートボンディングモード（デフォルト）を使用する場合は、次の表のように各ポートを StorageGRID のグリッドネットワークまたはクライアントネットワークに接続します。

| ポート | 接続先 |
| --- | --- |
| ポート 1 | クライアントネットワーク（オプション） |
| ポート 2 | Grid ネットワーク |
| ポート 3 | クライアントネットワーク（オプション） |
| ポート 4. | Grid ネットワーク |

- アグリゲートポートボンディングモードを使用する場合は、 1 つ以上のネットワークポートを 1 つ以上のスイッチに接続します。単一点障害を回避するために、 4 つのポートのうち少なくとも 2 つを接続する必要があります。1 つの LACP ボンドに複数のスイッチを使用する場合は、スイッチが MLAG または同等の機能をサポートしている必要があります。

3. StorageGRID の管理ネットワークを使用する場合は、アプライアンスの管理ネットワークポートをイーサネットケーブルで管理ネットワークに接続します。

電源コードの接続と電源の投入（**SG100**および**SG1000**）

## ネットワーク・ケーブルを接続したら、アプライアンスに電源を投入できます。

手順

1. アプライアンスの 2 つ電源装置のそれぞれに電源コードを接続します。
2. これらの 2 本の電源コードを、キャビネットまたはラック内の別々の配電ユニット（ PDU ）に接続します。
3. アプライアンス前面の電源ボタンが青色に点灯していない場合は、ボタンを押してアプライアンスの電源をオンにします。

   電源投入プロセス中は、電源ボタンを再度押さないでください。

4. エラーが発生した場合は、問題を修正します。
5. アプライアンスに前面ベゼルを取り付けます。

関連情報

"SG100およびSG1000アプライアンスのステータスインジケータの表示"

**SG100**および**SG1000**アプライアンスのステータスインジケータの表示

## アプライアンスには、アプライアンスコントローラと 2 本の SSD のステータスを確認するためのインジケータが搭載されています。

アプライアンスのインジケータとボタン

| | 表示 | 状態 |
|---|---|---|
| 1. | 電源ボタン | • 青色：アプライアンスの電源がオンになっています。<br>• Off ：アプライアンスの電源がオフになっています。 |
| 2. | リセットボタン | このボタンを使用して、コントローラのハードリセットを実行します。 |
| 3. | 識別ボタン | このボタンは、点滅、点灯、または消灯に設定できます。<br>• 青、点滅：キャビネットまたはラック内のアプライアンスを示します。<br>• 青、点灯：キャビネットまたはラック内のアプライアンスを示します。<br>• 消灯：キャビネットまたはラック内のアプライアンスを目視で識別できません。 |
| 4. | アラーム LED | • 黄色、点灯：エラーが発生しました。<br>• 注： * ブート時のコードとエラーコードを確認するには、 BMC インターフェイスにアクセスする必要があります。<br>• 消灯：エラーはありません。 |

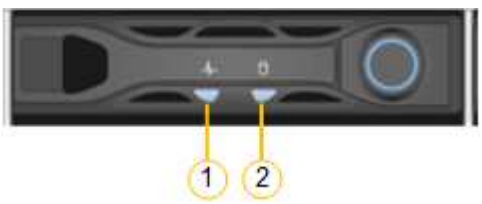
一般的なブートコード

アプライアンスのブート時やハードリセット後に、次の処理が実行されます。

1. ベースボード管理コントローラ（ BMC ）が、ブート処理のコード（発生したエラーを含む）を記録します。
2. 電源ボタンが点灯します。
3. ブート中にエラーが発生した場合は、アラーム LED が点灯します。

   ブート時のコードとエラーコードを表示するには、 BMC インターフェイスにアクセスする必要があります。

**SSD** インジケータ



| LED | 表示 | 状態 |
| --- | --- | --- |
| 1. | ドライブのステータス / 障害 | • 青（点灯）：ドライブはオンラインです<br>• 黄色（点滅）：ドライブ障害<br>• 消灯：スロットが空です |
| 2. | ドライブがアクティブです | 青（点滅）：ドライブにアクセス中です |

関連情報

"ハードウェアの設置のトラブルシューティング"

"BMCインターフェイスを設定しています"

## StorageGRID 接続を設定しています

サービスアプライアンスをノードとして StorageGRID システムに導入するには、アプライアンスと使用するネットワークの間の接続を設定する必要があります。ネットワークを設定するには、サービスアプライアンスにプリインストールされている StorageGRID アプライアンスインストーラにアクセスします。

手順

- "StorageGRID アプライアンスインストーラへのアクセス"
- "StorageGRID アプライアンスインストーラのバージョンの確認とアップグレード"
- "ネットワークリンクの設定（SG100およびSG1000）"
- "StorageGRID IPアドレスを設定しています"
- "ネットワーク接続の確認"
- "ポートレベルのネットワーク接続の確認"

### StorageGRID アプライアンスインストーラへのアクセス

アプライアンスと 3 つの StorageGRID ネットワーク（グリッドネットワーク、管理ネットワーク（オプション）、クライアントネットワーク（オプション））間の接続を設定するには、 StorageGRID アプライアンスインストーラにアクセスする必要があります。

必要なもの

- StorageGRID 管理ネットワークに接続できる管理クライアントを使用している必要があります。
- クライアントにサポートされているWebブラウザをインストールしておきます。
- 使用するすべての StorageGRID ネットワークにサービスアプライアンスを接続しておきます。
- これらのネットワークでのサービスアプライアンスの IP アドレス、ゲートウェイ、およびサブネットを確認しておきます。

- 使用するネットワークスイッチを設定しておきます。

このタスクについて

StorageGRID アプライアンスインストーラに最初にアクセスするときは、 DHCP によってサービスアプライアンスの管理ネットワークポートに割り当てられた IP アドレスを使用するか（管理ネットワークに接続されている場合）、サービスラップトップをサービスアプライアンスに直接接続できます。

手順

1. 可能であれば、サービスアプライアンスの管理ネットワークポートの DHCP アドレスを使用して StorageGRID アプライアンスインストーラにアクセスしてください。

   - SG100 管理ネットワーク・ポート *

   - SG1000 管理ネットワークポート *

   a. serrvices アプライアンスの前面にある MAC アドレスラベルを確認し、管理ネットワークポートの MAC アドレスを特定します。

      MAC アドレスラベルには、 BMC 管理ポートの MAC アドレスが記載されています。

   管理ネットワークポートの MAC アドレスを特定するには、ラベルに記載された 16 進数に * 2 * を追加する必要があります。たとえば、ラベルに記載されている MAC アドレスの末尾が * 09 * の場合、管理ポートの MAC アドレスの末尾は * 0B * となります。ラベルに記載された MAC アドレスの末尾が * （ *y* ） FF* の場合、管理ポートの MAC アドレスの末尾は * （ *y*+1 ） 01 * となります。この計算を簡単に行うには、 Windows で Calculator を開き、 Programmer モードに設定して Hex を選択し、 MAC アドレスを入力してから、 **+2=** と入力します。

   a. MAC アドレスをネットワーク管理者に伝え、管理者が管理ネットワークでのアプライアンスの DHCP アドレスを確認できるようにします。

   b. クライアントから、StorageGRID アプライアンスインストーラのURLとして「+」を入力します
      **`https://services-appliance_IP:8443`**

      の場合 `*services-appliance_IP*`DHCPアドレスを使用してください。

   c. セキュリティアラートが表示された場合は、ブラウザのインストールウィザードを使用して証明書を表示およびインストールします。

      次回この URL にアクセスしたときに、アラートは表示されません。

   StorageGRID アプライアンスインストーラのホームページが表示されます。このページに最初にアクセスしたときに表示される情報とメッセージは、アプライアンスと StorageGRID ネットワークの現在の接続状況によって異なります。エラーメッセージが表示された場合は、以降の手順で解決されます。

2. DHCP を使用して IP アドレスを取得できない場合は、リンクローカル接続を使用して StorageGRID アプライアンスインストーラにアクセスします。

a. イーサネットケーブルを使用して、サービスラップトップをサービスアプライアンスの右端の RJ-45 ポートに直接接続します。

- SG100 リンクローカル接続 *

- SG1000 リンクローカル接続 *

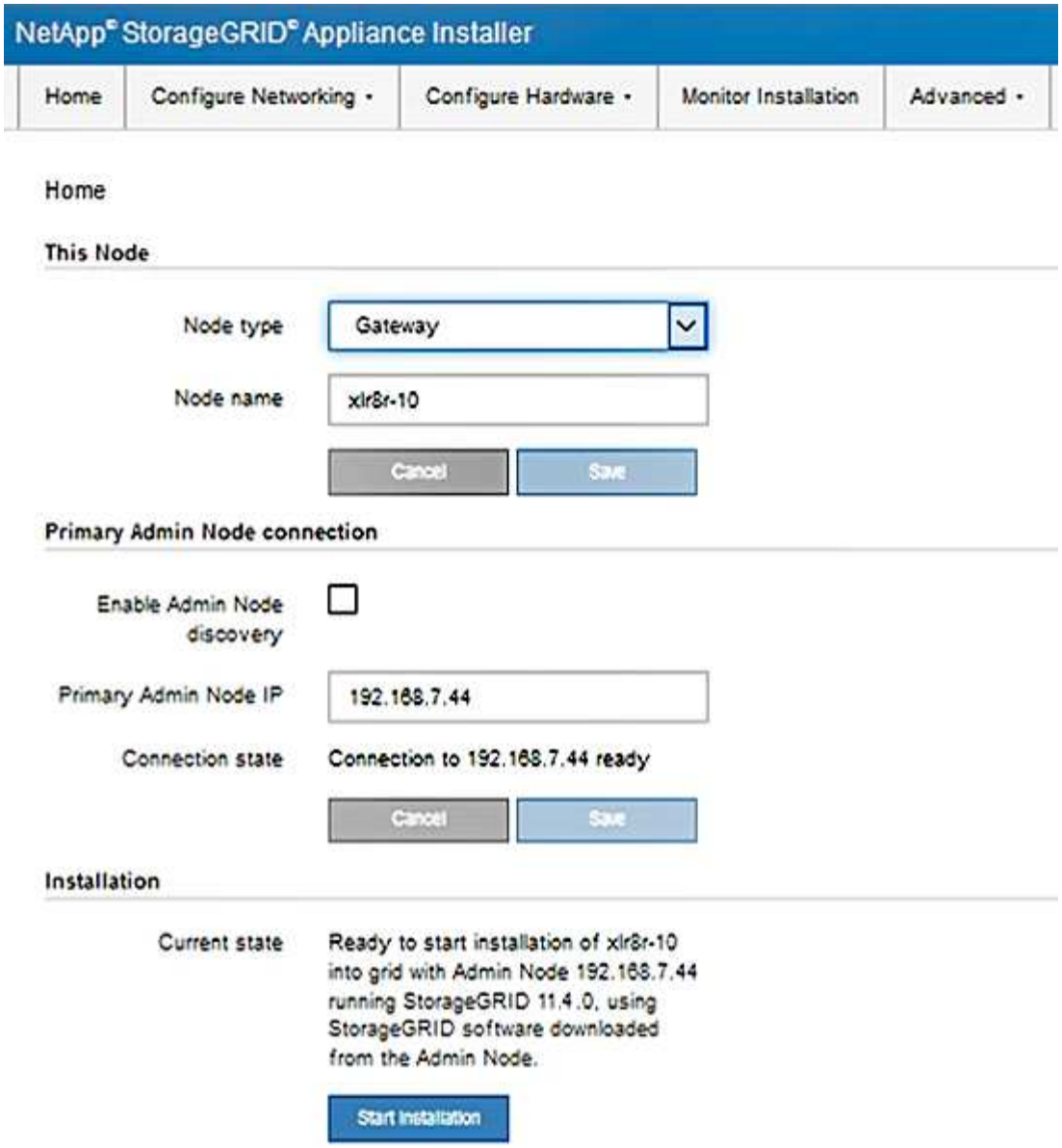
b. Web ブラウザを開きます。

c. StorageGRID アプライアンスインストーラのURLに+を入力します
**`https://169.254.0.1:8443`**

StorageGRID アプライアンスインストーラのホームページが表示されます。このページに最初にアクセスしたときに表示される情報とメッセージは、アプライアンスと StorageGRID ネットワークの現在の接続状況によって異なります。エラーメッセージが表示された場合は、以降の手順で解決されます。

> リンクローカル接続でホームページにアクセスできない場合は、サービスラップトップのIPアドレスをに設定します `169.254.0.2`をクリックして、もう一度やり直してください。

3. ホームページに表示されたメッセージを確認し、必要に応じてリンク設定と IP 設定を行います。




関連情報

"Web ブラウザの要件"

**StorageGRID** アプライアンスインストーラのバージョンの確認とアップグレード

StorageGRID のすべての機能がサポートされるようにするには、アプライアンスの StorageGRID アプライアンスインストーラのバージョンと StorageGRID システムにインストールされているソフトウェアのバージョンが一致している必要があります。

必要なもの

StorageGRID アプライアンスインストーラにアクセスしておきます。

このタスクについて

StorageGRID アプライアンスは、 StorageGRID アプライアンスインストーラがプリインストールされた状態で出荷されます。最近アップグレードした StorageGRID システムにアプライアンスを追加する場合は、そのアプライアンスを新しいノードとしてインストールする前に、 StorageGRID アプライアンスインストーラの

手動アップグレードが必要になることがあります。

新しい StorageGRID バージョンにアップグレードすると、 StorageGRID アプライアンスインストーラが自動的にアップグレードされます。インストールされているアプライアンスノードでは、 StorageGRID アプライアンスインストーラをアップグレードする必要はありません。この手順 が必要になるのは、以前のバージョンの StorageGRID アプライアンスインストーラを搭載したアプライアンスをインストールする場合のみです。

手順

1. StorageGRID アプライアンス・インストーラから、 * アドバンスト * > * アップグレード・ファームウェア * を選択します。
2. 現在のファームウェアバージョンとStorageGRID システムにインストールされているソフトウェアバージョンを比較します（Grid Managerから* Help **>** About *を選択します）。

   2 つのバージョンの 2 桁目の数字が一致している必要があります。たとえば、StorageGRID システムでバージョン11.* 5 。***x*.y_y__**を実行している場合、**StorageGRID** アプライアンスインストーラのバージョンは**3.** 5 *._z_にする必要があります。

3. アプライアンスに StorageGRID アプライアンスインストーラの下位バージョンがインストールされている場合は、 StorageGRID のネットアップのダウンロードページにアクセスします。

   "ネットアップのダウンロード： StorageGRID"

   ネットアップアカウントのユーザ名とパスワードを使用してサインインします。

4. StorageGRID アプライアンス * 対応するバージョンのサポート・ファイルと対応するチェックサム・ファイルをダウンロードします。

   StorageGRID アプライアンスファイルのサポートファイルは、です `.zip` すべてのStorageGRID アプライアンスモデルの最新および以前のファームウェアバージョンを、各コントローラタイプのサブディレクトリに格納してアーカイブする。

   StorageGRID アプライアンスファイルのサポートファイルをダウンロードしたら、を展開します `.zip` StorageGRID アプライアンスインストーラのインストールに関する重要な情報については、READMEファイルをアーカイブして参照してください。

5. StorageGRID アプライアンスインストーラのファームウェアのアップグレードページの手順に従って、次の手順を実行します。
   a. コントローラタイプとチェックサムファイルに適したサポートファイル（ファームウェアイメージ）をアップロードします。
   b. 非アクティブなパーティションをアップグレードします。
   c. パーティションを再起動してスワップします。
   d. 2番目のパーティションをアップグレードします。

関連情報

"StorageGRID アプライアンスインストーラへのアクセス"

ネットワークリンクの設定（**SG100**および**SG1000**）

## アプライアンスをグリッドネットワーク、クライアントネットワーク、および管理ネッ

トワークに接続するために使用するポートのネットワークリンクを設定できます。リンク速度およびポートボンディングモードとネットワークボンディングモードを設定できます。

必要なもの

- ケーブルのタイプとリンク速度に応じて、必要な追加の機器を入手しておきます。
- 選択した速度をサポートするスイッチにネットワークポートを接続しておきます。

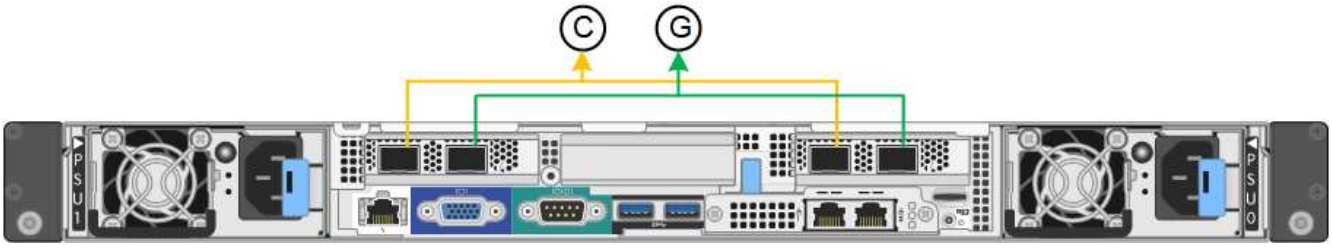
アグリゲートポートボンディングモード、 LACP ネットワークボンディングモード、または VLAN タギングを使用する場合

- アプライアンスのネットワークポートを、 VLAN と LACP をサポートするスイッチに接続しておきます。
- 複数のスイッチを LACP ボンドに加える場合は、 Multi-Chassis Link Aggregation （ MLAG ）グループまたは同等の機能をサポートするスイッチを使用します。
- VLAN 、 LACP 、 MLAG などを使用するようにスイッチを設定する方法について理解しておく必要があります。
- 各ネットワークに使用する一意の VLAN タグを確認しておきます。この VLAN タグが各ネットワークパケットに追加され、ネットワークトラフィックが正しいネットワークにルーティングされます。

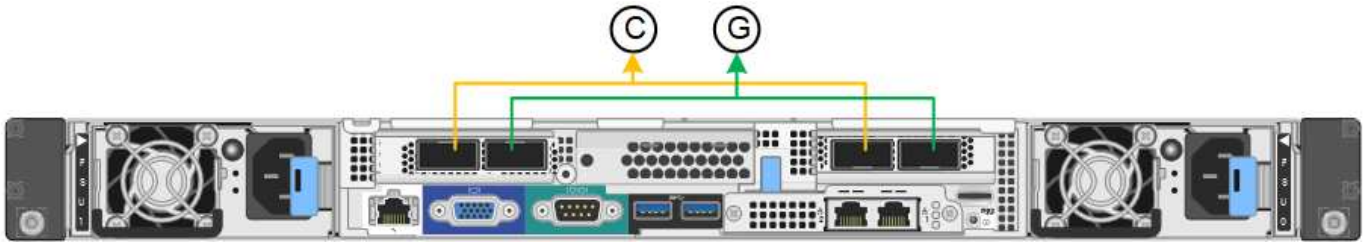
このタスクについて

次の図では、 4 つのネットワークポートが固定ポートボンディングモードでボンディングされています（デフォルトの構成）。

- SG100 固定ポートボンディングモード *



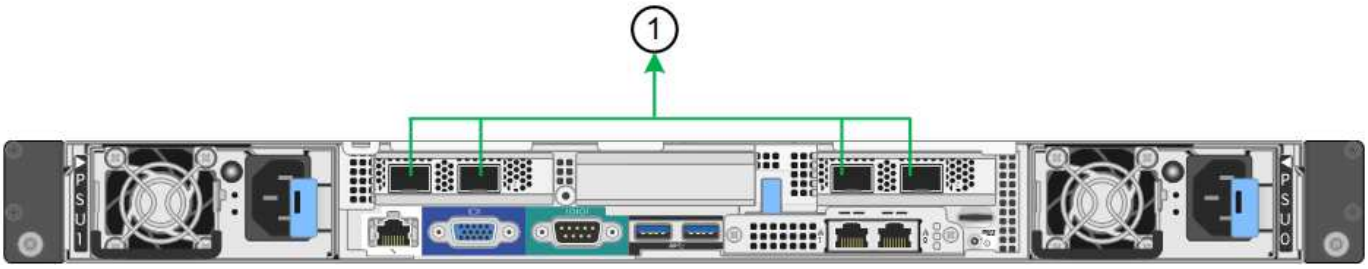

- SG1000 の固定ポートボンディングモード *



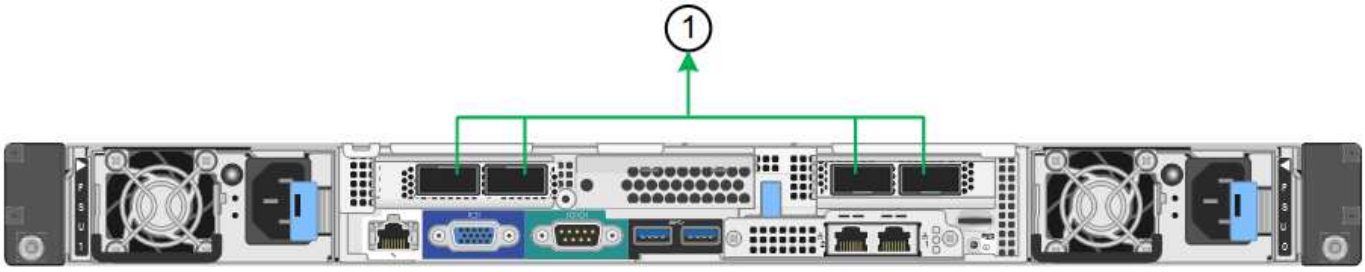

| | ボンディングされるポート |
|---|---|
| C | このネットワークを使用する場合、ポート 1 とポート 3 がクライアントネットワーク用にボンディングされます。 |
| G | ポート 2 とポート 4 がグリッドネットワーク用にボンディングされます。 |

次の図では、 4 つのネットワークポートが Aggregate ポートボンディングモードでボンディングされています。

- SG100 アグリゲートポートボンディングモード *




- SG1000 Aggregate ポートボンディングモード *




| | ボンディングされるポート |
|---|---|
| 1. | 4 つのポートすべてを 1 つの LACP ボンドにグループ化して、すべてのポートをグリッドネットワークとクライアントネットワークのトラフィックに使用できるようにします。 |

次の表に、 4 つのネットワークポートを設定するためのオプションをまとめます。デフォルトの設定は太字で示しています。デフォルト以外の設定を使用する場合にのみ、 Link Configuration ページで設定を行う必要があります。

LACP 送信ハッシュポリシーは、デフォルトで layer2+3 モードに設定されています。必要に応じて、グリッド管理 API を使用して layer3+4 モードに変更できます。

- * 固定（デフォルト）ポートボンディングモード *

| ネットワークボンディングモード | クライアントネットワークが無効な場合（デフォルト） | クライアントネットワークが有効になりました |
| --- | --- | --- |
| アクティブ/バックアップ（デフォルト） | • ポート 2 と 4 がグリッドネットワークにアクティブ / バックアップボンドを使用します。<br>• ポート 1 と 3 は使用されません。<br>• VLAN タグはオプションです。 | • ポート 2 と 4 がグリッドネットワークにアクティブ / バックアップボンドを使用します。<br>• ポート 1 と 3 がクライアントネットワークに Active-Backup ボンドを使用します。<br>• ネットワーク管理者用に、両方のネットワークに VLAN タグを指定できます。 |
| LACP （ 802.3ad ） | • ポート 2 と 4 がグリッドネットワークに LACP ボンドを使用します。<br>• ポート 1 と 3 は使用されません。<br>• VLAN タグはオプションです。 | • ポート 2 と 4 がグリッドネットワークに LACP ボンドを使用します。<br>• ポート 1 と 3 がクライアントネットワークに LACP ボンドを使用します。<br>• ネットワーク管理者用に、両方のネットワークに VLAN タグを指定できます。 |

• * アグリゲートポートボンディングモード *

| ネットワークボンディングモード | クライアントネットワークが無効な場合（デフォルト） | クライアントネットワークが有効になりました |
| --- | --- | --- |
| LACP （ 802.3ad ）のみ | • ポート 1~4 がグリッドネットワークに単一の LACP ボンドを使用します。<br>• 単一の VLAN タグでグリッドネットワークのパケットが識別されます。 | • ポート 1~4 がグリッドネットワークとクライアントネットワークに単一の LACP ボンドを使用します。<br>• 2 つの VLAN タグで、グリッドネットワークのパケットとクライアントネットワークのパケットを分離できます。 |

詳細については、サービスアプライアンスの GbE ポートの接続に関する記事を参照してください。

次の図では、 SG100 上の 2 つの 1GbE 管理ポートが管理ネットワーク用に Active-Backup ネットワークボンディングモードでボンディングされています。

次の図では、アプライアンスの 2 つの 1GbE 管理ポートが管理ネットワーク用に Active-Backup ネットワークボンディングモードでボンディングされています。

• SG100 管理ネットワーク・ポートがボンディングされています *

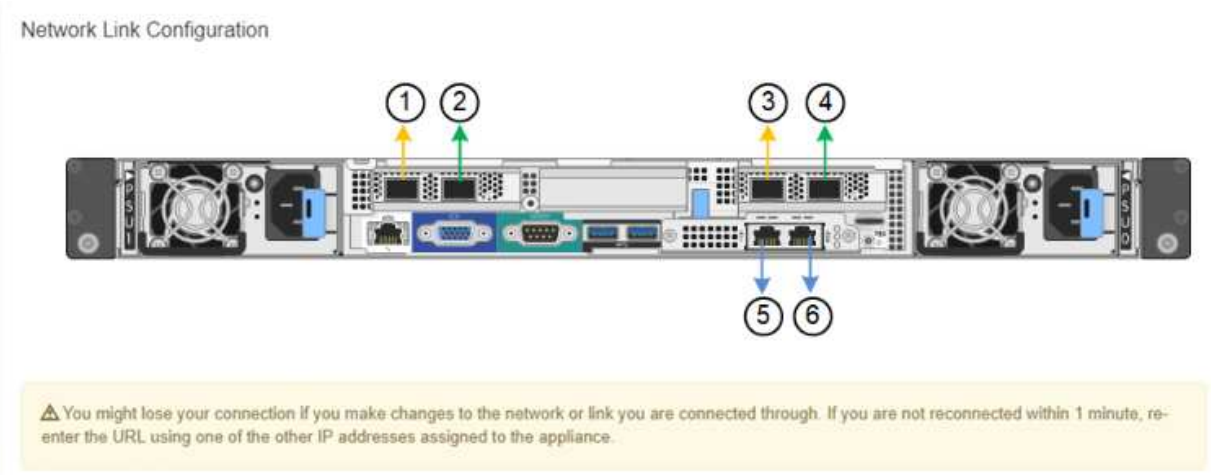
- SG1000 管理ネットワークのポートがボンディングされています *

手順

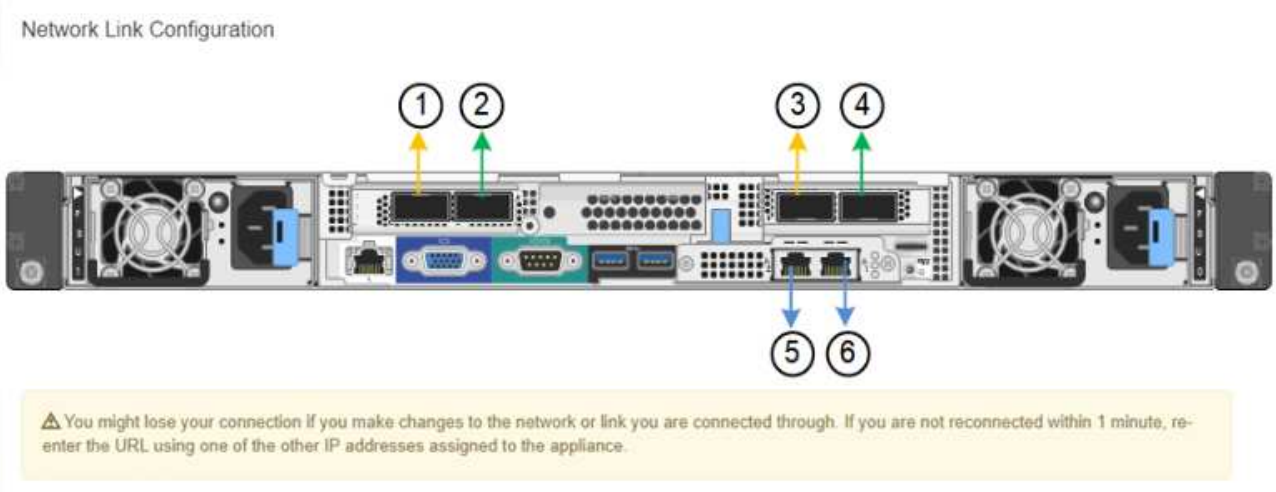
1. StorageGRID アプライアンスインストーラのメニューバーから、 *Configure Networking *>*Link Configuration * をクリックします。

   Network Link Configuration ページには、アプライアンスの図と、ネットワークポートおよび管理ポートの番号が表示されます。

   ◦ SG100 ポート *




   ◦ SG1000 ポート *



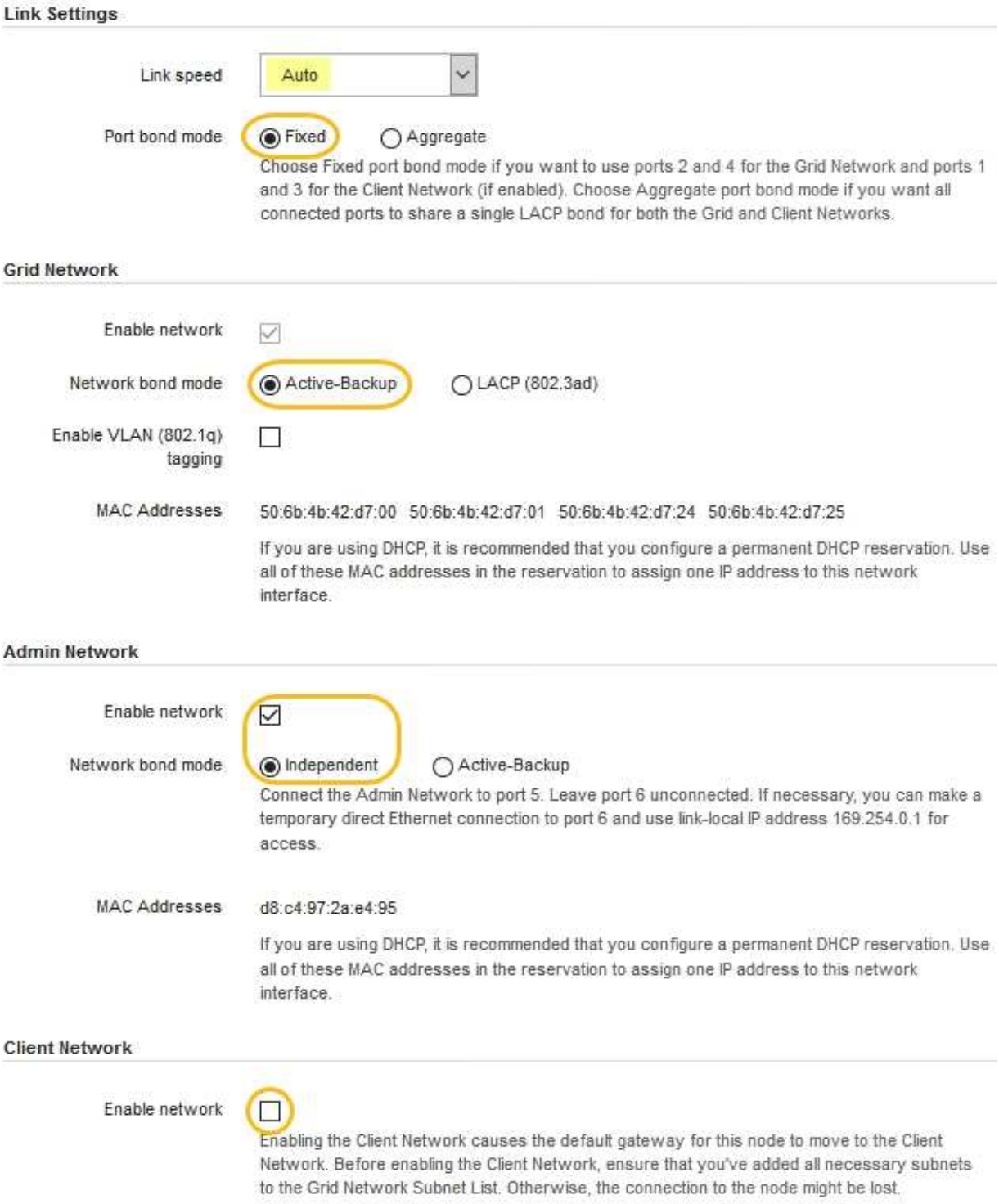

Link Status テーブルには、番号が付けられたポート（ SG1000 を参照）のリンク状態と速度が表示されます。

**Link Status**

| Link | State | Speed (Gbps) |
|---|---|---|
| 1 | Up | 100 |
| 2 | Down | N/A |
| 3 | Down | N/A |
| 4 | Down | N/A |
| 5 | Up | 1 |
| 6 | Up | 1 |

このページに初めてアクセスしたときの動作は次のとおりです。

- * リンク速度 * は * 自動 * に設定されています。
- * ポートボンディングモード * は「 * Fixed 」に設定されます。
- * グリッドネットワークの場合、ネットワークボンディングモード * が「アクティブ / バックアップ」に設定されます。
- 管理ネットワーク * が有効になっており、ネットワークボンディングモードが * Independent * に設定されています。
- クライアントネットワーク * が無効になっています。



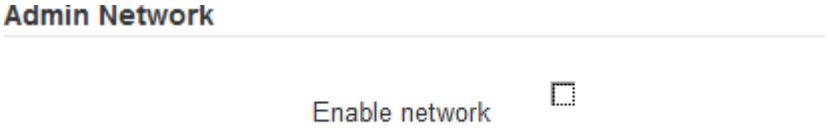

2. [* Link speed * （リンク速度 * ） ] ドロップダウンリストから、ネットワークポートのリンク速度を選択します。

   グリッドネットワークとクライアントネットワークに使用するネットワークスイッチも、この速度をサポートし、この速度に対応するように設定する必要があります。設定されたリンク速度に適したアダプタまたはトランシーバを使用する必要があります。このオプションはリンク速度と前方誤り訂正（ FEC ）モードの両方をリンクパートナーとネゴシエートするため、可能な場合は自動リンク速度を使用します。

3. 使用する StorageGRID ネットワークを有効または無効にします。

グリッドネットワークは必須です。このネットワークは無効にできません。

a. アプライアンスが管理ネットワークに接続されていない場合は、管理ネットワークの * ネットワークを有効にする * チェックボックスの選択を解除します。



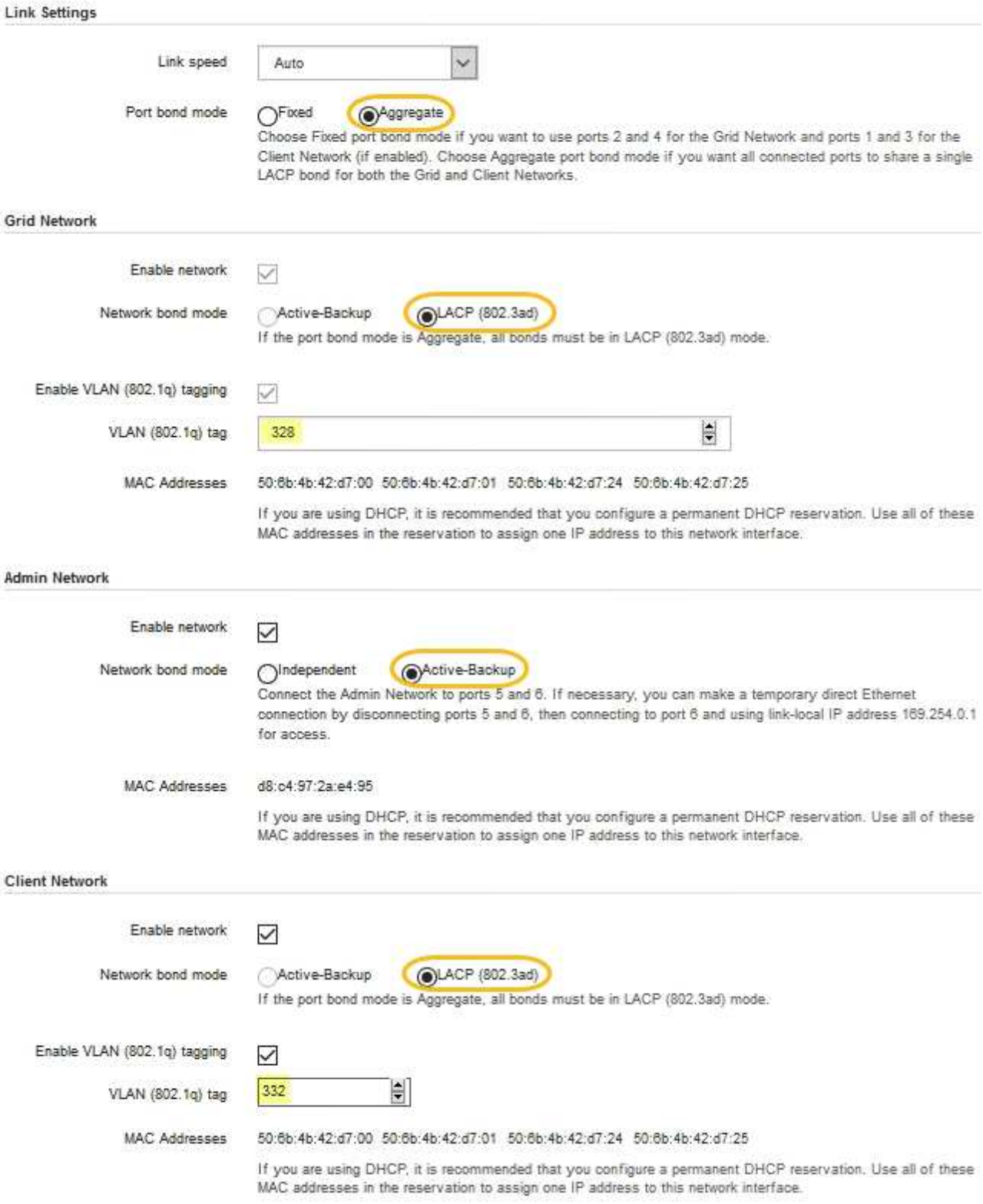

b. アプライアンスがクライアントネットワークに接続されている場合は、クライアントネットワークの * ネットワークを有効にする * チェックボックスをオンにします。

これで、データ NIC ポートでのクライアントネットワークの設定が表示されます。

4. 表を参照して、ポートボンディングモードとネットワークボンディングモードを設定します。

次の例では、次のよう

- * グリッドネットワークとクライアントネットワークでアグリゲート * と * LACP * が選択されました。各ネットワークに一意の VLAN タグを指定する必要があります。値は 0~4095 の間で選択できます。
- * 管理ネットワーク用に選択されたアクティブ / バックアップ * 。




5. 選択に問題がなければ、 * 保存 * をクリックします。

接続しているネットワークまたはリンクを変更すると、接続が失われる可能性があります。1分以内に再接続されない場合は、アプライアンスに割り当てられている他のIPアドレスのいずれかを使用してStorageGRID アプライアンスインストーラのURLを再入力します：+

**`https://services_appliance_IP:8443`**

関連情報

"追加の機器と工具の入手（SG100およびSG1000）"

**StorageGRID IP**アドレスを設定しています

## StorageGRID アプライアンスインストーラを使用して、 StorageGRID のグリッドネットワーク、管理ネットワーク、クライアントネットワークでサービスアプライアンスに使用される IP アドレスとルーティング情報を設定します。

このタスクについて

接続された各ネットワークでアプライアンスの静的 IP を割り当てるか、 DHCP サーバでアドレスの永久リースを割り当てる必要があります。

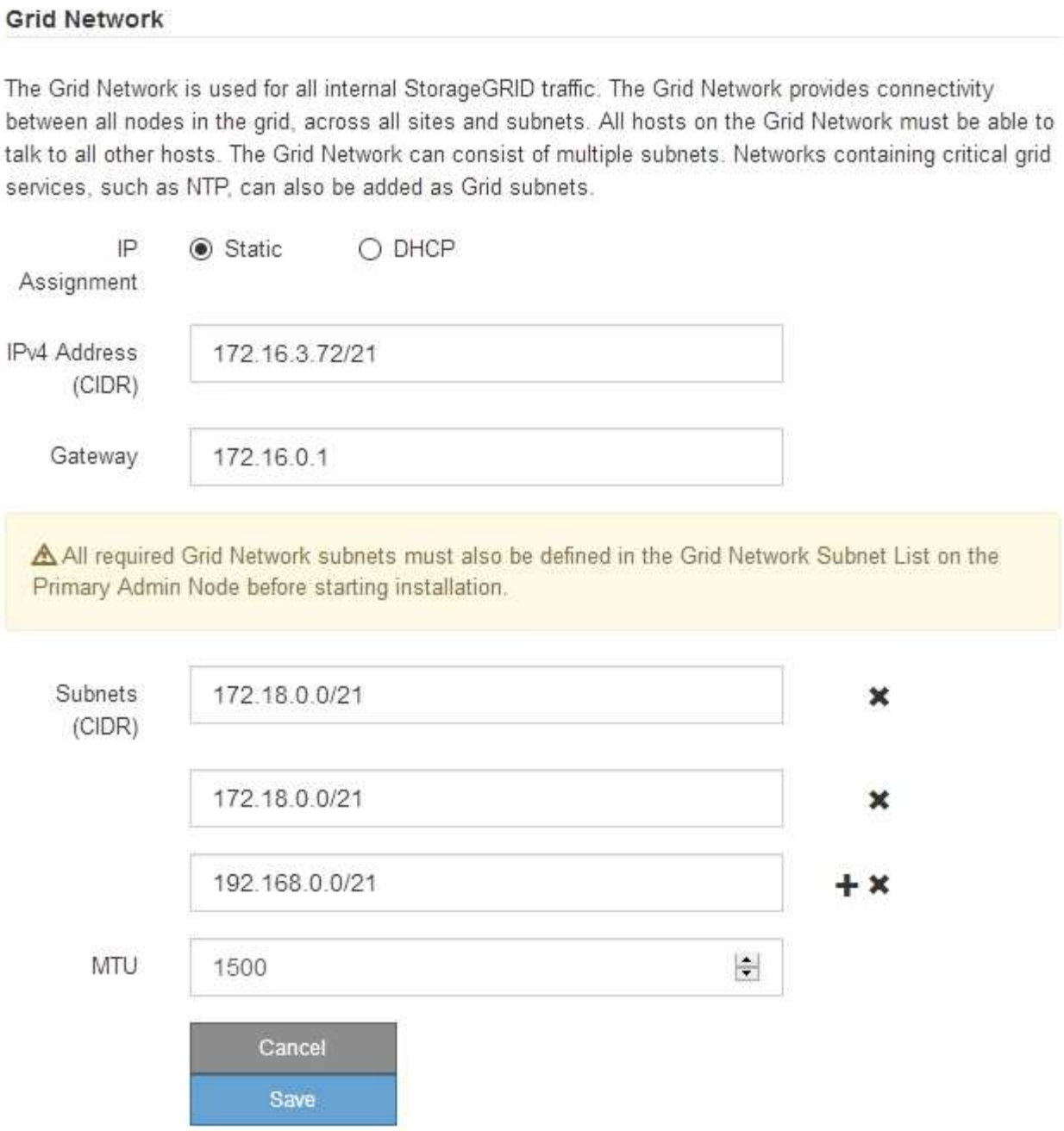
リンク設定を変更する場合は、サービスアプライアンスのリンク設定の変更手順を参照してください。

手順

1. StorageGRID アプライアンスインストーラで、 * ネットワークの設定 * > * IP 構成 * を選択します。

   [IP Configuration] ページが表示されます。

2. グリッドネットワークを設定するには、ページの * グリッドネットワーク * セクションで * 静的 * または * DHCP * のいずれかを選択します。




3. 「 * Static * 」を選択した場合は、次の手順に従ってグリッドネットワークを設定します。
   a. CIDR 表記を使用して静的 IPv4 アドレスを入力します。
   b. ゲートウェイを入力します。

      ネットワークにゲートウェイがない場合は、同じ静的 IPv4 アドレスを再入力します。

   c. ジャンボフレームを使用する場合は、 MTU フィールドを 9000 などのジャンボフレームに適した値に変更します。それ以外の場合は、デフォルト値 1500 のままにします。

      ネットワークの MTU 値は、ノードが接続されているスイッチポートに設定されている値と同じである必要があります。そうしないと、ネットワークパフォーマンスの問題やパケット損失が発生する可能性があります。

ネットワークのパフォーマンスを最大限に高めるには、すべてのノードのグリッドネットワークインターフェイスで MTU 値がほぼ同じになるように設定する必要があります。個々のノードのグリッドネットワークの MTU 設定に大きな違いがある場合は、 * Grid Network MTU mismatch * アラートがトリガーされます。MTU 値はすべてのネットワークタイプで同じである必要はありません。

d. [ 保存（ Save ） ] をクリックします。

IP アドレスを変更すると、ゲートウェイとサブネットのリストも変更される可能性があります。

StorageGRID アプライアンスインストーラへの接続が失われた場合は、割り当てた新しい静的 IP アドレスを使用して URL を再入力します。たとえば、「+」と入力します
`https://services_appliance_IP:8443`

e. グリッドネットワークのサブネットのリストが正しいことを確認します。

グリッドサブネットがある場合は、グリッドネットワークゲートウェイが必要です。指定するすべてのグリッドサブネットが、このゲートウェイ経由でアクセス可能であることが必要です。StorageGRID のインストールを開始するときに、プライマリ管理ノードのグリッドネットワークサブネットリストでこれらのサブネットも定義する必要があります。

デフォルトルートはリストされません。クライアントネットワークが有効になっていない場合は、デフォルトルートがグリッドネットワークゲートウェイを使用します。

- サブネットを追加するには、挿入アイコンをクリックします ➕ アイコン"] をクリックします。
- 使用されていないサブネットを削除するには、削除アイコンをクリックします ✖。

f. [ 保存（ Save ） ] をクリックします。

4. 「 * DHCP * 」を選択した場合は、次の手順に従ってグリッドネットワークを設定します。

a. [**DHCP**] ラジオボタンを選択した後、 [**Save**] をクリックします。

[* IPv4 アドレス * ] 、 [ * ゲートウェイ * ] 、および [ * サブネット * ] フィールドには、自動的に値が入力されます。DHCP サーバが MTU 値を割り当てるように設定されている場合は、 **MTU** フィールドにその値が入力され、フィールドは読み取り専用になります。

Web ブラウザは、 StorageGRID アプライアンスインストーラの新しい IP アドレスに自動的にリダイレクトされます。

b. グリッドネットワークのサブネットのリストが正しいことを確認します。

グリッドサブネットがある場合は、グリッドネットワークゲートウェイが必要です。指定するすべてのグリッドサブネットが、このゲートウェイ経由でアクセス可能であることが必要です。StorageGRID のインストールを開始するときに、プライマリ管理ノードのグリッドネットワークサブネットリストでこれらのサブネットも定義する必要があります。

デフォルトルートはリストされません。クライアントネットワークが有効になっていない場合は、デフォルトルートがグリッドネットワークゲートウェイを使用します。

- サブネットを追加するには、挿入アイコンをクリックします ➕ アイコン"] をクリックします。

- 使用されていないサブネットを削除するには、削除アイコンをクリックします ✖。

c. ジャンボフレームを使用する場合は、 MTU フィールドを 9000 などのジャンボフレームに適した値に変更します。それ以外の場合は、デフォルト値 1500 のままにします。

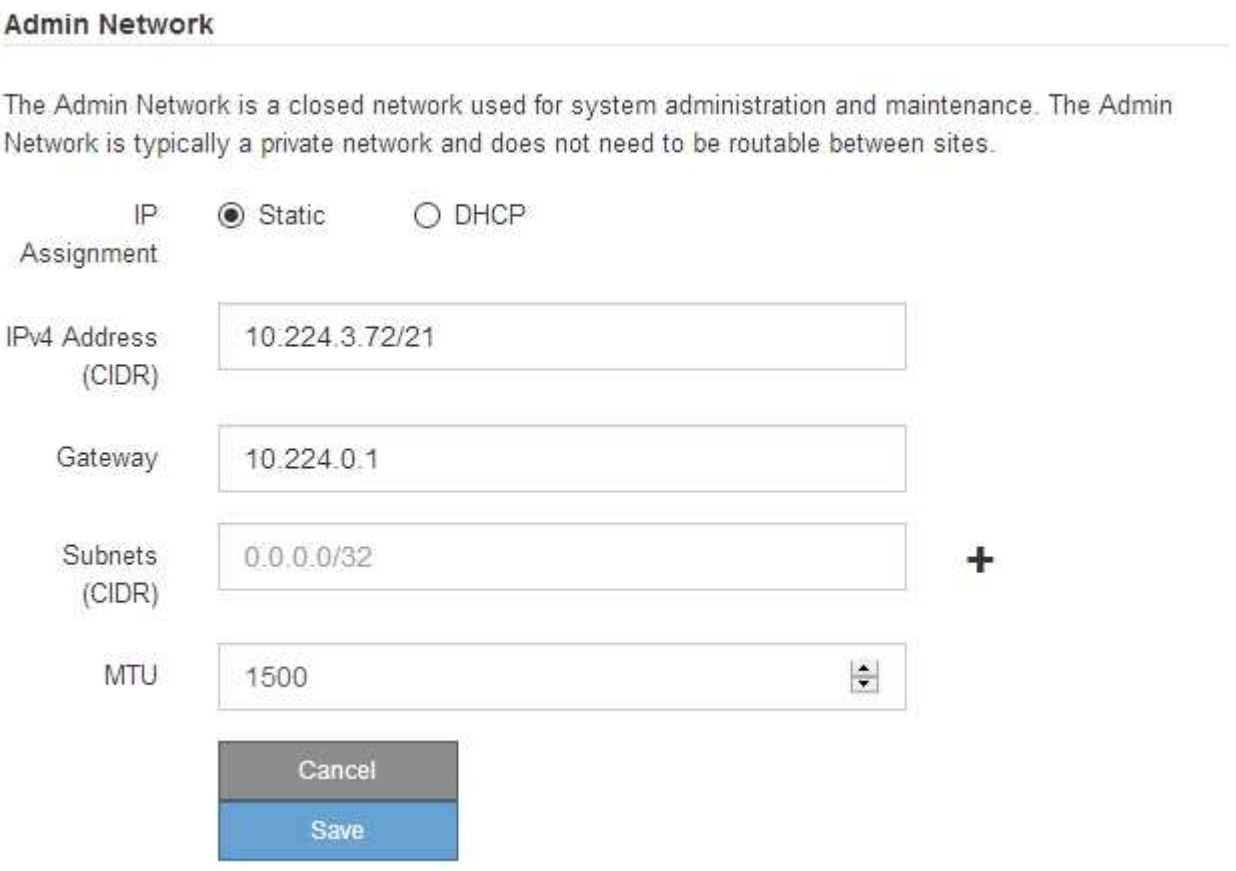
ネットワークの MTU 値は、ノードが接続されているスイッチポートに設定されている値と同じである必要があります。そうしないと、ネットワークパフォーマンスの問題やパケット損失が発生する可能性があります。

ネットワークのパフォーマンスを最大限に高めるには、すべてのノードのグリッドネットワークインターフェイスで MTU 値がほぼ同じになるように設定する必要があります。個々のノードのグリッドネットワークの MTU 設定に大きな違いがある場合は、 * Grid Network MTU mismatch * アラートがトリガーされます。MTU 値はすべてのネットワークタイプで同じである必要はありません。

a. [ 保存（ Save ） ] をクリックします。

5. 管理ネットワークを設定するには、ページの管理ネットワークセクションで * 静的 * または * DHCP * のいずれかを選択します。

管理ネットワークを設定するには、 Link Configuration ページで管理ネットワークを有効にする必要があります。




6. 「 * Static * 」を選択した場合は、次の手順に従って管理ネットワークを設定します。

a. アプライアンスの管理ポート 1 に対して、 CIDR 表記を使用して静的 IPv4 アドレスを入力します。

管理ポート 1 は、アプライアンス右端にある 2 つの 1GbE RJ45 ポートのうち、左側のポートです。

b. ゲートウェイを入力します。

ネットワークにゲートウェイがない場合は、同じ静的 IPv4 アドレスを再入力します。

c. ジャンボフレームを使用する場合は、 MTU フィールドを 9000 などのジャンボフレームに適した値に変更します。それ以外の場合は、デフォルト値 1500 のままにします。

ネットワークの MTU 値は、ノードが接続されているスイッチポートに設定されている値と同じである必要があります。そうしないと、ネットワークパフォーマンスの問題やパケット損失が発生する可能性があります。

d. [ 保存（ Save ） ] をクリックします。

IP アドレスを変更すると、ゲートウェイとサブネットのリストも変更される可能性があります。

StorageGRID アプライアンスインストーラへの接続が失われた場合は、割り当てた新しい静的 IP アドレスを使用して URL を再入力します。たとえば、「+」と入力します
**`https://services_appliance:8443`**

e. 管理ネットワークのサブネットのリストが正しいことを確認します。

指定したゲートウェイを使用してすべてのサブネットにアクセスできることを確認する必要があります。

管理ネットワークゲートウェイを使用するデフォルトルートは作成できません。

- サブネットを追加するには、挿入アイコンをクリックします ➕ アイコン"] をクリックします。
- 使用されていないサブネットを削除するには、削除アイコンをクリックします ✖。

f. [ 保存（ Save ） ] をクリックします。

7. [**DHCP**] を選択した場合は、次の手順に従って管理ネットワークを設定します。

a. [**DHCP**] ラジオボタンを選択した後、 [**Save**] をクリックします。

[* IPv4 アドレス * ] 、 [ * ゲートウェイ * ] 、および [ * サブネット * ] フィールドには、自動的に値が入力されます。DHCP サーバが MTU 値を割り当てるように設定されている場合は、 **MTU** フィールドにその値が入力され、フィールドは読み取り専用になります。

Web ブラウザは、 StorageGRID アプライアンスインストーラの新しい IP アドレスに自動的にリダイレクトされます。

b. 管理ネットワークのサブネットのリストが正しいことを確認します。

指定したゲートウェイを使用してすべてのサブネットにアクセスできることを確認する必要があります。

管理ネットワークゲートウェイを使用するデフォルトルートは作成できません。

- サブネットを追加するには、挿入アイコンをクリックします ➕ アイコン"] をクリックします。

- 使用されていないサブネットを削除するには、削除アイコンをクリックします ✖。

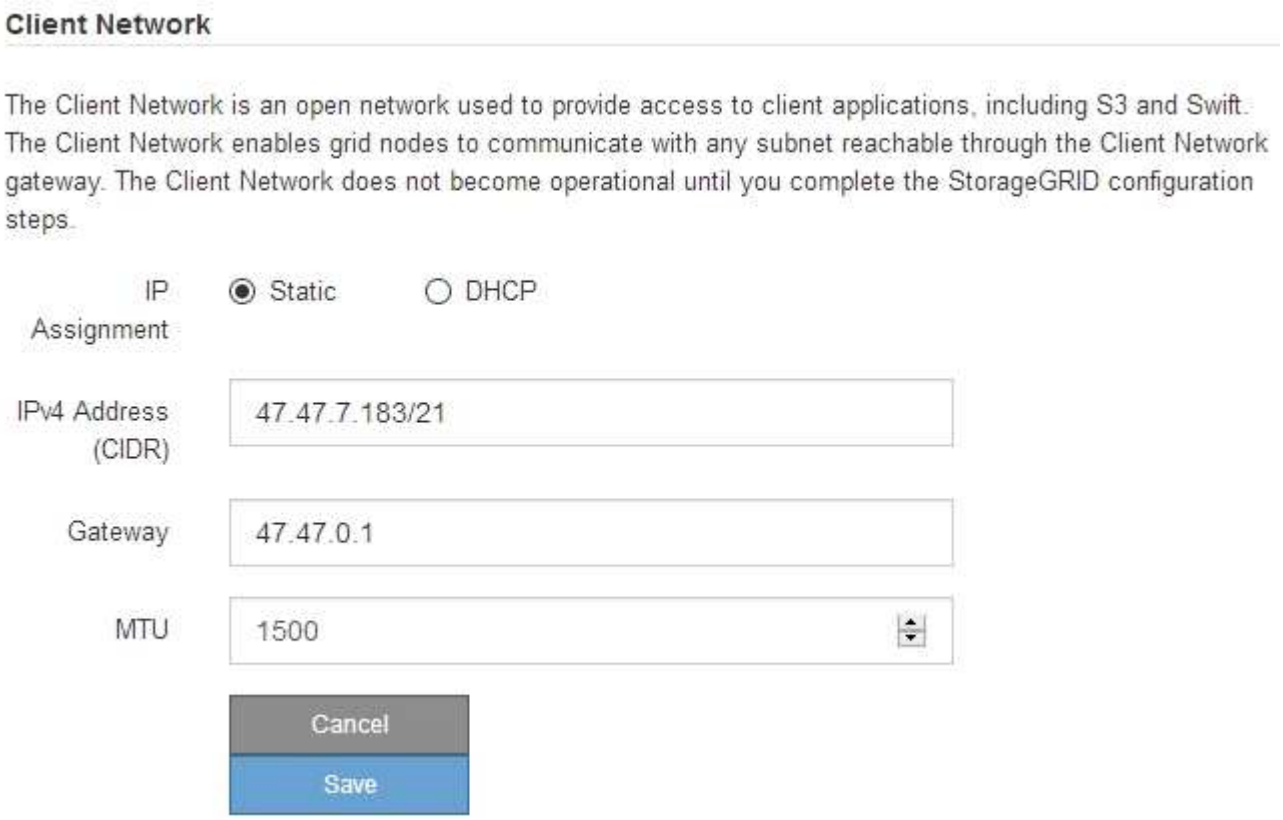
c. ジャンボフレームを使用する場合は、 MTU フィールドを 9000 などのジャンボフレームに適した値に変更します。それ以外の場合は、デフォルト値 1500 のままにします。

> ネットワークの MTU 値は、ノードが接続されているスイッチポートに設定されている値と同じである必要があります。そうしないと、ネットワークパフォーマンスの問題やパケット損失が発生する可能性があります。

d. [ 保存（ Save ） ] をクリックします。

8. クライアントネットワークを設定するには、ページの * クライアントネットワーク * セクションで * 静的 * または * DHCP * のいずれかを選択します。

> クライアントネットワークを設定するには、 Link Configuration ページで Client Network を有効にする必要があります。




9. * Static * を選択した場合は、次の手順に従ってクライアントネットワークを設定します。

a. CIDR 表記を使用して静的 IPv4 アドレスを入力します。

b. [ 保存（ Save ） ] をクリックします。

c. クライアントネットワークゲートウェイの IP アドレスが正しいことを確認します。

> クライアントネットワークが有効になっている場合は、デフォルトルートが表示されます。デフォルトルートはクライアントネットワークゲートウェイを使用し、クライアントネットワークが有効になっている間は別のインターフェイスに移動できません。

d. ジャンボフレームを使用する場合は、 MTU フィールドを 9000 などのジャンボフレームに適した値に変更します。それ以外の場合は、デフォルト値 1500 のままにします。

> ネットワークの MTU 値は、ノードが接続されているスイッチポートに設定されている値と同じである必要があります。そうしないと、ネットワークパフォーマンスの問題やパケット損失が発生する可能性があります。

e. [ 保存（ Save ） ] をクリックします。

10. **[DHCP]** を選択した場合は、次の手順に従ってクライアントネットワークを設定します。

a. **[DHCP]** ラジオボタンを選択した後、 **[Save]** をクリックします。

**[IPv4 Address]** フィールドと **[Gateway]** フィールドが自動的に入力されます。DHCP サーバが MTU 値を割り当てるように設定されている場合は、 **MTU** フィールドにその値が入力され、フィールドは読み取り専用になります。

Web ブラウザは、 StorageGRID アプライアンスインストーラの新しい IP アドレスに自動的にリダイレクトされます。

a. ゲートウェイが正しいことを確認します。

> クライアントネットワークが有効になっている場合は、デフォルトルートが表示されます。デフォルトルートはクライアントネットワークゲートウェイを使用し、クライアントネットワークが有効になっている間は別のインターフェイスに移動できません。

b. ジャンボフレームを使用する場合は、 MTU フィールドを 9000 などのジャンボフレームに適した値に変更します。それ以外の場合は、デフォルト値 1500 のままにします。

> ネットワークの MTU 値は、ノードが接続されているスイッチポートに設定されている値と同じである必要があります。そうしないと、ネットワークパフォーマンスの問題やパケット損失が発生する可能性があります。

関連情報

"サービスアプライアンスのリンク設定の変更"

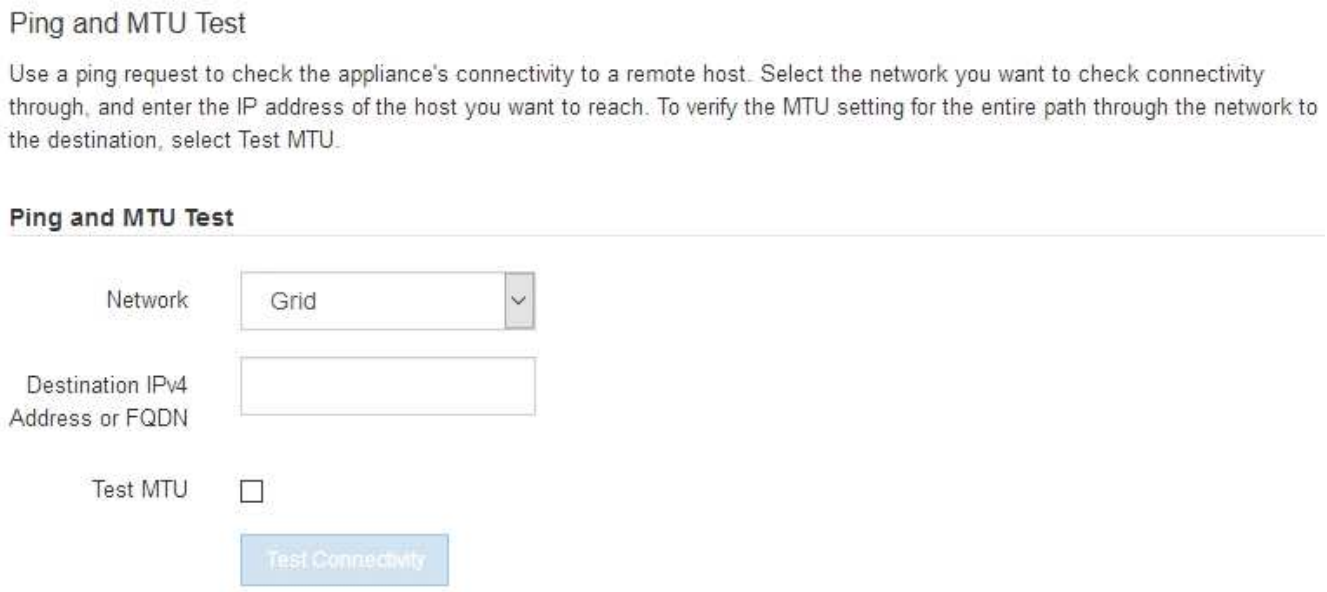
ネットワーク接続の確認

使用する StorageGRID ネットワークに、アプライアンスからアクセスできることを確認する必要があります。ネットワークゲートウェイ経由のルーティングを検証するには、StorageGRID アプライアンスインストーラと異なるサブネット上の IP アドレスとの接続をテストする必要があります。MTU 設定を確認することもできます。

手順

1. StorageGRID アプライアンスインストーラのメニューバーから、 *Configure Networking *>*Ping and MTU Test * をクリックします。

[Ping and MTU Test] ページが表示されます。




2. [* ネットワーク *] ドロップダウンボックスから、テストするネットワークを選択します。グリッド、管理、またはクライアント。
3. そのネットワーク上のホストの IPv4 アドレスまたは完全修飾ドメイン名（ FQDN ）を入力します。

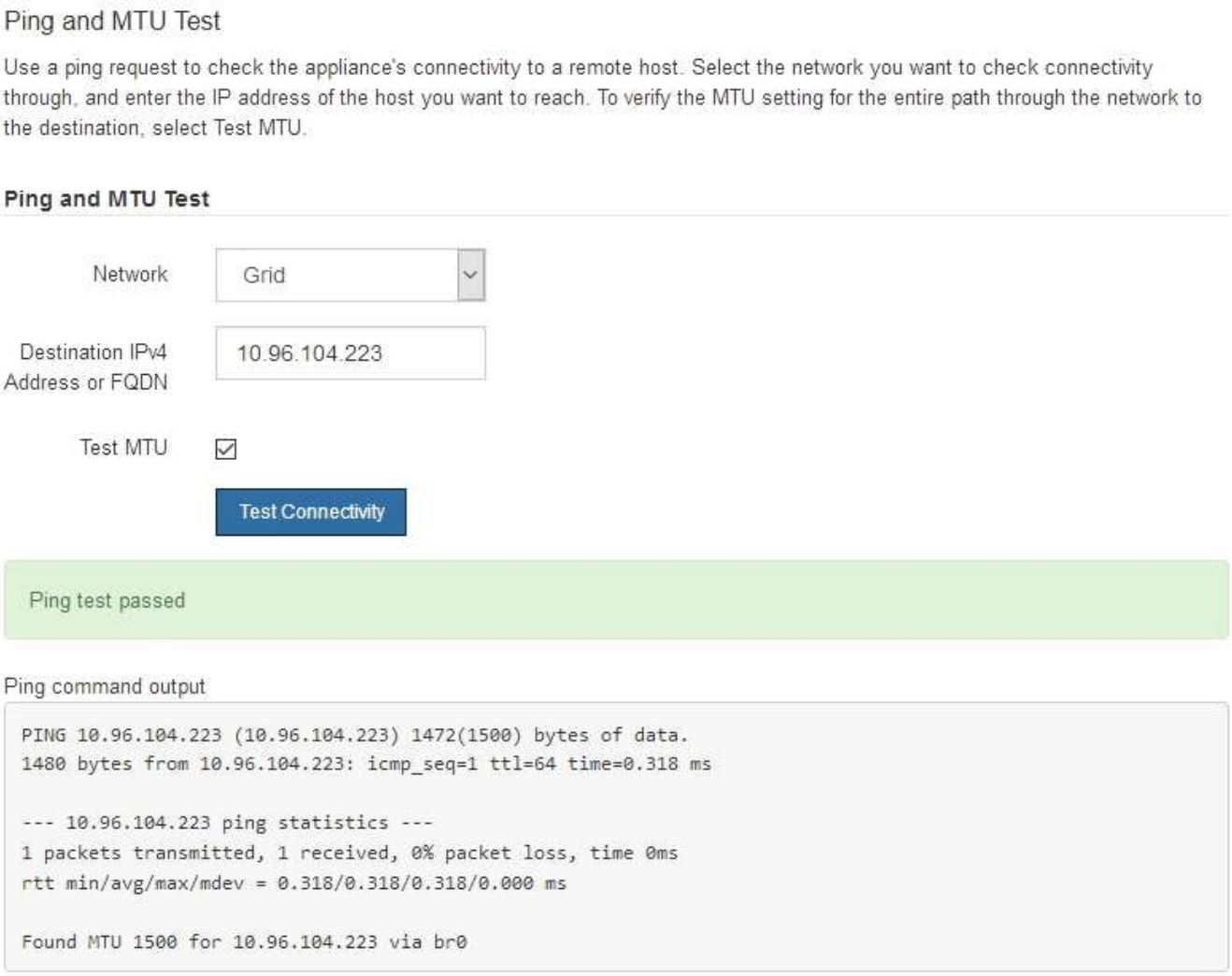
   たとえば、ネットワーク上のゲートウェイやプライマリ管理ノードに ping を送信できます。

4. 必要に応じて、 * Test MTU * チェックボックスをオンにして、ネットワーク経由でデスティネーションへのパス全体の MTU 設定を確認します。

   たとえば、アプライアンスノードと別のサイトのノードの間のパスをテストできます。

5. [ 接続のテスト * ] をクリックします。

   ネットワーク接続が有効な場合は、「 Ping test passed 」メッセージと ping コマンドの出力が表示されます。




関連情報

"ネットワークリンクの設定（SG100およびSG1000）"

"MTU設定を変更します"

ポートレベルのネットワーク接続の確認

## StorageGRID アプライアンスインストーラとその他のノードの間のアクセスがファイアウォールの妨げにならないように、 StorageGRID アプライアンスインストーラが指定した IP アドレスまたはアドレス範囲にある特定の TCP ポートまたはポートセットに接続できることを確認します。

このタスクについて

StorageGRID アプライアンスインストーラに付属のポートのリストを使用して、アプライアンスとグリッドネットワーク内の他のノードの間の接続をテストできます。

また、外部 NFS サーバや DNS サーバで使用されるポートなど、管理ネットワークとクライアントネットワーク、および UDP ポートで接続をテストすることもできます。これらのポートの一覧については、StorageGRID ネットワークのガイドラインにあるポートリファレンスを参照してください。

ポート接続テーブルに表示されているグリッドネットワークポートは、StorageGRID バージョン11.5.0に対してのみ有効です。各ノードタイプに適したポートを確認するには、使用している StorageGRID のバージョンに対応したネットワークガイドラインを確認する必要があります。

手順

1. StorageGRID アプライアンスインストーラから、 **Configure Networking *>** Port Connectivity Test (nmap)* をクリックします。

   Port Connectivity Test ページが表示されます。

   ポート接続テーブルには、グリッドネットワークでの TCP 接続を必要とするノードタイプが表示されます。各ノードタイプについて、アプライアンスにアクセスできる必要があるグリッドネットワークのポートがテーブルに表示されます。

   The following node types require TCP connectivity on the Grid Network.

| Node Type | Grid Network Ports |
|---|---|
| Admin Node | 22,80,443,1504,1505,1506,1508,7443,9999 |
| Storage Node without ADC | 22,1139,1502,1506,1511,7001,9042,9999,18002,18017,18019,18082,18083,18200 |
| Storage Node with ADC | 22,1139,1501,1502,1506,1511,7001,9042,9999,18000,18001,18002,18003,18017,18019,18082,18083,18200,19000 |
| API Gateway | 22,1506,1507,9999 |
| Archive Node | 22,1506,1509,9999,11139 |

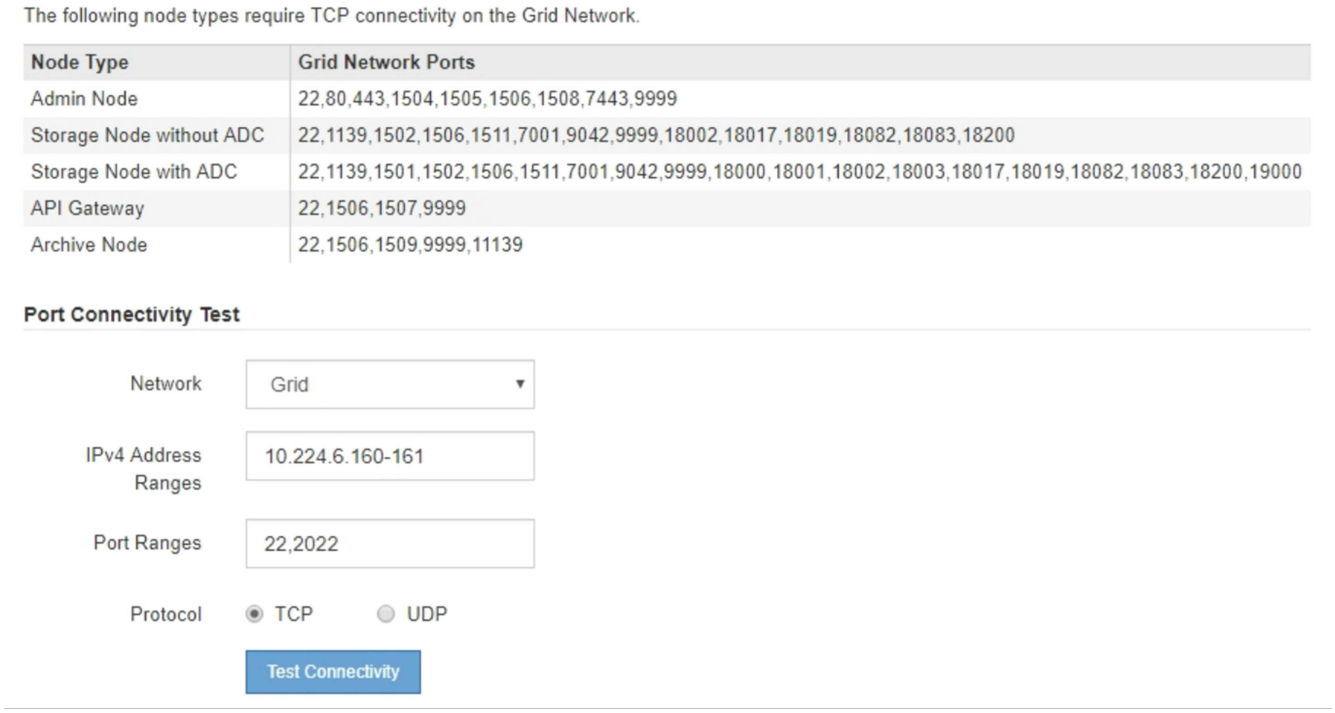
   表に記載されたアプライアンスポートとグリッドネットワーク内のその他のノードの間の接続をテストできます。

2. [* ネットワーク *] ドロップダウンから、テストするネットワークを選択します。 * グリッド * 、 * 管理者 * 、または * クライアント * 。
3. そのネットワーク上のホストの IPv4 アドレスの範囲を指定します。

   たとえば、ネットワーク上のゲートウェイやプライマリ管理ノードをプローブできます。

   次の例に示すように、ハイフンを使用して範囲を指定します。

4. TCP ポート番号、カンマで区切ったポートのリスト、またはポートの範囲を入力します。

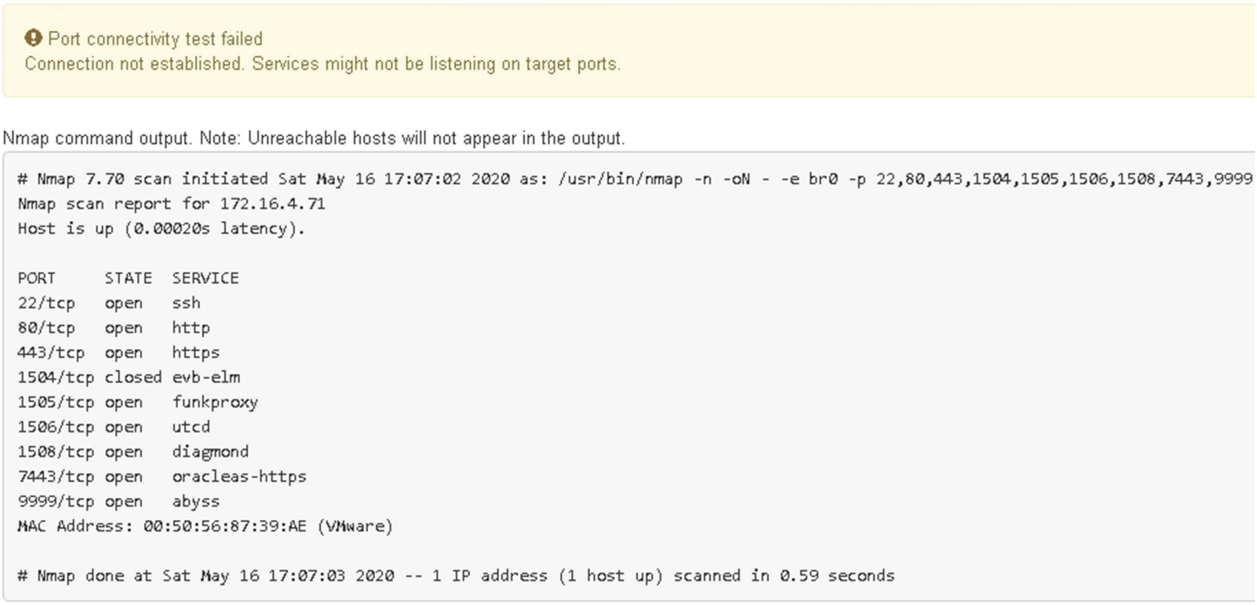



5. [ 接続のテスト * ] をクリックします。

   ◦ 選択したポートレベルのネットワーク接続が有効な場合は、「 Port connectivity test passed 」というメッセージが緑色のバナーに表示されます。nmap コマンドの出力は、バナーの下に表示されます。

   ◦ ポートレベルのネットワーク接続がリモートホストに確立されても ' ホストが選択したポートの 1 つ以上をリッスンしていない場合は ' ポート接続テストに失敗しましたというメッセージが黄色のバナーに表示されますnmap コマンドの出力は、バナーの下に表示されます。

     ホストがリッスンしていないリモート・ポートの状態はすべて「 closed 」です。 たとえば、接続しようとしているノードがインストール済みの状態で、 StorageGRID NMS サービスがまだ実行されていない場合に、黄色のバナーが表示されることがあります。




- 選択した 1 つ以上のポートに対してポートレベルのネットワーク接続を確立できない場合は、「 Port connectivity test failed 」というメッセージが赤いバナーに表示されます。nmap コマンドの出力は、バナーの下に表示されます。

  赤いバナーは、リモートホストのポートへの TCP 接続試行が行われたが、送信者には何も返されなかったことを示します。応答が返されない場合、ポートの状態は「 filtered 」となり、ファイアウォールによってブロックされている可能性があります。

  「閉」のポートも一覧表示されます。

関連情報

"ネットワークガイドライン"

## BMCインターフェイスを設定しています

サービスアプライアンスのベースボード管理コントローラ（ BMC ）のユーザインターフェイスには、ハードウェアに関するステータス情報が表示され、サービスアプライアンスで SNMP 設定やその他のオプションを設定できます。

手順

- "BMCインターフェイスのrootパスワードを変更しています"
- "BMC管理ポートのIPアドレスを設定します"
- "BMCインターフェイスへのアクセス"
- "サービスアプライアンスのSNMPを設定します"
- "アラート用のEメール通知の設定"

### BMCインターフェイスのrootパスワードを変更しています

セキュリティを確保するために、 BMC の root ユーザのパスワードを変更する必要があります。

必要なもの

管理クライアントがサポートされているWebブラウザを使用している必要があります。

このタスクについて

初めてアプライアンスをインストールするとき、BMCではrootユーザのデフォルトパスワードが使用されます(`root/calvin`）。システムを保護するために、 root ユーザのパスワードを変更する必要があります。

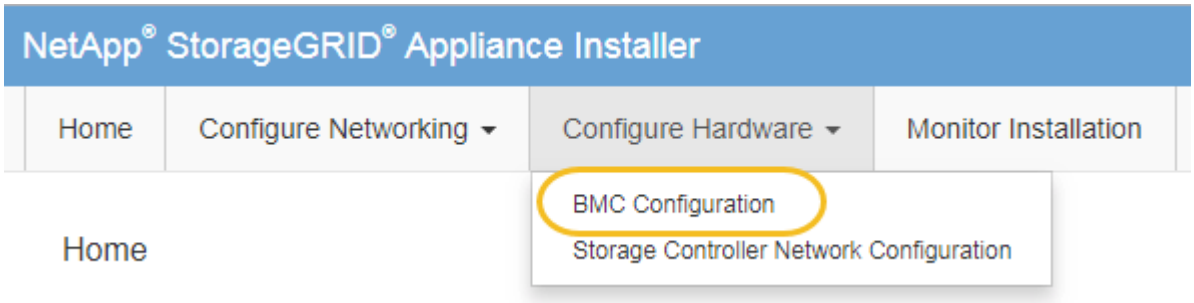
手順

1. クライアントから、StorageGRID アプライアンスインストーラのURLを入力します：+ **`https://services_appliance_IP:8443`**

   の場合 `services_appliance_IP`には、任意のStorageGRID ネットワーク上のアプライアンスのIPアドレスを使用します。

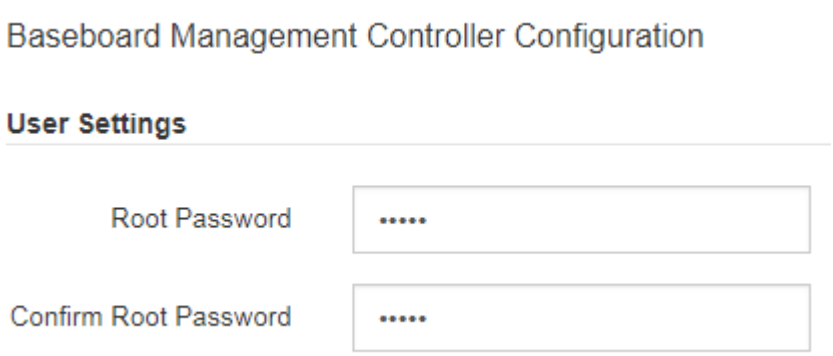
   StorageGRID アプライアンスインストーラのホームページが表示されます。

2. [ ハードウェアの設定 *>*BMC 構成 *] を選択します。




[Baseboard Management Controller Configuration] ページが表示されます。

3. root アカウントの新しいパスワードを 2 つのフィールドに入力します。



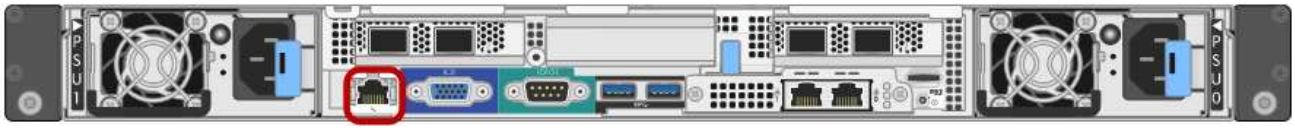

4. [ 保存（ Save ） ] をクリックします。

**BMC**管理ポートの**IP**アドレスを設定します

## BMC インターフェイスにアクセスする前に、サービスアプライアンス上の BMC 管理ポートの IP アドレスを設定する必要があります。

必要なもの

- 管理クライアントがサポートされているWebブラウザを使用している必要があります。
- StorageGRID ネットワークに接続できる管理クライアントを使用している必要があります。
- BMC 管理ポートが、使用する管理ネットワークに接続されている必要があります。
- SG100 BMC 管理ポート *



- SG1000 BMC 管理ポート *

このタスクについて

BMC 管理ポートでは、サポート目的で下位レベルのハードウェアアクセスが許可されます。このポートは、信頼されているセキュアな内部管理ネットワークにのみ接続してください。該当するネットワークがない場合は、テクニカルサポートから BMC 接続の要請があった場合を除き、 BMC ポートを接続しないか、またはブロックしたままにしてください。

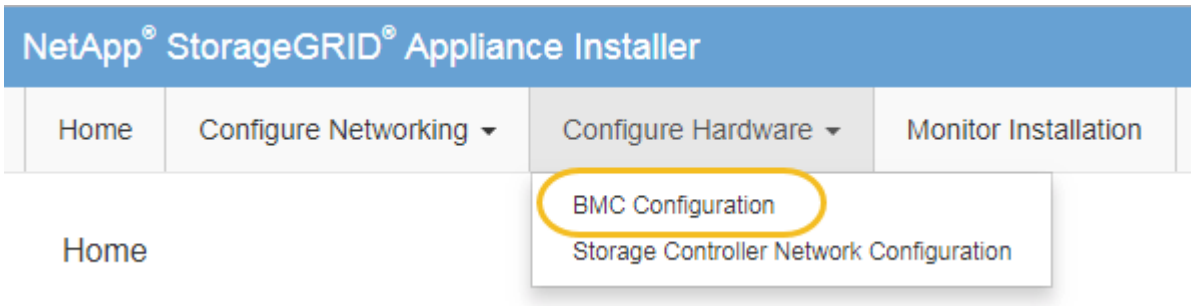
手順

1. クライアントから、StorageGRID アプライアンスインストーラのURLを入力します：+
**`https://services_appliance_IP:8443`**

の場合 `_services_appliance_IP_`には、任意のStorageGRID ネットワーク上のアプライアンスのIPアドレスを使用します。

StorageGRID アプライアンスインストーラのホームページが表示されます。

2. [ ハードウェアの設定 *>*BMC 構成 *] を選択します。

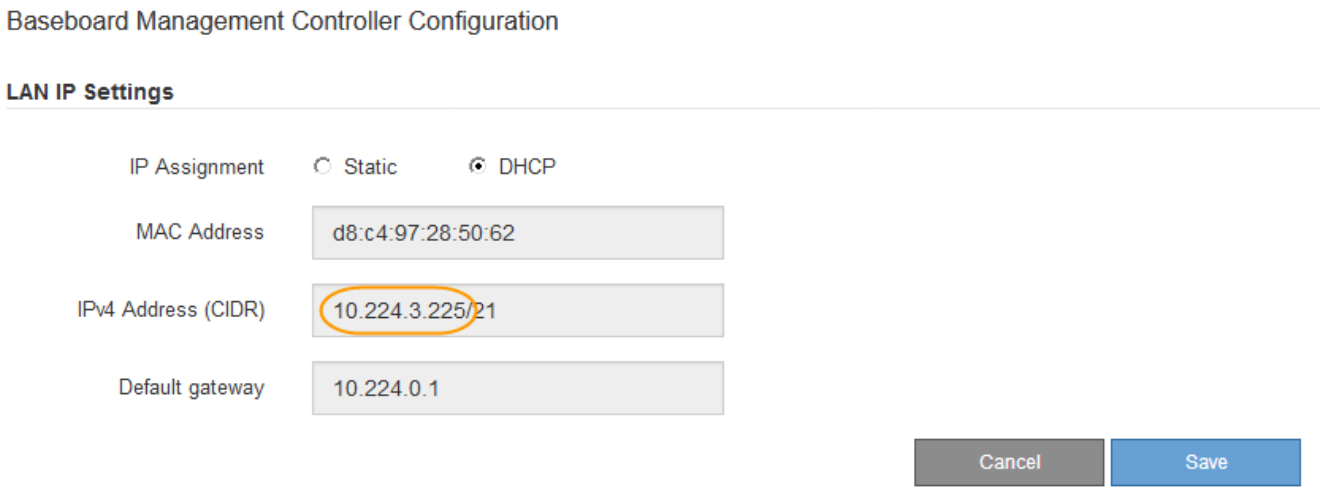



[Baseboard Management Controller Configuration] ページが表示されます。

3. 自動的に表示される IPv4 アドレスを書き留めます。

このポートに IP アドレスを割り当てるためのデフォルトの方法は、 DHCP です。

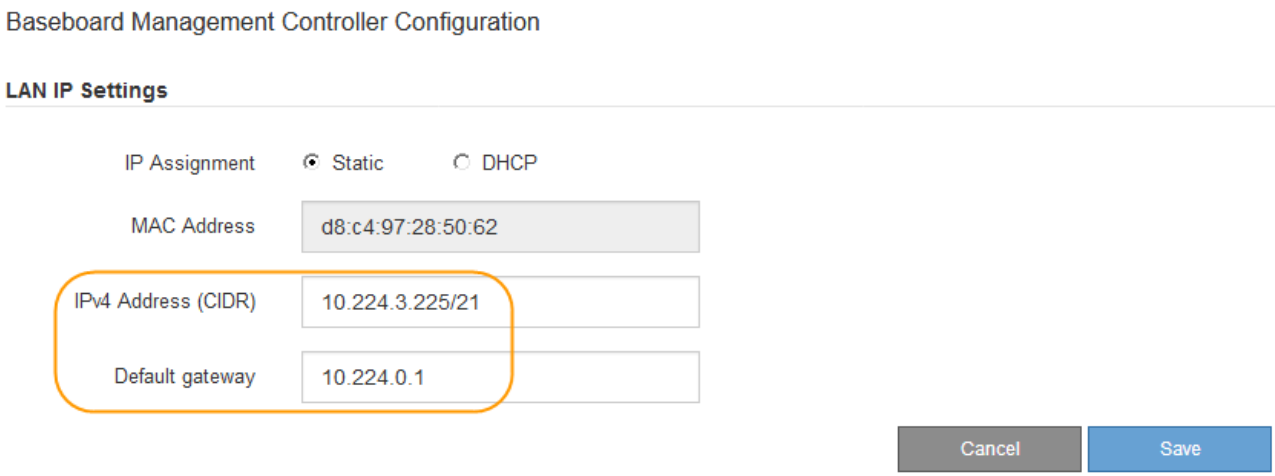
DHCP 値が表示されるまでに数分かかる場合があります。




4. 必要に応じて、 BMC 管理ポートに静的 IP アドレスを設定します。

BMC 管理ポートに静的 IP を割り当てるか、 DHCP サーバでアドレスの永久リースを割り当てる必要があります。

a. 「 * Static * 」を選択します。
b. CIDR 表記を使用して IPv4 アドレスを入力します。
c. デフォルトゲートウェイを入力します。




d. [ 保存（ Save ） ] をクリックします。

変更が適用されるまで数分かかる場合があります。

**BMC**インターフェイスへのアクセス

## BMC 管理ポートの DHCP または静的 IP アドレスを使用して、サービスアプライアンスの BMC インターフェイスにアクセスできます。

必要なもの

- 管理クライアントがサポートされているWebブラウザを使用している必要があります。
- サービスアプライアンスの BMC 管理ポートが、使用する管理ネットワークに接続されている必要があります。
- SG100 BMC 管理ポート *

- SG1000 BMC 管理ポート *

手順

1. BMCインターフェイスのURLとして「+」を入力します
**`https://BMC_Port_IP`**

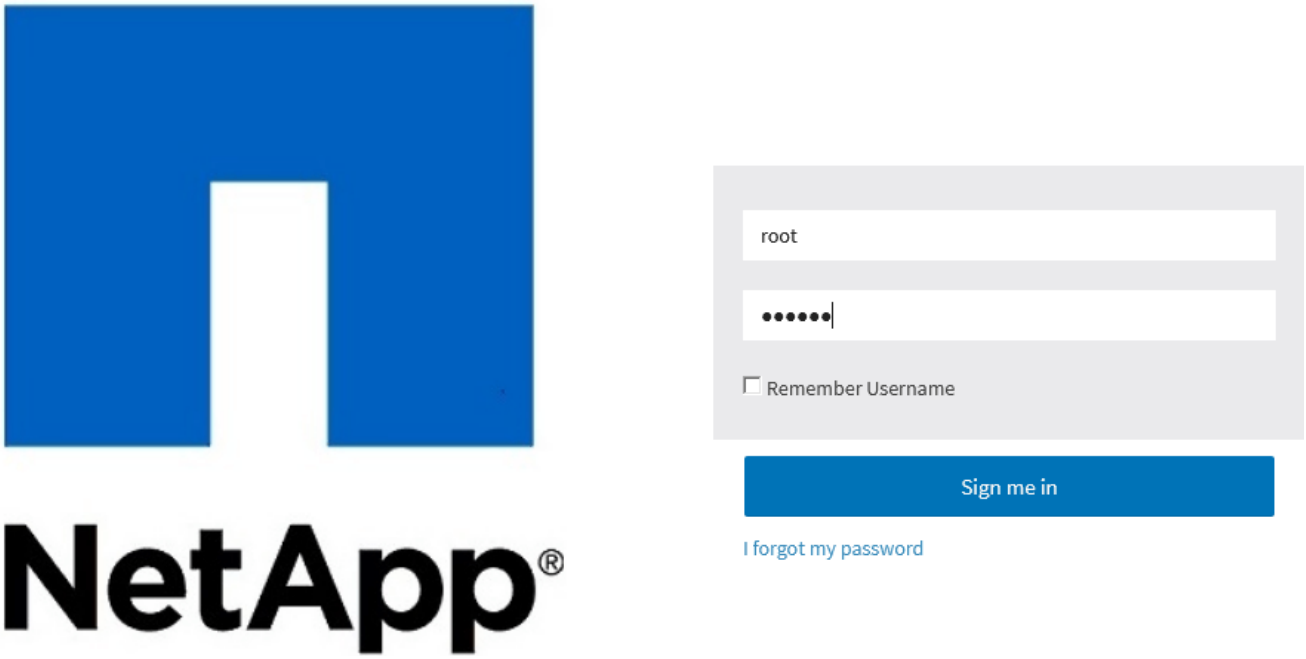
の場合 `*BMC_Port_IP*`BMC管理ポートのDHCPまたは静的IPアドレスを使用します。

BMC のサインインページが表示されます。

2. rootのユーザ名とパスワードを入力します。デフォルトのrootパスワード+を変更したときに設定したパス

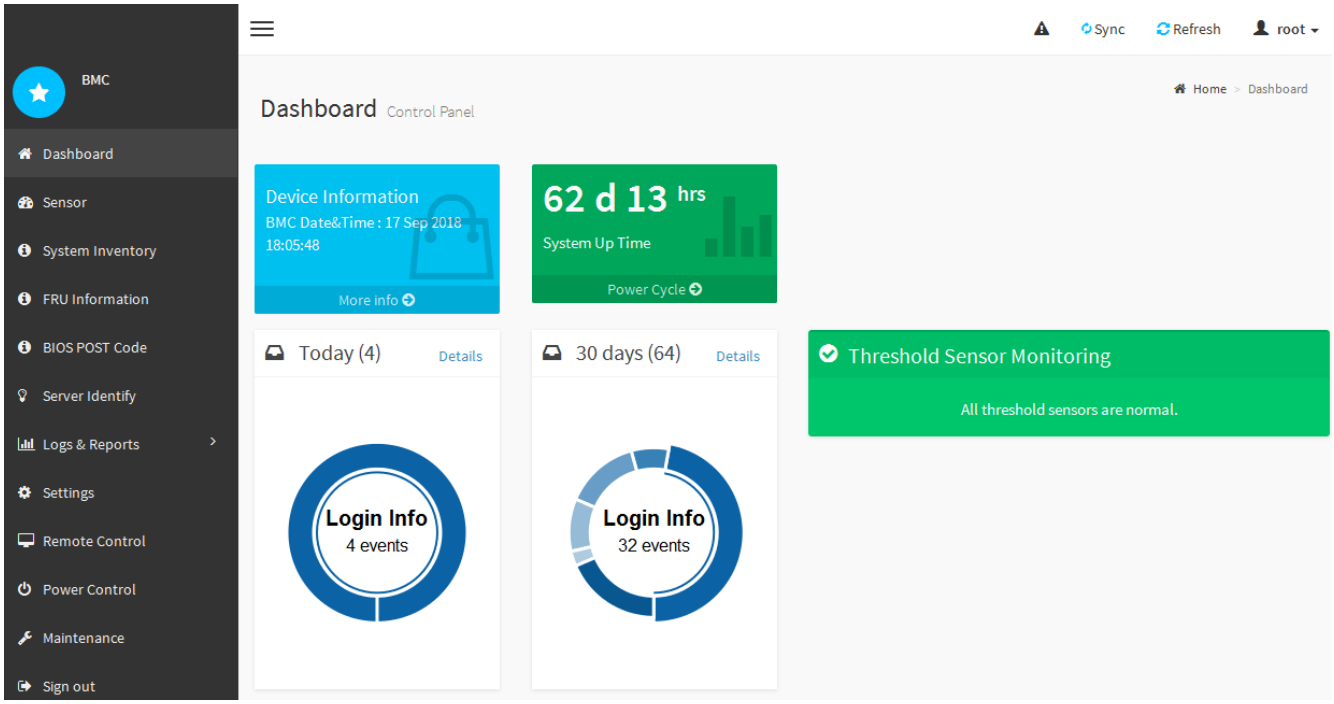
ワードを使用します
**root**

***password***




3. [ サインイン（ Sign me in ） ] をクリックします

   BMC ダッシュボードが表示されます。




4. 必要に応じて、 **Settings**>*User Management* を選択し、「 disabled 」ユーザをクリックして、追加のユーザを作成します。

ユーザが初めてサインインすると、セキュリティを強化するためにパスワードの変更を求められる場合があります。

関連情報

"BMCインターフェイスのrootパスワードを変更しています"

サービスアプライアンスの**SNMP**を設定します

ハードウェアの SNMP の設定に精通している場合は、 BMC インターフェイスを使用してサービスアプライアンスの SNMP 設定を行うことができます。セキュリティで保護されたコミュニティストリングを指定し、 SNMP トラップを有効にし、 SNMP の送信先を最大 5 つ指定できます。

必要なもの

- BMC ダッシュボードへのアクセス方法を確認しておく必要があります。
- SNMPv1-v2c 機器の SNMP 設定経験が必要です。

手順

1. BMC ダッシュボードで、 * Settings * > * SNMP Settings * を選択します。
2. SNMP 設定ページで、 * SNMP V1/V2* を有効にするを選択し、読み取り専用コミュニティストリングと読み取り / 書き込みコミュニティストリングを指定します。

   読み取り専用コミュニティストリングは、ユーザ ID やパスワードのようなものです。侵入者がネットワーク設定に関する情報を取得できないようにするには、この値を変更する必要があります。読み取り / 書き込みコミュニティストリングは、不正な変更からデバイスを保護します。

3. 必要に応じて、 * トラップを有効にする * を選択し、必要な情報を入力します。

   IP アドレスを使用して、各 SNMP トラップの送信先 IP を入力します。完全修飾ドメイン名はサポートされません。

   サービスアプライアンスから SNMP コンソールが異常な状態になったときに通知をすぐに送信するには、トラップを有効にします。トラップは、リンクの稼働 / 停止状態、しきい値を超えた温度、トラフィックの増加を示している場合があります。

4. 必要に応じて、 [ テストトラップの送信 ] をクリックして設定をテストします。
5. 設定が正しい場合は、 * 保存 * をクリックします。

アラート用の**E**メール通知の設定

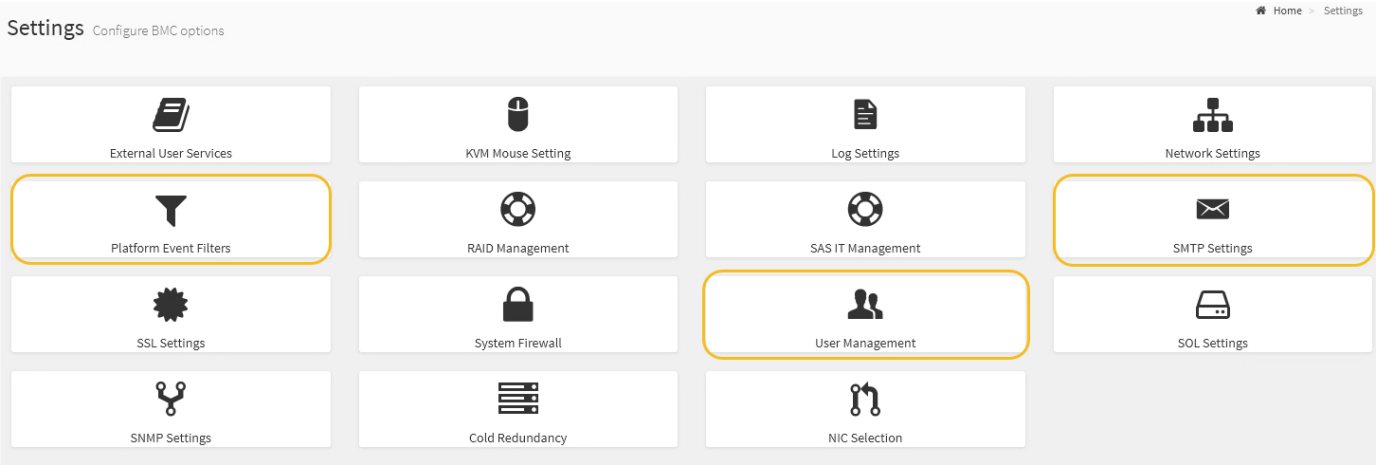
アラート発生時に E メール通知が送信されるようにするには、 BMC インターフェイスを使用して SMTP 設定、ユーザ、 LAN 宛先、アラートポリシー、およびイベントフィルタを設定する必要があります。

必要なもの

BMC ダッシュボードへのアクセス方法を確認しておく必要があります。

このタスクについて

BMC インターフェイスでは、 [ 設定 ] ページの *SMTP 設定 * 、 * ユーザー管理 * 、および * プラットフォーム・イベント・フィルタ * オプションを使用して、電子メール通知を設定します。




手順

1. SMTP を設定します。
   a. [ * 設定 * > * SMTP 設定 * ] を選択します。
   b. [ 送信者電子メール ID] に、有効な電子メールアドレスを入力します。

      この E メールアドレスは、 BMC が E メールを送信したときの送信元アドレスとして提供されます。

2. アラートを受信するようにユーザを設定します。
   a. BMC ダッシュボードで、 * Settings * > * User Management * を選択します。
   b. アラート通知を受信するユーザを少なくとも 1 人追加してください。

      ユーザに設定する E メールアドレスは、 BMC がアラート通知の送信先アドレスです。たとえば、「 notification-user 」などの一般的なユーザーを追加し、テクニカルサポートチームの Email宛先リストの電子メールアドレスを使用できます。

3. LAN 宛先にアラートを設定します。
   a. [ * 設定 * > * プラットフォーム・イベント・フィルタ * > * LAN 宛先 * ] を選択します。
   b. LAN 宛先を少なくとも 1 つ設定します。
      - [ 宛先の種類 ] で [**Email**] を選択します。
      - BMC Username には、前に追加したユーザ名を選択します。
      - 複数のユーザを追加し、すべてのユーザが通知メールを受信できるようにするには、ユーザごとに LAN 宛先を追加する必要があります。
   c. テストアラートを送信します。
4. アラートポリシーを設定して、 BMC がアラートを送信するタイミングと場所を定義できるようにします。
   a. [ * 設定 * > * プラットフォーム・イベント・フィルタ * > * アラート・ポリシー * ] を選択します。
   b. LAN 宛先ごとに少なくとも 1 つのアラートポリシーを設定します。

- [ ポリシーグループ番号（ Policy Group Number ） ] で、 * 1 * を選択します。
- ［ ポリシーアクション ］ で、 ［ * 常にこの宛先にアラートを送信する * ］ を選択します。
- LAN チャンネルの場合、 * 1 * を選択します。
- [Destination Selector] で、ポリシーの LAN 宛先を選択します。

5. イベントフィルタを設定して、さまざまなイベントタイプのアラートを適切なユーザに送信します。
   a. [ * 設定 * > * プラットフォーム・イベント・フィルタ * > * イベント・フィルタ * ] を選択します。
   b. Alert Policy Group Number （アラートポリシーグループ番号）に * 1 * を入力します。
   c. アラートポリシーグループに通知するイベントごとにフィルタを作成します。
      - 電源アクション、特定のセンサーイベント、またはすべてのイベントのイベントフィルタを作成できます。
      - 監視するイベントが不明な場合は、センサーの種類として「 * すべてのセンサー * 」を選択し、イベントオプションとして「すべてのイベント * 」を選択します。不要な通知を受け取った場合は、選択内容をあとで変更できます。

## オプション：ノード暗号化を有効にする

ノードの暗号化を有効にすると、アプライアンス内のディスクを安全なキー管理サーバ（ KMS ）暗号化によってサイト内での物理的な損失やデータの削除から保護することができます。アプライアンスのインストール時にノード暗号化を選択して有効にする必要があります。また、 KMS 暗号化プロセスが開始されると、ノード暗号化の選択を解除できません。

必要なもの

StorageGRID の管理手順の KMS に関する情報を確認します。

このタスクについて

ノード暗号化が有効になっているアプライアンスは、 StorageGRID サイト用に設定されている外部キー管理サーバ（ KMS ）に接続します。各 KMS （または KMS クラスタ）は、サイトにあるすべてのアプライアンスノードの暗号化キーを管理します。これらのキーは、ノード暗号化が有効なアプライアンスで、各ディスク上のデータを暗号化および復号化します。

Grid Manager StorageGRID では、アプライアンスのインストール前またはインストール後に KMS を設定できます。詳細については、 StorageGRID の管理手順の KMS とアプライアンスの設定に関する情報を参照してください。

- アプライアンスをインストールする前に KMS を設定すると、 KMS で制御される暗号化が開始されます。この暗号化は、アプライアンスでノード暗号化を有効にし、 KMS が設定されている StorageGRID サイトに追加します。
- アプライアンスをインストールする前に KMS が設定されていない場合は、 KMS が設定され、アプライアンスノードを含むサイトで利用可能になった時点で、ノード暗号化が有効になっている各アプライアンスで KMS 制御された暗号化が実行されます。

> ノード暗号化が有効になっているアプライアンスより前に存在するデータは、設定されたKMSに接続する前に、セキュアでない一時キーで暗号化されます。キーが KMS から提供される値に設定されるまで、アプライアンスの取り外しや盗難は防止されません。

ディスクの復号化に KMS キーが必要な場合を除いて、アプライアンス上のデータを取得することはできず、データが実質的に失われます。これは、 KMS から復号化キーを取得できない場合に発生します。顧客が KMS 設定をクリアするか、 KMS キーの有効期限が切れるか、 KMS への接続が失われるか、 KMS キーがインストールされている StorageGRID システムからアプライアンスが削除されると、キーにアクセスできなくなります。

手順

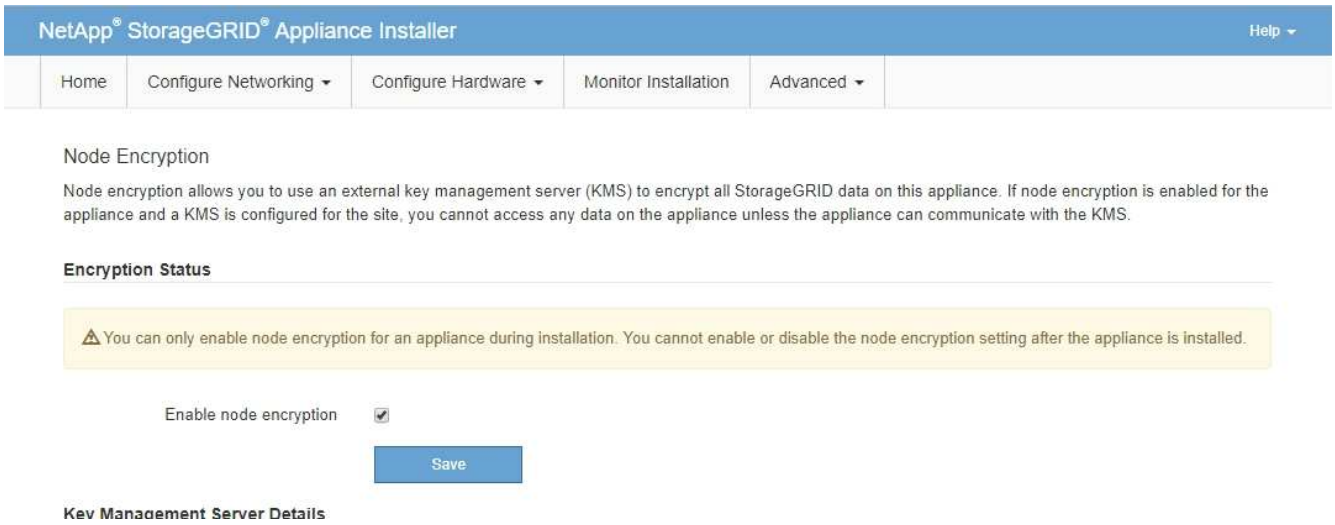
1. ブラウザを開き、アプライアンスのコンピューティングコントローラの IP アドレスのいずれかを入力します。[+]
**`https://Controller_IP:8443`**

   *`Controller_IP`* は、3つのStorageGRID ネットワークのいずれかでのコンピューティングコントローラ（ストレージコントローラではない）のIPアドレスです。

   StorageGRID アプライアンスインストーラのホームページが表示されます。

   > アプライアンスを KMS キーで暗号化すると、アプライアンスディスクを復号化する際に同じ KMS キーを使用する必要がなくなります。

2. Configure Hardware * > * Node Encryption * を選択します。




3. [ ノード暗号化を有効にする *] を選択します。

   保存を選択し、アプライアンスノードがStorageGRID システム内のKMS暗号化キーにアクセスしてディスク暗号化を開始するまでは、「ノード暗号化を有効にする」を選択解除してデータ損失のリスクを回避できます。アプライアンスのインストール後、ノード暗号化を無効にすることはできません。

   > KMS を含む StorageGRID サイトにノード暗号化が有効になっているアプライアンスを追加すると、そのノードで KMS 暗号化を使用するのを停止することはできません。

4. [ 保存（ Save ） ] を選択します。
5. アプライアンスを StorageGRID システムのノードとして導入します。

   KMS で制御される暗号化は、アプライアンスが StorageGRID サイト用に設定されている KMS キーにアクセスすると開始されます。KMS 暗号化プロセス中にインストーラによって進捗状況のメッセージが表示されます。この処理には、アプライアンス内のディスクボリュームの数によっては数分かかることがあ

ります。

アプライアンスは、最初に各ディスクボリュームにランダムな KMS 以外の暗号化キーを割り当てて構成します。ディスクはこの一時的な暗号化キーを使用して暗号化されます。このキーは、ノード暗号化が有効になっているアプライアンスが StorageGRID サイト用に設定されている KMS キーにアクセスするまではセキュリティ保護されません。

完了後

アプライアンスノードがメンテナンスモードのときに使用されているノード暗号化ステータス、 KMS の詳細、および証明書を確認できます。

関連情報

"StorageGRID の管理"

"メンテナンスモードでのノード暗号化の監視"

## サービスアプライアンスノードの導入

サービスアプライアンスは、プライマリ管理ノード、非プライマリ管理ノード、またはゲートウェイノードとして導入できます。SG100 と SG1000 アプライアンスは、両方ともゲートウェイノードと管理ノード（プライマリまたは非プライマリ）として同時に動作できます。

### プライマリ管理ノードとしてのサービスアプライアンスの導入

サービスアプライアンスをプライマリ管理ノードとして導入する場合は、アプライアンスに組み込みの StorageGRID アプライアンスインストーラを使用して StorageGRID ソフトウェアをインストールするか、インストールするソフトウェアバージョンをアップロードします。プライマリ管理ノードは、他のタイプのアプライアンスノードをインストールする前にインストールして設定する必要があります。プライマリ管理ノードは、グリッドネットワーク、およびオプションの管理ネットワークとクライアントネットワーク（いずれかまたは両方が設定されている場合）に接続できます。

必要なもの

- アプライアンスをラックまたはキャビネットに設置し、ネットワークに接続し、電源を投入しておきます。
- StorageGRID アプライアンスインストーラを使用して、アプライアンスのネットワークリンク、 IP アドレス、ポートの再マッピング（必要な場合）を設定しておきます。

ポートを再マッピングした場合、同じポートを使用してロードバランサエンドポイントを設定することはできません。再マッピングしたポートを使用してエンドポイントを作成できますが、これらのエンドポイントはロードバランササービスではなく、元の CLB ポートおよびサービスに再マッピングされます。ポートの再マッピングを削除するには、リカバリとメンテナンスの手順に従ってください。

CLB サービスは廃止されました。

- サポートされている Web ブラウザがインストールされたサービスラップトップを用意しておきます。
- アプライアンスに割り当てられている IP アドレスのいずれかを確認しておきます。接続されているどの StorageGRID ネットワークの IP アドレスでも使用できます。

このタスクについて

アプライアンスプライマリ管理ノードに StorageGRID をインストールするには、次の手順を実行します。

- StorageGRID ソフトウェアをインストールするには、 StorageGRID アプライアンスインストーラを使用します。別のバージョンのソフトウェアをインストールする場合は、まず StorageGRID アプライアンスインストーラを使用してソフトウェアをアップロードします。
- ソフトウェアがインストールされるまで待ちます。
- ソフトウェアがインストールされると、アプライアンスが自動的にリブートされます。

手順

1. ブラウザを開き、アプライアンスの IP アドレスを入力します。[+]
   **`https://services_appliance_IP:8443`**

   StorageGRID アプライアンスインストーラのホームページが表示されます。

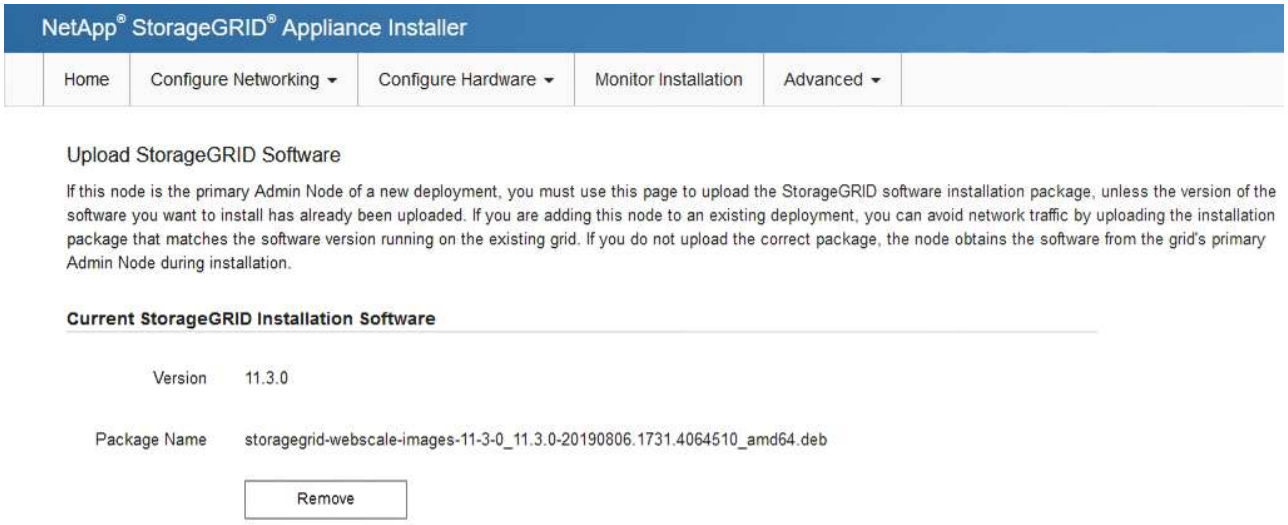
2. [ このノード * ] セクションで、 [ * プライマリ管理者 * ] を選択します。
3. [* Node name* （ノード名 * ） ] フィールドに、このアプライアンスノードに使用する名前を入力し、 [ * Save * （保存） ] をクリックします。

   このノード名は、 StorageGRID システムでこのアプライアンスノードに割り当てられ、グリッドノードは Grid Manager の Grid Nodes ページに表示されます。

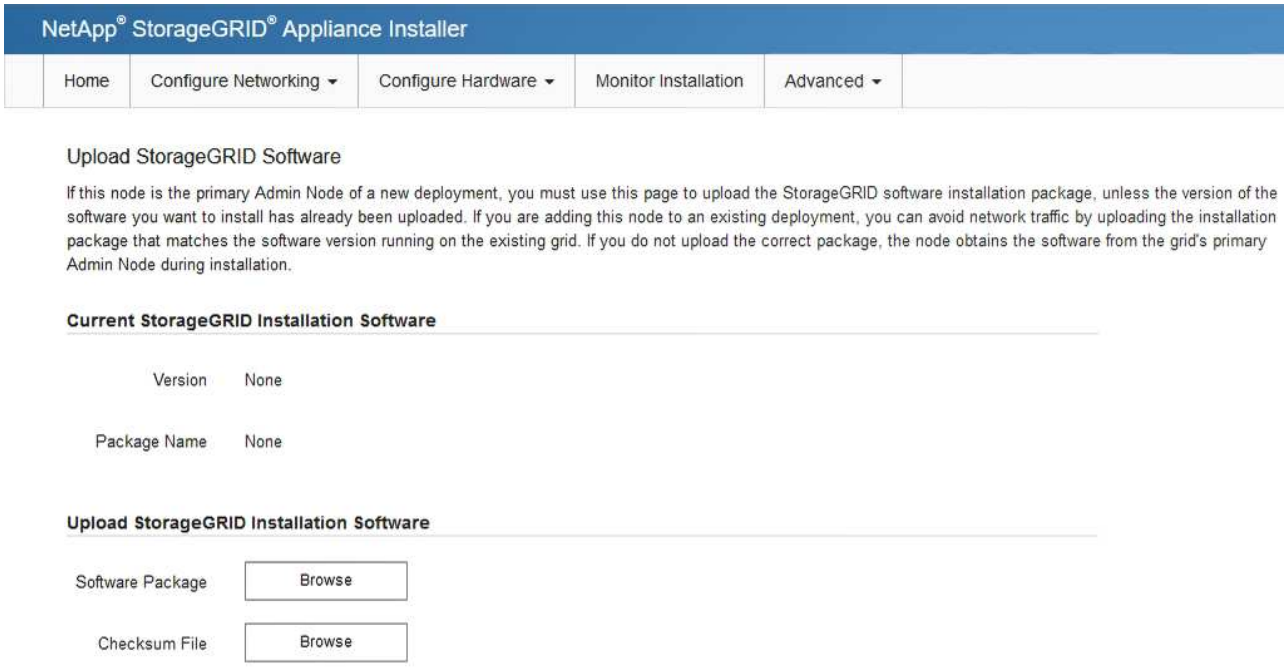
4. 別のバージョンの StorageGRID ソフトウェアをインストールする必要がある場合は、次の手順を実行します。
   a. ネットアップの StorageGRID ダウンロードページからインストールアーカイブをダウンロードします。

      "ネットアップのダウンロード： StorageGRID"

   b. アーカイブを展開します。
   c. StorageGRID アプライアンス・インストーラから、 * アドバンスト * > * StorageGRID ソフトウェアのアップロード * を選択します。
   d. [ 削除 ] をクリックして、現在のソフトウェアパッケージを削除します。




e. ダウンロードして解凍したソフトウェアパッケージの [**Browse**]( 参照 ) をクリックし、チェックサムファイルの [**Browse**]( 参照 ) をクリックします。



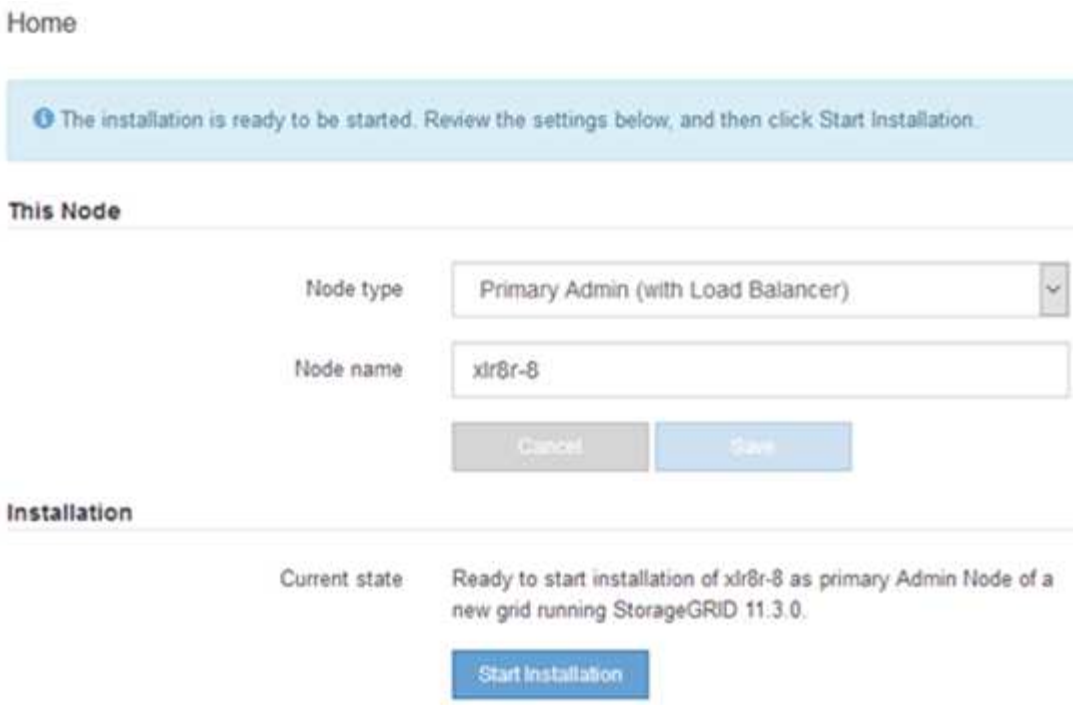

f. ホームページに戻るには、「 * Home * 」（ホーム）を選択します。

5. 現在の状態が「 Ready to start installation of primary Admin Node name with software version x.y' 」であり、「 Start Installation * 」ボタンが有効になっていることを確認します。

> 管理ノードアプライアンスをノードクローニングターゲットとして導入する場合は、ここで導入プロセスを停止して、リカバリとメンテナンスのためにノードクローニング手順 を継続します。

""

6. StorageGRID アプライアンスインストーラのホームページで、 * インストールの開始 * をクリックします。




現在の状態が「 Installation is in progress 」に変わり、「 Monitor Installation 」ページが表示されます。

モニタのインストールページに手動でアクセスする必要がある場合は、メニューバーから * モニタのインストール * をクリックします。

関連情報

"ゲートウェイノードまたは非プライマリ管理ノードとしてサービスアプライアンスを導入する"

ゲートウェイノードまたは非プライマリ管理ノードとしてサービスアプライアンスを導入する

## サービスアプライアンスをゲートウェイノードまたは非プライマリ管理ノードとして導入する場合は、アプライアンスに搭載されている StorageGRID アプライアンスインストーラを使用します。

必要なもの

- アプライアンスをラックまたはキャビネットに設置し、ネットワークに接続し、電源を投入しておきます。
- StorageGRID アプライアンスインストーラを使用して、アプライアンスのネットワークリンク、 IP アドレス、ポートの再マッピング（必要な場合）を設定しておきます。

ポートを再マッピングした場合、同じポートを使用してロードバランサエンドポイントを設定することはできません。再マッピングしたポートを使用してエンドポイントを作成できますが、これらのエンドポイントはロードバランササービスではなく、元の CLB ポートおよびサービスに再マッピングされます。ポートの再マッピングを削除するには、リカバリとメンテナンスの手順に従ってください。

CLB サービスは廃止されました。

- StorageGRID システムのプライマリ管理ノードを導入しておきます。
- StorageGRID アプライアンスインストーラの IP 設定ページに表示されるすべてのグリッドネットワークサブネットが、プライマリ管理ノードのグリッドネットワークサブネットリストで定義されている。
- サポートされている Web ブラウザがインストールされたサービスラップトップを用意しておきます。
- アプライアンスに割り当てられている IP アドレスを確認しておきます。接続されているどの StorageGRID ネットワークの IP アドレスでも使用できます。

このタスクについて

StorageGRID をサービスアプライアンスノードにインストールするには、次の手順を実行します。

- プライマリ管理ノードの IP アドレスおよびアプライアンスノードの名前を指定または確認します。
- インストールを開始し、ソフトウェアがインストールされるまで待ちます。

  アプライアンスゲートウェイノードのインストールが一時停止します。インストールを再開するには、Grid Manager にサインインし、グリッドノードをすべて承認し、 StorageGRID のインストールプロセスを完了します。非プライマリ管理ノードをインストールする場合、承認は必要ありません。

> SG100 と SG1000 サービスアプライアンスは同じサイトに導入しないでください。パフォーマンスが予測不能になる可能性があります

> 一度に複数のアプライアンスノードを導入する必要がある場合は、を使用してインストールプロセスを自動化できます `configure-sga.py` アプライアンスインストールスクリプト。また、アプライアンスインストーラを使用して、構成情報を含む JSON ファイルをアップロードすることもできます。を参照してください "アプライアンスのインストールと設定の自動化"。

手順

1. ブラウザを開き、アプライアンスの IP アドレスを入力します。

   **`https://Controller_IP:8443`**

   StorageGRID アプライアンスインストーラのホームページが表示されます。

2. プライマリ管理ノードの接続セクションで、プライマリ管理ノードの IP アドレスを指定する必要があるかどうかを確認します。

   このデータセンターに他のノードがすでにインストールされている場合は、プライマリ管理ノードまたは ADMIN_IP が設定された少なくとも 1 つのグリッドノードが同じサブネットにあるという想定で、StorageGRID アプライアンスインストーラがこの IP アドレスを自動的に検出します。

3. この IP アドレスが表示されない場合や変更する必要がある場合は、アドレスを指定します。

| オプション | 説明 |
| --- | --- |
| IP を手動で入力します | a. Enable Admin Node discovery * チェックボックスの選択を解除します。<br>b. IP アドレスを手動で入力します。<br>c. [ 保存（ Save ） ] をクリックします。<br>d. 新しい IP アドレスの接続状態が READY になるまで待ちます。 |
| 接続されたすべてのプライマリ管理ノードの自動検出 | a. Enable Admin Node discovery * チェックボックスを選択します。<br>b. 検出された IP アドレスのリストが表示されるまで待ちます。<br>c. このアプライアンスストレージノードを導入するグリッドのプライマリ管理ノードを選択します。<br>d. [ 保存（ Save ） ] をクリックします。<br>e. 新しい IP アドレスの接続状態が READY になるまで待ちます。 |

4. [* Node name* （ノード名 * ） ] フィールドに、このアプライアンスノードに使用する名前を入力し、 [ * Save * （保存） ] をクリックします。

   このノード名は、 StorageGRID システムでこのアプライアンスノードに割り当てられ、このタブは、 Grid Manager のノードページ（概要タブ）に表示されます。ノードを承認するときに、必要に応じて、この名前を変更できます。

5. 別のバージョンの StorageGRID ソフトウェアをインストールする必要がある場合は、次の手順を実行します。

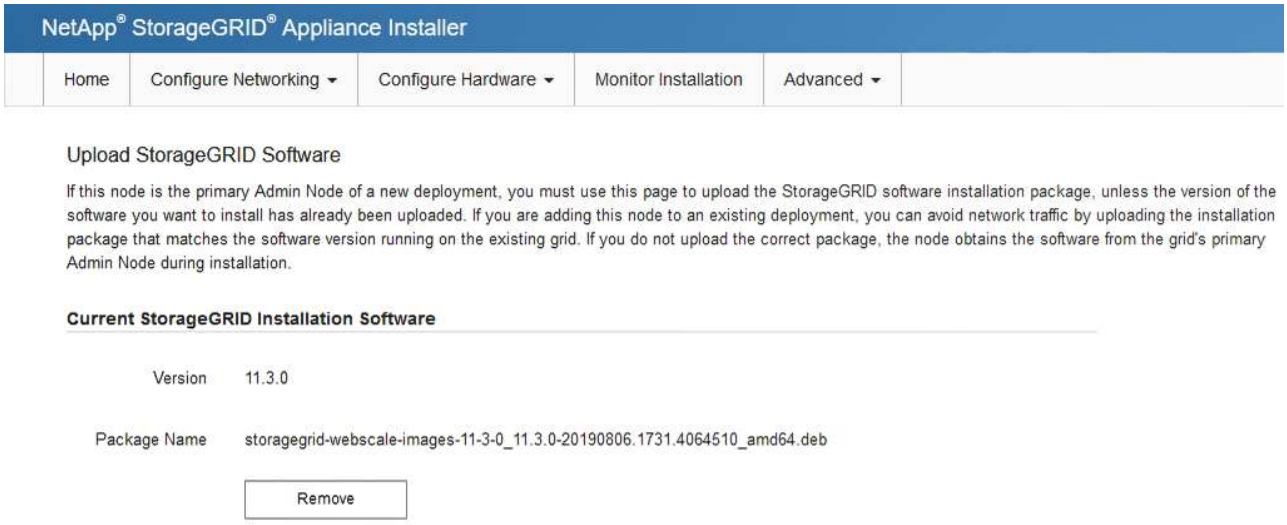
   a. ネットアップの StorageGRID ダウンロードページからインストールアーカイブをダウンロードします。

      "ネットアップのダウンロード： StorageGRID"

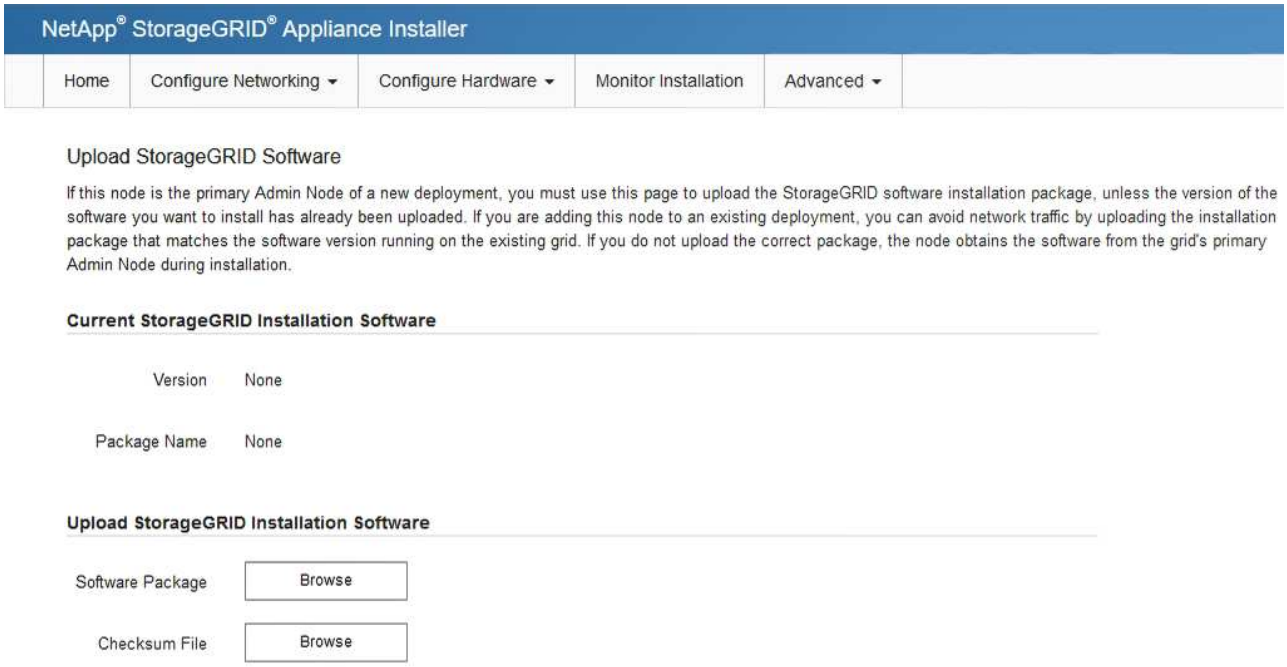
   b. アーカイブを展開します。

   c. StorageGRID アプライアンス・インストーラから、 * アドバンスト * > * StorageGRID ソフトウェアのアップロード * を選択します。

   d. [ 削除 ] をクリックして、現在のソフトウェアパッケージを削除します。




e. ダウンロードして解凍したソフトウェアパッケージの [**Browse**]( 参照 ) をクリックし、チェックサムファイルの [**Browse**]( 参照 ) をクリックします。

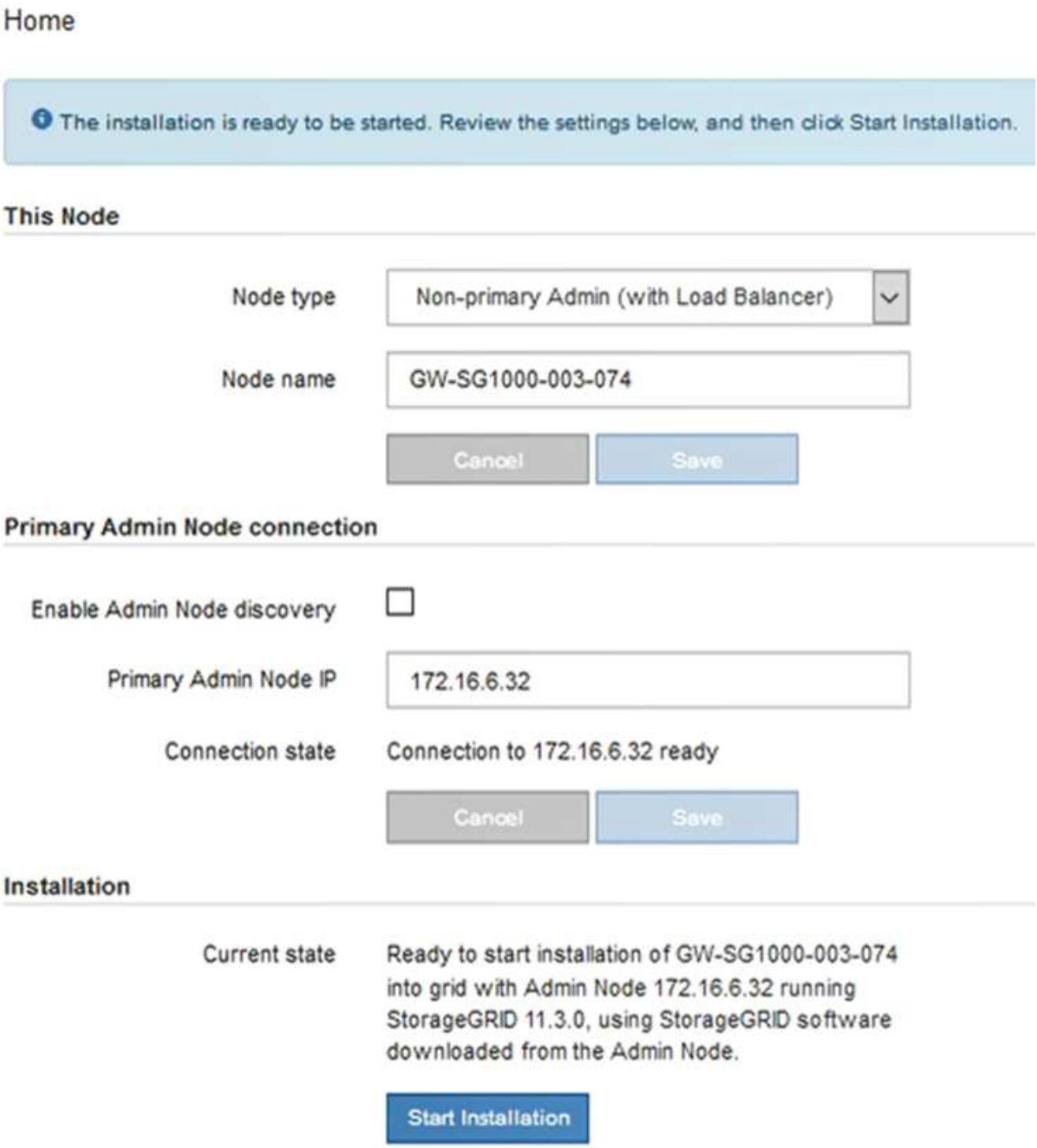



f. ホームページに戻るには、「 * Home * 」（ホーム）を選択します。

6. Installation（インストール）セクションで、現在の状態がのインストール開始準備完了（Ready to start installation）であることを確認します `node name` をプライマリ管理ノードでグリッドに追加します `admin_ip` "*インストールの開始*ボタンが有効になっていることを確認します。

   [Start Installation* （インストールの開始） ] ボタンが有効になっていない場合は、ネットワーク設定またはポート設定の変更が必要になることがあります。手順については、使用しているアプライアンスのインストールとメンテナンスの手順を参照してください。

7. StorageGRID アプライアンスインストーラのホームページで、 * インストールの開始 * をクリックします。




現在の状態が「 Installation is in progress 」に変わり、「 Monitor Installation 」ページが表示されます。

モニタのインストールページに手動でアクセスする必要がある場合は、メニューバーから * モニタのインストール * をクリックします。

8. グリッドに複数のアプライアンスノードがある場合は、アプライアンスごとに上記の手順を繰り返します。

関連情報

"プライマリ管理ノードとしてのサービスアプライアンスの導入"

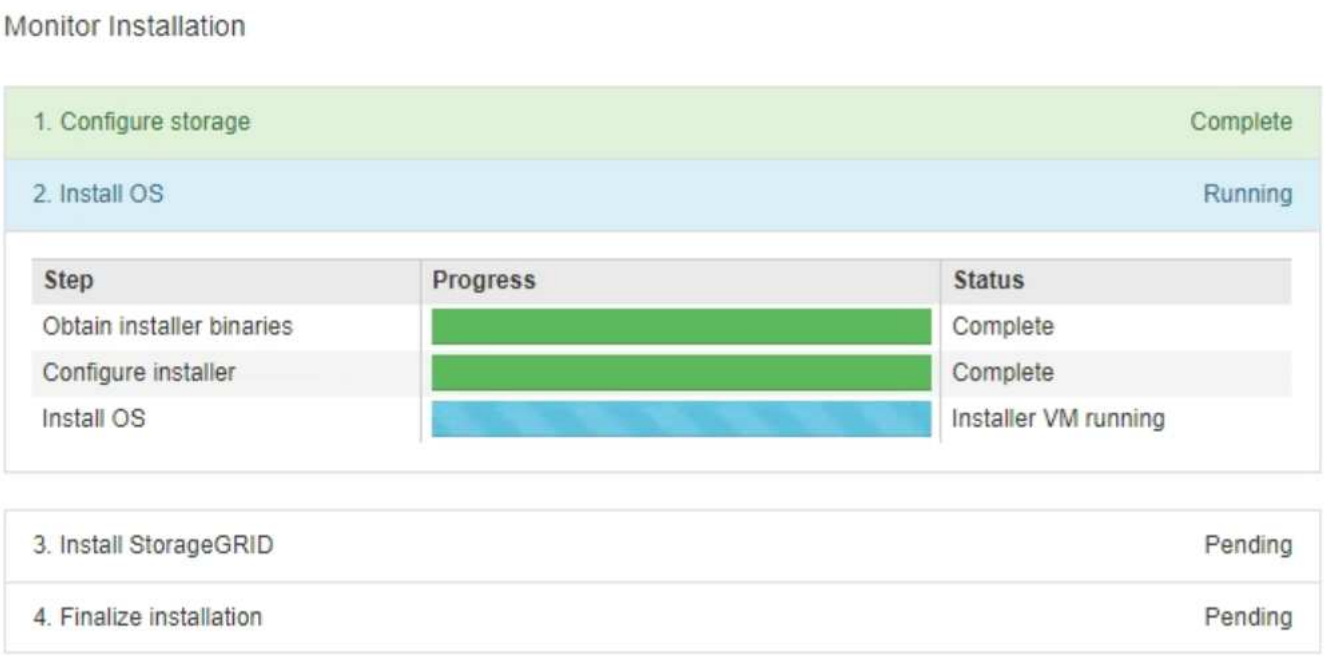
サービスアプライアンスのインストールの監視

StorageGRID アプライアンスインストーラでは、インストールが完了するまでステータスが提供されます。ソフトウェアのインストールが完了すると、アプライアンスがリブートされます。

手順

1. インストールの進行状況を監視するには、メニューバーの * インストールの監視 * をクリックします。

   Monitor Installation ページにインストールの進行状況が表示されます。




   青色のステータスバーは、現在進行中のタスクを示します。緑のステータスバーは、正常に完了したタスクを示します。

   インストーラは、以前のインストールで完了したタスクが再実行されないようにします。インストールを再実行している場合 ' 再実行する必要のないタスクは ' 緑色のステータスバーとステータスが [ スキップ済み ] と表示されます

2. インストールの最初の 2 つのステージの進行状況を確認します。

   ◦ * 1 。ストレージの構成 *

     インストーラがアプライアンスのドライブから既存の設定を消去し、ホストを設定します。

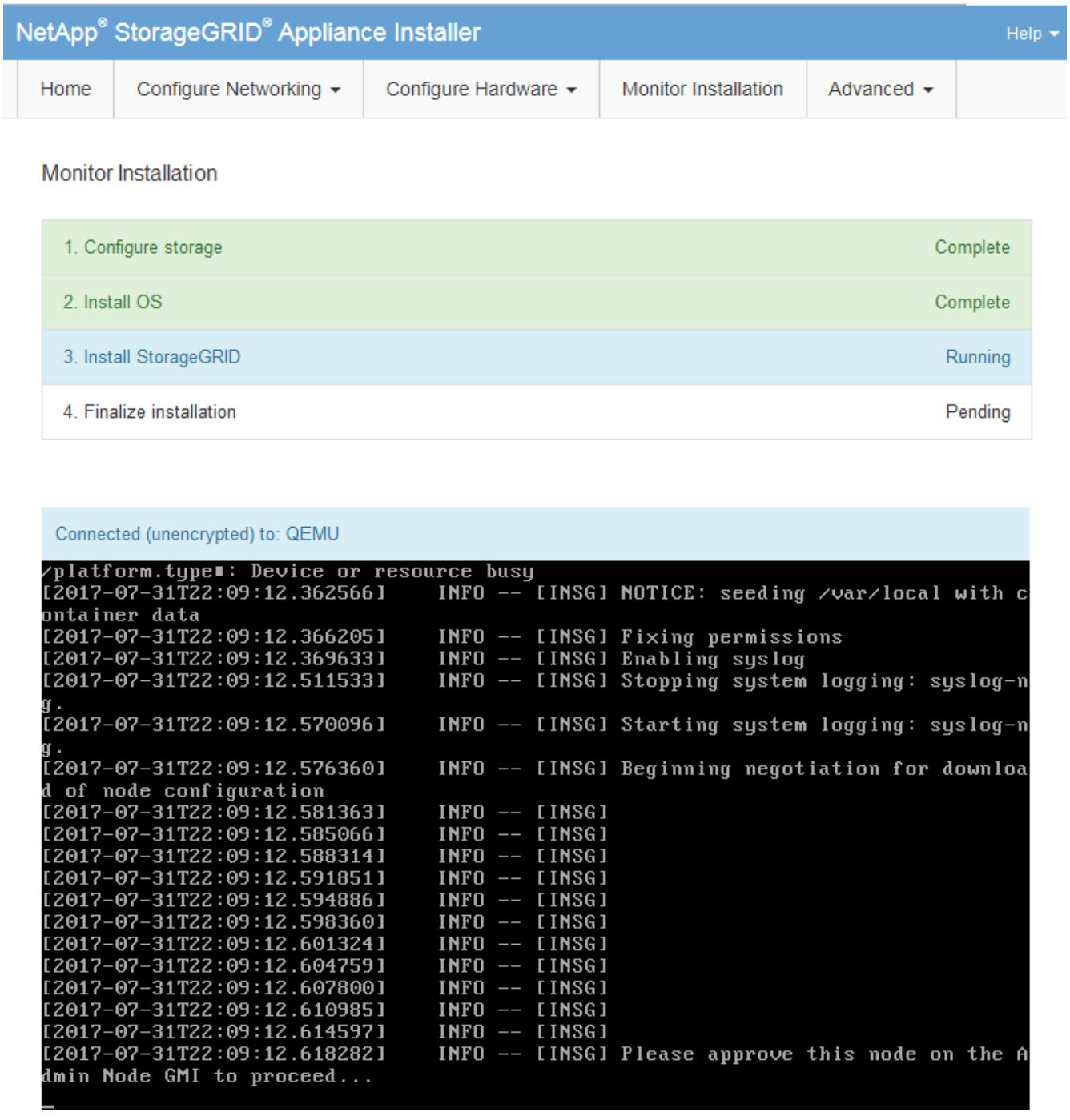
   ◦ ※ 2OS * をインストールします

     インストーラが StorageGRID のベースとなるオペレーティングシステムイメージをアプライアンスにコピーします。

3. 次のいずれかのプロセスが実行されるまで、インストールの進行状況を監視します。

   - プライマリ管理ノードを除くすべてのアプライアンスノードで、 Install StorageGRID ステージが一時停止し、組み込みのコンソールにメッセージが表示されて、グリッドマネージャを使用して管理ノードでこのノードを承認するように求められます。次の手順に進みます。
   - アプライアンスプライマリ管理ノードをインストールする場合、ノードを承認する必要はありません。アプライアンスがリブートされます。次の手順は省略できます。

   > アプライアンスプライマリ管理ノードをインストールしている場合、 5 つ目のステージが表示されます（ 4 つのフェーズを示すスクリーンショットの例を参照）。第 5 フェーズが 10 分以上たっても完了しない場合は、 Web ページを手動で更新してください。



4. グリッドマネージャに移動し、保留中のグリッドノードを承認して、StorageGRID のインストールプロセスを完了します。

   Grid Manager から * Install * をクリックすると、ステージ 3 が完了し、ステージ 4 * Finalize Installation * が開始されます。ステージ 4 が完了すると、アプライアンスがリブートされます。

アプライアンスのインストールと設定の自動化

## アプライアンスのインストールと設定、および StorageGRID システム全体の設定を自動化することができます。

このタスクについて

インストールと設定を自動化すると、複数の StorageGRID インスタンス、または大規模で複雑な StorageGRID インスタンスを 1 つ導入する場合に便利です。

インストールと設定を自動化するには、次のオプションを 1 つ以上使用します。

- アプライアンスの構成設定を指定した JSON ファイルを作成します。StorageGRID アプライアンスインストーラを使用して JSON ファイルをアップロードします。

  同じファイルを使用して、複数のアプライアンスを設定できます。

- StorageGRID を使用します`configure-sga.py` アプライアンスの設定を自動化するPythonスクリプト。
- 追加の Python スクリプトを使用して、 StorageGRID システム全体の他のコンポーネント（「グリッド」）を設定します。

Python スクリプトを StorageGRID 自動化で直接使用することも、 StorageGRID インストール REST API を独自に開発するグリッド導入および設定ツールで使用する例として使用することもできます。リカバリとメンテナンスの手順のStorageGRID インストールファイルのダウンロードと展開に関する情報を参照してください。

関連情報

""

**StorageGRID** アプライアンスインストーラを使用したアプライアンス設定の自動化

## 設定情報を含む JSON ファイルを使用して、アプライアンスの設定を自動化することができます。ファイルは StorageGRID アプライアンスインストーラを使用してアップロードします。

必要なもの

- アプライアンスは、 StorageGRID 11.5 以降と互換性のある最新のファームウェアを使用している必要があります。
- 設定するアプライアンスのStorageGRID アプライアンスインストーラに、サポートされているブラウザを使用して接続する必要があります。

このタスクについて

次の設定など、アプライアンスの設定作業を自動化することができます。

- グリッドネットワーク、管理ネットワーク、およびクライアントネットワークの IP アドレス
- BMC インターフェイス
- ネットワークリンク
  - ポートボンディングモード
  - ネットワークボンディングモード
  - リンク速度

アップロードした JSON ファイルを使用してアプライアンスを設定する方が、 StorageGRID アプライアンスインストーラの複数のページを使用して手動で設定を行うよりも効率的です。特に、多数のノードを設定する必要がある場合は効果的です。構成ファイルはノードごとに 1 つずつ適用する必要があります。

> アプライアンスのインストールと設定の両方を自動化したいと考えている経験豊富なユーザが、を使用できます `configure-sga.py` スクリプト：[+]"configure-sga.pyスクリプトを使用して、アプライアンスノードのインストールと設定を自動化する"

手順

1. 次のいずれかの方法で JSON ファイルを生成します。
   - ConfigBuilder アプリケーション

     "ConfigBuilder.netapp.com"

   - 。 `configure-sga.py` アプライアンス設定スクリプト。スクリプトは、 StorageGRID アプライアンスインストーラ（ * Help * > * アプライアンス構成スクリプト * ）からダウンロードできます。configure-sga.py スクリプトを使用して設定を自動化する手順を参照してください。

     "configure-sga.pyスクリプトを使用して、アプライアンスノードのインストールと設定を自動化する"

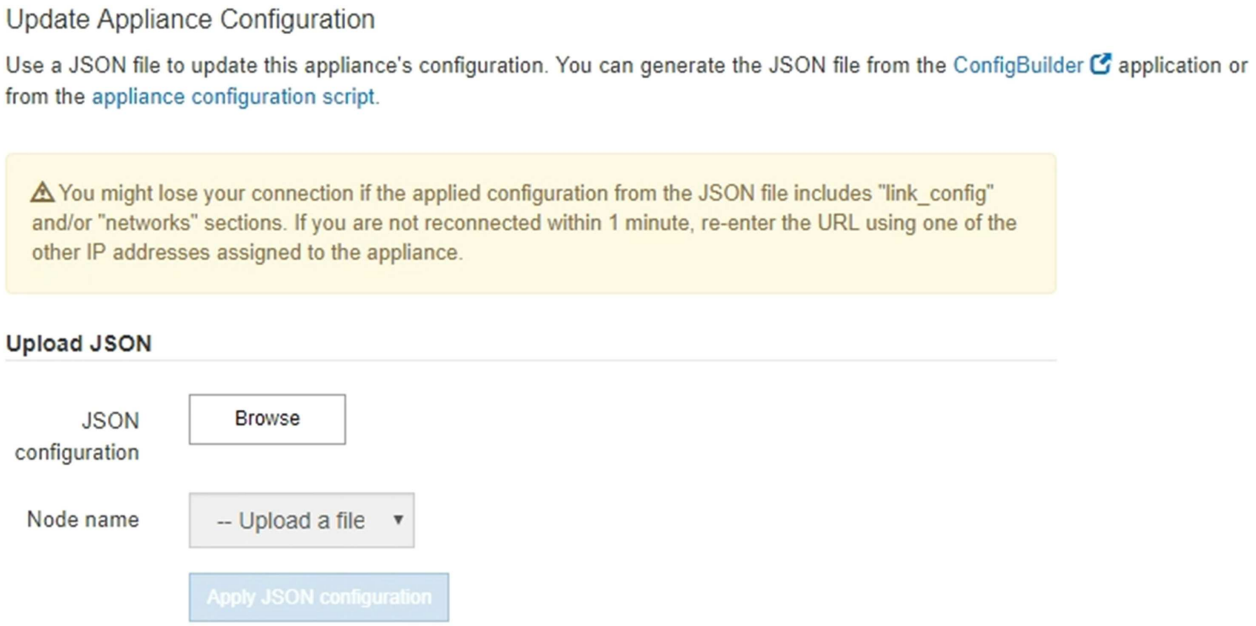
     JSON ファイル内のノード名は、次の要件に従う必要があります。

     - 1 文字以上 32 文字以下の有効なホスト名を指定する必要があります
     - アルファベット、数字、およびハイフンを使用できます
     - 1文字目または最後の文字をハイフンにすることはできません。また、数字だけを使用すること

       > JSON ファイル内のノード名（最上位の名前）が一意であることを確認してください。一意でないと、 JSON ファイルを使用して複数のノードを設定できません。

2. 「 * Advanced * > * Update Appliance Configuration * 」を選択します。

   [Update Appliance Configuration] ページが表示されます。




3. アップロードする設定の JSON ファイルを選択します。

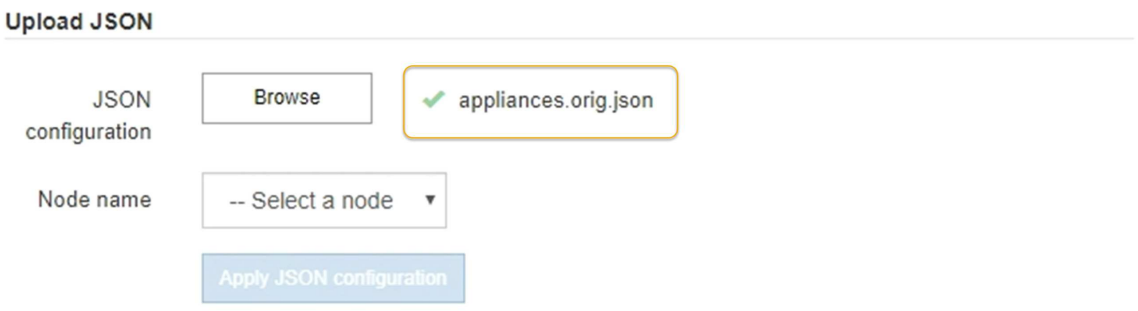
   a. [ * 参照 * ] を選択します。

   b. ファイルを探して選択します。

   c. 「 * 開く * 」を選択します。

   ファイルがアップロードされて検証されます。検証プロセスが完了すると、ファイル名が緑色のチェックマークの横に表示されます。

   JSON ファイルの構成に「 link_config 」、「 networks 」、またはその両方のセクションが含まれている場合は、アプライアンスへの接続が失われる可能性があります。1 分以内に再接続されない場合は、アプライアンスに割り当てられている他の IP アドレスのいずれかを使用して、アプライアンスの URL を再入力します。

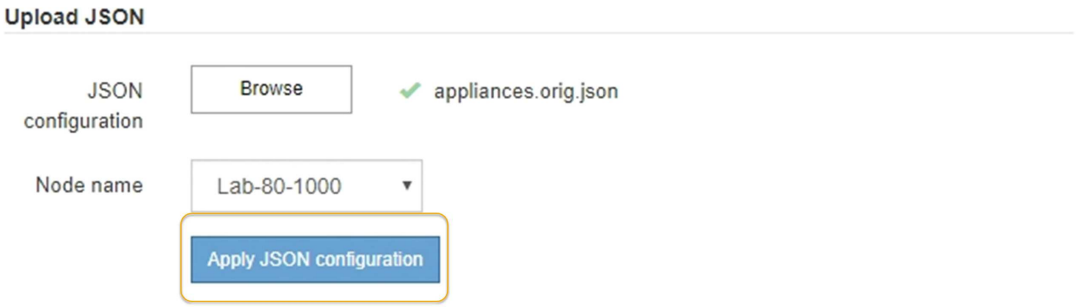



   ノード名 * ドロップダウンには、 JSON ファイルで定義された最上位のノード名が表示されます。

ファイルが有効でない場合、ファイル名は赤色で表示され、黄色のバナーにエラーメッセージが表示されます。無効なファイルはアプライアンスに適用されません。ConfigBuilder を使用して、有効な JSON ファイルを作成できます。

4. ノード名 * ドロップダウンのリストからノードを選択します。

   Apply JSON configuration * ボタンが有効になっている。




5. Apply JSON configuration * を選択します。

   選択したノードに構成が適用されます。

**configure-sga.py**スクリプトを使用して、アプライアンスノードのインストールと設定を自動化する

を使用できます `configure-sga.py` プライマリ管理ノードのインストールや設定など、StorageGRID アプライアンスノードのインストールタスクや設定タスクの多くを自動化するスクリプトです。このスクリプトは、設定するアプライアンスが多数ある場合に役立ちます。スクリプトを使用して、アプライアンスの設定情報を含む JSON ファイルを生成することもできます。

必要なもの

- アプライアンスをラックに設置し、ネットワークに接続し、電源を投入しておきます。
- StorageGRID アプライアンスインストーラを使用してプライマリ管理ノードのネットワークリンクと IP アドレスを設定しておきます。
- プライマリ管理ノードをインストールする場合は、その IP アドレスを確認しておきます。
- 他のノードをインストールして設定する場合は、プライマリ管理ノードが導入され、その IP アドレスを確認しておきます。
- プライマリ管理ノード以外のすべてのノードについて、 StorageGRID アプライアンスインストーラの IP 設定ページに表示されるすべてのグリッドネットワークサブネットが、プライマリ管理ノードのグリッドネットワークサブネットリストで定義されている。
- をダウンロードしておきます `configure-sga.py` ファイル。このファイルはインストール・アーカイブに含まれています。または、 StorageGRID アプライアンス・インストーラの * Help * > * Appliance Installation Script * をクリックしてアクセスできます。

この手順 は、コマンドラインインターフェイスを使用した経験のある上級ユーザを対象としています。また、 StorageGRID アプライアンスインストーラを使用して設定を自動化することもできます。[+]"StorageGRID アプライアンスインストーラを使用したアプライアンス設定の自動化"

手順

1. Python スクリプトを実行するために使用する Linux マシンにログインします。
2. スクリプト構文に関する一般的なヘルプおよび使用可能なパラメータの一覧を表示するには、次のように入力します。

```
configure-sga.py --help
```

   。 `configure-sga.py` スクリプトでは、次の5つのサブコマンド

   ◦ `advanced` BMCの設定、アプライアンスの現在の設定を含むJSONファイルの作成など、StorageGRID アプライアンスの高度な操作用

   ◦ `configure` RAIDモード、ノード名、およびネットワークパラメータを設定するために使用します

   ◦ `install` StorageGRID のインストールを開始する場合に使用します

   ◦ `monitor` StorageGRID インストールの監視用です

   ◦ `reboot` アプライアンスのリブート用です

   サブコマンド（advanced、configure、install、monitor、またはreboot）引数のあとにを入力すると `--help` オプションを指定すると、そのサブコマンド内で使用可能なオプションの詳細を示すヘルプテキストが表示されます
   `configure-sga.py` *`subcommand`* `--help`

3. アプライアンスノードの現在の設定を確認するには、以下のコマンドをどこに入力するかを確認します *`SGA-install-ip`* には、アプライアンスノードのいずれかのIPアドレスを指定します。+
`configure-sga.py configure` *`SGA-INSTALL-IP`*

   この結果には、プライマリ管理ノードの IP アドレスや管理、グリッド、クライアントネットワークに関する情報など、アプライアンスの現在の IP 情報が表示されます。

```
Connecting to +https://10.224.2.30:8443+ (Checking version and
connectivity.)
2021/02/25 16:25:11: Performing GET on /api/versions... Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/system-info... Received
200
2021/02/25 16:25:11: Performing GET on /api/v2/admin-connection...
Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/link-config... Received
200
2021/02/25 16:25:11: Performing GET on /api/v2/networks... Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/system-config... Received
200
```

```
StorageGRID Appliance
  Name:        LAB-SGA-2-30
  Node type:   storage

StorageGRID primary Admin Node
  IP:        172.16.1.170
  State:     unknown
  Message:   Initializing...
  Version:   Unknown

Network Link Configuration
  Link Status
        Link      State      Speed (Gbps)
        ----      -----      -----
        1         Up         10
        2         Up         10
        3         Up         10
        4         Up         10
        5         Up         1
        6         Down       N/A

  Link Settings
      Port bond mode:      FIXED
      Link speed:          10GBE

      Grid Network:        ENABLED
          Bonding mode:    active-backup
          VLAN:            novlan
          MAC Addresses:   00:a0:98:59:8e:8a  00:a0:98:59:8e:82

      Admin Network:       ENABLED
          Bonding mode:    no-bond
          MAC Addresses:   00:80:e5:29:70:f4

      Client Network:      ENABLED
          Bonding mode:    active-backup
          VLAN:            novlan
          MAC Addresses:   00:a0:98:59:8e:89  00:a0:98:59:8e:81

Grid Network
  CIDR:      172.16.2.30/21 (Static)
  MAC:       00:A0:98:59:8E:8A
  Gateway:   172.16.0.1
  Subnets:   172.17.0.0/21
             172.18.0.0/21
```

```
                192.168.0.0/21
    MTU:        1500

  Admin Network
    CIDR:       10.224.2.30/21 (Static)
    MAC:        00:80:E5:29:70:F4
    Gateway:    10.224.0.1
    Subnets:    10.0.0.0/8
                172.19.0.0/16
                172.21.0.0/16
    MTU:        1500

  Client Network
    CIDR:       47.47.2.30/21 (Static)
    MAC:        00:A0:98:59:8E:89
    Gateway:    47.47.0.1
    MTU:        2000

#####################################################################
#####   If you are satisfied with this configuration,    #####
##### execute the script with the "install" sub-command. #####
#####################################################################
```

4. 現在の設定のいずれかの値を変更する必要がある場合は、を使用します `configure` サブコマンドを使用して更新します。たとえば、アプライアンスがプライマリ管理ノードへの接続に使用するIPアドレスをに変更する場合などです `172.16.2.99`をクリックし、「+」と入力します
`configure-sga.py configure --admin-ip 172.16.2.99 SGA-INSTALL-IP`
5. アプライアンスの設定をJSONファイルにバックアップする場合は、advanced権限とを使用します `backup-file` サブコマンド。たとえば、IPアドレスを持つアプライアンスの設定をバックアップする場合などです *SGA-INSTALL-IP* を指定します `appliance-SG1000.json`をクリックし、「+」と入力します
`configure-sga.py advanced --backup-file appliance-SG1000.json SGA-INSTALL-IP`

   設定情報が格納された JSON ファイルは、スクリプトの実行元と同じディレクトリに書き込まれます。

   > 生成された JSON ファイルの最上位のノード名がアプライアンス名と一致していることを確認します。経験豊富なユーザで StorageGRID API について十分な知識がある場合を除き、このファイルに変更を加えないでください。

6. アプライアンスの設定に問題がなければ、を使用します `install` および `monitor` アプライアンスをインストールするためのサブコマンド：+
`configure-sga.py install --monitor SGA-INSTALL-IP`
7. アプライアンスをリブートする場合は、「+」を入力します
`configure-sga.py reboot SGA-INSTALL-IP`

# グリッドノードを導入したら、 StorageGRID システムの設定を自動化できます。

必要なもの

- インストールアーカイブにある次のファイルの場所を確認しておきます。

| ファイル名 | 説明 |
| --- | --- |
| `configure-storagegrid.py` | 設定を自動化するための Python スクリプト |
| `configure-storagegrid.sample.json` | スクリプトで使用するサンプル構成ファイル |
| `configure-storagegrid.blank.json` | スクリプトで使用する空の構成ファイルです |

- を作成しておきます `configure-storagegrid.json` 構成ファイルこのファイルを作成するには、サンプル構成ファイルを変更します (`configure-storagegrid.sample.json`)または空の構成ファイル (`configure-storagegrid.blank.json`) 。

このタスクについて

を使用できます `configure-storagegrid.py` Pythonスクリプトおよび `configure-storagegrid.json` StorageGRID システムの設定を自動化するための構成ファイル。

また、 Grid Manager またはインストール API を使用してシステムを設定することもできます。

手順

1. Python スクリプトを実行するために使用する Linux マシンにログインします。
2. インストールアーカイブを展開したディレクトリに移動します。

   たとえば、「+」と入力します
   `cd StorageGRID-Webscale-version/platform`

   ここで、 *platform* はです `debs`、 `rpms`または `vsphere`。

3. Python スクリプトを実行し、作成した構成ファイルを使用します。

   例：

```
./configure-storagegrid.py ./configure-storagegrid.json --start-install
```

完了後

リカバリパッケージ `.zip` 設定プロセスでファイルが生成され、インストールと設定を実行するディレクトリにダウンロードされます。グリッドノードで障害が発生した場合に StorageGRID システムをリカバリできるようにするために、リカバリパッケージファイルをバックアップする必要があります。たとえば、バックアップされたセキュアなネットワーク上の場所や、安全なクラウドストレージ上の場所にコピーします。

リカバリパッケージファイルには StorageGRID システムからデータを取得するための暗号キーとパスワードが含まれているため、安全に保管する必要があります。

ランダムパスワードを生成するように指定した場合は、を展開する必要があります `Passwords.txt` ファイルを開き、StorageGRID システムへのアクセスに必要なパスワードを探します。

```
######################################################################
##### The StorageGRID "recovery package" has been downloaded as: #####
#####           ./sgws-recovery-package-994078-rev1.zip          #####
#####   Safeguard this file as it will be needed in case of a    #####
#####                 StorageGRID node recovery.                 #####
######################################################################
```

StorageGRID システムがインストールおよび設定されると、確認メッセージが表示されます。

```
StorageGRID has been configured and installed.
```

インストール **REST API** の概要

## StorageGRID には、インストールタスクを実行するための REST API として、StorageGRID インストール API と StorageGRID アプライアンスインストーラ API の 2 つが用意されています。

どちらの API も、 Swagger オープンソース API プラットフォームを使用して API のドキュメントを提供しています。Swagger では、ユーザインターフェイスを使用してパラメータやオプションを変更した場合の API の動作を確認しながら、 API の開発を進めることができます。このドキュメントは、標準的な Web テクノロジと JavaScript Object Notation （ JSON ）データ形式について十分理解していることを前提としています。

API Docs Web ページを使用して実行する API 処理はすべてその場で実行されます。設定データやその他のデータを誤って作成、更新、または削除しないように注意してください。

各 REST API コマンドは、 API の URL 、 HTTP アクション、必須またはオプションの URL パラメータ、および想定される API 応答で構成されます。

#### **StorageGRID** インストール **API**

StorageGRID インストール API は、 StorageGRID システムを最初に設定するとき、およびプライマリ管理ノードのリカバリを実行する必要がある場合にのみ使用できます。インストール API には、 Grid Manager から HTTPS 経由でアクセスできます。

API のドキュメントにアクセスするには、プライマリ管理ノードのインストール用 Web ページに移動し、メニューバーから * Help * > * API Documentation * を選択します。

StorageGRID インストール API には次のセクションがあります。

- *config *-- API の製品リリースとバージョンに関連する操作。製品リリースバージョンおよびそのリリースでサポートされる API のメジャーバージョンを一覧表示できます。

- * grid * — グリッドレベルの設定操作。グリッドの詳細、グリッドネットワークのサブネット、グリッドパスワード、 NTP および DNS サーバの IP アドレスなど、グリッド設定を取得および更新できます。
- *nodes * — ノードレベルの設定操作。グリッドノードのリストを取得できるほか、グリッドノードの削除、設定、表示、およびグリッドノードの設定のリセットを行うことができます。
- *provision * — プロビジョニング操作。プロビジョニング処理を開始し、プロビジョニング処理のステータスを表示できます。
- * recovery * - プライマリ管理ノードのリカバリ処理。情報のリセット、リカバリパッケージのアップロード、リカバリの開始、およびリカバリ処理のステータスの表示を行うことができます。
- * recovery-package * — リカバリパッケージをダウンロードする処理。
- *sites * — サイトレベルの設定操作。サイトを作成、表示、削除、および変更できます。

#### StorageGRID アプライアンスインストーラ API

StorageGRID アプライアンスインストーラAPIには、からHTTPS経由でアクセスできます `Controller_IP:8443`。

API ドキュメントにアクセスするには、アプライアンスの StorageGRID アプライアンスインストーラのメニューバーから * Help * > * API Docs * を選択します。

StorageGRID アプライアンスインストーラ API には、次のセクションがあります。

- * clone * — ノードのクローニングを構成および制御するための処理。
- *encryption * — 暗号化を管理し、暗号化ステータスを表示するための処理。
- * ハードウェア構成 * — 接続されたハードウェアでシステム設定を構成するための操作。
- *installation * ：アプライアンスのインストールを開始し、インストール・ステータスを監視するための処理。
- * networking * — StorageGRID アプライアンスのグリッドネットワーク、管理ネットワーク、クライアントネットワークの設定、およびアプライアンスのポート設定に関連する処理です。
- * setup * - システムに関する情報の取得やプライマリ管理ノード IP の更新要求など、アプライアンスの初期インストール設定に役立つ処理。
- *support *--コントローラのリブートとログ取得のための処理。
- * upgrade * ：アプライアンス・ファームウェアのアップグレードに関連する操作
- **uploadsg** — StorageGRID インストールファイルをアップロードするための操作。

## ハードウェアの設置のトラブルシューティング

設置作業で問題が発生した場合は、ハードウェアのセットアップや接続の問題に関するトラブルシューティング情報を確認すると役立つことがあります。

関連情報

"ハードウェアのセットアップがハングしたように見えます"

"接続の問題のトラブルシューティング"

# アプライアンスに電源を投入すると、 BMC に一連のブート時コードが記録されます。BMC 管理ポートに接続されているグラフィカルコンソールでこれらのコードを確認できます。

必要なもの

- BMC ダッシュボードへのアクセス方法を確認しておく必要があります。
- Kernel-based Virtual Machine（KVM）を使用する場合は、KVMアプリケーションの導入および使用経験が必要です。
- Serial-Over-LAN （ SOL ）を使用する場合は、 IPMI SOL コンソールアプリケーションの使用経験が必要です。

手順

1. アプライアンスコントローラのブート時のコードを確認するための方法を選択し、必要な機器を揃えます。

| メソッド | 必要な機器 |
| --- | --- |
| VGA コンソール | • VGA 対応モニタ<br>• VGA ケーブル |
| KVM の略 | • KVMアプリケーション<br>• RJ-45 ケーブル |
| シリアルポート | • DB-9 シリアルケーブル<br>• 仮想シリアルターミナル |
| ソル | • 仮想シリアルターミナル |

2. VGA コンソールを使用する場合は、次の手順を実行します。
   a. VGA 対応モニタをアプライアンス背面の VGA ポートに接続します。
   b. モニタに表示されるコードを確認します。
3. BMC KVM を使用する場合は、次の手順を実行します。
   a. BMC 管理ポートに接続し、 BMC の Web インターフェイスにログインします。
   b. 「 * リモートコントロール * 」を選択します。
   c. KVM を起動します。
   d. 仮想モニタのコードを確認します。
4. シリアルポートと端末を使用している場合は、次の手順を実行します。
   a. アプライアンス背面の DB-9 シリアルポートに接続します。
   b. 設定を使用します `115200 8-N-1`。

c. シリアルターミナルに印刷されているコードを確認します。

5. SOL を使用する場合は、次の手順を実行します。

a. BMC の IP アドレスとログインクレデンシャルを使用して IPMI SOL に接続します。

```
ipmitool -I lanplus -H 10.224.3.91 -U root -P calvin sol activate
```

b. 仮想シリアルターミナルのコードを確認します。

6. 次の表を使用して、アプライアンスのコードを確認します。

| コード | を示します |
| --- | --- |
| こんにちは | マスターブートスクリプトが開始されました。 |
| HP | ネットワークインターフェイスカード（ NIC ）の更新が必要かどうかをシステムがチェックしています。 |
| 朝食付き | ファームウェアの更新の適用が完了し、システムがリブートしています。 |
| FP | ハードウェアサブシステムのファームウェアの更新の確認が完了しました。コントローラ間の通信サービスが開始されています。 |
| HC | 既存の StorageGRID のインストールデータがチェックされています。 |
| HO | StorageGRID アプライアンスは稼働しています。 |
| 高可用性 | StorageGRID が実行されています。 |

関連情報

"BMCインターフェイスへのアクセス"

アプライアンスのエラーコードの確認

アプライアンスのブート時にハードウェアエラーが発生すると、 BMC にエラーコードが記録されます。必要に応じて BMC インターフェイスを使用してこれらのエラーコードを確認し、テクニカルサポートと協力して問題 を解決できます。

必要なもの

- BMC ダッシュボードへのアクセス方法を確認しておく必要があります。

手順

1. BMC ダッシュボードで、 * BIOS POST Code * を選択します。

2. 現在のコードと前のコードについて表示された情報を確認します。

   次のいずれかのエラーコードが表示された場合は、テクニカルサポートに連絡して問題 を解決してください。

| コード | を示します |
| --- | --- |
| 0x0E | マイクロコードが見つかりません |
| 0x0F | マイクロコードがロードされません |
| 0x50 | メモリの初期化エラー。メモリタイプが無効か、メモリ速度に互換性がありません。 |
| 0x51 | メモリの初期化エラー。SPD の読み取りに失敗しました。 |
| 0x52 | メモリの初期化エラー。メモリサイズが無効か、メモリモジュールが一致しません。 |
| 0x53 | メモリの初期化エラー。使用可能なメモリが検出されませんでし |
| 0x54 | 不明なメモリ初期化エラー |
| 0x55 | メモリが取り付けられていません |
| 0x56 | CPU のタイプまたは速度が無効です |
| 0x57 | CPU が一致しません |
| 0x58 | CPU セルフテストに失敗したか、 CPU キャッシュエラーの可能性があります |
| 0x59 | CPU マイクロコードが見つからないか、マイクロコードの更新に失敗しました |
| 0x5A | 内部 CPU エラー |
| 0x5B | リセット PPI が使用できません |
| 0x5C | PEI フェーズの BMC セルフテストに失敗しました |
| 0xD0 | CPU の初期化エラー |

| コード | を示します |
| --- | --- |
| 0xD1 | ノースブリッジの初期化エラー |
| 0xD2 | サウスブリッジの初期化エラー |
| 0xd3 | 一部のアーキテクチャプロトコルが使用できません |
| 0xD4 | PCI リソースの割り当てエラー。リソース不足です。 |
| 0xD5 | レガシーオプション ROM 用のスペースがありません |
| 0xD6 | コンソール出力デバイスが見つかりません |
| 0xD7 | コンソール入力デバイスが見つかりません |
| 0xD8 | パスワードが無効です |
| 0xD9 | ブートオプションのロードエラー（ LoadImage がエラーを返しました） |
| 0xda | ブートオプションが失敗しました（ StartImage がエラーを返しました）。 |
| 0xDB | フラッシュの更新に失敗しました |
| 0xDC | リセットプロトコルは使用できません |
| 0xDD | DXE フェーズの BMC セルフテストに失敗しました |
| 0xE8 | MRC ： ERR_NO_MEMORY |
| 0xE9 | MRC ： ERR_LT_LOCK |
| 0xEA | MRC ： ERR_DDR_INIT |
| 0xEB | MRC ： ERR_MEM_TEST |
| 0xEC | MRC ： ERR_VENDER_Specific |
| 0xED | MRC ： ERR_DIMM_COMPAT |

| コード | を示します |
| --- | --- |
| 0xEE | MRC ： ERR_MRC_compatibility |
| 0xef | MRC ： ERR_MRC_STRUCT |
| 0xF0 | MRC ： ERR_SET_VDD |
| 0xf1 | MRC ： ERR_IOT_MEM_BUFFER |
| 0xF2 | MRC ： ERR_RC_INTERNAL |
| 0xF3 | MRC ： ERR_INVALL_REG_ACCESS |
| 0xF4 | MRC ： ERR_SET_MC_Freq |
| 0xf5 | MRC ： ERR_READ_MC_Freq |
| 0x70 | MRC ： ERR_DIMM_CHANNEL |
| 0x74 | MRC ： ERR_BIST チェック |
| 0xF6 | MRC ： ERR_SMBus |
| 0xF7 | MRC ： ERR_PCU |
| 0xf8 | MRC ： ERR_NGN |
| 0xF9 | MRC ： ERR_interleave_failure |

ハードウェアのセットアップがハングしたように見えます

## ハードウェア障害やケーブル接続エラーによってアプライアンスのブート処理が完了しなかった場合は、 StorageGRID アプライアンスインストーラを使用できなくなることがあります。

手順

1. アプライアンスの LED と、 BMC に表示されるブートコードとエラーコードを確認します。
2. 問題 の解決にサポートが必要な場合は、テクニカルサポートにお問い合わせください。

関連情報

"アプライアンスのブート時のコードを確認する"

"アプライアンスのエラーコードの確認"

# StorageGRID アプライアンスのインストール時に接続の問題が発生した場合は、以下に記載する対処策を実施する必要があります。

## アプライアンスに接続できません

## サービスアプライアンスに接続できない場合は、ネットワーク問題 があるか、またはハードウェアの設置が正常に完了していない可能性があります。

手順

1. アプライアンスのIPアドレスを使用してアプライアンスにpingを送信します。+
**`ping services_appliance_IP`**
2. ping からの応答がない場合は、正しい IP アドレスを使用していることを確認します。

   グリッドネットワーク、管理ネットワーク、またはクライアントネットワークでのアプライアンスの IP アドレスを使用できます。

3. IP アドレスが正しい場合は、アプライアンスのケーブル接続、 QSFP または SFP トランシーバ、およびネットワークのセットアップを確認します。

   この手順で問題 が解決しない場合は、テクニカルサポートにお問い合わせください。

4. ping が成功した場合は、 Web ブラウザを開きます。
5. StorageGRID アプライアンスインストーラのURLとして「+」を入力します
**`https://appliances_controller_IP:8443`**

   ホームページが表示されます。

## **StorageGRID** アプライアンスインストーラの実行中にサービスアプライアンスをリブートする

## StorageGRID アプライアンスインストーラの実行中に、サービスアプライアンスのリブートが必要になる場合があります。たとえば、インストールが失敗した場合はサービスアプライアンスのリブートが必要になることがあります。

このタスクについて

この手順 は、サービスアプライアンスで StorageGRID アプライアンスインストーラが実行されている場合にのみ適用されます。インストールが完了すると、 StorageGRID アプライアンスインストーラが使用できなくなるため、この手順は機能しなくなります。

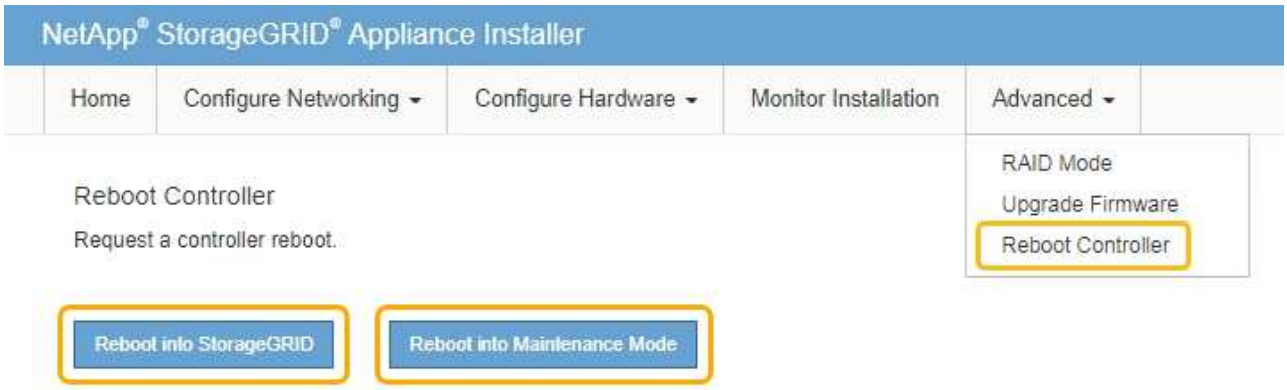
手順

1. StorageGRID アプライアンス・インストーラのメニュー・バーから、 [**Advanced**>*Reboot Controller*] をクリックします。

   Reboot Controller ページが表示されます。

2. StorageGRID アプライアンス・インストーラで、 [**Advanced**>*Reboot Controller*] をクリックし、次のいずれかのオプションを選択します。

- Reboot into StorageGRID * を選択し、ノードをグリッドに再追加してコントローラをリブートします。メンテナンスモードで作業を完了し、ノードを通常動作に戻す準備ができている場合は、このオプションを選択します。
- メンテナンスモードを維持したままコントローラをリブートするには、 * Reboot into Maintenance Mode * を選択します。このオプションは、グリッドに再追加する前にノードで追加のメンテナンス処理を実行する必要がある場合に選択しま
す。




サービスアプライアンスがリブートされます。

## アプライアンスのメンテナンス

アプライアンスのメンテナンス作業が必要になることがあります。このセクションの手順は、アプライアンスが StorageGRID システムにゲートウェイノードまたは管理ノードとしてすでに導入されていることを前提としています。

手順

- "アプライアンスをメンテナンスモードにします"
- "コントローラ識別LEDのオンとオフの切り替え"
- "コントローラのデータセンターへの配置"
- "サービスアプライアンスの交換"
- "サービスアプライアンスの電源装置の交換"
- "サービスアプライアンスのファンの交換"
- "サービスアプライアンスのドライブの交換"
- "サービスアプライアンスのリンク設定の変更"
- "MTU設定を変更します"
- "DNSサーバの設定を確認しています"
- "メンテナンスモードでのノード暗号化の監視"

# 特定のメンテナンス手順を実行する前に、アプライアンスをメンテナンスモードにする必要があります。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Maintenance または Root Access 権限が必要です。詳細については、 StorageGRID の管理手順を参照してください。

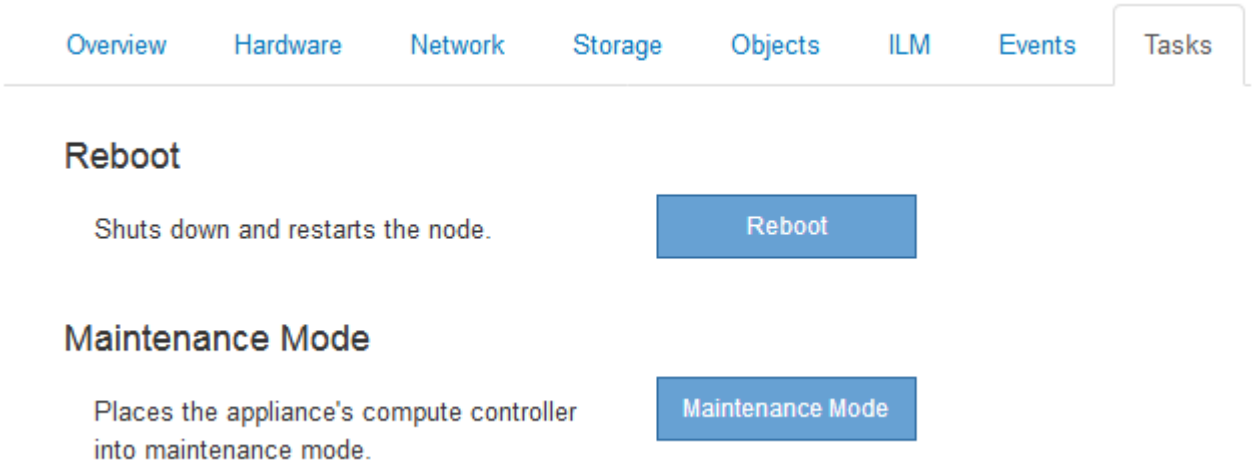
このタスクについて

StorageGRID アプライアンスをメンテナンスモードにすると、アプライアンスにリモートアクセスできなくなることがあります。

> 保守モードのStorageGRID アプライアンスのパスワードおよびホスト・キーは、アプライアンスが稼働していたときと同じままです。

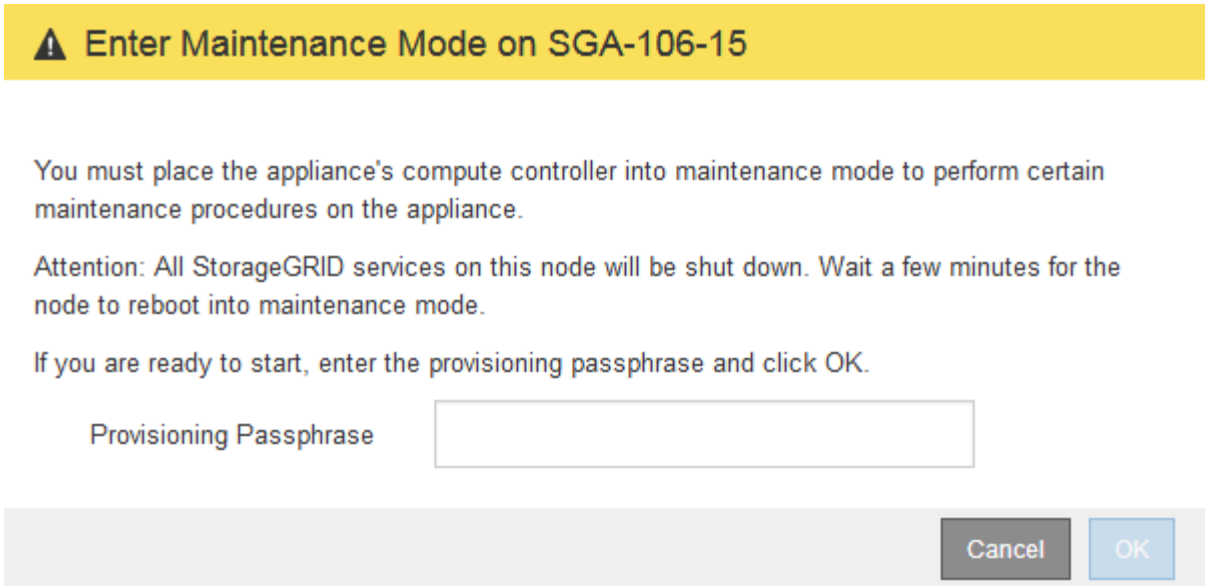
手順

1. Grid Managerから* Nodes *を選択します。
2. Nodes ページのツリービューで、アプライアンスストレージノードを選択します。
3. [ タスク ] を選択します。



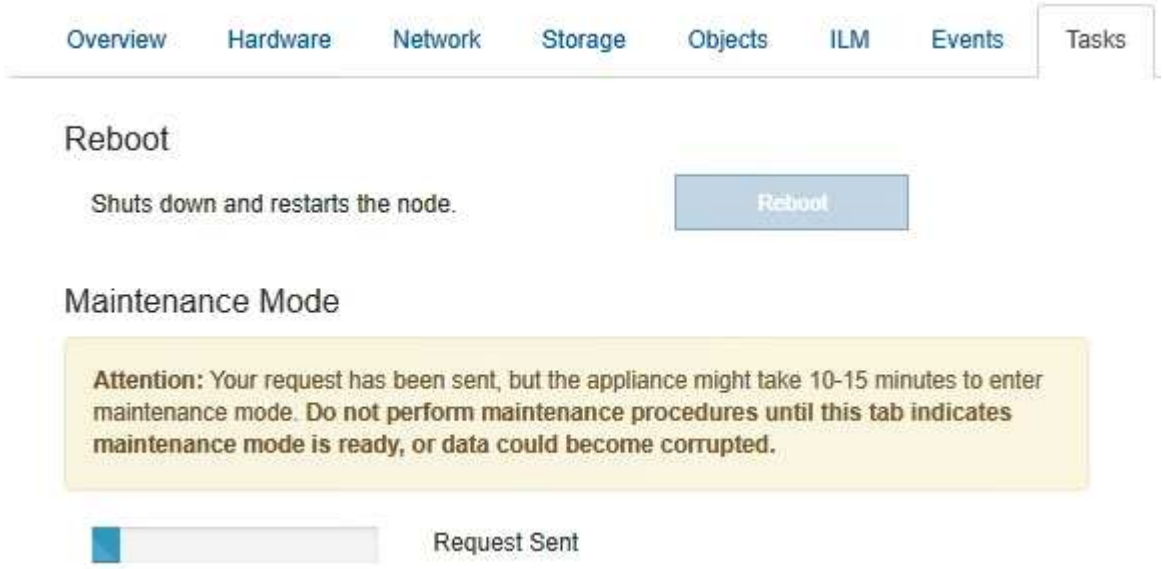

4. [* Maintenance Mode]*を選択します。

   確認のダイアログボックスが表示されます。

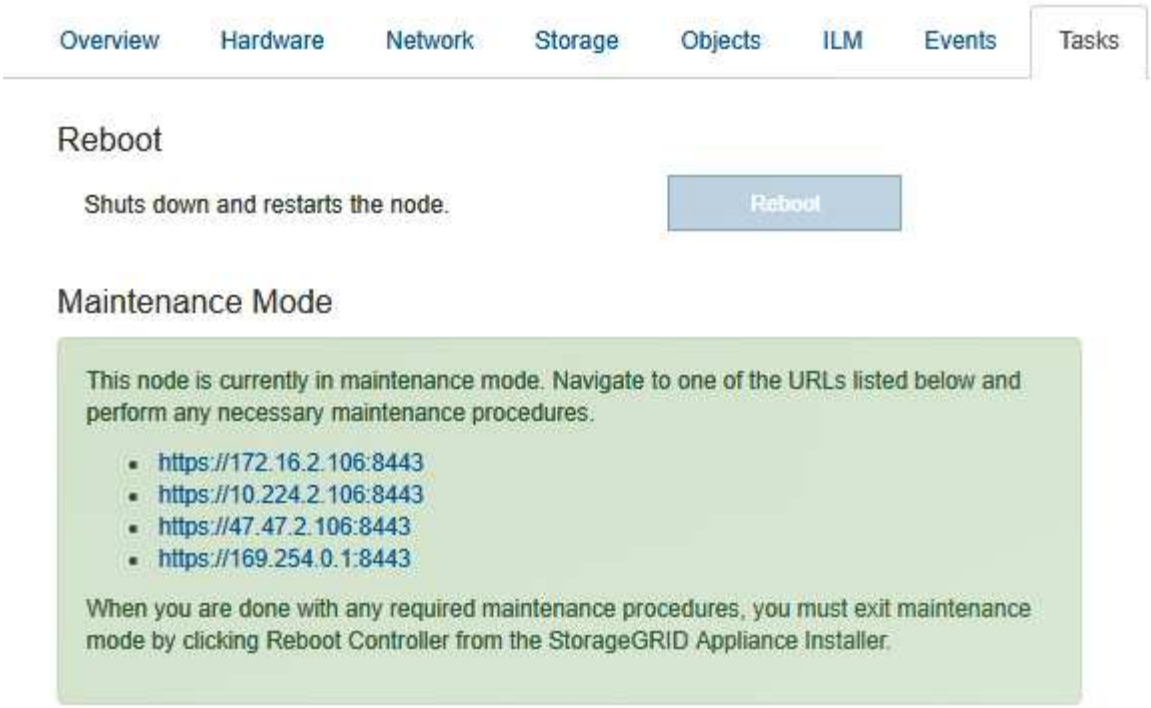



5. プロビジョニングパスフレーズを入力し、「 * OK 」を選択します。

進捗状況バーと一連のメッセージ（「 Request Sent 」、「 Stopping StorageGRID 」、「 Rebaling 」など）は、アプライアンスがメンテナンスモードに移行するための手順を完了していることを示しています。




アプライアンスがメンテナンスモードになっている場合は、 StorageGRID アプライアンスインストーラへのアクセスに使用できる URL が確認メッセージに表示されます。



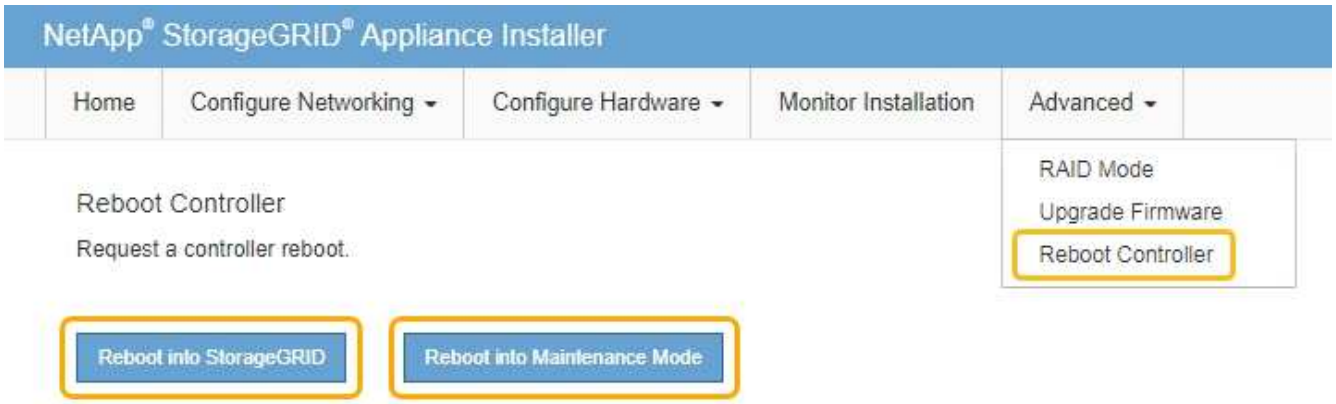

6. StorageGRID アプライアンスインストーラにアクセスするには、表示されたいずれかの URL にアクセスします。

   可能であれば、アプライアンスの管理ネットワークポートの IP アドレスを含む URL を使用します。

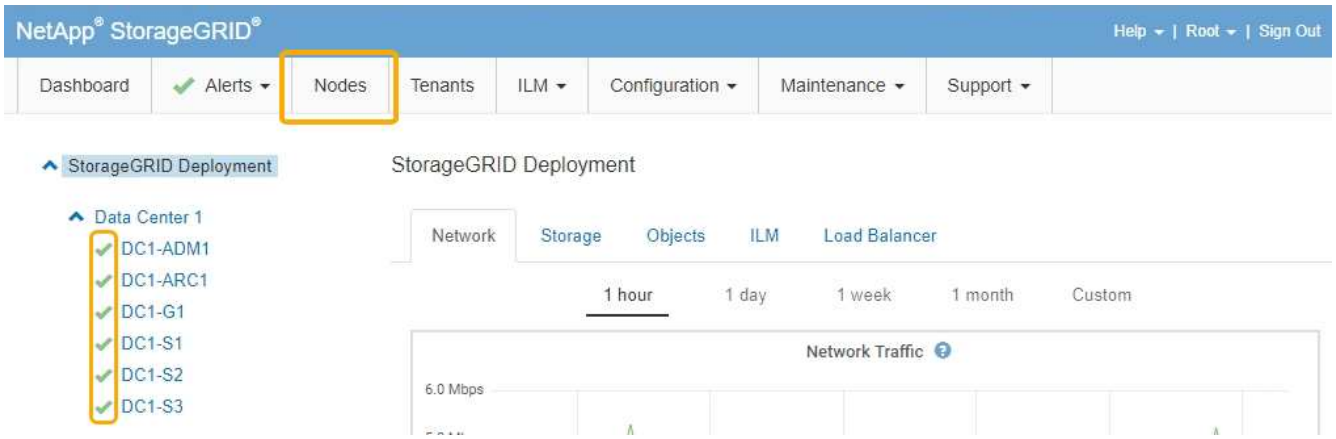
   > へのアクセス `https://169.254.0.1:8443` ローカル管理ポートに直接接続する必要があります。

7. StorageGRID アプライアンスインストーラで、アプライアンスがメンテナンスモードになっていることを確認します。

8. 必要なメンテナンスタスクを実行します。
9. メンテナンス作業が完了したら、メンテナンスモードを終了して通常のノードの運用を再開します。StorageGRID アプライアンス・インストーラから、 **Advanced**>* Reboot Controller* を選択し、 * Reboot into StorageGRID * を選択します。




アプライアンスがリブートしてグリッドに再参加するまでに最大 20 分かかることがあります。リブートが完了し、ノードが再びグリッドに参加したことを確認するには、 Grid Manager に戻ります。[ノード*（Nodes *）]タブには、通常のステータスが表示されます ✔ アクティブなアラートがなく、ノードがグリッドに接続されていることを示す、アプライアンスノードの場合。




コントローラ識別**LED**のオンとオフの切り替え

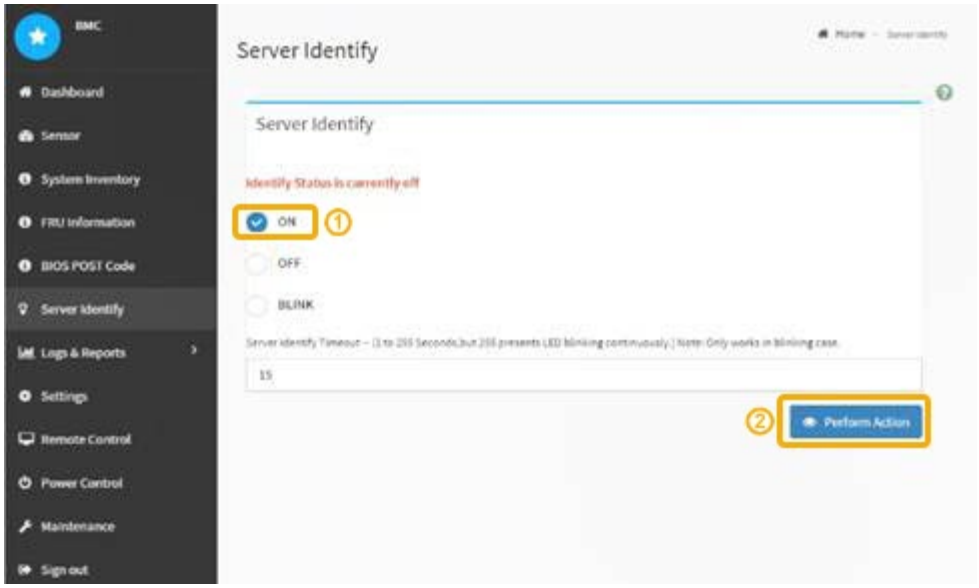
## コントローラの前面と背面にある青色の識別 LED は、データセンターでアプライアンスを特定するのに役立ちます。

必要なもの

識別するコントローラの BMC IP アドレスが必要です。

手順

1. コントローラの BMC インターフェイスにアクセスします。
2. 「 * サーバー識別 * 」を選択します。
3. 「 * オン * 」を選択し、「 * アクションの実行 * 」を選択します。




結果

青色の識別 LED は、コントローラの前面（図）と背面（図）に点灯します。

コントローラにベゼルが取り付けられている場合、前面の識別 LED が見えにくいことがあります。

完了後

コントローラ識別 LED を消灯するには、次の手順を実行します。

- コントローラの前面パネルにある識別 LED スイッチを押します。
- コントローラの BMC インターフェイスから、 * Server identify * を選択し、 * off * を選択して、 * Perform Action * を選択します。

コントローラの前面と背面の青色の識別 LED が消灯します。

関連情報

"コントローラのデータセンターへの配置"

"BMCインターフェイスへのアクセス"

コントローラのデータセンターへの配置

# ハードウェアのメンテナンスやアップグレードを実行できるように、コントローラを特定します。

必要なもの

- メンテナンスが必要なコントローラを特定しておきます。

  （オプション）データセンター内のコントローラの位置を確認するには、青色の識別 LED をオンにします。

  "コントローラ識別LEDのオンとオフの切り替え"

手順

1. データセンターでメンテナンスが必要なコントローラを特定します。

   - コントローラの前面または背面の LED が青色に点灯していることを確認します。

     前面の識別 LED はコントローラの前面ベゼルの背面にあり、ベゼルが取り付けられているかどうかを確認するのが困難な場合があります。

◦ 各コントローラの前面にあるタグで、一致するパーツ番号を確認します。

2. コントローラの前面ベゼルが取り付けられている場合は、前面パネルのコントロールとインジケータにアクセスするために取り外します。
3. オプション：コントローラの場所を確認するために使用した場合は、青色の識別 LED を消灯します。
   ◦ コントローラの前面パネルにある識別 LED スイッチを押します。
   ◦ コントローラの BMC インターフェイスを使用します。

   "コントローラ識別LEDのオンとオフの切り替え"

サービスアプライアンスの交換

## アプライアンスが適切に機能しない場合や障害が発生した場合は、交換が必要となることがあります。

必要なもの

- 交換するアプライアンスと同じパーツ番号の交換用アプライアンスを用意しておきます。
- アプライアンスに接続する各ケーブルを識別するためのラベルを用意しておきます。
- データセンター内で交換するアプライアンスの物理的な場所を確認しておきます。を参照してください "コントローラのデータセンターへの配置"。
- アプライアンスのメンテナンスモードが開始されました。を参照してください "アプライアンスをメンテナンスモードにします"。

このタスクについて

アプライアンスの交換中は、 StorageGRID ノードにアクセスできなくなります。アプライアンスが動作している場合は、この手順 の起動時に通常の方法でシャットダウンを実行できます。

> StorageGRID ソフトウェアをインストールする前にアプライアンスを交換すると、この手順 の完了後すぐに StorageGRID アプライアンスインストーラにアクセスできない場合があります。アプライアンスと同じサブネット上の他のホストから StorageGRID アプライアンスインストーラにアクセスすることはできますが、他のサブネット上のホストからはアクセスできません。この状態は 15 分以内に（元のアプライアンスのいずれかの ARP キャッシュエントリがタイムアウトした時点で）自動的に解消されます。あるいは、古い ARP キャッシュエントリをローカルルータまたはゲートウェイから手動でパージすれば、すぐにこの状態を解消できます。

手順

1. アプライアンスをメンテナンスモードにしたら、アプライアンスをシャットダウンします。
   a. グリッドノードにログインします。
      i. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
      ii. に記載されているパスワードを入力します `Passwords.txt` ファイル。
      iii. 次のコマンドを入力してrootに切り替えます。 `su -`
      iv. に記載されているパスワードを入力します `Passwords.txt` ファイル。

      rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

b. アプライアンスをシャットダウンします。+
**shutdown -h now**

2. アプライアンスの電源がオフになっていることを確認するには、次のいずれかの方法を使用します。
   - アプライアンスの前面にある電源 LED が消灯している。
   - BMC インターフェイスの電源制御ページに、アプライアンスがオフになっていることが示されます。
3. アプライアンスに接続されている StorageGRID ネットワークが DHCP サーバを使用している場合は、DNS / ネットワークおよび IP アドレスの設定を更新します。

   a. アプライアンス前面の MAC アドレスラベルを確認し、管理ネットワークポートの MAC アドレスを特定します。

   MAC アドレスラベルには、 BMC 管理ポートの MAC アドレスが記載されています。

   管理ネットワークポートの MAC アドレスを特定するには、ラベルに記載された 16 進数に * 2 * を追加する必要があります。たとえば、ラベルに記載されている MAC アドレスの末尾が * 09 * の場合、管理ポートの MAC アドレスの末尾は * 0B * となります。ラベルに記載された MAC アドレスの末尾が * （ *y* ） FF* の場合、管理ポートの MAC アドレスの末尾は * （ *y*+1 ） 01 * となります。この計算を簡単に行うには、 Windows で Calculator を開き、 Programmer モードに設定して Hex を選択し、 MAC アドレスを入力してから、 **+2=** と入力します。

   b. 取り外したアプライアンスの DNS / ネットワークおよび IP アドレスを交換用アプライアンスの MAC アドレスと関連付けるよう、ネットワーク管理者に依頼します。

   交換用アプライアンスに電源を投入する前に、元のアプライアンスのすべての IP アドレスが更新されたことを確認する必要があります。そうしないと、アプライアンスのブート時に新しい DHCP IP アドレスが取得されて、 StorageGRID に再接続できなくなることがあります。この手順では、アプライアンスに接続されているすべての StorageGRID ネットワークを環境 接続します。

元のアプライアンスが静的 IP アドレスを使用していた場合は、取り外したアプライアンスの IP アドレスが自動的に新しいアプライアンスで使用されます。

4. アプライアンスを取り外して交換します。

   a. ケーブルにラベルを付け、ケーブルとネットワークトランシーバを取り外します。

   パフォーマンスの低下を防ぐために、ケーブルをねじったり、折り曲げたり、はさんだり、踏みつけたりしないでください。

   b. 障害が発生したアプライアンスをキャビネットまたはラックから取り外します。

   c. 電源装置 2 台、冷却ファン 8 台、および SSD 2 台を障害が発生したアプライアンスから交換用アプライアンスに移します。

   これらのコンポーネントの交換手順に従ってください。

   d. 交換用アプライアンスをキャビネットまたはラックに設置します。

   e. ケーブルと光トランシーバを交換してください。

f. アプライアンスの電源を入れ、アプライアンスの LED とブート時のコードを監視します。

BMC インターフェイスを使用して、ブート時のステータスを監視します。

5. アプライアンスノードが Grid Manager に表示され、アラートが表示されていないことを確認します。

関連情報

"キャビネットまたはラックへのアプライアンスの設置（SG100およびSG1000）"

"SG100およびSG1000アプライアンスのステータスインジケータの表示"

"アプライアンスのブート時のコードを確認する"

サービスアプライアンスの電源装置の交換

## サービスアプライアンスには、冗長性を確保するために電源装置が 2 つあります。いずれかの電源装置に障害が発生した場合は、アプライアンスの電源の冗長性を維持するために、できるだけ早く交換する必要があります。

必要なもの

- 交換用電源装置を開封しておきます。
- データセンターの電源装置を交換するアプライアンスの物理的な場所を確認しておきます。

  "コントローラのデータセンターへの配置"

- もう1つの電源装置が搭載され、動作していることを確認しておきます。

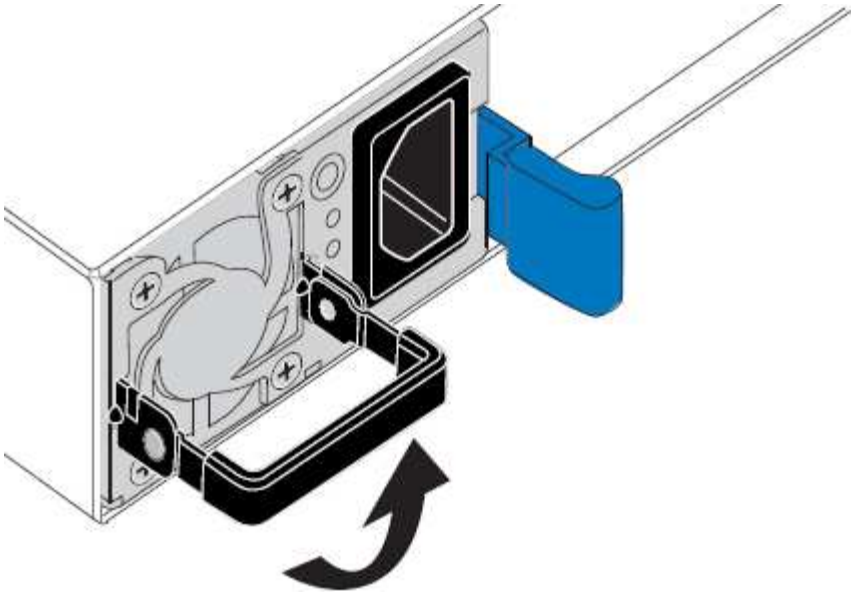
このタスクについて

次の図に、アプライアンスの背面からアクセスできる SG100 の 2 つの電源装置を示します。

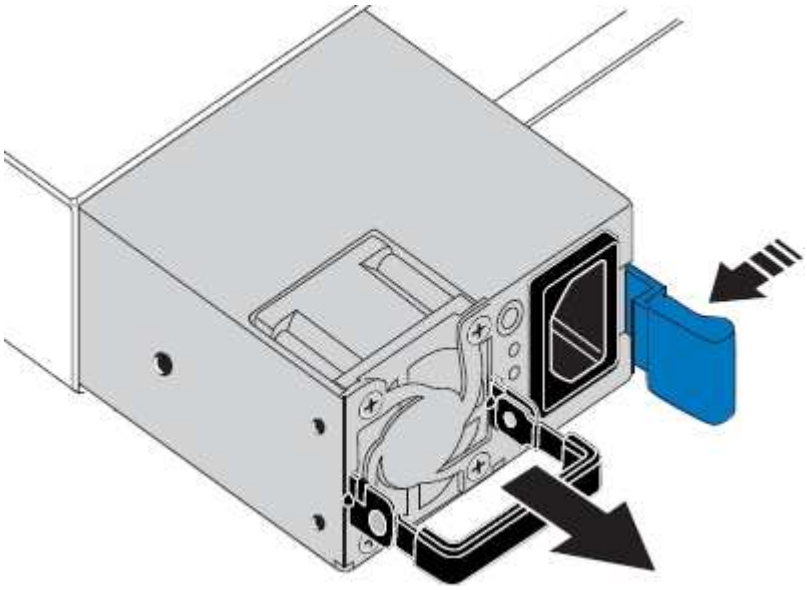
SG1000 の電源装置は同じです。

手順

1. 電源装置から電源コードを抜きます。
2. カムハンドルを持ち上げます。

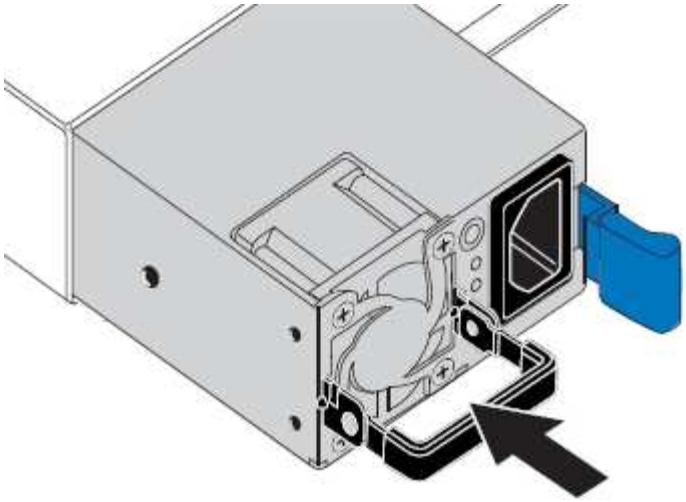


3. 青色のラッチを押し、電源装置を引き出します。



4. 交換用電源装置をシャーシにスライドさせて挿入します。

   ユニットをスライドさせて挿入するときは、青色のラッチが右側にあることを確認してください。



5. カムハンドルを下に押して、電源装置を固定します。
6. 電源コードを電源装置に接続し、緑色の LED が点灯することを確認します。

サービスアプライアンスのファンの交換

## サービスアプライアンスには、 8 つの冷却ファンがあります。いずれかのファンで障害が発生した場合は、アプライアンスの冷却が適切に行われるように、できるだけ早く交換する必要があります。

必要なもの

- 交換用ファンを開封しておきます。
- データセンターのファンを交換するアプライアンスの物理的な場所を確認しておきます。

  "コントローラのデータセンターへの配置"

- 他のファンが取り付けられ、動作していることを確認しておきます。
- アプライアンスのメンテナンスモードが開始されました。

  "アプライアンスをメンテナンスモードにします"

このタスクについて

ファンの交換中は、アプライアンスノードにアクセスできなくなります。

次の図は、サービスアプライアンスのファンを示しています。アプライアンスの上部カバーを取り外すと、冷却ファンがあります。

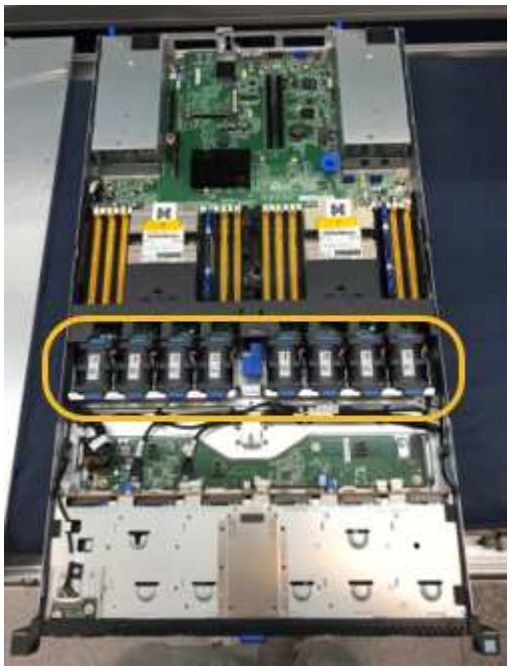
2 つの電源装置にもそれぞれファンが搭載されています。これらのファンはこの手順 には含まれていません。

手順

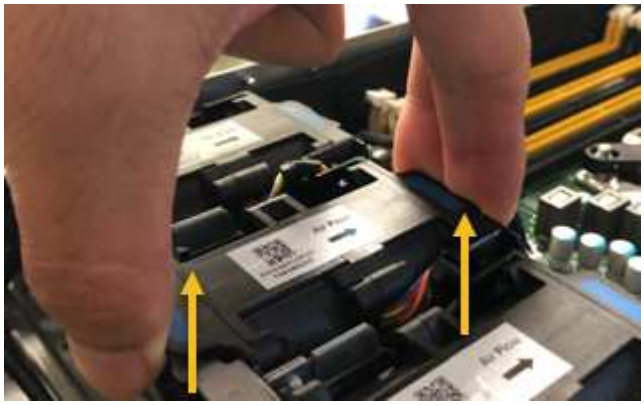
1. アプライアンスをメンテナンスモードにしたら、アプライアンスをシャットダウンします。
   a. グリッドノードにログインします。
      i. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
      ii. に記載されているパスワードを入力します `Passwords.txt` ファイル。
      iii. 次のコマンドを入力してrootに切り替えます。 `su -`
      iv. に記載されているパスワードを入力します `Passwords.txt` ファイル。

      rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

   b. サービスアプライアンスをシャットダウンします。+
      **`shutdown -h now`**
2. 次のいずれかの方法を使用して、サービスアプライアンスの電源がオフになっていることを確認します。
   - アプライアンスの前面にある電源 LED が消灯している。
   - BMC インターフェイスの電源制御ページに、アプライアンスがオフになっていることが示されます。
3. 上部カバーのラッチを持ち上げて、アプライアンスからカバーを取り外します。
4. 障害が発生しているファンを特定します。

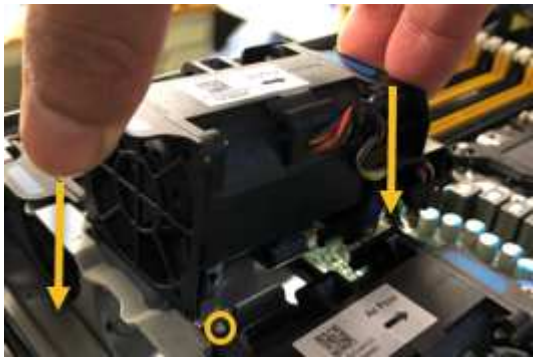


5. 障害が発生したファンをシャーシから取り出します。

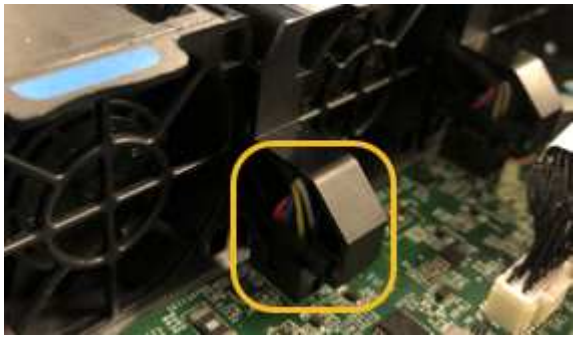


6. 交換用ファンをシャーシのオープンスロットにスライドさせて挿入します。

   ファンの端をガイドピンに合わせます。ピンは写真の丸で囲んでいます。



7. ファンのコネクタを回路基板にしっかりと押し込みます。



8. 上部カバーをアプライアンスに戻し、ラッチを押し下げてカバーを所定の位置に固定します。
9. アプライアンスの電源を入れ、コントローラの LED とブート時のコードを監視します。

   BMC インターフェイスを使用して、ブート時のステータスを監視します。

10. アプライアンスノードが Grid Manager に表示され、アラートが表示されていないことを確認します。

サービスアプライアンスのドライブの交換

## サービスアプライアンスの SSD には StorageGRID オペレーティングシステムが含まれ

ています。また、アプライアンスが管理ノードとして設定されている場合は、 SSD には監査ログ、指標、データベーステーブルも格納されています。冗長性を確保するために、ドライブは RAID 1 を使用してミラーリングさいずれかのドライブで障害が発生した場合は、できるだけ早く交換して冗長性を確保する必要があります。

必要なもの

- データセンターのドライブを交換するアプライアンスの物理的な場所を確認しておきます。

  "コントローラのデータセンターへの配置"

- どのドライブで障害が発生したかを確認するために、左側の LED が黄色で点滅していることを確認しました。

  動作中のドライブを取り外すと、アプライアンスノードが停止します。ステータスインジケータの表示に関する情報を参照して、障害を確認してください。

- 交換用ドライブを入手します。
- 適切な ESD 保護を用意しておきます。

手順

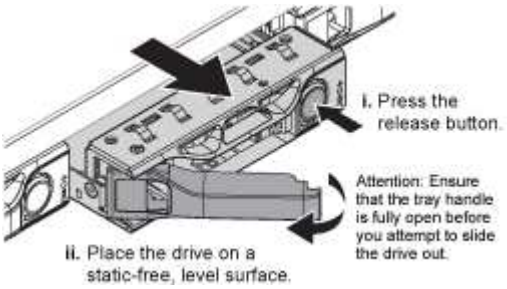
1. ドライブの左 LED が黄色に点滅していることを確認します。

   また、 Grid Manager を使用して SSD のステータスを監視することもできます。[ノード（ Nodes）]を選択し次に、を選択します **`Appliance Node`** >*ハードウェア*。ドライブで障害が発生すると、 Storage RAID Mode フィールドに、障害が発生したドライブに関するメッセージが表示されます。

2. ESD リストバンドのストラップの端を手首に巻き付け、静電気の放電を防ぐためにクリップの端をメタルアースに固定します。
3. 交換用ドライブを開封し、アプライアンスの近くの、静電気防止処置を施した平らな場所に置きます。

   梱包材はすべて保管しておいてください。

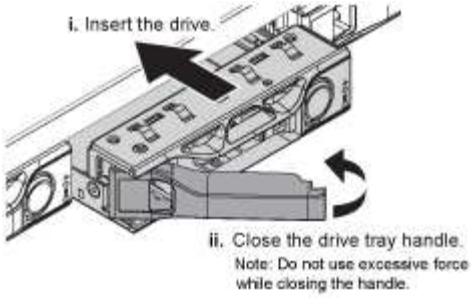
4. 障害が発生したドライブのリリースボタンを押します。




   ドライブのハンドルが途中まで開き、ドライブがスロットから外れます。

5. ハンドルを開き、ドライブを引き出して、静電気防止処置を施した平らな場所に置きます。
6. 交換用ドライブをドライブスロットに挿入する前に、ドライブのリリースボタンを押します。

   ラッチが開きます。




7. 交換用ドライブをスロットに挿入し、ドライブのハンドルを閉じます。

   ハンドルを閉じる際に力を入れすぎないように注意してください。

   ドライブが完全に挿入されると、カチッという音がします。

   ドライブは、動作中のドライブのミラーデータを使用して自動的にリビルドされます。グリッドマネージャを使用して、再構築のステータスを確認できます。[ノード（ Nodes）]を選択し次に、を選択します **`Appliance Node`** >*ハードウェア*。Storage RAID Mode フィールドには、ドライブが完全に再構築されるまで「 rebuilding 」というメッセージが表示されます。

8. ドライブの交換については、テクニカルサポートにお問い合わせください。

   障害が発生したドライブの返却手順については、テクニカルサポートにお問い合わせください。

サービスアプライアンスのリンク設定の変更

## サービスアプライアンスのイーサネットリンク設定を変更することができます。ポートボンディングモード、ネットワークボンディングモード、およびリンク速度を変更できます。

必要なもの

- アプライアンスはメンテナンスモードにする必要があります。StorageGRID アプライアンスをメンテナンスモードにすると、アプライアンスにリモートアクセスできなくなることがあります。

  "アプライアンスをメンテナンスモードにします"

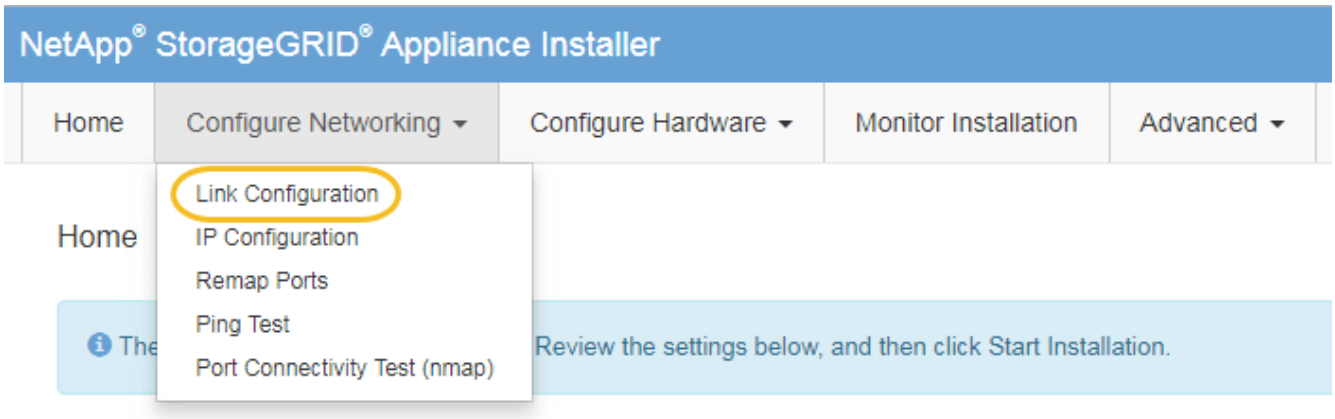
このタスクについて

サービスアプライアンスのイーサネットリンク設定を変更するオプションには、次のものがあります。

- ポートボンディングモード * を「 Fixed 」から「 Aggregate 」または「 Aggregate 」から「 Fixed 」に変更します
- ネットワークボンディングモード * を Active-Backup から LACP に、または LACP から Active-Backup に変更
- VLAN タグを有効または無効にするか、 VLAN タグの値を変更します
- リンク速度を変更する

手順

1. StorageGRID アプライアンスインストーラから、 **Configure Networking**>*Link Configuration* を選択します。




2. リンク設定に必要な変更を加えます。

   オプションの詳細については、「ネットワークリンクの設定」を参照してください。

3. 選択に問題がなければ、 * 保存 * をクリックします。

   接続しているネットワークまたはリンクを変更すると、接続が失われる可能性があります。1分以内に再接続されない場合は、アプライアンスに割り当てられている他のIPアドレスのいずれかを使用してStorageGRID アプライアンスインストーラのURLを再入力します：+
   **`https://services_appliance_IP:8443`**

4. アプライアンスの IP アドレスに対して必要な変更を行います。

   VLAN 設定を変更した場合は、アプライアンスのサブネットが変更されている可能性があります。アプライアンスのIPアドレスを変更する必要がある場合は、IPアドレスの設定手順に従います。

   "StorageGRID IPアドレスを設定しています"

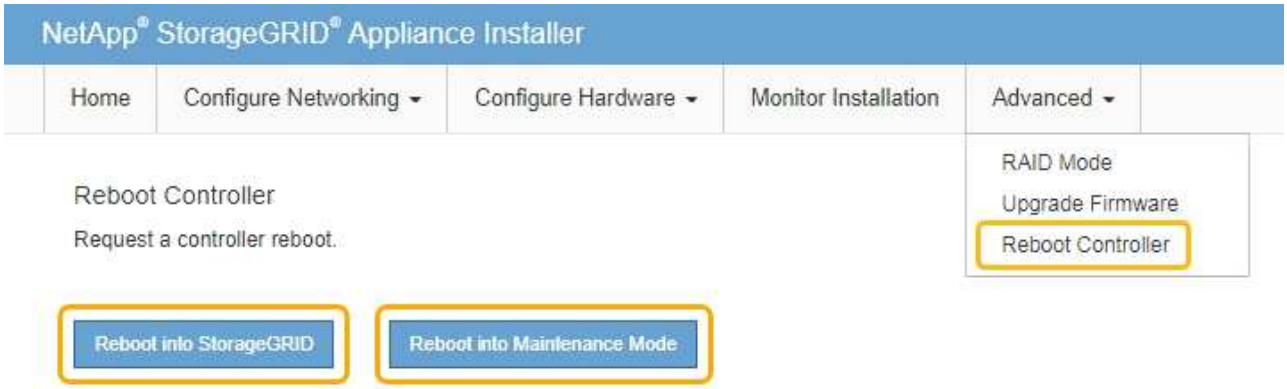
5. メニューから [ ネットワークの設定 *>*Ping テスト *] を選択します。
6. アプライアンスの設定時に行ったリンク設定の変更によって影響を受けた可能性のあるネットワーク上の IP アドレスに対して、 Ping Test ツールを使用して接続を確認します。

   最低でもプライマリ管理ノードのグリッドネットワーク IP アドレスと、 1 つ以上の他のノードのグリッドネットワーク IP アドレスについて、 ping が通ることを確認します。必要に応じて、ネットワークリンクの設定手順に戻って問題を修正します。

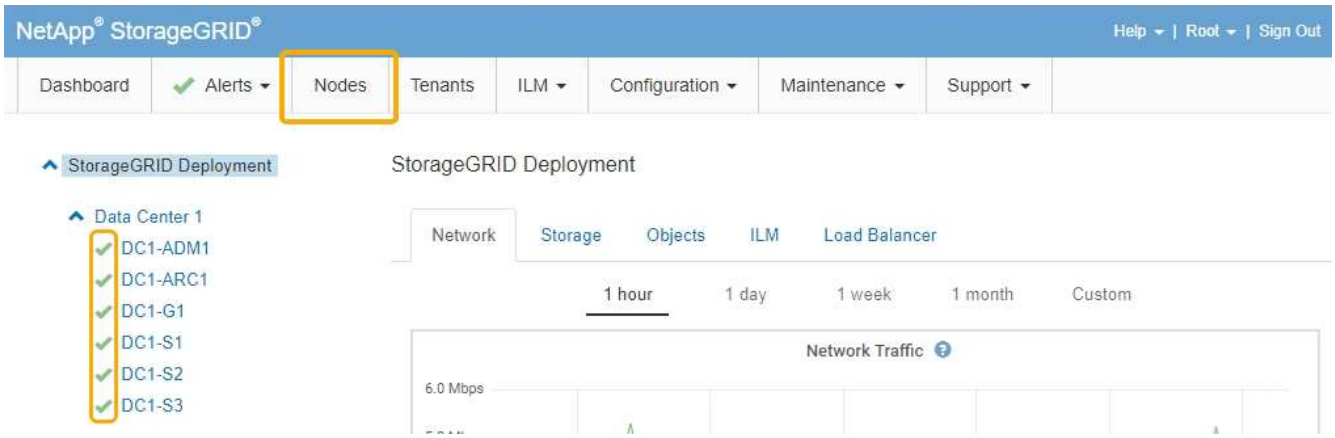
7. リンク設定の変更が問題なく機能していることを確認したら、ノードをリブートします。StorageGRID アプライアンス・インストーラから、 **Advanced**>*Reboot Controller* を選択し、次のいずれかのオプションを選択します。

   - Reboot into StorageGRID * を選択し、ノードをグリッドに再追加してコントローラをリブートします。メンテナンスモードで作業を完了し、ノードを通常動作に戻す準備ができている場合は、このオプションを選択します。
   - メンテナンスモードを維持したままコントローラをリブートするには、 * Reboot into Maintenance Mode * を選択します。このオプションは、グリッドに再追加する前にノードで追加のメンテナンス処

理を実行する必要がある場合に選択します。




アプライアンスがリブートしてグリッドに再参加するまでに最大 20 分かかることがあります。リブートが完了し、ノードが再びグリッドに参加したことを確認するには、 Grid Manager に戻ります。[ノード*（Nodes *）]タブには、通常のステータスが表示されます ✔ アクティブなアラートがなく、ノードがグリッドに接続されていることを示す、アプライアンスノードの場合。




**MTU**設定を変更します

## アプライアンスノードの IP アドレスを設定するときに割り当てた MTU 設定を変更できます。

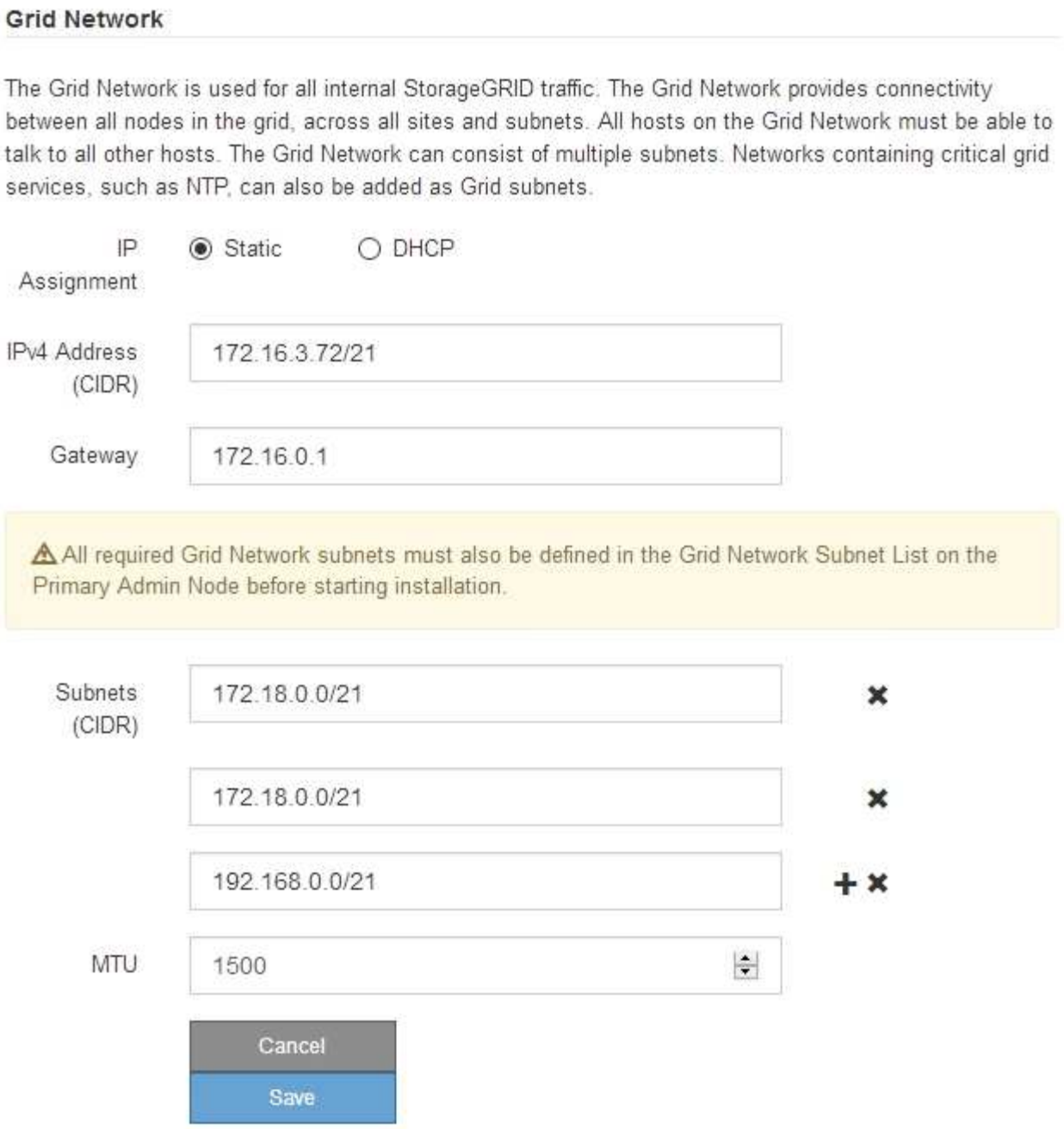
必要なもの

アプライアンスのメンテナンスモードが開始されました。

"アプライアンスをメンテナンスモードにします"

手順

1. StorageGRID アプライアンスインストーラから、 **Configure Networking**>*IP Configuration* を選択します。
2. グリッドネットワーク、管理ネットワーク、およびクライアントネットワークの MTU 設定に必要な変更を加えます。



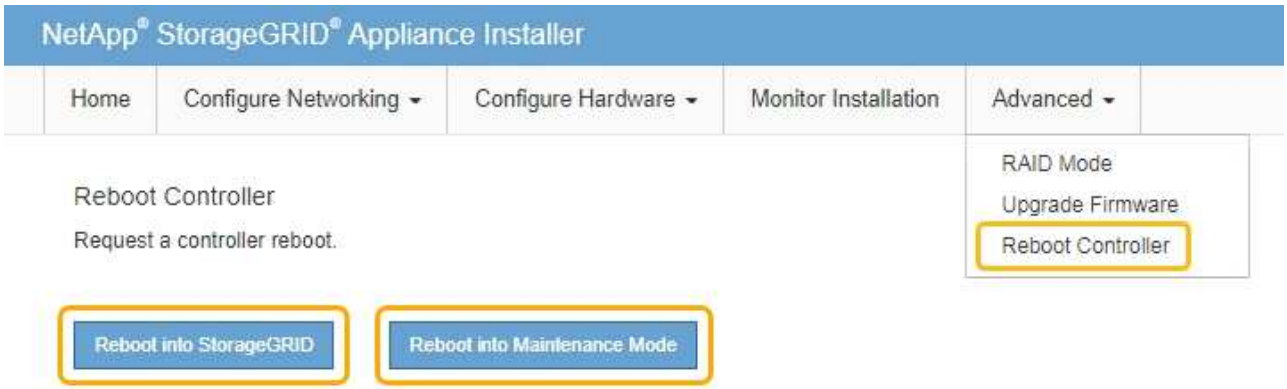

ネットワークの MTU 値は、ノードが接続されているスイッチポートに設定されている値と同じである必要があります。そうしないと、ネットワークパフォーマンスの問題やパケット損失が発生する可能性があります。

ネットワークのパフォーマンスを最大限に高めるには、すべてのノードのグリッドネットワークインターフェイスで MTU 値がほぼ同じになるように設定する必要があります。個々のノードのグリッドネットワークの MTU 設定に大きな違いがある場合は、 * Grid Network MTU mismatch * アラートがトリガーされます。MTU 値はすべてのネットワークタイプで同じである必要はありません。

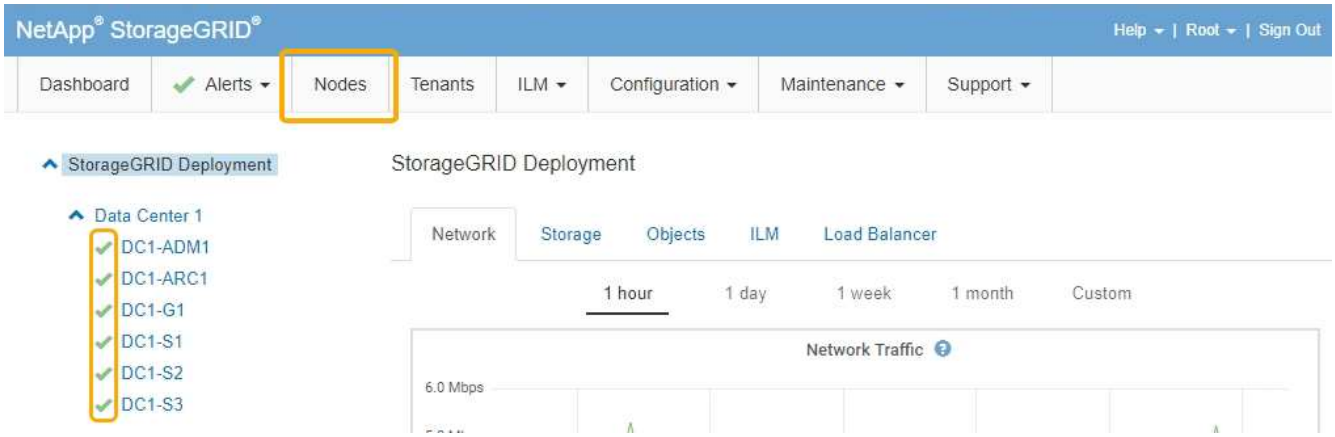
3. 設定に問題がなければ、「 * 保存 * 」を選択します。
4. ノードをリブートします。StorageGRID アプライアンス・インストーラから、 **Advanced**>*Reboot

Controller* を選択し、次のいずれかのオプションを選択します。

- Reboot into StorageGRID * を選択し、ノードをグリッドに再追加してコントローラをリブートします。メンテナンスモードで作業を完了し、ノードを通常動作に戻す準備ができている場合は、このオプションを選択します。
- メンテナンスモードを維持したままコントローラをリブートするには、 * Reboot into Maintenance Mode * を選択します。このオプションは、グリッドに再追加する前にノードで追加のメンテナンス処理を実行する必要がある場合に選択しま
す。




アプライアンスがリブートしてグリッドに再参加するまでに最大 20 分かかることがあります。リブートが完了し、ノードが再びグリッドに参加したことを確認するには、 Grid Manager に戻ります。[ノード*（Nodes *）]タブには、通常のステータスが表示されます ✔ アクティブなアラートがなく、ノードがグリッドに接続されていることを示す、アプライアンスノードの場合。




関連情報

"StorageGRID の管理"

**DNS**サーバの設定を確認しています

このアプライアンスノードで現在使用されているドメインネームシステム（ DNS ）サーバを確認し、一時的に変更することができます。

必要なもの

アプライアンスのメンテナンスモードが開始されました。

"アプライアンスをメンテナンスモードにします"

このタスクについて

KMS のホスト名は IP アドレスではなくドメイン名として指定されているため、暗号化されたアプライアンスがキー管理サーバ（ KMS ）または KMS クラスタに接続できない場合は、 DNS サーバ設定の変更が必要になることがあります。アプライアンスの DNS 設定に加えた変更は一時的なものであり、メンテナンスモードを終了すると失われます。これらの変更を永続的に行うには、Grid ManagerでDNSサーバを指定します（* Maintenance > Network > DNS Servers *）。

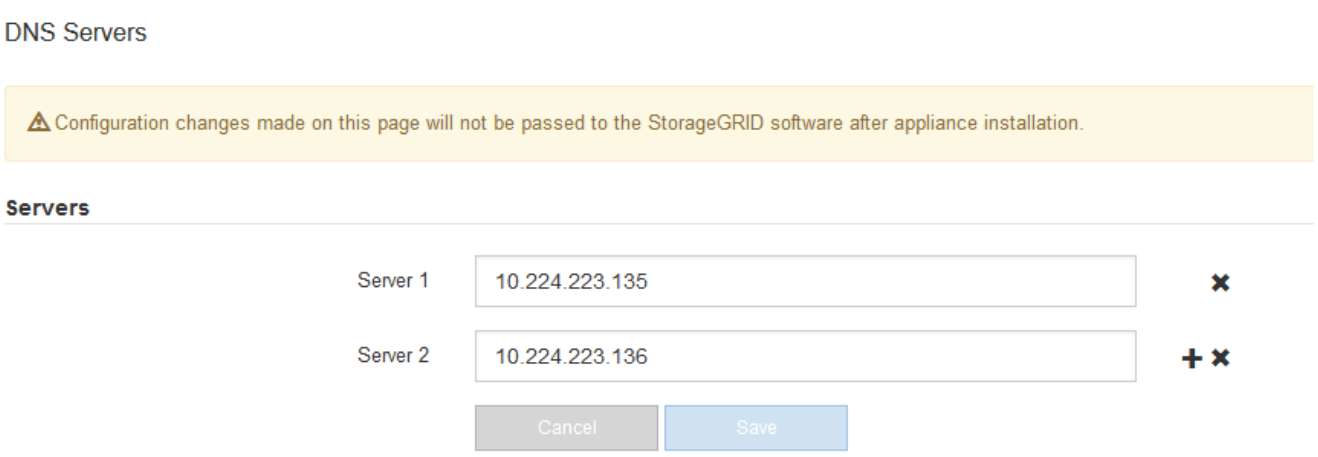
- DNS 設定の一時的な変更が必要になるのは、ホスト名に IP アドレスではなく完全修飾ドメイン名を使用して KMS サーバが定義されているノード暗号化アプライアンスのみです。
- ノード暗号化アプライアンスをドメイン名を使用して KMS に接続する場合は、グリッド用に定義されている DNS サーバの 1 つに接続する必要があります。これらの DNS サーバの 1 つが、ドメイン名を IP アドレスに変換します。
- ノードがグリッドの DNS サーバにアクセスできない場合、またはノード暗号化アプライアンスノードがオフラインのときにグリッド全体の DNS 設定を変更した場合は、ノードは KMS に接続できません。アプライアンス上の暗号化されたデータは、 DNS 問題 が解決されるまで復号化できません。

KMS 接続を回避する DNS 問題 を解決するには、 StorageGRID アプライアンスインストーラで 1 つ以上の DNS サーバの IP アドレスを指定します。この一時的な DNS 設定により、アプライアンスは KMS に接続してノード上のデータを復号化することができます。

たとえば、暗号化されたノードがオフラインのときにグリッドの DNS サーバが変更された場合、ノードは以前の DNS 値をまだ使用しているため、オンラインに戻った時点で KMS にアクセスできなくなります。StorageGRID アプライアンスインストーラで新しい DNS サーバの IP アドレスを入力すると、 KMS 接続を使用してノードのデータを復号化できます。

手順

1. StorageGRID アプライアンスインストーラから、 **Configure Networking *>*DNS Configuration** を選択します。
2. 指定した DNS サーバが正しいことを確認してください。




3. 必要に応じて、 DNS サーバを変更します。

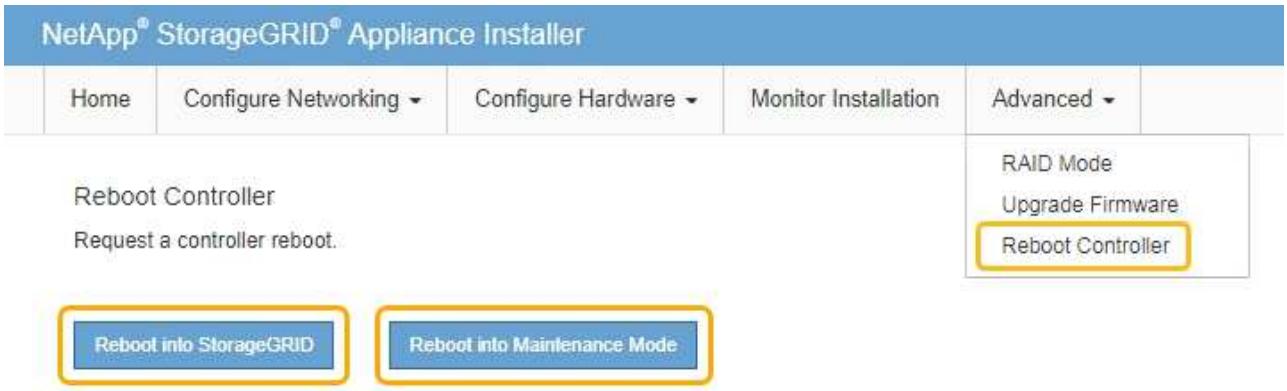
DNS 設定に対する変更は一時的なものであり、メンテナンスモードを終了すると失われます。

4. 一時的な DNS 設定に問題がなければ、 * 保存 * を選択します。

   ノードは、このページで指定されている DNS サーバ設定を使用して KMS に再接続し、ノード上のデータを復号化できるようにします。

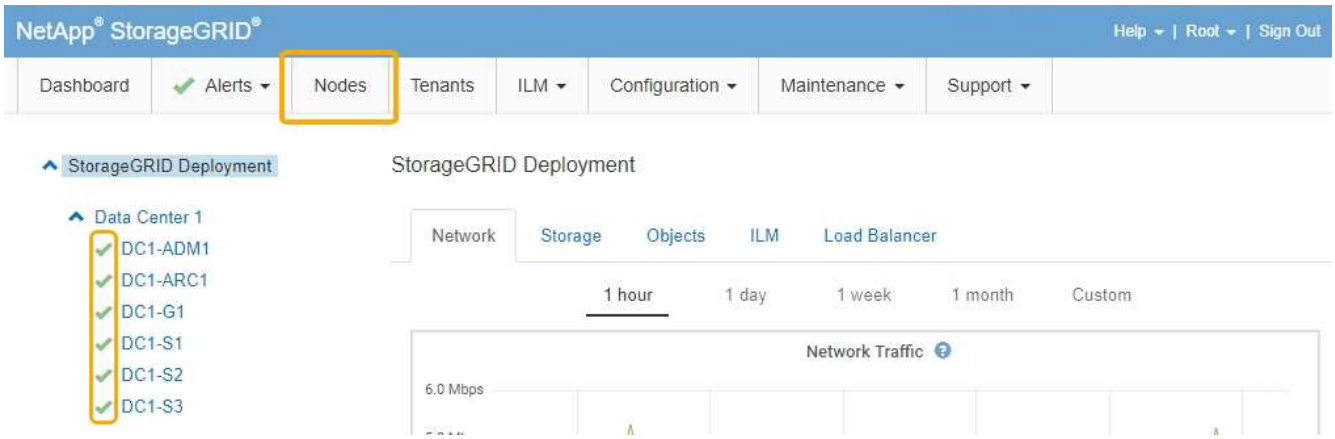
5. ノードデータが復号化されたら、ノードをリブートします。StorageGRID アプライアンス・インストーラから、 **Advanced**>*Reboot Controller* を選択し、次のいずれかのオプションを選択します。

   - Reboot into StorageGRID * を選択し、ノードをグリッドに再追加してコントローラをリブートします。メンテナンスモードで作業を完了し、ノードを通常動作に戻す準備ができている場合は、このオプションを選択します。
   - メンテナンスモードを維持したままコントローラをリブートするには、 * Reboot into Maintenance Mode * を選択します。このオプションは、グリッドに再追加する前にノードで追加のメンテナンス処理を実行する必要がある場合に選択します。




ノードがリブートしてグリッドに再び参加すると、 Grid Manager にリストされているシステム全体の DNS サーバが使用されます。グリッドに再追加したあとは、アプライアンスがメンテナンスモードのときに、 StorageGRID アプライアンスインストーラで指定された一時的な DNS サーバがアプライアンスで使用されなくなります。

アプライアンスがリブートしてグリッドに再参加するまでに最大 20 分かかることがあります。リブートが完了し、ノードが再びグリッドに参加したことを確認するには、 Grid Manager に戻ります。[ノード*（Nodes *）]タブには、通常のステータスが表示されます アクティブなアラートがなく、ノードがグリッドに接続されていることを示す、アプライアンスノードの場合。




メンテナンスモードでのノード暗号化の監視

# インストール中にアプライアンスのノード暗号化を有効にした場合は、ノード暗号化の状態やキー管理サーバ（ KMS ）の詳細など、各アプライアンスノードのノード暗号化ステータスを監視できます。

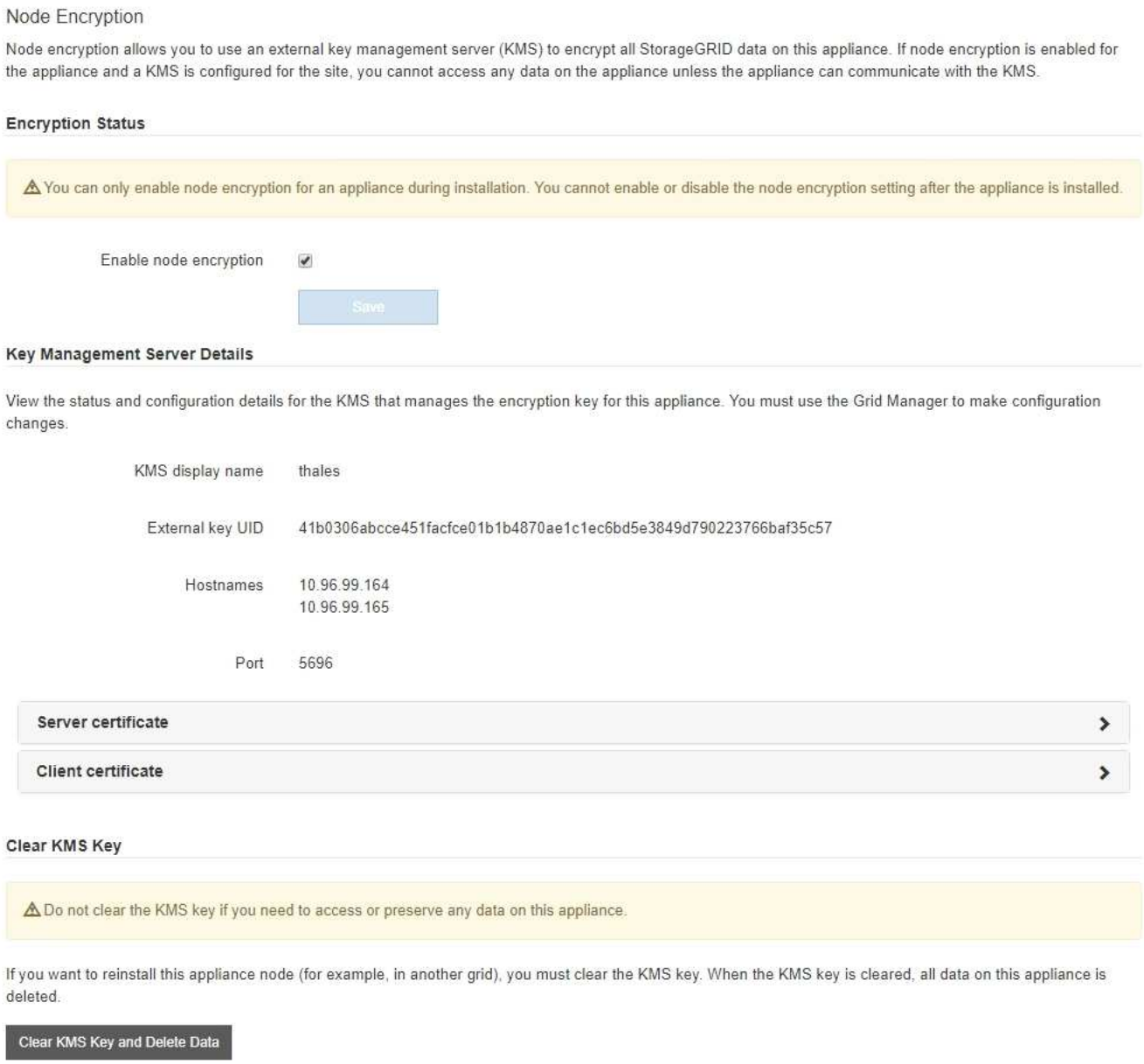
必要なもの

- インストール時にアプライアンスのノード暗号化を有効にしておく必要があります。アプライアンスのインストール後にノード暗号化を有効にすることはできません。
- アプライアンスはメンテナンスモードになりました。

  "アプライアンスをメンテナンスモードにします"

手順

1. StorageGRID アプライアンスインストーラから、 * ハードウェアの設定 * > * ノード暗号化 * を選択します。




Node Encryption のページには次の 3 つのセクションがあります。

- Encryption Status には、アプライアンスでノード暗号化が有効か無効かが表示されます。
- キー管理サーバの詳細には、アプライアンスの暗号化に使用されている KMS に関する情報が表示されます。サーバおよびクライアント証明書のセクションを展開すると、証明書の詳細およびステータスを表示できます。
  - 期限切れの証明書の更新など、証明書自体に関する問題に対処するには、 StorageGRID の管理手順の KMS に関する情報を参照してください。
  - KMS ホストへの接続で予期しない問題が発生する場合は、ドメインネームシステム（ DNS ）サーバが正しいこと、およびアプライアンスのネットワークが正しく設定されていることを確認してください。

    "DNSサーバの設定を確認しています"

  - 証明書の問題を解決できない場合は、テクニカルサポートにお問い合わせください。

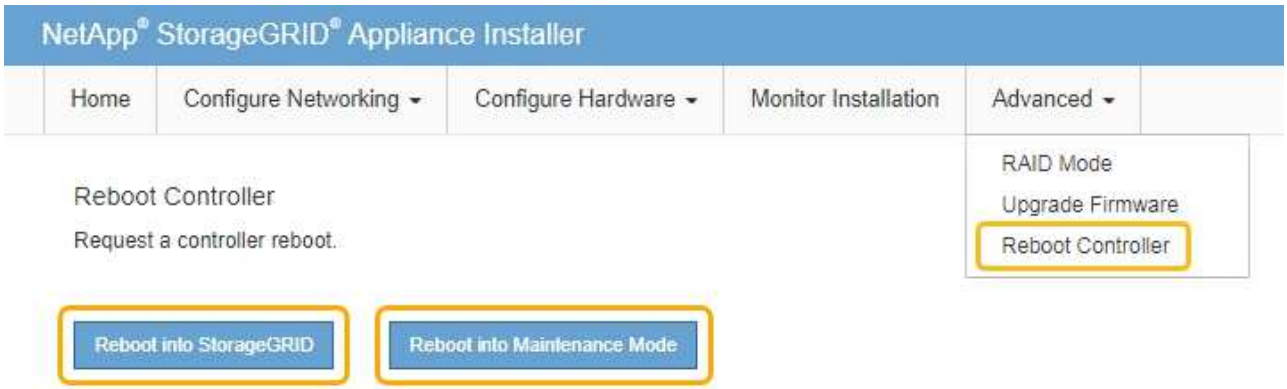
- KMS Key をクリアすると、アプライアンスのノード暗号化が無効になり、 StorageGRID サイト用に設定されているアプライアンスとキー管理サーバの間の関連付けが解除され、アプライアンスのすべてのデータが削除されます。別の StorageGRID システムにアプライアンスをインストールする前に、KMS キーをクリアする必要があります。

  "キー管理サーバ設定のクリア"

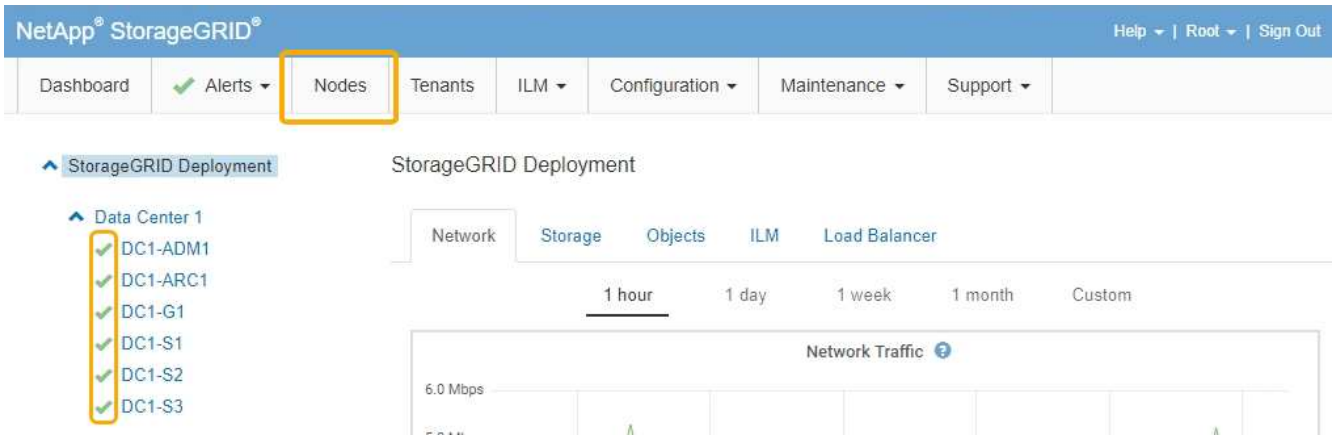
  KMS の設定をクリアすると、アプライアンスからデータが削除され、永久にアクセスできなくなります。このデータはリカバリできません。

2. ノード暗号化ステータスの確認が完了したら、ノードをリブートします。StorageGRID アプライアンス・インストーラから、 **Advanced**>*Reboot Controller* を選択し、次のいずれかのオプションを選択します。

   - Reboot into StorageGRID * を選択し、ノードをグリッドに再追加してコントローラをリブートします。メンテナンスモードで作業を完了し、ノードを通常動作に戻す準備ができている場合は、このオプションを選択します。
   - メンテナンスモードを維持したままコントローラをリブートするには、 * Reboot into Maintenance Mode * を選択します。このオプションは、グリッドに再追加する前にノードで追加のメンテナンス処理を実行する必要がある場合に選択します。




アプライアンスがリブートしてグリッドに再参加するまでに最大 20 分かかることがあります。リブートが完了し、ノードが再びグリッドに参加したことを確認するには、 Grid Manager に戻ります。[ノード*（Nodes *）]タブには、通常のステータスが表示されます ✔ アクティブなアラートがなく、ノードがグリッドに接続されていることを示す、アプライアンスノードの場合。




関連情報

"StorageGRID の管理"

キー管理サーバ設定のクリア

# キー管理サーバ（ KMS ）の設定をクリアすると、アプライアンスでノード暗号化が無効になります。KMS の設定をクリアすると、アプライアンスのデータは完全に削除され、アクセスできなくなります。このデータはリカバリできません。

必要なもの

アプライアンス上のデータを保持する必要がある場合は、KMSの設定をクリアする前に、ノードの運用停止手順 を実行する必要があります。

KMS をクリアすると、アプライアンスのデータが完全に削除され、アクセスできなくなります。このデータはリカバリできません。

ノードを運用停止して、格納されているデータをStorageGRID 内の他のノードに移動します。グリッドノードの運用停止手順については、リカバリとメンテナンスの手順を参照してください。

このタスクについて

アプライアンス KMS の設定をクリアすると、ノード暗号化が無効になり、アプライアンスノードと StorageGRID サイトの KMS の設定との間の関連付けが解除されます。その後、アプライアンスのデータが削除され、アプライアンスはインストール前の状態のままになります。このプロセスを元に戻すことはできません。

KMS の設定をクリアする必要があります。

- アプライアンスを別の StorageGRID システムにインストールする前に、 KMS を使用しない、または別の KMS を使用する前に、

同じ KMS キーを使用する StorageGRID システムにアプライアンスノードを再インストールする場合は、 KMS の設定をクリアしないでください。

- KMS 設定が失われて KMS キーをリカバリおよび再インストールできないノードをリカバリする前に、 KMS キーをリカバリできません。
- お客様のサイトで以前使用していたアプライアンスを返却する前に、

- ノード暗号化が有効になっているアプライアンスの運用を停止したあと。

> KMS をクリアして StorageGRID システム内の他のノードにデータを移動する前に、アプライアンスの運用を停止します。アプライアンスの運用を停止する前に KMS をクリアすると、データが失われるため、アプライアンスが動作しなくなる可能性があります。

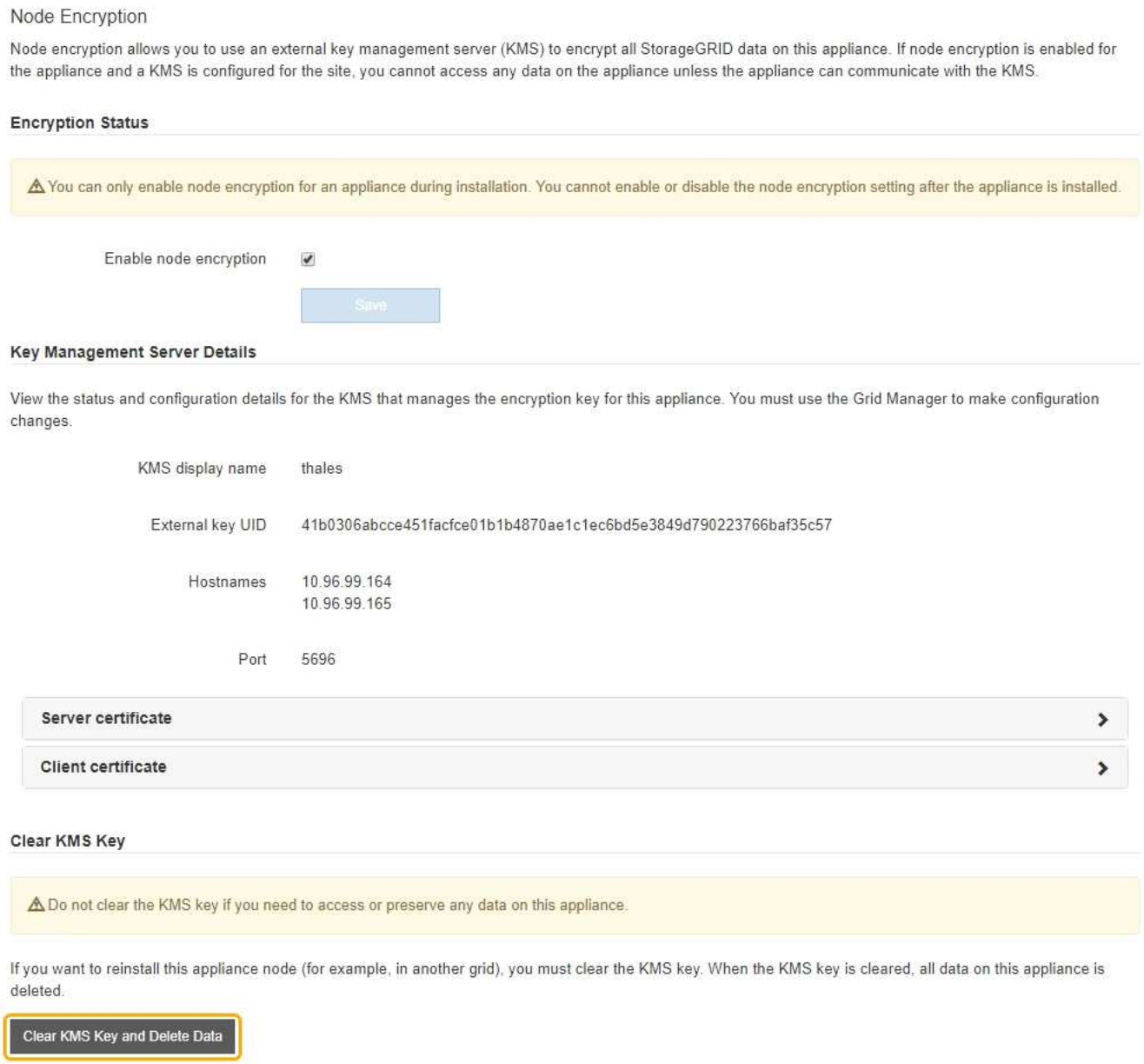
手順

1. ブラウザを開き、アプライアンスのコンピューティングコントローラの IP アドレスのいずれかを入力します。[+]
   **`https://Controller_IP:8443`**

   *`Controller_IP`* は、3つのStorageGRID ネットワークのいずれかでのコンピューティングコントローラ（ストレージコントローラではない）のIPアドレスです。

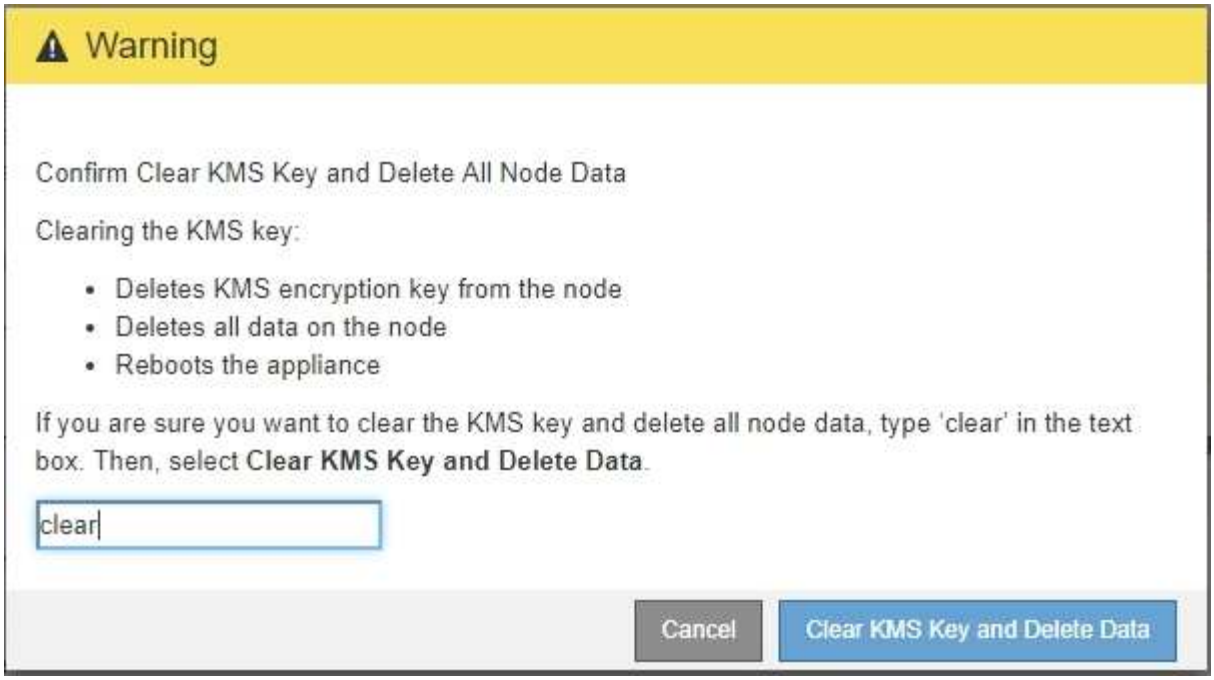
   StorageGRID アプライアンスインストーラのホームページが表示されます。

2. Configure Hardware * > * Node Encryption * を選択します。




KMS の設定をクリアすると、アプライアンス上のデータが完全に削除されます。このデータはリカバリできません。

3. ウィンドウの下部で、 * KMS キーをクリアしてデータを削除 * を選択します。
4. KMSの設定をクリアしても問題がない場合は、と入力します **`clear`** 「* KMSキーをクリアしてデータを削除*」を選択します。




KMS 暗号化キーとすべてのデータがノードから削除され、アプライアンスがリブートします。この処理には 20 分程度かかる場合があります。

5. ブラウザを開き、アプライアンスのコンピューティングコントローラの IP アドレスのいずれかを入力します。[+]
**`https://Controller_IP:8443`**

   *`Controller_IP`* は、3つのStorageGRID ネットワークのいずれかでのコンピューティングコントローラ（ストレージコントローラではない）のIPアドレスです。

   StorageGRID アプライアンスインストーラのホームページが表示されます。

6. Configure Hardware * > * Node Encryption * を選択します。
7. ノードの暗号化が無効になっていること、および * キー管理サーバの詳細 * および * KMS キーと削除 * のコントロールでキーと証明書の情報がウィンドウから削除されていることを確認します。

   アプライアンスでのノード暗号化の再インストールまでは、グリッドでのノード暗号化を再度有効にすることはできません。

完了後

アプライアンスがリブートし、 KMS がクリアされてインストール前の状態になっていることを確認したら、StorageGRID システムからアプライアンスを物理的に取り外すことができます。再インストールのためのアプライアンスの準備については、リカバリおよびメンテナンスの手順を参照してください。

関連情報

"StorageGRID の管理"

""

# 構成と管理

## StorageGRID の管理

StorageGRID システムの設定方法について説明します。

- "StorageGRID システムの管理"
- "StorageGRID への管理者アクセスの制御"
- "キー管理サーバを設定しています"
- "テナントの管理"
- "S3およびSwiftクライアント接続の設定"
- "StorageGRID ネットワークと接続の管理"
- "AutoSupport を設定しています"
- "ストレージノードの管理"
- "管理ノードの管理"
- "アーカイブノードの管理"
- "StorageGRID へのデータの移行"

### StorageGRID システムの管理

以下の手順に従って、 StorageGRID システムを設定および管理します。

以下の手順では、 Grid Manager を使用してグループとユーザを設定し、 S3 および Swift クライアントアプリケーションでオブジェクトの格納と読み出しを許可するテナントアカウントを作成する方法、 StorageGRID ネットワークの設定と管理、 AutoSupport の設定、ノード設定の管理などを行う方法について説明します。

> 情報ライフサイクル管理（ ILM ）ルールとポリシーを含むオブジェクトを管理する手順は、に移動されました"ILM を使用してオブジェクトを管理する"。

ここで説明する手順は、 StorageGRID システムのインストール後に設定、管理、およびサポートを行う技術担当者を対象としています。

必要なもの

- StorageGRID システムに関する一般的な知識が必要です。
- Linux のコマンドシェル、ネットワーク、サーバハードウェアのセットアップと設定について、詳しい知識が必要です。

#### Web ブラウザの要件

サポートされている Web ブラウザを使用する必要があります。

| Web ブラウザ | サポートされる最小バージョン |
| --- | --- |
| Google Chrome | 87 |
| Microsoft Edge の場合 | 87 |
| Mozilla Firefox | 84 |

ブラウザウィンドウの幅を推奨される値に設定してください。

| ブラウザの幅 | ピクセル |
| --- | --- |
| 最小（ Minimum ） | 1024 |
| 最適 | 1280 |

**Grid Manager**にサインインします

## Grid Manager のサインインページにアクセスするには、サポートされている Web ブラウザのアドレスバーに管理ノードの完全修飾ドメイン名（ FQDN ）または IP アドレスを入力します。

必要なもの

- ログインクレデンシャルが必要です。
- Grid ManagerのURLが必要です。
- サポートされているWebブラウザを使用する必要があります。
- Web ブラウザでクッキーが有効になっている必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

各 StorageGRID システムには、 1 つのプライマリ管理ノードと、任意の数のプライマリ以外の管理ノードが含まれています。任意の管理ノードでグリッドマネージャにサインインして、 StorageGRID システムを管理できます。ただし、管理ノードはまったく同じというわけではありません。

- ある管理ノードで実行されたアラームの確認応答（従来のシステム）は他の管理ノードにはコピーされません。そのため、各管理ノードでアラームについて異なる情報が表示される可能性があります。
- 一部のメンテナンス手順は、プライマリ管理ノードでしか実行できません。

管理ノードがハイアベイラビリティ（ HA ）グループに含まれている場合は、 HA グループの仮想 IP アドレスまたは仮想 IP アドレスにマッピングされる完全修飾ドメイン名を使用して接続します。プライマリ管理ノードが使用できない場合を除いてプライマリ管理ノード上のグリッドManagerにアクセスするよう、プライマリ管理ノードをグループの優先マスターとして選択してください。

手順

1. サポートされている Web ブラウザを起動します。

2. ブラウザのアドレスバーに、 Grid Manager の URL を入力します。

   `https://FQDN_or_Admin_Node_IP/`

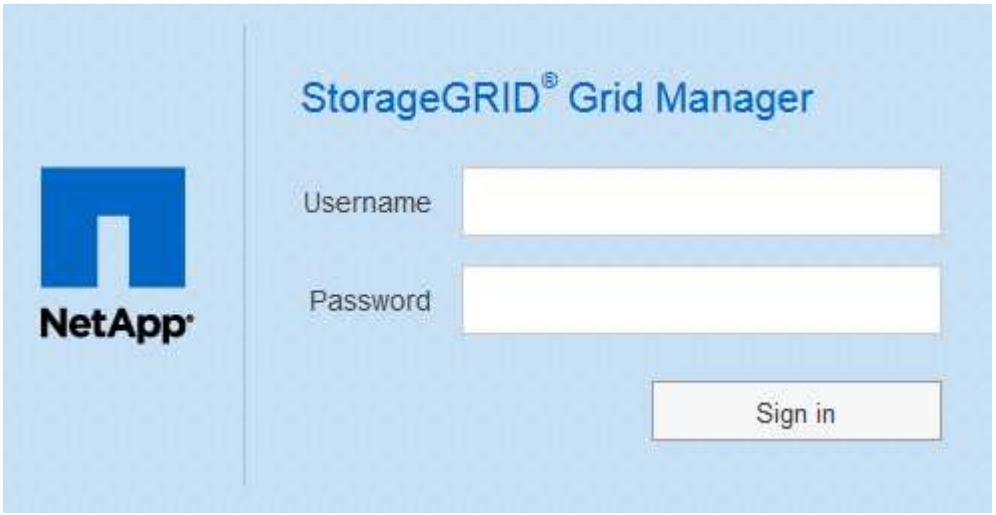
   ここで、 *FQDN_or_Admin_Node_IP* は、管理ノードの完全修飾ドメイン名またはIPアドレス、あるいは管理ノードのHAグループの仮想IPアドレスです。

   HTTPS（443）の標準ポート以外のポートでGrid Managerにアクセスする必要がある場合は、次のように入力します *FQDN_or_Admin_Node_IP* は完全修飾ドメイン名またはIPアドレス、portはポート番号です。

   `https://FQDN_or_Admin_Node_IP:port/`

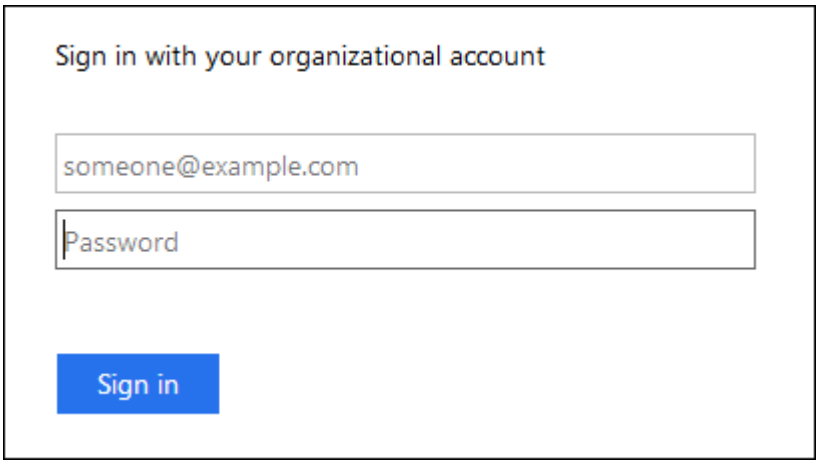
3. セキュリティアラートが表示された場合は、ブラウザのインストールウィザードを使用して証明書をインストールします。
4. Grid Manager にサインインします。

   - StorageGRID システムでシングルサインオン（ SSO ）が使用されていない場合は、次の手順を実行します。
     i. Grid Manager のユーザ名とパスワードを入力します。
     ii. [ * サインイン * ] をクリックします。

   - StorageGRID システムで SSO が有効になっており、このブラウザで初めて URL にアクセスした場合は、次の手順を実行します。
     i. [ * サインイン * ] をクリックします。[ アカウント ID] フィールドは空白のままにできます。

ii. 組織の SSO サインインページで標準の SSO クレデンシャルを入力します。例：

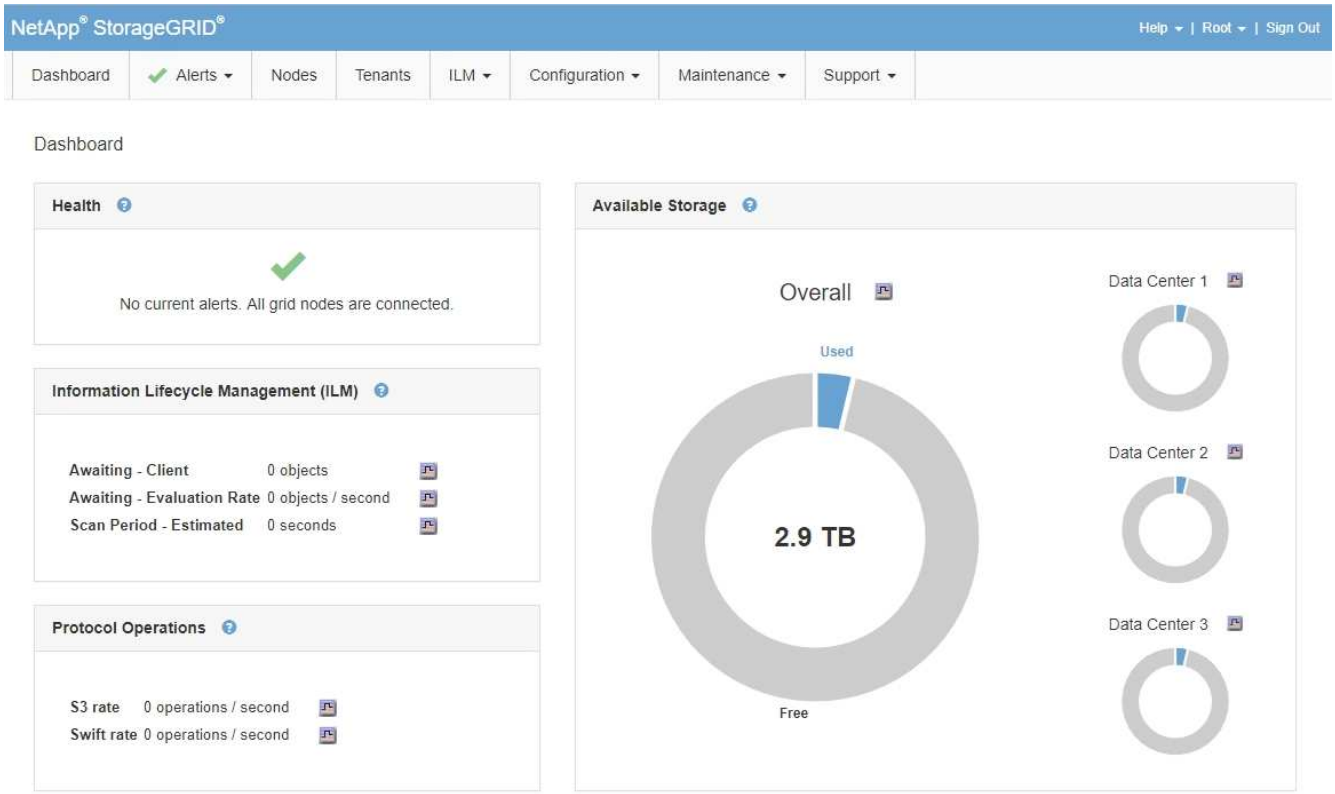



◦ StorageGRID システムで SSO が有効になっており、 Grid Manager またはテナントアカウントに以前にアクセスしたことがある場合は、次の手順を実行します。

i. 次のいずれかを実行します。

- 「* 0 *」（Grid ManagerのアカウントID）と入力し、*サインイン*をクリックします。
- 最近のアカウントのリストに* Grid Manager *が表示されている場合は、*サインイン*をクリックします。

ii. 組織の SSO サインインページで通常使用している SSO クレデンシャルを使用してサインインします。サインインすると、ダッシュボードが含まれた Grid Manager のホームページが表示されます。表示される情報については、StorageGRID の監視とトラブルシューティングの手順の「ダッシュボードの表示」を参照してください。




5. 別の管理ノードにサインインする場合は、次の手順を実行します。

| オプション | 手順 |
| --- | --- |
| SSO が有効になっていない | a. ブラウザのアドレスバーに、他の管理ノードの完全修飾ドメイン名または IP アドレスを入力します。必要に応じてポート番号を追加します。<br>b. Grid Manager のユーザ名とパスワードを入力します。<br>c. [ * サインイン * ] をクリックします。 |

| オプション | 手順 |
| --- | --- |
| SSO が有効です | ブラウザのアドレスバーに、他の管理ノードの完全修飾ドメイン名または IP アドレスを入力します。<br><br>1 つの管理ノードにサインインしたら、再度サインインしなくても他の管理ノードにアクセスできます。ただし、 SSO セッションが期限切れになると、クレデンシャルの再入力を求められます。<br><br>• 注： SSO は制限された Grid Manager ポートでは使用できません。ユーザをシングルサインオンで認証する場合は、デフォルトの HTTPS ポート（ 443 ）を使用する必要があります。 |

関連情報

"Web ブラウザの要件"

"ファイアウォールによるアクセス制御"

"サーバ証明書の設定"

"シングルサインオンを設定しています"

"管理者グループの管理"

"ハイアベイラビリティグループの管理"

"テナントアカウントを使用する"

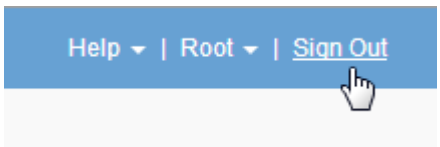
"トラブルシューティングを監視します"

### **Grid Manager**からサインアウトします

Grid Manager の使用が完了したら、サインアウトして、権限のないユーザが StorageGRID システムにアクセスできないようにする必要があります。ブラウザのクッキーの設定によっては、ブラウザを閉じてもシステムからサインアウトされない場合があります。

手順

1. ユーザインターフェイスの右上隅にある [**Sign Out**] リンクを探します。




2. [サインアウト]をクリックします。

| オプション | 説明 |
| --- | --- |
| SSO は使用されていません | 管理ノードからサインアウトされます。<br><br>Grid Manager のサインインページが表示されます。<br><br>• 注： * 複数の管理ノードにサインインした場合、各ノードからサインアウトする必要があります。 |
| SSO が有効です | アクセスしていたすべての管理ノードからサインアウトされます。StorageGRID のサインインページが表示されます。**Grid Manager** は、 [Recent Accounts] * ドロップダウンにデフォルトとして表示され、 [**Account ID**] フィールドには 0 と表示されます。<br><br>• 注： SSO が有効で Tenant Manager にもサインインしている場合は、 SSO からサインアウトするためにテナントアカウントからもサインアウトする必要があります。 |

関連情報

"シングルサインオンを設定しています"

"テナントアカウントを使用する"

パスワードを変更しています

## Grid Manager のローカルユーザは自分のパスワードを変更できます。

必要なもの

Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

このタスクについて

フェデレーテッドユーザとして StorageGRID にサインインする場合、またはシングルサインオン（ SSO ）が有効になっている場合は、 Grid Manager でパスワードを変更できません。代わりに、 Active Directory や OpenLDAP などの外部 ID ソースでパスワードを変更する必要があります。

手順

1. Grid Managerのヘッダーで、*自分の名前>パスワードの変更*を選択します。
2. 現在のパスワードを入力します。
3. 新しいパスワードを入力します。

   パスワードは 8 文字以上 32 文字以下にする必要があります。パスワードでは大文字と小文字が区別されます。

4. 新しいパスワードをもう一度入力します。

5. [ 保存（ Save ） ] をクリックします。

プロビジョニングパスフレーズを変更しています

この手順 を使用して、 StorageGRID プロビジョニングパスフレーズを変更します。パスフレーズは、リカバリ、拡張、およびメンテナンスの手順で必要になります。StorageGRID システムのグリッドトポロジ情報と暗号化キーを含むリカバリパッケージのバックアップをダウンロードする場合も、パスフレーズが必要です。

必要なもの

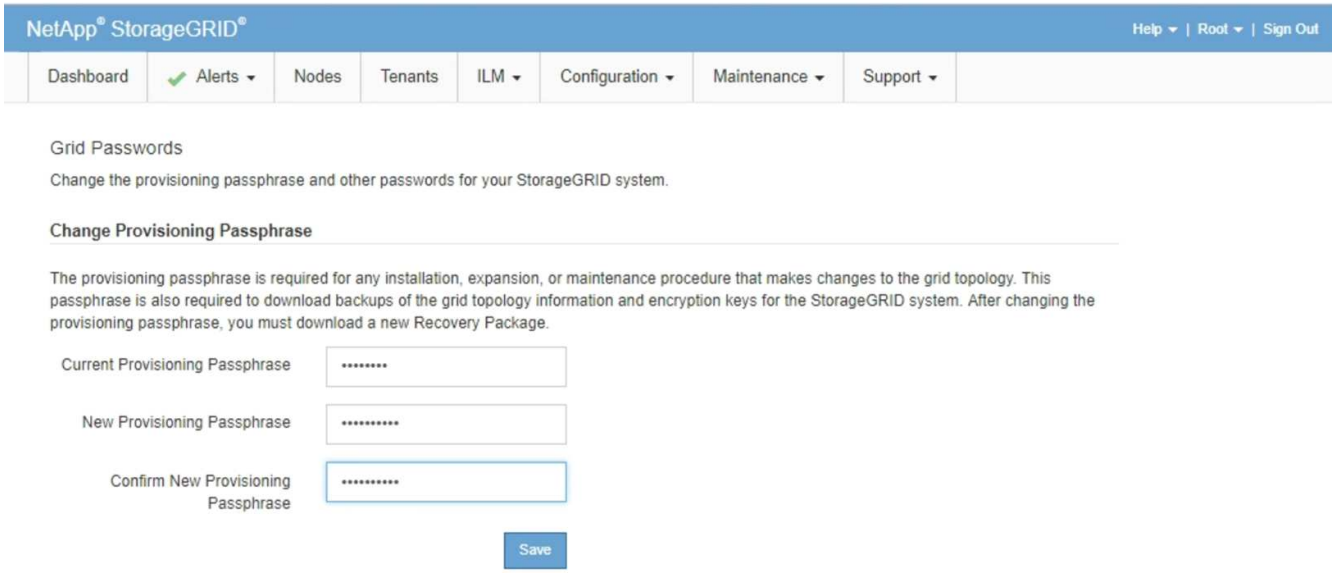
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- MaintenanceまたはRoot Access権限が必要です。
- 現在のプロビジョニングパスフレーズが必要です。

このタスクについて

プロビジョニングパスフレーズは、インストールやメンテナンスの手順の多くや、リカバリパッケージのダウンロードで必要になります。プロビジョニングパスフレーズは、に表示されません `Passwords.txt` ファイル。プロビジョニングパスフレーズを記録して、安全な場所に保管してください。

手順

1. [構成（Configuration ）**]>[***アクセス制御（* Access Control ）**]>[** Gridパスワード*（* Grid

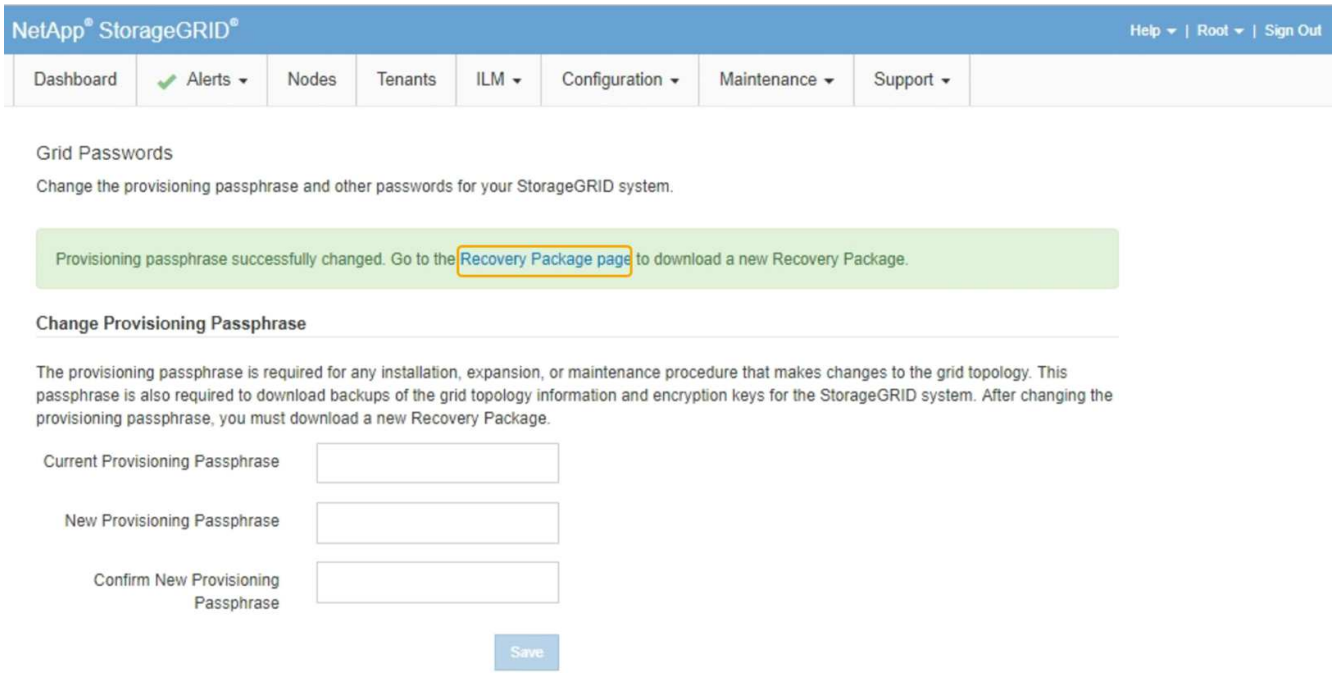



2. 現在のプロビジョニングパスフレーズを入力します。
3. 新しいリンフレーズを入力してください。パスフレーズには8文字以上32文字以下の文字列を含める必要があります。パスフレーズでは大文字と小文字が区別されます。

> 新しいプロビジョニングパスフレーズを安全な場所に保存します。インストール、拡張、およびメンテナンスの手順を実行する必要があります。

4. 新しいパスフレーズをもう一度入力し、*保存*をクリックします。

プロビジョニングパスフレーズの変更が完了すると、成功を示す緑のバナーが表示されます。変更には1分未満かかります。




5. 成功バナー内の*リカバリパッケージページ*リンクを選択します。
6. Grid Manager から新しいリカバリパッケージをダウンロードします。[* Maintenance **>]>[** Recovery Package]を選択し、新しいプロビジョニングパスフレーズを入力します。

> プロビジョニングパスフレーズを変更したら、すぐに新しいリカバリパッケージをダウンロードする必要があります。リカバリパッケージファイルは、障害が発生した場合にシステムをリストアするために使用します。

ブラウザセッションのタイムアウトを変更する

## Grid Manager ユーザと Tenant Manager ユーザが一定期間非アクティブになった場合にサインアウトするかどうかを制御できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

GUI の非アクティブ時のタイムアウトのデフォルト値は 900 秒（ 15 分）です。ユーザのブラウザセッションがこの時間以上アクティブでない場合、セッションはタイムアウトします。

必要に応じて、 GUI の Inactivity Timeout 表示オプションを設定して、タイムアウト時間を増減できます。

シングルサインオン（SSO）が有効になっていて、ユーザーのブラウザーセッションがタイムアウトした場合、システムはユーザーが手動で「サインアウト」をクリックしたかのように動作します。StorageGRID に再度アクセスするには、ユーザが SSO クレデンシャルを再入力する必要があります。

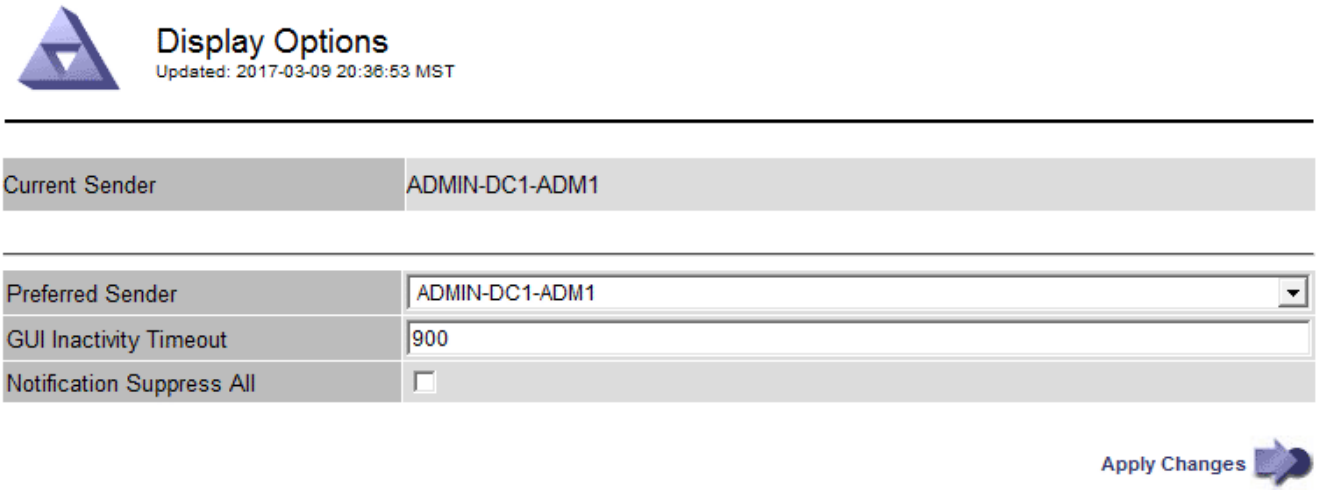
ユーザセッションのタイムアウトは、次の方法でも制御できます。

- システムセキュリティ用の、個別の設定不可能な StorageGRID タイマー。デフォルトでは、各ユーザの認証トークンはユーザがサインインしてから 16 時間後に期限切れになります。ユーザの認証が期限切れになると、 GUI の非アクティブ時のタイムアウト値に達していなくても、そのユーザは自動的にサインアウトされます。トークンを更新するには、再度サインインする必要があります。
- SSO が有効になっている StorageGRID では、アイデンティティプロバイダのタイムアウト設定が使用されます。

手順

1. * Configuration > System Settings > Display Options *を選択します。
2. * GUI の非アクティブ時のタイムアウト * には、 60 秒以上のタイムアウト時間を入力します。

   この機能を使用しない場合は、このフィールドを 0 に設定します。ユーザは、サインインしてから 16 時間後、認証トークンが期限切れになった時点でサインアウトされます。




3. [ 変更の適用 *] をクリックします。

   新しい設定は、現在サインインしているユーザには影響しません。新しいタイムアウト設定を有効にするには、ユーザが再度サインインするか、ブラウザを更新する必要があります。

関連情報

"シングルサインオンの仕組み"

"テナントアカウントを使用する"

**StorageGRID** ライセンス情報の表示

## グリッドの最大ストレージ容量など、 StorageGRID システムのライセンス情報を必要に応じていつでも表示できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

このタスクについて

この StorageGRID システムのソフトウェアライセンスを含む問題 がある場合、ダッシュボードのヘルスパネルにはライセンスステータスアイコンと * ライセンス * リンクが表示されます。この数値は、ライセンス関連の問題の数を示しています。

ステップ

ライセンスを表示するには、次のいずれかを実行します。

- ダッシュボードの正常性パネルで、ライセンスステータスアイコンまたは*ライセンス*リンクをクリックします。このリンクは、ライセンスを持つ問題 が存在する場合にのみ表示されます。
- [* Maintenance ** System * License（メンテナンス*システム*ライセンス）]を選択します。

ライセンスページが表示され、現在のライセンスに関する次の読み取り専用情報が提供されます。

- StorageGRID システム ID 。この StorageGRID インストールの一意の ID 番号です
- ライセンスのシリアル番号
- グリッドのライセンスが付与されているストレージ容量
- ソフトウェアライセンスの終了日
- サポートサービス契約の終了日
- ライセンステキストファイルの内容

StorageGRID 10.3 より前に発行されたライセンスの場合、ライセンスで許可されているストレージ容量はライセンスファイルに含まれておらず、値の代わりに「 See License Agreement 」というメッセージが表示されます。

**StorageGRID** ライセンス情報を更新しています

ライセンス内容に変更があった場合は、 StorageGRID システムのライセンス情報を更新する必要があります。たとえば、グリッド用のストレージ容量を追加で購入した場合は、ライセンス情報を更新する必要があります。

必要なもの

- StorageGRID システムに適用する新しいライセンスファイルが必要です。
- 特定のアクセス権限が必要です。
- プロビジョニングパスフレーズが必要です。

手順

1. [* Maintenance ** System * License（メンテナンス*システム*ライセンス）]を選択します。
2. StorageGRID システムのプロビジョニングパスフレーズを * プロビジョニングパスフレーズ * テキストボックスに入力します。
3. [* 参照 ] をクリックします。
4. [開く]ダイアログボックスで、新しいライセンスファイルを探して選択します (`.txt`)をクリックし、*開く*をクリックします。

   新しいライセンスファイルが検証され、表示されます。

5. [ 保存（ Save ） ] をクリックします。

グリッド管理**API**を使用する

## Grid Manager のユーザインターフェイスの代わりにグリッド管理 REST API を使用して、システム管理タスクを実行できます。たとえば、 API を使用して処理を自動化したり、ユーザなどの複数のエンティティを迅速に作成したりできます。

グリッド管理 API では、 Swagger オープンソース API プラットフォームを使用します。Swagger のわかりやすいユーザインターフェイスを使用して、開発者および一般のユーザは StorageGRID で API を使用してリアルタイムの処理を実行できます。

トップレベルのリソース

グリッド管理 API で使用可能な最上位のリソースは次のとおりです。

- `/grid`：Grid Managerユーザのみがアクセスでき、設定されているグループ権限に基づいてアクセスが制限されます。
- `/org`：テナントアカウントのローカルまたはフェデレーテッドLDAPグループに属するユーザのみがアクセスできます。詳細については、テナントアカウントの使用に関する情報を参照してください。
- `/private`：Grid Managerユーザのみがアクセスでき、設定されているグループ権限に基づいてアクセスが制限されます。これらのAPIは内部使用のみを目的としており、正式にドキュメント化されていません。また、これらのAPIは予告なく変更される場合があります。

関連情報

"テナントアカウントを使用する"

"Prometheus：クエリの基本"

グリッド管理 **API** の処理

## グリッド管理 API では、使用可能な API 処理が次のセクションに分類されます。

- *accounts * — 新規アカウントの作成や特定の使用状況の取得など ' ストレージ・テナント・アカウントを管理するためのオペレーション
- * alarms * - 現在のアラーム（レガシーシステム）をリストし、現在のアラートやノード接続状態の概要など、グリッドの健全性に関する情報を返す処理。
- *alert-history * — 解決済みアラートに関する操作。
- *alert-Receiver * — アラート通知受信者（電子メール）に関する操作。
- *alert-rules * — アラートルールに関する操作
- *alert-silences *-- アラートのサイレンスに関するオペレーション。
- * alerts * — アラートの処理。
- * audit * — 監査構成をリストおよび更新する処理。
- **auth** — ユーザセッション認証を実行するための操作。

  グリッド管理 API は、ベアラートークン認証方式をサポートしています。サインインするには、認証要求（つまり、 `POST /api/v3/authorize`）。ユーザが認証されると、セキュリティトークンが返されます。このトークンは、後続の API 要求（「 Authorization ： Bearer_token_ 」）のヘッダーで指定する必要があります。

  > StorageGRID システムでシングルサインオンが有効になっている場合は、別の手順による認証が必要です。「シングルサインオンが有効な場合の API へのサインイン」を参照してください。

  認証セキュリティの向上については、「クロスサイトリクエストフォージェリに対する保護」を参照してください。

- * client-certificates * — 外部監視ツールを使用して StorageGRID に安全にアクセスできるようにクライアント証明書を設定する処理。
- **config** — 製品リリースと Grid Management API のバージョンに関連する操作。製品のリリースバージョンおよびそのリリースでサポートされているグリッド管理 API のメジャーバージョンをリストし、廃止されたバージョンの API を無効にすることができます。
- * deactivated-features * — 非アクティブ化された可能性のある機能を表示する操作。
- *dns-servers * — 設定済みの外部 DNS サーバをリストおよび変更する処理。
- * endpoint-domain-names * — エンドポイントドメイン名をリストおよび変更する処理。
- * erasure-coding * — イレイジャーコーディングプロファイルに対する処理。
- *expansion *-- 拡張の操作 ( プロシージャレベル ) 。
- * expansion-nodes * - 拡張処理（ノードレベル）。
- * expansion-sitites * — 拡張の操作（サイトレベル）。
- * grid-networks * — グリッドネットワークリストをリストおよび変更する処理。
- * grid-password* - グリッドパスワード管理の操作。
- *groups * — ローカルグリッド管理者グループを管理し、フェデレーテッドグリッド管理者グループを外部 LDAP サーバから取得するための処理。
- * identity-source * — 外部のアイデンティティソースを設定する処理、およびフェデレーテッドグループとユーザ情報を手動で同期する処理。

- *ilm * — 情報ライフサイクル管理 (ILM; 情報ライフサイクル管理 ) の操作。
- **license** — StorageGRID ライセンスを取得および更新する処理。
- **logs** — ログファイルを収集してダウンロードするための操作。
- * メトリクス * — ある時点での瞬時の指標クエリや、一定期間にわたる指標クエリなど、 StorageGRID メトリックに対する処理。グリッド管理 API は、バックエンドのデータソースとして Prometheus システム監視ツールを使用します。Prometheus クエリの構築については、 Prometheus の Web サイトを参照してください。

> を含む指標*`private`* 名前には、内部使用のみを目的としています。これらの指標は、StorageGRID のリリース間で予告なく変更される可能性があります。

- * node-health * - ノードのヘルスステータスに関する処理。
- *ntp-servers * — 外部ネットワークタイムプロトコル（ NTP ）サーバをリストまたは更新する処理。
- * objects * — オブジェクトおよびオブジェクトメタデータに対する処理。
- **recovery** — リカバリ手順 の処理。
- * recovery-package * — リカバリパッケージをダウンロードする処理。
- *regions * — 領域の表示と作成のための操作。
- *s3-object-lock * — グローバルな S3 オブジェクトロック設定に対する処理。
- *server-certificate * — Grid Manager サーバ証明書を表示および更新する処理。
- *snmp * — 現在の SNMP 設定に対する操作。
- *traffic-classes *-- トラフィック分類ポリシーの操作。
- *untrusted-client-network * — 信頼されていないクライアントネットワーク構成に対する操作。
- * users * — Grid Manager ユーザーを表示および管理する操作。

**API**要求の実行

## Swagger のユーザインターフェイスでは、各 API 処理に関する詳細情報とドキュメントを参照できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

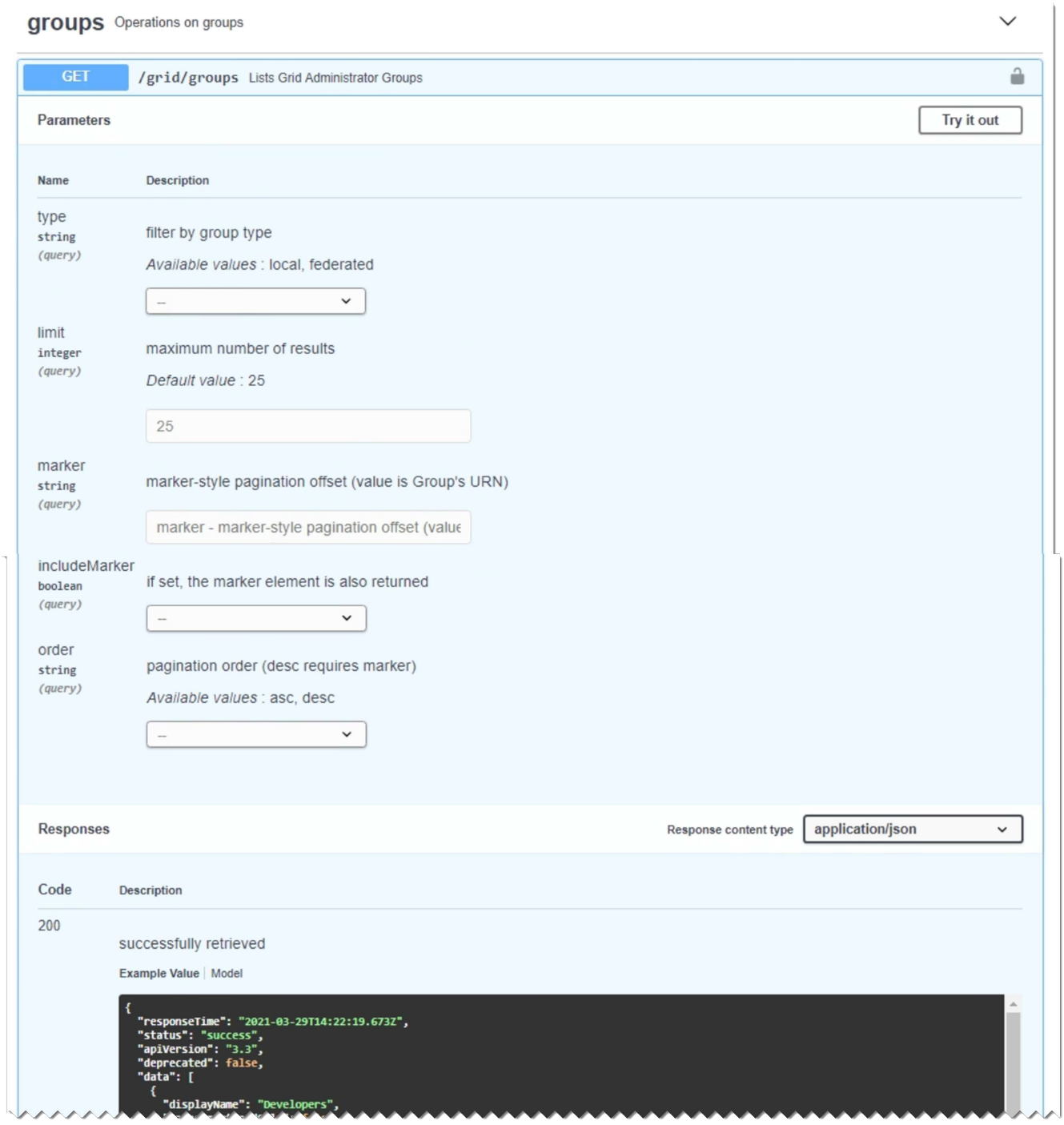
> API Docs Web ページを使用して実行する API 処理はすべてその場で実行されます。設定データやその他のデータを誤って作成、更新、または削除しないように注意してください。

手順

1. Grid Managerヘッダーから* Help > API Documentation *を選択します。
2. 目的の処理を選択します。

   API 処理を拡張すると、 GET 、 PUT 、 UPDATE 、 DELETE など、使用可能な HTTP アクションを確認できます。

3. HTTP アクションを選択して、要求の詳細を確認します。これには、エンドポイント URL 、必須またはオプションのパラメータのリスト、要求の本文の例（必要な場合）、想定される応答が含まれます。




4. グループやユーザの ID など、要求で追加のパラメータが必要かどうかを確認します。次に、これらの値を取得します。必要な情報を取得するために、先に別の API 要求の問題 が必要になることがあります。
5. 要求の本文の例を変更する必要があるかどうかを判断します。その場合は、[*Model]をクリックして各フィールドの要件を確認できます。
6. [* 試してみてください * ] をクリックします。
7. 必要なパラメータを指定するか、必要に応じて要求の本文を変更します。
8. [* Execute] をクリックします。

9. 応答コードを確認し、要求が成功したかどうかを判断します。

グリッド管理 **API** のバージョン管理

## グリッド管理 API では、バージョン管理を使用して無停止アップグレードがサポートされます。

たとえば、次の要求 URL ではバージョン 3 の API が指定されています。

```
https://hostname_or_ip_address/api/v3/authorize
```

旧バージョンとの互換性がない *_not compatible _ * の変更が行われると、テナント管理 API のメジャーバージョンが上がります。以前のバージョンと互換性がある _ * の変更を行うと、テナント管理 API のマイナーバージョンが上がります。互換性のある変更には、新しいエンドポイントやプロパティの追加などがあります。次の例は、変更のタイプに基づいて API バージョンがどのように更新されるかを示しています。

| **API** に対する変更のタイプ | 古いバージョン | 新しいバージョン |
|---|---|---|
| 旧バージョンと互換性があります | 2.1 | 2.2. |
| 旧バージョンとの互換性がありません | 2.1 | 3.0 |

StorageGRID ソフトウェアを初めてインストールした時点では、グリッド管理 API の最新のバージョンのみが有効になっています。ただし、 StorageGRID の新機能リリースにアップグレードした場合、少なくとも StorageGRID の機能リリース 1 つ分の間は、古い API バージョンにも引き続きアクセスできます。

> グリッド管理 API を使用して、サポートされるバージョンを設定できます。詳細については、 Swagger API のドキュメントの「 config 」セクションを参照してください。すべての Grid 管理 API クライアントを新しいバージョンを使用するように更新したら、古いバージョンのサポートを無効にする必要があります。

古い要求は、次の方法で廃止とマークされます。

- 応答ヘッダーが「 Deprecated ： true 」となる。
- JSON 応答の本文に「 deprecated ： true 」が追加される
- 廃止の警告が nms.log に追加される。例：

```
Received call to deprecated v1 API at POST "/api/v1/authorize"
```

現在のリリースでサポートされている**API**バージョンを確認します

サポートされている API のメジャーバージョンのリストを返すには、次の API 要求を使用します。

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2019-01-10T20:41:00.845Z",
  "status": "success",
  "apiVersion": "3.0",
  "data": [
    2,
    3
  ]
}
```

要求の**API**バージョンの指定

パスパラメータを使用してAPIバージョンを指定できます (`/api/v3`）またはヘッダー (`Api-Version: 3` ）。両方の値を指定した場合は、ヘッダー値がパス値よりも優先されます。

```
curl https://[IP-Address]/api/v3/grid/accounts

curl -H "Api-Version: 3" https://[IP-Address]/api/grid/accounts
```

クロスサイトリクエストフォージェリ（**CSRF**）の防止

CSRF トークンを使用してクッキーによる認証を強化すると、 StorageGRID に対するクロスサイトリクエストフォージェリ（ CSRF ）攻撃を防ぐことができます。Grid Manager と Tenant Manager はこのセキュリティ機能を自動的に有効にします。他の API クライアントは、サインイン時にこの機能を有効にするかどうかを選択できます。

攻撃者が別のサイト（たとえば、 HTTP フォーム POST を使用して）への要求をトリガーできる場合、サインインしているユーザのクッキーを使用して特定の要求を原因 が送信できます。

StorageGRID では、 CSRF トークンを使用して CSRF 攻撃を防ぐことができます。有効にした場合、特定のクッキーの内容が特定のヘッダーまたは特定の POST パラメータの内容と一致する必要があります。

この機能を有効にするには、を設定します `csrfToken` パラメータの値 `true` 認証中です。デフォルトはです `false`。

```
curl -X POST --header "Content-Type: application/json" --header "Accept:
application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

trueの場合は、Aです `GridCsrfToken` クッキーは、Grid Managerおよびへのサインインにランダムな値を使用して設定されます `AccountCsrfToken` クッキーは、Tenant Managerへのサインインではランダムな値で設定されます。

クッキーが存在する場合は、システムの状態を変更できるすべての要求（ POST 、 PUT 、 PATCH 、 DELETE ）には次のいずれかが含まれている必要があります。

- 。 `X-Csrf-Token` CSRFトークンクッキーの値がヘッダーに設定されています。
- エンドポイントがフォームエンコードされた本文を受け入れる場合：A `csrfToken` フォームエンコードされた要求の本文パラメータ。

その他の例および詳細については、オンラインの API ドキュメントを参照してください。

> CSRFトークンクッキーが設定されている要求では、も適用されます `"Content-Type: application/json"` CSRF攻撃からの保護がさらに強化されるために、JSON要求の本文が必要なすべての要求のヘッダー。

シングルサインオンが有効な場合は、**API**を使用します

## StorageGRID システムでシングルサインオン（SSO）が有効になっている場合、標準の認証API要求を使用してグリッド管理APIまたはテナント管理APIにサインインおよびサインアウトすることはできません。

シングルサインオンが有効な場合は、**API**へのサインイン

シングルサインオン（SSO）が有効になっている場合は、グリッド管理APIまたはテナント管理APIで有効なAD FSから認証トークンを取得するための一連のAPI要求を問題 で処理する必要があります。

必要なもの

- StorageGRID ユーザグループに属するフェデレーテッドユーザの SSO ユーザ名とパスワードが必要です。
- テナント管理 API にアクセスする場合は、テナントアカウント ID を確認しておきます。

このタスクについて

認証トークンを取得するには、次のいずれかの例を使用します。

- 。 `storagegrid-ssoauth.py` Pythonスクリプト。StorageGRID インストールファイルのディレクトリにあります (`./rpms` Red Hat Enterprise LinuxまたはCentOSの場合： `./debs` UbuntuまたはDebianの場合は、および `./vsphere` VMwareの場合）をクリックします。
- cURL 要求のワークフローの例。

  cURL ワークフローは、実行に時間がかかりすぎるとタイムアウトする場合があります。「A valid SubjectConfirmation was not found on this Response」というエラーが表示される可能性があります。

  > cURL ワークフローの例では、パスワードが他のユーザに表示されないように保護されていません。

URLエンコード問題 がある場合は、「Unsupported SAML version」というエラーが表示される可能性があり

ます。

手順

1. 認証トークンを取得するには、次のいずれかの方法を選択します。
   - を使用します `storagegrid-ssoauth.py` Pythonスクリプト。手順 2 に進みます。
   - curl 要求を使用します。手順 3 に進みます。
2. を使用する場合は、を参照してください `storagegrid-ssoauth.py` スクリプトを使用して、Pythonインタープリタにスクリプトを渡し、スクリプトを実行します。

   プロンプトが表示されたら、次の引数の値を入力します。

   - SSO ユーザ名
   - StorageGRID がインストールされているドメイン
   - StorageGRID のアドレス
   - テナント管理APIにアクセスする場合は、テナントアカウントIDを入力します。

   [+]
   ```
   python3 /tmp/storagegrid-ssoauth.py
   saml_user: my-sso-username
   saml_domain: my-domain
   sg_address: storagegrid.example.com
   tenant_account_id: 12345
   Enter the user's SAML password:
   ********************************************************************************

   ********************************************************************************
   StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
   ```

   StorageGRID 認証トークンが出力に表示されます。SSO を使用していない場合の API の使用方法と同様に、トークンを他の要求に使用できるようになりました。

3. cURL 要求を使用する場合は、次の手順 を使用します。

   a. サインインに必要な変数を宣言します。

   ```
   export SAMLUSER='my-sso-username'
   export SAMLPASSWORD='my-password'
   export SAMLDOMAIN='my-domain'
   export TENANTACCOUNTID='12345'
   export STORAGEGRID_ADDRESS='storagegrid.example.com'
   export AD_FS_ADDRESS='adfs.example.com'
   ```

   > グリッド管理APIにアクセスするには、として0を使用します `TENANTACCOUNTID`。

   b. 署名付き認証URLを受信するには、へのPOST要求を問題 に送信します `/api/v3/authorize-saml`をクリックし、応答からJSONエンコードを削除します。

次の例は、の署名付き認証URLに対するPOST要求を示しています `TENANTACCOUNTID`。結果は python-m json ツールに渡され、 JSON エンコードが削除されます。

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
  -H "accept: application/json" -H  "Content-Type: application/json"
\
  --data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

この例の応答には、 URL エンコードされた署名済み URL が含まれていますが、 JSON エンコードされたレイヤは含まれていません。

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZHLbsIwEEV%2FJTuv7...
sSl%2BfQ33cvfwA%3D&RelayState=12345",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

c. を保存します `SAMLRequest` 後続のコマンドで使用する応答から。

```
export SAMLREQUEST='fZHLbsIwEEV%2FJTuv7...sSl%2BfQ33cvfwA%3D'
```

d. AD FS からクライアント要求 ID を含む完全な URL を取得します。

1 つは、前の応答の URL を使用してログインフォームを要求する方法です。

```
curl
"https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=
$TENANTACCOUNTID" | grep 'form method="post" id="loginForm"'
```

応答にはクライアント要求 ID が含まれています。

```
<form method="post" id="loginForm" autocomplete="off"
novalidate="novalidate" onKeyPress="if (event && event.keyCode == 13)
Login.submitLoginRequest();" action="/adfs/ls/?
SAMLRequest=fZHRToMwFIZfhb...UJikvo77sXPw%3D%3D&RelayState=12345&clie
nt-request-id=00000000-0000-0000-ee02-0080000000de" >
```

e. 応答からクライアント要求 ID を保存します。

```
export SAMLREQUESTID='00000000-0000-0000-ee02-0080000000de'
```

f. 前の応答のフォームアクションにクレデンシャルを送信します。

```
curl -X POST
"https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=
$TENANTACCOUNTID&client-request-id=$SAMLREQUESTID" \
  --data
"UserName=$SAMLUSER@$SAMLDOMAIN&Password=$SAMLPASSWORD&AuthMethod=For
msAuthentication" --include
```

AD FS からヘッダーに追加情報 が含まれた 302 リダイレクトが返されます。

> SSO システムで多要素認証（ MFA ）が有効になっている場合、フォームポストには 2 つ目のパスワードまたはその他のクレデンシャルも含まれます。

```
HTTP/1.1 302 Found
Content-Length: 0
Content-Type: text/html; charset=utf-8
Location:
https://adfs.example.com/adfs/ls/?SAMLRequest=fZHRToMwFIZfhb...UJikvo
77sXPw%3D%3D&RelayState=12345&client-request-id=00000000-0000-0000-
ee02-0080000000de
Set-Cookie: MSISAuth=AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY=; path=/adfs;
HttpOnly; Secure
Date: Tue, 06 Nov 2018 16:55:05 GMT
```

g. を保存します `MSISAuth` 応答からのCookie。

```
export MSISAuth='AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY='
```

h. 認証 POST からクッキーを使用して、指定した場所に GET 要求を送信します。

```
curl
"https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=
$TENANTACCOUNTID&client-request-id=$SAMLREQUESTID" \
  --cookie "MSISAuth=$MSISAuth" --include
```

応答ヘッダーには、あとでログアウトに使用する AD FS セッション情報が含まれます。応答の本文には、非表示のフォームフィールドに SAMLResponse が含まれています。

```
HTTP/1.1 200 OK
Cache-Control: no-cache,no-store
Pragma: no-cache
Content-Length: 5665
Content-Type: text/html; charset=utf-8
Expires: -1
Server: Microsoft-HTTPAPI/2.0
P3P: ADFS doesn't have P3P policy, please contact your site's admin
for more details
Set-Cookie:
SamlSession=a3dpbnRlcnMtUHJpbWFyeS1BZG1pbi0xNzgmRmFsc2Umcng4NnJDZmFKV
XFxVWx3bkl1MnFuUSUzZCUzZCYmJiYmXzE3MjAyZTA5LThmMDgtNDRkZC04Yzg5LTQ3ND
UxYzA3ZjkzYw==; path=/adfs; HttpOnly; Secure
Set-Cookie: MSISAuthenticated=MTEvNy8yMDE4IDQ6MzI6NTkgUE0=;
path=/adfs; HttpOnly; Secure
Set-Cookie: MSISLoopDetectionCookie=MjAxOC0xMS0wNzoxNjozMjo1OVpcMQ==;
path=/adfs; HttpOnly; Secure
Date: Wed, 07 Nov 2018 16:32:59 GMT

<form method="POST" name="hiddenform"
action="https://storagegrid.example.com:443/api/saml-response">
  <input type="hidden" name="SAMLResponse"
value="PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4=" /><input
type="hidden" name="RelayState" value="12345" />
```

i. を保存します `SAMLResponse` 非表示フィールドから：

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. を使用して保存します `SAMLResponse`をクリックして、StorageGRID を作成します`/api/saml-response` StorageGRID 認証トークンの生成要求

の場合 `RelayState`をクリックします。グリッド管理APIにサインインする場合は、テナントアカウントIDを使用します。

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
  -H "accept: application/json" \
  --data-urlencode "SAMLResponse=$SAMLResponse" \
  --data-urlencode "RelayState=$TENANTACCOUNTID" \
  | python -m json.tool
```

応答には認証トークンが含まれています。

```
{
    "apiVersion": "3.0",
    "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
    "responseTime": "2018-11-07T21:32:53.486Z",
    "status": "success"
}
```

a. 認証トークンを応答にという名前で保存します `MYTOKEN`。

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

これで、を使用できます `MYTOKEN` その他の要求の場合は、SSOを使用していない場合のAPIの使用方法と同様です。

## シングルサインオンが有効な場合は、**API**からのサインアウト

シングルサインオン（ SSO ）が有効になっている場合は、グリッド管理 API またはテナント管理 API からサインアウトするための一連の API 要求を問題 で処理する必要があります。

### このタスクについて

必要に応じて、組織のシングルログアウトページからログアウトするだけで、 StorageGRID API からサインアウトできます。または、 StorageGRID からシングルログアウト（ SLO ）を実行することもできます。この場合、有効な StorageGRID ベアラトークンが必要です。

### 手順

1. 署名されたログアウト要求を生成するには、合格します `cookie "sso=true"` SLO APIで次の処理を実行します。

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

ログアウト URL が返されます。

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3
D",
    "responseTime": "2018-11-20T22:20:30.839Z",
    "status": "success"
}
```

2. ログアウト URL を保存します。

```
export
LOGOUT_REQUEST='https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEI
RfhZ...HcQ%3D%3D'
```

3. 要求をログアウト URL に送信し、 SLO を実行して StorageGRID にリダイレクトします。

```
curl --include "$LOGOUT_REQUEST"
```

302 応答が返されます。リダイレクト先は API のみのログアウトには適用されません。

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: MSISSignoutProtocol=U2FtbA==; expires=Tue, 20 Nov 2018
22:35:03 GMT; path=/adfs; HttpOnly; Secure
```

4. StorageGRID Bearer トークンを削除します。

StorageGRID Bearer トークンを削除すると、 SSO を使用しない場合と同じように動作します。状況 `cookie "sso=true"` を指定しないと、SSOの状態に影響を及ぼすことなくユーザがStorageGRID からログアウトされます。

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

A `204 No Content` 応答として、ユーザがサインアウトしたことが示されます。

```
HTTP/1.1 204 No Content
```

**StorageGRID** セキュリティ証明書を使用する

# セキュリティ証明書は、 StorageGRID コンポーネント間、および StorageGRID コンポーネントと外部システム間のセキュアで信頼された接続の確立に使用される小さいデータファイルです。

StorageGRID では、 2 種類のセキュリティ証明書が使用されます。

- * HTTPS 接続を使用する場合は、サーバー証明書 * が必要です。サーバ証明書は、クライアントとサーバ間のセキュアな接続を確立し、クライアントに対するサーバの ID を認証し、データのセキュアな通信パスを提供するために使用されます。サーバとクライアントには、それぞれ証明書のコピーがあります。
- * クライアント証明書 * は、クライアントまたはユーザー ID をサーバーに対して認証し、パスワードだけではなく、より安全な認証を提供します。クライアント証明書はデータを暗号化しません。

クライアントが HTTPS を使用してサーバに接続すると、サーバはサーバ証明書を返します。このサーバ証明書には公開鍵が含まれています。クライアントは、サーバの署名と証明書のコピーの署名を比較して、この証明書を検証します。署名が一致した場合、クライアントは同じ公開鍵を使用してサーバとのセッションを開始します。

StorageGRID は、一部の接続（ロードバランサエンドポイントなど）のサーバとして、または他の接続（ CloudMirror レプリケーションサービスなど）のクライアントとして機能します。

外部の認証局（ CA ）は、組織の情報セキュリティポリシーに完全に準拠した問題 カスタム証明書を作成できます。StorageGRID には、システムのインストール時に内部CA証明書を生成するCAも組み込まれています。デフォルトでは、これらの内部CA証明書を使用して、内部StorageGRID トラフィックが保護されます。非本番環境では内部CA証明書を使用できますが、本番環境では外部の認証局が署名したカスタム証明書を使用することを推奨します。証明書なしのセキュアでない接続もサポートされますが、推奨されません。

- カスタム CA 証明書では内部証明書は削除されませんが、カスタム証明書にはサーバ接続の検証用の証明書を指定する必要があります。
- すべてのカスタム証明書が、サーバ証明書のシステム強化ガイドラインを満たしている必要があります。

  "システムの保護対策"

- StorageGRID では、 CA からの証明書を 1 つのファイル（ CA 証明書バンドル）にバンドルすることがサポートされています。

> StorageGRID には、すべてのグリッドで同じオペレーティングシステムの CA 証明書も含まれています。本番環境では、オペレーティングシステムの CA 証明書の代わりに、外部の認証局によって署名されたカスタム証明書を指定してください。

サーバ証明書とクライアント証明書のタイプのバリエーションは、いくつかの方法で実装されます。システムを設定する前に、特定の StorageGRID 構成に必要なすべての証明書を準備しておく必要があります。

| 証明書 | 証明書のタイプ | 説明 | ナビゲーションの場所 | 詳細 |
| --- | --- | --- | --- | --- |
| 管理者クライアント証明書 | クライアント | StorageGRID が外部クライアントアクセスを認証できるように、各クライアントにインストールします。<br>• 許可された外部クライアントから StorageGRID Prometheus データベースにアクセスできるようにします。<br>• 外部ツールを使用して StorageGRID をセキュアに監視できます。 | 設定>*アクセス制御*>*クライアント証明書* | "管理者クライアント証明書の設定" |
| アイデンティティフェデレーション証明書 | サーバ | StorageGRID と外部のActive Directory、OpenLDAP、またはOracle Directory Server間の接続が認証されます。アイデンティティフェデレーションに使用され、管理者グループとユーザを外部システムで管理できます。 | 設定>*アクセス制御*>*アイデンティティフェデレーション* | "アイデンティティフェデレーションを使用する" |
| シングルサインオン（ SSO ）証明書 | サーバ | シングルサインオン（SSO）要求に使用されるActive Directoryフェデレーションサービス（AD FS）とStorageGRID 間の接続を認証します。 | 環境設定>*アクセスコントロール*>*シングルサインオン* | "シングルサインオンを設定しています" |

| 証明書 | 証明書のタイプ | 説明 | ナビゲーションの場所 | 詳細 |
| --- | --- | --- | --- | --- |
| キー管理サーバ（ KMS ）の証明書 | サーバとクライアント | StorageGRID と外部キー管理サーバ（ KMS ）の間の接続を認証します。この接続により、 StorageGRID アプライアンスノードに暗号化キーが提供されます。 | 構成>*システム設定*>*キー管理サーバ* | "キー管理サーバの追加（KMS）" |
| E メールアラート通知の証明書 | サーバとクライアント | アラート通知に使用される SMTP E メールサーバと StorageGRID 間の接続を認証します。<br>• SMTP サーバとの通信に Transport Layer Security （ TLS ）が必要な場合は、 E メールサーバの CA 証明書を指定する必要があります。<br>• SMTP E メールサーバで認証用のクライアント証明書が必要な場合にのみ、クライアント証明書を指定してください。 | アラート>*電子メールの設定* | "トラブルシューティングを監視します" |

| 証明書 | 証明書のタイプ | 説明 | ナビゲーションの場所 | 詳細 |
| --- | --- | --- | --- | --- |
| ロードバランサエンドポイントの証明書 | サーバ | S3またはSwiftクライアントとゲートウェイノードまたは管理ノード上のStorageGRID ロードバランササービスの間の接続を認証します。ロードバランサエンドポイントを設定する際に、ロードバランサ証明書をアップロードまたは生成します。クライアントアプリケーションは、StorageGRIDに接続してオブジェクトデータを保存および読み出す際にロードバランサ証明書を使用します。<br><br>*注：*ロードバランサ証明書は、通常のStorageGRID 処理で最も使用される証明書です。 | 設定>*ネットワーク設定*>*ロードバランサエンドポイント* | • "ロードバランサエンドポイントの設定"<br>• FabricPool のロードバランサエンドポイントの作成<br><br>"StorageGRID for FabricPool を設定します" |
| 管理インターフェイスのサーバ証明書 | サーバ | クライアントの Web ブラウザと StorageGRID 管理インターフェイスの間の接続を認証することで、ユーザがセキュリティの警告なしで Grid Manager とテナントマネージャにアクセスできるようにします。<br><br>この証明書は、 Grid 管理 API 接続とテナント管理 API 接続も認証します。<br><br>内部のCA証明書を使用するか、カスタム証明書をアップロードすることができます。 | 構成>*ネットワーク設定*>*サーバー証明書* | • "サーバ証明書の設定"<br>• "Grid ManagerおよびTenant Manager用のカスタムサーバ証明書を設定する" |

| 証明書 | 証明書のタイプ | 説明 | ナビゲーションの場所 | 詳細 |
| --- | --- | --- | --- | --- |
| クラウドストレージプールのエンドポイントの証明書 | サーバ | StorageGRID クラウドストレージプールから外部ストレージ（S3 GlacierやMicrosoft Azure BLOBストレージなど）への接続を認証します。クラウドプロバイダのタイプごとに別の証明書が必要です。 | • ilm >*ストレージ・プール | "ILM を使用してオブジェクトを管理する" |
| プラットフォームサービスのエンドポイント証明書 | サーバ | StorageGRID プラットフォームサービスから S3 ストレージリソースへの接続を認証します。 | • Tenant Manager * > * storage （ S3 ） * > * Platform services endpoints * | "テナントアカウントを使用する" |
| Object Storage API Service Endpoint Server証明書 | サーバ | ストレージノード上のLocal Distribution Router（LDR）サービスまたはゲートウェイノード上の廃止されたConnection Load Balancer（CLB）サービスへのセキュアなS3またはSwiftクライアント接続を認証します。 | 設定>*ネットワーク設定*>*ロードバランサエンドポイント* | "ストレージノードまたはCLBサービスへの接続用のカスタムサーバ証明書を設定する" |

例 **1** ：ロードバランササービス

この例では、 StorageGRID がサーバとして機能します。

1. ロードバランサエンドポイントを設定し、 StorageGRID でサーバ証明書をアップロードまたは生成します。
2. S3 または Swift クライアント接続をロードバランサエンドポイントに設定し、同じ証明書をクライアントにアップロードします。
3. クライアントは、データを保存または取得する際に HTTPS を使用してロードバランサエンドポイントに接続します。
4. StorageGRID は、公開鍵を含むサーバ証明書と、秘密鍵に基づく署名を返します。
5. クライアントは、サーバの署名と証明書のコピーの署名を比較して、この証明書を検証します。署名が一致した場合、クライアントは同じ公開鍵を使用してセッションを開始します。
6. クライアントがオブジェクトデータを StorageGRID に送信

例 2 ：外部キー管理サーバ（ KMS ）

この例では、 StorageGRID がクライアントとして機能します。

1. 外部キー管理サーバソフトウェアを使用する場合は、 StorageGRID を KMS クライアントとして設定し、 CA 署名済みサーバ証明書、パブリッククライアント証明書、およびクライアント証明書の秘密鍵を取得します。
2. Grid Manager を使用して KMS サーバを設定し、サーバ証明書とクライアント証明書およびクライアント秘密鍵をアップロードします。
3. StorageGRID ノードで暗号化キーが必要な場合、証明書からのデータと秘密鍵に基づく署名を含む KMS サーバに要求が送信されます。
4. KMS サーバは証明書の署名を検証し、 StorageGRID を信頼できることを決定します。
5. KMS サーバは、検証済みの接続を使用して応答します。

## StorageGRID への管理者アクセスの制御

StorageGRID システムへの管理者アクセスは、ファイアウォールポートを開くか閉じ、管理者グループとユーザを管理し、シングルサインオン（SSO）を設定し、StorageGRID 指標へのセキュアな外部アクセスを許可するクライアント証明書を提供することによって制御できます。

- "ファイアウォールによるアクセス制御"
- "アイデンティティフェデレーションを使用する"
- "管理者グループの管理"
- "ローカルユーザの管理"
- "StorageGRID にシングルサインオン（SSO）を使用する"
- "管理者クライアント証明書の設定"

### ファイアウォールによるアクセス制御

ファイアウォールでアクセスを制御するには、外部ファイアウォールで特定のポートを開くか、または閉じます。

#### 外部ファイアウォールでのアクセス制御

StorageGRID 管理ノード上のユーザインターフェイスと API へのアクセスは、外部ファイアウォールで特定のポートを開くか、または閉じることで制御できます。たとえば、システムアクセスを制御する他の方法に加えて、ファイアウォールでテナントが Grid Manager に接続できないようにすることができます。

| ポート | 説明 | ポートが開いている場合 |
| --- | --- | --- |
| 443 | 管理ノードのデフォルトの HTTPS ポート | Web ブラウザと管理 API クライアントは、 Grid Manager 、 Grid 管理 API 、 Tenant Manager 、およびテナント管理 API にアクセスできます。<br>• 注： * ポート 443 は一部の内部トラフィックにも使用されます。 |
| 8443 | 管理ノード上の制限された Grid Manager ポート | • Web ブラウザと管理 API クライアントは、 HTTPS を使用して Grid Manager とグリッド管理 API にアクセスできます。<br>• Web ブラウザと管理 API クライアントは、 Tenant Manager またはテナント管理 API にはアクセスできません。<br>• 内部コンテンツに対する要求は拒否されます。 |
| ポート 1 | 管理ノード上の制限された Tenant Manager ポート | • Web ブラウザと管理 API クライアントは HTTPS を使用して Tenant Manager とテナント管理 API にアクセスできます。<br>• Web ブラウザと管理 API クライアントは、 Grid Manager またはグリッド管理 API にはアクセスできません。<br>• 内部コンテンツに対する要求は拒否されます。 |

シングルサインオン（ SSO ）は、制限された Grid Manager ポートまたは Tenant Manager ポートでは使用できません。ユーザをシングルサインオンで認証する場合は、デフォルトの HTTPS ポート（ 443 ）を使用する必要があります。

関連情報

"Grid Managerにサインインします"

"StorageGRID がSSOを使用していない場合のテナントアカウントの作成"

"Summary ：クライアント接続の IP アドレスとポート"

"信頼されていないクライアントネットワークの管理"

"Ubuntu または Debian をインストールします"

"VMware をインストールする"

"Red Hat Enterprise Linux または CentOS をインストールします"

アイデンティティフェデレーションを使用する

アイデンティティフェデレーションを使用すると、グループやユーザを迅速に設定できます。また、ユーザは使い慣れたクレデンシャルを使用して StorageGRID にサインイン

できます。

アイデンティティフェデレーションの設定

管理者グループとユーザをActive Directory、OpenLDAP、Oracle Directory Serverなどの別のシステムで管理する場合は、アイデンティティフェデレーションを設定できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- シングルサインオン（SSO）を有効にする場合は、Active Directoryをフェデレーテッドアイデンティティソースとして使用し、AD FSをアイデンティティプロバイダとして使用する必要があります。「シングルサインオンの使用要件」を参照してください。
- アイデンティティプロバイダとしてActive Directory、OpenLDAP、またはOracle Directory Serverを使用している必要があります。

> 記載されていないLDAP v3サービスを使用する場合は、テクニカルサポートにお問い合わせください。

- LDAP サーバとの通信に Transport Layer Security （ TLS ）を使用する場合は、アイデンティティプロバイダが TLS 1.2 または 1.3 を使用している必要があります。

このタスクについて

次の種類のフェデレーテッドグループをインポートする場合は、Grid Managerのアイデンティティソースを設定する必要があります。

- 管理者グループ。管理者グループ内のユーザは、グループに割り当てられた管理権限に基づいて、 Grid Manager にサインインしてタスクを実行できます。
- 独自のアイデンティティソースを使用しないテナントのテナントユーザグループ。テナントグループ内のユーザは、 Tenant Manager でグループに割り当てられた権限に基づいてタスクを実行し、 Tenant Manager にサインインしてタスクを実行できます。

手順

1. [設定（Configuration ）**]>[***アクセス制御（* Access Control ）**]>[***アイデンティティフェデレーション
2. ［ * アイデンティティフェデレーションを有効にする * ］ を選択

   LDAPサーバを設定するためのフィールドが表示されます。

3. LDAP サービスタイプセクションで、設定する LDAP サービスのタイプを選択します。

   Active Directory 、 OpenLDAP 、または Other *を選択できます。

   > OpenLDAP *を選択した場合は、OpenLDAPサーバを設定する必要があります。OpenLDAPサーバの設定に関するガイドラインを参照してください。

   > Oracle Directory Server を使用する LDAP サーバーの値を設定するには、 * その他 * を選択します。

4. [* その他 *] を選択した場合は、 [LDAP 属性 ] セクションのフィールドに入力します。
   - * User Unique Name * ： LDAP ユーザの一意な ID が含まれている属性の名前。この属性はと同じです `sAMAccountName` Active Directoryおよびの場合 `uid` OpenLDAPの場合。Oracle Directory Server を設定する場合は、と入力します `uid`。
   - * User UUID * ： LDAP ユーザの永続的な一意な ID が含まれている属性の名前。この属性はと同じです `objectGUID` Active Directoryおよびの場合 `entryUUID` OpenLDAPの場合。Oracle Directory Serverを設定する場合は、と入力します `nsuniqueid`。指定した属性の各ユーザの値は、 16 バイトまたは文字列形式の 32 桁の 16 進数である必要があります。ハイフンは無視されます。
   - * Group Unique name *：LDAPグループの一意なIDが含まれている属性の名前。この属性はと同じです `sAMAccountName` Active Directoryおよびの場合 `cn` OpenLDAPの場合。Oracle Directory Serverを設定する場合は、と入力します `cn`。
   - * グループ UUID * ： LDAP グループの永続的な一意な ID が含まれている属性の名前。この属性はと同じです `objectGUID` Active Directoryおよびの場合 `entryUUID` OpenLDAPの場合。Oracle Directory Serverを設定する場合は、と入力します `nsuniqueid`。指定した属性の各グループの値は、16 バイトまたは文字列形式の 32 桁の 16 進数である必要があります。ハイフンは無視されます。
5. Configure LDAP server（LDAPサーバの設定）セクションで、必要なLDAPサーバおよびネットワーク接続情報を入力します。
   - * Hostname *：LDAPサーバのホスト名またはIPアドレス。
   - * Port * ： LDAP サーバへの接続に使用するポート。

     STARTTLS のデフォルトポートは 389 、 LDAPS のデフォルトポートは 636 です。ただし、ファイアウォールが正しく設定されていれば、任意のポートを使用できます。
   - * Username * ： LDAP サーバに接続するユーザの識別名（ DN ）の完全パス。

     Active Directory の場合は、ダウンレベルログオン名またはユーザープリンシパル名を指定することもできます。

     指定するユーザには、グループおよびユーザを表示する権限、および次の属性にアクセスする権限が必要です。

     - `sAMAccountName` または `uid`
     - `objectGUID`、 `entryUUID`` または `nsuniqueid`
     - `cn`
     - `memberOf` または `isMemberOf`
   - * Password * ：ユーザ名に関連付けられたパスワード。
   - * Group base DN *：グループを検索するLDAPサブツリーの識別名（DN）の完全パス。Active Directory では、ベース DN に対して相対的な識別名（ DC=storagegrid 、 DC=example 、 DC=com など）のグループをすべてフェデレーテッドグループとして使用できます。

     *グループの一意な名前*値は、所属する*グループのベースDN *内で一意である必要があります。
   - * User base DN*：ユーザを検索するLDAPサブツリーの識別名（DN）の完全パス。

*ユーザーの一意な名前*値は、それぞれが属する*ユーザーベースDN *内で一意である必要があります。

6. [* Transport Layer Security（TLS）*]セクションで、セキュリティ設定を選択します。
   - * STARTTLSを使用（推奨）*：STARTTLSを使用してLDAPサーバとの通信を保護します。これが推奨されるオプションです。
   - * LDAPS を使用 * ： LDAPS （ LDAP over SSL ）オプションでは、 TLS を使用して LDAP サーバへの接続を確立します。このオプションは互換性を確保するためにサポートされています。
   - * TLS を使用しないでください * ： StorageGRID システムと LDAP サーバの間のネットワークトラフィックは保護されません。

   Active Directory サーバで LDAP 署名が適用される場合、 [TLS を使用しない ] オプションの使用はサポートされていません。STARTTLS または LDAPS を使用する必要があります。

7. STARTTLS または LDAPS を選択した場合は、接続の保護に使用する証明書を選択します。
   - オペレーティング・システムの**CA**証明書を使用：オペレーティング・システムにインストールされているデフォルトのCA証明書を使用して接続を保護します。
   - * カスタム CA 証明書を使用 * ：カスタムセキュリティ証明書を使用します。

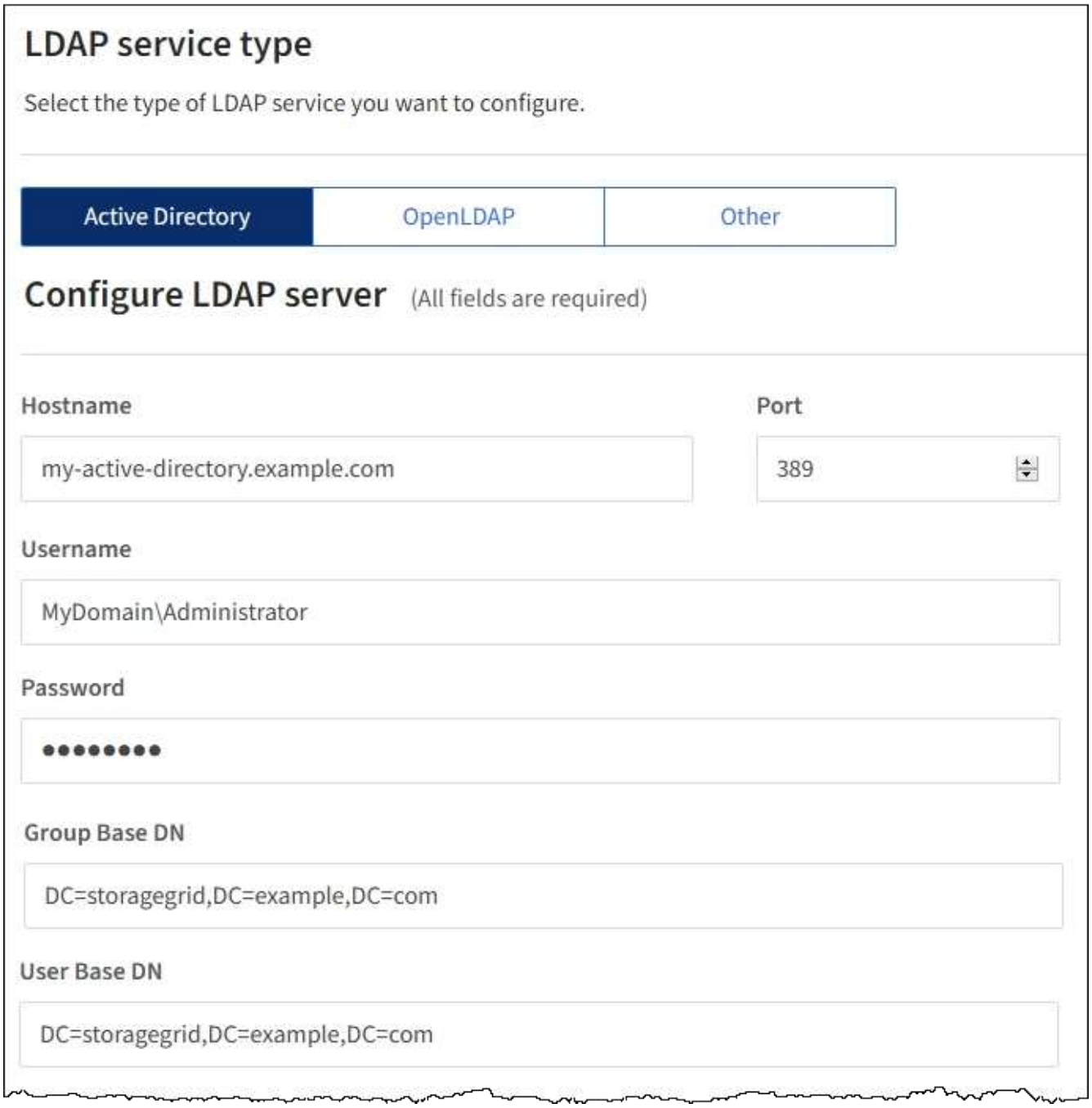
     この設定を選択した場合は、カスタムセキュリティ証明書をコピーして CA 証明書テキストボックスに貼り付けます。

8. 必要に応じて、*接続のテスト*を選択して、LDAPサーバーの接続設定を検証します。

   接続が有効な場合は、ページの右上に確認メッセージが表示されます。

9. 接続が有効な場合は、*保存*を選択します。

   次のスクリーンショットは、Active Directoryを使用するLDAPサーバの設定例を示しています。




関連情報

"発信 TLS 接続でサポートされる暗号"

"シングルサインオンの使用要件"

"テナントアカウントを作成します"

"テナントアカウントを使用する"

**OpenLDAP** サーバの設定に関するガイドライン

アイデンティティフェデレーションに OpenLDAP サーバを使用する場合は、 OpenLDAP サーバで特定の設定が必要です。

**memberof** オーバーレイと **refint** オーバーレイ

memberof オーバーレイと refint オーバーレイを有効にする必要があります。詳細については、OpenLDAPの管理者ガイドのリバースグループメンバーシップのメンテナンス手順を参照してください。

インデックス作成

次の OpenLDAP 属性とインデックスキーワードを設定する必要があります。

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

また、パフォーマンスを最適化するには、 Username のヘルプで説明されているフィールドにインデックスを設定してください。

OpenLDAPの管理者ガイドのリバースグループメンバーシップのメンテナンスに関する情報を参照してください。

関連情報

"OpenLDAP のドキュメント：バージョン 2.4 管理者ガイド"

アイデンティティソースとの強制同期

StorageGRID システムは、アイデンティティソースからフェデレーテッドグループおよびユーザを定期的に同期します。ユーザの権限をすぐに有効にしたり制限したりする必要がある場合は、同期を強制的に開始できます。

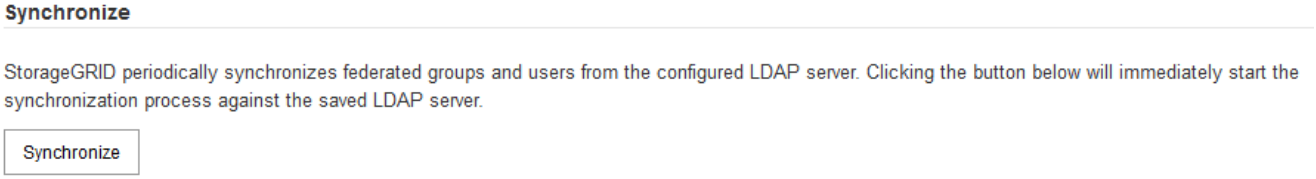
必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- アイデンティティソースが有効になっている必要があります。

手順

1. [設定（Configuration ）**]>[***アクセス制御（* Access Control ）**]>[***アイデンティティフェデレーション

   アイデンティティフェデレーションページが表示されます。「* Synchronize *」ボタンは、ページの下部にあります。

2. [同期化（Synchronize）]をクリックします

   同期が開始されたことを示す確認メッセージが表示されます。環境によっては、同期プロセスにしばらく

時間がかかることがあります。

> アイデンティティフェデレーション同期エラー * アラートは、アイデンティティソースからフェデレーテッドグループとユーザを同期する問題 がある場合にトリガーされます。

### アイデンティティフェデレーションの無効化

グループとユーザのアイデンティティフェデレーションを一時的または永続的に無効にすることができます。アイデンティティフェデレーションを無効にすると、 StorageGRID とアイデンティティソース間のやり取りは発生しません。ただし、設定は保持されるため、簡単に再度有効にすることができます。

#### 必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

#### このタスクについて

アイデンティティフェデレーションを無効にする前に、次の点に注意してください。

- フェデレーテッドユーザはサインインできなくなります。
- 現在サインインしているフェデレーテッドユーザは、セッションが有効な間は StorageGRID システムに引き続きアクセスできますが、セッションが期限切れになると以降はサインインできなくなります。
- StorageGRID システムとアイデンティティソース間の同期は行われず、同期されていないアカウントに対してはアラートやアラームが生成されません。
- シングルサインオン（SSO）が*有効*または*サンドボックスモード*に設定されている場合、*アイデンティティフェデレーションを有効にする*チェックボックスは無効になります。アイデンティティフェデレーションを無効にするには、シングルサインオンページの SSO ステータスが * 無効 * になっている必要があります。

#### 手順

1. [設定（Configuration ）]>[*アクセス制御（* Access Control ）]>[*アイデンティティフェデレーション
2. [アイデンティティフェデレーションを有効にする*]チェックボックスをオフにします。
3. [ 保存（ Save ） ] をクリックします。

#### 関連情報

"シングルサインオンを無効にしています"

## 管理者グループの管理

管理者グループを作成して、 1 人以上の管理者ユーザのセキュリティ権限を管理できます。StorageGRID システムへのアクセスを許可するには、ユーザがグループに属している必要があります。

### 管理者グループの作成

管理者グループを使用すると、 Grid Manager およびグリッド管理 API のどのユーザがどの機能や処理にアクセスできるかを決定できます。

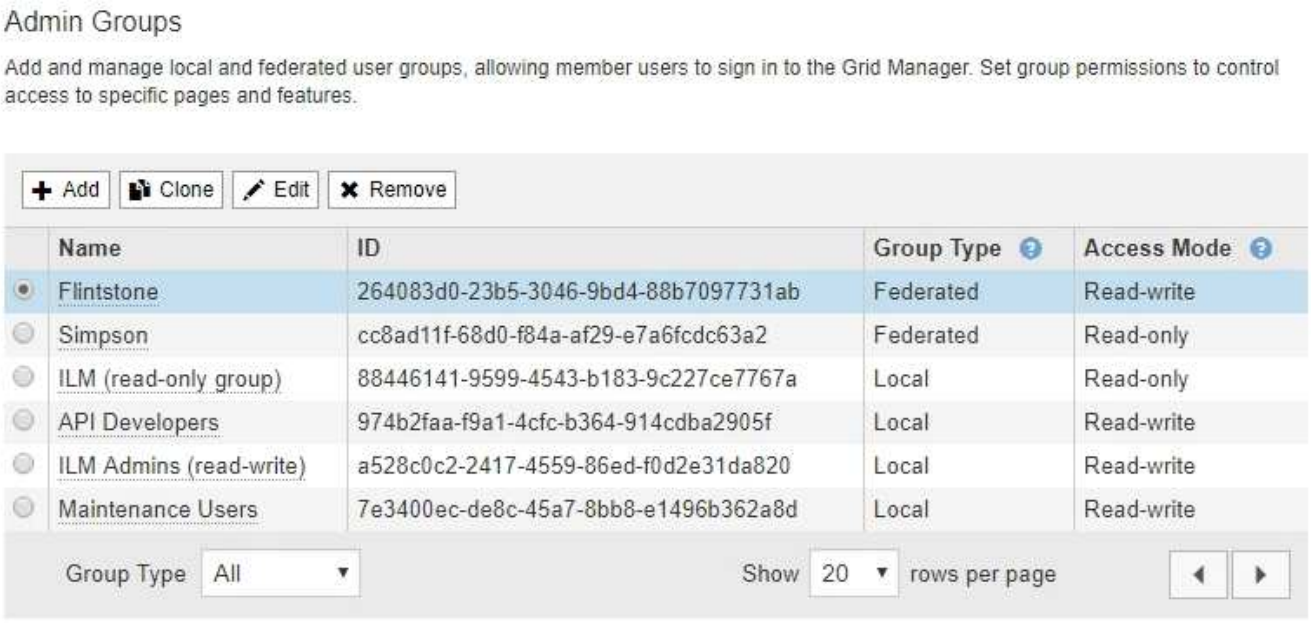
必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- フェデレーテッドグループをインポートする場合は、アイデンティティフェデレーションを設定済みで、インポートするフェデレーテッドグループが設定済みのアイデンティティソースにあらかじめ存在している必要があります。

手順

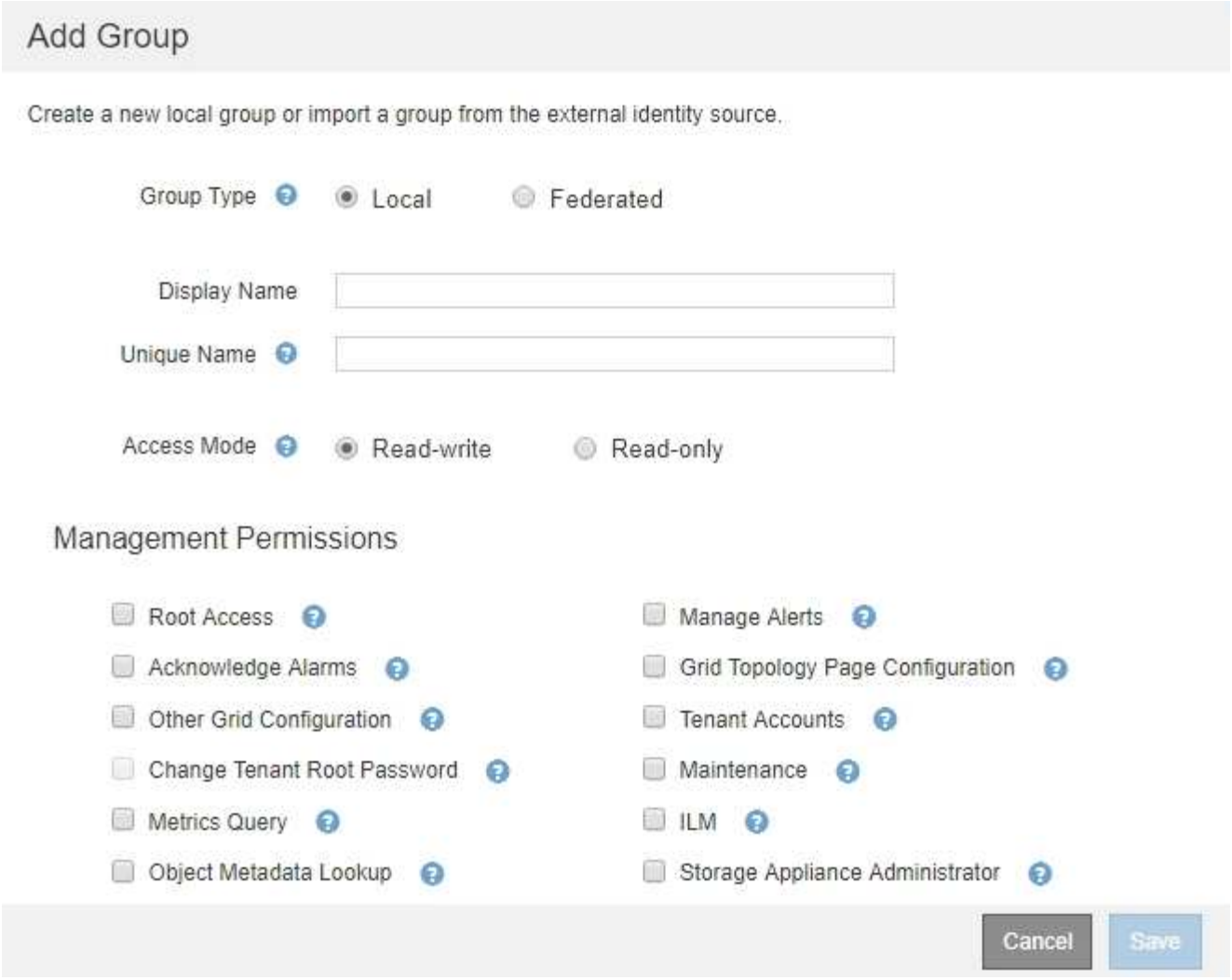
1. [構成アクセス制御管理者グループ*]を選択します。

   Admin Groupsページが表示され、既存の管理者グループが一覧表示されます。




2. 「 * 追加」を選択します。

   [Add Group]ダイアログボックスが表示されます。




3. [グループタイプ]で、StorageGRID 内でのみ使用されるグループを作成する場合は[ローカル*]を、アイデンティティソースからグループをインポートする場合は[フェデレーション*]を選択します。
4. 「ローカル」を選択した場合は、グループの表示名を入力します。表示名は、Grid Managerに表示される名前です。たとえば、「 Maintenance Users 」または「 ILM Administrators 」のようになります。
5. グループの一意の名前を入力します。
   - ローカル：任意の一意の名前を入力します。たとえば'ILM Administrators.`と入力します
   - * Federated *：設定されているアイデンティティソースに表示されるとおりにグループの名前を入力します。
6. *アクセスモード*では、グループ内のユーザがGrid ManagerおよびGrid管理APIで設定の変更や操作を実行できるかどうか、あるいは設定や機能のみを表示できるかどうかを選択します。
   - * 読み取り / 書き込み *（デフォルト）：ユーザは設定を変更し、管理権限で許可されている操作を実行できます。
   - * 読み取り専用 * ：ユーザーは設定と機能のみを表示できます。Grid Manager API や Grid 管理 API で変更や処理を行うことはできません。ローカルの読み取り専用ユーザは自分のパスワードを変更できます。

ユーザーが複数のグループに属していて、いずれかのグループが * 読み取り専用 * に設定されている場合、ユーザーは選択したすべての設定と機能に読み取り専用でアクセスできます。

7. 管理権限を1つ以上選択します。

   各グループに 1 つ以上の権限を割り当てる必要があります。そうしないと、グループに属するユーザは StorageGRID にサインインできません。

8. [ 保存（ Save ） ] を選択します。

   新しいグループが作成されます。ローカルグループの場合は、ユーザを追加できます。フェデレーテッドグループの場合は、どのユーザがグループに属するかはアイデンティティソースが管理します。

関連情報

"ローカルユーザの管理"

管理者グループの権限

管理者ユーザグループを作成する場合は、 Grid Manager の特定の機能へのアクセスを制御する権限を 1 つ以上選択します。その後、作成した 1 つ以上の管理者グループに各ユーザを割り当てて、ユーザが実行できるタスクを決定できます。

各グループに1つ以上の権限を割り当てる必要があります。そうしないと、そのグループに属するユーザはGrid Managerにサインインできません。

デフォルトでは、少なくとも 1 つの権限が割り当てられたグループに属するユーザは次のタスクを実行できます。

- Grid Manager にサインインします
- ダッシュボードを表示します
- ノードページを表示します
- グリッドトポロジを監視する
- 現在のアラートと解決済みのアラートを表示します
- 現在のアラームと履歴アラームの表示（従来のシステム）
- 自分のパスワードを変更する（ローカルユーザのみ）
- Configuration ページと Maintenance ページで特定の情報を表示します

以降のセクションでは、管理者グループの作成時または編集時に割り当てることができる権限について説明します。明示的に言及されていない機能には、Root Access権限が必要です。

ルートアクセス（ **Root Access** ）

この権限は、すべてのグリッド管理機能へのアクセスを許可します。

アラートの管理

この権限では、アラートを管理するためのオプションにアクセスできます。サイレンス、アラート通知、アラートルールを管理するには、この権限が必要です。

アラームの確認（レガシーシステム）

アラームの確認と応答を許可します（従来型システム）。サインインしたすべてのユーザが現在のアラームと履歴アラームを表示できます。

ユーザにグリッドトポロジの監視とアラームへの確認応答だけを許可するには、この権限を割り当てる必要があります。

**Grid**トポロジページの設定

この権限では、次のメニューオプションにアクセスできます。

- サポート*ツール*グリッドトポロジ*の各ページにある構成タブを参照してください。
- イベントカウントのリセット[ノード*イベント*]タブのリンク。

その他の**Grid**設定

この権限で、追加のグリッド設定オプションにアクセスできます。

> これらの追加オプションを表示するには、ユーザにGrid Topology Page Configuration権限が付与されている必要もあります。

- アラーム（レガシー・システム）：
  - グローバルアラーム
  - 従来のEメール設定
- * ILM * ：
  - ストレージプール
  - ストレージグレード
- 構成*ネットワーク設定
  - リンクコスト
- 環境設定*システム設定：
  - 表示オプション（Display Options）
  - グリッドオプション（Grid Options）
  - ストレージオプション
- コンフィグレーション*モニタリング：
  - イベント
- サポート：
  - AutoSupport

テナントアカウント

この権限は、* tenants * Tenant Accounts *ページへのアクセスを許可します。

> Grid管理APIのバージョン1（すでに廃止）では、この権限を使用してテナントグループのポリシーの管理、Swift管理者パスワードのリセット、およびrootユーザのS3アクセスキーの管理を行います。

テナントの**root**パスワードを変更

この権限は、テナントアカウントページの* rootパスワードの変更*オプションにアクセスして、テナントのローカルrootユーザのパスワードを変更できるユーザを制御することを可能にします。この権限を持たないユーザには、*Change Root Password *オプションは表示されません。

> この権限を割り当てるには、Tenant Accounts権限がグループに割り当てられている必要があります。

メンテナンス

この権限では、次のメニューオプションにアクセスできます。

- 環境設定*システム設定：
  - ドメイン名*
  - サーバ証明書*
- コンフィグレーション*モニタリング：
  - 監査*
- 設定*アクセス制御：
  - Gridのパスワード
- メンテナンス*メンテナンスタスク
  - 運用停止
  - 拡張
  - リカバリ
- メンテナンス*ネットワーク*：
  - DNSサーバ*
  - Gridネットワーク*
  - NTPサーバ*
- メンテナンス*システム*：
  - ライセンス*
  - リカバリパッケージ
  - ソフトウェア・アップデート
- サポート*ツール*：

- ログ

- Maintenance権限がないユーザは、アスタリスクの付いたページを表示できますが、編集することはできません。

指標クエリ

この権限は、[*Support*Tools*Metrics *]ページへのアクセスを提供します。また、グリッド管理 API の「指標」セクションを使用して、カスタムの Prometheus 指標クエリにアクセスすることもできます。

**ILM**

この権限は、次の * ILM * メニュー・オプションへのアクセスを提供します。

- イレイジャーコーディング
- ルール
- * ポリシー *
- リージョン

> 「* ILM ストレージ・プール」および「ILM ストレージ・グレード」メニュー・オプションへのアクセスは、「その他のGrid設定」および「Gridトポロジ・ページの設定」権限によって制御されます。

オブジェクトメタデータの検索

この権限は、* ILM * Object Metadata Lookup *メニューオプションへのアクセスを提供します。

ストレージアプライアンス管理者

この権限は、グリッドマネージャを介してストレージアプライアンスの E シリーズ SANtricity システムマネージャにアクセスすることを許可します。

権限とアクセスモードの相互作用

すべての権限について、グループのアクセスモード設定は、ユーザが設定を変更して処理を実行できるかどうか、またはユーザが関連する設定と機能のみを表示できるかどうかを決定します。ユーザーが複数のグループに属していて、いずれかのグループが * 読み取り専用 * に設定されている場合、ユーザーは選択したすべての設定と機能に読み取り専用でアクセスできます。

グリッド管理**API**からの機能の非アクティブ化

グリッド管理 API を使用すると、 StorageGRID システムの特定の機能を完全に非アクティブ化できます。機能を非アクティブ化すると、その機能に関連するタスクを実行する権限をユーザに割り当てることができなくなります。

このタスクについて

非活動化されたフィーチャーシステムを使用すると、 StorageGRID システムの特定のフィーチャーへのアクセスを禁止できます。機能の非アクティブ化は、rootユーザまたはRoot Access権限を持つ管理者グループに属しているユーザがその機能を使用できないようにする唯一の方法です。

この機能がどのように役立つかを理解するために、次のシナリオを検討してください。

_Company A は、テナントアカウントを作成して StorageGRID システムのストレージ容量をリースするサービスプロバイダです。容量をリースしている顧客のオブジェクトのセキュリティを保護するために、 A 社では、アカウントの導入後に自社の従業員がテナントアカウントにアクセスできないようにしたいと考えています。 _

_ 企業 A は、グリッド管理 API で Deactivate Features システムを使用することで、この目的を達成できます。Grid Manager（UIとAPIの両方）で* Change Tenant Root Password *機能を完全に非アクティブにすることで、A社はすべてのテナントアカウントのrootユーザのパスワードを変更できるようになります。_

非アクティブ化した機能の再アクティブ

デフォルトでは、グリッド管理 API を使用して、非アクティブ化した機能を再アクティブ化できます。ただし、非アクティブ化された機能が再アクティブ化されないようにするには、 * activateFeatures * 機能自体を非アクティブ化します。

> * activateFeatures * 機能を再アクティブ化できません。この機能を非アクティブ化すると、非アクティブ化した他の機能を永続的に再アクティブ化できなくなることに注意してください。失われた機能をリストアするには、テクニカルサポートにお問い合わせください。

詳細については、S3またはSwiftクライアントアプリケーションを実装する手順を参照してください。

手順

1. Swagger のグリッド管理 API のドキュメントにアクセスします。
2. Deactivate Features エンドポイントを探します。
3. * Change Tenant Root Password *などの機能を非アクティブ化するには、次のようにAPIに本文を送信します。

   ```
   { "grid": {"changeTenantRootPassword": true} }
   ```

   要求が完了すると、Change Tenant Root Password機能は無効になります。Change Tenant Root Password管理権限はユーザインターフェイスに表示されなくなり、テナントのrootパスワードを変更するAPI要求はすべて「403 Forbidden」エラーで失敗します。

4. すべての機能を再アクティブ化するには、次のような本文を API に送信します。

   ```
   { "grid": null }
   ```

   この要求が完了すると、Change Tenant Root Password機能を含むすべての機能が再アクティブ化されます。ユーザにRoot Access権限またはChange Tenant Root Password管理権限が割り当てられている場合は、Change Tenant Root Password管理権限がユーザインターフェイスに表示され、テナントのrootパスワードを変更するAPI要求はすべて成功します。

前述の例は、 _all_deactivated 機能を再アクティブ化します。非アクティブ化したままにする必要がある他の機能が非アクティブ化されている場合は、 PUT 要求でそれらを明示的に指定する必要があります。たとえば、Change Tenant Root Password機能を再アクティブ化して、Alarm Acknowledgment機能を非アクティブなままにするには、次のPUT要求を送信します。

```
{ "grid": { "alarmAcknowledgment": true } }
```

関連情報

"グリッド管理APIを使用する"

管理者グループの変更

管理者グループを変更して、グループに関連付けられている権限を変更できます。ローカル管理者グループについては、表示名を更新することもできます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

手順

1. [構成アクセス制御管理者グループ*]を選択します。
2. グループを選択します。

   システムに20個を超えるアイテムが含まれている場合は、各ページに一度に表示する行数を指定できます。その後、ブラウザの検索機能を使用して、現在表示されている行の特定の項目を検索できます。

3. [ 編集（ Edit ） ] をクリックします。
4. オプションで'ローカル・グループの場合は'たとえばMaintenance Usersのように'ユーザーに表示されるグループの名前を入力します

   一意の名前は内部グループ名であるため、変更できません。

5. 必要に応じて、グループのアクセスモードを変更します。
   - * 読み取り / 書き込み * （デフォルト）：ユーザは設定を変更し、管理権限で許可されている操作を実行できます。
   - * 読み取り専用 * ：ユーザーは設定と機能のみを表示できます。Grid Manager API や Grid 管理 API で変更や処理を行うことはできません。ローカルの読み取り専用ユーザは自分のパスワードを変更できます。

   ユーザーが複数のグループに属していて、いずれかのグループが * 読み取り専用 * に設定されている場合、ユーザーは選択したすべての設定と機能に読み取り専用でアクセスできます。

6. 必要に応じて、グループ権限を追加または削除します。

管理者グループの権限に関する情報を参照してください。

7. [ 保存（ Save ） ] を選択します。

関連情報

[管理者グループの権限]

管理者グループを削除しています

管理者グループを削除すると、システムからそのグループを削除し、グループに関連付けられているすべての権限を削除できます。管理者グループを削除すると、そのグループからすべての管理者ユーザが削除されますが、管理者ユーザは削除されません。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

グループを削除すると、そのグループに割り当てられているユーザは、別のグループから権限が付与されていないかぎり、Grid Managerへのすべてのアクセス権限を失います。

手順

1. [構成アクセス制御管理者グループ*]を選択します。
2. グループの名前を選択します。

   システムに20個を超えるアイテムが含まれている場合は、各ページに一度に表示する行数を指定できます。その後、ブラウザの検索機能を使用して、現在表示されている行の特定の項目を検索できます。

3. 「 * 削除」を選択します。
4. 「 * OK 」を選択します。

ローカルユーザの管理

## ローカルユーザを作成してローカル管理者グループに割り当て、そのユーザがアクセスできるGrid Manager機能を決定することができます。

Grid Managerには'ルートという名前の'事前定義されたローカル・ユーザが1つ含まれていますローカルユーザは追加および削除できますが、rootユーザを削除することはできません。

シングルサインオン（SSO）が有効になっている場合、ローカルユーザはStorageGRID にサインインできません。

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

ローカルユーザを作成しています

ローカル管理者グループを作成した場合は、1人以上のローカルユーザを作成し、各ユーザを1つ以上のグル

ープに割り当てることができます。このグループの権限は、ユーザがアクセスできるGrid Manager機能を制御します。

このタスクについて

作成できるのはローカルユーザだけで、作成したユーザはローカル管理者グループにのみ割り当てることができます。フェデレーテッドユーザとフェデレーテッドグループは、外部のアイデンティティソースを使用して管理されます。

手順

1. [構成（Configuration ）]>[*アクセス制御（* Access Control ）]>[*管理者ユーザー（* Admin Users *）
2. [ 作成（ Create ） ] をクリックします。
3. ユーザの表示名、一意の名前、およびパスワードを入力します。
4. アクセス権限を制御する1つ以上のグループにユーザを割り当てます。

   グループ名のリストは'グループ(Groups)テーブルから生成されます

5. [ 保存（ Save ） ] をクリックします。

関連情報

"管理者グループの管理"

ローカルユーザアカウントの変更

ローカル管理者ユーザのアカウントを変更して、ユーザの表示名またはグループメンバーシップを更新できます。ユーザが一時的にシステムにアクセスできないように設定することもできます。

このタスクについて

編集できるのはローカルユーザのみです。フェデレーテッドユーザの詳細は、外部のアイデンティティソースと自動的に同期されます。

手順

1. [構成（Configuration ）]>[*アクセス制御（* Access Control ）]>[*管理者ユーザー（* Admin Users *）
2. 編集するユーザを選択します。

   システムに20個を超えるアイテムが含まれている場合は、各ページに一度に表示する行数を指定できます。その後、ブラウザの検索機能を使用して、現在表示されている行の特定の項目を検索できます。

3. [ 編集（ Edit ） ] をクリックします。
4. 必要に応じて、名前またはグループメンバーシップを変更します。
5. 必要に応じて、ユーザが一時的にシステムにアクセスできないようにするには、*アクセス拒否*をオンにします。
6. [ 保存（ Save ） ] をクリックします。

   新しい設定は、次回ユーザがグリッドマネージャからサインアウトして再度サインインしたときに適用されます。

ローカルユーザのアカウントを削除する

Grid Managerへのアクセスが不要になったローカルユーザのアカウントを削除できます。

手順

1. [構成（Configuration ）]>[*アクセス制御（* Access Control ）]>[*管理者ユーザー（* Admin Users *）
2. 削除するローカルユーザを選択します。

   事前定義されたrootローカルユーザは削除できません。

   システムに20個を超えるアイテムが含まれている場合は、各ページに一度に表示する行数を指定できます。その後、ブラウザの検索機能を使用して、現在表示されている行の特定の項目を検索できます。

3. [ 削除（ Remove ） ] をクリックします。
4. [OK] をクリックします。

ローカルユーザのパスワードを変更する

ローカルユーザは、 Grid Manager のバナーで * Change Password * オプションを使用して自分のパスワードを変更できます。また、Admin Usersページへのアクセス権を持つユーザは、他のローカルユーザのパスワードを変更できます。

このタスクについて

変更できるのはローカルユーザのパスワードのみです。フェデレーテッドユーザは、自分のパスワードを外部のアイデンティティソース内で変更する必要があります。

手順

1. [構成（Configuration ）]>[*アクセス制御（* Access Control ）]>[*管理者ユーザー（* Admin Users *）
2. [ユーザー]ページで、ユーザーを選択します。

   システムに20個を超えるアイテムが含まれている場合は、各ページに一度に表示する行数を指定できます。その後、ブラウザの検索機能を使用して、現在表示されている行の特定の項目を検索できます。

3. [パスワードの変更*]をクリックします。
4. パスワードを入力して確認し、*保存*をクリックします。

**StorageGRID** にシングルサインオン（**SSO**）を使用する

StorageGRID システムでは、 Security Assertion Markup Language 2.0 （ SAML 2.0 ）標準を使用したシングルサインオン（ SSO ）がサポートされます。SSO が有効な場合は、 Grid Manager 、 Tenant Manager 、 Grid 管理 API 、またはテナント管理 API にアクセスするすべてのユーザを外部のアイデンティティプロバイダによって認証する必要があります。ローカルユーザは StorageGRID にサインインできません。

- "シングルサインオンの仕組み"
- "シングルサインオンの使用要件"
- "シングルサインオンを設定しています"

# シングルサインオン（ SSO ）を有効にする前に、 SSO が有効になった場合に StorageGRID のサインインとサインアウトのプロセスにどのような影響があるかを確認してください。

## SSOが有効な場合はサインインします

SSO が有効な場合に StorageGRID にサインインすると、組織の SSO ページにリダイレクトされてクレデンシャルが検証されます。

手順

1. Web ブラウザで、 StorageGRID 管理ノードの完全修飾ドメイン名または IP アドレスを入力します。

   StorageGRID のサインインページが表示されます。

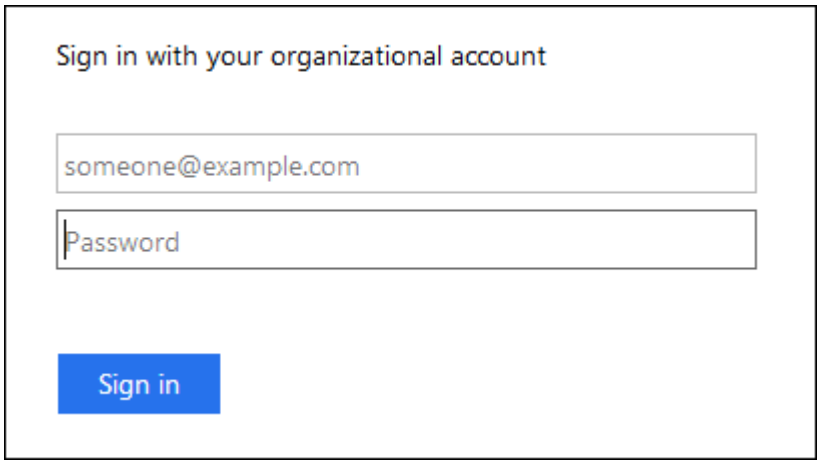
   - このブラウザで初めて URL にアクセスした場合は、アカウント ID の入力を求められます。

   - Grid Manager または Tenant Manager に以前にアクセスしていた場合は、最近のアカウントを選択するか、アカウント ID を入力するように求められます。

テナントアカウントの完全なURL（完全修飾ドメイン名またはIPアドレスのあとにを追加したもの）を入力すると、StorageGRID のサインインページは表示されません `/?accountId=20-digit-account-id`）。代わりに、組織の SSO サインインページがすぐに表示されます。このページでは、を実行できます SSO クレデンシャルを使用してサインインします。

2. Grid Manager と Tenant Manager のどちらにアクセスするかを指定します。
   - Grid Managerにアクセスするには、[ **Account ID**（アカウントID *）]フィールドを空白のままにします。アカウント**ID**として「 0 」を入力するか、最近のアカウントのリストに「 Grid Manager *」が表示されている場合はそれを選択します。
   - Tenant Manager にアクセスするには、 20 桁のテナントアカウント ID を入力するか、最近のアカウントのリストにテナントが表示されている場合は名前でテナントを選択します。
3. [サインイン]をクリックします

   StorageGRID は、組織の SSO サインインページにリダイレクトします。例：




4. [[signin_soS] SSO クレデンシャルを使用してサインインします。

   SSO クレデンシャルが正しい場合：

   a. アイデンティティプロバイダ（ IdP ）が StorageGRID に認証応答を返します。
   b. StorageGRID が認証応答を検証します。
   c. 応答が有効で、ユーザが適切なアクセス権限のあるフェデレーテッドグループに属している場合は、選択したアカウントに応じてGrid Managerまたはテナントマネージャにサインインされます。
5. 必要に応じて、他の管理ノードにアクセスします。または、適切な権限がある場合は Grid Manager またはテナントマネージャにアクセスします。

   SSO クレデンシャルを再入力する必要はありません。

**SSO**が有効な場合はサインアウトします

StorageGRID で SSO が有効になっている場合にサインアウトするとどうなるかは、サインイン先とサインアウト元によって異なります。

手順

1. ユーザインターフェイスの右上隅にある [**Sign Out**] リンクを探します。
2. [サインアウト]をクリックします。

   StorageGRID のサインインページが表示されます。[Recent Accounts] * ドロップダウンが更新されて、 * Grid Manager * またはテナント名が表示されるようになり、これらのユーザインターフェイスにあとからすばやくアクセスできるようになります。

| サインイン先 | サインアウト元 | サインアウトされる対象 |
| --- | --- | --- |
| 1 つ以上の管理ノードでグリッドマネージャを使用します | 任意の管理ノード上の Grid Manager | すべての管理ノード上の Grid Manager |
| 1 つ以上の管理ノード上の Tenant Manager | 任意の管理ノード上の Tenant Manager | すべての管理ノード上の Tenant Manager |
| Grid Manager と Tenant Manager の両方 | Grid Manager の略 | Grid Manager のみ。SSO からサインアウトするには、 Tenant Manager からもサインアウトする必要があります。 |

次の表は、単一のブラウザセッションを使用している場合にサインアウトしたときの動作をまとめたものです。複数のブラウザセッションで StorageGRID にサインインしている場合は、すべてのブラウザセッションから個別にサインアウトする必要があります。

シングルサインオンの使用要件

## StorageGRID システムでシングルサインオン（ SSO ）を有効にする前に、このセクションの要件を確認してください。

シングルサインオン（ SSO ）は、制限された Grid Manager ポートまたは Tenant Manager ポートでは使用できません。ユーザをシングルサインオンで認証する場合は、デフォルトの HTTPS ポート（ 443 ）を使用する必要があります。

アイデンティティプロバイダの要件

SSOのアイデンティティプロバイダ（IdP）は、次の要件を満たしている必要があります。

- 次のいずれかのバージョンのActive Directoryフェデレーションサービス（AD FS）
  - AD FS 4.0はWindows Server 2016に付属しています

    Windows Server 2016 でが使用されている必要があります "KB3201845 の更新プログラム"またはそれ以上。

  - AD FS 3.0 （ Windows Server 2012 R2 Update 以降に付属）。
- Transport Layer Security （ TLS ） 1.2 または 1.3
- Microsoft .NET Framework バージョン 3.5.1 以降

サーバ証明書の要件

StorageGRID は、各管理ノード上の管理インターフェイスのサーバ証明書を使用して、Grid Manager、テナントマネージャ、グリッド管理API、およびテナント管理APIへのアクセスを保護します。AD FS でStorageGRID 用にSSOの証明書利用者信頼を設定する際には、このサーバ証明書をAD FSへのStorageGRID 要求の署名証明書として使用します。

管理インターフェイス用のカスタムサーバ証明書をまだインストールしていない場合は、インストールしてください。インストールしたカスタムサーバ証明書はすべての管理ノードで使用され、すべてのStorageGRID 証明書利用者信頼で使用できます。

> 管理ノードのデフォルトサーバ証明書をAD FSの証明書利用者信頼に使用することは推奨されません。ノードに障害が発生した場合にそのノードをリカバリすると、新しいデフォルトサーバ証明書が生成されます。リカバリしたノードにサインインするには、AD FSの証明書利用者信頼を新しい証明書で更新する必要があります。

管理ノードのサーバ証明書にアクセスするには、ノードのコマンドシェルにログインしてに移動します `/var/local/mgmt-api` ディレクトリ。カスタムサーバ証明書の名前はです `custom-server.crt`。ノードのデフォルトサーバ証明書の名前はです `server.crt`。

関連情報

"ファイアウォールによるアクセス制御"

"Grid ManagerおよびTenant Manager用のカスタムサーバ証明書を設定する"

シングルサインオンを設定しています

シングルサインオン（ SSO ）が有効な場合、ユーザは、組織によって実装された SSO サインインプロセスを使用してクレデンシャルが許可されている場合にのみ、 Grid Manager 、テナントマネージャ、 Grid 管理 API 、またはテナント管理 API にアクセスできます。

- "フェデレーテッドユーザがサインインできることを確認しておき"
- "サンドボックスモードの使用"
- "AD FSでの証明書利用者信頼の作成"
- "証明書利用者信頼のテスト"
- "シングルサインオンの有効化"
- "シングルサインオンを無効にしています"
- "1つの管理ノードのシングルサインオンの一時的な無効化と再有効化"

フェデレーテッドユーザがサインインできることを確認しておき

シングルサインオン（ SSO ）を有効にする前に、少なくとも 1 人のフェデレーテッドユーザが既存のテナントアカウント用に Grid Manager および Tenant Manager にサインインできることを確認する必要があります。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- Active Directoryをフェデレーテッドアイデンティティソースとして使用し、AD FSをアイデンティティプロバイダとして使用している。

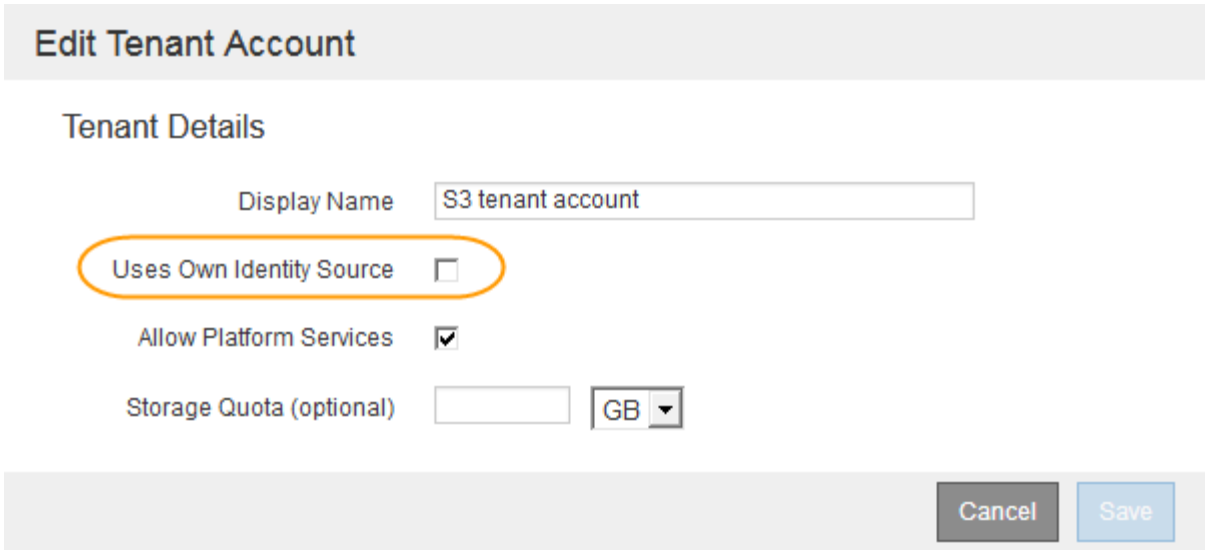
  "シングルサインオンの使用要件"

手順

1. 既存のテナントアカウントがある場合は、テナントが独自のアイデンティティソースを使用していないことを確認します。

   SSO を有効にすると、 Tenant Manager で設定されたアイデンティティソースが Grid Manager で設定されたアイデンティティソースによって上書きされます。テナントのアイデンティティソースに属するユーザは、 Grid Manager アイデンティティソースのアカウントがないかぎり、サインインできなくなります。

   a. 各テナントアカウントの Tenant Manager にサインインします。
   b. アクセス制御*>*アイデンティティフェデレーション*を選択します。
   c. ［アイデンティティフェデレーションを有効にする］チェックボックスがオフになっていることを確認します。
   d. その場合は、このテナントアカウントに使用されている可能性のあるフェデレーテッドグループが不要になっていることを確認し、チェックボックスをオフにして*保存*をクリックします。
2. フェデレーテッドユーザが Grid Manager にアクセスできることを確認します。
   a. Grid Managerから* Configuration > Access Control > Admin Groups *を選択します。
   b. Active Directoryアイデンティティソースから少なくとも1つのフェデレーテッドグループがインポートされていて、そのグループにRoot Access権限が割り当てられていることを確認します。
   c. サインアウトします。
   d. フェデレーテッドグループ内のユーザとして Grid Manager に再度サインインできることを確認します。
3. 既存のテナントアカウントがある場合は、Root Access権限を持つフェデレーテッドユーザがサインインできることを確認します。
   a. Grid Managerから* tenants *を選択します。
   b. テナントアカウントを選択し、*アカウントの編集*をクリックします。
   c. [独自のアイデンティティソースを使用する*]チェックボックスがオンになっている場合は、チェックボックスをオフにして、[保存*]をクリックします。




Tenant Accountsページが表示されます。

a. テナントアカウントを選択し、*サインイン*をクリックして、ローカルのrootユーザとしてテナントアカウントにサインインします。

b. Tenant Managerで、* Access Control > Groups *をクリックします。

c. Grid Managerから少なくとも1つのフェデレーテッドグループにこのテナント用のRoot Access権限が割り当てられていることを確認します。

d. サインアウトします。

e. フェデレーテッドグループ内のユーザとしてテナントに再度サインインできることを確認します。

関連情報

"シングルサインオンの使用要件"

"管理者グループの管理"

"テナントアカウントを使用する"

サンドボックスモードの使用

# サンドボックスモードを使用すると、StorageGRID ユーザにシングルサインオン（SSO）を適用する前に、Active Directoryフェデレーションサービス（AD FS）の証明書利用者信頼を設定およびテストできます。SSOを有効にしたあとにサンドボックスモードを再度有効にすると、新規および既存の証明書利用者信頼を設定またはテストできます。サンドボックスモードを再度有効にすると、StorageGRID ユーザーのSSOは一時的に無効に

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

SSOが有効な場合、ユーザが管理ノードにサインインしようとすると、StorageGRID からAD FSに認証要求が送信されます。次に、AD FSは、認証要求が成功したかどうかを示す認証応答をStorageGRID に返します。要求が成功した場合、応答にはユーザのUniversally Unique Identifier（UUID）が含まれます。

StorageGRID （サービスプロバイダ）とAD FS（アイデンティティプロバイダ）がユーザの認証要求を安全にやり取りできるようにするには、StorageGRID で特定の設定を行う必要があります。次に、AD FSを使用して、管理ノードごとに証明書利用者信頼を作成します。最後に、 StorageGRID に戻って SSO を有効にする必要があります。

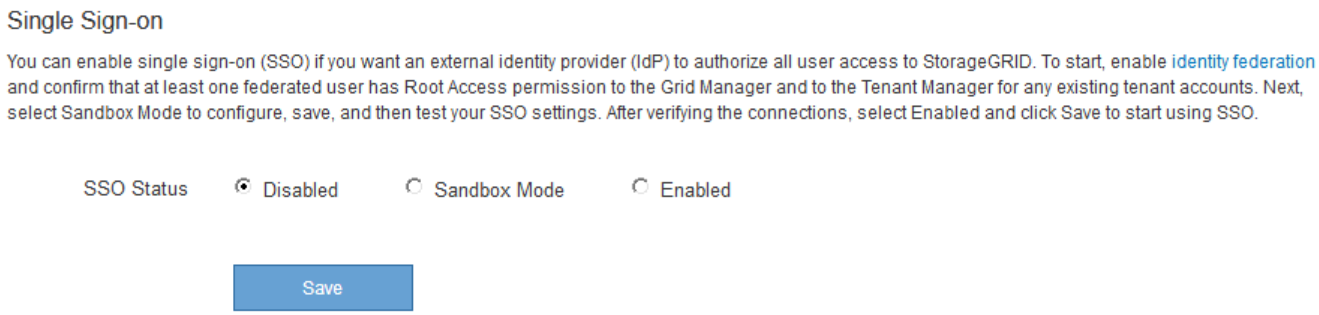
サンドボックスモードでは、 SSO を有効にする前に、この手順を簡単に実行し、すべての設定をテストできます。

サンドボックスモードは使用することを推奨しますが、必須ではありません。StorageGRID でSSOを設定した直後にAD FSの証明書利用者信頼を作成する準備ができている場合は、また、管理ノードごとにSSOプロセスとシングルログアウト（SLO）プロセスをテストする必要はありません。* enabled をクリックし、**StorageGRID** 設定を入力して、**AD FS**内の管理ノードごとに証明書利用者信頼を作成し、 Save *をクリックしてSSOを有効にします。

手順

1. 「* Configuration * Access Control * Single Sign-On *」を選択します。

   [Single Sign-On] ページが表示され、 [**Disabled**] オプションが選択されます。




   SSO Statusオプションが表示されない場合は、Active Directoryがフェデレーテッドアイデンティティソースとして設定されていることを確認します。「シングルサインオンの使用要件」を参照してください。

2. [サンドボックスモード]オプションを選択します。

   アイデンティティプロバイダと証明書利用者の設定が表示されます。［アイデンティティプロバイダ］セクションでは、［サービスタイプ］フィールドは読み取り専用です。ここには、使用しているアイデンティティフェデレーションサービスのタイプ（Active Directoryなど）が表示されます。

3. アイデンティティプロバイダセクションで、次の手順を実行します。

   a. フェデレーションサービス名をAD FSに表示されているとおりに入力します。

      フェデレーションサービス名を確認するには、Windows Server Managerに移動します。[ツール**AD FS管理]を選択します。[ アクション ] メニューから、 [ * フェデレーションサービスのプロパティの編集 * ] を選択します。フェデレーションサービス名が 2 番目のフィールドに表示されます。

b. StorageGRID 要求への応答としてアイデンティティプロバイダがSSO設定情報を送信するときに、Transport Layer Security（TLS）を使用して接続を保護するかどうかを指定します。

   - * オペレーティング・システムの CA 証明書を使用 * ：オペレーティング・システムにインストールされているデフォルトの CA 証明書を使用して、接続を保護します。
   - * カスタム CA 証明書を使用 * ：カスタム CA 証明書を使用して接続を保護します。

     この設定を選択した場合は、証明書を* CA証明書*テキストボックスにコピーして貼り付けます。

   - * Do not use TLS* ： TLS 証明書を使用して接続を保護しないでください。

4. 証明書利用者セクションで、StorageGRID 管理ノードに使用する証明書利用者信頼を設定するときに使用する証明書利用者IDを指定します。

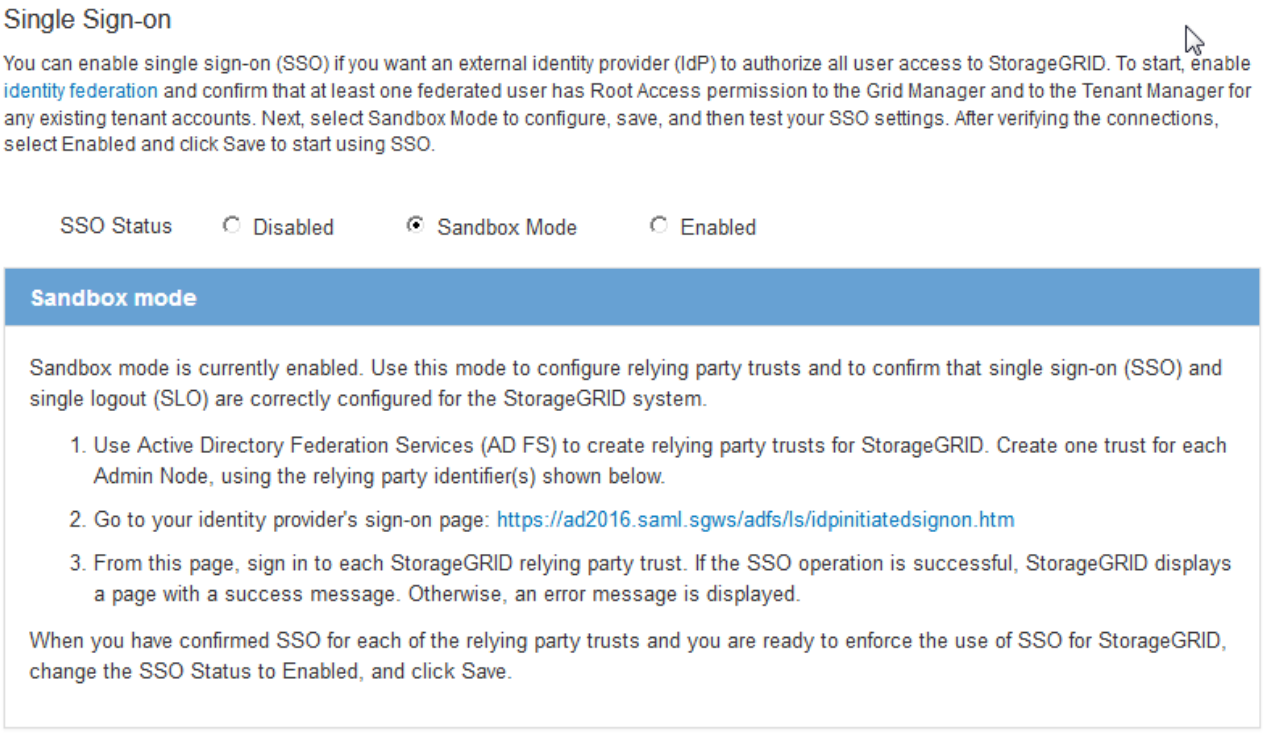
   - たとえば、グリッドに管理ノードが1つしかなく、今後管理ノードを追加する予定がない場合は、と入力します `SG` または `StorageGRID`。
   - グリッドに複数の管理ノードがある場合は、という文字列を含めます `[HOSTNAME]` を入力します。例： `SG-[HOSTNAME]`。これにより、管理ノードのホスト名に基づいて、各管理ノードの証明書利用者IDを含むテーブルが生成されます。+注：証明書利用者信頼はStorageGRID システム内の管理ノードごとに作成する必要があります。管理ノードごとに証明書利用者信頼を作成することで、ユーザは管理ノードに対して安全にサインイン / サインアウトすることができます。

5. [ 保存（ Save ） ] をクリックします。

   - 数秒間、 * Save * （保存）ボタンに緑色のチェックマークが表示されます。

   - サンドボックスモードの確認メッセージが表示され、サンドボックスモードが有効になっていることが確認されます。AD FSの使用時にもこのモードを使用して、管理ノードごとに証明書利用者信頼を設定し、シングルサインイン（SSO）プロセスとシングルログアウト（SLO）プロセスをテストできます。




関連情報

"シングルサインオンの使用要件"

**AD FS**での証明書利用者信頼の作成

Active Directory フェデレーションサービス（ AD FS ）を使用して、システム内の管理ノードごとに証明書利用者信頼を作成する必要があります。PowerShell コマンドを使用するか、 StorageGRID から SAML メタデータをインポートするか、またはデータを手動で入力することによって、証明書利用者信頼を作成できます。

**Windows PowerShell**を使用した証明書利用者信頼の作成

Windows PowerShell を使用して証明書利用者信頼を簡単に作成できます。

必要なもの

- StorageGRID でSSOを設定し、システム内の各管理ノードの完全修飾ドメイン名（またはIPアドレス）と証明書利用者IDを確認しておきます。

> 証明書利用者信頼は StorageGRID システム内の管理ノードごとに作成する必要があります。管理ノードごとに証明書利用者信頼を作成することで、ユーザは管理ノードに対して安全にサインイン / サインアウトすることができます。

- AD FS での証明書利用者信頼の作成経験があるか、または Microsoft AD FS のドキュメントを参照できる必要があります。
- AD FS 管理スナップインを使用していて、 Administrators グループに属している必要があります。

このタスクについて

以下の手順は、Windows Server 2016に付属のAD FS 4.0での手順です。Windows Server 2012 R2に含まれているAD FS 3.0を使用している場合は、手順 にわずかな違いがあります。不明な点がある場合は、Microsoft AD FS のドキュメントを参照してください。

手順

1. WindowsのスタートメニューからPowerShellアイコンを右クリックし、*管理者として実行*を選択します。
2. PowerShell コマンドプロンプトで、次のコマンドを入力します。

   ```
   Add-AdfsRelyingPartyTrust -Name "Admin_Node_Identifer" -MetadataURL
   "https://Admin_Node_FQDN/api/saml-metadata"
   ```

   - の場合 `Admin_Node_Identifier`では、管理ノードの証明書利用者IDをSingle Sign-Onページに表示されるとおりに入力します。例： `SG-DC1-ADM1。
   - の場合 `Admin_Node_FQDN`をクリックし、同じ管理ノードの完全修飾ドメイン名を入力します。（必要に応じて、ノードの IP アドレスを代わりに使用できます。ただし、 IP アドレスを入力した場合、その IP アドレスが変わったときには証明書利用者信頼を更新または再作成する必要があります）。
3. Windows Server Manager で、 * Tools * > * AD FS Management * を選択します。

   AD FS 管理ツールが表示されます。
4. 「 * AD FS * > * 証明書利用者信頼」を選択します。

   証明書利用者信頼のリストが表示されます。
5. 新しく作成した証明書利用者信頼にアクセス制御ポリシーを追加します。
   a. 作成した証明書利用者信頼を検索します。
   b. 信頼を右クリックし、 * アクセス制御ポリシーの編集 * を選択します。
   c. アクセス制御ポリシーを選択します。
   d. [*適用（Apply）]をクリックし、[OK]をクリックします
6. 新しく作成した証明書利用者信頼に要求発行ポリシーを追加します。
   a. 作成した証明書利用者信頼を検索します。
   b. 信頼を右クリックし、 ［ * クレーム発行ポリシーの編集 * ］ を選択します。
   c. [ルールの追加]をクリックします。
   d. ［ルールテンプレートの選択］ページで、リストから［* LDAP属性をクレームとして送信*］を選択し、［次へ］をクリックします。
   e. ［ ルールの設定 ］ ページで、このルールの表示名を入力します。

      たとえば、 **ObjectGUID to Name ID** と入力します。
   f. 属性ストアで、 * Active Directory * を選択します。
   g. マッピングテーブルの LDAP 属性列に、 * objectGUID * と入力します。
   h. マッピングテーブルの発信クレームタイプ列で、ドロップダウンリストから * 名前 ID * を選択します。

i. [完了]をクリックし、[OK]をクリックします。

7. メタデータが正常にインポートされたことを確認します。
   a. 証明書利用者信頼を右クリックしてプロパティを開きます。
   b. [**Endpoints**] 、 [***Identifiers**] 、および [**Signature**] タブのフィールドに値が入力されていることを確認します。

      メタデータがない場合は、フェデレーションメタデータアドレスが正しいことを確認するか、値を手動で入力します。

8. 上記の手順を繰り返して、 StorageGRID システム内のすべての管理ノードに対して証明書利用者信頼を設定します。
9. 完了したら、StorageGRID およびに戻ります "すべての証明書利用者信頼をテストします" 正しく設定されていることを確認します。

フェデレーションメタデータをインポートして証明書利用者信頼を作成する

各証明書利用者信頼の値をインポートするには、各管理ノードの SAML メタデータにアクセスします。

必要なもの

- StorageGRID でSSOを設定し、システム内の各管理ノードの完全修飾ドメイン名（またはIPアドレス）と証明書利用者IDを確認しておきます。

> ⓘ 証明書利用者信頼は StorageGRID システム内の管理ノードごとに作成する必要があります。管理ノードごとに証明書利用者信頼を作成することで、ユーザは管理ノードに対して安全にサインイン / サインアウトすることができます。

- AD FS での証明書利用者信頼の作成経験があるか、または Microsoft AD FS のドキュメントを参照できる必要があります。
- AD FS 管理スナップインを使用していて、 Administrators グループに属している必要があります。

このタスクについて

以下の手順は、Windows Server 2016に付属のAD FS 4.0での手順です。Windows Server 2012 R2に含まれているAD FS 3.0を使用している場合は、手順 にわずかな違いがあります。不明な点がある場合は、 Microsoft AD FS のドキュメントを参照してください。

手順

1. Windows Server Managerで、* Tools をクリックし、 AD FS Management *を選択します。
2. Actions（アクション）で、* Add（証明書利用者信頼の追加）*をクリックします。
3. [ようこそ]ページで、[クレーム対応]を選択し、[開始]をクリックします。
4. [ * オンラインまたはローカルネットワーク上で公開されている証明書利用者に関するデータをインポートする * ] を選択します。
5. * フェデレーションメタデータアドレス（ホスト名または URL ） * に、この管理ノードの SAML メタデータの場所を入力します。

   `https://Admin_Node_FQDN/api/saml-metadata`

の場合 `_Admin_Node_FQDN_`をクリックし、同じ管理ノードの完全修飾ドメイン名を入力します。（必要に応じて、ノードの IP アドレスを代わりに使用できます。ただし、 IP アドレスを入力した場合、その IP アドレスが変わったときには証明書利用者信頼を更新または再作成する必要があります）。

6. 証明書利用者信頼の追加ウィザードを実行し、証明書利用者信頼を保存して、ウィザードを閉じます。

   表示名を入力するときは、管理ノードの証明書利用者 ID を使用します。これは、 Grid Manager のシングルサインオンページに表示される情報とまったく同じです。例： `SG-DC1-ADM1`。

7. クレームルールを追加します。
   a. 信頼を右クリックし、 ［ * クレーム発行ポリシーの編集 * ］ を選択します。
   b. [ルールの追加：]をクリックします。
   c. ［ルールテンプレートの選択］ページで、リストから［* LDAP属性をクレームとして送信*］を選択し、［次へ］をクリックします。
   d. ［ ルールの設定 ］ ページで、このルールの表示名を入力します。

      たとえば、 **ObjectGUID to Name ID** と入力します。

   e. 属性ストアで、 * Active Directory * を選択します。
   f. マッピングテーブルの LDAP 属性列に、 * objectGUID * と入力します。
   g. マッピングテーブルの発信クレームタイプ列で、ドロップダウンリストから * 名前 ID * を選択します。
   h. [完了]をクリックし、[OK]をクリックします。
8. メタデータが正常にインポートされたことを確認します。
   a. 証明書利用者信頼を右クリックしてプロパティを開きます。
   b. **[Endpoints]** 、 **[*Identifiers]** 、および [**Signature**] タブのフィールドに値が入力されていることを確認します。

      メタデータがない場合は、フェデレーションメタデータアドレスが正しいことを確認するか、値を手動で入力します。

9. 上記の手順を繰り返して、 StorageGRID システム内のすべての管理ノードに対して証明書利用者信頼を設定します。
10. 完了したら、StorageGRID およびに戻ります "すべての証明書利用者信頼をテストします" 正しく設定されていることを確認します。

証明書利用者信頼の手動作成

証明書利用者信頼のデータをインポートしないことを選択した場合は、値を手動で入力できます。

必要なもの

- StorageGRID でSSOを設定し、システム内の各管理ノードの完全修飾ドメイン名（またはIPアドレス）と証明書利用者IDを確認しておきます。

証明書利用者信頼は StorageGRID システム内の管理ノードごとに作成する必要があります。管理ノードごとに証明書利用者信頼を作成することで、ユーザは管理ノードに対して安全にサインイン / サインアウトすることができます。

- StorageGRID 管理インターフェイス用にカスタム証明書をアップロードしておきます。または、コマンドシェルから管理ノードにログインする方法を確認しておきます。
- AD FS での証明書利用者信頼の作成経験があるか、または Microsoft AD FS のドキュメントを参照できる必要があります。
- AD FS 管理スナップインを使用していて、 Administrators グループに属している必要があります。

このタスクについて

以下の手順は、Windows Server 2016に付属のAD FS 4.0での手順です。Windows Server 2012 R2に含まれているAD FS 3.0を使用している場合は、手順 にわずかな違いがあります。不明な点がある場合は、 Microsoft AD FS のドキュメントを参照してください。

手順

1. Windows Server Managerで、* Tools をクリックし、 AD FS Management *を選択します。
2. Actions（アクション）で、* Add（証明書利用者信頼の追加）*をクリックします。
3. [ようこそ]ページで、[クレーム対応]を選択し、[開始]をクリックします。
4. [証明書利用者に関するデータを手動で入力する]を選択し、[次へ]をクリックします。
5. 証明書利用者信頼の追加ウィザードを実行します。

   a. この管理ノードの表示名を入力します。

      整合性を確保するために、管理ノードの証明書利用者 ID を使用してください。この ID は、 Grid Manager のシングルサインオンページに表示されます。例： `SG-DC1-ADM1`。

   b. オプションのトークン暗号化証明書を設定する手順は省略してください。

   c. ［ URL の設定 ］ ページで、 ［ * SAML 2.0 WebSSO プロトコルのサポートを有効にする * ］ チェックボックスをオンにします。

   d. 管理ノードの SAML サービスエンドポイントの URL を入力します。

      `https://Admin_Node_FQDN/api/saml-response`

      の場合 `*Admin_Node_FQDN*`で、管理ノードの完全修飾ドメイン名を入力します。（必要に応じて、ノードの IP アドレスを代わりに使用できます。ただし、 IP アドレスを入力した場合、その IP アドレスが変わったときには証明書利用者信頼を更新または再作成する必要があります）。

   e. Configure Identifiers ページで、同じ管理ノードの証明書利用者 ID を指定します。

      *Admin_Node_Identifier*

      の場合 *Admin_Node_Identifier*`では、管理ノードの証明書利用者`ID`を`Single Sign-On`ページに表示されるとおりに入力します。例： `SG-DC1-ADM1`。

   f. 設定を確認し、証明書利用者信頼を保存して、ウィザードを閉じます。

[ クレーム発行ポリシーの編集 ] ダイアログボックスが表示されます。

ダイアログボックスが表示されない場合は、信頼を右クリックし、 * クレーム発行ポリシーの編集 * を選択します。

6. ［クレームルール］ウィザードを開始するには、［ルールの追加］をクリックします。
   a. ［ルールテンプレートの選択］ページで、リストから［* LDAP属性をクレームとして送信*］を選択し、［次へ］をクリックします。
   b. ［ ルールの設定 ］ ページで、このルールの表示名を入力します。

      たとえば、 **ObjectGUID to Name ID** と入力します。

   c. 属性ストアで、 * Active Directory * を選択します。
   d. マッピングテーブルの LDAP 属性列に、 * objectGUID * と入力します。
   e. マッピングテーブルの発信クレームタイプ列で、ドロップダウンリストから * 名前 ID * を選択します。
   f. [完了]をクリックし、[OK]をクリックします。
7. 証明書利用者信頼を右クリックしてプロパティを開きます。
8. [* Endpoints] タブで、シングルログアウト（ SLO ）のエンドポイントを設定します。
   a. * SAMLの追加*をクリックします。
   b. [* Endpoint Type*>*SAML Logout*] を選択します。
   c. 「 * Binding * > * Redirect * 」を選択します。
   d. [**Trusted URL**] フィールドに、この管理ノードからのシングルログアウト（ SLO ）に使用する URL を入力します。

      `https://Admin_Node_FQDN/api/saml-logout`

   の場合 `*Admin_Node_FQDN*` をクリックし、管理ノードの完全修飾ドメイン名を入力します。（必要に応じて、ノードの IP アドレスを代わりに使用できます。ただし、 IP アドレスを入力した場合、その IP アドレスが変わったときには証明書利用者信頼を更新または再作成する必要があります）。

   a. [OK] をクリックします。
9. [* Signature*] タブで、この証明書利用者信頼の署名証明書を指定します。
   a. カスタム証明書を追加します。
      - StorageGRID にアップロードしたカスタム管理証明書がある場合は、その証明書を選択します。
      - カスタム証明書がない場合は、管理ノードにログインしてに進みます `/var/local/mgmt-api` 管理ノードのディレクトリにを追加します `custom-server.crt` 証明書ファイル。

        *注：*管理ノードのデフォルト証明書を使用 (`server.crt`）は推奨されません。管理ノードで障害が発生した場合、ノードをリカバリする際にデフォルトの証明書が再生成されるため、証明書利用者信頼を更新する必要があります。

   b. [*適用（Apply）]をクリックし、[OK]をクリックします。

証明書利用者のプロパティが保存されて閉じられます。

10. 上記の手順を繰り返して、 StorageGRID システム内のすべての管理ノードに対して証明書利用者信頼を設定します。
11. 完了したら、StorageGRID およびに戻ります "すべての証明書利用者信頼をテストします" 正しく設定されていることを確認します。

証明書利用者信頼のテスト

## StorageGRID に対するシングルサインオン（SSO）の使用を適用する前に、シングルサインオンとシングルログアウト（SLO）が正しく設定されていることを確認します。管理ノードごとに証明書利用者信頼を作成した場合は、管理ノードごとにSSOとSLOを使用できることを確認します。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- AD FSに1つ以上の証明書利用者信頼を設定しておきます。

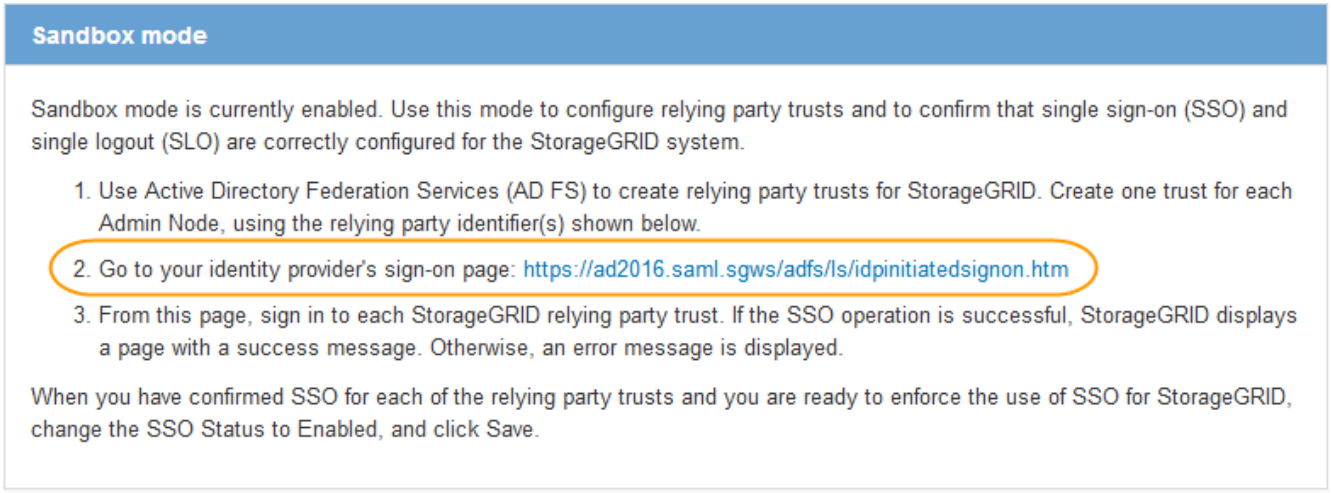
手順

1. 「* Configuration * Access Control * Single Sign-On *」を選択します。

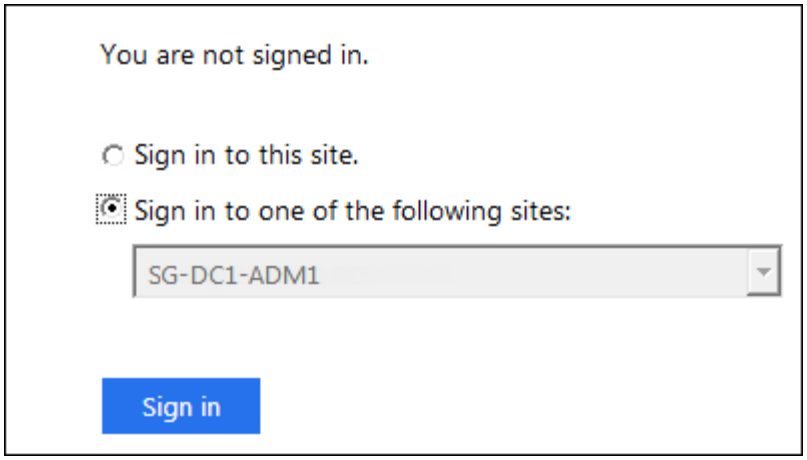
   [シングルサインオン]ページが表示され、[サンドボックスモード]オプションが選択されます。

2. サンドボックスモードの手順で、アイデンティティプロバイダのサインオンページへのリンクを探します。

   このURLは、[**Federated Service Name**]フィールドに入力した値から取得されます。




3. リンクをクリックするか、URLをコピーしてブラウザに貼り付け、アイデンティティプロバイダのサインオンページにアクセスします。
4. SSOを使用してStorageGRID にサインインできることを確認するには、*次のいずれかのサイトにサインイン*を選択し、プライマリ管理ノードの証明書利用者IDを選択して*サインイン*をクリックします。




ユーザ名とパスワードの入力を求めるプロンプトが表示されます。

5. フェデレーテッドユーザのユーザ名とパスワードを入力します。
   - SSO サインインおよびログアウト処理が成功すると、成功のメッセージが表示されます。

     ✔ Single sign-on authentication and logout test completed successfully.

   - SSO 処理が失敗すると、エラーメッセージが表示されます。問題 を修正し、ブラウザのクッキーを消去してやり直してください。
6. 上記の手順を繰り返して、他のすべての管理ノードにサインインできることを確認します。

   すべてのSSOサインインおよびログアウト処理が成功したら、SSOを有効にすることができます。

シングルサインオンの有効化

## サンドボックスモードを使用してすべてのStorageGRID 証明書利用者信頼をテストしたら、シングルサインオン（SSO）を有効にすることができます。

必要なもの

- アイデンティティソースから少なくとも1つのフェデレーテッドグループをインポートして、そのグループにRoot Access管理権限を割り当てておく必要があります。既存のテナントアカウントに対して、少なくとも1人のフェデレーテッドユーザがGrid ManagerとTenant ManagerへのRoot Access権限を持っていることを確認する必要があります。
- サンドボックスモードを使用して、すべての証明書利用者信頼をテストしておく必要があります。

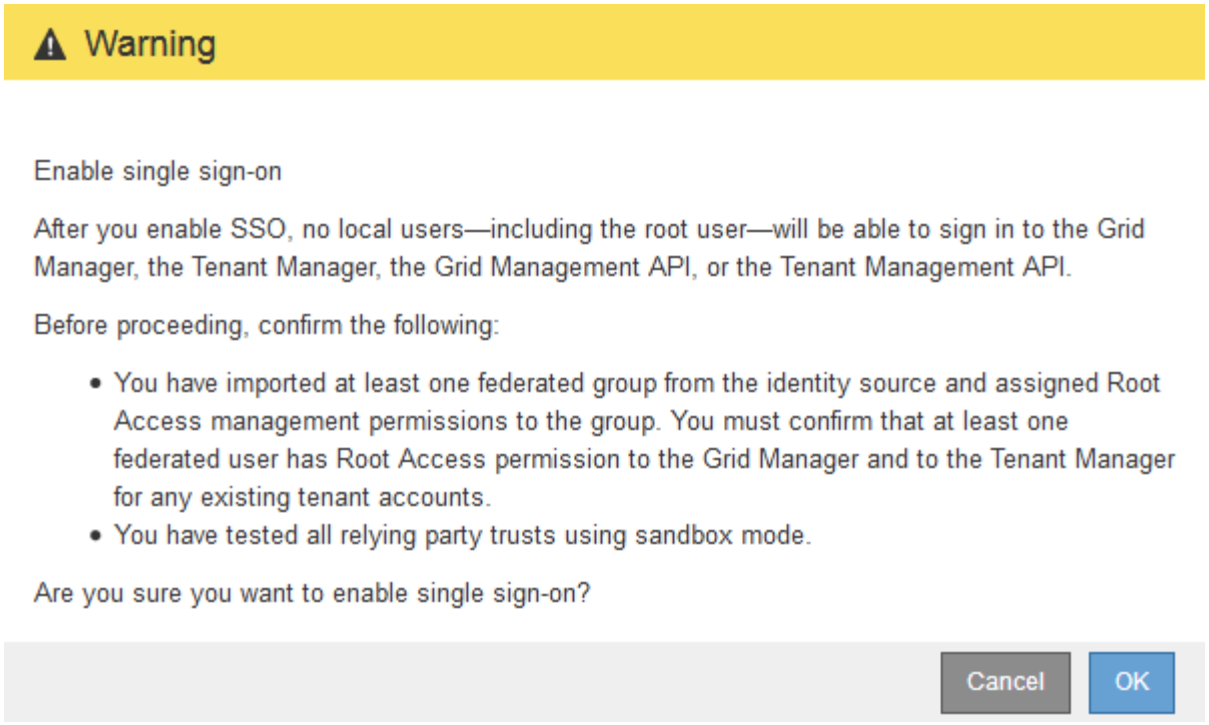
手順

1. 「* Configuration * Access Control * Single Sign-On *」を選択します。

   [シングルサインオン]ページが開き、[サンドボックスモード]が選択されます。

2. SSO ステータスを * Enabled * に変更します。
3. [ 保存（ Save ） ] をクリックします。

   警告メッセージが表示されます。




4. 警告を確認し、* OK *をクリックします。

   シングルサインオンが有効になりました。

   すべてのユーザがSSOを使用してGrid Manager、テナントマネージャ、グリッド管理API、およびテナント管理APIにアクセスする必要があります。ローカルユーザは StorageGRID にアクセスできなくなります。

シングルサインオンを無効にしています

不要になった場合はシングルサインオン（ SSO ）を無効にすることができます。アイデンティティフェデレーションを無効にする場合は、事前にシングルサインオンを無効にする必要があります。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

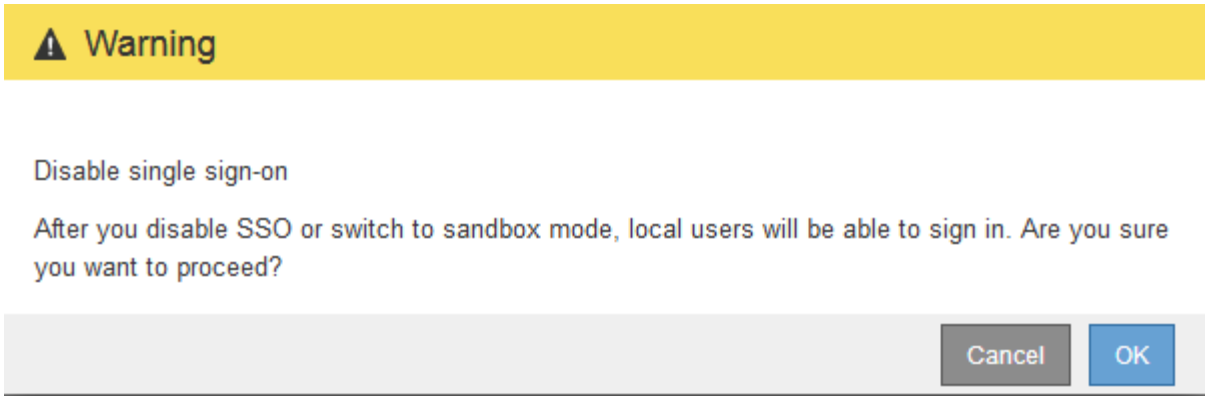
手順

1. 「* Configuration * Access Control * Single Sign-On *」を選択します。

   [Single Sign-On] ページが表示されます。

2. [* Disabled *（無効 * ） ] オプションを選択します。
3. [ 保存（ Save ） ] をクリックします。

   ローカルユーザがサインインできるようになったことを示す警告メッセージが表示されます。




4. [OK] をクリックします。

   次回 StorageGRID にサインインすると、 StorageGRID のサインインページが表示され、ローカルユーザまたはフェデレーテッド StorageGRID ユーザのユーザ名とパスワードを入力する必要があります。

## 1つの管理ノードのシングルサインオンの一時的な無効化と再有効化

シングルサインオン（ SSO ）システムが停止すると、 Grid Manager にサインインできない場合があります。この場合は、 1 つの管理ノードに対して SSO を一時的に無効にしてから再度有効にすることができます。SSO を無効にしてから再度有効にするには、ノードのコマンドシェルにアクセスする必要があります。

必要なもの

- 特定のアクセス権限が必要です。
- を用意しておく必要があります `Passwords.txt` ファイル。
- ローカルのrootユーザのパスワードを確認しておく必要があります。

このタスクについて

1 つの管理ノードに対して SSO を無効にすると、ローカルの root ユーザとして Grid Manager にサインインできます。StorageGRID システムを保護するために、ノードのコマンドシェルを使用してサインアウト後すぐに管理ノードの SSO を再度有効にする必要があります。

> 1 つの管理ノードに対して SSO を無効にしても、グリッド内の他の管理ノードの SSO 設定には影響しません。Grid Manager のシングルサインオンページの * SSO * を有効にするチェックボックスはオンのままで、既存の SSO 設定はすべて更新しないかぎり維持されます。

手順

1. 管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@Admin_Node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

      rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

2. 次のコマンドを実行します。`disable-saml`

   環境 this admin Node only コマンドのメッセージが表示されます。

3. SSO を無効にすることを確認します。

   ノードでシングルサインオンが無効になったことを示すメッセージが表示されます。

4. Web ブラウザから、同じ管理ノード上の Grid Manager にアクセスする。

   SSO を無効にしたため、 Grid Manager のサインインページが表示されます。

5. ユーザ名「 root 」とローカルの root ユーザのパスワードを使用してサインインします。
6. SSO 設定の修正が必要なために SSO を一時的に無効にした場合は、次の手順を実行します
   a. 「* Configuration * Access Control * Single Sign-On *」を選択します。
   b. 正しくない SSO 設定または古い SSO 設定を変更します。
   c. [ 保存（ Save ） ] をクリックします。

      シングルサインオンページで* Save *をクリックすると、グリッド全体でSSOが自動的に再有効化されます。

7. 他の理由で Grid Manager へのアクセスが必要であったために SSO を一時的に無効にした場合は、次の手順を実行します。
   a. 必要なタスクを実行します。
   b. [サインアウト]をクリックして、Grid Managerを閉じます。
   c. 管理ノードで SSO を再度有効にします。次のいずれかの手順を実行します。

      - 次のコマンドを実行します。 `enable-saml`

        環境 this admin Node only コマンドのメッセージが表示されます。

      SSO を有効にすることを確認します。

   ノードでシングルサインオンが有効になったことを示すメッセージが表示されます。

   - グリッドノードをリブートします。 `reboot`

8. Web ブラウザから、同じ管理ノードから Grid Manager にアクセスする。
9. StorageGRID のサインインページが表示され、グリッドマネージャにアクセスするには SSO クレデンシャルを入力する必要があることを確認します。

関連情報

"シングルサインオンを設定しています"

管理者クライアント証明書の設定

## クライアント証明書を使用すると、許可された外部クライアントがStorageGRID

Prometheusデータベースにアクセスできるようになります。クライアント証明書は、外部ツールを使用してStorageGRID を監視するためのセキュアな方法を提供します。

外部の監視ツールを使用してStorageGRID にアクセスする必要がある場合は、グリッドマネージャを使用してクライアント証明書をアップロードまたは生成し、証明書の情報を外部ツールにコピーする必要があります。

管理者クライアント証明書を追加する

クライアント証明書を追加するには、独自の証明書を指定するか、またはGrid Managerを使用して証明書を生成します。

必要なもの

- Root Access 権限が必要です。
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 管理ノードのIPアドレスまたはドメイン名を確認しておく必要があります。
- StorageGRID 管理インターフェイスのサーバ証明書を設定し、対応するCAバンドルを用意しておく必要があります
- 独自の証明書をアップロードする場合は、証明書の公開鍵と秘密鍵がローカルコンピュータ上にある必要があります。

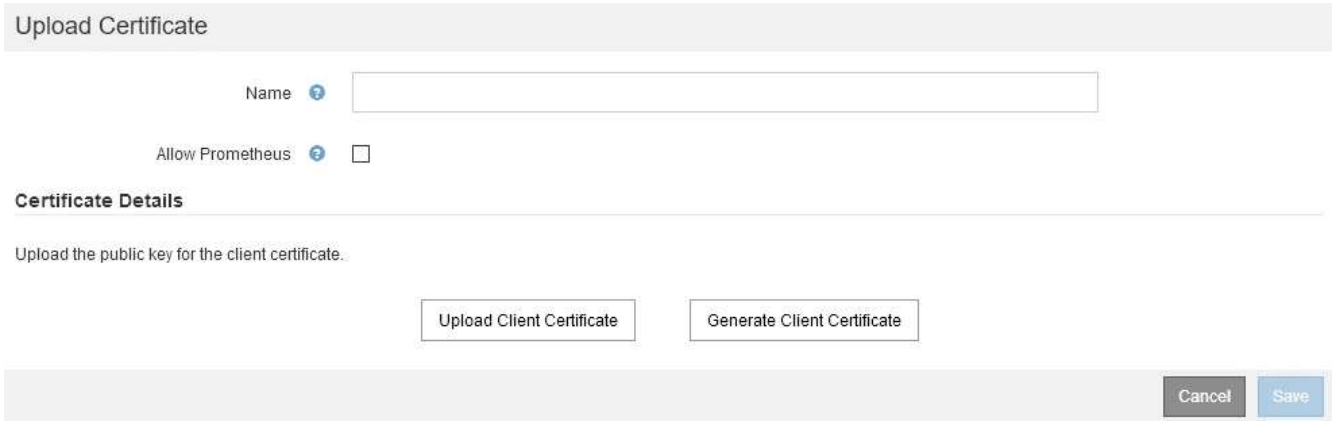
手順

1. Grid Managerで、* Configuration > Access Control > Client Certificates *を選択します。

   [Client Certificates]ページが表示されます。

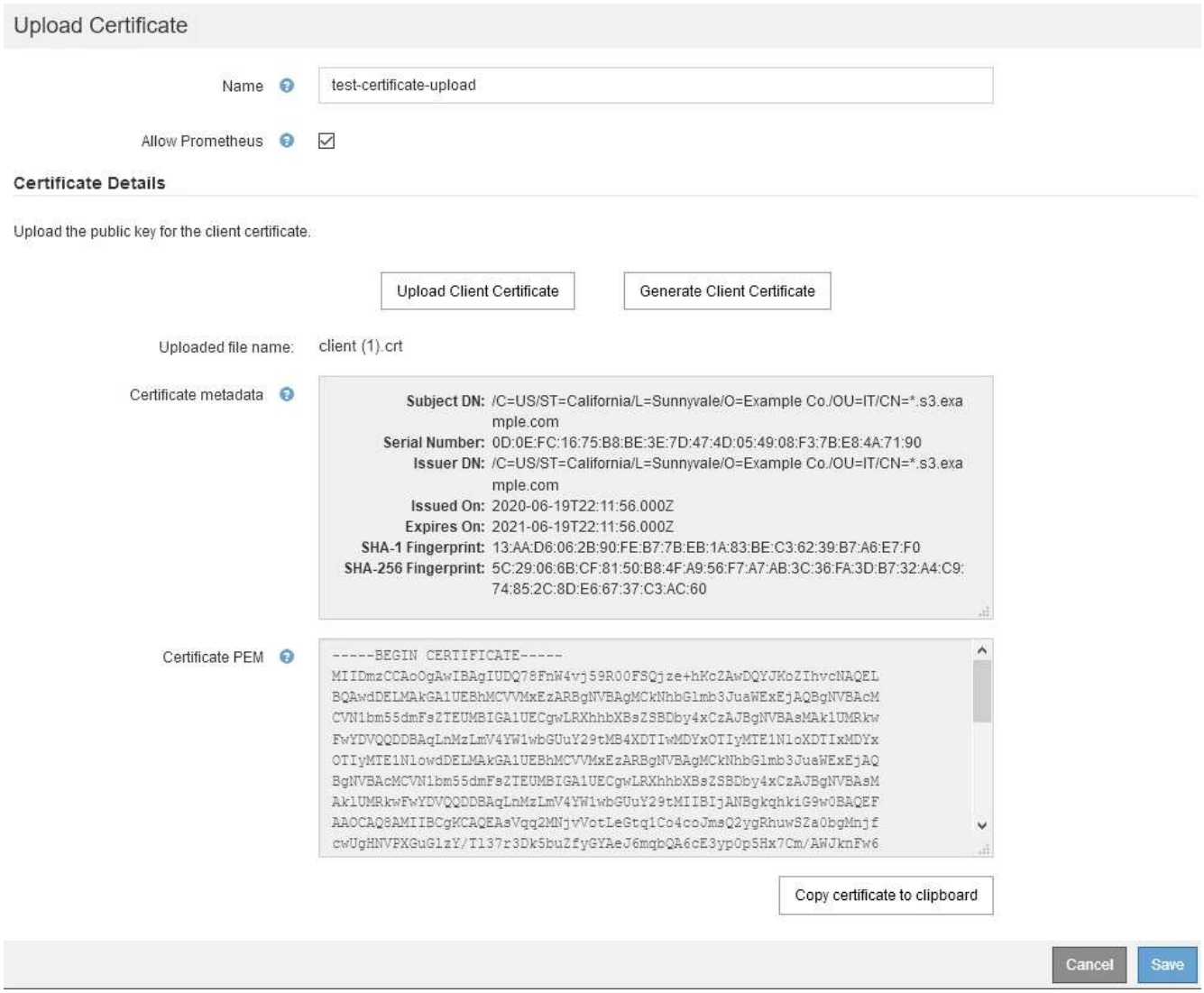
2. 「 * 追加」を選択します。

   証明書のアップロードページが表示されます。




3. 証明書の名前を1～32文字で入力します。
4. 外部の監視ツールを使用してPrometheus指標にアクセスするには、* Prometheus *を許可するチェックボックスをオンにします。
5. 証明書をアップロードまたは生成します。
   a. 証明書をアップロードするには、に進みます こちらをご覧ください。
   b. 証明書を生成するには、に進みます こちらをご覧ください。
6. [upload_cert]]証明書をアップロードするには、次の手順を実行します。
   a. [クライアント証明書のアップロード]を選択します。
   b. 証明書の公開鍵を参照します。

      証明書の公開鍵をアップロードすると、「Certificate metadata」フィールドと「Certificate PEM」フィールドに値が入力されます。




a. [証明書をクリップボードにコピーする*]を選択し、証明書を外部監視ツールに貼り付けます。

b. 編集ツールを使用して、秘密鍵をコピーして外部の監視ツールに貼り付けます。

c. 証明書をGrid Managerに保存するには、* Save *を選択します。

7. [generate-cert]]証明書を生成するには、次の手順を実行します。

a. [クライアント証明書の生成]を選択します。

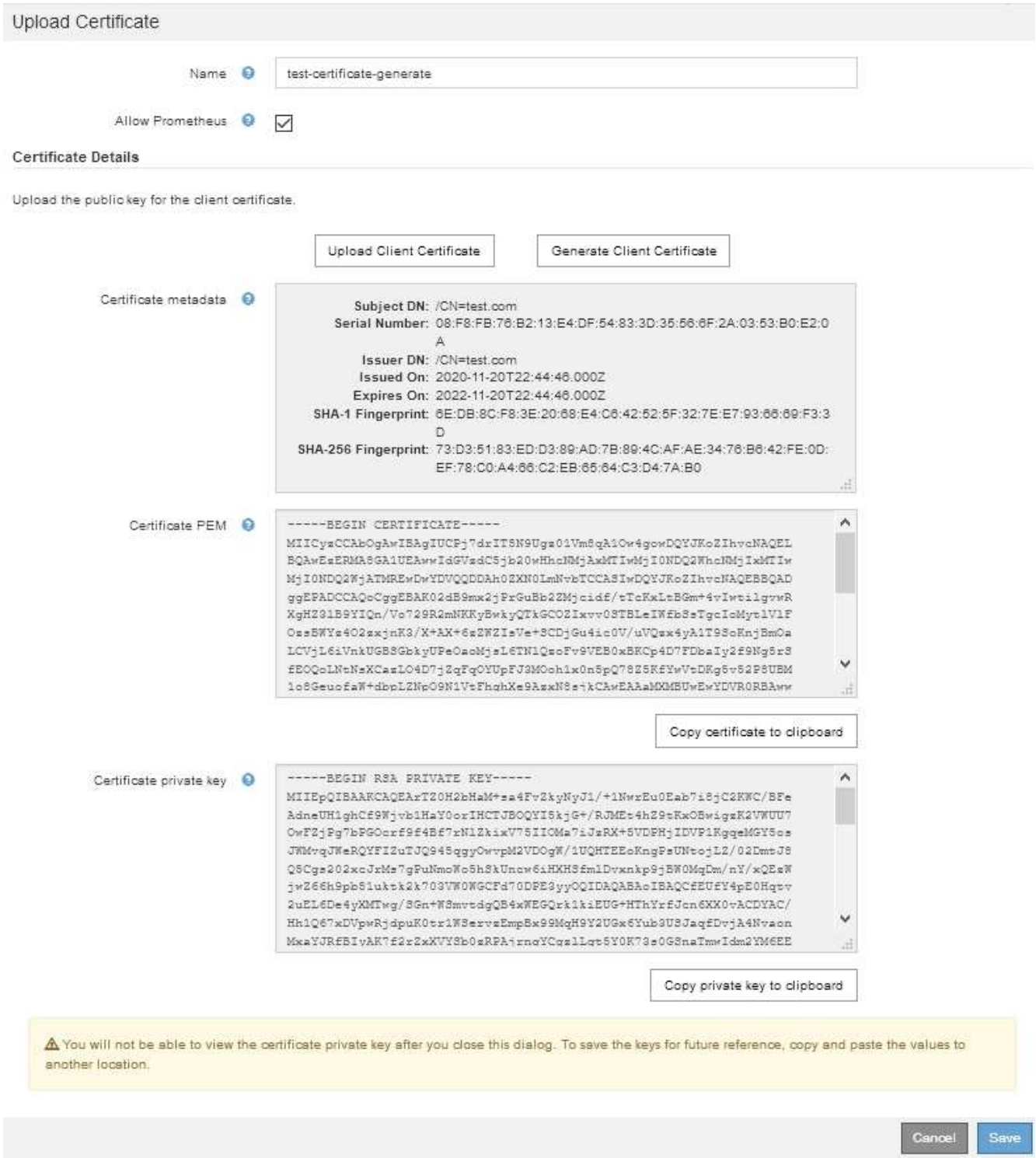
b. 管理ノードのドメイン名またはIPアドレスを入力します。

c. 必要に応じて、証明書を所有する管理者を識別するために、[X.509 subject（Distinguished Name（DN;認定者名）]とも呼ばれる）を入力します。

d. 必要に応じて、証明書の有効日数を選択します。デフォルトは730日です。

e. [*Generate （生成） ] を選択します

「* Certificate metadata 」、「 Certificate PEM *」、および「Certificate private key *」の各フィールドに値が入力されます。




a. [証明書をクリップボードにコピーする*]を選択し、証明書を外部監視ツールに貼り付けます。

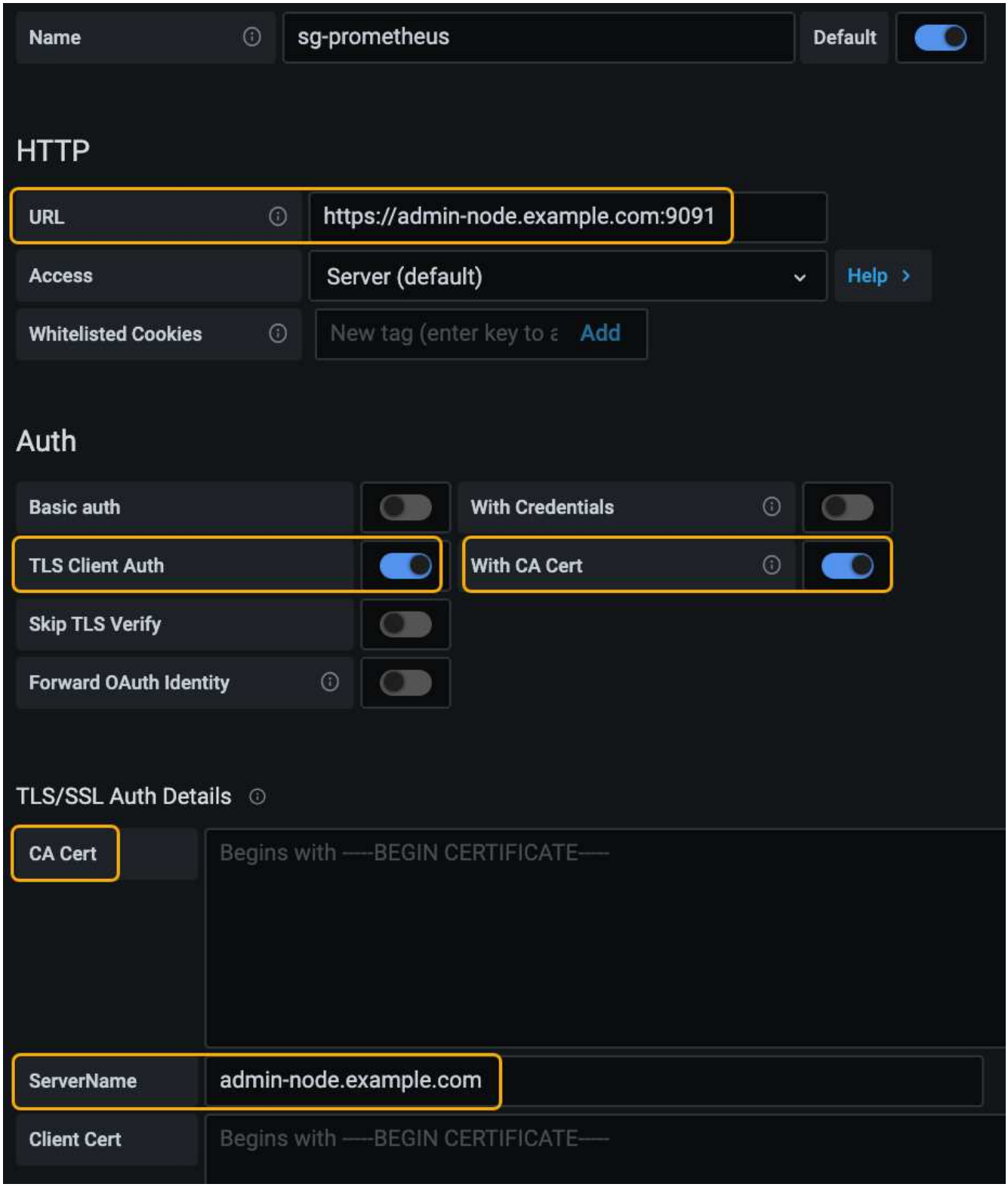
b. 秘密鍵をクリップボードにコピー*を選択し、外部監視ツールに貼り付けます。

> このダイアログボックスを閉じると、秘密鍵を表示できなくなります。キーを安全な場所にコピーします。

c. 証明書をGrid Managerに保存するには、* Save *を選択します。

8. Grafana などの外部監視ツールで次の設定を行います。

Grafana の例は次のスクリーンショットで示されています。




a. * 名前 * ：接続の名前を入力します。

   StorageGRID ではこの情報は必要ありませんが、接続をテストするための名前を指定する必要があります。

b. * URL * ：管理ノードのドメイン名または IP アドレスを入力します。HTTPS とポート 9091 を指定し

ます。

例： `https://admin-node.example.com:9091`

c. CA証明書を使用して、* TLSクライアント認証*および*を有効にします。

d. TLS/SSL Auth Detailsの下で、管理インターフェイスのサーバ証明書またはCAバンドルを**CA Cert**にコピーして貼り付けます。

e. * ServerName* ：管理ノードのドメイン名を入力します。

servernameは、管理インターフェイスのサーバ証明書に表示されるドメイン名と一致する必要があります。

f. StorageGRID またはローカルファイルからコピーした証明書と秘密鍵を保存してテストします。

これで、外部の監視ツールを使用して StorageGRID から Prometheus 指標にアクセスできるようになります。

指標の詳細については、StorageGRID の監視とトラブルシューティングの手順を参照してください。

関連情報

"StorageGRID セキュリティ証明書を使用する"

"Grid ManagerおよびTenant Manager用のカスタムサーバ証明書を設定する"

"トラブルシューティングを監視します"

### 管理者クライアント証明書の編集

証明書を編集して、名前を変更したり、Prometheusアクセスを有効または無効にしたり、現在の証明書の期限が切れたときに新しい証明書をアップロードしたりできます。

必要なもの

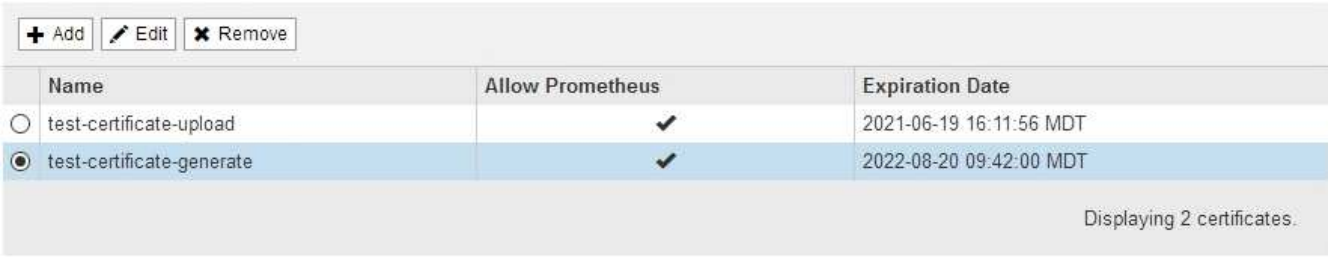
- Root Access 権限が必要です。
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 管理ノードのIPアドレスまたはドメイン名を確認しておく必要があります。
- 新しい証明書と秘密鍵をアップロードする場合は、ローカルコンピュータ上でそれらの証明書が使用可能である必要があります。

手順

1. [* Configuration > Access Control > Client Certificates *]を選択します。

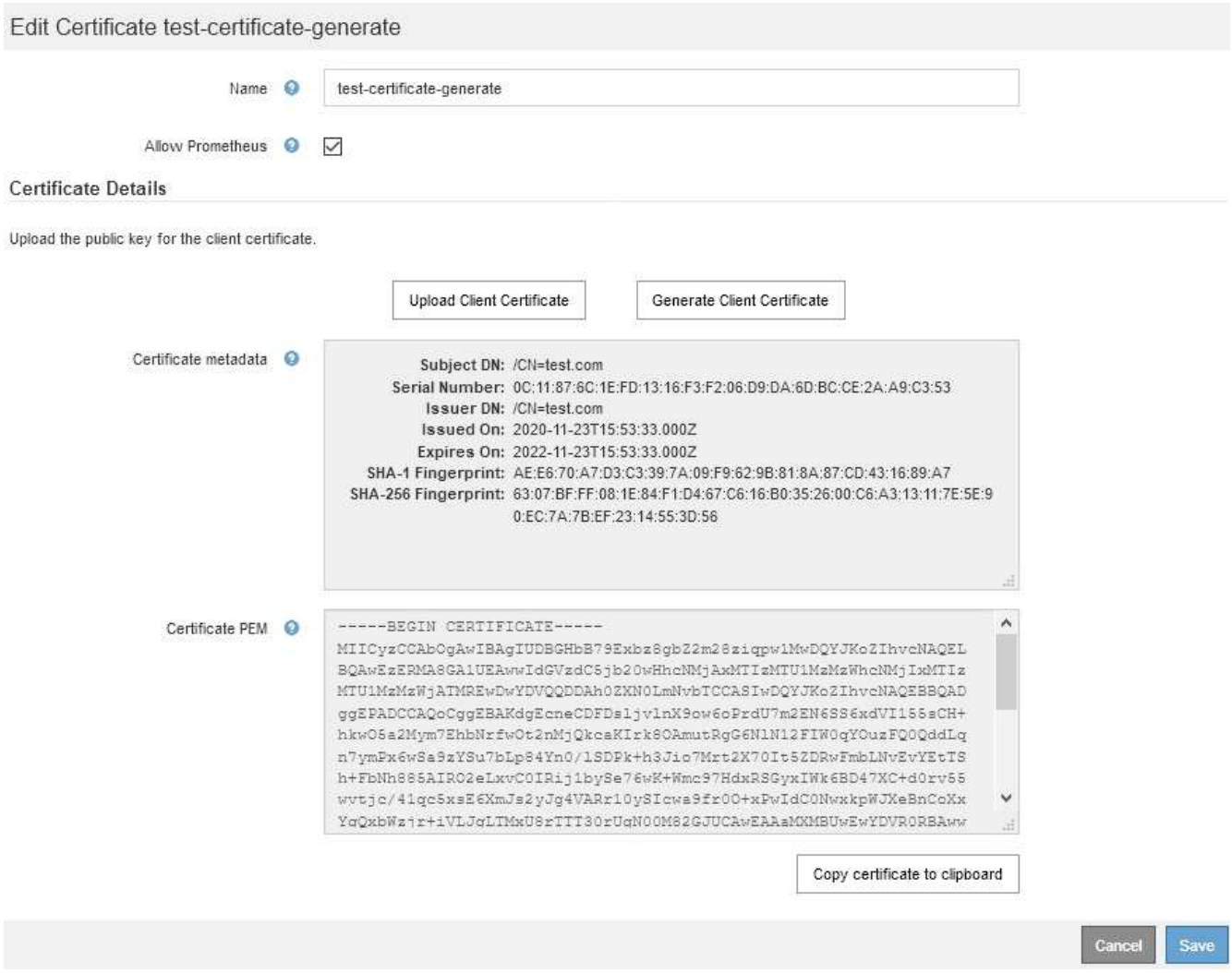
[Client Certificates]ページが表示されます。既存の証明書のリストが表示されます。

証明書の有効期限が表に記載されています。証明書の有効期限が近づいた場合、またはすでに有効期限が切れた場合は、メッセージが表に表示され、アラートがトリガーされます。




2. 編集する証明書の左側にあるオプションボタンを選択します。
3. 「 * 編集 * 」を選択します。

   [Edit Certificate]ダイアログボックスが表示されます。




4. 証明書に必要な変更を加えます。
5. 証明書をGrid Managerに保存するには、* Save *を選択します。
6. 新しい証明書をアップロードした場合：
   a. [証明書をクリップボードにコピーする*]を選択して、証明書を外部監視ツールに貼り付けます。
   b. 編集ツールを使用して、新しい秘密鍵をコピーして外部の監視ツールに貼り付けます。
   c. 外部の監視ツールで証明書と秘密鍵を保存してテストします。

7. 新しい証明書を生成した場合：
   a. [証明書をクリップボードにコピーする*]を選択して、証明書を外部監視ツールに貼り付けます。
   b. [プライベートキーをクリップボードにコピーする*]を選択して、証明書を外部監視ツールに貼り付けます。

      このダイアログボックスを閉じると、秘密鍵を表示したりコピーしたりすることはできなくなります。キーを安全な場所にコピーします。

   c. 外部の監視ツールで証明書と秘密鍵を保存してテストします。

管理者クライアント証明書を削除しています

不要になった証明書は削除できます。

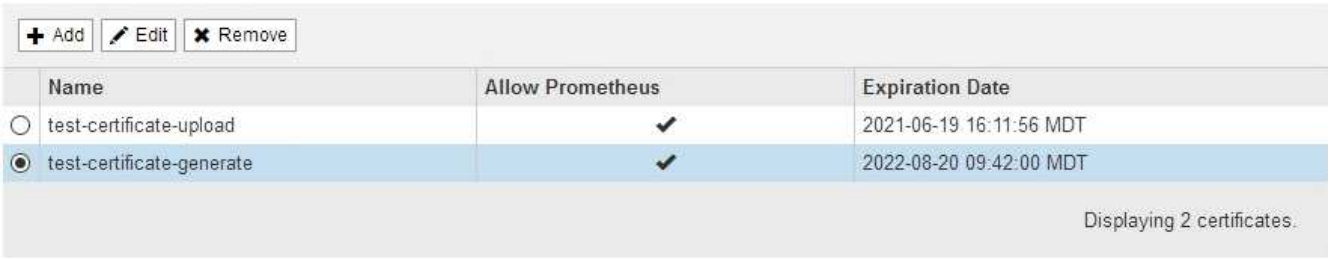
必要なもの

- Root Access 権限が必要です。
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

手順

1. [* Configuration > Access Control > Client Certificates *]を選択します。

   [Client Certificates]ページが表示されます。既存の証明書のリストが表示されます。




2. 削除する証明書の左側にあるオプションボタンを選択します。
3. 「 * 削除」を選択します。

   確認のダイアログボックスが表示されます。

4. 「 * OK 」を選択します。

証明書が削除されます。

## キー管理サーバを設定しています

## 1 つ以上の外部キー管理サーバ（ KMS ）を設定して、特別に設定したアプライアンスノード上のデータを保護することができます。

### キー管理サーバ（ **KMS** ）とは何ですか？

キー管理サーバ（ KMS ）は、関連する StorageGRID サイトの StorageGRID アプライアンスノードに Key Management Interoperability Protocol （ KMIP ）を使用して暗号化キーを提供する外部のサードパーティシステムです。

インストール時にノード暗号化 * 設定が有効になっている StorageGRID アプライアンスノードのノード暗号化キーを管理するには、 1 つ以上のキー管理サーバを使用します。これらのアプライアンスノードでキー管理サーバを使用すると、アプライアンスをデータセンターから削除した場合でも、データを保護できます。アプライアンスのボリュームを暗号化すると、ノードが KMS と通信できないかぎり、アプライアンスのデータにアクセスすることはできません。

> StorageGRID では、アプライアンスノードの暗号化と復号化に使用する外部キーは作成も管理もされません。外部キー管理サーバを使用して StorageGRID データを保護する場合は、そのサーバの設定方法を理解し、暗号化キーの管理方法を理解しておく必要があります。キー管理タスクの実行については、この手順では説明していません。サポートが必要な場合は、キー管理サーバのドキュメントを参照するか、テクニカルサポートにお問い合わせください。

### **StorageGRID** 暗号化方式の確認

## StorageGRID には、データを暗号化するためのさまざまなオプションがあります。使用可能な方法を確認して、データ保護の要件を満たす方法を決定する必要があります。

次の表に、 StorageGRID で使用できる暗号化方式の概要を示します。

| 暗号化オプション | 動作の仕組み | 環境 |
| --- | --- | --- |
| Grid Manager からキー管理サーバ（ KMS ）を取得します | StorageGRID サイト用のキー管理サーバ（* Configuration > System Settings > Key Management Server *）を設定し、アプライアンスでノード暗号化を有効にします。次に、アプライアンスノードが KMS に接続して、 Key Encryption Key （ KEK ；キー暗号化キー）を要求します。このキーは、各ボリュームのデータ暗号化キー（ DEK ）を暗号化および復号化します。 | インストール中にノード暗号化 * が有効になっているアプライアンスノード。アプライアンスのすべてのデータは、物理的な損失やデータセンターからの削除から保護されます。一部の StorageGRID ストレージおよびサービスアプライアンスで使用できます。 |

| 暗号化オプション | 動作の仕組み | 環境 |
| --- | --- | --- |
| SANtricity System Manager のドライブセキュリティ | ストレージアプライアンスでドライブセキュリティ機能が有効になっている場合は、 SANtricity System Manager を使用してセキュリティキーを作成および管理できます。このキーは、セキュリティ保護されたドライブ上のデータにアクセスするために必要です。 | Full Disk Encryption （ FDE ）ドライブまたは連邦情報処理標準（ FIPS ）ドライブが搭載されたストレージアプライアンス。セキュリティ保護されたドライブ上のデータは、すべて物理的な損失やデータセンターからの削除から保護されます。一部のストレージアプライアンスまたはサービスアプライアンスでは使用できません。<br><br>"SG6000 ストレージアプライアンス"<br><br>"SG5700 ストレージアプライアンス"<br><br>"SG5600 ストレージアプライアンス" |
| 格納オブジェクトの暗号化グリッドオプション | • Stored Object Encryption オプションは**Grid Manager**で有効にできます（ Configuration > System Settings > Grid Options *）。有効にすると、バケットレベルまたはオブジェクトレベルで暗号化されていない新しいオブジェクトは取り込み時に暗号化されます。 | 新たに取り込まれたS3およびSwiftオブジェクトデータ。格納されている既存のオブジェクトは暗号化されません。オブジェクトメタデータやその他の機密データは暗号化されません。<br><br>"格納オブジェクトの暗号化を設定する" |
| S3 バケットの暗号化 | バケットの暗号化を有効にするには、 PUT Bucket 暗号化要求を問題 に設定します。オブジェクトレベルで暗号化されていない新しいオブジェクトは取り込み時に暗号化されます。 | 新たに取り込まれたS3オブジェクトデータのみ。バケットに暗号化を指定する必要があります。既存のバケットオブジェクトは暗号化されません。オブジェクトメタデータやその他の機密データは暗号化されません。<br><br>"S3 を使用する" |

| 暗号化オプション | 動作の仕組み | 環境 |
| --- | --- | --- |
| S3 オブジェクトのサーバ側の暗号化（ SSE ） | オブジェクトを格納してを含めるS3要求を問題 した `x-amz-server-side-encryption` 要求ヘッダー。 | 新たに取り込まれたS3オブジェクトデータのみ。オブジェクトに暗号化を指定する必要があります。オブジェクトメタデータやその他の機密データは暗号化されません。<br><br>キーは StorageGRID で管理されます。<br><br>"S3 を使用する" |
| ユーザ指定のキーによる S3 オブジェクトのサーバ側暗号化（ SSE-C ） | オブジェクトを格納する S3 要求を問題 し、 3 つの要求ヘッダーを含めます。<br><br>• `x-amz-server-side-encryption-customer-algorithm`<br>• `x-amz-server-side-encryption-customer-key`<br>• `x-amz-server-side-encryption-customer-key-MD5` | 新たに取り込まれたS3オブジェクトデータのみ。オブジェクトに暗号化を指定する必要があります。オブジェクトメタデータやその他の機密データは暗号化されません。<br><br>キーは StorageGRID の外部で管理されます。<br><br>"S3 を使用する" |
| 外部ボリュームまたはデータストアの暗号化 | 導入プラットフォームで暗号化がサポートされている場合は、StorageGRID の外部の暗号化方式を使用して、ボリュームまたはデータストア全体を暗号化できます。 | すべてのボリュームまたはデータストアが暗号化されていることを前提として、すべてのオブジェクトデータ、メタデータ、およびシステム構成データ。<br><br>外部暗号化方式を使用すると、暗号化アルゴリズムと暗号キーを厳密に制御できます。は、記載されている他の方法と組み合わせることができます。 |

| 暗号化オプション | 動作の仕組み | 環境 |
| --- | --- | --- |
| StorageGRID の外部でのオブジェクトの暗号化 | StorageGRID に取り込まれる前にオブジェクトデータとメタデータを暗号化するには、 StorageGRID の外部の暗号化メソッドを使用します。 | オブジェクトデータとメタデータのみ（システム設定データは暗号化されません）。<br><br>外部暗号化方式を使用すると、暗号化アルゴリズムと暗号キーを厳密に制御できます。は、記載されている他の方法と組み合わせることができます。<br><br>"Amazon Simple Storage Service - Developer Guide ：クライアント側の暗号化を使用したデータの保護" |

複数の暗号化方式を使用する

要件に応じて、一度に複数の暗号化方式を使用できます。例：

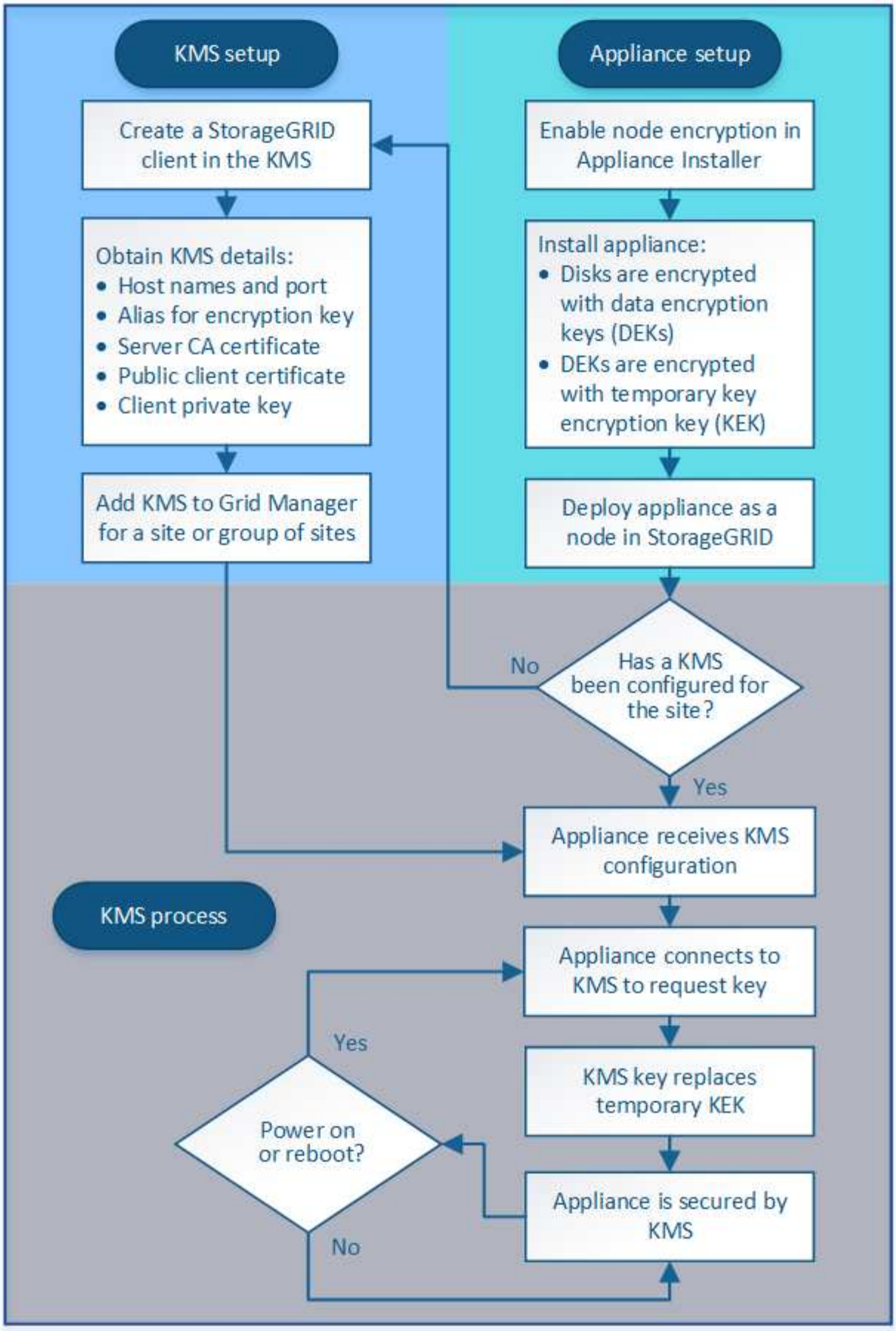
- KMS を使用してアプライアンスノードを保護したり、 SANtricity システムマネージャのドライブセキュリティ機能を使用して、同じアプライアンス内の自己暗号化ドライブ上のデータを「二重に暗号化」することもできます。
- KMS を使用してアプライアンスノード上のデータを保護したり、格納されているオブジェクト暗号化グリッドオプションを使用してすべてのオブジェクトを取り込み時に暗号化することもできます。

暗号化を必要とするオブジェクトがごく一部しかない場合は、暗号化をバケットレベルまたは個々のオブジェクトレベルで制御することを検討してください。複数レベルの暗号化を有効にすると、パフォーマンスコストが増加します。

**KMS** とアプライアンスの設定の概要

キー管理サーバ（ KMS ）を使用してアプライアンスノード上の StorageGRID データを保護する前に、 1 つ以上の KMS サーバを設定してアプライアンスノードのノード暗号化を有効にするという 2 つの設定タスクを完了しておく必要があります。これらの 2 つの設定タスクが完了すると、キー管理プロセスが自動的に実行されます。

フローチャートは、 KMS を使用してアプライアンスノード上の StorageGRID データを保護する手順の概要を示しています。




フローチャートには、 KMS のセットアップとアプライアンスのセットアップが並行して行われていることが

示されています。ただし、要件に基づいて、新しいアプライアンスノードのノード暗号化を有効にする前後にキー管理サーバをセットアップできます。

### キー管理サーバのセットアップ（KMS）

キー管理サーバのセットアップには、主に次の手順が含まれます。

| ステップ | を参照してください |
| --- | --- |
| KMS ソフトウェアにアクセスし、各 KMS または KMS クラスタに StorageGRID 用のクライアントを追加します。 | "KMSでクライアントとしてStorageGRID を設定する" |
| KMS で StorageGRID クライアントの必要な情報を入手します。 | "KMSでクライアントとしてStorageGRID を設定する" |
| Grid Manager に KMS を追加して 1 つのサイトまたはデフォルトのサイトグループに割り当て、必要な証明書をアップロードして、 KMS の設定を保存します。 | "キー管理サーバの追加（KMS）" |

### アプライアンスのセットアップ

KMS を使用するためにアプライアンスノードをセットアップするには、次の手順に従います。

1. アプライアンスのハードウェア構成フェーズでは、 StorageGRID アプライアンスインストーラを使用してアプライアンスのノード暗号化 * 設定を有効にします。

   > グリッドにアプライアンスを追加したあとに * Node Encryption * 設定を有効にすることはできません。また、ノード暗号化が有効になっていないアプライアンスでは外部キー管理を使用できません。

2. StorageGRID アプライアンスインストーラを実行します。インストール時に、次のように各アプライアンスボリュームにランダムデータ暗号化キー（ DEK ）が割り当てられます。
   - DEK は、各ボリュームのデータの暗号化に使用されます。これらのキーは、アプライアンス OS で Linux Unified Key Setup （ LUKS ； Linux Unified Key Setup ）ディスク暗号化を使用して生成され、変更することはできません。
   - 各 DEK は、 KEK （ Master Key Encryption Key ）によって暗号化されます。最初の KEK は、アプライアンスが KMS に接続できるまで DEK を暗号化する一時キーです。
3. StorageGRID にアプライアンスノードを追加します。

詳細については、次を参照してください。

- "SG100 SG1000サービスアプライアンス"
- "SG6000 ストレージアプライアンス"
- "SG5700 ストレージアプライアンス"
- "SG5600 ストレージアプライアンス"

キー管理の暗号化プロセス（自動的に実行）

キー管理の暗号化には、次の高度な手順が含まれています。これらの手順は自動的に実行されます。

1. ノードの暗号化が有効になっているアプライアンスをグリッドにインストールすると、 StorageGRID は、新しいノードを含むサイトに KMS 設定が存在するかどうかを確認します。
   - KMS がすでにサイト用に設定されている場合、アプライアンスは KMS の設定を受信します。
   - KMS がサイト用にまだ設定されていない場合は、サイトに KMS を設定し、アプライアンスが KMS の設定を受信するまで、アプライアンス上のデータは一時的な KEK によって暗号化されたままになります。
2. アプライアンスは KMS 設定を使用して KMS に接続し、暗号化キーを要求します。
3. KMS は暗号化キーをアプライアンスに送信します。KMS の新しいキーは一時的な KEK に代わるものであり、アプライアンスボリュームの DEK の暗号化と復号化に使用されるようになりました。

   暗号化されたアプライアンスノードから設定された KMS に接続する前に存在するデータは、すべて一時キーで暗号化されます。ただし、一時キーを KMS 暗号化キーに置き換えるまでは、アプライアンスボリュームをデータセンターから削除できないようにする必要があります。

4. アプライアンスの電源をオンにするか再接続すると、 KMS に接続してキーを要求します。揮発性メモリに保存されたキーは、停電や再起動の際に存続することはできません。

キー管理サーバを使用する際の考慮事項と要件

# 外部キー管理サーバ（ KMS ）を設定する前に、考慮事項と要件を確認しておく必要があります。

**KMIP** の要件

StorageGRID は KMIP バージョン 1.4 をサポートしています。

"Key Management Interoperability Protocol （キー管理相互運用性プロトコル）仕様バージョン 1.4"

アプライアンスノードと設定された KMS の間の通信には、セキュアな TLS 接続が使用されます。StorageGRID では、 KMIP で次の TLS v1.2 暗号をサポートしています。

- TLS_ECDHE_RSA_with _AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_With _AES_256_GCM_SHA384

ノード暗号化を使用する各アプライアンスノードに、サイト用に設定した KMS または KMS クラスタへのネットワークアクセスがあることを確認してください。

ネットワークのファイアウォールの設定で、各アプライアンスノードが Key Management Interoperability Protocol （ KMIP ）の通信に使用するポートを介して通信できるようにする必要があります。デフォルトの KMIP ポートは 5696 です。

サポートされているアプライアンスはどれですか。

キー管理サーバ（ KMS ）を使用して、「ノード暗号化 * 」が有効になっているグリッド内の StorageGRID アプライアンスの暗号化キーを管理できます。この設定は、 StorageGRID アプライアンスインストーラを使

用してアプライアンスをインストールするハードウェア構成の段階でのみ有効にできます。

> グリッドにアプライアンスを追加したあとにノードの暗号化を有効にすることはできません。また、ノード暗号化が有効になっていないアプライアンスでは外部キー管理を使用できません。

設定されている KMS は、次の StorageGRID アプライアンスおよびアプライアンスノードで使用できます。

| アプライアンス | ノードタイプ |
| --- | --- |
| SG1000 サービスアプライアンス | 管理ノードまたはゲートウェイノード |
| SG100 サービスアプライアンス | 管理ノードまたはゲートウェイノード |
| SG6000 ストレージアプライアンス | ストレージノード |
| SG5700 ストレージアプライアンス | ストレージノード |
| SG5600 ストレージアプライアンス | ストレージノード |

次のようなソフトウェアベース（非アプライアンス）のノードでは、設定された KMS を使用することはできません。

- 仮想マシン（ VM ）として導入されたノード
- Linuxホスト上のDockerコンテナ内に導入されたノード

これらの他のプラットフォームに導入されたノードでは、データストアまたはディスクレベルで StorageGRID 外部の暗号化を使用できます。

#### キー管理サーバを設定する必要があるのはいつですか？

新規インストールの場合は、テナントを作成する前に Grid Manager で 1 つ以上のキー管理サーバをセットアップするのが一般的です。この順序により、ノード上に格納されるオブジェクトデータよりも先にノードが保護されます。

Grid Manager では、アプライアンスノードのインストール前またはインストール後にキー管理サーバを設定できます。

#### 必要なキー管理サーバの数

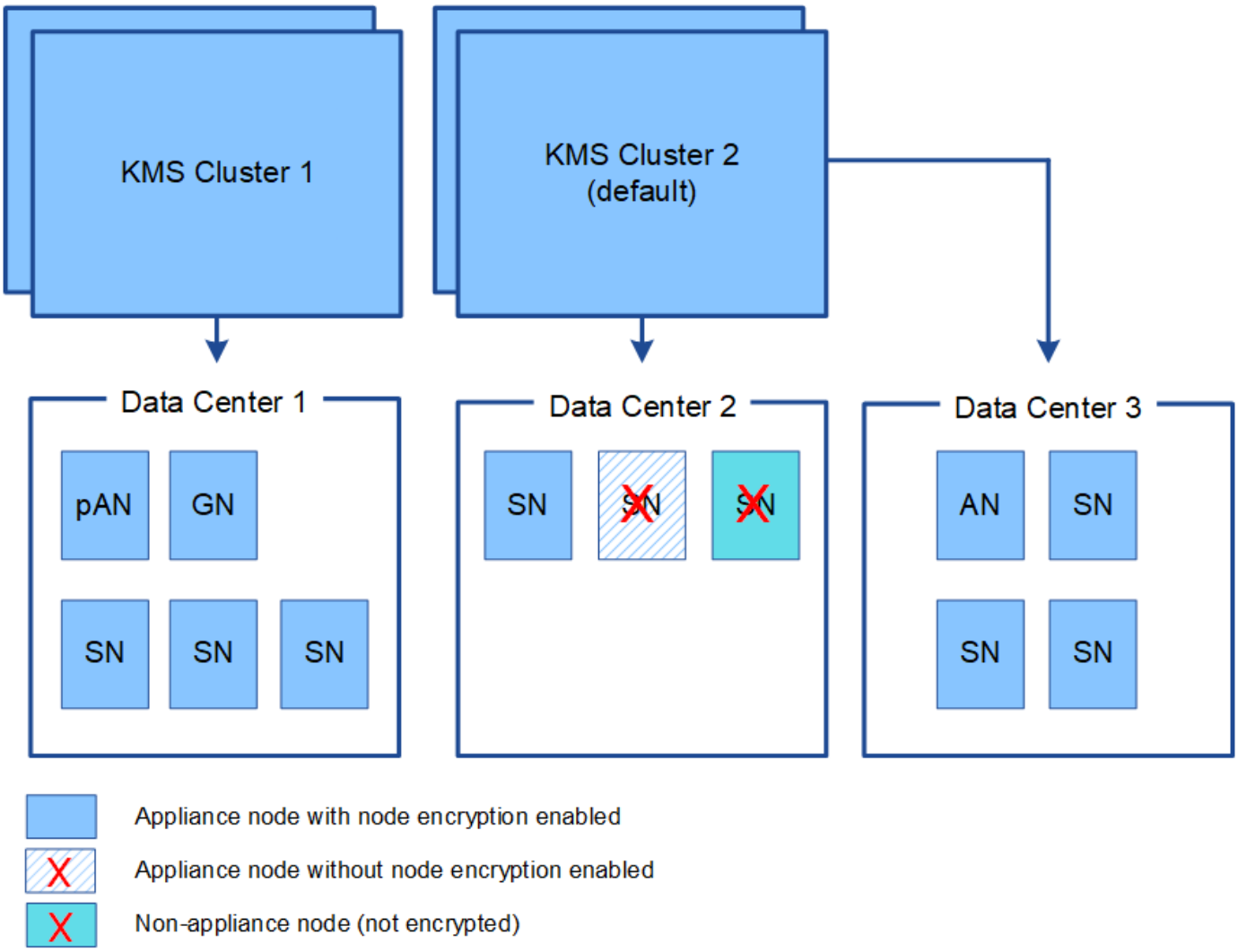
1 つ以上の外部キー管理サーバを設定して、 StorageGRID システム内のアプライアンスノードに暗号化キーを提供できます。各 KMS は、 1 つのサイトまたはサイトグループにある StorageGRID アプライアンスノードに単一の暗号化キーを提供します。

StorageGRID は KMS クラスタの使用をサポートしています。各 KMS クラスタには、設定と暗号化キーを共有するレプリケートされた複数のキー管理サーバが含まれます。高可用性構成のフェイルオーバー機能が向上するため、 KMS クラスタをキー管理に使用することを推奨します。

たとえば、 StorageGRID システムに 3 つのデータセンターサイトがあるとします。1 つの KMS クラスタを設定して、データセンター 1 のすべてのアプライアンスノードともう 1 つの KMS クラスタのキーを取得し、

他のすべてのサイトにあるすべてのアプライアンスノードのキーを取得することができます。2 つ目の KMS クラスタを追加すると、データセンター 2 とデータセンター 3 にデフォルトの KMS を設定できます。

非アプライアンスノードや、インストール時に * Node Encryption * が有効になっていないアプライアンスノードでは、 KMS を使用できないことに注意してください。




キーをローテーションするとどうなりますか。

セキュリティのベストプラクティスとして、設定された各 KMS で使用される暗号化キーを定期的にローテーションすることを推奨します。

暗号化キーをローテーションするときは、 KMS ソフトウェアを使用して、最後に使用したバージョンのキーを同じキーの新しいバージョンにローテーションします。完全に別のキーに回転させないでください。

> キーのローテーションは、 Grid Manager 内の KMS のキー名（エイリアス）を変更しては実行しないでください。代わりに、 KMS ソフトウェアのキーバージョンを更新してキーをローテーションしてください。以前のキーに使用したものと同じキーエイリアスを新しいキーに使用します。設定されている KMS のキーエイリアスを変更すると、 StorageGRID がデータを復号化できなくなる可能性があります。

新しいキーバージョンが利用可能になった場合：

- このサービスは、 KMS に関連付けられているサイトにある暗号化されたアプライアンスノードに自動的に配信されます。キーが回転した後 1 時間以内に分配が行われる必要があります。
- 新しいキーバージョンが配布されたときに暗号化アプライアンスノードがオフラインになっている場合、ノードはリブート後すぐに新しいキーを受け取ります。
- 何らかの理由でアプライアンスボリュームの暗号化に新しいキーバージョンを使用できない場合は、アプライアンスノードに対して * KMS 暗号化キーローテーション failed * アラートがトリガーされます。このアラートの解決方法については、テクニカルサポートへの問い合わせが必要になることがあります。

アプライアンスノードは暗号化したあとに再利用できますか。

暗号化されたアプライアンスを別の StorageGRID システムにインストールする必要がある場合は、先にグリッドノードの運用を停止して、オブジェクトデータを別のノードに移動しておく必要があります。その後、StorageGRID アプライアンスインストーラを使用して KMS の設定をクリアします。KMS の設定をクリアすると、「ノード暗号化 * 」設定が無効になり、アプライアンスノードと StorageGRID サイトの KMS 設定の間の関連付けが解除されます。

KMS 暗号化キーにアクセスできないため、アプライアンスに残っているデータにはアクセスできなくなり、永続的にロックされます。

"SG100 SG1000サービスアプライアンス"

"SG6000 ストレージアプライアンス"

"SG5700 ストレージアプライアンス"

"SG5600 ストレージアプライアンス"

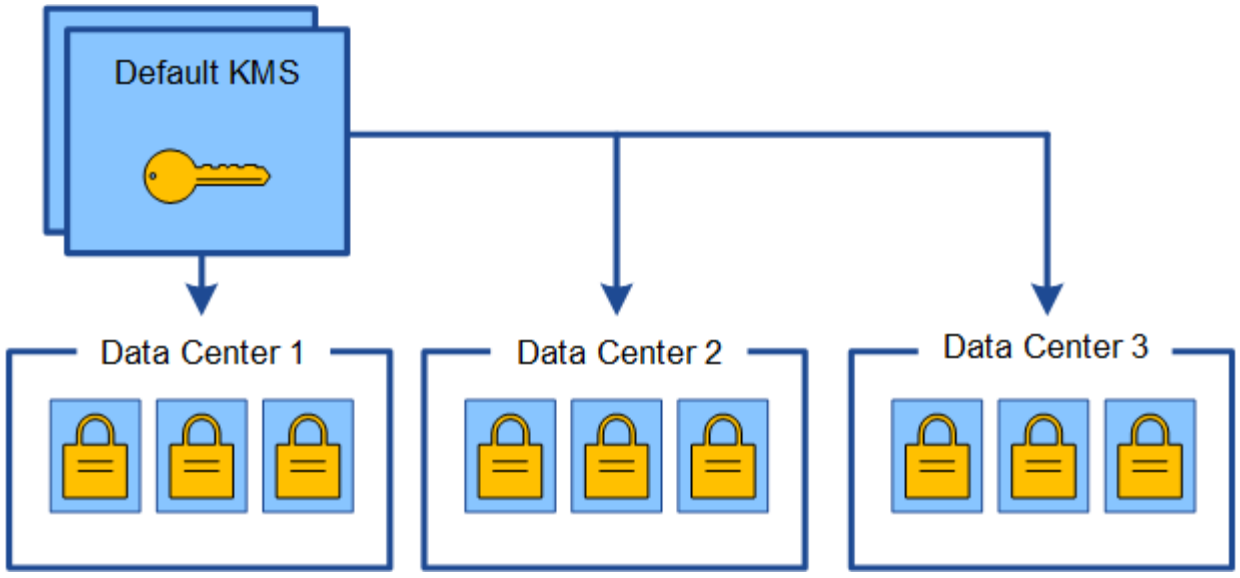
サイトの **KMS** を変更する際の考慮事項

## 各キー管理サーバ（ KMS ）または KMS クラスタは、 1 つのサイトまたはサイトグループにあるすべてのアプライアンスノードに暗号化キーを提供します。サイトで使用する KMS を変更する必要がある場合は、暗号化キーを KMS から別の KMS にコピーする必要があります。

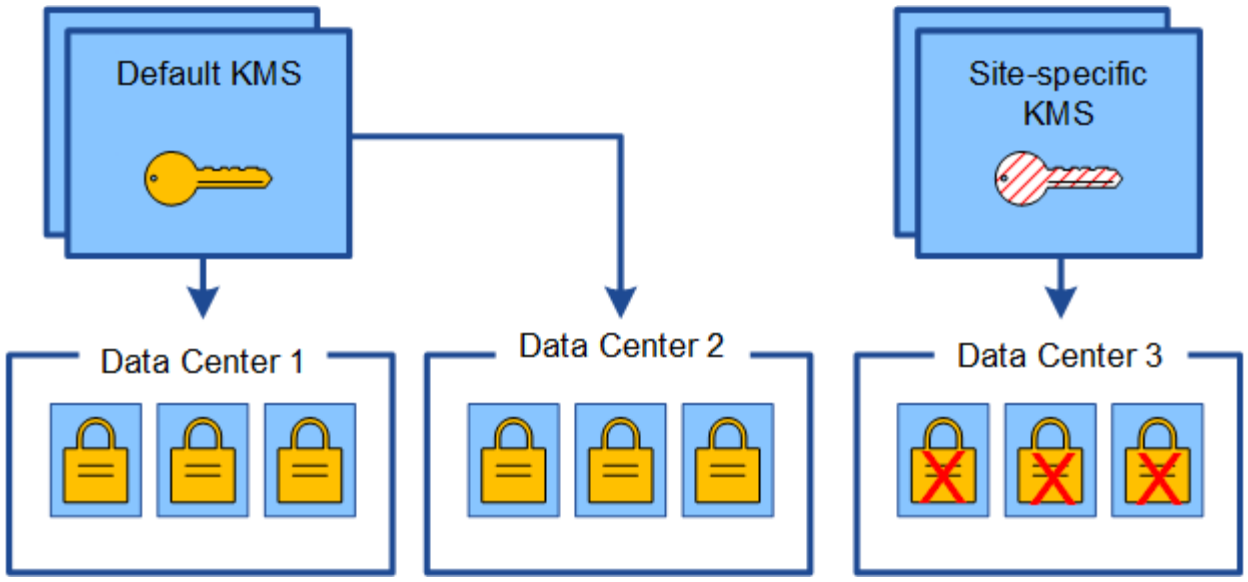
サイトで使用されている KMS を変更する場合は、そのサイトで以前に暗号化したアプライアンスノードを新しい KMS に格納されているキーを使用して復号化できることを確認する必要があります。場合によっては、暗号化キーの現在のバージョンを元の KMS から新しい KMS にコピーする必要があります。サイトで暗号化されたアプライアンスノードを復号化するために、 KMS に正しいキーがあることを確認する必要があります。

例：

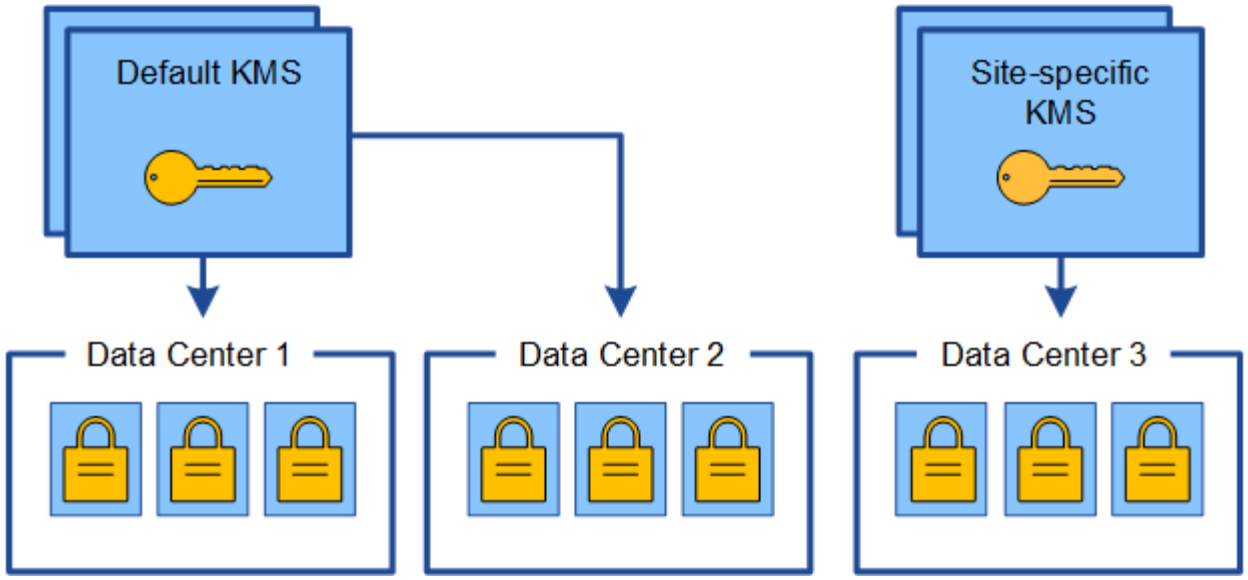
1. 最初に、専用の KMS がない環境 のすべてのサイトを設定します。
2. KMS を保存すると、「 Node Encryption * 」設定が有効になっているすべてのアプライアンスノードが KMS に接続して暗号化キーを要求します。このキーは、すべてのサイトのアプライアンスノードの暗号化に使用されます。同じキーを使用して、これらのアプライアンスを復号化する必要もあります。




3. 1 つのサイト（図のデータセンター 3 ）にサイト固有の KMS を追加することにしました。ただし、アプライアンスノードはすでに暗号化されているため、サイト固有の KMS の設定を保存しようとすると検証エラーが発生します。このエラーは、サイト固有の KMS に、そのサイトでノードを復号化するための正しいキーがないことが原因で発生します。




4. 問題 に対応するには、現在のバージョンの暗号化キーをデフォルトの KMS から新しい KMS にコピーします。（技術的には、元のキーを同じエイリアスを持つ新しいキーにコピーします。元のキーが新しいキーの前のバージョンになります）。 サイト固有の KMS に、データセンター 3 でアプライアンスノードを復号化するための正しいキーが付与されるようになり、 StorageGRID に保存できるようになりました。




サイトに使用する **KMS** を変更するユースケース

次の表に、サイトの KMS を変更する一般的なケースに必要な手順をまとめます。

| サイトの **KMS** を変更するユースケース | 必要な手順 |
| --- | --- |
| サイト固有の KMS エントリが 1 つ以上あり、それらのエントリの 1 つをデフォルトの KMS として使用する必要があります。 | サイト固有の KMS を編集します。[ * キー管理対象 * ] フィールドで、別の KMS （デフォルト KMS ）で管理されていないサイト * を選択します。サイト固有の KMS がデフォルトの KMS として使用されるようになります。専用の KMS を使用していないサイトにも適用されます。<br><br>"キー管理サーバの編集（KMS）" |
| デフォルトの KMS を使用して、拡張時に新しいサイトを追加する必要があります。新しいサイトにはデフォルトの KMS を使用しないでください。 | 1. 新しいサイトにあるアプライアンスノードがデフォルトの KMS によって暗号化済みの場合は、KMS ソフトウェアを使用して、現在のバージョンの暗号化キーをデフォルトの KMS から新しい KMS にコピーします。<br>2. Grid Manager を使用して新しい KMS を追加し、サイトを選択します。<br><br>"キー管理サーバの追加（KMS）" |

| サイトの **KMS** を変更するユースケース | 必要な手順 |
| --- | --- |
| サイトの KMS で別のサーバを使用するとします。 | 1. サイトのアプライアンスノードが既存の KMS によって暗号化済みの場合は、 KMS ソフトウェアを使用して、既存の KMS から新しい KMS に暗号化キーの現在のバージョンをコピーします。<br>2. Grid Manager を使用して既存の KMS 設定を編集し、新しいホスト名または IP アドレスを入力します。<br><br>"キー管理サーバの追加（KMS）" |

**KMS**でクライアントとして**StorageGRID** を設定する

## KMS を StorageGRID に追加する前に、各外部キー管理サーバまたは KMS クラスタのクライアントとして StorageGRID を設定する必要があります。

このタスクについて

これらの手順は、 Thales CipherTrust Manager k170v 、バージョン 2.0 、 2.1 、および 2.2 に適用されます。StorageGRID で別のキー管理サーバを使用する方法については、テクニカルサポートにお問い合わせください。

"Thales CipherTrust マネージャ"

手順

1. KMS ソフトウェアから、使用する KMS または KMS クラスタごとに StorageGRID クライアントを作成します。

   各 KMS は、 1 つのサイトまたはサイトグループにある StorageGRID アプライアンスノードの単一の暗号化キーを管理します。

2. KMS ソフトウェアから、 KMS または KMS クラスタごとに AES 暗号化キーを作成します。

   暗号化キーはエクスポート可能である必要があります。

3. KMS または KMS クラスタごとに次の情報を記録します。

   この情報は、 KMS を StorageGRID に追加するときに必要になります。

   - 各サーバのホスト名または IP アドレス。
   - KMS で使用される KMIP ポート。
   - KMS 内の暗号化キーのキーエイリアス。

   > ⓘ 暗号化キーは KMS にすでに存在している必要があります。StorageGRID は KMS キーを作成または管理しません。

4. KMS または KMS クラスタごとに、認証局（ CA ）が署名したサーバ証明書または PEM でエンコードされた各 CA 証明書ファイルを含む証明書バンドルを、証明書チェーンの順序で連結して取得します。

サーバ証明書を使用すると、外部 KMS は StorageGRID に対して自身を認証できます。

- 証明書では、 Privacy Enhanced Mail （ PEM ） Base-64 エンコード X.509 形式を使用する必要があります。
- 各サーバ証明書の Subject Alternative Name （ SAN ）フィールドには、 StorageGRID が接続する完全修飾ドメイン名（ FQDN ）または IP アドレスを含める必要があります。

> StorageGRID で KMS を設定する場合は、「 * Hostname * 」フィールドに同じ FQDN または IP アドレスを入力する必要があります。

- サーバ証明書は、 KMS の KMIP インターフェイスで使用されている証明書と一致する必要があります。通常はポート 5696 が使用されます。

5. 外部 KMS によって StorageGRID に発行されたパブリッククライアント証明書とクライアント証明書の秘密鍵を取得します。

   クライアント証明書は、 StorageGRID が KMS に対して自身を認証することを許可します。

キー管理サーバの追加（**KMS**）

## StorageGRID キー管理サーバウィザードを使用して、各 KMS または KMS クラスタを追加します。

必要なもの

- を確認しておく必要があります "キー管理サーバを使用する際の考慮事項と要件"。
- が必要です "KMS でクライアントとして StorageGRID を設定"をクリックし、KMSまたはKMSクラスタごとに必要な情報を確認しておく必要があります
- Root Access 権限が必要です。
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

このタスクについて

可能環境 であれば、サイト固有のキー管理サーバを設定してから、別の KMS で管理されていないデフォルトの KMS を設定してください。最初にデフォルトの KMS を作成すると、グリッド内のノードで暗号化されたすべてのアプライアンスがデフォルトの KMS で暗号化されます。サイト固有の KMS をあとで作成するには、まず、暗号化キーの現在のバージョンをデフォルトの KMS から新しい KMS にコピーする必要があります。

"サイトの KMS を変更する際の考慮事項"

手順

1. "手順 1 ： KMS の詳細を入力します"
2. "手順 2 ：サーバ証明書をアップロードする"
3. "手順 3 ：クライアント証明書をアップロードする"

手順 **1** ： **KMS** の詳細を入力します

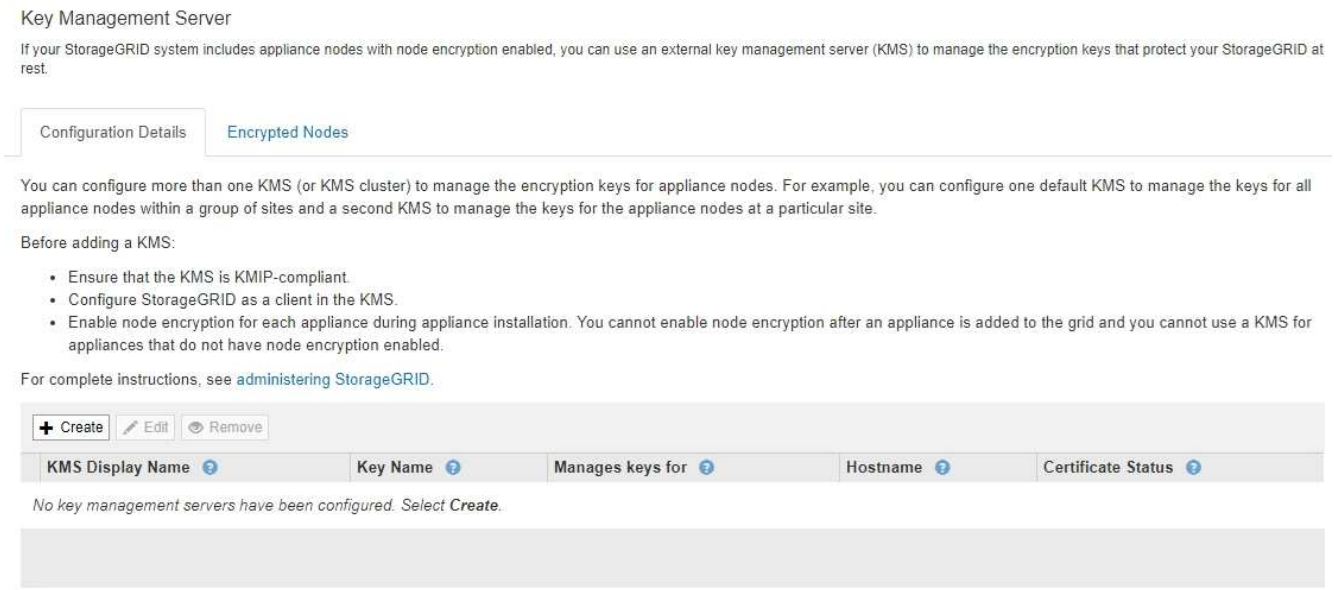
## キー管理サーバの追加ウィザードの手順 1 （ KMS の詳細を入力）で、 KMS または

# KMS クラスタの詳細を指定します。

手順

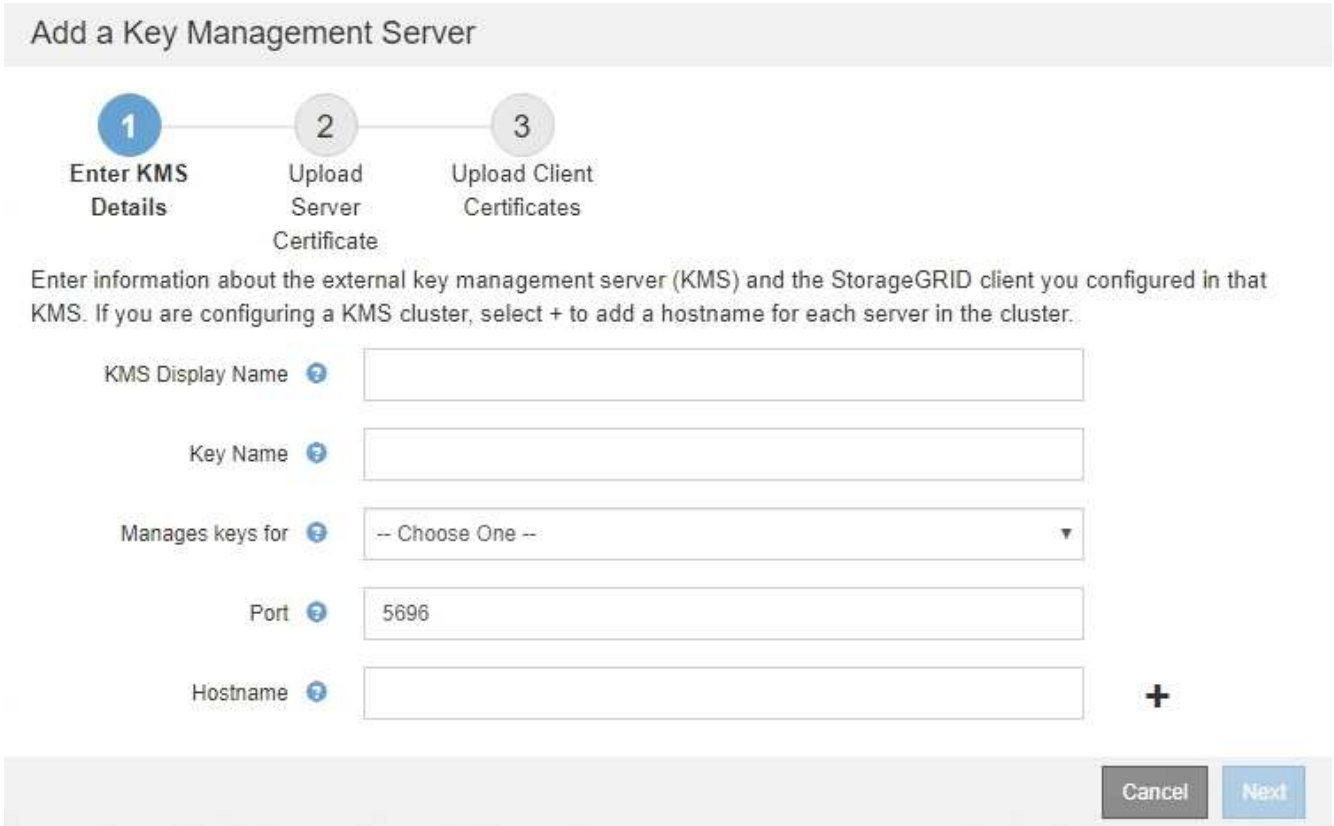
1. 「* Configuration * System Settings ** Key Management Server *」を選択します。

   [Key Management Server] ページが表示され、 [Configuration] [Details] タブが選択されます。




2. 「 * Create * 」を選択します。

   Add a Key Management Server （キー管理サーバの追加）ウィザードの手順 1 （ KMS の詳細を入力）が表示されます。



3. KMS および設定した StorageGRID クライアントの情報を KMS で入力します。

| フィールド | 説明 |
| --- | --- |
| KMS 表示名 | この KMS を特定するのに役立つわかりやすい名前。1~64 文字で指定します。 |
| キー名 | KMS 内の StorageGRID クライアントの正確なキーエイリアス。1~255 文字で指定する必要があります。 |
| のキーを管理します | この KMS に関連する StorageGRID サイトを参照してください。可能であれば、サイト固有のキー管理サーバを設定してから、環境 で他の KMS で管理されていないすべてのサイトをデフォルトの KMS で設定する必要があります。<br>• 特定のサイトのアプライアンスノードの暗号化キーをこの KMS で管理する場合は、サイトを選択します。<br>• 「 * Sites not managed by another KMS （デフォルト KMS ） * 」を選択して、専用の KMS とその後の拡張で追加したサイトに適用されるデフォルトの KMS を設定します。<br>◦ 注： * 以前にデフォルト KMS で暗号化されていたサイトを選択しても、新しい KMS に元の暗号化キーの現在のバージョンを提供しなかった場合、 KMS の設定を保存すると、検証エラーが発生します。 |
| ポート | KMS サーバが Key Management Interoperability Protocol （ KMIP ）の通信に使用するポート。デフォルトでは、 KMIP 標準ポートである 5696 が使用されます。 |
| ホスト名 | KMS の完全修飾ドメイン名または IP アドレス。<br>• 注： * サーバ証明書の SAN フィールドには、ここに入力する FQDN または IP アドレスを含める必要があります。そうしないと、StorageGRID は KMS クラスタ内のすべてのサーバに接続できなくなります。 |

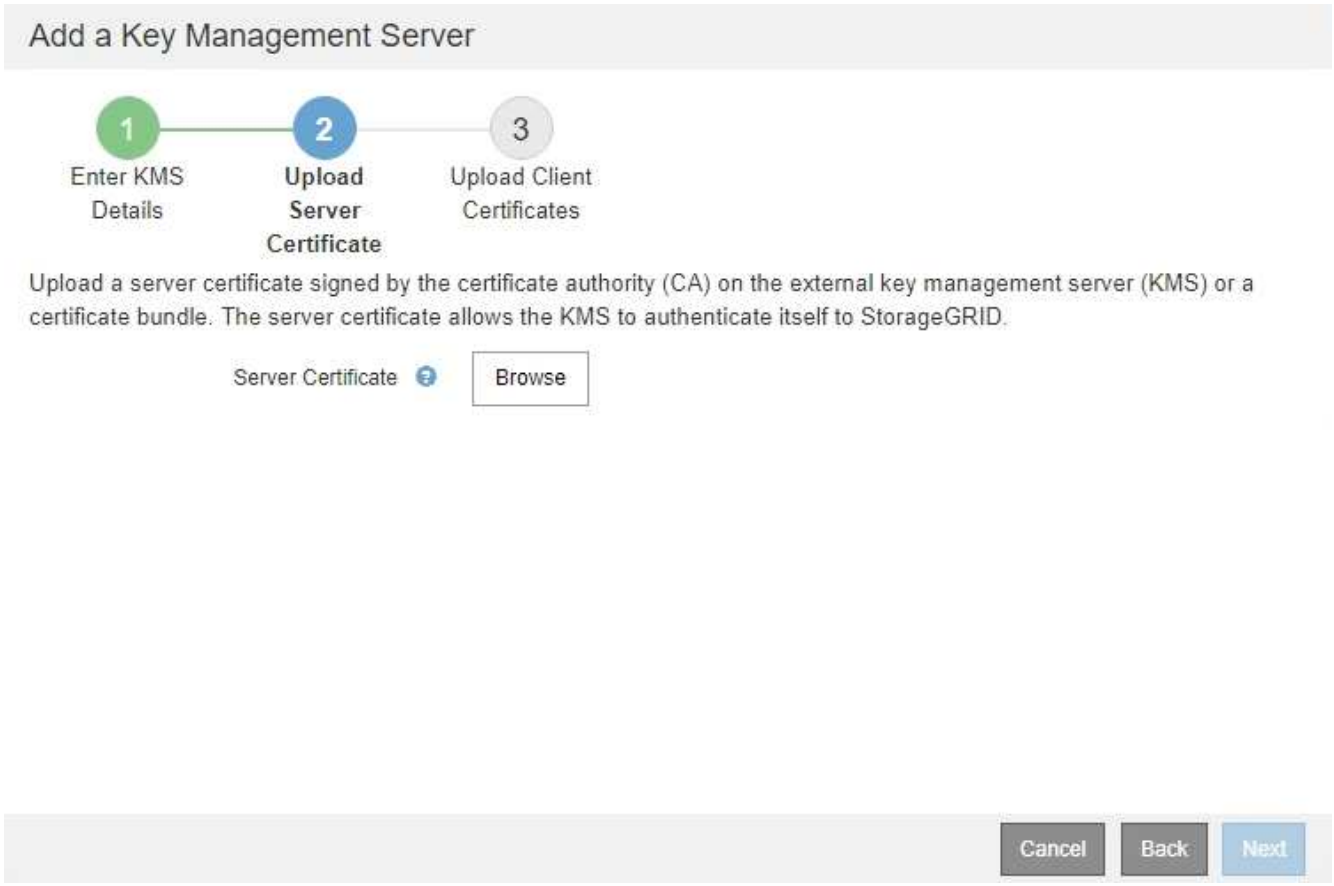
4. KMS クラスタを使用している場合は、プラス記号を選択します ➕ クラスタ内の各サーバのホスト名を追加します。
5. 「 * 次へ * 」を選択します。

   キー管理サーバの追加ウィザードの手順2（サーバ証明書をアップロード）が表示されます。

キー管理サーバの追加ウィザードの手順 2 （サーバ証明書をアップロード）で、 KMS のサーバ証明書（または証明書バンドル）をアップロードします。サーバ証明書を使用すると、外部 KMS は StorageGRID に対して自身を認証できます。

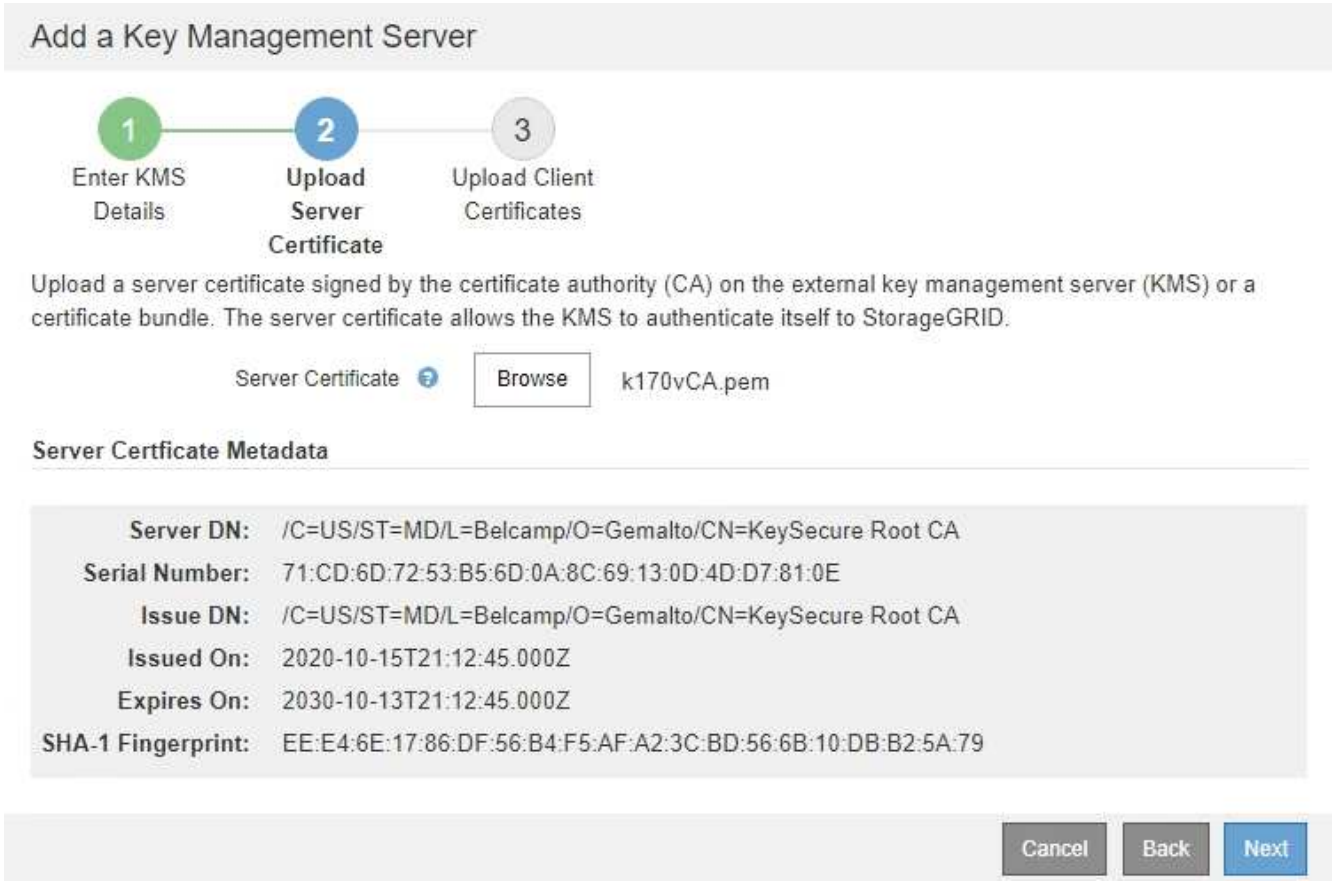
手順

1. 手順 2 （サーバー証明書のアップロード） * から、保存されているサーバー証明書または証明書バンドルの場所を参照します。




2. 証明書ファイルをアップロードします。

   サーバ証明書のメタデータが表示されます。




証明書バンドルをアップロードした場合は、各証明書のメタデータが独自のタブに表示されます。

3. 「 * 次へ * 」を選択します。

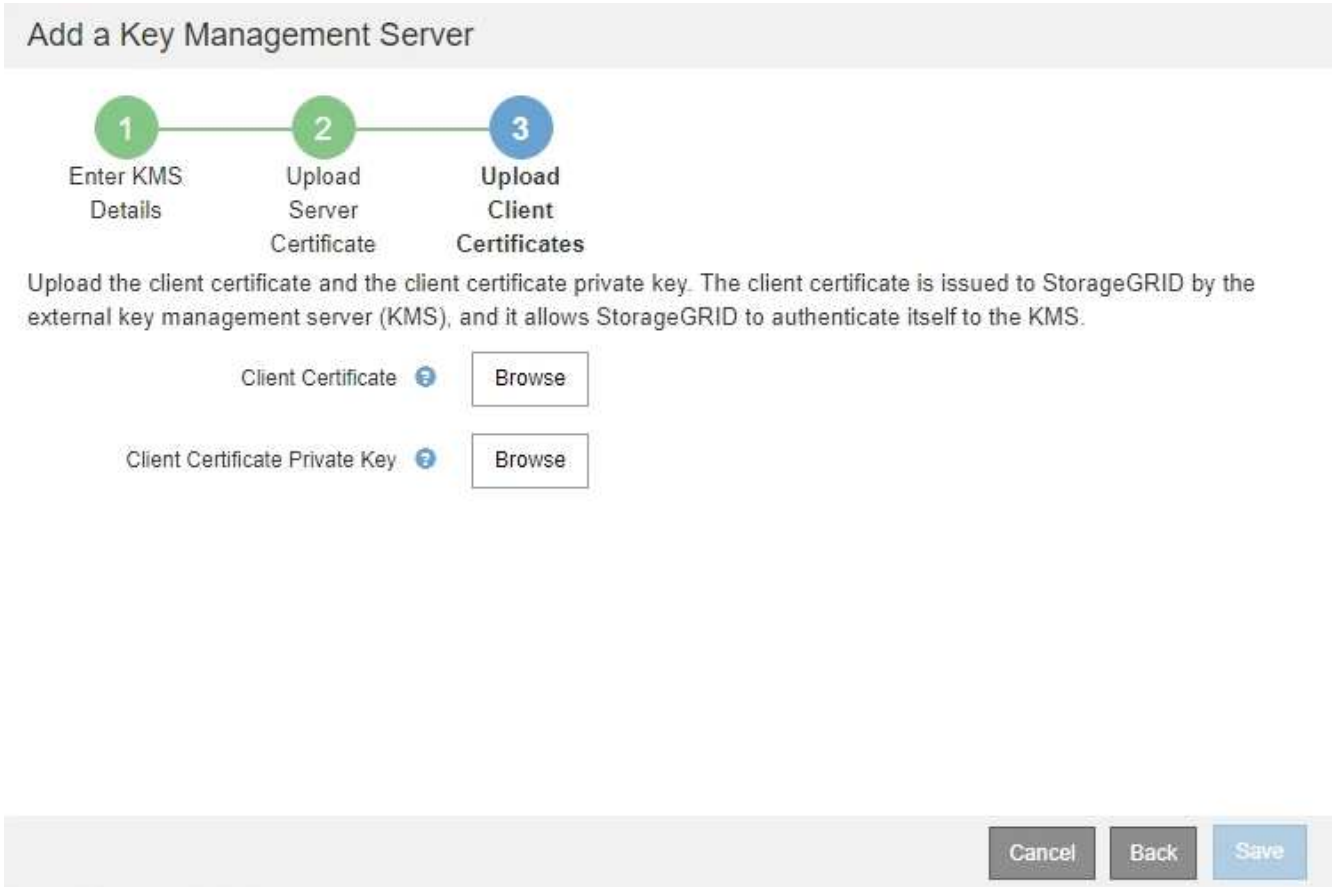
   Add a Key Management Serverウィザードの手順3（クライアント証明書をアップロード）が表示されます。

手順 **3** ：クライアント証明書をアップロードする

キー管理サーバの追加ウィザードの手順 3 （クライアント証明書をアップロード）で、クライアント証明書とクライアント証明書の秘密鍵をアップロードします。クライアント証明書は、 StorageGRID が KMS に対して自身を認証することを許可します。

手順

1. * 手順 3 （クライアント証明書をアップロード） * から、クライアント証明書の場所を参照します。

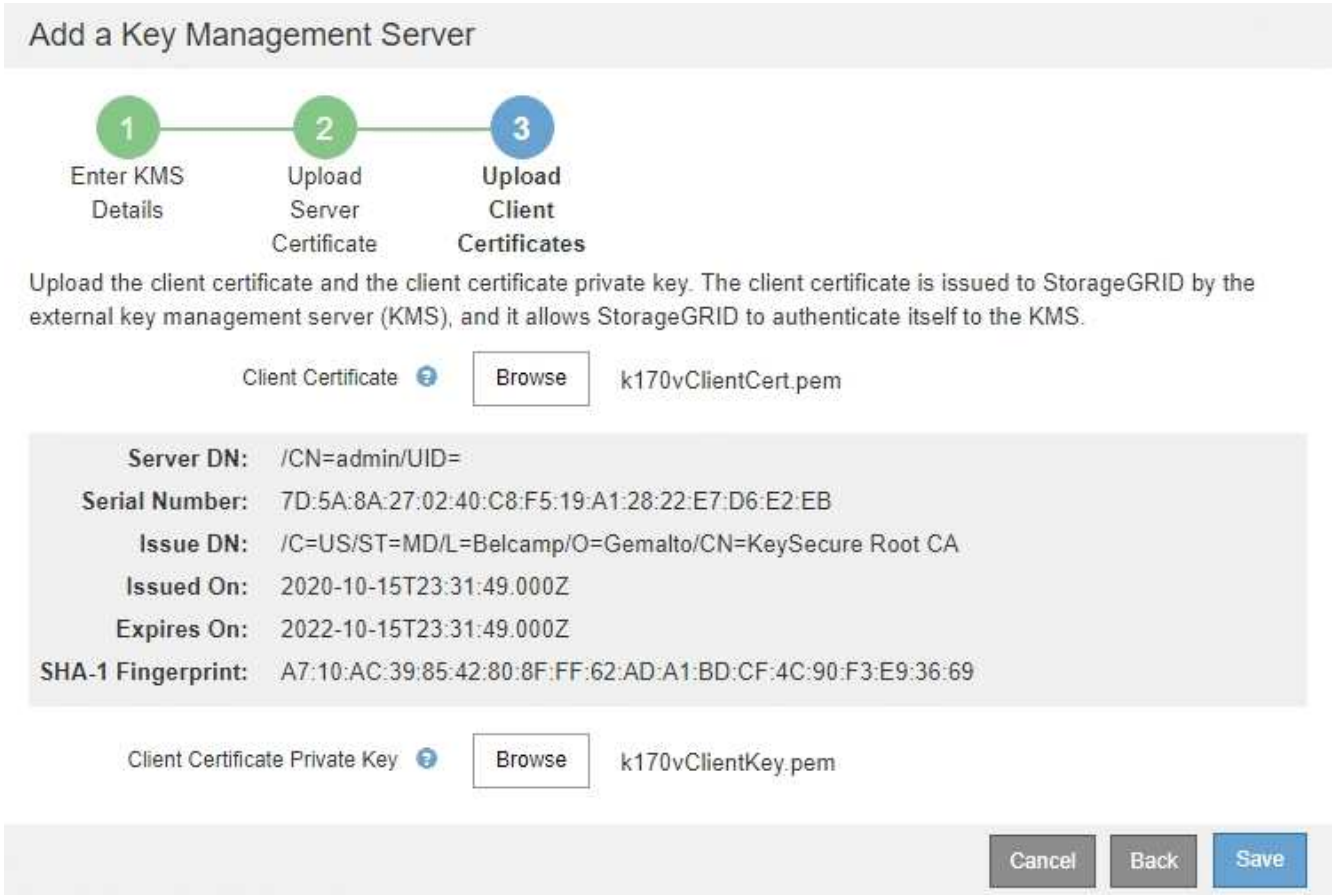



2. クライアント証明書ファイルをアップロードします。

   クライアント証明書のメタデータが表示されます。

3. クライアント証明書の秘密鍵の場所を参照します。
4. 秘密鍵ファイルをアップロードします。

   クライアント証明書とクライアント証明書の秘密鍵のメタデータが表示されます。




5. [ 保存（ Save ） ] を選択します。

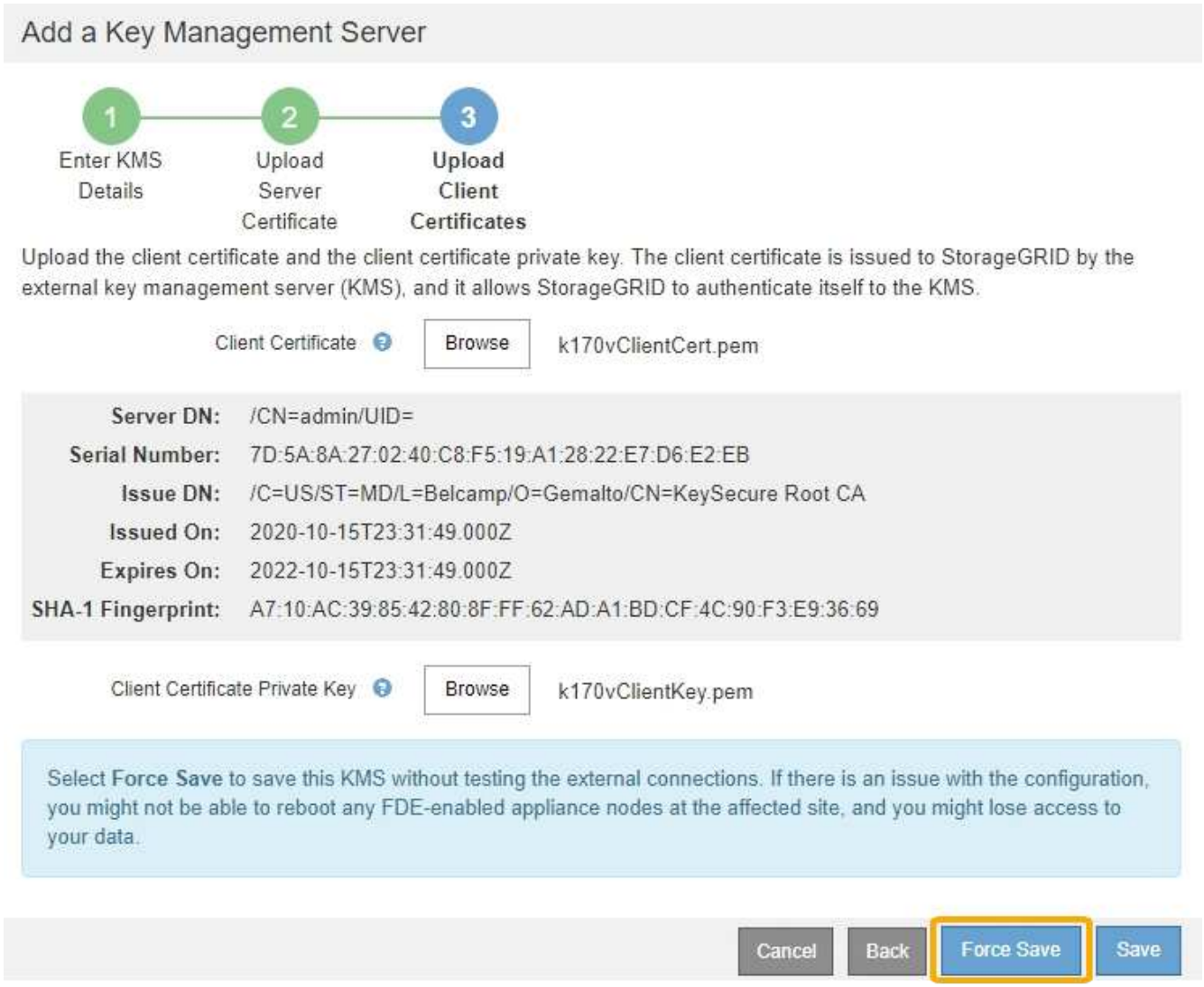
   キー管理サーバとアプライアンスノードの間の接続をテストします。すべての接続が有効で、正しいキーが KMS にある場合は、新しいキー管理サーバが Key Management Server ページの表に追加されます。

   > KMS を追加すると、すぐに [Key Management Server] ページの証明書ステータスが [Unknown （不明） ] と表示されます。各証明書の実際のステータスの StorageGRID 取得には 30 分程度かかる場合があります。最新のステータスを表示するには、 Web ブラウザの表示を更新する必要があります。

6. 「 * Save * （保存）」を選択したときにエラーメッセージが表示された場合は、メッセージの詳細を確認し、「 * OK * 」を選択します。

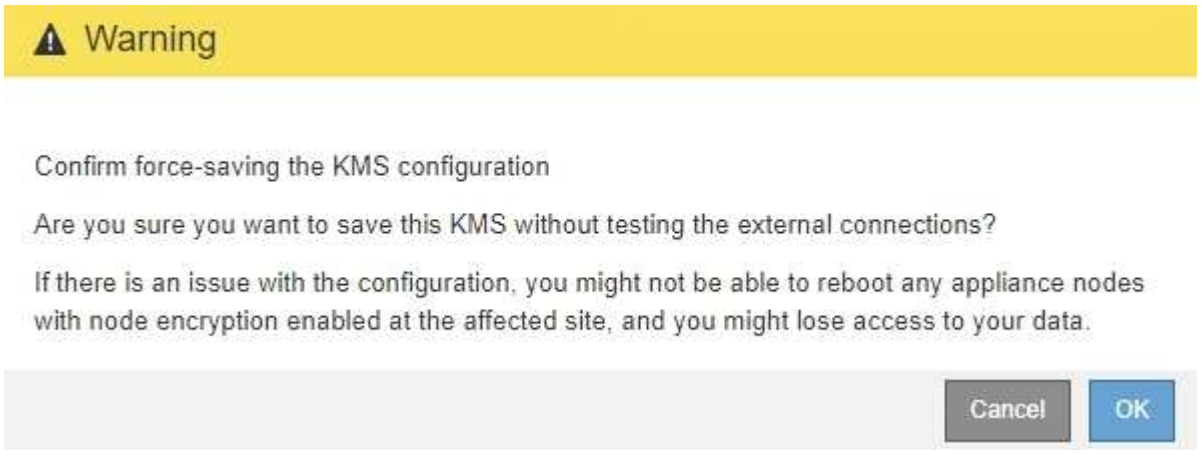
   たとえば、接続テストに失敗した場合は、 422 ： Unprocessable Entity エラーが返されることがあります。

7. 外部接続をテストせずに現在の設定を保存する必要がある場合は、 * 強制保存 * を選択します。




[ 強制保存 ] を選択すると KMS の設定が保存されますが、各アプライアンスからその KMS への外部接続はテストされません。構成を含む問題 がある場合、該当するサイトでノード暗号化が有効になっているアプライアンスノードをリブートできない可能性があります。問題が解決するまでデータにアクセスできなくなる可能性があります。

8. 確認の警告を確認し、設定を強制的に保存する場合は、「 * OK 」を選択します。



KMS の設定は保存されますが、 KMS への接続はテストされません。

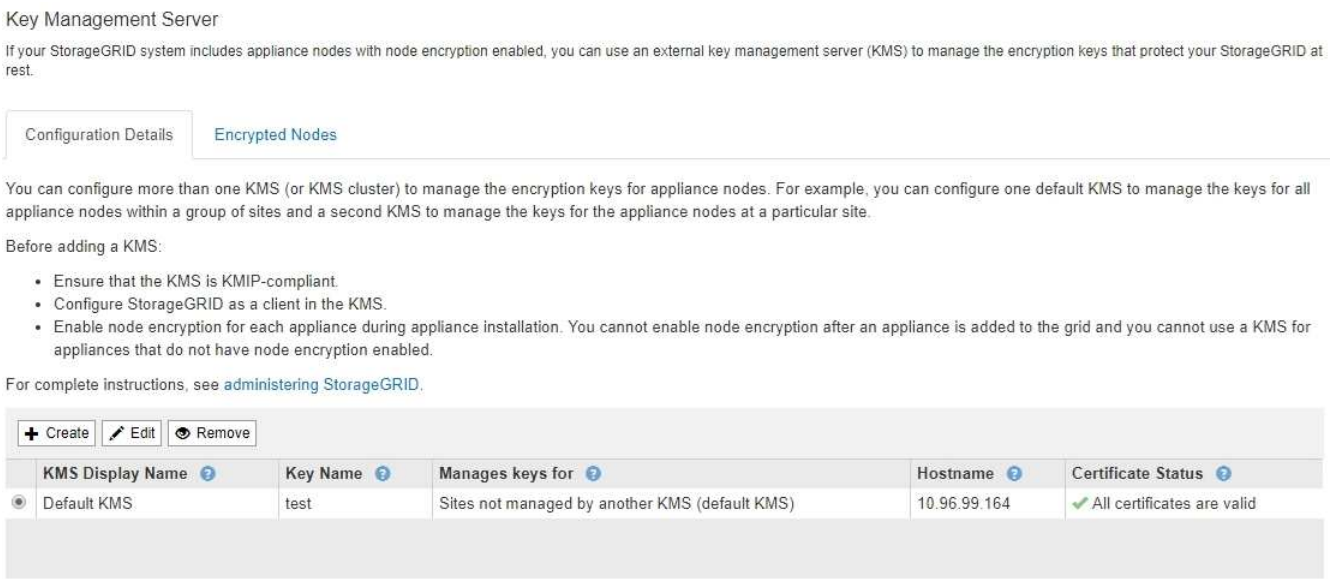
### KMSの詳細を確認する

StorageGRID システム内の各キー管理サーバ（ KMS ）に関する情報を確認することができます。これには、サーバ証明書とクライアント証明書の現在のステータスも含まれます。

手順

1. 「* Configuration * System Settings ** Key Management Server *」を選択します。

   [Key Management Server] ページが表示されます。Configuration Details タブには、設定されているすべてのキー管理サーバが表示されます。




2. 各 KMS について、表の情報を確認します。

| フィールド | 説明 |
| --- | --- |
| KMS 表示名 | KMS の説明的な名前。 |
| キー名 | KMS 内の StorageGRID クライアントのキーエイリアス。 |
| のキーを管理します | KMS に関連付けられている StorageGRID サイト。<br><br>このフィールドには、特定の StorageGRID サイトの名前、または別の KMS （デフォルト KMS ）で管理されていないサイト * が表示されます |

| フィールド | 説明 |
| --- | --- |
| ホスト名 | KMS の完全修飾ドメイン名または IP アドレス。<br><br>2 台のキー管理サーバからなるクラスタがある場合は、両方のサーバの完全修飾ドメイン名または IP アドレスが表示されます。クラスタに複数のキー管理サーバがある場合は、最初の KMS の完全修飾ドメイン名または IP アドレスと、クラスタ内の追加のキー管理サーバの数が表示されます。<br><br>例： `10.10.10.10 and 10.10.10.11` または `10.10.10.10 and 2 others`。<br><br>クラスタ内のすべてのホスト名を表示するには、KMS を選択して「 * Edit * 」を選択します。 |
| 証明書のステータス | サーバ証明書、オプションの CA 証明書、およびクライアント証明書の現在の状態：有効、期限が切れている、期限が近づいている、または不明。<br><br>• 注： StorageGRID * 証明書のステータスが更新されるまで 30 分程度かかる場合があります。現在の値を表示するには、 Web ブラウザの表示を更新する必要があります。 |

3. 証明書のステータスが不明の場合は、 30 分ほど待ってから Web ブラウザを更新してください。

> KMS を追加すると、すぐに [Key Management Server] ページの証明書ステータスが [Unknown （不明） ] と表示されます。各証明書の実際のステータスの StorageGRID 取得には 30 分程度かかる場合があります。実際のステータスを確認するには、 Web ブラウザの表示を更新する必要があります。

4. 証明書のステータス列に、証明書の有効期限が切れている、または有効期限が近づいていることが示されている場合は、できるだけ早く問題 に対処してください。

   StorageGRID の監視とトラブルシューティングの手順で、* KMS CA証明書の有効期限*、* KMSクライアント証明書の有効期限*、および* KMSサーバ証明書の有効期限*アラートの推奨される対処方法を参照してください。

> データアクセスを維持するために、証明書の問題はできるだけ早く対処する必要があります。

関連情報

"トラブルシューティングを監視します"

暗号化されたノードの表示

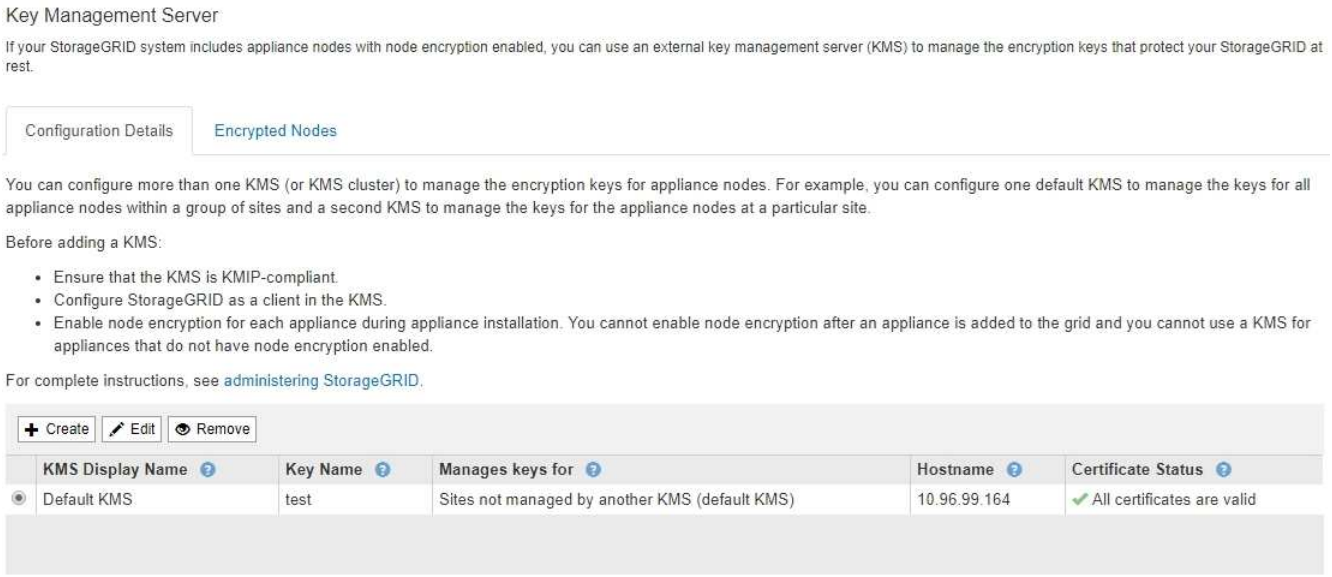
## StorageGRID システムでノード暗号化 * 設定が有効になっているアプライアンスノード

に関する情報を表示できます。

手順

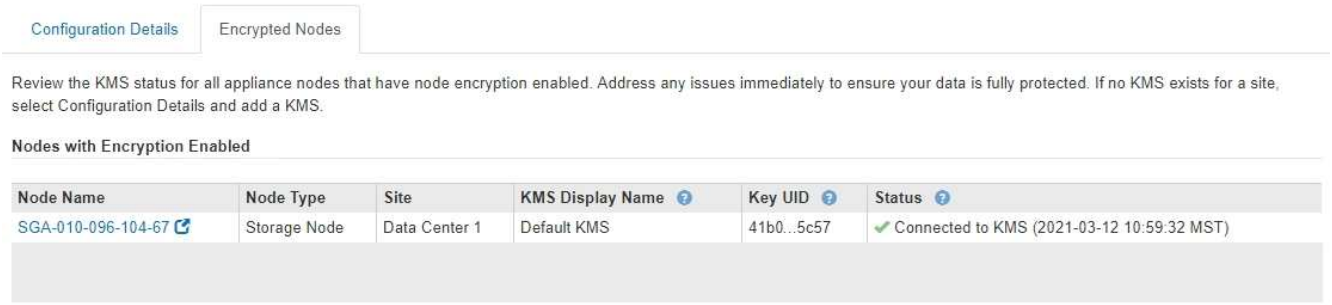
1. 「* Configuration * System Settings ** Key Management Server *」を選択します。

   [Key Management Server] ページが表示されます。Configuration Details タブには、設定済みのすべてのキー管理サーバが表示されます。




2. ページの上部から、 [* 暗号化されたノード * ] タブを選択します。

   [Encrypted Nodes] タブには、 StorageGRID システムでノード暗号化 * 設定が有効になっているアプライアンスノードが表示されます。




3. 各アプライアンスノードについて、表の情報を確認します。

| 列（**Column**） | 説明 |
| --- | --- |
| ノード名 | アプライアンスノードの名前。 |
| ノードタイプ（ Node Type ） | ノードのタイプ。 Storage 、 Admin 、または Gateway 。 |
| サイト | ノードがインストールされている StorageGRID サイトの名前。 |
| KMS 表示名 | ノードに使用される KMS の説明的な名前。<br><br>KMS が表示されていない場合は '[ 構成の詳細 ] タブを選択して KMS を追加します<br><br>"キー管理サーバの追加（KMS）" |
| キー UID | アプライアンスノードでデータの暗号化と復号化に使用する暗号化キーの一意の ID 。キー UID 全体を表示するには、セルにカーソルを合わせます。<br><br>ダッシュ（ - - ）は、キー UID が不明であることを示します。アプライアンスノードと KMS 間の接続問題 が原因である可能性があります。 |
| ステータス | KMS とアプライアンスノード間の接続のステータス。ノードが接続されている場合は、タイムスタンプが 30 分ごとに更新されます。KMS の設定変更後に接続ステータスが更新されるまで数分かかることがあります。<br><br>• 注： * 新しい値を表示するには、 Web ブラウザを更新する必要があります。 |

4. ステータス列に KMS 問題 と表示されている場合は、問題 にすぐに対処してください。

   通常の KMS 操作中、ステータスは * KMS * に接続されます。ノードがグリッドから切断されると、ノードの接続状態が（意図的に停止しているか不明である）と表示されます。

   その他のステータスメッセージは、同じ名前の StorageGRID アラートに対応します。

   ◦ KMS の設定をロードできませんでした
   ◦ KMS 接続エラー
   ◦ KMS 暗号化キー名が見つかりません
   ◦ KMS 暗号化キーのローテーションに失敗しました
   ◦ KMS キーでアプライアンスボリュームを復号化できませんでした
   ◦ KMSが構成されていませんStorageGRID の監視とトラブルシューティングの手順で、これらのアラートに対する推奨される対処方法を確認してください。

問題が発生した場合は、データを完全に保護するために、すぐに対処する必要があります。

関連情報

"トラブルシューティングを監視します"

キー管理サーバの編集（**KMS**）

# 証明書の有効期限が近づいている場合など、キー管理サーバの設定の編集が必要になることがあります。

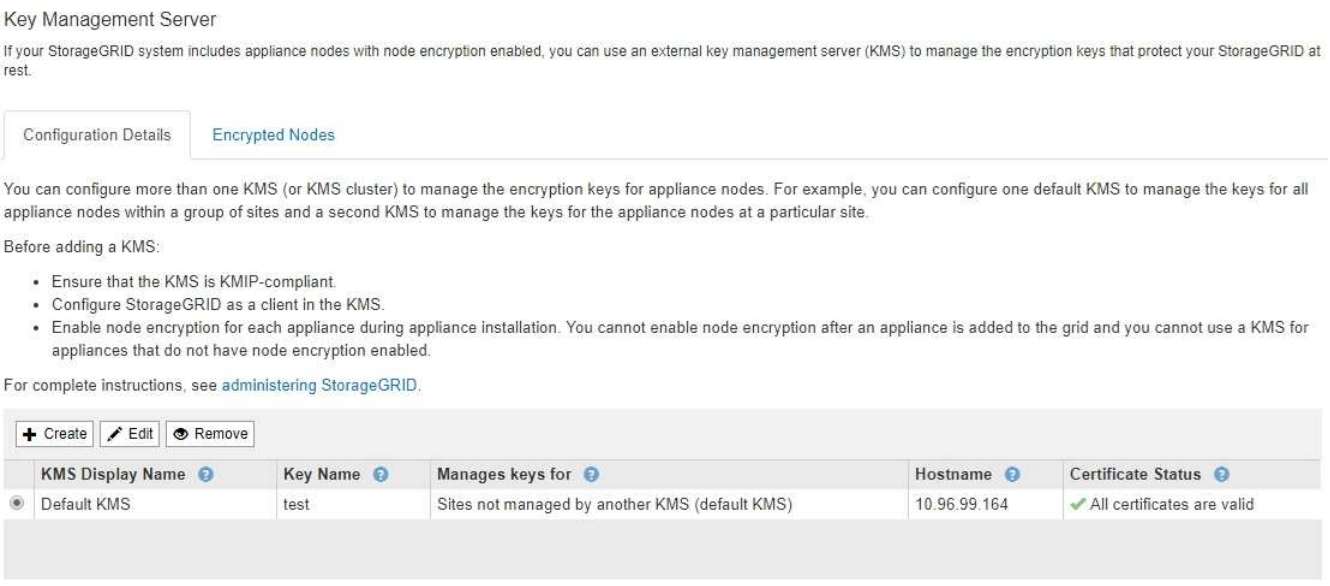
必要なもの

- を確認しておく必要があります "キー管理サーバを使用する際の考慮事項と要件"。
- KMS用に選択したサイトを更新する予定がある場合は、を確認しておく必要があります "サイトの KMS を変更する際の考慮事項"。
- Root Access 権限が必要です。
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

手順

1. 「* Configuration * System Settings ** Key Management Server *」を選択します。

   Key Management Server ページが表示され、設定済みのすべてのキー管理サーバが表示されます。




2. 編集する KMS を選択し、「 * 編集」を選択します。
3. 必要に応じて、キー管理サーバの編集ウィザードの * 手順 1 （ KMS の詳細を入力） * で詳細を更新します。

| フィールド | 説明 |
| --- | --- |
| KMS 表示名 | この KMS を特定するのに役立つわかりやすい名前。1~64 文字で指定します。 |
| キー名 | KMS 内の StorageGRID クライアントの正確なキーエイリアス。1~255 文字で指定する必要があります。<br><br>キー名の編集が必要になることはほとんどありません。たとえば、エイリアスの名前が KMS で変更された場合や、以前のキーのすべてのバージョンが新しいエイリアスのバージョン履歴にコピーされている場合は、キー名を編集する必要があります。<br><br>KMS のキー名 ( エイリアス ) を変更して、キーの回転を試みないでください。代わりに、 KMS ソフトウェアのキーバージョンを更新してキーをローテーションしてください。StorageGRID では、以前に使用されていたすべてのキーバージョン（および今後使用するすべてのバージョン）に、同じキーエイリアスを使用して KMS からアクセスできることが必要です。設定されている KMS のキーエイリアスを変更すると、StorageGRID がデータを復号化できなくなる可能性があります。<br><br>"キー管理サーバを使用する際の考慮事項と要件" |
| のキーを管理します | サイト固有の KMS を編集していて ' デフォルトの KMS がまだない場合は ' オプションで ' 別の KMS ( デフォルト KMS ) で管理されていないサイト * を選択しますこの選択により、サイト固有の KMS がデフォルトの KMS に変換されます。これは、専用の KMS を持たないすべてのサイトと、拡張時に追加されたサイトに適用されます。<br><br>• 注： * サイト固有の KMS を編集している場合、別のサイトを選択することはできません。デフォルトの KMS を編集する場合は ' 特定のサイトを選択することはできません |
| ポート | KMS サーバが Key Management Interoperability Protocol （ KMIP ）の通信に使用するポート。デフォルトでは、 KMIP 標準ポートである 5696 が使用されます。 |
| ホスト名 | KMS の完全修飾ドメイン名または IP アドレス。<br><br>• 注： * サーバ証明書の SAN フィールドには、ここに入力する FQDN または IP アドレスを含める必要があります。そうしないと、 StorageGRID は KMS クラスタ内のすべてのサーバに接続できなくなります。 |

4. KMS クラスタを構成する場合は、プラス記号を選択します ➕ クラスタ内の各サーバのホスト名を追加します。
5. 「 * 次へ * 」を選択します。

キー管理サーバの編集ウィザードの手順 2 （サーバ証明書をアップロード）が表示されます。

6. サーバー証明書を置き換える必要がある場合は、 * 参照 * を選択して新しいファイルをアップロードします。
7. 「 * 次へ * 」を選択します。

   キー管理サーバの編集ウィザードの手順 3 （クライアント証明書をアップロード）が表示されます。

8. クライアント証明書とクライアント証明書の秘密鍵を置き換える必要がある場合は、 * 参照 * を選択して新しいファイルをアップロードします。
9. [ 保存（ Save ） ] を選択します。

   キー管理サーバと影響を受けるサイトのすべてのノード暗号化アプライアンスノードの間の接続をテストします。すべてのノード接続が有効で、 KMS に正しいキーがある場合は、キー管理サーバが Key Management Server ページの表に追加されます。

10. エラーメッセージが表示された場合は、メッセージの詳細を確認し、「 * OK * 」を選択します。

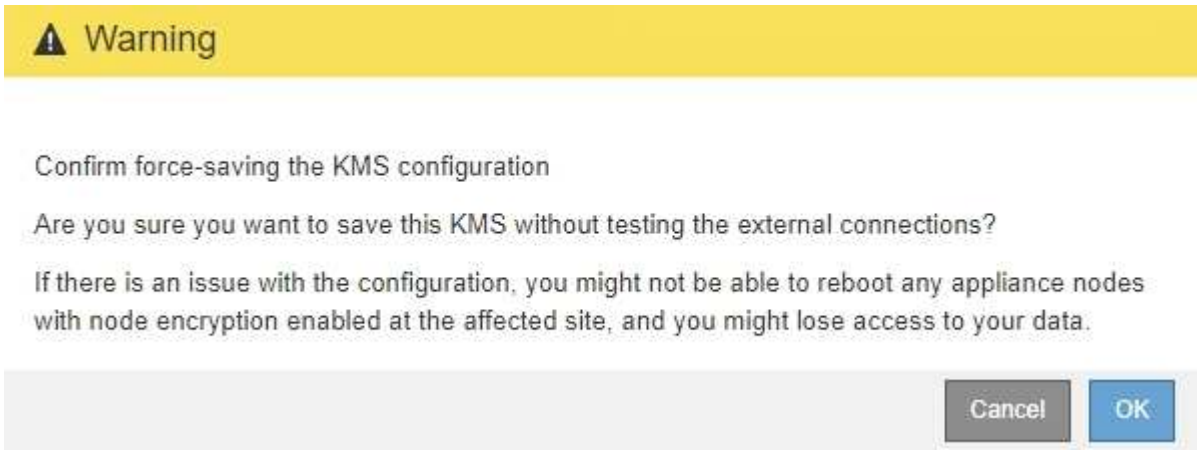
    たとえば、この KMS 用に選択したサイトが別の KMS によってすでに管理されている場合や、接続テストに失敗した場合は、「 422 ： Unprocessable Entity 」というエラーが表示されます。

11. 接続エラーを解決する前に現在の設定を保存する必要がある場合は、 * 強制保存 * を選択します。

    [ 強制保存 ] を選択すると KMS の設定が保存されますが、各アプライアンスからその KMS への外部接続はテストされません。構成を含む問題 がある場合、該当するサイトでノード暗号化が有効になっているアプライアンスノードをリブートできない可能性があります。問題が解決するまでデータにアクセスできなくなる可能性があります。

    KMS の設定が保存されます。

12. 確認の警告を確認し、設定を強制的に保存する場合は、「 * OK 」を選択します。




KMS の設定は保存されますが、 KMS への接続はテストされません。

キー管理サーバの削除（**KMS**）

場合によっては、キー管理サーバの削除が必要になることがあります。たとえば、サイ

トの運用を停止した場合は、サイト固有の KMS を削除できます。

必要なもの

- を確認しておく必要があります "キー管理サーバを使用する際の考慮事項と要件"。
- Root Access 権限が必要です。
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

このタスクについて

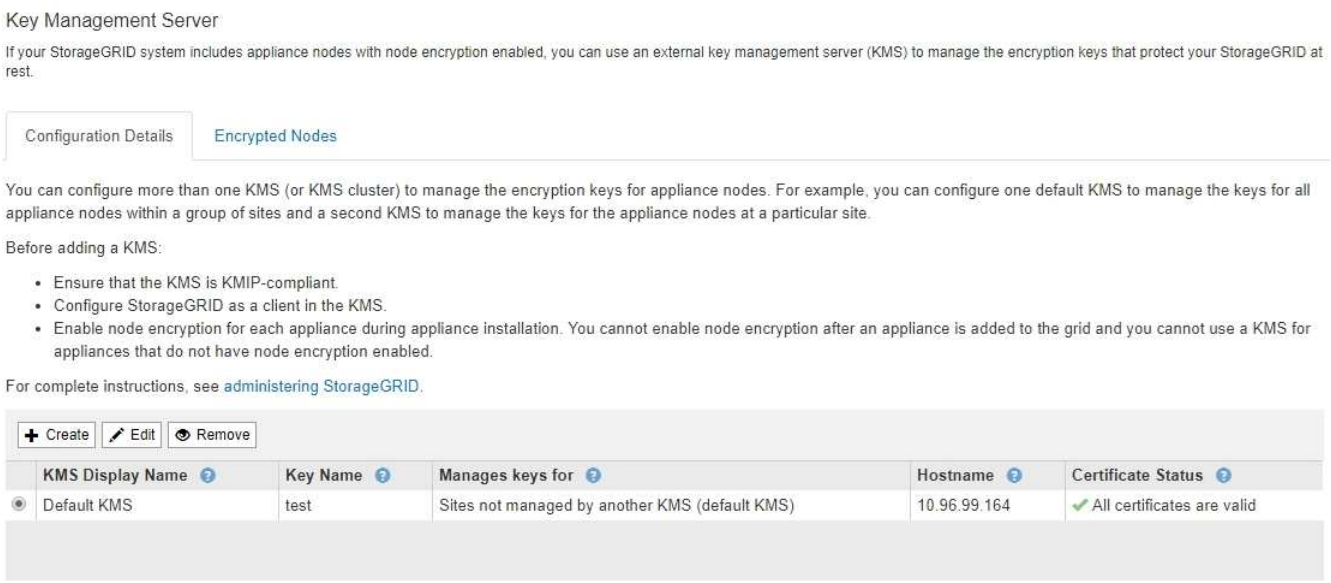
KMS は以下の場合に削除できます。

- サイトの運用が停止された場合や、ノードの暗号化が有効なアプライアンスノードがサイトに含まれていない場合は、サイト固有の KMS を削除できます。
- ノード暗号化が有効なアプライアンスノードがあるサイトごとにサイト固有の KMS がすでに存在する場合は、デフォルトの KMS を削除できます。

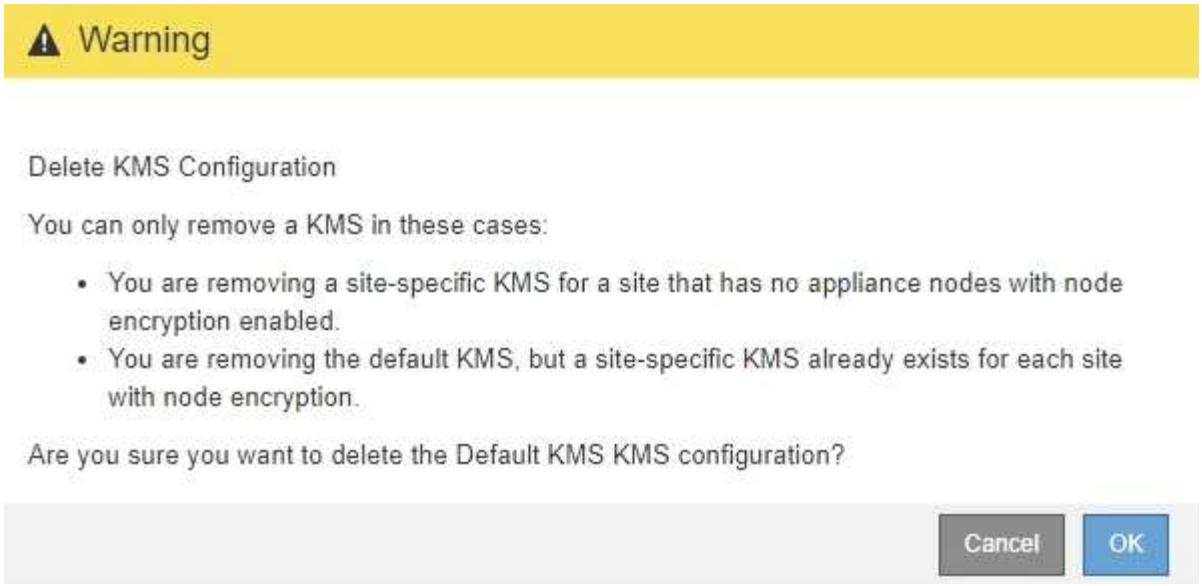
手順

1. 「* Configuration * System Settings ** Key Management Server *」を選択します。

   Key Management Server ページが表示され、設定済みのすべてのキー管理サーバが表示されます。




2. 削除する KMS のラジオボタンを選択し、「 * Remove * 」を選択します。
3. 警告ダイアログで考慮事項を確認します。




4. 「 * OK 」を選択します。

KMS の設定は削除されます。

## テナントの管理

グリッド管理者は、 S3 および Swift クライアントがオブジェクトの格納と読み出し、ストレージ使用状況の監視、および StorageGRID システムを使用してクライアントが実行できる操作の管理に使用するテナントアカウントを作成して管理します。

### テナントアカウントとは

テナントアカウントは、 Simple Storage Service （ S3 ） REST API または Swift REST API を使用するクライアントアプリケーションが、 StorageGRID でオブジェクトの格納や読み出しを行うことを可能にします。

各テナントアカウントで使用できるプロトコルは 1 つで、アカウントの作成時に指定します。両方のプロトコルを使用して StorageGRID システムにオブジェクトの格納や読み出しを行うには、テナントアカウントを 2 つ作成する必要があります。 1 つは S3 バケットとオブジェクト用、もう 1 つは Swift コンテナとオブジェクト用です。各テナントアカウントには、専用のアカウント ID 、許可されたグループとユーザ、バケットまたはコンテナ、およびオブジェクトがあります。

必要に応じて、システムに格納されているオブジェクトをエンティティごとに分ける場合は、追加のテナントアカウントを作成します。たとえば、次のようなユースケースでは複数のテナントアカウントをセットアップできます。

- * エンタープライズのユースケース：エンタープライズアプリケーションで StorageGRID システムを管理する場合は、組織内の部門ごとにグリッドのオブジェクトストレージを分離する必要があります。この場合は、マーケティング部門、カスタマーサポート部門、人事部門などのテナントアカウントを作成できます。

> S3 クライアントプロトコルを使用する場合は、 S3 バケットとバケットポリシーを使用してエンタープライズ内の部門間でオブジェクトを分離できます。テナントアカウントを使用する必要はありません。詳細については、 S3 クライアントアプリケーションを実装する手順を参照してください。

- * サービスプロバイダのユースケース：サービスプロバイダとして StorageGRID システムを管理する場合は、グリッド上のストレージをリースするエンティティごとにグリッドのオブジェクトストレージを分離できます。この場合は、 A 社、 B 社、 C 社などのテナントアカウントを作成します。

テナントアカウントを作成および設定する

テナントアカウントを作成する際には次の情報を指定します。

- テナントアカウントの表示名。
- テナントアカウントで使用されるクライアントプロトコル（ S3 または Swift ）。
- S3 テナントアカウントの場合：テナントアカウントに S3 バケットでプラットフォームサービスを使用する権限があるかどうか。テナントアカウントにプラットフォームサービスの使用を許可する場合は、プラットフォームサービスを使用できるようグリッドを設定する必要があります。「プラットフォームサービスの管理」を参照してください。
- 必要に応じて、テナントアカウントのストレージクォータ — テナントのオブジェクトで使用可能な最大ギガバイト数、テラバイト数、ペタバイト数。クォータを超過すると、テナントは新しいオブジェクトを作成できなくなります。

> テナントのストレージクォータは、物理容量（ディスクのサイズ）ではなく、論理容量（オブジェクトのサイズ）を表します。

- StorageGRID システムでアイデンティティフェデレーションが有効になっている場合は、テナントアカウントを設定するための Root Access 権限が割り当てられているフェデレーテッドグループ。
- StorageGRID システムでシングルサインオン（ SSO ）が使用されていない場合は、テナントアカウントが独自のアイデンティティソースを使用するか、グリッドのアイデンティティソースを共有するか、およびテナントのローカル root ユーザの初期パスワード。

テナントアカウントが作成されたら、次のタスクを実行できます。

- * グリッドのプラットフォームサービスの管理 * ：テナントアカウントでプラットフォームサービスを有効にする場合は、プラットフォームサービスメッセージの配信方法と、 StorageGRID 環境でプラットフォームサービスを使用する際のネットワーク要件を理解しておく必要があります。
- * テナントアカウントのストレージ使用状況を監視 * ：テナントがアカウントの使用を開始したら、 Grid Manager を使用して各テナントが消費するストレージ容量を監視できます。

  テナントにクォータを設定している場合は、「テナントクォータ使用率が高い * 」アラートを有効にして、テナントがクォータを消費しているかどうかを確認できます。有効にすると、テナントのクォータの 90% が使用されたときにこのアラートがトリガーされます。詳細については、 StorageGRID の監視とトラブルシューティングの手順にあるアラートリファレンスを参照してください。

- * クライアント処理の設定 * ：一部のタイプのクライアント処理が禁止されているかどうかを設定できます。

**S3**テナントを設定する

S3 テナントアカウントが作成されたら、テナントユーザは Tenant Manager にアクセスして次のようなタスクを実行できます。

- アイデンティティフェデレーションの設定（グリッドとアイデンティティソースを共有する場合を除く）、およびローカルグループとユーザの作成

- S3 アクセスキーの管理
- S3 バケットの作成と管理を行う
- ストレージ使用状況を監視しています
- プラットフォームサービスの使用（有効な場合）

S3 テナントユーザは、 Tenant Manager を使用して S3 アクセスキーとバケットを作成および管理できますが、オブジェクトを取り込みおよび管理するには S3 クライアントアプリケーションを使用する必要があります。

**Swift**テナントを設定します

Swift テナントアカウントが作成されたら、テナントの root ユーザは Tenant Manager にアクセスして次のようなタスクを実行できます。

- アイデンティティフェデレーションの設定（グリッドとアイデンティティソースを共有する場合を除く）、およびローカルグループとユーザの作成
- ストレージ使用状況を監視しています

Swift ユーザが Tenant Manager にアクセスするには、 Root Access 権限が必要です。ただし Root Access 権限では、 Swift REST API に認証してコンテナを作成したりオブジェクトを取り込んだりすることはできません。Swift REST API に認証するには、 Swift 管理者の権限が必要です。

関連情報

"テナントアカウントを使用する"

テナントアカウントを作成します

## StorageGRID システム内のストレージへのアクセスを制御するために、少なくとも 1 つのテナントアカウントを作成する必要があります。

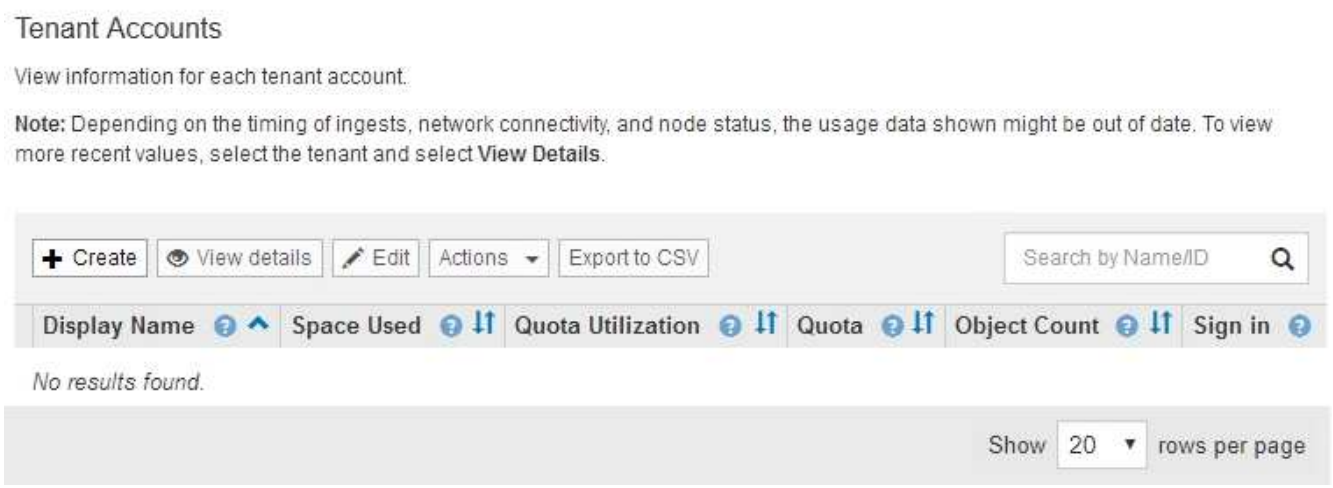
必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

手順

1. 「* tenants *」を選択します

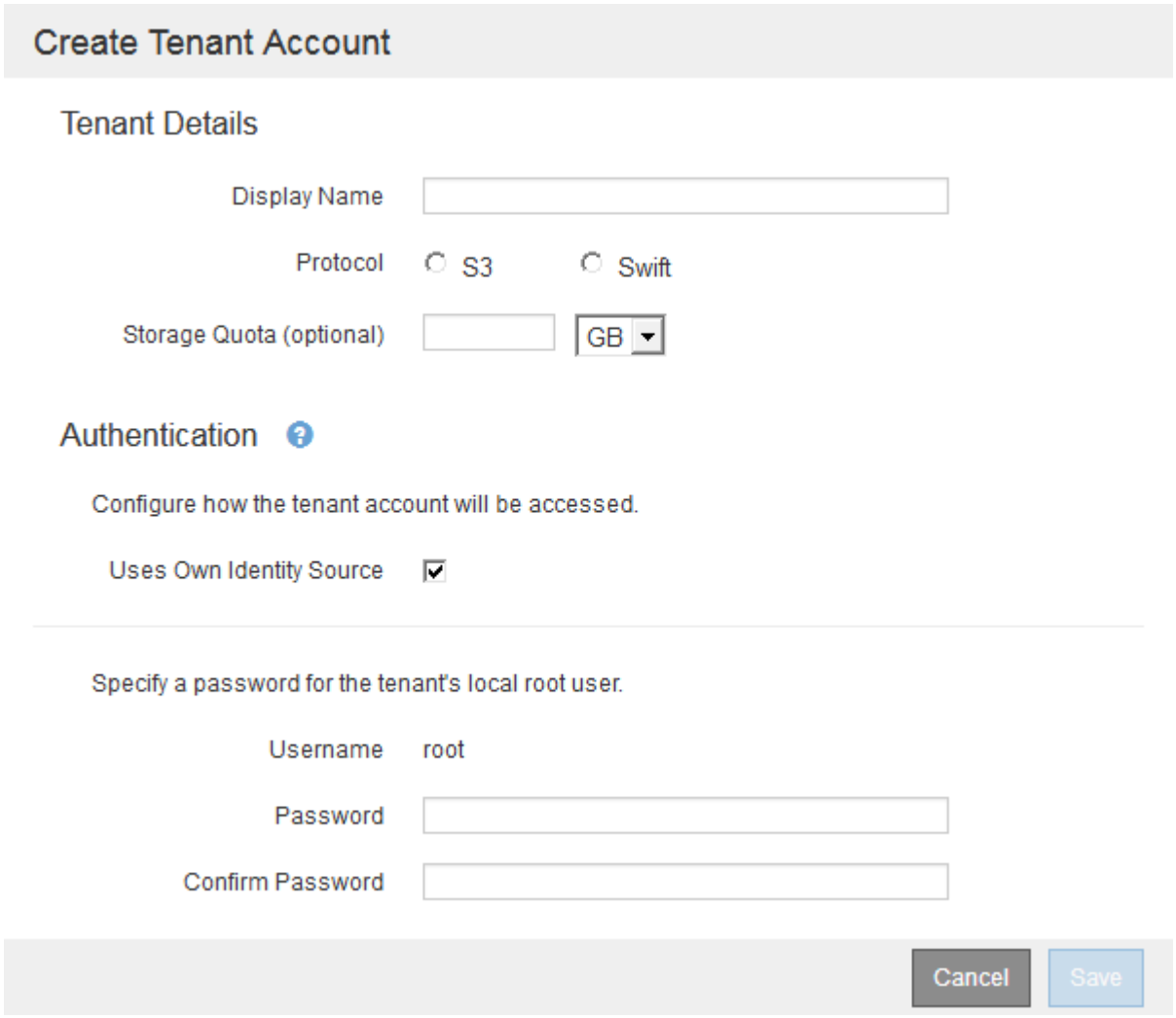
   Tenant Accountsページが表示され、既存のテナントアカウントの一覧が表示されます。



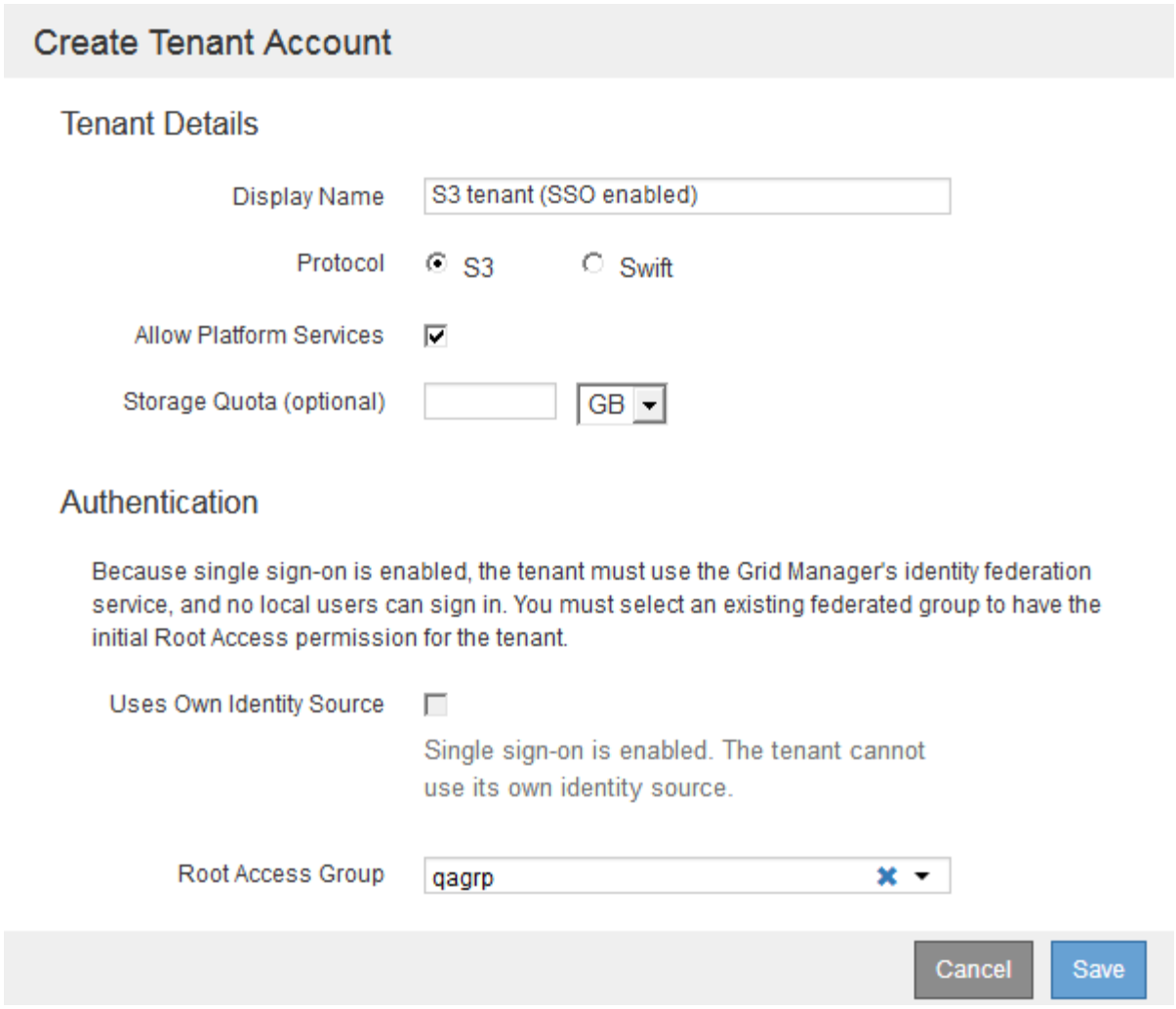

2. 「 * Create * 」を選択します。

Create Tenant Accountページが表示されます。このページに表示されるフィールドは、StorageGRID システムでシングルサインオン（SSO）が有効になっているかどうかによって異なります。

- SSOを使用していない場合、Create Tenant Accountページは次のようになります。




- SSOが有効な場合、Create Tenant Accountページは次のようになります。




関連情報

"アイデンティティフェデレーションを使用する"

"シングルサインオンを設定しています"

**StorageGRID** が**SSO**を使用していない場合のテナントアカウントの作成

テナントアカウントを作成する際は、名前、クライアントプロトコル、およびオプションでストレージクォータを指定します。StorageGRID がシングルサインオン（SSO）を使用していない場合は、テナントアカウントが独自のアイデンティティソースを使用するかどうかを指定し、テナントのローカルrootユーザの初期パスワードを設定する必要があります。

このタスクについて

Grid Manager用に設定されているアイデンティティソースをテナントアカウントで使用し、テナントアカウントにフェデレーテッドグループへのRoot Access権限を付与する場合は、そのフェデレーテッドグループをGrid Managerにインポートしておく必要があります。この管理グループに Grid Manager の権限を割り当てる必要はありません。の手順を参照してください "管理者グループの管理"。

手順

1. [表示名]テキストボックスに、このテナントアカウントの表示名を入力します。

   表示名は一意である必要はありません。作成したテナントアカウントには、一意の数値アカウントIDが割り当てられます。

2. このテナントアカウントで使用するクライアントプロトコルとして、* S3 または Swift *を選択します。
3. S3テナントアカウントの場合は、このテナントでS3バケットにプラットフォームサービスを使用しないようにする場合を除き、プラットフォームサービスの許可*チェックボックスをオンのままにしておきます。

   プラットフォームサービスが有効になっている場合、テナントは外部サービスにアクセスするCloudMirror レプリケーションなどの機能を使用できます。これらの機能の使用を無効にすることで、テナントが消費するネットワーク帯域幅またはその他のリソースの量を制限できます。「プラットフォームサービスの管理」を参照してください。

4. [ストレージクォータ]テキストボックスに、このテナントのオブジェクトで使用可能にする最大ギガバイト数、テラバイト数、またはペタバイト数をオプションで入力します。次に、ドロップダウンリストから単位を選択します。

   このテナントのクォータを無制限にする場合は、このフィールドを空白のままにします。

   テナントのストレージクォータは、物理容量（ディスクのサイズ）ではなく、論理容量（オブジェクトのサイズ）を表します。ILMのコピーおよびイレイジャーコーディングは、クォータの使用量にはカウントされません。クォータを超過すると、テナントアカウントは新しいオブジェクトを作成できなくなります。

   各テナントアカウントのストレージ使用状況を監視するには、「使用状況」を選択します。テナントアカウントは、Tenant Managerのダッシュボードまたはテナント管理APIを使用してストレージ使用状況を監視することもできます。ノードがグリッド内の他のノードから切断されていると、テナントのストレージ使用状況の値が最新ではなくなる場合があります。合計はネットワーク接続が回復すると更新されます。

5. テナントで独自のグループとユーザを管理する場合は、次の手順を実行します。
   a. [独自のアイデンティティソースを使用する*]チェックボックスをオンにします(デフォルト)。

      このチェックボックスをオンにしてテナントグループとユーザにアイデンティティフェデレーションを使用する場合、テナントが独自のアイデンティティソースを設定する必要があります。テナントアカウントを使用する手順を参照してください。

   b. テナントのローカルrootユーザのパスワードを指定します。
6. テナントがGrid Manager用に設定されたグループとユーザを使用する場合は、次の手順を実行します。
   a. [独自のアイデンティティソースを使用する*]チェックボックスをオフにします。
   b. 次のいずれか、または両方を実行します。
      - Root Access Groupフィールドで、テナントに対する最初のRoot Access権限を持つ既存のフェデレーテッドグループをGrid Managerから選択します。

適切な権限がある場合は、フィールドをクリックすると、Grid Managerから既存のフェデレーテッドグループが表示されます。それ以外の場合は、グループの一意の名前を入力します。

- テナントのローカルrootユーザのパスワードを指定します。

7. [ 保存（ Save ） ] をクリックします。

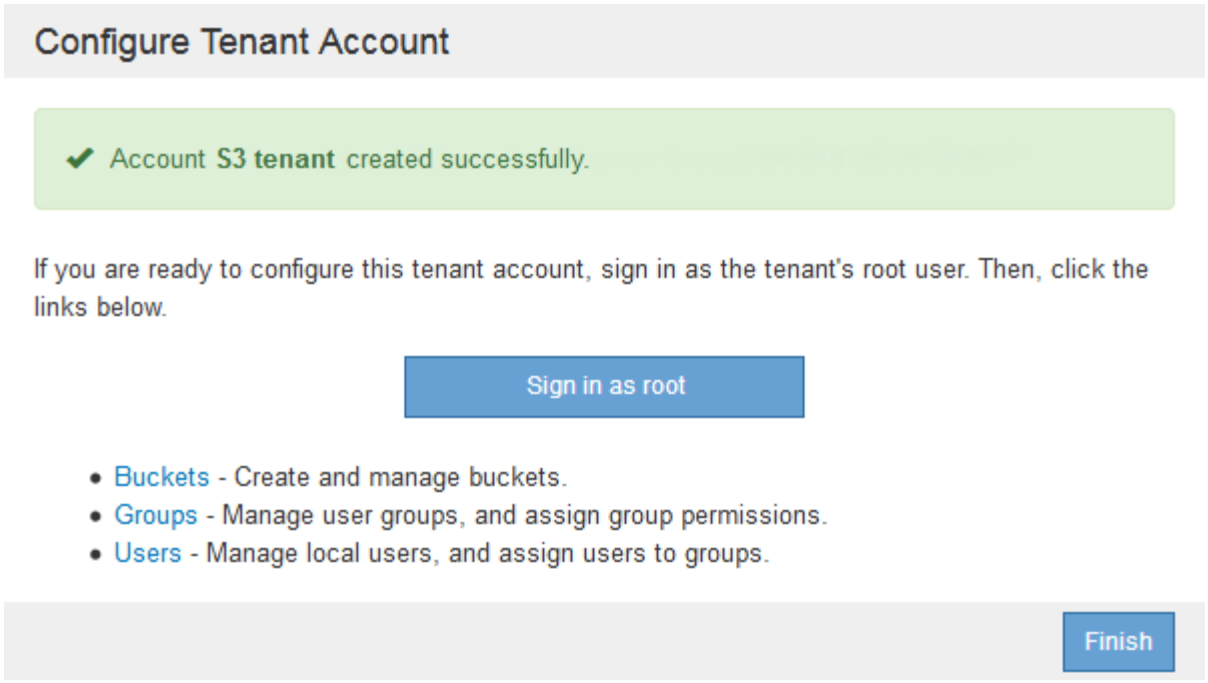
   テナントアカウントが作成されます。

8. 必要に応じて、新しいテナントにアクセスします。それ以外の場合は、の手順に進みます テナントへのアクセスはあとで行います。

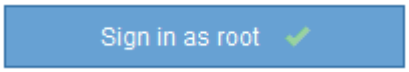
| 実行する作業 | 手順 |
| --- | --- |
| 制限されたポートでGrid Managerにアクセスします | このテナントアカウントへのアクセス方法の詳細については、「* Restricted *」をクリックしてください。<br><br>Tenant Manager の URL の形式は次のとおりです。<br><br>`https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/`<br><br>• *FQDN_or_Admin_Node_IP* は、管理ノードの完全修飾ドメイン名またはIPアドレスです<br>• *port* は、テナント専用ポートです<br>• *20-digit-account-id* は、テナントの一意のアカウントIDです |
| ポート443でGrid Managerにアクセスしているが、ローカルrootユーザのパスワードを設定していない | [サインイン]をクリックし、ルートアクセスフェデレーテッドグループにユーザのクレデンシャルを入力します。 |
| ポート443でGrid Managerにアクセスし、ローカルrootユーザのパスワードを設定した | 次の手順に進みます rootとしてサインインします。 |

9. rootとしてテナントにサインインします。

   a. Configure Tenant Account（テナントアカウントの設定）ダイアログボックスで、* Sign in as root（**root**としてサインイン）ボタンをクリックします。




緑のチェックマークがボタン上に表示されます。これは、rootユーザとしてテナントアカウントにサインインしていることを示しています。




a. リンクをクリックしてテナントアカウントを設定します。

   各リンクをクリックすると、 Tenant Manager の対応するページが開きます。このページの手順については、テナントアカウントの使用手順を参照してください。

b. [ 完了 ] をクリックします。

10. あとでテナントにアクセスするには、次の手順を実行します。

| 使用するポート | 次のいずれかを実行 ... |
| --- | --- |
| ポート 443 | • Grid Managerで* tenants を選択し、テナント名の右側にある Sign In *をクリックします。<br>• Web ブラウザにテナントの URL を入力します。<br>`https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/`<br>◦ *FQDN_or_Admin_Node_IP* は、管理ノードの完全修飾ドメイン名またはIPアドレスです<br>◦ *20-digit-account-id* は、テナントの一意のアカウントIDです |

| 使用するポート | 次のいずれかを実行 ... |
| --- | --- |
| 制限されたポート | • Grid Managerから* tenants を選択し、 Restricted *をクリックします。<br>• Web ブラウザにテナントの URL を入力します。<br>`https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id`<br>◦ *FQDN_or_Admin_Node_IP* は、管理ノードの完全修飾ドメイン名またはIPアドレスです<br>◦ *port* は、テナント専用の制限付きポートです<br>◦ *20-digit-account-id* は、テナントの一意のアカウントIDです |

関連情報

"ファイアウォールによるアクセス制御"

"S3テナントアカウント用のプラットフォームサービスの管理"

"テナントアカウントを使用する"

**SSO**が有効な場合のテナントアカウントの作成

テナントアカウントを作成する際は、名前、クライアントプロトコル、およびオプションでストレージクォータを指定します。StorageGRID でシングルサインオン（SSO）が有効になっている場合は、テナントアカウントを設定するためのRoot Access権限が割り当てられているフェデレーテッドグループも指定します。

手順

1. [表示名]テキストボックスに、このテナントアカウントの表示名を入力します。

   表示名は一意である必要はありません。作成したテナントアカウントには、一意の数値アカウントIDが割り当てられます。

2. このテナントアカウントで使用するクライアントプロトコルとして、* S3 または Swift *を選択します。
3. S3テナントアカウントの場合は、このテナントでS3バケットにプラットフォームサービスを使用しないようにする場合を除き、プラットフォームサービスの許可*チェックボックスをオンのままにしておきます。

   プラットフォームサービスが有効になっている場合、テナントは外部サービスにアクセスする CloudMirror レプリケーションなどの機能を使用できます。これらの機能の使用を無効にすることで、テナントが消費するネットワーク帯域幅またはその他のリソースの量を制限できます。「プラットフォームサービスの管理」を参照してください。

4. [ストレージクォータ]テキストボックスに、このテナントのオブジェクトで使用可能にする最大ギガバイト数、テラバイト数、またはペタバイト数をオプションで入力します。次に、ドロップダウンリストから単位を選択します。

このテナントのクォータを無制限にする場合は、このフィールドを空白のままにします。

> テナントのストレージクォータは、物理容量（ディスクのサイズ）ではなく、論理容量（オブジェクトのサイズ）を表します。ILMのコピーおよびイレイジャーコーディングは、クォータの使用量にはカウントされません。クォータを超過すると、テナントアカウントは新しいオブジェクトを作成できなくなります。

> 各テナントアカウントのストレージ使用状況を監視するには、「使用状況」を選択します。テナントアカウントは、Tenant Managerのダッシュボードまたはテナント管理APIを使用してストレージ使用状況を監視することもできます。ノードがグリッド内の他のノードから切断されていると、テナントのストレージ使用状況の値が最新ではなくなる場合があります。合計はネットワーク接続が回復すると更新されます。

5. [独自のアイデンティティソースを使用する*]チェックボックスがオフになっており、無効になっていることに注意してください。

   SSOが有効であるため、テナントはGrid Manager用に設定されたアイデンティティソースを使用する必要があります。ローカルユーザはサインインできません。

6. [* Root Access Group]フィールドで、テナントに対する最初のRoot Access権限を持つ既存のフェデレーテッドグループをGrid Managerから選択します。

   > 適切な権限がある場合は、フィールドをクリックすると、Grid Managerから既存のフェデレーテッドグループが表示されます。それ以外の場合は、グループの一意の名前を入力します。

7. [ 保存（ Save ） ] をクリックします。

   テナントアカウントが作成されます。Tenant Accountsページが表示され、新しいテナントの行が追加されます。

8. Root Accessグループのユーザは、必要に応じて新しいテナントの* Sign In *リンクをクリックしてTenant Managerにすぐにアクセスし、テナントを設定できます。それ以外の場合は、テナントアカウントの管理者に*サインイン*リンクのURLを提供します。（テナントのURLは、いずれかの管理ノードの完全修飾ドメイン名またはIPアドレスのあとにを追加したものです `/?accountId=20-digit-account-id`.）

   > テナントアカウントのRoot Accessグループに属していない場合は、* Sign In *をクリックするとアクセス拒否のメッセージが表示されます。

関連情報

"シングルサインオンを設定しています"

"S3テナントアカウント用のプラットフォームサービスの管理"

"テナントアカウントを使用する"

テナントのローカル**root**ユーザのパスワードを変更する

テナントのローカル root ユーザがアカウントからロックアウトされた場合は、 root ユー

ザのパスワード変更が必要になることがあります。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

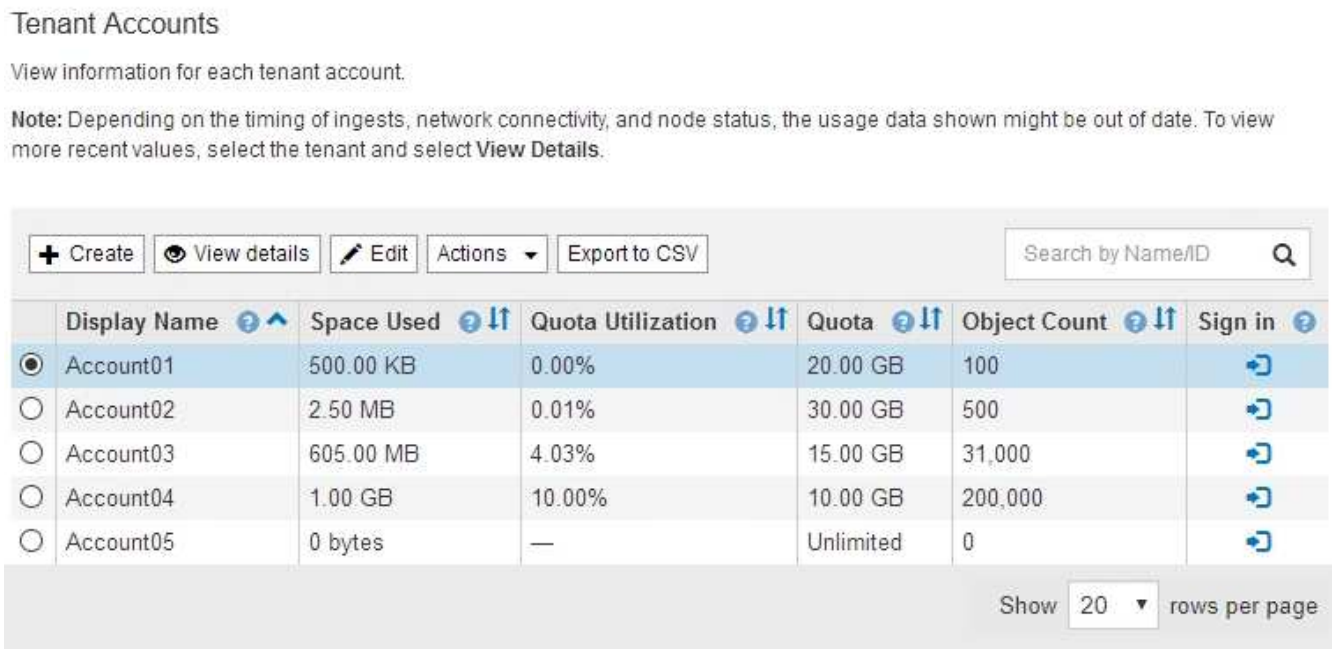
このタスクについて

StorageGRID システムでシングルサインオン（ SSO ）が有効になっている場合、ローカル root ユーザはテナントアカウントにサインインできません。rootユーザのタスクを実行するには、テナントのRoot Access権限を持つフェデレーテッドグループにユーザが属している必要があります。

手順

1. 「* tenants *」を選択します

   Tenant Accountsページが表示され、既存のテナントアカウントがすべてリストされます。

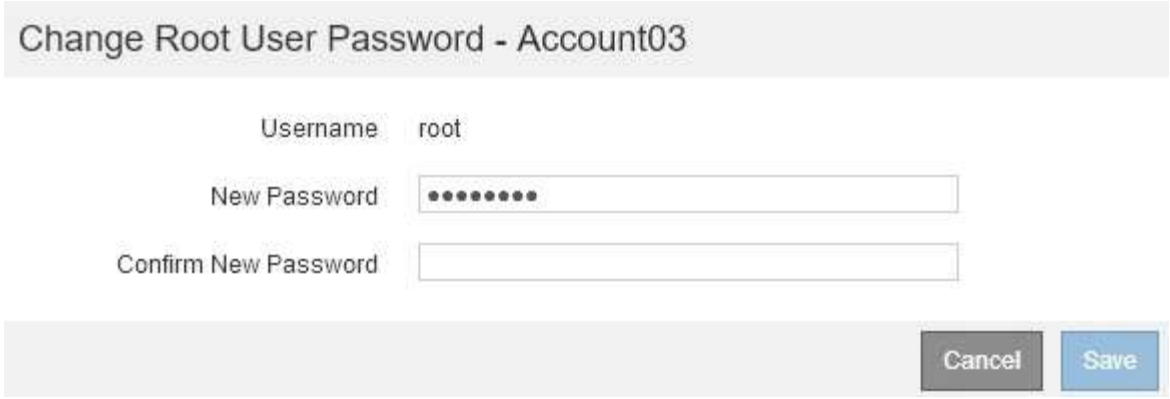



2. 編集するテナントアカウントを選択します。

   システムに20個を超えるアイテムが含まれている場合は、各ページに一度に表示する行数を指定できます。検索ボックスを使用して、表示名またはテナントIDでテナントアカウントを検索します。

   [詳細の表示]、[編集]、[アクション]ボタンが有効になります。

3. [アクション（* Actions ）]ドロップダウンから、[*ルートパスワードの変更（Change Root Password）]を選択します。




4. テナントアカウントの新しいパスワードを入力します。
5. [ 保存（ Save ） ] を選択します。

関連情報

"StorageGRID への管理者アクセスの制御"

テナントアカウントを編集する

テナントアカウントを編集して、表示名の変更、アイデンティティソース設定の変更、プラットフォームサービスの許可または禁止、ストレージクォータの入力を行うことができます。

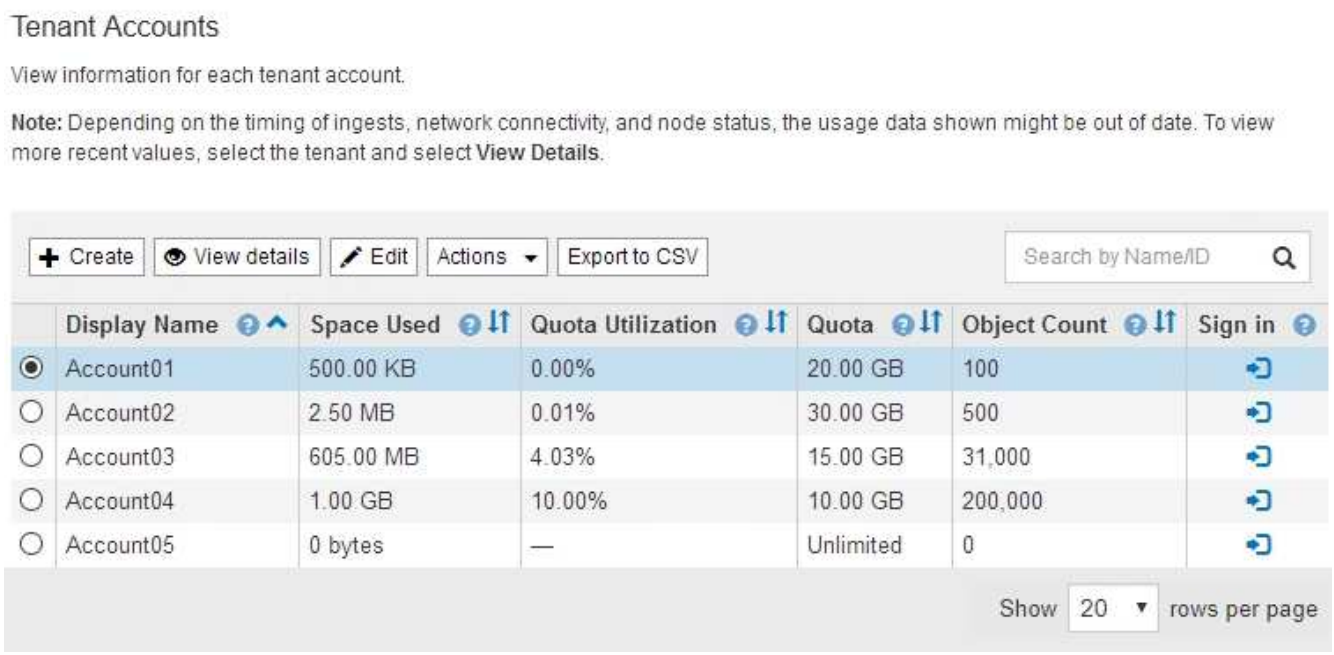
必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

手順

1. 「* tenants *」を選択します

   Tenant Accountsページが表示され、既存のテナントアカウントがすべてリストされます。

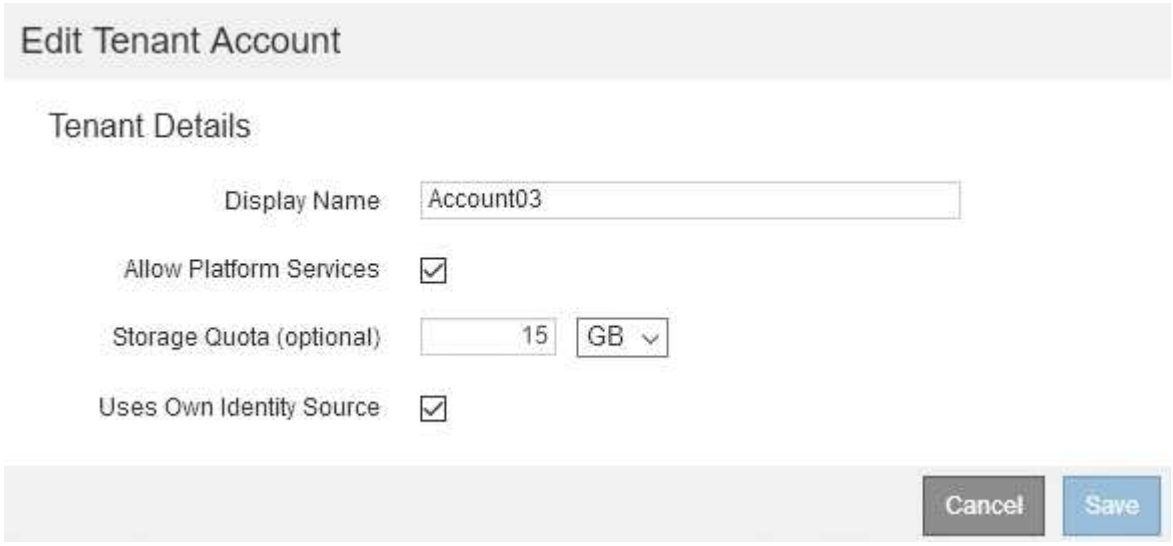



2. 編集するテナントアカウントを選択します。

   システムに20個を超えるアイテムが含まれている場合は、各ページに一度に表示する行数を指定できます。検索ボックスを使用して、表示名またはテナントIDでテナントアカウントを検索します。

3. 「 * 編集 * 」を選択します。

   Edit Tenant Accountページが表示されます。この例は、シングルサインオン（ SSO ）を使用しないグリッドを対象としています。このテナントアカウントには、独自のアイデンティティソースが設定されていません。




4. 必要に応じて、フィールドの値を変更します。
   a. このテナントアカウントの表示名を変更します。
   b. テナントアカウントがS3バケットにプラットフォームサービスを使用できるかどうかを確認するには、プラットフォームサービスを許可する*チェックボックスの設定を変更します。

プラットフォームサービスをすでに使用しているテナントに対してこのオプションを無効にすると、テナントがS3バケット用に設定しているサービスが停止します。エラーメッセージはテナントに送信されません。たとえば、テナントで S3 バケットに CloudMirror レプリケーションが設定されている場合は、引き続きバケットにオブジェクトを格納できますが、エンドポイントとして設定された外部の S3 バケットにはこれらのオブジェクトのコピーが作成されなくなります。

c. ストレージクォータ*の場合、このテナントのオブジェクトで使用可能な最大ギガバイト数、テラバイト数、またはペタバイト数を変更します。このテナントのクォータを無制限にする場合は、このフィールドを空白のままにします。

   テナントのストレージクォータは、物理容量（ディスクのサイズ）ではなく、論理容量（オブジェクトのサイズ）を表します。ILMのコピーおよびイレイジャーコーディングは、クォータの使用量にはカウントされません。

   各テナントアカウントのストレージ使用状況を監視するには、「使用状況」を選択します。テナントアカウントは、Tenant Managerのダッシュボードまたはテナント管理APIを使用して自分の使用状況を監視することもできます。ノードがグリッド内の他のノードから切断されていると、テナントのストレージ使用状況の値が最新ではなくなる場合があります。合計はネットワーク接続が回復すると更新されます。

d. テナントアカウントで独自のアイデンティティソースを使用するか、Grid Manager用に設定されたアイデンティティソースを使用するかを決定するには、* Use own Identity Source *チェックボックスの設定を変更します。

   [独自のアイデンティティソースを使用する]チェックボックスが次の場合：

   - 無効にしてオンにした場合、テナントでは独自のアイデンティティソースがすでに有効になっています。Grid Manager 用に設定されたアイデンティティソースを使用するには、テナント側で独自のアイデンティティソースを無効にする必要があります。
   - StorageGRID システムで SSO が有効になっている場合は、無効にしてオフにします。テナントは、 Grid Manager 用に設定されたアイデンティティソースを使用する必要があります。

5. [ 保存（ Save ） ] を選択します。

関連情報

"S3テナントアカウント用のプラットフォームサービスの管理"

"テナントアカウントを使用する"

テナントアカウントを削除する

## システムに対するテナントのアクセス権を完全に削除する場合は、テナントアカウントを削除します。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- テナントアカウントに関連付けられているすべてのバケット（ S3 ）、コンテナ（ Swift ）、およびオブ

ジェクトを削除しておく必要があります。

手順

1. 「* tenants *」を選択します
2. 削除するテナントアカウントを選択します。

   システムに20個を超えるアイテムが含まれている場合は、各ページに一度に表示する行数を指定できます。検索ボックスを使用して、表示名またはテナントIDでテナントアカウントを検索します。

3. [アクション（* Actions ）]ドロップダウンから、[*削除（ Remove）]を選択します。
4. 「 * OK 」を選択します。

関連情報

"StorageGRID への管理者アクセスの制御"

**S3**テナントアカウント用のプラットフォームサービスの管理

## S3 テナントアカウントでプラットフォームサービスを有効にする場合は、テナントがそのサービスの使用に必要な外部リソースにアクセスできるようにグリッドを設定する必要があります。

- "プラットフォームサービスとは"
- "プラットフォームサービス用のネットワークとポート"
- "サイト単位のプラットフォームサービスメッセージの配信"
- "プラットフォームサービスのトラブルシューティング"

プラットフォームサービスとは

## プラットフォームサービスには、 CloudMirror レプリケーション、イベント通知、および検索統合サービスがあります。

これらのサービスを使用すると、テナントの S3 バケットで次の機能を使用できます。

- * CloudMirror レプリケーション * ： StorageGRID CloudMirror レプリケーションサービスは、 StorageGRID バケットから指定された外部のデスティネーションに特定のオブジェクトをミラーリングするために使用します。

  たとえば、 CloudMirror レプリケーションを使用して特定の顧客レコードを Amazon S3 にミラーリングし、 AWS サービスを利用してデータを分析することができます。

  > ソースバケットで S3 オブジェクトのロックが有効になっている場合、 CloudMirror レプリケーションはサポートされません。

- * 通知 * ：バケット単位のイベント通知は、オブジェクトに対して実行された特定の処理に関する通知を、指定された外部の Amazon Simple Notification Service ™（ SNS ）に送信するために使用します。

  たとえば、バケットに追加された各オブジェクトについてアラートが管理者に送信されるように設定できます。この場合、オブジェクトは重大なシステムイベントに関連付けられているログファイルです。

S3 オブジェクトのロックが有効になっているバケットでイベント通知を設定することはできますが、オブジェクトの S3 オブジェクトロックメタデータ（ Retain Until Date および Legal Hold のステータスを含む）は通知メッセージに含まれません。

- * 検索統合サービス * ：検索統合サービスは、外部サービスを使用してメタデータを検索または分析できるように、指定された Elasticsearch インデックスに S3 オブジェクトメタデータを送信するために使用します。

  たとえば、リモートの Elasticsearch サービスに S3 オブジェクトメタデータを送信するようにバケットを設定できます。次に、 Elasticsearch を使用してバケット間で検索を実行し、オブジェクトメタデータのパターンに対して高度な分析を実行できます。

  S3 オブジェクトロックが有効なバケットでは Elasticsearch 統合を設定できますが、オブジェクトの S3 オブジェクトロックメタデータ（ Retain Until Date および Legal Hold のステータスを含む）は通知メッセージに含まれません。

プラットフォームサービスを使用すると、テナントで、外部ストレージリソース、通知サービス、データの検索または分析サービスを利用できるようになります。通常、プラットフォームサービスのターゲットは StorageGRID 環境の外部にあるため、テナントにこれらのサービスの使用を許可するかどうかを決める必要があります。この方法を使用する場合は、テナントアカウントを作成または編集するときにプラットフォームサービスの使用を有効にする必要があります。テナントで生成されたプラットフォームサービスのメッセージが宛先に届くようにネットワークを設定する必要もあります。

プラットフォームサービスの使用に関する推奨事項

プラットフォームサービスを使用する前に、次の推奨事項を確認してください。

- CloudMirror のレプリケーション、通知、検索統合を必要とする S3 要求ではアクティブなテナントが 100 個を超えないようにします。アクティブなテナントが 100 を超えると、 S3 クライアントのパフォーマンスが低下する可能性があります。
- StorageGRID システムの S3 バケットで、バージョン管理と CloudMirror レプリケーションの両方が有効になっている場合は、デスティネーションエンドポイントでも S3 バケットのバージョン管理を有効にします。これにより、 CloudMirror レプリケーションでエンドポイントに同様のオブジェクトバージョンを生成できます。

関連情報

"テナントアカウントを使用する"

"ストレージプロキシを設定しています"

"トラブルシューティングを監視します"

プラットフォームサービス用のネットワークとポート

## S3 テナントにプラットフォームサービスの使用を許可する場合は、プラットフォームサービスのメッセージがデスティネーションに配信されるようにグリッドのネットワークを設定する必要があります。

テナントアカウントを作成または更新する際に、 S3 テナントアカウントのプラットフォームサービスを有効にできます。プラットフォームサービスが有効になっている場合、テナントは、その S3 バケットからの

CloudMirror レプリケーション、イベント通知、または検索統合のメッセージのデスティネーションとして機能するエンドポイントを作成できます。これらのプラットフォームサービスメッセージは、 ADC サービスを実行しているストレージノードからデスティネーションエンドポイントに送信されます。

たとえば、テナントは次のタイプのデスティネーションエンドポイントを設定できます。

- ローカルでホストされる Elasticsearch クラスタ
- Simple Notification Service （ SNS ）メッセージの受信をサポートするローカルアプリケーション
- StorageGRID の同じインスタンス上または別のインスタンス上の、ローカルにホストされる S3 バケット
- Amazon Web Services 上のエンドポイントなどの外部エンドポイント。

プラットフォームサービスメッセージが確実に配信されるように、 ADC ストレージノードが含まれるネットワークを設定する必要があります。デスティネーションエンドポイントへのプラットフォームサービスメッセージの送信に、次のポートを使用できることを確認する必要があります。

デフォルトでは、プラットフォームサービスメッセージは次のポートで送信されます。

- **80** ：エンドポイント URI が http で始まる場合
- **442** ： https で始まるエンドポイント URI の場合

エンドポイントの作成や編集を行う際に、テナントで別のポートを指定できます。

> StorageGRID 環境が CloudMirror レプリケーションのデスティネーションとして使用されている場合は、ポート 80 または 443 以外のポートにレプリケーションメッセージが送信される可能性があります。デスティネーション StorageGRID 環境で S3 に使用されているポートがエンドポイントで指定されていることを確認してください。

非透過型プロキシサーバを使用する場合は、ストレージプロキシの設定で、インターネット上のエンドポイントなどの外部エンドポイントへのメッセージの送信を許可する必要もあります。

関連情報

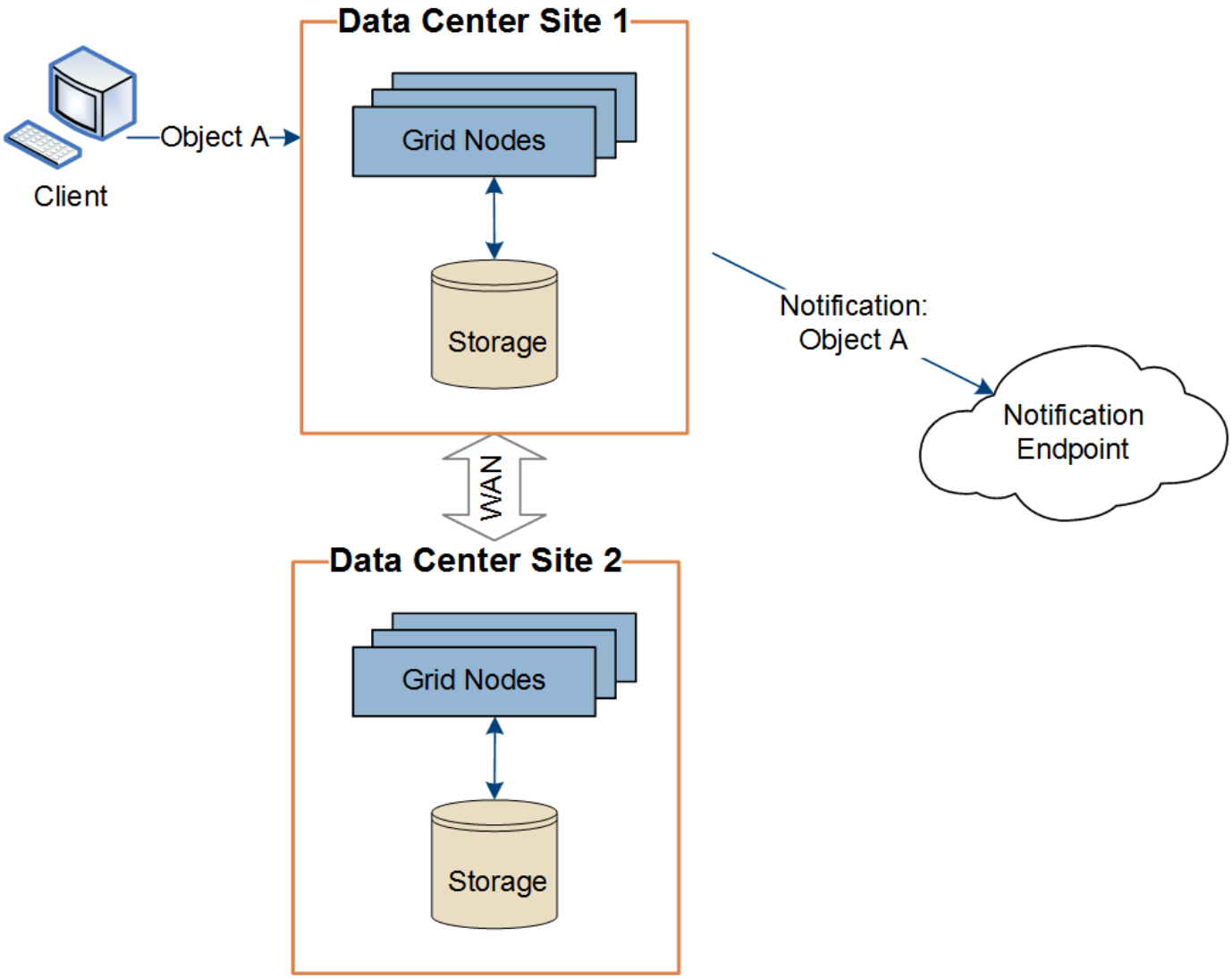
"ストレージプロキシを設定しています"

"テナントアカウントを使用する"

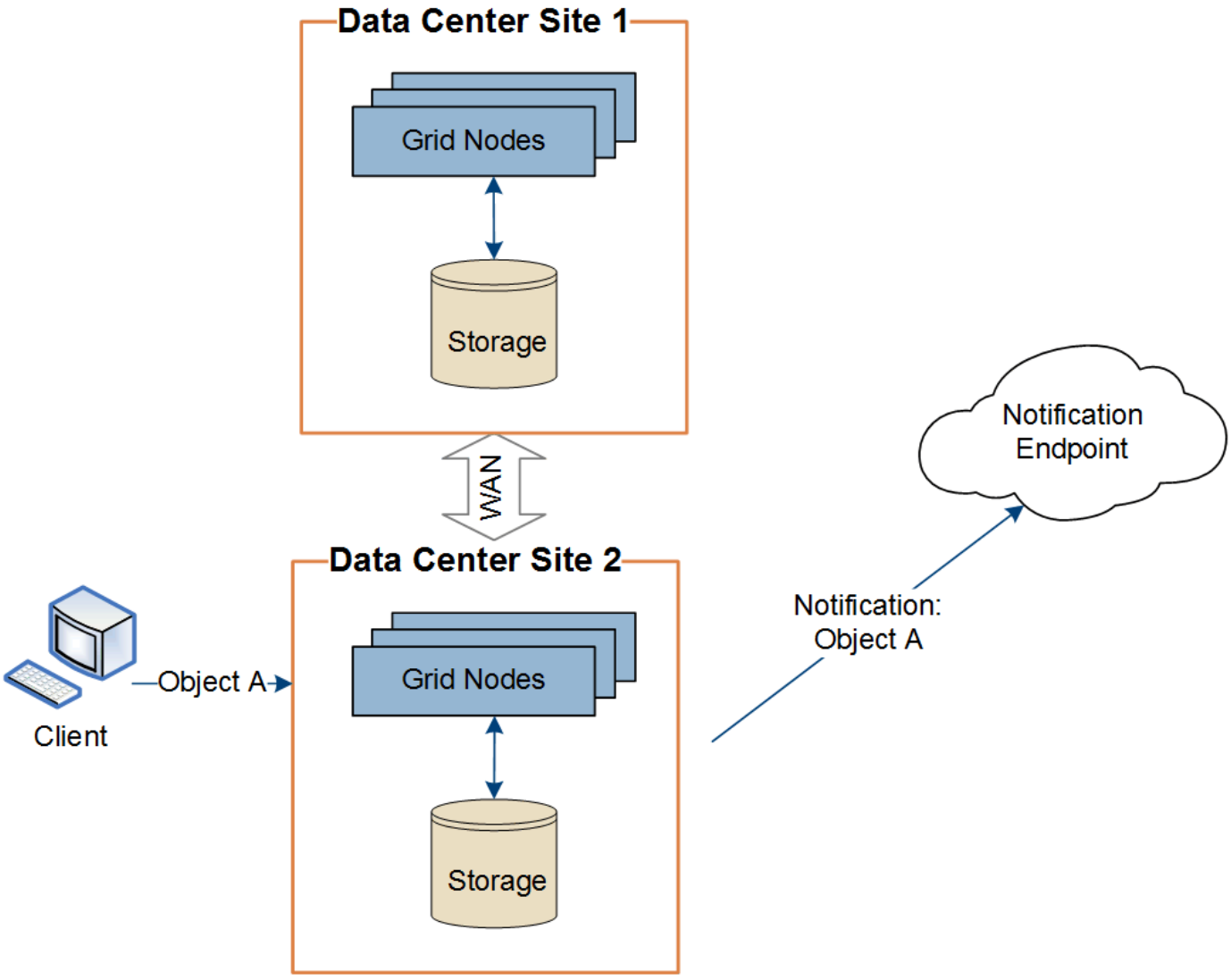
サイト単位のプラットフォームサービスメッセージの配信

## プラットフォームサービスの処理はすべてサイト単位で実行されます。

つまり、テナントがクライアントを使用してデータセンターサイト 1 のゲートウェイノードに接続し、オブジェクトに対して S3 API の Create 処理を実行すると、その処理に関する通知はデータセンターサイト 1 からトリガーされて送信されます。




クライアントが続けてデータセンターサイト 2 から同じオブジェクトに対して S3 API の Delete 処理を実行すると、その処理に関する通知はデータセンターサイト 2 からトリガーされて送信されます。




プラットフォームサービスメッセージを宛先に配信できるように、各サイトのネットワークが設定されていることを確認します。

プラットフォームサービスのトラブルシューティング

プラットフォームサービスで使用されるエンドポイントは、テナントユーザが Tenant Manager で作成および管理します。ただし、テナントでプラットフォームサービスの設定または使用に関する問題がテナントで発生した場合は、グリッドマネージャを使用して問題 を解決できる可能性があります。

新しいエンドポイントに関する問題

テナントでプラットフォームサービスを使用するには、 Tenant Manager を使用してエンドポイントを 1 つ以上作成する必要があります。各エンドポイントは、 StorageGRID S3 バケット、 Amazon Web Services バケット、 Simple Notification Service トピック、ローカルまたは AWS でホストされる Elasticsearch クラスタなど、 1 つのプラットフォームサービスの外部のデスティネーションを表します。各エンドポイントには、外部リソースの場所と、そのリソースへのアクセスに必要なクレデンシャルが含まれます。

テナントでエンドポイントを作成すると、 StorageGRID システムによって、そのエンドポイントが存在するかどうかと、指定されたクレデンシャルでアクセスできるかどうかが検証されます。エンドポイントへの接続

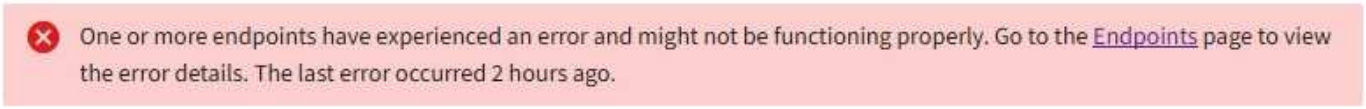
は、各サイトの 1 つのノードから検証されます。

エンドポイントの検証が失敗した場合は、その理由を記載したエラーメッセージが表示されます。テナントユーザは、問題 を解決してから、エンドポイントの作成をもう一度実行する必要があります。

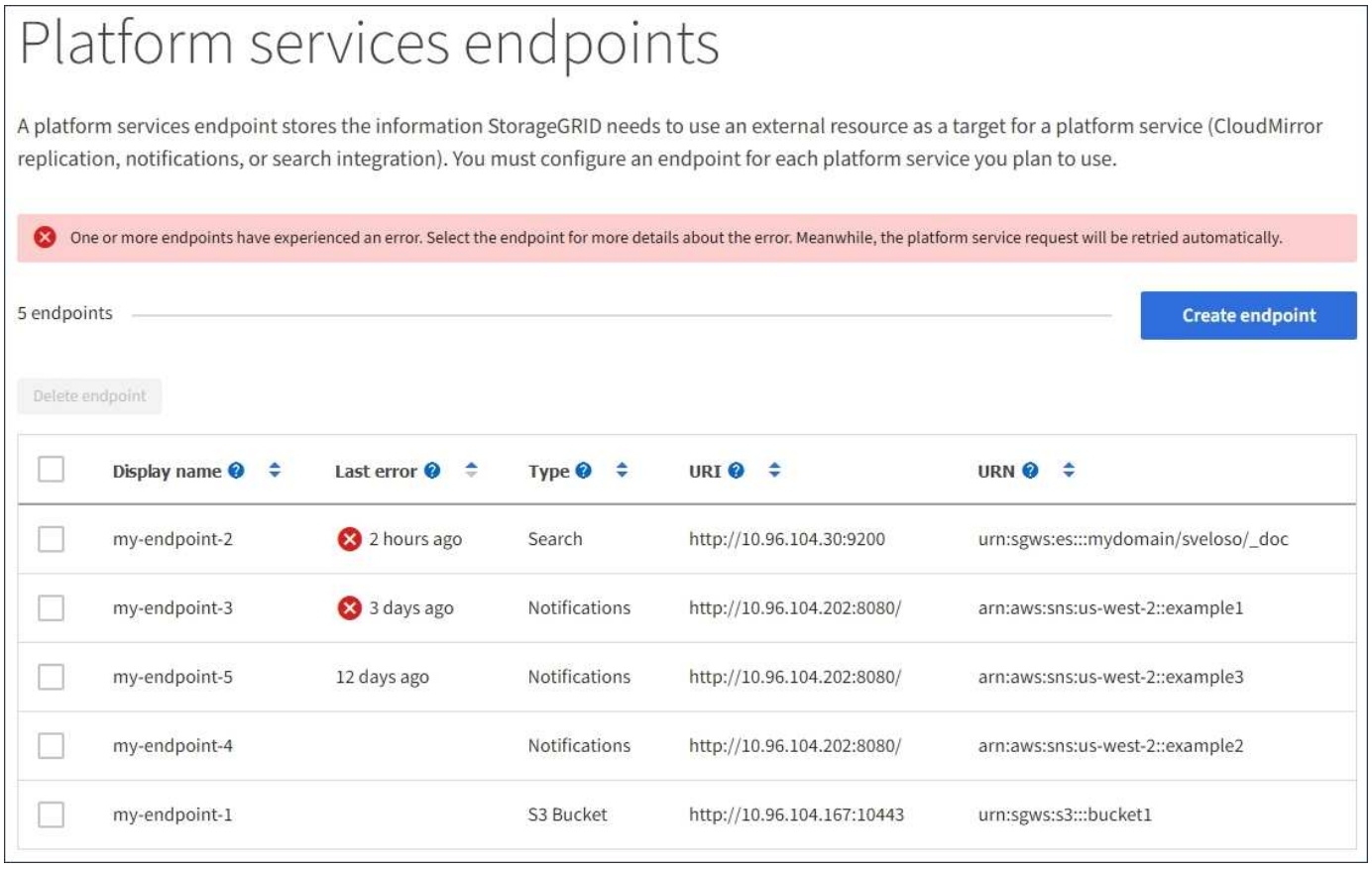
テナントアカウントでプラットフォームサービスが有効でない場合は、エンドポイントの作成が失敗します。

既存のエンドポイントに関する問題

StorageGRID が既存のエンドポイントにアクセスしようとしたときにエラーが発生した場合は、テナントマネージャのダッシュボードにメッセージが表示されます。




テナントユーザは、エンドポイントページに移動して各エンドポイントの最新のエラーメッセージを確認し、エラーが発生してからの時間を特定できます。[* Last error*] 列には、各エンドポイントの最新のエラーメッセージとエラーが発生してからの経過時間が表示されます。が含まれるエラーです アイコンは過去 7 日以内に発生しました。




「 * Last error * 」列の一部のエラーメッセージには、かっこ内にログ ID が含まれている場合があります。グリッド管理者やテクニカルサポートは、この ID を使用して、 bycast.log のエラーに関する詳細情報を確認できます。

## プロキシサーバに関連する問題

ストレージノードとプラットフォームサービスエンドポイントの間にストレージプロキシを設定している場合、プロキシサービスで StorageGRID からのメッセージが許可されていないとエラーが発生する可能性があります。これらの問題を解決するには、プロキシサーバの設定を調べて、プラットフォームサービス関連のメッセージがブロックされていないことを確認してください。

## エラーが発生したかどうかを確認しています

過去 7 日間にエンドポイントエラーが発生した場合は、 Tenant Manager のダッシュボードにアラートメッセージが表示されます。エラーの詳細を確認するには、エンドポイントのページに移動します。

## クライアント処理が失敗する

一部のプラットフォームサービスの問題により、 S3 バケットに対する原因 クライアント処理が失敗することがあります。たとえば、内部の Replicated State Machine （ RSM ）サービスが停止した場合や、配信のためにキューに登録されたプラットフォームサービスメッセージが多すぎる場合は、 S3 クライアント処理が失敗します。

サービスのステータスを確認するには、次の手順に従います。

1. Support **>** Tools **>** Grid Topology *を選択します。
2. [***site *>*_Storage Node***>*SSM*>*Services] を選択します。

## リカバリ可能なエンドポイントエラーとリカバリ不能なエンドポイントエラー

エンドポイントの作成後に、さまざまな理由からプラットフォームサービス要求のエラーが発生することがあります。一部のエラーは、ユーザが対処することでリカバリできます。たとえば、リカバリ可能なエラーは次のような原因で発生する可能性があります。

- ユーザのクレデンシャルが削除されたか、期限切れになっています。
- デスティネーションバケットが存在しません。
- 通知を配信できません。

StorageGRID でリカバリ可能なエラーが発生した場合は、成功するまでプラットフォームサービス要求が再試行されます。

その他のエラーはリカバリできません。たとえば、エンドポイントが削除されるとリカバリ不能なエラーが発生します。

StorageGRID でリカバリ不能なエンドポイントのエラーが発生すると、Grid ManagerでTotal Events（SMTT）アラームが生成されます。Total Eventsアラームを表示するには、次の手順を実行し

1. [ノード（ Nodes）]を選択し
2. 「***site *>* grid node_name >*** Events *」を選択します。
3. 表の一番上に Last Event が表示されます。

   イベントメッセージは、にも表示されます `/var/local/log/bycast-err.log`。

4. SMTT アラームに記載されている指示に従って問題 を修正します。

5. [イベントカウントのリセット]をクリックします。
6. プラットフォームサービスメッセージが配信されていないオブジェクトについてテナントに通知します。
7. テナントで、オブジェクトのメタデータまたはタグを更新することで、失敗したレプリケーションまたは通知を再度トリガーするよう指定します。

   テナントでは、既存の値を再送信し、不要な変更を回避できます。

### プラットフォームサービスメッセージを配信できません

デスティネーションでプラットフォームサービスメッセージの受信を妨げる問題 が検出された場合、バケットに対する処理は成功しますが、プラットフォームサービスメッセージは配信されません。たとえば、デスティネーションでクレデンシャルが更新されたため StorageGRID がデスティネーションサービスを認証できなくなった場合に、このエラーが発生することがあります。

リカバリ不能なエラーによってプラットフォームサービスメッセージを配信できない場合は、Grid ManagerでTotal Events（SMTT）アラームが生成されます。

### プラットフォームサービス要求のパフォーマンスが低下します

要求が送信されるペースがデスティネーションエンドポイントで要求を受信できるペースを超えると、StorageGRID ソフトウェアはバケットの受信 S3 要求を調整する場合があります。スロットルは、デスティネーションエンドポイントへの送信を待機している要求のバックログが生じている場合にのみ発生します。

明らかな影響は、受信 S3 要求の実行時間が長くなることだけです。パフォーマンスが大幅に低下していることが検出されるようになった場合は、取り込み速度を下げるか、容量の大きいエンドポイントを使用する必要があります。要求のバックログが増え続けると、クライアント S3 処理（ PUT 要求など）が失敗します。

通常、 CloudMirror 要求には、検索統合やイベント通知の要求よりも多くのデータ転送が含まれるため、デスティネーションエンドポイントのパフォーマンスによる影響を受ける可能性が高くなります。

### プラットフォームサービス要求が失敗しました

プラットフォームサービスの要求の失敗率を表示するには、次の手順を実行します。

1. [ノード（ Nodes）]を選択し
2. [**_site *>*Platform Services**] を選択します。
3. ［障害発生率の要求］チャートを表示します。

**Platform services unavailable** アラート

「 * Platform services unavailable * 」アラートは、実行中または使用可能な RSM サービスがあるストレージノードが少なすぎるために、サイトでプラットフォームサービスの処理を実行できないことを示しています。

RSM サービスは、プラットフォームサービス要求がそれぞれのエンドポイントに確実に送信されるようにします。

このアラートを解決するには、サイトのどのストレージノードに RSM サービスが含まれているかを特定します（ RSM サービスは、 ADC サービスがあるストレージノードにあります）。 そのあと、それらのストレージノードの過半数が稼働していて使用可能であることを確認します。

RSM サービスを含む複数のストレージノードでサイトで障害が発生すると、そのサイトに対する保留中のプラットフォームサービス要求はすべて失われます。

プラットフォームサービスエンドポイントに関するその他のトラブルシューティングガイダンス

プラットフォームサービスエンドポイントのトラブルシューティングに関する追加情報 の詳細については、テナントアカウントの使用手順を参照してください。

"テナントアカウントを使用する"

関連情報

"トラブルシューティングを監視します"

"ストレージプロキシを設定しています"

## S3およびSwiftクライアント接続の設定

グリッド管理者は設定オプションを管理して、 S3 および Swift テナントがクライアントアプリケーションを StorageGRID システムに接続してデータの格納と読み出しを行う方法を制御します。クライアントとテナントのさまざまな要件を満たすために、多数のオプションが用意されています。

クライアントアプリケーションは、次のいずれかに接続することで、オブジェクトを格納または読み出すことができます。

- 管理ノードまたはゲートウェイノード上のロードバランササービス、または必要に応じて、管理ノードまたはゲートウェイノードのハイアベイラビリティ（ HA ）グループの仮想 IP アドレス
- ゲートウェイノード上の CLB サービス、または必要に応じて、ゲートウェイノードのハイアベイラビリティグループの仮想 IP アドレス

CLB サービスは廃止されました。StorageGRID 11.3 より前に設定されたクライアントは、ゲートウェイノード上の CLB サービスを引き続き使用できます。ロードバランシングに StorageGRID を使用する他のすべてのクライアントアプリケーションは、ロードバランササービスを使用して接続する必要があります。

- 外部ロードバランサを使用するかどうかに関係なく、ストレージノードに追加されます

StorageGRID システムには、必要に応じて次の機能も設定できます。

- ロードバランササービス：クライアントがロードバランササービスを使用できるようにするには、クライアント接続用のロードバランサエンドポイントを作成します。ロードバランサエンドポイントを作成する際には、ポート番号、エンドポイントで HTTP / HTTPS 接続を許可するかどうか、エンドポイントを使用するクライアントのタイプ（ S3 または Swift ）、 HTTPS 接続に使用する証明書（該当する場合）を指定します。
- * 信頼されていないクライアントネットワーク * ：信頼されていないクライアントネットワークとして設定することで、クライアントネットワークのセキュリティを強化できます。クライアントネットワークが信頼されていない場合、クライアントはロードバランサエンドポイントを使用して接続する必要があります。
- ハイアベイラビリティグループ：ゲートウェイノードまたは管理ノードのHAグループを作成してアクテ

ィブ/バックアップ構成を作成できます。また、ラウンドロビンDNSや他社製ロードバランサと複数のHAグループを使用してアクティブ/アクティブ構成を実現することもできます。クライアント接続は、 HA グループの仮想 IP アドレスを使用して確立されます。

ストレージノードに直接接続するか、 CLB サービス（廃止予定）を使用して StorageGRID に接続するクライアントに対しては、 HTTP の使用を有効にし、 S3 クライアントには S3 API エンドポイントのドメイン名を設定できます。

**Summary** ：クライアント接続の **IP** アドレスとポート

クライアントアプリケーションは、グリッドノードの IP アドレスおよびそのノード上のサービスのポート番号を使用して StorageGRID に接続できます。ハイアベイラビリティ（ HA ）グループが設定されている場合は、 HA グループの仮想 IP アドレスを使用してクライアントアプリケーションを接続できます。

このタスクについて

次の表に、クライアントが StorageGRID に接続できるさまざまな方法、および接続のタイプごとに使用される IP アドレスとポートを示します。以下の手順では、ロードバランサエンドポイントとハイアベイラビリティ（ HA ）グループがすでに設定されている場合に Grid Manager でこの情報を検索する方法について説明します。

| 接続が確立される場所 | クライアントが接続するサービス | **IP** アドレス | ポート |
| --- | --- | --- | --- |
| HA グループ | ロードバランサ | HA グループの仮想 IP アドレス | • ロードバランサエンドポイントのポート |
| HA グループ | CLB の機能です<br>• 注： * CLB サービスは廃止されました。 | HA グループの仮想 IP アドレス | デフォルトの S3 ポート：<br>• HTTPS ： 8082<br>• HTTP ： 8084<br>デフォルトの Swift ポート：<br>• HTTPS ： 8083<br>• HTTP ： 8085 |
| 管理ノード | ロードバランサ | 管理ノードの IP アドレス | • ロードバランサエンドポイントのポート |
| ゲートウェイノード | ロードバランサ | ゲートウェイノードの IP アドレス | • ロードバランサエンドポイントのポート |

| 接続が確立される場所 | クライアントが接続するサービス | **IP** アドレス | ポート |
| --- | --- | --- | --- |
| ゲートウェイノード | CLB の機能です<br>• 注： * CLB サービスは廃止されました。 | ゲートウェイノードの IP アドレス<br>• 注：デフォルトでは、 CLB および LDR の HTTP ポートは有効になっていません。 | デフォルトの S3 ポート：<br>• HTTPS ： 8082<br>• HTTP ： 8084<br>デフォルトの Swift ポート：<br>• HTTPS ： 8083<br>• HTTP ： 8085 |
| ストレージノード | LDR | ストレージノードの IP アドレス | デフォルトの S3 ポート：<br>• HTTPS ： 18082<br>• HTTP ： 18084<br>デフォルトの Swift ポート：<br>• HTTPS ： 18083<br>• HTTP ： 18085 |

例

ゲートウェイノードの HA グループのロードバランサエンドポイントに S3 クライアントを接続するには、次のように構造化された URL を使用します。

- `https://VIP-of-HA-group:LB-endpoint-port`

たとえば、 HA グループの仮想 IP アドレスが 192.0.2.5 で S3 ロードバランサエンドポイントのポート番号が 10443 の場合、 S3 クライアントは次の URL を使用して StorageGRID に接続できます。

- `https://192.0.2.5:10443`

Swift クライアントをゲートウェイノードの HA グループのロードバランサエンドポイントに接続するには、次のように構造化された URL を使用します。

- `https://VIP-of-HA-group:LB-endpoint-port`

たとえば、 HA グループの仮想 IP アドレスが 192.0.2.6 で、 Swift ロードバランサエンドポイントのポート番号が 10444 の場合、 Swift クライアントは次の URL を使用して StorageGRID に接続できます。

- `https://192.0.2.6:10444`

クライアントが StorageGRID への接続に使用する IP アドレスに DNS 名を設定できます。ローカルネットワーク管理者にお問い合わせください。

手順

1. サポートされているブラウザを使用してGrid Managerにサインインします。
2. グリッドノードの IP アドレスを確認するには、次の手順を実行します。
   a. [ノード（ Nodes）]を選択し
   b. 接続する管理ノード、ゲートウェイノード、またはストレージノードを選択します。
   c. [* Overview * （概要 * ） ] タブを選択します。
   d. Node Information セクションで、ノードの IP アドレスを確認します。
   e. Show More *をクリックして、IPv6アドレスとインターフェイスマッピングを表示します。

      クライアントアプリケーションから、リスト内の任意の IP アドレスへの接続を確立できます。

      - * eth0 ： * グリッドネットワーク
      - * eth1 ： * 管理ネットワーク（オプション）
      - * eth2 ： * クライアントネットワーク（オプション）

      表示されている管理ノードまたはゲートウェイノードがハイアベイラビリティグループのアクティブノードである場合は、 HA グループの仮想 IP アドレスが eth2 に表示されます。

3. ハイアベイラビリティグループの仮想 IP アドレスを検索するには、次の手順を実行します。
   a. * Configuration > Network Settings > High Availability Groups *を選択します。
   b. HA グループの仮想 IP アドレスを表で確認します。
4. ロードバランサエンドポイントのポート番号を確認するには、次の手順を実行します。
   a. [* Configuration > Network Settings > Load Balancer Endpoints *]を選択します。

      Load Balancer Endpoints ページが表示され、設定済みのエンドポイントのリストが表示されます。

   b. エンドポイントを選択し、*エンドポイントの編集*をクリックします。

      [Edit Endpoint] ウィンドウが開き、エンドポイントに関する追加の詳細が表示されます。

   c. 選択したエンドポイントが正しいプロトコル（S3またはSwift）で使用するように設定されていることを確認し、* Cancel *をクリックします。
   d. クライアント接続に使用するエンドポイントのポート番号をメモします。

      ポート番号が 80 または 443 の場合は、管理ノードで予約されているため、エンドポイントはゲートウェイノードにのみ設定されます。それ以外のポートはすべて、ゲートウェイノードと管理ノードの両方に設定されます。

負荷分散の管理

## StorageGRID のロードバランシング機能を使用して、 S3 / Swift クライアントからの取り込み / 読み出しワークロードを処理できます。ロードバランシングは、複数のストレ

ージノードにワークロードと接続を分散することで、速度と接続容量を最大化します。

StorageGRID システムでは、次の方法でロードバランシングを実現できます。

- 管理ノードとゲートウェイノードにインストールされているロードバランササービスを使用します。ロードバランササービスはレイヤ 7 のロードバランシングを提供し、クライアント要求の TLS ターミネーション、要求の検査、およびストレージノードへの新しいセキュアな接続の確立を実施します。これは推奨されるロードバランシングメカニズムです。
- ゲートウェイノードにのみインストールされているConnection Load Balancer（CLB）サービスを使用します。CLB サービスはレイヤ 4 のロードバランシングを提供し、リンクコストをサポートします。

  CLB サービスは廃止されました。

- サードパーティ製ロードバランサを統合します。詳細については、ネットアップのアカウント担当者にお問い合わせください。

ロードバランシングの仕組み - ロードバランササービス

## ロードバランササービスは、クライアントアプリケーションからの受信ネットワーク接続を複数のストレージノードに分散します。ロードバランシングを有効にするには、Grid Manager を使用してロードバランサエンドポイントを設定する必要があります。

ロードバランサエンドポイントは管理ノードまたはゲートウェイノードにのみ設定できます。これらのノードタイプにはロードバランササービスが含まれているためです。ストレージノードまたはアーカイブノードにエンドポイントを設定することはできません。

各ロードバランサエンドポイントは、ポート、プロトコル（HTTPまたはHTTPS）、サービスタイプ（S3またはSwift）、およびバインドモードを指定します。HTTPS エンドポイントにはサーバ証明書が必要です。バインドモードでは、エンドポイントポートのアクセスを次のように制限できます。

- 特定のハイアベイラビリティ（HA）仮想IPアドレス（VIP）
- 特定のノードの特定のネットワークインターフェイス

ポートに関する考慮事項

クライアントは、ロードバランササービスを実行しているノードに設定された任意のエンドポイントにアクセスできます。ただしポート 80 と 443 は例外で、管理ノードではこれらのノードが予約されているため、これらのポートに設定されたエンドポイントはゲートウェイノードでのみロードバランシング処理をサポートします。

ポートを再マッピングした場合、同じポートを使用してロードバランサエンドポイントを設定することはできません。再マッピングしたポートを使用してエンドポイントを作成できますが、これらのエンドポイントはロードバランササービスではなく、元の CLB ポートおよびサービスに再マッピングされます。ポートの再マッピングを削除するには、リカバリとメンテナンスの手順に従ってください。

CLB サービスは廃止されました。

**CPU** の可用性

S3 / Swift トラフィックをストレージノードに転送する際、各管理ノードおよびゲートウェイノード上のロー

ドバランササービスは独立して動作します。重み付きのプロセスを使用すると、ロードバランササービスは、より多くの要求をより多くの CPU を使用可能なストレージノードにルーティングします。ノード CPU 負荷情報は数分ごとに更新されますが、重み付けがより頻繁に更新される場合があります。ノードの使用率が 100% になった場合や、ノードの利用率のレポートに失敗した場合でも、すべてのストレージノードには最小限のベースとなる重みの値が割り当てられます。

CPU の可用性に関する情報が、ロードバランササービスが配置されているサイトに制限されている場合があります。

関連情報

""

ロードバランサエンドポイントの設定

# ロードバランサエンドポイントを作成、編集、および削除できます。

## ロードバランサエンドポイントの作成

各ロードバランサエンドポイントは、ポート、ネットワークプロトコル（HTTPまたはHTTPS）、およびサービスタイプ（S3またはSwift）を指定します。HTTPSエンドポイントを作成する場合は、サーバ証明書をアップロードまたは生成する必要があります。

必要なもの

- Root Access 権限が必要です。
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- ロードバランササービスに使用するポートをすでに再マッピングしている場合は、再マッピングを削除しておく必要があります。

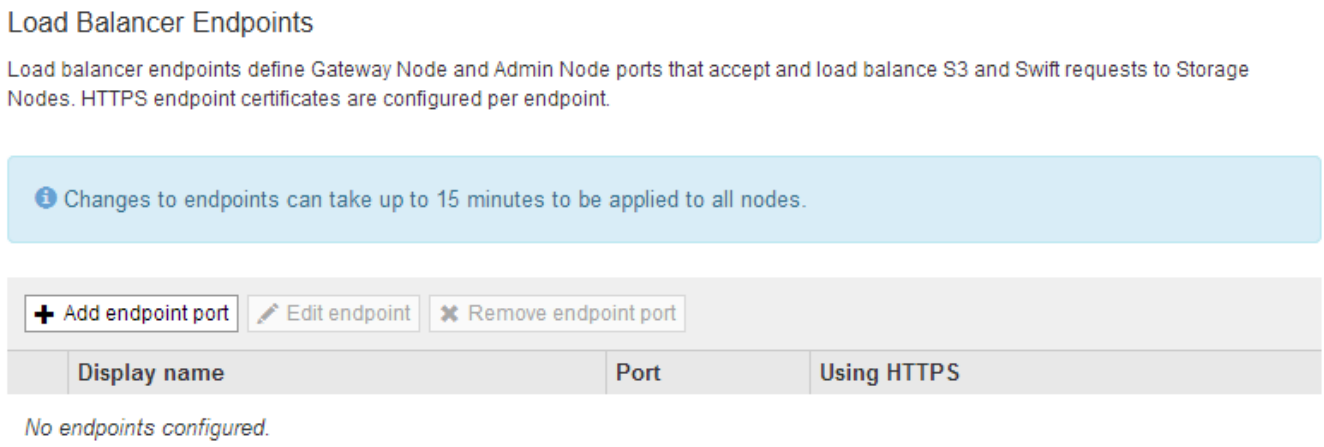
> ポートを再マッピングした場合、同じポートを使用してロードバランサエンドポイントを設定することはできません。再マッピングしたポートを使用してエンドポイントを作成できますが、これらのエンドポイントはロードバランササービスではなく、元の CLB ポートおよびサービスに再マッピングされます。ポートの再マッピングを削除するには、リカバリとメンテナンスの手順に従ってください。

> CLB サービスは廃止されました。

手順

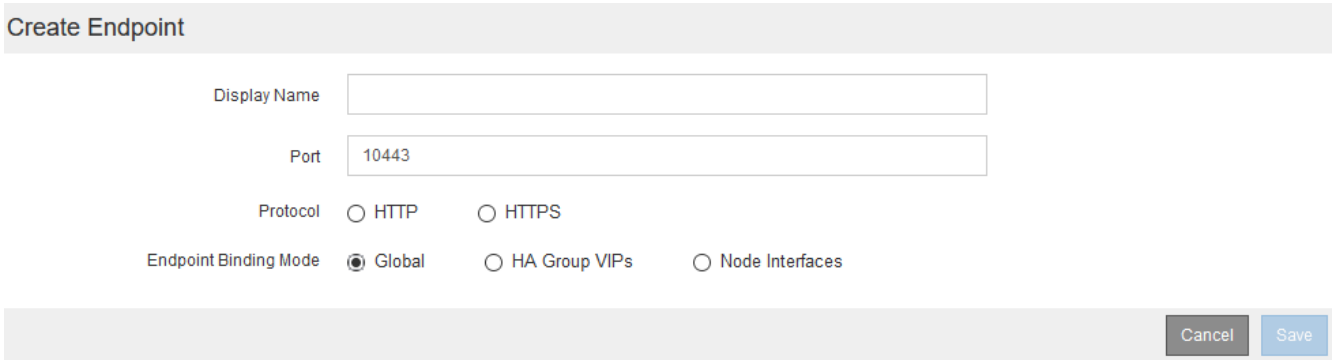
1. [* Configuration > Network Settings > Load Balancer Endpoints *]を選択します。

   Load Balancer Endpointsページが表示されます。




2. [エンドポイントの追加]を選択します。

   [Create Endpoint]ダイアログボックスが表示されます。



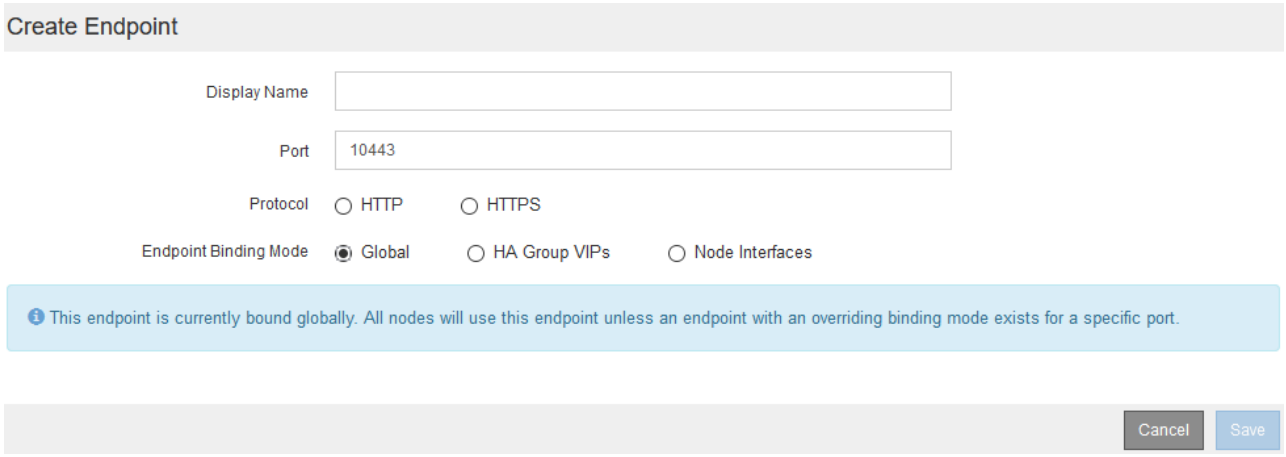

3. ロードバランサエンドポイントのページのリストに表示されるエンドポイントの表示名を入力します。
4. ポート番号を入力するか、あらかじめ入力されているポート番号をそのまま使用します。

   ポート番号80または443は管理ノードで予約されているため、これらのポートを入力すると、エンドポイントはゲートウェイノードにのみ設定されます。

   他のグリッドサービスで使用されているポートは使用できません。内部および外部の通信に使用されるポートの一覧については、ネットワークのガイドラインを参照してください。

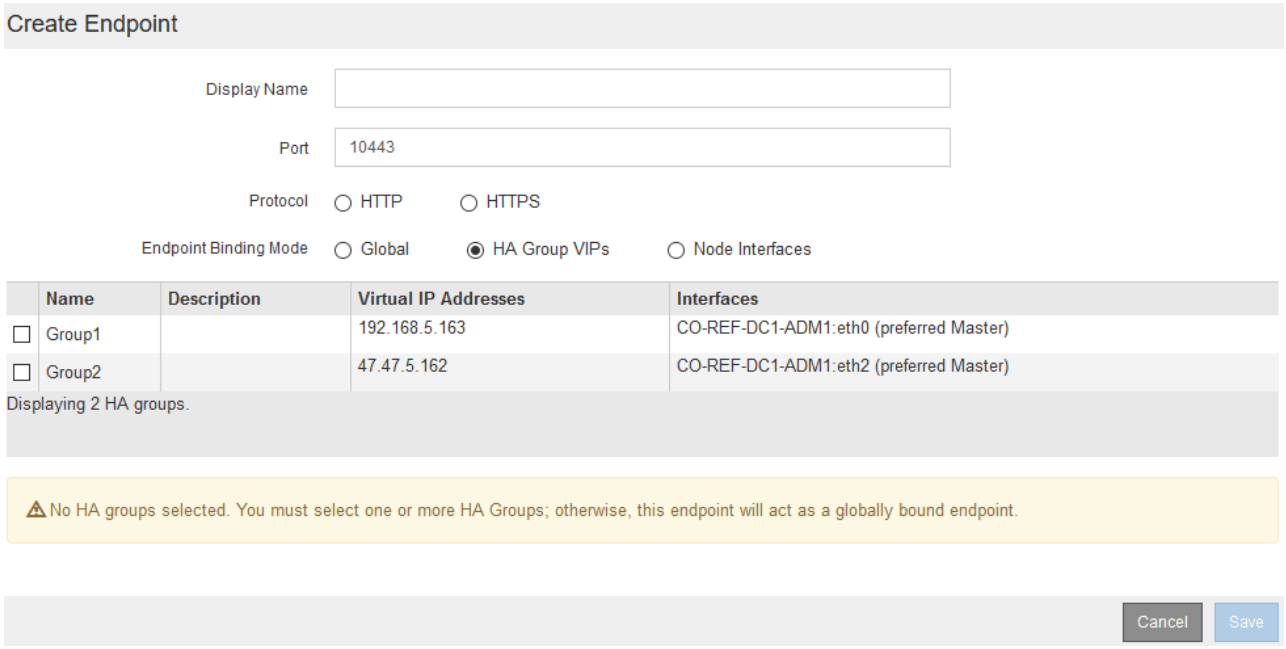
5. このエンドポイントのネットワークプロトコルを指定するには、「* HTTP 」または「 HTTPS *」を選択します。
6. エンドポイントバインディングモードを選択します。

   - * Global *（デフォルト）：指定したポート番号のすべてのゲートウェイノードと管理ノードでエンドポイントにアクセスできます。



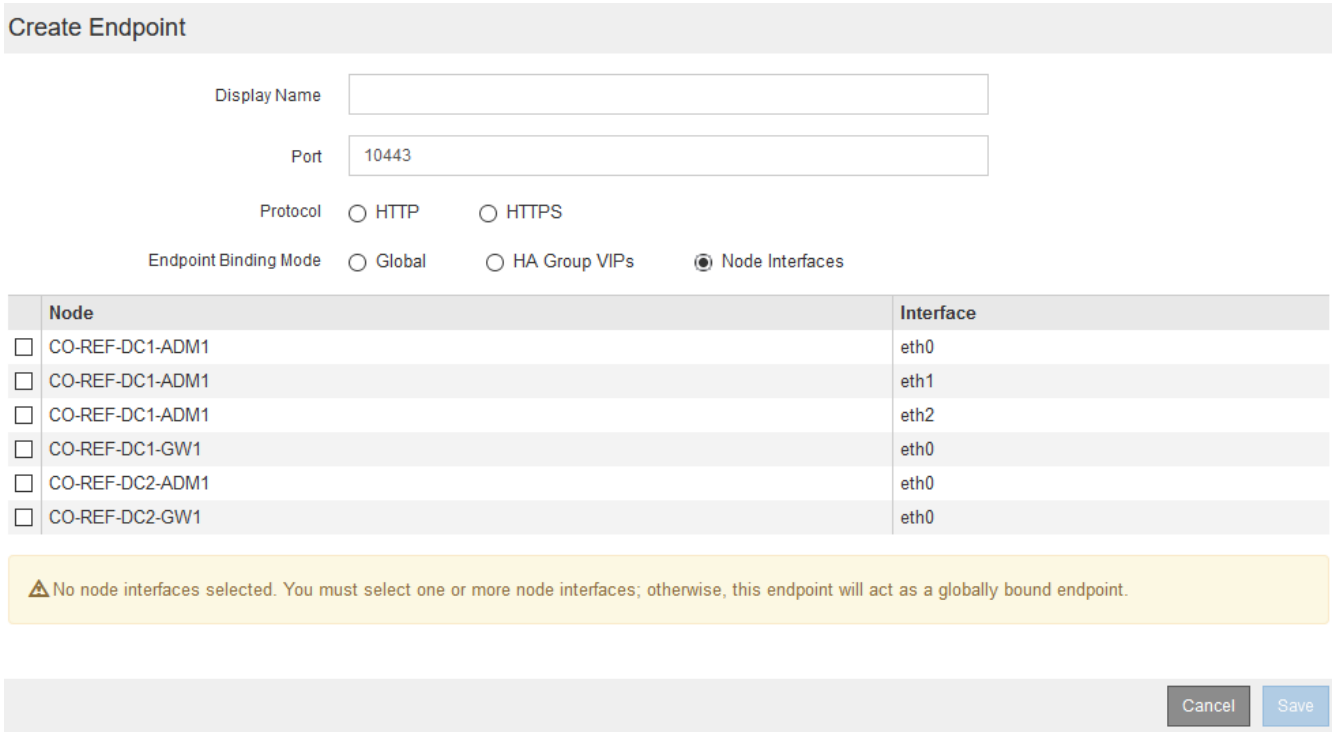

- * HA Group VIP *：エンドポイントには、選択したHAグループに定義された仮想IPアドレスからのみアクセスできます。このモードで定義されたエンドポイントは、エンドポイントによって定義されたHAグループが互いに重複しないかぎり、同じポート番号を再利用できます。

  仮想IPアドレスが割り当てられたエンドポイントを表示するHAグループを選択します。




- ノードインターフェイス：エンドポイントには、指定したノードとネットワークインターフェイスでのみアクセスできます。このモードで定義されたエンドポイントは、相互に重複しないかぎり、同じポート番号を再利用できます。

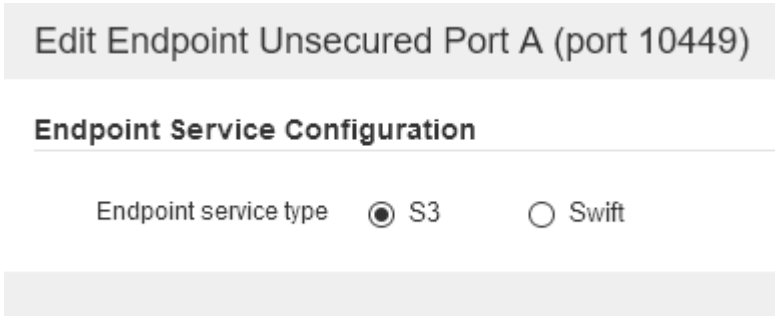
  エンドポイントを表示するノードインターフェイスを選択します。




7. [ 保存（ Save ） ] を選択します。

   [Edit Endpoint]ダイアログボックスが表示されます。

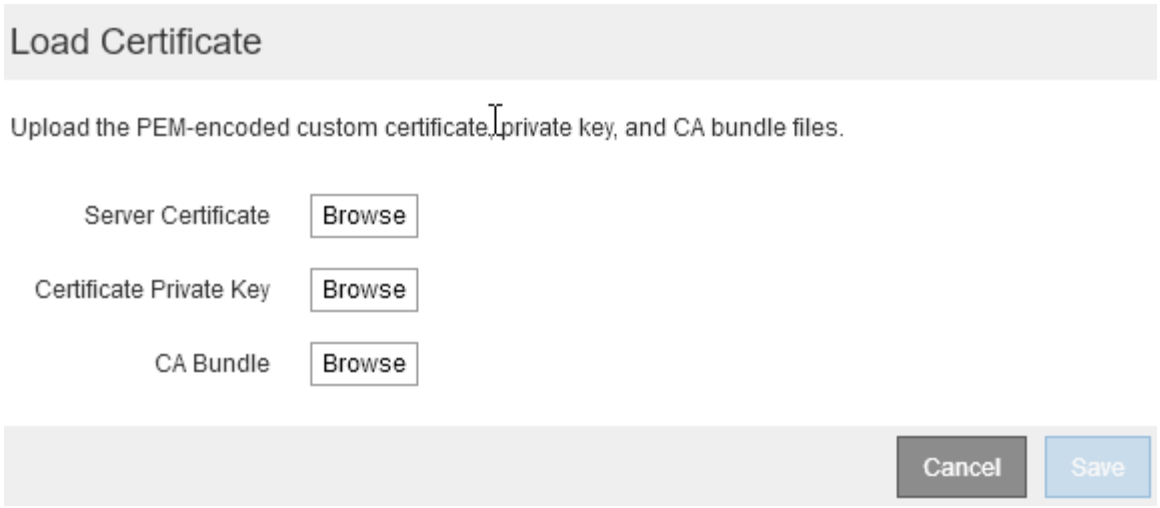
8. エンドポイントで処理するトラフィックのタイプを指定するには、「* S3 」または「 Swift *」を選択します。




9. *HTTP*を選択した場合は、*Save*を選択します。

   セキュアでないエンドポイントが作成されます。ロードバランサエンドポイントのページのテーブルには、エンドポイントの表示名、ポート番号、プロトコル、およびエンドポイントIDが表示されます。

10. [* HTTPS*]を選択し、証明書をアップロードする場合は、[証明書のアップロード]を選択します。




a. サーバ証明書と証明書の秘密鍵を参照します。

   S3クライアントがS3 APIエンドポイントのドメイン名を使用して接続できるようにするには、クライアントがグリッドへの接続に使用する可能性のあるすべてのドメイン名に一致するマルチドメイン証明書またはワイルドカード証明書を使用します。たとえば、サーバ証明書でドメイン名を使用しているとします `*.example.com`。

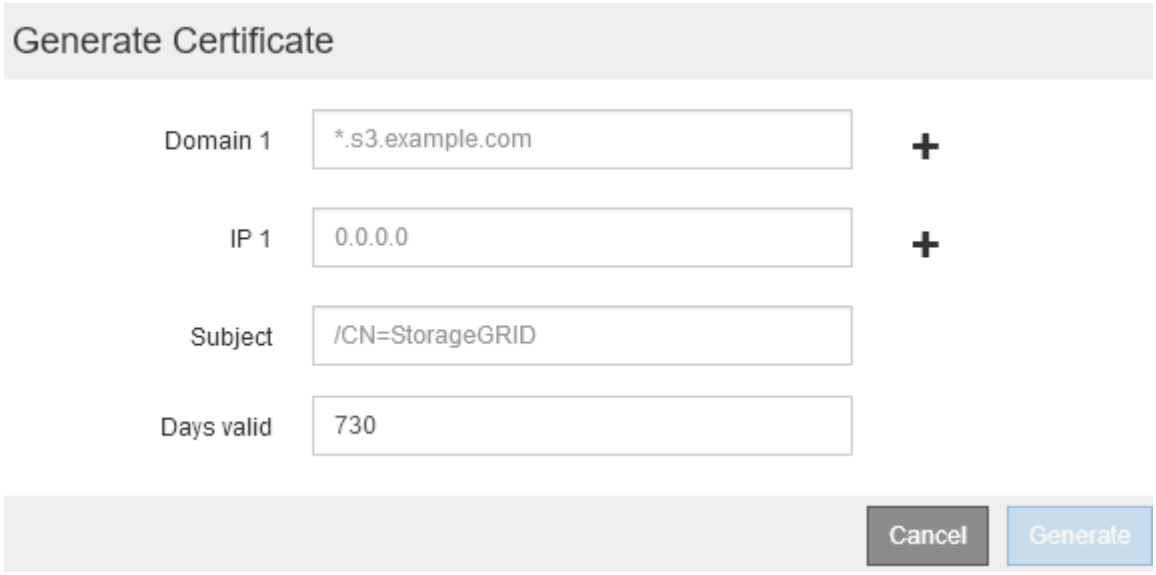
"S3 APIエンドポイントのドメイン名を設定しています"

a. 必要に応じて、CAバンドルを参照します。

b. [ 保存（ Save ） ] を選択します。

   エンドポイントのPEMでエンコードされた証明書データが表示されます。

11. [* HTTPS*]を選択し、証明書を生成する場合は、[証明書の生成]を選択します。




a. ドメイン名またはIPアドレスを入力します。

   ワイルドカードを使用して、ロードバランササービスを実行しているすべての管理ノードとゲートウェイノードの完全修飾ドメイン名を表すことができます。例： `*.sgws.foo.com` ワイルドカード*を

使用して表します `gn1.sgws.foo.com` および `gn2.sgws.foo.com`。

"S3 APIエンドポイントのドメイン名を設定しています"

a. 選択するオプション ➕ をクリックして、他のドメイン名またはIPアドレスを追加します。

   ハイアベイラビリティ（HA）グループを使用する場合は、HA仮想IPのドメイン名とIPアドレスを追加します。

b. 必要に応じて、証明書を所有するユーザを識別するために、[X.509 subject]（識別名（DN）とも呼ばれる）を入力します。

c. 必要に応じて、証明書の有効日数を選択します。デフォルトは730日です。

d. [*Generate （生成） ] を選択します

   エンドポイントの証明書メタデータとPEMでエンコードされた証明書データが表示されます。

12. [ 保存（ Save ） ] をクリックします。

    エンドポイントが作成されます。ロードバランサエンドポイントのページのテーブルには、エンドポイントの表示名、ポート番号、プロトコル、およびエンドポイントIDが表示されます。

関連情報

""

"ネットワークガイドライン"

"ハイアベイラビリティグループの管理"

"信頼されていないクライアントネットワークの管理"

ロードバランサエンドポイントの編集

セキュアでない（HTTP）エンドポイントの場合、エンドポイントのサービスタイプ（S3またはSwift）を変更できます。セキュアな（HTTPS）エンドポイントの場合、エンドポイントのサービスタイプを編集して、セキュリティ証明書を表示または変更できます。

必要なもの

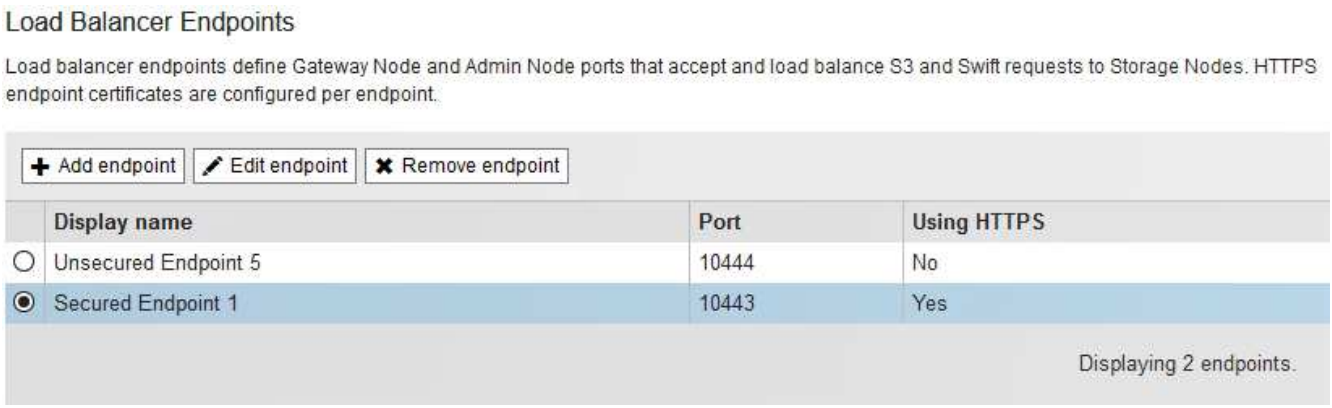
- Root Access 権限が必要です。
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

手順

1. [* Configuration > Network Settings > Load Balancer Endpoints *]を選択します。

   Load Balancer Endpointsページが表示されます。既存のエンドポイントがテーブルに表示されます。

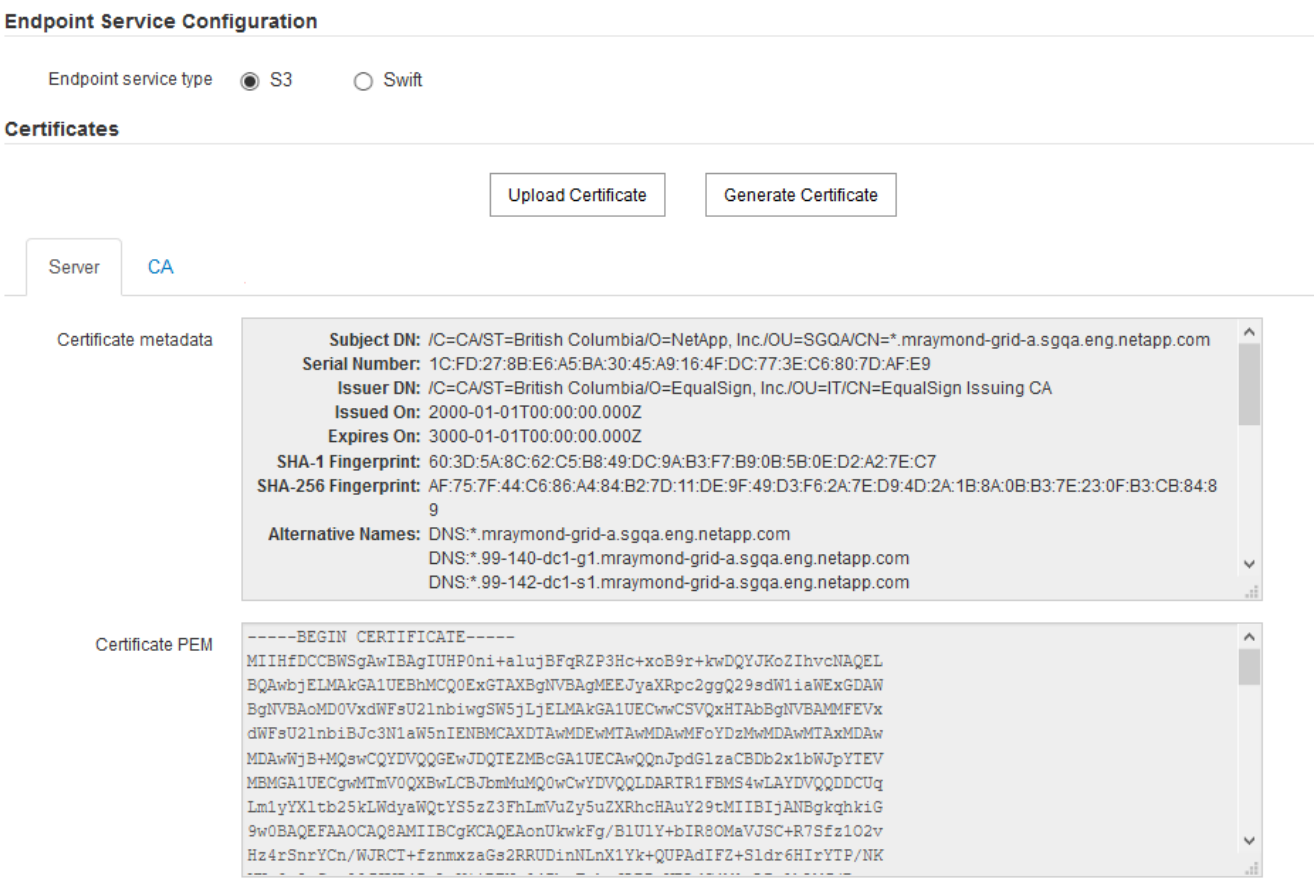
   まもなく期限切れになる証明書を含むエンドポイントが表に示されます。




2. 編集するエンドポイントを選択します。
3. *エンドポイントの編集*をクリックします。

   [Edit Endpoint]ダイアログボックスが表示されます。

   セキュアでない（HTTP）エンドポイントの場合は、ダイアログボックスの[Endpoint Service Configuration]セクションだけが表示されます。セキュア（HTTPS）エンドポイントの場合、次の例に示すように、ダイアログボックスの[Endpoint Service Configuration]セクションと[Certificates]セクションが表示されます。




4. エンドポイントに必要な変更を加えます。

   セキュアでない（HTTP）エンドポイントの場合、次の操作を実行できます。

- エンドポイントのサービスタイプをS3またはSwiftに変更します。
- エンドポイントバインディングモードを変更します。セキュアな（HTTPS）エンドポイントの場合、次の操作を実行できます。
- エンドポイントのサービスタイプをS3またはSwiftに変更します。
- エンドポイントバインディングモードを変更します。
- セキュリティ証明書を表示します。
- 現在の証明書の有効期限が切れたとき、または有効期限が近づいたときに、新しいセキュリティ証明書をアップロードまたは生成します。

  タブを選択して、デフォルトのStorageGRID サーバ証明書またはアップロードされたCA署名証明書に関する詳細情報を表示します。

> 既存のエンドポイントのプロトコルを変更する場合は、たとえばHTTPからHTTPSに変更する場合は、新しいエンドポイントを作成する必要があります。ロードバランサエンドポイントの作成手順に従って、必要なプロトコルを選択します。

5. [ 保存（ Save ） ] をクリックします。

関連情報

[ロードバランサエンドポイントの作成]

## ロードバランサエンドポイントの削除

不要になったロードバランサエンドポイントは削除できます。

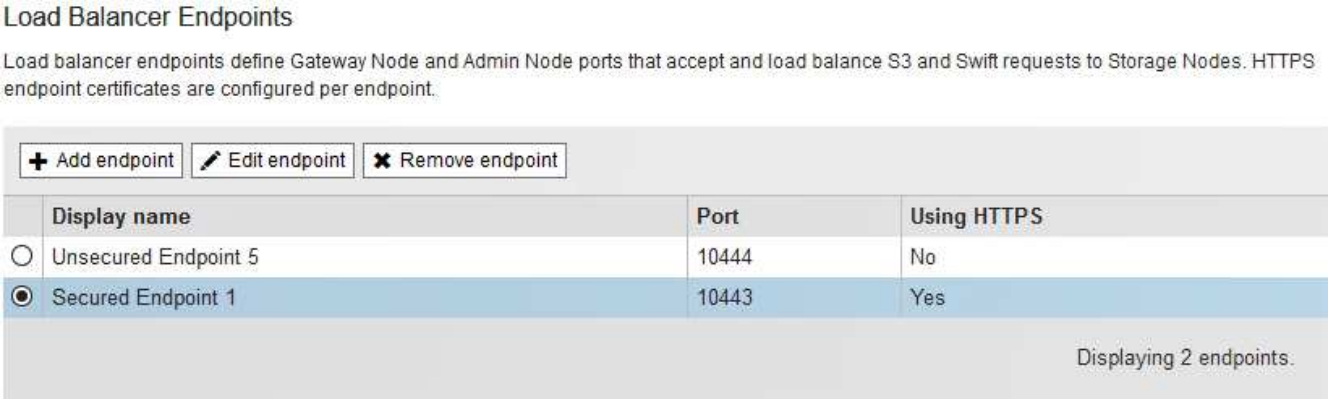
必要なもの

- Root Access 権限が必要です。
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

手順

1. [* Configuration > Network Settings > Load Balancer Endpoints *]を選択します。

   Load Balancer Endpointsページが表示されます。既存のエンドポイントがテーブルに表示されます。




2. 削除するエンドポイントの左側にあるオプションボタンを選択します。

3. [エンドポイントの削除*]をクリックします。

   確認のダイアログボックスが表示されます。

4. [OK] をクリックします。

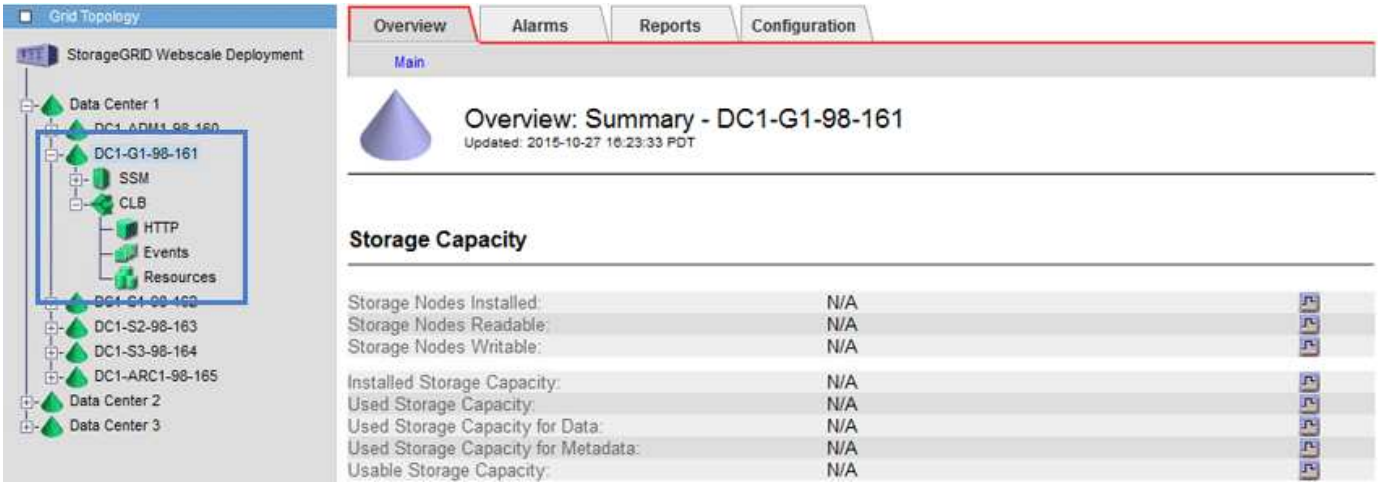
   エンドポイントが削除されます。

ロードバランシングの仕組み **- CLB** サービス

## ゲートウェイノード上の Connection Load Balancer （ CLB ）サービスは廃止されました。ロードバランササービスが推奨されるロードバランシングメカニズムになりました。

CLB サービスはレイヤ 4 ロードバランシングを使用して、可用性、システムの負荷、および管理者が設定したリンクコストに基づいて、クライアントアプリケーションからの受信 TCP ネットワーク接続を最適なストレージノードに分散します。最適なストレージノードが選択されると、 CLB サービスは双方向のネットワーク接続を確立し、選択されたノードとの間でトラフィックを転送します。CLB は、受信ネットワーク接続を転送するときにグリッドネットワーク設定を考慮しません。

CLBサービスに関する情報を表示するには、* Support **>** Tools **>** Grid Topology を選択し、 CLB *とその下のオプションを選択できるようになるまでゲートウェイノードを拡張します。




CLB サービスを使用する場合は、 StorageGRID システムのリンクコストを設定することを検討してください。

関連情報

"リンクコストとは"

"リンクコストを更新しています"

信頼されていないクライアントネットワークの管理

## クライアントネットワークを使用している場合は、明示的に設定されたエンドポイントでのみインバウンドクライアントトラフィックを受け入れることで、悪意のある攻撃から StorageGRID を保護できます。

デフォルトでは、各グリッドノードのクライアントネットワークは *trusted_* です。つまり、StorageGRID は、使用可能なすべての外部ポートでの各グリッドノードへのインバウンド接続をデフォルトで信頼します（ネットワークガイドラインの外部通信に関する情報を参照）。

各ノードのクライアントネットワークを「 *untrusted_* 」に指定することで、 StorageGRID システムに対する悪意ある攻撃の脅威を軽減できます。ノードのクライアントネットワークが信頼されていない場合、ノードはロードバランサエンドポイントとして明示的に設定されたポートのインバウンド接続だけを受け入れます。

例 **1** ：ゲートウェイノードが **HTTPS S3** 要求のみを受け入れる

ゲートウェイノードで、 HTTPS S3 要求を除くクライアントネットワーク上のすべてのインバウンドトラフィックを拒否するとします。この場合、次の一般的な手順を実行します。

1. Load Balancer Endpoints ページで、ポート 443 で S3 over HTTPS のロードバランサエンドポイントを設定します。
2. Untrusted Client Networks ページで、ゲートウェイノードのクライアントネットワークが信頼されていないことを指定します。

設定を保存すると、ポート 443 での HTTPS S3 要求と ICMP エコー（ ping ）要求を除き、ゲートウェイノードのクライアントネットワーク上のすべてのインバウンドトラフィックが破棄されます。

例 **2** ：ストレージノードが **S3** プラットフォームサービス要求を送信する

あるストレージノードからのアウトバウンド S3 プラットフォームサービストラフィックは有効にするが、クライアントネットワークでそのストレージノードへのインバウンド接続は禁止するとします。この場合は、次の手順を実行します。

- Untrusted Client Networks ページで、ストレージノード上のクライアントネットワークが信頼されていないことを指定します。

設定を保存すると、ストレージノードはクライアントネットワークで受信トラフィックを受け入れなくなりますが、 Amazon Web Services へのアウトバウンド要求は引き続き許可します。

関連情報

"ネットワークガイドライン"

"ロードバランサエンドポイントの設定"

ノードのクライアントネットワークの指定は信頼されていません

## クライアントネットワークを使用している場合は、各ノードのクライアントネットワー

クが信頼されているかどうかを指定できます。拡張で追加した新しいノードのデフォルト設定を指定することもできます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限が必要です。
- 管理ノードまたはゲートウェイノードが明示的に設定されたエンドポイントでのみインバウンドトラフィックを受け入れるように設定する場合は、ロードバランサエンドポイントを定義しておきます。

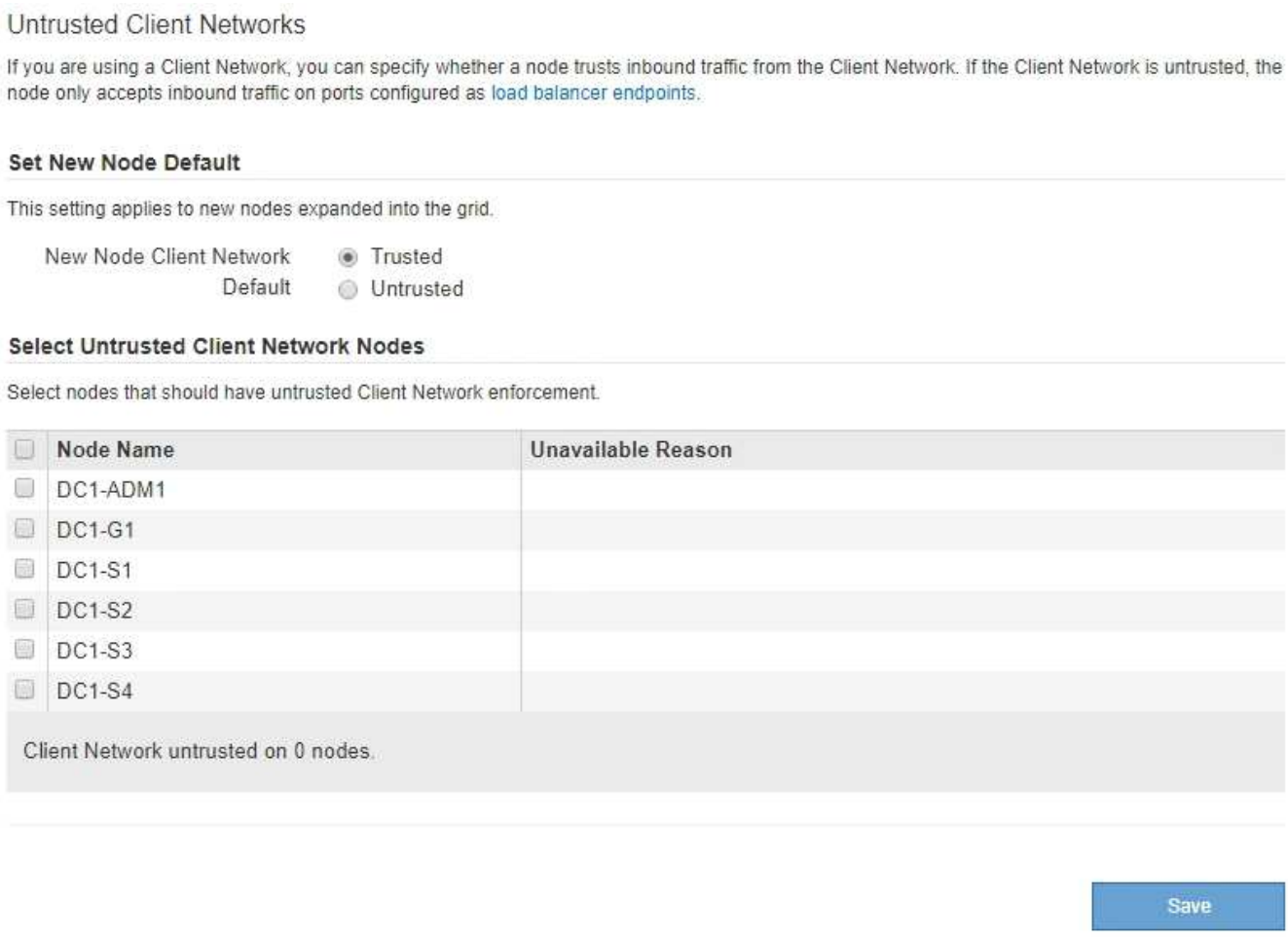
> ロードバランサエンドポイントが設定されていないと、既存のクライアント接続が失敗する可能性があります。

手順

1. 「* Configuration * Network Settings * Untrusted Client Network *」を選択します。

   [Untrusted Client Networks]ページが表示されます。

   このページには、StorageGRID システム内のすべてのノードが表示されます。ノードのクライアントネットワークが信頼されている必要がある場合は、 Unavailable Reason 列にエントリが表示されます。




2. Set New Node Default * セクションで、拡張手順 で新しいノードをグリッドに追加するときのデフォルト設定を指定します。

- * Trusted * ：拡張でノードが追加されるときに、そのクライアントネットワークが信頼されます。
- * Untrusted * ：拡張でノードが追加されるときに、そのクライアントネットワークは信頼されません。必要に応じて、このページに戻って新しいノードの設定を変更できます。

この設定は、 StorageGRID システム内の既存のノードには影響しません。

3. Select Untrusted Client Network Nodes * セクションで、明示的に設定されたロードバランサエンドポイントでのみクライアント接続を許可するノードを選択します。

   タイトルのチェックボックスをオンまたはオフにすると、すべてのノードを選択または選択解除できます。

4. [ 保存（ Save ） ] をクリックします。

   新しいファイアウォールルールがすぐに追加され、適用されます。ロードバランサエンドポイントが設定されていないと、既存のクライアント接続が失敗する可能性があります。

関連情報

"ロードバランサエンドポイントの設定"

ハイアベイラビリティグループの管理

## ハイアベイラビリティ（HA）グループを使用して、S3 / Swiftクライアントに可用性の高いデータ接続を提供できます。HAグループを使用して、Grid ManagerとTenant Managerへの可用性の高い接続を提供することもできます。

- "HAグループとは"
- "HAグループの使用方法"
- "HA グループの設定オプション"
- "ハイアベイラビリティグループを作成する"
- "ハイアベイラビリティグループの編集"
- "ハイアベイラビリティグループを削除しています"

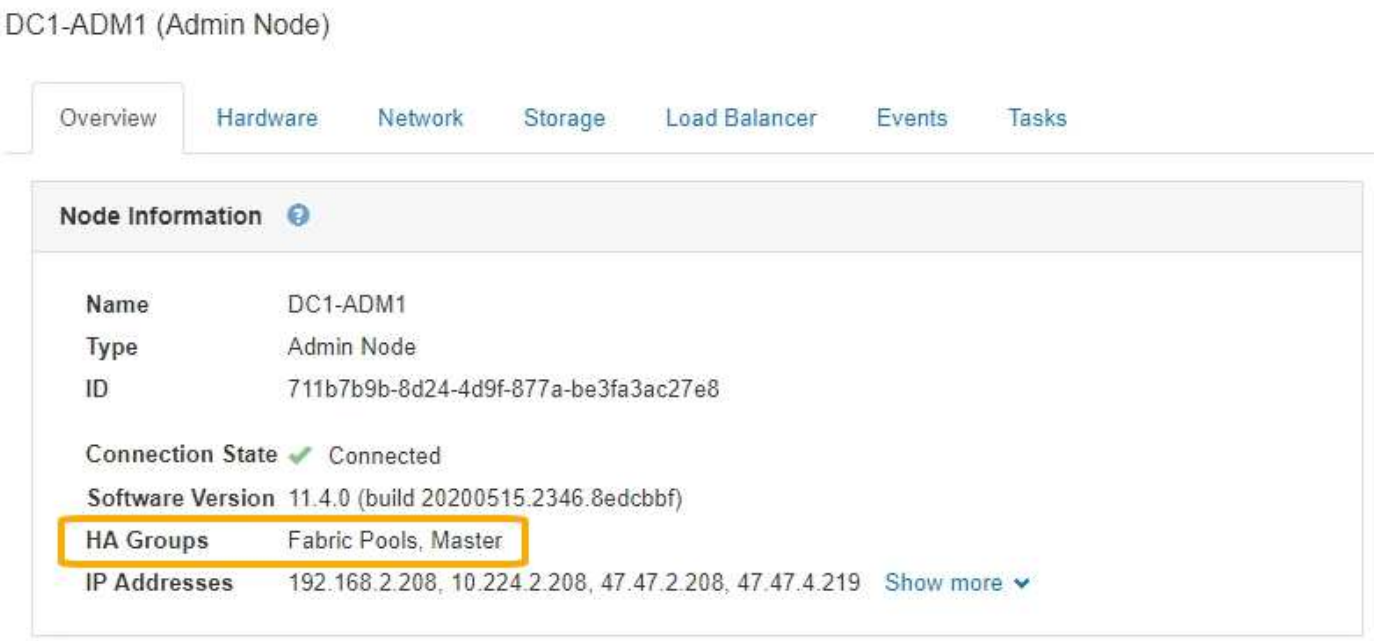
**HA**グループとは

## ハイアベイラビリティグループは、仮想IPアドレス（VIP）を使用してゲートウェイノードまたは管理ノードサービスへのアクティブ/バックアップアクセスを提供します。

HAグループは、管理ノードとゲートウェイノード上の1つ以上のネットワークインターフェイスで構成されます。HAグループを作成するときは、グリッドネットワーク（eth0）またはクライアントネットワーク（eth2）に属するネットワークインターフェイスを選択します。HAグループ内のすべてのインターフェイスは、同じネットワークサブネット内に存在する必要があります。

HAグループは、グループ内のアクティブインターフェイスに追加された仮想IPアドレスを1つ以上維持します。アクティブインターフェイスが使用できなくなった場合、仮想IPアドレスは別のインターフェイスに移動します。このフェイルオーバープロセスにかかる時間は通常数秒です。クライアントアプリケーションへの影響はほとんどなく、通常の再試行で処理を続行できます。

HAグループ内のアクティブインターフェイスがマスターに、他のすべてのインターフェイスは、バックアップとして指定されます。これらの指定を表示するには、* Nodes **>*_node_name >** Overview *を選択します。




HAグループを作成する際には、1つのインターフェイスを優先マスターに指定します。優先マスターは、障害が発生してVIPアドレスがバックアップインターフェイスに再割り当てされない限り、アクティブインターフェイスです。障害が解決されると、VIPアドレスは自動的に優先マスターに戻されます。

フェイルオーバーは、次のいずれかの理由でトリガーされる可能性があります。

- インターフェイスが設定されているノードが停止する。
- インターフェイスが設定されているノードと他のすべてのノードとの接続が少なくとも2分間失われます
- アクティブインターフェイスが停止する。
- ロードバランササービスが停止する。
- ハイアベイラビリティサービスが停止します。

> アクティブインターフェイスをホストするノードの外部でネットワーク障害が発生した場合、フェイルオーバーがトリガーされないことがあります。同様に、 CLB サービス（廃止予定）の障害、またはグリッドマネージャまたはテナントマネージャのサービスの障害によって、フェイルオーバーはトリガーされません。

HAグループに3つ以上のノードのインターフェイスが含まれている場合、フェイルオーバー中にアクティブインターフェイスは他のノードのインターフェイスに移動する可能性があります。

**HA**グループの使用方法

## ハイアベイラビリティ（HA）グループはいくつかの理由で使用できます。

- HA グループは、 Grid Manager または Tenant Manager への可用性の高い管理接続を提供します。
- HA グループは、 S3 / Swift クライアントに可用性の高いデータ接続を提供できます。
- インターフェイスが 1 つしかない HA グループでは、多数の VIP アドレスを指定したり、 IPv6 アドレス

を明示的に設定したりできます。

HA グループは、グループに含まれるすべてのノードが同じサービスを提供する場合にのみ高可用性を提供できます。HA グループを作成するときは、必要なサービスを提供するタイプのノードからインターフェイスを追加してください。

- * 管理ノード * ：ロードバランササービスが含まれ、 Grid Manager またはテナントマネージャへのアクセスを有効にします。
- * ゲートウェイノード * ：ロードバランササービスと CLB サービス（廃止）が含まれます。

| **HA** グループの目的 | このタイプのノードを **HA** グループに追加します |
| --- | --- |
| Grid Manager へのアクセス | • プライマリ管理ノード（優先マスター）<br>• 非プライマリ管理ノード<br><br>*注：*プライマリ管理ノードが優先マスターである必要があります。一部のメンテナンス手順は、プライマリ管理ノードでしか実行できません。 |
| Tenant Manager のみにアクセスします | • プライマリ管理ノードまたは非プライマリ管理ノード |
| S3 または Swift クライアントアクセス - ロードバランササービス | • 管理ノード<br>• ゲートウェイノード |
| S3 または Swift クライアントアクセス - CLB サービス<br><br>• 注： * CLB サービスは廃止されました。 | • ゲートウェイノード |

**Grid Manager** または **Tenant Manager** で **HA** グループを使用する場合の制限事項

Grid ManagerまたはTenant Managerのサービスで障害が発生しても、HAグループ内でフェイルオーバーはトリガーされません。

フェイルオーバーの発生時に Grid Manager または Tenant Manager にサインインしている場合はサインアウトされるため、再度サインインしてタスクを再開する必要があります。

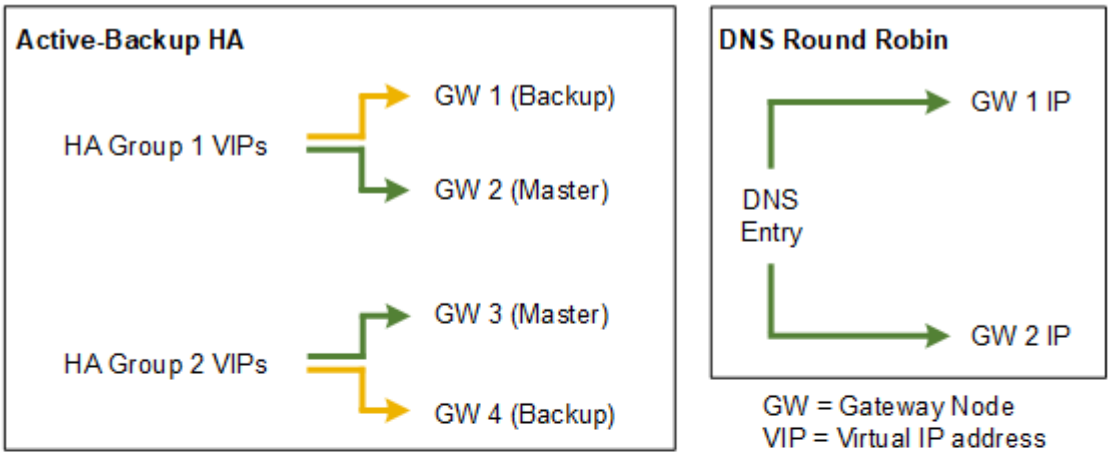
プライマリ管理ノードを使用できない場合は、一部のメンテナンス手順を実行できません。フェイルオーバー中は、 Grid Manager を使用して StorageGRID システムを監視できます。

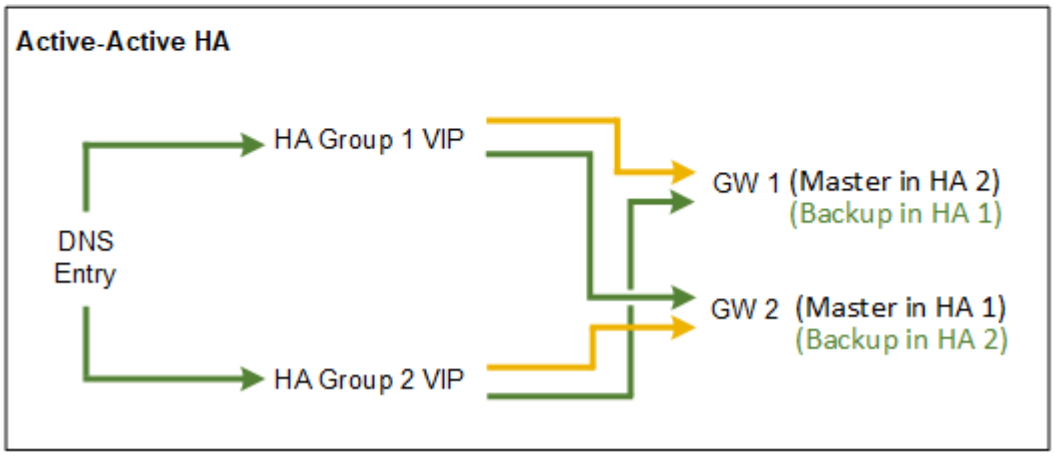
**CLB** サービスで **HA** グループを使用する場合の制限事項

CLB サービスに障害が発生しても、 HA グループ内でフェイルオーバーはトリガーされません。

CLB サービスは廃止されました。

次の図は、 HA グループのさまざまな構成例を示しています。各オプションには長所と短所があります。




「アクティブ/アクティブHA」の例に示すように、複数の重複するHAグループを作成する場合、合計スループットはノード数とHAグループ数が増えるほど上昇します。ノードとHAグループをそれぞれ3つ以上配置すると、1つのノードをオフラインにする必要があるメンテナンス手順の実行中も、いずれかのVIPを使用して処理を継続できます。

次の表は、図に示す各 HA 構成のメリットをまとめたものです。

| 設定 | 利点 | 欠点 |
| --- | --- | --- |
| アクティブ / バックアップ HA | • StorageGRID で管理され、外部のコンポーネントを必要としません。<br>• 高速フェイルオーバー。 | • HA グループ内の 1 つのノードだけがアクティブです。各 HA グループで少なくとも 1 つのノードがアイドル状態になります。 |

| 設定 | 利点 | 欠点 |
| --- | --- | --- |
| DNS ラウンドロビン | • 総スループットが向上します。<br>• アイドル状態のホストはありません。 | • クライアントの動作によってはフェイルオーバーが低速になる可能性があります。<br>• StorageGRID の外部でハードウェアを構成する必要があります。<br>• ユーザによる健全性チェックが必要です。 |
| アクティブ/アクティブ | • トラフィックが複数の HA グループに分散されます。<br>• HA グループの数が増えるほど総スループットが向上します。<br>• 高速フェイルオーバー。 | • 設定がより複雑になります。<br>• StorageGRID の外部でハードウェアを構成する必要があります。<br>• ユーザによる健全性チェックが必要です。 |

ハイアベイラビリティグループを作成する

# 1つ以上のハイアベイラビリティ（HA）グループを作成して、管理ノードまたはゲートウェイノード上のサービスへの可用性の高いアクセスを提供できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限が必要です。

このタスクについて

HAグループに追加するインターフェイスは次の条件を満たしている必要があります。

- インターフェイスは、ゲートウェイノードまたは管理ノードのものである必要があります。
- インターフェイスはグリッドネットワーク（eth0）またはクライアントネットワーク（eth2）に属している必要があります。
- インターフェイスには、DHCPではなく固定IPアドレスまたは静的IPアドレスを設定する必要があります。

手順

1. * Configuration > Network Settings > High Availability Groups *を選択します。

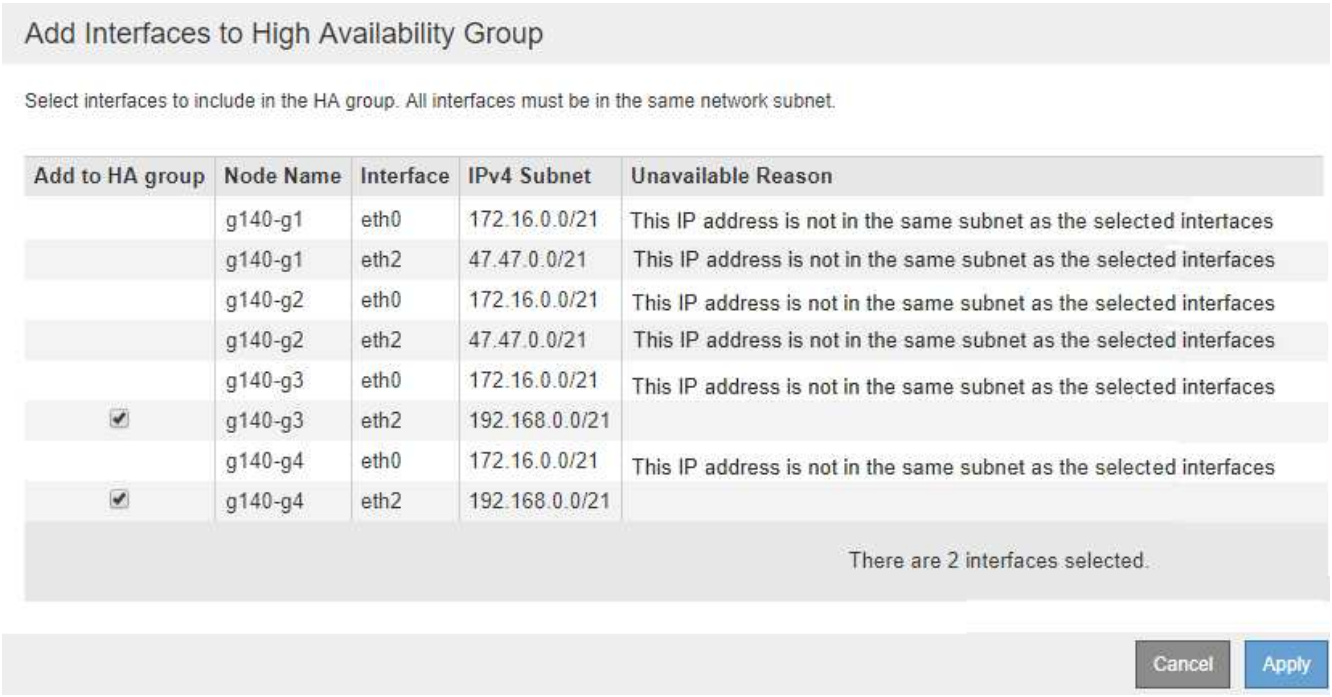
   [High Availability Groups]ページが表示されます。

2. [ 作成（ Create ） ] をクリックします。

   Create High Availability Groupダイアログボックスが表示されます。

3. HAグループの名前を入力し、必要に応じて概要 を入力します。
4. [Select Interfaces]をクリックします。

   Add Interfaces to High Availability Groupダイアログボックスが表示されます。この表には、使用可能なノード、インターフェイス、およびIPv4サブネットが表示されます。




   IPアドレスがDHCPによって割り当てられている場合、インターフェイスはリストに表示されません。

5. Add to HA group *列で、HAグループに追加するインターフェイスのチェックボックスを選択します。

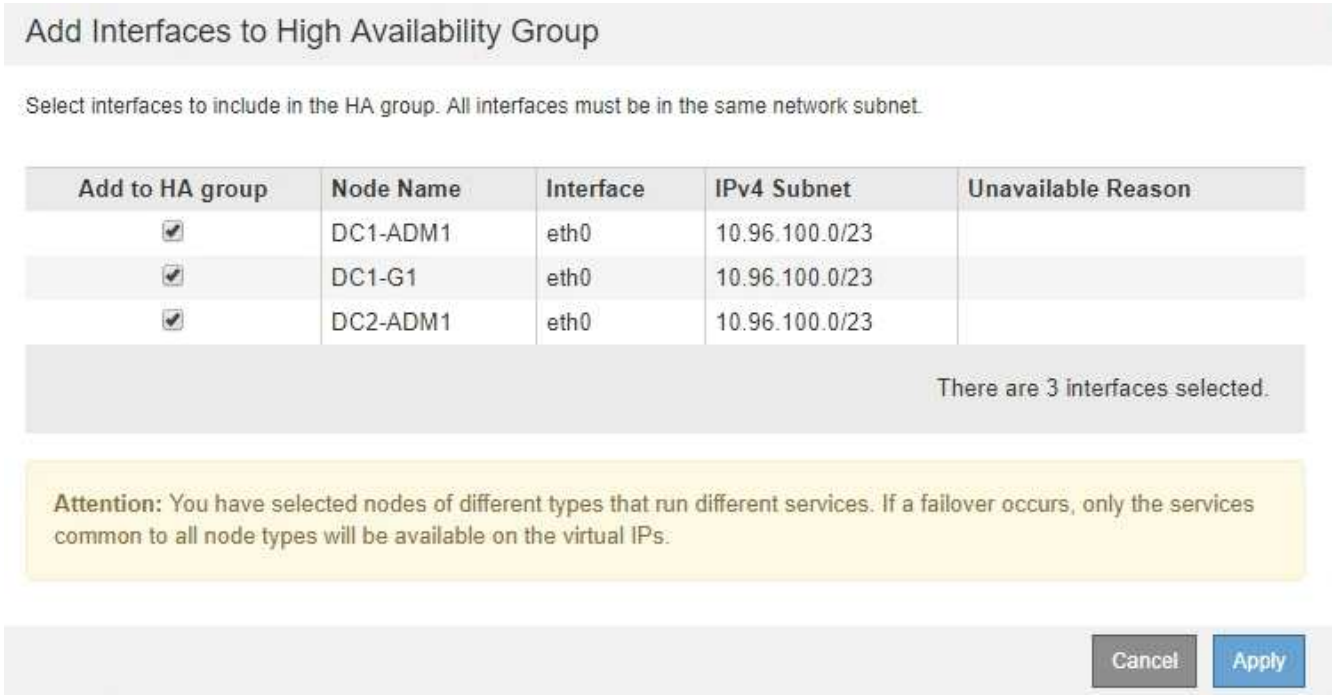
   インターフェイスの選択に関する次のガイドラインに注意してください。

   - インターフェイスを少なくとも 1 つ選択してください。
   - 複数のインターフェイスを選択する場合は、すべてのインターフェイスがグリッドネットワーク（eth0）またはクライアントネットワーク（eth2）上に存在する必要があります。
   - すべてのインターフェイスは、同じサブネット内または共通のプレフィックスを持つサブネット内に存在する必要があります。

IPアドレスは最小のサブネット（最大のプレフィックスを持つサブネット）に制限されます。

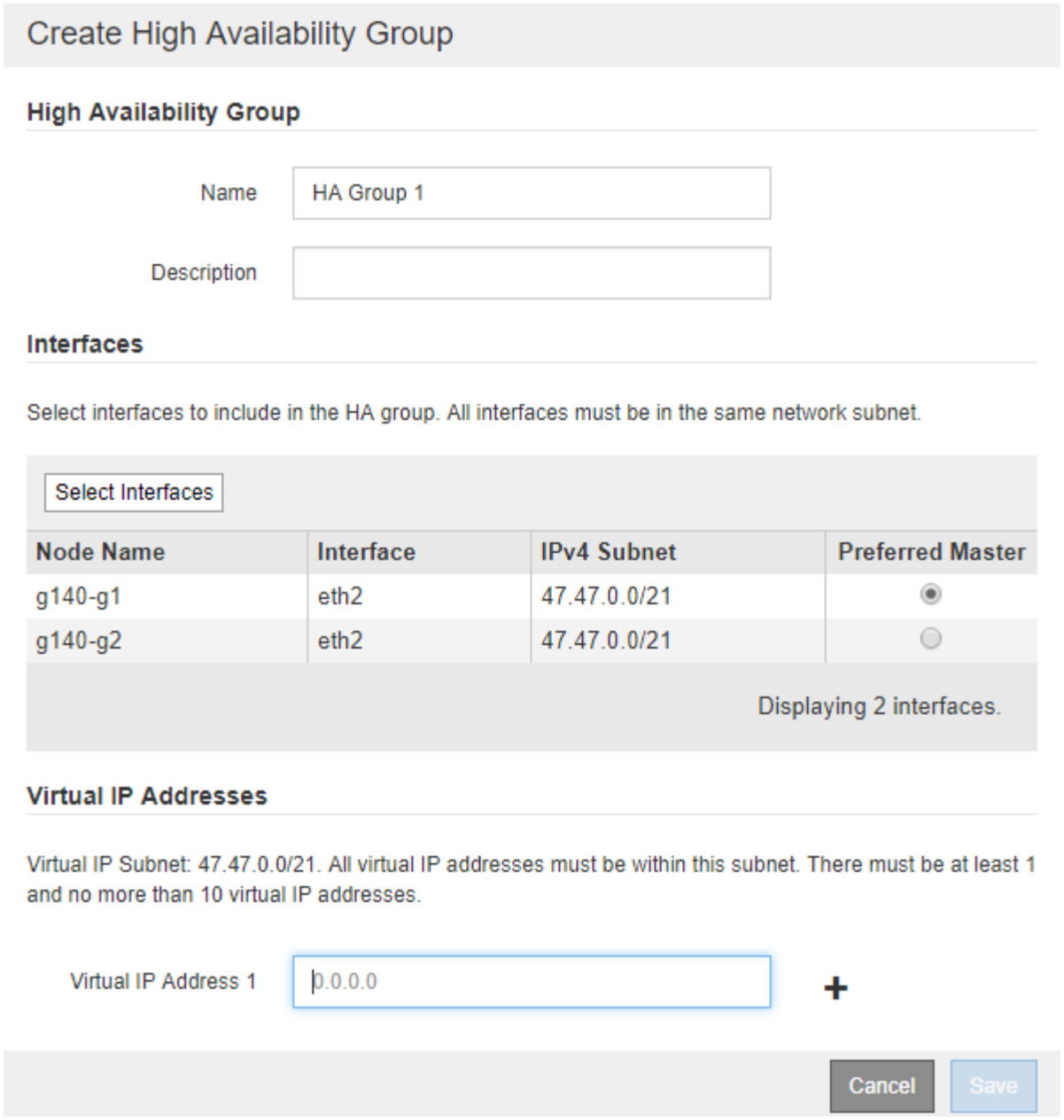
- 異なるタイプのノード上のインターフェイスを選択した場合、フェイルオーバーが発生すると、選択したノードに共通するサービスのみが仮想IPで使用可能になります。
  - Grid ManagerまたはTenant ManagerのHA保護用に2つ以上の管理ノードを選択します。
  - ロードバランササービスのHA保護を利用する場合は、管理ノード、ゲートウェイノード、またはその両方を2つ以上選択します。
  - CLBサービスのHA保護を行うゲートウェイノードを2つ以上選択します。

    CLB サービスは廃止されました。




6. [ 適用（ Apply ） ] をクリックします。

選択したインターフェイスは、Create High Availability GroupページのInterfacesセクションに表示されます。デフォルトでは、リストの最初のインターフェイスが優先マスターとして選択されます。




7. 別のインターフェイスを優先マスターにする場合は、[* Preferred Master*（優先マスター*）]列でそのインターフェイスを選択します。

   優先マスターは、障害が発生してVIPアドレスがバックアップインターフェイスに再割り当てされない限り、アクティブインターフェイスです。

   HAグループがGrid Managerへのアクセスを提供する場合は、プライマリ管理ノード上のインターフェイスを優先マスターとして選択する必要があります。一部のメンテナンス手順は、プライマリ管理ノードでしか実行できません。

8. ページの仮想IPアドレスセクションに、HAグループの仮想IPアドレスを1~10個入力します。プラス記号（+）をクリックして、複数のIPアドレスを追加します。

   IPv4 アドレスを少なくとも 1 つ指定する必要があります。必要に応じて、追加の IPv4 アドレスと IPv6 アドレスを指定できます。

IPv4アドレスは、すべてのメンバーインターフェイスで共有されるIPv4サブネット内にある必要があります。

9. [ 保存（ Save ） ] をクリックします。

   HA グループが作成され、設定済みの仮想 IP アドレスを使用できるようになります。

関連情報

"Red Hat Enterprise Linux または CentOS をインストールします"

"VMware をインストールする"

"Ubuntu または Debian をインストールします"

"負荷分散の管理"

ハイアベイラビリティグループの編集

# ハイアベイラビリティ（HA）グループを編集して、グループ名や概要 を変更したり、インターフェイスを追加または削除したり、仮想IPアドレスを追加または更新したりできます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限が必要です。

このタスクについて

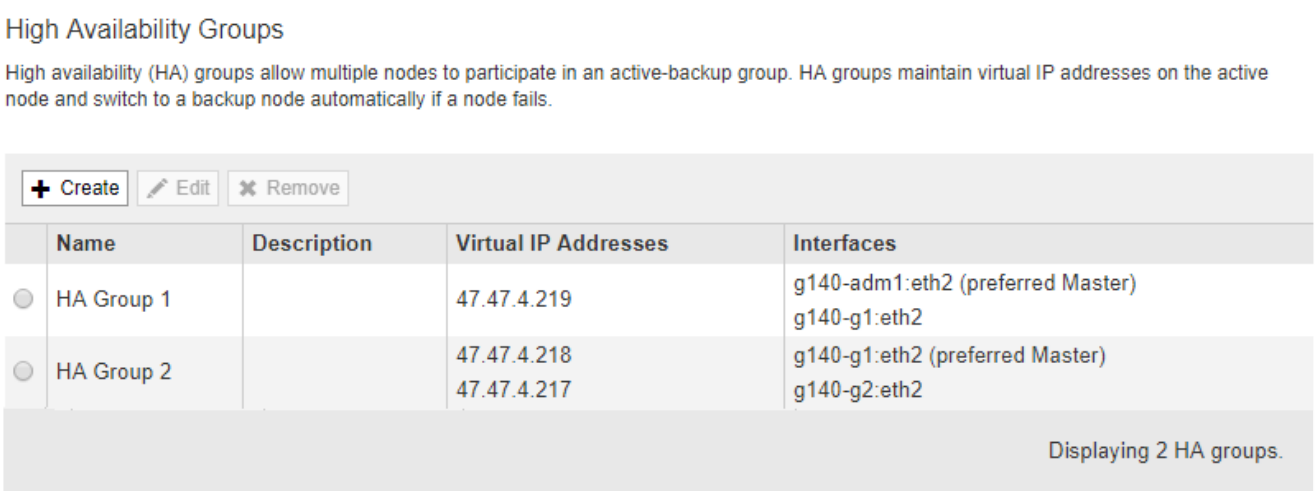
HAグループを編集する理由には、次のようなものがあります。

- 既存のグループにインターフェイスを追加しています。すでにグループに割り当てられている他のインターフェイスと同じサブネット内のインターフェイスのIPアドレスを指定する必要があります。
- HAグループからのインターフェイスの削除たとえば、グリッドネットワークまたはクライアントネットワークのノードのインターフェイスがHAグループで使用されている場合、サイトの開始や手順 のノードの運用停止はできません。

手順

1. * Configuration > Network Settings > High Availability Groups *を選択します。

   [High Availability Groups]ページが表示されます。

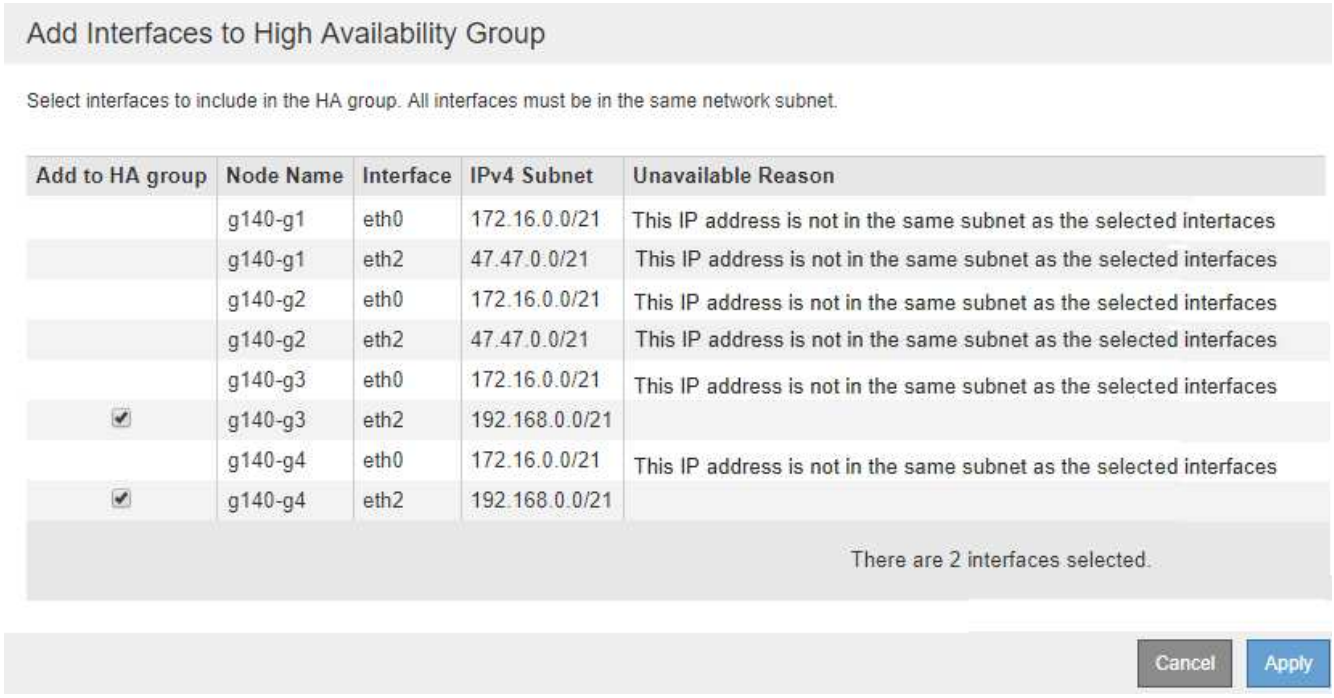



2. 編集するHAグループを選択し、* Edit *をクリックします。

   Edit High Availability Groupダイアログボックスが表示されます。

3. 必要に応じて、グループの名前または概要 を更新します。
4. 必要に応じて、* Select interfaces *をクリックして、HAグループのインターフェイスを変更します。

   Add Interfaces to High Availability Groupダイアログボックスが表示されます。




   IPアドレスがDHCPによって割り当てられている場合、インターフェイスはリストに表示されません。

5. チェックボックスをオンまたはオフにして、インターフェイスを追加または削除します。

   インターフェイスの選択に関する次のガイドラインに注意してください。

   ◦ インターフェイスを少なくとも 1 つ選択してください。

- 複数のインターフェイスを選択する場合は、すべてのインターフェイスがグリッドネットワーク（eth0）またはクライアントネットワーク（eth2）上に存在する必要があります。
- すべてのインターフェイスは、同じサブネット内または共通のプレフィックスを持つサブネット内に存在する必要があります。

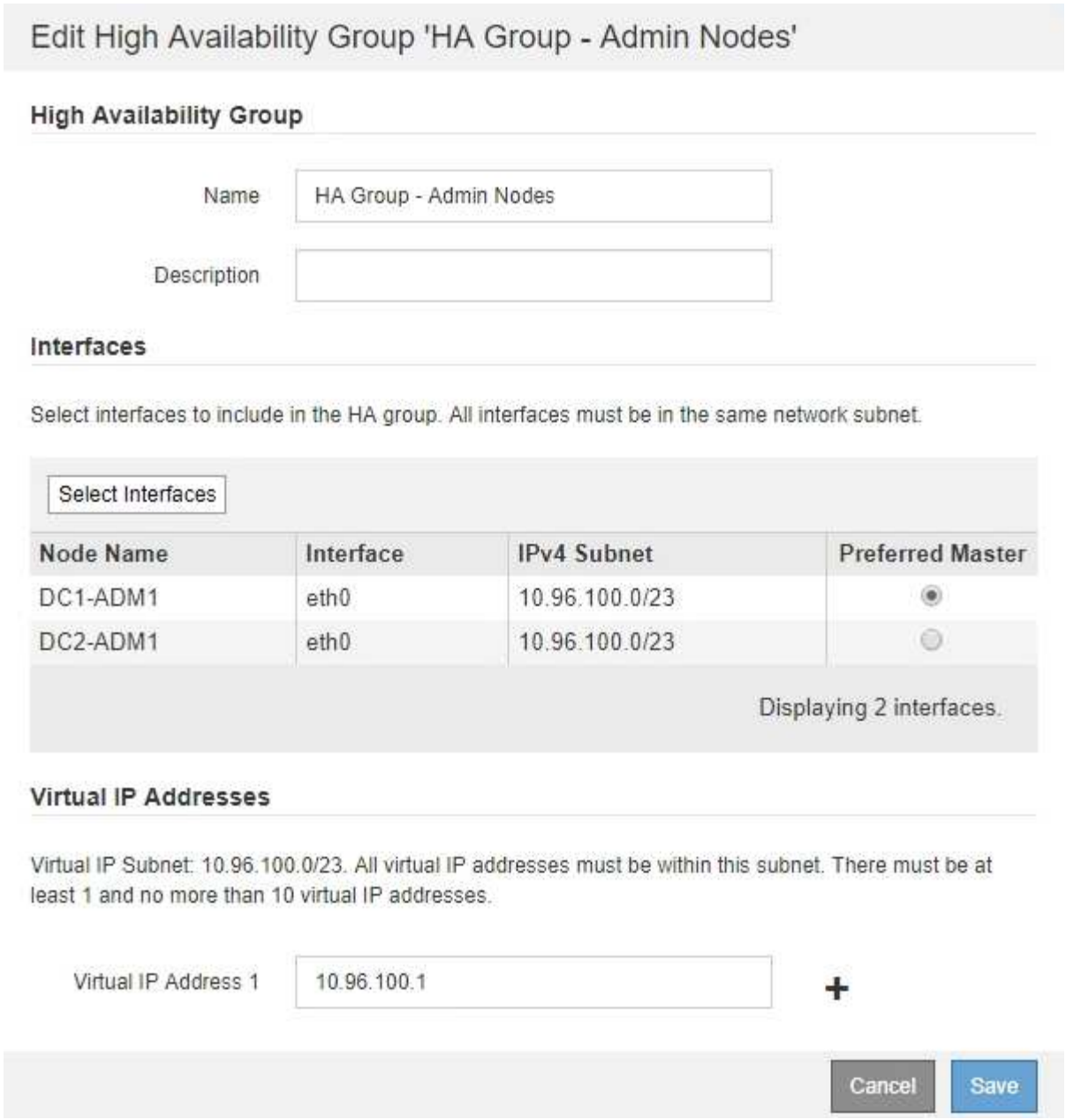
  IPアドレスは最小のサブネット（最大のプレフィックスを持つサブネット）に制限されます。

- 異なるタイプのノード上のインターフェイスを選択した場合、フェイルオーバーが発生すると、選択したノードに共通するサービスのみが仮想IPで使用可能になります。
  - Grid ManagerまたはTenant ManagerのHA保護用に2つ以上の管理ノードを選択します。
  - ロードバランササービスのHA保護を利用する場合は、管理ノード、ゲートウェイノード、またはその両方を2つ以上選択します。
  - CLBサービスのHA保護を行うゲートウェイノードを2つ以上選択します。

    CLB サービスは廃止されました。

6. [ 適用（ Apply ） ] をクリックします。

   選択したインターフェイスがページのインターフェイスセクションに表示されます。デフォルトでは、リストの最初のインターフェイスが優先マスターとして選択されます。




7. 別のインターフェイスを優先マスターにする場合は、[* Preferred Master*（優先マスター*）]列でそのインターフェイスを選択します。

   優先マスターは、障害が発生してVIPアドレスがバックアップインターフェイスに再割り当てされない限り、アクティブインターフェイスです。

   HAグループがGrid Managerへのアクセスを提供する場合は、プライマリ管理ノード上のインターフェイスを優先マスターとして選択する必要があります。一部のメンテナンス手順は、プライマリ管理ノードでしか実行できません。

8. 必要に応じて、HAグループの仮想IPアドレスを更新します。

   IPv4 アドレスを少なくとも 1 つ指定する必要があります。必要に応じて、追加の IPv4 アドレスと IPv6 アドレスを指定できます。

   IPv4アドレスは、すべてのメンバーインターフェイスで共有されるIPv4サブネット内にある必要がありま

す。

9. [ 保存（ Save ） ] をクリックします。

   HAグループが更新されました。

ハイアベイラビリティグループを削除しています

# 使用しなくなったハイアベイラビリティ（HA）グループを削除できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限が必要です。

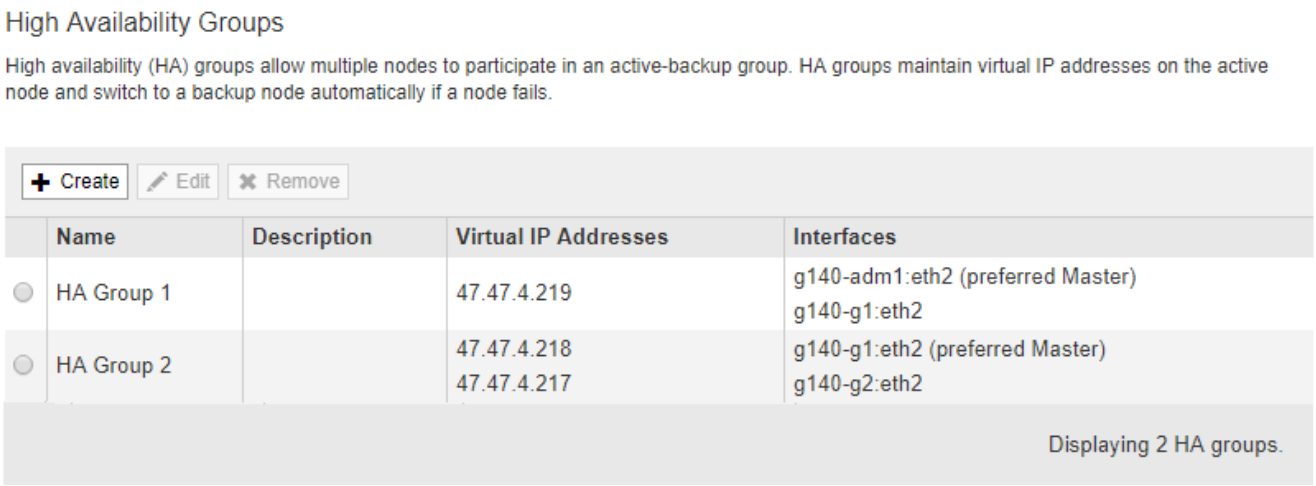
このタスクを実行します

HAグループを削除すると、そのグループのいずれかの仮想IPアドレスを使用するように設定されているS3またはSwiftクライアントはStorageGRID に接続できなくなります。クライアントの停止を回避するには、該当するS3またはSwiftクライアントアプリケーションをすべて更新してからHAグループを削除する必要があります。各クライアントを更新して、別のIPアドレスを使用して接続します。たとえば、別のHAグループの仮想IPアドレスや、インストール時またはDHCPを使用してインターフェイスに設定されたIPアドレスなどです。

手順

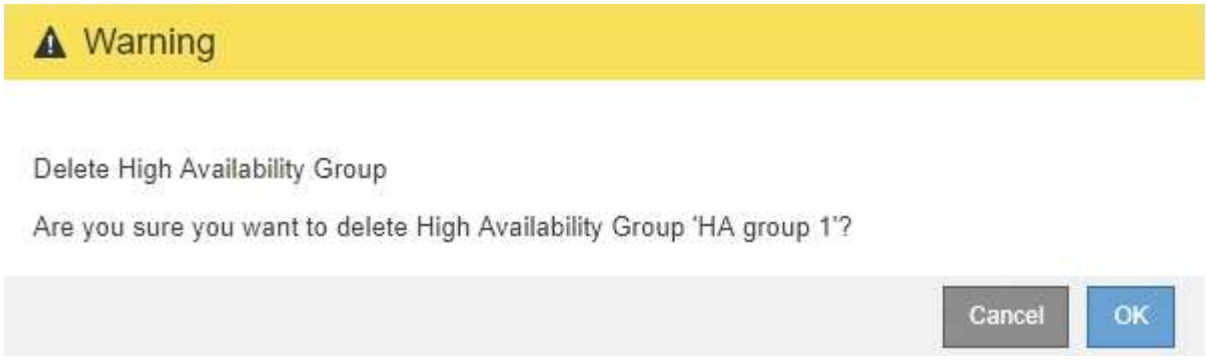
1. * Configuration > Network Settings > High Availability Groups *を選択します。

   [High Availability Groups]ページが表示されます。




2. 削除するHAグループを選択し、* Remove *をクリックします。

   Delete High Availability Groupという警告が表示されます。




3. [OK] をクリックします。

   HAグループが削除されます。

**S3 API**エンドポイントのドメイン名を設定しています

## S3 仮想ホスト形式の要求をサポートするには、 Grid Manager を使用して、 S3 クライアントの接続先となるエンドポイントのドメイン名のリストを設定する必要があります。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- グリッドのアップグレードが進行中でないことを確認しておく必要があります。

  ドメイン名の設定は、グリッドのアップグレードの進行中は変更しないでください。

このタスクについて

クライアントがS3エンドポイントのドメイン名を使用できるようにするには、次の作業をすべて実行する必要があります。

- Grid Manager を使用して、 S3 エンドポイントのドメイン名を StorageGRID システムに追加します。
- クライアントが StorageGRID への HTTPS 接続に使用する証明書が、クライアントが必要とするすべてのドメイン名に対して署名されていることを確認します。

  たとえば、エンドポイントがの場合などです `s3.company.com`、HTTPS接続に使用する証明書にが含まれていることを確認する必要があります `s3.company.com` エンドポイントとエンドポイントのワイルドカードSubject Alternative Name（SAN）： `*.s3.company.com`。

- クライアントが使用する DNS サーバを設定します。クライアントが接続に使用する IP アドレスの DNS レコードを含め、ワイルドカード名を含む必要なすべてのエンドポイントドメイン名をレコードが参照するようにします。

クライアントは、ゲートウェイノード、管理ノード、またはストレージノードの IP アドレスを使用するか、ハイアベイラビリティグループの仮想 IP アドレスに接続することで、StorageGRID に接続できます。DNS レコードに正しい IP アドレスを追加するためには、クライアントアプリケーションがグリッドに接続する方法を理解しておく必要があります。

クライアントがHTTPS接続に使用する証明書は、クライアントがグリッドに接続する方法によって異なります。

- ロードバランササービスを使用して接続する場合、クライアントは特定のロードバランサエンドポイント用の証明書を使用します。

  各ロードバランサエンドポイントには独自の証明書があり、異なるエンドポイントドメイン名を認識するように各エンドポイントを設定できます。

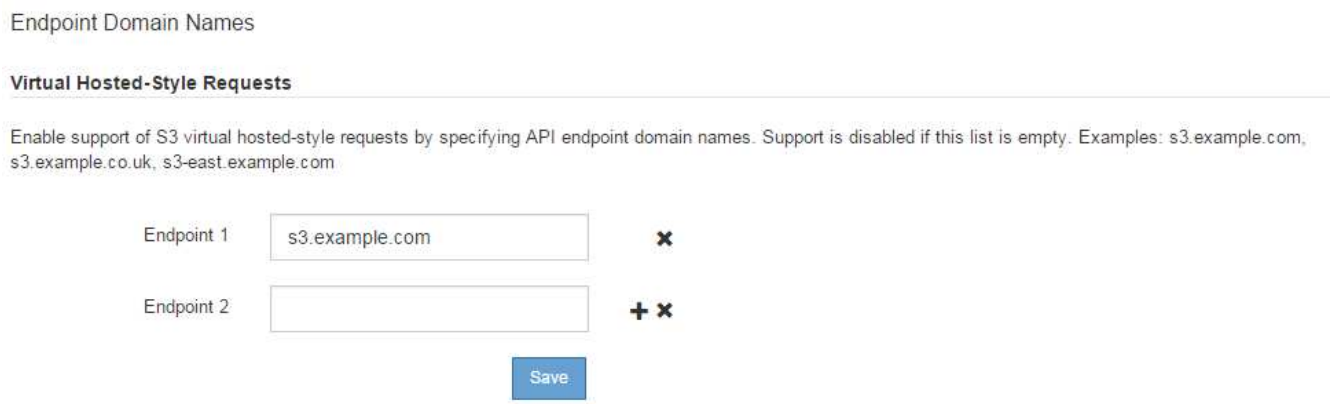
- クライアントがストレージノードまたはゲートウェイノード上のCLBサービスに接続する場合、クライアントは、必要なエンドポイントのドメイン名をすべて追加して更新されたグリッドのカスタムサーバ証明書を使用します。

  CLB サービスは廃止されました。

手順

1. [環境設定]>[ネットワーク設定]>[ドメイン名]を選択します。

   [Endpoint Domain Names] ページが表示されます。




2. （+）アイコンを使用してフィールドを追加し、* Endpoint *フィールドにS3 APIエンドポイントのドメイン名のリストを入力します。

   このリストが空の場合、 S3 仮想ホスト形式の要求のサポートは無効になります。

3. [ 保存（ Save ） ] をクリックします。
4. クライアントが使用するサーバ証明書が、必要なエンドポイントのドメイン名と一致していることを確認します。
   - ロードバランササービスを使用するクライアントの場合は、クライアントが接続するロードバランサエンドポイントに関連付けられている証明書を更新します。

◦ ストレージノードに直接接続するクライアント、またはゲートウェイノード上のCLBサービスを使用するクライアントの場合は、グリッドのカスタムサーバ証明書を更新します。

5. エンドポイントのドメイン名要求を解決するために必要な DNS レコードを追加します。

結果

これで、クライアントがエンドポイントを使用するようになります `bucket.s3.company.com`を指定すると、DNSサーバが正しいエンドポイントに解決され、証明書がエンドポイントを認証します。

関連情報

"S3 を使用する"

"IPアドレスを表示しています"

"ハイアベイラビリティグループを作成する"

"ストレージノードまたはCLBサービスへの接続用のカスタムサーバ証明書を設定する"

"ロードバランサエンドポイントの設定"

## クライアント通信での**HTTP**の有効化

デフォルトでは、クライアントアプリケーションは、ストレージノードへのすべての接続、またはゲートウェイノード上の廃止された CLB サービスへのすべての接続に、HTTPS ネットワークプロトコルを使用します。非本番環境のグリッドのテストなどの目的で、これらの接続に対して HTTP を有効にすることもできます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

S3 / Swift クライアントがストレージノードへの HTTP 接続を直接確立する必要がある場合、またはゲートウェイノード上の廃止された CLB サービスへの HTTP 接続を確立する必要がある場合にのみ、このタスクを実行します。

HTTPS 接続のみを使用するクライアント、またはロードバランササービスに接続するクライアントでは、（各ロードバランサエンドポイントで HTTP または HTTPS を使用するように設定できるため）このタスクを実行する必要はありません。詳細については、ロードバランサエンドポイントの設定に関する情報を参照してください。

を参照してください "Summary ：クライアント接続の IP アドレスとポート" ストレージノードへの接続時、または HTTP または HTTPS を使用して廃止された CLB サービスへの接続時に使用するポート S3 および Swift クライアントを取得する

> 要求が暗号化されずに送信されるため、本番環境のグリッドで HTTP を有効にする場合は注意してください。

手順

1. 「環境設定*システム設定*グリッドオプション*」を選択します。

2. [ ネットワークオプション ] セクションで、 [* HTTP 接続を有効にする *] チェックボックスをオンにします。

3. [ 保存（ Save ） ] をクリックします。

関連情報

"ロードバランサエンドポイントの設定"

"S3 を使用する"

"Swift を使用します"

許可するクライアント処理の制御

## PreventClientModification グリッドオプションを選択して、特定の HTTP クライアント処理を拒否することができます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

クライアント変更の禁止は、システム全体の設定です。[ クライアント変更を禁止する ] オプションを選択すると、次の要求が拒否されます。

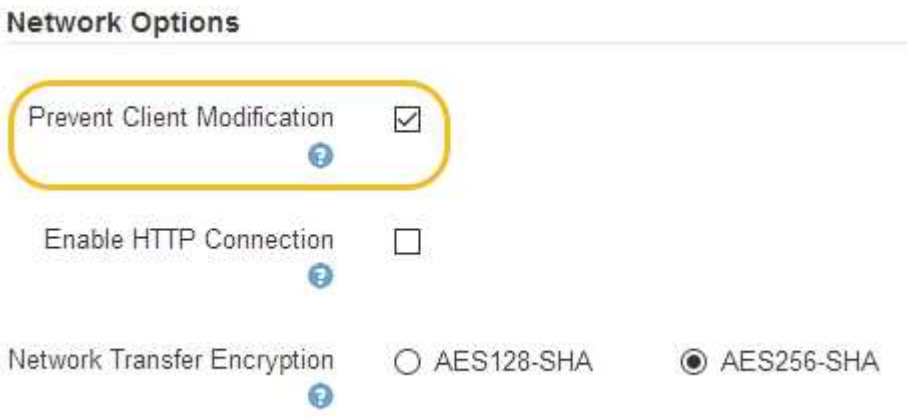
- * S3 REST API *
  - バケットの削除要求
  - 既存オブジェクトのデータ、ユーザ定義メタデータ、または S3 オブジェクトのタグを変更するすべての要求

> この設定は、バージョン管理が有効なバケットには適用されません。バージョン管理によって、すでにオブジェクトデータ、ユーザ定義メタデータ、オブジェクトのタグを変更できないようになっています。

- * Swift REST API *
  - コンテナの削除要求
  - 既存のオブジェクトを変更する要求。たとえば、 Put Overwrite 、 Delete 、 Metadata Update などの処理が拒否されます。

手順

1. 「環境設定*システム設定*グリッドオプション*」を選択します。
2. [ ネットワークオプション ] セクションで、 [ クライアントの変更を禁止する *] チェックボックスをオンにします。




3. [ 保存（ Save ） ] をクリックします。

## StorageGRID ネットワークと接続の管理

グリッドマネージャを使用して、 StorageGRID のネットワークと接続を設定および管理できます。

を参照してください "S3およびSwiftクライアント接続の設定" を参照して、 S3 または Swift クライアントを接続する方法を確認してください。

- "StorageGRID ネットワークのガイドライン"
- "IPアドレスを表示しています"
- "発信 TLS 接続でサポートされる暗号"
- "ネットワーク転送の暗号化の変更"
- "サーバ証明書の設定"
- "ストレージプロキシを設定しています"
- "管理プロキシの設定"
- "トラフィック分類ポリシーの管理"
- "リンクコストとは"

### StorageGRID ネットワークのガイドライン

StorageGRID では、グリッドノードあたり最大 3 つのネットワークインターフェイスがサポートされ、各グリッドノードのネットワークをセキュリティやアクセスの要件に応じて設定することができます。

グリッドノードのネットワークを変更または追加するには、リカバリとメンテナンスの手順を参照してください。ネットワークトポロジの詳細については、ネットワークの手順を参照してください。

**Grid** ネットワーク

必須グリッドネットワークは、すべての内部 StorageGRID トラフィックに使用されます。このネットワークによって、グリッド内のすべてのノードが、すべてのサイトおよびサブネットにわたって相互に接続されます。

管理ネットワーク

任意。通常、管理ネットワークはシステムの管理とメンテナンスに使用されます。クライアントプロトコルアクセスにも使用できます。管理ネットワークは通常はプライベートネットワークであり、サイト間でルーティング可能にする必要はありません。

クライアントネットワーク

任意。クライアントネットワークはオープンネットワークで、主に S3 および Swift クライアントアプリケーションへのアクセスに使用されます。そのため、グリッドネットワークを分離してセキュリティを確保できます。クライアントネットワークは、ローカルゲートウェイ経由でアクセス可能なすべてのサブネットと通信できます。

ガイドライン

- 各 StorageGRID グリッドノードには、割り当て先のネットワークごとに専用のネットワークインターフェイス、 IP アドレス、サブネットマスク、およびゲートウェイが必要です。
- 1 つのグリッドノードに複数のインターフェイスを設定することはできません。
- 各ネットワークのグリッドノードごとに、単一のゲートウェイがサポートされます。このゲートウェイはノードと同じサブネット上に配置する必要があります。必要に応じて、より複雑なルーティングをゲートウェイに実装できます。
- 各ノードでは、各ネットワークが特定のネットワークインターフェイスにマッピングされます。

| ネットワーク | インターフェイス名 |
| --- | --- |
| グリッド（ Grid ） | eth0 |
| 管理（オプション） | Eth1 |
| クライアント（オプション） | eth2 |

- ノードが StorageGRID アプライアンスに接続されている場合は、ネットワークごとに特定のポートが使用されます。詳細については、使用しているアプライアンスのインストール手順を参照してください。
- デフォルトルートはノードごとに自動的に生成されます。eth2 が有効な場合、 0.0.0.0/0 は eth2 のクライアントネットワークを使用します。eth2 が無効な場合、 0.0.0.0/0 は eth0 のグリッドネットワークを使用します。
- クライアントネットワークは、グリッドノードがグリッドに参加するまで動作状態になりません
- グリッドが完全にインストールされる前にインストールユーザインターフェイスにアクセスできるよう

に、グリッドノード導入時に管理ネットワークを設定できます。

関連情報

""

"ネットワークガイドライン"

**IP**アドレスを表示しています

StorageGRID システムの各グリッドノードの IP アドレスを表示できます。コマンドラインでこの IP アドレスを使用してグリッドノードにログインし、さまざまなメンテナンス手順を実行できます。

必要なもの

Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

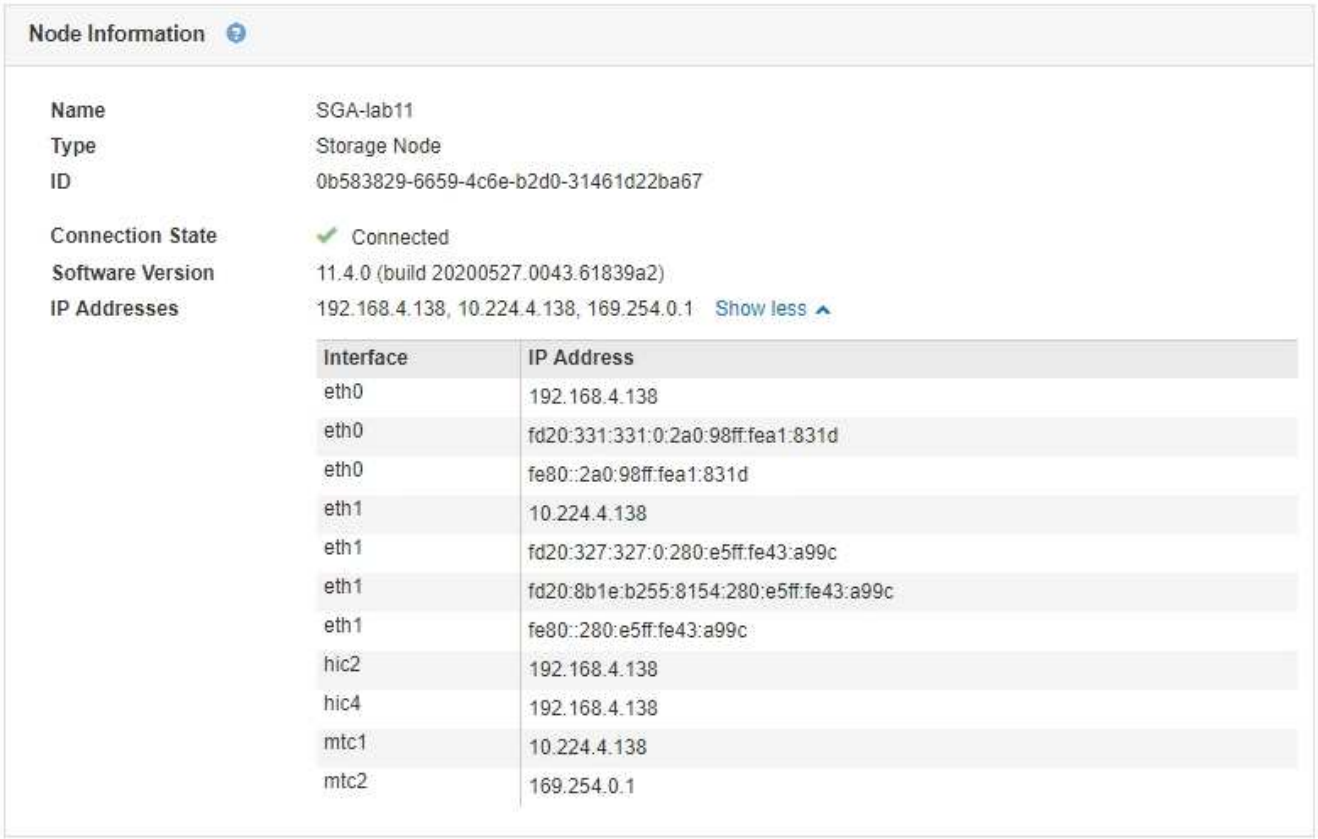
このタスクについて

IPアドレス変更の詳細については、リカバリおよびメンテナンスの手順を参照してください。

手順

1. ノード*>**grid node**>* Overview *を選択します。
2. [IP Addresses]のタイトルの右にある[**Show More**]をクリックします。

   このグリッドノードの IP アドレスがテーブルに表示されます。



関連情報

""

発信 **TLS** 接続でサポートされる暗号

# StorageGRID システムでは、アイデンティティフェデレーションとクラウドストレージプールに使用される外部システムへの Transport Layer Security （ TLS ）接続でサポートされる暗号スイートに制限があります。

サポートされる **TLS** のバージョン

StorageGRID では、アイデンティティフェデレーションとクラウドストレージプールに使用される外部システムへの接続で TLS 1.2 と TLS 1.3 がサポートされます。

外部システムとの互換性を確保するために、外部システムとの使用がサポートされている TLS 暗号が選択されています。S3 または Swift クライアントアプリケーションで使用できる暗号のリストは、このリストよりも大容量です。

> プロトコルのバージョン、暗号、鍵交換アルゴリズム、 MAC アルゴリズムなどの TLS 設定オプションは、 StorageGRID では設定できません。これらの設定について具体的なご要望がある場合は、ネットアップのアカウント担当者にお問い合わせください。

サポートされている **TLS 1.2** 暗号スイート

次の TLS 1.2 暗号スイートがサポートされています。

- TLS_ECDHE_RSA_With _AES_128_GCM_SHA256
- TLS_ECDHE_RSA_with _AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_With _AES_128_GG_SHA256
- TLS_ECDHE_ECDSA_With _AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305
- TLS_RSA_With _AES_128_GCM _SHA256
- TLS_RSA_With _AES_256_GCM_SHA384

サポートされている **TLS 1.3** 暗号スイート

次の TLS 1.3 暗号スイートがサポートされています。

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM _SHA256

ネットワーク転送の暗号化の変更

# StorageGRID システムでは、 Transport Layer Security （ TLS ）を使用して、グリッドノード間の内部制御トラフィックを保護します。Network Transfer Encryption オプショ

ンは、グリッドノード間の制御トラフィックを暗号化するために TLS で使用されるアルゴリズムを設定します。この設定はデータ暗号化には影響しません。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

デフォルトでは、ネットワーク転送の暗号化には AES256-SHA アルゴリズムが使用されます。AES128-SHA アルゴリズムを使用して暗号化することもできます。

手順

1. 「環境設定*システム設定*グリッドオプション*」を選択します。
2. ネットワークオプションセクションで、ネットワーク転送の暗号化を * AES128-SHA * または * AES256-SHA * （デフォルト）に変更します。

3. [ 保存（ Save ） ] をクリックします。

サーバ証明書の設定

## StorageGRID システムで使用されるサーバ証明書をカスタマイズできます。

StorageGRID システムは、用途が異なる複数のセキュリティ証明書を使用します。

- 管理インターフェイスのサーバ証明書：Grid Manager、Tenant Manager、Grid管理API、およびテナント管理APIへのアクセスを保護するために使用します。
- ストレージAPIのサーバ証明書：ストレージノードおよびゲートウェイノードへのアクセスを保護するために使用します。これらのノードは、APIクライアントアプリケーションがオブジェクトデータをアップロードおよびダウンロードするために使用します。

インストール時に作成されたデフォルトの証明書を使用できるほか、デフォルトの証明書のいずれか、または両方を独自のカスタム証明書に置き換えることもできます。

サポートされているカスタムサーバ証明書のタイプ

StorageGRID システムでは、RSAまたはECDSA（Elliptic Curve Digital Signature Algorithm）で暗号化されたカスタムサーバ証明書がサポートされます。

StorageGRID でREST APIのクライアント接続を保護する方法の詳細については、S3またはSwiftの実装ガイドを参照してください。

ロードバランサエンドポイントの証明書

StorageGRID では、ロードバランサエンドポイントに使用する証明書は別に管理されます。ロードバランサ証明書を設定するには、ロードバランサエンドポイントの設定手順を参照してください。

関連情報

"S3 を使用する"

"Swift を使用します"

"ロードバランサエンドポイントの設定"

**Grid Manager**および**Tenant Manager**用のカスタムサーバ証明書を設定する

# デフォルトの StorageGRID サーバ証明書を単一のカスタムサーバ証明書に置き換えると、ユーザがグリッドマネージャとテナントマネージャにアクセスする際にセキュリティの警告が表示されなくなります。

このタスクについて

デフォルトでは、管理ノードごとに、グリッド CA によって署名された証明書が 1 つずつ発行されます。これらの CA 署名証明書は、単一の共通するカスタムサーバ証明書および対応する秘密鍵で置き換えることができます。

1つのカスタムサーバ証明書がすべての管理ノードに対して使用されるため、Grid ManagerおよびTenant Managerへの接続時にクライアントがホスト名を確認する必要がある場合は、ワイルドカード証明書またはマルチドメイン証明書として指定する必要があります。グリッド内のすべての管理ノードに一致するカスタム証明書を定義してください。

設定はサーバ上で行う必要があります。また、使用しているルート認証局（CA）によっては、ユーザがGrid ManagerおよびTenant Managerへのアクセスに使用するWebブラウザにルートCA証明書をインストールすることも必要になります。

サーバ証明書の問題によって処理が中断されないようにするために、このサーバ証明書の有効期限が近づくと、Expiration of server certificate for Management Interface アラートと**Legacy Management Interface Certificate Expiry**（**MCEP**）アラームの両方がトリガーされます。必要に応じて、 Support **>** Tools **>** Grid Topology を選択することにより、現在のサービス証明書が期限切れになるまでの日数を表示できます。次に、「***_ primary Admin Node_***>* CMN **>** Resources *」を選択します。

IP アドレスではなくドメイン名を使用して Grid Manager または Tenant Manager にアクセスする場合は、次のいずれかの場合に証明書のエラーが表示され、バイパスするオプションはありません。

- カスタム管理インターフェイスサーバ証明書の有効期限が切れます。
- カスタムの管理インターフェイスサーバ証明書をデフォルトのサーバ証明書に戻した場合。

手順

1. [* Configuration **]>[** Network Settings **]>[** Server Certificates*]を選択します。
2. Management Interface Server Certificateセクションで、* Install Custom Certificate *をクリックします。

3. 必要なサーバ証明書ファイルをアップロードします。
   - サーバー証明書：カスタムサーバー証明書ファイル（`.crt`）。
   - * Server Certificate Private Key *：カスタムサーバ証明書の秘密鍵ファイル（`.key`）。

     EC 秘密鍵は 224 ビット以上である必要があります。RSA 秘密鍵は 2048 ビット以上にする必要があります。

   - **CA Bundle**：各中間発行認証局（CA）の証明書を含む単一のファイル。このファイルには、 PEM でエンコードされた各 CA 証明書ファイルが、証明書チェーンの順序で連結して含まれている必要があります。
4. [ 保存（ Save ） ] をクリックします。

   以降すべての新しいクライアント接続には、カスタムサーバ証明書が使用されます。

   タブを選択して、デフォルトのStorageGRID サーバ証明書またはアップロードされたCA署名証明書に関する詳細情報を表示します。

   新しい証明書をアップロードしたあと、関連する証明書の有効期限アラート（またはレガシーアラーム）がクリアされるまでに最大1日かかります。

5. Web ブラウザが更新されたことを確認するには、ページをリフレッシュしてください。

**Grid Manager**および**Tenant Manager**用のデフォルトのサーバ証明書のリストア

## Grid ManagerおよびTenant Managerでデフォルトのサーバ証明書を使用するように戻すことができます。

手順

1. [* Configuration **]>[** Network Settings **]>[** Server Certificates*]を選択します。
2. Manage Interface Server Certificateセクションで、* Use Default Certificates *をクリックします。
3. 確認ダイアログボックスで * OK * をクリックする。

   デフォルトのサーバ証明書をリストアすると、設定したカスタムサーバ証明書ファイルは削除され、システムからはリカバリできなくなります。以降すべての新しいクライアント接続には、デフォルトのサーバ証明書が使用されます。

4. Web ブラウザが更新されたことを確認するには、ページをリフレッシュしてください。

ストレージノードまたは**CLB**サービスへの接続用のカスタムサーバ証明書を設定する

## ストレージノードまたはゲートウェイノード上のCLBサービス（廃止）へのS3またはSwiftクライアント接続に使用するサーバ証明書は、置き換えることができます。置き換え用のカスタムサーバ証明書は組織に固有のものです。

このタスクについて

デフォルトでは、すべてのストレージノードに、グリッド CA によって署名された X.509 サーバ証明書が発行されます。これらの CA 署名証明書は、単一の共通するカスタムサーバ証明書および対応する秘密鍵で置き

換えることができます。

1 つのカスタムサーバ証明書がすべてのストレージノードに対して使用されるため、ストレージエンドポイントへの接続時にクライアントがホスト名を確認する必要がある場合は、ワイルドカード証明書またはマルチドメイン証明書として指定する必要があります。グリッド内のすべてのストレージノードに一致するカスタム証明書を定義してください。

サーバでの設定が完了したら、使用しているルート認証局（CA）によっては、ユーザがシステムへのアクセスに使用するS3またはSwift APIクライアントにルートCA証明書をインストールすることも必要になる場合があります。

> ⓘ サーバ証明書の問題によって処理が中断されないようにするために、Expiration of server certificate for Storage API Endpoints アラートと、ルートサーバ証明書の有効期限が近づくと従来の**Storage API Service Endpoints Certificate Expiry**（**SCEP**）アラームの両方がトリガーされます。必要に応じて、「 Support **Tools * Grid Topology *** 」を選択することにより、現在のサービス証明書が期限切れになるまでの日数を表示できます。次に、「***_ primary Admin Node_** CMN * Resources *」を選択します。

カスタム証明書は、クライアントがゲートウェイノード上の廃止されたCLBサービスを使用してStorageGRIDに接続する場合、またはクライアントがストレージノードに直接接続する場合にのみ使用されます。管理ノードまたはゲートウェイノード上のロードバランササービスを使用してStorageGRID に接続するS3またはSwiftクライアントは、ロードバランサエンドポイント用に設定された証明書を使用します。

> ⓘ *ロードバランサエンドポイント証明書の有効期限*アラートは、まもなく期限切れになるロードバランサエンドポイントに対してトリガーされます。

手順

1. [* Configuration **]>[** Network Settings **]>[** Server Certificates*]を選択します。
2. Object Storage API Service Endpoints Server Certificateセクションで、* Install Custom Certificate *をクリックします。
3. 必要なサーバ証明書ファイルをアップロードします。
   - サーバー証明書：カスタムサーバー証明書ファイル (`.crt`）。
   - * Server Certificate Private Key *：カスタムサーバ証明書の秘密鍵ファイル (`.key`）。

     > ⓘ EC 秘密鍵は 224 ビット以上である必要があります。RSA 秘密鍵は 2048 ビット以上にする必要があります。

   - **CA Bundle**：各中間発行認証局（CA）の証明書を含む単一のファイル。このファイルには、 PEM でエンコードされた各 CA 証明書ファイルが、証明書チェーンの順序で連結して含まれている必要があります。
4. [ 保存（ Save ） ] をクリックします。

   以降すべての新しいAPIクライアント接続には、カスタムサーバ証明書が使用されます。

   タブを選択して、デフォルトのStorageGRID サーバ証明書またはアップロードされたCA署名証明書に関する詳細情報を表示します。

新しい証明書をアップロードしたあと、関連する証明書の有効期限アラート（またはレガシーアラーム）がクリアされるまでに最大1日かかります。

5. Web ブラウザが更新されたことを確認するには、ページをリフレッシュしてください。

関連情報

"S3 を使用する"

"Swift を使用します"

"S3 APIエンドポイントのドメイン名を設定しています"

**S3**および**Swift**の**REST API**エンドポイント用のデフォルトサーバ証明書のリストア

## S3およびSwiftのREST APIエンドポイント用のデフォルトサーバ証明書を使用する設定に戻すことができます。

手順

1. [* Configuration **]>[** Network Settings **]>[** Server Certificates*]を選択します。
2. Object Storage API Service Endpoints Server Certificateセクションで、* Use Default Certificates *をクリックします。
3. 確認ダイアログボックスで * OK * をクリックする。

   オブジェクトストレージAPIエンドポイント用のデフォルトサーバ証明書をリストアすると、設定したカスタムサーバ証明書ファイルは削除され、システムからはリカバリできなくなります。以降すべての新しいAPIクライアント接続には、デフォルトのサーバ証明書が使用されます。

4. Web ブラウザが更新されたことを確認するには、ページをリフレッシュしてください。

**StorageGRID** システムの**CA**証明書をコピーしています

## StorageGRID は、内部の認証局（CA）を使用して内部トラフィックを保護します。独自の証明書をアップロードしても、この証明書は変更されません。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

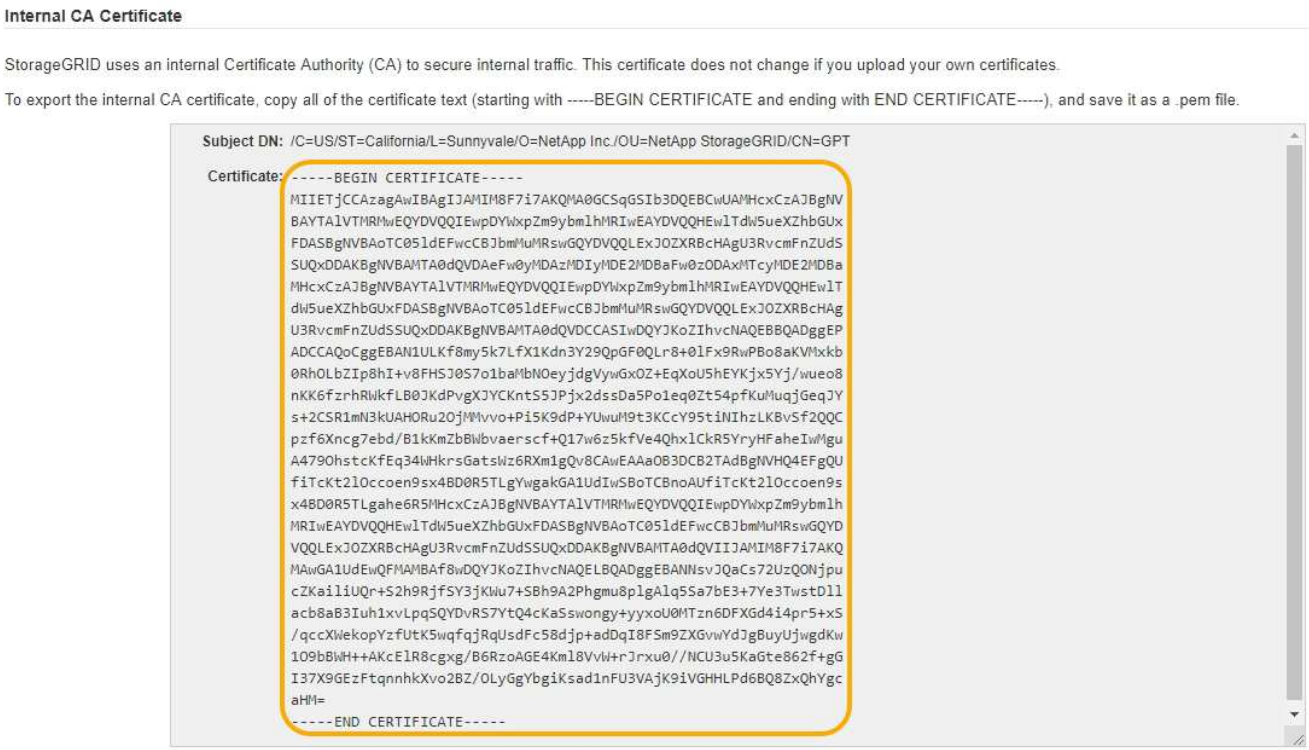
このタスクについて

カスタムサーバ証明書が設定されている場合、クライアントアプリケーションはカスタムサーバ証明書を使用してサーバを検証する必要があります。StorageGRID システムから CA 証明書をコピーしない。

手順

1. [* Configuration **]>[** Network Settings **]>[** Server Certificates*]を選択します。
2. [内部**CA**証明書（* Internal CA Certificate *）]セクションで、すべての証明書テキストを選択します。

   を含める必要があります `-----BEGIN CERTIFICATE-----` および `-----END CERTIFICATE-----` を選択します。




3. 選択したテキストを右クリックし、*コピー*を選択します。
4. コピーした証明書をテキストエディタに貼り付けます。
5. 拡張子を付けてファイルを保存します `.pem`。

   例： `storagegrid_certificate.pem`

**FabricPool** 用の**StorageGRID** 証明書を設定しています

厳密なホスト名検証を実行する S3 クライアントでは、 FabricPool を使用する ONTAP クライアントなどの厳密なホスト名検証の無効化をサポートしていない場合は、ロードバランサエンドポイントの設定時にサーバ証明書を生成またはアップロードできます。

必要なもの

- 特定のアクセス権限が必要です。
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

このタスクについて

ロードバランサエンドポイントを作成する際には、自己署名サーバ証明書を生成するか、既知の認証局（CA）によって署名された証明書をアップロードできます。本番環境では、既知の CA によって署名された証明書を使用する必要があります。CA によって署名された証明書は、システムを停止することなくローテーションできます。また、中間者攻撃に対する保護としても優れているため、セキュリティも強化されます。

次の手順は、 FabricPool を使用する S3 クライアントを対象とした一般的なガイドラインです。詳細な情報と手順については、StorageGRID for FabricPool の設定手順を参照してください。

ゲートウェイノード上の別の Connection Load Balancer （ CLB ）サービスは廃止され、 FabricPool での使用は推奨されなくなりました。

手順

1. 必要に応じて、 FabricPool で使用するハイアベイラビリティ（ HA ）グループを設定します。
2. FabricPool で使用する S3 ロードバランサエンドポイントを作成します。

   HTTPSロードバランサエンドポイントを作成する際に、サーバ証明書、証明書の秘密鍵、およびCAバンドルのアップロードを求めるプロンプトが表示されます。

3. ONTAP でクラウド階層として StorageGRID を接続します。

   ロードバランサエンドポイントのポートと、アップロードした CA 証明書で使用する完全修飾ドメイン名を指定します。次に、 CA 証明書を指定します。

   > ⓘ 中間 CA が StorageGRID 証明書を発行した場合は、中間 CA 証明書を指定する必要があります。StorageGRID 証明書がルート CA によって直接発行された場合は、ルート CA 証明書を指定する必要があります。

関連情報

"StorageGRID for FabricPool を設定します"

管理インターフェイス用の自己署名サーバ証明書の生成

## スクリプトを使用して、ホスト名の厳密な検証が必要な管理APIクライアント用の自己署名サーバ証明書を生成できます。

必要なもの

- 特定のアクセス権限が必要です。
- を用意しておく必要があります `Passwords.txt` ファイル。

このタスクについて

本番環境では、既知の認証局（CA）によって署名された証明書を使用する必要があります。CA によって署名された証明書は、システムを停止することなくローテーションできます。また、中間者攻撃に対する保護としても優れているため、セキュリティも強化されます。

手順

1. 各管理ノードの完全修飾ドメイン名（ FQDN ）を取得します。
2. プライマリ管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

      rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。
3. 新しい自己署名証明書を使用して StorageGRID を設定します。

```
$ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
```

- の場合 `--domains`、ワイルドカードを使用して、すべての管理ノードの完全修飾ドメイン名を表します。例： `*.ui.storagegrid.example.com` ワイルドカード*を使用して表します `admin1.ui.storagegrid.example.com` および `admin2.ui.storagegrid.example.com`。
- 設定 `--type` 終了： `management` Grid ManagerおよびTenant Managerで使用される証明書を設定するため。
- デフォルトでは、生成された証明書の有効期間は 1 年間（ 365 日）です。この期間を過ぎる前に証明書を再作成する必要があります。を使用できます `--days` デフォルトの有効期間を上書きする引数。

> ⓘ 証明書の有効期間は、で始まります `make-certificate` を実行します。管理APIクライアントがStorageGRID と同じ時間ソースと同期されるようにしてください。同期されていないと、クライアントが証明書を拒否する可能性があります。

```
$ sudo make-certificate --domains *.ui.storagegrid.example.com --type
management --days 365
```

出力には、管理 API クライアントで必要なパブリック証明書が含まれています。

4. 証明書を選択してコピーします。

   BEGIN タグと END タグも含めて選択してください。

5. コマンドシェルからログアウトします。 `$ exit`
6. 証明書が設定されたことを確認します。
   a. Grid Manager にアクセスします。
   b. 「* Configuration * Server Certificates * Management Interface Server Certificate *」を選択します。
7. コピーしたパブリック証明書を使用するように管理APIクライアントを設定します。BEGIN タグと END タグを含めてください。

ストレージプロキシを設定しています

プラットフォームサービスまたはクラウドストレージプールを使用している場合は、ストレージノードと外部の S3 エンドポイントの間に非透過型プロキシを設定できます。たとえば、インターネット上のエンドポイントなどの外部エンドポイントへプラットフォームサービスメッセージを送信する場合などには、非透過型プロキシが必要です。

必要なもの

- 特定のアクセス権限が必要です。
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

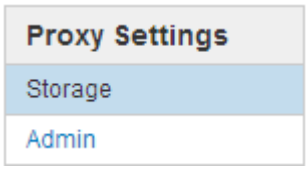
このタスクについて

設定できるストレージプロキシは 1 つです。

手順

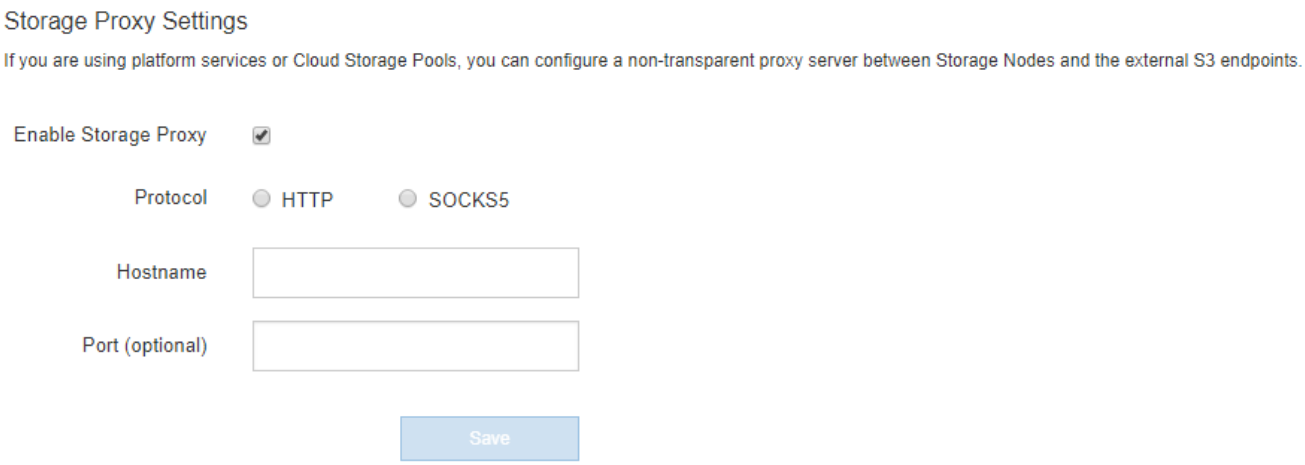
1. [環境設定*ネットワーク設定*プロキシ設定]を選択します。

   ストレージプロキシの設定ページが表示されます。デフォルトでは、サイドバーメニューで「 * Storage * 」が選択されています。




2. Enable Storage Proxy （ストレージプロキシの有効化）チェックボックスを選択します。

   ストレージプロキシを設定するためのフィールドが表示されます。




3. 非透過型ストレージプロキシのプロトコルを選択します。
4. プロキシサーバのホスト名または IP アドレスを入力します。
5. 必要に応じて、プロキシサーバへの接続に使用するポートを入力します。

   プロトコルにデフォルトのポート 80 を使用する場合は、このフィールドを空白のままにできます。 HTTP の場合は 80 、 SOCKS5 の場合は 1080 です。

6. [ 保存（ Save ） ] をクリックします。

   ストレージプロキシが保存されたら、プラットフォームサービスまたはクラウドストレージプールの新しいエンドポイントを設定してテストできます。

   プロキシの変更が有効になるまでに最大 10 分かかることがあります。

7. プロキシサーバの設定をチェックして、 StorageGRID からのプラットフォームサービス関連メッセージがブロックされないようにします。

完了後

ストレージプロキシを無効にする必要がある場合は、*ストレージプロキシを有効にする*チェックボックスの選択を解除し、*保存*をクリックします。

関連情報

"プラットフォームサービス用のネットワークとポート"

"ILM を使用してオブジェクトを管理する"

管理プロキシの設定

# HTTPまたはHTTPSを使用してAutoSupport メッセージを送信する場合は、管理ノードとテクニカルサポート（AutoSupport ）の間に非透過型プロキシサーバを設定できます。

必要なもの

- 特定のアクセス権限が必要です。
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

このタスクについて

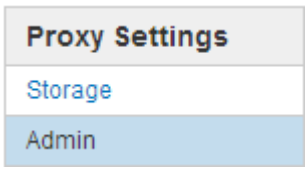
設定できる管理プロキシは 1 つです。

手順

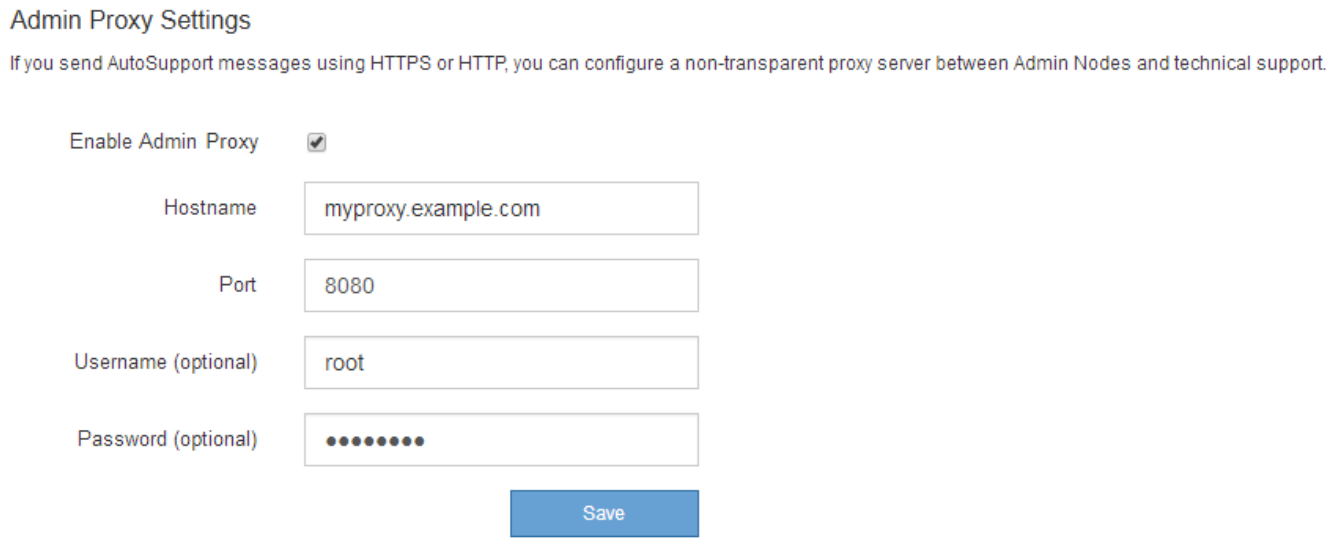
1. [環境設定*ネットワーク設定*プロキシ設定]を選択します。

   Admin Proxy Settings ページが表示されます。デフォルトでは、サイドバーメニューで「 * Storage * 」が選択されています。

2. サイドバーのメニューから、 **Admin** を選択します。




3. [ 管理プロキシを有効にする *] チェックボックスをオンにします。




4. プロキシサーバのホスト名または IP アドレスを入力します。

5. プロキシサーバへの接続に使用するポートを入力します。
6. 必要に応じて、プロキシユーザ名を入力します。

   プロキシサーバでユーザ名が不要な場合は、このフィールドを空白のままにします。

7. 必要に応じて、プロキシパスワードを入力します。

   プロキシサーバでパスワードが不要な場合は、このフィールドを空白のままにします。

8. [ 保存（ Save ） ] をクリックします。

   管理プロキシが保存されると、管理ノードとテクニカルサポートの間にプロキシサーバが設定されます。

   プロキシの変更が有効になるまでに最大 10 分かかることがあります。

9. プロキシを無効にする必要がある場合は、*管理者プロキシを有効にする*チェックボックスの選択を解除し、*保存*をクリックします。

関連情報

"AutoSupport メッセージのプロトコルの指定"

トラフィック分類ポリシーの管理

サービス品質（ QoS ）サービスを強化するために、トラフィック分類ポリシーを作成して、さまざまなタイプのネットワークトラフィックを識別および監視できます。これらのポリシーは、トラフィックの制限と監視に役立ちます。

トラフィック分類ポリシーは、ゲートウェイノードおよび管理ノードの StorageGRID ロードバランササービス上のエンドポイントに適用されます。トラフィック分類ポリシーを作成するには、ロードバランサエンドポイントを作成しておく必要があります。

ルールとオプションの制限を一致させる

各トラフィック分類ポリシーには、次のエンティティに関連するネットワークトラフィックを識別する 1 つ以上の一致ルールが含まれています。

- バケット
- テナント
- サブネット（クライアントを含む IPv4 サブネット）
- エンドポイント（ロードバランサエンドポイント）

StorageGRID は、ルールの目的に応じて、ポリシー内のルールに一致するトラフィックを監視します。ポリシーのルールに一致するトラフィックは、そのポリシーによって処理されます。逆に、指定されたエンティティを除くすべてのトラフィックを照合するルールを設定できます。

必要に応じて、次のパラメータに基づいてポリシーの制限を設定できます。

- 総帯域幅

- 総帯域幅アウト
- 同時読み取り要求
- 同時書き込み要求
- での要求ごとの帯域幅
- 要求ごとの帯域幅アウト
- 読み取り要求レート
- 書き込み要求の速度

ポリシーを作成して、アグリゲートの帯域幅を制限したり、要求ごとの帯域幅を制限したりできます。ただし、 StorageGRID では、両方のタイプの帯域幅を同時に制限することはできません。アグリゲートの帯域幅の制限により、制限のないトラフィックにパフォーマンスが若干低下する可能性があります。

トラフィック制限

トラフィック分類ポリシーを作成した場合、トラフィックは設定したルールおよび制限のタイプに応じて制限されます。集約または要求ごとの帯域幅制限の場合、要求は、設定したレートでストリームインまたはアウトされます。StorageGRID では 1 つの速度しか適用できないため、最も特定のポリシーがマッチするのはマッチャーのタイプです。それ以外のすべての制限タイプでは、クライアント要求は 250 ミリ秒遅延し、一致するポリシー制限を超える要求に対しては 503 スローダウン応答を受信します。

Grid Manager では、トラフィックチャートを表示して、ポリシーが想定したトラフィック制限を適用していることを確認できます。

**SLA**でのトラフィック分類ポリシーの使用

トラフィック分類ポリシーを容量制限およびデータ保護とともに使用して、容量、データ保護、およびパフォーマンスに固有のサービスレベル契約（ SLA ）を適用できます。

トラフィック分類の制限は、ロードバランサごとに実装されます。複数のロードバランサに同時にトラフィックが分散されている場合、合計最大速度は指定した速度制限の倍数になります。

次の例は、 SLA の 3 つの階層を示しています。トラフィック分類ポリシーを作成して、各 SLA 層のパフォーマンス目標を達成できます。

| サービスレベル階層 | 容量 | データ保護 | パフォーマンス | コスト |
|---|---|---|---|---|
| ゴールド | 1 PB のストレージを使用できます | 3 コピーの ILM ルール | 25 、 000 要求 / 秒<br><br>5 GB/ 秒（ 40 Gbps ）の帯域幅 | $$/ 月 |
| シルバー | 250 TB のストレージを使用できます | 2 コピーの ILM ルール | 10 K 要求 / 秒<br><br>1.25 GB/ 秒（ 10 Gbps ）の帯域幅 | $/ 月 |

| サービスレベル階層 | 容量 | データ保護 | パフォーマンス | コスト |
| --- | --- | --- | --- | --- |
| ブロンズ | 100TB のストレージを使用できます | 2 コピーの ILM ルール | 5 、 000 要求 / 秒<br><br>1 GB/ 秒（ 8 Gbps ）の帯域幅 | 月あたりのコスト |

トラフィック分類ポリシーの作成

# バケット、テナント、 IP サブネット、またはロードバランサエンドポイントごとにネットワークトラフィックを監視し、必要に応じて制限する場合は、トラフィック分類ポリシーを作成します。必要に応じて、帯域幅、同時要求数、または要求速度に基づいてポリシーの制限を設定できます。

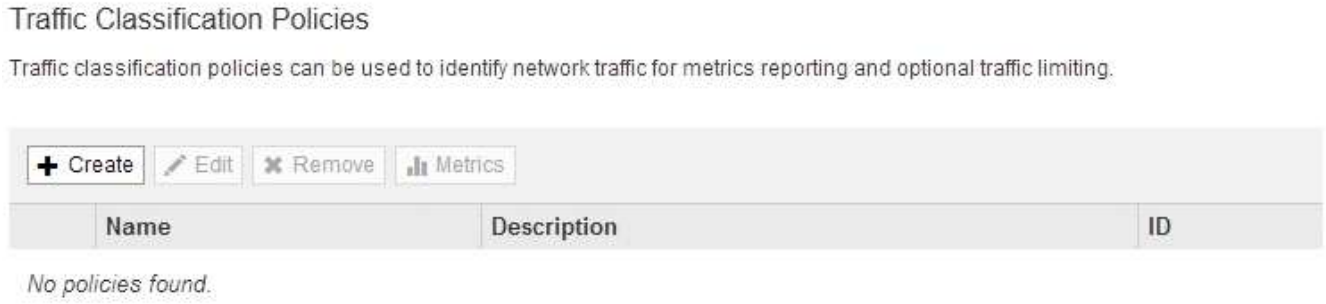
必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限が必要です。
- 照合するロードバランサエンドポイントを作成しておく必要があります。
- 該当するテナントを作成しておく必要があります。

手順

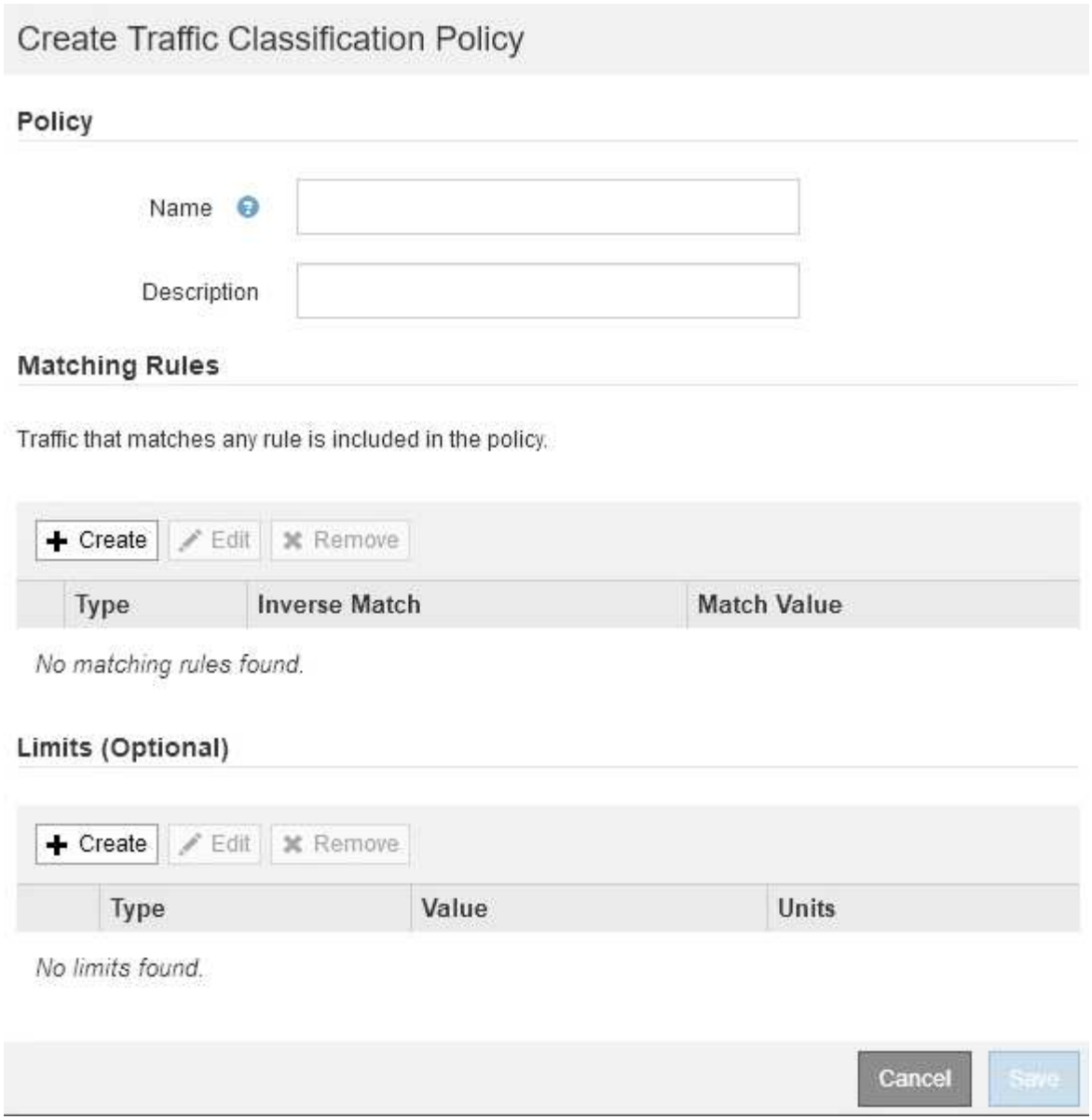
1. [* Configuration **]>[** Network Settings **]>[** Traffic Classification]を選択します。

   [Traffic Classification Policies] ページが表示されます。

2. [ 作成（ Create ） ] をクリックします。

   Create Traffic Classification Policy ダイアログボックスが表示されます。




3. [* 名前 *] フィールドに、ポリシーの名前を入力します。

   ポリシーを識別できるように、わかりやすい名前を入力します。

4. 必要に応じて、 * 概要 * フィールドにポリシーの概要 を追加します。

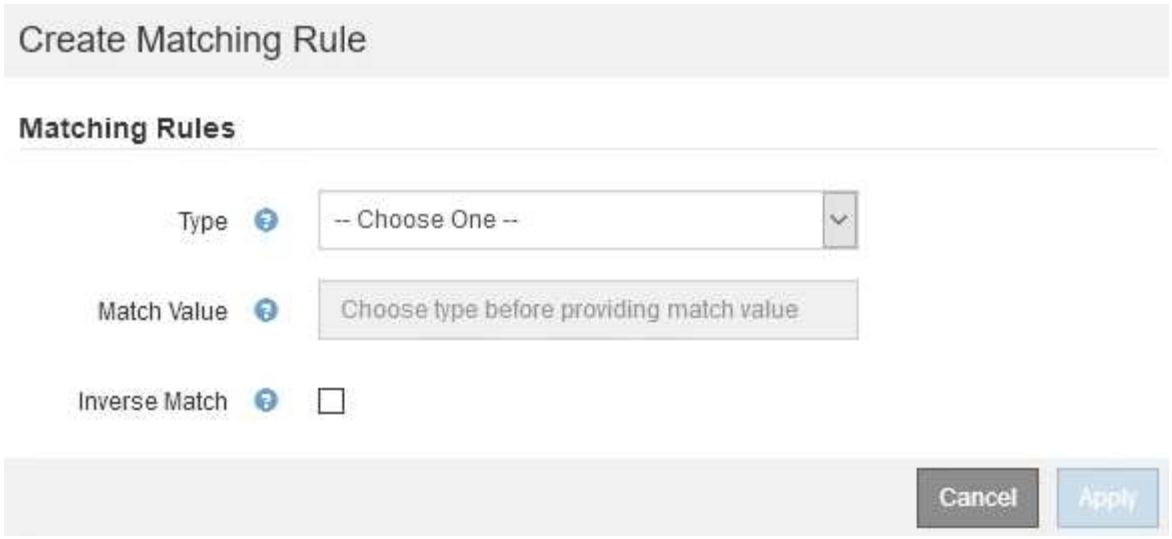
   たとえば、このトラフィック分類ポリシー環境 の内容と制限する内容を説明します。

5. ポリシーに一致するルールを 1 つ以上作成します。

   一致ルールは、このトラフィック分類ポリシーの影響を受けるエンティティを制御します。たとえば、このポリシーを特定のテナントのネットワークトラフィックに適用する場合は、テナントを選択します。または、このポリシーを特定のロードバランサエンドポイントのネットワークトラフィックに適用する場合は、 [Endpoint] を選択します。

   a. [マッチングルール（Matching Rules *）]セクションで[*作成（Create *）]をクリックし

      [Create Matching Rule] ダイアログボックスが表示されます。




b. [* タイプ *] ドロップダウンから、一致するルールに含めるエンティティのタイプを選択します。

c. [**match value**] フィールドに、選択したエンティティのタイプに基づいて照合値を入力します。

   - Bucket ：バケット名を入力します。
   - Bucket Regex ：一連のバケット名と一致するために使用される正規表現を入力します。

     正規表現は固定されていません。バケット名の先頭にある ｛キャレット｝ アンカーを使用し、名前の末尾に $ アンカーを使用します。

   - CIDR ： IPv4 サブネットを CIDR 表記で入力し、目的のサブネットと一致させます。
   - Endpoint ：既存のエンドポイントのリストからエンドポイントを選択します。これは、ロードバランサエンドポイントのページで定義したロードバランサエンドポイントです。
   - テナント：既存のテナントのリストからテナントを選択します。テナントの一致は、アクセス対象のバケットの所有権に基づきます。バケットへの匿名アクセスは、バケットを所有するテナントと一致します。

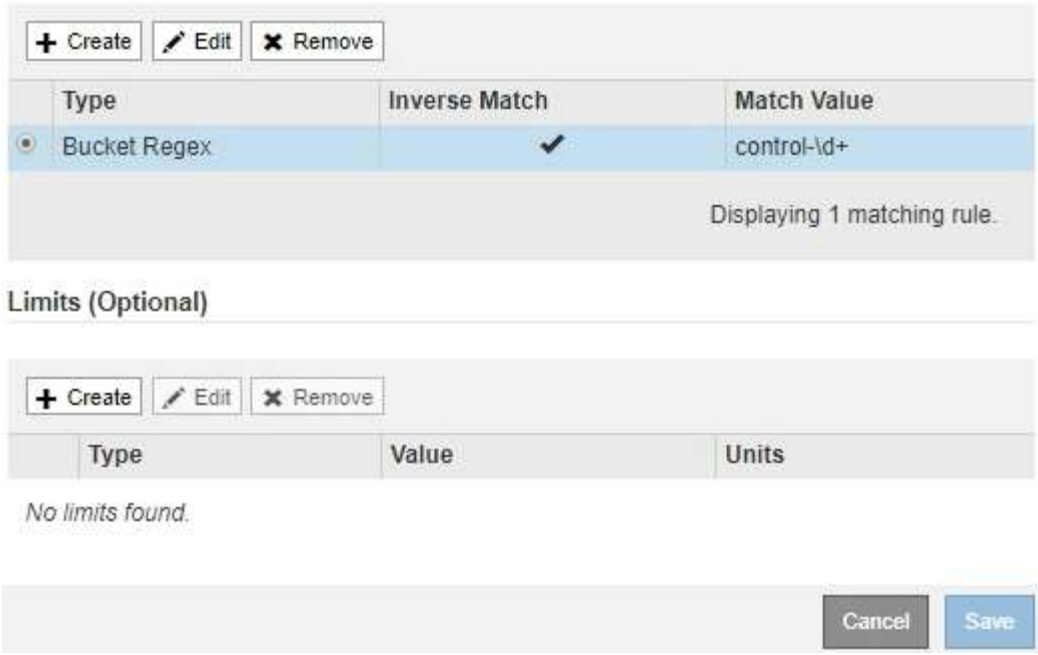
d. 定義した Type および Match 値と一致するすべての TRAFFER_EXCEPT _Traffic を照合する場合は、* Inverse * チェックボックスをオンにします。それ以外の場合は、このチェックボックスをオフのままにします。

   たとえば、このポリシーをいずれかのロードバランサエンドポイントを除くすべてのエンドポイントに適用する場合は、除外するロードバランサエンドポイントを指定し、 * Inverse * を選択します。

   > 少なくとも 1 つが逆マッチャーである複数のマッチャーを含むポリシーの場合、すべてのリクエストに一致するポリシーを作成しないように注意してください。

e. [ 適用（ Apply ） ] をクリックします。

   ルールが作成され、 [Matching Rules] テーブルに表示されます。




a. ポリシーに対して作成するルールごとに上記の手順を繰り返します。

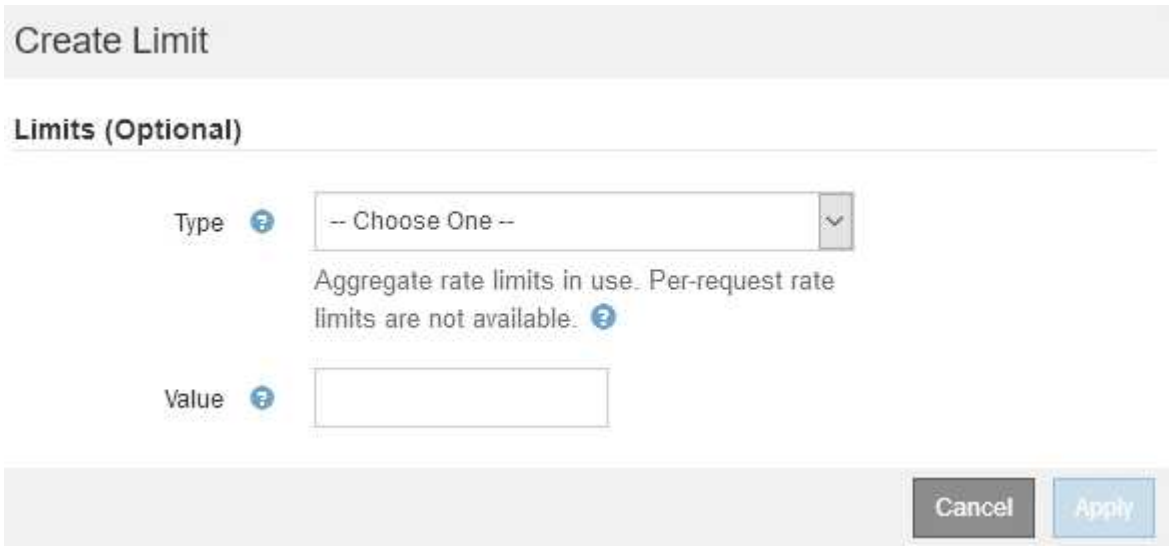
ルールに一致するトラフィックは、ポリシーによって処理されます。

6. 必要に応じて、ポリシーの制限を作成します。

制限を作成しない場合でも、ポリシーに一致するネットワークトラフィックを監視できるように StorageGRID で指標が収集されます。

a. 「制限」セクションで「*作成」をクリックします。

境界を作成（ Create Limit ）ダイアログボックスが表示されます。




b. [* タイプ *] ドロップダウンから、ポリシーに適用する制限のタイプを選択します。

次のリストの * in * は S3 または Swift クライアントから StorageGRID ロードバランサへのトラフィ

ックを表し、 * out * はロードバランサから S3 または Swift クライアントへのトラフィックを表しています。

- 総帯域幅
- 総帯域幅アウト
- 同時読み取り要求
- 同時書き込み要求
- での要求ごとの帯域幅
- 要求ごとの帯域幅アウト
- 読み取り要求レート
- 書き込み要求の速度

> ポリシーを作成して、アグリゲートの帯域幅を制限したり、要求ごとの帯域幅を制限したりできます。ただし、 StorageGRID では、両方のタイプの帯域幅を同時に制限することはできません。アグリゲートの帯域幅の制限により、制限のないトラフィックにパフォーマンスが若干低下する可能性があります。

帯域幅の制限については、設定された制限のタイプに最も一致するポリシーが StorageGRID によって適用されます。たとえば、トラフィックを一方向のみに制限するポリシーがある場合、帯域幅制限が設定されている他のポリシーと一致するトラフィックがあっても、反対方向のトラフィックは無制限になります。StorageGRID は、帯域幅制限の「ベスト」マッチを次の順序で実装します。

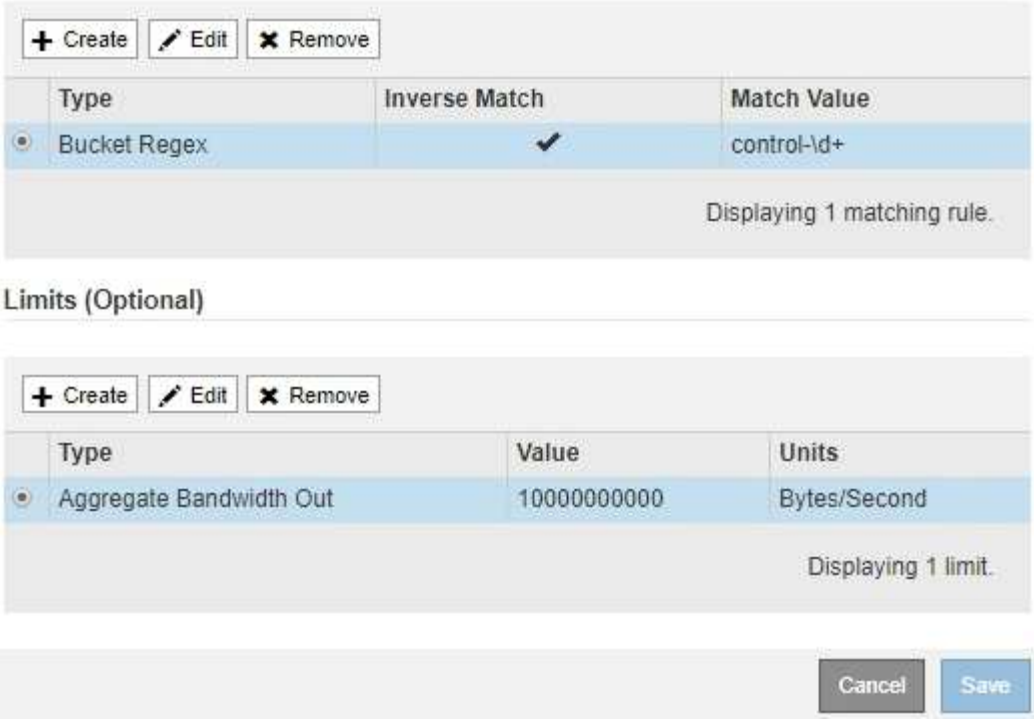
- 正確な IP アドレス（ /32 マスク）
- 正確なバケット名
- バケットの正規表現
- テナント
- エンドポイント
- 正確でない CIDR の一致（ /32 ではない）
- 逆一致

c. [* 値 *] フィールドに、選択した制限のタイプの数値を入力します。

制限を選択すると、想定される単位が表示されます。

d. [ 適用（ Apply ） ] をクリックします。

境界が作成され、 [ 境界（ Limits ） ] テーブルにリストされます。



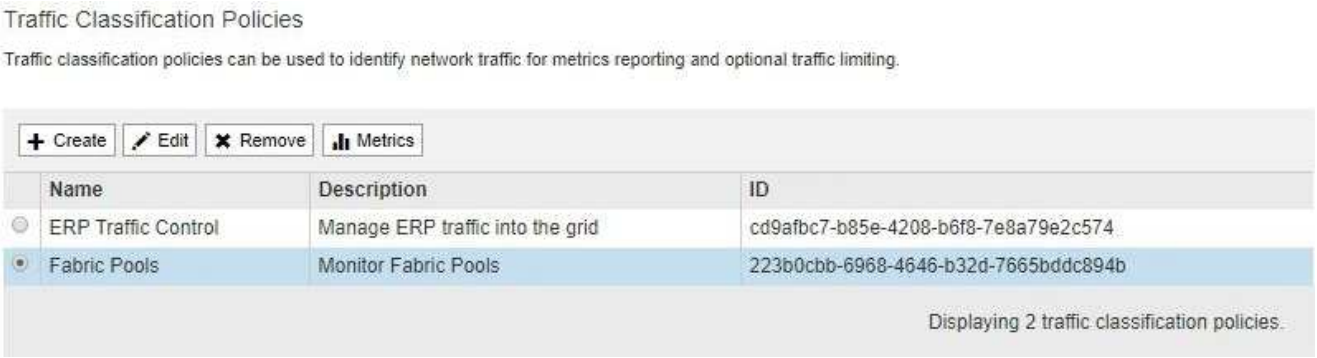

e. ポリシーに追加する上限ごとに、上記の手順を繰り返します。

たとえば、 SLA 階層に 40Gbps の帯域幅制限を作成する場合は、制限されたアグリゲート帯域幅と合計帯域幅の制限を作成し、各帯域幅を 40Gbps に設定します。

1 秒あたりのメガバイト数をギガビット / 秒に変換するには、 8 倍にします。たとえば、 125 MB/ 秒は 1 、 000 Mbps または 1 Gbps に相当します。

7. ルールと制限の作成が完了したら、*保存*をクリックします。

ポリシーが保存され、 Traffic Classification Policies テーブルにリストされます。




S3 および Swift クライアントトラフィックがトラフィック分類ポリシーに従って処理されるようになりました。トラフィックチャートを表示して、ポリシーが想定したトラフィック制限を適用していることを確認できます。

関連情報

"負荷分散の管理"

"ネットワークトラフィックメトリックの表示"

トラフィック分類ポリシーを編集する

# トラフィック分類ポリシーを編集して、その名前または概要 を変更したり、ポリシーのルールや制限を作成、編集、削除したりできます。

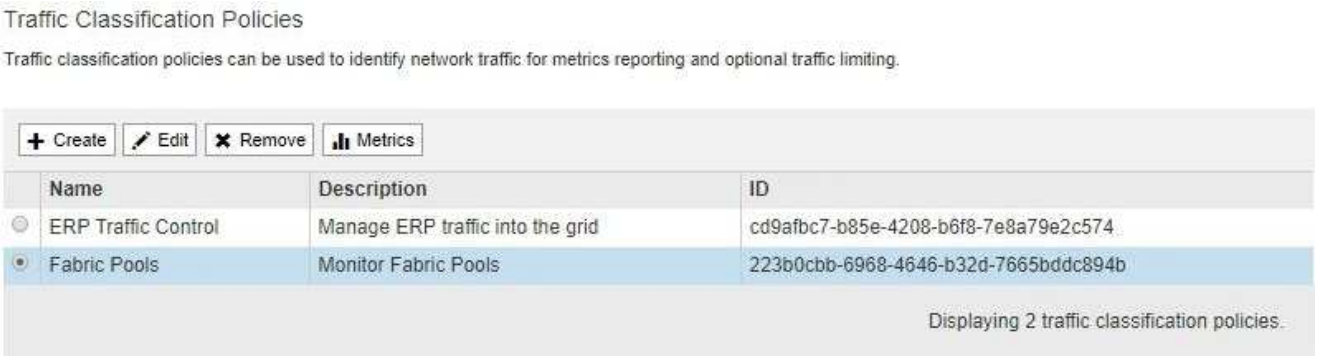
必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限が必要です。

手順

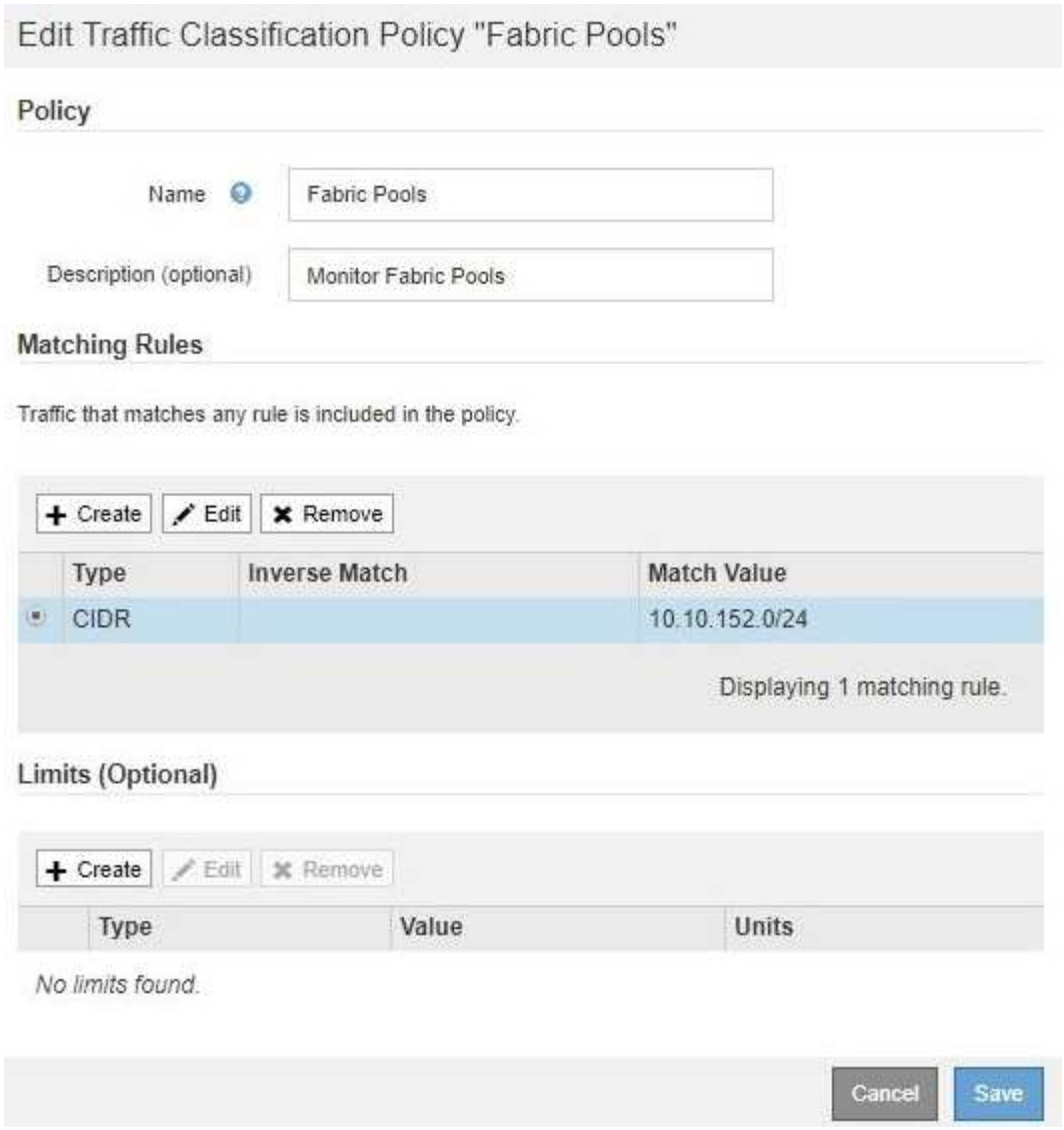
1. [* Configuration **]>[** Network Settings **]>[** Traffic Classification]を選択します。

   [Traffic Classification Policies] ページが表示され、既存のポリシーがテーブルにリストされます。




2. 編集するポリシーの左側にあるオプションボタンを選択します。
3. [ 編集（ Edit ） ] をクリックします。

   Edit Traffic Classification Policy ダイアログボックスが表示されます。




4. 必要に応じて、一致するルールと制限を作成、編集、または削除します。
   a. 一致するルールまたは制限を作成するには、*作成*をクリックし、ルールの作成または制限の作成の手順に従います。
   b. 一致するルールまたは制限を編集するには、ルールまたは制限のラジオボタンを選択し、[一致するルール*]セクションまたは[制限]セクションで[編集]をクリックして、ルールの作成または制限の作成の手順に従います。
   c. 一致するルールまたは制限を削除するには、ルールまたは制限のラジオボタンを選択し、*削除*をクリックします。次に、[OK]をクリックして、ルールまたは制限を削除することを確認します。
5. ルールまたは制限の作成または編集が終了したら、*適用*をクリックします。
6. ポリシーの編集が完了したら、*保存*をクリックします。

   ポリシーに加えた変更が保存され、ネットワークトラフィックはトラフィック分類ポリシーに従って処理されるようになりました。トラフィックチャートを表示して、ポリシーが想定したトラフィック制限を適用していることを確認できます。

トラフィック分類ポリシーを削除する

# トラフィック分類ポリシーが不要になった場合は、削除できます。

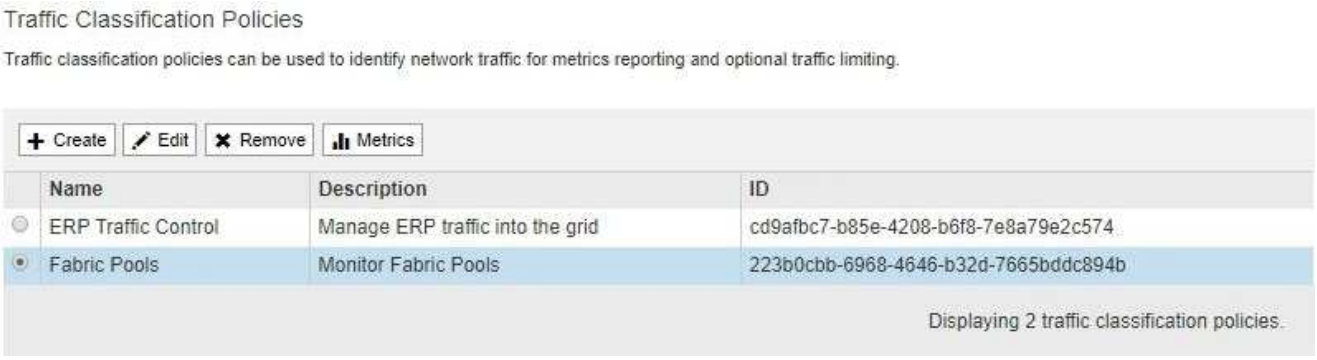
必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限が必要です。

手順

1. [* Configuration **]>[** Network Settings **]>[** Traffic Classification]を選択します。

   [Traffic Classification Policies] ページが表示され、既存のポリシーがテーブルにリストされます。




2. 削除するポリシーの左側にあるオプションボタンを選択します。
3. [ 削除（ Remove ） ] をクリックします。

   警告ダイアログボックスが表示されます。

4. [OK]をクリックして、ポリシーを削除することを確認します。

   ポリシーが削除されます。

ネットワークトラフィックメトリックの表示

# Traffic Classification Policies ページから使用可能なグラフを表示することで、ネットワークトラフィックを監視できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

- Root Access 権限が必要です。

このタスクについて

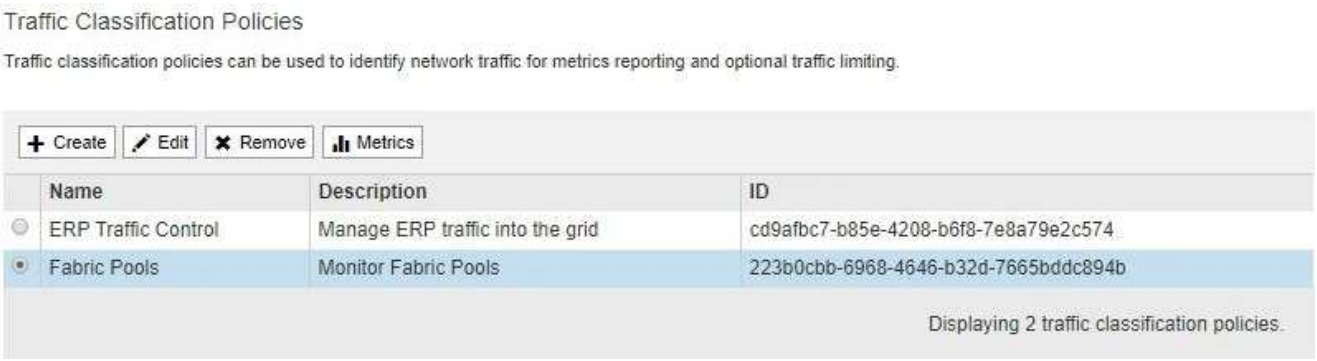
既存のトラフィック分類ポリシーでは、ロードバランササービスのメトリックを表示して、ポリシーがネットワーク全体のトラフィックを正常に制限しているかどうかを判断できます。グラフ内のデータは、ポリシーの調整が必要かどうかを判断するのに役立ちます。

トラフィック分類ポリシーに制限が設定されていない場合でも、メトリックが収集され、グラフにはトラフィックの傾向を把握するのに役立つ情報が表示されます。

手順

1. [* Configuration **]>[** Network Settings **]>[** Traffic Classification]を選択します。

   [Traffic Classification Policies] ページが表示され、既存のポリシーがテーブルにリストされます。




2. 指標を表示するポリシーの左側にあるラジオボタンを選択します。
3. [メトリクス]をクリックします。

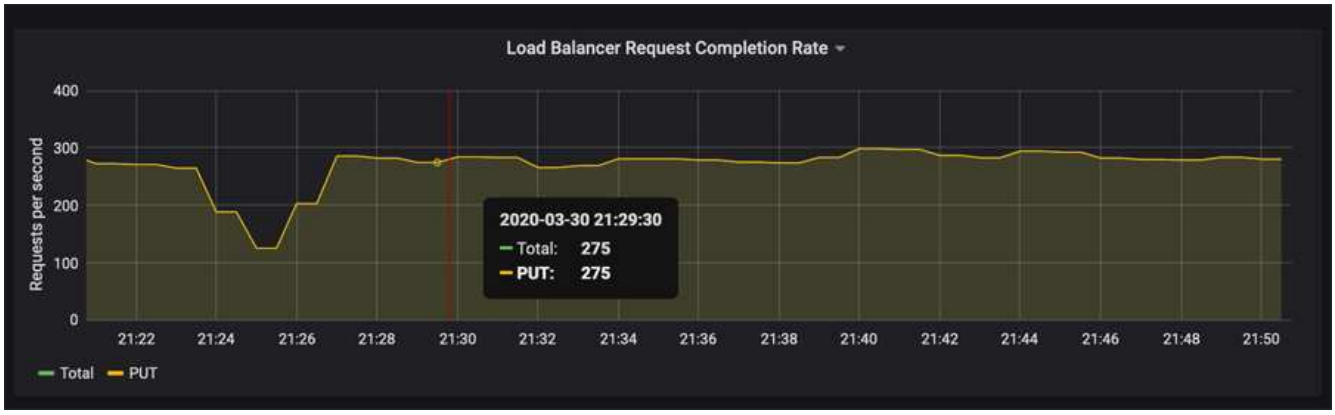
   新しいブラウザウィンドウが開き、 Traffic Classification Policy グラフが表示されます。このグラフには、選択したポリシーに一致するトラフィックのメトリックだけが表示されます。

   その他のポリシーを選択して表示するには、 * policy * プルダウンを使用します。

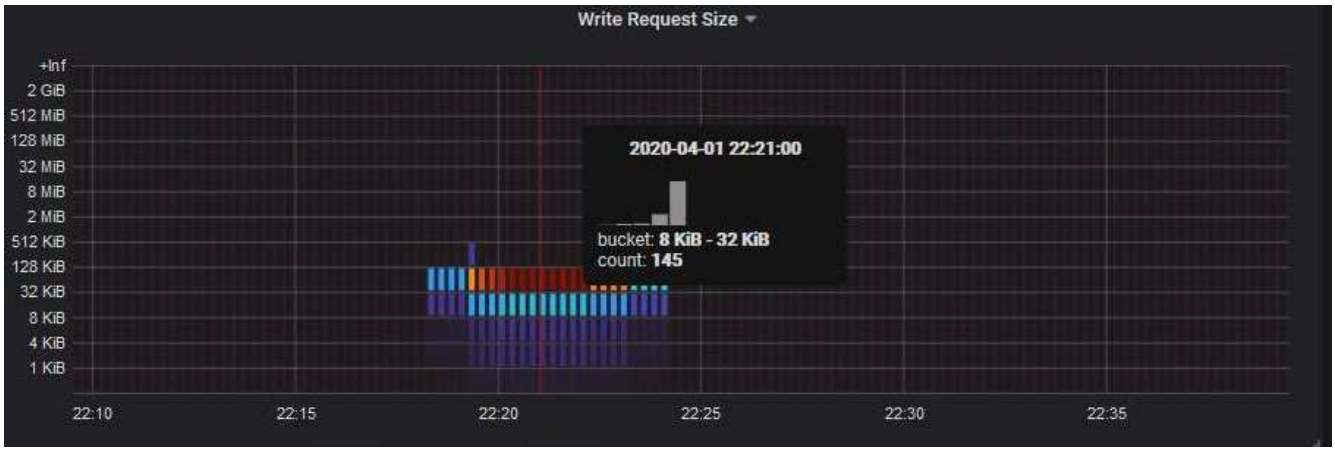
Web ページには次のグラフが表示されます。

- ロードバランサ要求トラフィック：このグラフは、ロードバランサエンドポイントと要求を送信しているクライアントの間で伝送されるデータのスループットを、 1 秒あたりのビット数で 3 分間の移動平均を提供します。
- ロードバランサの要求完了率：このグラフには、 1 秒あたりの完了済み要求数の 3 分間の移動平均が、要求タイプ（ GET 、 PUT 、 HEAD 、 DELETE ）別に示されます。この値は、新しい要求のヘッダーが検証されると更新されます。
- Error Response Rate ：このグラフには、 1 秒あたりにクライアントに返されたエラー応答数の 3 分間の移動平均が、エラー応答コード別に示されます。
- Average Request Duration （ Non-Error ）：このグラフには、要求期間の 3 分間の移動平均が、要求タイプ（ GET 、 PUT 、 HEAD 、 DELETE ）別に示されます。要求期間は、要求ヘッダーがロードバランササービスによって解析された時点から始まり、完全な応答本文がクライアントに返された時点で終了します。
- オブジェクトサイズ別の書き込み要求速度：このヒートマップは、オブジェクトサイズに基づいて書き込み要求が完了した時点での 3 分間の移動平均を提供します。この場合、書き込み要求は PUT 要求のみを参照します。
- オブジェクトサイズ別の読み取り要求速度：このヒートマップでは、オブジェクトサイズに基づいて読み取り要求が完了した時点での 3 分間の移動平均が提供されます。この場合、読み取り要求は GET 要求のみを参照します。ヒートマップの色は、個々のグラフ内のオブジェクトサイズの相対的な頻度を示します。クーラの色（紫や青など）は相対レートが低いことを示し、暖色の色（オレンジや赤など）は相対レートが高いことを示します。

4. 折れ線グラフにカーソルを合わせると、グラフの特定の部分の値がポップアップで表示されます。




5. ヒートマップにカーソルを合わせると、サンプルの日時、カウントに集約されたオブジェクトサイズ、およびその期間の 1 秒あたりのリクエスト数を示すポップアップが表示されます。




6. 左上の * Policy * プルダウンを使用して、別のポリシーを選択します。

   選択したポリシーのグラフが表示されます。

7. または、* Support *メニューからグラフにアクセスします。
   a. [* Support*]>[* Tools]>[* Metrics]を選択します。
   b. ページの * Grafana * セクションで、 * Traffic Classification Policy * を選択します。
   c. ページ左上のプルダウンからポリシーを選択します。

      トラフィック分類ポリシーは、その ID によって識別されます。ポリシー ID は、 Traffic Classification Policies ページにリストされます。

8. グラフを分析して、ポリシーがトラフィックを制限している頻度と、ポリシーを調整する必要があるかどうかを判断します。

関連情報

"トラブルシューティングを監視します"

リンクコストとは

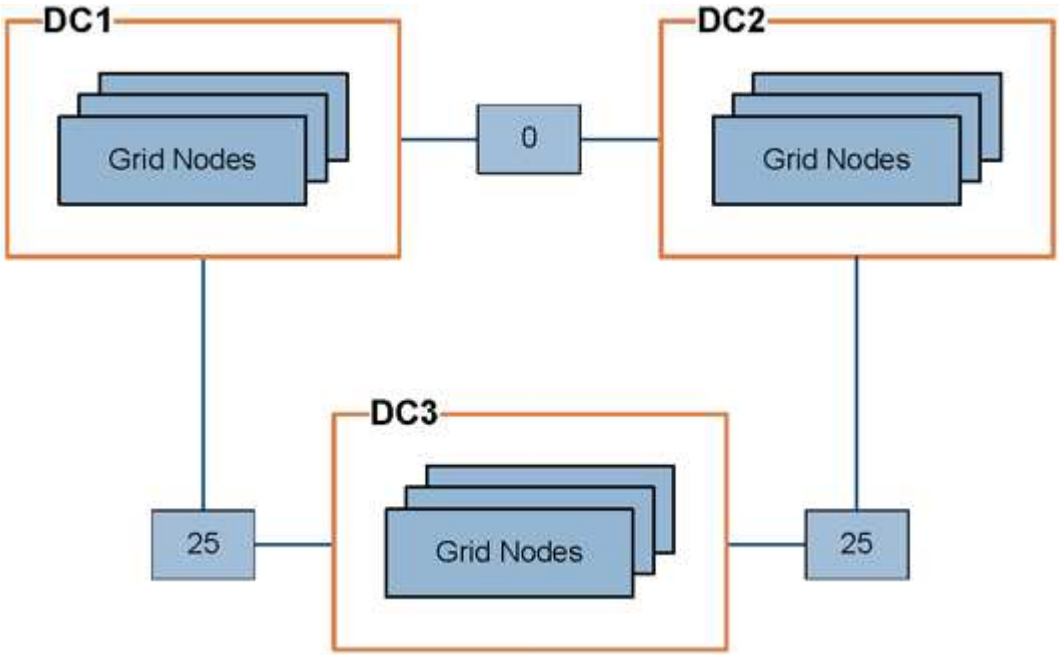
リンクコストを使用すると、複数のデータセンターサイトが存在する場合に、要求されたサービスを提供するデータセンターサイトの優先順位を決定できます。サイト間のレ

イテンシに合わせてリンクコストを調整できます。

- リンクコストは、オブジェクトの読み出しにどのオブジェクトコピーを使用するかを優先的に処理するために使用されます。
- リンクコストは、グリッド管理 API およびテナント管理 API で、使用する内部 StorageGRID サービスを決定するために使用されます。
- リンクコストは、ゲートウェイノード上のCLBサービスがクライアント接続を転送するために使用します。

> CLB サービスは廃止されました。

次の図は、サイト間でリンクコストが設定されている 3 つのサイトグリッドを示しています。




- ゲートウェイノード上の CLB サービスは、同じデータセンターサイトにあるすべてのストレージノード、およびリンクコストが 0 のデータセンターサイトにクライアント接続を均等に分散します。

  この例で、データセンターサイト 1 （ DC1 ）にあるゲートウェイノードは、 DC1 にあるストレージノードと DC2 にあるストレージノードにクライアント接続を均等に分散します。DC3 にあるゲートウェイノードは、 DC3 にあるストレージノードにのみクライアント接続を送信します。

- 複数のレプリケートコピーが存在するオブジェクトを読み出す場合、 StorageGRID はリンクコストが最も低いデータセンターにあるコピーを読み出します。

  この例で、 DC2 にあるクライアントアプリケーションが DC1 と DC3 の両方に格納されているオブジェクトを読み出す場合、 DC1 から DC2 へのリンクコストは 0 で、 DC3 から DC2 へのリンクコスト（ 25 ）よりも低いため、オブジェクトは DC1 から読み出されます。

リンクコストは、測定単位を伴わない任意の相対的な数値です。たとえば、使用にあたってリンクコスト 50 の優先度はリンクコスト 25 よりも低くなります。次の表に、よく使用されるリンクコストを示します。

| リンク | リンクコスト | 注： |
| --- | --- | --- |
| 物理データセンターサイト間 | 25 （デフォルト） | WAN リンクで接続されたデータセンター。 |
| 同じ物理的な場所にある論理データセンターサイト間 | 0 | 同じ物理ビルディングまたはキャンパスにある論理データセンターを LAN で接続します。 |

関連情報

"ロードバランシングの仕組み - CLB サービス"

リンクコストを更新しています

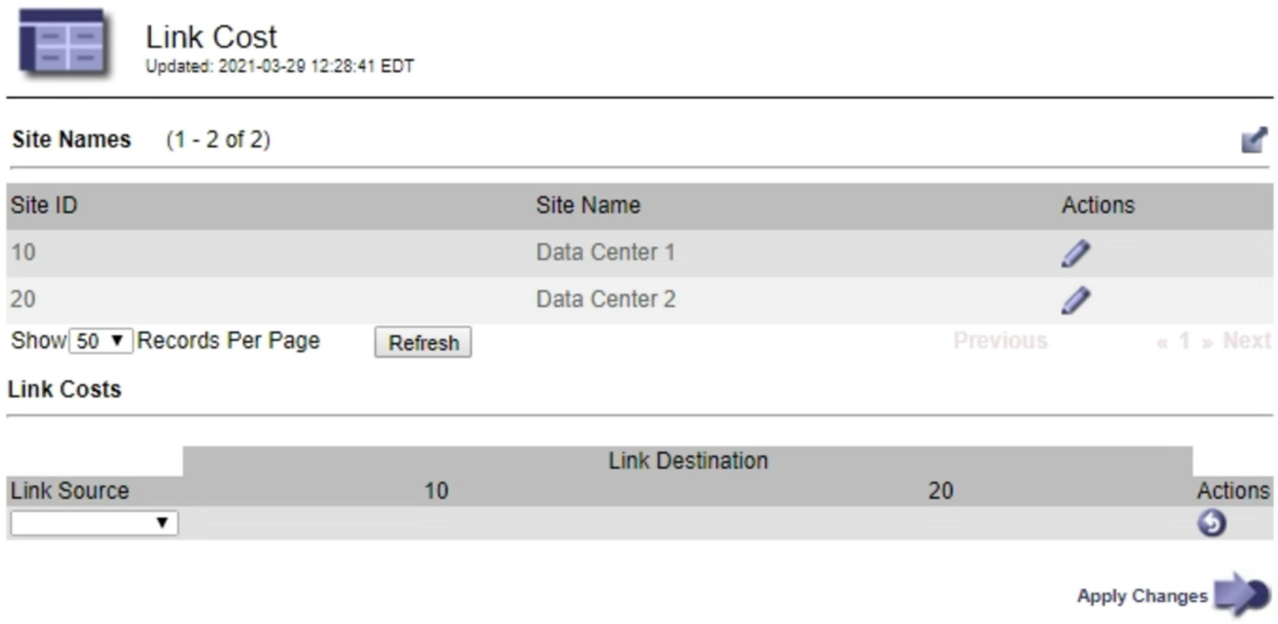
# データセンターサイト間のリンクコストを更新して、サイト間のレイテンシを反映させることができます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Grid Topology Page Configuration権限が必要です。

手順

1. [環境設定]>[ネットワーク設定]>[リンクコスト]を選択します。




2. [ リンク先 * ] でサイトを選択し、 [ リンク先 * ] に 0 ～ 100 のコスト値を入力します。

   リンク元がリンク先と同じ場合は、リンクコストを変更できません。

   変更をキャンセルするには、をクリックします * 復帰 * 。

3. [ 変更の適用 *] をクリックします。

## AutoSupport を設定しています

AutoSupport 機能を使用すると、 StorageGRID システムのヘルスメッセージおよびステータスメッセージをテクニカルサポートに送信できます。AutoSupport を使用すると、問題の特定と解決にかかる時間を大幅に短縮できます。また、システムのストレージニーズを監視し、新しいノードやサイトを追加する必要があるかどうかを判断するための支援も行います。必要に応じて、 1 つの別の送信先に AutoSupport メッセージを送信するように設定できます。

### AutoSupport メッセージに含まれる情報

AutoSupport メッセージには次のような情報が含まれます。

- StorageGRID ソフトウェアのバージョン
- オペレーティングシステムのバージョン
- システムレベルおよび場所レベルの属性情報
- 最新のアラートとアラーム（従来型システム）
- 履歴データを含む、すべてのグリッドタスクの現在のステータス
- ノード*グリッドノード**イベント*ページに表示されるイベント情報
- 管理ノードデータベースの使用率
- 失われた、または欠落しているオブジェクトの数
- Grid の設定
- NMS エンティティ
- アクティブな ILM ポリシー
- プロビジョニングされたグリッド仕様ファイル
- 診断メトリック

AutoSupport 機能および個々の AutoSupport オプションは、 StorageGRID の初回インストール時に有効にするか、あとから有効にすることができます。AutoSupport が有効になっていない場合は、Grid ManagerDashboardにメッセージが表示されます。このメッセージには、 AutoSupport 設定ページへのリンクが含まれています。

「x」記号を選択できます をクリックしてメッセージを閉じます。このメッセージは、AutoSupport が無効なままであっても、ブラウザキャッシュがクリアされるまで表示されません。

### Active IQ を使用する

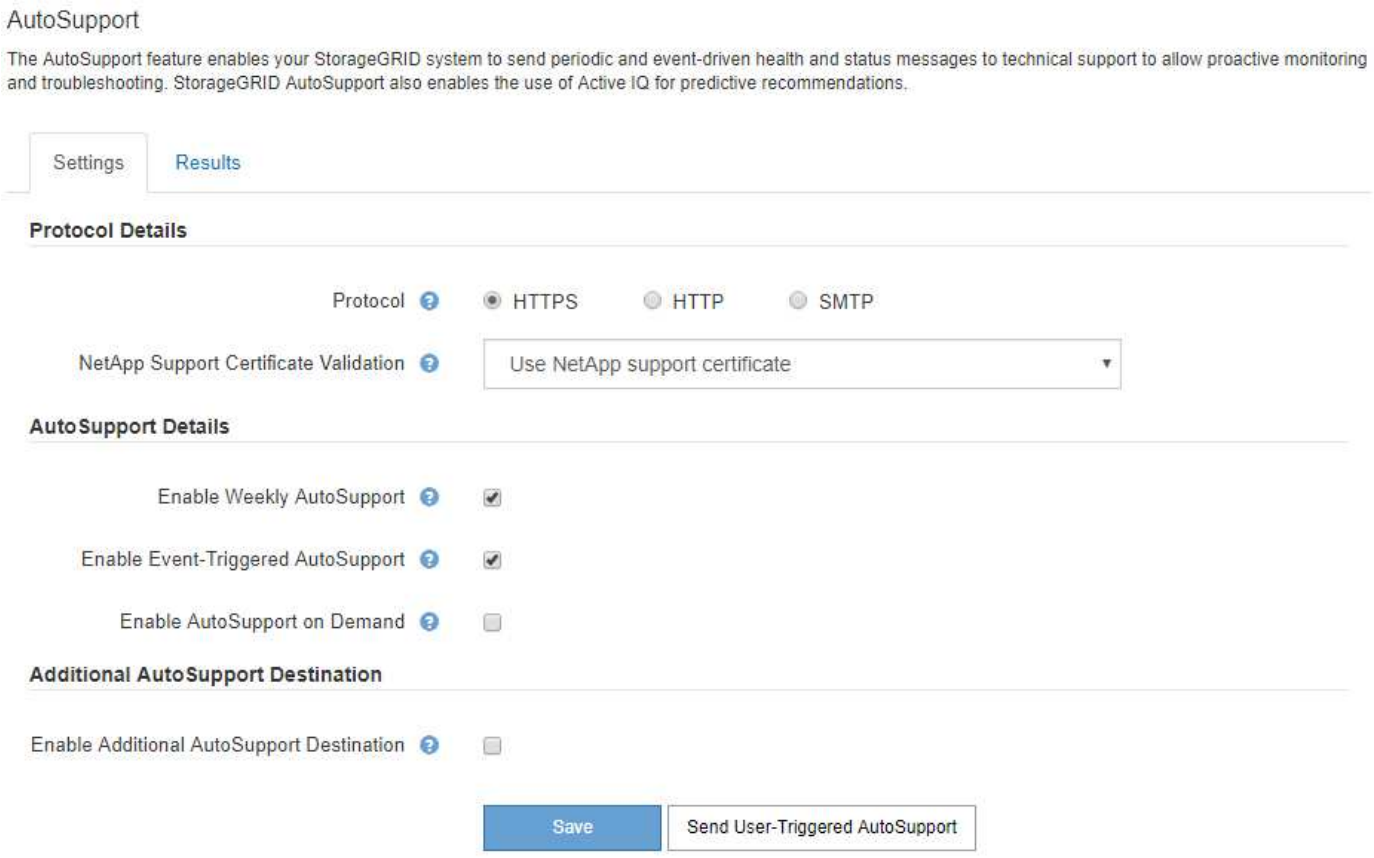
Active IQ は、ネットアップのインストールベースが提供する予測分析と集合知を活用する、クラウドベースのデジタルアドバイザです。継続的なリスク評価、予測アラート、規範となるガイダンス、自動化されたアクションによって、問題が発生する前に予防できます。これにより、システムの健全性が向上し、システムの可用性が向上します。

NetApp Support Siteの Active IQ ダッシュボードと機能を使用する場合は、 AutoSupport を有効にする必要があります。

"Active IQ Digital Advisorのドキュメント"

### AutoSupport 設定にアクセスしています

AutoSupport はGrid Manager（* Support > Tools > AutoSupport *）を使用して設定します。「 * AutoSupport * 」ページには、 * 設定 * と * 結果 * の 2 つのタブがあります。




### AutoSupport メッセージを送信するためのプロトコル

AutoSupport メッセージの送信には、次の 3 つのプロトコルのいずれかを選択できます。

- HTTPS
- HTTP
- SMTP

HTTPS または HTTP を使用して AutoSupport メッセージを送信する場合は、管理ノードとテクニカルサポートの間に非透過型プロキシサーバを設定できます。

SMTP を AutoSupport メッセージのプロトコルとして使用する場合は、 SMTP メールサーバを設定する必要があります。

### AutoSupport オプション

AutoSupport メッセージをテクニカルサポートに送信するには、次のオプションを任意に組み合わせて使用できます。

- * 週単位 * ： AutoSupport メッセージを週に 1 回自動的に送信します。デフォルト設定： Enabled （有効）。
- * イベントトリガー型 * ： 1 時間ごと、または重大なシステムイベントが発生したときに、 AutoSupport メッセージを自動的に送信します。デフォルト設定： Enabled （有効）。
- * On Demand * ： StorageGRID システムが AutoSupport メッセージを自動的に送信するようテクニカルサポートから要求できます。これは、問題 がアクティブに機能している場合に便利です（ HTTPS AutoSupport 転送プロトコルが必要）。デフォルト設定： Disabled （無効）。
- * User-triggered * ： AutoSupport メッセージをいつでも手動で送信します。

関連情報

"ネットアップサポート"

### AutoSupport メッセージのプロトコルの指定

## AutoSupport メッセージの送信には、3つのプロトコルのいずれかを使用できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限または Other Grid Configuration 権限が必要です。
- AutoSupport メッセージの送信用にHTTPSプロトコルまたはHTTPプロトコルを使用する場合は、プライマリ管理ノードへのアウトバウンドインターネットアクセスを直接提供するか、プロキシサーバを使用して提供しておく必要があります（インバウンド接続は不要です）。
- HTTPSまたはHTTPプロトコルの使用時にプロキシサーバを使用する場合は、管理プロキシサーバを設定しておく必要があります。
- AutoSupport メッセージのプロトコルとしてSMTPを使用する場合は、SMTPメールサーバを設定しておく必要があります。アラームの E メール通知には同じメールサーバ設定（従来のシステム）が使用されます。

このタスクについて

AutoSupport メッセージは、次のいずれかのプロトコルを使用して送信できます。

- * HTTPS * ：これはデフォルトで、新規インストールに推奨される設定です。HTTPS プロトコルはポート 443 を使用します。AutoSupport On Demand 機能を有効にする場合は、 HTTPS プロトコルを使用する必要があります。
- * HTTP * ：このプロトコルは、インターネット経由でデータを送信する際にプロキシサーバーが HTTPS に変換する信頼された環境で使用されない限り、安全ではありません。HTTP プロトコルはポート 80 を使用します。
- * SMTP * ： AutoSupport メッセージを E メールで送信する場合は、このオプションを使用します。SMTPをAutoSupport メッセージのプロトコルとして使用する場合は、[Legacy Email Setup]ページ

（* Support * Alarms（レガシー）* **Legacy Email Setup**）でSMTPメールサーバを設定する必要があります。

> StorageGRID 11.2 より前のリリースでは、 SMTP が AutoSupport メッセージに使用できる唯一のプロトコルでした。以前のバージョンの StorageGRID をインストールしていた場合は、 SMTP がプロトコルとして選択されている可能性があります。

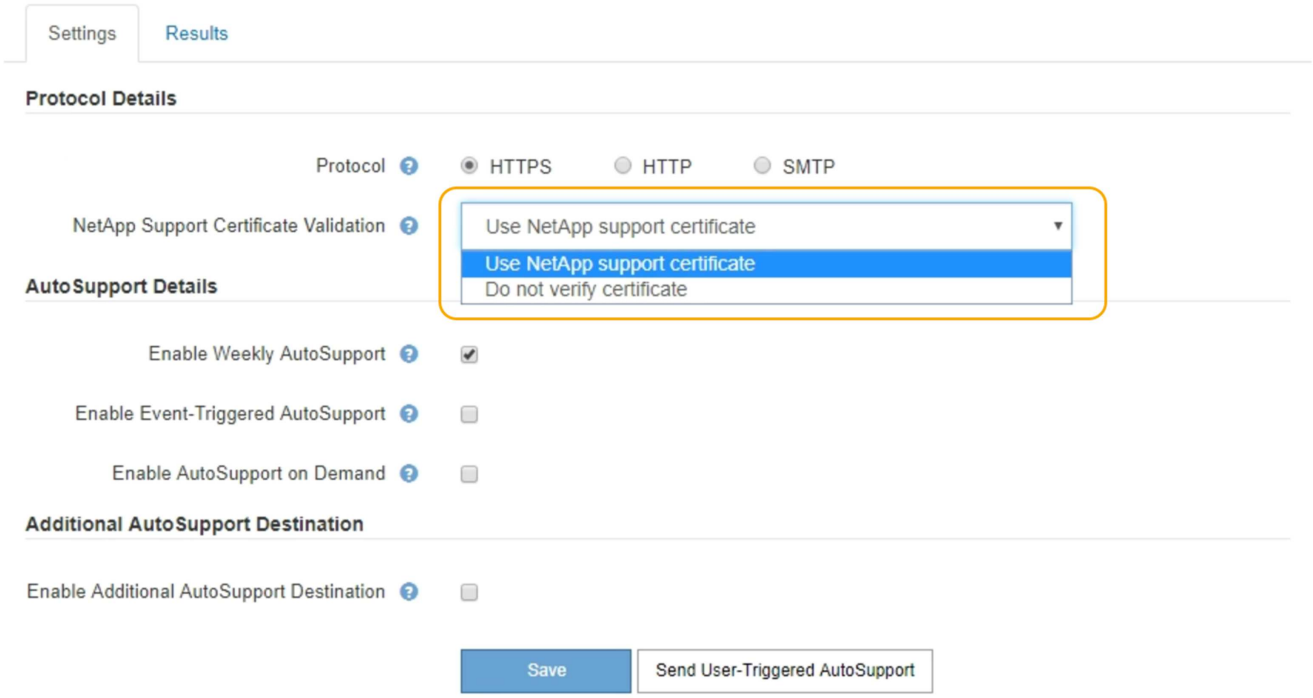
設定したプロトコルは、すべてのタイプの AutoSupport メッセージの送信に使用されます。

手順

1. [サポート（Support ）]>[*ツール（* Tools ）]>[ AutoSupport （*）]

   AutoSupport ページが表示され、 * 設定 * タブが選択されます。

2. AutoSupport メッセージの送信に使用するプロトコルを選択します。




3. ネットアップサポート証明書の検証*を選択します。

   - ネットアップサポート証明書を使用（デフォルト）：証明書の検証により、AutoSupport メッセージの送信がセキュアになります。ネットアップサポート証明書は、 StorageGRID ソフトウェアとともにすでにインストールされています。
   - Do not verify certificate（証明書を検証しない）：このオプションは、証明書の一時的な問題が発生した場合など、証明書の検証を使用しない十分な理由がある場合にのみ選択します。

4. [ 保存（ Save ） ] を選択します。

   毎週、ユーザトリガー型、およびイベントトリガー型のすべてのメッセージが選択したプロトコルを使用して送信されます。

関連情報

"管理プロキシの設定"

**AutoSupport On Demand**の有効化

AutoSupport On Demand は、テクニカルサポートが問題解決に積極的に取り組んでいる場合に役立ちます。AutoSupport On Demandを有効にすると、テクニカルサポートはユーザの介入を必要とせずにAutoSupport メッセージの送信を要求できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限または Other Grid Configuration 権限が必要です。
- 週次AutoSupport メッセージを有効にしておく必要があります。
- 転送プロトコルをHTTPSに設定しておく必要があります。

このタスクについて

この機能を有効にすると、テクニカルサポートは、StorageGRID システムに対してAutoSupport メッセージを自動的に送信するよう要求できます。テクニカルサポートは、 AutoSupport On Demand クエリのポーリング間隔も設定できます。

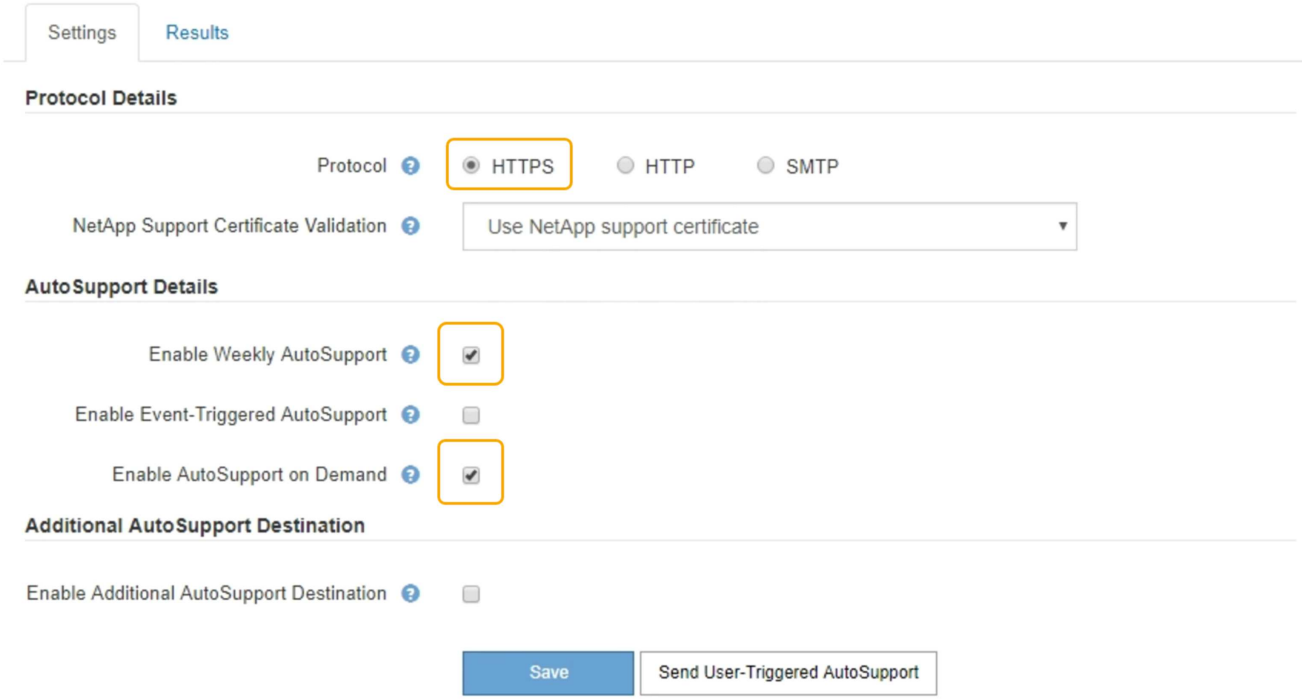
テクニカルサポートは、 AutoSupport On Demand を有効または無効にすることはできません。

手順

1. [サポート（Support ）**]>[***ツール（* Tools ）**]>[** AutoSupport （*）]

   AutoSupport ページが表示され、 * 設定 * タブが選択されます。

2. ページの「* Protocol Details *」セクションで、「HTTPS」ラジオボタンを選択します。




3. [ 週次 AutoSupport を有効にする *] チェックボックスをオンにします。
4. [ オンデマンド AutoSupport を有効にする *] チェックボックスをオンにします。

5. [ 保存（ Save ） ] を選択します。

   AutoSupport On Demand は有効になっており、テクニカルサポートは AutoSupport On Demand 要求を StorageGRID に送信できます。

## 週次**AutoSupport** メッセージの無効化

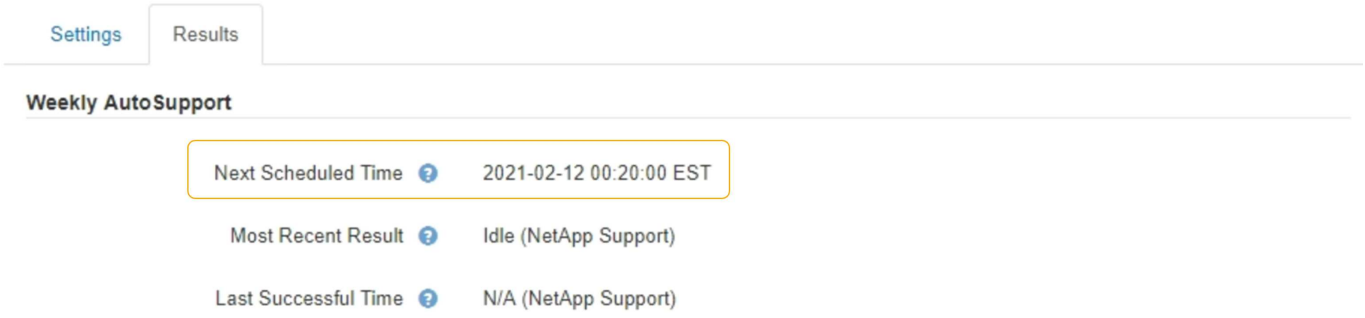
デフォルトでは、 StorageGRID システムは週に 1 回ネットアップサポートに AutoSupport メッセージを送信するように設定されています。

### 必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限または Other Grid Configuration 権限が必要です。

### このタスクについて

週次AutoSupport メッセージが送信されるタイミングを確認するには、「* AutoSupport **>** Results 」ページの「 Weekly AutoSupport 」の「 Next Scheduled Time *」を参照してください。



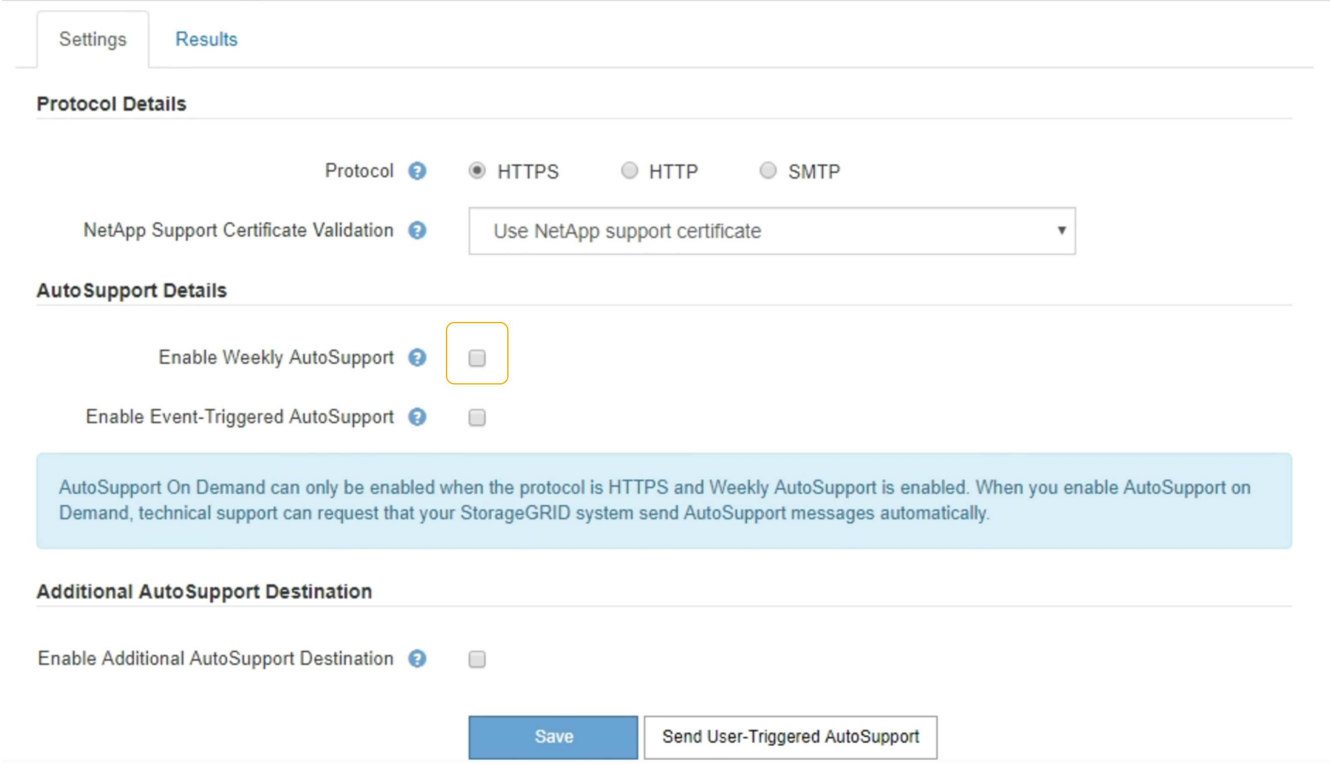

AutoSupport メッセージの自動送信はいつでも無効にすることができます。

### 手順

1. [サポート（Support ）**]>[***ツール（* Tools ）**]>[** AutoSupport （*）]

   AutoSupport ページが表示され、 * 設定 * タブが選択されます。

2. [毎週AutoSupport を有効にする*]チェックボックスをオフにします。




3. [ 保存（ Save ） ] を選択します。

イベントトリガー型**AutoSupport** メッセージを無効にします

デフォルトでは、 StorageGRID システムは、重要なアラートやその他の重大なシステムイベントが発生したときに AutoSupport メッセージをネットアップサポートに送信するように設定されています。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限または Other Grid Configuration 権限が必要です。

このタスクについて

イベントトリガー型 AutoSupport メッセージはいつでも無効にすることができます。

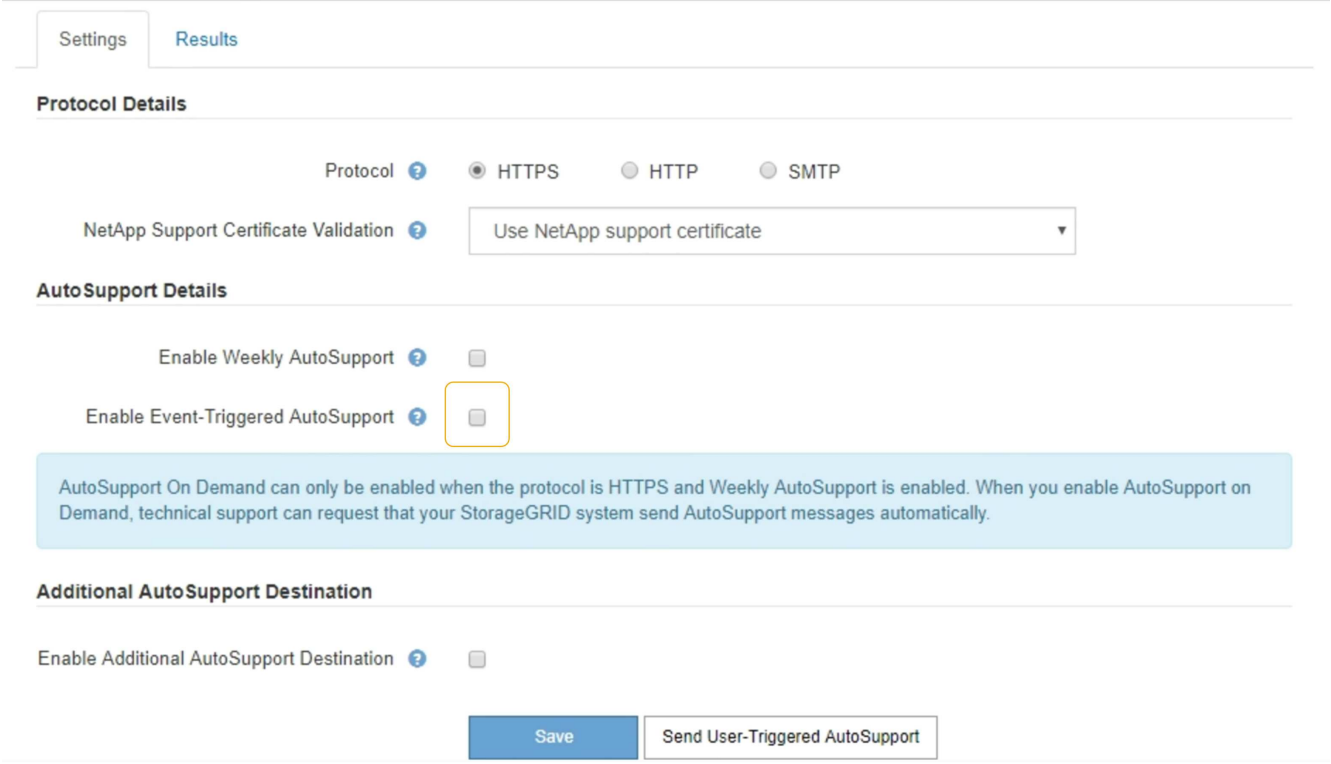
> システム全体で E メール通知を停止した場合は、イベントトリガー型 AutoSupport メッセージも生成されません。（「* Configuration * **System Settings * Display Options *」**（設定*システム設定*表示オプション）を選択します。次に、 [* 通知（ Notification ） ] [ すべてを抑制（ Suppress All ） ] を選択

手順

1. [サポート（Support ）**]>[***ツール（* Tools ）**]>[** AutoSupport （*）]

   AutoSupport ページが表示され、 * 設定 * タブが選択されます。

2. Enable Event-triggered AutoSupport *チェックボックスをオフにします。




3. [ 保存（ Save ） ] を選択します。

手動での**AutoSupport** メッセージのトリガー

## テクニカルサポートによる StorageGRID システムの問題のトラブルシューティングを支援するために、 AutoSupport メッセージの送信を手動でトリガーできます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限または Other Grid Configuration 権限が必要です。

手順

1. [サポート（Support ）**]>[***ツール（* Tools ）**]>[** AutoSupport （*）]

   AutoSupport ページが表示され、 * 設定 * タブが選択されます。

2. [ ユーザー起動 AutoSupport 送信 ] を選択します。

   StorageGRID は、テクニカルサポートに AutoSupport メッセージを送信しようとします。試行に成功した場合は、 [ 結果（ Results ） ] タブの [ 最新結果（ Recent Result ） ] * 値と [ 前回成功した時間（ Last Successful Time ） ] * 値が更新されます。問題がある場合、「最新の結果 * 」の値が「失敗」に更新され、 StorageGRID は AutoSupport メッセージの送信を再試行しません。

   ユーザトリガー型 AutoSupport メッセージを送信したあと、 1 分後にブラウザの AutoSupport ページを更新して最新の結果にアクセスします。

**AutoSupport** デスティネーションを追加しています

# AutoSupport を有効にすると、ヘルスメッセージとステータスメッセージがネットアップサポートに送信されます。すべての AutoSupport メッセージに対して、追加の送信先を 1 つ指定できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限または Other Grid Configuration 権限が必要です。

このタスクについて

AutoSupport メッセージの送信に使用されるプロトコルの確認または変更については、AutoSupport プロトコルの指定手順を参照してください。

SMTP プロトコルを使用して、 AutoSupport メッセージを追加の送信先に送信することはできません。

"AutoSupport メッセージのプロトコルの指定"

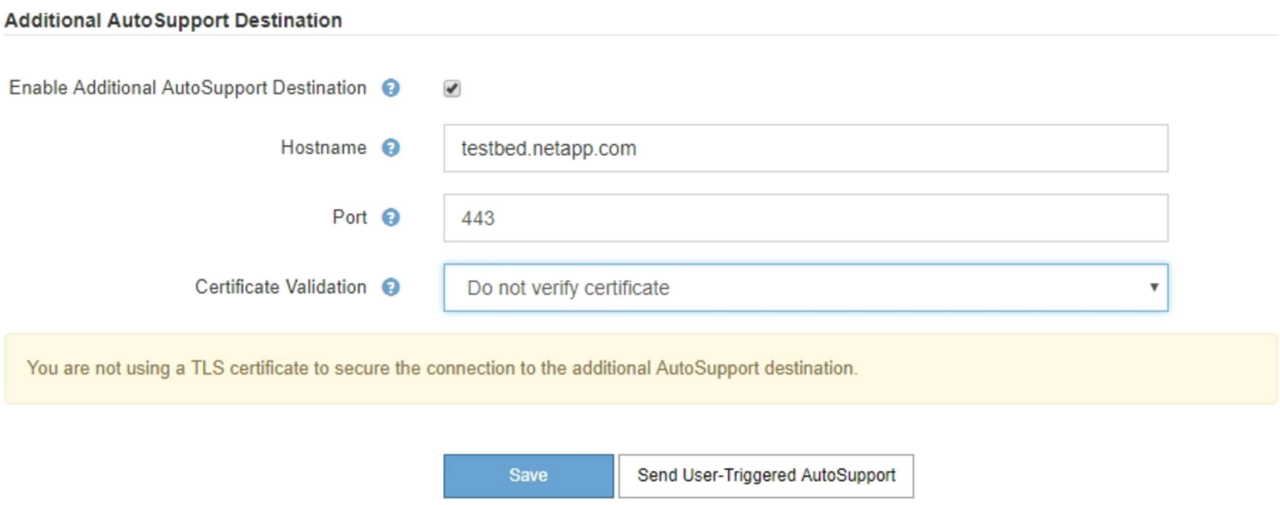
手順

1. [サポート（Support ）**]>[***ツール（* Tools ）**]>[** AutoSupport （*）]

   AutoSupport ページが表示され、 * 設定 * タブが選択されます。

2. [ 追加の AutoSupport 送信先を有効にする *] を選択します。

   追加の AutoSupport Destination フィールドが表示されます。

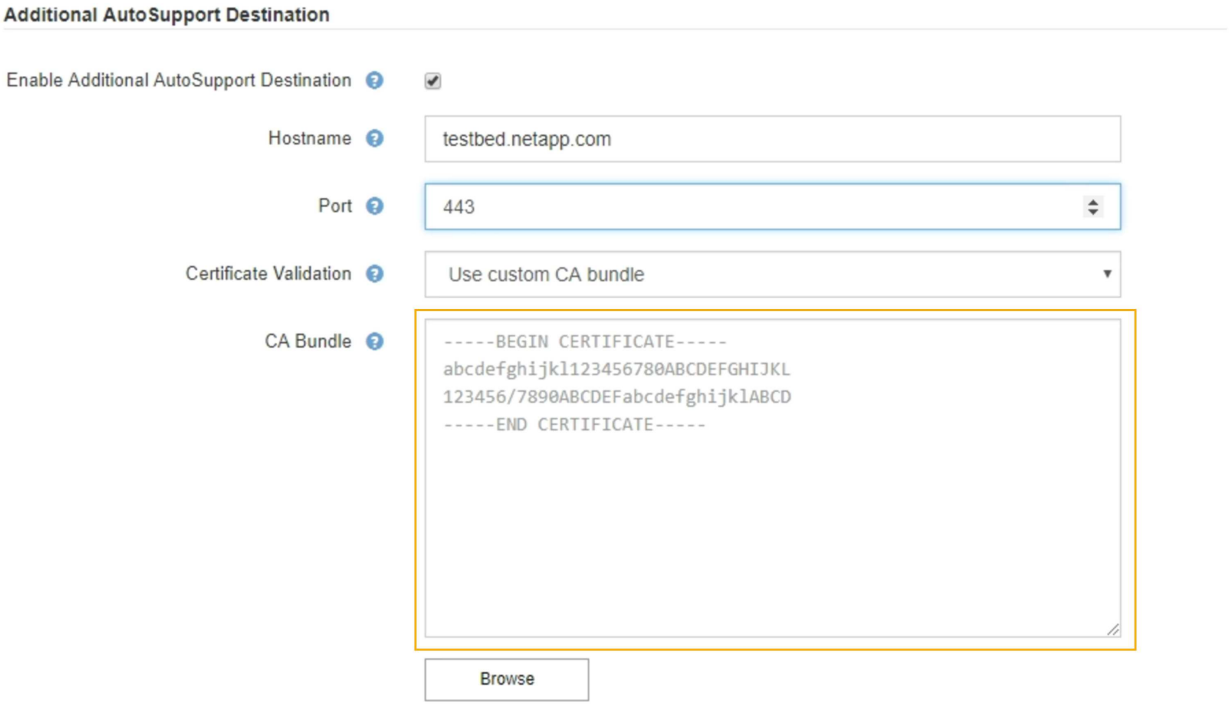



3. 追加の AutoSupport デスティネーションサーバのサーバホスト名または IP アドレスを入力します。

   追加の送信先は 1 つだけ入力できます。

4. 追加の AutoSupport デスティネーションサーバへの接続に使用するポートを入力します（デフォルトは、 HTTP の場合はポート 80 、 HTTPS の場合はポート 443 ）。

5. 証明書の検証とともに AutoSupport メッセージを送信するには、 [ 証明書の検証 *] ドロップダウンで [ カスタム CA バンドルを使用する *] を選択します。次に、次のいずれかを実行します。
   - 編集ツールを使用して、 PEM でエンコードされた各 CA 証明書ファイルのすべての内容を、証明書チェーンの順序で連結された * CA Bundle* フィールドにコピーして貼り付けます。を含める必要があります `----BEGIN CERTIFICATE----` および `----END CERTIFICATE----` を選択します。




   - [ * 参照 * ] を選択し、証明書が含まれているファイルに移動し、 [ * 開く * ] を選択してファイルをアップロードします。証明書の検証により、 AutoSupport メッセージの送信を安全に行うことができます。
6. 証明書の検証を行わずに AutoSupport メッセージを送信するには、 [ 証明書の検証 *] ドロップダウンで [ 証明書を検証しない *] を選択します。

   このオプションは、証明書の検証を使用しない理由がある場合（証明書に一時的な問題がある場合など）にのみ選択してください。

   「 You are not using a TLS certificate to secure connection to the additional AutoSupport destination. 」というメッセージが表示されます。

7. [ 保存（ Save ） ] を選択します。

   それ以降に送信される毎週、イベントトリガー型、およびユーザトリガー型の AutoSupport メッセージは、すべて追加の送信先に送信されます。

### StorageGRID 経由でのEシリーズAutoSupport メッセージの送信

EシリーズSANtricity System ManagerのAutoSupport メッセージは、ストレージアプライアンスの管理ポートではなくStorageGRID 管理ノードからテクニカルサポートに送信できます。

必要なもの

- Grid Managerにはサポートされているwebブラウザを使用してサインインします。
- Storage Appliance Administrator権限またはRoot Access権限が必要です。

> Grid Manager を使用して SANtricity System Manager にアクセスするには、 SANtricity ファームウェア 8.70 以降が必要です。

このタスクについて

E シリーズ AutoSupport メッセージには、ストレージハードウェアの詳細が記載されており、 StorageGRID システムから送信される他の AutoSupport メッセージよりも具体的です。

SANtricity System Manager で特殊なプロキシサーバアドレスを設定して、アプライアンスの管理ポートを使用せずに StorageGRID 管理ノード経由で送信される AutoSupport メッセージを原因 に設定します。この方法で送信される AutoSupport メッセージは、 Grid Manager で設定されている可能性がある優先送信者と管理者のプロキシ設定に基づいています。

Grid Managerで管理プロキシサーバを設定する場合は、管理プロキシの設定手順を参照してください。

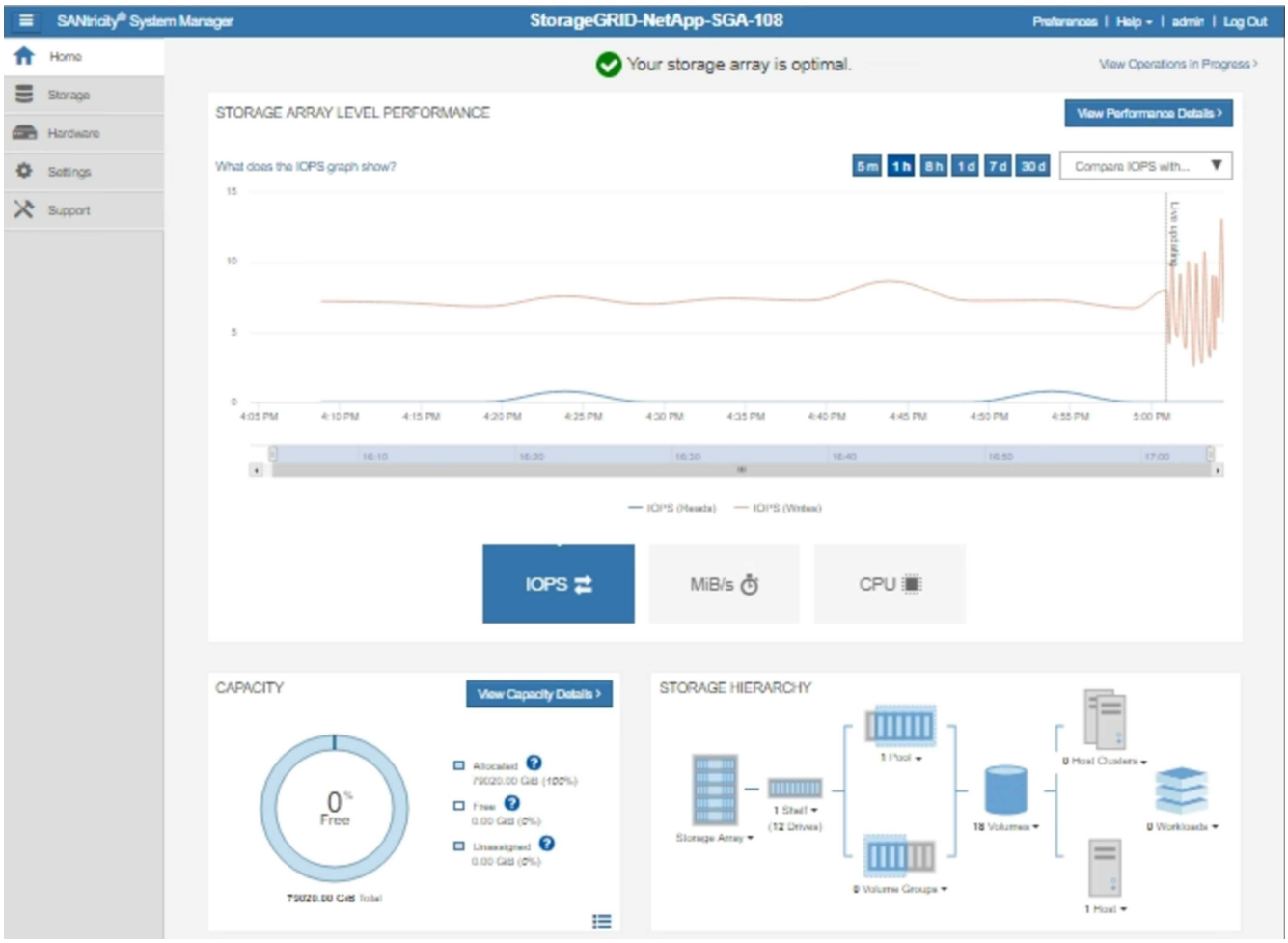
"管理プロキシの設定"

> この手順 は、 E シリーズ AutoSupport メッセージ用に StorageGRID プロキシサーバを設定するためだけに使用します。EシリーズAutoSupport の設定情報の詳細については、Eシリーズのドキュメントセンターを参照してください。
>
> "NetApp Eシリーズシステムのドキュメントセンター"

手順

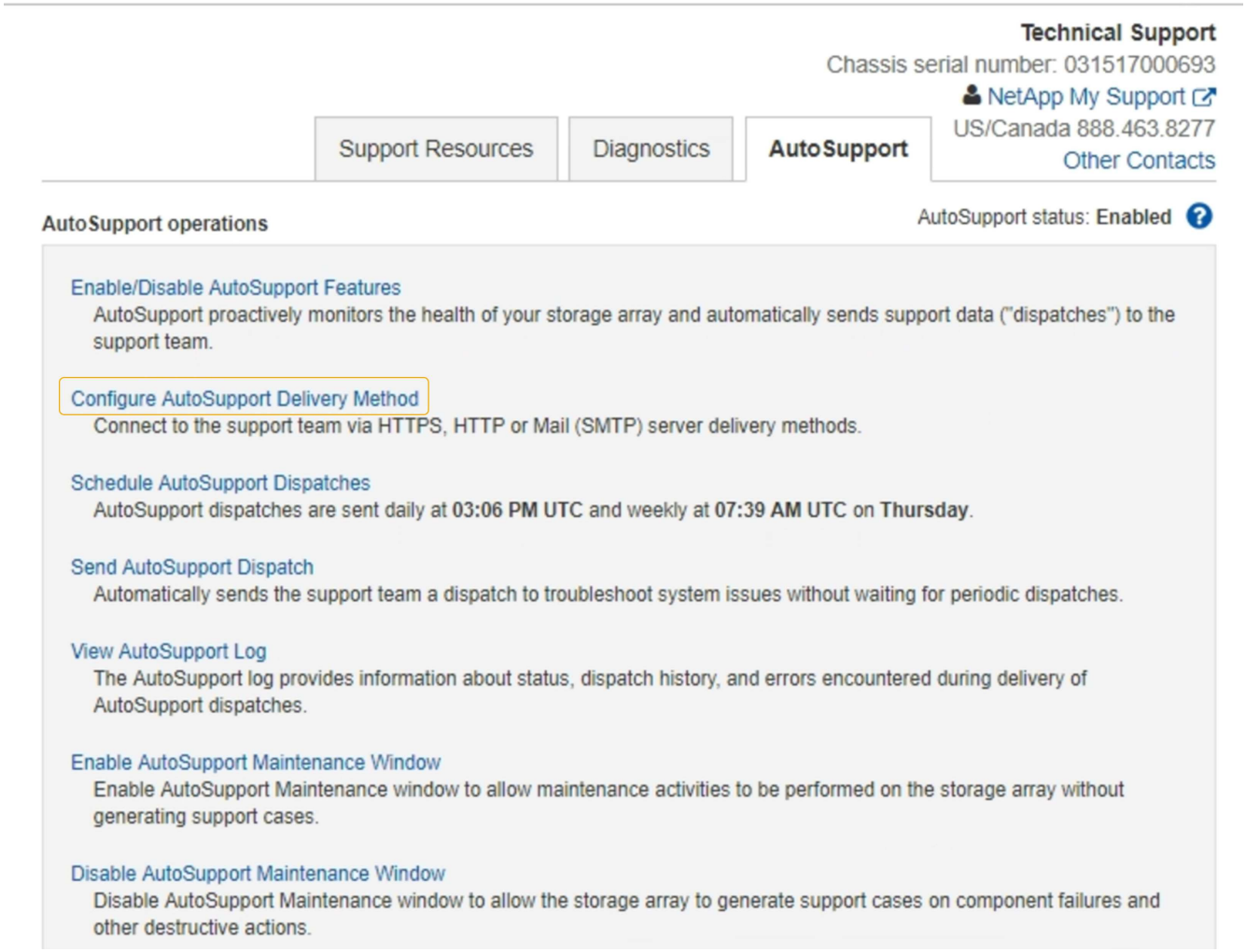
1. Grid Managerで、* Nodes *を選択します。
2. 左側のノードのリストから、設定するストレージアプライアンスノードを選択します。
3. SANtricity System Manager* を選択します。

   SANtricity の System Manager ホームページが表示されます。



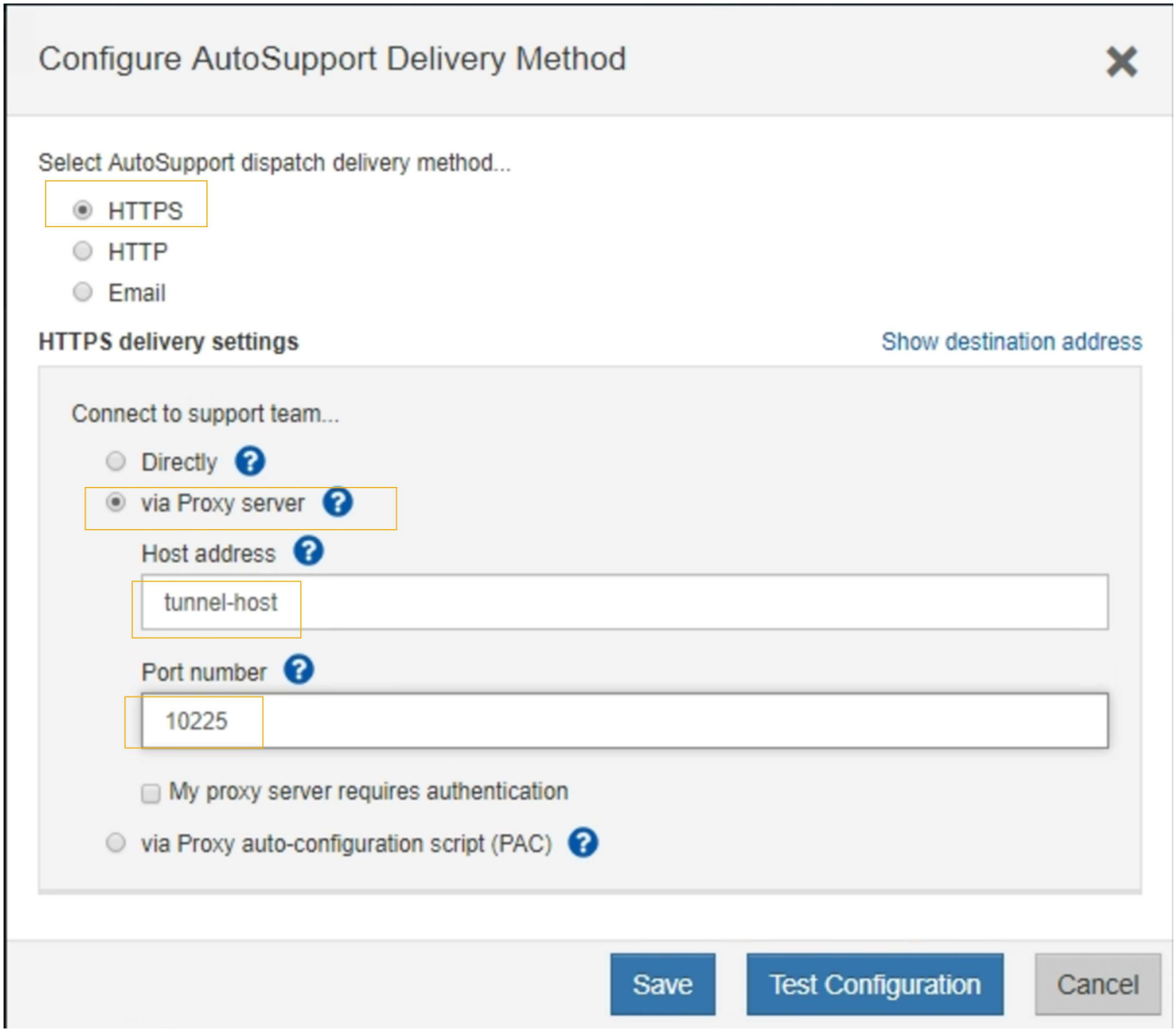

4. [* Support*>]>[* Support center*]>[* AutoSupport *]を選択します。

   AutoSupport operations ページが表示されます。




5. AutoSupport 配信方法の設定 * を選択します。

   AutoSupport 配信方法の設定ページが表示されます。




6. 配信方法として「 * HTTPS * 」を選択します。

   HTTPS プロトコルを有効にする証明書が事前にインストールされています。

7. プロキシサーバー経由 * を選択します。
8. 入力するコマンド `tunnel-host` を入力します。

   `tunnel-host` は、管理ノードを使用してEシリーズAutoSupport メッセージを送信する特別なアドレスです。

9. 入力するコマンド `10225` をクリックします。

   `10225` は、アプライアンスのEシリーズコントローラからAutoSupport メッセージを受信するStorageGRID プロキシサーバのポート番号です。

10. AutoSupport プロキシサーバーのルーティングと設定をテストするには、 * テスト構成 * を選択します。

    正しい場合は、緑色のバナーのメッセージ「 AutoSupport 設定が確認されました。」が表示されます。

テストに失敗した場合は、赤いバナーが表示されます。StorageGRID の DNS 設定とネットワークを確認し、優先送信者である管理ノードがNetApp Support Siteに接続できることを確認してから、もう一度テストを実行してください。

11. [ 保存（ Save ） ] を選択します。

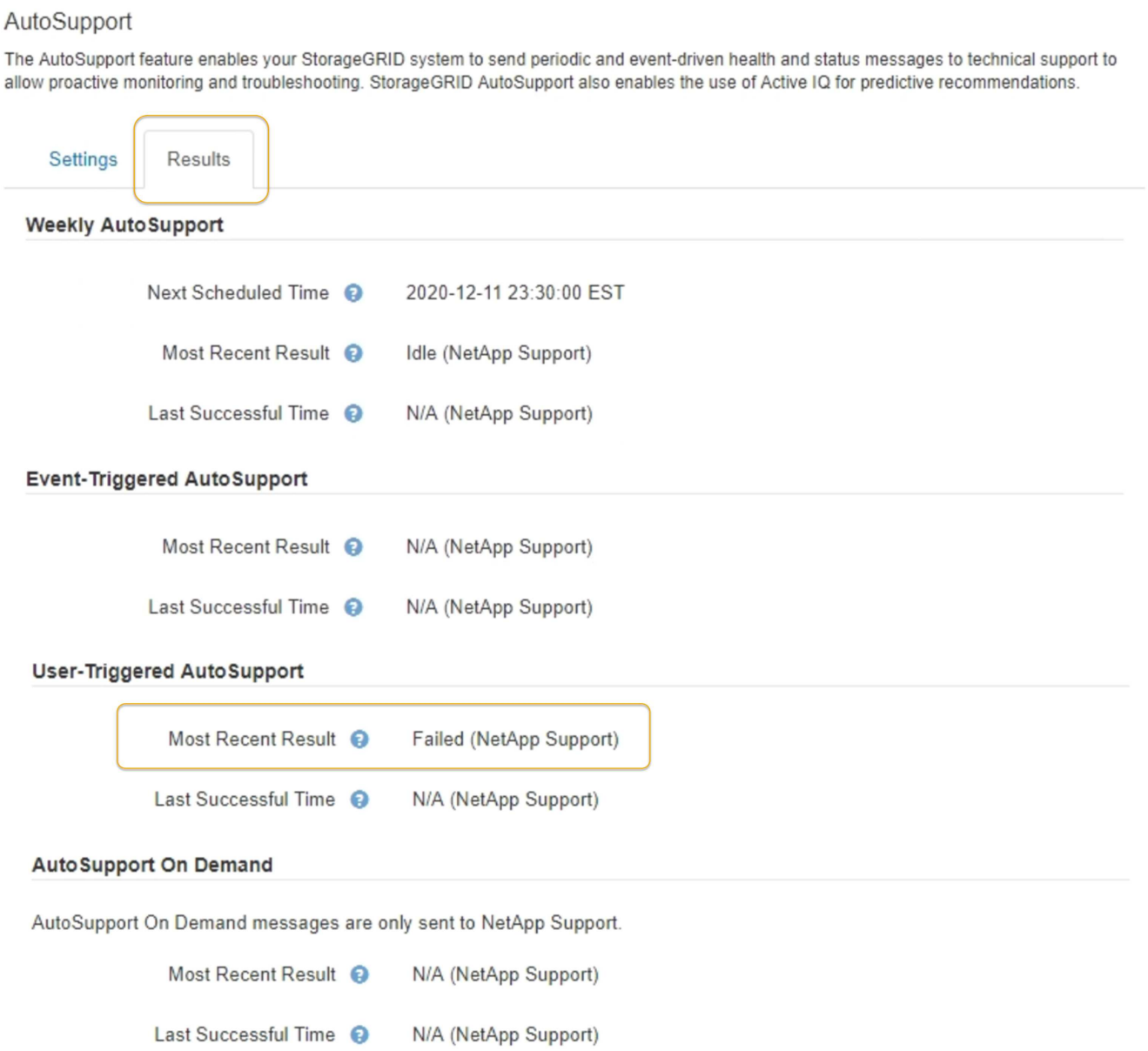
構成が保存され ' AutoSupport 配信方法が構成されましたという確認メッセージが表示されます

**AutoSupport** メッセージのトラブルシューティング

AutoSupport メッセージの送信が失敗すると、 StorageGRID システムは AutoSupport メッセージのタイプに応じて異なる処理を行います。AutoSupport メッセージのステータスを確認するには、サポート*ツール AutoSupport *結果*を選択します。

> E メール通知をシステム全体で停止した場合は、イベントトリガー型 AutoSupport メッセージが生成されなくなります。（「* Configuration * **System Settings** * **Display Options** *」（設定*システム設定*表示オプション）を選択します。次に、 [* 通知（ Notification ） ] [ すべてを抑制（ Suppress All ） ] を選択

AutoSupport メッセージの送信に失敗すると、 AutoSupport ページの * Results * タブに「 Failed 」と表示されます。




週次 **AutoSupport** メッセージのエラーです

週単位の AutoSupport メッセージの送信に失敗した場合、 StorageGRID システムは次の処理を行います。

1. 最新の結果属性を更新して再試行します。
2. 4 分間隔で 15 回、 1 時間 AutoSupport メッセージの再送信を試みます。
3. 送信エラーが 1 時間発生した後、最新の結果属性を失敗に更新します。
4. AutoSupport メッセージの送信を、次にスケジュールされた時刻に再試行します。
5. NMS サービスが利用できないことが原因でメッセージの送信が失敗した場合、および 7 日以内にメッセージが送信された場合は、 AutoSupport の定期送信スケジュールを維持します。
6. 7 日以上メッセージが送信されていない場合は、 NMS サービスが使用可能な状態に戻った時点で AutoSupport メッセージが送信されます。

ユーザトリガー型またはイベントトリガー型の **AutoSupport** メッセージのエラーです

ユーザトリガー型またはイベントトリガー型の AutoSupport メッセージの送信に失敗した場合、StorageGRID システムは次の処理を行います。

1. 既知のエラーの場合は、エラーメッセージが表示されます。たとえば、ユーザが正しいEメール設定を指定せずにSMTPプロトコルを選択した場合、次のエラーが表示されます。 `AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`
2. メッセージの再送信は試行されません。
3. にエラーを記録します `nms.log`。

プロトコルとしてSMTPが選択されている場合に問題が発生した場合は、StorageGRID システムのEメールサーバが正しく設定されていることと、Eメールサーバが実行されていることを確認します（* Support アラーム（レガシー） Legacy Email Setup *）。AutoSupport ページに次のエラーメッセージが表示される場合があります。 `AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

E メールサーバの設定方法については、を参照してください "監視とトラブルシューティングの手順"。

#### **AutoSupport** メッセージのエラーの修正

プロトコルとして SMTP が選択されている状況で問題が発生した場合は、 StorageGRID システムの E メールサーバが正しく設定されていることと、 E メールサーバが実行されていることを確認します。AutoSupport ページに次のエラーメッセージが表示される場合があります。 `AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

関連情報

"トラブルシューティングを監視します"

## ストレージノードの管理

ストレージノードは、ディスクストレージの容量とサービスを提供します。ストレージノードを管理するには、各ノードの使用可能なスペース量を監視し、しきい値を設定し、ストレージノードの設定を適用します。

- "ストレージノードとは"
- "ストレージオプションの管理"
- "オブジェクトメタデータストレージの管理"
- "格納オブジェクトのグローバル設定"
- "ストレージノード設定"
- "容量が上限に達したストレージノードの管理"

### ストレージノードとは

ストレージノードは、オブジェクトデータとメタデータを管理および格納します。各 StorageGRID システムには、少なくとも 3 つのストレージノードが必要です。サイトが

## 複数ある場合は、 StorageGRID システム内の各サイトにも 3 つのストレージノードが必要です。

ストレージノードには、ディスク上のオブジェクトデータとメタデータを格納、移動、検証し、読み出すために必要なサービスとプロセスを提供します。ストレージノードに関する詳細情報は、* Nodes *ページで確認できます。

#### **ADC**サービスとは

Administrative Domain Controller （ ADC ）サービスは、グリッドノードとその相互接続を認証します。ADC サービスは、サイトにある最初の 3 つのストレージノード上でホストされます。

ADC サービスは、サービスの場所や可用性などのトポロジ情報を管理します。あるグリッドノードが別のグリッドノードからの情報を必要とする場合や、別のグリッドノードによる処理を必要とする場合、そのグリッドノードは ADC サービスにアクセスして要求に最適なグリッドノードを見つけます。また、ADCサービスはStorageGRID 環境の設定バンドルのコピーを保持するため、すべてのグリッドノードは現在の設定情報を取得できます。ストレージノードのADC情報は、グリッドトポロジのページ（サポート*グリッドトポロジ）で表示できます。

分散された処理および孤立した処理に対応するため、各 ADC サービスは、証明書、設定バンドル、およびサービスやトポロジに関する情報を、 StorageGRID システム内の他の ADC サービスと同期します。

一般に、すべてのグリッドノードは少なくとも 1 つの ADC サービスへの接続を維持し、これにより、グリッドノードは常に最新情報にアクセスします。ADC サービスに接続したグリッドノードは他のグリッドノードの証明書をキャッシュするため、ある ADC サービスが利用できない場合でも既知のグリッドノードを使用して引き続き機能できます。新しいグリッドノードが接続を確立するためには、 ADC サービスを使用する必要があります。

ADC サービスは接続された各グリッドノードからトポロジ情報を収集します。このグリッドノード情報には、 CPU 負荷、使用可能なディスクスペース（ストレージがある場合）、サポートされているサービス、およびグリッドノードのサイト ID が含まれます。その他のサービスは、トポロジクエリを介して ADC サービスにトポロジ情報を要求します。ADC サービスは、 StorageGRID システムから受信した最新情報で各クエリに応答します。

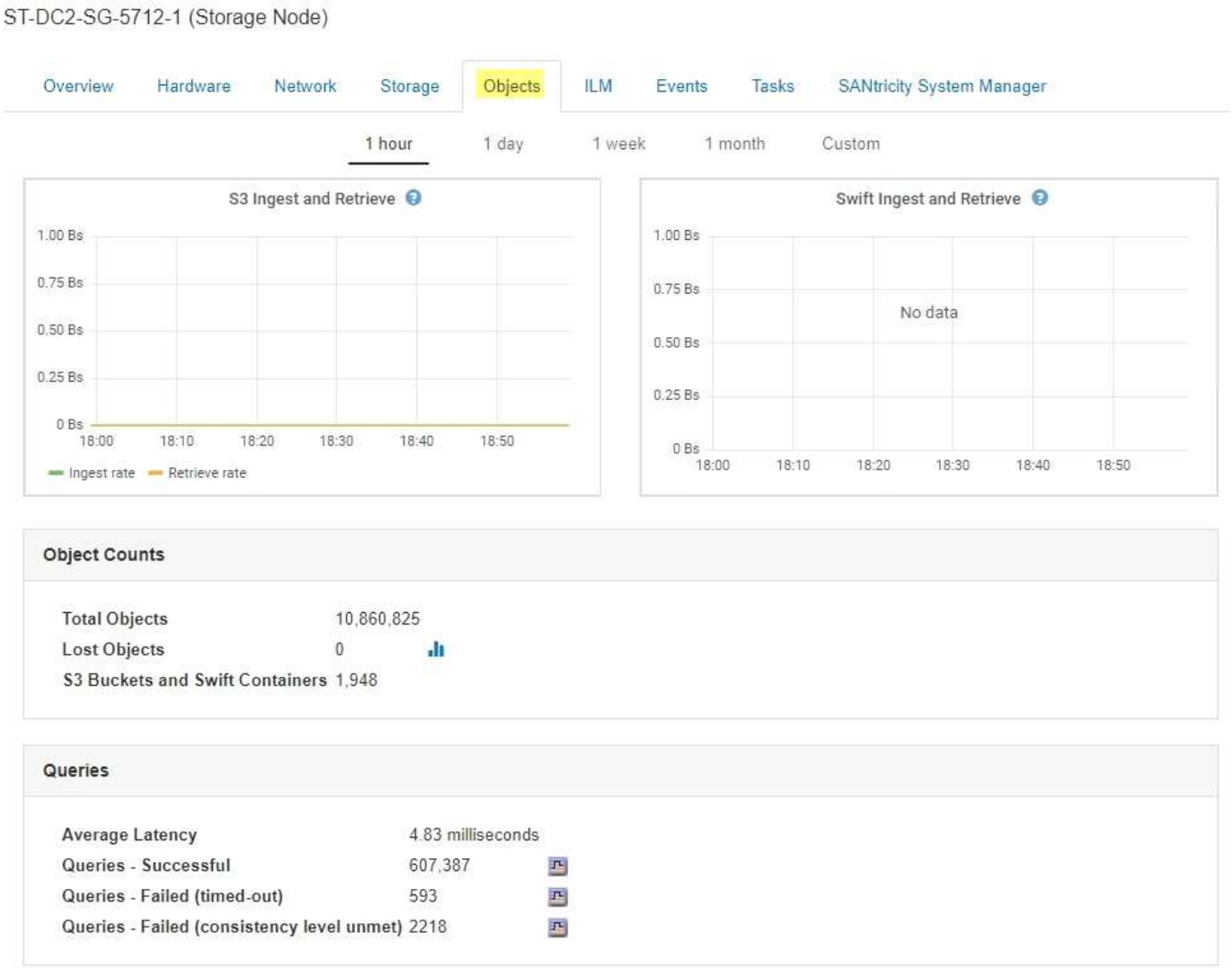
#### **DDS**サービスとは

Distributed Data Store （ DDS ）サービスはストレージノードによってホストされ、 Cassandra データベースとのインターフェイスを提供して、 StorageGRID システムに格納されているオブジェクトメタデータに対してバックグラウンドタスクを実行します。

#### オブジェクト数

DDS サービスは、 StorageGRID システムに取り込まれたオブジェクトの合計数と、システムでサポートされている各インターフェイス（ S3 または Swift ）を使用して取り込まれたオブジェクトの合計数を追跡します。

任意のストレージノードのNodesページのObjectsタブには、Total Objectsの数が表示されます。




クエリ

特定の DDS サービスを使用したメタデータストアに対するクエリの平均実行時間、成功したクエリの合計数、およびタイムアウト問題 が原因で失敗したクエリの合計数を特定できます。

クエリ情報を確認して、メタデータストアである Cassandra の健常性を監視できます。これは、システムの取り込みと読み出しのパフォーマンスに影響します。たとえば、平均的なクエリのレイテンシが遅く、タイムアウトが原因で失敗したクエリの数が多い場合は、メタデータストアの負荷が高いか、または別の処理を実行中である可能性があります。

整合性の問題が原因で失敗したクエリの合計数を確認することもできます。整合性レベルの問題は、特定の DDS サービスを使用してクエリを実行した際に使用可能なメタデータストアの数が不足しているために発生します。

診断ページを使用すると、グリッドの現在の状態の追加情報 を取得できます。を参照してください "診断の実行"。

整合性の保証と制御

StorageGRID は、新しく作成されたオブジェクトのリードアフターライト整合性を保証します。正常に完了した PUT 処理に続く GET 処理では、新しく書き込まれたデータを読み取ることができます。既存のオブジ

ェクトの上書き、メタデータの更新、および削除の整合性レベルは、結果整合性です。

#### LDRサービスとは

Local Distribution Router （ LDR ）サービスは各ストレージノードによってホストされ、 StorageGRID システムのコンテンツ転送を処理します。コンテンツ転送には、データストレージ、ルーティング、要求処理など、多数のタスクが含まれます。LDR サービスは、データ転送の負荷とデータトラフィック機能を処理し、StorageGRID システムの作業の大部分を担います。

LDR サービスは次のタスクを処理します。

- クエリ
- 情報ライフサイクル管理（ ILM ）のアクティビティ
- オブジェクトの削除
- オブジェクトデータのストレージ
- 別の LDR サービス（ストレージノード）からのオブジェクトデータの転送
- データストレージ管理
- プロトコルインターフェイス（ S3 および Swift ）

また、 LDR サービスは、 StorageGRID システムが取り込まれた各オブジェクトに割り当てる一意な「コンテンツハンドル」（ UUID ）と S3 および Swift オブジェクトのマッピングを管理します。

#### クエリ

LDR クエリには、読み出しおよびアーカイブ処理におけるオブジェクトの場所のクエリが含まれます。クエリの平均実行時間、成功したクエリの合計数、およびタイムアウト問題 が原因で失敗したクエリの合計数を特定できます。

クエリ情報を確認して、メタデータストアの健常性を監視できます。メタデータストアの健常性は、システムの取り込みと読み出しのパフォーマンスに影響します。たとえば、平均的なクエリのレイテンシが遅く、タイムアウトが原因で失敗したクエリの数が多い場合は、メタデータストアの負荷が高いか、または別の処理を実行中である可能性があります。

整合性の問題が原因で失敗したクエリの合計数を確認することもできます。整合性レベルの問題は、特定の LDR サービスを使用してクエリを実行した際に使用可能なメタデータストアの数が不足しているために発生します。

診断ページを使用すると、グリッドの現在の状態の追加情報 を取得できます。を参照してください "診断の実行"。

#### ILM アクティビティ

情報ライフサイクル管理（ ILM ）指標を使用すると、 ILM 実装に対してオブジェクトが評価される速度を監視できます。これらの指標は、ダッシュボードまたは各ストレージノードのノードページのILMタブで確認できます。

#### オブジェクトストア

LDR サービスの基盤となるデータストレージは、一定数のオブジェクトストア（ストレージボリュームとも呼ばれます）に分割されます。各オブジェクトストアは個別のマウントポイントです。

ストレージノードのオブジェクトストアは、ノードページのストレージタブで確認できます。

**Object Stores**

| ID | Size | Available | Replicated Data | EC Data | Object Data (%) | Health |
|---|---|---|---|---|---|---|
| 0000 | 4.40 TB | 1.35 TB | 43.99 GB | 0 bytes | 1.00% | No Errors |
| 0001 | 1.97 TB | 1.57 TB | 44.76 GB | 351.14 GB | 20.09% | No Errors |
| 0002 | 1.97 TB | 1.46 TB | 43.29 GB | 465.20 GB | 25.81% | No Errors |
| 0003 | 1.97 TB | 1.70 TB | 43.51 GB | 223.98 GB | 13.58% | No Errors |
| 0004 | 1.97 TB | 1.92 TB | 44.03 GB | 0 bytes | 2.23% | No Errors |
| 0005 | 1.97 TB | 1.46 TB | 43.67 GB | 463.36 GB | 25.73% | No Errors |
| 0006 | 1.97 TB | 1.92 TB | 43.10 GB | 1.61 GB | 2.27% | No Errors |
| 0007 | 1.97 TB | 1.35 TB | 46.05 GB | 575.24 GB | 31.53% | No Errors |
| 0008 | 1.97 TB | 1.81 TB | 46.00 GB | 112.84 GB | 8.06% | No Errors |
| 0009 | 1.97 TB | 1.57 TB | 43.91 GB | 352.72 GB | 20.13% | No Errors |
| 000A | 1.97 TB | 1.70 TB | 44.31 GB | 226.81 GB | 13.76% | No Errors |
| 000B | 1.97 TB | 1.92 TB | 43.17 GB | 780.07 MB | 2.23% | No Errors |
| 000C | 1.97 TB | 1.58 TB | 44.32 GB | 339.56 GB | 19.48% | No Errors |
| 000D | 1.97 TB | 1.82 TB | 44.47 GB | 107.34 GB | 7.70% | No Errors |
| 000E | 1.97 TB | 1.68 TB | 43.07 GB | 241.70 GB | 14.45% | No Errors |
| 000F | 2.03 TB | 1.50 TB | 44.57 GB | 475.47 GB | 25.67% | No Errors |

ストレージノード内のオブジェクトストアは、ボリューム ID と呼ばれる 0000 ~ 002F の 16 進数で識別されます。最初のオブジェクトストア（ボリューム 0 ）では、 Cassandra データベースのオブジェクトメタデータ用にスペースがリザーブされます。このボリュームの残りのスペースはオブジェクトデータに使用されます。他のすべてのオブジェクトストアはオブジェクトデータ専用です。オブジェクトデータにはレプリケートコピーとイレイジャーコーディングフラグメントがあります。

レプリケートコピーのスペース使用量を均等にするために、特定のオブジェクトのオブジェクトデータは、使用可能なストレージスペースに基づいて 1 つのオブジェクトストアに格納されます。1 つ以上のオブジェクトストアの容量を使い果たした場合は、ストレージノード上の容量がなくなるまで、残りのオブジェクトストアが引き続きオブジェクトを格納します。

### メタデータの保護

オブジェクトメタデータは、オブジェクトの変更時刻や格納場所など、オブジェクトに関連する情報またはオブジェクトの概要 です。StorageGRID は Cassandra データベースにオブジェクトメタデータを格納します。Cassandra データベースは LDR サービスと連携します。

冗長性を確保してオブジェクトメタデータを損失から保護するために、各サイトでオブジェクトメタデータのコピーが 3 つ保持されます。各サイトのすべてのストレージノードに均等にコピーが分散されます。このレプリケーションは設定できず、自動的に実行されます。

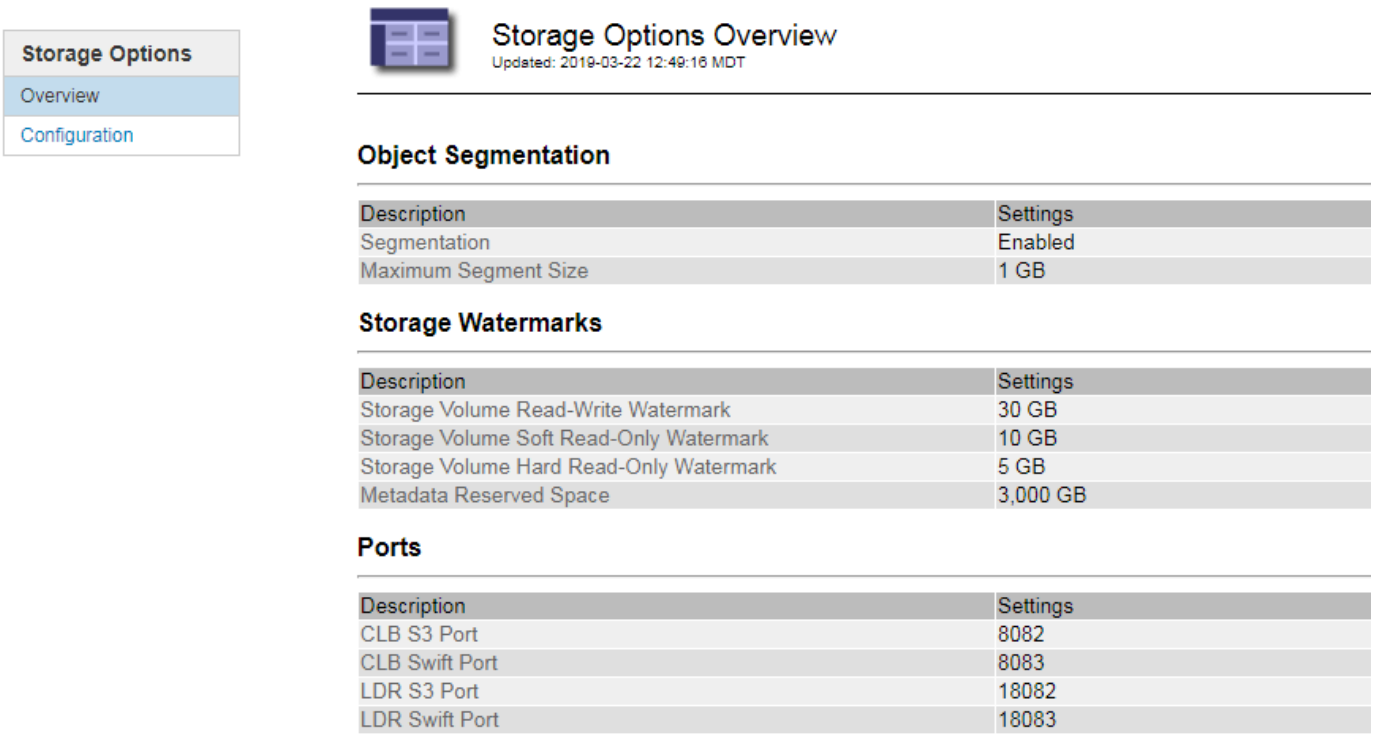
"オブジェクトメタデータストレージの管理"

### ストレージオプションの管理

ストレージオプションは、Grid Managerの設定メニューを使用して表示および設定できます。ストレージオプションには、オブジェクトのセグメント化設定と、ストレージウォーターマークの現在の値が含まれます。ゲートウェイノード上の廃止された CLB サー

ビスおよびストレージノード上の LDR サービスで使用されている S3 および Swift ポートを表示することもできます。

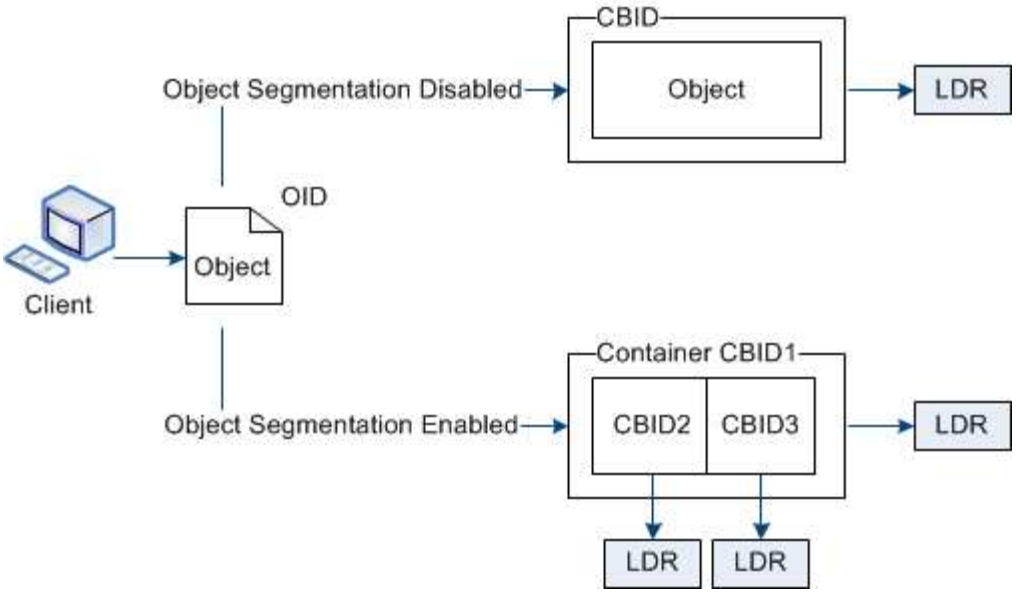
ポート割り当ての詳細については、を参照してください "Summary ：クライアント接続の IP アドレスとポート"。




オブジェクトのセグメント化とは

## オブジェクトのセグメント化は、 1 つのオブジェクトを小さな固定サイズのオブジェクトに分割して、大きいオブジェクトによるストレージとリソースの使用を最適化するプロセスです。S3 のマルチパートアップロードでもセグメント化されたオブジェクトが作成され、各パートを表すオブジェクトが 1 つ作成されます。

オブジェクトが StorageGRID システムに取り込まれると、 LDR サービスはオブジェクトを複数のセグメントに分割し、すべてのセグメントのヘッダー情報をコンテンツとして表示するセグメントコンテナを作成します。




StorageGRID システムに、ターゲットタイプが「Cloud Tiering - Simple Storage Service」で、ターゲットのアーカイブストレージシステムがAmazon Web Services（AWS）のアーカイブノードが含まれている場合、最大セグメントサイズは4.5GiB（4、831、838、208バイト）以下にする必要があります。これは、AWS PUTの最大サイズである5GBを超えないようにするための上限です。この値を超えるAWSへの要求は失敗します。

セグメントコンテナを読み出す際、 LDR サービスは各セグメントから元のオブジェクトを組み立て、クライアントに返します。

コンテナとセグメントは同じストレージノードに格納する必要はありません。コンテナとセグメントは任意のストレージノードに格納できます。

各セグメントは StorageGRID システムによって個別に処理され、 Managed Objects や Stored Objects などの属性の対象としてカウントされます。たとえば、 StorageGRID システムに格納されているオブジェクトが 2 つのセグメントに分割された場合、取り込みが完了すると次のように Managed Objects の値が 3 つ増えます。

セグメントコンテナ + セグメント 1 + セグメント 2 = 3 個の格納オブジェクト

大きいオブジェクトを処理する際のパフォーマンスを向上させるには、次の点を確認します。

- 各ゲートウェイおよびストレージノードに、必要なスループットに十分なネットワーク帯域幅があること。たとえば、グリッドネットワークとクライアントネットワークは 10Gbps イーサネットインターフェイス上に別々に設定します。
- 必要なスループットに十分な数のゲートウェイノードとストレージノードが導入されていること。
- 各ストレージノードのディスク IO パフォーマンスが、必要なスループットに対して十分であること。

ストレージボリュームのウォーターマークとは

StorageGRID では、ストレージボリュームのウォーターマークを使用して、ストレージノードで使用可能なスペースの量を監視できます。ノードで使用可能なスペース量が設定されたウォーターマークよりも少なくなると、Storage Status（SSTS）アラームがトリガーされて、ストレージノードを追加する必要があるかどうかを判断できます。

ストレージ・ボリューム・ウォーターマークの現在の設定を表示するには'[構成*ストレージ・オプション*概要*]を選択します

Storage Options Overview

Updated: 2019-10-09 13:09:30 MDT

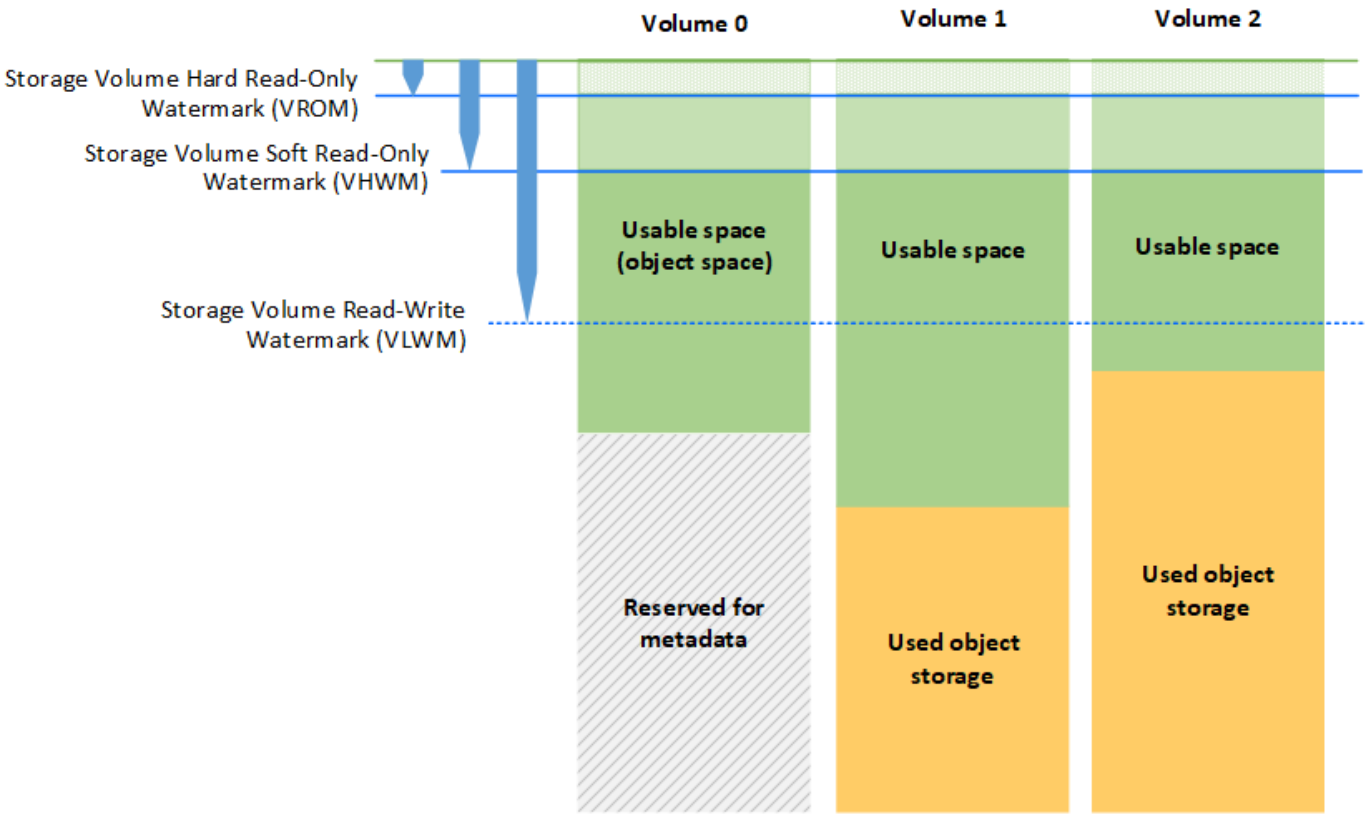
### Object Segmentation

| Description | Settings |
|---|---|
| Segmentation | Enabled |
| Maximum Segment Size | 1 GB |

### Storage Watermarks

| Description | Settings |
|---|---|
| Storage Volume Read-Write Watermark | 30 GB |
| Storage Volume Soft Read-Only Watermark | 10 GB |
| Storage Volume Hard Read-Only Watermark | 5 GB |
| Metadata Reserved Space | 3,000 GB |

次の図は、ボリュームを3つ含むストレージノードでの、3つのストレージボリュームウォーターマークの相対的な位置を示しています。各ストレージノード内で、StorageGRID がオブジェクトメタデータ用にボリューム0のスペースをリザーブし、そのボリュームの残りのスペースはオブジェクトデータに使用されます。他のすべてのボリュームはオブジェクトデータ専用のボリュームです。オブジェクトデータにはレプリケートコピーとイレイジャーコーディングフラグメントがあります。




ストレージボリュームウォーターマークは、ストレージノード内の各ボリュームに必要な最小空きスペースを示すシステム全体のデフォルト値で、この値を超えると、StorageGRID によってノードの読み取り/書き込み動作が変更されたり、アラームがトリガーされたりします。StorageGRID が処理を実行するには、すべてのボリュームがウォーターマークに達する必要があります。一部のボリュームに必要な最小空きスペース量を超えると、アラームはトリガーされず、ノードの読み取り/書き込み動作も変更されません。

**Storage Volume Soft Read-Only Watermark（Vhwm）**

Storage Volume Soft Read-Only Watermarkは、オブジェクトデータに使用可能なノードのスペースがフルに近づいていることを示す最初のウォーターマークです。このウォーターマークは'ノードがソフト読み取り専用モードにならないようにするために'ストレージ・ノード内の各ボリュームに必要な空きスペースの量を表しますソフト読み取り専用モードでは、ストレージノードはStorageGRID システムの他の要素にサービスが読み取り専用であることをアドバタイズしますが、保留中の書き込み要求はすべて実行します。

各ボリュームの空きスペース量がこのウォーターマークを下回ると、Storage Status（SSTS）アラームがNoticeレベルでトリガーされ、ストレージノードはソフト読み取り専用モードに移行します。

たとえば、 Storage Volume Soft Read-Only Watermark がデフォルト値の 10GB に設定されているとします。ストレージノード内の各ボリュームの空きスペースが10GB未満になると、SSTSアラームがNoticeレベルでトリガーされ、ストレージノードはソフト読み取り専用モードに移行します。

#### Storage Volume Hard Read-Only Watermark（VROM）

Storage Volume Hard Read-Only Watermarkは、オブジェクトデータに使用可能なノードのスペースがフルに近づいていることを示す2つ目のウォーターマークです。このウォーターマークは'ノードがハード読み取り専用モードにならないようにするために'ストレージ・ノード内の各ボリュームに必要な空きスペースの量を表しますハード読み取り専用モードでは、ストレージノードは読み取り専用となり、書き込み要求を受け付けません。

ストレージノード内のすべてのボリュームの空きスペース量がこのウォーターマークを下回ると、Storage Status（SSTS）アラームがMajorレベルでトリガーされ、ストレージノードはハード読み取り専用モードに移行します。

たとえば、Storage Volume Hard Read-Only Watermarkがデフォルト値の5GBに設定されているとします。ストレージノード内の各ストレージボリュームの空きスペースが5GB未満になると、SSTSアラームがMajorレベルでトリガーされ、ストレージノードはハード読み取り専用モードに移行します。

Storage Volume Hard Read-Only Watermarkの値は、Storage Volume Soft Read-Only Watermarkの値より小さくする必要があります。

#### Storage Volume Read-Write Watermark（VLWM）

読み取り専用モードに移行したストレージボリューム読み取り/書き込みウォーターマークのみの環境 ストレージノード。このウォーターマークは、ストレージノードが再度読み取り/書き込み可能になるタイミングを決定します。

たとえば、あるストレージノードがハード読み取り専用モードに移行したとします。Storage Volume Read-Write Watermarkが30GB（デフォルト）に設定されている場合、ノードが再度読み取り/書き込み可能になるためには、ストレージノード内の各ストレージボリュームの空きスペースが5GBから30GBに増える必要があります。

Storage Volume Read-Write Watermarkの値は、Storage Volume Soft Read-Only Watermarkの値より大きくする必要があります。

関連情報

"容量が上限に達したストレージノードの管理"

オブジェクトメタデータストレージの管理

# StorageGRID システムのオブジェクトメタデータ容量は、そのシステムに格納できるオブジェクトの最大数を制御します。StorageGRID システムに新しいオブジェクトを格納するための十分なスペースを確保するには、 StorageGRID がオブジェクトメタデータを格納する場所と方法を理解する必要があります。

オブジェクトメタデータとは

オブジェクトメタデータは、オブジェクトについて記述された任意の情報です。StorageGRID では、オブジェクトメタデータを使用してグリッド全体のすべてのオブジェクトの場所を追跡し、各オブジェクトのライフサイクルを継続的に管理します。

StorageGRID のオブジェクトの場合、オブジェクトメタデータには次の種類の情報が含まれます。

- システムメタデータ（各オブジェクトの一意の ID （ UUID ）、オブジェクト名、 S3 バケットまたは

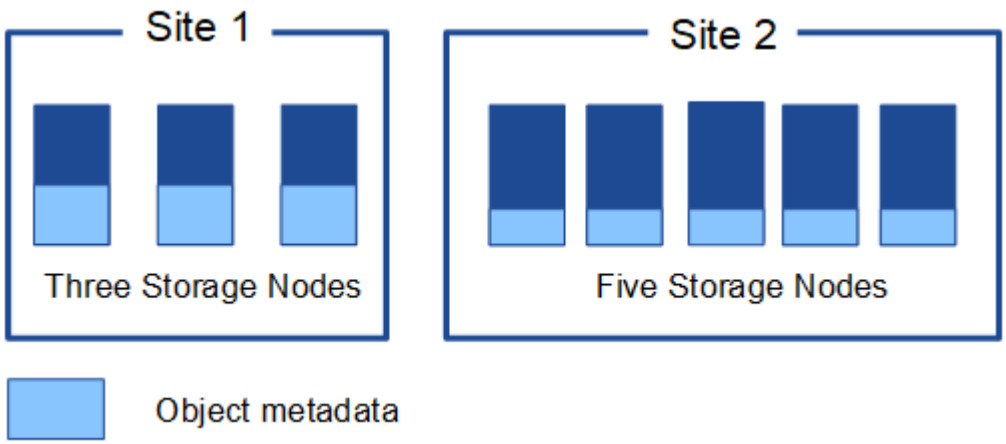
Swift コンテナの名前、テナントアカウントの名前または ID 、オブジェクトの論理サイズ、オブジェクトの作成日時など）、 オブジェクトが最後に変更された日時。

- オブジェクトに関連付けられているカスタムユーザメタデータのキーと値のペア。
- S3 オブジェクトの場合、オブジェクトに関連付けられているオブジェクトタグのキーと値のペア。
- レプリケートオブジェクトコピーの場合、各コピーの現在の格納場所。
- イレイジャーコーディングオブジェクトコピーの場合、各フラグメントの現在の格納場所。
- クラウドストレージプール内のオブジェクトコピーの場合、外部バケットの名前とオブジェクトの一意の識別子を含むオブジェクトの場所。
- セグメント化されたオブジェクトやマルチパートオブジェクトの場合、セグメント ID とデータサイズ。

### オブジェクトメタデータの格納方法

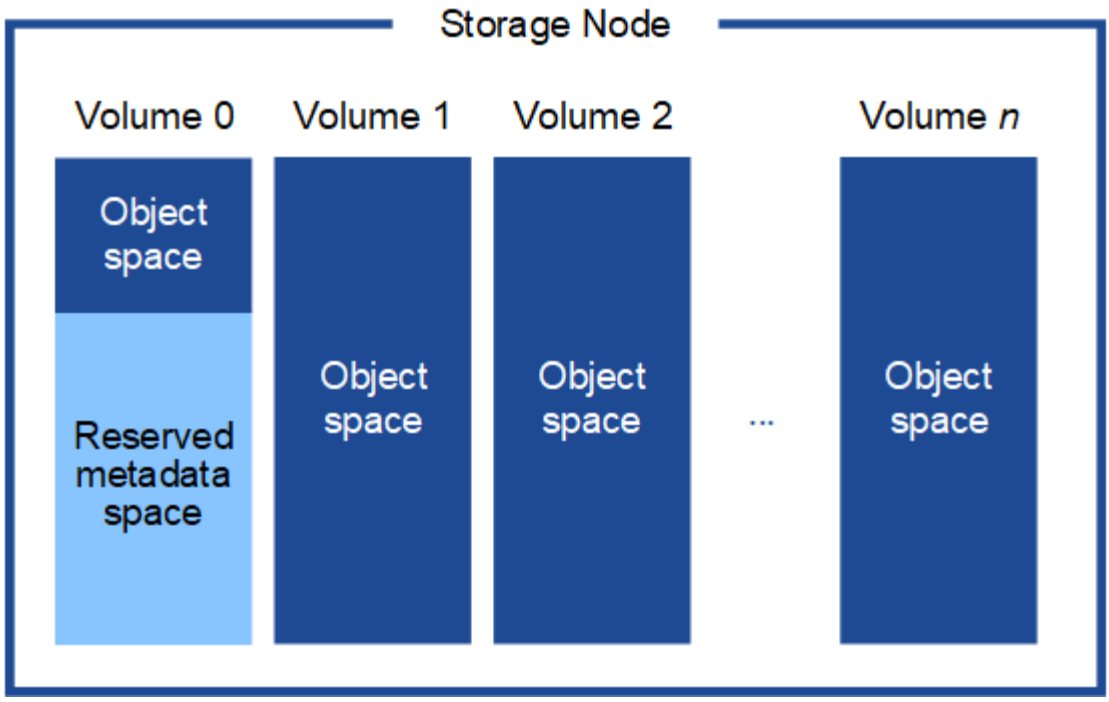
StorageGRID は Cassandra データベースにオブジェクトメタデータを保持し、 Cassandra データベースはオブジェクトデータとは別に格納されます。冗長性を確保し、オブジェクトメタデータを損失から保護するために、 StorageGRID は各サイトのシステム内のすべてのオブジェクトにメタデータのコピーを 3 つずつ格納します。オブジェクトメタデータの 3 つのコピーが各サイトのすべてのストレージノードに均等に分散されます。

この図は、 2 つのサイトのストレージノードを表しています。各サイトに同じ量のオブジェクトメタデータがあり、そのサイトのストレージノード間で均等に分散されます。




### オブジェクトメタデータの格納先

この図は、単一のストレージノードのストレージボリュームを表しています。




図に示すように、 StorageGRID は各ストレージノードのストレージボリューム 0 にオブジェクトメタデータ用のスペースをリザーブします。リザーブスペースを使用してオブジェクトメタデータを格納し、重要なデータベース処理を実行します。ストレージボリューム 0 の残りのスペースとストレージノード内のその他すべてのストレージボリュームは、オブジェクトデータ（レプリケートコピーとイレイジャーコーディングフラグメント）専用に使用されます。

特定のストレージノードでオブジェクトメタデータ用にリザーブされているスペースの量は、次に示すいくつかの要因によって決まります。

#### **Metadata Reserved Space** の設定

Metadata Reserved Space _ は、各ストレージノードのボリューム 0 でメタデータ用にリザーブされるスペースの量を表すシステム全体の設定です。次の表に、StorageGRID 11.5のこの設定のデフォルト値を示します。

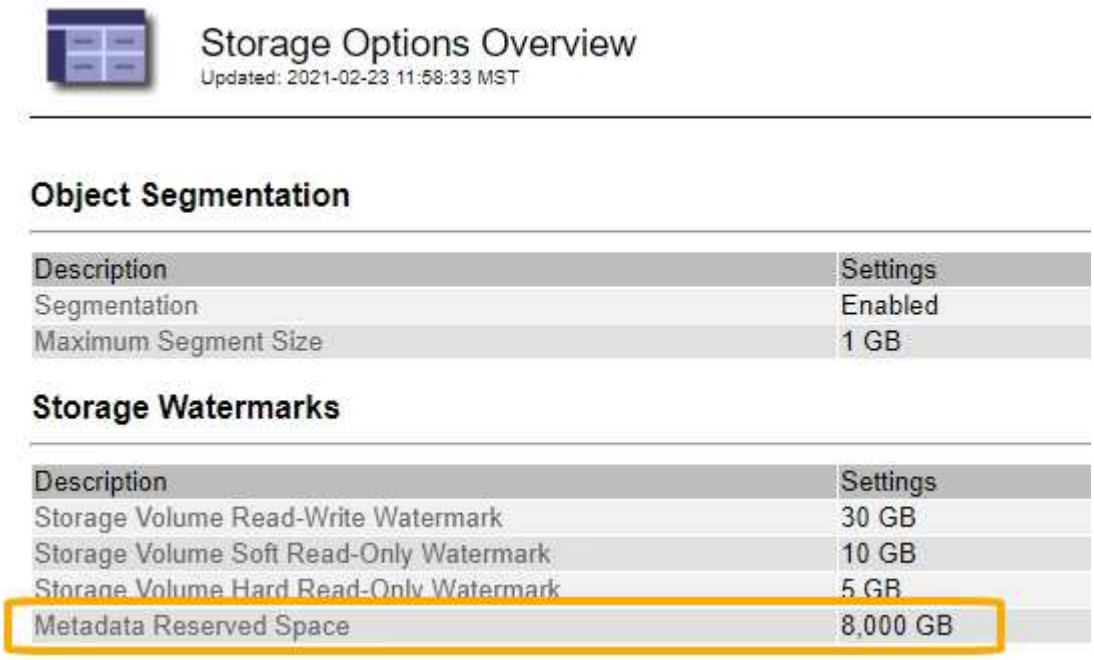
- StorageGRID の最初のインストール時に使用していたソフトウェアバージョン。
- 各ストレージノード上の RAM の容量。

| **StorageGRID** の初期インストールに使用するバージョン | ストレージノード上の **RAM** の容量 | **StorageGRID 11.5** のデフォルトの**Metadata Reserved Space**設定 |
|---|---|---|
| 11.5 | グリッド内の各ストレージノードで 128GB 以上 | 8 TB （ 8 、 000 GB ） |
| | グリッド内の任意のストレージノードで 128GB 未満 | 3TB （ 3 、 000GB ） |
| 11.1 ～ 11.4 | いずれかのサイトの各ストレージノードで 128GB 以上 | 4TB （ 4 、 000GB ） |

| **StorageGRID** の初期インストールに使用するバージョン | ストレージノード上の **RAM** の容量 | **StorageGRID 11.5** のデフォルトの**Metadata Reserved Space**設定 |
|---|---|---|
| | 各サイトのストレージノードで 128GB 未満 | 3TB （ 3 、 000GB ） |
| 11.0 以前 | 任意の金額 | 2TB （ 2 、 000 GB ） |

StorageGRID システムの Metadata Reserved Space 設定を表示するには、次の手順を実行します。

1. * Configuration **>** System Settings **>** Storage Options *を選択します。
2. Storage Watermarks テーブルで、 * Metadata Reserved Space * を探します。




スクリーンショットでは、「 * Metadata Reserved Space * 」の値が 8 、 000 GB （ 8 TB ）になっています。StorageGRID 11.5の新規インストールでは、各ストレージノードに128GB以上のRAMが搭載されます。

メタデータ用にリザーブされている実際のスペース

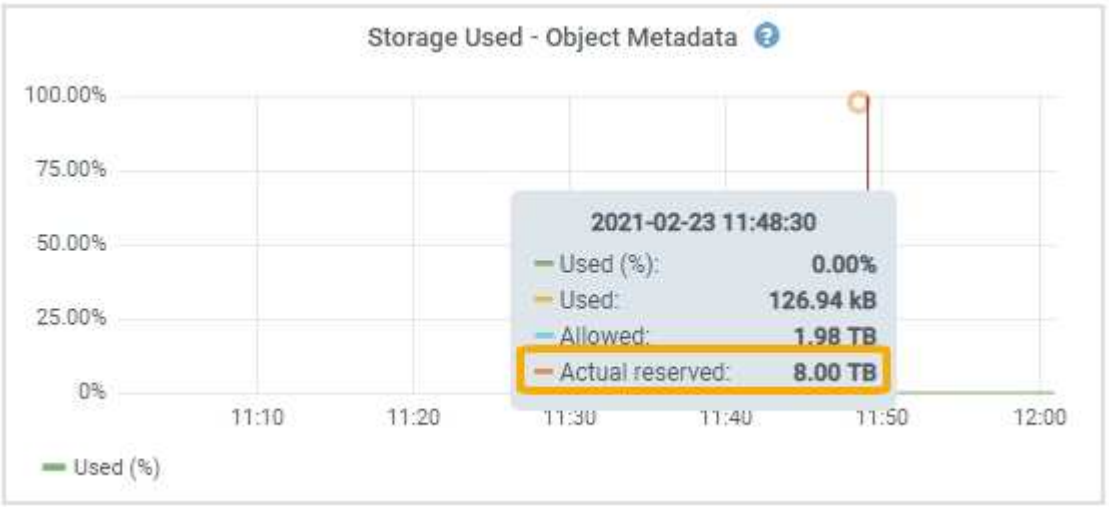
システム全体の Metadata Reserved Space 設定とは異なり、オブジェクトメタデータ用の実際のリザーブスペースは、ストレージノードごとに決定されます。ある特定のストレージノードについて、メタデータ用に実際にリザーブされるスペースは、ノードのボリューム 0 のサイズとシステム全体の * Metadata Reserved Space * 設定によって異なります。

| ノードのボリューム **0** のサイズ | メタデータ用にリザーブされている実際のスペース |
|---|---|
| 500GB 未満（非本番環境で使用） | ボリューム 0 の 10% |

| ノードのボリューム **0** のサイズ | メタデータ用にリザーブされている実際のスペース |
| --- | --- |
| 500GB 以上 | 次の値のうち小さい方：<br>• ボリューム 0<br>• Metadata Reserved Space の設定 |

特定のストレージノードでメタデータ用にリザーブされている実際のスペースを表示するには、次の手順を実行します

1. Grid Managerから* Nodes *>*_ Storage Node_*を選択します。
2. [ * ストレージ * ] タブを選択します。
3. 「使用済みストレージ — オブジェクトメタデータ」グラフにカーソルを合わせ、「実際に予約されている容量 * 」の値を探します。




スクリーンショットでは、実際の予約数 * の値は 8TB です。このスクリーンショットは、StorageGRID 11.5 を新規にインストールした大規模ストレージノードを示しています。システム全体の Metadata Reserved Space 設定がこのストレージノードのボリューム 0 よりも小さいため、このノードの実際のリザーブスペースは Metadata Reserved Space 設定と同じです。

actual reserved *値は次のPrometheus指標に対応します。

```
storagegrid_storage_utilization_metadata_reserved_bytes
```

実際にリザーブされているメタデータスペースの例

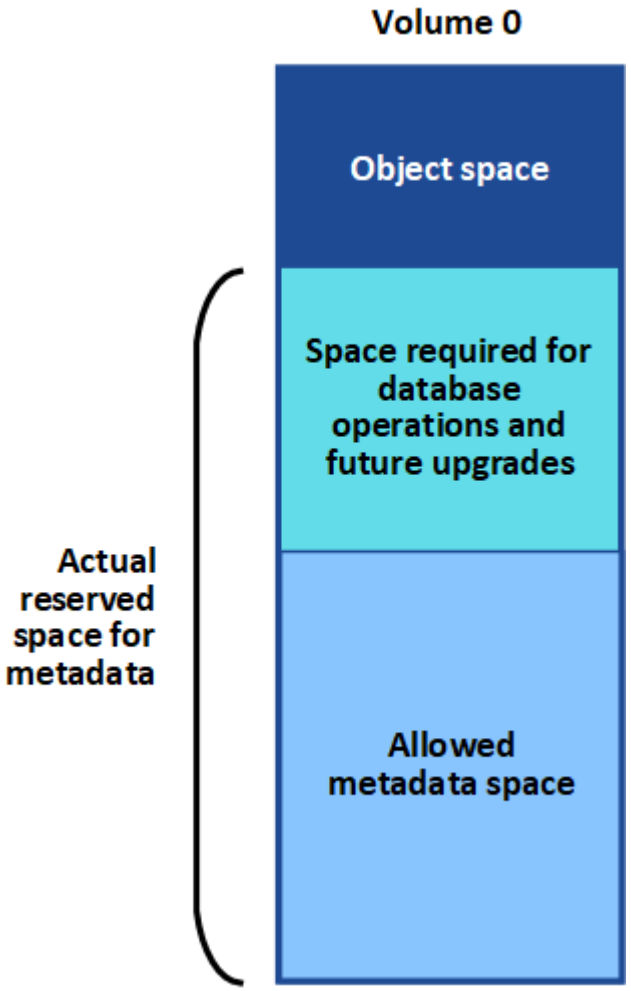
バージョン11.5を使用して新しいStorageGRID システムをインストールするとします。この例では、各ストレージノードの RAM が 128GB を超え、ストレージノード 1 （ SN1 ）のボリューム 0 が 6TB であるとします。次の値に基づきます。

- システム全体の * Metadata Reserved Space * が 8TB に設定されている（ストレージノードごとに128GBを超えるRAMが搭載されている場合、この値はStorageGRID 11.5の新規インストールでのデフォルト値です）。

- SN1 のメタデータ用にリザーブされている実際のスペースは 6TB です。（ボリューム 0 が * Metadata Reserved Space * 設定より小さいため、ボリューム全体がリザーブされます）。

許可されているメタデータスペースです

メタデータ用に実際に予約されている各ストレージノードは、オブジェクトメタデータに使用できるスペース（許容されるメタデータスペース _ ）と、重要なデータベース処理（コンパクションや修復など）や将来のハードウェアおよびソフトウェアのアップグレードに必要なスペースに分割されます。許可されるメタデータスペースは、オブジェクトの全体的な容量を決定します。



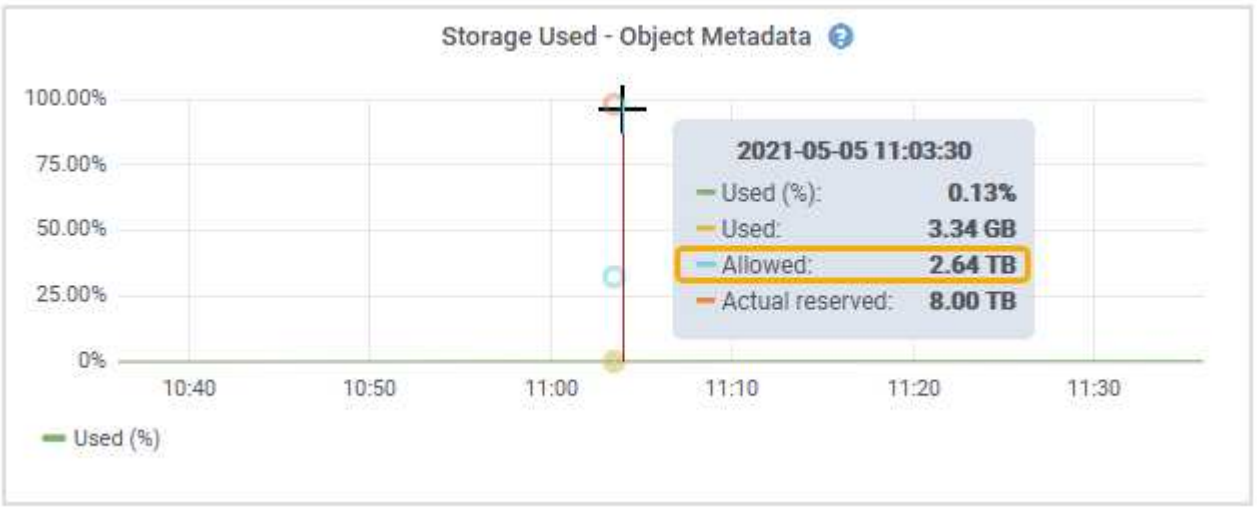

次の表は、 StorageGRID がストレージノードで許可されるメタデータスペースの値をどのように決定するかを示しています。

| メタデータ用にリザーブされている実際のスペース | 許可されているメタデータスペースです |
| --- | --- |
| 4TB以下 | メタデータ用にリザーブされている実際のスペースの 60% 。最大 1.98 TB |
| 4TBを超える | （メタデータ用に実際にリザーブされるスペース−1TB）×60%、最大2.64 TB |

StorageGRID システムで任意のストレージノードに2.64TBを超えるメタデータを格納（または格納する予定がある場合）がある場合、許可されるメタデータスペースが増加することがあります。各ストレージノードのRAMが128GBを超え、かつストレージボリューム0に空きスペースがある場合は、ネットアップの営業担当者にお問い合わせください。要件を確認し、可能であれば各ストレージノードで許可されているメタデータスペースを増やします。

ストレージノードで使用可能なメタデータスペースを表示するには、次の手順を実行します。

1. Grid Managerから* Node *>*_ Storage Node_*を選択します。
2. [ * ストレージ * ] タブを選択します。
3. 「使用済みストレージ — オブジェクトメタデータ」グラフにカーソルを合わせ、「使用可能な値 * 」を探します。




スクリーンショットでは、「許可」の値は 2.64TB です。これは、メタデータ用に実際にリザーブされているスペースが 4TB を超えるストレージノードの最大値です。

「 * Allowed * 」の値は、次の Prometheus 指標に対応します。

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

許可されるメタデータスペースの例

バージョン11.5を使用してStorageGRID システムをインストールするとします。この例では、各ストレージノードの RAM が 128GB を超え、ストレージノード 1 （ SN1 ）のボリューム 0 が 6TB であるとします。次の値に基づきます。

- システム全体の * Metadata Reserved Space * が 8TB に設定されている（各ストレージノードのRAMが128GBを超えている場合、StorageGRID 11.5のデフォルト値です）。
- SN1 のメタデータ用にリザーブされている実際のスペースは 6TB です。（ボリューム 0 が * Metadata Reserved Space * 設定より小さいため、ボリューム全体がリザーブされます）。
- SN1 でメタデータに使用できるスペースは 2.64 TB です。（実際のリザーブスペースの最大値です）。

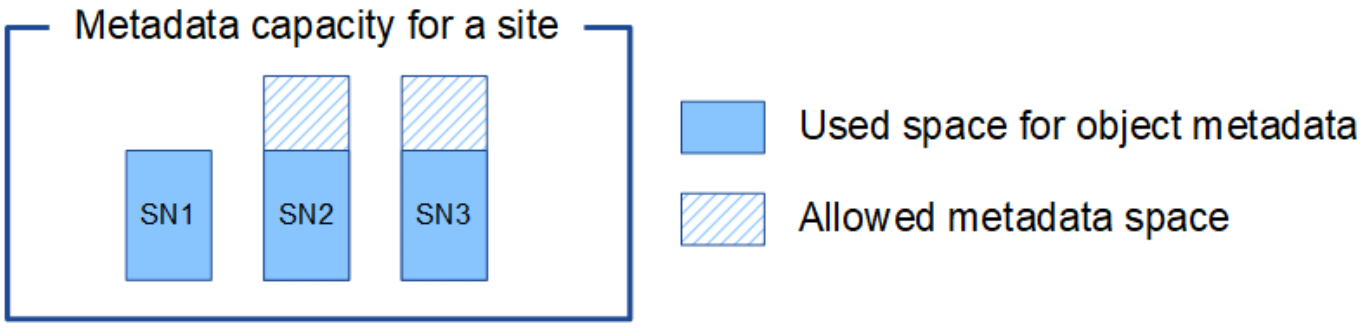
前述したように、 StorageGRID は各サイトのストレージノードにオブジェクトメタデータを均等に分散します。このため、サイトにサイズが異なるストレージノードがある場合、サイトで一番小さいノードがサイトのメタデータ容量を決定します。

次の例を考えてみましょう。

- サイズの異なる 3 つのストレージノードを含む単一サイトのグリッドがある。
- Metadata Reserved Space * の設定は 4TB です。
- ストレージノードには、リザーブされている実際のメタデータスペースと許可されているメタデータスペースについて、次の値があります。

| ストレージノード | ボリューム **0** のサイズ | リザーブされている実際のメタデータスペースです | 許可されているメタデータスペースです |
|---|---|---|---|
| SN1. | 2.2 TB | 2.2 TB | 1.32TB をサポートします |
| SN2. | 5 TB | 4 TB | 1.98 TB |
| SN3 | 6TB | 4 TB | 1.98 TB |

オブジェクトメタデータはサイトのストレージノード間で均等に分散されるため、この例の各ノードが格納できるメタデータは 1.32TB です。SN2 と SN3 で許可されるメタデータスペースのうち、 0.66TB を追加で使用することはできません。




同様に、 StorageGRID は各サイトで StorageGRID システムのすべてのオブジェクトメタデータを管理するため、 StorageGRID システム全体のメタデータ容量は最小サイトのオブジェクトメタデータ容量で決まります。

また、オブジェクトメタデータの容量はオブジェクトの最大数に制御されるため、一方のノードがメタデータの容量を超えると、実質的にグリッドがフルになります。

関連情報

- 各ストレージノードのオブジェクトメタデータ容量を監視する方法については、次の資料を参照してください。

  "トラブルシューティングを監視します"

- システムのオブジェクトメタデータ容量を増やすには、新しいストレージノードを追加する必要があります。

  "グリッドを展開します"

格納オブジェクトのグローバル設定

## グリッドオプションを使用すると、 StorageGRID システムに格納されているすべてのオブジェクトについて、格納オブジェクトの圧縮や格納オブジェクトの暗号化などの設定を行うことができます。設定を行うことができます。

- "格納オブジェクトの圧縮を設定しています"
- "格納オブジェクトの暗号化を設定する"
- "格納オブジェクトのハッシュの設定"

格納オブジェクトの圧縮を設定しています

## [ 格納オブジェクトの圧縮 ] グリッドオプションを使用すると、 StorageGRID に格納されているオブジェクトのサイズを縮小して、オブジェクトのストレージ消費量を抑えることができます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

デフォルトでは、 [ 格納オブジェクトの圧縮 ] グリッドオプションは無効になっています。このオプションを有効にすると、 StorageGRID は、ロスレス圧縮を使用して各オブジェクトを保存時に圧縮します。

> この設定を変更すると、新しい設定が適用されるまで約 1 分かかります。設定した値は、パフォーマンスと拡張用にキャッシュされます。

このオプションを有効にする前に、次の点に注意してください。

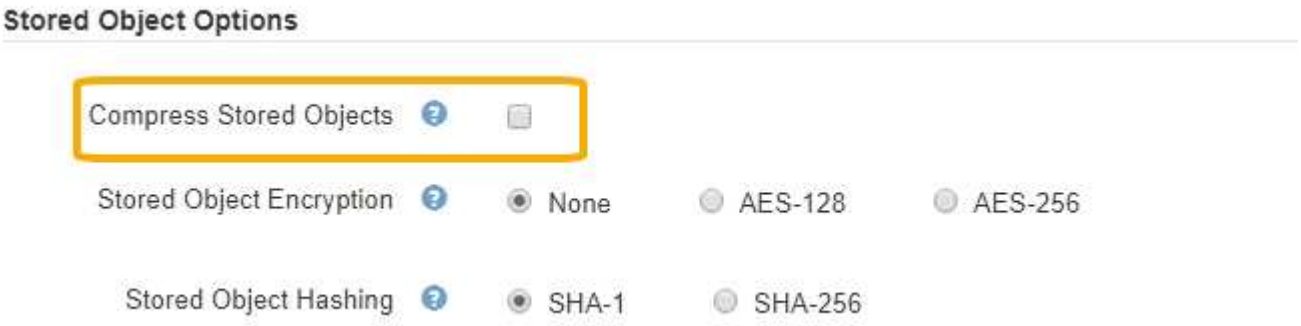
- 格納されるデータの圧縮率がわかっている場合を除き、圧縮を有効にしないでください。
- StorageGRID にオブジェクトを保存するアプリケーションは、オブジェクトを圧縮してから保存することがあります。クライアントアプリケーションがオブジェクトを StorageGRID に保存する前に圧縮している場合は、 [ 格納オブジェクトの圧縮 ] を有効にしてもオブジェクトのサイズはさらに縮小されません。
- NetApp FabricPool と StorageGRID を併用する場合は、圧縮を有効にしないでください。
- Compress Stored Objects グリッドオプションを有効にした場合は、 S3 および Swift クライアントアプリケーションでバイト範囲を指定した GET Object 処理を実行しないでください。StorageGRID は要求されたバイトにアクセスするためにオブジェクトを圧縮解除する必要があるため ' これらの “range read” 操作は非効率的です非常に大きなオブジェクトから小さい範囲のバイト数を要求する GET Object 処理は特に効率が悪く、たとえば、 50GB の圧縮オブジェクトから 10MB の範囲を読み取る処理は非効率的です。

  圧縮オブジェクトから範囲を読み取ると、クライアント要求がタイムアウトする可能性があります。

オブジェクトを圧縮する必要があり、クライアントアプリケーションが範囲読み取りを使用する必要がある場合は、アプリケーションの読み取りタイムアウトを増やしてください。

手順

1. 「環境設定*システム設定*グリッドオプション*」を選択します。
2. [ 格納オブジェクトのオプション ] セクションで、 [ 格納オブジェクトの圧縮 *] チェックボックスをオンにします。




3. [ 保存（ Save ） ] をクリックします。

格納オブジェクトの暗号化を設定する

## オブジェクトストアが侵害された場合に読み取り可能な形式でデータを読み出せないようにするには、格納オブジェクトを暗号化します。デフォルトでは、オブジェクトは暗号化されません。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

格納オブジェクトの暗号化を使用すると、 S3 または Swift 経由で取り込まれたすべてのオブジェクトデータを暗号化できます。この設定を有効にすると、新たに取り込まれたすべてのオブジェクトが暗号化されますが、既存の格納オブジェクトに対する変更はありません。暗号化を無効にすると、現在暗号化されているオブジェクトは暗号化されたままですが、新しく取り込まれたオブジェクトは暗号化されませ

この設定を変更すると、新しい設定が適用されるまで約 1 分かかります。設定した値は、パフォーマンスと拡張用にキャッシュされます。

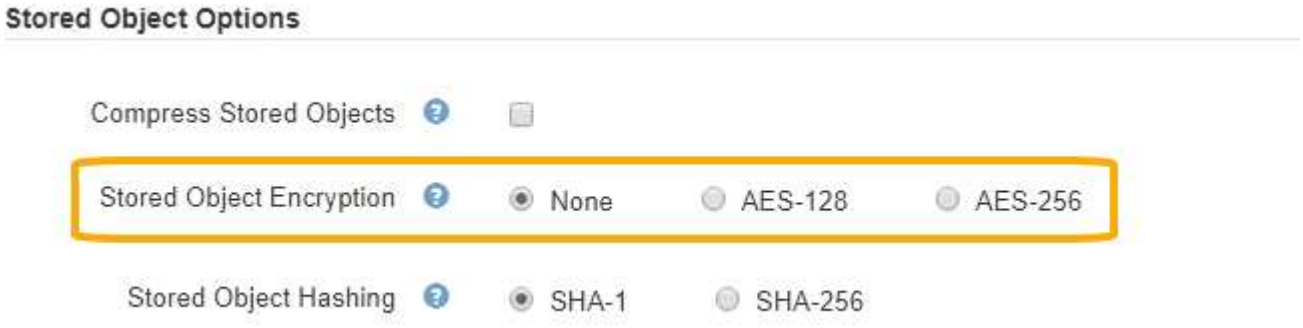
格納オブジェクトは、 AES - 128 または AES - 256 暗号化アルゴリズムを使用して暗号化できます。

格納オブジェクトの暗号化設定は、バケットレベルまたはオブジェクトレベルの暗号化で暗号化されていない S3 オブジェクトにのみ適用されます。

手順

1. 「環境設定*システム設定*グリッドオプション*」を選択します。

2. [ 格納オブジェクトのオプション ] セクションで、 [ 格納オブジェクトの暗号化 ] を [ * なし * （デフォルト） ] 、 [ * AES-128 * ] 、または [ * AES-256 * ] に変更します。




3. [ 保存（ Save ） ] をクリックします。

格納オブジェクトのハッシュの設定

# 格納オブジェクトのハッシュオプションは、オブジェクトの整合性の検証に使用するハッシュアルゴリズムを指定します。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

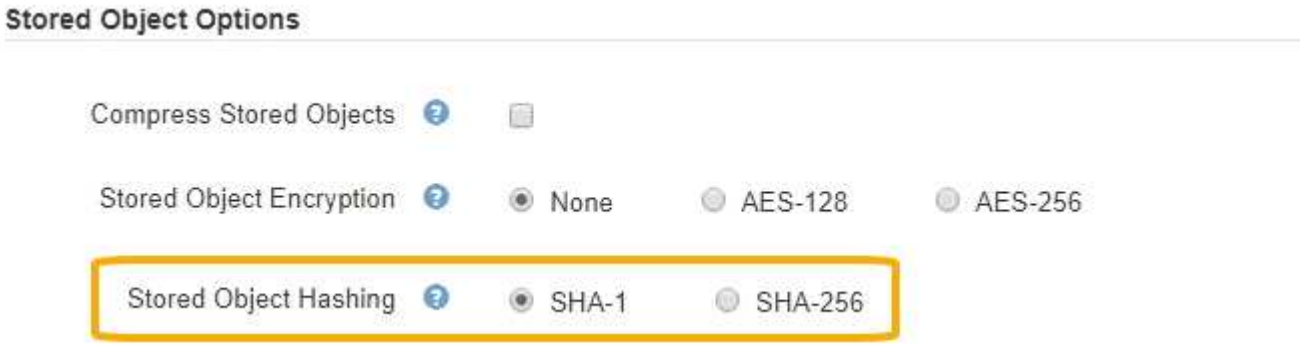
このタスクについて

デフォルトでは、オブジェクトデータはSHA-1アルゴリズムを使用してハッシュされます。SHA-256 アルゴリズムには追加の CPU リソースが必要で、整合性検証には一般的に推奨されていません。

この設定を変更すると、新しい設定が適用されるまで約 1 分かかります。設定した値は、パフォーマンスと拡張用にキャッシュされます。

手順

1. 「環境設定*システム設定*グリッドオプション*」を選択します。
2. 格納オブジェクトのオプションセクションで、格納オブジェクトのハッシュを * SHA-1 * （デフォルト）または * SHA-256 * に変更します。




3. [ 保存（ Save ） ] をクリックします。

# 各ストレージノードは、いくつかの設定とカウンタを使用します。アラーム（従来のシステム）をクリアするには、現在の設定の表示またはカウンタのリセットが必要になる場合があります。

ドキュメントで特に指示された場合を除き、ストレージノード設定を変更する前にテクニカルサポートにお問い合わせください。必要に応じて、イベントカウンタをリセットしてレガシーアラームをクリアできます。

ストレージノードの設定とカウンタにアクセスするには、次の手順を実行します。

1. Support **>** Tools **>** Grid Topology *を選択します。
2. 「 * *site* * > * _ *Storage Node** 」を選択します。
3. ストレージノードを展開し、サービスまたはコンポーネントを選択します。
4. [* 構成 *] タブを選択します。

次の表に、ストレージノードの構成設定をまとめます。

**LDR**

| 属性名（**Attribute Name**） | コード | 説明 |
| --- | --- | --- |
| HTTP State のことです | HSTE | S3 、 Swift 、およびその他の内部 StorageGRID トラフィックの HTTP プロトコルの現在の状態。<br>• Offline ：処理は許可されず、クライアントアプリケーションが LDR サービスへの HTTP セッションを開こうとするとエラーメッセージが表示されます。アクティブなセッションは正常終了します。<br>• Online ：処理は正常に続行されます |
| HTTP を自動起動します | HTAS | • このオプションを選択すると、再起動時のシステムの状態は * LDR * > * Storage * コンポーネントの状態によって異なります。再起動時に * ldr*>* Storage* コンポーネントが読み取り専用の場合、 HTTP インターフェイスも読み取り専用です。LDR * > * Storage * コンポーネントが Online の場合、 HTTP も Online になります。それ以外の場合は、 HTTP インターフェイスは Offline 状態のままです。<br>• 選択しない場合、 HTTP インターフェイスは明示的に有効にするまで Offline のままです。 |

**LDR>** データストア

| 属性名（ **Attribute Name** ） | コード | 説明 |
| --- | --- | --- |
| Lost Objects 数をリセットします | RCOR | このサービス上にある損失オブジェクト数のカウンタをリセットします。 |

**LDR > Storage** の順にクリックします

| 属性名（ **Attribute Name** ） | コード | 説明 |
| --- | --- | --- |
| ストレージの状態 — 望ましい | SSD | ストレージコンポーネントに求める状態をユーザが設定できます。LDR サービスはこの値を読み取り、指定されたステータスに一致するように試みます。この値は、再起動後も維持されます。<br><br>たとえば、この設定を使用すると、使用可能なストレージスペースが十分にある場合でも、ストレージを強制的に読み取り専用にすることができます。これはトラブルシューティングに役立ちます。<br><br>この属性には次のいずれかの値を指定できます。<br><br>• Offline ：目的の状態が Offline の場合、 LDR サービスは * LDR * > * Storage * コンポーネントをオフラインにします。<br>• Read-only ： LDR サービスはストレージを読み取り専用にし、新しいコンテンツの受け入れを停止します。開いているセッションが閉じられるまでの短時間の間、コンテンツが引き続きストレージノードに保存される可能性があります。<br>• Online ：通常のシステム運用中は、値を Online のままにします。ストレージの状態 — ストレージコンポーネントの現在の状態は ' 使用可能なオブジェクトストレージ容量などの LDR サービスの状態に基づいてサービスによって動的に設定されますスペースが少ない場合、コンポーネントは読み取り専用になります。 |
| ヘルスチェックタイムアウト | SHCT | ストレージボリュームが正常であるとみなされるために、ヘルスチェックテストが完了する必要のある秒数。この値は、サポートから指示があった場合にのみ変更してください。 |

**LDR > Verification** の順に選択します

| 属性名（**Attribute Name**） | コード | 説明 |
| --- | --- | --- |
| 欠落オブジェクト数のリセット | VCMI | OMIS （ Missing Objects Detected ）の数をリセットします。フォアグラウンド検証の完了後にのみ使用してください。欠落しているレプリケートオブジェクトデータは、 StorageGRID システムによって自動的にリストアされます。 |
| 確認します | FVOV | フォアグラウンド検証を実行するオブジェクトストアを選択します。 |
| 検証レート | VPRI （ VPRI ） | バックグラウンド検証を実行する際のレートを設定します。バックグラウンド検証レートの設定に関する情報を参照してください。 |
| 破損オブジェクト数のリセット | VCCR | バックグラウンド検証中に見つかった、破損しているレプリケートされたオブジェクトデータのカウンタをリセットします。このオプションを使用すると、 OCOR （ Corrupt Objects Detected ）アラームの状態をクリアできます。詳細については、 StorageGRID の監視とトラブルシューティングの手順を参照してください。 |
| 隔離オブジェクトを削除します | OQRT の場合 | 破損したオブジェクトを隔離ディレクトリから削除し、隔離されたオブジェクトの数をゼロにリセットして、 Quarantined Objects Detected （ OQRT ）アラームをクリアします。このオプションは、破損したオブジェクトが StorageGRID システムによって自動的にリストアされたあとに使用します。<br><br>Lost Objects アラームがトリガーされた場合、テクニカルサポートが隔離されたオブジェクトにアクセスを試みる可能性があります。隔離されたオブジェクトが、データのリカバリや、オブジェクトコピーの破損の原因となった根本的な問題のデバッグに役立つ場合があります。 |

**LDR>** イレイジャーコーディング

| 属性名（**Attribute Name**） | コード | 説明 |
| --- | --- | --- |
| 書き込みエラー数をリセットします | RSWF | イレイジャーコーディングオブジェクトデータのストレージノードへの書き込みエラーのカウンタをリセットします。 |
| 読み取りエラー数をリセットします | RSRF | イレイジャーコーディングオブジェクトデータのストレージノードからの読み取りエラーのカウンタをリセットします。 |

| 属性名（**Attribute Name**） | コード | 説明 |
| --- | --- | --- |
| Reset Deletes Failure Count （エラーカウントをリセット） | 自衛隊 | イレイジャーコーディングオブジェクトデータのストレージノードからの削除エラーのカウンタをリセットします。 |
| 破損コピーのリセット検出数 | RSCC | ストレージノード上にあるイレイジャーコーディングオブジェクトデータの破損コピー数のカウンタをリセットします。 |
| 破損フラグメントのリセット検出数 | RSCD | ストレージノード上にあるイレイジャーコーディングオブジェクトデータの破損フラグメントのカウンタをリセットします。 |
| 欠落フラグメントの検出数をリセットします | RSMD | ストレージノード上にあるイレイジャーコーディングオブジェクトデータの欠落フラグメントのカウンタをリセットします。フォアグラウンド検証の完了後にのみ使用してください。 |

**LDR > Replication** の順に選択します

| 属性名（**Attribute Name**） | コード | 説明 |
| --- | --- | --- |
| インバウンドレプリケーションエラー数をリセットします | RICR | インバウンドレプリケーションエラーのカウンタをリセットします。これを使用すると、 RIRF （ Inbound Replication - - Failed ）アラームをクリアできます。 |
| アウトバウンドレプリケーションのエラー数をリセットします | ROCR | アウトバウンドレプリケーションエラーのカウンタをリセットします。これを使用すると、 RORF （ Outbound Replications - - Failed ）アラームをクリアできます。 |
| インバウンドレプリケーションを無効にします | DSIR | メンテナンスまたは手順 のテストの一環としてインバウンドレプリケーションを無効にする場合に選択します。通常の運用中はオフのままにします。<br><br>インバウンドレプリケーションを無効にすると、オブジェクトをストレージノードから読み出して StorageGRID システム内の別の場所へコピーすることはできますが、他の場所からこのストレージノードへオブジェクトをコピーすることはできません。つまり、 LDR サービスは読み取り専用です。 |

| 属性名（**Attribute Name**） | コード | 説明 |
| --- | --- | --- |
| アウトバウンドレプリケーションを無効にします | DSOR | メンテナンスまたは手順 のテストの一環としてアウトバウンドレプリケーション（ HTTP 読み出し用のコンテンツ要求を含む）を無効にする場合に選択します。通常の運用中はオフのままにします。<br><br>アウトバウンドレプリケーションを無効にすると、このストレージノードにオブジェクトをコピーすることはできますが、ストレージノードからオブジェクトを読み出して StorageGRID システム内の別の場所へコピーすることはできません。LDR サービスは書き込み専用です。 |

関連情報

"トラブルシューティングを監視します"

容量が上限に達したストレージノードの管理

## ストレージノードの容量が上限に達した場合は、新しいストレージを追加して StorageGRID システムを拡張する必要があります。ストレージボリュームの追加、ストレージ拡張シェルフの追加、ストレージノードの追加の 3 つのオプションがあります。

ストレージボリュームを追加しています

各ストレージノードは最大数のストレージボリュームをサポートします。定義されている最大値はプラットフォームによって異なります。ストレージノードのストレージボリュームが最大数より少ない場合は、ボリュームを追加して容量を増やすことができます。StorageGRID システムの拡張手順を参照してください。

ストレージ拡張シェルフの追加

SG6060 などの一部の StorageGRID アプライアンスストレージノードで、追加のストレージシェルフがサポートされます。拡張機能が最大容量まで拡張されていない StorageGRID アプライアンスがある場合は、ストレージシェルフを追加して容量を増やすことができます。StorageGRID システムの拡張手順を参照してください。

ストレージノードの追加

ストレージノードを追加してストレージ容量を増やすことができます。ストレージを追加する場合は、現在アクティブな ILM ルールと容量の要件について慎重に検討する必要があります。StorageGRID システムの拡張手順を参照してください。

関連情報

"グリッドを展開します"

## 管理ノードの管理

## StorageGRID 環境の各サイトには管理ノードを1つ以上配置できます。

- "管理ノードとは"
- "複数の管理ノードを使用する"
- "プライマリ管理ノードの特定"
- "優先送信者を選択しています"
- "通知のステータスとキューの表示"
- "管理ノードによる確認済みアラームの表示（従来のシステム）"
- "監査クライアントアクセスを設定しています"

管理ノードとは

## 管理ノードは、システムの設定、監視、ロギングなどの管理サービスを提供します。各グリッドにはプライマリ管理ノードが 1 つ必要で、冗長性を確保するために任意の数の非プライマリ管理ノードを設定できます。

Grid Manager または Tenant Manager にサインインすると、管理ノードに接続されます。どの管理ノードにも接続が可能で、各管理ノードに表示される StorageGRID システムのビューもほぼ同じです。ただし、メンテナンス手順はプライマリ管理ノードを使用して実行する必要があります。

管理ノードを使用して、 S3 および Swift クライアントトラフィックの負荷を分散することもできます。

管理ノードは次のサービスをホストします。

- AMS サービス
- CMN サービス
- NMS サービス
- Prometheus サービス
- ロードバランササービスとハイアベイラビリティサービス（ S3 および Swift クライアントトラフィックをサポート）

管理ノードは、グリッド管理 API とテナント管理 API からの要求を処理する管理アプリケーションプログラムインターフェイス（ mgmt-api ）もサポートします。

### AMS サービスとは

Audit Management System （ AMS ）サービスは、システムアクティビティとイベントを追跡します。

### CMN サービスとは

Configuration Management Node （ CMN ）サービスは、すべてのサービスで必要とされる接続およびプロトコルの機能について、システム全体での設定を管理します。CMN サービスはグリッドタスクの実行および監視にも使用されます。StorageGRID 環境ごとに CMN サービスは 1 つだけです。CMN サービスをホストする管理ノードをプライマリ管理ノードと呼びます。

### NMS サービスとは

Network Management System （ NMS ）サービスは、 StorageGRID システムのブラウザベースのインターフェイスであるグリッドマネージャに表示される、監視、レポート、および設定のオプションを提供します。

### Prometheus サービスとは

Prometheus サービスは、すべてのノードのサービスから時系列の指標を収集します。

関連情報

"グリッド管理APIを使用する"

"テナントアカウントを使用する"

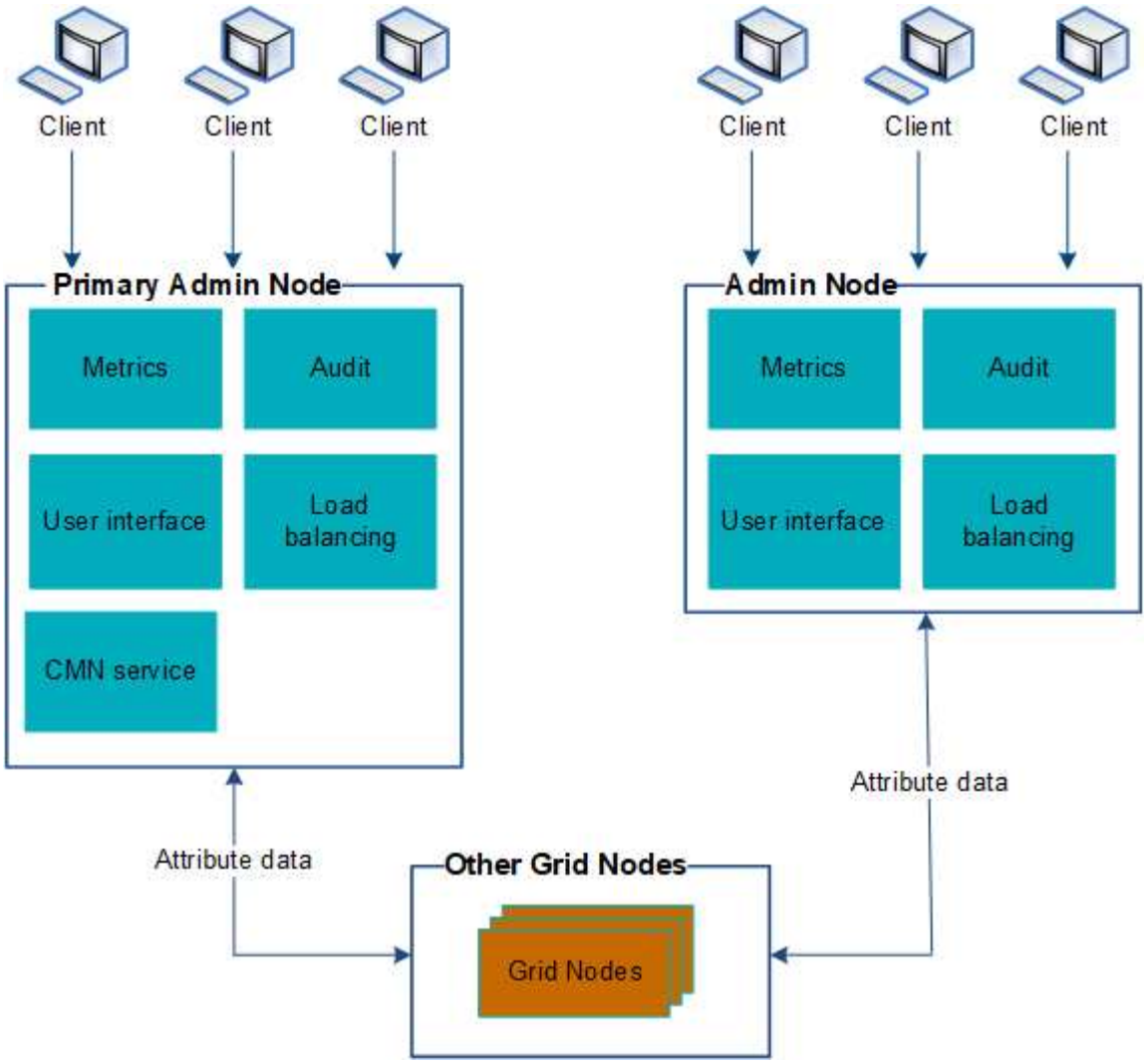
"負荷分散の管理"

"ハイアベイラビリティグループの管理"

### 複数の管理ノードを使用する

StorageGRID システムには複数の管理ノードを含めることができます。これにより、 1 つの管理ノードに障害が発生した場合でも、 StorageGRID システムを継続的に監視して設定することができます。

ある管理ノードが使用できなくなっても属性の処理は続行され、アラートとアラーム（従来のシステム）は引き続きトリガーされ、 E メール通知と AutoSupport メッセージは引き続き送信されます。ただし、通知と AutoSupport メッセージ以外のフェイルオーバー保護は提供されません。特に、ある管理ノードからのアラームの確認応答は他の管理ノードにはコピーされません。




管理ノードに障害が発生した場合、次の 2 つの方法で StorageGRID システムを引き続き表示および設定することができます。

- Web クライアントは使用可能な他の管理ノードに再接続できます。
- システム管理者が管理ノードのハイアベイラビリティグループを設定している場合、 Web クライアントは HA グループの仮想 IP アドレスを使用して引き続き Grid Manager または Tenant Manager にアクセスできます。

> HA グループを使用している場合、マスター管理ノードに障害が発生するとアクセスが中断します。ユーザは、 HA グループの仮想 IP アドレスがグループ内の別の管理ノードにフェイルオーバーしたあとで、再度サインインする必要があります。

一部のメンテナンスタスクはプライマリ管理ノードでしか実行できません。プライマリ管理ノードに障害が発生した場合、そのノードをリカバリするまでは、 StorageGRID システムは完全に機能している状態ではありません。

関連情報

"ハイアベイラビリティグループの管理"

プライマリ管理ノードの特定

# プライマリ管理ノードは CMN サービスをホストします。一部のメンテナンス手順は、プライマリ管理ノードでしか実行できません。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

手順

1. Support **>** Tools **>** Grid Topology *を選択します。
2. [**_site **管理ノード]を選択し、をクリックします ➕ をクリックしてトポロジツリーを展開し、この管理ノードでホストされているサービスを表示します。

   プライマリ管理ノードは CMN サービスをホストします。

3. この管理ノードが CMN サービスをホストしていない場合、他の管理ノードを確認します。

優先送信者を選択しています

# StorageGRID 環境に複数の管理ノードが含まれている場合は、通知の優先送信者となる管理ノードを選択できます。デフォルトでは、プライマリ管理ノードが選択されますが、任意の管理ノードを優先送信者にすることができます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

「* Configuration * System Settings * Display Options *」ページに、現在優先送信者として選択されている管理ノードが表示されます。デフォルトでは、プライマリ管理ノードが選択されます。

通常のシステム運用では、優先送信者のみが次の通知を送信します。

- AutoSupport メッセージ
- SNMP 通知
- アラート E メール
- アラーム E メール（レガシーシステム）

ただし、他のすべての管理ノード（スタンバイ送信者）が優先送信者を監視します。問題が検出された場合は、スタンバイ送信者もこれらの通知を送信できます。

次の場合、優先送信者とスタンバイ送信者の両方が通知を送信することがあります。

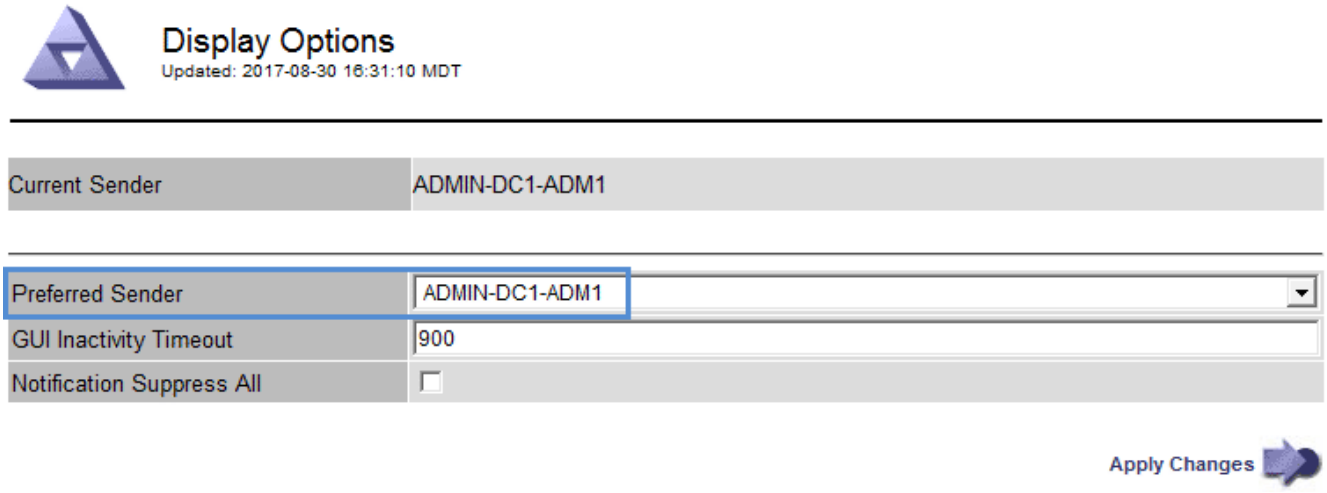
- 管理ノードどうしが「孤立した」状態になると、優先送信者とスタンバイ送信者の両方が通知の送信を試み、通知が重複して届く可能性があります。
- スタンバイ送信者が優先送信者に関する問題を検出して通知の送信を開始したあとで、優先送信者が通知

を再び送信できるようになることがあります。この場合、重複する通知が送信される可能性があります。優先送信者に関するエラーが検出されなくなると、スタンバイ送信者は通知の送信を停止します。

アラーム通知と AutoSupport メッセージをテストするときは、すべての管理ノードからテスト E メールが送信されます。アラート通知をテストするときは、すべての管理ノードにサインインして接続を確認する必要があります。

手順

1. * Configuration > System Settings > Display Options *を選択します。
2. [ 表示オプション ] メニューから、 [ * オプション * ] を選択します。
3. 優先送信者として設定する管理ノードをドロップダウンリストから選択します。



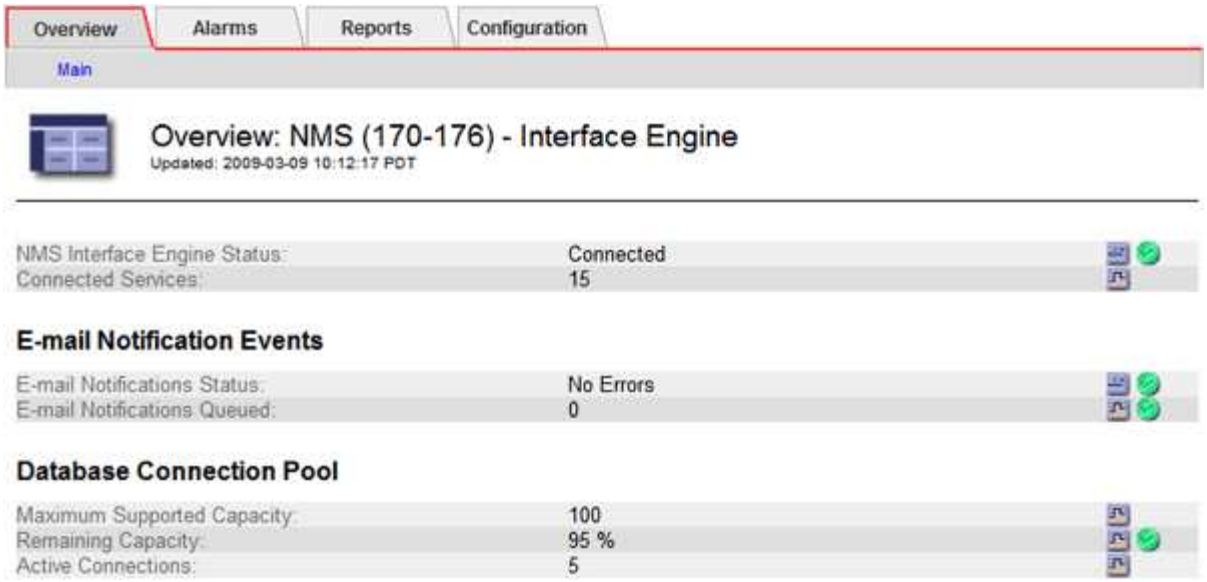

4. [ 変更の適用 *] をクリックします。

   管理ノードが通知の優先送信者として設定されます。

通知のステータスとキューの表示

管理ノードのNMSサービスは、メールサーバに通知を送信します。NMS サービスの現在のステータスとその通知キューのサイズは、 Interface Engine ページで確認できます。

Interface Engineページにアクセスするには、* Support > Tools > Grid Topology を選択します。最後に、 ***site _ * > * _Admin Node*** > * NMS * > * Interface Engine * を選択します。

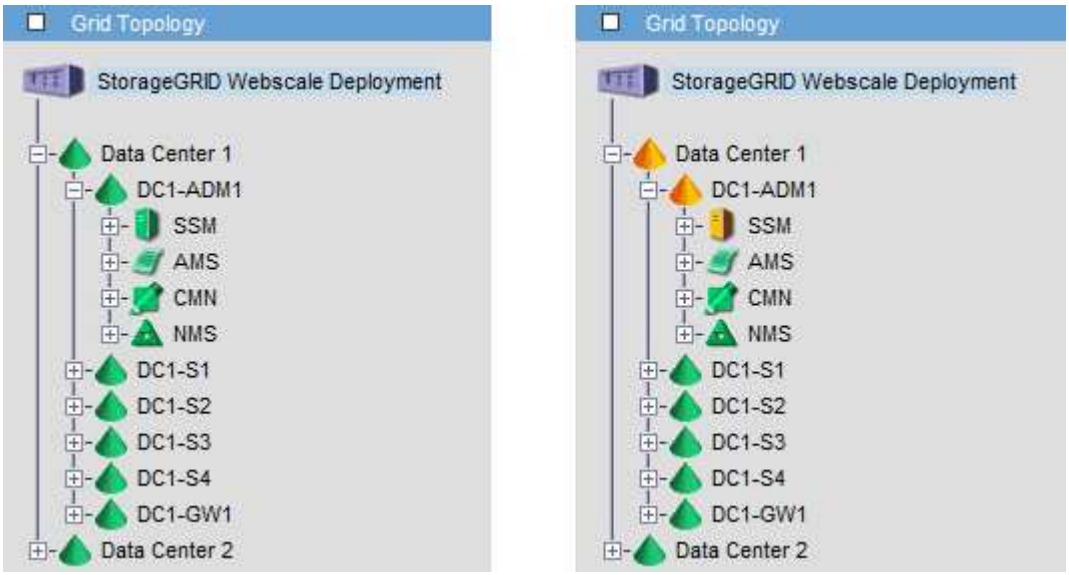



通知は E メール通知キューを通じて処理され、トリガーされた順にメールサーバに送信されます。通知の送信時に問題（ネットワーク接続エラーなど）が発生してメールサーバが使用できなくなった場合は、メールサーバへの再送信が 60 秒間試行されます。60 秒経ってもメールサーバに送信されなかった通知は通知キューから破棄され、キュー内の次の通知の送信が試行されます。通知が送信されずに通知キューから破棄されることがあるため、通知が送信されずにアラームがトリガーされる可能性があります。通知が送信されずにキューから破棄された場合は、 MINS （ E メール通知ステータス） Minor アラームがトリガーされます。

管理ノードによる確認済みアラームの表示（従来のシステム）

ある管理ノードのアラームを確認しても、確認済みのアラームは他の管理ノードにはコピーされません。確認応答は他の管理ノードにはコピーされないため、グリッドトポロジツリーでは各管理ノードで同じように表示されない場合があります。

この違いは、 Web クライアントに接続する場合に役立ちます。Web クライアントでは、管理者のニーズに基づいて、 StorageGRID システムをさまざまな方法で表示できます。




通知は、確認応答が発生した管理ノードから送信されます。

監査クライアントアクセスを設定しています

管理ノードは、 Audit Management System （ AMS ）サービスを介して、監査対象のすべてのシステムイベントを、監査共有からアクセス可能なログファイルに記録します。監査共有はインストール時に各管理ノードに追加されます。監査ログへのアクセスを簡単にするためには、 CIFS と NFS の両方についてクライアントから監査共有へのアクセスを設定します。

StorageGRID システムは、確認応答を使用して、ログファイルに書き込まれる前に監査メッセージが失われないようにします。AMS サービスまたは中間の監査リレーサービスがメッセージの制御を確認するまで、メッセージはサービスのキューに残ります。

詳細については、監査メッセージを確認する手順を参照してください。

CIFS または NFS を使用するオプションがある場合は、 nfs を選択します。

CIFS / Samba を使用した監査エクスポートは廃止されており、 StorageGRID の今後のリリースで削除される予定です。

関連情報

"管理ノードとは"

"監査ログを確認します"

"ソフトウェアをアップグレードする"

**CIFS**の監査クライアントを設定しています

監査クライアントの設定に使用する手順 は、認証方式 (Windows ワークグループまたは Windows Active Directory) によって異なります。追加した監査共有は、読み取り専用の共有として自動的に有効になります。

CIFS / Samba を使用した監査エクスポートは廃止されており、 StorageGRID の今後のリリースで削除される予定です。

関連情報

"ソフトウェアをアップグレードする"

ワークグループの監査クライアントの設定

この手順 は、監査メッセージの取得先である StorageGRID 環境内の管理ノードごとに実行します。

必要なもの

- を用意しておく必要があります `Passwords.txt` root / adminアカウントのパスワードを含むファイル（SAIDパッケージ内にあります）。
- を用意しておく必要があります `Configuration.txt` ファイル（SAIDパッケージ内にあります）。

このタスクについて

CIFS / Samba を使用した監査エクスポートは廃止されており、 StorageGRID の今後のリリースで削除される予定です。

手順

1. プライマリ管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

      rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

2. すべてのサービスの状態が「Running」または「Verified」であることを確認します。 `storagegrid-status`

   すべてのサービスが「 Running 」または「 Verified 」でない場合は、問題を解決してから続行してください。

3. コマンドラインに戻り、 * Ctrl * + * C * を押します。
4. CIFS設定ユーティリティを起動します。 `config_cifs.rb`

```
------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
------------------------------------------------------------------
```

5. Windows ワークグループの認証を設定します。

   認証がすでに設定されている場合は、確認メッセージが表示されます。認証がすでに設定されている場合は、次の手順に進みます。

   a. 入力するコマンド `set-authentication`
   b. WindowsワークグループまたはActive Directoryのインストールを求めるプロンプトが表示されたら、次のように入力します。 `workgroup`
   c. プロンプトが表示されたら、ワークグループの名前を入力します。 *`workgroup_name`*
   d. プロンプトが表示されたら、わかりやすいNetBIOS名を設定します。 *`netbios_name`*

または

Enter * キーを押して管理ノードのホスト名を NetBIOS 名として使用します。

スクリプトによって Samba サーバが再起動され、変更が適用されます。この処理にかかる時間は 1 分未満です。認証を設定したら、監査クライアントを追加します。

a. プロンプトが表示されたら、 * Enter * を押します。

CIFS 設定ユーティリティが表示されます。

6. 監査クライアントを追加します。

a. 入力するコマンド `add-audit-share`

共有は読み取り専用として自動的に追加されます。

b. プロンプトが表示されたら、ユーザまたはグループを追加します。 *user*

c. プロンプトが表示されたら、監査ユーザ名を入力します。 *audit_user_name*

d. プロンプトが表示されたら、監査ユーザのパスワードを入力します。 *password*

e. プロンプトが表示されたら、確認のためにもう一度同じパスワードを入力します。 *password*

f. プロンプトが表示されたら、 * Enter * を押します。

CIFS 設定ユーティリティが表示されます。

ディレクトリを入力する必要はありません。監査ディレクトリ名は事前に定義されています。

7. 複数のユーザまたはグループが監査共有へのアクセスを許可されている場合は、ユーザを追加します。

a. 入力するコマンド `add-user-to-share`

有効な共有に番号が振られ、リストに表示されます。

b. プロンプトが表示されたら、監査エクスポート共有の番号を入力します。 *share_number*

c. プロンプトが表示されたら、ユーザまたはグループを追加します。 `user`

または `group`

d. プロンプトが表示されたら、監査ユーザまたはグループの名前を入力します。 *audit_user or audit_group*

e. プロンプトが表示されたら、 * Enter * を押します。

CIFS 設定ユーティリティが表示されます。

f. 監査共有に追加するユーザまたはグループごとに、上記の手順を繰り返します。

8. 必要に応じて、設定を確認します。 `validate-config`

サービスがチェックされて表示されます。次のメッセージは無視してかまいません。

```
Can't find include file /etc/samba/includes/cifs-interfaces.inc
Can't find include file /etc/samba/includes/cifs-filesystem.inc
Can't find include file /etc/samba/includes/cifs-custom-config.inc
Can't find include file /etc/samba/includes/cifs-shares.inc
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit
(16384)
```

a. プロンプトが表示されたら、 * Enter * を押します。

監査クライアント設定が表示されます。

b. プロンプトが表示されたら、 * Enter * を押します。

CIFS 設定ユーティリティが表示されます。

9. CIFS設定ユーティリティを閉じます。 `exit`
10. Sambaサービスを開始します。 `service smbd start`
11. StorageGRID 環境が単一サイトの場合は、次の手順に進みます。

または

StorageGRID 環境で他のサイトに管理ノードが含まれている場合は、必要に応じてこれらの監査共有を有効にします。

a. サイトの管理ノードにリモートからログインします。
   i. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
   ii. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   iii. 次のコマンドを入力してrootに切り替えます。 `su -`
   iv. に記載されているパスワードを入力します `Passwords.txt` ファイル。
b. 同じ手順を繰り返して、追加の管理ノードごとに監査共有を設定します。
c. リモート管理ノードへのリモートのSecure Shellログインを終了します。 `exit`
12. コマンドシェルからログアウトします。 `exit`

関連情報

"ソフトウェアをアップグレードする"

**Active Directory**の監査クライアントを設定しています

## この手順 は、監査メッセージの取得先である StorageGRID 環境内の管理ノードごとに実行します。

必要なもの

- を用意しておく必要があります `Passwords.txt` root / adminアカウントのパスワードを含むファイル（SAIDパッケージ内にあります）。
- CIFS Active Directoryのユーザ名とパスワードが必要です。
- を用意しておく必要があります `Configuration.txt` ファイル（SAIDパッケージ内にあります）。

CIFS / Samba を使用した監査エクスポートは廃止されており、 StorageGRID の今後のリリースで削除される予定です。

手順

1. プライマリ管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

   rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。
2. すべてのサービスの状態が「Running」または「Verified」であることを確認します。 `storagegrid-status`

   すべてのサービスが「 Running 」または「 Verified 」でない場合は、問題を解決してから続行してください。
3. コマンドラインに戻り、 * Ctrl * + * C * を押します。
4. CIFS設定ユーティリティを起動します。 `config_cifs.rb`

```
------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
------------------------------------------------------------------
```

5. Active Directoryの認証を設定します。 `set-authentication`

   ほとんどの環境では、監査クライアントを追加する前に認証を設定する必要があります。認証がすでに設定されている場合は、確認メッセージが表示されます。認証がすでに設定されている場合は、次の手順に進みます。

a. ワークグループまたはActive Directoryのインストールを求めるプロンプトが表示されたら、次のよう `ad`

b. プロンプトが表示されたら、 AD ドメインの名前（短いドメイン名）を入力します。

c. プロンプトが表示されたら、ドメインコントローラの IP アドレスまたは DNS ホスト名を入力します。

d. プロンプトが表示されたら、完全なドメインレルム名を入力します。

大文字を使用します。

e. winbind サポートの有効化を求めるプロンプトが表示されたら、「 * y * 」と入力します。

Winbind は AD サーバのユーザおよびグループの情報を解決するために使用されます。

f. プロンプトが表示されたら、 NetBIOS 名を入力します。

g. プロンプトが表示されたら、 * Enter * を押します。

CIFS 設定ユーティリティが表示されます。

6. ドメインに参加します。

a. CIFS設定ユーティリティが起動していない場合は、起動します。 `config_cifs.rb`

b. ドメインに参加します。 `join-domain`

c. 管理ノードが現在ドメインの有効なメンバーかどうかテストするよう求めるプロンプトが表示されます。この管理ノードがドメインに参加していない場合は、次のように入力します。 `no`

d. プロンプトが表示されたら、管理者のユーザ名を指定します。 *`administrator_username`*

ここで、 *`administrator_username`* は、StorageGRID ユーザ名ではなく、CIFS Active Directoryのユーザ名です。

e. プロンプトが表示されたら、管理者のパスワードを入力します。 *`administrator_password`*

はい *`administrator_password`* は、StorageGRID パスワードではなく、CIFS Active Directoryのユーザ名です。

f. プロンプトが表示されたら、 * Enter * を押します。

CIFS 設定ユーティリティが表示されます。

7. ドメインに参加したことを確認します。

a. ドメインに参加します。 `join-domain`

b. サーバが現在ドメインの有効なメンバーかどうかをテストするよう求められたら、次のように入力します。 `y`

「 Join is OK 」というメッセージが表示される場合は、ドメインに正常に参加しています。このメッセージが表示されない場合は、もう一度認証を設定してドメインに参加してください。

c. プロンプトが表示されたら、 * Enter * を押します。

CIFS 設定ユーティリティが表示されます。

8. 監査クライアントを追加します。 `add-audit-share`
   a. ユーザまたはグループの追加を求めるプロンプトが表示されたら、次のように入力します。 `user`
   b. 監査ユーザ名の入力を求めるプロンプトが表示されたら、監査ユーザ名を入力します。
   c. プロンプトが表示されたら、 * Enter * を押します。

      CIFS 設定ユーティリティが表示されます。

9. 複数のユーザまたはグループが監査共有へのアクセスを許可されている場合は、ユーザを追加します。 `add-user-to-share`

   有効な共有に番号が振られ、リストに表示されます。

   a. 監査エクスポート共有の数を入力します。
   b. ユーザまたはグループの追加を求めるプロンプトが表示されたら、次のように入力します。 `group`

      監査グループ名の入力を求められます。

   c. 監査グループ名を求めるプロンプトが表示されたら、監査ユーザグループの名前を入力します。
   d. プロンプトが表示されたら、 * Enter * を押します。

      CIFS 設定ユーティリティが表示されます。

   e. 監査共有に追加するユーザまたはグループごとに、この手順を繰り返します。

10. 必要に応じて、設定を確認します。 `validate-config`

    サービスがチェックされて表示されます。次のメッセージは無視してかまいません。

    - インクルードファイルが見つかりません `/etc/samba/includes/cifs-interfaces.inc`
    - インクルードファイルが見つかりません `/etc/samba/includes/cifs-filesystem.inc`
    - インクルードファイルが見つかりません `/etc/samba/includes/cifs-interfaces.inc`
    - インクルードファイルが見つかりません `/etc/samba/includes/cifs-custom-config.inc`
    - インクルードファイルが見つかりません `/etc/samba/includes/cifs-shares.inc`
    - RLIMIT_max ： rlimit_max （ 1024 ）を Windows の最小制限（ 16384 ）に増やす

      「 security=ads 」と「 password server 」パラメータは同時に指定しないでください（ Samba は、接続する正しい DC を自動的に検出します）。

      i. プロンプトが表示されたら、 * Enter * を押して監査クライアントの設定を表示します。
      ii. プロンプトが表示されたら、 * Enter * を押します。

      CIFS 設定ユーティリティが表示されます。

11. CIFS設定ユーティリティを閉じます。 `exit`

12. StorageGRID 環境が単一サイトの場合は、次の手順に進みます。

    または

    StorageGRID 環境で他のサイトに管理ノードが含まれている場合は、必要に応じてこれらの監査共有を有効にします。

    a. サイトの管理ノードにリモートからログインします。
        i. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
        ii. に記載されているパスワードを入力します `Passwords.txt` ファイル。
        iii. 次のコマンドを入力してrootに切り替えます。 `su -`
        iv. に記載されているパスワードを入力します `Passwords.txt` ファイル。
    b. 同じ手順を繰り返して、管理ノードごとに監査共有を設定します。
    c. 管理ノードへのリモートのSecure Shellログインを終了します。 `exit`

13. コマンドシェルからログアウトします。 `exit`

関連情報

"ソフトウェアをアップグレードする"

**CIFS**監査共有へのユーザまたはグループの追加

## AD 認証と統合されている CIFS 監査共有にユーザまたはグループを追加できます。

必要なもの

- を用意しておく必要があります `Passwords.txt` root / adminアカウントのパスワードを含むファイル（SAIDパッケージ内にあります）。
- を用意しておく必要があります `Configuration.txt` ファイル（SAIDパッケージ内にあります）。

このタスクについて

次の手順 は、 AD 認証と統合されている監査共有用です。

> CIFS / Samba を使用した監査エクスポートは廃止されており、 StorageGRID の今後のリリースで削除される予定です。

手順

1. プライマリ管理ノードにログインします。
    a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`
    b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
    c. 次のコマンドを入力してrootに切り替えます。 `su -`
    d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

    rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

2. すべてのサービスの状態が「 Running 」または「 Verified 」であることを確認します。入力するコマンド `storagegrid-status`

   すべてのサービスが「 Running 」または「 Verified 」でない場合は、問題を解決してから続行してください。

3. コマンドラインに戻り、 * Ctrl * + * C * を押します。
4. CIFS設定ユーティリティを起動します。 `config_cifs.rb`

```
------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
------------------------------------------------------------------
```

5. ユーザまたはグループの追加を開始します。 `add-user-to-share`

   設定済みの監査共有に番号が振られ、リストに表示されます。

6. プロンプトが表示されたら、監査共有（audit-export）の番号を入力します。 *`audit_share_number`*

   この監査共有へのアクセスをユーザまたはグループに許可するかどうかの確認を求められます。

7. プロンプトが表示されたら、ユーザまたはグループを追加します。 `user` または `group`
8. プロンプトが表示されたら、この AD 監査共有のユーザまたはグループ名を入力します。

   サーバのオペレーティングシステムと CIFS サービスの両方で、ユーザまたはグループが読み取り専用として監査共有に追加されます。Samba 設定がリロードされ、ユーザまたはグループが監査クライアント共有にアクセスできるようになります。

9. プロンプトが表示されたら、 * Enter * を押します。

   CIFS 設定ユーティリティが表示されます。

10. 監査共有に追加するユーザまたはグループごとに、上記の手順を繰り返します。
11. 必要に応じて、設定を確認します。 `validate-config`

    サービスがチェックされて表示されます。次のメッセージは無視してかまいません。

    - include ファイル /etc/samba/include/cifs-interfaces.in が見つかりません
    - include ファイル /etc/samba/include/cifs-filesystem.in が見つかりません

- include ファイル /etc/samba/include/cifs-custom-config.in が見つかりません
- include ファイル /etc/samba/include/cifs-shares.in が見つかりません
  i. プロンプトが表示されたら、 * Enter * を押して監査クライアントの設定を表示します。
  ii. プロンプトが表示されたら、 * Enter * を押します。

12. CIFS設定ユーティリティを閉じます。 `exit`
13. 次の状況に応じて、追加の監査共有を有効にする必要があるかどうかを判断します。
    - StorageGRID 環境が単一サイトの場合は、次の手順に進みます。
    - StorageGRID 環境で他のサイトに管理ノードが含まれている場合は、必要に応じてこれらの監査共有を有効にします。
      i. サイトの管理ノードにリモートからログインします。
         A. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
         B. に記載されているパスワードを入力します `Passwords.txt` ファイル。
         C. 次のコマンドを入力してrootに切り替えます。 `su -`
         D. に記載されているパスワードを入力します `Passwords.txt` ファイル。
      ii. 同じ手順を繰り返して、管理ノードごとに監査共有を設定します。
      iii. リモート管理ノードへのリモートのSecure Shellログインを終了します。 `exit`
14. コマンドシェルからログアウトします。 `exit`

**CIFS**監査共有からのユーザまたはグループの削除

## 監査共有にアクセス可能な最後のユーザまたはグループを削除することはできません。

必要なもの

- を用意しておく必要があります `Passwords.txt` rootアカウントのパスワードを含むファイル（SAIDパッケージ内にあります）。
- を用意しておく必要があります `Configuration.txt` ファイル（SAIDパッケージ内にあります）。

このタスクについて

CIFS / Samba を使用した監査エクスポートは廃止されており、 StorageGRID の今後のリリースで削除される予定です。

手順

1. プライマリ管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

   rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

2. CIFS設定ユーティリティを起動します。 `config_cifs.rb`

```
------------------------------------------------------------------
| Shares                 | Authentication         | Config          |
------------------------------------------------------------------
| add-audit-share        | set-authentication     | validate-config |
| enable-disable-share   | set-netbios-name       | help            |
| add-user-to-share      | join-domain            | exit            |
| remove-user-from-share | add-password-server    |                 |
| modify-group           | remove-password-server |                 |
|                        | add-wins-server        |                 |
|                        | remove-wins-server     |                 |
------------------------------------------------------------------
```

3. ユーザまたはグループの削除を開始します。 `remove-user-from-share`

   管理ノードで使用可能な監査共有に番号が振られ、リストに表示されます。監査共有には「 audit-export 」というラベルが付けられています。

4. 監査共有の番号を入力します。 *`audit_share_number`*
5. ユーザまたはグループの削除を求めるプロンプトが表示されたら、次のように入力します `user` または `group`

   監査共有のユーザまたはグループに番号が振られ、リストに表示されます。

6. 削除するユーザまたはグループに対応する番号を入力します。 *`number`*

   監査共有が更新され、ユーザまたはグループは監査共有にアクセスできなくなります。例：

```
Enabled shares
 1. audit-export
Select the share to change: 1
Remove user or group? [User/group]: User
Valid users for this share
1. audituser
2. newaudituser
Select the user to remove: 1

Removed user "audituser" from share "audit-export".

Press return to continue.
```

7. CIFS設定ユーティリティを閉じます。 `exit`
8. StorageGRID 環境で他のサイトに管理ノードが含まれている場合は、必要に応じて各サイトで監査共有を無効にします。

9. 設定が完了したら、各コマンドシェルからログアウトします。 `exit`

関連情報

"ソフトウェアをアップグレードする"

**CIFS**監査共有のユーザ名またはグループ名を変更する

## CIFS 監査共有のユーザまたはグループの名前を変更するには、新しいユーザまたはグループを追加してから古いユーザまたはグループを削除します。

このタスクについて

CIFS / Samba を使用した監査エクスポートは廃止されており、 StorageGRID の今後のリリースで削除される予定です。

手順

1. 名前を更新した新しいユーザまたはグループを監査共有に追加します。
2. 古いユーザ名またはグループ名を削除します。

関連情報

"ソフトウェアをアップグレードする"

"CIFS監査共有へのユーザまたはグループの追加"

"CIFS監査共有からのユーザまたはグループの削除"

**CIFS**監査の統合の検証

## 監査共有は読み取り専用です。ログファイルはコンピュータアプリケーションによって読み取られることを目的としていますが、ファイルを開けるかどうかは検証の対象に含まれていません。Windows のエクスプローラウィンドウに監査ログファイルが表示されれば、検証は十分とみなされます。接続を検証したら、すべてのウィンドウを閉じます。

**NFS**の監査クライアントの設定

## 監査共有は読み取り専用の共有として自動的に有効になります。

必要なもの

- を用意しておく必要があります `Passwords.txt` rootまたはadminのパスワードを含むファイル（SAIDパッケージ内にあります）。
- を用意しておく必要があります `Configuration.txt` ファイル（SAIDパッケージ内にあります）。
- 監査クライアントがNFSバージョン3（NFSv3）を使用している必要があります。

このタスクについて

この手順 は、監査メッセージの取得先である StorageGRID 環境内の管理ノードごとに実行します。

手順

1. プライマリ管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

      rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。
2. すべてのサービスの状態が「 Running 」または「 Verified 」であることを確認します。入力するコマンド `storagegrid-status`

   「 Running 」または「 Verified 」でないサービスがある場合は、問題を解決してから続行してください。
3. コマンドラインに戻ります。Ctrl キーを押しながら * C キーを押します。
4. NFS 設定ユーティリティを起動します。入力するコマンド `config_nfs.rb`

```
----------------------------------------------------------------------
| Shares                | Clients               | Config           |
----------------------------------------------------------------------
| add-audit-share       | add-ip-to-share       | validate-config  |
| enable-disable-share  | remove-ip-from-share  | refresh-config   |
|                       |                       | help             |
|                       |                       | exit             |
----------------------------------------------------------------------
```

5. 監査クライアントを追加します。 `add-audit-share`
   a. プロンプトが表示されたら、監査共有用の監査クライアントのIPアドレスまたはIPアドレス範囲を入力します。 `client_IP_address`
   b. プロンプトが表示されたら、 * Enter * を押します。
6. 複数の監査クライアントに監査共有へのアクセスを許可する場合は、ユーザのIPアドレスを追加します。 `add-ip-to-share`
   a. 監査共有の番号を入力します。 *`audit_share_number`*
   b. プロンプトが表示されたら、監査共有用の監査クライアントのIPアドレスまたはIPアドレス範囲を入力します。 *`client_IP_address`*
   c. プロンプトが表示されたら、 * Enter * を押します。

      NFS 設定ユーティリティが表示されます。
   d. 監査共有に追加する監査クライアントごとに、上記の手順を繰り返します。
7. 必要に応じて、設定を確認します。
   a. 次のように入力します。 `validate-config`

サービスがチェックされて表示されます。

b. プロンプトが表示されたら、 * Enter * を押します。

NFS 設定ユーティリティが表示されます。

c. NFS設定ユーティリティを閉じます。 `exit`

8. 他のサイトで監査共有を有効にする必要があるかどうかを確認します。
   - StorageGRID 環境が単一サイトの場合は、次の手順に進みます。
   - StorageGRID 環境で他のサイトに管理ノードが含まれている場合は、必要に応じてこれらの監査共有を有効にします。
     i. サイトの管理ノードにリモートからログインします。
        A. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
        B. に記載されているパスワードを入力します `Passwords.txt` ファイル。
        C. 次のコマンドを入力してrootに切り替えます。 `su -`
        D. に記載されているパスワードを入力します `Passwords.txt` ファイル。
     ii. 同じ手順を繰り返して、追加の管理ノードごとに監査共有を設定します。
     iii. リモート管理ノードへのリモートの Secure Shell ログインを終了します。入力するコマンド `exit`
9. コマンドシェルからログアウトします。 `exit`

NFS 監査クライアントは、 IP アドレスに基づいて監査共有へのアクセスが許可されます。新しい NFS 監査クライアントに共有に IP アドレスを追加して監査共有へのアクセスを許可するか、または IP アドレスを削除して既存の監査クライアントを削除します。

### 監査共有への**NFS**監査クライアントの追加

## NFS 監査クライアントは、 IP アドレスに基づいて監査共有へのアクセスが許可されます。新しい NFS 監査クライアントに監査共有へのアクセスを許可するには、そのクライアントの IP アドレスを監査共有に追加します。

必要なもの

- を用意しておく必要があります `Passwords.txt` root / adminアカウントのパスワードを含むファイル（SAIDパッケージ内にあります）。
- を用意しておく必要があります `Configuration.txt` ファイル（SAIDパッケージ内にあります）。
- 監査クライアントがNFSバージョン3（NFSv3）を使用している必要があります。

手順

1. プライマリ管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`

d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

2. NFS設定ユーティリティを起動します。 `config_nfs.rb`

```
----------------------------------------------------------------------
| Shares                | Clients               | Config           |
----------------------------------------------------------------------
| add-audit-share       | add-ip-to-share       | validate-config  |
| enable-disable-share  | remove-ip-from-share  | refresh-config   |
|                       |                       | help             |
|                       |                       | exit             |
----------------------------------------------------------------------
```

3. 入力するコマンド `add-ip-to-share`

管理ノードで有効になっている NFS 監査共有のリストが表示されます。監査共有はのように表示されます。 `/var/local/audit/export`

4. 監査共有の番号を入力します。 *`audit_share_number`*
5. プロンプトが表示されたら、監査共有用の監査クライアントのIPアドレスまたはIPアドレス範囲を入力します。 *`client_IP_address`*

監査クライアントが監査共有に追加されます。

6. プロンプトが表示されたら、 * Enter * を押します。

NFS 設定ユーティリティが表示されます。

7. 監査共有に追加する監査クライアントごとに、この手順を繰り返します。
8. 必要に応じて、設定を確認します。 `validate-config`

サービスがチェックされて表示されます。

a. プロンプトが表示されたら、 * Enter * を押します。

NFS 設定ユーティリティが表示されます。

9. NFS設定ユーティリティを閉じます。 `exit`
10. StorageGRID 環境が単一サイトの場合は、次の手順に進みます。

StorageGRID 環境で他のサイトに管理ノードが含まれている場合は、必要に応じてこれらの監査共有を有効にします。

a. サイトの管理ノードにリモートからログインします。

i. 次のコマンドを入力します。 `ssh admin@`*`grid_node_IP`*

ii. に記載されているパスワードを入力します `Passwords.txt` ファイル。

iii. 次のコマンドを入力してrootに切り替えます。 `su -`

iv. に記載されているパスワードを入力します `Passwords.txt` ファイル。

b. 同じ手順を繰り返して、管理ノードごとに監査共有を設定します。

c. リモート管理ノードへのリモートのSecure Shellログインを終了します。 `exit`

11. コマンドシェルからログアウトします。 `exit`

**NFS**監査の統合の検証

## 監査共有を設定して NFS 監査クライアントを追加したら、監査クライアント共有をマウントし、監査共有のファイルにアクセスできることを確認します。

手順

1. AMS サービスをホストしている管理ノードのクライアント側 IP アドレスを使用して、接続（またはクライアントシステムでの操作）を検証します。入力するコマンド `ping IP_address`

   サーバが応答して接続を示していることを確認します。

2. クライアントのオペレーティングシステムに適したコマンドを使用して、読み取り専用の監査共有をマウントします。Linux コマンドの例は次のとおりです（ 1 行で入力します）。

   ```
   mount -t nfs -o hard,intr Admin_Node_IP_address:/var/local/audit/export
   myAudit
   ```

   AMS サービスをホストしている管理ノードの IP アドレスと、監査システムの事前定義された共有名を使用します。マウントポイントには、クライアントが選択した任意の名前を使用できます（例： *myAudit* 前のコマンドを参照）。

3. 監査共有のファイルにアクセスできることを確認します。入力するコマンド `ls myAudit /*`

   ここで、 *myAudit* は、監査共有のマウントポイントです。少なくとも 1 つのログファイルが表示されている必要があります。

監査共有からの**NFS**監査クライアントの削除

## NFS 監査クライアントは、 IP アドレスに基づいて監査共有へのアクセスが許可されます。既存の監査クライアントを削除するには、その IP アドレスを削除します。

必要なもの

- を用意しておく必要があります `Passwords.txt` root / adminアカウントのパスワードを含むファイル（SAIDパッケージ内にあります）。
- を用意しておく必要があります `Configuration.txt` ファイル（SAIDパッケージ内にあります）。

このタスクについて

監査共有にアクセス可能な最後の IP アドレスを削除することはできません。

手順

1. プライマリ管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

   rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

2. NFS設定ユーティリティを起動します。 `config_nfs.rb`

```
------------------------------------------------------------------
| Shares                | Clients               | Config          |
------------------------------------------------------------------
| add-audit-share       | add-ip-to-share       | validate-config |
| enable-disable-share  | remove-ip-from-share  | refresh-config  |
|                       |                       | help            |
|                       |                       | exit            |
------------------------------------------------------------------
```

3. 監査共有からIPアドレスを削除します。 `remove-ip-from-share`

   サーバで設定されている監査共有に番号が振られ、リストに表示されます。監査共有はのように表示されます。 `/var/local/audit/export`

4. 監査共有に対応する番号を入力します。 *`audit_share_number`*

   監査共有へのアクセスを許可している IP アドレスに番号が振られ、リストに表示されます。

5. 削除する IP アドレスに対応する番号を入力します。

   監査共有が更新され、この IP アドレスの監査クライアントからのアクセスは許可されなくなります。

6. プロンプトが表示されたら、 * Enter * を押します。

   NFS 設定ユーティリティが表示されます。

7. NFS設定ユーティリティを閉じます。 `exit`
8. StorageGRID 環境が複数データセンターサイトの環境であり、他のサイトにも管理ノードが含まれている場合は、必要に応じてこれらの監査共有を無効にします。
   a. 各サイトの管理ノードにリモートからログインします。
      i. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
      ii. に記載されているパスワードを入力します `Passwords.txt` ファイル。
      iii. 次のコマンドを入力してrootに切り替えます。 `su -`

iv. に記載されているパスワードを入力します `Passwords.txt` ファイル。

b. 同じ手順を繰り返して、追加の管理ノードごとに監査共有を設定します。

c. リモート管理ノードへのリモートのSecure Shellログインを終了します。 `exit`

9. コマンドシェルからログアウトします。 `exit`

**NFS**監査クライアントの**IP**アドレスの変更

1. 既存の NFS 監査共有に新しい IP アドレスを追加します。
2. 元の IP アドレスを削除します。

関連情報

"監査共有へのNFS監査クライアントの追加"

"監査共有からのNFS監査クライアントの削除"

# アーカイブノードの管理

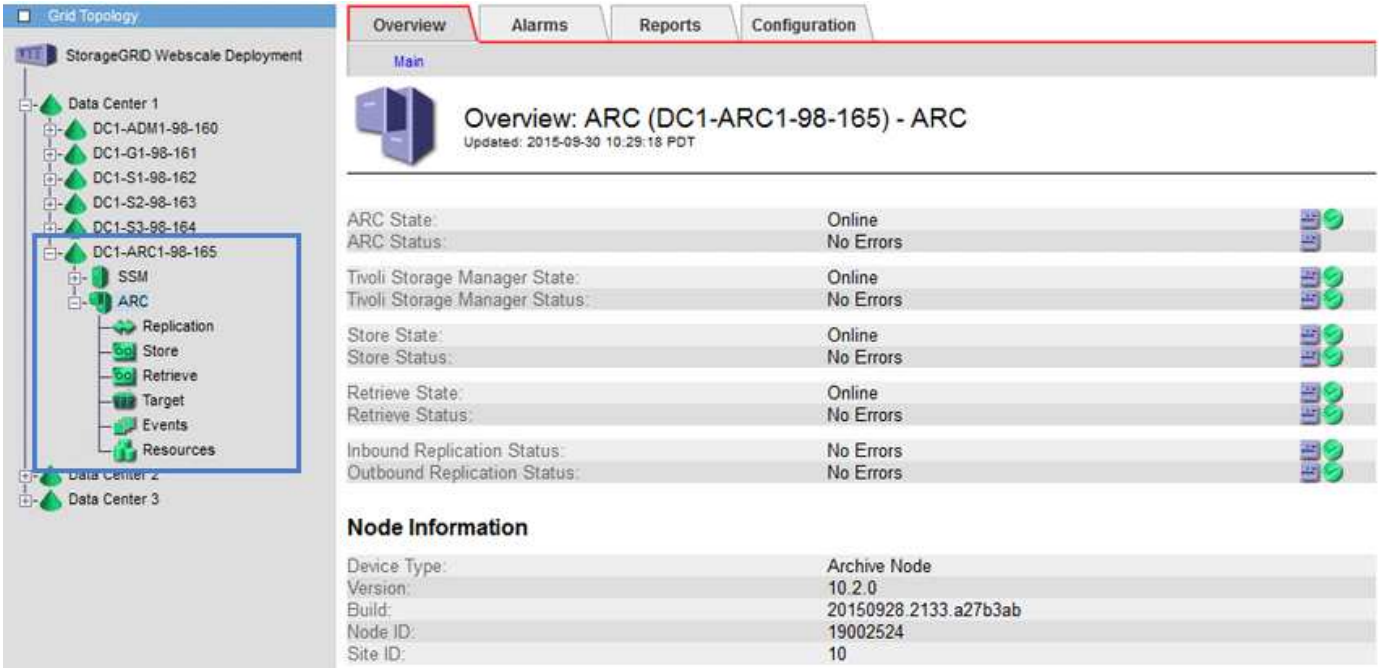
## 必要に応じて、StorageGRID システムの各データセンターサイトにアーカイブノードを導入して、Tivoli Storage Manager（TSM）などの外部アーカイブストレージシステムに接続できます。

外部ターゲットへの接続を設定したあと、 TSM のパフォーマンスを最適化するようにアーカイブノードを設定できます。 TSM サーバの容量が上限に近づいている場合や TSM サーバを使用できない場合は、アーカイブノードをオフラインにできます。また、レプリケーションと読み出しを設定できます。アーカイブノードにカスタムアラームを設定することもできます。

- "アーカイブノードとは"
- "アーカイブストレージへのアーカイブノード接続を設定しています"
- "アーカイブノード用のカスタムアラームの設定"
- "Tivoli Storage Managerを統合する"

アーカイブノードとは

## アーカイブノードは、オブジェクトデータの長期保管用に外部アーカイブストレージシステムをターゲットとするインターフェイスを提供します。また、この接続、および StorageGRID システムとターゲットの外部アーカイブストレージシステム間でのオブジェクトデータ転送も監視します。




削除はできないが定期的にはアクセスされないオブジェクトデータは、ストレージノードの回転式ディスクから、クラウドやテープなどの外部アーカイブストレージにいつでも移動できます。オブジェクトデータをこのようにアーカイブするには、データセンターサイトのアーカイブノードを設定し、次にこのアーカイブノードをコンテンツ配置手順の「ターゲット」として選択した ILM ルールを設定します。アーカイブノードは、アーカイブされたオブジェクトデータ自体の管理は行いません。これは外部アーカイブデバイスによって行われます。

オブジェクトメタデータはアーカイブされず、ストレージノードに残ります。

**ARC** サービスとは

## Archive Node's Archive（ARC）サービスは、TSMミドルウェア経由のテープなど、外部アーカイブストレージへの接続を設定できる管理インターフェイスです。

ARC サービスは、外部のアーカイブストレージシステムと連携することにより、ニアラインストレージ用にオブジェクトデータを送信し、クライアントアプリケーションがアーカイブされたオブジェクトを要求したときに読み出しを実行します。クライアントアプリケーションがアーカイブされたオブジェクトを要求すると、ストレージノードは ARC サービスからオブジェクトデータを要求します。ARC サービスは外部のアーカイブストレージシステムに要求を送信し、アーカイブストレージシステムは要求されたオブジェクトデータを読み出して ARC サービスに送信します。ARC サービスはオブジェクトデータを検証してストレージノードに転送し、ストレージノードは要求元のクライアントアプリケーションにオブジェクトを返します。

TSM ミドルウェア経由でテープにアーカイブされたオブジェクトデータに対する要求は、読み出し効率が向上するように管理されます。要求は、テープに格納されているオブジェクトの順番と同じになるように順序が調整されたうえで、ストレージデバイスへの送信用のキューに登録されます。アーカイブデバイスによっては、異なるボリューム上のオブジェクトに対する複数の要求を同時に処理できます。

アーカイブストレージへのアーカイブノード接続を設定しています

## 外部アーカイブに接続するようにアーカイブノードを設定する場合は、ターゲットタイプを選択する必要があります。

StorageGRID システムでは、S3インターフェイスを使用したクラウドへのオブジェクトデータのアーカイブ、またはTivoli Storage Manager（TSM）ミドルウェアを使用したテープへのオブジェクトデータのアーカイブがサポートされます。

アーカイブノードにアーカイブターゲットのタイプを設定したあとに、そのタイプを変更することはできません。

- "S3 APIを使用したクラウドへのアーカイブ"
- "TSMミドルウェア経由でテープにアーカイブ"
- "アーカイブノードの読み出し設定を構成しています"
- "アーカイブノードのレプリケーションを設定しています"

**S3 API**を使用したクラウドへのアーカイブ

アーカイブノードは、 Amazon Web Services （ AWS ）に直接接続するように設定することも、 S3 API を使用して StorageGRID システムと連携可能な他のシステムに接続するように設定することもできます。

S3 API を使用してアーカイブノードから外部のアーカイブストレージシステムにオブジェクトを移動する処理は、より多くの機能を提供する ILM Cloud Storage Pools に置き換えられました。Cloud Tiering - Simple Storage Service （ S3 ） * オプションは引き続きサポートされていますが、代わりにクラウドストレージプールの実装を推奨します。

「 Cloud Tiering - Simple Storage Service （ S3 ） * 」オプションを指定してアーカイブノードを現在使用している場合は、クラウドストレージプールへのオブジェクトの移行を検討してください。情報ライフサイクル管理を使用してオブジェクトを管理する手順を参照してください。

関連情報

"ILM を使用してオブジェクトを管理する"

**S3 API**の接続を設定します

S3 インターフェイスを使用してアーカイブノードに接続する場合は、 S3 API の接続を設定する必要があります。これらの設定が完了するまで ARC サービスは外部アーカイブストレージシステムと通信できないため、 Major アラーム状態のままです。

S3 API を使用してアーカイブノードから外部のアーカイブストレージシステムにオブジェクトを移動する処理は、より多くの機能を提供する ILM Cloud Storage Pools に置き換えられました。Cloud Tiering - Simple Storage Service （ S3 ） * オプションは引き続きサポートされていますが、代わりにクラウドストレージプールの実装を推奨します。

「 Cloud Tiering - Simple Storage Service （ S3 ） * 」オプションを指定してアーカイブノードを現在使用している場合は、クラウドストレージプールへのオブジェクトの移行を検討してください。情報ライフサイクル管理を使用してオブジェクトを管理する手順を参照してください。

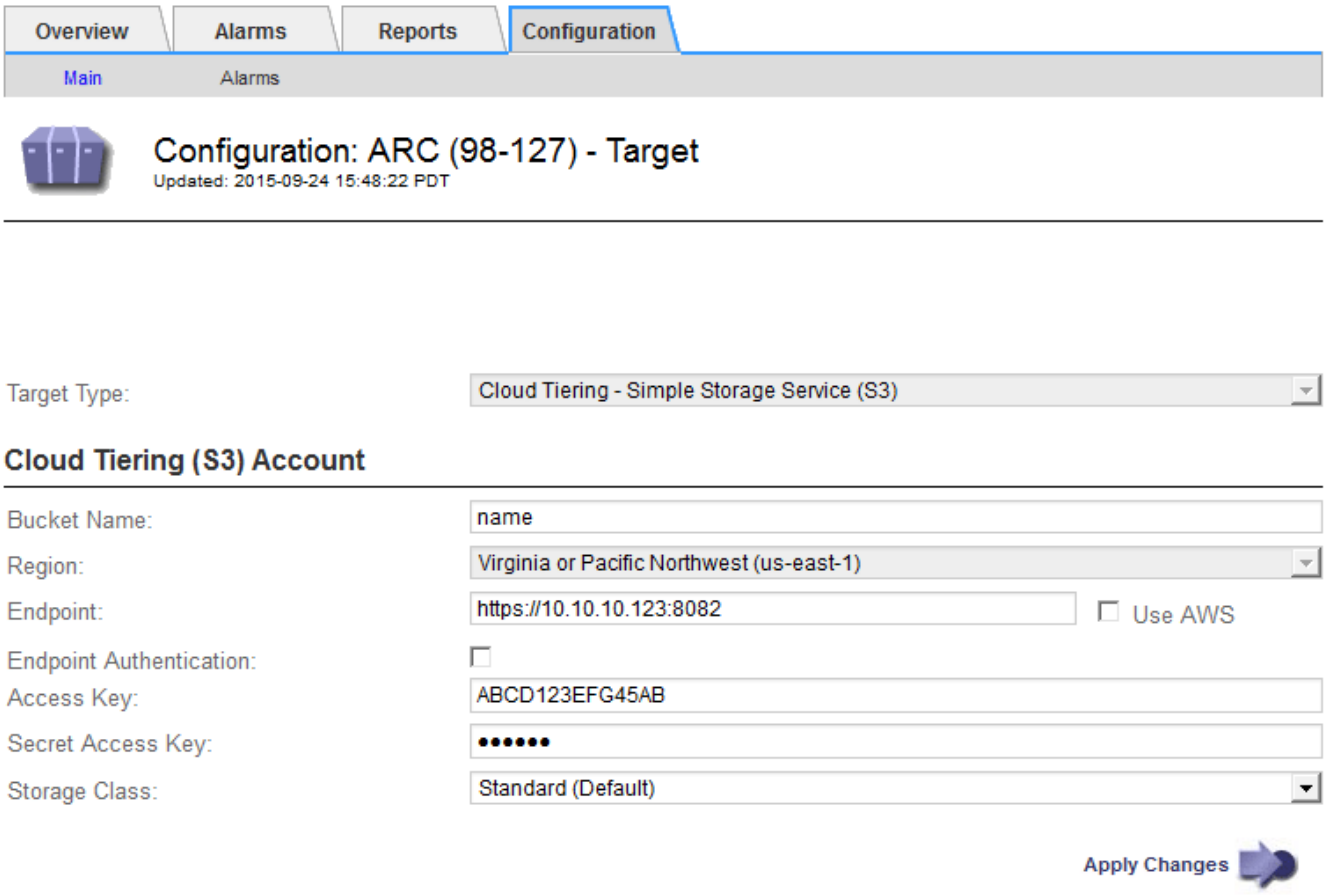
必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

- 特定のアクセス権限が必要です。
- ターゲットのアーカイブストレージシステム上にバケットを作成しておく必要があります。
  - このバケットは1つのアーカイブノード専用にする必要があります。他のアーカイブノードやアプリケーションでは使用できません。
  - バケットには、場所に応じた適切なリージョンを選択する必要があります。
  - バケットのバージョン管理は一時停止に設定する必要があります。
- オブジェクトのセグメント化を有効にして、最大セグメントサイズは4.5GiB（4、831、838、208バイト）以下にする必要があります。S3 が外部アーカイブストレージシステムとして使用されている場合、この値を超える S3 API 要求は失敗します。

手順

1. Support > Tools > Grid Topology *を選択します。
2. アーカイブノード* ARC *ターゲット*を選択します。
3. * Configuration * > * Main * を選択します。




4. ターゲットタイプドロップダウンリストから * Cloud Tiering - Simple Storage Service （ S3 ） * を選択します。

ターゲットタイプを選択するまで、構成設定は使用できません。

5. アーカイブノードからターゲットの外部の S3 対応アーカイブストレージシステムへの接続に使用するクラウドの階層化（ S3 ）アカウントを設定します。

このページのフィールドのほとんどはわかりやすいもので、説明を必要としません。以下は、説明が必要なフィールドです。

- * Region * ： * Use AWS * が選択されている場合にのみ選択できます。バケットのリージョンと同じリージョンを選択する必要があります。
- * Endpoint * および * Use AWS * ： Amazon Web Services （ AWS ）の場合は、「 * Use AWS * 」を選択します。* エンドポイント * には、バケット名属性とリージョン属性に基づいてエンドポイント URL が自動的に入力されます。例：

  ```
  https://bucket.region.amazonaws.com
  ```

  AWS 以外のターゲットの場合は、ポート番号を含め、バケットをホストしているシステムの URL を入力します。例：

```
https://system.com:1080
```

- * エンドポイント認証 *: デフォルトで有効になっています。外部アーカイブストレージシステムへのネットワークが信頼されている場合は、チェックボックスをオフにして、対象の外部アーカイブストレージシステムのエンドポイントの SSL 証明書およびホスト名検証を無効にすることができます。StorageGRID システムの別のインスタンスがターゲットのアーカイブストレージデバイスであり、システムに公開署名された証明書が設定されている場合、このチェックボックスはオンのままでかまいません。
- * ストレージクラス * ：通常のストレージには「 * Standard （デフォルト） * 」を選択します。簡単に再作成できるオブジェクトに対してのみ、「冗長性の低下」を選択します。* 冗長性の低下 * 信頼性の低い低コストのストレージを提供します。ターゲットのアーカイブストレージシステムが StorageGRID システムの別のインスタンスの場合、ストレージクラス * はオブジェクトの取り込み時に実行されるオブジェクトの中間コピー数を、デュアルコミットがオブジェクトの取り込み時に使用される場合にターゲットシステムで制御します。

6. [ 変更の適用 *] をクリックします。

   指定した設定が検証され、 StorageGRID システムに適用されます。いったん設定したターゲットは変更できません。

関連情報

"ILM を使用してオブジェクトを管理する"

**S3 API**の接続設定の変更

## S3 API を使用して外部のアーカイブストレージシステムに接続するようにアーカイブノードを設定したあとで接続が変更された場合、一部の設定を変更できます。

必要なもの

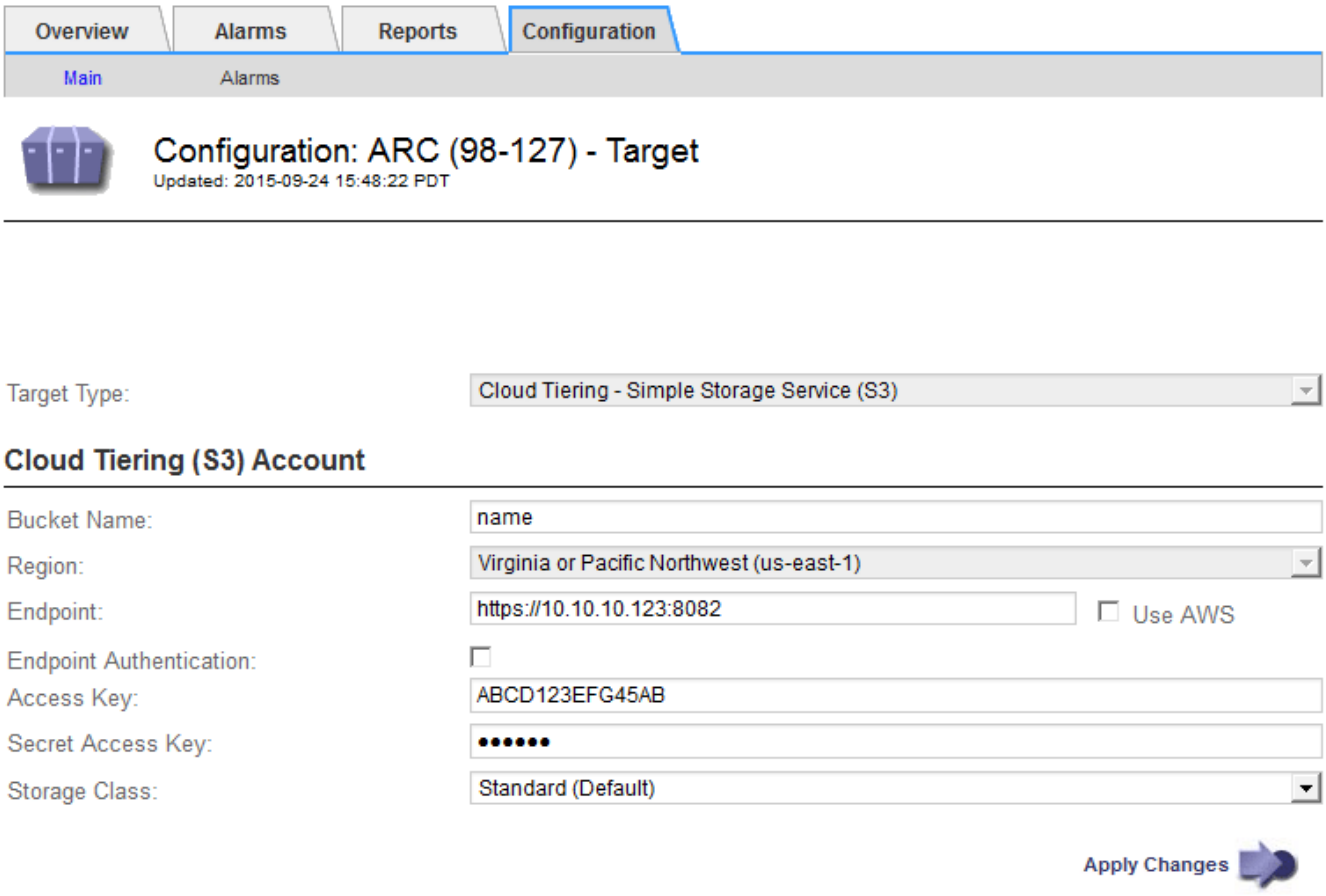
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

クラウドの階層化（ S3 ）アカウントを変更した場合は、アーカイブノードによって以前にバケットに取り込まれたすべてのオブジェクトを含む、バケットへの読み取り / 書き込みアクセスがユーザアクセスクレデンシャルに割り当てられている必要があります。

手順

1. Support > Tools > Grid Topology *を選択します。
2. 「アーカイブノード **ARC** ターゲット」を選択します。
3. * Configuration * > * Main * を選択します。




4. 必要に応じて、アカウント情報を変更します。

   ストレージクラスを変更すると、新しいオブジェクトデータは新しいストレージクラスで格納されます。既存のオブジェクトは、引き続き取り込み時に設定したストレージクラスで格納されます。

   バケット名、リージョン、およびエンドポイントは AWS の値を使用し、変更することはできません。

5. [ 変更の適用 *] をクリックします。

クラウドの階層化サービスの状態を変更しています

## クラウドの階層化サービスの状態を変更することで、 S3 API を使用して接続する外部のアーカイブストレージシステムに対してアーカイブノードが読み取り / 書き込みできるかどうかを制御できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

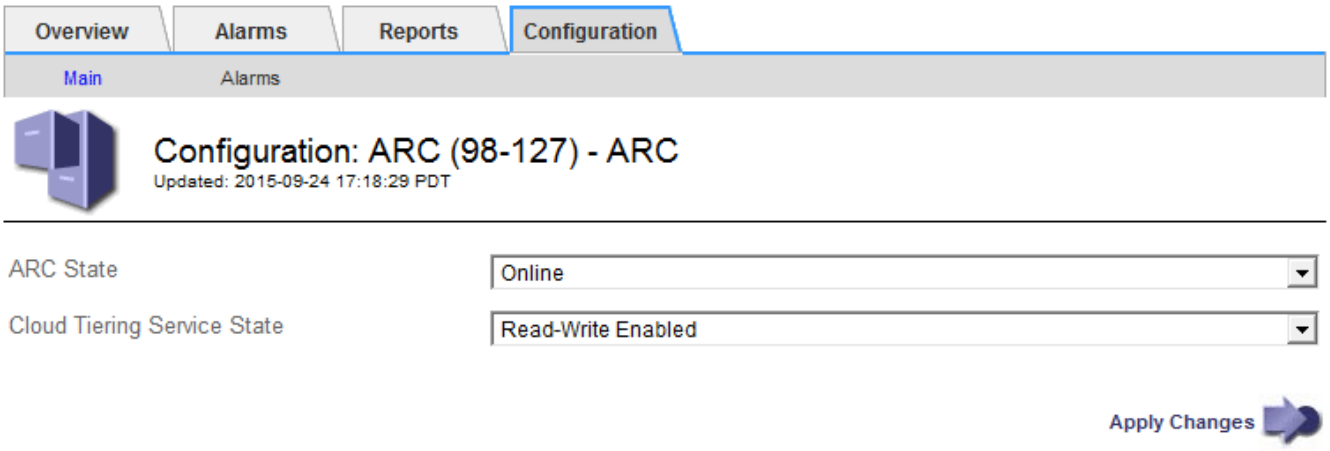
- 特定のアクセス権限が必要です。
- アーカイブノードが設定されている必要があります。

このタスクについて

クラウドの階層化サービスの状態を「 * Read-Write Disabled 」に変更すると、アーカイブノードを効果的にオフラインにできます。

手順

1. Support **>** Tools **>** Grid Topology *を選択します。
2. 「 * _ アーカイブノード _ * > * ARC * 」を選択します。
3. * Configuration * > * Main * を選択します。




4. クラウドの階層化サービスの状態 * を選択します。
5. [ 変更の適用 *] をクリックします。

**S3 API**接続のストア障害数のリセット

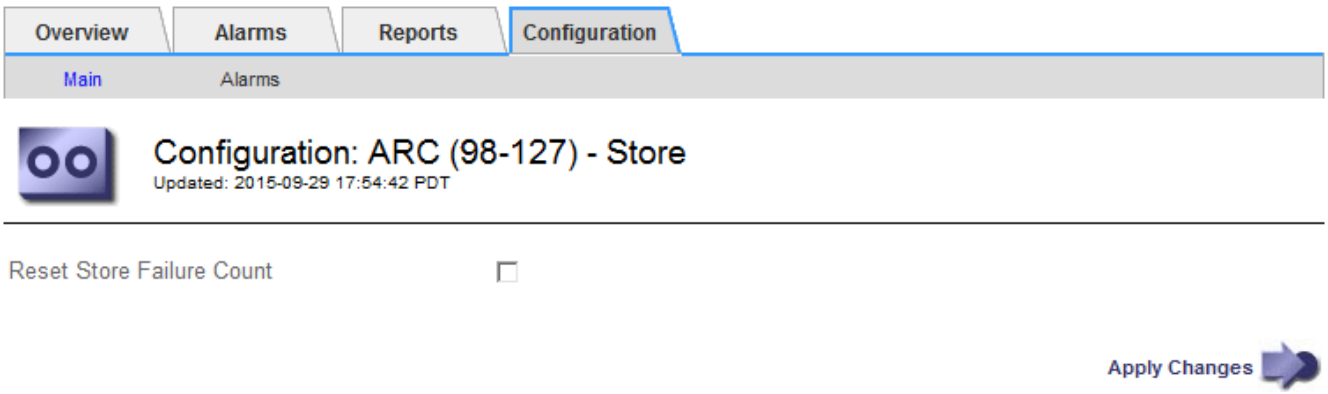
## アーカイブノードが S3 API 経由でアーカイブストレージシステムに接続している場合は、ストア障害数をリセットでき、 ARVF （ Store Failures ）アラームをクリアできます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

手順

1. Support **>** Tools **>** Grid Topology *を選択します。
2. 「*アーカイブノード **ARC** Store *」を選択します。
3. * Configuration * > * Main * を選択します。




4. 「 Reset Store Failure Count 」を選択します。
5. [ 変更の適用 *] をクリックします。

   Store Failures 属性がゼロにリセットされます。

### 「**Cloud Tiering - S3**」からクラウドストレージプールへのオブジェクトの移行

現在 Cloud Tiering - Simple Storage Service （ S3 ） * 機能を使用してオブジェクトデータを S3 バケットに階層化している場合は、代わりにクラウドストレージプールへのオブジェクトの移行を検討してください。クラウドストレージプールは拡張性に優れたアプローチを提供し、 StorageGRID システム内のすべてのストレージノードを活用します。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- クラウド階層化用に設定された S3 バケットにオブジェクトが格納済みである。

> オブジェクトデータを移行する前に、ネットアップのアカウント担当者に問い合わせて関連するコストについて把握してください。

このタスクについて

ILM から見た場合、クラウドストレージプールはストレージプールに似ています。ただし、ストレージプールは StorageGRID システム内のストレージノードまたはアーカイブノードで構成されますが、クラウドストレージプールは外部の S3 バケットで構成されます。

オブジェクトを「 Cloud Tiering - S3 」からクラウドストレージプールに移行する前に、 S3 バケットを作成し、 StorageGRID にクラウドストレージプールを作成する必要があります。次に、新しい ILM ポリシーを作成し、クラウド階層化バケットにオブジェクトを格納するために使用していた ILM ルールをコピーし、同じオブジェクトをクラウドストレージプールに格納するように変更します。

オブジェクトがクラウドストレージプールに格納されている場合、それらのオブジェクトのコピーを StorageGRID にも格納することはできません。現在クラウド階層化に使用している ILM ルールが複数の場所に同時にオブジェクトを格納するように設定されている場合は、その機能が失われるため、このオプションの移行を引き続き実行するかどうかを検討してください。移行を続行する場合は、既存のルールをコピーするのではなく、新しいルールを作成する必要があります。

手順

1. クラウドストレージプールを作成

   クラウドストレージプールに新しい S3 バケットを使用して、クラウドストレージプールで管理されるデータのみが含まれるようにします。

2. クラウド階層化バケットに格納する原因 オブジェクトをアクティブな ILM ポリシーで特定します。
3. 該当するルールをコピーします。
4. コピーしたルールで、配置場所を新しいクラウドストレージプールに変更します。
5. コピーしたルールを保存します。
6. 新しいルールを使用する新しいポリシーを作成します。
7. 新しいポリシーをシミュレートしてアクティブ化します。

   新しいポリシーがアクティブ化されて ILM 評価が実行されると、クラウド階層化用に設定された S3 バケットからクラウドストレージプール用に設定された S3 バケットにオブジェクトが移動します。グリッド上の使用可能なスペースに影響はありません。クラウドストレージプールに移動されたオブジェクトは、クラウド階層化バケットから削除されます。

関連情報

"ILM を使用してオブジェクトを管理する"

**TSM**ミドルウェア経由でのテープへのアーカイブ

# Tivoli Storage Manager （ TSM ）サーバをターゲットとするようにアーカイブノードを構成できます。 TSM サーバは、テープライブラリを含むランダムまたはシーケンシャルアクセスのストレージデバイスとの間でオブジェクトデータを格納および読み出すための論理インターフェイスです。

アーカイブノードの ARC サービスは TSM サーバに対するクライアントとして機能し、 Tivoli Storage Manager をアーカイブストレージシステムと通信するためのミドルウェアとして使用します。

## TSM 管理クラス

TSM ミドルウェアによって定義された管理クラスは、 TSM のバックアップおよびアーカイブ処理がどのように機能するかを示します。この管理クラスを使用して、 TSM サーバによって適用されるコンテンツ用のルールを指定できます。これらのルールは StorageGRID システムの ILM ポリシーとは独立して機能します。オブジェクトは永続的に格納され、アーカイブノードによっていつでも読み出し可能であるという StorageGRID システムの要件と矛盾しないことが必要です。アーカイブノードから TSM サーバにオブジェクトデータが送信されたあと、 TSM サーバが管理するテープにオブジェクトデータが格納される間、 TSM のライフサイクルと保持のルールが適用されます。

TSM 管理クラスは、アーカイブノードから TSM サーバにオブジェクトデータが送信されたあと、データの場所または保持のルールを適用するために TSM サーバで使用されます。たとえば、データベースのバックアップとして識別されたオブジェクト（新しいデータで上書き可能な一時的コンテンツ）を、アプリケーションデータ（無期限に保持する必要のある固定コンテンツ）とは別の方法で処理できます。

**TSM**ミドルウェアへの接続を設定しています

# アーカイブノードが Tivoli Storage Manager （ TSM ）ミドルウェアと通信するためには、いくつかの設定を行う必要があります。

必要なもの

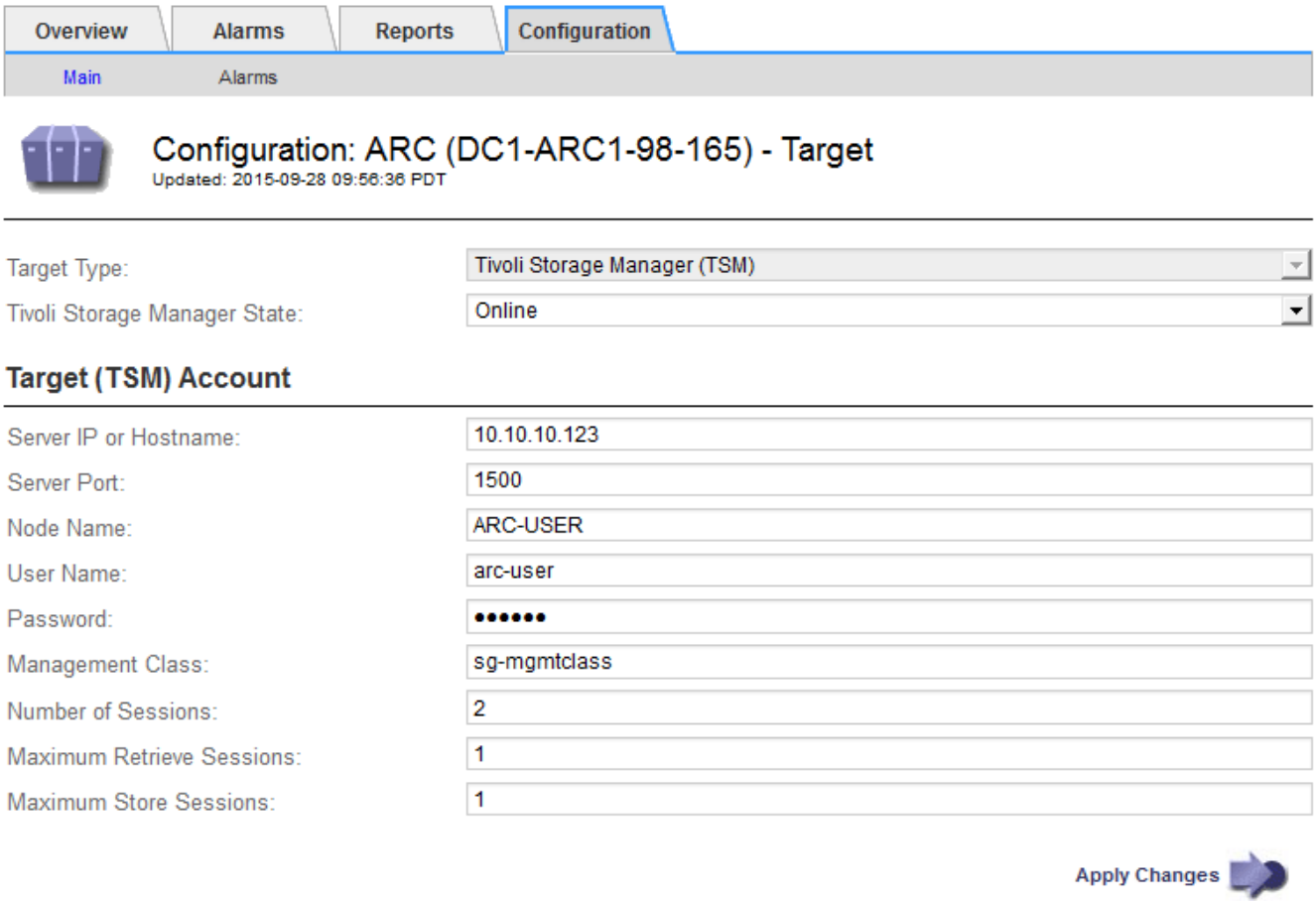
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

これらの設定が完了するまで ARC サービスは Tivoli Storage Manager と通信できないため、 Major アラーム状態のままです。

手順

1. Support **>** Tools **>** Grid Topology *を選択します。
2. 「アーカイブノード **ARC** ターゲット」を選択します。
3. * Configuration * > * Main * を選択します。



4. [ ターゲット・タイプ ] ドロップダウン・リストから **'[** Tivoli Storage Manager(TSM)*] を選択します
5. Tivoli Storage Manager State * では、 TSM ミドルウェアサーバからの読み出しを防ぐために「 * Offline * 」を選択します。

   デフォルトでは、「 Tivoli Storage Manager State 」は「 Online 」に設定されています。つまり、アーカイブノードは TSM ミドルウェアサーバからオブジェクトデータを読み出すことができます。

6. 次の情報を入力します。

   - * Server IP or Hostname * ： ARC サービスが使用する TSM ミドルウェアサーバの IP アドレスまたは完全修飾ドメイン名を指定します。デフォルトの IP アドレスは 127.0.0.1 です。
   - * Server Port * ： ARC サービスの接続先の TSM ミドルウェアサーバ上のポート番号を指定します。デフォルトは 1500 です。
   - * Node Name * ：アーカイブノードの名前を指定します。TSM ミドルウェアサーバに登録した名前（ arc - user ）を入力する必要があります。
   - * User Name * ： ARC サービスが TSM サーバへのログインに使用するユーザ名を指定します。デフォルトのユーザ名（ arc - user ）またはアーカイブノード用に指定した管理ユーザを入力します。
   - * Password * ： ARC サービスが TSM サーバへのログインに使用するパスワードを指定します。
   - * 管理クラス * ：オブジェクトが StorageGRID システムに保存されるときに管理クラスが指定されていない場合や、指定した管理クラスが TSM ミドルウェアサーバ上で定義されていない場合に使用するデフォルトの管理クラスを指定します。
   - * Number of Sessions * ： TSM ミドルウェアサーバ上にあるアーカイブノード専用のテープドライブの数を指定します。アーカイブノードは、最大でマウントポイントごとに 1 つのセッションと少数（ 5 つ未満）の追加セッションを同時に作成します。

     アーカイブノードを登録または更新したときには、この値を MAXNUMMP （マウントポイントの最大数）と同じ値に変更する必要があります（登録コマンドでは、値が設定されていない場合の MAXNUMMP のデフォルト値は 1 です）。

   また、 TSM サーバの MAXSESSIONS の値を、 ARC サービス用に設定されている Sessions の数以上の数値に変更する必要があります。TSM サーバ上の MAXSESSIONS のデフォルト値は 25 です。

   - * Maximum Retrieve Sessions * ： ARC サービスが読み出し処理用に TSM ミドルウェアサーバに対して開くことができるセッションの最大数を指定します。ほとんどの場合、適切な値は「セッション数 - ストアセッションの最大数」です。1 つのテープ・ドライブを共有してストレージと取得を行う必要がある場合は ' セッション数に等しい値を指定します
   - * Maximum Store Sessions * ： ARC サービスがアーカイブ処理用に TSM ミドルウェアサーバに対して開くことができる同時セッションの最大数を指定します。

     この値は、対象のアーカイブストレージシステムが一杯で、読み出しのみが可能な場合を除き、 1 に設定する必要があります。すべてのセッションを読み出しに使用するには、この値を 0 に設定します。

7. [ 変更の適用 *] をクリックします。

**TSM**ミドルウェアセッション用のアーカイブノードの最適化

アーカイブノードのセッションを設定することで、 Tivoli Server Manager （ TSM ）に

# 接続するアーカイブノードのパフォーマンスを最適化できます。

必要なもの

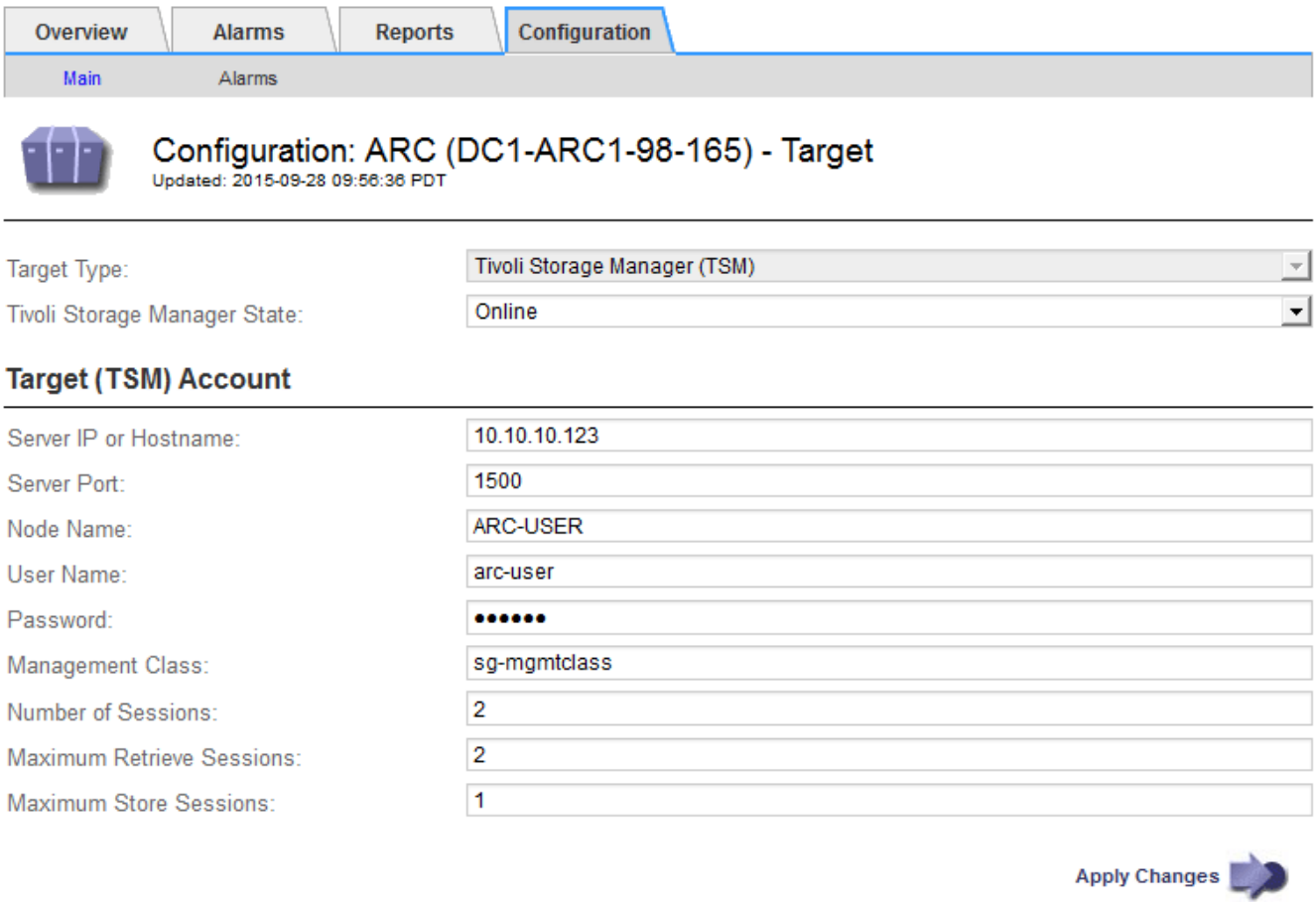
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

通常、アーカイブノードが TSM ミドルウェアサーバに対して同時に開くことができるセッションの数は、TSM サーバが所有するアーカイブノード専用のテープドライブの数に設定されます。1 本のテープドライブがストレージ用に割り当てられ、残りは読み出し用に割り当てられます。ただし、ストレージノードがアーカイブノードのコピーからリビルドされている場合や、アーカイブノードが読み取り専用モードで動作している場合は、読み出しセッションの最大数を同時セッション数と同じに設定することで、 TSM サーバのパフォーマンスを最適化できます。したがって、すべてのドライブを同時に読み出しに使用できます。また、必要に応じて、これらのドライブのうち 1 つをストレージに使用することもできます。

手順

1. Support **>** Tools **>** Grid Topology *を選択します。
2. 「アーカイブノード **ARC** ターゲット」を選択します。
3. * Configuration * > * Main * を選択します。
4. Maximum Retrieve Sessions * を Number of Sessions * と同じに変更します。




5. [ 変更の適用 *] をクリックします。

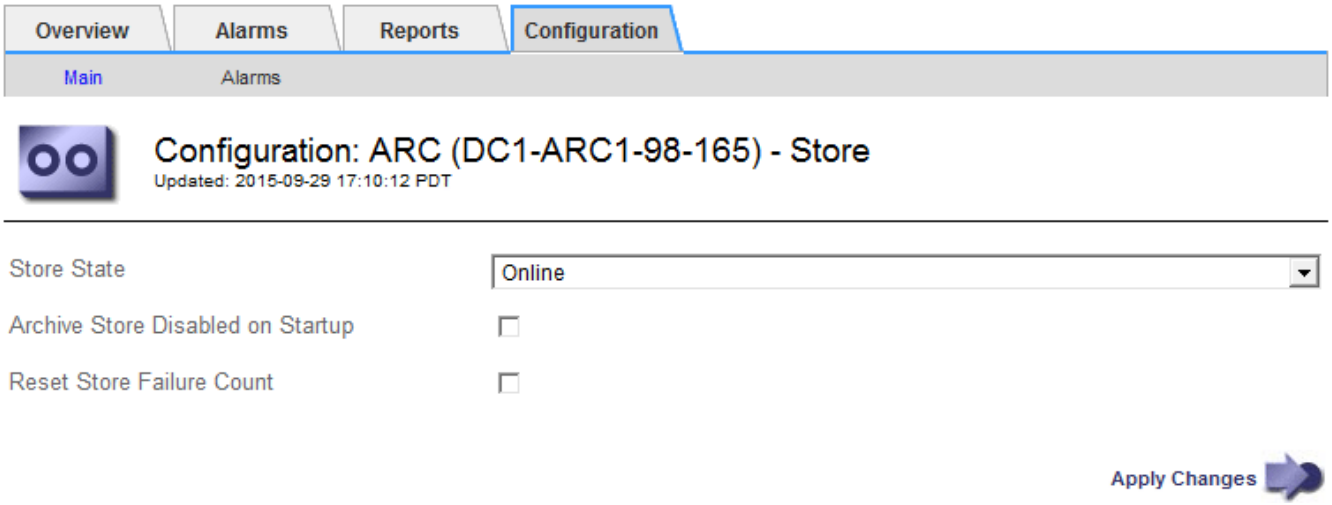
# アーカイブノードが TSM ミドルウェアサーバに接続している場合は、アーカイブノードのアーカイブストアの状態をオンラインまたはオフラインに設定できます。また、アーカイブノードの初回起動時にアーカイブストアを無効にしたり、関連するアラーム用に追跡されているエラー数をリセットしたりすることもできます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

手順

1. Support > Tools > Grid Topology *を選択します。
2. 「*アーカイブノード **ARC** Store *」を選択します。
3. * Configuration * > * Main * を選択します。




4. 必要に応じて次の設定を変更します。
   - Store State ：コンポーネントの状態を次のいずれかに設定します。
     - Online ：アーカイブノードはオブジェクトデータを処理してアーカイブストレージシステムに格納できます。
     - Offline ：アーカイブノードはオブジェクトデータを処理してアーカイブストレージシステムに格納できません。
   - Archive Store Disabled on Startup ：オンにすると、アーカイブストアコンポーネントは再起動後も読み取り専用のままになります。ターゲットのアーカイブストレージシステムへの格納を継続的に無効にする場合に使用します。対象のアーカイブストレージシステムでコンテンツを受け入れられない場合に便利です。
   - Reset Store Failure Count ：ストア障害のカウンタをリセットします。この設定を使用して、 ARVF （ Stores Failure ） アラームをクリアできます。
5. [ 変更の適用 *] をクリックします。

関連情報

"TSMサーバの容量が上限に達した場合のアーカイブノードの管理"

**TSM**サーバの容量が上限に達した場合のアーカイブノードの管理

TSM サーバには、管理対象の TSM データベースまたはアーカイブメディアストレージの容量が上限に近づいている場合にアーカイブノードに通知する手段がありません。アーカイブノードは、 TSM サーバが新しいコンテンツの受け入れを停止したあとも引き続き TSM サーバに転送するオブジェクトデータを受け入れますが、TSM サーバが管理するメディアにこのコンテンツを書き込むことはできません。アラームがトリガーされます。この状況を回避するには、 TSM サーバをプロアクティブに監視します。

必要なもの

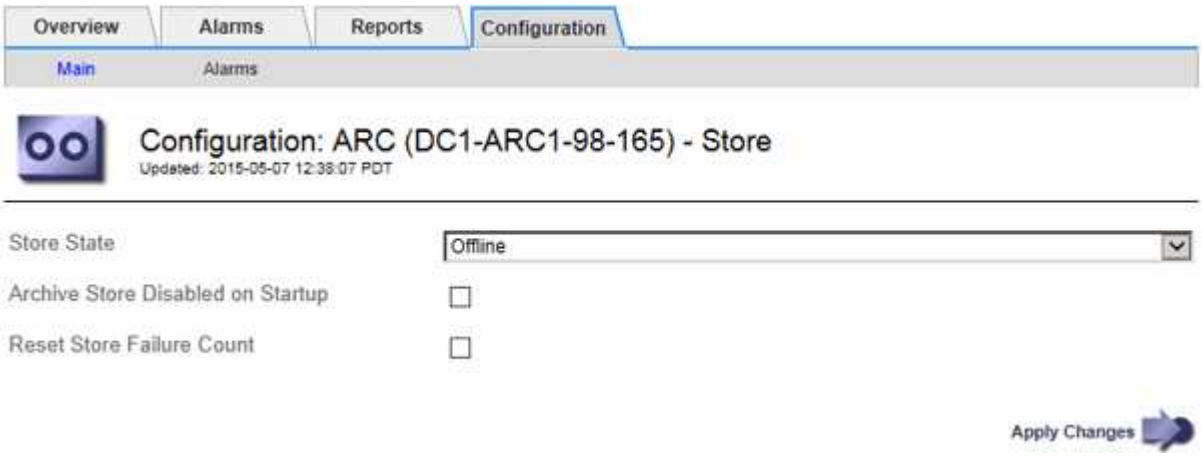
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

ARCサービスからTSMサーバにさらにコンテンツが送信されないようにするには、* ARC * Store *コンポーネントをオフラインにします。この手順 は、 TSM サーバがメンテナンスに使用できないときにアラームを生成しない場合にも役立ちます。

手順

1. Support **>** Tools **>** Grid Topology *を選択します。
2. 「*アーカイブノード **ARC** Store *」を選択します。
3. * Configuration * > * Main * を選択します。




4. 「Store State」を「」に変更します `Offline`。
5. 「 Archive Store Disabled on Startup * 」を選択します。
6. [ 変更の適用 *] をクリックします。

**TSM**ミドルウェアが容量の限界に達した場合にアーカイブノードを読み取り専用に設定

ターゲットの TSM ミドルウェアサーバが容量の限界に達した場合、読み出しのみを実行するようにアーカイブノードを最適化できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

手順

1. Support **>** Tools **>** Grid Topology *を選択します。
2. 「アーカイブノード **ARC** ターゲット」を選択します。
3. * Configuration * > * Main * を選択します。
4. Maximum Retrieve Sessions を Number of Sessions に示されている同時セッション数と同じ数に変更します
5. 最大ストアセッション数を 0 に変更します。

> アーカイブノードが読み取り専用の場合、最大ストアセッション数を 0 に変更する必要はありません。ストアセッションは作成されません。

6. [ 変更の適用 *] をクリックします。

アーカイブノードの読み出し設定を構成しています

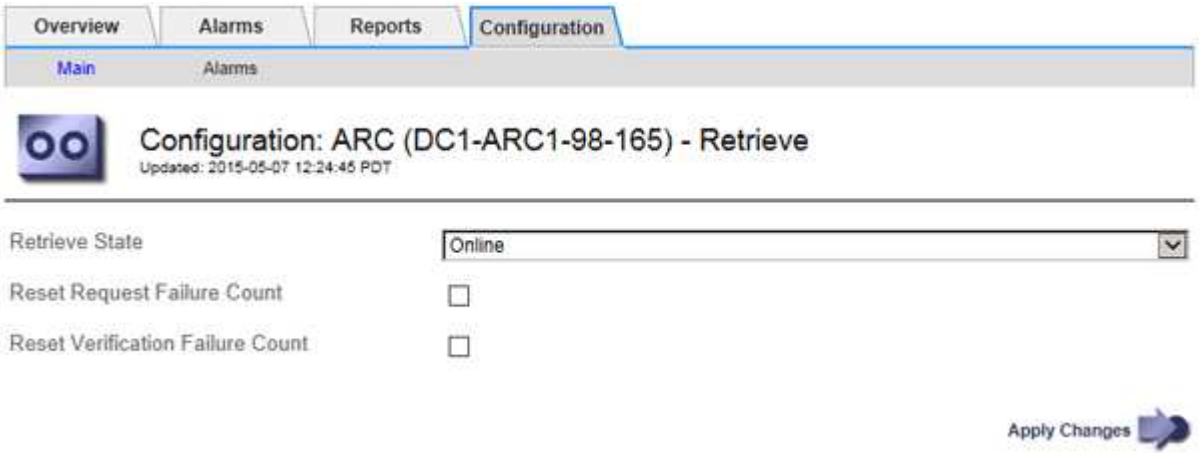
## アーカイブノードの読み出し設定を行って、状態をオンラインまたはオフラインに設定したり、関連するアラームで追跡されているエラー数をリセットしたりできます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

手順

1. Support **>** Tools **>** Grid Topology *を選択します。
2. アーカイブノード* ARC *読み出し*を選択します。
3. * Configuration * > * Main * を選択します。




4. 必要に応じて次の設定を変更します。

- * Retrieve State * ：コンポーネントの状態を次のいずれかに設定します。
  - Online ：グリッドノードがアーカイブメディアデバイスからオブジェクトデータを読み出すことができます。
  - Offline ：グリッドノードはオブジェクトデータを読み出すことができません。
- Reset Request Failures Count ：オンにすると、要求エラーのカウンタがリセットされます。この設定を使用して、 ARRF （ Request Failures ）アラームをクリアできます。
- Reset Verification Failure Count ：オンにすると、読み出したオブジェクトデータの検証エラーのカウンタがリセットされます。この設定を使用して、 ARRV （ Verification Failures ）アラームをクリアできます。

5. [ 変更の適用 *] をクリックします。

アーカイブノードのレプリケーションを設定しています

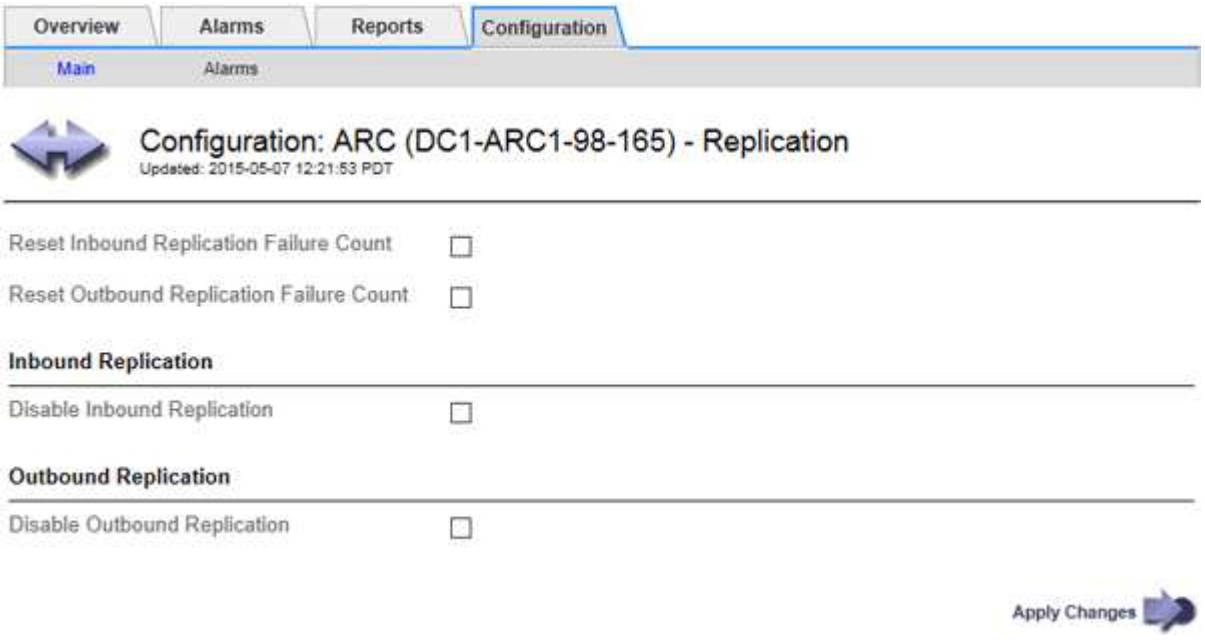
## アーカイブノードのレプリケーション設定を行って、インバウンドおよびアウトバウンドのレプリケーションを無効にしたり、関連するアラームで追跡されているエラー数をリセットしたりできます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

手順

1. Support **>** Tools **>** Grid Topology *を選択します。
2. 「 * _ アーカイブノード _ * > * ARC * > * レプリケーション * 」を選択します。
3. * Configuration * > * Main * を選択します。




4. 必要に応じて次の設定を変更します。
   - * Reset Inbound Replication Failure Count * ：インバウンドレプリケーションエラーのカウンタをリセ

ットする場合に選択します。この設定を使用して、 RIRF （ Inbound Replications - - Failed ）アラームをクリアできます。

- **Reset Outbound Replication Failure Count** ：アウトバウンドレプリケーションエラーのカウンタをリセットする場合に選択します。これを使用すると、 RORF （ Outbound Replications - - Failed ）アラームをクリアできます。
- * インバウンド複製を無効にする *: メンテナンスまたは手順 のテストの一環としてインバウンド複製を無効にする場合に選択します。通常の運用中はオフのままにします。

  インバウンドレプリケーションを無効にすると、 ARC サービスからオブジェクトデータを読み出して StorageGRID システム内の別の場所へレプリケートすることはできますが、システム内の別の場所からこの ARC サービスにオブジェクトをレプリケートすることはできません。ARC サービスは読み取り専用です。

- * アウトバウンドレプリケーションの無効化 * ：メンテナンスまたはテスト用手順 の一環としてアウトバウンドレプリケーション（ HTTP 読み出し用のコンテンツ要求を含む）を無効にする場合は、このチェックボックスを選択します。通常の運用中はオフのままにします。

  アウトバウンドレプリケーションを無効にすると、この ARC サービスにオブジェクトデータをコピーして ILM ルールに従うことはできますが、 ARC サービスからオブジェクトデータを読み出して StorageGRID システム内の別の場所へコピーすることはできません。ARC サービスは書き込み専用です。

5. [ 変更の適用 *] をクリックします。

アーカイブノード用のカスタムアラームの設定

## ARQL 属性と ARRL 属性のカスタムアラームを設定する必要があります。これらの属性は、アーカイブノードがアーカイブストレージシステムからオブジェクトデータを読み出す際の速度と効率を監視します。

- ARQL ：平均キュー長。アーカイブストレージシステムから読み出し用にキューに登録されたオブジェクトデータの平均時間（マイクロ秒）。
- ARRL ：平均リクエストレイテンシ。アーカイブノードがアーカイブストレージシステムからオブジェクトデータを読み出すために必要な平均時間（マイクロ秒）。

これらの属性の許容値は、アーカイブストレージシステムの設定および使用方法によって異なります。（ * ARC * > * Retrieve * > * Overview * > * Main * に移動します）。 要求のタイムアウトに設定された値や、取得要求に使用できるセッション数は特に影響を受けます。

統合が完了したら、アーカイブノードによるオブジェクトデータの読み出しを監視して、通常の読み出し時間およびキューの長さを確認します。次に、異常な動作状態が発生した場合にトリガーされる、 ARQL と ARRL のカスタムアラームを作成します。

関連情報

"トラブルシューティングを監視します"

**Tivoli Storage Manager**を統合する

## ここでは、アーカイブノードをTivoli Storage Manager（TSM）サーバと統合する際のベストプラクティスとセットアップ情報について、TSMサーバの設定に影響を及ぼすアー

カイブノードの動作の詳細も含めて説明します。

- "アーカイブノードの設定と処理"
- "構成のベストプラクティス"
- "アーカイブノードのセットアップを完了します"

アーカイブノードの設定と処理

## StorageGRID システムは、オブジェクトが無期限に保存され、常にアクセス可能な場所として、アーカイブノードを管理します。

オブジェクトが取り込まれると、 StorageGRID システムに対して定義されている情報ライフサイクル管理（ ILM ）ルールに基づいて、アーカイブノードを含む必要なすべての場所にコピーが作成されます。アーカイブノードは TSM サーバに対するクライアントとして機能し、 StorageGRID ソフトウェアのインストール時に TSM クライアントライブラリがアーカイブノードにインストールされます。ストレージ用にアーカイブノードに転送されたオブジェクトデータは、 TSM サーバに直接保存されます。TSM サーバへの保存前にアーカイブノードがオブジェクトデータをステージングしたり、オブジェクトを集約したりすることはありません。ただし、データ速度が保証されれば、アーカイブノードから TSM サーバに 1 回のトランザクションで複数のコピーを送信できます。

アーカイブノードから TSM サーバに保存されたオブジェクトデータは、ライフサイクル / 保持ポリシーに従って TSM サーバで管理されます。これらの保持ポリシーは、アーカイブノードの処理に対応するように定義する必要があります。つまり、アーカイブノードによって保存されたオブジェクトデータは、アーカイブノードによって削除されないかぎり、無期限に保存されていつでもアーカイブノードからアクセスできる必要があります。

StorageGRID システムの ILM ルールと TSM サーバのライフサイクル / 保持ポリシーの間に接続は確立されていません。それぞれが互いに独立して動作します。ただし、各オブジェクトが StorageGRID システムに取り込まれる際に、そのオブジェクトに TSM 管理クラスを割り当てることができます。この管理クラスは、オブジェクトデータとともに TSM サーバに渡されます。オブジェクトタイプごとに異なる管理クラスを割り当てると、オブジェクトデータを別々のストレージプールに配置したり、必要に応じて異なる移行ポリシーや保持ポリシーを適用したりするように TSM サーバを設定できます。たとえば、データベースのバックアップとして識別されたオブジェクト（新しいデータで上書き可能な一時的コンテンツ）を、アプリケーションデータ（無期限に保持する必要のある固定コンテンツ）とは別の方法で処理できます。

アーカイブノードは新規または既存の TSM サーバと統合でき、専用の TSM サーバは必要ありません。TSM サーバは、サイズが予想される最大負荷に対応していれば、他のクライアントと共有できます。TSM は、アーカイブノードとは別のサーバまたは仮想マシンにインストールする必要があります。

複数のアーカイブノードから同じ TSM サーバに書き込むように設定できますが、この設定が推奨されるのは、アーカイブノードが異なるデータセットを TSM サーバに書き込む場合のみです。各アーカイブノードが同じオブジェクトデータのコピーをアーカイブに書き込む場合は、複数のアーカイブノードを同じ TSM サーバに書き込む設定は推奨されません。後者のシナリオでは、本来ならばオブジェクトデータの独立した、冗長コピーとなるはずが、両方のコピーが単一点障害（ TSM サーバ）となります。

アーカイブノードは、 TSM の Hierarchical Storage Management （ HSM ；階層型ストレージ管理）コンポーネントは使用しません。

構成のベストプラクティス

## TSM サーバをサイジングおよび設定する場合、アーカイブノードとの連携を最適化する

ベストプラクティスがあります。

TSM サーバをサイジングおよび設定する際には、次の点を考慮する必要があります。

- アーカイブノードは TSM サーバに保存する前にオブジェクトを集約しないため、アーカイブノードに書き込まれるすべてのオブジェクトへの参照を格納できるように TSM データベースをサイジングする必要があります。
- アーカイブノードソフトウェアでは、テープまたはその他のリムーバブルメディアにオブジェクトを直接書き込む際のレイテンシが許容されません。したがって TSM サーバには、リムーバブルメディアが使用されるたびにアーカイブノードが最初にデータを保存する初期ストレージ用のディスクストレージプールを設定する必要があります。
- イベントベースの保持を使用するには、 TSM の保持ポリシーを設定する必要があります。アーカイブノードでは、作成ベースの TSM 保持ポリシーはサポートされません。保持ポリシーでは、推奨設定である retmin=0 および retver=0 （アーカイブノードが保持イベントをトリガーしたときに保持が開始され、その後 0 日間保持される）を使用してください。ただし、これらの retmin 値および retver 値はオプションです。

ディスクプールは、テーププールにデータを移行するように設定する必要があります（つまり、テーププールをディスクプールの NXTSTGPOOL に設定します）。テーププールは、両方のプールに同時に書き込むディスクプールのコピープールとしては設定しないでください（つまり、テーププールをディスクプールの COPYSTGPOOL にすることはできません）。アーカイブノードデータを含むテープのオフラインコピーを作成するには、 TSM サーバの 2 つ目のテーププールとして、アーカイブノードのデータ用に使用されるテーププールのコピープールを設定します。

アーカイブノードのセットアップを完了します

インストールプロセスを完了した時点ではアーカイブノードは機能していません。StorageGRID システムが TSM アーカイブノードにオブジェクトを保存できるようにするには、 TSM サーバのインストールと設定を完了し、 TSM サーバと通信するようにアーカイブノードを設定する必要があります。

TSMの読み出しおよび格納セッションを最適化する方法については、アーカイブストレージの管理に関する情報を参照してください。

- "アーカイブノードの管理"

必要に応じて次の IBM のドキュメントを参照し、 StorageGRID システムでアーカイブノードと TSM サーバを統合する準備をしてください。

- "『 IBM Tape Device Drivers Installation and User's Guide 』（ IBM テープデバイスドライバインストールおよびユーザーズガイド）"
- "IBM Tape Device Drivers Programming Reference"

新しい**TSM**サーバをインストールしています

アーカイブノードを新規または既存の TSM サーバと統合できます。新しい TSM サーバをインストールする場合は、 TSM のドキュメントの指示に従ってインストールを完了してください。

アーカイブノードを TSM サーバと同じマシンでホストすることはできません。

**TSM**サーバの設定

## このセクションでは、 TSM のベストプラクティスに従って TSM サーバを準備する手順を記載します。

次の手順では、のプロセスについて説明します。

- TSM サーバ上でディスクストレージプール、およびテープストレージプール（必要な場合）を定義します
- アーカイブノードから保存されたデータ用に TSM 管理クラスを使用するドメインポリシーを定義し、そのドメインポリシーを使用するようにノードを登録します

これらの手順はあくまで参考であり、 TSM のドキュメントに代わるものでも、すべての構成に適した完全な手順がすべて記載されているわけでもありません。環境に固有の手順は、詳細な要件を把握し、 TSM サーバのすべてのドキュメントに精通している TSM 管理者に確認する必要があります。

**TSM**テープストレージプールとディスクストレージプールを定義する

## アーカイブノードはディスクストレージプールに書き込みます。コンテンツをテープにアーカイブするには、コンテンツをテープストレージプールに移動するようにディスクストレージプールを設定する必要があります。

このタスクについて

1 台の TSM サーバに対し、 Tivoli Storage Manager でテープストレージプールとディスクストレージプールを定義する必要があります。ディスクプールを定義したら、ディスクボリュームを作成してディスクプールに割り当てます。TSM サーバでディスクのみのストレージを使用する場合、テーププールは必要ありません。

テープストレージプールを作成する前に、 TSM サーバでいくつかの手順を完了しておく必要があります。（テープライブラリを作成し、テープライブラリにドライブを少なくとも 1 本作成します。サーバからライブラリへのパスとサーバからドライブへのパスを定義し、ドライブのデバイスクラスを定義します）。 これらの手順の詳細は、サイトのハードウェア構成とストレージ要件によって異なります。詳細については、 TSM のドキュメントを参照してください。

以下に、このプロセスの手順を示します。サイトの要件は導入の要件によって異なることに注意してください。設定の詳細および手順については、 TSM のドキュメントを参照してください。

以下のコマンドを実行するには、管理者権限を使用してサーバにログオンし、 dsmadmc ツールを使用する必要があります。

手順

1. テープライブラリを作成します。

   ```
   define library tapelibrary libtype=scsi
   ```

   ここで *tapelibrary* はテープライブラリの任意の名前で、の値です `libtype` テープライブラリのタイプによって異なる場合があります。

2. サーバからテープライブラリへのパスを定義します。

   ```
   define path servername tapelibrary srctype=server desttype=library device=lib-devicename
   ```

   - *servername* はTSMサーバの名前です
   - *tapelibrary* は、定義したテープライブラリの名前です
   - *lib-devicename* は、テープライブラリのデバイス名です

3. ライブラリのドライブを定義します。

   ```
   define drive tapelibrary drivename
   ```

   - *drivename* は、ドライブに指定する名前です
   - *tapelibrary* は、定義したテープライブラリの名前です

     ハードウェア構成によっては、追加のドライブを設定することが必要になる場合があります。（たとえば、 1 つのテープライブラリからの入力が 2 つあるファイバチャネルスイッチに TSM サーバが接続されている場合は、入力ごとにドライブを定義します）。

4. サーバから定義したドライブへのパスを定義します。

   ```
   define path servername drivename srctype=server desttype=drive
   library=tapelibrary device=drive-dname
   ```

   - *drive-dname* は、ドライブのデバイス名です
   - *tapelibrary* は、定義したテープライブラリの名前です

     テープライブラリ用に定義したドライブごとに、別のを使用してこの手順を繰り返します *drivename* および *drive-dname* をクリックします。

5. ドライブのデバイスクラスを定義します。

   ```
   define devclass DeviceClassName devtype=lto library=tapelibrary
   format=tapetype
   ```

   - *DeviceClassName* は、デバイスクラスの名前です
   - *lto* は、サーバに接続されているドライブのタイプです
   - *tapelibrary* は、定義したテープライブラリの名前です
   - *tapetype* は、テープのタイプです。たとえば、ultrium3です

6. ライブラリのインベントリにテープボリュームを追加します。

   ```
   checkin libvolume tapelibrary
   ```

   *tapelibrary* は、定義したテープライブラリの名前です。

7. プライマリテープストレージプールを作成します。

```
define stgpool SGWSTapePool DeviceClassName description=description
collocate=filespace maxscratch=XX
```

- *SGWSTapePool* はアーカイブノードのテープストレージプールの名前です。テープストレージプールには（ TSM サーバが想定する命名規則に沿ってさえいれば）任意の名前を選択できます。
- *DeviceClassName* は、テープライブラリのデバイスクラス名です。
- *description* はストレージプールの概要 で、を使用してTSMサーバに表示できます `query stgpool` コマンドを実行しますたとえば ' アーカイブ・ノード用のテープ・ストレージ・プールなどです
- *collocate=filespace* は、TSMサーバが同じファイルスペースのオブジェクトを1つのテープに書き込む必要があることを指定します。
- XX は次のいずれかです。
  - テープライブラリ内の空のテープの数（アーカイブノードだけがライブラリを使用している場合）。
  - StorageGRID システム用に割り当てられているテープの数（テープライブラリが共有されている場合）。

8. TSM サーバで、ディスクストレージプールを作成します。TSM サーバの管理コンソールで、と入力します

```
define stgpool SGWSDiskPool disk description=description
maxsize=maximum_file_size nextstgpool=SGWSTapePool highmig=percent_high
lowmig=percent_low
```

- *SGWSDiskPool* はアーカイブノードのディスクプールの名前です。ディスクストレージプールには（ TSM が想定する命名規則に沿ってさえいれば）任意の名前を選択できます。
- *description* はストレージプールの概要 で、を使用してTSMサーバに表示できます `query stgpool` コマンドを実行しますたとえば ' アーカイブ・ノード用のディスク・ストレージ・プールなどです
- *maximum_file_size* ディスクプールにキャッシュされるのではなく、このサイズよりも大きいオブジェクトをテープに直接書き込みます。を設定することを推奨します *maximum_file_size* を10 GBに設定します。
- *nextstgpool=SGWSTapePool* は、ディスクストレージプールをアーカイブノード用に定義したテープストレージプールと関連付けます。
- *percent_high* ディスクプールの内容のテーププールへの移行を開始する値を設定します。を設定することを推奨します *percent_high* を0に設定すると、データがすぐに移行されます
- *percent_low* テープ・プールへの移行を停止する値を設定します。を設定することを推奨します *percent_low* を0に設定して、ディスクプールをクリアします。

9. TSM サーバで、 1 つ以上のディスクボリュームを作成してディスクプールに割り当てます。

```
define volume SGWSDiskPool volume_name formatsize=size
```

- *SGWSDiskPool* はディスクプール名です。
- *volume_name* はボリュームの完全パスです（例： `/var/local/arc/stage6.dsm`）をテープに転送する準備として、TSMサーバ上でディスクプールの内容を書き込みます。
- *size* は、ディスクボリュームのサイズ（MB単位）です。

たとえば、テープボリュームの容量が 200GB の場合、ディスクプールのコンテンツで 1 つのテープを使い切るようなディスクボリュームを 1 個作成するには、 size の値を 200000 に設定します。

ただし、 TSM サーバがディスクプール内の各ボリュームに書き込むことができるため、小さいサイズのディスクボリュームを複数作成する方がよい場合もあります。たとえばテープサイズが 250GB の場合、 10GB （ 10000 ）のディスクボリュームを 25 個作成します。

TSM サーバは、ディスクボリューム用にディレクトリ内のスペースを事前に割り当てます。この処理には、完了までに時間がかかることがあります（ 200GB のディスクボリュームの場合は 3 時間以上）。

ドメインポリシーの定義とノードの登録

## アーカイブノードから保存されたデータ用に TSM 管理クラスを使用するドメインポリシーを定義し、そのドメインポリシーを使用するようにノードを登録する必要があります。

Tivoli Storage Manager （ TSM ）でアーカイブノードのクライアントパスワードの期限が切れると、アーカイブノードのプロセスでメモリリークが発生する可能性があります。アーカイブノードのクライアントユーザ名 / パスワードの期限が切れないように TSM サーバを設定してください。

アーカイブノードとして使用するノードを TSM サーバに登録する（または既存のノードを更新する）場合は、そのノードが書き込み処理に使用できるマウントポイントの数を指定する必要があります。そのためには、 REGISTER NODE コマンドで MAXNUMMP パラメータを指定します。通常、マウントポイントの数は、アーカイブノードに割り当てられているテープドライブのヘッド数と同じです。TSM サーバの MAXNUMMP に指定する数は、アーカイブノードの *ARC * > * Target * > * Configuration * > * Main * > * Maximum Store Sessions * に設定された値以上である必要があります 同時ストアセッション数はアーカイブノードでサポートされないため、値は 0 または 1 に設定されます。

TSM サーバ用に設定した MAXSESSIONS の値によって、すべてのクライアントアプリケーションが TSM サーバに対して開くことのできる最大セッション数が制御されます。TSM で指定する MAXSESSIONS の値は、アーカイブノードの Grid Manager で * ARC * > * Target * > * Configuration * > * Main * > * Sessions * に指定されている値以上である必要があります。アーカイブノードは、最大でマウントポイントごとに 1 つのセッションと少数（ 5 つ未満）の追加セッションを同時に作成します。

アーカイブノードに割り当てられているTSMノードは、カスタムドメインポリシーを使用します `tsm-domain`。。 `tsm-domain` ドメイン・ポリシーは'標準ドメイン・ポリシーの変更バージョンであり'テープに書き込むように構成され'アーカイブ先がStorageGRID システムのストレージ・プールに設定されています（*`SGWSDiskPool`*）。

ドメインポリシーを作成およびアクティブ化するには、管理者権限を使用して TSM サーバにログインし、 dsmadmc ツールを使用する必要があります。

ドメインポリシーを作成してアクティブ化します

## アーカイブノードから送信されたデータを保存するように TSM サーバを設定するには、ドメインポリシーを作成してアクティブ化する必要があります。

手順

1. ドメインポリシーを作成します。

```
copy domain standard tsm-domain
```

2. 既存の管理クラスを使用しない場合は、次のいずれかを入力します。

```
define policyset tsm-domain standard

define mgmtclass tsm-domain standard default
```

*default* は、導入用のデフォルトの管理クラスです。

3. 適切なストレージプールにコピーグループを作成します。（ 1 行に）次のように入力します。

```
define copygroup tsm-domain standard default type=archive
destination=SGWSDiskPool retinit=event retmin=0 retver=0
```

*default* は、アーカイブノードのデフォルトの管理クラスです。の値 `retinit`、 `retmin`および `retver` アーカイブノードで現在使用されている保持動作を反映するように選択されています

> 設定しないでください `retinit` 終了： `retinit=create`。設定 `retinit=create` 保持イベントを使用してTSMサーバからコンテンツが削除されるため、アーカイブノードからコンテンツが削除されないようにします。

4. 管理クラスをデフォルトに割り当てます。

```
assign defmgmtclass tsm-domain standard default
```

5. 新しいポリシーセットをアクティブに設定します。

```
activate policyset tsm-domain standard
```

activate コマンドを入力したときに表示される「 no backup copy group 」警告は無視してください。

6. 新しいポリシーセットを使用するノードを TSM サーバに登録します。TSM サーバで、次のように（ 1 行に）入力します。

```
register node arc-user arc-password passexp=0 domain=tsm-domain
MAXNUMMP=number-of-sessions
```

aarc-user と arc-password は、アーカイブノードで定義したクライアントノード名とパスワードです。また、 MAXNUMMP の値は、アーカイブノードの格納セッション用に予約されているテープドライブの数に設定されます。

> デフォルトでは、ノードを登録すると、管理ユーザ ID がクライアント所有者の権限で作成され、パスワードが定義されます。

## StorageGRID へのデータの移行

日常業務に StorageGRID システムを使用しながら、同時に StorageGRID システムに大量のデータを移行できます。

次のセクションでは、 StorageGRID システムへの大量のデータ移行について、その概要と計画方法を説明します。データ移行の一般的なガイドではなく、移行を実行するための詳細な手順も記載されていません。このセクションのガイドラインと手順に従って、日常業務を中断せずに StorageGRID システムにデータを効率的に移行し、移行したデータが StorageGRID システムによって適切に処理されるようにしてください。

- "StorageGRID システムの容量の確認"
- "移行データのILMポリシーの決定"
- "移行が処理に及ぼす影響"
- "データ移行のスケジュール設定"
- "データ移行の監視"
- "移行アラーム用のカスタム通知の作成"

**StorageGRID** システムの容量の確認

## StorageGRID システムに大量のデータを移行する前に、予想されるボリュームを処理できるディスク容量が StorageGRID システムにあることを確認します。

StorageGRID システムにアーカイブノードが含まれていて、移行するオブジェクトのコピーをニアラインストレージ（テープなど）に保存する場合は、アーカイブノードのストレージに予想される移行量に対応する十分な容量があることを確認します。

容量評価の一環として、移行を計画しているオブジェクトのデータプロファイルを確認し、必要なディスク容量を計算します。StorageGRID システムのディスク容量の監視に関する詳細については、StorageGRID の監視とトラブルシューティングの手順を参照してください。

関連情報

"トラブルシューティングを監視します"

"ストレージノードの管理"

移行データの**ILM**ポリシーの決定

## StorageGRID システムの ILM ポリシーは、作成されるコピーの数とその格納先、および保持期間を決定します。ILM ポリシーは、オブジェクトをフィルタリングする方法、および一定の期間にわたってオブジェクトデータを管理する方法を記述した一連の ILM ルールで構成されます。

移行データの使用方法およびその要件によっては、日常業務に使用する ILM ルールとは別の、移行データに固有の ILM ルールを定義することができます。たとえば、日常的なデータ管理と移行対象のデータに異なる規制要件が適用される場合、異なるグレードのストレージに異なる数の移行データのコピーが必要となる可能性があります。

移行データと日常業務で保存されるオブジェクトデータを一意に区別できる場合は、移行データにのみ適用されるルールを設定できます。

いずれかのメタデータ条件を使用してデータのタイプを確実に識別できる場合は、この条件を使用して移行データにのみ適用される ILM ルールを定義できます。

データ移行を開始する前に、 StorageGRID システムの ILM ポリシーとそのポリシーが移行データにどのよう

に適用されるかを確認し、 ILM ポリシーへの変更があればテストしておく必要があります。

> ILM ポリシーが正しく指定されていないと、原因 によるリカバリ不能なデータ損失が発生する可能性があります。ポリシーを想定どおりに機能させるには、 ILM ポリシーをアクティブ化する前に、 ILM ポリシーに加えたすべての変更をよく確認してください。

関連情報

"ILM を使用してオブジェクトを管理する"

移行が処理に及ぼす影響

## StorageGRID システムは、オブジェクトを効率的に格納して読み出せるようにすること、およびオブジェクトデータとメタデータの冗長コピーをシームレスに作成することでデータ損失に対する優れた保護を提供することを目的に設計されています。

ただし、日常的なシステム運用に影響が及ばないように、または極端なケースでは StorageGRID システムに障害が発生してデータが失われないように、この章の手順に従ってデータ移行を慎重に管理する必要があります。

大量のデータを移行すると、システムに新たな負荷がかかります。StorageGRID システムの負荷が高い場合は、オブジェクトの格納および読み出し要求への応答が遅くなります。その結果、日常業務に不可欠な格納および読み出し要求が影響を受ける可能性があります。移行は、原因 のその他の運用上の問題にもなります。たとえば、ストレージノードの容量が上限に近づい原因 ている場合は、一括取り込みによって断続的に大きな負荷がかかると、ストレージノードが読み取り専用と読み書き可能の間で何度も切り替わり、そのたびに通知が生成されます。

負荷の高い状態が続く場合、オブジェクトデータとメタデータの完全な冗長性を確保するために StorageGRID システムが実行する必要のあるさまざまな処理がキューに溜まっていきます。

移行中に StorageGRID システムを安全かつ効率的に運用するためには、本書のガイドラインに従ってデータ移行を慎重に管理する必要があります。データの移行にあたっては、オブジェクトを複数のバッチで取り込むか、または取り込み量を常に調整します。そのうえで、 StorageGRID システムを常時監視し、さまざまな属性値が超えようにします。

データ移行のスケジュール設定

## 主要な業務時間中はデータを移行しないでください。データの移行は、夕方や週末など、システムの使用率が低い時間帯にのみ実施してください。

アクティビティが高い期間には、できるだけデータ移行をスケジュールしないでください。ただし、アクティビティレベルが高い期間を完全に回避することが現実的でない場合はそのまま進めてかまいません。その場合は、関連する属性を注意深く監視し、許容値を超えた場合に対処する必要があります。

関連情報

"データ移行の監視"

データ移行の監視

## 所定の期間内にILMポリシーに従ってデータが配置されるよう、必要に応じてデータ移行を監視し、調整する必要があります。

次の表に、データ移行中に監視する必要がある属性とその内容を示します。

取り込み速度を抑制するためにレート制限を指定したトラフィック分類ポリシーを使用する場合は、次の表に示す統計情報とともに、観察されたレートを監視し、必要に応じて制限を減らすことができます。

| モニタ | 説明 |
| --- | --- |
| ILM による評価を待機しているオブジェクトの数 | 1. Support **>** Tools **>** Grid Topology *を選択します。<br>2. [***deployment***概要***Main***]を選択します。<br>3. ILM アクティビティセクションで、次の属性について表示されるオブジェクトの数を監視します。<br>◦ * Awaiting - All （ XQUZ ） * ： ILM による評価を待機しているオブジェクトの合計数です。<br>◦ * Awaiting - Client （ XCQZ ） * ：クライアント処理（取り込みなど）から ILM による評価を待機しているオブジェクトの合計数です。<br>4. これらの属性のどちらかに対して表示されるオブジェクトの数が 100 、 000 を超えた場合は、オブジェクトの取り込み速度を調整して、 StorageGRID システムへの負荷を軽減してください。 |
| ターゲットアーカイブシステムのストレージ容量 | ILM ポリシーによって、移行対象データのコピーがターゲットアーカイブストレージシステム（テープまたはクラウド）に保存される場合は、ターゲットアーカイブストレージシステムの容量を監視して、移行対象データ用の十分な容量が確保されていることを確認してください。 |
| アーカイブノード ARC * Store * | 「 Store Failures （ ARVF ） * 」属性のアラームがトリガーされた場合、対象のアーカイブストレージシステムの容量が上限に達している可能性があります。ターゲットアーカイブストレージシステムをチェックして、アラームをトリガーした問題を解決してください。 |

移行アラーム用のカスタム通知の作成

## StorageGRID では、特定の値が推奨されるしきい値を超えた場合に移行を監視するシステム管理者にアラート通知またはアラーム（従来のシステム）通知を送信することができます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- アラート（またはアラーム）通知のEメールを設定しておく必要があります。

手順

1. データ移行中に監視するPrometheusの指標またはStorageGRID 属性ごとに、カスタムのアラートルールまたはグローバルカスタムアラームを作成します。

   アラートはPrometheusの指標値に基づいてトリガーされます。属性値に基づいてアラームがトリガーさ

れます。詳細については、StorageGRID の監視とトラブルシューティングの手順を参照してください。

2. データ移行が完了したら、カスタムのアラートルールまたはグローバルカスタムアラームを無効にします。

   グローバルカスタムアラームはデフォルトアラームを上書きします。

関連情報

"トラブルシューティングを監視します"

# ILM を使用してオブジェクトを管理する

情報ライフサイクルルールとポリシーを使用してオブジェクトを管理する方法、およびS3オブジェクトロックを使用してオブジェクト保持に関する規制に準拠する方法について説明します。

- "情報ライフサイクル管理によるオブジェクトの管理"
- "S3オブジェクトロックでオブジェクトを管理する"
- "ILM ルールとポリシーの例"

## 情報ライフサイクル管理によるオブジェクトの管理

StorageGRID システムのオブジェクトを管理するには、情報ライフサイクル管理（ ILM ）ルールとポリシーを設定します。ILM ルールとポリシーは、オブジェクトデータのコピーを作成して分散し、一定の期間にわたって管理する方法を StorageGRID に指示します。

ILM ルールと ILM ポリシーを設計して実装するには、慎重な計画が必要です。運用要件、 StorageGRID システムのトポロジ、オブジェクト保護のニーズ、使用可能なストレージタイプについて理解しておく必要があります。次に、さまざまなタイプのオブジェクトをどのようにコピー、分散、および格納するかを決定する必要があります。

- "オブジェクトのライフサイクル全体にわたる ILM の動作"
- "ILM ポリシーとは"
- "ILM ルールとは"
- "ストレージグレード、ストレージプール、ECプロファイル、リージョンを作成する"
- "ILMルールを作成する"
- "ILMポリシーを作成する"
- "ILMルールおよびILMポリシーの操作"

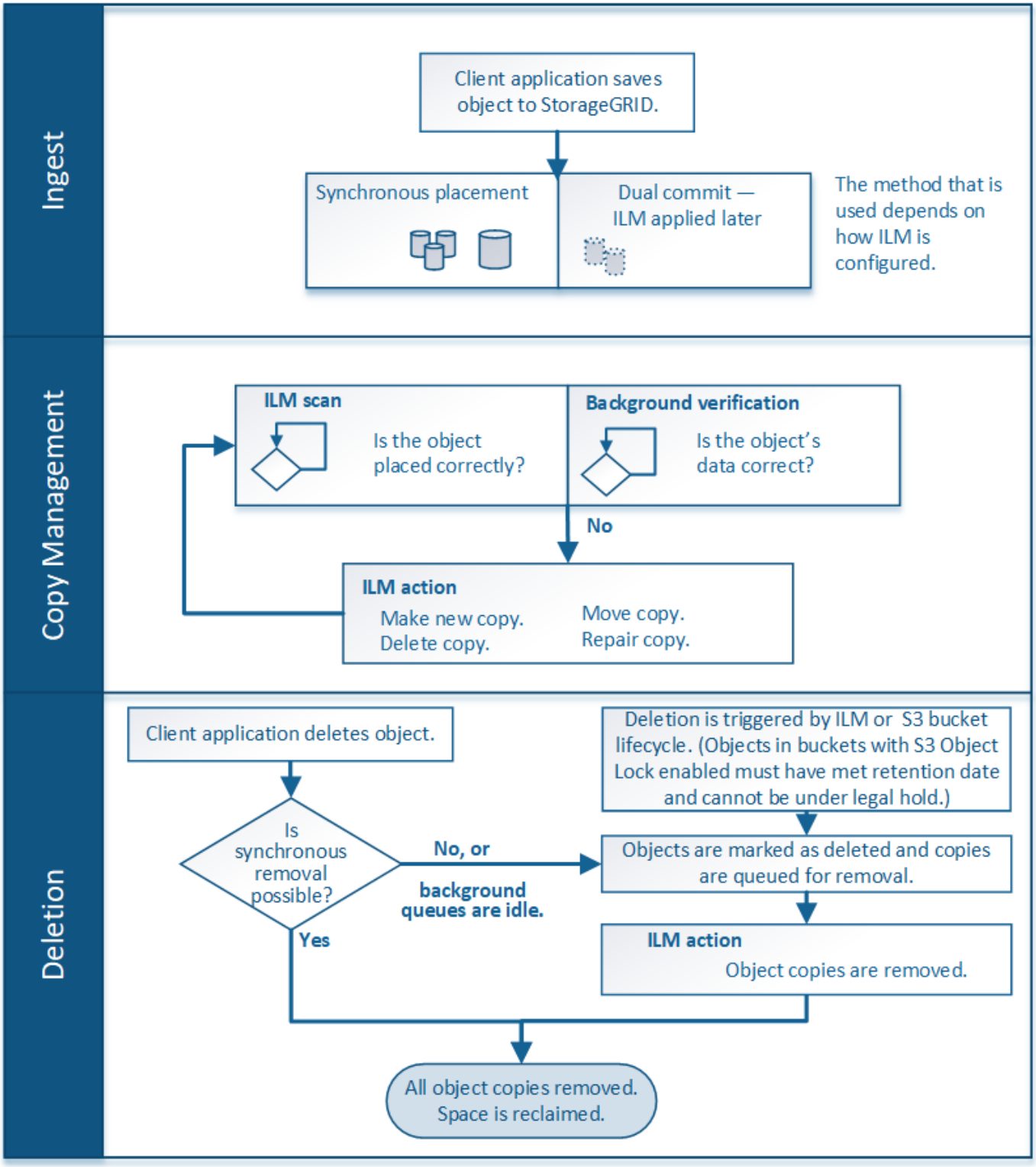
### オブジェクトのライフサイクル全体にわたる **ILM** の動作

StorageGRID での ILM を使用したオブジェクト管理方法を理解することは、ポリシーをより効果的に設計するうえで役立ちます。

- * 取り込み： S3 または Swift クライアントアプリケーションが StorageGRID システムへの接続を確立してオブジェクトを保存すると取り込みが開始され、 StorageGRID がクライアントに「 ingest successful 」メッセージを返すと取り込みが完了します。ILM 要件の指定方法に応じて、 ILM の手順を即座に適用（同期配置）するか、中間コピーを作成して ILM をあとから適用（デュアルコミット）することで、オブジェクトデータは取り込み時に保護されます。
- * コピー管理 * ： ILM の配置手順に指定された数とタイプのオブジェクトコピーを作成すると、 StorageGRID はオブジェクトの場所を管理し、オブジェクトを損失から保護します。
  - ILM のスキャンと評価： StorageGRID は、グリッドに格納されているオブジェクトのリストを継続的にスキャンし、現在のコピーが ILM 要件を満たしているかどうかを確認します。タイプ、数、または場所が異なるオブジェクトコピーが必要となった場合、 StorageGRID は必要に応じてコピーを作成、削除、または移動します。
  - バックグラウンド検証： StorageGRID は、バックグラウンド検証を継続的に実行して、オブジェクトデータの整合性をチェックします。問題が検出されると、 StorageGRID は、現在の ILM 要件を満たす場所に、新しいオブジェクトコピーまたは置き換え用のイレイジャーコーディングオブジェクトフラグメントを自動的に作成します。StorageGRID の監視とトラブルシューティングの手順を参照してください。
- * オブジェクトの削除 * ： StorageGRID システムからすべてのコピーが削除されると、オブジェクトの管理は終了します。オブジェクトは、クライアントによる削除要求、または S3 バケットライフサイクルの終了が原因の ILM による削除または削除が原因で削除されます。

> S3 オブジェクトロックが有効になっているバケット内のオブジェクトがリーガルホールドの対象である場合、または retain-until date が指定されていても未達成の場合、オブジェクトを削除することはできません。

次の図は、オブジェクトのライフサイクル全体にわたる ILM の動作をまとめたものです。




関連情報

"トラブルシューティングを監視します"

オブジェクトの取り込み方法

StorageGRID は、オブジェクトに一致するILMルールの指定に従って、同期配置またはデュアルコミットを実行し、取り込み時にオブジェクトを保護します。

S3またはSwiftクライアントがオブジェクトをグリッドに格納すると、次のどちらかの方法でStorageGRIDにオブジェクトが取り込まれます。

- 同期配置：StorageGRID は、ILM要件を満たすために必要なすべてのオブジェクトコピーをただちに作成します。すべてのコピーが作成されると、StorageGRID は「ingest successful」メッセージをクライアントに送信します。

  StorageGRID は、すべてのオブジェクトコピーをただちに作成できない場合（必要な場所が一時的に使用できない場合など）、クライアントに「ingest failed」というメッセージを送信します。または、ILMルールの作成時に選択した内容に応じて、中間オブジェクトコピーの作成とILMの評価を実行します。

- デュアル・コミット：StorageGRID は'それぞれ異なるストレージ・ノード上に'オブジェクトの中間コピーを2つ作成し'クライアントにingest successfulメッセージを送信します次に、StorageGRID はオブジェクトをILM評価のキューに登録します。

  StorageGRID によるILM評価では、中間コピーがILMルールの配置手順を満たしているかどうかが最初にチェックされます。たとえば、2つの中間コピーが2コピーのILMルールの手順を満たしていても、イレイジャーコーディングルールの手順を満たしていない場合があります。中間コピーがILMの手順を満たしていない場合、StorageGRID は新しいオブジェクトコピーを作成し、不要な中間コピーをすべて削除します。

  StorageGRID が中間コピーを2つ作成できない場合（ネットワーク問題 が2つ目のコピーを作成できない場合など）、StorageGRID は再試行しません。取り込みは失敗します。

> S3 / Swiftクライアントでは、を指定することで、StorageGRID が取り込み時に1つの中間コピーを作成するように指定できます `REDUCED_REDUNDANCY` ストレージクラス。詳細については、S3 / Swiftクライアントを実装する手順を参照してください。

デフォルトでは、StorageGRID は同期配置を使用して取り込み時にオブジェクトを保護します。

関連情報

"取り込みのデータ保護オプション"

"S3 を使用する"

"Swift を使用します"

取り込みのデータ保護オプション

ILM ルールを作成する際には、取り込み時にオブジェクトを保護するためのオプションとして、 Dual commit 、 Balanced 、または Strict のいずれかを指定します。選択したオプションに応じて、 StorageGRID は、中間コピーを作成してオブジェクトをキューに登録し、あとで ILM 評価を実行するか、または同期配置を使用してコピーをただちに作成して ILM 要件を満たします。

デュアルコミット

Dual commit オプションを選択すると、 StorageGRID は 2 つの異なるストレージノード上に中間オブジェクトコピーをただちに作成し、「 ingest successful 」メッセージをクライアントに返します。オブジェクトは ILM 評価のキューに登録され、ルールの配置手順を満たすコピーはあとで作成されます。

#### Dual commit オプションを使用する状況

次のいずれかの場合に Dual commit オプションを使用します。

- マルチサイトの ILM ルールを使用しており、クライアントの取り込みレイテンシを考慮する必要があります。Dual commit を使用する場合は、 ILM を満たしていないデュアルコミットコピーの作成と削除の作業をグリッドで確実に実行できるようにする必要があります。具体的には、
  - ILM のバックログが発生しないように、グリッドの負荷が十分に低い必要があります。
  - グリッドにハードウェアリソース（ IOPS 、 CPU 、メモリ、ネットワーク帯域幅など）が余剰である。
- マルチサイトの ILM ルールを使用していて、通常はサイト間の WAN 接続のレイテンシが高くなっているか、帯域幅が制限されている。このシナリオでは、 Dual commit オプションを使用するとクライアントのタイムアウトを回避できます。Dual commit オプションを選択する前に、現実的なワークロードでクライアントアプリケーションをテストする必要があります。

#### strict

Strict オプションを選択すると、 StorageGRID は取り込み時に同期配置を使用してルールの配置手順で指定されたすべてのオブジェクトコピーをただちに作成します。必要なストレージの場所が一時的に使用できないなどの理由で、 StorageGRID がすべてのコピーを作成できない場合は、取り込みが失敗します。クライアントは処理を再試行する必要があります。

#### Strict オプションを使用する場合

Strict オプションは、 ILM ルールに指定された場所にのみオブジェクトをただちに格納するための運用または規制上の要件がある場合に使用してください。たとえば、規制要件を満たすために、 Strict オプションと Location Constraint 高度なフィルタを使用して、オブジェクトが特定のデータセンターに格納されないようにする必要があります。

"例 5 ：取り込み動作が Strict の場合の ILM ルールとポリシー"

#### 中間（ Balanced ）

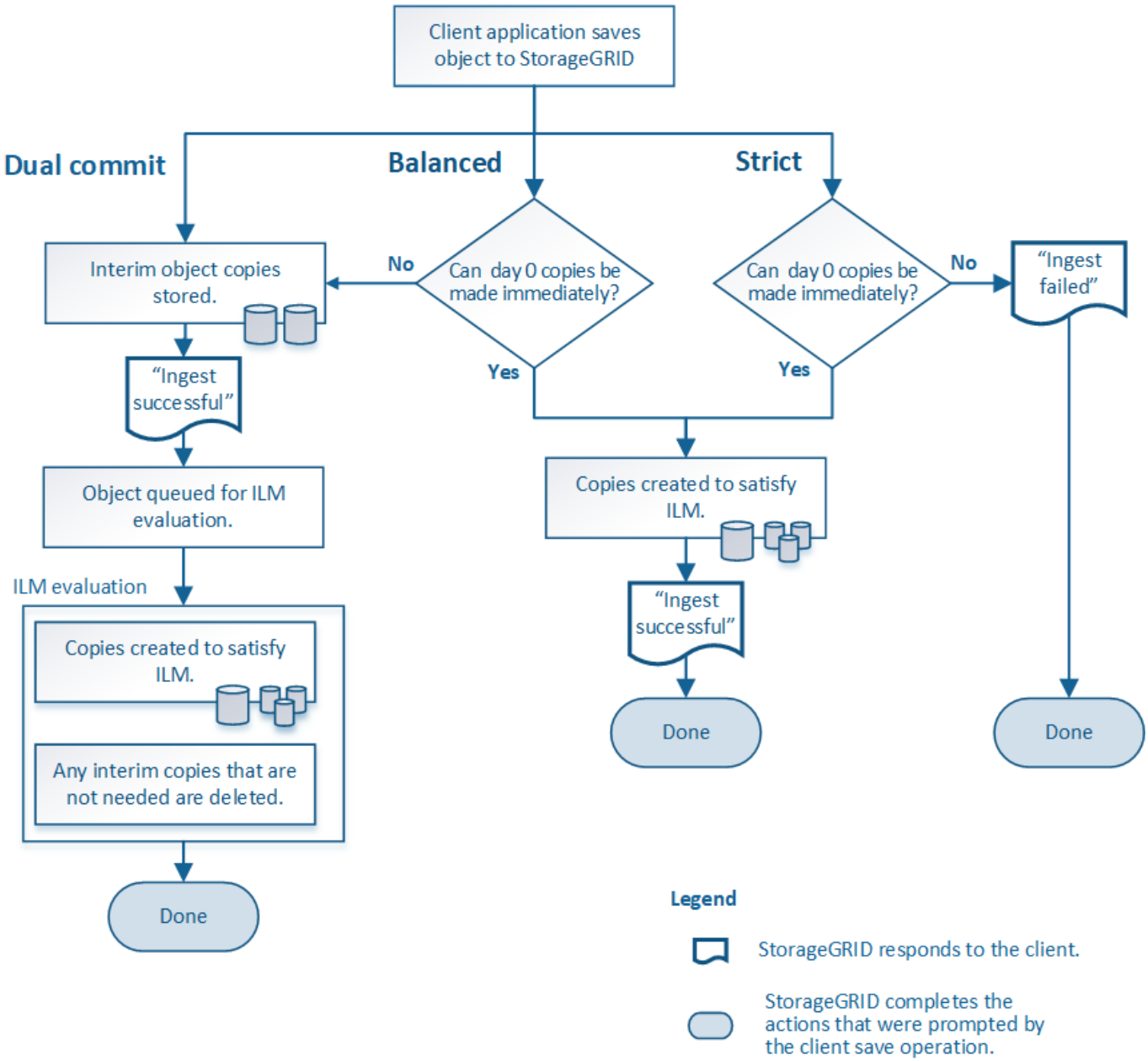
Balanced オプションを選択した場合も、 StorageGRID は、取り込み時に同期配置を使用してルールの配置手順で指定されたすべてのコピーをただちに作成します。Strict オプションと違い、 StorageGRID がすべてのコピーをただちに作成できない場合は、代わりに Dual commit を使用します。

#### Balanced オプションを使用する状況

Balanced オプションは、データ保護、グリッドパフォーマンス、および取り込みの成功の最適な組み合わせを実現するために使用します。Balanced は、 ILM ルールウィザードのデフォルトオプションです。

#### 3 つの取り込みオプションのフローチャート

フローチャートは、次のいずれかの取り込みオプションを使用するILMルールにオブジェクトが一致した場合の動作を示しています。




関連情報

"オブジェクトの取り込み方法"

データ保護オプションのメリット、デメリット、および制限事項

取り込み時にデータを保護するための 3 つのオプション（ Balanced 、 Strict 、 Dual commit ）のそれぞれのメリットとデメリットを理解することは、 ILM ルールに選択するオプションを決定する際に役立ちます。

**Balanced** オプションと **Strict** オプションのメリット

取り込み時に中間コピーを作成する Dual commit と比較すると、 2 つの同期配置オプションには次のメリットがあります。

- * Better データ セキュリティ * ：オブジェクトデータは、 ILM ルールの配置手順に従ってただちに保護さ

れます。配置手順は、複数の格納場所の障害など、さまざまな障害状況からオブジェクトを保護するように設定できます。Dual commit で保護できるのは、単一のローカルコピーの損失のみです。

- * グリッド処理の効率化 * ：各オブジェクトは、取り込み時に 1 回だけ処理されます。StorageGRID システムで中間コピーを追跡または削除する必要がないため、処理の負荷が軽減され、消費されるデータベーススペースも少なくてすみます。
- * （ Balanced ） Recommended * ： Balanced オプションは、最適な ILM 効率を実現します。Strict 取り込み動作が必要であるか、グリッドが Dual commit に使用するためのすべての条件を満たしていないかぎり、 Balanced オプションを使用することを推奨します。
- * （ Strict ）オブジェクトの場所が明らか * ： Strict オプションは、 ILM ルールの配置手順に従ってオブジェクトがただちに格納されることを保証します。

**Balanced** オプションと **Strict** オプションのデメリット

Dual commit と比較すると、 Balanced オプションと Strict オプションにはいくつかのデメリットがあります。

- * クライアントの取り込み時間が長くなる * ：クライアントの取り込みレイテンシが長くなる可能性があります。Balanced オプションと Strict オプションを使用する場合、すべてのイレイジャーコーディングフラグメントまたはレプリケートコピーが作成されて格納されるまで、「 ingest successful 」メッセージはクライアントに返されません。しかし、ほとんどの場合、オブジェクトデータは最終的な配置までの時間をはるかに短縮できます。
- * （ Strict ）取り込みエラーの増加 * ： Strict オプションでは、 StorageGRID が ILM ルールに指定されたすべてのコピーをただちに作成できないと取り込みが失敗します。必要なストレージの場所が一時的にオフラインになっている場合や、ネットワークでサイト間のオブジェクトコピーが原因 で遅延している場合には、取り込みに失敗する可能性が高くなります。
- * （ Strict ） S3 マルチパートアップロードでは、状況によっては想定どおりに配置されない可能性がある * ： Strict では、オブジェクトが ILM ルールの指定どおりに配置されるか、あるいは取り込みが失敗するかのどちらかの結果が想定されます。ところが、 S3 マルチパートアップロードの場合、オブジェクトの各パートの取り込み時に ILM が評価され、マルチパートアップロードが完了した時点でオブジェクト全体に対して ILM が評価されます。そのため、次の状況では想定どおりに配置されないことがあります。
  - * S3 マルチパートアップロードの実行中に ILM が変更された場合 * ：各パートはその取り込み時にアクティブなルールに従って配置されるため、マルチパートアップロードが完了した時点でオブジェクトの一部のパートが現在の ILM 要件を満たしていない可能性があります。この場合、オブジェクトの取り込みは失敗しません。代わりに、正しく配置されていないパートは ILM ルールによる再評価の対象としてキューに登録され、あとで正しい場所に移動されます。
  - * ILM ルールがサイズでフィルタリングする場合 * ：パーツに対して ILM を評価する際、 StorageGRID はオブジェクトのサイズではなくパーツのサイズでフィルタリングします。つまり、オブジェクト全体としては ILM 要件を満たしていない場所にオブジェクトのパーツが格納される可能性があります。たとえば、 10GB 以上のオブジェクトをすべて DC1 に格納し、それより小さいオブジェクトをすべて DC2 に格納するルールの場合、 10 パートからなるマルチパートアップロードの 1GB の各パートは取り込み時に DC2 に格納されます。オブジェクトに対して ILM が評価されると、オブジェクトのすべてのパートが DC1 に移動されます。
- * （ Strict ）オブジェクトタグまたはメタデータが更新され、新たに必要となった配置を実行できなくても取り込みが失敗しない * ： Strict では、オブジェクトが ILM ルールの指定どおりに配置されるか、あるいは取り込みが失敗するかのどちらかの結果が想定されます。ただし、グリッドにすでに格納されているオブジェクトのメタデータまたはタグを更新しても、オブジェクトは再取り込みされません。そのため、更新によってトリガーされるオブジェクト配置の変更は、すぐには実行されず、通常のバックグラウンド ILM プロセスで ILM が再評価されると、配置変更が行われます。必要な配置変更を行えない場合（新たに必要となった場所が使用できない場合など）は、更新されたオブジェクトは配置変更が可能になるまで現在の場所に残ります。

### Balanced オプションと Strict オプションを使用したオブジェクトの配置に関する制限事項

次のいずれかの配置手順を含む ILM ルールには、 Balanced オプションまたは Strict オプションを使用できません。

- クラウドストレージプールへの配置： 0 日目
- アーカイブノードへの配置： 0 日目
- ルールの参照時間としてユーザ定義の作成時間が設定されている場合のクラウドストレージプールまたはアーカイブノードでの配置

StorageGRID ではクラウドストレージプールまたはアーカイブノードにコピーを同期的に作成できず、ユーザ定義の作成時間が現在の状態に解決される場合があるため、このような制限があります。

### ILM ルールと整合性制御がデータ保護に与える影響

ILM ルールと選択した整合性制御は、どちらもオブジェクトの保護方法に影響します。これらの設定は対話的に操作できます。

たとえば、 ILM ルールに対して選択した取り込み動作はオブジェクトコピーの初期配置に影響し、オブジェクトの格納時に使用される整合性制御はオブジェクトメタデータの初期配置に影響します。StorageGRID では、クライアント要求に対応するためにオブジェクトのメタデータとそのデータの両方にアクセスする必要があるため、整合性レベルと取り込み動作に一致する保護レベルを選択することで、より適切な初期データ保護と予測可能なシステム応答を実現できます。

StorageGRID で使用できる整合性制御の概要を以下に示します。

- * all * ：すべてのノードが即座にオブジェクトメタデータを受け取り、受け取れない場合は要求が失敗します。
- * strong-global * ：オブジェクトのメタデータがすべてのサイトにただちに分散されます。すべてのサイトのすべてのクライアント要求について、リードアフターライト整合性が保証されます。
- * strong-site * ：オブジェクトのメタデータがただちにサイトの他のノードに分散されます。1 つのサイト内のすべてのクライアント要求について、リードアフターライト整合性が保証されます。
- * read-after-new-write * ：新規オブジェクトについてはリードアフターライト整合性が提供され、オブジェクトの更新については結果整合性が提供されます。高可用性が確保され、データ保護が保証されます。
- * available * （ HEAD オペレーションについては結果整合性）：「 read-after-new-write 」整合性レベルと動作は同じですが、 HEAD オペレーションについては結果整合性のみを提供します。

> 整合性レベルを選択する前に、S3またはSwiftクライアントアプリケーションの作成手順の設定の完全な概要 を確認してください。デフォルト値を変更する前に、利点と制限事項を理解しておく必要があります。

### 整合性制御と ILM ルールの連動の例

次の ILM ルールと次の整合性レベル設定の 2 サイトグリッドがあるとします。

- * ILM ルール * ：ローカルサイトとリモートサイトに 1 つずつ、 2 つのオブジェクトコピーを作成します。Strict 取り込み動作が選択されています。
- * 整合性レベル *:"Strong-GLOBAL" ( オブジェクトメタデータはすべてのサイトにただちに分散されます )

クライアントがオブジェクトをグリッドに格納すると、 StorageGRID は両方のオブジェクトをコピーし、両方のサイトにメタデータを分散してからクライアントに成功を返します。

オブジェクトは、取り込みが成功したことを示すメッセージが表示された時点で損失から完全に保護されます。たとえば、取り込み直後にローカルサイトが失われた場合、オブジェクトデータとオブジェクトメタデータの両方のコピーがリモートサイトに残っています。オブジェクトを完全に読み出し可能にしている。

代わりに同じ ILM ルールと「 strong-site 」整合性レベルを使用する場合は、オブジェクトデータがリモートサイトにレプリケートされたあとで、オブジェクトメタデータがそこに分散される前に、クライアントに成功メッセージが送信される可能性があります。この場合、オブジェクトメタデータの保護レベルがオブジェクトデータの保護レベルと一致しません。取り込み直後にローカルサイトが失われると、オブジェクトメタデータが失われます。オブジェクトを読み出すことができません。

整合性レベルと ILM ルールの間の関係は複雑になる可能性があります。サポートが必要な場合は、ネットアップにお問い合わせください。

関連情報

"レプリケーションとは"

"イレイジャーコーディングとは"

"イレイジャーコーディングスキームとは"

"例 5 ：取り込み動作が Strict の場合の ILM ルールとポリシー"

"S3 を使用する"

"Swift を使用します"

オブジェクトの格納方法（レプリケーションまたはイレイジャーコーディング）

StorageGRID では、レプリケートコピーを格納するかイレイジャーコーディングコピーを格納することで、オブジェクトを損失から保護できます。作成するコピーのタイプは、ILMルールの配置手順で指定します。

- "レプリケーションとは"
- "シングルコピーレプリケーションを使用しない理由"
- "イレイジャーコーディングとは"
- "イレイジャーコーディングスキームとは"
- "イレイジャーコーディングのメリット、デメリット、および要件"

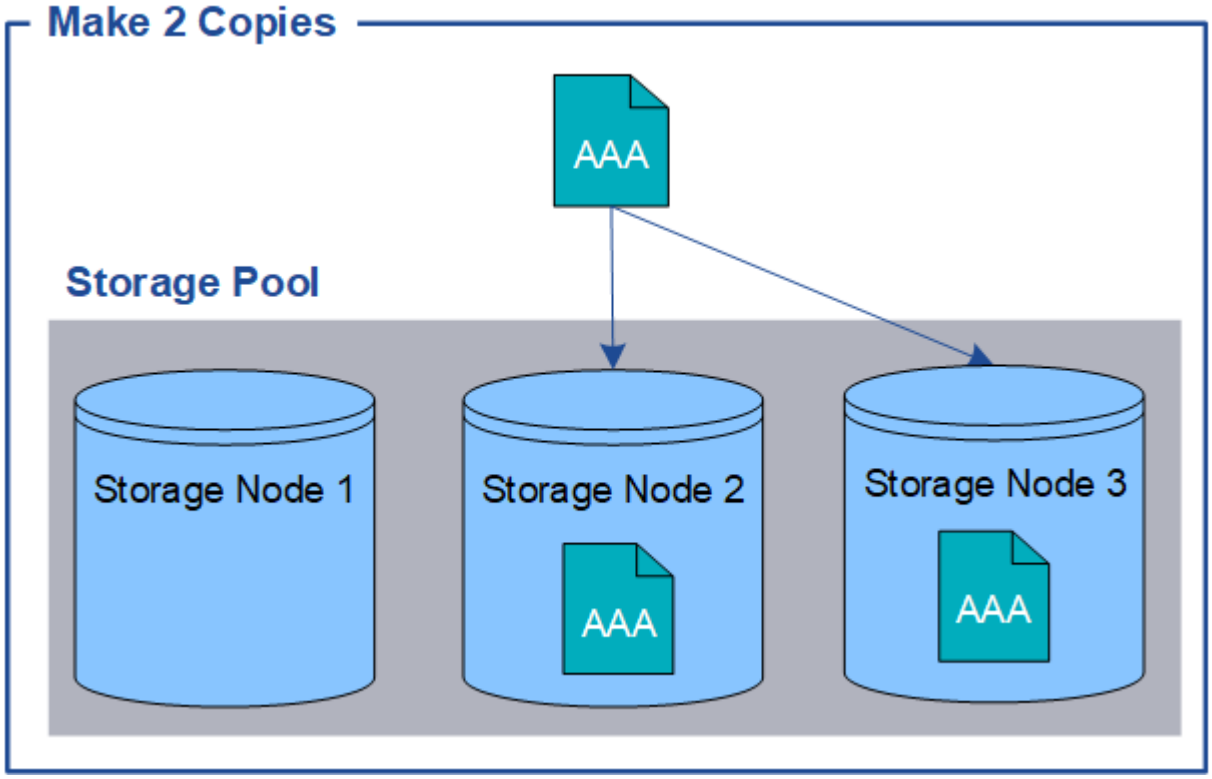
レプリケーションとは

レプリケーションは、 StorageGRID がオブジェクトデータを格納するために使用する 2 つの方法のうちの 1 つです。レプリケーションを使用する ILM ルールにオブジェクトが一致すると、オブジェクトデータの完全なコピーが作成され、ストレージノードまたはアーカイブノードに格納されます。

レプリケートコピーを作成するように ILM ルールを設定する場合は、作成するコピーの数、コピーを配置す

る場所、およびそれぞれの場所にコピーを格納する期間を指定します。

次の例の ILM ルールは、各オブジェクトのレプリケートコピーを 2 つずつ、 3 つのストレージノードからなるストレージプールに配置するように指定されています。




このルールにオブジェクトが一致した場合、 StorageGRID はオブジェクトのコピーを 2 つ作成して、ストレージプール内の別々のストレージノードにそれぞれのコピーを配置します。この 2 つのコピーは、使用可能な 3 つのストレージノードのうちのいずれか 2 つに配置されます。この場合、ストレージノード 2 と 3 に配置されています。コピーは 2 つあるため、ストレージプール内のいずれかのノードで障害が発生した場合でもオブジェクトを読み出すことができます。

StorageGRID が任意のストレージノードに格納できるレプリケートコピーは 1 つのオブジェクトにつき 1 つだけです。グリッドにストレージノードが 3 つあり、 4 コピーの ILM ルールを作成した場合、作成されるコピーはストレージノードごとに 1 つだけになります。ILM placement unAchievable * アラートがトリガーされ、 ILM ルールを完全に適用できなかったことを示します。

関連情報

"ストレージプールとは"

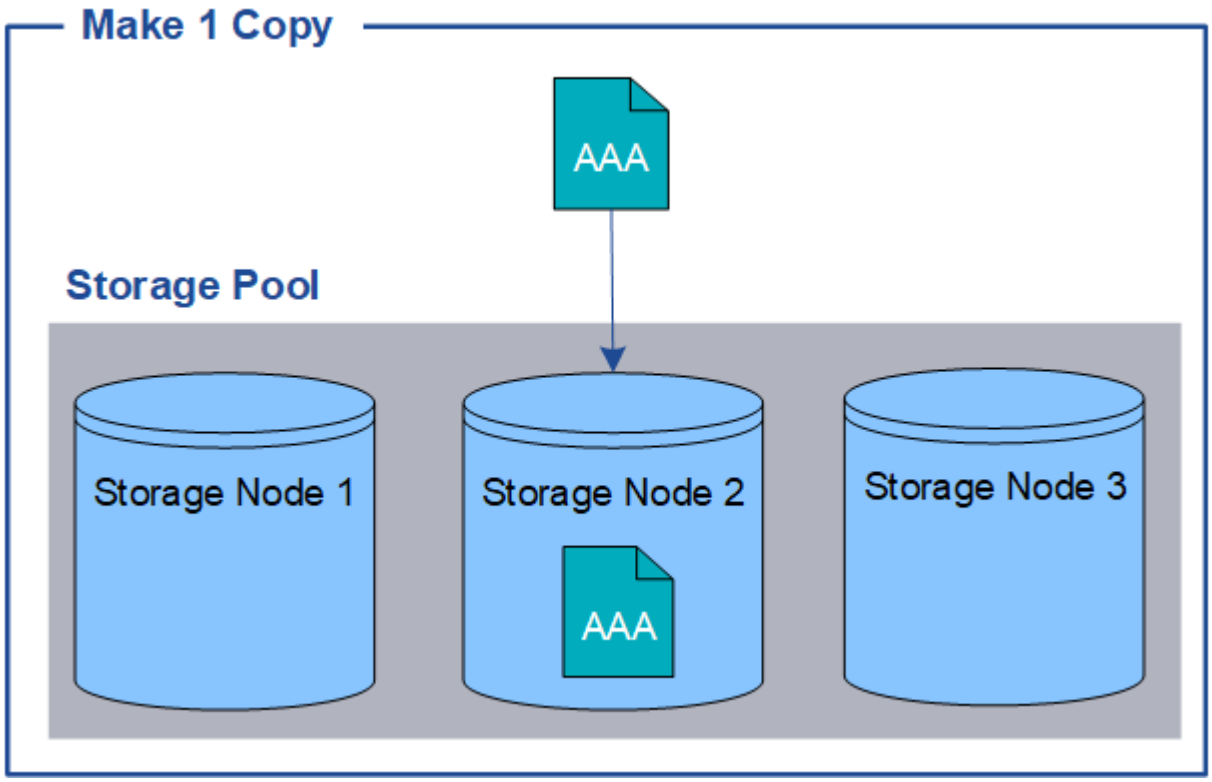
"複数のストレージプールを使用したサイト間レプリケーション"

シングルコピーレプリケーションを使用しない理由

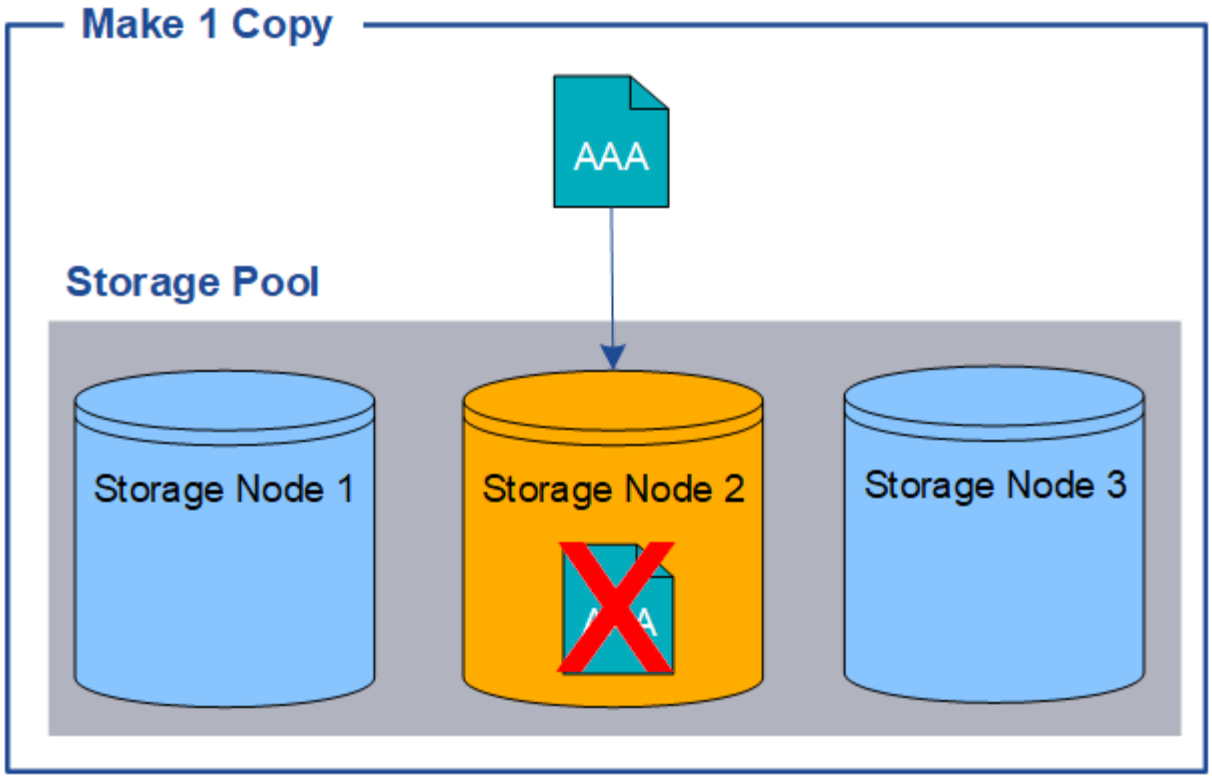
レプリケートコピーを作成する ILM ルールを作成するときは、配置手順の任意の期間に少なくとも 2 つのコピーを指定する必要があります。

レプリケートコピーを 1 つだけ作成する ILM ルールは、どの期間も使用しないでください。オブジェクトのレプリケートコピーが 1 つしかない場合、ストレージノードに障害が発生したり、重大なエラーが発生すると、そのオブジェクトは失われます。また、アップグレードなどのメンテナンス作業中は、オブジェクトへのアクセスが一時的に失われます。

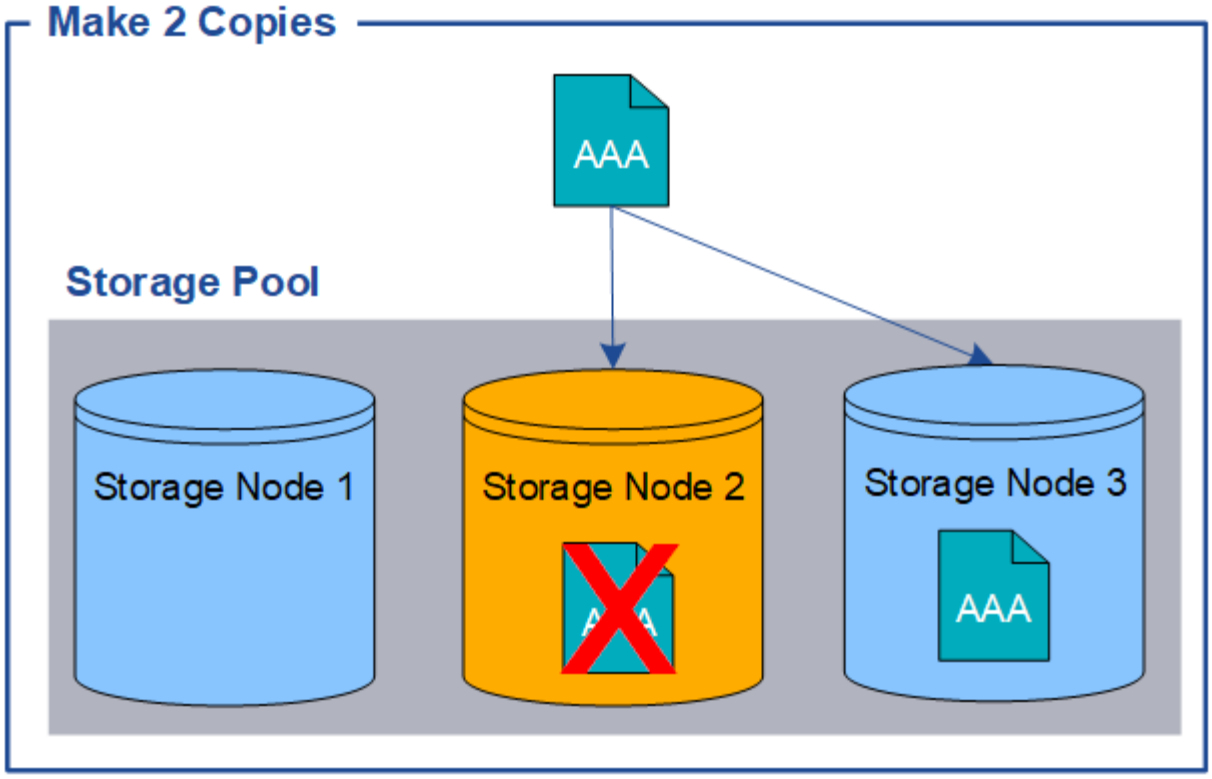
次の例では、 Make 1 Copy ILM ルールによって、 1 つのオブジェクトのレプリケートコピーを 3 つのストレージノードからなるストレージプールに配置するように指定しています。このルールに一致するオブジェクトが取り込まれると、 StorageGRID は 1 つのストレージノードにのみコピーを配置します。




ILM ルールにオブジェクトのレプリケートコピーが 1 つしか作成されていない場合、ストレージノードが使用できなくなるとオブジェクトにアクセスできなくなります。この例では、アップグレードやその他のメンテナンス手順 の実行中など、ストレージノード 2 がオフラインになるとオブジェクト AAA へのアクセスが一時的に失われます。ストレージノード 2 で障害が発生すると、オブジェクト AAA が完全に失われます。



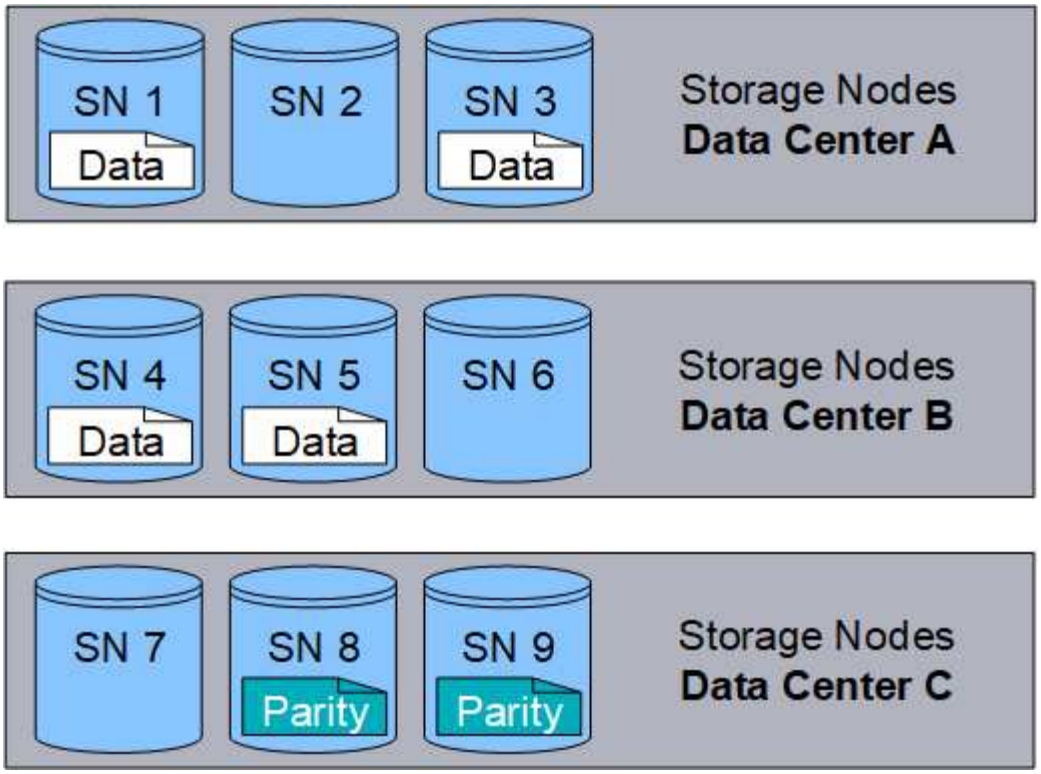

オブジェクトデータの損失を防ぐには、レプリケーションで保護するすべてのオブジェクトのコピーを常に 2 つ以上作成する必要があります。コピーが複数ある場合も、 1 つのストレージノードに障害が発生した場合やオフラインになった場合でもオブジェクトにアクセスできます。



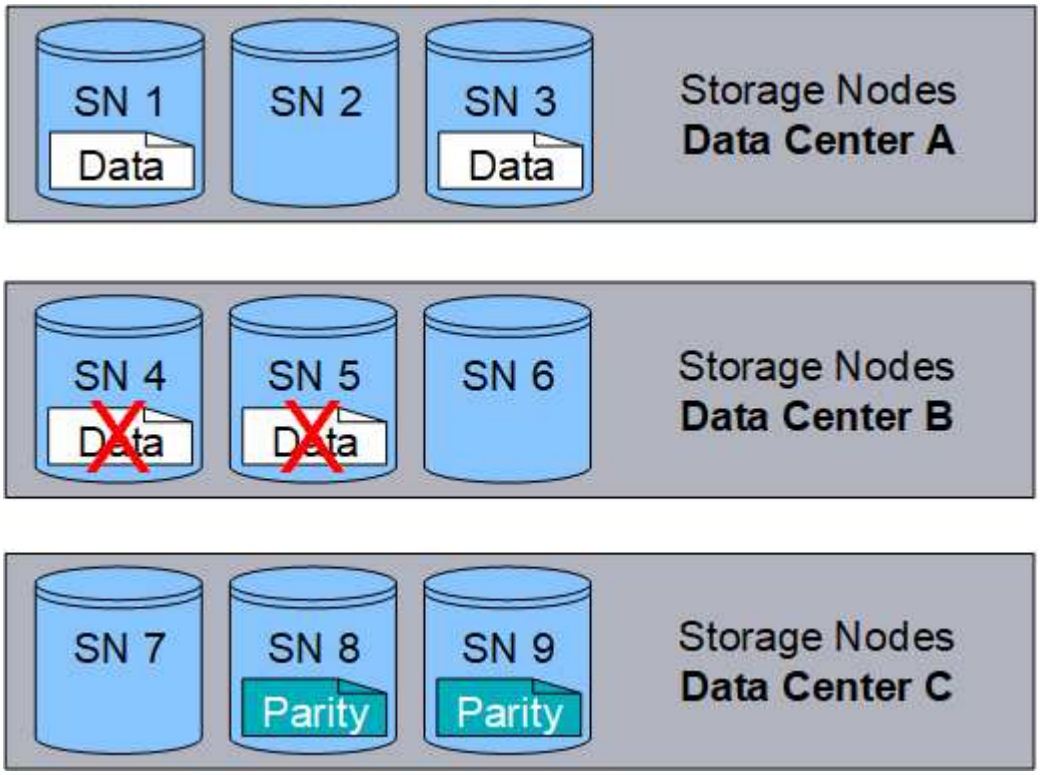

イレイジャーコーディングとは

# イレイジャーコーディングは、オブジェクトデータを格納するために StorageGRID で使用される 2 つ目の方法です。StorageGRID がイレイジャーコーディングコピーを作成するために設定された ILM ルールとオブジェクトを照合する場合は、オブジェクトデータを複数のデータフラグメントに分割し、追加のパリティフラグメントを計算して、各フラグメントを別のストレージノードに格納します。アクセスされたオブジェクトは、格納されたフラグメントを使用して再アセンブルされます。データフラグメントまたはパリティフラグメントが破損したり失われたりしても、イレイジャーコーディングアルゴリズムが残りのデータフラグメントとパリティフラグメントを使用してそのフラグメントを再作成します。

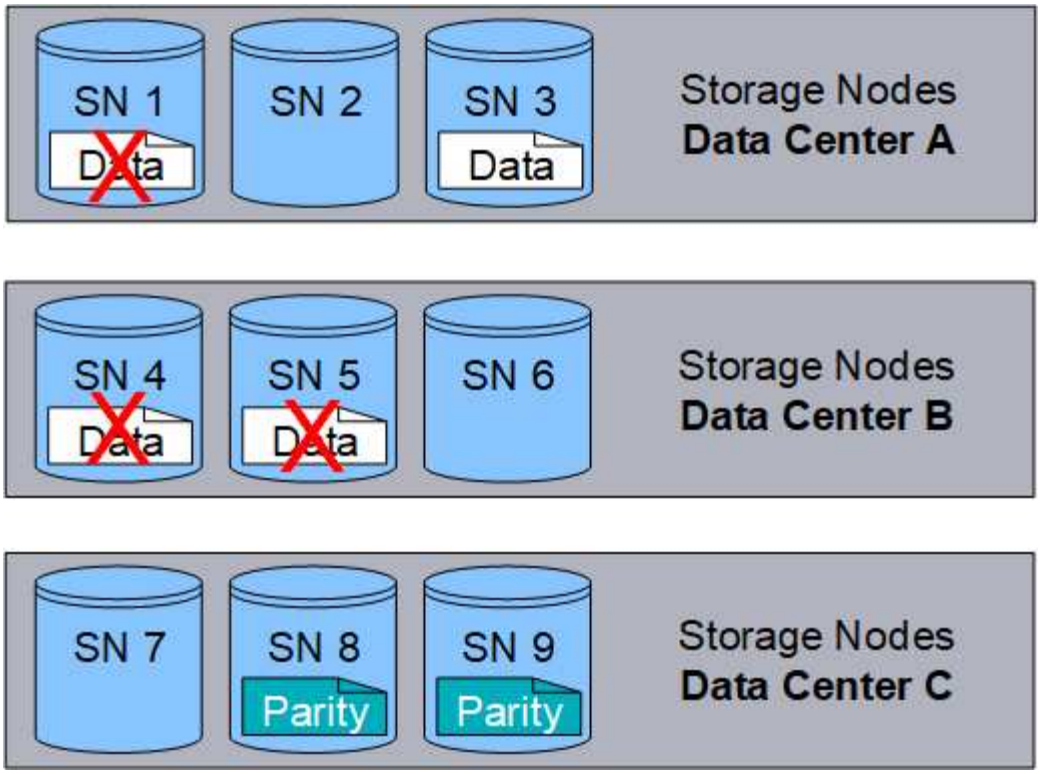
次の例は、オブジェクトのデータに対するイレイジャーコーディングアルゴリズムの使用方法を示しています。この例の ILM ルールでは 4+2 のイレイジャーコーディングスキームを使用します。各オブジェクトは 4 つのデータフラグメントに等分され、オブジェクトデータから 2 つのパリティフラグメントが計算されます。ノードやサイトの障害時にもデータが保護されるよう、 6 つの各フラグメントは 3 つのデータセンターサイトの別々のノードに格納されます。




4+2 のイレイジャーコーディングスキームでは、少なくとも 9 個のストレージノードが必要です。このノードには、 3 つのサイトそれぞれに 3 個のストレージノードが必要です。6 つのうちのいずれか 4 つのフラグメント（データまたはパリティ）が使用可能であれば、オブジェクトを読み出すことができます。最大 2 つのフラグメントが失われても、オブジェクトデータが失われることはありません。データセンターサイト全体で障害が発生した場合でも、他のすべてのフラグメントに引き続きアクセスできれば、オブジェクトの読み出しまたは修復が可能です。




3 つ以上のストレージノードが失われると、オブジェクトを読み出せなくなります。




関連情報

"ストレージプールとは"

"イレイジャーコーディングスキームとは"

"イレイジャーコーディングプロファイルの設定"

イレイジャーコーディングスキームとは

ILM ルールにイレイジャーコーディングプロファイルを設定する場合は、使用するストレージプールを構成するストレージノードとサイトの数に基づいて、使用可能なイレイジャーコーディングスキームを選択します。イレイジャーコーディングスキームは、各オブジェクト用に作成されるデータフラグメントとパリティフラグメントの数を制御します。

StorageGRID システムは、 Reed-Solomon イレイジャーコーディングアルゴリズムを使用します。このアルゴリズムは、オブジェクトを k 個のデータフラグメントに分割して、 m 個のパリティフラグメントを計算します。k + m = n 個のフラグメントが n 個のストレージノードに分散され、データ保護を提供します。失われたフラグメントまたは破損したフラグメントは、オブジェクトが保持できる最大 m 個です。k 個のフラグメントがオブジェクトの読み出しまたは修復に必要です。

イレイジャーコーディングプロファイルを設定する場合は、ストレージプールについて次のガイドラインに従ってください。

- ストレージプールには 3 つ以上のサイト、または 1 つのサイトだけが含まれている必要があります。

> ストレージプールにサイトが 2 つ含まれている場合、イレイジャーコーディングプロファイルは設定できません。

- 3 つ以上のサイトを含むストレージプールのイレイジャーコーディングスキーム
- 1 サイトのストレージプールのイレイジャーコーディングスキーム

- デフォルトのストレージプール、すべてのストレージノード、またはデフォルトサイトであるすべてのサイトを含むストレージプールは使用しないでください。
- ストレージプールには少なくとも *k* + *m*+1 ストレージノードを含める必要があります。

  必要なストレージノードの最小数は、 _ k + m_. です。ただし、必要なストレージノードが一時的に使用できない場合に、少なくとも 1 つのストレージノードを追加することで、取り込みエラーや ILM バックログが発生するのを防ぐことができます。

イレイジャーコーディングスキームのストレージオーバーヘッドは、パリティフラグメントの数（ *m*） をデータフラグメントの数（ *k* ）で割ることによって計算されます。ストレージオーバーヘッドを使用して、各イレイジャーコーディングオブジェクトに必要なディスクスペースを計算できます。

```
disk space = object size + (object size * storage overhead)
```

たとえば、 4+2 スキームを使用して 10MB のオブジェクト（ストレージオーバーヘッドが 50% ）を格納すると、そのオブジェクトが消費するグリッドストレージは 15MB です。6+3 のストレージオーバーヘッドを含む 6+2 スキームを使用して同じ 10MB のオブジェクトを格納すると、オブジェクトが消費するサイズは約 13.3 MB になります。

合計値が最も小さいイレイジャーコーディングスキーム（ _k + m_that ）をニーズに合わせて選択します。フラグメント数が少ないイレイジャーコーディングスキームは全体的に計算効率が高く、 1 つのオブジェクトに作成されて分散（または取得）されるフラグメント数が少なくて済むため、フラグメントサイズが大きいためパフォーマンスが向上し、ストレージの追加が必要になった場合に拡張時に必要なノード数が少なくて済みます。（ストレージ拡張の計画については、 StorageGRID の拡張手順を参照してください）。

**3** つ以上のサイトを含むストレージプールのイレイジャーコーディングスキーム

次の表に、 3 つ以上のサイトを含むストレージプールについて、 StorageGRID で現在サポートされているイレイジャーコーディングスキームを示します。これらの方式はいずれもサイト障害からの保護を提供します。1 つのサイトが失われてもオブジェクトには引き続きアクセスできます。

サイト損失の保護を提供するイレイジャーコーディングスキームの場合、ストレージプールに推奨されるストレージノードの数は各サイトに少なくとも 3 つのストレージノードが必要なため _ k + m_+1 を超えています。

| イレイジャーコーディングスキーム（ *k* + *m*） | サイトの最小数 | 各サイトで推奨されるストレージノードの数 | 推奨されるストレージノードの総数 | サイト障害からの保護 | ストレージオーバーヘッド |
|---|---|---|---|---|---|
| 4+2 | 3. | 3. | 9. | はい。 | 50% |
| 6+2 | 4. | 3. | 12. | はい。 | 33% |
| 8+2 | 5. | 3. | 15 | はい。 | 25% |
| 6 + 3 | 3. | 4. | 12. | はい。 | 50% |

| イレイジャーコーディングスキーム（ *k* + *m*） | サイトの最小数 | 各サイトで推奨されるストレージノードの数 | 推奨されるストレージノードの総数 | サイト障害からの保護 | ストレージオーバーヘッド |
|---|---|---|---|---|---|
| 9 + 3 | 4. | 4. | 16 | はい。 | 33% |
| 2+1 | 3. | 3. | 9. | はい。 | 50% |
| 4+1 | 5. | 3. | 15 | はい。 | 25% |
| 6+1 | 7. | 3. | 21 | はい。 | 17% |
| 7+5 | 3. | 5. | 15 | はい。 | 71% |

StorageGRID では、サイトごとに少なくとも 3 つのストレージノードが必要です。7+5 スキームを使用するには、各サイトに少なくとも 4 つのストレージノードが必要。サイトごとに 5 つのストレージノードを使用することを推奨します。

サイト保護を提供するイレイジャーコーディングスキームを選択する場合は、次の要素の相対的な重要性を調整します。

- * フラグメント数 * ：フラグメントの総数が少ないほど、一般にパフォーマンスと拡張の柔軟性が向上します。
- * フォールトトレランス * ：パリティセグメントの数を増やすことでフォールトトレランスが向上します（ _m_の 値が大きい場合）。
- * ネットワーク・トラフィック *: 障害から回復する場合、フラグメント数の多いスキーム（つまり、 *k* + *m*） を使用すると、より多くのネットワーク・トラフィックが生成されます。
- * ストレージ・オーバーヘッド * ：オーバーヘッドの大きいスキームでは、オブジェクトごとにより多くのストレージ・スペースが必要です。

たとえば、 4+2 と 6+3 のどちらかのスキーム（どちらも 50% のストレージオーバーヘッドがある）を選ぶ場合、フォールトトレランスをさらに高める必要がある場合は 6+3 のスキームを選択します。ネットワークリソースが制限されている場合は、 4+2 のスキームを選択します。他のすべての要素が等しい場合は、フラグメントの合計数が少ないため、 4+2 を選択します。

使用するスキームが不明な場合は、 4+2 または 6+3 を選択するか、テクニカルサポートにお問い合わせください。

**1** サイトのストレージプールのイレイジャーコーディングスキーム

1 サイトのストレージプールでは、サイトに十分な数のストレージノードがある場合、 3 つ以上のサイト用に定義されたすべてのイレイジャーコーディングスキームがサポートされます。

必要なストレージノードの最小数は *k* + *m_1* ですが、 *_k* + *m*+1 ストレージノードを含むストレージプールを推奨します。たとえば、 2+1 イレイジャーコーディングスキームには少なくとも 3 つのストレージノードからなるストレージプールが必要ですが、推奨されるストレージノード数は 4 つです。

| イレイジャーコーディングスキーム（ *k* + *m*） | ストレージノードの最小数 | 推奨されるストレージノードの数 | ストレージオーバーヘッド |
|---|---|---|---|
| 4+2 | 6. | 7. | 50% |
| 6+2 | 8. | 9. | 33% |
| 8+2 | 10. | 11. | 25% |
| 6 + 3 | 9. | 10. | 50% |
| 9 + 3 | 12. | 13 | 33% |
| 2+1 | 3. | 4. | 50% |
| 4+1 | 5. | 6. | 25% |
| 6+1 | 7. | 8. | 17% |
| 7+5 | 12. | 13 | 71% |

関連情報

"グリッドを展開します"

イレイジャーコーディングのメリット、デメリット、および要件

## レプリケーションとイレイジャーコーディングのどちらを使用してオブジェクトデータを損失から保護するかを決定する前に、イレイジャーコーディングのメリット、デメリット、および要件を理解しておく必要があります。

### イレイジャーコーディングのメリット

イレイジャーコーディングは、レプリケーションに比べて信頼性、可用性、ストレージ効率に優れています。

- * 信頼性 * ：信頼性はフォールトトレランス、つまり同時にデータを失うことなく維持できる障害の数によって判断されます。レプリケーションでは、複数の同一コピーが異なるノード上およびサイト間に格納されます。イレイジャーコーディングの場合、オブジェクトはデータフラグメントとパリティフラグメントにエンコードされ、多数のノードとサイトに分散されます。この分散によってサイトとノード両方の障害からの保護を提供します。イレイジャーコーディングは、同等のストレージコストでレプリケーションよりも優れた信頼性を提供します。
- * 可用性 * ：可用性は、ストレージノードに障害が発生した場合や、ノードにアクセスできなくなった場合にオブジェクトを読み出すことができるかどうかによって定義されます。イレイジャーコーディングは、同等のストレージコストでレプリケーションよりも優れた可用性を提供します。
- * Storage Efficiency * ：可用性と信頼性が同等レベルの場合、イレイジャーコーディングで保護されたオブジェクトが消費するディスクスペースは、同じオブジェクトをレプリケーションで保護する場合よりも少なくなります。たとえば、 10MB のオブジェクトを 2 つのサイトにレプリケートするとディスクスペースを 20MB （ 2 つのコピー）消費しますが、 6+3 のイレイジャーコーディングスキームを使用して 3 つ

のサイトにイレイジャーコーディングされたオブジェクトが消費するディスクスペースは 15MB のみです。

> イレイジャーコーディングオブジェクトのディスクスペースは、オブジェクトサイズにストレージオーバーヘッドを加えたものです。ストレージオーバーヘッドの割合は、パリティフラグメント数をデータフラグメント数で割って算出します。

### イレイジャーコーディングのデメリット

レプリケーションと比較した場合のイレイジャーコーディングのデメリットは次のとおりです。

- より多くのストレージノードとサイトが必要です。たとえば、 6+3 のイレイジャーコーディングスキームを使用する場合は、 3 つのサイトに少なくとも 3 つのストレージノードが必要です。一方、オブジェクトデータをレプリケートする場合は、各コピーに必要なストレージノードは 1 つだけです。
- ストレージの拡張にかかるコストと複雑さが増大します。レプリケーションを使用する環境を拡張するには、オブジェクトコピーを作成するすべての場所にストレージ容量を追加するだけです。イレイジャーコーディングを使用する環境を拡張する場合は、使用中のイレイジャーコーディングスキームと、既存のストレージノードの使用率の両方を考慮する必要があります。たとえば、既存のノードが 100% フルになるまで待つ場合は、少なくとも _k + m_Storage ノードを追加する必要があります。ただし、既存のノードが 70% フルになった時点で拡張する場合は、サイトごとに 2 つのノードを追加し、使用可能なストレージ容量を最大化できます。詳細については、StorageGRID の拡張手順を参照してください。
- 地理的に分散したサイトでイレイジャーコーディングを使用する場合は、読み出しのレイテンシが上昇します。イレイジャーコーディングされてリモートサイトに分散されたオブジェクトのフラグメントを WAN 接続経由で読み出す場合、レプリケートされてローカル（クライアントの接続先と同じサイト）で利用可能なオブジェクトよりも時間がかかります。
- 地理的に分散したサイトでイレイジャーコーディングを使用する場合は、特に WAN ネットワーク接続経由でオブジェクトを頻繁に読み出したり修復したりするケースでは読み出しと修復の WAN ネットワークトラフィックが増大します。
- サイト間でイレイジャーコーディングを使用する場合は、サイト間のネットワークレイテンシの上昇に伴ってオブジェクトの最大スループットが大幅に低下します。この最大スループットの低下は TCP ネットワークのスループットが低下したことによるもので、 StorageGRID システムによるオブジェクトフラグメントの格納 / 読み出し速度に影響します。
- コンピューティングリソースの利用率が向上します。

### イレイジャーコーディングを使用する状況

イレイジャーコーディングは次の要件に最適です。

- 1MBを超えるオブジェクト

> イレイジャーコーディングコピーに関連付けられているフラグメント数の管理でオーバーヘッドが発生するため、200KB以下のオブジェクトにはイレイジャーコーディングを使用しないでください。

- 頻繁に読み出されないコンテンツの長期保存またはコールドストレージ。
- 高いデータ可用性と信頼性。
- サイトやノードの障害に対する保護

- ストレージ効率
- 複数のレプリケートコピーではなく 1 つのイレイジャーコーディングコピーのみを使用して効率的にデータを保護する必要のある単一サイト環境
- サイト間レイテンシが 100 ミリ秒未満の複数サイト環境

関連情報

"グリッドを展開します"

オブジェクト保持期間の決定方法

# StorageGRID には、グリッド管理者と個々のテナントユーザが、オブジェクトを格納する期間を指定するためのオプションがあります。通常、テナントユーザが指定した保持手順は、グリッド管理者が指定した保持手順よりも優先されます。

## テナントユーザによるオブジェクト保持期間の制御方法

テナントユーザは、主に次の 3 つの方法でオブジェクトを StorageGRID に格納する期間を制御できます。

- グリッドでグローバルな S3 オブジェクトのロック設定が有効になっている場合、 S3 テナントユーザは S3 オブジェクトのロックを有効にしたバケットを作成し、 S3 REST API を使用して、そのバケットに追加された各オブジェクトバージョンの最新の保持設定とリーガルホールド設定を指定できます。
  - リーガルホールドの対象になっているオブジェクトバージョンは、どの方法でも削除できません。
  - オブジェクトバージョンの retain-until - date に到達するまでは、どのメソッドでもそのバージョンを削除することはできません。
  - S3 オブジェクトロックが有効なバケット内のオブジェクトは ILM によって「無期限」に保持されます。 ただし、それまでの保持期間が終了したあとは、クライアント要求やバケットライフサイクルの終了によってオブジェクトバージョンを削除できます。

    "S3オブジェクトロックでオブジェクトを管理する"

- S3 テナントユーザは、 Expiration アクションを指定するライフサイクル設定をバケットに追加できます。バケットライフサイクルが存在する場合、クライアントがオブジェクトを削除しないかぎり、 StorageGRID は Expiration アクションで指定された日付または日数が経過するまでオブジェクトを格納します。
- S3 / Swift クライアントは、オブジェクトの削除要求を問題 に送信できます。StorageGRID は、オブジェクトを削除するか保持するかを決定する際に、常に S3 バケットライフサイクルまたは ILM よりもクライアントの削除要求を優先します。

## グリッド管理者によるオブジェクト保持期間の制御方法

グリッド管理者は、 ILM の配置手順を使用してオブジェクトの格納期間を制御します。オブジェクトが ILM ルールに一致した場合、 StorageGRID は ILM ルールの最後の期間が経過するまでそのオブジェクトを格納します。配置手順に「 forever 」が指定されている場合、オブジェクトは無期限に保持されます。

オブジェクトの保持期間を誰が制御するかに関係なく、格納するオブジェクトコピーのタイプ（レプリケートまたはイレイジャーコーディング）とコピーの場所（ストレージノード、クラウドストレージプール、またはアーカイブノード）は ILM 設定によって制御されます。

### S3 バケットライフサイクルと ILM の相互作用

S3 バケットライフサイクルの Expiration アクションは、常に ILM 設定よりも優先されます。その結果、 ILM のオブジェクト配置手順がすべて終了したあとも、オブジェクトがグリッドに保持されることがあります。

#### オブジェクト保持の例

S3 オブジェクトロック、バケットライフサイクル設定、クライアントの削除要求、 ILM の相互作用について、より深く理解するために次の例を検討してください。

##### 例 1 ： S3 バケットライフサイクルのオブジェクト保持期間が ILM よりも長い

**ILM**

2 つのコピーを 1 年間保存（ 365 日）

バケットライフサイクル

2 年（ 730 日）でオブジェクトが期限切れになる

結果

StorageGRID はオブジェクトを 730 日間格納します。StorageGRID は、バケットライフサイクル設定を使用して、オブジェクトを削除するか保持するかを決定します。

> ILM よりもバケットライフサイクルのオブジェクト保持期間の方が長い場合でも、格納するコピーの数とタイプを決定する際には引き続き StorageGRID の配置手順が使用されます。この例では、 366 日目から 730 日目までの間、オブジェクトの 2 つのコピーが StorageGRID に引き続き格納されます。

##### 例 2 ： S3 バケットライフサイクルのオブジェクト保持期間よりも短い

**ILM**

2 つのコピーを 2 年間（ 730 日）格納する

バケットライフサイクル

1 年（ 365 日）でオブジェクトを期限切れにする

結果

StorageGRID は 365 日目にオブジェクトのコピーを両方削除します。

##### 例 3 ：クライアントによる削除は、バケットライフサイクルと ILM よりも優先されます

**ILM**

2 つのコピーをストレージ・ノードに無期限に保存

バケットライフサイクル

2 年（ 730 日）でオブジェクトが期限切れになる

クライアントの削除要求

発行日： 400 日目

結果

StorageGRID は、クライアントの削除要求に応じて 400 日目にオブジェクトのコピーを両方削除します。

例 **4** ： **S3** オブジェクトロックはクライアントの削除要求を上書きします

**S3** オブジェクトのロック

オブジェクトバージョンの retain-until は、 2026-03-31 です。リーガルホールドは有効ではありません。

準拠 **ILM** ルール

2 つのコピーをストレージ・ノードに無期限に保存します

クライアントの削除要求

2024-03-331 発行。

結果

retain-until はまだ 2 年前の時点であるため、 StorageGRID はオブジェクトバージョンを削除しません。

関連情報

"S3オブジェクトロックでオブジェクトを管理する"

"S3 を使用する"

"ILM ルールの配置手順とは"

オブジェクトの削除方法

# StorageGRID は、クライアント要求に直接応答してオブジェクトを削除するか、 S3 バケットライフサイクルの終了または ILM ポリシーの要件に応じて自動的にオブジェクトを削除します。オブジェクトのさまざまな削除方法と StorageGRID による削除要求の処理方法を理解しておくと、オブジェクトをより効率的に管理できるようになります。

StorageGRID では、次のいずれかの方法でオブジェクトを削除できます。

- 同期削除： StorageGRID がクライアントの削除要求を受け取ると、すべてのオブジェクトコピーがただちに削除されます。コピーが削除されると、削除が成功したことがクライアントに通知されます。
- オブジェクトは削除キューに登録されます。 StorageGRID が削除要求を受け取ると、オブジェクトは削除キューに登録され、削除が成功したことがクライアントにすぐに通知されます。オブジェクトコピーは、あとでバックグラウンド ILM 処理によって削除されます。

StorageGRID では、オブジェクトを削除する際に、削除のパフォーマンスを最適化し、削除のバックログを最小限に抑え、スペースを最も早く解放する方法を使用します。

次の表は、 StorageGRID がどのような場合に各メソッドを使用するかを

| 削除方法 | 使用時 |
| --- | --- |
| オブジェクトは削除キューに登録されます | 次の条件のいずれか * が当てはまる場合：<br>• 次のいずれかのイベントによってオブジェクトの自動削除がトリガーされた：<br>◦ S3 バケットのライフサイクル設定の有効期限または日数に達した。<br>◦ ILM ルールに指定された最後の期間が経過した。<br>• 注： S3 オブジェクトのロックが有効になっているバケット内のオブジェクトは、リーガルホールドの対象である場合や、 retain-until date を指定したものの、まだ満たされていない場合は削除できません。<br>• S3 / Swift クライアントが削除を要求し、次の条件を 1 つ以上満たしている：<br>◦ オブジェクトの場所が一時的に使用できないなどの理由で、 30 秒以内にコピーを削除できない。<br>◦ バックグラウンド削除キューがアイドル状態である。 |
| オブジェクトをただちに削除（同期削除） | S3 / Swift クライアントが削除要求を行い、次の * すべての条件が満たされている場合：<br>• すべてのコピーを 30 秒以内に削除できる。<br>• バックグラウンド削除キューには処理するオブジェクトが含まれています。 |

S3 / Swift クライアントが削除要求を行うと、 StorageGRID はまずオブジェクトを削除キューに追加します。その後、同期削除の実行に切り替えます。処理対象となるオブジェクトがバックグラウンド削除キューに含まれていることを確認することで、 StorageGRID は、クライアントによる削除のバックログが発生しないようにしつつ、特に同時実行性の低いクライアントに対してより効率的に削除を処理できます。

**StorageGRID** によるオブジェクトの削除方法が及ぼす影響を理解しておく必要があります

StorageGRID によるオブジェクトの削除方法は、システムの動作に影響を及ぼす可能性があります。

- StorageGRID StorageGRID で同期削除が実行されると、結果がクライアントに返されるまでに最大 30 秒かかることがあります。つまり、実際には StorageGRID がオブジェクトを削除キューに登録する場合よりも短時間でコピーが削除されるにもかかわらず、より長くかかっているという印象をクライアントに与える可能性があります。
- 一括削除の実行中にそのパフォーマンスを注意深く監視していると、一定数のオブジェクトが削除されたあとに削除の速度が遅くなったように見えることがあります。この変更は、 StorageGRID がオブジェクトを削除キューへ登録する方法から同期削除に切り替えたときに発生します。削除速度が低下したように見えても、オブジェクトコピーの削除速度が遅くなったわけではありません。一方で、スペースの開放にかかる時間は、平均すると短くなっています。

大量のオブジェクトを削除する場合に、スペースを短時間で解放することが優先されるのであれば、 ILM などの方法を使用してオブジェクトを削除するのではなく、クライアント要求を使用することを検討してください。一般に、クライアントによって削除が実行された場合、 StorageGRID は同期削除を使用できるため、ス

ペースはより短時間で解放されます。

オブジェクトの削除後にスペースを解放するために必要な時間は、次の要因によって異なります。

- オブジェクトコピーが同期的に削除されるか、またはキューに登録されたあとで削除されるか（クライアントの削除要求の場合）。
- グリッド内のオブジェクトの数や、オブジェクトコピーが削除対象キューに登録される場合のグリッドリソースの可用性などのその他の要因（クライアントによる削除およびその他の方法の場合）。

**S3** バージョン管理オブジェクトの削除方法

S3 バケットでバージョン管理が有効になっている場合、 StorageGRID は、削除要求に応答する際、要求が S3 クライアント、 S3 バケットライフサイクルの終了、 ILM ポリシーの要件のいずれによるものであるかにかかわらず、 Amazon S3 の動作に従います。

オブジェクトがバージョン管理されている場合、オブジェクトの削除要求は現在のバージョンのオブジェクトを削除せず、スペースも解放しません。代わりに ' オブジェクト削除要求は ' 最新バージョンのオブジェクトとして削除マーカーを作成するだけで ' 以前のバージョンのオブジェクトは noncurrent になります

オブジェクトが削除されていなくても、 StorageGRID は現在のバージョンのオブジェクトが使用できなくなったかのように動作します。そのオブジェクトに対する要求は 404 NotFound を返します。ただし、最新でないオブジェクトデータは削除されていないため、最新でないバージョンのオブジェクトを指定する要求は成功します。

バージョン管理オブジェクトを削除するときにスペースを解放するには、次のいずれかを実行する必要があります。

- * S3クライアント要求*：S3 DELETE Object要求でオブジェクトのバージョン番号を指定します (`DELETE /object?versionId=ID`）。この要求は、指定したバージョンのオブジェクトコピーだけを削除します（他のバージョンは引き続きスペースを消費します）。
- バケットライフサイクル：を使用します `NoncurrentVersionExpiration` をクリックします。NoncurrentDays で指定した日数に達すると、 StorageGRID は最新でないオブジェクトバージョンのコピーをすべて完全に削除します。これらのオブジェクトバージョンはリカバリできません。
- * ILM * ： ILM ポリシーに 2 つの ILM ルールを追加します。最新でないバージョンのオブジェクトに一致する場合は、最初のルールで「 * noncurrent Time * 」を参照時間として使用します。2 つ目のルールの * 取り込み時間 * を現在のバージョンと一致させます。「 * noncurrent Time * 」ルールは、「 * Ingest Time * 」ルールの上のポリシーに含める必要があります。

関連情報

"S3 を使用する"

"例 4 ： S3 バージョン管理オブジェクトの ILM ルールとポリシー"

**ILM** ポリシーとは

情報ライフサイクル管理（ ILM ）ポリシーは、優先順位が付けられた一連の ILM ルールです。 StorageGRID システムが時間の経過に伴ってオブジェクトデータを管理する方法を決定します。

**ILM** ポリシーによるオブジェクトの評価方法

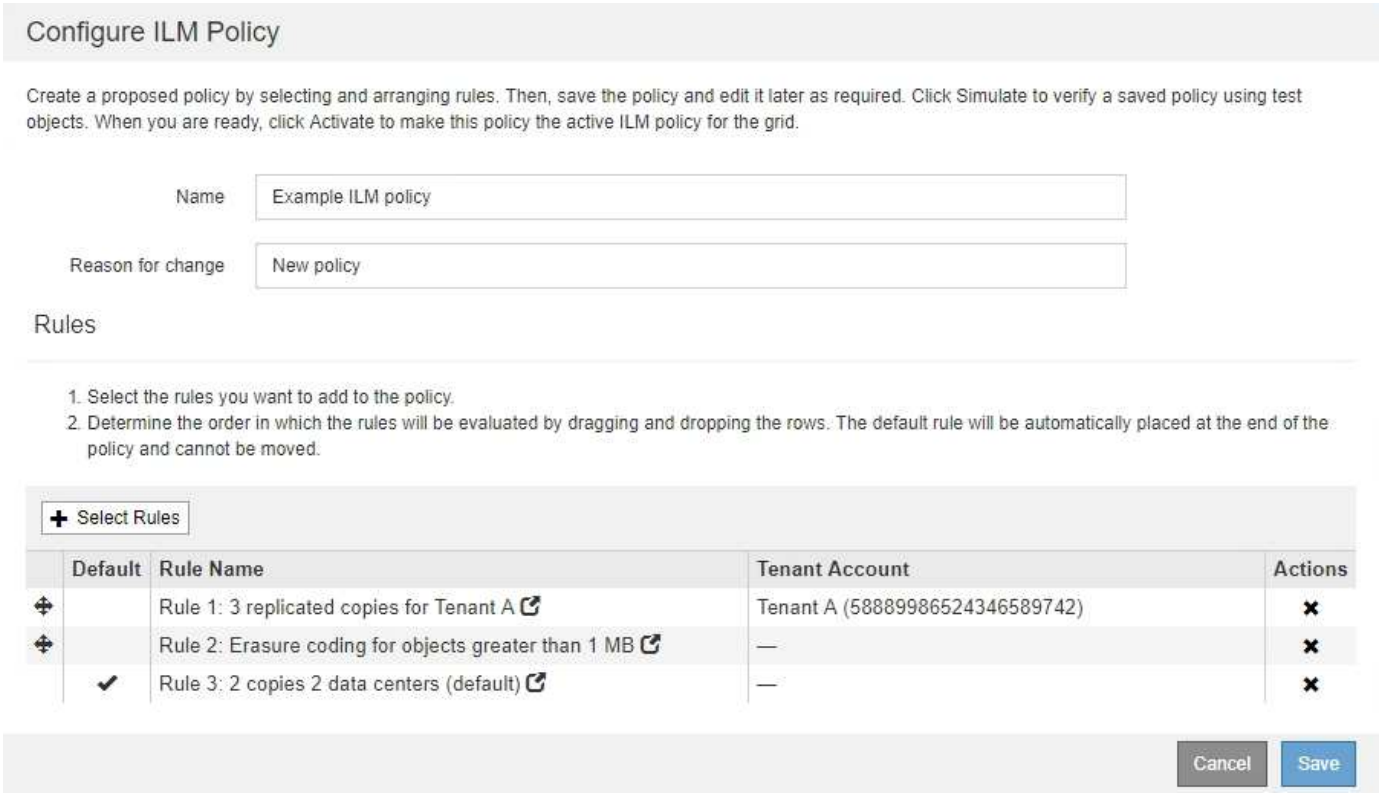
StorageGRID システムのアクティブな ILM ポリシーは、すべてのオブジェクトの配置、期間、データ保護を制御します。

クライアントがオブジェクトを StorageGRID に保存すると、オブジェクトはアクティブポリシー内の順序付けられた ILM ルールに照らして次のように評価されます。

1. ポリシー内の最初のルールのフィルタがオブジェクトに一致すると、オブジェクトはそのルールの取り込み動作に従って取り込まれ、そのルールの配置手順に従って格納されます。
2. 最初のルールのフィルタがオブジェクトに一致しない場合、オブジェクトは一致が見つかるまでポリシー内の後続の各ルールに照らして評価されます。
3. どのルールもオブジェクトに一致しない場合は、ポリシー内のデフォルトルールの取り込み動作と配置手順が適用されます。デフォルトルールはポリシー内の最後のルールであり、フィルタは使用できません。

**ILM** ポリシーの例

この例の ILM ポリシーは 3 つの ILM ルールを使用します。

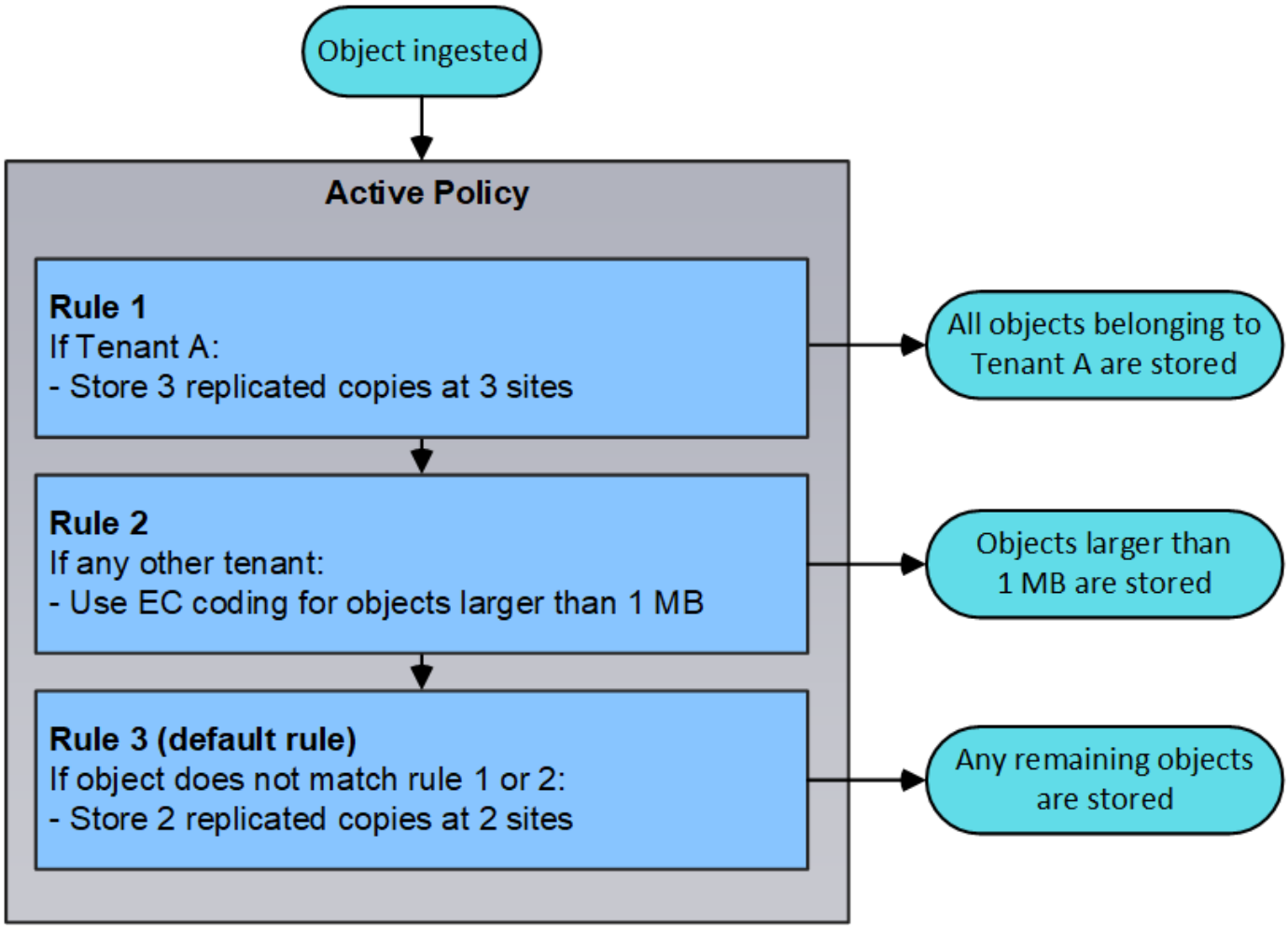



この例では、ルール 1 はテナント A に属するすべてのオブジェクトに一致しますこれらのオブジェクトは、3 つのサイトに 3 つのレプリケートコピーとして格納されます。他のテナントに属するオブジェクトはルール 1 に一致しないため、ルール 2 に照らして評価されます。

ルール2では、他のテナントのすべてのオブジェクトが一致しますが、1MBより大きいオブジェクトのみが該当します。これらのオブジェクトは、 3 つのサイトで 6+3 のイレイジャーコーディングを使用して格納されます。ルール 2 がオブジェクト 1MB 以下に一致しないため、これらのオブジェクトはルール 3 に照らして評価されます。

ルール 3 はポリシー内の最後のルールで、デフォルトのルールであり、フィルタは使用しません。ルール 3

では、ルール 1 またはルール 2 に一致しないすべてのオブジェクトのレプリケートコピーを 2 つ作成します（ 1MB 以下のテナント A に属していないオブジェクト）。



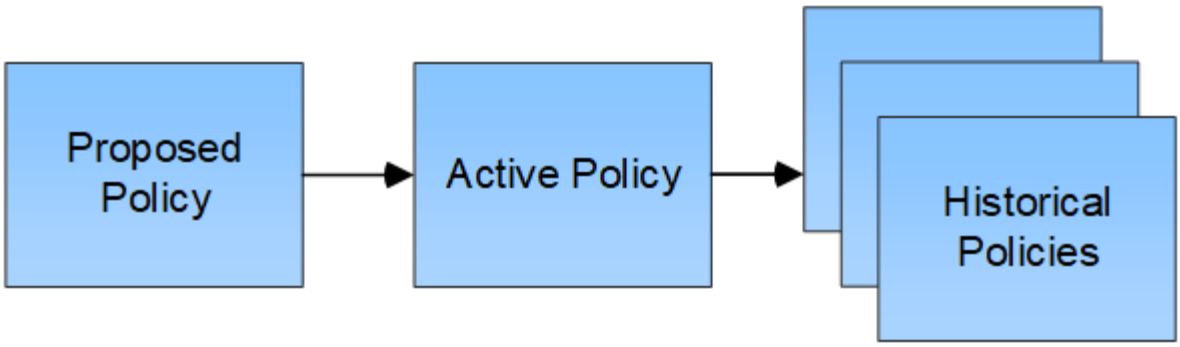

ドラフトポリシー、アクティブポリシー、履歴ポリシーとは

各 StorageGRID システムには、アクティブな ILM ポリシーが 1 つ必要です。StorageGRID システムでは、ドラフトの ILM ポリシーを 1 つと任意の数の履歴ポリシーを使用できます。

初めて ILM ポリシーを作成するときは、 ILM ルールを 1 つ以上選択して特定の順序で並べ、ドラフトポリシーを作成します。ドラフトポリシーをシミュレートして動作を確認したら、そのポリシーをアクティブ化してアクティブポリシーを作成します。

新しい ILM ポリシーをアクティブ StorageGRID 化すると、そのポリシーを使用して、既存のオブジェクトと新たに取り込まれたオブジェクトを含むすべてのオブジェクトが管理されます。新しいポリシーの ILM ルールが実装されたときに、既存のオブジェクトが新しい場所に移動されることがあります。

ドラフトポリシーをアクティブ化すると、それまでのアクティブポリシーは履歴ポリシーになります。ILM 履歴ポリシーは削除できません。




関連情報

"ILMポリシーを作成する"

**ILM** ルールとは

オブジェクトを管理するには、一連の情報ライフサイクル管理（ ILM ）ルールを作成して 1 つの ILM ポリシーにまとめます。システムに取り込まれた各オブジェクトは、アクティブポリシーに照らして評価されます。ポリシー内のルールがオブジェクトのメタデータに一致すると、ルールの手順に従って、 StorageGRID がそのオブジェクトをコピーして格納します。

ILM ルールでは次の項目を定義

- 格納するオブジェクト。ルールはすべてのオブジェクトに適用することも、ルール環境 を構成するオブジェクトを特定するフィルタを指定することもできます。たとえば、特定のテナントアカウント、特定の S3 バケットまたは Swift コンテナ、または特定のメタデータ値に関連付けられたオブジェクトにのみルールを適用できます。
- ストレージのタイプと場所。オブジェクトは、ストレージノード、クラウドストレージプール、またはアーカイブノードに格納できます。
- 作成するオブジェクトコピーのタイプ。コピーはレプリケートまたはイレイジャーコーディングできます。
- レプリケートコピーの場合は、作成されるコピーの数。
- イレイジャーコーディングコピーにはイレイジャーコーディングスキームを使用します。
- オブジェクトのストレージの場所とコピーのタイプの経時的変化。
- オブジェクトがグリッドに取り込まれるときにオブジェクトデータを保護する方法（同期配置またはデュアルコミット）。

オブジェクトメタデータは ILM ルールによって管理されません。代わりに、オブジェクトメタデータはメタデータストア内の Cassandra データベースに格納されます。データを損失から保護するために、オブジェクトメタデータの 3 つのコピーが各サイトで自動的に維持されます。コピーはすべてのストレージノードに均等に分散されます。

**ILM** ルールの要素

ILM ルールには次の 3 つの要素があります。

- * フィルタ条件 * ：ルールの基本フィルタと高度なフィルタにより、ルール環境 で使用するオブジェクトが定義されます。オブジェクトがすべてのフィルタに一致する場合、 StorageGRID はルールを適用し、

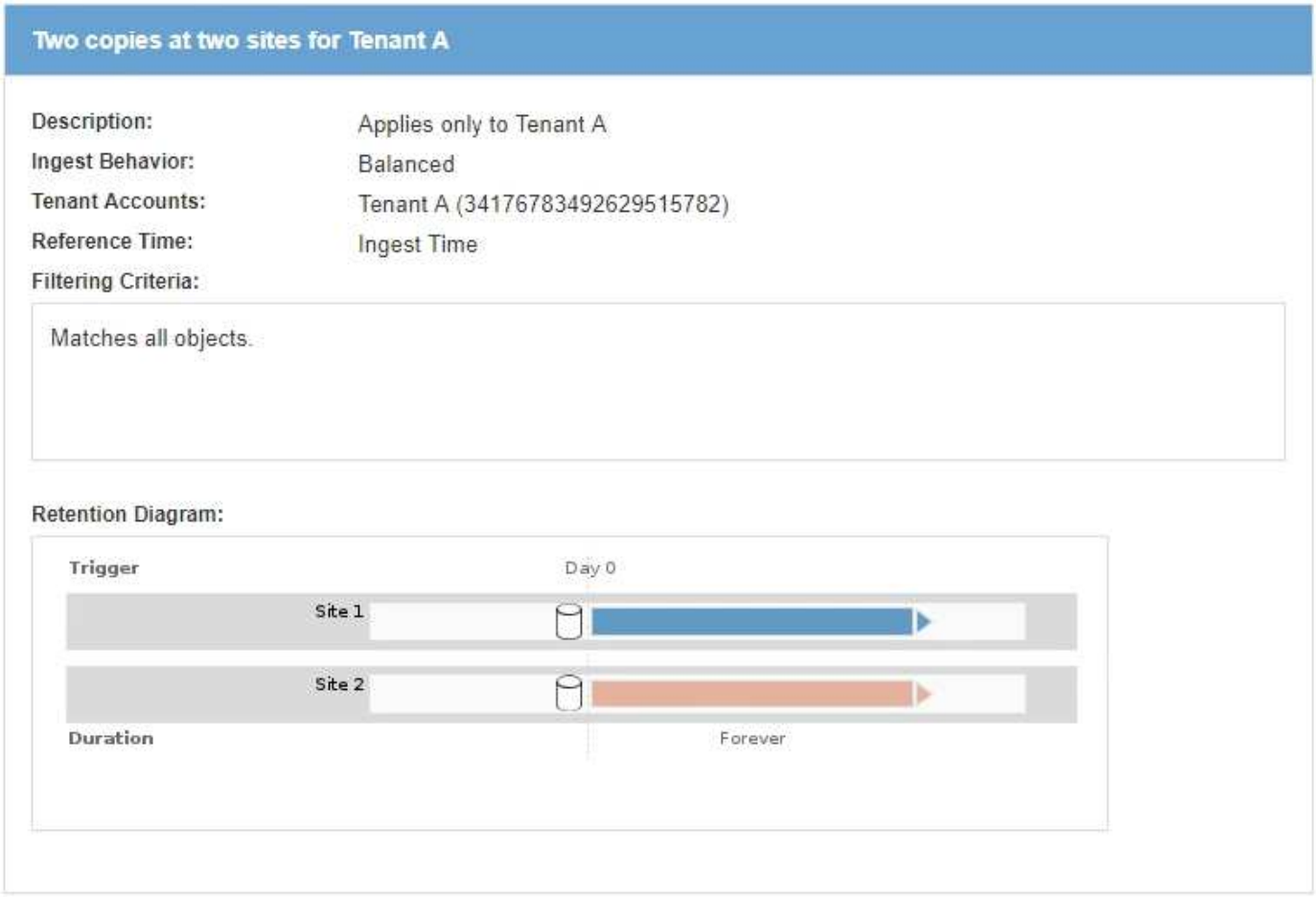
ルールの配置手順で指定されたオブジェクトコピーを作成します。

- * 配置手順 * ：ルールの配置手順によって、オブジェクトコピーの数、タイプ、および場所が定義されます。各ルールに一連の配置手順を含めることで、時間の経過に伴うオブジェクトコピーの数、タイプ、場所を変更することができます。1 つの配置の期間が終了すると、次の配置手順が次の ILM 評価で自動的に適用されます。
- * 取り込み動作 * ：ルールの取り込み動作は、 S3 または Swift クライアントがオブジェクトをグリッドに保存する際の処理を定義します。取り込み動作は、ルールの手順に従ってオブジェクトコピーがすぐに配置されるか、または中間コピーが作成されて配置手順があとから適用されるかを制御します。

**ILM** ルールの例

次の ILM ルールの例では、テナント A に属するオブジェクトの環境 を設定しますこれらのオブジェクトのレプリケートコピーを 2 つ作成し、各コピーを別々のサイトに格納します。この 2 つのコピーは「無期限」に保持されます。つまり、 StorageGRID はこれらのコピーを自動的に削除しません。これらのオブジェクトは、クライアントの削除要求によって削除されるか、バケットライフサイクルが終了するまで、StorageGRID によって保持されます。

このルールでは、取り込み動作に Balanced オプションが使用されます。 2 つのサイトの配置手順は、テナント A がオブジェクトを StorageGRID に保存するとすぐに適用されます。ただし、両方の必要なコピーをただちに作成することはできません。たとえば、テナント A がオブジェクトを保存したときにサイト 2 に到達できない場合、 StorageGRID はサイト 1 のストレージノードに 2 つの中間コピーを作成します。サイト 2 が使用可能になると、 StorageGRID はそのサイトで必要なコピーを作成します。




関連情報

"取り込みのデータ保護オプション"

"ストレージプールとは"

"クラウドストレージプールとは"

"オブジェクトの格納方法（レプリケーションまたはイレイジャーコーディング）"

"ILM ルールのフィルタリングとは"

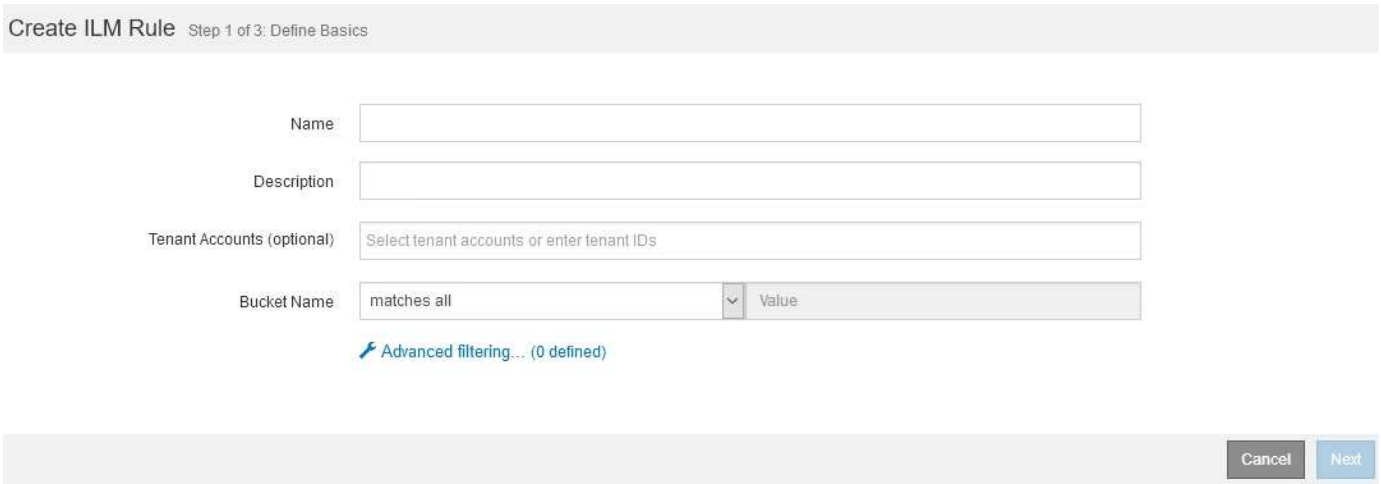
"ILM ルールの配置手順とは"

**ILM** ルールのフィルタリングとは

## ILM ルールを作成する際には、フィルタを指定して環境 ルールを構成するオブジェクトを特定します。

最も単純なケースは、ルールでフィルタを使用しない場合です。環境 のすべてのオブジェクトでフィルタを使用しないルールがある場合は、 ILM ポリシーの最後の（デフォルト）ルールである必要があります。デフォルトルールは、別のルールのフィルタに一致しないオブジェクトに対するストレージの手順を提供します。

基本フィルタを使用すると、大規模なオブジェクトグループに異なるルールを適用できます。Create ILM Rule ウィザードの Define Basics ページの基本フィルタを使用して、特定のテナントアカウント、特定の S3 バケットまたは Swift コンテナ、あるいはその両方にルールを適用できます。




これらの基本フィルタを使用すると、多数のオブジェクトに異なるルールを簡単に適用できます。たとえば、会社の財務記録は規制要件を満たすために保存し、マーケティング部門のデータは日々の業務を円滑に進めるために保存しなければならない場合があります。部門ごとに別々のテナントアカウントを作成するか、またはデータを部門ごとに別々の S3 バケットに分離したあとで、すべての財務記録を環境 で処理するルールを 1 つ作成し、環境 ですべてのマーケティングデータを処理するもう 1 つのルールを作成することができます。

Create ILM Rule ウィザードの * Advanced Filtering * ページでは、詳細な制御を行うことができます。次のオブジェクトプロパティに基づいてオブジェクトを選択するフィルタを作成できます。

- 取り込み時間
- 最終アクセス時間
- オブジェクト名のすべてまたは一部（キー）
- S3 バケットのリージョン（場所の制約）

- オブジェクトのサイズ
- ユーザメタデータ
- S3 オブジェクトタグ

非常に特定の条件でオブジェクトをフィルタリングできます。たとえば、病院の画像診断部門が保管するオブジェクトは、 30 日以内に頻繁に使用され、その後はあまり使用されない可能性があります。一方、患者の通院情報を格納するオブジェクトは、医療ネットワークの本部請求部門にコピーする必要があります。オブジェクト名、サイズ、 S3 オブジェクトタグ、またはその他の関連条件に基づいて各タイプのオブジェクトを識別するフィルタを作成してから、それぞれのオブジェクトセットを適切に格納するルールを別々に作成できます。

必要に応じて、基本フィルタと高度なフィルタを 1 つのルールにまとめることもできます。たとえば、マーケティング部門では、サイズの大きな画像ファイルをベンダーレコードとは異なる方法で格納しなければならない場合があります。一方、人事部門では、特定の地域の人事レコードとポリシー情報を一元的に格納する必要があります。この場合は、テナントアカウントでフィルタリングするルールを作成して各部門からレコードを分離し、各ルールで高度なフィルタを使用してルール環境 に固有のタイプのオブジェクトを識別します。

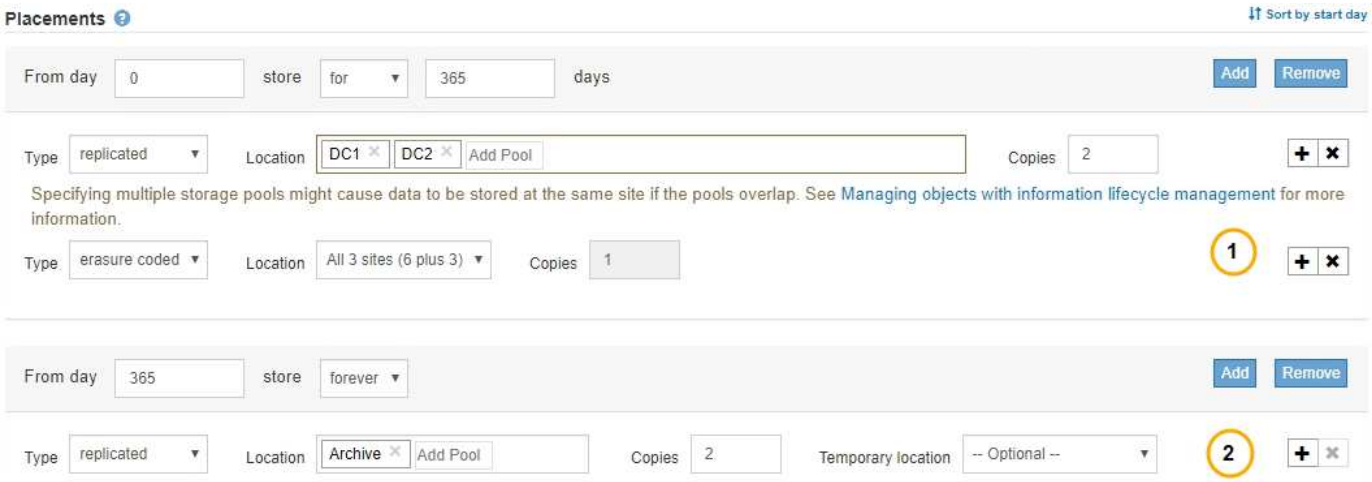
**ILM** ルールの配置手順とは

## 配置手順は、オブジェクトデータを格納する場所、タイミング、および方法を決定します。ILM ルールには 1 つ以上の配置手順を含めることができます。各配置手順環境 は一定期間です。

配置手順を作成するには、配置を適用するタイミング（期間）、作成するコピーのタイプ（レプリケートまたはイレイジャーコーディング）、およびコピーの格納先（1つ以上のストレージの場所）を指定します。単一のルール内で、1つの期間に複数の配置を指定でき、また複数の期間にそれぞれ違う配置手順を指定できます。

- 1つの期間に複数のオブジェクト配置を指定するには、プラス記号アイコンをクリックします ＋ をクリックして、期間に複数の行を追加します。
- 複数の期間にオブジェクト配置を指定するには、*追加*ボタンをクリックして次の期間を追加します。次に、期間内に 1 行以上の行を指定します。

この例は、 Create ILM Rule ウィザードの Define PI配置 ページを示しています。



| | |
|---|---|
| 1 | 1 つ目の配置手順には、 1 年目に 2 つの行があります。<br>1. 1 行目では、 2 つのデータセンターサイトに 2 つのレプリケートオブジェクトコピーが作成されます。<br>2. 2 行目には、 3 つのデータセンターサイトを使用して 6+3 のイレイジャーコーディングコピーが作成されます。 |
| 2 | 2 つ目の配置手順では、 1 年後にアーカイブコピーを 2 つ作成し、それらのコピーを無期限に保持します。 |

ルールに一連の配置手順を定義する場合は、少なくとも 1 つの配置手順が 0 日目に開始し、定義した期間の間にギャップがないことを確認する必要があります。 そして、最終的な配置手順は無期限またはオブジェクトコピーが不要になるまで継続されます。

ルールの各期間が終了すると、次の期間のコンテンツ配置手順が適用されます。新しいオブジェクトコピーが作成され、不要なコピーは削除されます。

ストレージグレード、ストレージプール、**EC**プロファイル、リージョンを作成する

StorageGRID システム用のILMルールを作成する前に、オブジェクトの格納場所を定義し、希望するコピーのタイプを決め、必要に応じてS3リージョンを設定する必要があります。

- "ストレージグレードを作成して割り当てます"
- "ストレージプールを設定しています"
- "クラウドストレージプールの使用"
- "イレイジャーコーディングプロファイルの設定"
- "リージョンの設定（オプション、S3のみ）"

ストレージグレードを作成して割り当てます

ストレージグレードは、ストレージノードで使用されているストレージのタイプを表します。サイトのすべてのノードではなく、特定のストレージノードに特定のオブジェクトを配置するように ILM ルールを設定する場合は、ストレージグレードを作成します。たとえば、 StorageGRID オールフラッシュストレージアプライアンスなどの最速のストレージノードに特定のオブジェクトを格納できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

複数のタイプのストレージを使用する場合は、各タイプを識別するストレージグレードを必要に応じて作成できます。ストレージグレードを作成すると、ストレージプールの構成時に特定のタイプのストレージノードを選択できるようになります。

ストレージグレードが重要でない場合（すべてのストレージノードが同じ場合など）は、この手順 をスキップし、ストレージプールの構成時にデフォルトのストレージグレードである All Storage Nodes を使用できます。

拡張で新しいストレージノードを追加すると、そのノードが「すべてのストレージノード」のデフォルトのストレージグレードに追加されます。その結果、次のようになります

- 「 All Storage Nodes 」グレードのストレージプールを使用する ILM ルールの場合、拡張の完了後すぐに新しいノードを使用できます。
- カスタムのストレージグレードを含むストレージプールを使用する ILM ルールの場合、以下に示すようにカスタムのストレージグレードをノードに手動で割り当てるまで新しいノードは使用されません。

> ストレージグレードは必要以上に作成しないでください。たとえば、ストレージノードごとにストレージグレードを作成するのではなく、各ストレージグレードを複数のノードに割り当てます。ストレージグレードを 1 つのノードにしか割り当てていない場合、そのノードが使用できなくなると原因 のバックログが発生する可能性があります。

手順

1. 「* ILM > Storage Grades *」を選択します。
2. ストレージグレードを作成します。

   a. 定義する必要があるストレージグレードごとに、*挿入*をクリックします アイコン"] をクリックして行を追加し、ストレージグレードのラベルを入力します。

      デフォルトのストレージグレードは変更できません。StorageGRID システムの拡張時に追加される新しいストレージノード用に予約されています。

Storage Grades

Updated: 2017-05-26 11:22:39 MDT

**Storage Grade Definitions**

| Storage Grade | Label | Actions |
|---|---|---|
| 0 | Default | |
| 1 | disk | |

**Storage Grades**

| LDR | Storage Grade | Actions |
|---|---|---|
| Data Center 1/DC1-S1/LDR | Default | |
| Data Center 1/DC1-S2/LDR | Default | |
| Data Center 1/DC1-S3/LDR | Default | |
| Data Center 2/DC2-S1/LDR | Default | |
| Data Center 2/DC2-S2/LDR | Default | |
| Data Center 2/DC2-S3/LDR | Default | |
| Data Center 3/DC3-S1/LDR | Default | |
| Data Center 3/DC3-S2/LDR | Default | |
| Data Center 3/DC3-S3/LDR | Default | |

Apply Changes

a. 既存のストレージグレードを編集するには、*編集*をクリックします をクリックし、必要に応じてラベルを変更します。

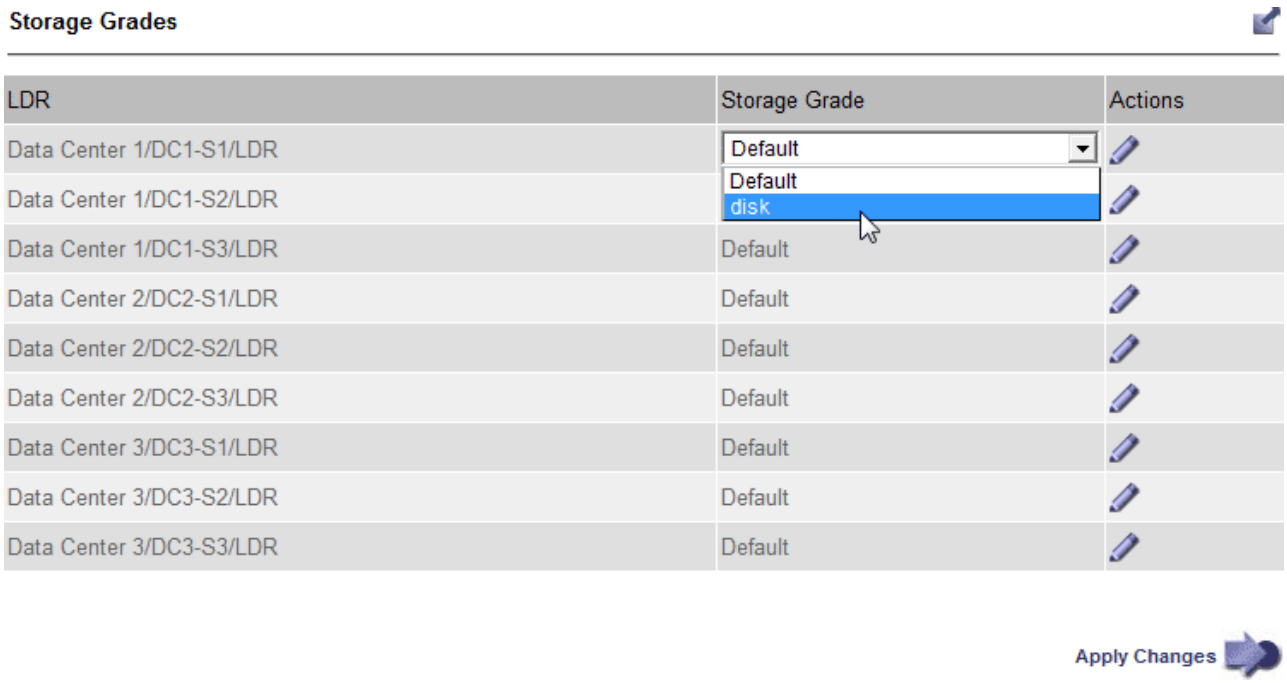
ストレージグレードを削除することはできません。

b. [ 変更の適用 *] をクリックします。

これで、ストレージグレードをストレージノードに割り当てることができます。

3. ストレージノードにストレージグレードを割り当てます。

a. 各ストレージノードのLDRサービスで、* Edit *をクリックします をクリックし、リストからストレージグレードを選択します。




特定のストレージノードにストレージグレードを割り当てることができるのは 1 回だけです。障害からリカバリしたストレージノードでは、以前に割り当てられていたストレージグレードが維持されます。ILM ポリシーをアクティブ化したあとに、この割り当てを変更しないでください。割り当てが変更されると、新しいストレージグレードに基づいてデータが格納されます。

a. [ 変更の適用 *] をクリックします。

ストレージプールを設定しています

ILMルールを定義する際には、ストレージプールを使用してオブジェクトの格納場所を指定します。ストレージプールを作成する前に、ストレージプールに関するガイドラインを確認してください。

- "ストレージプールとは"
- "ストレージプールの作成に関するガイドラインを次に示します"
- "複数のストレージプールを使用したサイト間レプリケーション"
- "一時的な場所としてのストレージプールの使用（廃止）"
- "ストレージプールを作成します"
- "ストレージプールの詳細を表示しています"
- "ストレージプールを編集する"
- "ストレージプールを削除しています"

ストレージプールとは

ストレージプールは、ストレージノードまたはアーカイブノードを論理的にグループ化したものです。ストレージプールの設定で、 StorageGRID システムがオブジェクトデー

タを格納する場所と、使用するストレージのタイプを決定します。

ストレージプールには 2 つの属性があります。

- * ストレージグレード * ：ストレージノードの場合は、バッキングストレージの相対的なパフォーマンス。
- * サイト * ：オブジェクトを格納するデータセンター。

ストレージプールは、オブジェクトデータの格納先を決定するために ILM ルールで使用されます。レプリケーションのための ILM ルールを設定する際は、ストレージノードまたはアーカイブノードを含むストレージプールを 1 つ以上選択します。イレイジャーコーディングプロファイルを作成する際は、ストレージノードを含むストレージプールを選択します。

ストレージプールの作成に関するガイドラインを次に示します

## ストレージプールを設定して使用する場合は、次のガイドラインに従ってください。

すべてのストレージプールのガイドライン

- StorageGRID には、デフォルトのストレージプールとすべてのストレージノードが含まれ、デフォルトサイト、すべてのサイト、およびデフォルトのストレージグレードであるすべてのストレージノードが使用されます。新しいデータセンターサイトを追加するたびに、 All Storage Nodes ストレージプールが自動的に更新されます。

> ⓘ All Storage Nodes ストレージプールまたはすべてのサイトサイトサイトは、拡張に追加する新しいサイトが自動的に更新されて追加されるため、推奨されません。これは動作ではない可能性があります。All Storage Nodes ストレージプールまたはデフォルトサイトを使用する前に、レプリケートコピーとイレイジャーコーディングコピーに関するガイドラインをよく確認してください。

- ストレージプールの設定は可能なかぎりシンプルにします。必要以上に多くのストレージプールを作成しないでください。
- できるだけ多くのノードを含むストレージプールを作成します。各ストレージプールには 2 つ以上のノードを含める必要があります。ノードが不十分なストレージプールでは、ノードが使用できなくなった場合に原因 ILM バックログが発生する可能性があります。
- 重複する（ 1 つ以上の同じノードを含む）ストレージプールを作成または使用することは避けてください。ストレージプールが重複していると、オブジェクトデータの複数のコピーが同じノードに保存される可能性があります。

レプリケートコピーに使用するストレージプールのガイドライン

- サイトごとに異なるストレージプールを作成します。次に、ルールごとに配置手順でサイト固有のストレージプールを 1 つ以上指定します。各サイトにストレージプールを使用すると、レプリケートされたオブジェクトコピーが想定どおりに配置されるようになります（たとえば、サイト障害から保護するために、各サイトのすべてのオブジェクトのコピーが 1 つずつ）。
- 拡張でサイトを追加する場合は、新しいサイト用の新しいストレージプールを作成します。次に、新しいサイトに格納するオブジェクトを制御するために ILM ルールを更新します。
- 通常は、デフォルトのストレージプール、すべてのストレージノード、またはデフォルトサイトであるすべてのサイトを含むストレージプールを使用しないでください。

イレイジャーコーディングされたコピーに使用するストレージプールのガイドラインを次に示します

- イレイジャーコーディングデータ用にアーカイブノードを使用することはできません。
- ストレージプールに含まれるストレージノードとサイトの数によって、使用できるイレイジャーコーディングスキームが決まります。
- ストレージプールにサイトが 2 つしかない場合、そのストレージプールをイレイジャーコーディングに使用することはできません。2 つのサイトを含むストレージプールではイレイジャーコーディングスキームを使用できません。
- 通常は、デフォルトのストレージプール、すべてのストレージノード、またはデフォルトサイトを含むすべてのサイトのいずれかのイレイジャーコーディングプロファイル内のストレージプールを使用しないでください。

> グリッドにサイトが 1 つしかない場合、イレイジャーコーディングプロファイルに「すべてのストレージノード」ストレージプールまたは「すべてのサイト」デフォルトサイトを使用することはできません。これにより、 2 つ目のサイトが追加された場合にイレイジャーコーディングプロファイルが無効になるのを防ぐことができます。

- 高スループットが必要な場合、サイト間のネットワークレイテンシが 100 ミリ秒を超える状況では、複数のサイトを含むストレージプールを作成することは推奨されません。レイテンシが上昇すると TCP ネットワークのスループットが低下するため、 StorageGRID がオブジェクトフラグメントを作成、配置、読み出す速度は大幅に低下します。スループットの低下は、オブジェクトの取り込みと読み出しの達成可能な最大速度に影響する（ Strict または Balanced が取り込み動作として選択されている場合）か、 ILM キューのバックログが発生する可能性があります（ Dual Commit が取り込み動作として選択されている場合）。
- 可能であれば、選択するイレイジャーコーディングスキームに必要な最小数よりも多くのストレージノードをストレージプールに含めてください。たとえば、 6+3 のイレイジャーコーディングスキームを使用する場合は、 9 個以上のストレージノードが必要です。ただし、サイトごとに少なくとも 1 つのストレージノードを追加することを推奨します。
- ストレージノードはサイト間にできるだけ均等に分散します。たとえば、 6+3 のイレイジャーコーディングスキームをサポートするには、 3 つのサイトにそれぞれ 1 つ以上のストレージノードを含むストレージプールを設定します。

アーカイブされたコピーに使用するストレージプールのガイドラインを次に示します

- ストレージノードとアーカイブノードの両方を含むストレージプールは作成できません。アーカイブされたコピーには、アーカイブノードのみを含むストレージプールが必要です。
- アーカイブノードが含まれたストレージプールを使用する場合は、ストレージノードが含まれたストレージプール上に、 1 つ以上のレプリケートコピーまたはイレイジャーコーディングコピーを保持する必要もあります。
- グローバルな S3 オブジェクトロック設定が有効になっていて準拠 ILM ルールを作成する場合は、アーカイブノードが含まれたストレージプールを使用できません。S3 オブジェクトロックを使用してオブジェクトを管理する手順を参照してください。
- アーカイブノードの Target Type が「 Cloud Tiering - Simple Storage Service （ S3 ）」の場合、そのアーカイブノードは自身のストレージプールに含まれている必要があります。StorageGRID の管理手順を参照してください。

関連情報

"レプリケーションとは"

"イレイジャーコーディングとは"

"イレイジャーコーディングスキームとは"

"複数のストレージプールを使用したサイト間レプリケーション"

"一時的な場所としてのストレージプールの使用（廃止）"

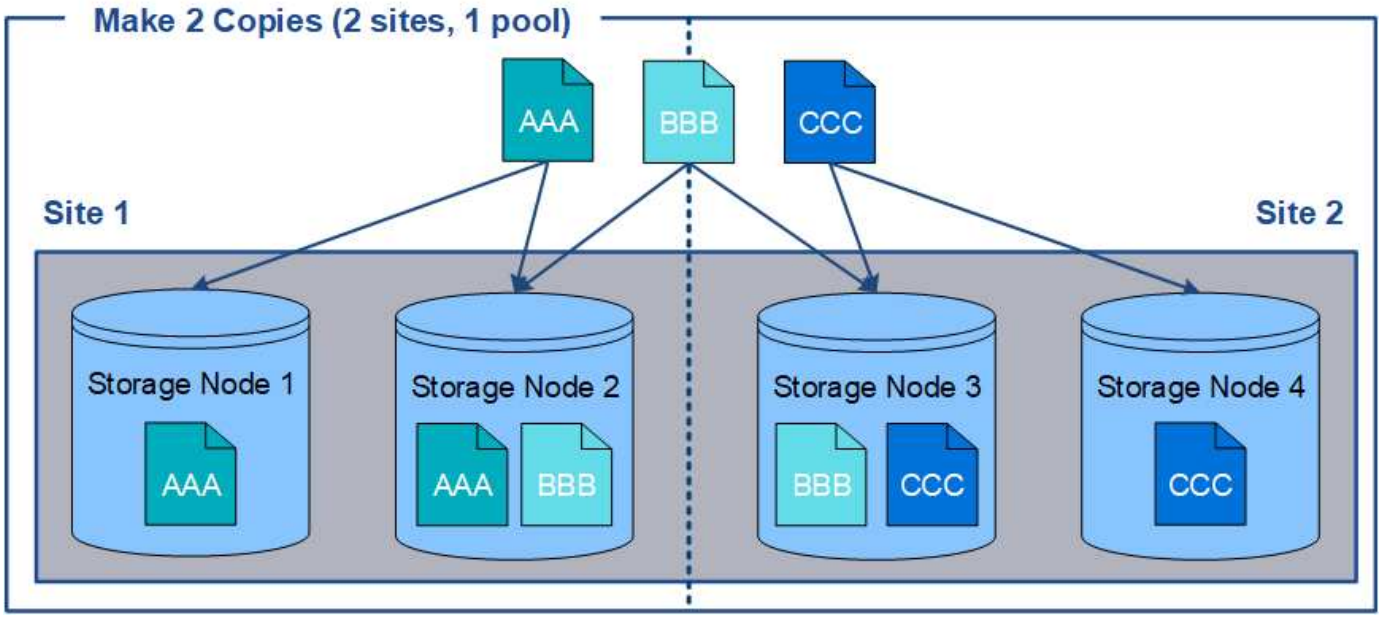
"S3オブジェクトロックでオブジェクトを管理する"

"StorageGRID の管理"

複数のストレージプールを使用したサイト間レプリケーション

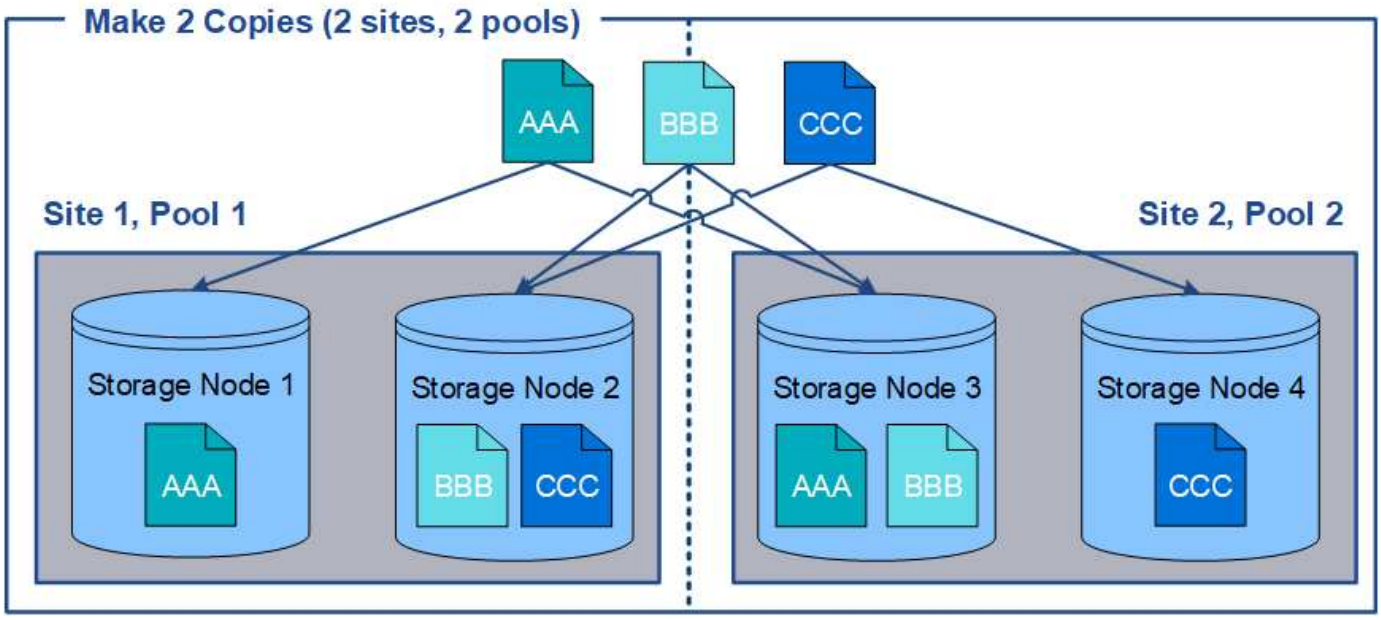
StorageGRID 環境に複数のサイトが含まれている場合は、各サイトにストレージプールを 1 つずつ作成し、ルールの配置手順に両方のストレージプールを指定することで、サイト障害から保護できます。たとえば、 2 つのレプリケートコピーを作成する ILM ルールを設定して、 2 つのサイトのストレージプールを指定すると、各オブジェクトのコピーが各サイトに 1 つずつ配置されます。2 つのコピーを作成するルールを設定して 3 つのストレージプールを指定すると、 2 つのコピーが別々のサイトに格納される際、ストレージプール間のディスク使用量のバランスを保つようにコピーが分散されます。

次の例は、 ILM ルールによって 2 つのサイトのストレージノードを含む単一のストレージプールにレプリケートオブジェクトコピーが配置された場合にどうなるかを示しています。レプリケートコピーがストレージプール内の使用可能な任意のノードに配置されるため、一部のオブジェクトのすべてのコピーが 1 つのサイト内にのみ配置される可能性があります。この例では、システムはオブジェクト AAA の 2 つのコピーをサイト 1 の別々のストレージノードに、オブジェクト CCC の 2 つのコピーをサイト 2 の別々のストレージノードに格納しています。いずれかのサイトで障害が発生したりアクセスできなくなった場合、保護されるのはオブジェクト BBB だけです。




一方、この例は、複数のストレージプールを使用した場合のオブジェクトの格納方法を示しています。この例の ILM ルールは、各オブジェクトのレプリケートコピーを 2 つ作成して 2 つのストレージプールに分散するように指定されています。各ストレージプールには一方のサイトのすべてのストレージノードが含まれていま

す。各オブジェクトのコピーは各サイトに格納されるため、オブジェクトデータはサイトの障害やサイトへのアクセス障害から保護されます。




複数のストレージプールを使用する場合は、次の点に注意してください。

- n 個のコピーを作成する場合は、 n 個以上のストレージプールを追加する必要があります。たとえば、 3 つのコピーを作成するようにルールが設定されている場合は、ストレージプールを 3 つ以上指定する必要があります。
- コピーの数がストレージプールの数と同じ場合は、オブジェクトのコピーが 1 つずつ各ストレージプールに格納されます。
- コピーの数がストレージプールの数より少ない場合、プール間のディスク使用量のバランスを維持し、複数のコピーが同じストレージプールに格納されないようにコピーが分散されます。
- ストレージプールが重複している（同じストレージノードを含んでいる）場合は、オブジェクトのすべてのコピーが 1 つのサイトにのみ保存される可能性があります。選択したストレージプールに同じストレージノードが含まれていないことを確認する必要があります。

一時的な場所としてのストレージプールの使用（廃止）

ストレージプールを 1 つ含むオブジェクトの配置を使用して ILM ルールを作成する場合は、一時的な場所として使用する 2 つ目のストレージプールを指定するように求められます。

一時的な場所は廃止されており、今後のリリースで削除される予定です。ストレージプールは、新しい ILM ルールの一時的な場所として選択しないでください。

Strict 取り込み動作を選択した場合（ Create ILM Rule ウィザードのステップ 3 ）、一時的な場所は無視されます。

関連情報

"取り込みのデータ保護オプション"

# ストレージプールを作成することで、 StorageGRID システムがオブジェクトデータを格納する場所と、使用するストレージのタイプを決定します。各ストレージプールには、サイトとストレージグレードがそれぞれ 1 つ以上含まれています。

## 必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- ストレージプールの作成に関するガイドラインを確認しておく必要があります。

## このタスクについて

ストレージプールは、オブジェクトデータの格納場所を決定します。必要なストレージプールの数は、グリッド内のサイトの数と、レプリケートコピーまたはイレイジャーコーディングコピーのタイプによって異なります。

- レプリケーションおよび単一サイトのイレイジャーコーディングの場合は、サイトごとにストレージプールを作成します。たとえば、レプリケートオブジェクトコピーを 3 つのサイトに格納する場合は、ストレージプールを 3 つ作成します。
- 3 つ以上のサイトでイレイジャーコーディングする場合は、サイトごとに 1 つのエントリを含むストレージプールを 1 つ作成します。たとえば、 3 つのサイトにまたがるオブジェクトをイレイジャーコーディングする場合は、ストレージプールを 1 つ作成します。プラスアイコンを選択します ➕ アイコン"] をクリックして、各サイトのエントリを追加します。

> ⓘ イレイジャーコーディングプロファイルで使用されるストレージプールには、デフォルトの All Sites サイトを含めないでください。代わりに、イレイジャーコーディングデータを格納するサイトごとにストレージプールにエントリを追加します。を参照してください この手順を実行します たとえば、のように指定します。

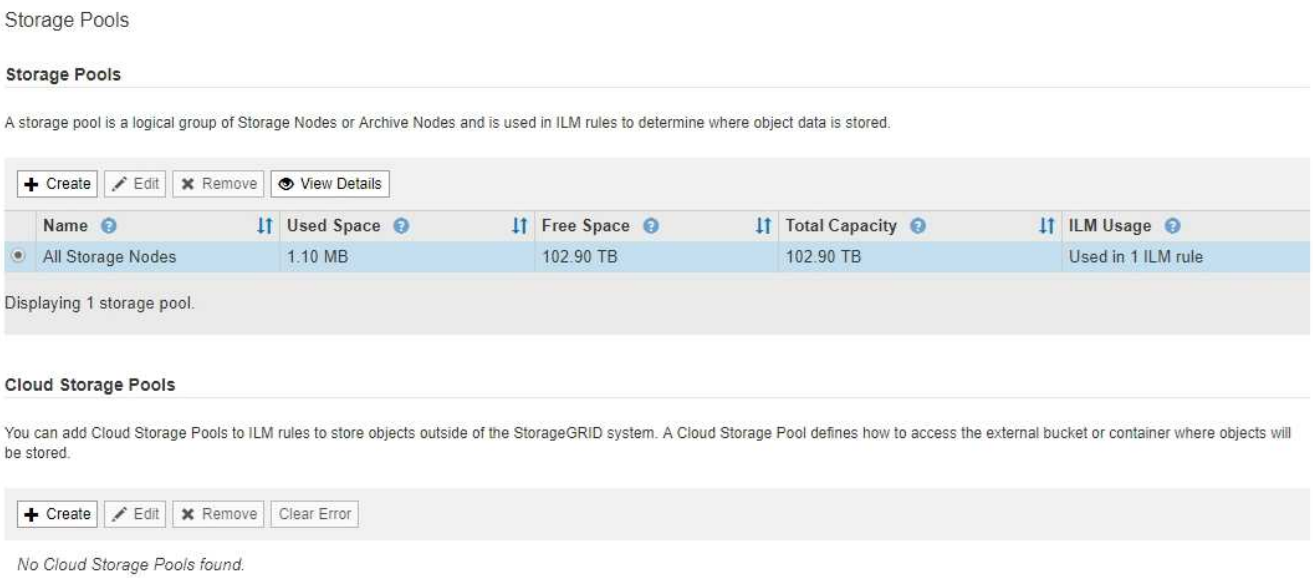
- ストレージグレードが複数ある場合は、 1 つのサイトに異なるストレージグレードを含むストレージプールを作成しないでください。

  "ストレージプールの作成に関するガイドラインを次に示します"

## 手順

1. ILM > Storage Pools *を選択します。

   Storage Pools （ストレージプール）ページが表示され、定義済みのすべてのストレージプールがリストされます。

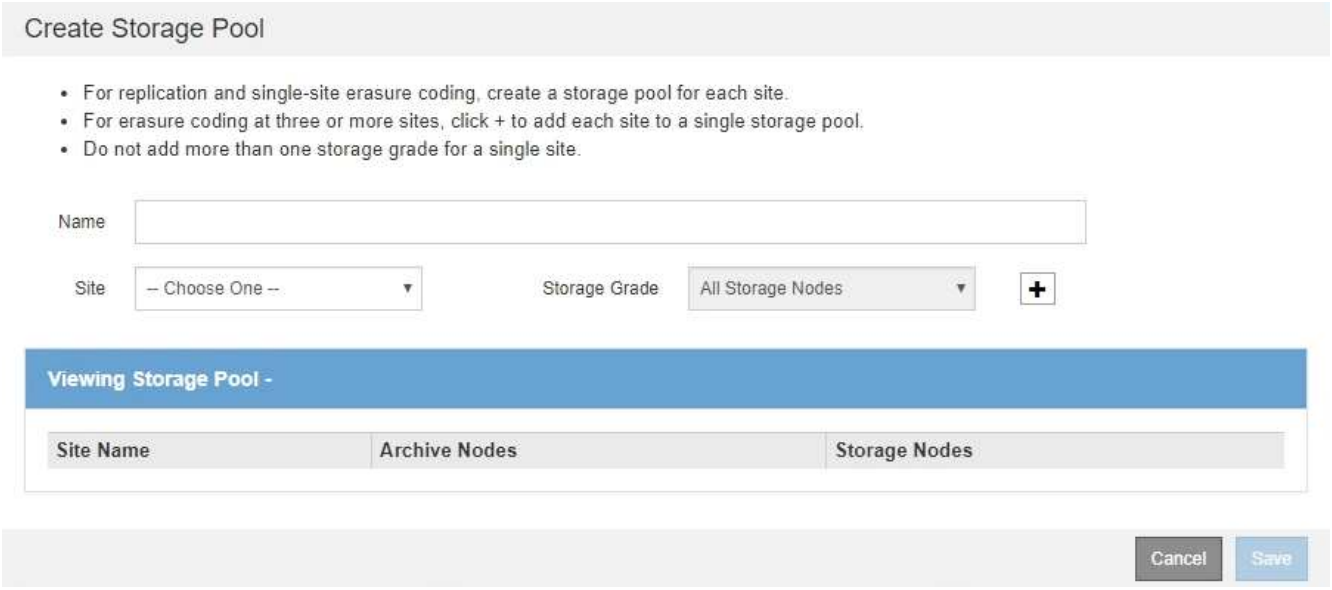



リストには、システムデフォルトのストレージプール、システムデフォルトサイトのすべてのサイトを使用するすべてのストレージノード、およびデフォルトのストレージグレードであるすべてのストレージノードが含まれます。

> All Storage Nodes ストレージプールは、新しいデータセンターサイトを追加するたびに自動的に更新されるため、 ILM ルールでこのストレージプールを使用することは推奨されません。

2. 新しいストレージプールを作成するには、「 * 作成」を選択します。

   Create Storage Pool （ストレージプールの作成）ダイアログボックスが表示されます。




3. ストレージプールの一意の名前を入力します。

   イレイジャーコーディングプロファイルと ILM ルールを設定するときに識別しやすい名前を使用してください。

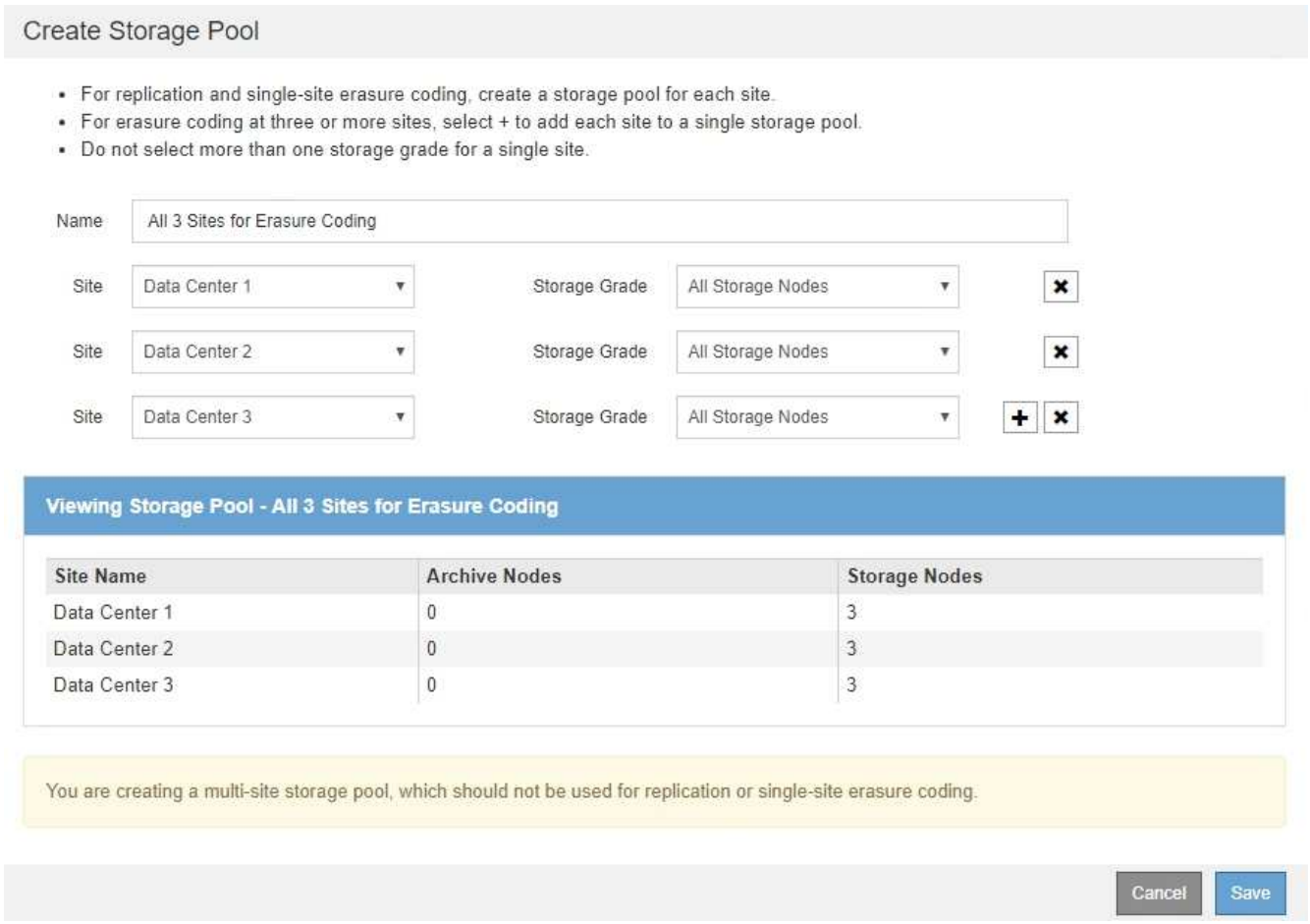
4. [*Site *] ドロップダウン・リストから ' このストレージ・プールのサイトを選択します

   サイトを選択すると、表内のストレージノードとアーカイブノードの数が自動的に更新されます。

5. ストレージグレード * ドロップダウンリストから、 ILM ルールでこのストレージプールを使用する場合に使用するストレージのタイプを選択します。

   デフォルトの All Storage Nodes ストレージグレードには、選択したサイトのすべてのストレージノードが含まれます。Default Archive Nodes ストレージグレードには、選択したサイトのすべてのアーカイブノードが含まれます。グリッド内のストレージノード用にストレージグレードを追加で作成している場合、そのグレードもドロップダウンに表示されます。

6. [[entries] ]] マルチサイトイレイジャーコーディングプロファイルでストレージプールを使用する場合は、を選択します ➕ アイコン"] をクリックして、各サイトのエントリをストレージプールに追加します。




   重複するエントリを作成したり、 * アーカイブノード * ストレージグレードとストレージノードを含むストレージグレードの両方を含むストレージプールを作成したりすることはできません。

   サイトに複数のエントリを追加しても、ストレージグレードが異なる場合は警告が表示されます。

   エントリを削除するには、を選択します ✖。

7. 選択に問題がなければ、 * 保存 * を選択します。

新しいストレージプールがリストに追加されます。

関連情報

"ストレージプールの作成に関するガイドラインを次に示します"

ストレージプールの詳細を表示しています

# ストレージプールの詳細を表示して、ストレージプールの使用場所を確認したり、含まれているノードやストレージグレードを確認したりできます。

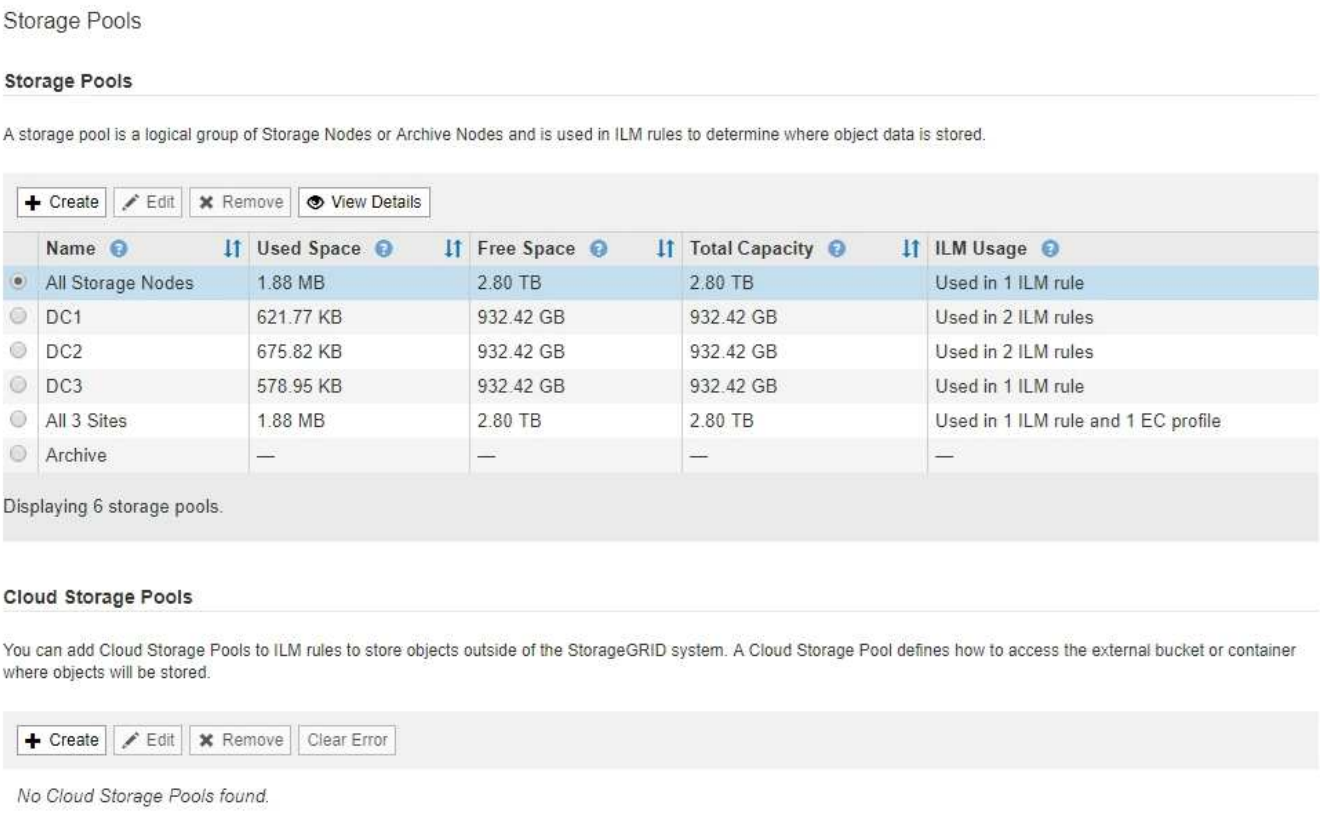
必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

手順

1. ILM > Storage Pools *を選択します。

   Storage Pools （ストレージプール）ページが表示されます。このページには、定義済みのストレージプールがすべて表示されます。




   この表には、ストレージノードを含む各ストレージプールに関する次の情報が含まれています。

   - * Name * ：ストレージプールの一意の表示名。
   - * Used Space * ：ストレージプールにオブジェクトを格納するために現在使用されているスペースの量。

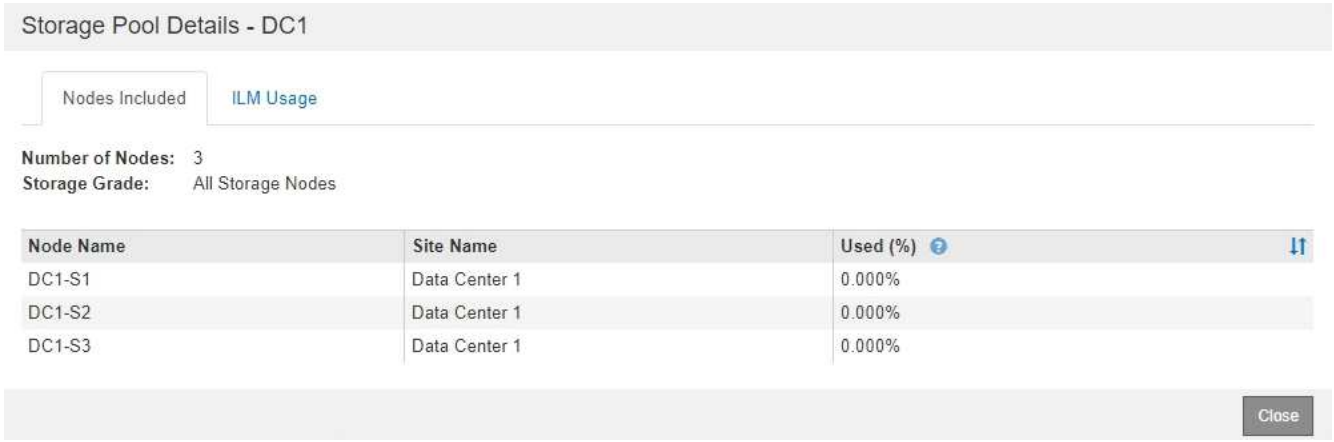
- * Free Space * ：ストレージプールにオブジェクトを格納するために使用可能な残りのスペース。
- * Total Capacity * ：ストレージプールのサイズ。ストレージプール内のすべてのノードのオブジェクトデータに使用可能なスペースの合計に相当します。
- * ILM Usage * ：ストレージプールの現在の使用状況。ストレージプールは、使用されていない場合や、 1 つ以上の ILM ルール、イレイジャーコーディングプロファイル、またはその両方で使用されている場合があります。

> 使用中のストレージプールは削除できません。

2. 特定のストレージプールの詳細を表示するには、そのラジオボタンを選択し、「 * 詳細を表示 * 」を選択します。

   Storage Pool Details モーダルが表示されます。

3. 「 Nodes included * 」タブを表示して、ストレージプールに含まれるストレージノードまたはアーカイブノードについて確認します。



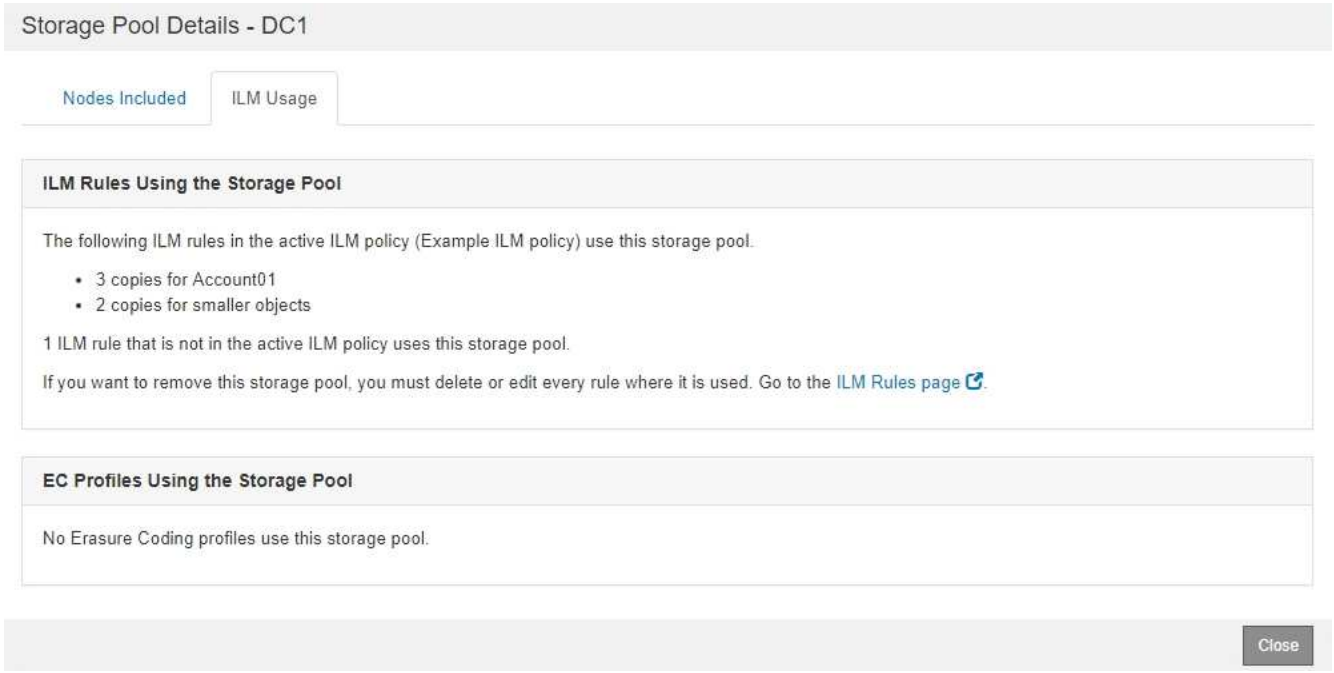

   この表には、ノードごとに次の情報が記載されています。

   - ノード名
   - サイト名
   - 使用済み（ % ）：ストレージノードの場合、オブジェクトデータに使用されている合計使用可能スペースの割合。この値にはオブジェクトメタデータは含まれません。

> 各ストレージノードのStorage Used - Object Dataチャートにも同じ使用済み（%）値が表示されます（* Nodes ***>*Storage Node***>* Storage *）。

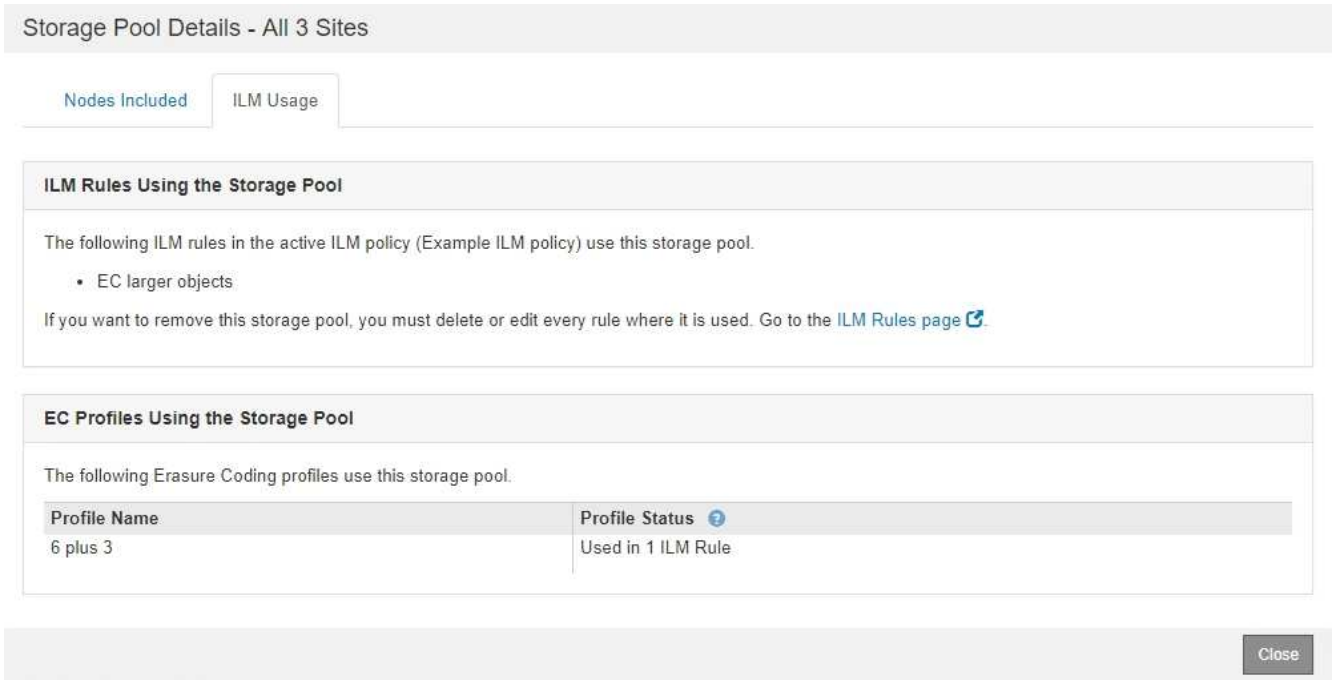
4. 「 * ILM Usage * 」タブを選択して、ストレージプールが現在 ILM ルールやイレイジャーコーディングプロファイルで使用されているかどうかを確認します。

   この例では、 DC1 ストレージプールは、アクティブな ILM ポリシーに含まれる 2 つのルールとアクティブなポリシーに含まれない 1 つのルールという 3 つの ILM ルールで使用されます。




ILM ルールで使用されているストレージプールは削除できません。

この例では、 All 3 Sites ストレージプールがイレイジャーコーディングプロファイルで使用されています。そのイレイジャーコーディングプロファイルは、アクティブな ILM ポリシー内の 1 つの ILM ルールによって使用されます。




イレイジャーコーディングプロファイルで使用されているストレージプールは削除できません。

5. 必要に応じて、 * ILM Rules ページ * に移動し、ストレージプールを使用するルールの確認と管理を行います。

ILM ルールの操作手順を参照してください。

6. ストレージプールの詳細の表示が完了したら、「 * 閉じる * 」を選択します。

関連情報

"ILMルールおよびILMポリシーの操作"

ストレージプールを編集する

## ストレージプールを編集して、名前を変更したり、サイトやストレージグレードを更新したりできます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- ストレージプールの作成に関するガイドラインを確認しておく必要があります。
- アクティブなILMポリシーのルールで使用されているストレージプールを編集する場合は、変更がオブジェクトデータの配置にどのように影響するかを考慮する必要があります。

このタスクについて

アクティブな ILM ポリシーで使用されているストレージプールに新しいストレージグレードを追加する場合は、新しいストレージグレードのストレージノードが自動的には使用されないことに注意してください。StorageGRID で新しいストレージグレードを強制的に使用するには、編集したストレージプールを保存したあとに新しい ILM ポリシーをアクティブ化する必要があります。

手順

1. ILM > Storage Pools *を選択します。

   Storage Pools （ストレージプール）ページが表示されます。

2. 編集するストレージプールのラジオボタンを選択します。

   All Storage Nodes ストレージプールは編集できません。

3. 「 * 編集 * 」を選択します。
4. 必要に応じて、ストレージプール名を変更します。
5. 必要に応じて、他のサイトとストレージグレードを選択します。

   ストレージプール原因 がイレイジャーコーディングプロファイルで使用されている場合や、イレイジャーコーディングスキームを無効に変更する場合、サイトまたはストレージグレードを変更することはできません。たとえば、イレイジャーコーディングプロファイルで使用されているストレージプールにサイトが 1 つしかないストレージグレードが含まれている場合、サイトが 2 つのストレージグレードを使用することはできません。これは、変更によってイレイジャーコーディングスキームが無効になるためです。

6. [ 保存（ Save ） ] を選択します。

完了後

アクティブな ILM ポリシーで使用されているストレージプールに新しいストレージグレードを追加した場合は、新しい ILM ポリシーをアクティブ化して StorageGRID に新しいストレージグレードを強制的に使用させます。たとえば、既存の ILM ポリシーのクローンを作成し、そのクローンをアクティブ化します。

ストレージプールを削除しています

## 使用されていないストレージプールは削除できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

手順

1. ILM > Storage Pools *を選択します。

   Storage Pools （ストレージプール）ページが表示されます。

2. テーブルの ILM Usage 列を参照して、ストレージプールを削除できるかどうかを確認します。

   ストレージプールが ILM ルールまたはイレイジャーコーディングプロファイルで使用されている場合、ストレージプールを削除することはできません。必要に応じて、 * View Details * > * ILM Usage * の順に選択して、ストレージプールの使用場所を決定します。

3. 削除するストレージプールが使用されていない場合は、ラジオボタンを選択します。
4. 「 * 削除」を選択します。
5. 「 * OK 」を選択します。

クラウドストレージプールの使用

## クラウドストレージプールを使用して、StorageGRID オブジェクトをS3 GlacierやMicrosoft Azure BLOBストレージなどの外部ストレージに移動できます。オブジェクトをグリッドの外部に移動すると、低コストのストレージ階層を活用した長期間のアーカイブが可能になります。

- "クラウドストレージプールとは"
- "クラウドストレージプールオブジェクトのライフサイクル"
- "クラウドストレージプールを使用する状況"
- "クラウドストレージプールに関する考慮事項"
- "クラウドストレージプールと CloudMirror レプリケーションを比較しています"
- "クラウドストレージプールの作成"
- "クラウドストレージプールの編集"
- "クラウドストレージプールの削除"
- "クラウドストレージプールのトラブルシューティング"

# クラウドストレージプールとは

クラウドストレージプールでは、 ILM を使用して StorageGRID システムの外部にオブジェクトデータを移動できます。たとえば、 Amazon S3 Glacier 、 S3 Glacier Deep Archive 、 Microsoft Azure Blob Storage のアーカイブアクセス階層など、アクセス頻度の低いオブジェクトを低コストのクラウドストレージに移動できます。または、 StorageGRID オブジェクトのクラウドバックアップを保持して、ディザスタリカバリを強化することもできます。

ILM から見た場合、クラウドストレージプールはストレージプールに似ています。どちらの場所にオブジェクトを格納する場合も、 ILM ルールの配置手順の作成時にプールを選択します。ただし、ストレージプールは StorageGRID システム内のストレージノードまたはアーカイブノードで構成されますが、クラウドストレージプールは外部のバケット（ S3 ）またはコンテナ（ Azure BLOB ストレージ）で構成されます。

次の表に、ストレージプールとクラウドストレージプールの比較と、類似点と相違点を示します。

| | ストレージプール | クラウドストレージプール |
|---|---|---|
| 作成方法 | Grid Managerで* ILM *>*ストレージプール*オプションを使用する。<br><br>ストレージプールを作成する前に、ストレージグレードをセットアップする必要があります。 | Grid Managerで* ILM *>*ストレージプール*オプションを使用する。<br><br>クラウドストレージプールを作成する前に、外部のバケットまたはコンテナをセットアップする必要があります。 |
| 作成できるプール数 | 無制限。 | 最大 10 個。 |

| | ストレージプール | クラウドストレージプール |
| --- | --- | --- |
| オブジェクトの格納先 | StorageGRID 内の 1 つ以上のストレージノードまたはアーカイブノード。 | StorageGRID システムの外部にある Amazon S3 バケットまたは Azure BLOB ストレージコンテナ。<br><br>クラウドストレージプールが Amazon S3 バケットの場合：<br><br>• 必要に応じて、 Amazon S3 Glacier や S3 Glacier Deep Archive などの低コストの長期保存用ストレージにオブジェクトを移行するようにバケットライフサイクルを設定できます。外部ストレージシステムが Glacier ストレージクラスと S3 POST Object restore API をサポートしている必要があります。<br>• AWS Commercial クラウド サービス（ C2S ）で使用するクラウドストレージプールを作成できます。 C2S は AWS Secret Region をサポートします。<br><br>クラウドストレージプールが Azure BLOB ストレージコンテナの場合、 StorageGRID はオブジェクトをアーカイブ層に移行します。<br><br>• 注：一般に、クラウドストレージプールに使用するコンテナには Azure Blob Storage のライフサイクル管理を設定しないでください。クラウドストレージプール内のオブジェクトに対する POST Object restore 処理が、設定されたライフサイクルの影響を受ける可能性があります。 |
| オブジェクトの配置を制御する要素 | アクティブな ILM ポリシーの ILM ルール。 | アクティブな ILM ポリシーの ILM ルール。 |
| 使用されるデータ保護方法 | レプリケーションまたはイレイジャーコーディング。 | レプリケーション： |
| 各オブジェクトに許可されるコピー数 | 複数。 | クラウドストレージプールに 1 つ、また必要に応じて StorageGRID に 1 つ以上のコピーを作成します。<br><br>• 注： * 1 つのオブジェクトを複数のクラウドストレージプールに一度に格納することはできません。 |

| | ストレージプール | クラウドストレージプール |
|---|---|---|
| 利点は何ですか？ | オブジェクトにいつでもすばやくアクセスできる。 | 低コストのストレージ。 |

クラウドストレージプールオブジェクトのライフサイクル

## クラウドストレージプールを実装する前に、クラウドストレージプールのタイプごとに格納されているオブジェクトのライフサイクルを確認してください。

関連情報

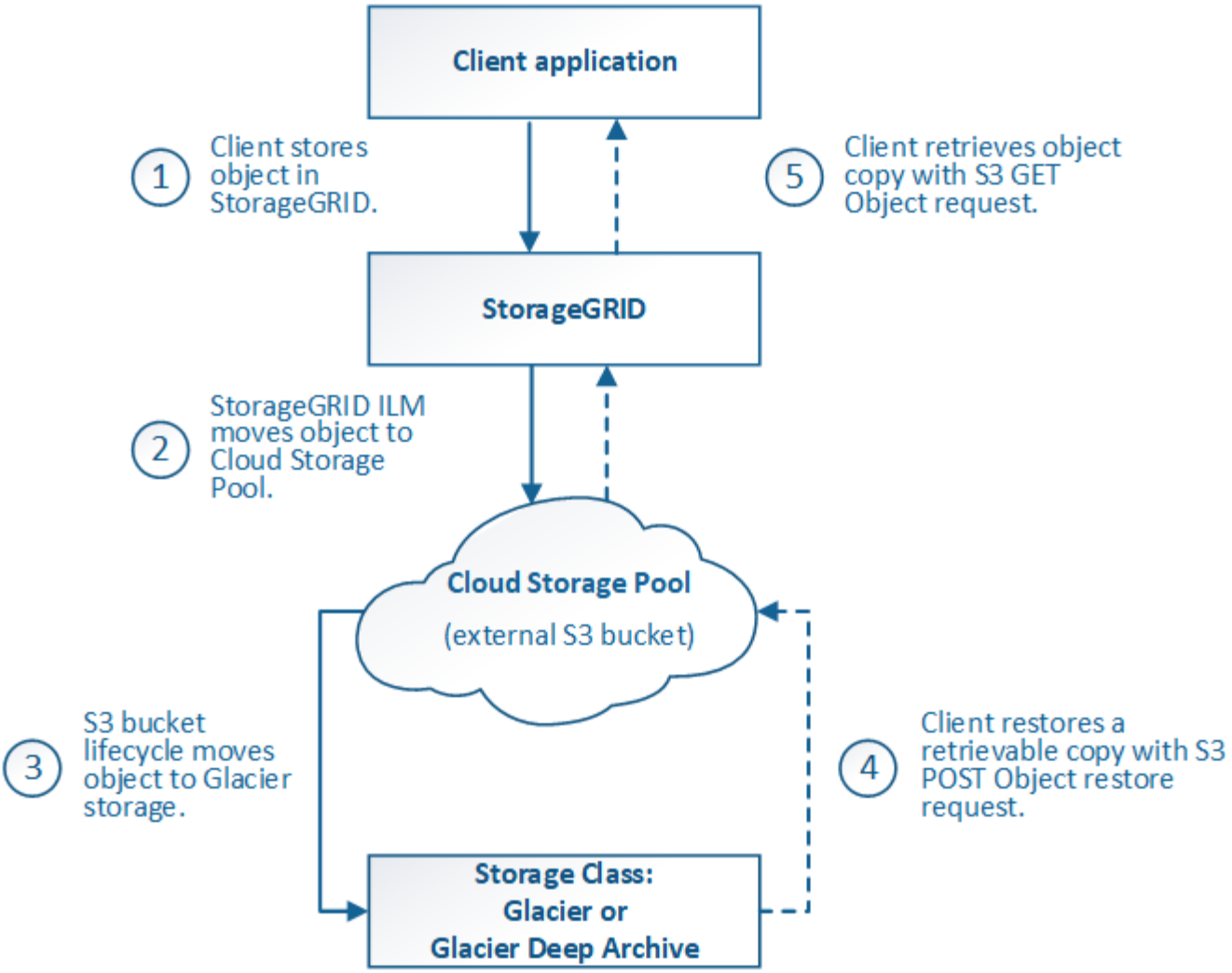
S3 ：クラウドストレージプールオブジェクトのライフサイクル

Azure ：クラウドストレージプールオブジェクトのライフサイクル]

### S3 ：クラウドストレージプールオブジェクトのライフサイクル

次の図は、 S3 クラウドストレージプールに格納されているオブジェクトのライフサイクルステージを示しています。

この図と説明にある「 Glacier 」は、 Glacier ストレージクラスと Glacier Deep Archive ストレージクラスの両方を意味します。ただし例外が 1 つあり、 Glacier Deep Archive ストレージクラスでは Expedited リストア階層はサポートされず、Bulk または Standard のみがサポートされます。




1. * StorageGRID * に格納されているオブジェクト

   ライフサイクルを開始するために、クライアントアプリケーションがオブジェクトを StorageGRID に格納します。

2. * オブジェクトを S3 クラウドストレージプールに移動 *

   - S3 クラウドストレージプールを配置場所として使用する ILM ルールにオブジェクトが一致した場合、 StorageGRID はクラウドストレージプールで指定された外部の S3 バケットにオブジェクトを移動します。
   - オブジェクトが S3 クラウドストレージプールに移動されると、クライアントアプリケーションは、オブジェクトが Glacier ストレージに移行されていないかぎり、 StorageGRID から S3 GET Object 要求を使用してオブジェクトを読み出すことができます。

3. * オブジェクトを Glacier に移行（読み出し不可の状態） *

   - 必要に応じて、オブジェクトを Glacier ストレージに移行できます。たとえば外部の S3 バケットが、ライフサイクル設定を使用してオブジェクトを即座または数日後に Glacier ストレージに移行できます。

オブジェクトを移行する場合は、外部の S3 バケット用のライフサイクル設定を作成する必要があります。また、 Glacier ストレージクラスを実装し、 S3 POST Object restore API をサポートするストレージ解決策 を使用する必要があります。

Swift クライアントによって取り込まれたオブジェクトには、クラウドストレージプールを使用しないでください。Swift では POST Object restore 要求がサポートされないため、StorageGRID は S3 Glacier ストレージに移行された Swift オブジェクトを読み出せません。これらのオブジェクトを読み出す Swift GET object 要求は失敗します（ 403 Forbidden ）。

- 移行中、クライアントアプリケーションは S3 HEAD Object 要求を使用してオブジェクトのステータスを監視できます。

4. * Glacier ストレージからオブジェクトをリストア *

   オブジェクトが Glacier ストレージに移行されている場合、クライアントアプリケーションは S3 POST Object restore 要求を問題 で実行して、読み出し可能なコピーを S3 クラウドストレージプールにリストアできます。要求では、クラウドストレージプールでコピーを利用できる日数と、リストア処理に使用するデータアクセス階層（ Expedited 、 Standard 、 Bulk ）を指定します。読み出し可能なコピーの有効期限に達すると、コピーは自動的に読み出し不可能な状態に戻ります。

   StorageGRID 内のストレージノードにもオブジェクトのコピーが存在する場合、 POST Object restore 要求を実行して Glacier からオブジェクトをリストアする必要はありません。GET Object 要求を使用してローカルコピーを直接読み出すことができます。

5. * オブジェクトが取得されました *

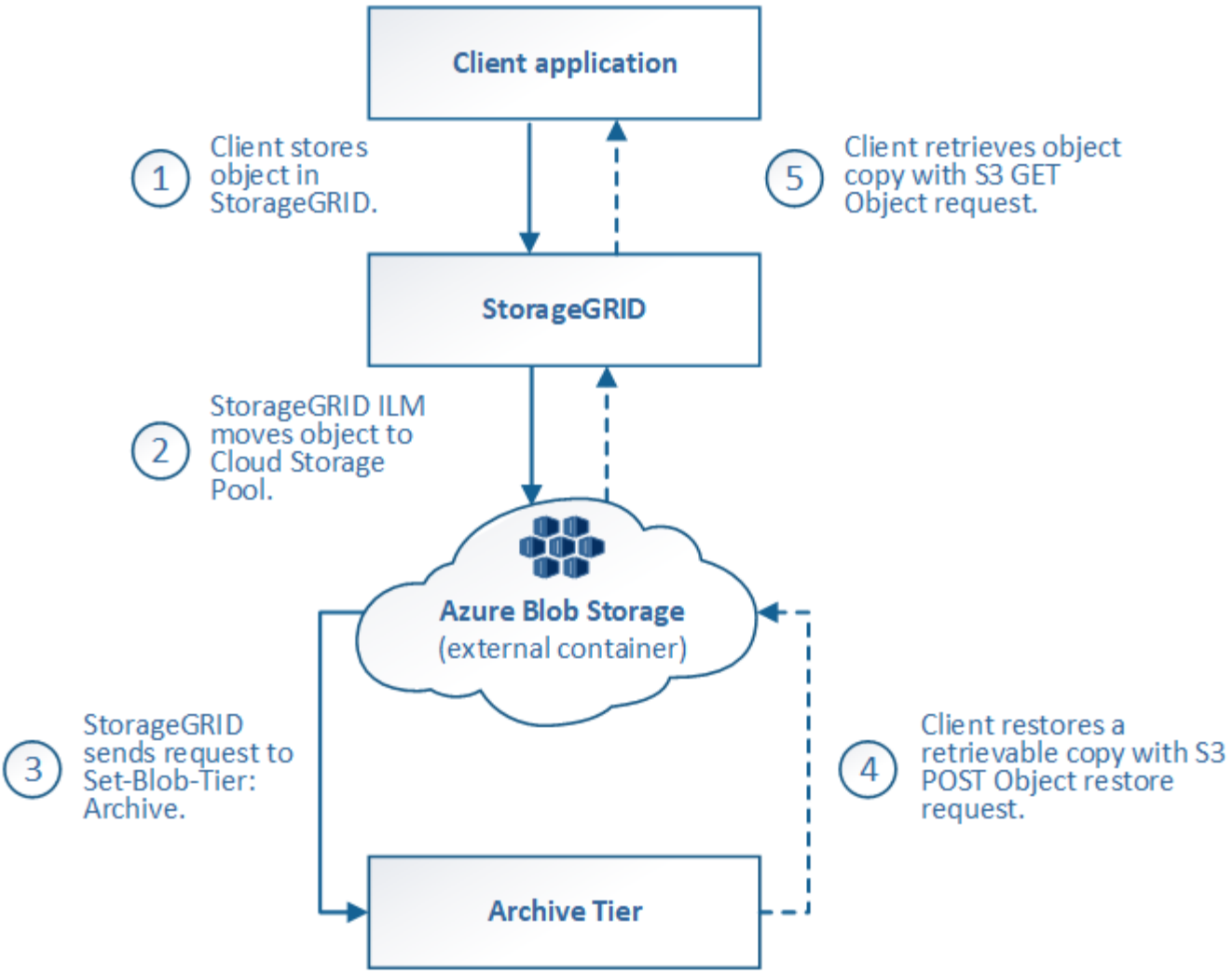
   オブジェクトがリストアされると、クライアントアプリケーションは GET Object 要求を問題 で実行して、リストアされたオブジェクトを読み出すことができます。

関連情報

"S3 を使用する"

**Azure** ：クラウドストレージプールオブジェクトのライフサイクル

次の図は、 Azure クラウドストレージプールに格納されているオブジェクトのライフサイクルステージを示しています。




1. * StorageGRID * に格納されているオブジェクト

   ライフサイクルを開始するために、クライアントアプリケーションがオブジェクトを StorageGRID に格納します。

2. * オブジェクトを Azure クラウドストレージプールに移動 *

   Azure クラウドストレージプールを配置場所として使用する ILM ルールにオブジェクトが一致した場合、StorageGRID はクラウドストレージプールで指定された外部の Azure BLOB ストレージコンテナにオブジェクトを移動します

   > Swift クライアントによって取り込まれたオブジェクトには、クラウドストレージプールを使用しないでください。Swift では POST Object restore 要求がサポートされないため、StorageGRID は Azure BLOB ストレージのアーカイブ層に移行された Swift オブジェクトを読み出せません。これらのオブジェクトを読み出す Swift GET object 要求は失敗します（ 403 Forbidden ）。

3. * オブジェクトをアーカイブ層に移行（読み出し不可の状態） *

   オブジェクトを Azure クラウドストレージプールに移動すると、 StorageGRID は自動的にオブジェクトを Azure BLOB ストレージのアーカイブ層に移行します。

4. * アーカイブ層からオブジェクトを復元 *

   オブジェクトがアーカイブ層に移行されている場合、クライアントアプリケーションは S3 POST Object restore 要求を問題 で実行して、読み出し可能なコピーを Azure クラウドストレージプールにリストアできます。

   POST Object Restore を受け取った StorageGRID は、オブジェクトを一時的に Azure BLOB ストレージのクール層に移行します。POST Object restore 要求の有効期限に達すると、 StorageGRID はオブジェクトをアーカイブ層に戻します。

   > StorageGRID 内のストレージノードにもオブジェクトのコピーが存在する場合、 POST Object restore 要求を実行してアーカイブアクセス階層からオブジェクトをリストアする必要はありません。GET Object 要求を使用してローカルコピーを直接読み出すことができます。

5. * オブジェクトが取得されました *

   オブジェクトが Azure クラウドストレージプールにリストアされると、クライアントアプリケーションは、リストアされたオブジェクトを読み出すための GET Object 要求を問題 に送信できます。

クラウドストレージプールを使用する状況

## クラウドストレージプールは、いくつかのユースケースで大きなメリットをもたらします。

外部の場所にある **StorageGRID** データのバックアップ

クラウドストレージプールを使用して、 StorageGRID オブジェクトを外部の場所にバックアップできます。

StorageGRID 内のコピーにアクセスできない場合は、クラウドストレージプール内のオブジェクトデータを使用してクライアント要求を処理できます。ただし、クラウドストレージプール内のバックアップオブジェクトコピーにアクセスするには、問題 S3 POST Object restore 要求が必要になる場合があります。

クラウドストレージプール内のオブジェクトデータは、ストレージボリュームまたはストレージノードの障害が原因で失われたデータを StorageGRID からリカバリする場合にも使用できます。オブジェクトのコピーがクラウドストレージプールにしか残っていない場合、 StorageGRID はオブジェクトを一時的にリストアして、リカバリされたストレージノードに新しいコピーを作成します。

バックアップ解決策 を実装するには

1. 単一のクラウドストレージプールを作成する。
2. ストレージノードにオブジェクトコピーを（レプリケートコピーまたはイレイジャーコーディングコピーとして）同時に格納し、クラウドストレージプールにオブジェクトコピーを 1 つ格納する ILM ルールを設定します。
3. ルールを ILM ポリシーに追加します。次に、ポリシーをシミュレートしてアクティブ化します。

**StorageGRID** から外部の場所へのデータの階層化

クラウドストレージプールを使用して、 StorageGRID システムの外部にオブジェクトを格納できます。たとえば、保持する必要のあるオブジェクトが多数あり、それらのオブジェクトにアクセスすることはほとんどありません。クラウドストレージプールを使用してオブジェクトを低コストのストレージに階層化し、

StorageGRID のスペースを解放できます。

階層化解決策 を実装するには：

1. 単一のクラウドストレージプールを作成する。
2. 使用頻度の低いオブジェクトをストレージノードからクラウドストレージプールに移動する ILM ルールを設定します。
3. ルールを ILM ポリシーに追加します。次に、ポリシーをシミュレートしてアクティブ化します。

複数のクラウドエンドポイントを維持する

複数のクラウドにオブジェクトデータを階層化またはバックアップする場合は、複数のクラウドストレージプールを設定できます。ILM ルールのフィルタを使用して、各クラウドストレージプールに格納するオブジェクトを指定できます。たとえば、一部のテナントやバケットのオブジェクトを Amazon S3 Glacier に格納し、その他のテナントやバケットのオブジェクトを Azure BLOB ストレージに格納することができます。または、 Amazon S3 Glacier と Azure BLOB ストレージ間でデータを移動することもできます。複数のクラウドストレージプールを使用する場合、オブジェクトを格納できるクラウドストレージプールは一度に 1 つだけであることに注意してください。

複数のクラウドエンドポイントを実装するには、次

1. 最大 10 個のクラウドストレージプールを作成できます。
2. 適切なタイミングで適切なオブジェクトデータを各クラウドストレージプールに格納する ILM ルールを設定します。たとえば、バケット A のオブジェクトをクラウドストレージプール A に格納し、バケット B のオブジェクトをクラウドストレージプール B に格納しますまたは、オブジェクトを Cloud Storage Pool A に一定期間保存してから、クラウドストレージプール B に移動します
3. ルールを ILM ポリシーに追加します。次に、ポリシーをシミュレートしてアクティブ化します。

クラウドストレージプールに関する考慮事項

## クラウドストレージプールを使用して StorageGRID システムからオブジェクトを移動する場合は、クラウドストレージプールの設定と使用に関する考慮事項を確認しておく必要があります。

一般的な考慮事項

- 一般に、 Amazon S3 Glacier や Azure BLOB ストレージなどのクラウドアーカイブストレージにはオブジェクトデータを低コストで格納することができます。ただし、クラウドアーカイブストレージからデータを読み出すコストは比較的高くなります。全体的なコストを最小限に抑えるには、クラウドストレージプール内のオブジェクトにアクセスするタイミングと頻度を考慮する必要があります。クラウドストレージプールの使用は、アクセス頻度の低いコンテンツにのみ推奨されます。
- Swift クライアントによって取り込まれたオブジェクトには、クラウドストレージプールを使用しないでください。Swift では POST Object restore 要求がサポートされないため、 StorageGRID は S3 Glacier ストレージや Azure BLOB ストレージのアーカイブ層に移行された Swift オブジェクトを読み出せません。これらのオブジェクトを読み出す Swift GET object 要求は失敗します（ 403 Forbidden ）。
- クラウドストレージプールターゲットからオブジェクトを読み出すレイテンシが増加しているため、FabricPool でクラウドストレージプールを使用することはサポートされていません。

## クラウドストレージプールの作成に必要な情報

クラウドストレージプールを作成する前に、クラウドストレージプールに使用する外部の S3 バケットまたは Azure BLOB ストレージコンテナを作成する必要があります。その後、 StorageGRID でクラウドストレージプールを作成する際に、次の情報を指定する必要があります。

- プロバイダタイプ： Amazon S3 または Azure BLOB ストレージ。
- Amazon S3 を選択した場合は、クラウドストレージプールが AWS Secret Region （ * CAP （ C2S Access Portal ） * ）で使用するかどうかを示します。
- バケットまたはコンテナの正確な名前。
- バケットまたはコンテナへのアクセスに必要なサービスエンドポイント。
- バケットまたはコンテナへのアクセスに必要な認証。
  - * S3 * ：必要に応じて、アクセスキー ID とシークレットアクセスキー。
  - *C2S * ： CAP サーバから一時的なクレデンシャルを取得するための完全な URL 。サーバ CA 証明書、クライアント証明書、クライアント証明書の秘密鍵、および秘密鍵が暗号化されている場合は復号化するためのパスフレーズ。
  - *Azure BLOB ストレージ * ：アカウント名とアカウントキー。これらのクレデンシャルにはコンテナに対する完全な権限が必要です。
- 必要に応じて、バケットまたはコンテナへの TLS 接続を検証するカスタム CA 証明書を指定します。

## クラウドストレージプールに使用するポートに関する考慮事項

指定したクラウドストレージプールとの間でオブジェクトを ILM ルールによって移動できるようにするには、システムのストレージノードが含まれるネットワークを設定する必要があります。次のポートがクラウドストレージプールと通信できることを確認してください。

デフォルトでは、クラウドストレージプールは次のポートを使用します。

- **80** ：エンドポイント URI が http で始まる場合
- **442** ： https で始まるエンドポイント URI の場合

クラウドストレージプールを作成または編集するときに、別のポートを指定できます。

非透過型プロキシサーバを使用する場合は、ストレージプロキシの設定で、インターネット上のエンドポイントなどの外部エンドポイントへのメッセージの送信を許可する必要もあります。

## コストに関する考慮事項

クラウドストレージプールを使用してクラウド内のストレージにアクセスするには、クラウドへのネットワーク接続が必要です。クラウドストレージプールを使用して StorageGRID とクラウドの間で移動するデータ量の予測に基づいて、クラウドへのアクセスに使用するネットワークインフラのコストを考慮し、適切にプロビジョニングする必要があります。

StorageGRID が外部のクラウドストレージプールエンドポイントに接続すると、さまざまな要求を実行して接続を監視し、必要な処理を確実に実行できるようにします。これらの要求には追加コストが伴いますが、クラウドストレージプールの監視にかかるコストは、 S3 または Azure にオブジェクトを格納する場合の全体的なコストのごくわずかです。

外部クラウドストレージプールのエンドポイントから StorageGRID にオブジェクトを戻す必要がある場合、より大きなコストが発生する可能性があります。次のいずれかの場合、オブジェクトが StorageGRID に戻ることがあります。

- オブジェクトの唯一のコピーがクラウドストレージプールにあり、オブジェクトを StorageGRID に格納することにした場合。その場合は、 ILM ルールとポリシーを再設定するだけです。ILM 評価が実行されると、 StorageGRID はクラウドストレージプールからオブジェクトを読み出す要求を複数実行します。次に、 StorageGRID は指定された数のレプリケートコピーまたはイレイジャーコーディングコピーをローカルに作成します。オブジェクトが StorageGRID に戻ると、クラウドストレージプール内のコピーは削除されます。
- ストレージノードの障害が原因でオブジェクトが失われた場合。オブジェクトのコピーがクラウドストレージプールにしか残っていない場合、 StorageGRID はオブジェクトを一時的にリストアして、リカバリされたストレージノードに新しいコピーを作成します。

> オブジェクトがクラウドストレージプールから StorageGRID に戻ると、 StorageGRID は各オブジェクトに対してクラウドストレージプールエンドポイントに対して複数の要求を実行します。大量のオブジェクトを移動する場合は、事前にテクニカルサポートに問い合わせて、期間と関連コストの見積もりを依頼してください。

**S3** ：クラウドストレージプールバケットに必要な権限

クラウドストレージプールに使用される外部の S3 バケットポリシーで、バケットへのオブジェクトの移動、オブジェクトのステータスの取得、必要に応じた Glacier ストレージからのオブジェクトのリストアなどを行うために、 StorageGRID 権限を付与する必要があります。理想的には、StorageGRID にはバケットへのフルコントロールアクセスが必要です (`s3:*`）。ただし、これができない場合は、バケットポリシーで次のS3権限をStorageGRID に付与する必要があります。

- `s3:AbortMultipartUpload`
- `s3:DeleteObject`
- `s3:GetObject`
- `s3:ListBucket`
- `s3:ListBucketMultipartUploads`
- `s3:ListMultipartUploadParts`
- `s3:PutObject`
- `s3:RestoreObject`

**S3**：外部バケットのライフサイクルに関する考慮事項

StorageGRID とクラウドストレージプールに指定された外部の S3 バケット間のオブジェクトの移動は、StorageGRID の ILM ルールとアクティブな ILM ポリシーによって制御されます。一方、クラウドストレージプールに指定された外部の S3 バケットから Amazon S3 Glacier または S3 Glacier Deep Archive （あるいは Glacier ストレージクラスを実装するストレージ解決策 ）へのオブジェクトの移行は、そのバケットのライフサイクル設定によって制御されます。

クラウドストレージプールからオブジェクトを移行する場合は、外部の S3 バケットに適切なライフサイクル設定を作成する必要があります。また、 Glacier ストレージクラスを実装し、かつ S3 POST Object restore API をサポートするストレージ解決策 を使用する必要があります。

たとえば、 StorageGRID からクラウドストレージプールに移動されたすべてのオブジェクトをすぐに Amazon S3 Glacier ストレージに移行するとします。この場合、単一のアクション（ * Transition * ）を指定する外部の S3 バケットでライフサイクル設定を次のように作成します。

```
<LifecycleConfiguration>
  <Rule>
    <ID>Transition Rule</ID>
    <Filter>
       <Prefix></Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>0</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>
```

このルールは、すべてのバケットオブジェクトを作成された日（ StorageGRID からクラウドストレージプールに移動された日）に Amazon S3 Glacier に移行します。

> 外部バケットのライフサイクルを設定する場合、 * Expiration * アクションを使用してオブジェクトの期限を定義しないでください。Expiration アクション期限切れのオブジェクトを削除するために、外部ストレージシステムを原因 します。期限切れのオブジェクトにあとで StorageGRID からアクセスしようとしても、削除されたオブジェクトは見つかりません。

クラウドストレージプール内のオブジェクトを（Amazon S3 Glacierではなく）S3 Glacier Deep Archiveに移行する場合は、と指定します `<StorageClass>DEEP_ARCHIVE</StorageClass>` をバケットライフサイクルに追加します。ただし、を使用できないことに注意してください `Expedited` S3 Glacier Deep Archiveからオブジェクトをリストアする階層。

**Azure** ：アクセス層に関する考慮事項

Azure ストレージアカウントを設定する場合は、デフォルトのアクセス層をホットまたはクールに設定できます。クラウドストレージプールで使用するストレージアカウントを作成する場合は、デフォルト階層としてホット階層を使用する必要があります。StorageGRID はオブジェクトをクラウドストレージプールに移動するとすぐに階層をアーカイブに設定しますが、デフォルト設定をホットにしておくことで、最低期間の 30 日前にクール階層から削除されたオブジェクトに対する早期削除料金が発生しません。

**Azure** ：ライフサイクル管理はサポートされていません

クラウドストレージプールで使用するコンテナには Azure BLOB ストレージのライフサイクル管理を使用しないでください。ライフサイクル処理が Cloud Storage Pool の処理の妨げになることがあります。

関連情報

"クラウドストレージプールの作成"

"S3 ：クラウドストレージプールの認証情報の指定"

"C2S S3 ：クラウドストレージプールの認証情報の指定"

"Azure：クラウドストレージプールの認証情報の指定"

"StorageGRID の管理"

クラウドストレージプールと **CloudMirror** レプリケーションを比較しています

## クラウドストレージプールの使用を開始するにあたって、クラウドストレージプールとStorageGRID CloudMirror レプリケーションサービスの類似点と相違点を理解しておくと役立ちます。

| | クラウドストレージプール | **CloudMirror** レプリケーションサービス |
|---|---|---|
| 主な目的は何ですか？ | クラウドストレージプールはアーカイブターゲットとして機能します。クラウドストレージプール内のオブジェクトコピーは、オブジェクトの唯一のコピーにすることも、追加のコピーにすることもできます。つまり、オンプレミスに 2 つのコピーを保持するのではなく、 StorageGRID 内に保持できるコピーは 1 つだけで、クラウドストレージプールにコピーを送信できます。 | CloudMirror レプリケーションサービスを使用すると、テナントで、 StorageGRID （ソース）内のバケットから外部の S3 バケット（デスティネーション）にオブジェクトを自動的にレプリケートできます。CloudMirror レプリケーションでは、独立した S3 インフラにオブジェクトの独立したコピーが作成されます。 |
| セットアップ方法は？ | クラウドストレージプールは、グリッドマネージャまたはグリッド管理 API を使用して、ストレージプールと同じ方法で定義されます。クラウドストレージプールは、 ILM ルールの配置先として選択できます。ストレージプールはストレージノードのグループで構成されますが、クラウドストレージプールはリモートの S3 または Azure エンドポイント（ IP アドレス、クレデンシャルなど）を使用して定義されます。 | テナントユーザは、Tenant ManagerまたはS3 APIを使用してCloudMirrorエンドポイント（IPアドレス、クレデンシャルなど）を定義することによってCloudMirrorレプリケーションを設定します。CloudMirror エンドポイントのセットアップ後、そのテナントアカウントが所有するバケットは、 CloudMirror エンドポイントを参照するように設定できます。 |
| 設定は誰が担当しますか？ | 通常はグリッド管理者 | 通常はテナントユーザ |
| デスティネーションは何ですか？ | • 互換性のある任意の S3 インフラ（ Amazon S3 を含む）<br>• Azure BLOB アーカイブ層 | • 互換性のある任意の S3 インフラ（ Amazon S3 を含む） |
| オブジェクトをデスティネーションに移動する原因は何ですか？ | アクティブな ILM ポリシー内の 1 つ以上の ILM ルール。ILM ルールは、 StorageGRID がクラウドストレージプールに移動するオブジェクトとオブジェクトを移動するタイミングを定義します。 | CloudMirror エンドポイントを使用して設定されたソースバケットに新しいオブジェクトを取り込む処理。 CloudMirror エンドポイントを使用してバケットが設定される前のソースバケットに含まれていたオブジェクトは、変更されていないかぎりレプリケートされません。 |

| | クラウドストレージプール | **CloudMirror** レプリケーションサービス |
|---|---|---|
| オブジェクトの読み出し方法 | アプリケーションは、クラウドストレージプールに移動されたオブジェクトを読み出すために、 StorageGRID への要求を行う必要があります。オブジェクトの唯一のコピーがアーカイブストレージに移行された場合、StorageGRID はオブジェクトのリストアプロセスを管理して読み出し可能にします。 | デスティネーションバケット内のミラーコピーは独立したコピーであるため、アプリケーションは、 StorageGRID または S3 デスティネーションに要求を行うことでオブジェクトを読み出すことができます。たとえば、CloudMirror レプリケーションを使用してパートナー組織にオブジェクトをミラーリングするとします。パートナーは、独自のアプリケーションを使用して、 S3 デスティネーションからオブジェクトを直接読み取ったり更新したりできます。StorageGRID を使用する必要はありません。 |
| デスティネーションから直接読み取ることはできますか。 | いいえクラウドストレージプールに移動されるオブジェクトは StorageGRID によって管理されます。読み取り要求は StorageGRID に転送する必要があります（ StorageGRID がクラウドストレージプールからの読み出しを実行します）。 | はい。ミラーコピーは独立したコピーであるためです。 |
| オブジェクトがソースから削除された場合はどうなりますか？ | オブジェクトもクラウドストレージプールから削除されます。 | 削除操作は複製されません。削除したオブジェクトは StorageGRID バケットには存在しなくなりますが、デスティネーションバケットには引き続き存在します。同様に、デスティネーションバケット内のオブジェクトもソースに影響を与えることなく削除できます。 |
| 災害後（ StorageGRID システムが動作していない）にどのようにしてオブジェクトにアクセスしますか。 | 障害が発生した StorageGRID ノードをリカバリする必要があります。このプロセスでは、レプリケートされたオブジェクトのコピーをクラウドストレージプールのコピーを使用してリストアすることができます。 | CloudMirror デスティネーション内のオブジェクトコピーは StorageGRID から独立しているため、 StorageGRID ノードがリカバリされる前に直接アクセスできます。 |

関連情報

"StorageGRID の管理"

クラウドストレージプールの作成

クラウドストレージプールを作成 StorageGRID する際には、 StorageGRID がオブジェクトの格納に使用する外部バケットまたはコンテナの名前と場所、クラウドプロバイダのタイプ（ Amazon S3 または Azure Blob Storage ）、および外部のバケットまたはコンテナにアクセスするために必要な情報を指定します。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- クラウドストレージプールの設定に関するガイドラインを確認しておく必要があります。
- クラウドストレージプールが参照する外部のバケットまたはコンテナが存在している必要があります。
- バケットまたはコンテナにアクセスするためのすべての認証情報が必要です。

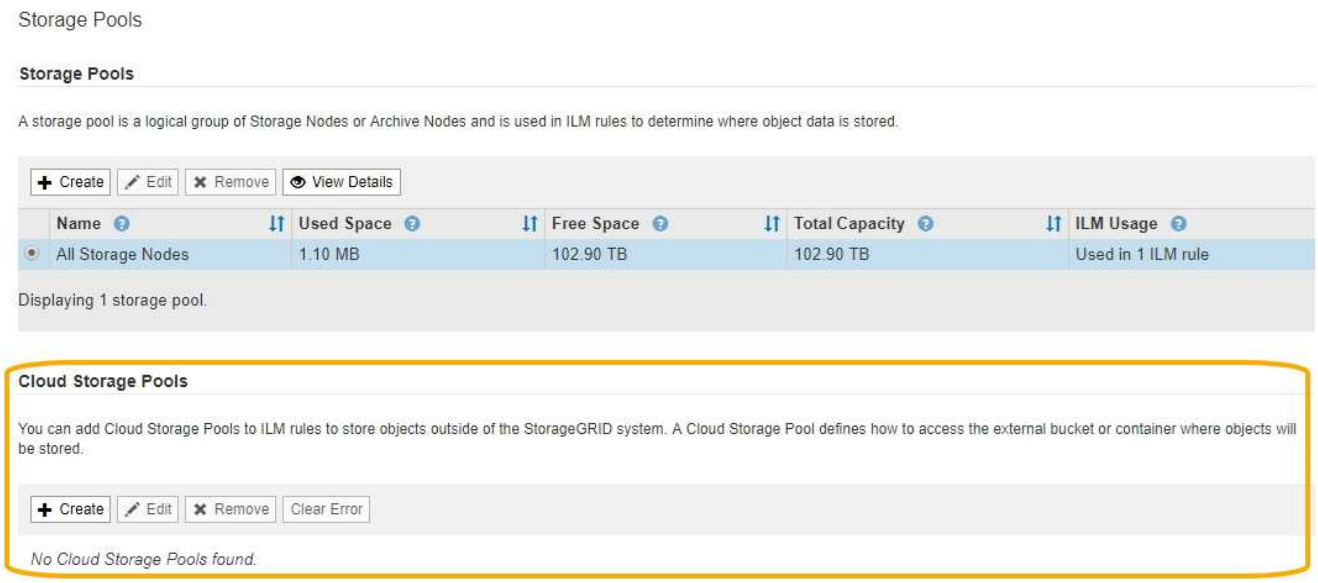
このタスクについて

クラウドストレージプールは、単一の外部の S3 バケットまたは Azure BLOB ストレージコンテナを指定します。クラウドストレージプールは保存後すぐに StorageGRID で検証されます。そのため、クラウドストレージプールに指定されたバケットまたはコンテナが存在し、アクセス可能であることを確認しておく必要があります。

手順

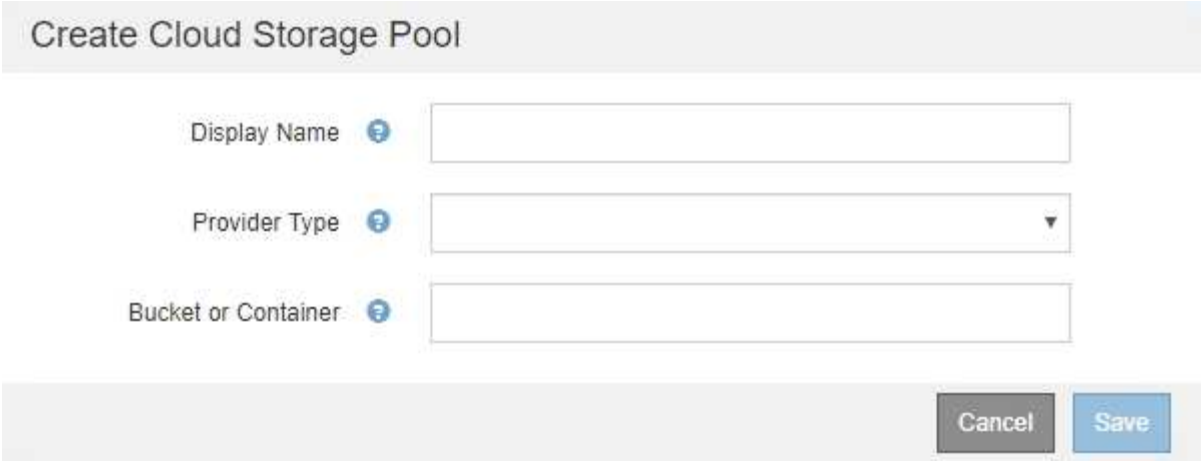
1. ILM > Storage Pools *を選択します。

   Storage Pools （ストレージプール）ページが表示されます。このページには、ストレージプールとクラウドストレージプールの 2 つのセクションがあります。




2. ページのクラウドストレージプールセクションで、*作成*をクリックします。

   Create Cloud Storage Pool （クラウドストレージプールの作成）ダイアログボックスが表示されます。




3. 次の情報を入力します。

| フィールド | 説明 |
| --- | --- |
| 表示名 | クラウドストレージプールとその目的を簡単に説明する名前。ILM ルールを設定するときに識別しやすい名前を使用してください。 |
| プロバイダタイプ | このクラウドストレージプールに使用するクラウドプロバイダ：<br>• Amazon S3（S3またはC2S S3クラウドストレージプールの場合はこのオプションを選択します）<br>• Azure BLOBストレージ<br>◦ 注：[ プロバイダタイプ ] を選択すると、ページの下部に [ サービスエンドポイント ] 、 [ 認証 ] 、および [ サーバ検証 ] セクションが表示されます。 |
| バケットまたはコンテナ | クラウドストレージプール用に作成された外部の S3 バケットまたは Azure コンテナの名前。バケットまたはコンテナの名前は正確に指定する必要があります。一致していないと、クラウドストレージプールの作成が失敗します。クラウドストレージプールの保存後にこの値を変更することはできません。 |

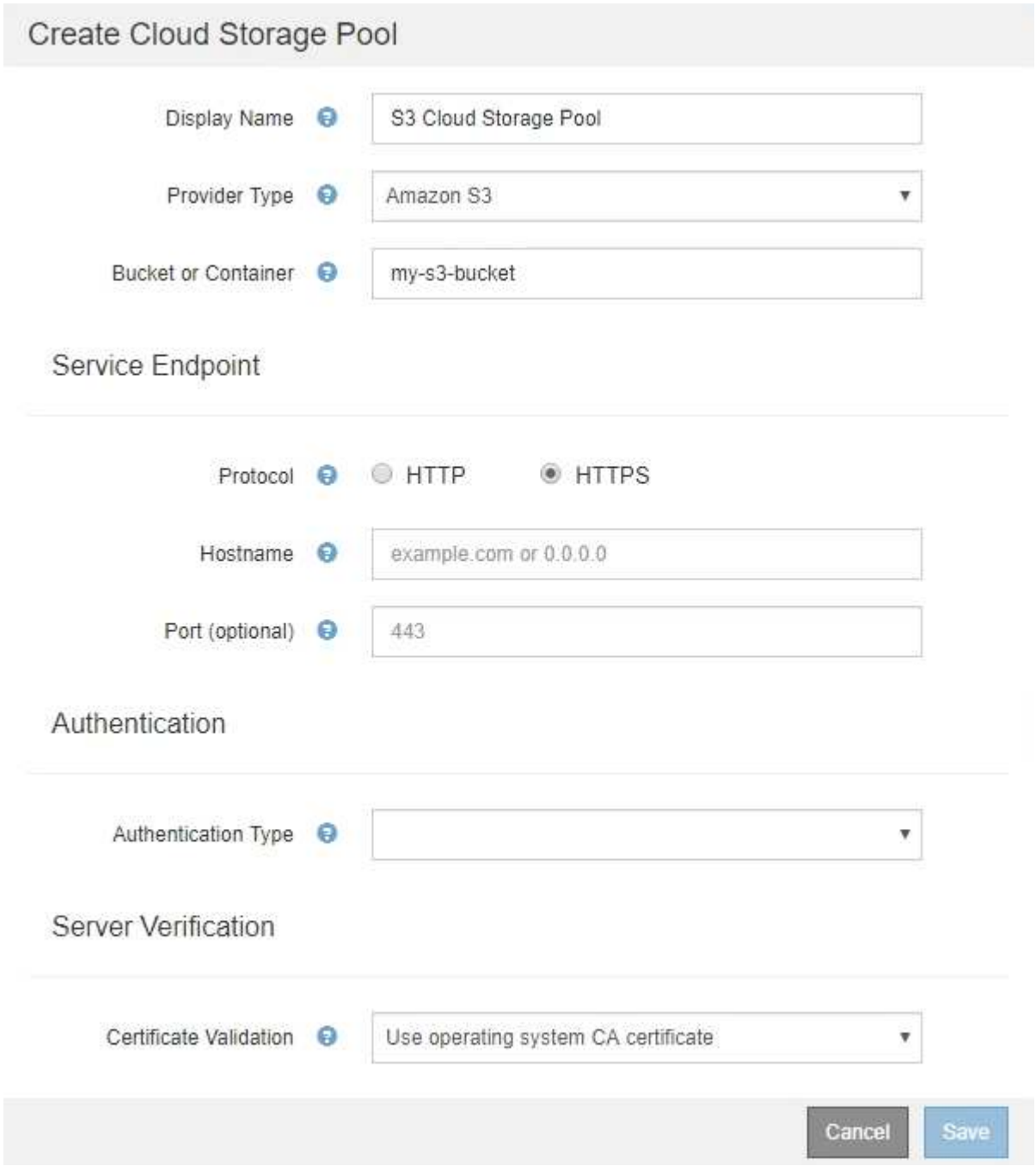
4. 選択したプロバイダータイプに基づいて、ページの [Service Endpoint] 、 [Authentication] 、および [Server Verification] セクションを完了します。
   - "S3 ：クラウドストレージプールの認証情報の指定"
   - "C2S S3 ：クラウドストレージプールの認証情報の指定"
   - "Azure：クラウドストレージプールの認証情報の指定"

**S3** ：クラウドストレージプールの認証情報の指定

S3 用のクラウドストレージプールを作成する場合は、クラウドストレージプールのエンドポイントで必要な認証のタイプを選択する必要があります。匿名を指定するか、アクセスキー ID とシークレットアクセスキーを入力できます。

必要なもの

- クラウドストレージプールの基本情報を入力し、プロバイダタイプとして* Amazon S3 *を指定しておく必要があります。




- アクセスキー認証を使用している場合は、外部のS3バケットのアクセスキーIDとシークレットアクセスキーを把握しておく必要があります。

手順

1. 「 * Service Endpoint * 」セクションで、次の情報を入力します。

   a. クラウドストレージプールに接続するときに使用するプロトコルを選択します。

      デフォルトのプロトコルは HTTPS です。

b. クラウドストレージプールのサーバのホスト名または IP アドレスを入力します。

例：

```
s3-aws-region.amazonaws.com
```

バケット名はこのフィールドに含めないでください。バケット名は「 * Bucket 」フィールドまたは「 Container * 」フィールドに入力します。

a. 必要に応じて、クラウドストレージプールへの接続時に使用するポートを指定します。

デフォルトのポート（ HTTPS の場合はポート 443 、 HTTP の場合はポート 80 ）を使用する場合は、このフィールドを空白のままにします。

2. [* 認証 *] セクションで、クラウドストレージプールエンドポイントに必要な認証のタイプを選択します。

| オプション | 説明 |
| --- | --- |
| アクセスキー | Cloud Storage Pool バケットにアクセスするには、アクセスキー ID とシークレットアクセスキーが必要です。 |
| 匿名 | すべてのユーザが Cloud Storage Pool バケットにアクセスできます。アクセスキー ID とシークレットアクセスキーは不要です。 |
| CAP （ C2S Access Portal ） | C2S S3 にのみ使用されます。に進みます "C2S S3 ：クラウドストレージプールの認証情報の指定"。 |

3. アクセスキーを選択した場合は、次の情報を入力します。

| オプション | 説明 |
| --- | --- |
| アクセスキー ID | 外部バケットを所有するアカウントのアクセスキー ID 。 |
| シークレットアクセスキー | 関連付けられているシークレットアクセスキー。 |

4. Server Verification セクションで、クラウドストレージプールへの TLS 接続用の証明書を検証する方法を選択します。

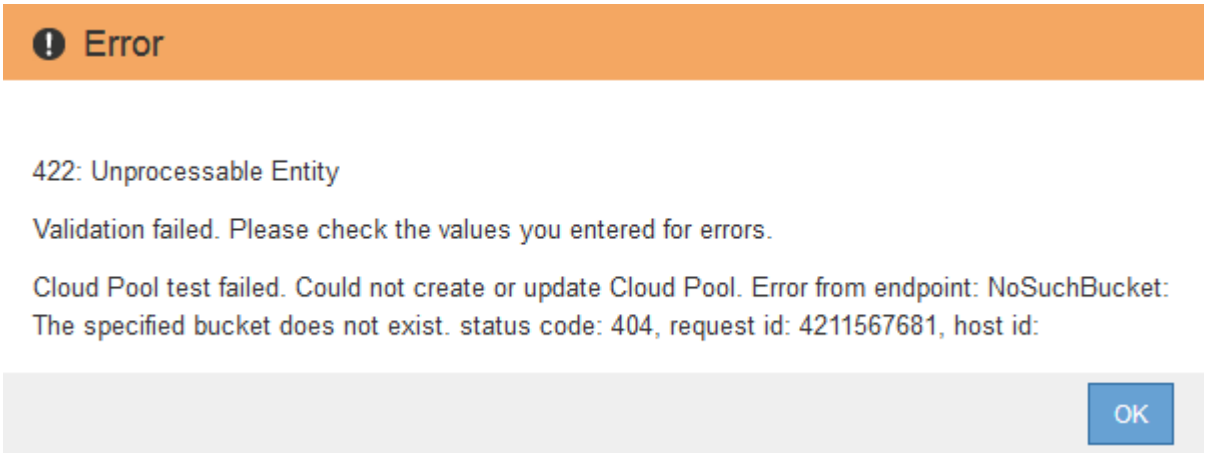
| オプション | 説明 |
| --- | --- |
| オペレーティングシステムの CA 証明書を使用します | オペレーティングシステムにインストールされているデフォルトのCA証明書を使用して接続を保護します。 |
| カスタム CA 証明書を使用する | カスタム CA 証明書を使用する。Select New *をクリックし、PEMでエンコードされたCA証明書をアップロードします。 |
| 証明書を検証しないでください | TLS 接続に使用される証明書は検証されません。 |

5. [ 保存（ Save ） ] をクリックします。

クラウドストレージプールを保存すると、 StorageGRID では次の処理が実行されます。

- バケットとサービスエンドポイントが存在し、指定したクレデンシャルを使用してそれらにアクセスできることを検証します。
- バケットをクラウドストレージプールとして識別するために、バケットにマーカーファイルを書き込みます。このファイルは削除しないでください `x-ntap-sgws-cloud-pool-uuid`。

クラウドストレージプールの検証に失敗すると、その理由を記載したエラーメッセージが表示されます。たとえば、証明書エラーが発生した場合や、指定したバケットが存在しない場合などにエラーが報告されます。




クラウドストレージプールのトラブルシューティングの手順を参照し、問題 を解決してから、クラウドストレージプールをもう一度保存してください。

関連情報

"クラウドストレージプールのトラブルシューティング"

**C2S S3** ：クラウドストレージプールの認証情報の指定

## Commercial クラウド サービス （ C2S ） S3 サービスをクラウドストレージプールとして使用するには、認証タイプとして C2S Access Portal （ CAP ）を設定し、StorageGRID が C2S アカウント内の S3 バケットにアクセスするための一時的なクレデンシャルを要求できるようにする必要があります。

必要なもの

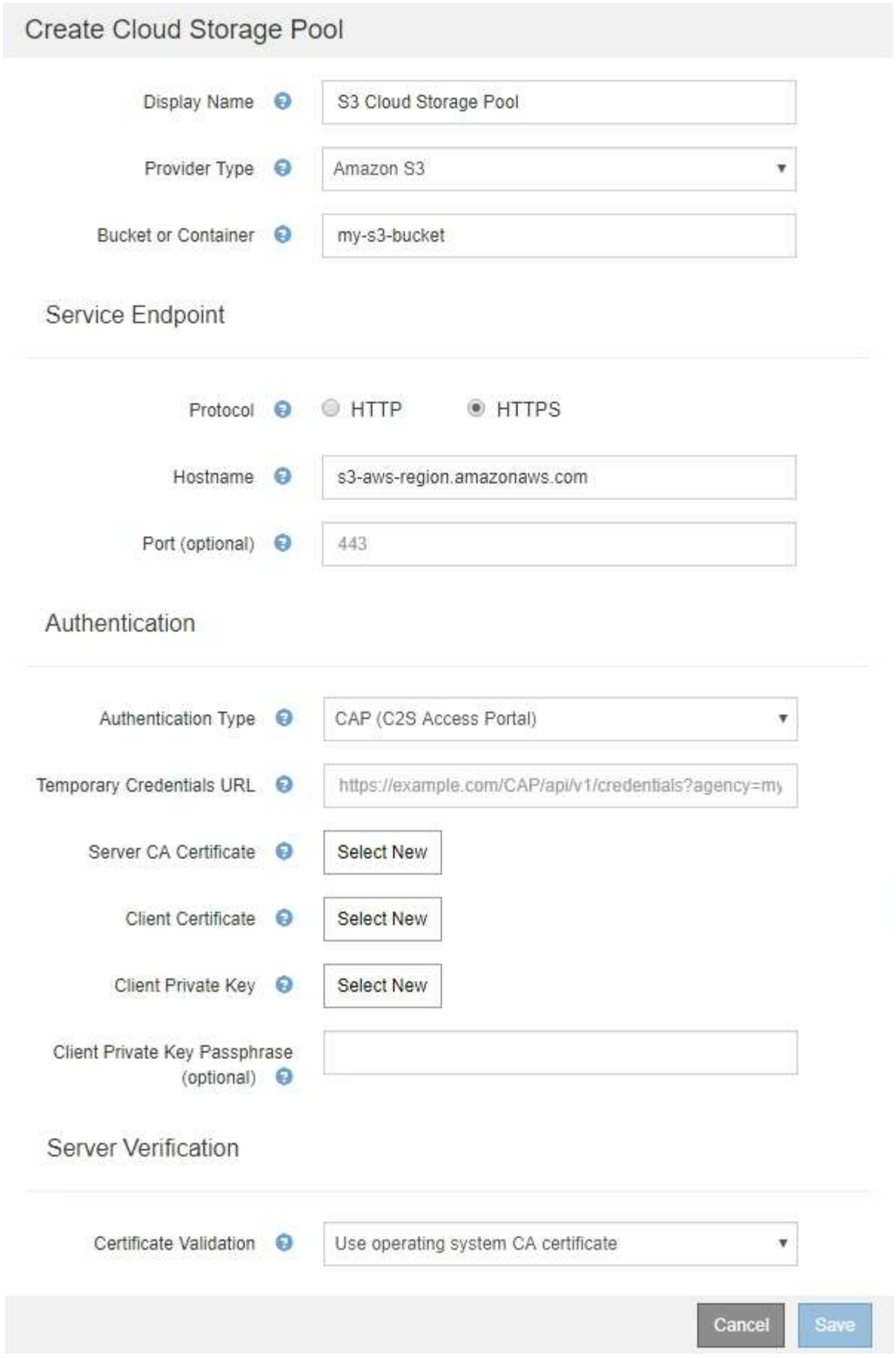
- サービスエンドポイントを含むAmazon S3クラウドストレージプールの基本情報を入力しておく必要があります。
- StorageGRID がCAPサーバから一時的なクレデンシャルを取得するために使用する、C2Sアカウントに割り当てられている必須/オプションのAPIパラメータをすべて含む完全なURLが必要です。
- 該当する公的認証局（CA）が発行したサーバCA証明書が必要です。StorageGRID は、この証明書を使用して CAP サーバの識別情報を確認します。サーバ CA 証明書は PEM エンコードを使用している必要があります。
- 該当する公的認証局（CA）が発行したクライアント証明書が必要です。StorageGRID は、この証明書を使用して CAP サーバに対して自身を識別します。クライアント証明書は PEM エンコードを使用し、C2S アカウントへのアクセスが許可されている必要があります。

- クライアント証明書のPEMでエンコードされた秘密鍵が必要です。
- クライアント証明書の秘密鍵が暗号化されている場合は、復号化用のパスフレーズが必要です。

手順

1. [* 認証 **]** セクションで、 **[** 認証タイプ **]** ドロップダウンから ***CAP (C2S Access Portal)*** を選択します。

   CAP C2S の認証フィールドが表示されます。


Create Cloud Storage Pool
Display Name
S3 Cloud Storage Pool
Provider Type
Amazon S3
Bucket or Container
my-s3-bucket
Service Endpoint
Protocol
HTTP
HTTPS
Hostname
s3-aws-region.amazonaws.com
Port (optional)
443
Authentication
Authentication Type
CAP (C2S Access Portal)
Temporary Credentials URL
https://example.com/CAP/api/v1/credentials?agency=my
Server CA Certificate
Select New
Client Certificate
Select New
Client Private Key
Select New
Client Private Key Passphrase (optional)
Server Verification
Certificate Validation
Use operating system CA certificate
Cancel
Save

2. 次の情報を入力します。

   a. [*Temporary Credentials URL] には、 StorageGRID が CAP サーバから一時的なクレデンシャルを取得するために使用する完全な URL を入力します。これには、 C2S アカウントに割り当てられている必須およびオプションの API パラメータがすべて含まれます。

   b. サーバーCA証明書*の場合は、*新規選択*をクリックし、StorageGRID がCAPサーバーの検証に使用するPEMでエンコードされたCA証明書をアップロードします。

   c. *クライアント証明書*の場合は、*新しい*を選択をクリックし、StorageGRID がCAPサーバに対して自身を識別するために使用するPEMでエンコードされた証明書をアップロードします。

   d. *クライアント秘密鍵*の場合は、*新規選択*をクリックし、クライアント証明書のPEMでエンコードされた秘密鍵をアップロードします。

      秘密鍵が暗号化されている場合は、従来の形式を使用する必要があります。（ PKCS #8 で暗号化された形式はサポートされていません）。

   e. クライアントの秘密鍵が暗号化されている場合は、クライアントの秘密鍵を復号化するためのパスフレーズを入力します。それ以外の場合は、 [* クライアント秘密キーのパスフレーズ * ] フィールドを空白のままにします。

3. Server Verification セクションで、次の情報を指定します。

   a. 「 * 証明書の検証 * 」で、「 * カスタム CA 証明書を使用する * 」を選択します。

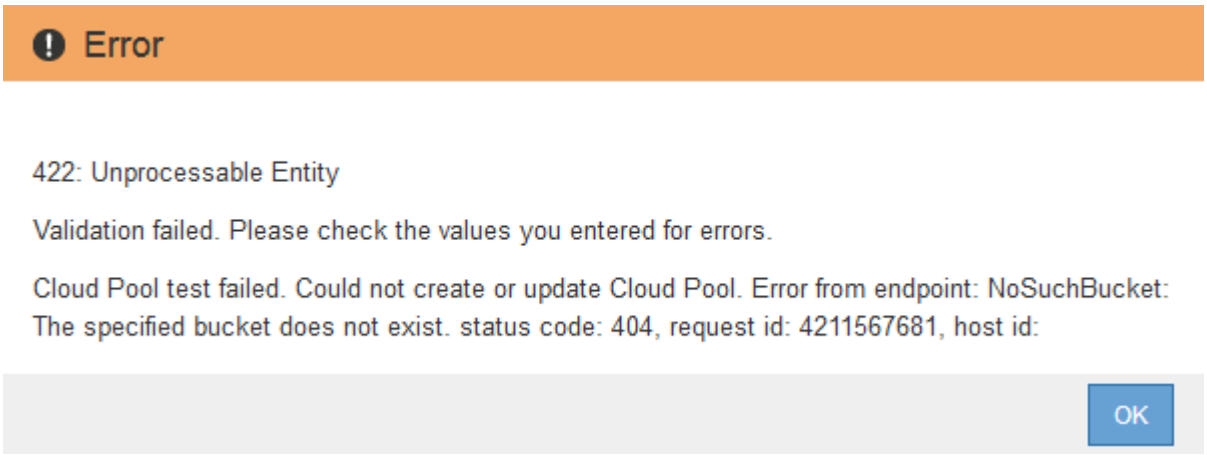
   b. Select New *をクリックし、PEMでエンコードされたCA証明書をアップロードします。

4. [ 保存（ Save ） ] をクリックします。

クラウドストレージプールを保存すると、 StorageGRID では次の処理が実行されます。

- バケットとサービスエンドポイントが存在し、指定したクレデンシャルを使用してそれらにアクセスできることを検証します。
- バケットをクラウドストレージプールとして識別するために、バケットにマーカーファイルを書き込みます。このファイルは削除しないでください `x-ntap-sgws-cloud-pool-uuid`。

クラウドストレージプールの検証に失敗すると、その理由を記載したエラーメッセージが表示されます。たとえば、証明書エラーが発生した場合や、指定したバケットが存在しない場合などにエラーが報告されます。




クラウドストレージプールのトラブルシューティングの手順を参照し、問題 を解決してから、クラウドストレージプールをもう一度保存してください。

関連情報

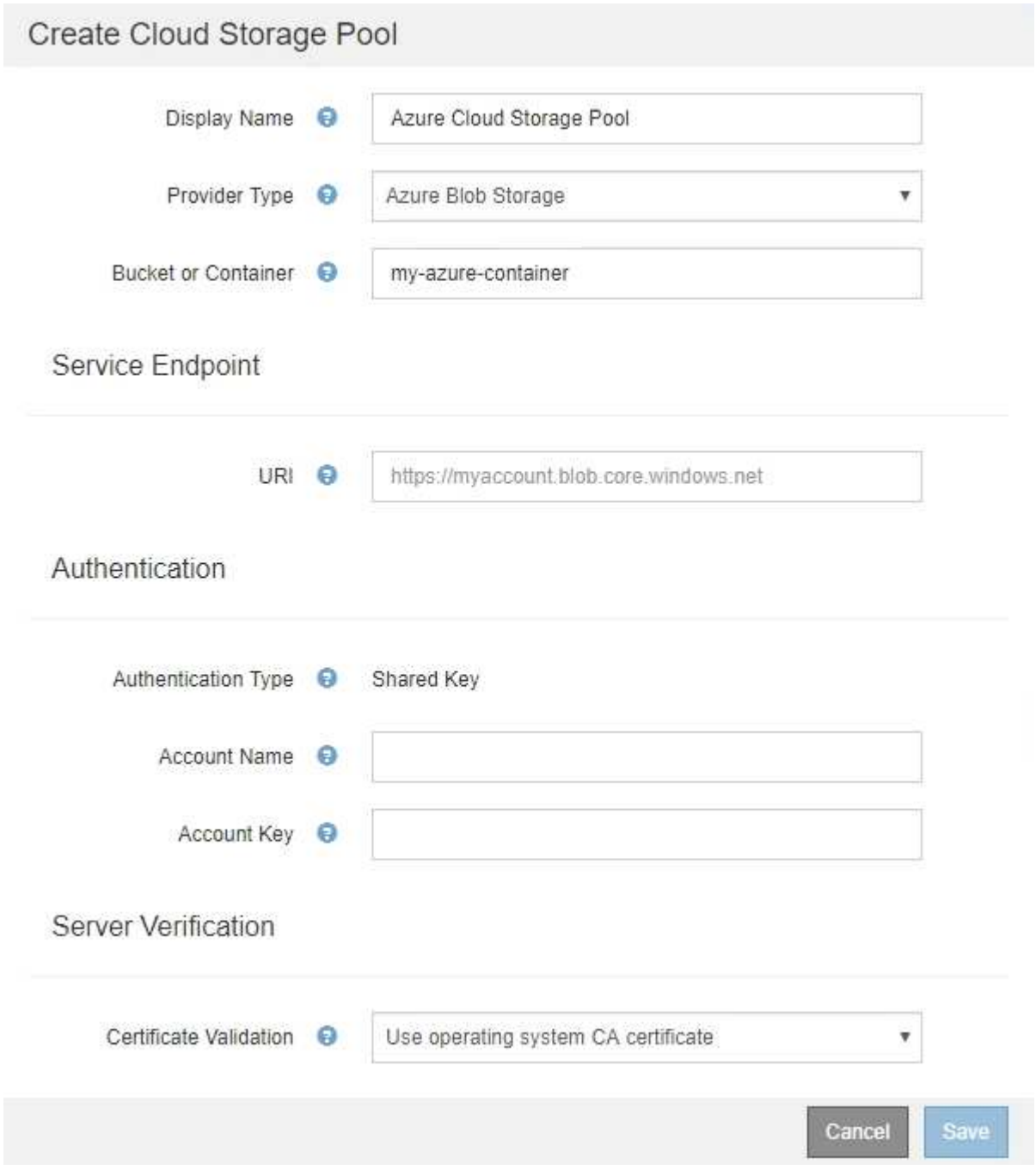
"クラウドストレージプールのトラブルシューティング"

**Azure**：クラウドストレージプールの認証情報の指定

Azure BLOB ストレージ用のクラウドストレージプールを作成する場合は、StorageGRID がオブジェクトの格納に使用する外部コンテナのアカウント名とアカウントキーを指定する必要があります。

必要なもの

- クラウドストレージプールの基本情報を入力し、プロバイダタイプとして「* Azure Blob Storage 」を指定しておく必要があります。***Authentication Type** フィールドに Shared Key* が表示されます。



- クラウドストレージプールに使用されるBLOBストレージコンテナへのアクセスに使用するUniform Resource Identifier（URI）を確認しておく必要があります。
- ストレージアカウントの名前とシークレットキーを把握しておく必要があります。これらの値は Azure portal を使用して確認できます。

手順

1. 「 * サービスエンドポイント * 」セクションで、クラウドストレージプールに使用される BLOB ストレージコンテナへのアクセスに使用する Uniform Resource Identifier （ URI ）を入力します。

   次のいずれかの形式で指定します。

   - `https://host:port`
   - `http://host:port`

   ポートを指定しない場合、デフォルトでは HTTPS URI にはポート 443 が、 HTTP URI にはポート 80 が使用されます。* Azure BLOBストレージコンテナのURIの例*：
   `https://myaccount.blob.core.windows.net`

2. [* 認証 * （ * Authentication * ） ] セクションで、次の情報を入力します。

   a. **Account Name** に、外部サービスコンテナを所有する BLOB ストレージアカウントの名前を入力します。

   b. 「 * Account Key * 」に、 BLOB ストレージアカウントのシークレットキーを入力します。

   Azure エンドポイントの場合は、共有キー認証を使用する必要があります。

3. [ サーバ検証 * ] セクションで、クラウドストレージプールへの TLS 接続用証明書の検証に使用する方法を選択します。

| オプション | 説明 |
| --- | --- |
| オペレーティングシステムの CA 証明書を使用します | オペレーティングシステムにインストールされているデフォルトのCA証明書を使用して接続を保護します。 |
| カスタム CA 証明書を使用する | カスタム CA 証明書を使用する。[Select New]をクリックし、PEMでエンコードされた証明書をアップロードします。 |
| 証明書を検証しないでください | TLS 接続に使用される証明書は検証されません。 |

4. [ 保存（ Save ） ] をクリックします。

クラウドストレージプールを保存すると、 StorageGRID では次の処理が実行されます。

- コンテナと URI が存在し、指定したクレデンシャルを使用してアクセスできることを検証します。
- クラウドストレージプールとして識別するためにコンテナにマーカーファイルを書き込みます。このファイルは削除しないでください `x-ntap-sgws-cloud-pool-uuid`。

クラウドストレージプールの検証に失敗すると、その理由を記載したエラーメッセージが表示されます。たとえば、証明書エラーが発生した場合や、指定したコンテナが存在しない場合などにエラーが報告されます。

クラウドストレージプールのトラブルシューティングの手順を参照し、問題 を解決してから、クラウドストレージプールをもう一度保存してください。

関連情報

"クラウドストレージプールのトラブルシューティング"

クラウドストレージプールの編集

## クラウドストレージプールを編集して、名前、サービスエンドポイント、またはその他の詳細を変更できます。ただし、クラウドストレージプールの S3 バケットまたは Azure コンテナを変更することはできません。

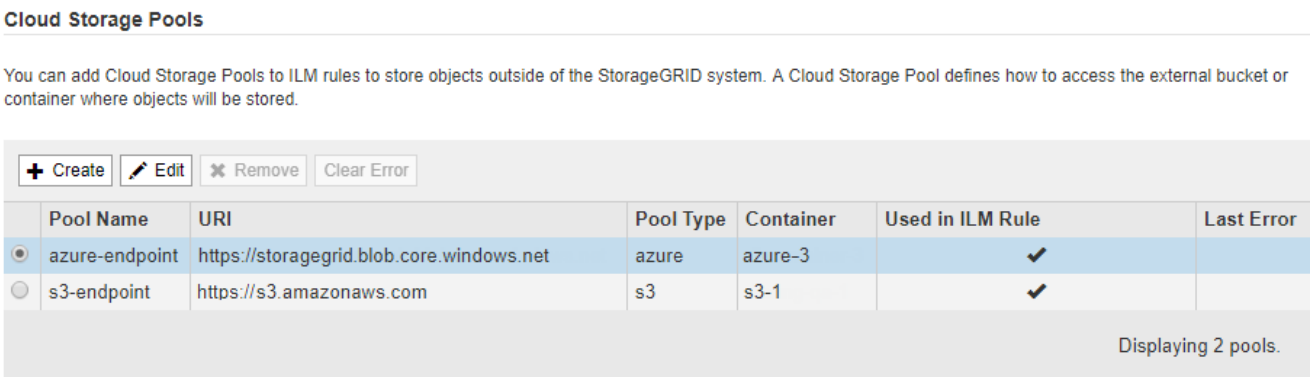
必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- クラウドストレージプールの設定に関するガイドラインを確認しておく必要があります。

手順

1. ILM > Storage Pools *を選択します。

   Storage Pools （ストレージプール）ページが表示されます。Cloud Storage Pools テーブルには、既存のクラウドストレージプールが表示されます。




2. 編集するクラウドストレージプールのラジオボタンを選択します。
3. [ 編集（ Edit ） ] をクリックします。
4. 必要に応じて、表示名、サービスエンドポイント、認証クレデンシャル、または証明書の検証方法を変更します。

   クラウドストレージプールのプロバイダタイプ、 S3 バケット、 Azure コンテナを変更することはできません。

   以前にサーバ証明書またはクライアント証明書をアップロードした場合は、現在使用中の証明書を確認するために [ 現在の証明書を表示 ] を選択できます。

5. [ 保存（ Save ） ] をクリックします。

   クラウドストレージプールを保存すると、バケットまたはコンテナとサービスエンドポイントが存在し、

指定したクレデンシャルでそれらにアクセスできることが StorageGRID によって検証されます。

クラウドストレージプールの検証が失敗すると、エラーメッセージが表示されます。たとえば、証明書エラーが発生した場合はエラーが報告されます。

クラウドストレージプールのトラブルシューティングの手順を参照し、問題 を解決してから、クラウドストレージプールをもう一度保存してください。

関連情報

"クラウドストレージプールに関する考慮事項"

"クラウドストレージプールのトラブルシューティング"

クラウドストレージプールの削除

## ILM ルールで使用されておらず、オブジェクトデータが含まれていないクラウドストレージプールを削除できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- S3 バケットまたは Azure コンテナにオブジェクトが含まれていないことを確認します。クラウドストレージプールにオブジェクトが含まれている場合、そのストレージプールを削除しようとするとエラーが発生します。「クラウドストレージプールのトラブルシューティング」を参照してください。

> クラウドストレージプールを作成すると、 StorageGRID はバケットまたはコンテナにマーカーファイルを書き込み、クラウドストレージプールとして識別します。このファイルは削除しないでください `x-ntap-sgws-cloud-pool-uuid`。

- プールを使用している可能性のある ILM ルールを削除しておきます。

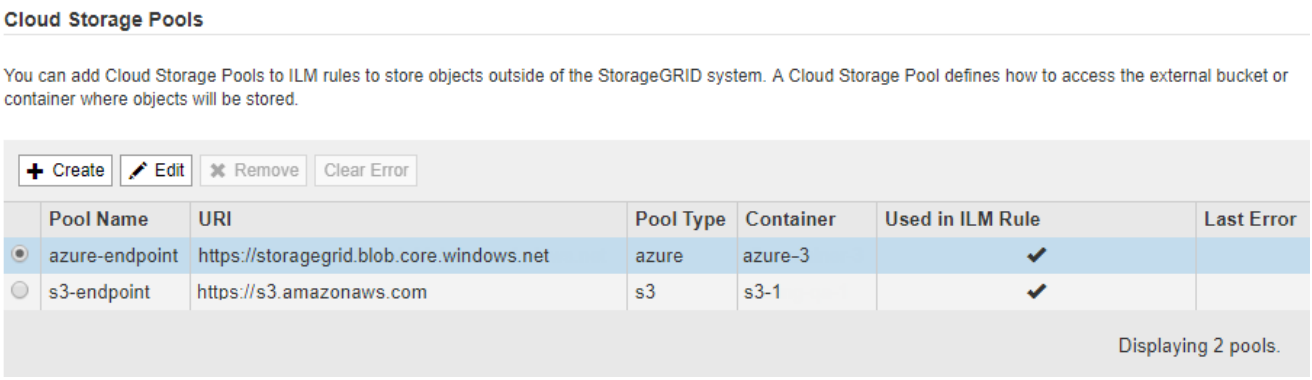
手順

1. ILM > Storage Pools *を選択します。

   Storage Pools （ストレージプール）ページが表示されます。

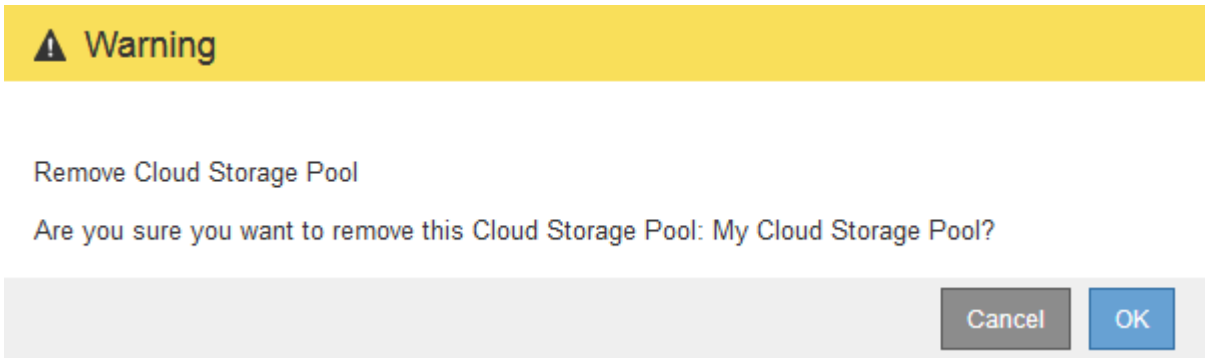
2. ILM ルールで現在使用されていないクラウドストレージプールのラジオボタンを選択します。

   ILM ルールで使用されているクラウドストレージプールは削除できません。「 * 削除」ボタンは無効になっています。




3. [ 削除（ Remove ） ] をクリックします。

   確認の警告が表示されます。




4. [OK] をクリックします。

   クラウドストレージプールが削除されます。

関連情報

"クラウドストレージプールのトラブルシューティング"

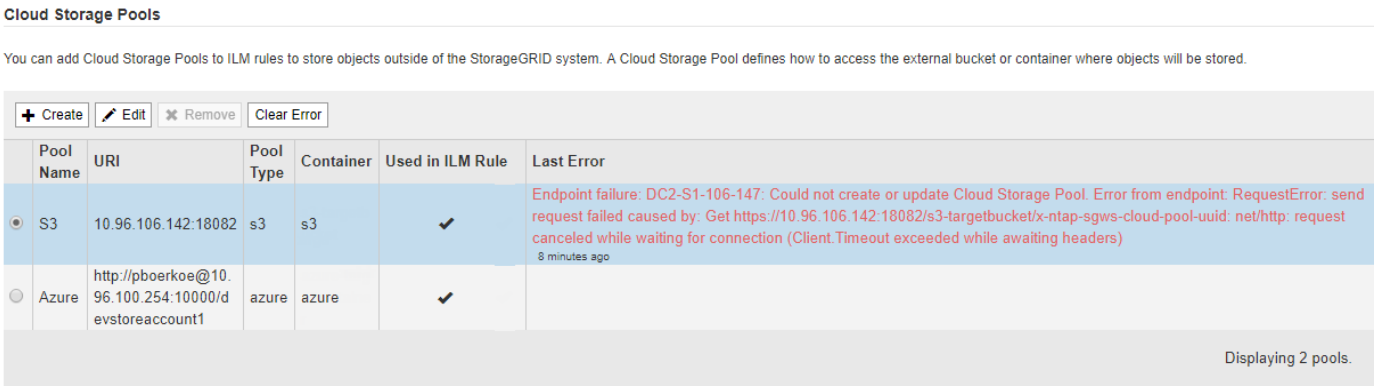
クラウドストレージプールのトラブルシューティング

## クラウドストレージプールの作成、編集、削除時にエラーが発生した場合は、以下のトラブルシューティング手順を使用して問題 を解決してください。

エラーが発生したかどうかを確認しています

StorageGRID では、すべてのクラウドストレージプールの健全性チェックを 1 分に 1 回実行して、クラウドストレージプールにアクセスできること、およびプールが正常に機能していることを確認します。健全性チェックで問題 が検出されると、ストレージプールページのクラウドストレージプールテーブルの前回のエラー列にメッセージが表示されます。

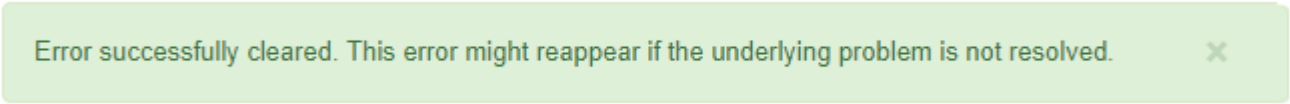
次の表は、各クラウドストレージプールで検出された最新のエラーと、エラーが発生してからの時間を示しています。




また、過去 5 分以内に新しいクラウドストレージプールのエラーが発生したことが健全性チェックで検出されると、 * クラウドストレージプール接続エラー * アラートがトリガーされます。このアラートのEメール通知を受信した場合は、ストレージプールのページ（* ILM *>*ストレージプール*を選択）に移動し、Last Error 列のエラーメッセージを確認して、以下のトラブルシューティング・ガイドラインを参照してください。

エラーが解決されたかどうかを確認しています

エラーの原因となっている問題を解決したら、エラーが解決されたかどうかを確認できます。Cloud Storage Poolページで、エンドポイントのオプションボタンを選択し、* Clear Error *をクリックします。StorageGRID がクラウドストレージプールのエラーをクリアしたことを示す確認メッセージが表示されます。




原因となっている問題が解決されると、エラーメッセージは表示されなくなります。ただし、根本的な問題が修正されていない場合（または別のエラーが発生した場合）は、数分以内に Last Error 列にエラーメッセージが表示されます。

エラー：このクラウドストレージプールには予期しないコンテンツが含まれています

クラウドストレージプールを作成、編集、または削除しようとすると、このエラーが発生する場合があります。このエラーは、バケットまたはコンテナにが含まれている場合に発生します `x-ntap-sgws-cloud-pool-uuid` マーカーファイルですが、想定されるUUIDがファイルにありません。

通常、このエラーが表示されるのは、新しいクラウドストレージプールを作成していて、 StorageGRID の別のインスタンスがすでに同じクラウドストレージプールを使用している場合のみです。

問題 を修正するには、次の手順を実行します。

- 組織内のユーザがこのクラウドストレージプールを使用していないことを確認します。
- を削除します `x-ntap-sgws-cloud-pool-uuid` ファイルして、クラウドストレージプールの設定を再試行してください。

エラー：クラウドストレージプールを作成または更新できませんでした。エンドポイントからのエラーです

クラウドストレージプールを作成または編集しようとすると、このエラーが発生する場合があります。このエラーは、何らかの接続または構成の問題 が原因で StorageGRID がクラウドストレージプールに書き込めないことを示しています。

問題 を修正するには、エンドポイントからのエラーメッセージを確認します。

- エラーメッセージにが含まれている場合 `Get *url*: EOF`をクリックし、クラウドストレージプールに使用されるサービスエンドポイントが、HTTPSを必要とするコンテナまたはバケットにHTTPプロトコルを使用していないことを確認します。
- エラーメッセージにが含まれている場合 `Get *url*: net/http: request canceled while waiting for connection` をクリックして、ストレージノードがクラウドストレージプールに使用するサービスエンドポイントにアクセスできるようにネットワーク設定で許可されていることを確認します。
- その他のすべてのエンドポイントエラーメッセージについては、次のいずれか、または複数の操作を試してください。
  - クラウドストレージプール用に入力した名前と同じ名前の外部コンテナまたはバケットを作成して、新しいクラウドストレージプールを再度保存します。
  - クラウドストレージプール用に指定したコンテナまたはバケット名を修正して、新しいクラウドストレージプールを再度保存します。

エラー： **CA** 証明書を解析できませんでした

クラウドストレージプールを作成または編集しようとすると、このエラーが発生する場合があります。このエラーは、クラウドストレージプールの設定時に入力した証明書を StorageGRID が解析できなかった場合に発生します。

問題 を修正するには、指定した CA 証明書に問題がないかどうかを確認します。

エラー：この **ID** のクラウドストレージプールが見つかりませんでした

クラウドストレージプールを編集または削除しようとすると、このエラーが発生する場合があります。このエラーは、次のいずれかの理由でエンドポイントが 404 応答を返した場合に発生します。

- クラウドストレージプールに使用されたクレデンシャルに、バケットの読み取り権限がありません。
- クラウドストレージプールに使用されるバケットにはが含まれません `x-ntap-sgws-cloud-pool-uuid` マーカーファイル。

問題 を修正するには、次の手順をいくつか実行します。

- 設定したアクセスキーに関連付けられているユーザに必要な権限があることを確認します。
- 必要な権限があるクレデンシャルを使用してクラウドストレージプールを編集します。
- 権限が正しい場合は、サポートにお問い合わせください。

エラー：クラウドストレージプールの内容を確認できませんでした。エンドポイントからのエラーです

クラウドストレージプールを削除しようとすると、このエラーが発生する場合があります。このエラーは、何らかの接続または設定問題 が原因で、 StorageGRID がクラウドストレージプールバケットのコンテンツを読み取れないことを示しています。

問題 を修正するには、エンドポイントからのエラーメッセージを確認します。

エラー： **Objects have already been placed in this bucket**

クラウドストレージプールを削除しようとすると、このエラーが発生する場合があります。ILM によって移動されたデータ、クラウドストレージプールの設定前にバケットに配置されていたデータ、またはクラウドストレージプールの作成後に他のソースによってバケットに配置されたデータが含まれているクラウドストレージプールは削除できません。

問題 を修正するには、次の手順をいくつか実行します。

- 「クラウドストレージプールオブジェクトのライフサイクル」の手順に従って、オブジェクトを StorageGRID に戻します。
- 残りのオブジェクトが ILM によってクラウドストレージプールに配置されていないことが確実な場合は、バケットからオブジェクトを手動で削除します。

> ILM によって配置された可能性のあるクラウドストレージプールからは、オブジェクトを手動で削除しないでください。手動で削除したオブジェクトにあとで StorageGRID からアクセスしようとしても、削除したオブジェクトは見つかりません。

エラー：クラウドストレージプールにアクセスしようとして、プロキシで外部エラーが発生しました

ストレージノードとクラウドストレージプールに使用する外部の S3 エンドポイントの間に非透過型ストレージプロキシを設定した場合に、このエラーが発生する可能性があります。このエラーは、外部プロキシサーバがクラウドストレージプールのエンドポイントに到達できない場合に発生します。たとえば、 DNS サーバがホスト名を解決できない場合や、外部ネットワークの問題 が存在する場合があります。

問題 を修正するには、次の手順をいくつか実行します。

- クラウドストレージプールの設定（* ILM **>***ストレージプール）を確認します。
- ストレージプロキシサーバのネットワーク設定を確認します。

関連情報

"クラウドストレージプールオブジェクトのライフサイクル"

イレイジャーコーディングプロファイルの設定

イレイジャーコーディングプロファイルを設定するには、ストレージプールを6+3などのイレイジャーコーディングスキームと関連付けます。これにより、ILMルールの配置手順を設定する際に、イレイジャーコーディングプロファイルを選択できるようになります。オブジェクトがルールに一致すると、イレイジャーコーディングスキームに従ってデータフラグメントとパリティフラグメントが作成され、ストレージプール内の格納場所に分散されます。

- "イレイジャーコーディングプロファイルの作成"
- "イレイジャーコーディングプロファイルの名前変更"
- "イレイジャーコーディングプロファイルを非アクティブ化する"

# イレイジャーコーディングプロファイルを作成するには、ストレージノードを含むストレージプールをイレイジャーコーディングスキームに関連付けます。この関連付けにより、作成されるデータフラグメントおよびパリティフラグメントの数と、各フラグメントをどこに分散配置するかが決まります。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- サイトを1つだけ含むストレージプール、または3つ以上のサイトを含むストレージプールを作成しておく必要があります。サイトが 2 つだけのストレージプールではイレイジャーコーディングスキームを使用できません。

このタスクについて

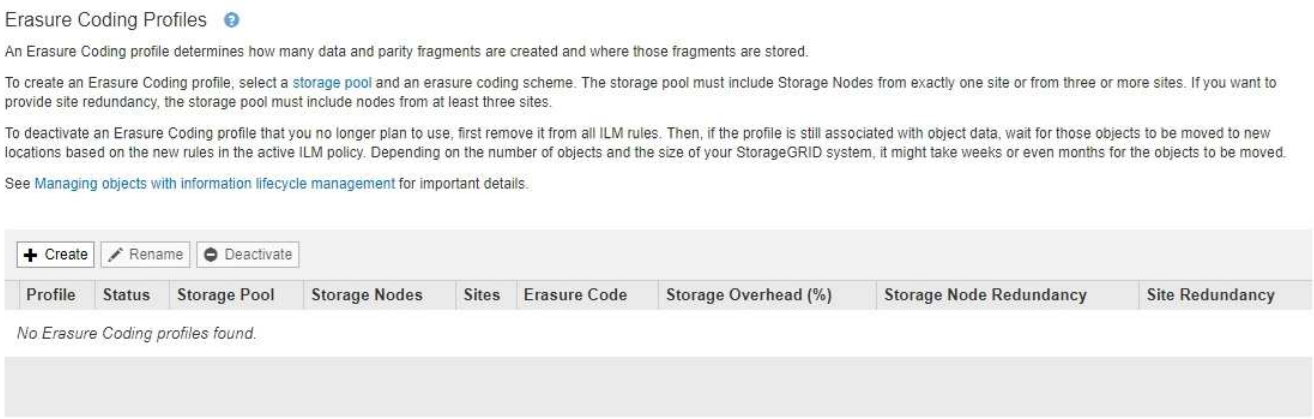
イレイジャーコーディングプロファイルで使用するストレージプールには、サイトが 1 つだけ、または 3 つ以上含まれている必要があります。サイトの冗長性を確保するには、ストレージプールにサイトが少なくとも 3 つ必要です。

ストレージノードを含むストレージプールを選択する必要があります。イレイジャーコーディングデータ用にアーカイブノードを使用することはできません。

手順

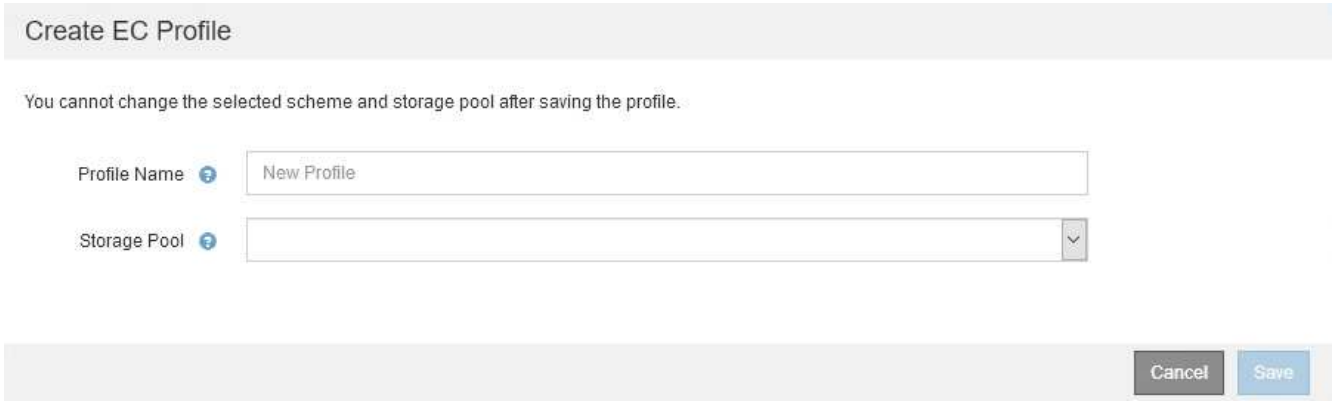
1. ILM * > * イレイジャーコーディング * を選択します。

   イレイジャーコーディングのプロファイルページが表示されます。




2. [ 作成（ Create ） ] をクリックします。

   EC プロファイルの作成ダイアログボックスが表示されます。




3. イレイジャーコーディングプロファイルの一意の名前を入力します。

   イレイジャーコーディングプロファイル名は一意である必要があります。既存のプロファイルの名前を使用すると、そのプロファイルが非アクティブ化されていても、検証エラーが発生します。

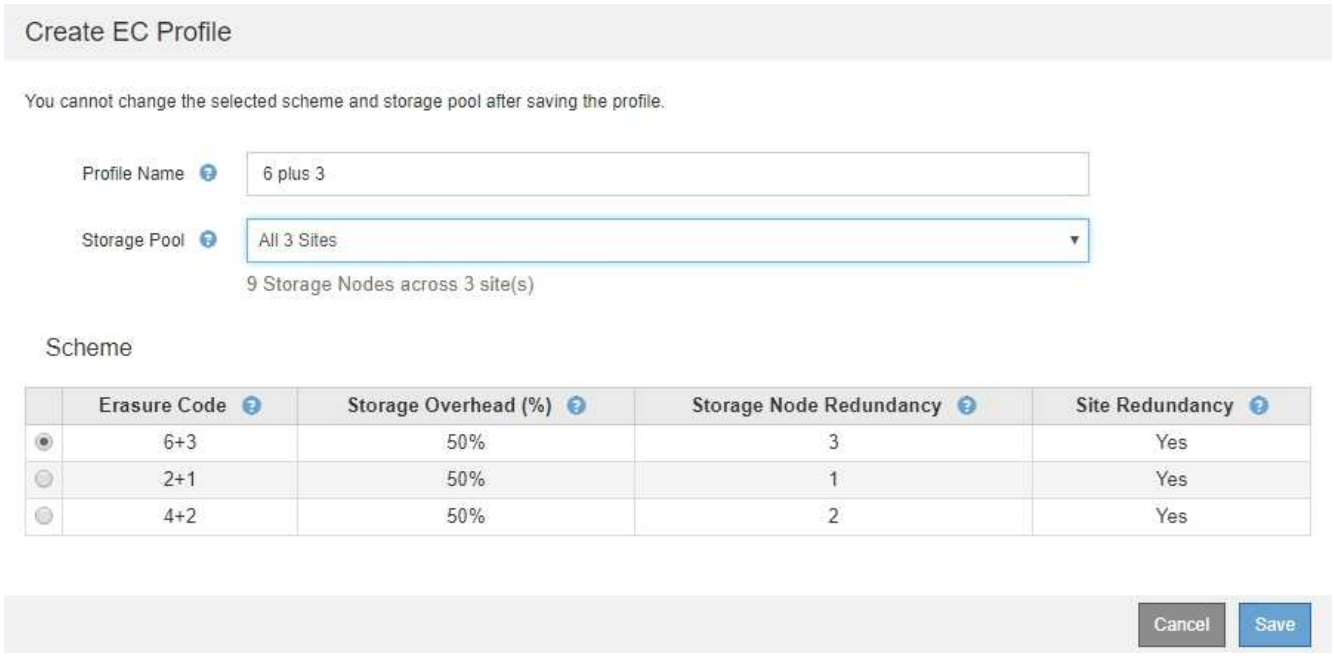
   > ILM ルールの配置手順で、イレイジャーコーディングプロファイル名がストレージプール名に追加されます。

4. このイレイジャーコーディングプロファイル用に作成したストレージプールを選択します。

   > グリッドにサイトが 1 つしかない場合、デフォルトのストレージプール、すべてのストレージノード、またはデフォルトサイトであるすべてのサイトを含むストレージプールは使用できません。これにより、 2 つ目のサイトが追加された場合にイレイジャーコーディングプロファイルが無効になるのを防ぐことができます。

   > ストレージプールにサイトが 2 つだけ含まれている場合、そのストレージプールをイレイジャーコーディングに使用することはできません。2 つのサイトを含むストレージプールではイレイジャーコーディングスキームを使用できません。

   ストレージプールを選択すると、プール内のストレージノードとサイトの数に基づいて、使用可能なイレイジャーコーディングスキームのリストが表示されます。




使用可能な各イレイジャーコーディングスキームについて次の情報が表示されます。

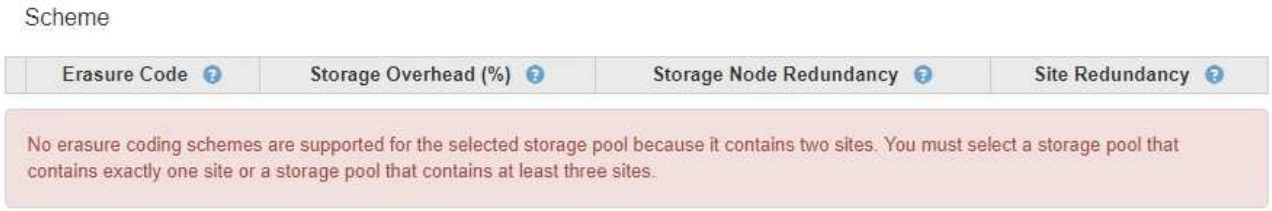
- * イレイジャーコーディングコード * ：イレイジャーコーディングスキームの名前。データフラグメント + パリティフラグメントの形式で表されます。
- * ストレージオーバーヘッド（ % ） * ：オブジェクトのデータサイズを基準とした、パリティフラグメントに必要な追加のストレージ。ストレージオーバーヘッド = パリティフラグメントの総数 / データフラグメントの総数。
- * ストレージノードの冗長性 * ：オブジェクトデータの読み出しが可能な状態で、損失が許容されるストレージノードの数。
- * Site Redundancy * ：選択したイレイジャーコーディングで、サイトが 1 つ失われてもオブジェクトデータの読み出しが可能かどうかを示します。

  サイトの冗長化を確保するには、選択したストレージプールに複数のサイトが含まれていて、どのサイトが失われても十分な数のストレージノードが各サイトに配置されている必要があります。たとえば、 6+3 のイレイジャーコーディングスキームを使用してサイトの冗長化を確保するためには、選択したストレージプールにサイトが 3 つ以上含まれていて、各サイトにストレージノードが 3 つ以上含まれている必要があります。

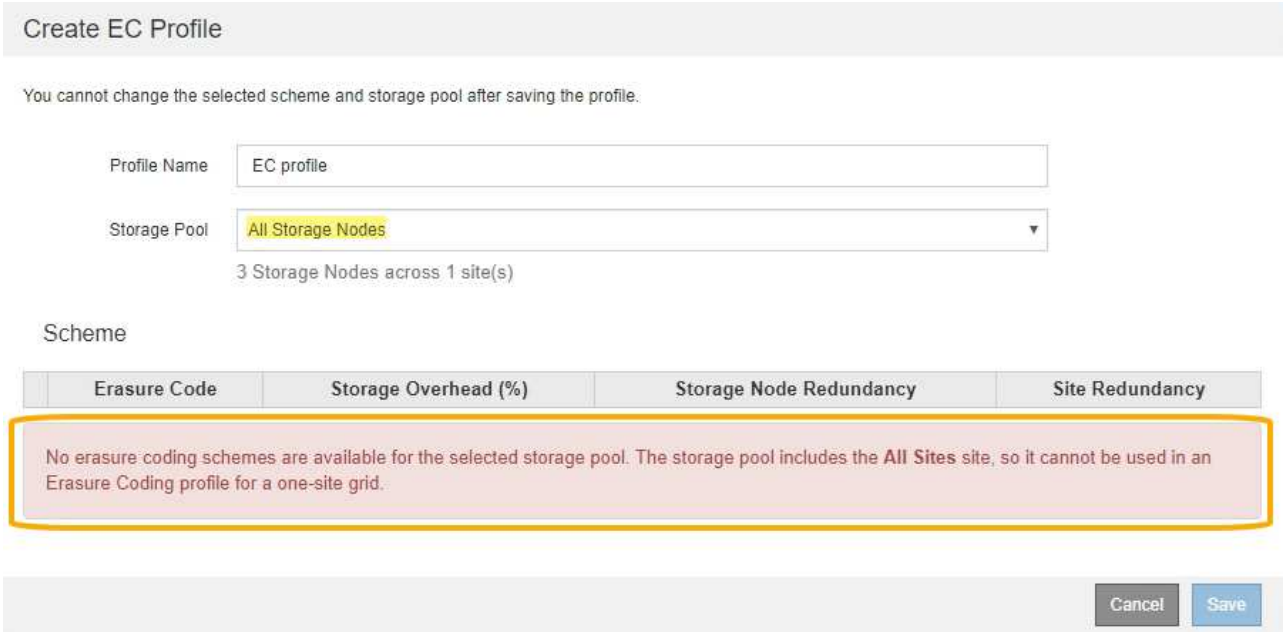
  メッセージは次の場合に表示されます。

- 選択したストレージプールではサイトの冗長性が確保されません。選択したストレージプールに含まれているサイトが 1 つだけの場合は、次のメッセージが表示されます。ノードを障害から保護する場合は、 ILM ルールでこのイレイジャーコーディングプロファイルを使用できます。

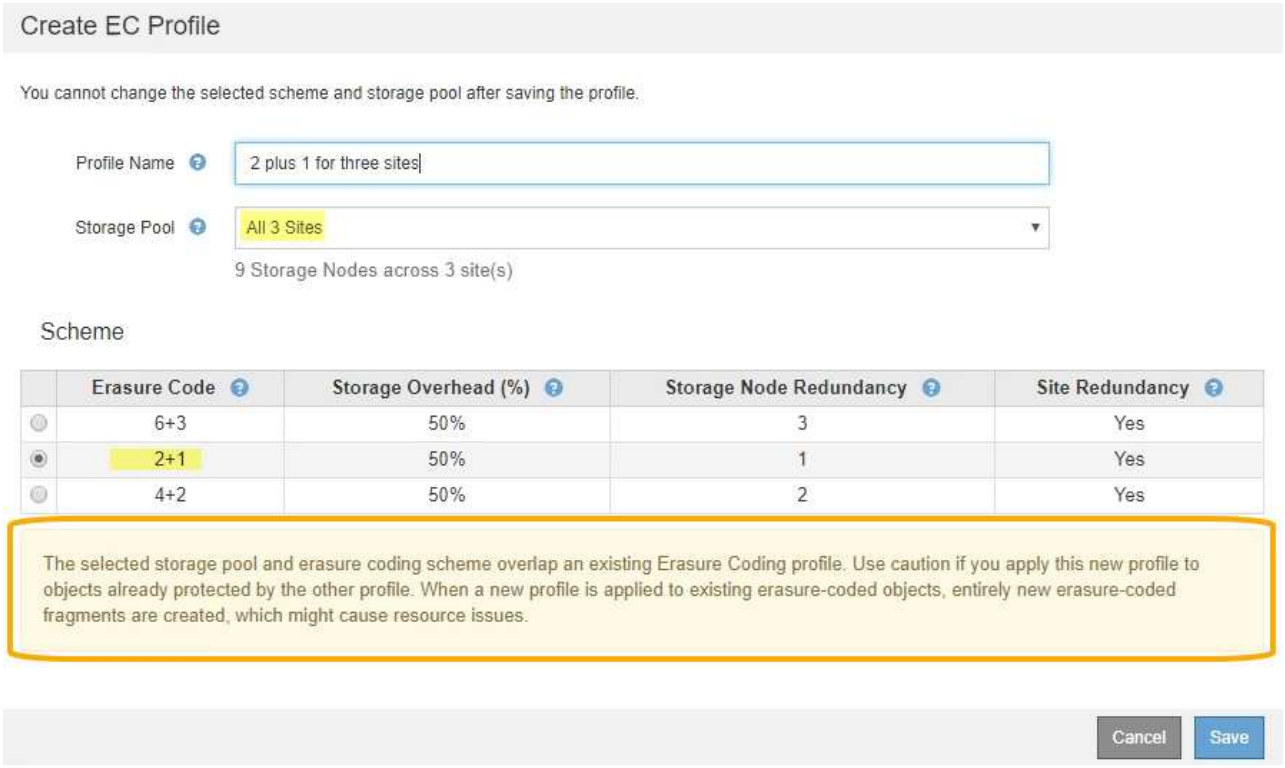
- 選択したストレージプールがイレイジャーコーディングスキームの要件を満たしていません。たとえば、選択したストレージプールに含まれているサイトが 2 つだけの場合は、次のメッセージが表示されます。イレイジャーコーディングを使用してオブジェクトデータを保護する場合は、サイトが 1 つだけ、または 3 つ以上のストレージプールを選択する必要があります。




- グリッドに含まれるサイトが 1 つだけで、デフォルトのストレージプールかすべてのストレージノード、またはデフォルトサイトであるすべてのサイトを含むストレージプールを選択した場合。




- 選択したイレイジャーコーディングスキームとストレージプールが、別のイレイジャーコーディングプロファイルと重複しています。




この例では、別のイレイジャーコーディングプロファイルで 2+1 スキームを使用しており、他のプロファイルのストレージプールでも All 3 Sites ストレージプールのいずれかのサイトを使用しているため、警告メッセージが表示されます。

この新しいプロファイルを作成することはできませんが、 ILM ポリシーでプロファイルの使用を開始する際は十分に注意する必要があります。この新しいプロファイルを他のプロファイルですでに保護されている既存のイレイジャーコーディングオブジェクトに適用すると、 StorageGRID によって完全に新しいオブジェクトフラグメントのセットが作成されます。既存の 2+1 フラグメントは再利用されない。イレイジャーコーディングスキームが同じであっても、あるイレイジャーコーディングプロファイルから別のプロファイルに移行すると、リソースの問題が発生する可能性があります。

5. 複数のイレイジャーコーディングスキームが表示される場合は、使用するスキームを 1 つ選択します。

   どのイレイジャーコーディングスキームを使用するかを決めるにあたっては、フォールトトレランス（パリティセグメントの数が多いほど高くなる）と修復に必要なネットワークトラフィック（フラグメントの数が多いほどネットワークトラフィックも増加する）のバランスを考慮する必要があります。たとえば、4+2 と 6+3 のどちらかのスキームを選ぶ場合、パリティを増やしてフォールトトレランスを向上させる必要がある場合は 6+3 のスキームを選択します。ノード修復時のネットワーク使用量を削減するためにネットワークリソースが制限されている場合は、 4+2 のスキームを選択します。

6. [ 保存（ Save ） ] をクリックします。

イレイジャーコーディングプロファイルの名前変更

## イレイジャーコーディングプロファイルの名前を変更して、プロファイルの内容をより明確にすることができます。

必要なもの

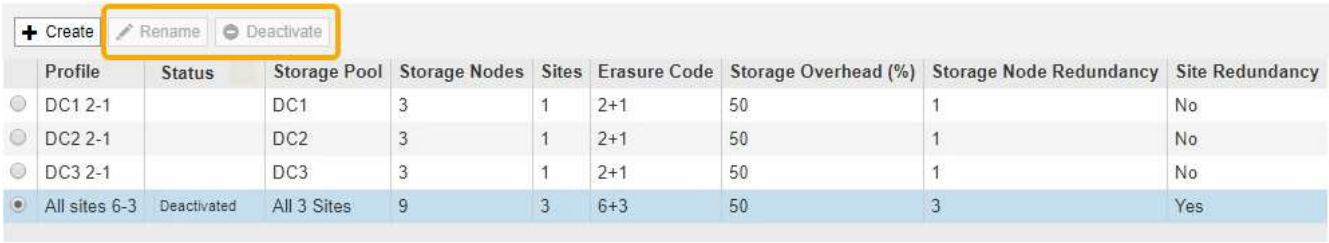
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

- 特定のアクセス権限が必要です。

手順

1. ILM * > * イレイジャーコーディング * を選択します。

   イレイジャーコーディングのプロファイルページが表示されます。[ 名前の変更 * （ Rename * ） ] ボタンと [ 非活動化 * （ Deactivate * ） ] ボタンの両方が無効




2. 名前を変更するプロファイルを選択します。

   [ 名前の変更 * （ Rename * ） ] ボタンと [ 非活動化 * （ Deactivate * ） ] ボタンが有効

3. [ 名前の変更 *] をクリックします。

   EC プロファイルの名前変更ダイアログボックスが表示されます。

4. イレイジャーコーディングプロファイルの一意の名前を入力します。

   ILM ルールの配置手順で、イレイジャーコーディングプロファイル名がストレージプール名に追加されます。

   イレイジャーコーディングプロファイル名は一意である必要があります。既存のプロファイルの名前を使用すると、そのプロファイルが非アクティブ化されていても、検証エラーが発生します。

5. [ 保存（ Save ） ] をクリックします。

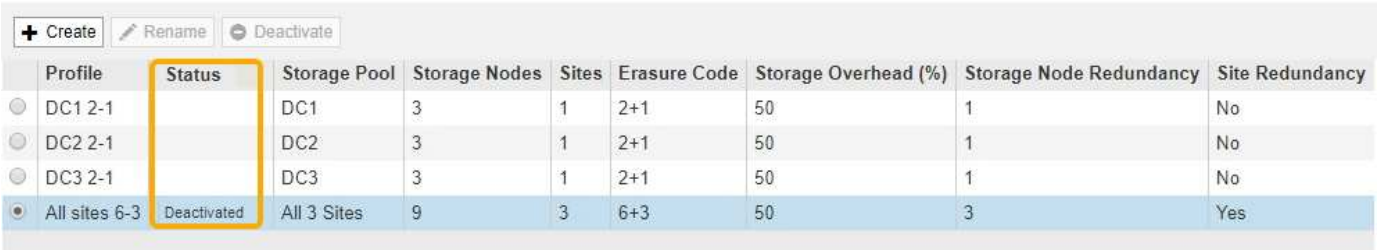
# 使用する予定がなくなったイレイジャーコーディングプロファイルや、プロファイルが現在どの ILM ルールでも使用されていないプロファイルは、非アクティブ化できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- イレイジャーコーディングされたデータ修復処理または運用停止手順が実行中でないことを確認しておく必要があります。いずれかの処理の実行中にイレイジャーコーディングプロファイルを非アクティブ化しようとすると、エラーメッセージが返されます。

このタスクについて

イレイジャーコーディングプロファイルを非アクティブ化しても、プロファイルはイレイジャーコーディングのプロファイルページに表示されますが、ステータスは * deactivated* になります。




| | Profile | Status | Storage Pool | Storage Nodes | Sites | Erasure Code | Storage Overhead (%) | Storage Node Redundancy | Site Redundancy |
|---|---|---|---|---|---|---|---|---|---|
| ○ | DC1 2-1 | | DC1 | 3 | 1 | 2+1 | 50 | 1 | No |
| ○ | DC2 2-1 | | DC2 | 3 | 1 | 2+1 | 50 | 1 | No |
| ○ | DC3 2-1 | | DC3 | 3 | 1 | 2+1 | 50 | 1 | No |
| ◉ | All sites 6-3 | Deactivated | All 3 Sites | 9 | 3 | 6+3 | 50 | 3 | Yes |

非アクティブ化されたイレイジャーコーディングプロファイルは使用できなくなります。非アクティブ化したプロファイルは、 ILM ルールの配置手順の作成時に表示されません。非アクティブ化したプロファイルは再アクティブ化できません。

StorageGRID では、次のいずれかに該当する場合はイレイジャーコーディングプロファイルを非アクティブ化できません。

- イレイジャーコーディングプロファイルは現在 ILM ルールで使用されています。
- ILM ルールではイレイジャーコーディングプロファイルが使用されなくなりましたが、プロファイルのオブジェクトデータとパリティのフラグメントはまだ存在します。

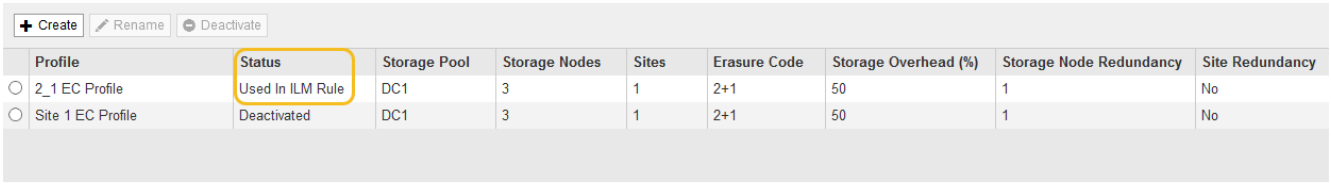
手順

1. ILM * > * イレイジャーコーディング * を選択します。

   イレイジャーコーディングのプロファイルページが表示されます。[ 名前の変更 * （ Rename * ） ] ボタンと [ 非活動化 * （ Deactivate * ） ] ボタンの両方が無効

2. ステータス * 列を確認して、非アクティブ化するイレイジャーコーディングプロファイルが ILM ルールで使用されていないことを確認します。

   ILM ルールで使用されているイレイジャーコーディングプロファイルは非アクティブ化できません。この例では、少なくとも 1 つの ILM ルールで * 2_1 EC プロファイル * が使用されています。

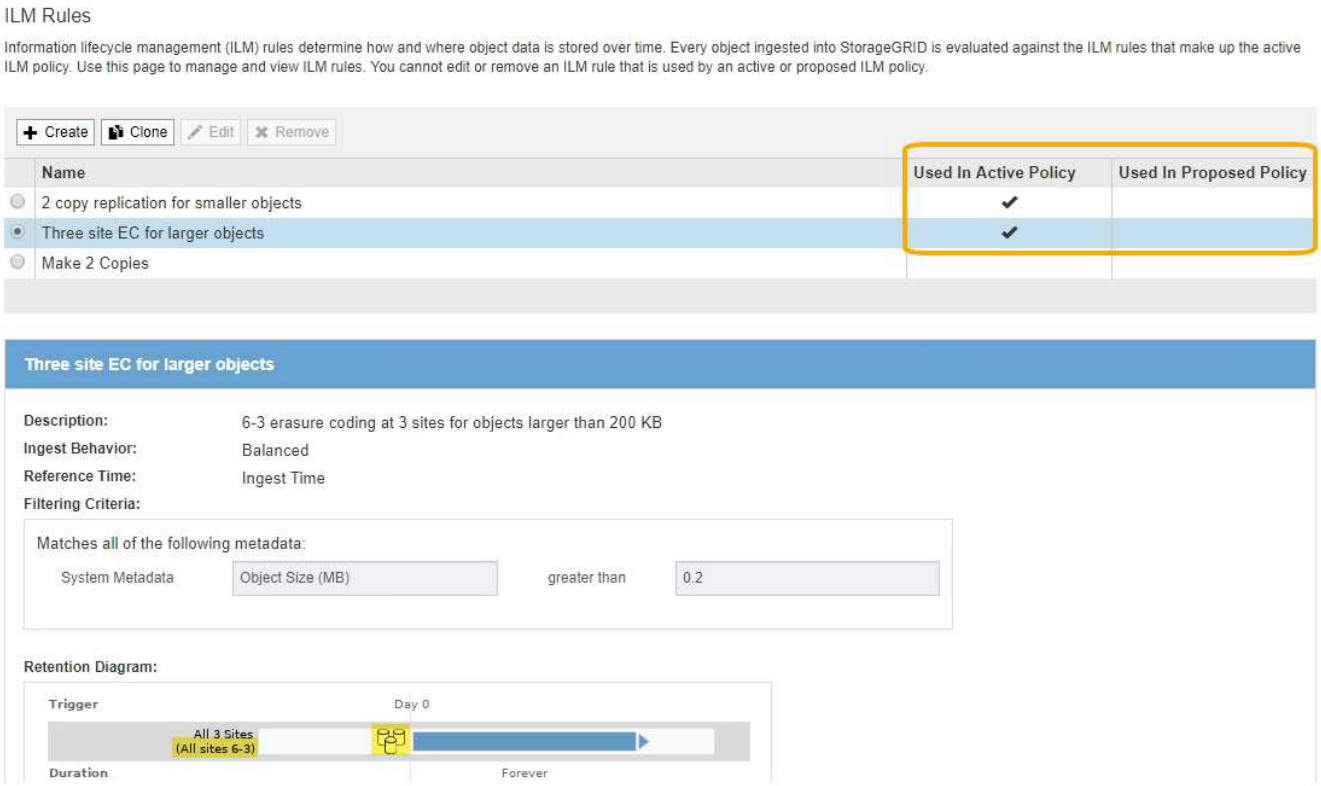



3. プロファイルが ILM ルールで使用されている場合は、次の手順を実行します。

   a. [* ILM*>* Rules] を選択します。

   b. 表示されているルールごとに、オプションボタンを選択し、保持図を確認して、非アクティブ化するイレイジャーコーディングプロファイルがルールで使用されているかどうかを判断します。

      この例では、「 3 サイト EC for larger objects 」ルールで、「 * All 3 Sites * 」というストレージプールと「 * all sites 6+3 * イレイジャーコーディングプロファイル」を使用しています。イレイジャーコーディングプロファイルは次のアイコンで表されます。




   a. 非アクティブ化するイレイジャーコーディングプロファイルを ILM ルールが使用している場合は、そのルールがアクティブな ILM ポリシーとドラフトポリシーのどちらで使用されているかを確認します。

      この例では、アクティブな ILM ポリシーで大容量オブジェクト * ルール用の * 3 サイト EC が使用されています。

   b. イレイジャーコーディングプロファイルの使用場所に基づいて、表に記載された追加の手順を実行します。

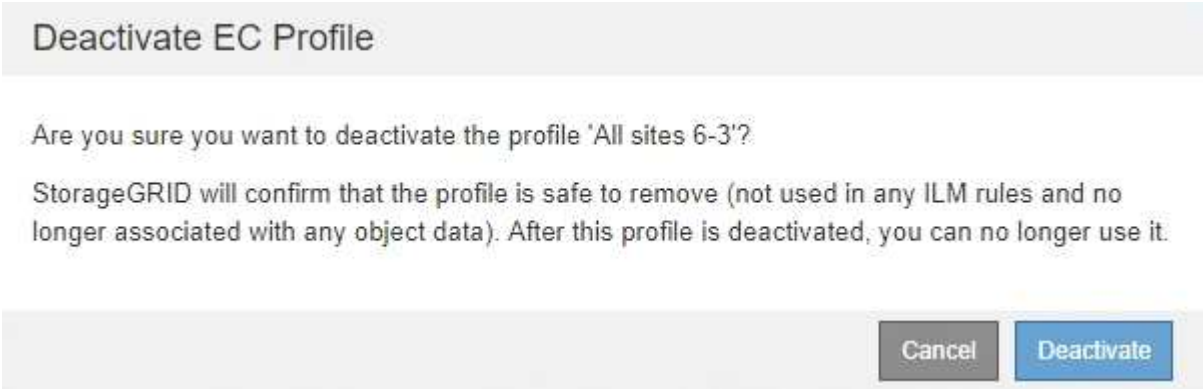
| プロファイルはどこで使用されていますか？ | プロファイルを非アクティブ化する前に実行する追加手順 | 追加の手順を参照してください |
| --- | --- | --- |
| ILM ルールでは使用されません | 追加の手順は必要ありません。この手順に進みます。 | _ なし _ |
| ILM ポリシーで使用されたことのない ILM ルール | i. 該当する ILM ルールをすべて編集または削除します。ルールを編集する場合は、イレイジャーコーディングプロファイルを使用するすべての配置を削除します。<br>ii. この手順に進みます。 | "ILMルールおよびILMポリシーの操作" |
| アクティブな ILM ポリシーに現在含まれている ILM ルール | i. アクティブポリシーのクローンを作成します。<br>ii. イレイジャーコーディングプロファイルを使用する ILM ルールを削除します。<br>iii. オブジェクトを確実に保護するために、新しい ILM ルールを 1 つ以上追加します。<br>iv. 新しいポリシーを保存、シミュレート、およびアクティブ化します。<br>v. 新しいポリシーが適用され、追加した新しいルールに基づいて既存のオブジェクトが新しい場所に移動されるまで待ちます。<br>◦ 注： StorageGRID システムのオブジェクト数とサイズによっては、新しい ILM ルールに基づいてオブジェクトを新しい場所に移動するのに数週間から数カ月かかる場合があります。<br>データに関連付けられたままイレイジャーコーディングプロファイルを安全に非アクティブ化しようとしても、非アクティブ化処理は失敗します。プロファイルを非アクティブ化する準備ができていない場合は、エラーメッセージが表示されます。<br>vi. ポリシーから削除したルールを編集または削除します。ルールを編集する場合は、イレイジャーコーディングプロファイルを使用するすべての配置を削除します。<br>vii. この手順に進みます。 | • "ILMポリシーを作成する"<br>• "ILMルールおよびILMポリシーの操作" |

| プロファイルはどこで使用されていますか？ | プロファイルを非アクティブ化する前に実行する追加手順 | 追加の手順を参照してください |
| --- | --- | --- |
| ドラフトの ILM ポリシーに現在含まれている ILM ルール | i. ドラフトポリシーを編集します。<br>ii. イレイジャーコーディングプロファイルを使用する ILM ルールを削除します。<br>iii. すべてのオブジェクトが保護されるように 1 つ以上の新しい ILM ルールを追加します。<br>iv. ドラフトポリシーを保存します。<br>v. ポリシーから削除したルールを編集または削除します。ルールを編集する場合は、イレイジャーコーディングプロファイルを使用するすべての配置を削除します。<br>vi. この手順に進みます。 | • "ILMポリシーを作成する"<br>• "ILMルールおよびILMポリシーの操作" |
| ILM 履歴ポリシー内の ILM ルール | i. ルールを編集または削除します。ルールを編集する場合は、イレイジャーコーディングプロファイルを使用するすべての配置を削除します。（このルールは履歴ポリシーに履歴ルールとして表示されます）。<br>ii. この手順に進みます。 | • "ILMルールおよびILMポリシーの操作" |

c. プロファイルが ILM ルールで使用されていないことを確認するには、イレイジャーコーディングのプロファイルページをリフレッシュしてください。

4. プロファイルが ILM ルールで使用されていない場合は、ラジオボタンを選択し、 * Deactivate * を選択します。

[EC プロファイルを非活動化（ Deactivate EC Profile ） ] ダイアログボックスが表示




5. プロファイルを非活動化してもよい場合は、 [ * 非活動化 * （ * Deactivate * ） ] を選択します。

◦ StorageGRID でイレイジャーコーディングプロファイルを非アクティブ化できる場合、ステータスは * deactivated* になります。これで、どの ILM ルールにもこのプロファイルを選択できなくなりました。

◦ StorageGRID がプロファイルを非アクティブ化できない場合は、エラー・メッセージが表示されます。たとえば、オブジェクトデータがまだこのプロファイルに関連付けられている場合は、エラーメ

ッセージが表示されます。無効化プロセスを再度実行する前に、数週間待つ必要がある場合があります。

リージョンの設定（オプション、**S3**のみ）

# ILM ルールは S3 バケットが作成されたリージョンに基づいてオブジェクトをフィルタリングできるため、オブジェクトのリージョンによって異なるストレージに格納できます。S3 バケットのリージョンをルールのフィルタとして使用する場合は、システム内のバケットで使用できるリージョンを最初に作成しておく必要があります。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

S3 バケットを作成する際は、特定のリージョンにバケットを作成するように指定できます。リージョンを指定すると地理的にユーザにより近い場所にバケットを配置でき、レイテンシの最適化、コストの最小化、規制要件への対応を実現できます。

ILM ルールの作成時には、 S3 バケットに関連付けられているリージョンを高度なフィルタとして使用できます。たとえば、 us-west-2 リージョンで作成された S3 バケット内のオブジェクトにのみ適用するルールを作成できます。そのうえで、そのリージョン内のデータセンターサイトにあるストレージノードにオブジェクトのコピーを配置してレイテンシを最適化するように指定できます。

リージョンを設定する場合は、次の注意事項に従ってください。

- デフォルトでは、すべてのバケットが us-east-1 リージョンに属しているとみなされます。
- Tenant Manager またはテナント管理 API を使用してバケットを作成するとき、または S3 の PUT Bucket API 要求の LocationConstraint 要求要素を使用してバケットを作成するときにデフォルト以外のリージョンを指定する前に、 Grid Manager を使用してリージョンを作成する必要があります。StorageGRID で定義されていないリージョンを PUT Bucket 要求で使用すると、エラーが発生します。
- S3 バケットの作成時には正確なリージョン名を使用する必要があります。リージョン名では大文字と小文字が区別されます。 2 文字以上 32 文字以下にする必要があります。有効な文字は、数字、アルファベット、およびハイフンです。

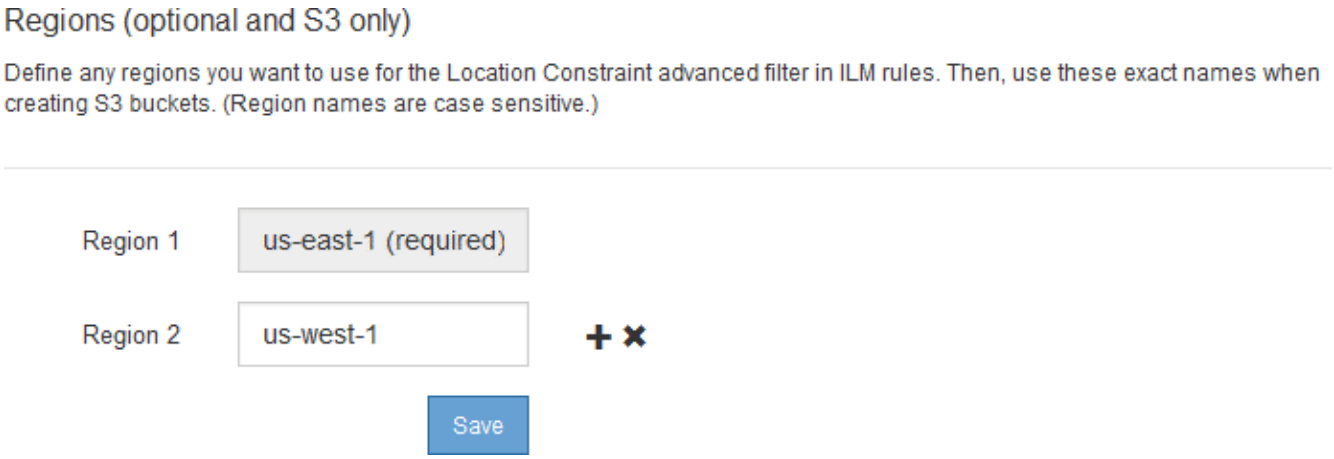
> EU は、 eu-west-1 のエイリアスとはみなされません。EU または eu-west-1 リージョンを使用する場合は、正確な名前を使用する必要があります。

- アクティブな ILM ポリシーやドラフトの ILM ポリシー内で現在使用されているリージョンを削除または変更することはできません。
- ILM ルールで高度なフィルタとして使用されているリージョンが無効な場合でも、そのルールをドラフトポリシーに追加できます。ただし、ドラフトポリシーを保存またはアクティブ化しようとするとエラーが発生します。（無効なリージョンは、 ILM ルールで高度なフィルタとして使用しているリージョンをあとで削除した場合や、グリッド管理 API を使用してルールを作成し、定義していないリージョンを指定した場合に発生することがあります）。
- あるリージョンを使用して S3 バケットを作成したあとにそのリージョンを削除した場合、高度なフィルタ「 Location Constraint 」を使用してそのバケット内のオブジェクトを検索するにはリージョンを再び追加する必要があります。

手順

1. [* ILM*>* Regions* ] を選択します。

   Regions ページが表示され、現在定義されているリージョンがリストされます。*領域1 *はデフォルト領域を示します。 `us-east-1`（変更または削除できません）。




2. リージョンを追加するには：

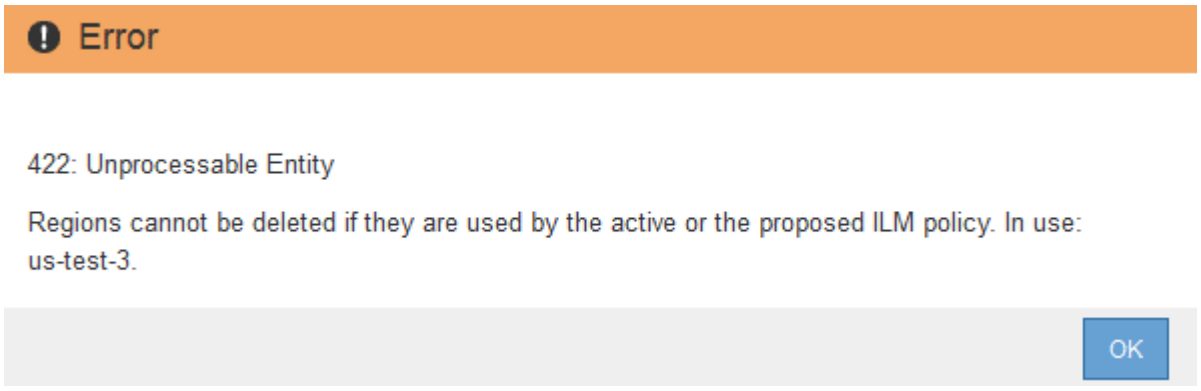
   a. 挿入アイコンをクリックします ✚ アイコン"] をクリックします。

   b. S3 バケットの作成時に使用するリージョンの名前を入力します。

      対応する S3 バケットの作成時には、正確なリージョン名を LocationConstraint 要求の要素として使用する必要があります。

3. 未使用の領域を削除するには、削除アイコンをクリックします ✖。

   アクティブポリシーまたはドラフトポリシーで現在使用されているリージョンを削除しようとすると、エラーメッセージが表示されます。




4. 変更が完了したら、*保存*をクリックします。

   Create ILM Rule ウィザードの Advanced Filtering ページの * Location Constraint * リストからこれらのリージョンを選択できるようになりました。

関連情報

"ILMルールで高度なフィルタを使用する"

# ILM ルールを使用して、時間の経過に伴うオブジェクトデータの配置を管理できます。ILM ルールを作成するには、 Create ILM Rule ウィザードを使用します。

作業を開始する前に

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- このルール環境 を使用するテナントアカウントを指定する場合は、Tenant Accounts権限が必要です。または、各アカウントのアカウントIDを確認しておく必要があります。
- 最終アクセス時間のメタデータでオブジェクトをフィルタリングするルールの場合、 S3 の場合はバケットで、 Swift の場合はコンテナで最終アクセス時間の更新が有効になっている必要があります。
- レプリケートコピーを作成する場合は、使用するストレージプールまたはクラウドストレージプールを設定しておく必要があります。
- イレイジャーコーディングコピーを作成する場合は、イレイジャーコーディングプロファイルを設定しておく必要があります。
- に精通している必要があります "取り込みのデータ保護オプション"。
- S3オブジェクトロックで使用する準拠ルールを作成する必要がある場合は、を参照しておく必要があります "S3 オブジェクトのロックの要件"。

> ポリシーのデフォルトのILMルールを作成するには、代わりに次の手順 を使用します。 "デフォルトのILMルールを作成する"。

このタスクについて

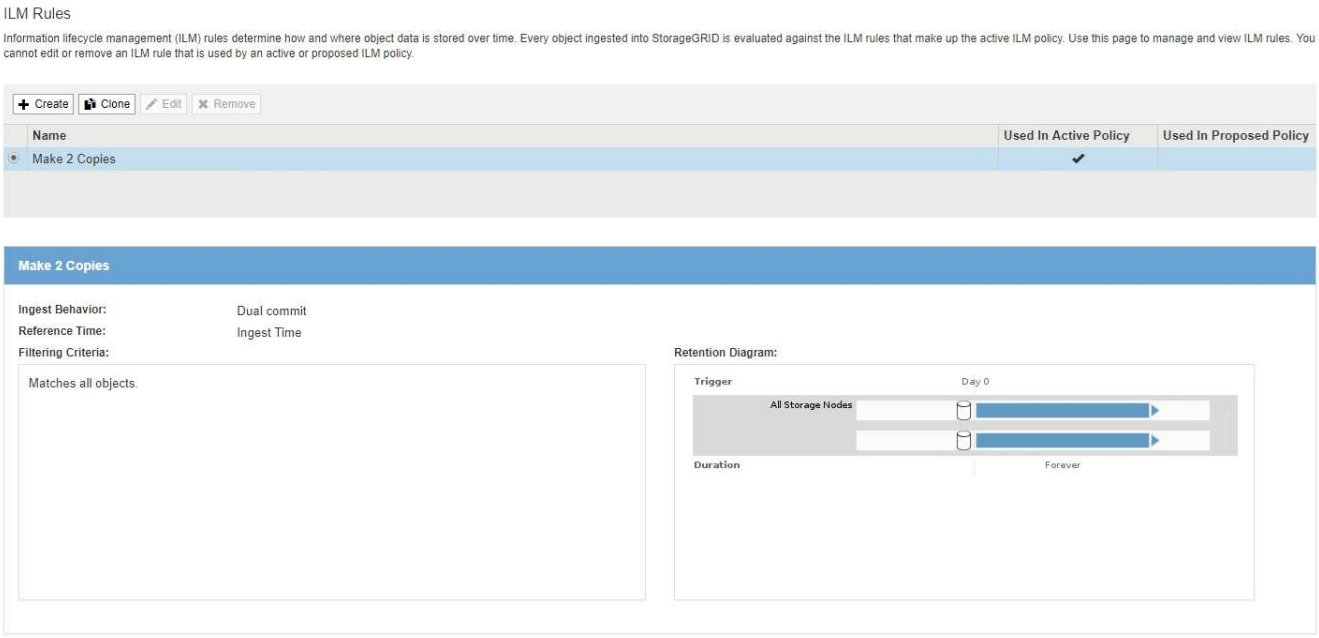
ILM ルールを作成する場合は、次の点

- StorageGRID システムのトポロジとストレージ構成を考慮します。
- 作成するオブジェクトコピーのタイプ（レプリケートまたはイレイジャーコーディング）および各オブジェクトに必要なコピー数を検討します。
- StorageGRID システムに接続するアプリケーションで使用されるオブジェクトメタデータのタイプを決定します。ILM ルールは、メタデータに基づいてオブジェクトをフィルタリングします。
- 時間の経過に伴うオブジェクトコピーの配置先を検討します。
- 取り込み時のデータ保護に使用するオプション（Balanced、Strict、Dual commit）を決定します。

手順

1. [* ILM*>* Rules] を選択します。

   ILM ルールページが表示され、組み込みのルールである Make 2 Copies が選択されます。




StorageGRID システムでグローバルな S3 オブジェクトのロック設定が有効になっている場合、 ILM ルールページの外観は少し異なります。サマリテーブルには * 準拠 * 列が含まれ、選択したルールの詳細には * 準拠 * フィールドが含まれます。

2. 「 * Create * 」を選択します。

   Create ILM Rule ウィザードの Step 1 （ Define Basics ）が表示されます。基本の定義ページを使用して、ルール環境 で使用するオブジェクトを定義します。

関連情報

"S3 を使用する"

"Swift を使用します"

"イレイジャーコーディングプロファイルの設定"

"ストレージプールを設定しています"

"クラウドストレージプールの使用"

"取り込みのデータ保護オプション"

"S3オブジェクトロックでオブジェクトを管理する"

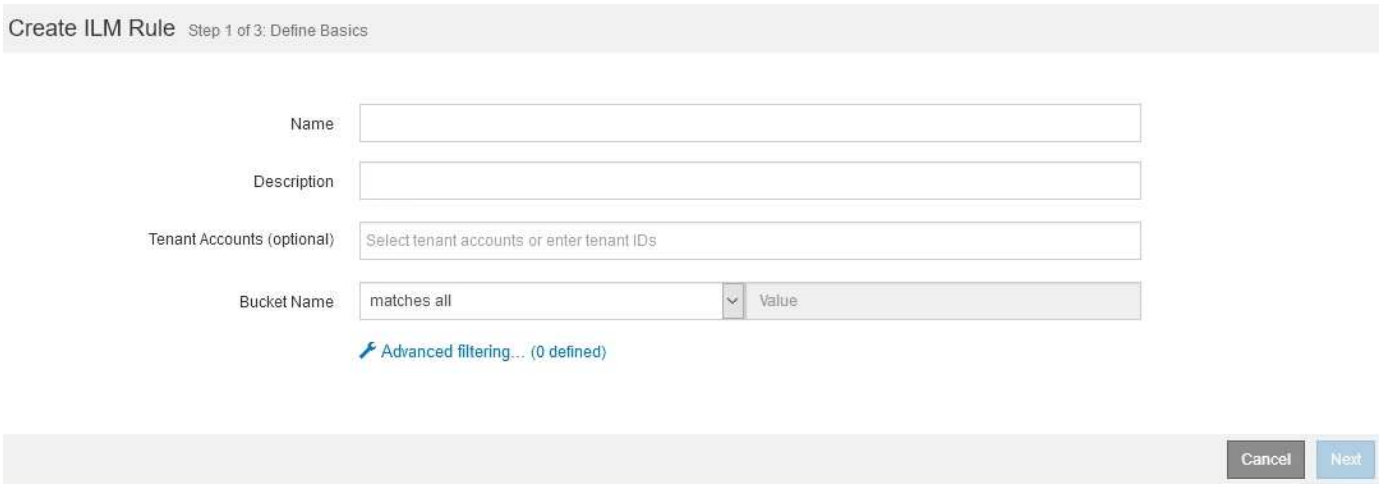
ステップ **1/3** ：基本事項を定義します

## Create ILM Rule ウィザードのステップ 1 （ Define Basics ）では、ルールの基本フィルタと高度なフィルタを定義できます。

このタスクについて

StorageGRID は、 ILM ルールに照らしてオブジェクトを評価する際に、オブジェクトメタデータをルールのフィルタと比較します。オブジェクトメタデータがすべてのフィルタに一致した場合、 StorageGRID はルー

ルを使用してオブジェクトを配置します。すべてのオブジェクトに適用するルールを設計したり、 1 つ以上のテナントアカウントやバケット名などの基本的なフィルタや、オブジェクトのサイズやユーザメタデータなどの高度なフィルタを指定したりできます。



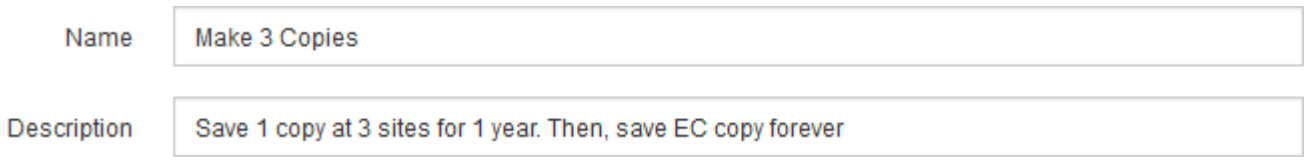

手順

1. [* 名前 *] フィールドに、ルールの一意の名前を入力します。

   1~64 文字で指定する必要があります。

2. 必要に応じて、ルールの短い概要 を * 概要 * フィールドに入力します。

   あとから識別しやすいように、ルールの目的や機能を指定してください。




3. 必要に応じて、このルールを適用する S3 または Swift テナントアカウントを 1 つ以上選択します。このルールですべてのテナントを環境 に設定する場合は、このフィールドを空白のままにします。

   Root Access権限またはTenant Accounts権限がない場合は、リストからテナントを選択できません。代わりに、テナント ID を入力するか、複数の ID をカンマで区切って入力します。

4. 必要に応じて、このルールを適用する S3 バケットまたは Swift コンテナを指定します。

   「 * matches all * 」が選択されている場合（デフォルト）、「環境 all S3 bucketes 」または「 Swift containers 」というルールが適用されます。

5. 必要に応じて、 ［ * 高度なフィルタリング * ］ を選択し、追加のフィルタを指定します。

   高度なフィルタを設定しない場合は、基本フィルタに一致するすべてのオブジェクトを環境 ルールに追加します。

> このルールでイレイジャーコーディングコピーを作成する場合は、「高度なフィルタリング」を選択します。次に、高度なフィルタ「* Object Size（MB）」を追加し、「 greater than 0.2 *」に設定します。サイズフィルタを使用すると、2MB以下のオブジェクトはイレイジャーコーディングされません。

6. 「 * 次へ * 」を選択します。

ステップ 2 （配置を定義）が表示されます。

関連情報

"ILM ルールのフィルタリングとは"

"ILMルールで高度なフィルタを使用する"

"ステップ 2 / 3 ：配置を定義する"

**ILM**ルールで高度なフィルタを使用する

高度なフィルタを使用すると、メタデータに基づいて特定のオブジェクトにのみ適用する ILM ルールを作成できます。ルールに対して高度なフィルタを設定するには、照合するメタデータのタイプを選択し、演算子を選択して、メタデータ値を指定します。オブジェクトが評価されると、高度なフィルタに一致するメタデータを含むオブジェクトにのみ ILM ルールが適用されます。

次の表に、高度なフィルタで指定できるメタデータタイプ、各タイプのメタデータに使用できる演算子、および想定されるメタデータ値を示します。

| メタデータタイプ | サポートされる演算子 | メタデータ値 |
| --- | --- | --- |
| 取り込み時間（マイクロ秒） | • が等しい<br>• が同じではありません<br>• より小さい<br>• が次の値以下です<br>• が次の値より大きい<br>• が次の値以上である | オブジェクトが取り込まれた日時。<br>• 注：新しい ILM ポリシーをアクティブ化する際にリソースの問題が発生しないように、既存のオブジェクトの数が多い場合は、ルールで取り込み時間の高度なフィルタを使用することができます。既存のオブジェクトが不必要に移動されないようにするために、新しいポリシーが適用されるおおよその時間よりも長くなるように取り込み時間を設定します。 |
| キーを押します | • が等しい<br>• が同じではありません<br>• が含まれます<br>• にはを含めません<br>• がで始まります<br>• で始まるものではありません<br>• が次の値で終わる<br>• で終わることはありません | 一意の S3 または Swift オブジェクトキーのすべてまたは一部。<br>たとえば、で終わるオブジェクトを照合できます `.txt` またはで開始します `test-object/`。 |

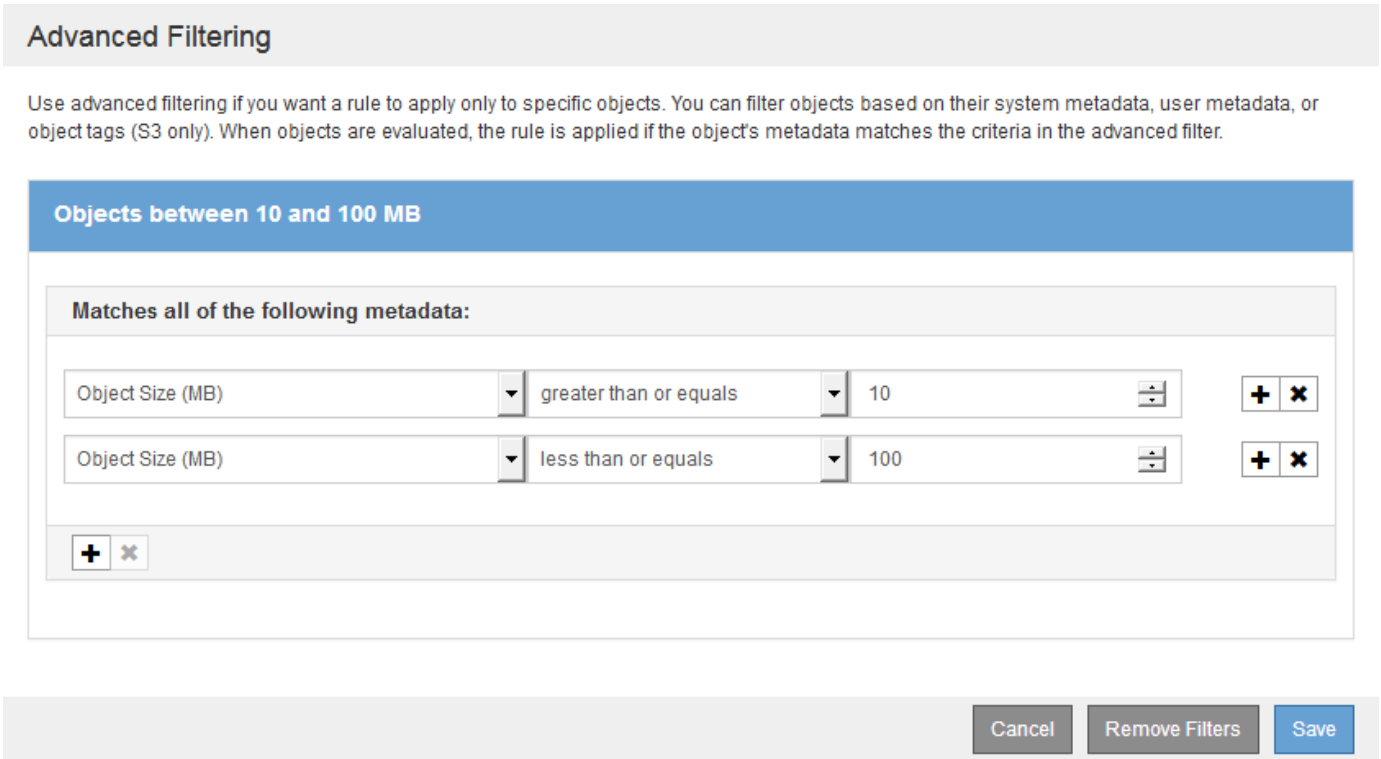
| メタデータタイプ | サポートされる演算子 | メタデータ値 |
| --- | --- | --- |
| 最終アクセス時間（マイクロ秒） | • が等しい<br>• が同じではありません<br>• より小さい<br>• が次の値以下です<br>• が次の値より大きい<br>• が次の値以上である<br>• が存在します<br>• は存在しません | オブジェクトが最後に読み出された（読み取られた、または表示された）日時。<br>• 注：最終アクセス時間を高度なフィルタとして使用する場合は、 S3 バケットまたは Swift コンテナに対して最終アクセス時間の更新を有効にする必要があります。<br>"ILMルールで最終アクセス日時を使用する" |
| 場所の制約（ S3 のみ） | • が等しい<br>• が同じではありません | S3 バケットが作成されたリージョン。表示されるリージョンを定義するには、 * ilm * > * Regions * を使用します。<br>• 注： us-east-1 の値は、 us-east-1 リージョンで作成されたバケット内のオブジェクト、およびリージョンが指定されていないバケット内のオブジェクトに一致します。<br>"リージョンの設定（オプション、S3のみ）" |
| オブジェクトサイズ（ MB ） | • が等しい<br>• が次の値と等しくない<br>• より小さい<br>• が次の値以下です<br>• が次の値より大きい<br>• が次の値以上である | オブジェクトのサイズ（ MB 単位）。<br>1MB未満のオブジェクトサイズでフィルタリングするには、10進値を入力します。たとえば、イレイジャーコーディングコピーを作成するルールの場合は、「* Object Size（MB）* advanced filter」を「* greater than 0.2 *」に設定します。この設定により、200KB以下のオブジェクトにイレイジャーコーディングが使用されることはありません。<br>*注意：*ブラウザの種類とロケールの設定によって、小数点としてピリオドまたはカンマを使用する必要があるかどうかが制御されます。 |

| メタデータタイプ | サポートされる演算子 | メタデータ値 |
| --- | --- | --- |
| ユーザメタデータ | • が含まれます<br>• が次の値で終わる<br>• が等しい<br>• が存在します<br>• にはを含めません<br>• で終わることはありません<br>• が同じではありません<br>• は存在しません<br>• で始まるものではありません<br>• がで始まります | キーと値のペア。 * User Metadata Name * はキー、 * User Metadata Value * は値です。<br><br>たとえば、ユーザメタデータがあるオブジェクトでフィルタリングするには、のように指定します `color=blue`、を指定します `color` ユーザーメタデータ名*の場合、 `equals` 演算子の場合は、および `blue` For * User Metadata Value *を参照してください。<br><br>• 注： * ユーザメタデータ名では大文字と小文字は区別されませんが、値では大文字と小文字が区別されます。 |
| オブジェクトタグ（ S3 のみ） | • が含まれます<br>• が次の値で終わる<br>• が等しい<br>• が存在します<br>• にはを含めません<br>• で終わることはありません<br>• が同じではありません<br>• は存在しません<br>• で始まるものではありません<br>• がで始まります | キーと値のペア。 * オブジェクトタグ名 * はキー、 * オブジェクトタグ値 * は値です。<br><br>たとえば、オブジェクトタグがのオブジェクトでフィルタリングする場合などです `Image=True`、を指定します `Image` *オブジェクトタグ名*の場合、 `equals` 演算子の場合は、および `True` for * Object Tag value *。<br><br>• 注： * オブジェクトタグ名とオブジェクトタグ値では、大文字と小文字が区別されます。これらの項目は、オブジェクトに対して定義されたとおりに正確に入力する必要があります。 |

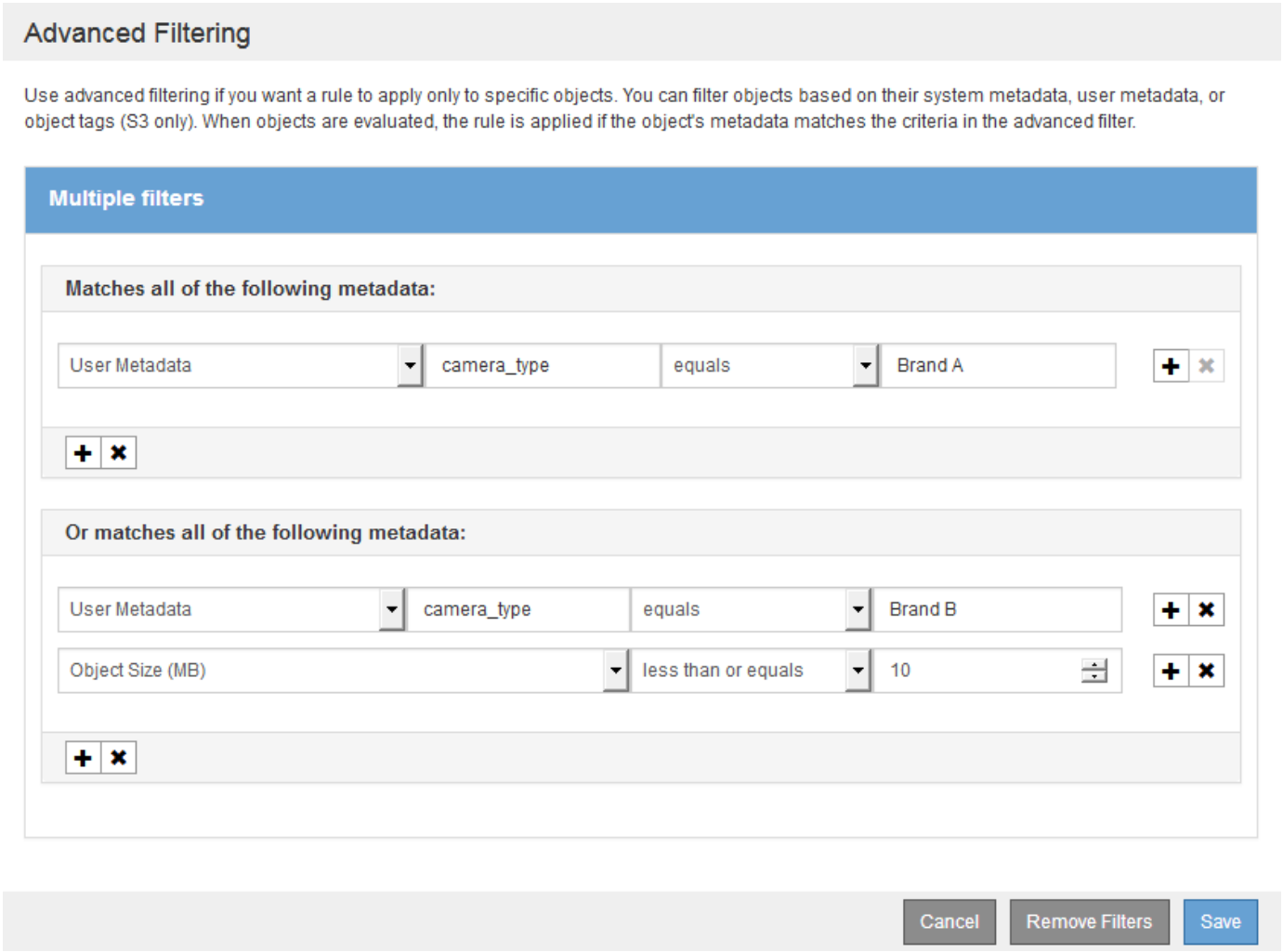
複数のメタデータタイプと値を指定する

高度なフィルタを定義する場合は、複数のタイプのメタデータと複数のメタデータ値を指定できます。たとえば、サイズが 10~100MB のオブジェクトに一致するルールを設定するには、 * Object Size * メタデータタイプを選択し、 2 つのメタデータ値を指定します。

- 最初のメタデータ値で 10MB 以上のオブジェクトを指定します。
- 2 番目のメタデータ値で 100MB 以下のオブジェクトを指定します。




複数のエントリを使用すると、照合するオブジェクトを正確に制御できます。次の例では、 camera_type ユーザメタデータの値が Brand A または Brand B の環境 オブジェクトをルールします。ただし、ルールでは、10MB より小さい Brand B のオブジェクトのみが環境 されます。




関連情報

"ILMルールで最終アクセス日時を使用する"

"リージョンの設定（オプション、S3のみ）"

ステップ **2 / 3** ：配置を定義する

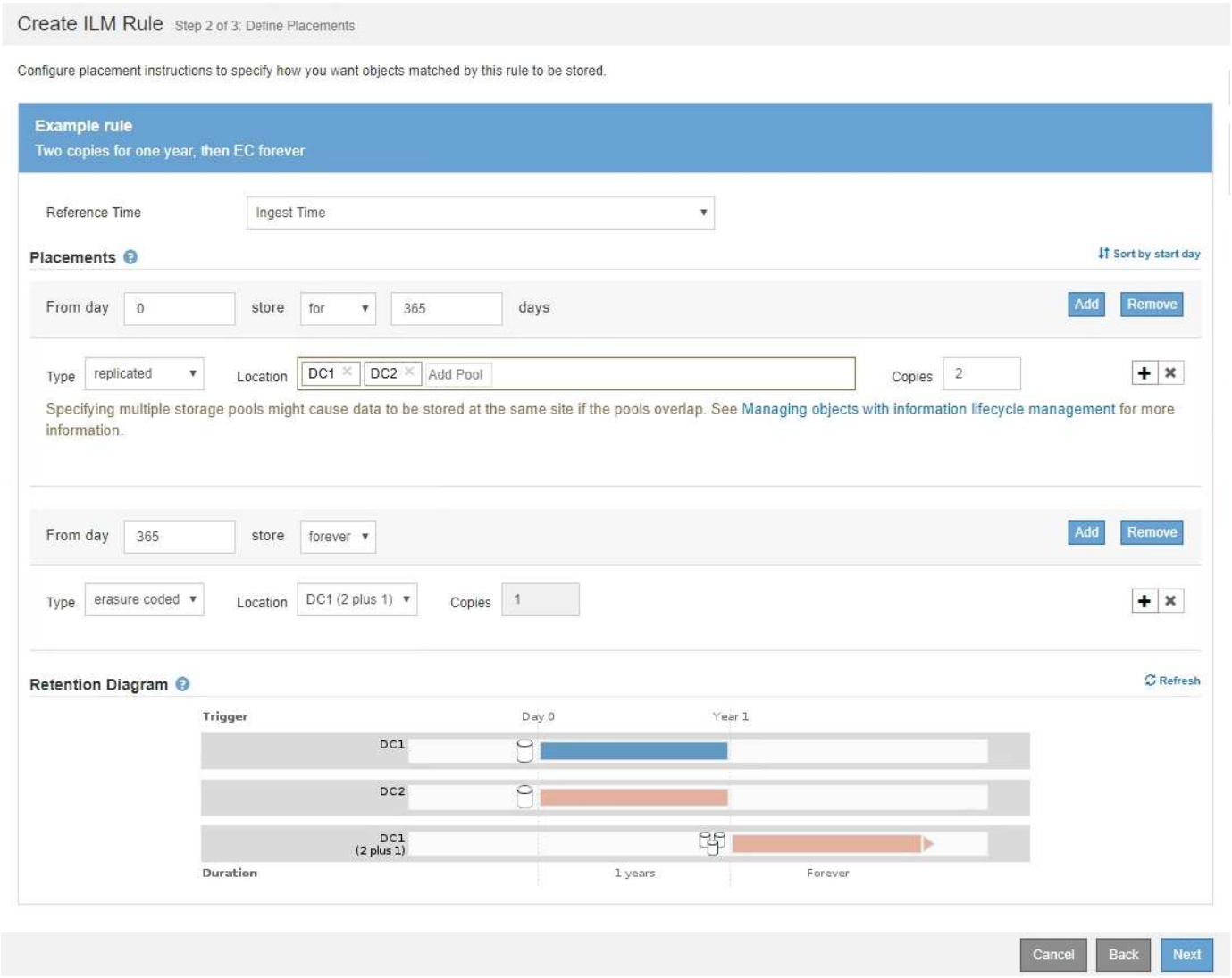
## Create ILM Rule ウィザードのステップ 2 （配置を定義）では、オブジェクトを格納する期間、コピーのタイプ（レプリケートまたはイレイジャーコーディング）、格納場所、およびコピーの数を決定する配置手順を定義できます。

このタスクについて

ILM ルールには 1 つ以上の配置手順を含めることができます。各配置手順環境 は一定期間です。複数の手順を使用する場合は、期間が連続していて、少なくとも 1 つの手順が 0 日目に開始されている必要があります。手順は無期限に、またはオブジェクトコピーが不要になるまで継続できます。

複数のタイプのコピーを作成する場合や、期間中に別々の場所を使用する場合は、各配置手順に複数の行を追加することができます。

この ILM ルールの例では、最初の 1 年間にレプリケートコピーを 2 つ作成します。各コピーは、別々のサイトのストレージプールに保存されます。1 年後、 2+1 のイレイジャーコーディングコピーが作成され、 1 つのサイトにのみ保存されます。




手順

1. [ * 基準時間 * （ * Reference Time * ） ] で、配置手順の開始時間の計算に使用する時間のタイプを選択します。

| オプション | 説明 |
| --- | --- |
| 取り込み時間 | オブジェクトが取り込まれた時間。 |
| 最終アクセス時間 | オブジェクトが最後に読み出された（読み取られた、または表示された）時間。<br><br>• 注：このオプションを使用するには、 S3 バケットまたは Swift コンテナに対する最終アクセス時間の更新が有効になっている必要があります。<br><br>"ILMルールで最終アクセス日時を使用する" |

| オプション | 説明 |
| --- | --- |
| 最新でなくなった時間 | 新しいバージョンが取り込まれて最新バージョンになったことが原因で、あるオブジェクトバージョンが最新でなくなった時間。<br><br>• 注：最新でない時間は、バージョン管理が有効なバケット内の S3 オブジェクトにのみ適用されます。<br><br>このオプションを使用すると、最新でないオブジェクトバージョンをフィルタリングすることで、バージョン管理オブジェクトによるストレージへの影響を軽減できます。「例4：S3バージョン管理オブジェクトのILMルールとポリシー」を参照してください。 |
| ユーザ定義の作成時間 | ユーザ定義のメタデータで指定された時間。 |

準拠ルールを作成する場合は、 * 取り込み時間 * を選択する必要があります。

2. [ 配置（ Plations] ）セクションで、最初の期間の開始時間と期間を選択します。

   たとえば ' 最初の年のオブジェクトを格納する場所を指定することができます ("365 日の場合は 0 日 ")少なくとも 1 つの手順は 0 日目から開始する必要があります。

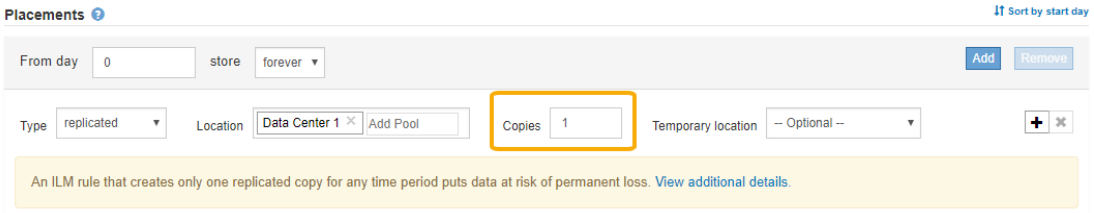
3. レプリケートコピーを作成する場合は、次の手順を実行します。
   a. [* タイプ ] ドロップダウンリストから、 **[*Replicated-]** を選択します。
   b. ［ * 場所 * ］ フィールドで、追加するストレージ・プールごとに ［ * プールの追加 * ］ を選択します。
      - ストレージプールを 1 つしか指定しない場合、 StorageGRID は 1 つのオブジェクトのレプリケートコピーを任意のストレージノードに 1 つだけ格納できます。グリッドにストレージノードが 3 つある場合は、コピー数として 4 を選択すると、各ストレージノードにコピーが 1 つずつ、合計 3 つだけ作成されます。

        ILM placement unAchievable * アラートがトリガーされ、 ILM ルールを完全に適用できなかったことを示します。

      - 複数のストレージプールを指定する場合は、次の点に注意してください。 *
        - コピー数をストレージプール数よりも多くすることはできません。
        - コピーの数がストレージプールの数と同じ場合は、オブジェクトのコピーが 1 つずつ各ストレージプールに格納されます。
        - コピーの数がストレージプールの数より少ない場合、プール間のディスク使用量のバランスを維持し、サイトがオブジェクトのコピーを複数取得しないようにコピーが分散されます。
        - ストレージプールが重複している（同じストレージノードを含んでいる）場合は、オブジェクトのすべてのコピーが 1 つのサイトにのみ保存される可能性があります。そのため、デフォルトの All Storage Nodes ストレージプールと別のストレージプールは指定しないでください。

c. 作成するコピーの数を選択します。

コピー数を 1 に変更すると、警告が表示されます。ある期間にレプリケートコピーを 1 つしか作成しない ILM ルールには、データが永続的に失われるリスクがあります。ある期間にオブジェクトのレプリケートコピーが1つしか存在しない場合、ストレージノードに障害が発生したり、重大なエラーが発生すると、そのオブジェクトは失われます。また、アップグレードなどのメンテナンス作業中は、オブジェクトへのアクセスが一時的に失われます。




これらのリスクを回避するには、次のいずれかの操作を行います。

- 期間のコピー数を増やします。
- プラス記号アイコンをクリックします ➕ 期間中に追加のコピーを作成します。次に、別のストレージプールまたはクラウドストレージプールを選択します。
- 「 * Replicated * 」ではなく、「 * erasure Coded * 」を選択します。このルールですべての期間に対して複数のコピーを作成するようすでに定義されている場合は、この警告を無視してかまいません。

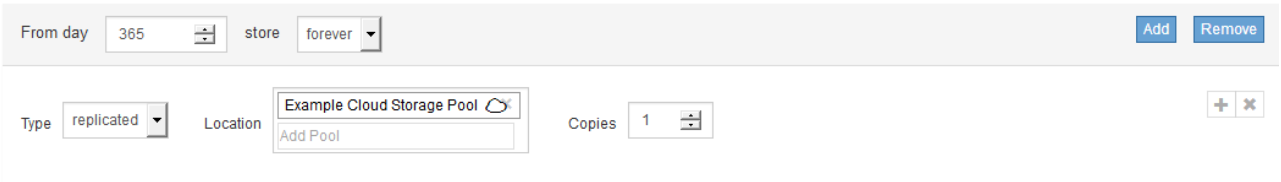
d. ストレージプールを 1 つしか指定していない場合は、「 * 一時的な場所 * 」フィールドは無視してください。

一時的な場所は廃止され、今後のリリースで削除される予定です。

4. オブジェクトをクラウドストレージプールに格納する場合は、次の手順を実行します。

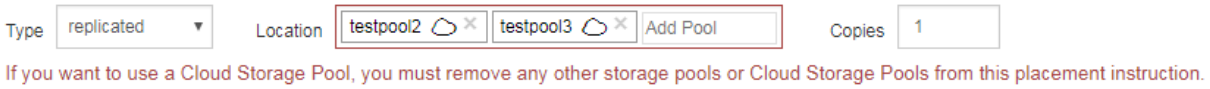
a. [* タイプ ] ドロップダウンリストから、 **[*Replicated-]** を選択します。

b. [ * 場所 * ] フィールドで、 [ * プールの追加 * ] を選択します。次に、クラウドストレージプールを選択します。

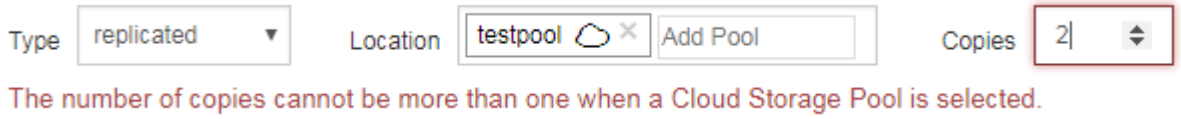



クラウドストレージプールを使用する場合は、次の点に注意してください。

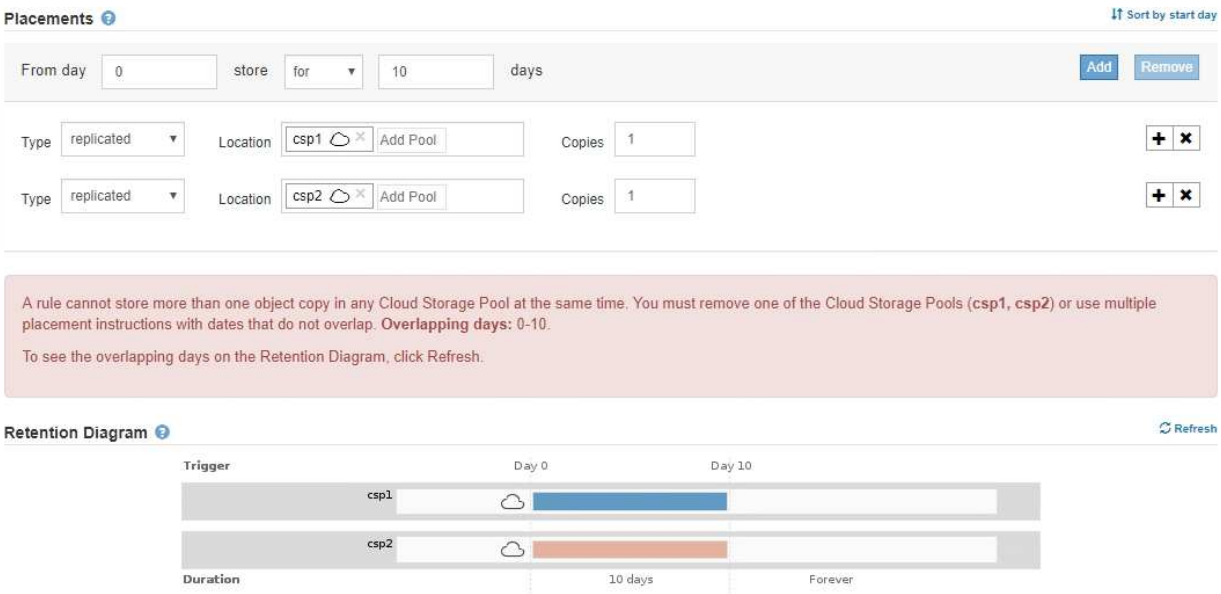
- 1 つの配置手順で複数のクラウドストレージプールを選択することはできません。同様に、クラウドストレージプールとストレージプールを同じ配置手順で選択することはできません。



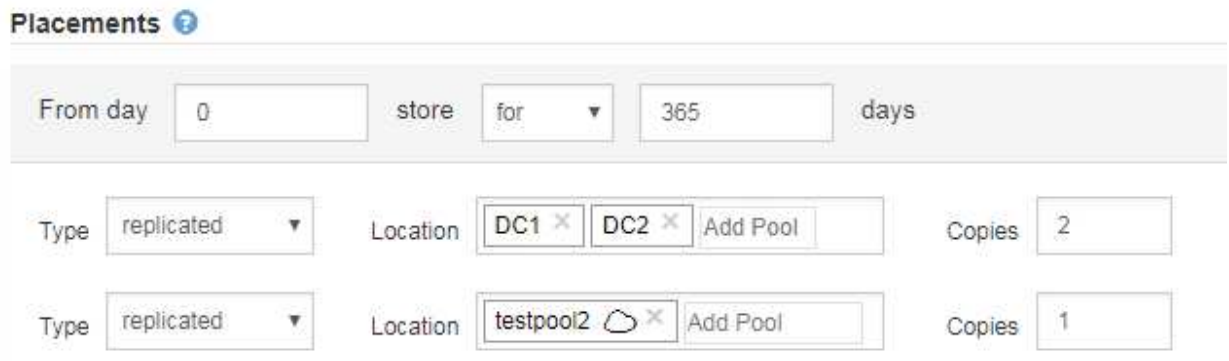

- 任意のクラウドストレージプールに格納できるオブジェクトのコピーは 1 つだけです。「 * Copies * 」を 2 以上に設定すると、エラーメッセージが表示されます。




- どのクラウドストレージプールにも、複数のオブジェクトコピーを同時に格納することはできません。クラウドストレージプールを使用する複数の配置で日付が重複している場合や、同じ配置内の複数の行でクラウドストレージプールを使用している場合は、エラーメッセージが表示されます。




- オブジェクトをレプリケートコピーまたはイレイジャーコーディングコピーとして StorageGRID に格納するときに、オブジェクトをクラウドストレージプールに格納することができます。ただし、この例に示すように、各場所のコピーの数とタイプを指定できるように、配置手順には複数の行を含める必要があります。



5. イレイジャーコーディングコピーを作成する場合は、次の手順を実行します。

   a. [ * タイプ * （ * Type * ） ] ドロップダウンリストから [ * イレイジャーコーディング * （ * erasure Coded * ） ] を選択

      コピーの数が 1 に変わります。200KB 以下のオブジェクトを無視する高度なフィルタがルールに含まれていない場合は警告が表示されます。

      Do not use erasure coding for objects that are 200 KB or smaller. Select **Back** to return to Step 1. Then, use **Advanced filtering** to set the Object Size (MB) filter to "greater than 0.2".

      200KB 未満のオブジェクトにはイレイジャーコーディングを使用しないでください。イレイジャーコーディングされた非常に小さなフラグメントを管理するオーバーヘッドは発生しません。

   b. オブジェクトサイズの警告が表示された場合は、次の手順に従ってクリアします。

      i. 「戻る」を選択して、ステップ1に戻ります。

      ii. 「高度なフィルタリング」を選択します。

      iii. [オブジェクトサイズ(MB)]フィルタを「0.2より大きい」に設定します。

   c. 格納場所を選択します。

      イレイジャーコーディングコピーの格納場所には、ストレージプール名とイレイジャーコーディングプロファイル名が続けて含まれます。

6. 必要に応じて、別の期間を追加するか、別の場所に追加のコピーを作成します。

   ◦ プラスアイコンをクリックして、同じ期間に追加のコピーを別の場所に作成します。

   ◦ 別の期間を配置手順に追加するには、* Add *をクリックします。

      最終期間が * forever * で終わる場合を除き、オブジェクトは最終期間の終了時に自動的に削除されます。

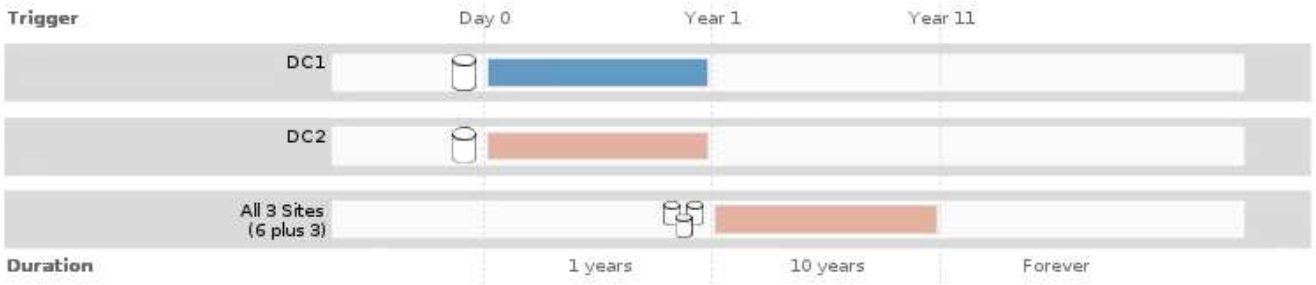
7. [更新]をクリックして保持図を更新し’配置手順を確認します

   図の中の各ラインは、オブジェクトコピーをいつどこに配置するかを示しています。コピーのタイプは次のいずれかのアイコンで表されます。

| | |
|---|---|
| | レプリケートコピー |
| | イレイジャーコーディングコピー |

| | |
|---|---|
| | クラウドストレージプールのコピー |

この例では、 2 つのレプリケートコピーが 2 つのストレージプール（ DC1 と DC2 ）に 1 年間保存されます。その後、 3 つのサイトで 6+3 のイレイジャーコーディングスキームを使用して、イレイジャーコーディングコピーがさらに 10 年間保存されます。11 年後、オブジェクトは StorageGRID から削除されます。




8. 「 * 次へ * 」をクリックします。

ステップ 3 （取り込み動作の定義）が表示されます。

関連情報

"ILM ルールの配置手順とは"

"例 4 ： S3 バージョン管理オブジェクトの ILM ルールとポリシー"

"シングルコピーレプリケーションを使用しない理由"

"S3オブジェクトロックでオブジェクトを管理する"

"一時的な場所としてのストレージプールの使用（廃止）"

"ステップ 3 / 3 ：取り込み動作を定義する"

**ILM**ルールで最終アクセス日時を使用する

最終アクセス時間を ILM ルールの参照時間として使用できます。たとえば、過去 3 カ月間に表示されたオブジェクトをローカルストレージノードに残しておき、最近表示されていないオブジェクトをオフサイトの場所に移動することができます。特定の日付に最後にアクセスされたオブジェクトにのみ ILM ルールを適用する場合は、高度なフィルタとして最終アクセス時間を使用することもできます。

このタスクについて

ILM ルールで最終アクセス日時を使用する前に、次の考慮事項を確認してください。

- 参照時間として最終アクセス時間を使用する場合、オブジェクトの最終アクセス時間を変更しても ILM 評価はすぐには開始されない点に注意してください。オブジェクトの配置が評価され、バックグラウンド ILM がオブジェクトを評価したときに必要に応じてオブジェクトが移動されます。この処理には、オブジェクトがアクセスされてから 2 週間以上かかる場合があります。

  最終アクセス時間に基づいて ILM ルールを作成する際には、このレイテンシを考慮し、短い期間（ 1 カ月

未満）を使用する配置は避けてください。

- 高度なフィルタまたは参照時間として最終アクセス時間を使用する場合は、 S3 バケットに対して最終アクセス時間の更新を有効にしておく必要があります。Tenant Manager またはテナント管理 API を使用できます。

> 最終アクセス時間の更新は Swift コンテナでは常に有効ですが、 S3 バケットではデフォルトで無効になっています。

> 最終アクセス時間の更新を有効にすると、特に小さなオブジェクトを含むシステムのパフォーマンスが低下する可能性があります。これは、オブジェクトが読み出されるたびに StorageGRID が新しいタイムスタンプでオブジェクトを更新する必要があるためです。

次の表に、バケット内のすべてのオブジェクトについて、さまざまなタイプの要求について最終アクセス時間が更新されるかどうかを示します。

| 要求のタイプ | 最終アクセス時間の更新が無効になったときに最終アクセス時間を更新するかどうか | 最終アクセス時間の更新が有効になったときに最終アクセス時間を更新するかどうか |
|---|---|---|
| オブジェクト、そのアクセス制御リスト、またはメタデータの読み出し要求 | いいえ | はい。 |
| オブジェクトメタデータの更新要求 | はい。 | はい。 |
| バケット間でのオブジェクトのコピー要求 | • ソースコピーに対しては、「いいえ」と指定します<br>• デスティネーションコピーについては、はい | • ソースコピーについては、はい<br>• デスティネーションコピーについては、はい |
| マルチパートアップロードの完了要求 | はい、アセンブルされたオブジェクトの場合 | はい、アセンブルされたオブジェクトの場合 |

関連情報

"S3 を使用する"

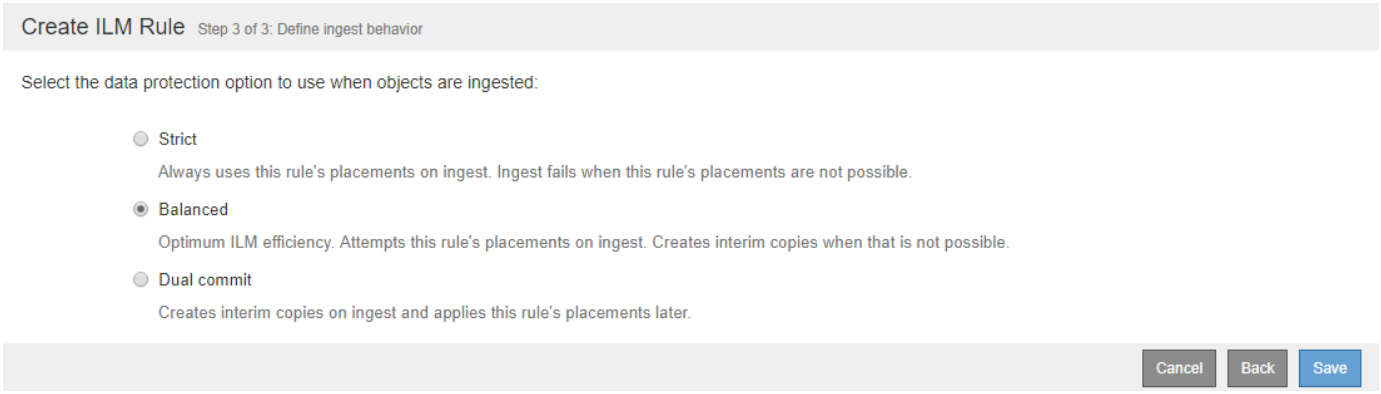
"テナントアカウントを使用する"

ステップ **3 / 3** ：取り込み動作を定義する

## Create ILM Rule ウィザードのステップ 3 （取り込み動作の定義）では、このルールでフィルタリングされたオブジェクトを取り込み時に保護する方法を選択できます。

このタスクについて

StorageGRID は、中間コピーを作成してオブジェクトをキューに登録し、あとで ILM 評価を実行するか、またはコピーを作成してルールの配置手順をすぐに満たすことができます。




手順

1. オブジェクトの取り込み時に使用するデータ保護オプションを選択します。

| オプション | 説明 |
| --- | --- |
| strict | 取り込み時に必ずこのルールの配置手順を使用します。このルールの配置手順が不可能な場合、取り込みは失敗します。 |
| 中間（ Balanced ） | 最適な ILM 効率取り込み時にこのルールの配置手順を試行し、不可能な場合に中間コピーを作成します。 |
| デュアルコミット | 取り込み時に中間コピーを作成し、このルールの配置手順をあとで適用します。 |

「 Balanced 」は、ほとんどの場合に適した データ セキュリティ と効率性を組み合わせたソリューションです。「 Strict 」または「 Dual commit 」は一般に特定の要件を満たすために使用します。

詳細については、「取り込みのデータ保護オプションとは」および「各データ保護オプションの長所と短所」を参照してください。

Strict オプションまたは Balanced オプションを選択してルールで次のいずれかの配置を使用している場合は、エラーメッセージが表示されます。

- クラウドストレージプール： 0 日目
- アーカイブノード： 0 日目
- ルールでユーザ定義の作成時間を参照時間として使用する場合は、クラウドストレージプールまたはアーカイブノード

2. [ 保存（ Save ） ] をクリックします。

ILM ルールが保存されます。ルールは、 ILM ポリシーに追加されてアクティブ化されるまでは有効になりません。

関連情報

"取り込みのデータ保護オプション"

"データ保護オプションのメリット、デメリット、および制限事項"

"例 5 ：取り込み動作が Strict の場合の ILM ルールとポリシー"

"ILMポリシーを作成する"

デフォルトの**ILM**ルールを作成する

# すべてのILMポリシーに、オブジェクトをフィルタリングしないデフォルトルールが設定されている必要があります。ILMポリシーを作成する前に、ポリシーのデフォルトルールとして使用できるILMルールを少なくとも1つ作成する必要があります。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

デフォルトルールは、ILMポリシーで評価される最後のルールであるため、フィルタは使用できません。デフォルトルールの配置手順は、ポリシー内の別のルールに一致しないオブジェクトに適用されます。

次のポリシーの例では、最初のルールがテナント A に属するオブジェクトにのみ適用されますデフォルトルールである最後のルールは、他のすべてのテナントアカウントに属する環境 オブジェクトです。

デフォルトルールを作成するときは、次の要件に注意してください。

- デフォルトのルールは、ポリシーの最後のルールとして自動的に配置されます。
- デフォルトルールでは、基本フィルタまたは詳細フィルタは使用できません。
- デフォルトのルールでレプリケートコピーを作成する必要があります。

> イレイジャーコーディングコピーを作成するルールはポリシーのデフォルトルールとして使用しないでください。イレイジャーコーディングルールでは、高度なフィルタを使用して、小さなオブジェクトがイレイジャーコーディングされないようにします。

- 一般に、デフォルトルールではオブジェクトを無期限に保持する必要があります。
- S3 オブジェクトのグローバルロック設定を使用している（または有効にする）場合は、アクティブポリシーまたはドラフトポリシーのデフォルトルールが準拠している必要があります。

手順

1. [* ILM*>* Rules] を選択します。

   ILM ルールページが表示されます。

2. 「 * Create * 」を選択します。

Create ILM Rule ウィザードの Step 1 （ Define Basics ）が表示されます。

3. [* 名前 *] フィールドに、ルールの一意の名前を入力します。
4. 必要に応じて、ルールの短い概要 を * 概要 * フィールドに入力します。
5. [* Tenant Accounts] フィールドは空白のままにします。

   デフォルトのルールをすべてのテナントアカウントに適用する必要があります。

6. Bucket Name * フィールドは空白のままにします。

   デフォルトルールは、すべての S3 バケットと Swift コンテナに適用する必要があります。

7. 「 * 高度なフィルタリング * 」は選択しないでください

   デフォルトルールでフィルタを指定することはできません。

8. 「 * 次へ * 」を選択します。

   ステップ 2 （配置を定義）が表示されます。

9. デフォルトルールの配置手順を指定します。
   - デフォルトルールではオブジェクトを無期限に保持する必要があります。デフォルトルールによってオブジェクトが無期限に保持されない場合、新しいポリシーをアクティブ化すると警告が表示されます。これが想定どおりの動作であることを確認する必要があります。
   - デフォルトのルールでレプリケートコピーを作成する必要があります。

     イレイジャーコーディングコピーを作成するルールはポリシーのデフォルトルールとして使用しないでください。イレイジャーコーディングルールでは、高度なフィルタ「 * Object Size （ MB ） than 0.2 」を含めて、小さいオブジェクトがイレイジャーコーディングされないようにします。

   - S3 オブジェクトのグローバルロック設定を使用している（または有効にする）場合は、デフォルトルールが準拠している必要があります。
     - 2 つ以上のレプリケートオブジェクトコピーまたは 1 つのイレイジャーコーディングコピーを作成する。
     - これらのコピーが、配置手順の各ラインの間、ストレージノード上に存在している必要があります。
     - オブジェクトコピーをクラウドストレージプールに保存することはできません。
     - オブジェクトコピーをアーカイブノードに保存することはできません。
     - 配置手順の少なくとも 1 行は、参照時間として取り込み時間を使用して 0 日目から開始する必要があります。
     - 配置手順の少なくとも 1 行は「無期限」である必要があります。
10. [更新]をクリックして保持図を更新し’配置手順を確認します
11. 「 * 次へ * 」をクリックします。

    ステップ 3 （取り込み動作の定義）が表示されます。

12. オブジェクトの取り込み時に使用するデータ保護オプションを選択し、 * 保存 * を選択します。

### ILMポリシーを作成する

ILM ポリシーを作成するには、最初に ILM ルールを選択して配置します。次に、以前に取り込まれたオブジェクトに対してドラフトポリシーをシミュレートし、その動作を確認します。ドラフトポリシーが意図したとおりに機能していることを確認したら、そのポリシーをアクティブ化してアクティブポリシーを作成できます。

> ILM ポリシーが正しく設定されていないと、リカバリできないデータ損失が発生する可能性があります。ILM ポリシーをアクティブ化する前に、 ILM ポリシーおよびその ILM ルールを慎重に確認し、次に ILM ポリシーをシミュレートします。ILM ポリシーが意図したとおりに機能することを必ず確認してください。

#### ILM ポリシーの作成に関する考慮事項

- システムに組み込まれているポリシーである Baseline 2 Copies Policy をテストシステムでのみ使用します。このポリシーの Make 2 Copies ルールは、すべてのサイトを含む All Storage Nodes ストレージプールを使用します。StorageGRID システムに複数のサイトがある場合は、 1 つのオブジェクトのコピーが同じサイトに 2 つ配置される可能性があります。
- 新しいポリシーを設計する際には、グリッドに取り込まれる可能性のあるさまざまなタイプのオブジェクトをすべて考慮してください。それらのオブジェクトに一致し、必要に応じて配置するルールがポリシーに含まれていることを確認してください。
- ILM ポリシーはできるだけシンプルにします。これにより、時間が経って StorageGRID システムに変更が加えられ、オブジェクトデータが意図したとおりに保護されないという危険な状況を回避できます。
- ポリシー内のルールの順序が正しいことを確認してください。ポリシーをアクティブ化すると、新規および既存のオブジェクトがリスト内の順にルールによって評価されます。たとえば、ポリシー内の最初のルールがオブジェクトに一致する場合、そのルールは他のルールによって評価されません。
- すべての ILM ポリシーの最後のルールはデフォルトの ILM ルールであり、フィルタを使用することはできません。オブジェクトが別のルールに一致していない場合は、デフォルトルールによって、そのオブジェクトの配置場所と保持期間が制御されます。
- 新しいポリシーをアクティブ化する前に、ポリシーによって既存のオブジェクトの配置が変更されていないかどうかを確認します。既存のオブジェクトの場所を変更すると、新しい配置が評価されて実装される際に一時的なリソースの問題が発生する可能性があります。

関連情報

"ILM ポリシーとは"

"例 6 ： ILM ポリシーを変更する"

#### ドラフトのILMポリシーを作成します

ドラフトの ILM ポリシーを新規に作成できます。同じルールセットを使用する場合は、現在のアクティブポリシーをクローニングして作成できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

- 特定のアクセス権限が必要です。
- ドラフトポリシーに追加するILMルールを作成しておく必要があります。必要に応じて、ドラフトポリシーを保存して追加のルールを作成し、ドラフトポリシーを編集して新しいルールを追加できます。
- フィルタを含まないポリシー用のデフォルトのILMルールを作成しておく必要があります。

  "デフォルトのILMルールを作成する"

このタスクについて

ドラフトの ILM ポリシーを作成する主な理由は次のとおりです。

- 新しいサイトを追加した場合、そのサイトにオブジェクトを配置するために新しい ILM ルールを使用する必要があります。
- サイトの運用を停止しているときは、そのサイトを参照するすべてのルールを削除する必要があります。
- 新しいテナントには特別なデータ保護要件があります。
- クラウドストレージプールの使用を開始した。

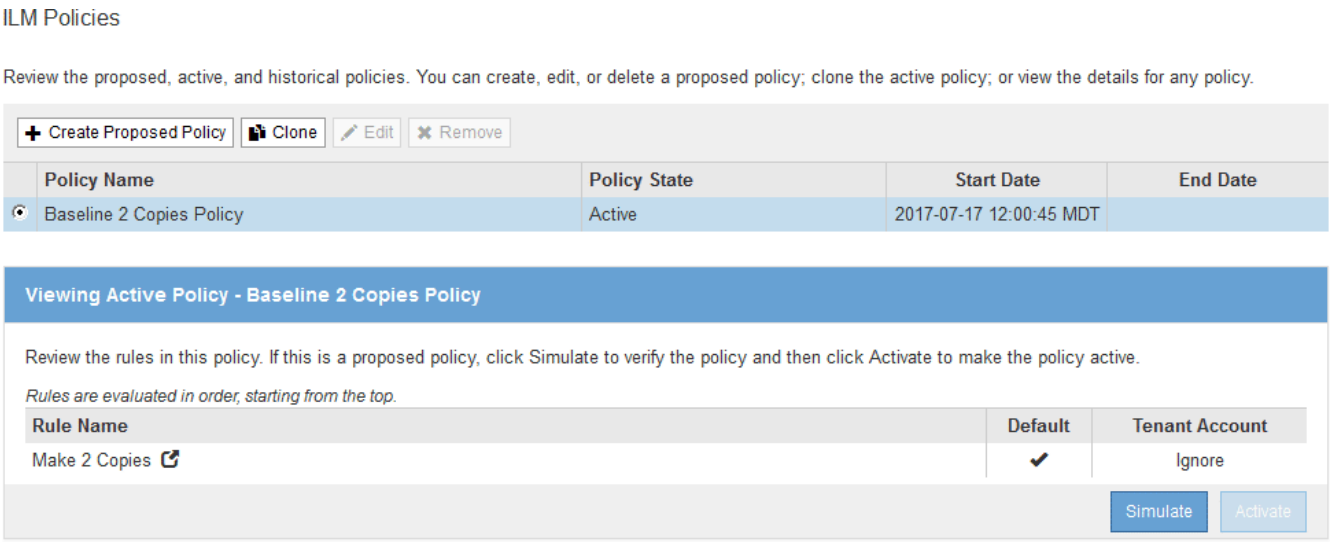
> システムに組み込まれているポリシーである Baseline 2 Copies Policy をテストシステムでのみ使用します。このポリシーの Make 2 Copies ルールは、すべてのサイトを含む All Storage Nodes ストレージプールを使用します。StorageGRID システムに複数のサイトがある場合は、1 つのオブジェクトのコピーが同じサイトに 2 つ配置される可能性があります。

> グローバルなS3オブジェクトのロック設定が有効になっている場合は、ポリシーの作成手順が少し異なります。S3 オブジェクトロックが有効になっているバケットの要件を ILM ポリシーが準拠していることを確認する必要があります。
>
> "S3オブジェクトのロックが有効になったあとのILMポリシーの作成"

手順

1. 「 * ILM * > * Policies * 」を選択します。

   ILM ポリシーページが表示されます。このページでは、ドラフトポリシー、アクティブポリシー、履歴ポリシーのリストを確認し、 または、ドラフトポリシーを削除するか、アクティブポリシーをクローニングするか、すべてのポリシーの詳細を表示します。

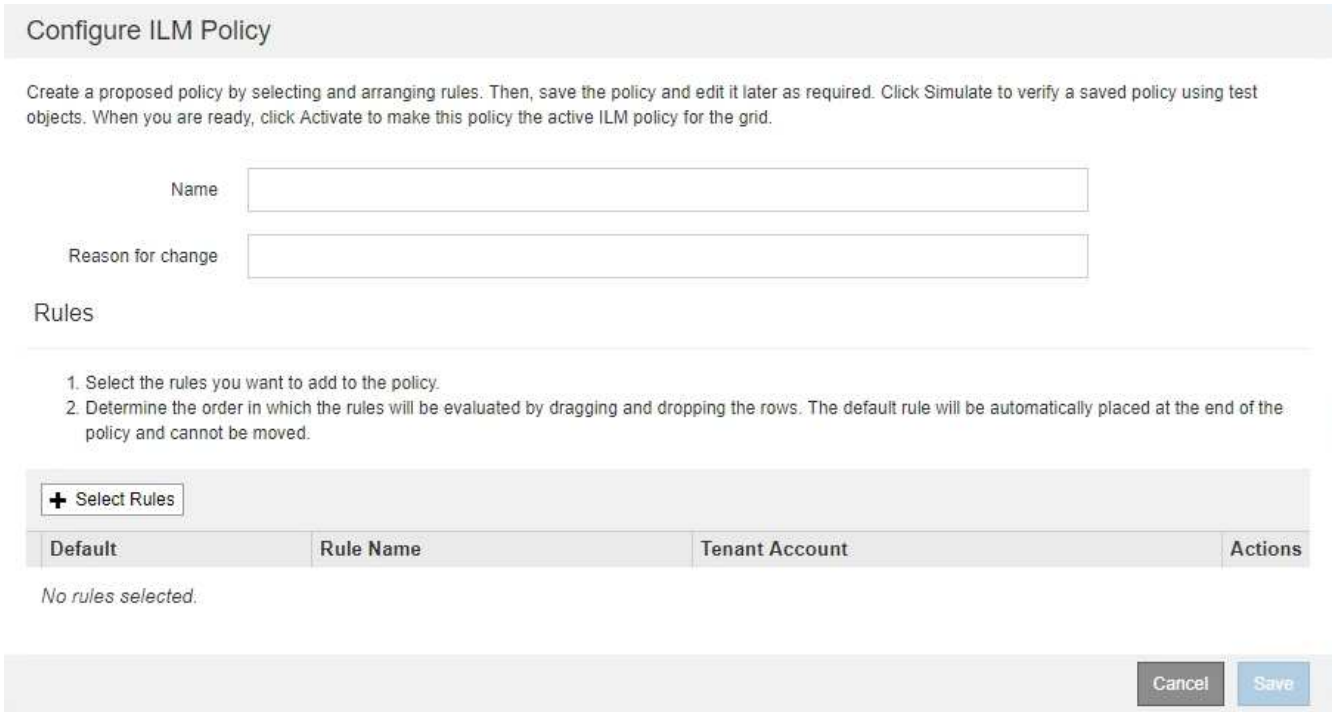



2. ドラフトの ILM ポリシーを作成する方法を決定します。

| オプション | 手順 |
| --- | --- |
| ルールが選択されていない新しいドラフトポリシーを作成します | a. ドラフトのILMポリシーが現在存在する場合は、そのポリシーを選択し、*削除*をクリックします。<br><br>既存のドラフトポリシーがある場合、新しいドラフトポリシーを作成することはできません。<br><br>b. [ドラフトポリシーの作成]をクリックします。 |
| アクティブポリシーに基づいてドラフトポリシーを作成します | a. ドラフトのILMポリシーが現在存在する場合は、そのポリシーを選択し、*削除*をクリックします。<br><br>すでにドラフトポリシーが存在する場合、アクティブポリシーをクローニングすることはできません。<br><br>b. テーブルからアクティブポリシーを選択します。<br>c. [* Clone* ] をクリックします。 |
| 既存のドラフトポリシーを編集します | a. テーブルからドラフトポリシーを選択します。<br>b. [ 編集（ Edit ） ] をクリックします。 |

Configure ILM Policy （ ILM ポリシーの設定）ダイアログボックスが表示されます。

新しいドラフトポリシーを作成する場合は、すべてのフィールドが空白になり、ルールは選択されません。




アクティブなポリシーを複製する場合、 * 名前 * フィールドにはアクティブなポリシーの名前が表示され、バージョン番号（この例では「 v2 」）が付加されます。アクティブポリシーで使用されているルールが選択され、現在の順序で表示されます。

3. [* 名前 *] フィールドに、ドラフトポリシーの一意の名前を入力します。

   1 文字以上 64 文字以下で入力する必要があります。アクティブポリシーをクローニングする場合は、現在の名前にバージョン番号を付加したものを使用することも、新しい名前を入力することもできます。

4. [ 変更理由（ Reason for change ） ] フィールドに、新しいドラフトポリシーを作成する理由を入力します。

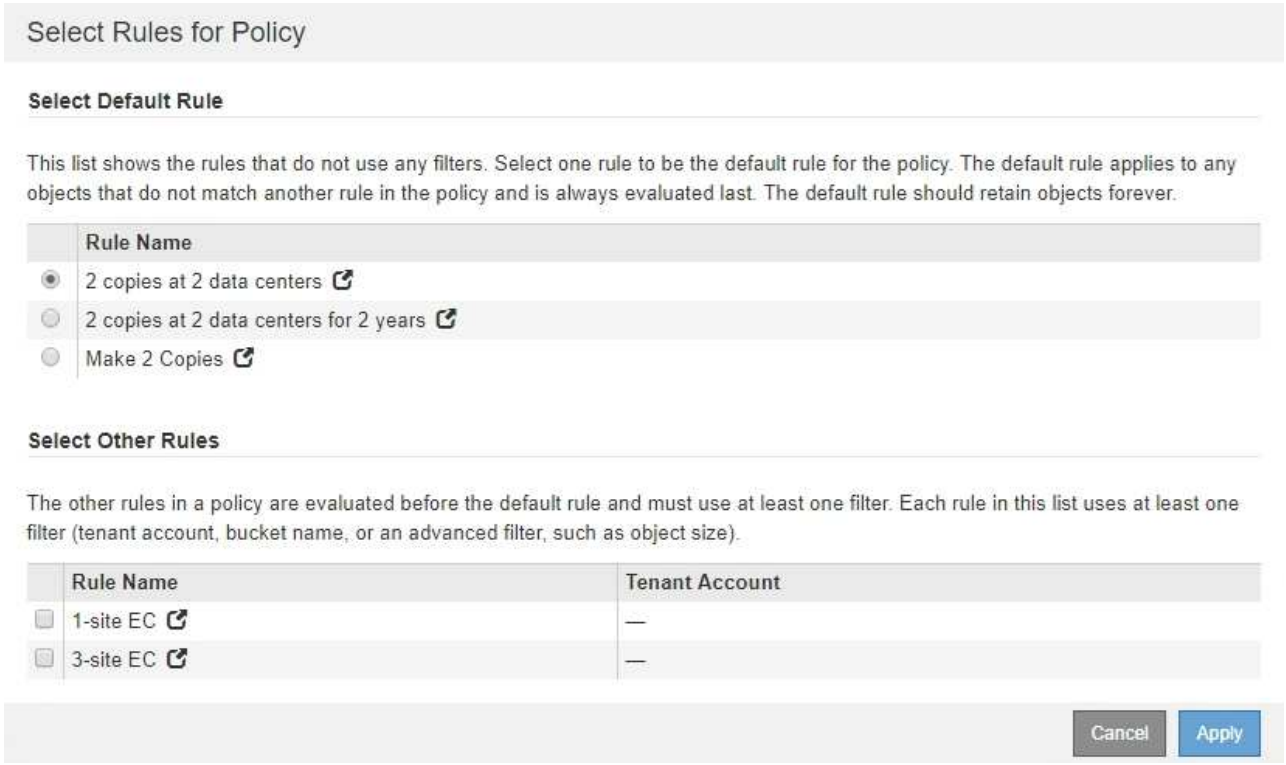
   1 文字以上 128 文字以下で入力する必要があります。

5. ポリシーにルールを追加するには、 * ルールの選択 * を選択します。

   [Select Rules for Policy] ダイアログボックスが表示され、定義済みのすべてのルールが一覧表示されます。ポリシーをクローニングする場合は、次の手順を実行します。

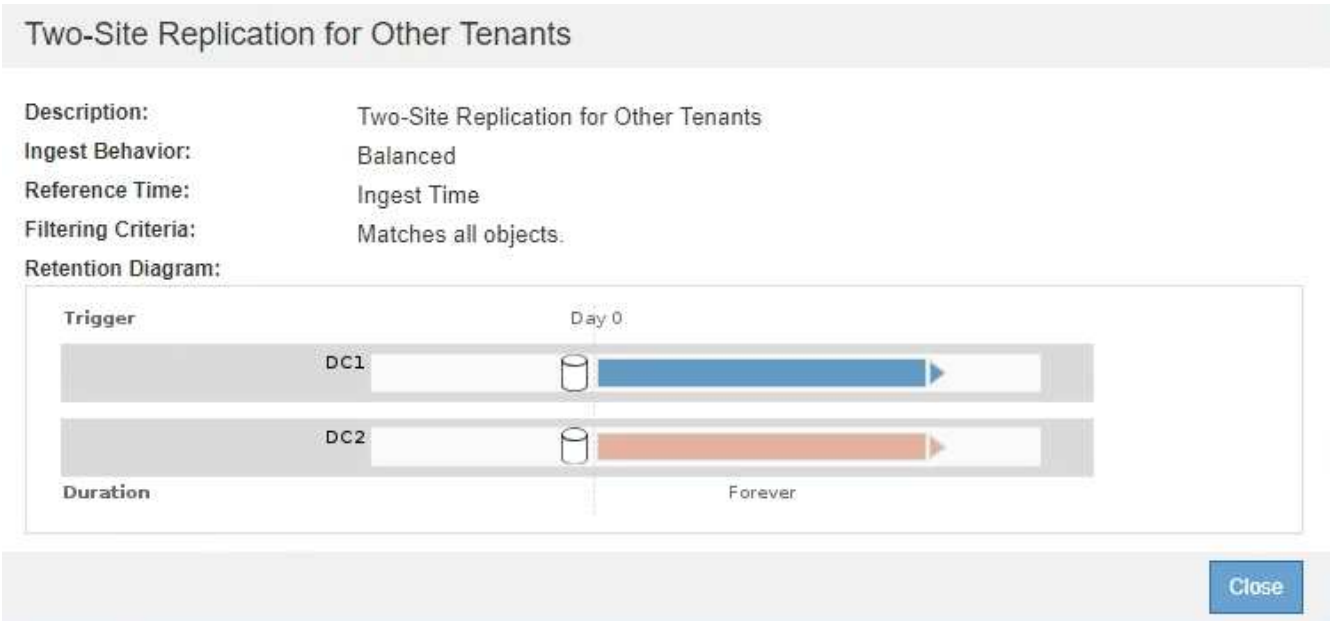
   - クローニングするポリシーで使用されているルールが選択されます。
   - クローニングするポリシーで、デフォルトルールではないフィルタを使用していないルールが使用されている場合は、それらのルールを 1 つだけ残して、それを除くすべてのルールを削除するように求められます。
   - デフォルトルールでフィルタを使用している場合は、新しいデフォルトルールを選択するように求められます。

◦ デフォルトルールが最後のルールではない場合は、ボタンを使用して新しいポリシーの末尾にルールを移動できま
す。




6. ルール名または詳細アイコンを選択します をクリックすると、そのルールの設定が表示されます。

この例は、 2 つのレプリケートコピーを 2 つのサイトに作成する ILM ルールの詳細を示しています。




7. [ デフォルトルールを選択（ * Select Default Rule ） ] セクションで、ドラフトポリシーにデフォルトルールを 1 つ選択します。

デフォルトルールは、ポリシー内の別のルールに一致しないオブジェクトの環境 を作成します。デフォルトルールではフィルタを使用できず、常に最後に評価されます。

ルールが[Select Default Rule]セクションに表示されない場合は、ILMポリシーページを終了してデフォルトルールを作成する必要があります。

"デフォルトのILMルールを作成する"

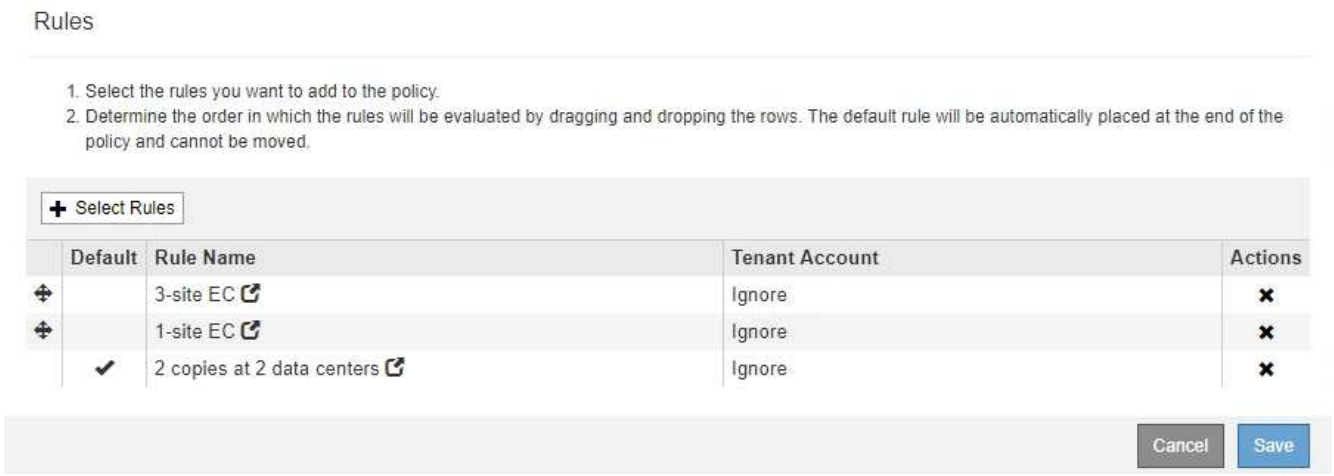
Make 2 Copies ルールをポリシーのデフォルトルールとして使用しないでください。Make 2 Copies ルールは、 1 つのストレージプールであるすべてのストレージノードを使用します。このプールにはすべてのサイトが含まれています。StorageGRID システムに複数のサイトがある場合は、 1 つのオブジェクトのコピーが同じサイトに 2 つ配置される可能性があります。

8. [ その他のルールを選択してください ] セクションで、ポリシーに含める他のルールを選択します。

   他のルールはデフォルトルールの前に評価され、少なくとも1つのフィルタ（テナントアカウント、バケット名、オブジェクトサイズなどの高度なフィルタ）を使用する必要があります。

9. ルールの選択が完了したら、 * 適用 * を選択します。

   選択したルールが表示されます。デフォルトのルールは末尾にあり、その上に他のルールがあります。




デフォルトルールによってオブジェクトが無期限に保持されない場合は、警告が表示されます。このポリシーをアクティブ化するときは、デフォルトルールの配置手順を経過したとき（バケットライフサイクルによってオブジェクトが長期間保持されないかぎり）に StorageGRID がオブジェクトを削除することを確認する必要があります。

10. デフォルト以外のルールの行をドラッグアンドドロップして、ルールが評価される順序を決定します。

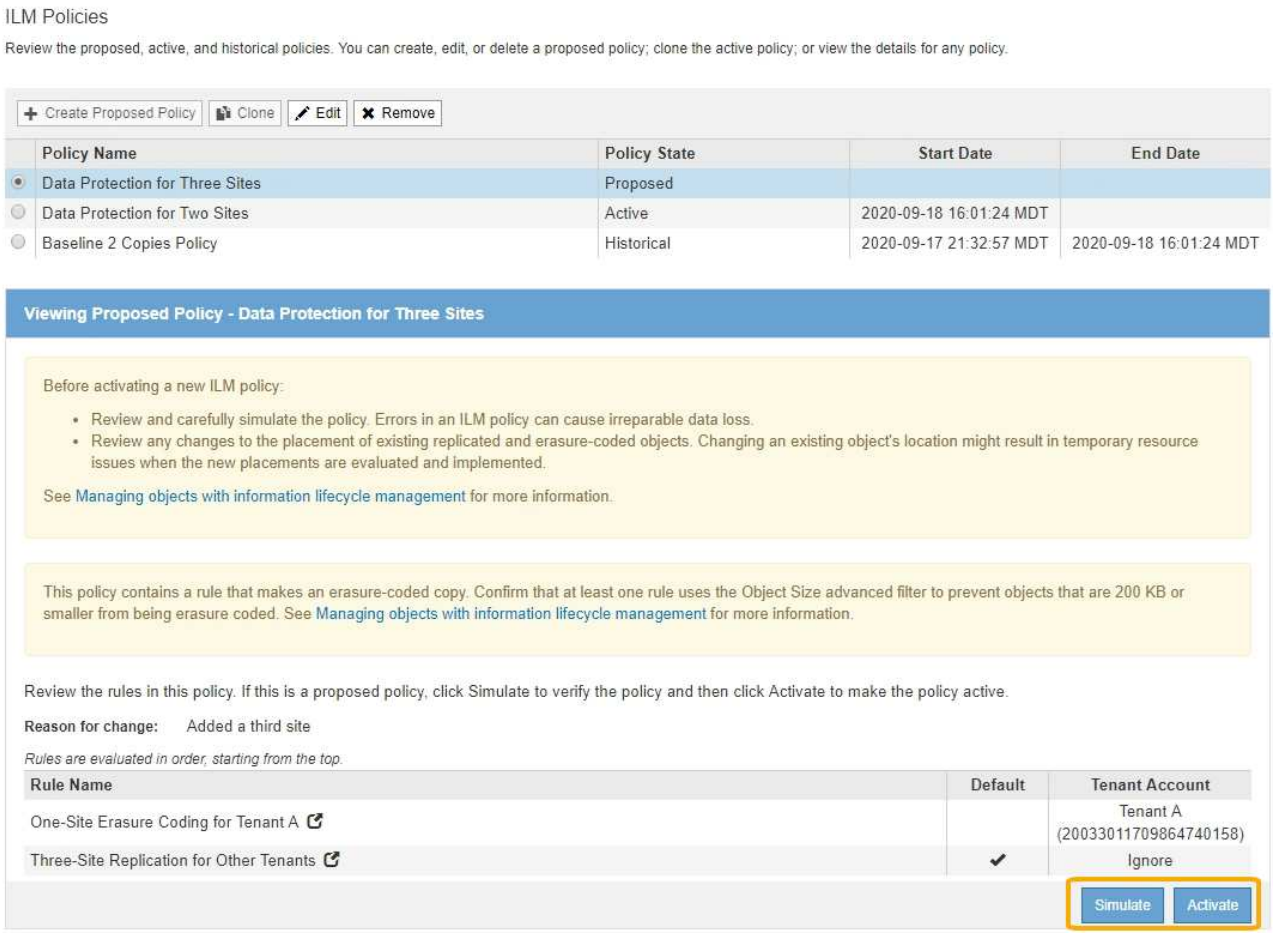
    デフォルトのルールは移動できません。

ILM ルールの順序が正しいことを確認してください。ポリシーをアクティブ化すると、新規および既存のオブジェクトがリスト内の順にルールによって評価されます。

11. 必要に応じて、削除アイコンをクリックします ✖ ポリシーに不要なルールを削除するには、 [ ルールの選択 ] を選択してルールを追加します。
12. 完了したら、 * 保存 * を選択します。

    ILM ポリシーページが更新されます。

    - 保存したポリシーがドラフトとして表示されます。ドラフトポリシーには開始日と終了日がありません。
    - [ シミュレート（ Simulate ） ] および [ 活動化（ Activate ） ] * ボタンが有効になります。




13. に進みます "ILMポリシーをシミュレートする"。

関連情報

"ILM ポリシーとは"

"S3オブジェクトロックでオブジェクトを管理する"

**S3**オブジェクトのロックが有効になったあとの**ILM**ポリシーの作成

グローバルな S3 オブジェクトのロック設定が有効になっている場合は、ポリシーの作成手順が少し異なります。S3 オブジェクトロックが有効になっているバケットの要件を

# ILM ポリシーが準拠していることを確認する必要があります。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- StorageGRID システムでグローバルなS3オブジェクトロック設定が有効になっている必要があります。

> グローバルなS3オブジェクトのロック設定が有効になっていない場合は、代わりにドラフトポリシーの作成手順を使用してください。
>
> "ドラフトのILMポリシーを作成します"

- ドラフトポリシーに追加する準拠ILMルールと非準拠ILMルールを作成しておく必要があります。必要に応じて、ドラフトポリシーを保存して追加のルールを作成し、ドラフトポリシーを編集して新しいルールを追加できます。

  "例 7 ： S3 オブジェクトロックの準拠 ILM ポリシー"

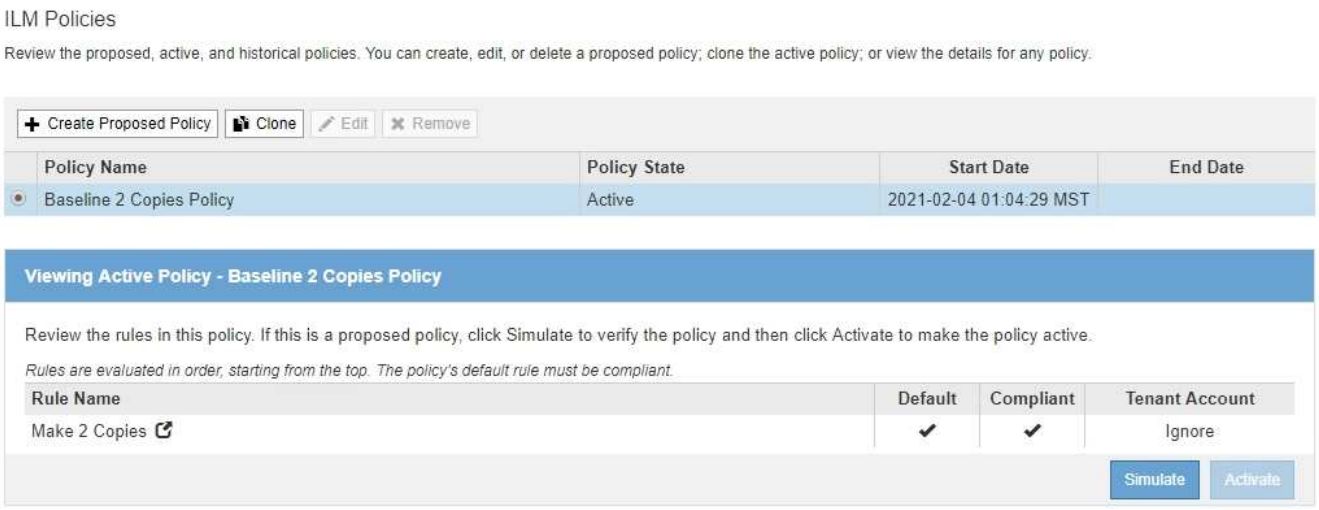
- ポリシーの準拠デフォルトのILMルールを作成しておく必要があります。

  "デフォルトのILMルールを作成する"

手順

1. 「 * ILM * > * Policies * 」を選択します。

   ILM ポリシーページが表示されます。グローバルな S3 オブジェクトのロック設定が有効になっている場合は、 ILM ポリシーページに準拠している ILM ルールが表示されます。




2. [* 名前 *] フィールドに、ドラフトポリシーの一意の名前を入力します。

   1 文字以上 64 文字以下で入力する必要があります。

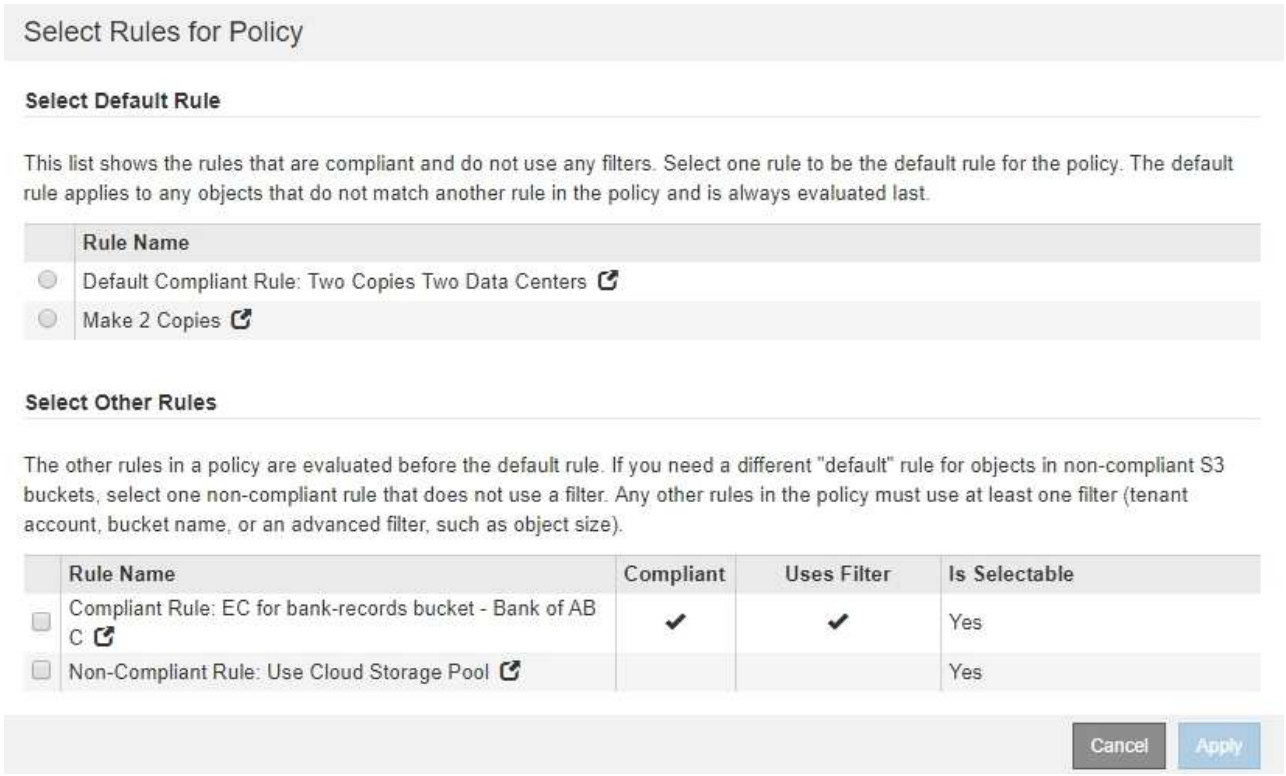
3. [ 変更理由（ Reason for change ） ] フィールドに、新しいドラフトポリシーを作成する理由を入力します。

1 文字以上 128 文字以下で入力する必要があります。

4. ポリシーにルールを追加するには、 * ルールの選択 * を選択します。

   [Select Rules for Policy] ダイアログボックスが表示され、定義済みのすべてのルールが一覧表示されます。

   - ［ デフォルトルールの選択 ］ セクションには、準拠ポリシーのデフォルトになるルールがリストされます。フィルタを使用しない準拠ルールが含まれています。
   - [ その他のルールの選択 ] セクションには、このポリシーに選択できる他の準拠ルールと非準拠ルールが一覧表示されま
     す。




5. ルール名または詳細アイコンを選択します をクリックすると、そのルールの設定が表示されます。
6. [ デフォルトルールを選択（ * Select Default Rule ） ] セクションで、ドラフトポリシーにデフォルトルールを 1 つ選択します。

   このセクションの表には、準拠ルールのみが表示され、フィルタは使用されません。

   ルールが[Select Default Rule]セクションに表示されない場合は、ILMポリシーページを終了して、準拠するデフォルトルールを作成する必要があります。

   "デフォルトのILMルールを作成する"

   Make 2 Copies ルールをポリシーのデフォルトルールとして使用しないでください。Make 2 Copies ルールは、 1 つのストレージプールであるすべてのストレージノードを使用します。このプールにはすべてのサイトが含まれています。このルールを使用すると、 1 つのオブジェクトの複数のコピーが同じサイトに配置される場合があります。

7. [ その他のルールを選択してください ] セクションで、ポリシーに含める他のルールを選択します。

a. 非準拠 S3 バケット内のオブジェクトに別の「デフォルト」ルールが必要な場合は、必要に応じて、フィルタを使用しない非準拠ルールを 1 つ選択します。

   たとえば、クラウドストレージプールやアーカイブノードを使用して、 S3 オブジェクトロックが有効になっていないバケットにオブジェクトを格納できます。

   フィルタを使用しない非準拠ルールは 1 つだけ選択できます。1 つのルールを選択すると、 [ 選択可能 ] 列には、フィルタのない他の非準拠ルールについては [ * いいえ ] と表示されます。

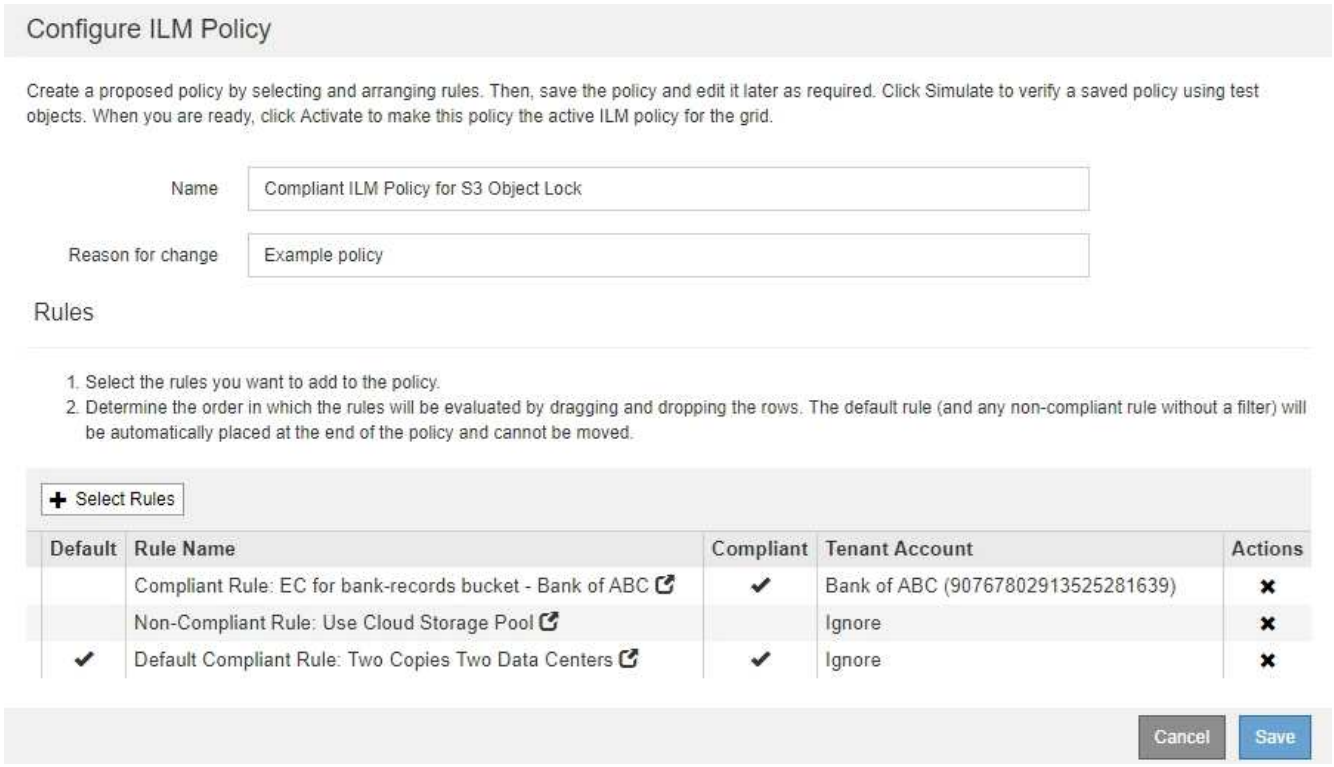
a. ポリシーで使用する他の準拠ルールと非準拠ルールを選択します。

   他のルールでは、少なくとも 1 つのフィルタ（テナントアカウント、バケット名、オブジェクトサイズなどの高度なフィルタ）を使用する必要があります。

8. ルールの選択が完了したら、 * 適用 * を選択します。

   選択したルールが表示されます。デフォルトのルールは末尾にあり、その上に他のルールがあります。非準拠の「デフォルト」ルールも選択した場合、そのルールはポリシーの 2 番目から最後までのルールとして追加されます。

   この例では、最後のルール「 2 Copies 2 Data Center 」がデフォルトルールで、準拠ルールでフィルタがありません。2 番目から最後までのルールである Cloud Storage Pool にもフィルタはありませんが、準拠していません。




。

9. デフォルト以外のルールの行をドラッグアンドドロップして、ルールが評価される順序を決定します。

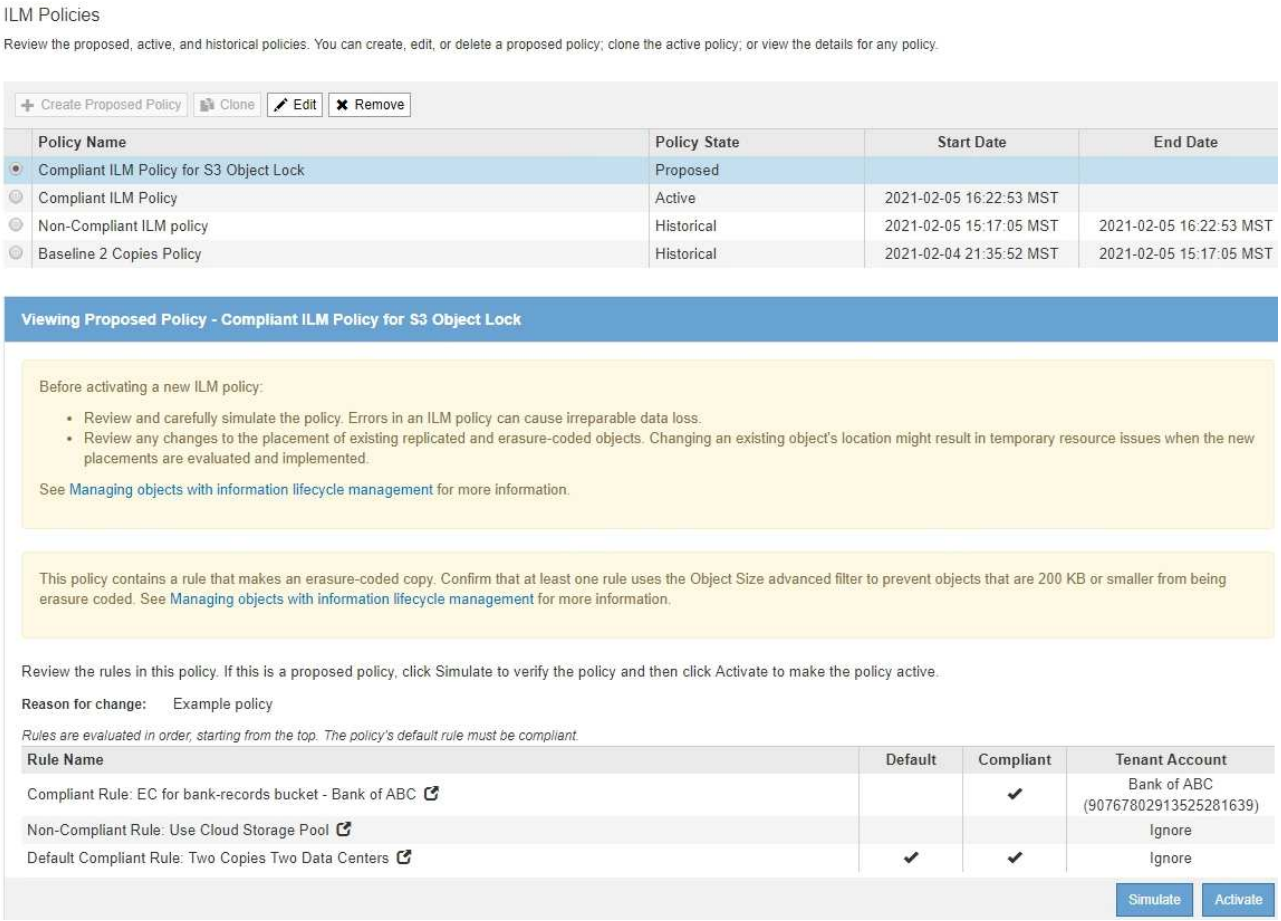
   デフォルトのルールまたは非準拠の「デフォルト」ルールは移動できません。

ILM ルールの順序が正しいことを確認してください。ポリシーをアクティブ化すると、新規および既存のオブジェクトがリスト内の順にルールによって評価されます。

10. 必要に応じて、削除アイコンをクリックします ポリシーに不要なルールを削除するには、 [ ルールの選択 ] を選択してルールを追加します。
11. 完了したら、 * 保存 * を選択します。

    ILM ポリシーページが更新されます。

    - 保存したポリシーがドラフトとして表示されます。ドラフトポリシーには開始日と終了日がありません。
    - [ シミュレート（ Simulate ） ] および [ 活動化（ Activate ） ] * ボタンが有効になります。




12. に進みます "ILMポリシーをシミュレートする"。

**ILM**ポリシーをシミュレートする

ポリシーをアクティブ化して本番環境のデータに適用する前に、テストオブジェクトでドラフトポリシーをシミュレートする必要があります。シミュレーション期間は、アクティブ化して本番環境のデータに適用する前にポリシーを安全にテストするための、スタンドアロン環境を提供します。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- テストする各オブジェクトのS3バケット/オブジェクトキーまたはSwiftコンテナ/オブジェクト名を確認しておく必要があります。また、それらのオブジェクトを取り込んでおく必要があります。

このタスクについて

ドラフトポリシーをテストするオブジェクトは慎重に選択する必要があります。ポリシーを確実にシミュレートするには、各ルールのフィルタごとに少なくとも 1 つのオブジェクトをテストする必要があります。

たとえば、バケット A のオブジェクトに一致するルールとバケット B のオブジェクトに一致するルールを含むポリシーを確実にテストするためには、少なくともバケット A から 1 つとバケット B から 1 つオブジェクトを選択する必要があります。ポリシーに他のすべてのオブジェクトを配置するデフォルトルールが含まれている場合は、別のバケットのオブジェクトを少なくとも1つテストする必要があります。

ポリシーをシミュレートする場合は、次の点を考慮します。

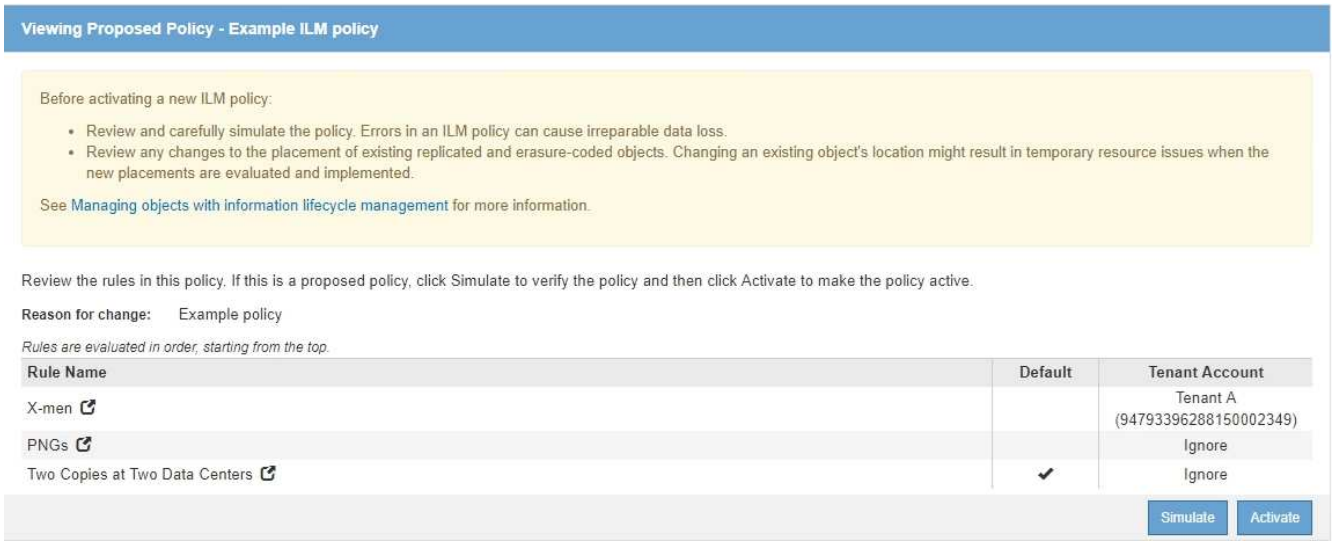
- ポリシーを変更したら、ドラフトポリシーを保存します。次に、保存したドラフトポリシーの動作をシミュレートします。
- ポリシーをシミュレートするとポリシー内の ILM ルールがテストオブジェクトをフィルタリングするため、各オブジェクトにどのルールが適用されたかを確認できます。ただし、オブジェクトのコピーは作成されず、配置もされません。シミュレーションを実行しても、データ、ルール、ポリシーはいっさい変更されません。
- シミュレーションページでは、 ILM ポリシーページを閉じるか別のページに移動するか更新するまで、テストしたオブジェクトが保持されます。
- シミュレーションは、一致したルールの名前を返します。どのストレージプールまたはイレイジャーコーディングプロファイルが有効かを確認するには、ルール名または詳細アイコンをクリックして保持図を表示します。
- S3 のバージョン管理が有効な場合、ポリシーはオブジェクトの現在のバージョンに対してのみシミュレートされます。

手順

1. ルールを選択して配置し、ドラフトポリシーを保存します。

   この例のポリシーには 3 つのルールがあります。

| ルール名 | フィルタ | コピーのタイプ | 保持 |
| --- | --- | --- | --- |
| 男性用 | • テナント A<br>• ユーザメタデータ（シリーズ = x-men ） | 2 つのデータセンターに 2 つのコピーを保持 | 2 年 |
| PNGs | キーの末尾は .png です | 2 つのデータセンターに 2 つのコピーを保持 | 5 年 |
| 2 つのコピーで 2 つのデータセンターを構成し | _ なし _ | 2 つのデータセンターに 2 つのコピーを保持 | 永遠に |

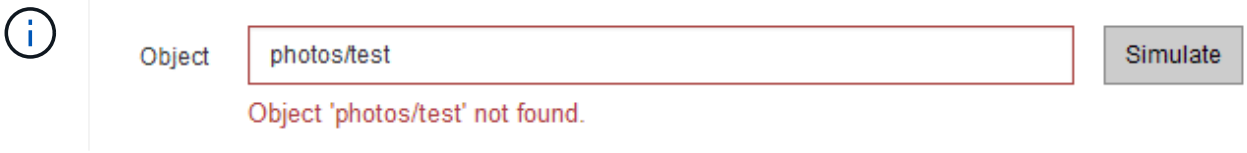



2. * Simulate *をクリックします。

   Simulation ILM Policy （シミュレーション ILM ポリシー）ダイアログボックスが表示されます。

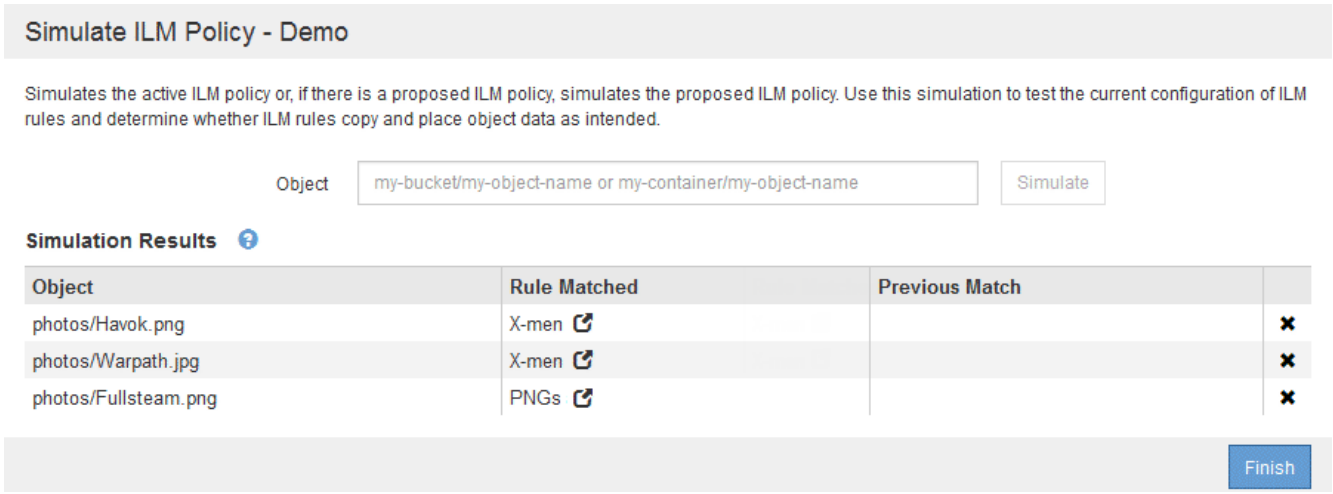
3. * Object フィールドに、テストオブジェクトの**S3**バケット/オブジェクトキーまたは**Swift**コンテナ/オブジェクト名を入力し、 Simulate *をクリックします。

   取り込まれていないオブジェクトを指定するとメッセージが表示されます。




4. [ * シミュレーション結果 * （ Simulation Results ） ] で、各オブジェクトが正しいルールに一致していることを確認します。

   この例では、を使用しています `Havok.png` および `Warpath.jpg` オブジェクトが「X-men」ルールに正しく一致しました。。 `Fullsteam.png` オブジェクト。には含まれません `series=x-men` ユーザメタデータは「X-men」ルールには一致しませんでしたが、「PNGs」ルールに正しく一致しました。3 つのオブジェクトがすべて他のルールに一致したため、デフォルトルールは使用されませんでした。



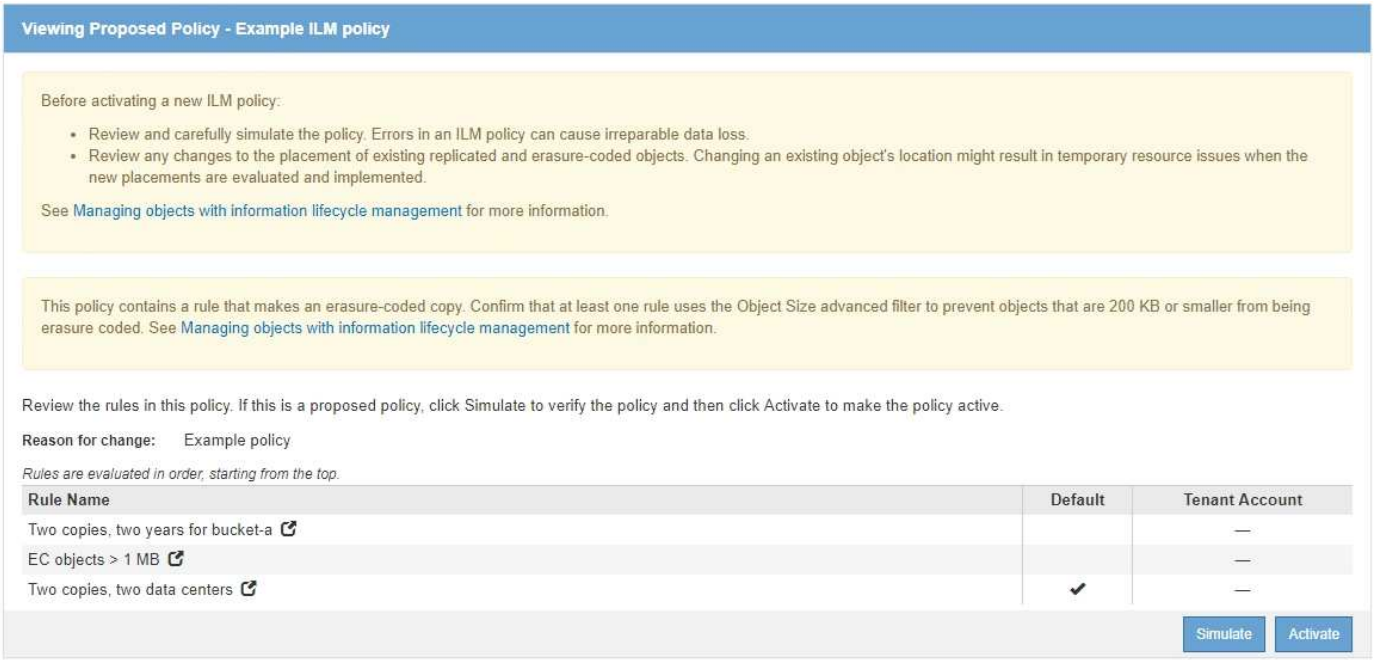
# 以下の例は、ILMポリシーをアクティブ化する前にシミュレートして、ILMルールを確認する方法を示しています。

## 例**1**：ドラフトの**ILM**ポリシーをシミュレートしてルールを確認する

この例は、ドラフトポリシーをシミュレートしてルールを確認する方法を示しています。

この例では、 2 つのバケットに取り込まれたオブジェクトに対して * サンプルの ILM ポリシー * をシミュレートします。このポリシーには、次の 3 つのルールが含まれています。

- 最初のルール「 * 2 copies 、 buckets-a * 」の 2 年間は、 bucket-a のオブジェクトにのみ適用されます
- 2番目のルールのメニュー：ECオブジェクト[1MB ]、環境 Allバケット。ただし1MBを超えるオブジェクトでフィルタリングします。
- 3番目のルールはデフォルトルールであり、フィルタは含まれません。



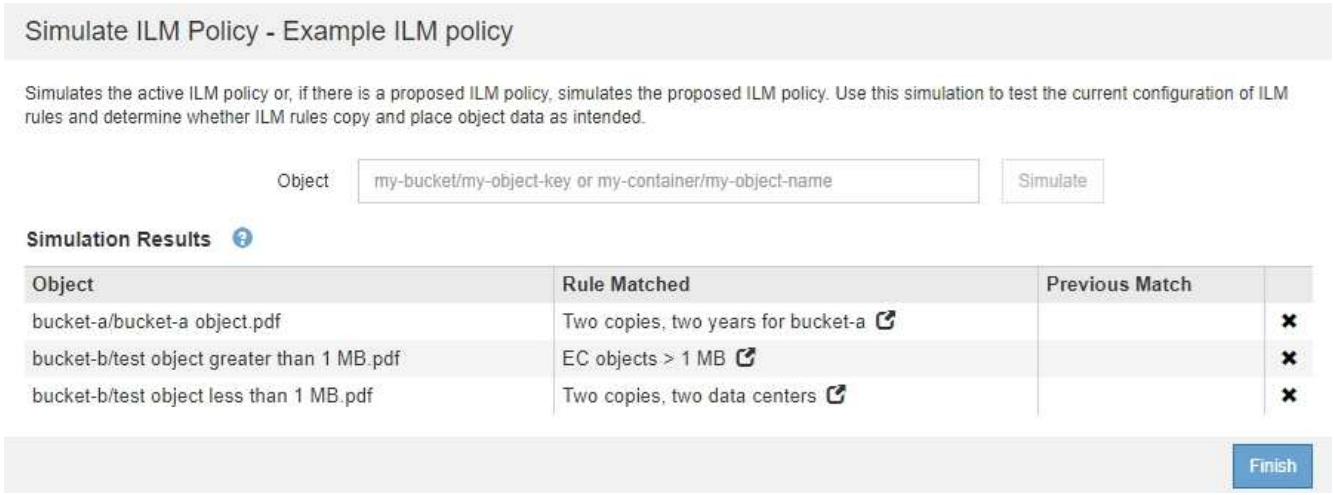

手順

1. ルールを追加してポリシーを保存したら、* Simulate *をクリックします。

   Simulate ILM Policy ダイアログボックスが表示されます。

2. * Object フィールドに、テストオブジェクトの**S3**バケット/オブジェクトキーまたは**Swift**コンテナ/オブジェクト名を入力し、 Simulate *をクリックします。

   シミュレーション結果が表示され、ポリシー内のどのルールがテストした各オブジェクトに一致したかが示されます。




3. 各オブジェクトが正しいルールに一致したことを確認します。

   次の例では、

   a. `bucket-a/bucket-a object.pdf` のオブジェクトをフィルタリングする最初のルールを正しくマッチングしました `bucket-a`。

   b. `bucket-b/test object greater than 1 MB.pdf` がにあります `bucket-b`では、最初のルールと一致しませんでした。代わりに、 1MB を超えるオブジェクトをフィルタリングする 2 つ目のルールに正しく一致しました。

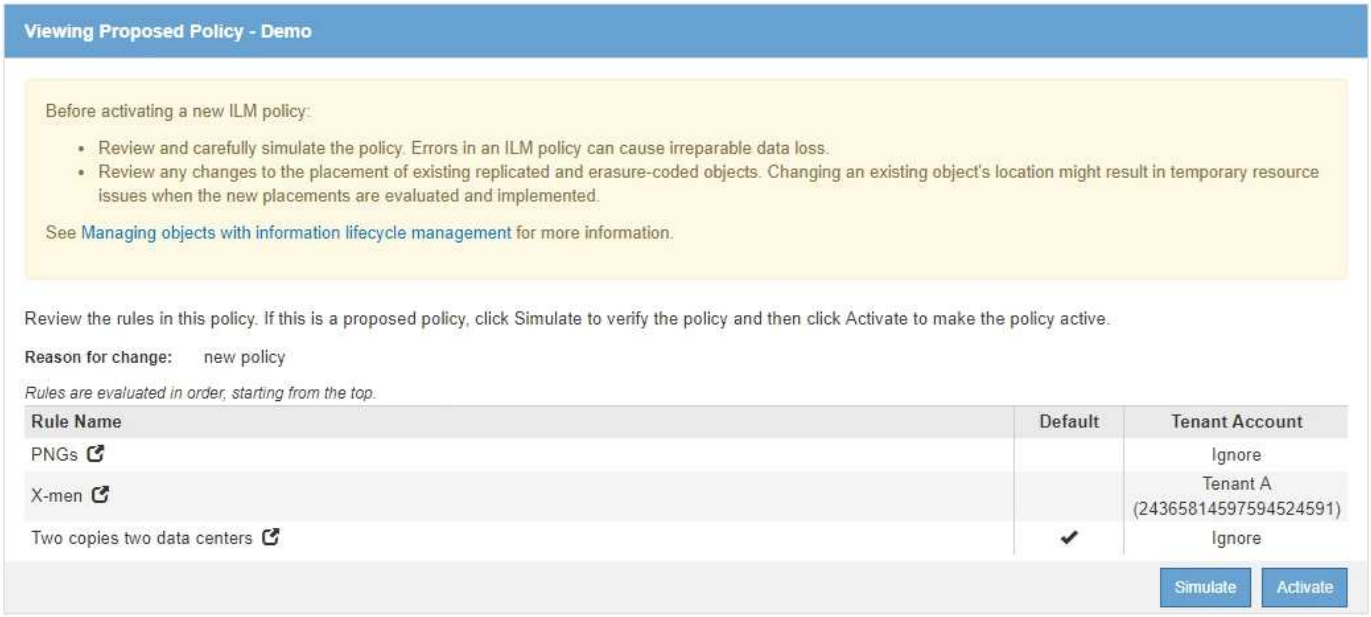
   c. `bucket-b/test object less than 1 MB.pdf` 最初の2つのルールのフィルタに一致しなかったため、フィルタが含まれていないデフォルトルールによって配置されます。

例 **2** ：ドラフトの **ILM** ポリシーをシミュレートする際にルールの順序を変更する

この例では、ポリシーをシミュレートする際に、ルールの順序を変更して結果を変更する方法を示します。

この例では、 * Demo * ポリシーをシミュレートします。このポリシーの目的は次の 3 つのルールで、 series = x -men ユーザメタデータを含むオブジェクトを検索することです。

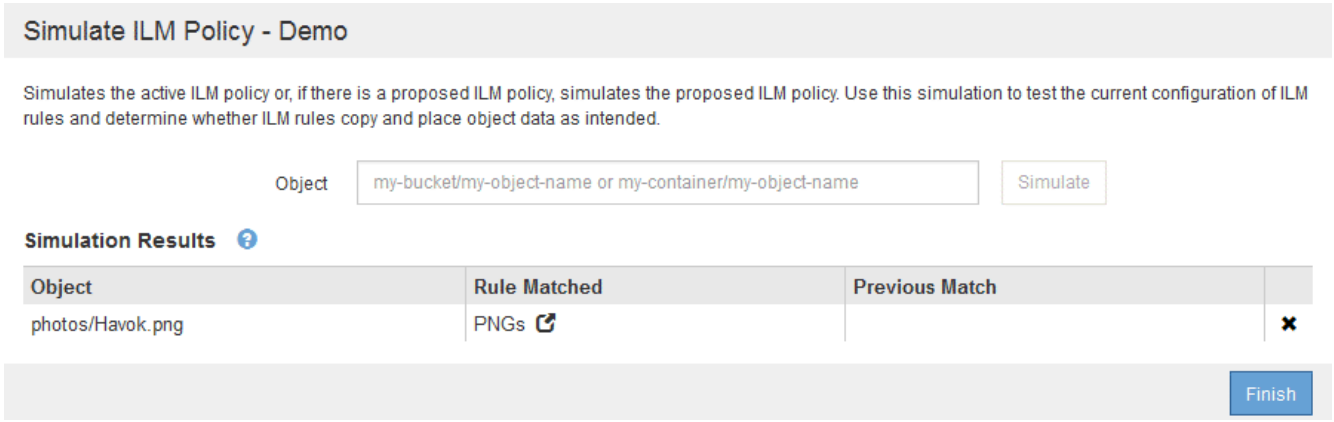
- 最初のルール「* PNGs *」はで終わるキー名に対してフィルタを適用します `.png`。
- 2つ目のルール「* X-men」はテナントAのオブジェクトにのみ適用され、フィルタを適用します `series=x-men` ユーザメタデータ。
- 最後のルール「 * 2 Copies 2 data centers * 」はデフォルトルールで、最初の 2 つのルールに一致しないオブジェクトに一致します。




手順

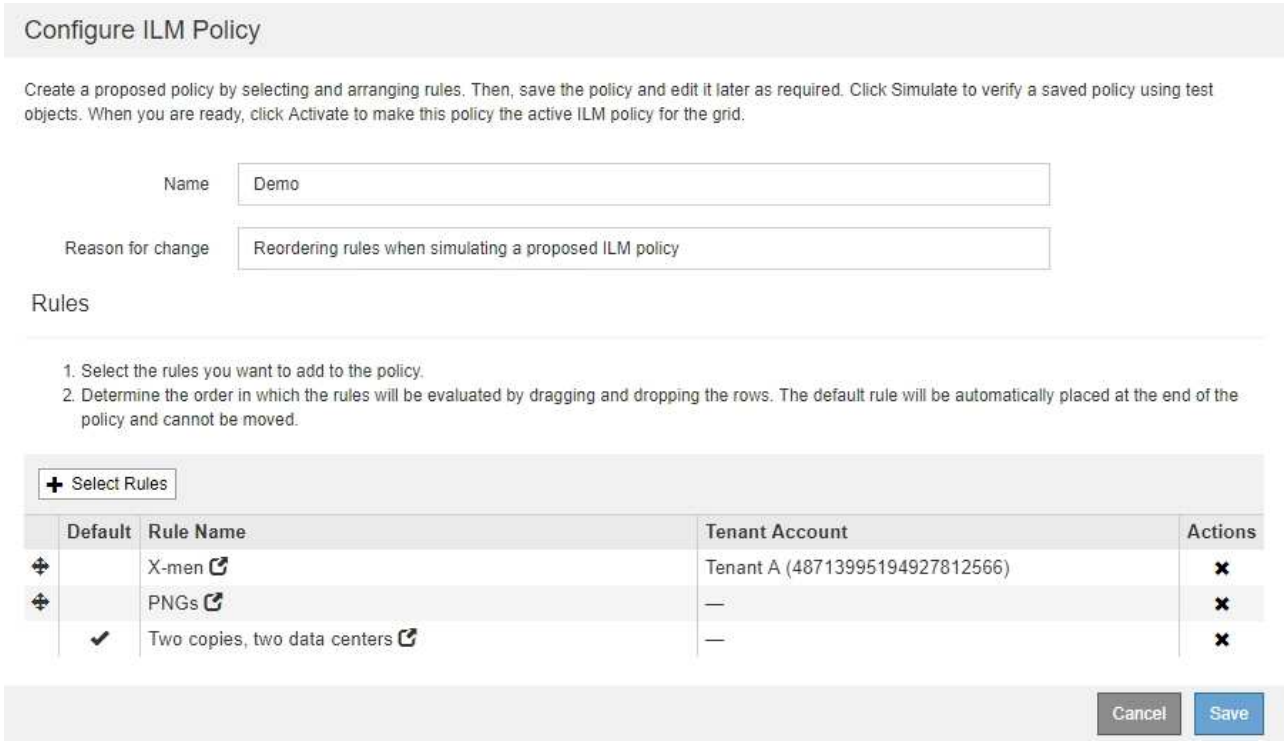
1. ルールを追加してポリシーを保存したら、* Simulate *をクリックします。
2. * Object フィールドに、テストオブジェクトの**S3**バケット/オブジェクトキーまたは**Swift**コンテナ/オブジェクト名を入力し、 Simulate *をクリックします。

   シミュレーション結果が表示され、が表示されます `Havok.png` オブジェクトは「* PNGs *」ルールに一致しました。




   ただし、そのルールはです `Havok.png` オブジェクトは* X-men *ルールをテストすることを意図していました。

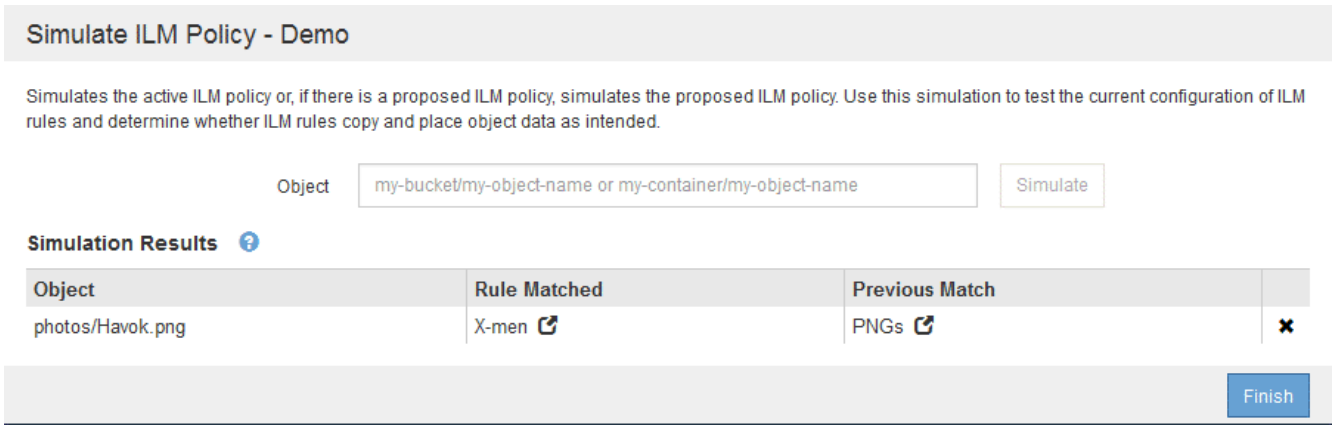
3. 問題 を解決するには、ルールの順序を変更します。
   a. Finish *をクリックして、Simulate ILM Policyページを閉じます。
   b. * Edit *をクリックして、ポリシーを編集します。
   c. 「 * X-men 」ルールをリストの先頭にドラッグします。




d. [ 保存（ Save ） ] をクリックします。

4. * Simulate *をクリックします。

以前にテストしたオブジェクトが更新したポリシーに照らして再評価され、新しいシミュレーション結果が表示されます。この例では、Rule Matched列にが表示されています `Havok.png` 想定どおりに「X-men」メタデータルールに一致します。以前の一致列には、 PNGs ルールが以前のシミュレーションでオブジェクトに一致したことが示されます。



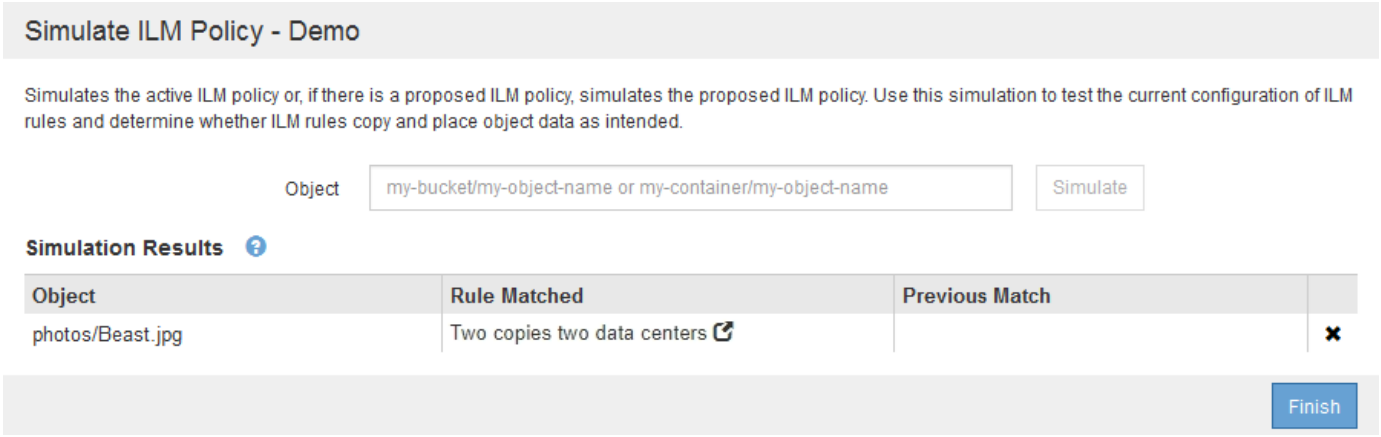

[ ポリシーの設定 ] ページを開いたままにしておくと、テストオブジェクトの名前を再入力しなくても、変更後にポリシーを再シミュレートできます。

例 **3** ：ドラフトの **ILM** ポリシーをシミュレートする際にルールを修正する

この例では、ポリシーをシミュレートしてポリシー内のルールを修正し、シミュレーションを続行する方法を示します。

この例では、 * Demo * ポリシーをシミュレートします。このポリシーの目的は、が含まれるオブジェクトを

検索することです `series=x-men` ユーザメタデータ。ただし、に対してシミュレートしたところ予期しない結果が発生しました `Beast.jpg` オブジェクト。オブジェクトが「 X-men 」メタデータルールではなくデフォルトルールに一致しましたが、 2 つのデータセンターがコピーされています。

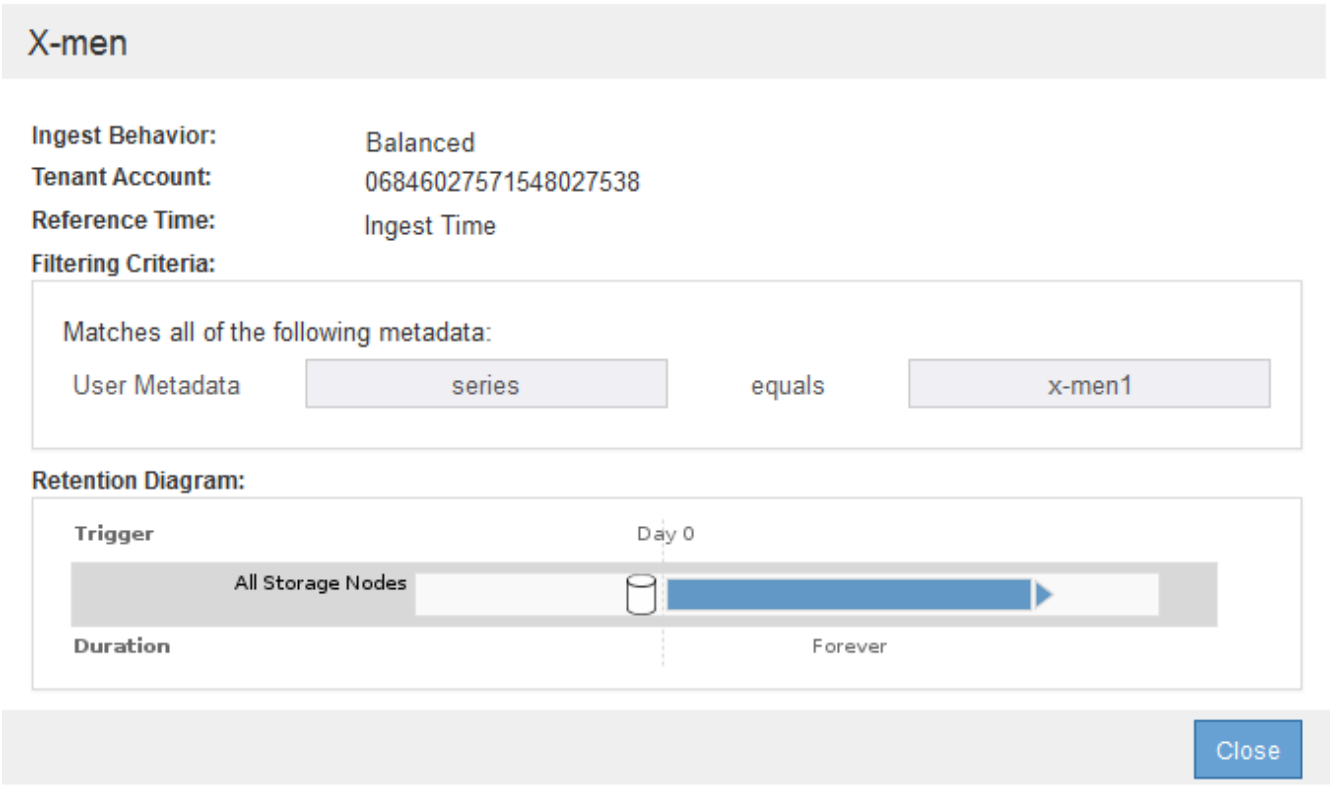



テストオブジェクトがポリシー内の想定したルールに一致しない場合は、ポリシー内の各ルールを調べてエラーを修正する必要があります。

手順

1. ポリシー内のルールごとに、ルール名または詳細アイコンをクリックしてルール設定を確認します をクリックします。
2. ルールのテナントアカウント、参照時間、およびフィルタ条件を確認します。

   この例では、「 X-men 」ルールのメタデータにエラーがあります。メタデータ値は「 x-men. 」ではなく「 x-men1 」として入力されました。



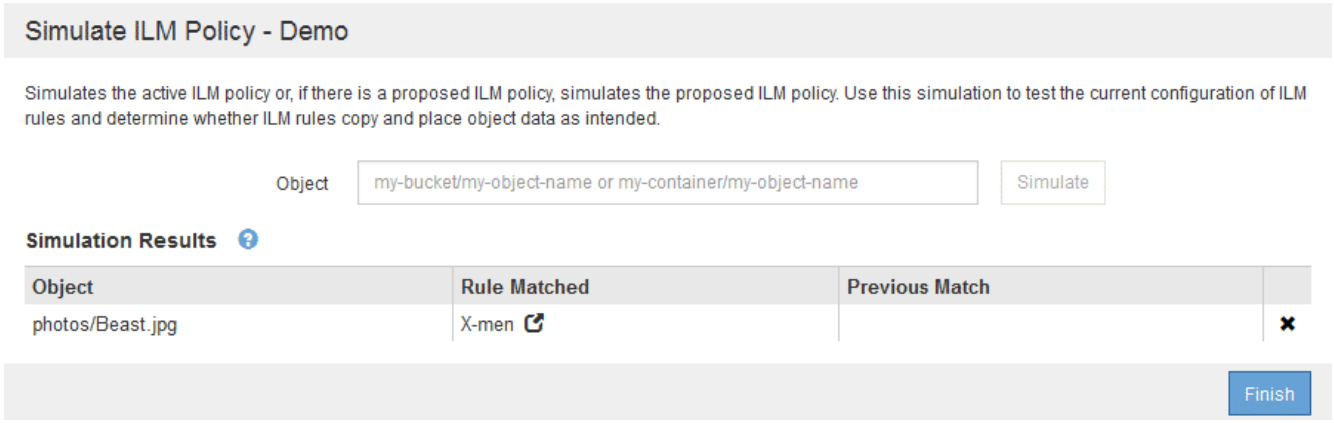
3. このエラーを解決するには、次のようにルールを修正します。
   - ルールがドラフトポリシーに含まれている場合は、ルールをクローニングするか、ポリシーから削除してポリシーを編集できます。
   - ルールがアクティブポリシーに含まれている場合は、ルールをクローニングする必要があります。アクティブポリシーのルールは編集または削除できません。

| オプション | 説明 |
| --- | --- |
| ルールをクローニングしています | i. [* ILM*>* Rules] を選択します。<br>ii. 不正なルールを選択し、* Clone *をクリックします。<br>iii. 誤った情報を変更して、*保存*をクリックします。<br>iv. 「 * ILM * > * Policies * 」を選択します。<br>v. ドラフトポリシーを選択し、* Edit *をクリックします。<br>vi. [ルールの選択]をクリックします。<br>vii. 新しいルールのチェックボックスをオンにし、元のルールのチェックボックスをオフにして、*適用*をクリックします。<br>viii. [ 保存（ Save ） ] をクリックします。 |
| ルールを編集しています | i. ドラフトポリシーを選択し、* Edit *をクリックします。<br>ii. 削除アイコンをクリックします ✖ 誤ったルールを削除するには、*保存*をクリックします。<br>iii. [* ILM*>* Rules] を選択します。<br>iv. 不正なルールを選択し、*編集*をクリックします。<br>v. 誤った情報を変更して、*保存*をクリックします。<br>vi. 「 * ILM * > * Policies * 」を選択します。<br>vii. ドラフトポリシーを選択し、* Edit *をクリックします。<br>viii. 修正したルールを選択し、*適用*をクリックして、*保存*をクリックします。 |

4. もう一度シミュレーションを実行します。

> ILM ポリシーページから移動してルールを編集したため、以前にシミュレーションで入力したオブジェクトは表示されなくなりました。オブジェクトの名前を再入力する必要があります。

この例では、修正した「X-men」ルールがに一致します `Beast.jpg` に基づくオブジェクト `series=x-men` ユーザメタデータ（期待どおり）。




**ILM**ポリシーをアクティブ化します

# ドラフトの ILM ポリシーに ILM ルールを追加してポリシーをシミュレートし、ポリシーが想定どおりに動作することを確認したら、ドラフトポリシーをアクティブ化できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- ドラフトのILMポリシーを保存し、シミュレートしておく必要があります。

> 原因 ポリシーにエラーがあると、回復不能なデータ損失が発生する可能性があります。ポリシーをアクティブ化する前によく確認およびシミュレートし、想定どおりに機能することを確認してください。

> 新しい ILM ポリシーをアクティブ化すると、 StorageGRID は、そのポリシーを使用して、既存のオブジェクトと新たに取り込まれたオブジェクトを含むすべてのオブジェクトを管理します。新しい ILM ポリシーをアクティブ化する前に、既存のレプリケートオブジェクトとイレイジャーコーディングオブジェクトの配置に対する変更を確認してください。既存のオブジェクトの場所を変更すると、新しい配置が評価されて実装される際に一時的なリソースの問題が発生する可能性があります。

このタスクについて

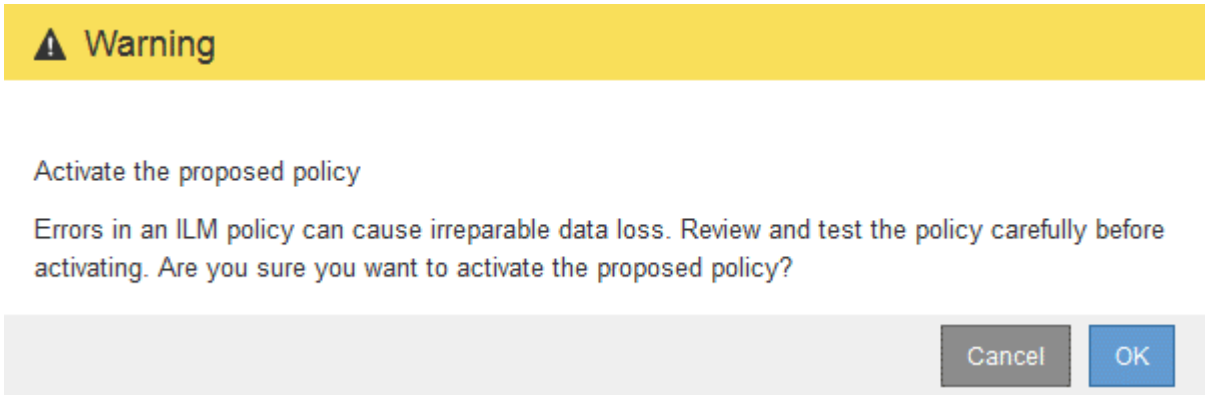
ILM ポリシーをアクティブ化すると、システムは新しいポリシーをすべてのノードに配布します。ただし、すべてのグリッドノードが新しいアクティブポリシーを受信できるようになるまで、新しいポリシーが実際には有効にならない場合があります。グリッドオブジェクトが誤って削除されないように、システムが新しいアクティブポリシーの実装を待機する場合もあります。

- データの冗長性や耐久性を向上させる変更をポリシーに加えた場合、変更内容はすぐに実装されます。たとえば、 2 コピーのルールではなく 3 コピーのルールを含む新しいポリシーをアクティブ化した場合、そのポリシーはすぐに実装されます。これは、データの冗長性が向上するためです。
- データの冗長性や耐久性を低下させる可能性のある変更をポリシーに加えた場合、変更内容はすべてのグリッドノードが使用可能になるまで実装されません。たとえば、 3 コピーのルールではなく 2 コピーのルールを使用する新しいポリシーをアクティブ化すると、新しいポリシーは「 Active 」とマークされますが、すべてのノードがオンラインで使用可能になるまで有効になりません。

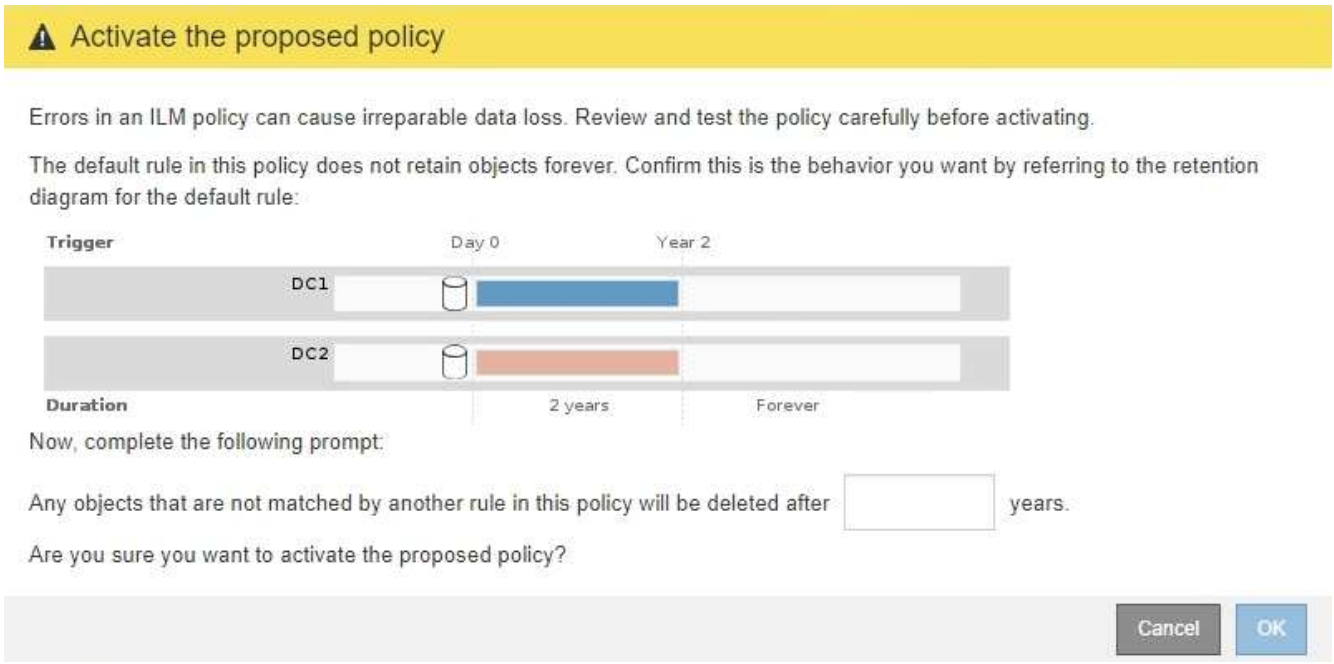
手順

1. ドラフトポリシーをアクティブ化する準備ができたら、ILMポリシーページでポリシーを選択し、*アクティブ化*をクリックします。

   警告メッセージが表示され、ドラフトポリシーをアクティブ化するかどうかの確認を求められます。




   ポリシーのデフォルトルールがオブジェクトを無期限に保持しない場合は、警告メッセージにプロンプトが表示されます。この例の保持図では、デフォルトルールによって 2 年後にオブジェクトが削除されることが示されています。テキストボックスに「 * 2 * 」と入力して、ポリシー内の別のルールに一致しないオブジェクトが 2 年後に StorageGRID から削除されることを確認する必要があります。

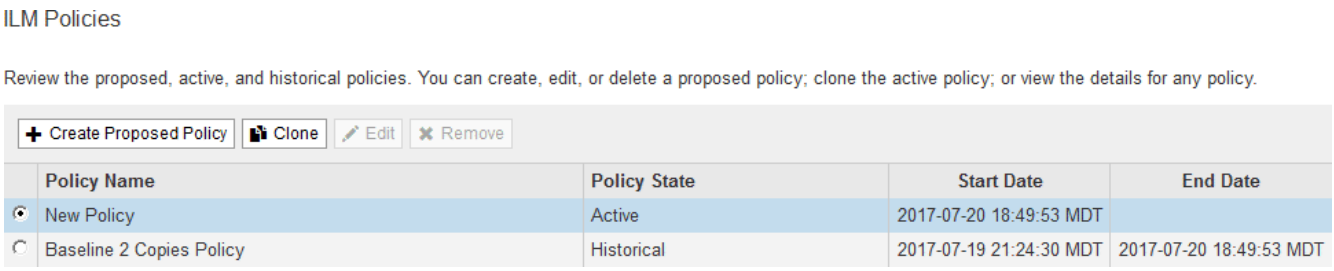



2. [OK] をクリックします。

結果

新しい ILM ポリシーがアクティブ化されると次のようになります。

- ポリシーのポリシーの状態がアクティブと表示されます。[ 開始日 ] エントリには、ポリシーがアクティブ化された日時が表示されます。




- 以前にアクティブだったポリシーが、ポリシーの状態が Historical と表示されます。[ 開始日 ] と [ 終了日 ] のエントリは、ポリシーがアクティブになった日時と、ポリシーが有効でなくなった日時を示します。

関連情報

"例 6 ： ILM ポリシーを変更する"

オブジェクトメタデータの検索による**ILM**ポリシーの検証

## ILM ポリシーをアクティブ化したら、そのポリシーを表すテストオブジェクトを StorageGRID システムに取り込む必要があります。次に、オブジェクトメタデータの検索を実行して、コピーが意図したとおりに作成され、正しい場所に配置されていることを確認します。

必要なもの

- 次のいずれかのオブジェクト ID が必要です。
  - **UUID** ：オブジェクトの Universally Unique Identifier です。UUID はすべて大文字で入力します。
  - * CBID * ： StorageGRID 内のオブジェクトの一意の識別子。監査ログからオブジェクトの CBID を取得できます。CBID はすべて大文字で入力します。
  - * S3 のバケットとオブジェクトキー * ：オブジェクトが S3 インターフェイスから取り込まれた場合、クライアントアプリケーションはバケットとオブジェクトキーの組み合わせを使用してオブジェクトを格納および識別します。
  - * Swift のコンテナとオブジェクト名 * ：オブジェクトが Swift インターフェイスから取り込まれた場合、クライアントアプリケーションはコンテナとオブジェクト名の組み合わせを使用してオブジェクトを格納および識別します。

手順

1. オブジェクトを取り込みます。
2. 「* ILM > Object Metadata Lookup *」を選択します。
3. [ * 識別子 * （ * Identifier * ） ] フィールドにオブジェクトの識別子を入力します。

   UUID 、 CBID 、 S3 バケット / オブジェクトキー、または Swift コンテナ / オブジェクト名を入力できます。

4. [*検索（Look Up）]をクリックします。

   オブジェクトメタデータの検索結果が表示されます。このページには、次の種類の情報が表示されます。

   - システムメタデータ（オブジェクト ID （ UUID ）、オブジェクト名、コンテナの名前、テナントアカウントの名前または ID 、オブジェクトの論理サイズ、オブジェクトの作成日時、オブジェクトの最終変更日時など）。
   - オブジェクトに関連付けられているカスタムユーザメタデータのキーと値のペア。
   - S3 オブジェクトの場合、オブジェクトに関連付けられているオブジェクトタグのキーと値のペア。
   - レプリケートオブジェクトコピーの場合、各コピーの現在の格納場所。
   - イレイジャーコーディングオブジェクトコピーの場合、各フラグメントの現在の格納場所。
   - クラウドストレージプール内のオブジェクトコピーの場合、外部バケットの名前とオブジェクトの一意の識別子を含むオブジェクトの場所。
   - セグメント化されたオブジェクトとマルチパートオブジェクトの場合、セグメント ID とデータサイズを含むオブジェクトセグメントのリスト。100 個を超えるセグメントを持つオブジェクトの場合は、最初の 100 個のセグメントだけが表示されます。
   - 未処理の内部ストレージ形式のすべてのオブジェクトメタデータ。この未加工のメタデータには、リリース間で維持されるとはかぎらない内部のシステムメタデータが含まれます。

     次の例では、 2 つのレプリケートコピーとして格納された S3 テストオブジェクトのオブジェクトメタデータの検索結果が表示されています。

**System Metadata**

| | |
|---|---|
| Object ID | A12E96FF-B13F-4905-9E9E-45373F6E7DA8 |
| Name | testobject |
| Container | source |
| Account | t-1582139188 |
| Size | 5.24 MB |
| Creation Time | 2020-02-19 12:15:59 PST |
| Modified Time | 2020-02-19 12:15:59 PST |

**Replicated Copies**

| Node | Disk Path |
|---|---|
| 99-97 | /var/local/rangedb/2/p/06/0B/00nM8H$|TFbnQQ}|CV2E |
| 99-99 | /var/local/rangedb/1/p/12/0A/00nM8H$|TFboW28|CXG% |

**Raw Metadata**


```
{
    "TYPE": "CTNT",
    "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
    "NAME": "testobject",
    "CBID": "0x8823DE7EC7C10416",
    "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
    "PPTH": "source",
    "META": {
        "BASE": {
            "PAWS": "2",
```


5. オブジェクトが正しい場所に格納され、コピーのタイプが正しいことを確認します。

監査オプションが有効になっている場合は、監査ログを監視して「 ORLM Object Rules Met 」というメッセージを探すこともできます。ORLM 監査メッセージからは、 ILM 評価プロセスのより詳細なステータスを確認できますが、オブジェクトデータの配置が正しいかどうかや、 ILM ポリシーが完全かどうかに関する情報は得られません。これは自分で評価する必要があります。詳細については、監査メッセージに関する情報を参照してください。

関連情報

"監査ログを確認します"

"S3 を使用する"

"Swift を使用します"

# ILM ルールと ILM ポリシーを作成したあとも、引き続きストレージ要件の変化に合わせて設定を変更できます。

## **ILM**ルールを削除する

ILM ルールのリストを管理しやすくするためには、使用しない ILM ルールを削除してください。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

> ILM ルールは、アクティブポリシーまたはドラフトポリシーで現在使用されている場合は削除できません。ポリシーを使用している ILM ルールを削除する必要がある場合は、まず次の手順を実行する必要があります。
>
> 1. アクティブポリシーをクローニングするか、ドラフトポリシーを編集します。
> 2. ポリシーから ILM ルールを削除します。
> 3. 新しいポリシーを保存、シミュレート、およびアクティブ化して、オブジェクトが想定どおりに保護されるようにします。

手順

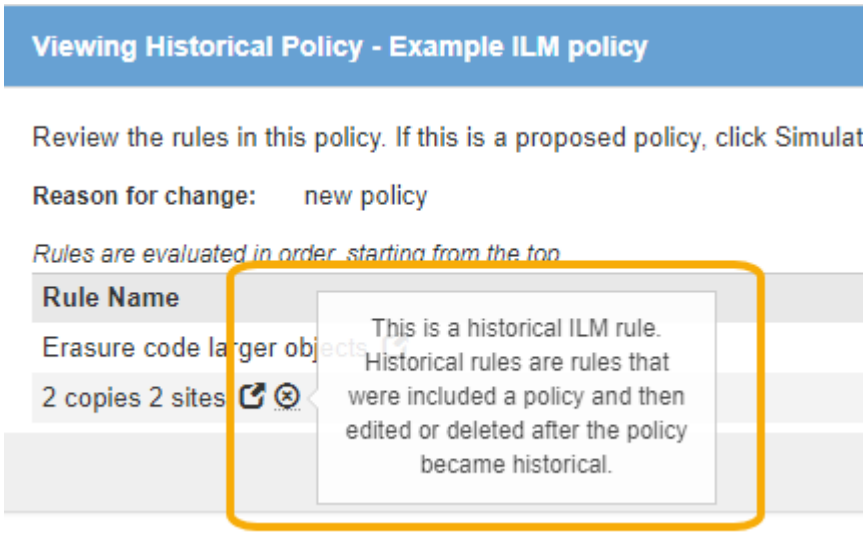
1. [* ILM*>* Rules] を選択します。
2. 削除するルールのテーブルエントリを確認します。

   ルールがアクティブな ILM ポリシーまたはドラフトの ILM ポリシーで使用されていないことを確認します。

3. 削除するルールが使用されていない場合は、ラジオボタンを選択し、 * 削除 * を選択します。
4. 「 * OK 」を選択して、 ILM ルールを削除することを確認します。

   ILM ルールが削除されます。

履歴ポリシーで使用されているルールを削除すると、が削除されます ⊗ ポリシーを表示するとルールのアイコンが表示されます。これは、ルールが履歴ルールになったことを示します。




関連情報

"ILMポリシーを作成する"

**ILM**ルールを編集する

ILM ルールを編集して、フィルタまたは配置手順を変更しなければならない場合があります。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

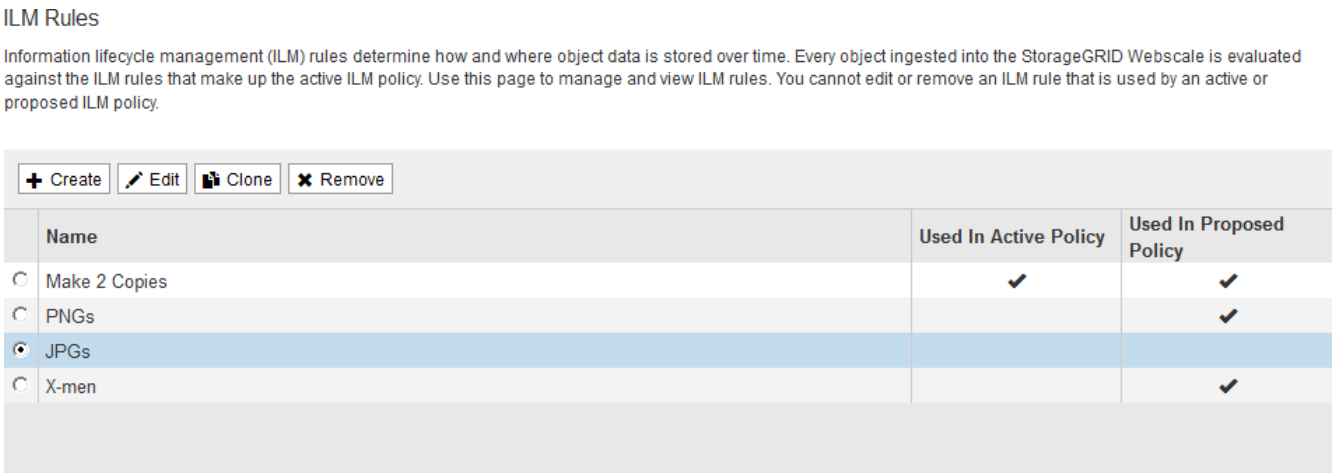
ドラフトの ILM ポリシーまたはアクティブな ILM ポリシーで使用されているルールを編集することはできません。代わりに、これらのルールをクローニングして、クローニングしたコピーに必要な変更を加えることができます。組み込みの ILM ルール（ Make 2 Copies ）や StorageGRID バージョン 10.3 より前に作成された ILM ルールも編集できません。

編集原因 したルールをアクティブな ILM ポリシーに追加する前に、オブジェクトの配置手順の変更によってシステムの負荷が増大する可能性があることに注意してください。

手順

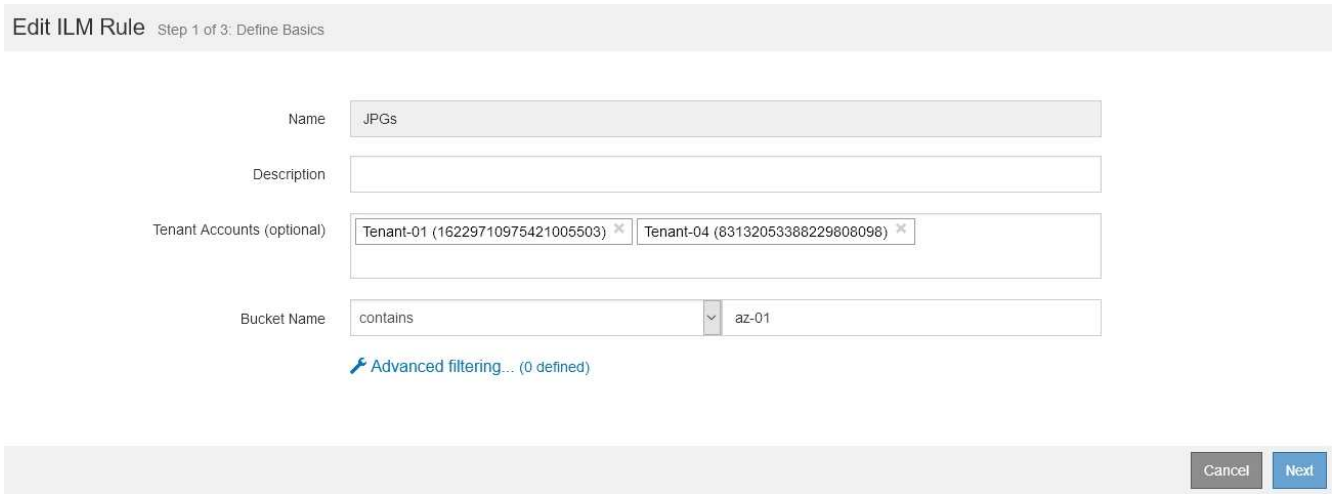
1. [* ILM*>* Rules] を選択します。

   ILM ルールページが表示されます。このページには、使用可能なすべてのルールと、アクティブポリシーまたはドラフトポリシーで使用されているルールが表示されます。




2. 使用されていないルールを選択し、*編集*をクリックします。

   ILM ルールの編集ウィザードが開きます。

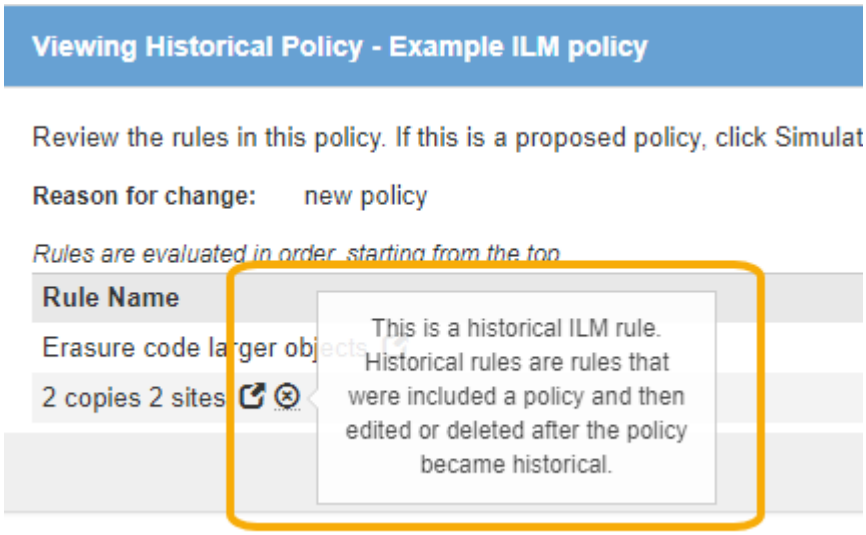



3. ILMルールの作成手順と高度なフィルタを使用する手順に従って、Edit ILM Ruleウィザードの各ページのオプションを設定します。

   ILM ルールの編集時に、 ILM ルールの名前を変更することはできません。

4. [ 保存（ Save ） ] をクリックします。

履歴ポリシーで使用されているルールを編集すると、が表示されます ⊗ ポリシーを表示するとルールのアイコンが表示されます。これは、ルールが履歴ルールになったことを示します。




関連情報

"ILMルールを作成する"

"ILMルールで高度なフィルタを使用する"

**ILM**ルールをクローニングする

ドラフトの ILM ポリシーまたはアクティブな ILM ポリシーで使用されているルールを編集することはできません。代わりに、ルールをクローニングして、クローニングしたコピーに必要な変更を加えることができます。その後、必要に応じてドラフトポリシーから元のルールを削除し、変更後のバージョンに置き換えることができます。バージョン 10.2 以前の StorageGRID を使用して作成された ILM ルールはクローニングできません。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

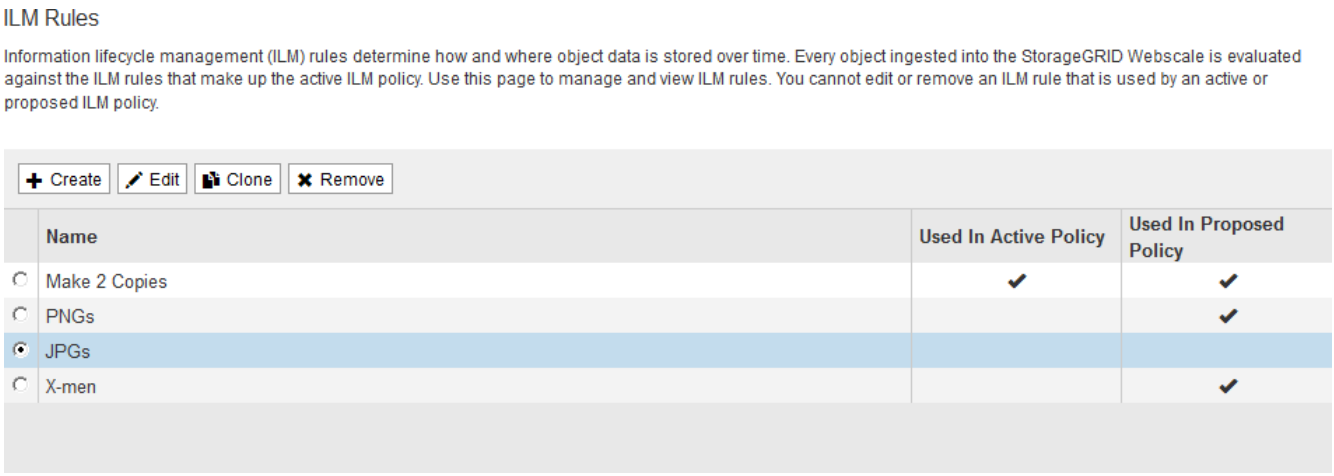
このタスクについて

アクティブな ILM ポリシー原因 にクローニングされたルールを追加する前に、オブジェクトの配置手順の変更によってシステムの負荷が増加する可能性があることに注意してください。

手順

1. [* ILM*>* Rules] を選択します。

   ILM ルールページが表示されます。




2. クローニングするILMルールを選択し、* Clone *をクリックします。

   Create ILM Rule ウィザードが開きます。

3. ILM ルールの編集手順に従い、高度なフィルタを使用して、クローニングされたルールを更新します。

   ILM ルールをクローニングする場合は、新しい名前を入力する必要があります。

4. [ 保存（ Save ） ] をクリックします。

   新しい ILM ルールが作成されます。

関連情報

"ILMルールおよびILMポリシーの操作"

"ILMルールで高度なフィルタを使用する"

**ILM**ポリシーアクティビティキューの表示

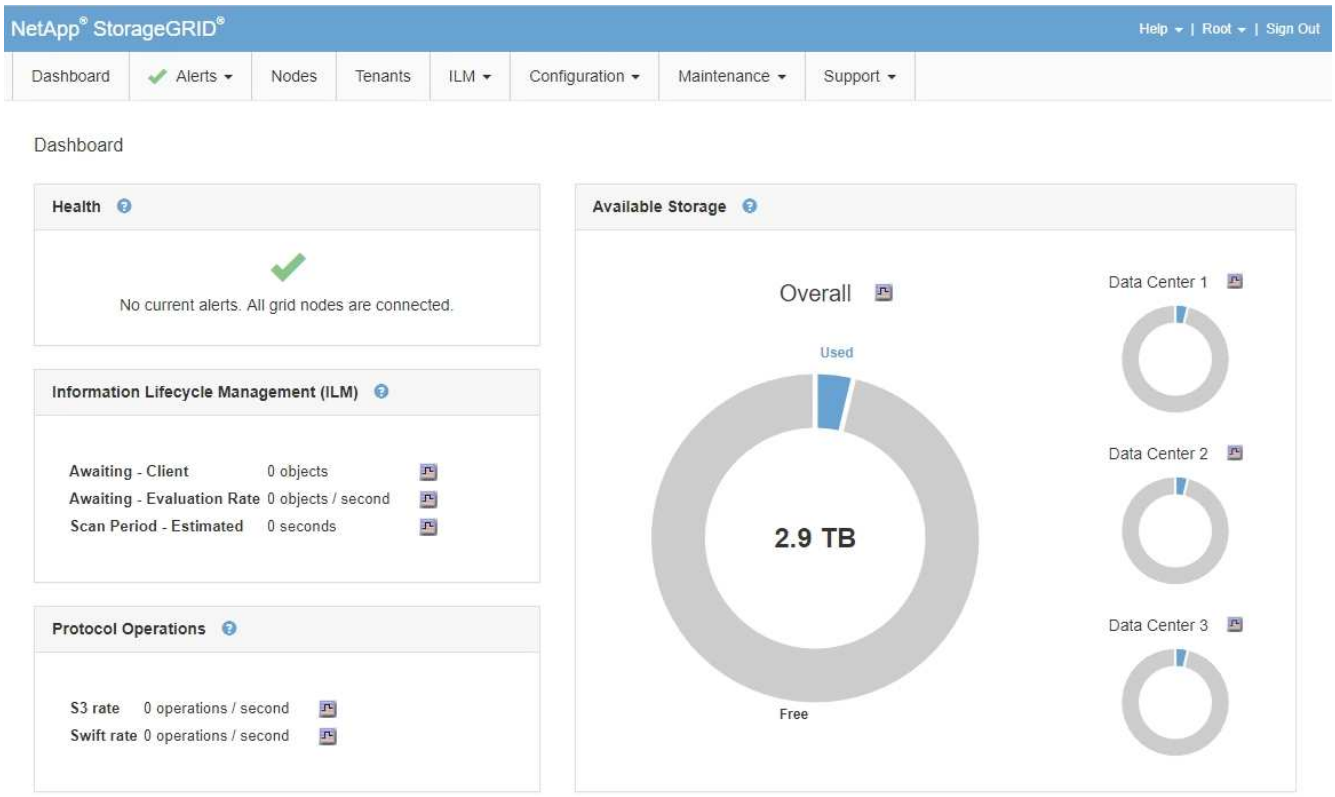
ILM ポリシーに対する評価を待機している、キュー内のオブジェクトの数をいつでも表示できます。システムパフォーマンスを確認するために、 ILM 処理キューの監視が必要になる場合があります。キューが大きい場合は、システムが取り込み速度に対応できていない、クライアントアプリケーションからの負荷が大きすぎる、何らかの異常な状態が存在する、などが考えられます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

手順

1. 「 * ダッシュボード * 」を選択します。




2. 情報ライフサイクル管理（ ILM ）セクションを監視する。

   疑問符をクリックできます をクリックすると、このセクションの項目の概要 が表示されます。

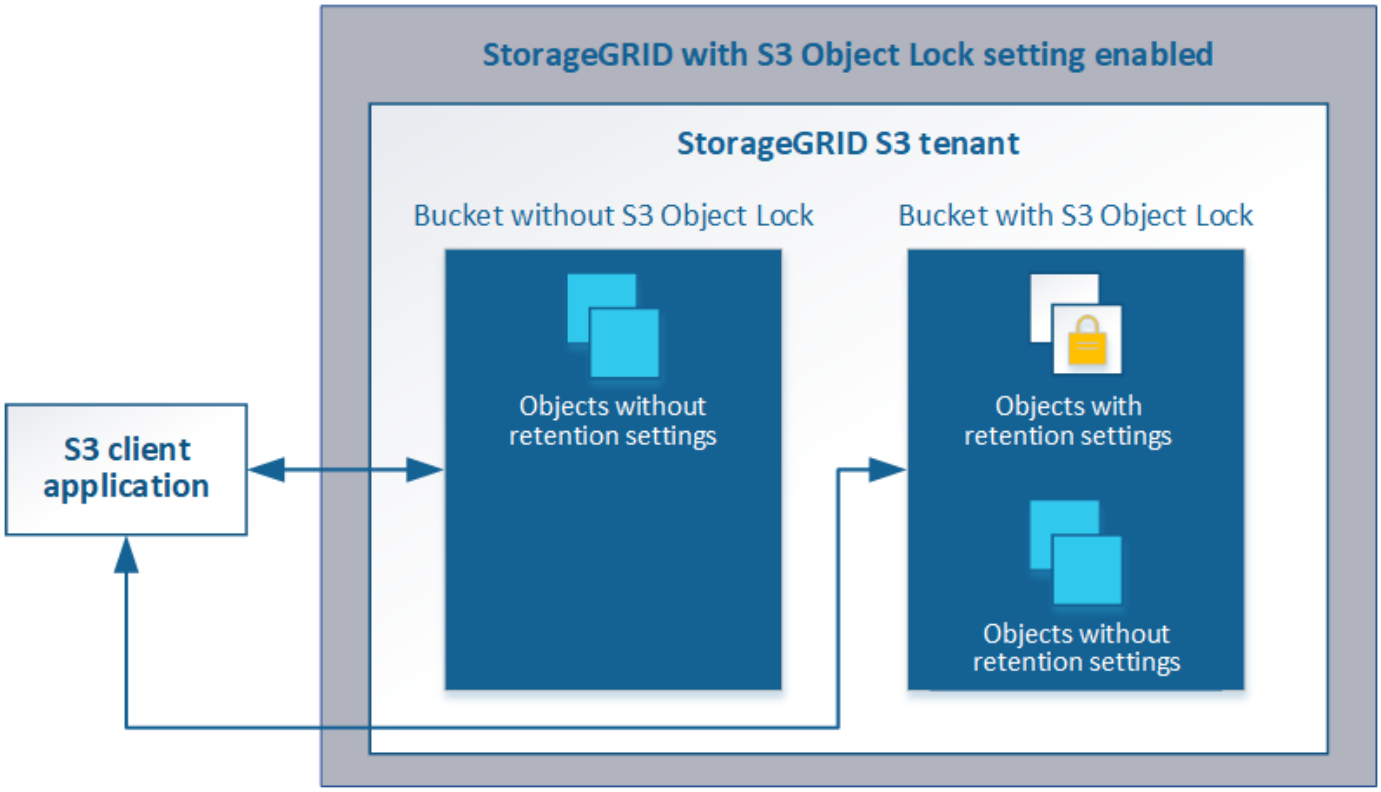
## S3オブジェクトロックでオブジェクトを管理する

グリッド管理者は、 StorageGRID システムで S3 オブジェクトロックを有効にし、準拠 ILM ポリシーを実装して、特定の S3 バケット内のオブジェクトが指定した期間にわたって削除または上書きされないようにすることができます。

### S3 オブジェクトのロックとは何ですか？

StorageGRID S3 オブジェクトロック機能は、 Amazon Simple Storage Service （Amazon S3 ）での S3 オブジェクトロックに相当するオブジェクト保護解決策 です。

図に示すように、 StorageGRID システムでグローバルな S3 オブジェクトのロック設定が有効になっている場合、 S3 テナントアカウントでは、 S3 オブジェクトのロックを有効にしているかどうかに関係なくバケットを作成できます。バケットで S3 オブジェクトのロックが有効になっている場合、 S3 クライアントアプリケーションは、そのバケット内の任意のオブジェクトバージョンの保持設定を必要に応じて指定できます。オブジェクトのバージョンには、 S3 オブジェクトロックで保護するように指定された保持設定が必要です。




StorageGRID S3 オブジェクトロック機能は、 Amazon S3 準拠モードと同等の単一の保持モードを提供します。デフォルトでは、保護されたオブジェクトバージョンは、どのユーザーでも上書きまたは削除できません。StorageGRID S3 オブジェクトのロック機能では、ガバナンスモードはサポートされず、特別な権限を持つユーザは保持設定を省略したり保護されたオブジェクトを削除したりすることはできません。

バケットで S3 オブジェクトロックが有効になっている場合、 S3 クライアントアプリケーションは、オブジェクトの作成時または更新時に、次のオブジェクトレベルの保持設定のいずれか、または両方を必要に応じて指定できます。

- **Retain Until - date** ：オブジェクトバージョンの retain-until - date が将来の日付である場合、オブジェクトは読み出し可能ですが、変更または削除することはできません。必要に応じて、オブジェクトの retain-date を増やすことはできますが、この日付を減らすことはできません。
- * リーガルホールド * ：オブジェクトバージョンにリーガルホールドを適用すると、そのオブジェクトがただちにロックされます。たとえば、調査または法的紛争に関連するオブジェクトにリーガルホールドを設定する必要がある場合があります。リーガルホールドには有効期限はありませんが、明示的に削除されるまで保持されます。リーガルホールドは、それまでの保持期間とは関係ありません。

これらの設定の詳細については、の「Using S3 object lock」を参照してください "S3 REST API のサポートされる処理と制限事項"。

**S3** オブジェクトロックと従来の準拠の比較

StorageGRID 11.5のS3オブジェクトロック機能は、以前のバージョンのStorageGRID で使用できた準拠機能に代わる機能です。新しいS3オブジェクトロック機能はAmazon S3の要件に準拠しているため、「従来のコンプライアンス」と呼ばれる独自のStorageGRID 準拠機能は廃止されています。

グローバル準拠設定を有効にしている場合は、StorageGRID 11.5にアップグレードすると、新しいグローバ

ルS3オブジェクトロック設定が自動的に有効になります。テナントユーザは、StorageGRID 11.5で準拠を有効にした新しいバケットを作成できなくなります。ただし、必要に応じて、テナントユーザは既存の従来の準拠バケットを引き続き使用および管理できます。これには次のタスクの実行が含まれます。

- 従来の準拠が有効になっている既存のバケットに新しいオブジェクトを取り込む。
- 従来の準拠が有効になっている既存のバケットの保持期間を延長する。
- 従来の準拠が有効になっている既存のバケットの自動削除設定を変更する。
- 従来の準拠が有効になっている既存のバケットにリーガルホールドを適用する。
- リーガルホールドを解除する。

"ネットアップのナレッジベース： StorageGRID 11.5 でレガシー準拠バケットを管理する方法"

以前のバージョンの StorageGRID で従来の準拠機能を使用していた場合、次の表を参照して、 StorageGRID の S3 オブジェクトロック機能と比較する方法を確認してください。

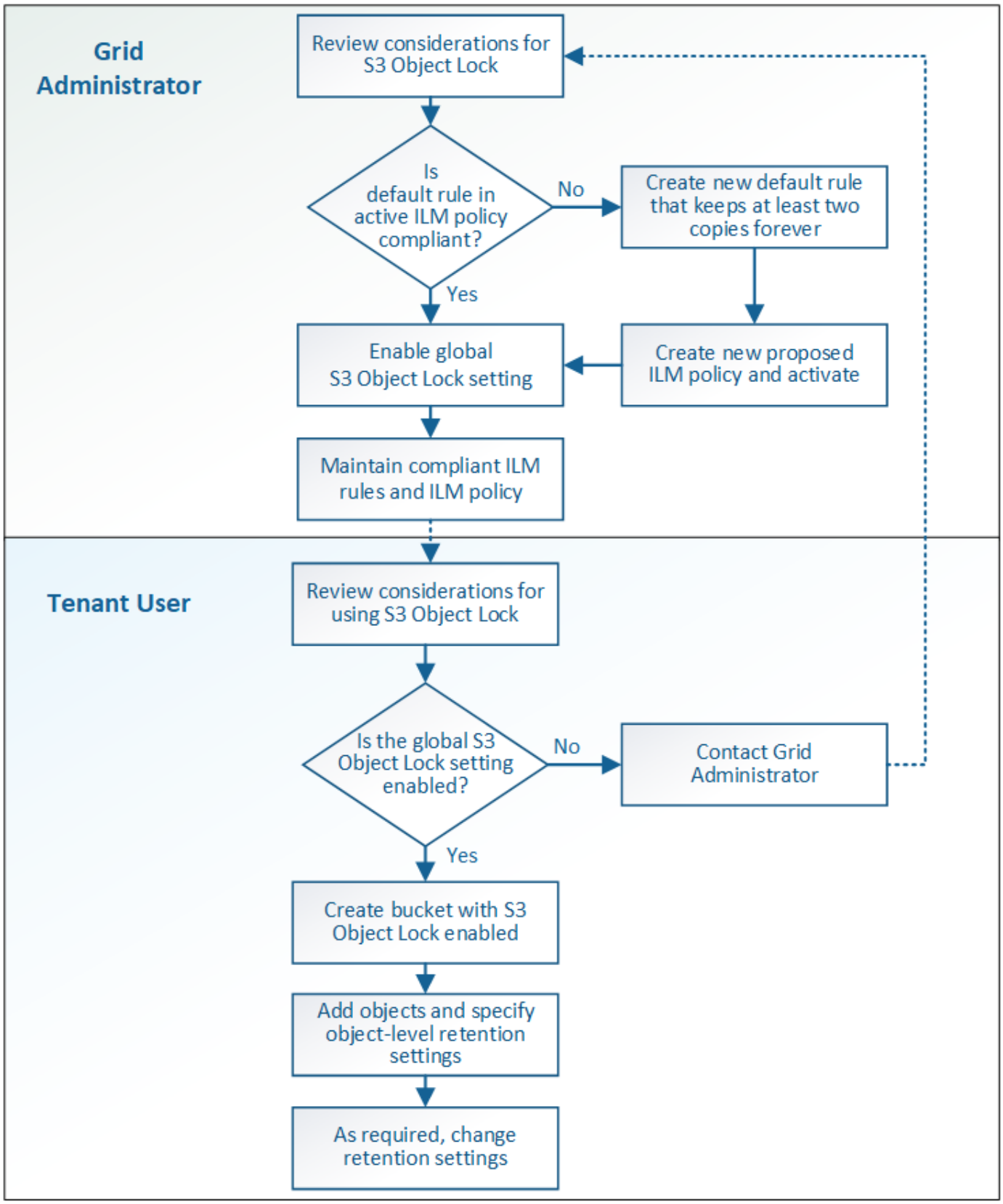
| | **S3** オブジェクトロック（新規） | コンプライアンス（レガシー） |
|---|---|---|
| この機能はグローバルにどのように有効になりますか。 | Grid Managerから* Configuration > System Settings > S3 Object Lock *を選択します。 | サポートは終了しました。<br><br>*注：グローバル準拠設定を有効にしている場合、StorageGRID 11.5にアップグレードすると、グローバルなS3オブジェクトロック設定が自動的に有効になります。 |
| バケットで機能を有効にするにはどうすればよいですか？ | Tenant Manager 、テナント管理 API 、または S3 REST API を使用して新しいバケットを作成するときは、 S3 オブジェクトロックを有効にする必要があります。 | 準拠を有効にした新しいバケットを作成することはできなくなりました。ただし、既存の準拠バケットには引き続き新しいオブジェクトを追加できます。 |
| バケットのバージョン管理はサポートされているか | はい。バケットのバージョン管理は必須であり、バケットで S3 オブジェクトのロックが有効になっている場合は自動的に有効になります。 | いいえ従来の準拠機能では、バケットのバージョン管理は許可されていません。 |
| オブジェクト保持はどのように設定されますか。 | ユーザーは、オブジェクトバージョンごとに retain-until date を設定できます。 | ユーザはバケット全体の保持期間を設定する必要があります。保持期間を指定すると、バケット内のすべてのオブジェクトが環境 で保持されます。 |
| バケットには保持とリーガルホールドのデフォルト設定を適用できるか。 | いいえS3オブジェクトのロックが有効になっているStorageGRID バケットでは、デフォルトの保持期間は使用されません。代わりに、オブジェクトバージョンごとにretain-dateを指定できます。 | はい。 |

| | **S3** オブジェクトロック（新規） | コンプライアンス（レガシー） |
|---|---|---|
| 保持期間は変更できますか。 | オブジェクトバージョンの retain-until は、上げることはできますが、減らすことはできません。 | バケットの保持期間は、増やすことはできますが、減らすことはできません。 |
| リーガルホールドはどこで制御されますか？ | バケット内のオブジェクトバージョンにリーガルホールドを適用したり、リーガルホールドを解除したりできます。 | リーガルホールドはバケットに適用され、バケット内のすべてのオブジェクトに適用されます。 |
| オブジェクトを削除できるのはいつですか。 | オブジェクトがリーガルホールドの対象でない場合は、 retain-until 日に達したあとでオブジェクトバージョンを削除できます。 | バケットがリーガルホールドの対象でない場合は、保持期間が過ぎたあとにオブジェクトを削除できます。オブジェクトは自動または手動で削除できます。 |
| バケットライフサイクル設定はサポートされていますか。 | はい。 | いいえ |

**S3** オブジェクトロックのワークフロー

## グリッド管理者は、テナントユーザと緊密に連携し、保持要件に応じてオブジェクトが保護されるようにする必要があります。

次のワークフロー図は、 S3 オブジェクトロックの使用手順の概要を示しています。以下の手順は、グリッド管理者およびテナントユーザが実行します。




**Grid** 管理者タスク

ワークフロー図に示されているように、 S3 テナントユーザが S3 オブジェクトロックを使用できるようにするには、グリッド管理者が次の 2 つのタスクを実行する必要があります。

1. 準拠 ILM ルールを少なくとも 1 つ作成し、アクティブな ILM ポリシー内のデフォルトルールに設定します。
2. StorageGRID システム全体で、グローバルな S3 オブジェクトロック設定を有効にします。

テナントユーザタスク

グローバルな S3 オブジェクトのロック設定を有効にしたあと、テナントは次のタスクを実行できます。

1. S3 オブジェクトのロックを有効にしたバケットを作成する。
2. これらのバケットにオブジェクトを追加し、オブジェクトレベルの保持期間とリーガルホールドの設定を指定します。
3. 必要に応じて、個々のオブジェクトの保持期間を更新するか、リーガルホールド設定を変更します。

関連情報

"テナントアカウントを使用する"

"S3 を使用する"

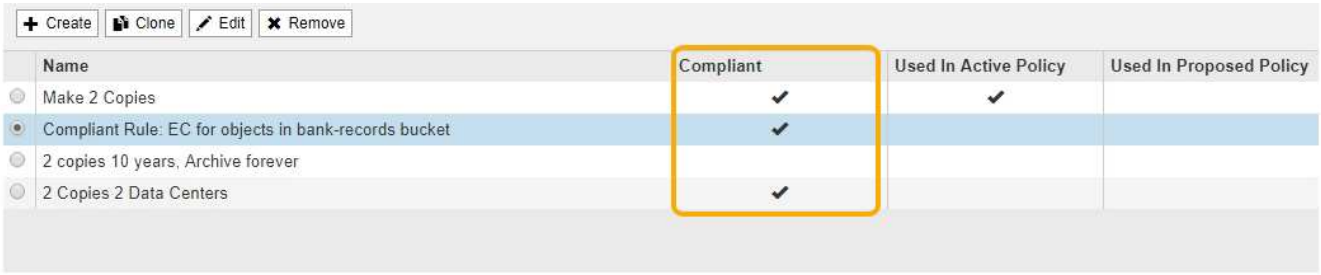
**S3** オブジェクトのロックの要件

グローバルな S3 オブジェクトのロック設定を有効にするための要件、準拠 ILM ルールおよび ILM ポリシーを作成するための要件、および StorageGRID が S3 オブジェクトロックを使用するバケットとオブジェクトに適用する制限事項を確認しておく必要があります。

グローバルな **S3** オブジェクトロック設定を使用するための要件

- S3 テナントが S3 オブジェクトロックを有効にしてバケットを作成できるようにするには、 Grid Manager またはグリッド管理 API を使用してグローバルな S3 オブジェクトロック設定を有効にする必要があります。
- グローバルな S3 オブジェクトのロック設定を有効にすると、すべての S3 テナントアカウントで S3 オブジェクトのロックを有効にしてバケットを作成できるようになります。
- グローバルな S3 オブジェクトのロック設定を有効にしたあとに、設定を無効にすることはできません。
- アクティブなILMポリシーのデフォルトルールが_Compliant _でないとグローバルなS3オブジェクトロックを有効にすることはできません（つまり、デフォルトルールはS3オブジェクトロックが有効になっているバケットの要件を満たす必要があります）。
- グローバルな S3 オブジェクトのロック設定が有効になっている場合、ポリシーのデフォルトルールが準拠していないと、ドラフトの ILM ポリシーを新規作成したり、既存のドラフトの ILM ポリシーをアクティブ化したりすることはできません。グローバルな S3 オブジェクトのロック設定を有効にすると、 ILM ルールおよび ILM ポリシーのページに、準拠している ILM ルールが表示されます。

  次の例では、 ILM ルールページに、 S3 オブジェクトのロックが有効になっているバケットに準拠した 3 つのルールが表示されています。

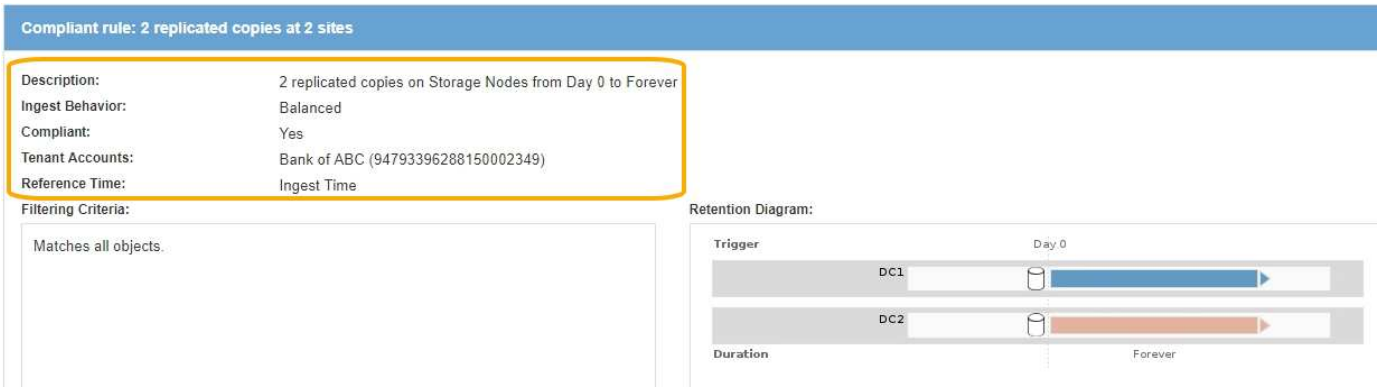


準拠 **ILM** ルールの要件

グローバルな S3 オブジェクトのロック設定を有効にする場合は、アクティブな ILM ポリシーのデフォルトルールが準拠していることを確認する必要があります。準拠ルールは、 S3 オブジェクトのロックが有効になっているバケットと従来の準拠が有効になっている既存のバケットの両方の要件を満たします。

- 2 つ以上のレプリケートオブジェクトコピーまたは 1 つのイレイジャーコーディングコピーを作成する。
- これらのコピーが、配置手順の各ラインの間、ストレージノード上に存在している必要があります。
- オブジェクトコピーをクラウドストレージプールに保存することはできません。
- オブジェクトコピーをアーカイブノードに保存することはできません。
- 配置手順の 1 行以上が、参照時間として * 取り込み時間 * を使用して 0 日目から開始されている必要があります。
- 配置手順の少なくとも 1 行は「無期限」である必要があります。

たとえば、次のルールは S3 オブジェクトのロックを有効にしたバケットの要件を満たしています。2 つの複製オブジェクト・コピーを取り込み時（ 0 日目）から「無期限」に格納します。 オブジェクトは 2 つのデータセンターのストレージノードに格納されます。




アクティブな **ILM** ポリシーとドラフトの **ILM** ポリシーの要件

グローバルな S3 オブジェクトのロック設定が有効になっている場合は、アクティブな ILM ポリシーとドラフ

トの ILM ポリシーに、準拠ルールと非準拠ルールの両方を含めることができます。

- アクティブな ILM ポリシーまたはドラフトの ILM ポリシーのデフォルトルールは、準拠ルールである必要があります。
- 非準拠ルールは、 S3 オブジェクトロックが有効になっていないバケット内のオブジェクト、または従来の準拠機能が有効になっていないオブジェクトのみに適用されます。
- 準拠ルールは任意のバケット内のオブジェクトに適用できます。 S3 オブジェクトのロックや従来の準拠を有効にする必要はありません。

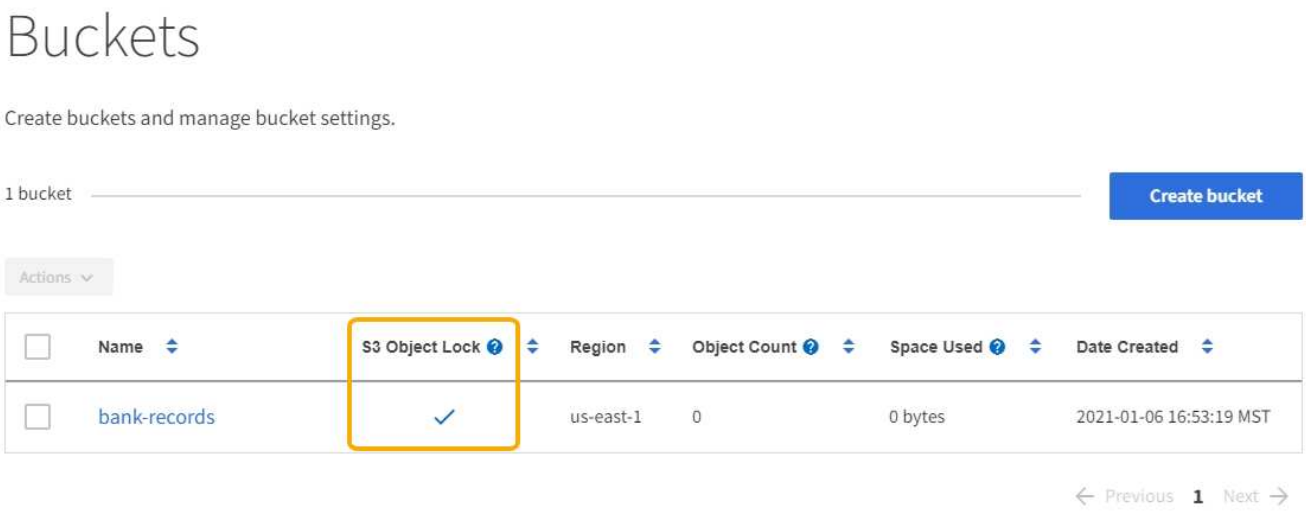
準拠 ILM ポリシーには、次の 3 つのルールが含まれる場合があります。

1. S3 オブジェクトのロックが有効な特定のバケット内にオブジェクトのイレイジャーコーディングコピーを作成する準拠ルール。EC コピーは、 0 日目から無期限にストレージノードに格納されます。
2. 2 つのレプリケートオブジェクトコピーを作成してストレージノードに 1 年間保存したあと、 1 つのオブジェクトコピーをアーカイブノードに移動して無期限に格納する非準拠ルール。このルールでは、 S3 オブジェクトロックまたはレガシー準拠が有効になっていない環境 バケットのみが無期限に格納され、アーカイブノードを使用するため、バケットのみが有効になります。
3. 2 つのレプリケートオブジェクトコピーを 0 日目からストレージノードに無期限に作成するデフォルトの準拠ルール。このルールは、最初の 2 つのルールでフィルタリングされなかったすべてのバケットのオブジェクトを環境 します。

**S3** オブジェクトのロックを有効にした場合のバケットの要件

- StorageGRID システムでグローバルな S3 オブジェクトロック設定が有効になっている場合は、テナントマネージャ、テナント管理 API 、または S3 REST API を使用して、 S3 オブジェクトロックを有効にしたバケットを作成できます。

  次の Tenant Manager の例では、 S3 オブジェクトのロックが有効になっているバケットを示しています。




- S3 オブジェクトのロックを使用する場合は、バケットの作成時に S3 オブジェクトのロックを有効にする必要があります。既存のバケットに対して S3 オブジェクトロックを有効にすることはできません。
- S3 オブジェクトロックでは、バケットのバージョン管理が必要です。バケットで S3 オブジェクトのロックが有効になっている場合は、そのバケットのバージョン管理が StorageGRID で自動的に有効になります。

- S3 オブジェクトのロックを有効にしてバケットを作成したあとに、そのバケットの S3 オブジェクトのロックを無効にしたりバージョン管理を一時停止したりすることはできません。
- S3オブジェクトのロックが有効になっているStorageGRID バケットでは、デフォルトの保持期間はありません。代わりに、S3クライアントアプリケーションは、そのバケットに追加されるオブジェクトバージョンごとに保持期限とリーガルホールド設定を指定できます。
- バケットライフサイクル設定は S3 オブジェクトライフサイクルバケットでサポートされます。
- CloudMirror レプリケーションは、 S3 オブジェクトロックが有効になっているバケットではサポートされません。

#### S3 オブジェクトのロックが有効になっているバケット内のオブジェクトの要件

- S3クライアントアプリケーションは、S3オブジェクトのロックで保護する必要があるオブジェクトごとに保持設定を指定する必要があります。
- オブジェクトバージョンの retain-until date は増やすことができますが、この値を減らすことはできません。
- 係争中の訴訟や規制上の調査に関する通知があった場合、オブジェクトバージョンをリーガルホールドの対象にすることで関連情報を保持できます。オブジェクトバージョンがリーガルホールドの対象になっている場合は、それが retain-until 日に達しても、そのオブジェクトを StorageGRID から削除することはできません。リーガルホールドを解除すると、それまで保持期限に達した場合にオブジェクトバージョンを削除できるようになります。
- S3 オブジェクトロックにはバージョン管理されたバケットを使用する必要があります。保持設定はオブジェクトのバージョンごとに適用されます。オブジェクトバージョンには、 retain-until date 設定とリーガルホールド設定の両方を設定できます。ただし、オブジェクトバージョンを保持することはできません。また、どちらも保持することはできません。オブジェクトの retain-une-date 設定またはリーガルホールド設定を指定すると、要求で指定されたバージョンのみが保護されます。オブジェクトの以前のバージョンはロックされたまま、オブジェクトの新しいバージョンを作成できます。

#### S3 オブジェクトのロックが有効なバケット内のオブジェクトのライフサイクル

S3 オブジェクトのロックが有効になっているバケットに保存された各オブジェクトは、次の 3 つの段階を経て処理されます。

1. * オブジェクトの取り込み *
    - S3 オブジェクトのロックが有効になっているバケットにオブジェクトのバージョンを追加するときに、 S3 クライアントアプリケーションはオプションでオブジェクトの保持設定を指定できます（ retain-until date 、 legal hold 、または both ）。StorageGRID は、そのオブジェクトのメタデータを生成します。これには、一意のオブジェクト ID （ UUID ）と取り込み日時が含まれます。
    - 保持設定のあるオブジェクトのバージョンが取り込まれたあとに、そのデータと S3 ユーザ定義メタデータを変更することはできません。
    - StorageGRID は、オブジェクトメタデータをオブジェクトデータとは別に格納します。各サイトですべてのオブジェクトメタデータのコピーを 3 つ保持します。
2. * オブジェクト保持 *
    - オブジェクトの複数のコピーが StorageGRID によって格納される。コピーの正確な数、タイプ、格納場所は、アクティブな ILM ポリシーの準拠ルールによって決まります。
3. * オブジェクトの削除 *
    - オブジェクトは、 retain-until - date に到達したときに削除できます。

- リーガルホールドの対象になっているオブジェクトは削除できません。

関連情報

"テナントアカウントを使用する"

"S3 を使用する"

"S3 オブジェクトロックと従来の準拠の比較"

"例 7 ： S3 オブジェクトロックの準拠 ILM ポリシー"

"監査ログを確認します"

## S3オブジェクトのロックをグローバルに有効にする

オブジェクトデータの保存時に S3 テナントアカウントが規制要件に準拠する必要がある場合は、 StorageGRID システム全体で S3 オブジェクトのロックを有効にする必要があります。グローバルな S3 オブジェクトのロック設定を有効にすると、 S3 テナントユーザは S3 オブジェクトのロックでバケットとオブジェクトを作成および管理できるようになります。

必要なもの

- Root Access 権限が必要です。
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- S3オブジェクトロックのワークフローを確認し、考慮事項を把握しておく必要があります。
- アクティブなILMポリシーのデフォルトルールは準拠ルールである必要があります。

  "デフォルトのILMルールを作成する"

  "ILMポリシーを作成する"

このタスクについて

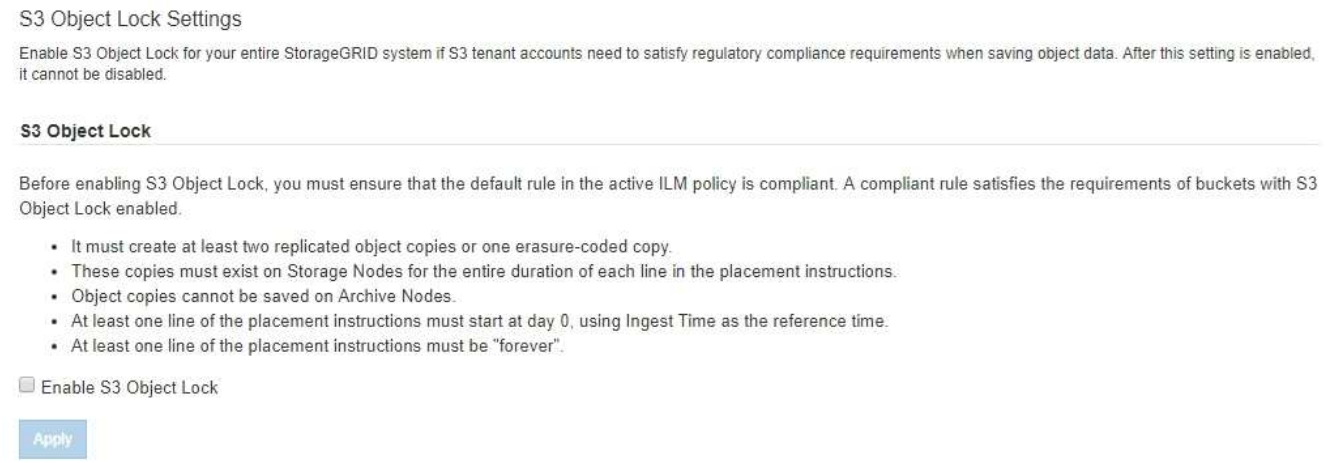
テナントユーザが S3 オブジェクトのロックを有効にした新しいバケットを作成できるようにするには、グリッド管理者がグローバルな S3 オブジェクトロック設定を有効にする必要があります。この設定を有効にすると、あとで無効にすることはできません。

> 以前のバージョンのStorageGRID を使用してグローバル準拠設定を有効にした場合は、StorageGRID バージョン11.5にアップグレードすると新しいS3オブジェクトロック設定が自動的に有効になります。既存の準拠バケットの設定の管理には引き続きStorageGRID を使用できますが、新しい準拠バケットを作成することはできません。
>
> "ネットアップのナレッジベース： StorageGRID 11.5 でレガシー準拠バケットを管理する方法"

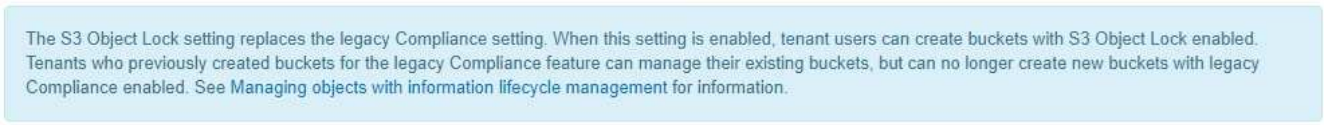
手順

1. * Configuration > System Settings > S3 Object Lock *を選択します。

   S3 Object Lock Settings （ S3 オブジェクトロック設定）ページが表示されます。

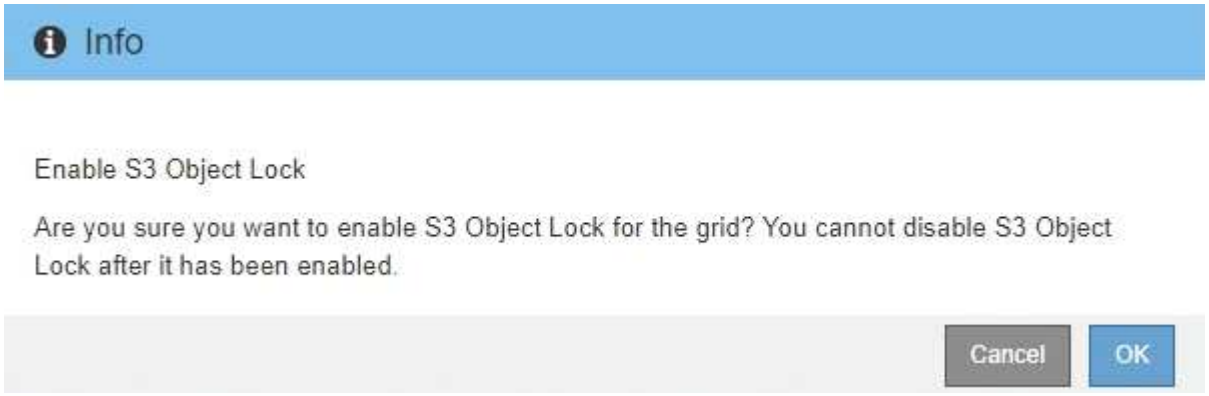



以前のバージョンの StorageGRID を使用してグローバル準拠設定を有効にした場合、ページには次の注が表示されます。




2. S3 オブジェクトロックを有効にする * を選択します。
3. * 適用 * を選択します。

   確認のダイアログボックスが表示され、有効にした S3 オブジェクトのロックを無効にできないことを通知するメッセージが表示されます。

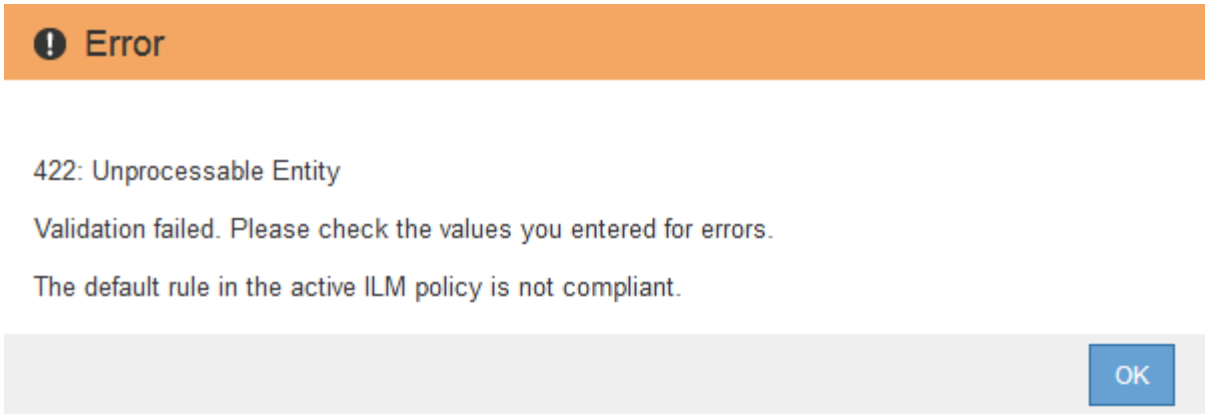



4. システム全体に対して S3 オブジェクトロックを永続的に有効にしてもよろしいですか？ * OK * を選択します。

   「 * OK * 」を選択した場合：

   ◦ アクティブな ILM ポリシーのデフォルトルールが準拠している場合は、グリッド全体で S3 オブジェクトのロックが有効になり、無効にすることはできません。

   ◦ デフォルトルールが準拠していない場合は、準拠ルールをデフォルトルールとして含む新しい ILM ポリシーを作成してアクティブ化する必要があることを示すエラーメッセージが表示されます。「 * OK 」を選択し、新しいドラフトポリシーを作成してシミュレートし、アクティブ化します。




完了後

グローバルなS3オブジェクトのロック設定を有効にしたあとで、新しいILMポリシーを作成できます。設定を有効にすると、 ILM ポリシーに、準拠デフォルトルールと非準拠デフォルトルールの両方をオプションで含めることができます。たとえば、 S3 オブジェクトロックが有効になっていないバケット内のオブジェクトに対してフィルタが適用されていない非準拠ルールを使用できます。

関連情報

"S3オブジェクトのロックが有効になったあとのILMポリシーの作成"

"ILMルールを作成する"

"ILMポリシーを作成する"

"S3 オブジェクトロックと従来の準拠の比較"

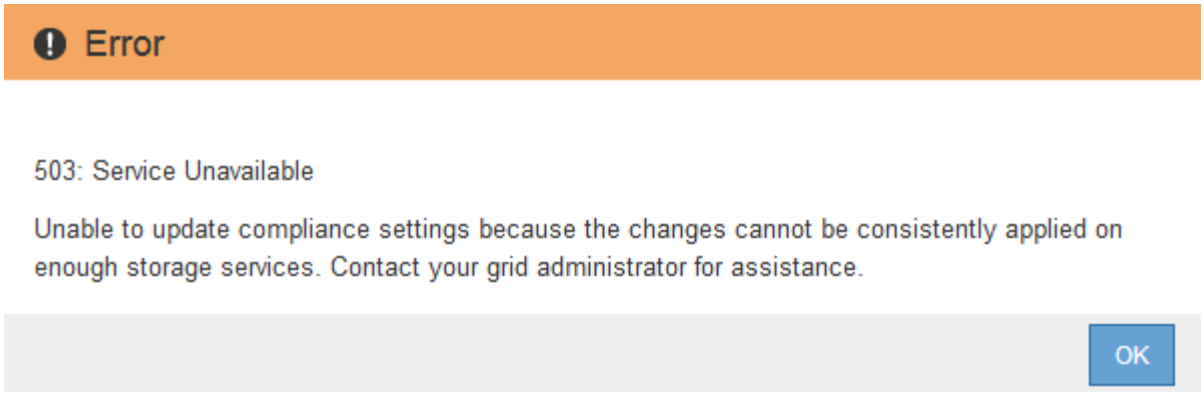
**S3**オブジェクトロックまたは従来の準拠設定の更新時に発生した整合性エラーを解決する

## データセンターサイトまたはサイトの複数のストレージノードが使用できなくなった場合は、 S3 テナントユーザが S3 オブジェクトロックまたは従来の準拠設定に変更を適用できるよう支援する必要があります。

S3 オブジェクトロック（または従来の準拠）が有効になっているバケットを使用するテナントユーザは、特定の設定を変更できます。たとえば、 S3 オブジェクトロックを使用するテナントユーザがオブジェクトのバージョンをリーガルホールドの対象にする必要がある場合があります。

テナントユーザが S3 バケットまたはオブジェクトバージョンの設定を更新すると、 StorageGRID はグリッド全体ですぐにバケットまたはオブジェクトメタデータを更新します。データセンターサイトまたは複数のストレージノードが使用できないためにメタデータを更新できない場合は、エラーメッセージが表示されます。具体的には、

- Tenant Manager ユーザには次のエラーメッセージが表示されます。




- テナント管理APIユーザとS3 APIユーザは、の応答コードを受け取ります `503 Service Unavailable` 同様のメッセージテキストを含む。

このエラーを解決するには、次の手順を実行します。

1. できるだけ早く、すべてのストレージノードまたはサイトを利用できる状態に戻します。
2. 各サイトで十分な数のストレージノードを利用可能にできない場合は、テクニカルサポートに問い合わせて、ノードをリカバリし、変更がグリッド全体に一貫して適用されるようにしてください。
3. 基盤となる問題 が解決されたら、テナントユーザに設定の変更を再試行するよう通知してください。

関連情報

"テナントアカウントを使用する"

"S3 を使用する"

""

## ILM ルールとポリシーの例

このセクションの例は、独自のILMルールとポリシーのベースとして使用できます。

- "例 1 ：オブジェクトストレージの ILM ルールとポリシー"
- "例 2 ： EC オブジェクトサイズのフィルタリング用の ILM ルールとポリシー"
- "例 3 ：画像ファイルの保護を強化する ILM ルールとポリシー"
- "例 4 ： S3 バージョン管理オブジェクトの ILM ルールとポリシー"
- "例 5 ：取り込み動作が Strict の場合の ILM ルールとポリシー"
- "例 6 ： ILM ポリシーを変更する"
- "例 7 ： S3 オブジェクトロックの準拠 ILM ポリシー"

### 例 1 ：オブジェクトストレージの ILM ルールとポリシー

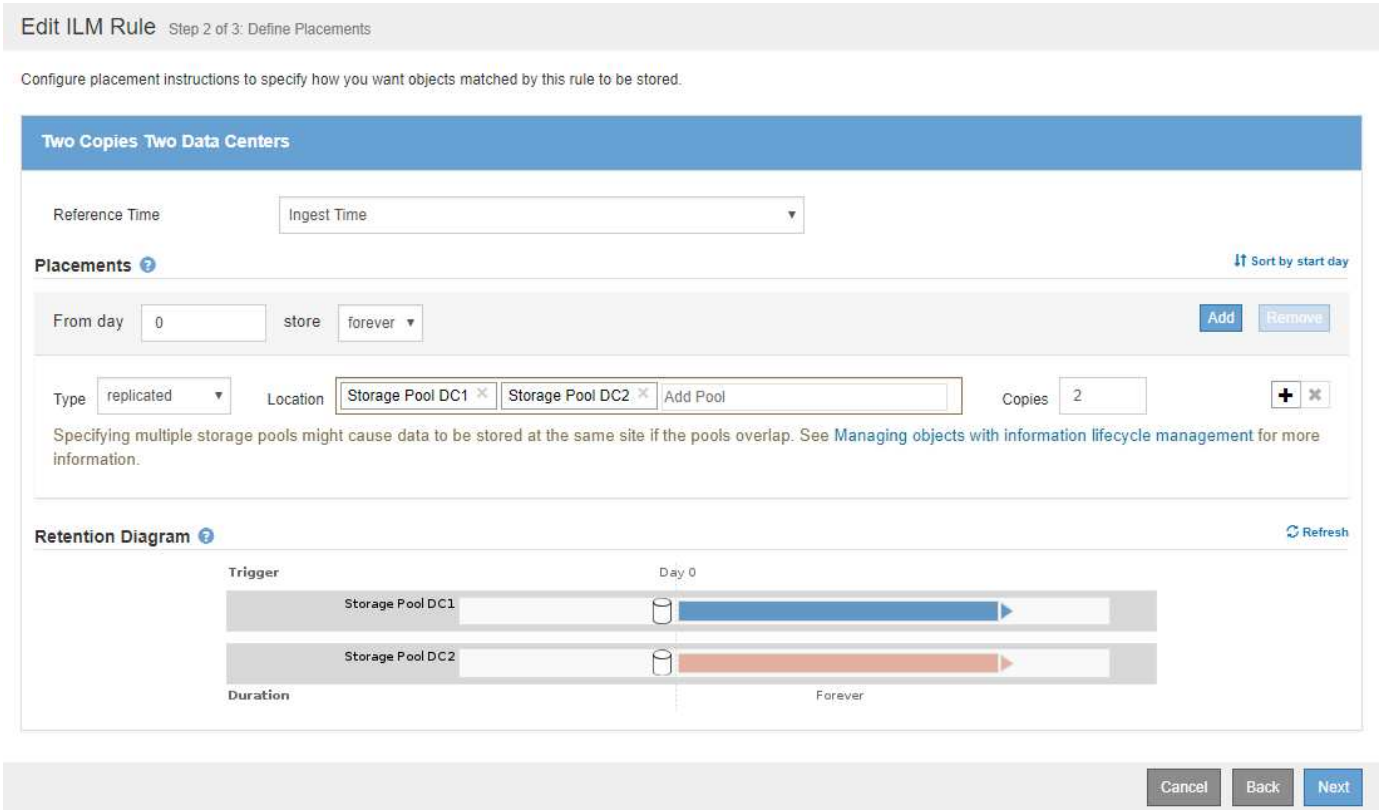
以下に記載するサンプルルールとポリシーをベースに、それぞれのオブジェクトの保護および保持要件を満たす ILM ポリシーを定義できます。

以下の ILM ルールとポリシーは一例にすぎません。ILM ルールを設定する方法は多数あります。新しいポリシーをアクティブ化する前に、ドラフトポリシーをシミュレートして、コンテンツの損失を防ぐためにドラフトポリシーが想定どおりに機能することを確認してください。

例 **1** の **ILM** ルール **1** ： **2** つのデータセンターへのオブジェクトデータのコピー

この ILM ルールの例では、 2 つのデータセンター内のストレージプールにオブジェクトデータをコピーします。

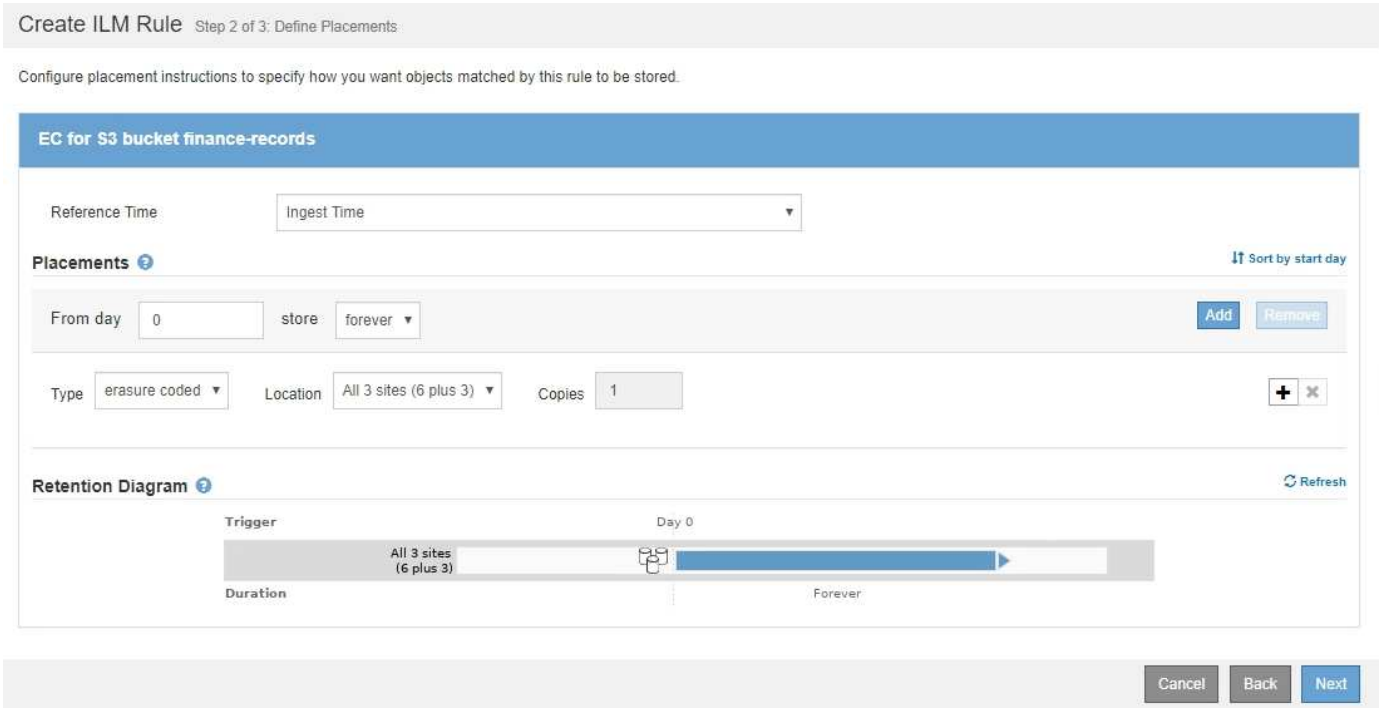
| ルール定義 | 値の例 |
| --- | --- |
| ストレージプール | 別々のデータセンターに 2 つのストレージプール、 Storage Pool DC1 および Storage Pool DC2 |
| ルール名 | 2 つのコピーで 2 つのデータセンターを構成し |
| 参照時間 | 取り込み時間 |
| コンテンツ配置 | 0 日目にレプリケートされたコピーを 2 つ無期限に保存 — Storage Pool DC1 に 1 つ、 Storage Pool DC2 に 1 つ。 |




例 **1** の **ILM** ルール **2** ：イレイジャーコーディングプロファイルとバケットの照合

この ILM ルールの例では、イレイジャーコーディングプロファイルと S3 バケットを使用して、オブジェクトの格納先と格納期間を決定します。

| ルール定義 | 値の例 |
| --- | --- |
| イレイジャーコーディングプロファイル | • 3 つのデータセンター（ 3 つすべてのサイト）にまたがる 1 つのストレージプール<br>• 6+3 イレイジャーコーディングスキームを使用 |
| ルール名 | S3 バケット finance-records の EC |
| 参照時間 | 取り込み時間 |
| コンテンツ配置 | finance-records という名前の S3 バケット内のオブジェクトに対し、イレイジャーコーディングコピーをイレイジャーコーディングプロファイルで指定されたプールに 1 つ作成します。このコピーを無期限に保持します。 |

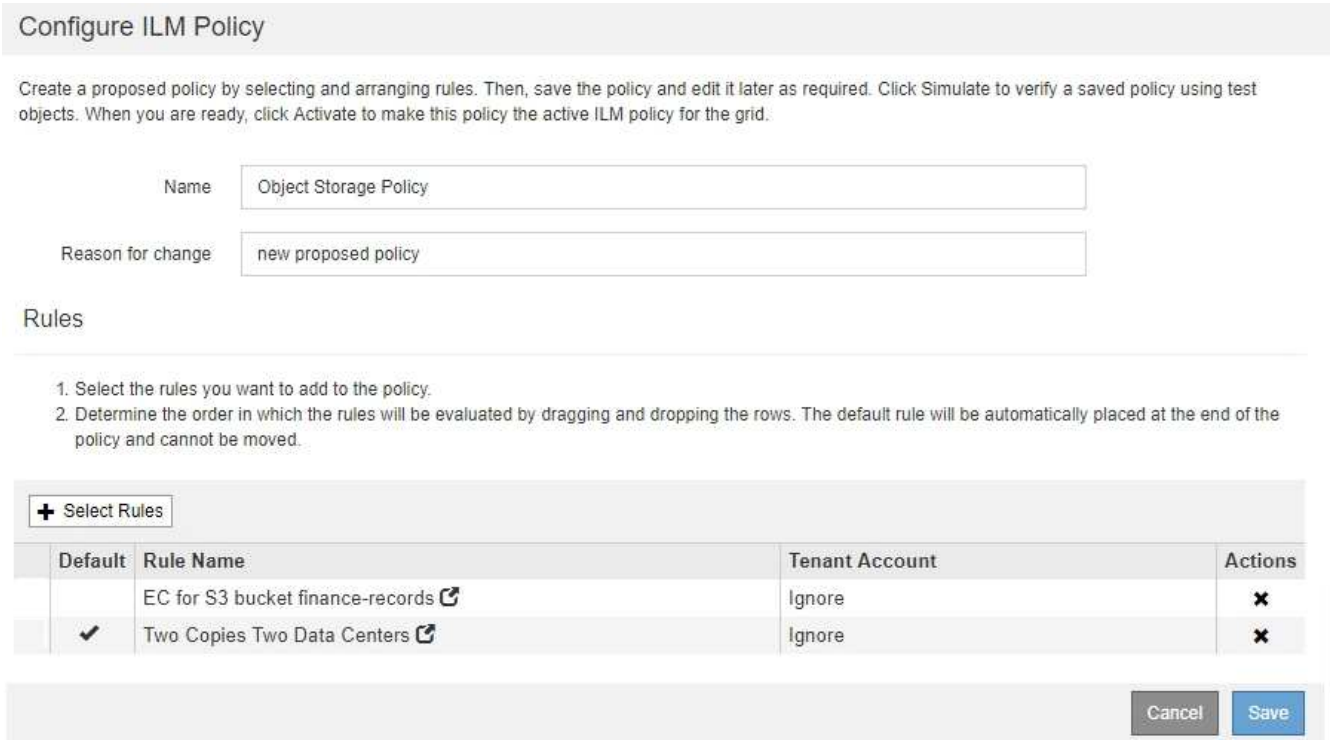



例 **1** の **ILM** ポリシー

StorageGRID システムでは、高度で複雑な ILM ポリシーを設計できますが、実際には、ほとんどの ILM ポリシーはシンプルです。

マルチサイトトポロジの一般的な ILM ポリシーには、次のような ILM ルールが含まれています。

- 取り込み時に、6+3イレイジャーコーディングを使用して、という名前のS3バケットに属するすべてのオブジェクトを格納します `finance-records` 3箇所のデータセンターに分散
- オブジェクトが最初の ILM ルールに一致しない場合は、ポリシーのデフォルトの ILM ルールである 2 つのデータセンターを使用して、 DC1 と DC2 の 2 つのデータセンターにそのオブジェクトのコピーを格納します。




例 **2** ： **EC** オブジェクトサイズのフィルタリング用の **ILM** ルールとポリシー

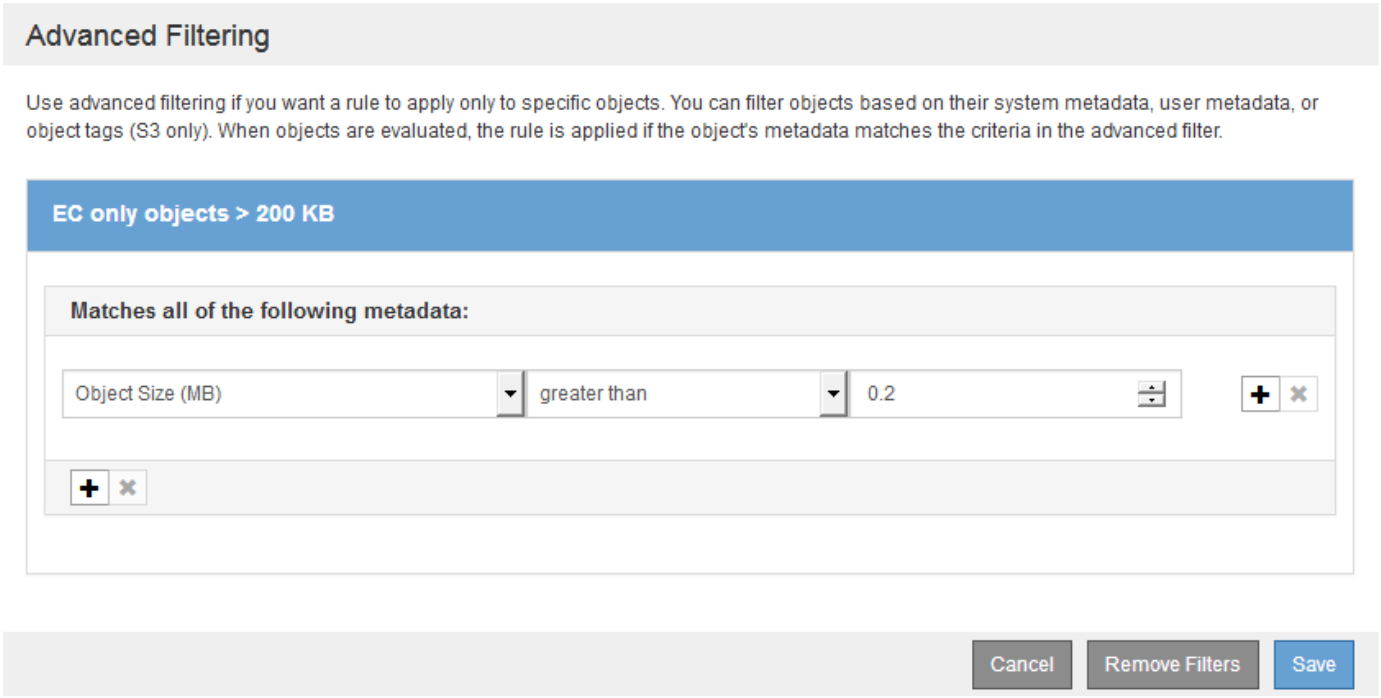
以下に記載するサンプルルールとポリシーをベースに、オブジェクトサイズでフィルタリングして EC の推奨要件を満たす ILM ポリシーを定義できます。

以下の ILM ルールとポリシーは一例にすぎません。ILM ルールを設定する方法は多数あります。新しいポリシーをアクティブ化する前に、ドラフトポリシーをシミュレートして、コンテンツの損失を防ぐためにドラフトポリシーが想定どおりに機能することを確認してください。

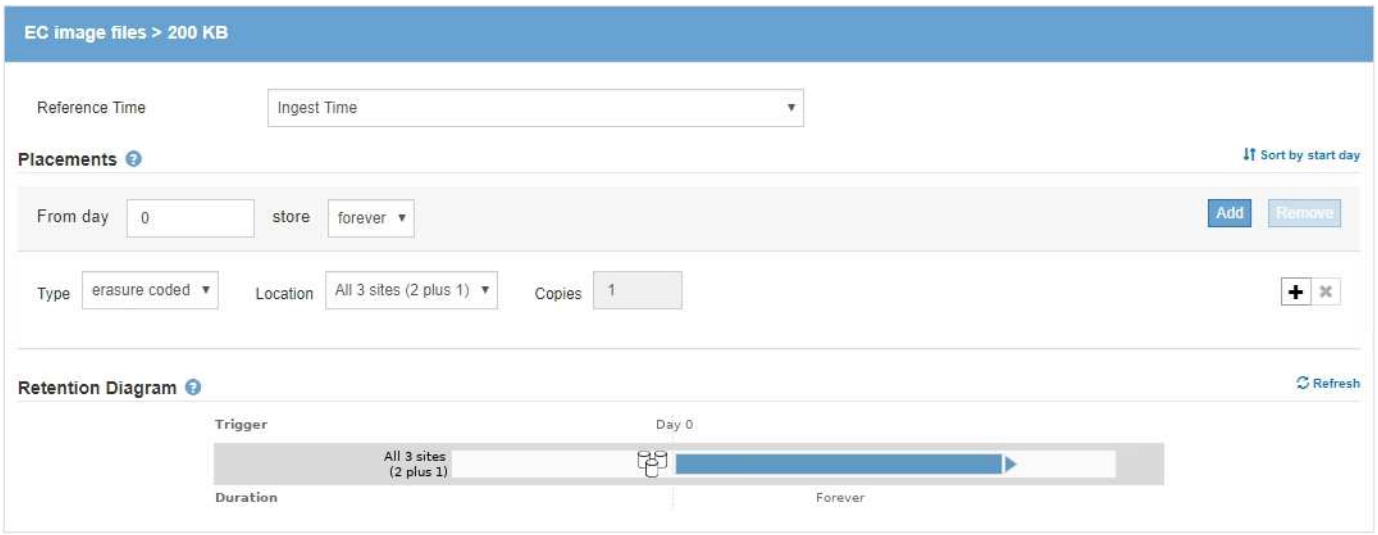
例**2**の**ILM**ルール**1**：**200KB**を超えるすべてのオブジェクトにイレイジャーコーディングを使用します

このILMルールの例では、200KB（0.20MB）を超えるすべてのオブジェクトをイレイジャーコーディングします。

| ルール定義 | 値の例 |
| --- | --- |
| ルール名 | ECのみのオブジェクト>200KB |
| 参照時間 | 取り込み時間 |
| オブジェクトサイズの高度なフィルタリング | オブジェクトサイズ（MB）が0.20より大きい |
| コンテンツ配置 | 3 つのサイトを使用して 2+1 のイレイジャーコーディングコピーを作成 |




配置手順は、3つのサイトすべてを使用して2+1のイレイジャーコーディングコピーを作成するように指定します。

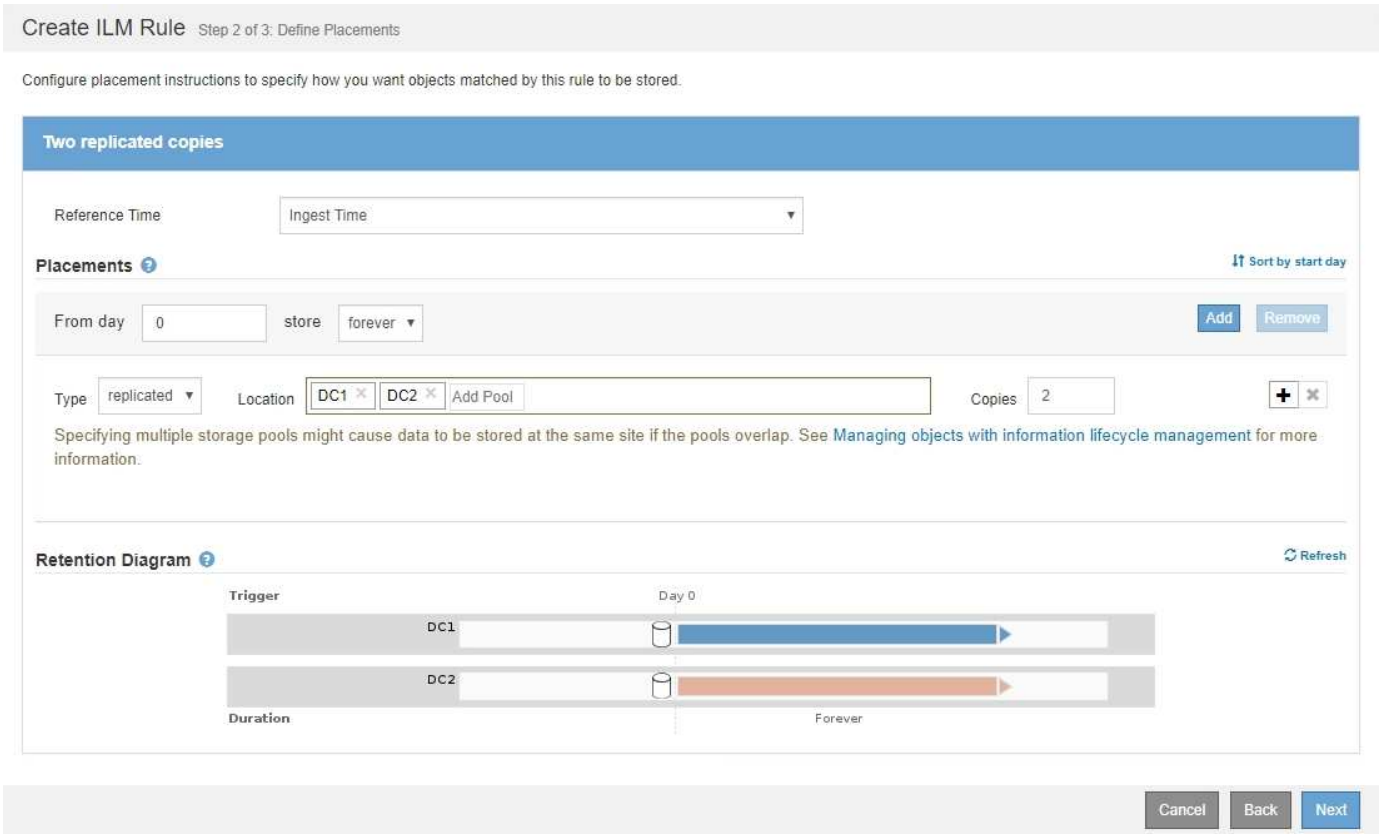



例 **2** の **ILM** ルール **2** ：レプリケートされたコピーを **2** つ

この ILM ルールの例では、レプリケートコピーを 2 つ作成し、オブジェクトサイズではフィルタリングしません。このルールはポリシー内の2番目のルールです。例2のILMルール1が200KBを超えるすべてのオブジェクトを除外するため、例2のILMルール2は200KB以下の環境 オブジェクトのみを除外します。

| ルール定義 | 値の例 |
| --- | --- |
| ルール名 | 2 つのレプリケートコピー |
| 参照時間 | 取り込み時間 |

| ルール定義 | 値の例 |
| --- | --- |
| オブジェクトサイズの高度なフィルタリング | なし |
| コンテンツ配置 | レプリケートコピーを 2 つ作成して、 DC1 と DC2 の 2 つのデータセンターに保存します |

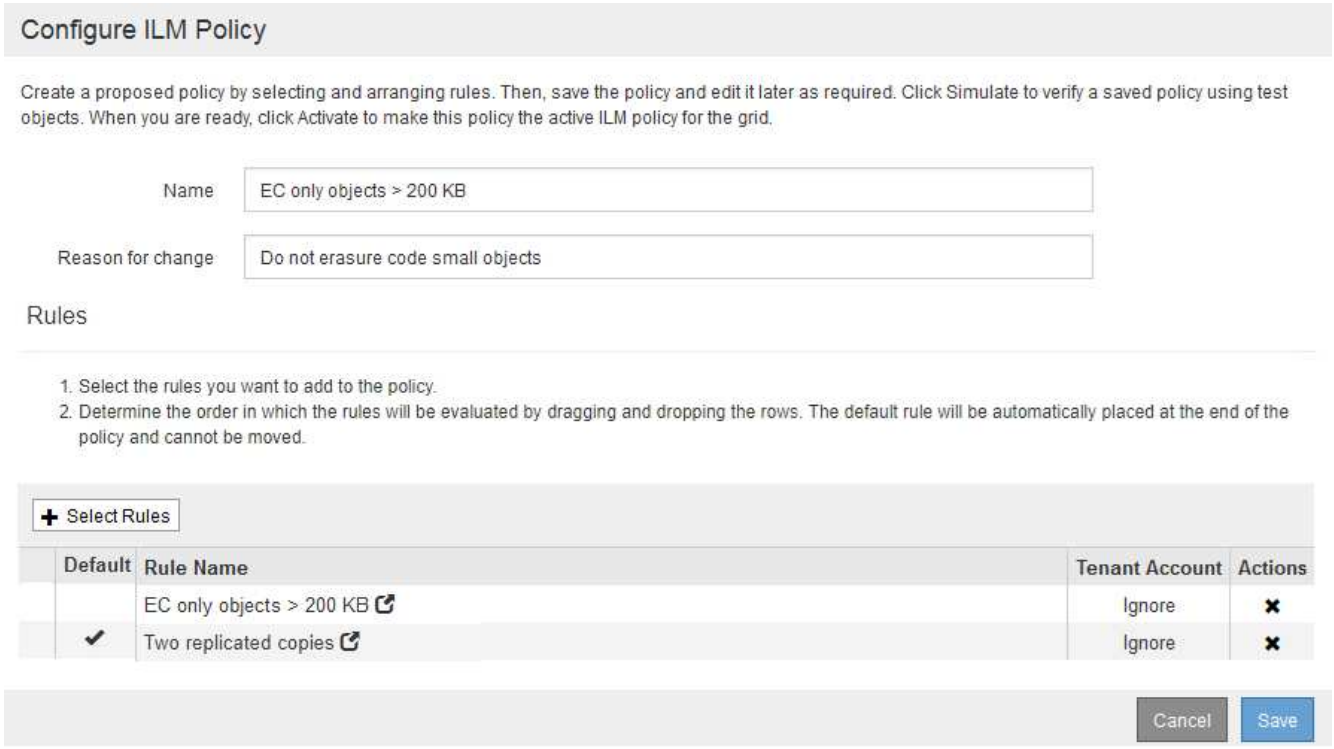



例2のILMポリシー：200KBを超えるオブジェクトにイレイジャーコーディングを使用

このポリシーの例では、200KBを超えるオブジェクトがイレイジャーコーディングされます。他のすべてのオブジェクトから2つのレプリケートコピーが作成されます。

この例のILMポリシーには、次のILMルールが含まれています。

- 200KBを超えるすべてのオブジェクトをイレイジャーコーディングします。
- オブジェクトが最初のILMルールに一致しない場合は、デフォルトのILMルールを使用して、そのオブジェクトのレプリケートコピーを2つ作成します。200KBを超えるオブジェクトはルール1で除外されているため、ルール2では200KB以下の環境 オブジェクトのみが除外されます。




例 **3** ：画像ファイルの保護を強化する **ILM** ルールとポリシー

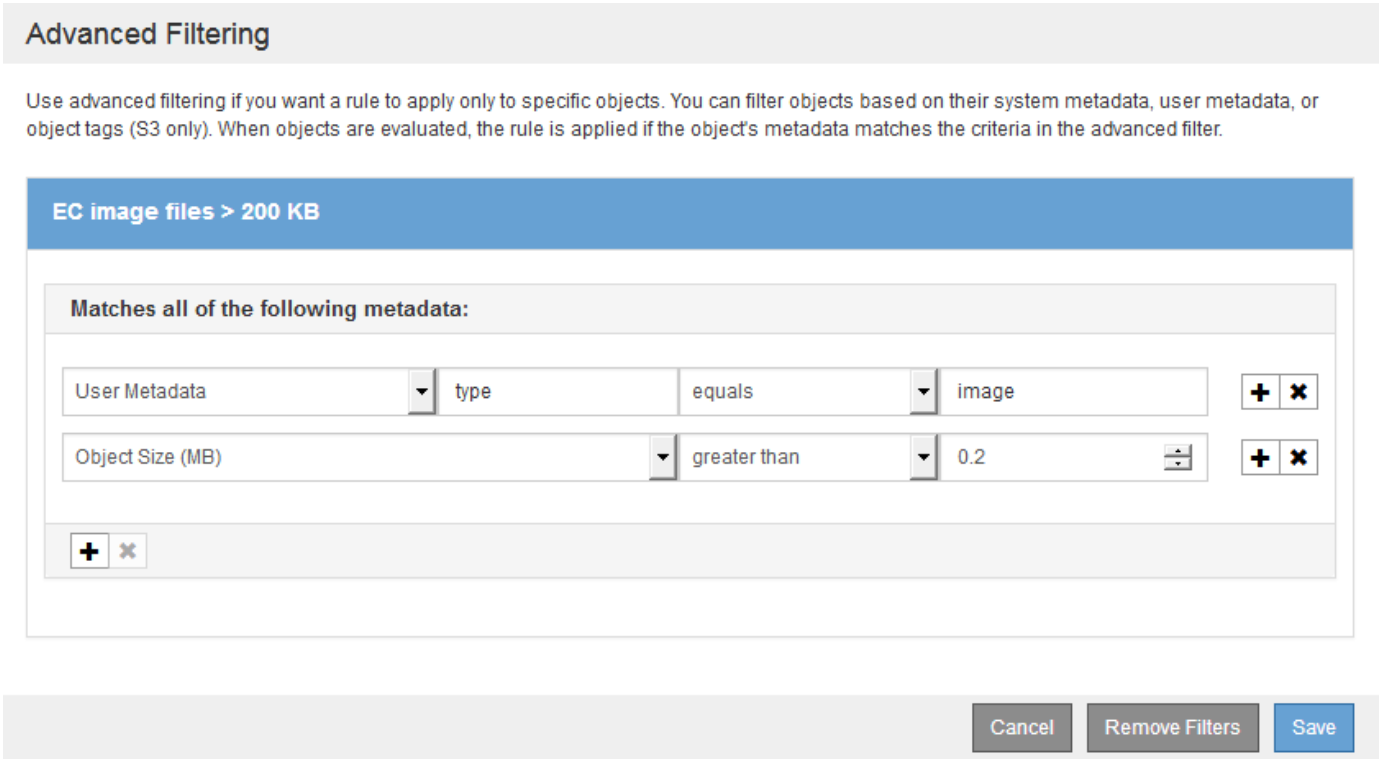
## 以下に記載するサンプルルールとポリシーを使用して、200KBを超える画像をイレイジャーコーディングし、200KB以下の画像からコピーを3つ作成できます。

以下の ILM ルールとポリシーは一例にすぎません。ILM ルールを設定する方法は多数あります。新しいポリシーをアクティブ化する前に、ドラフトポリシーをシミュレートして、コンテンツの損失を防ぐためにドラフトポリシーが想定どおりに機能することを確認してください。

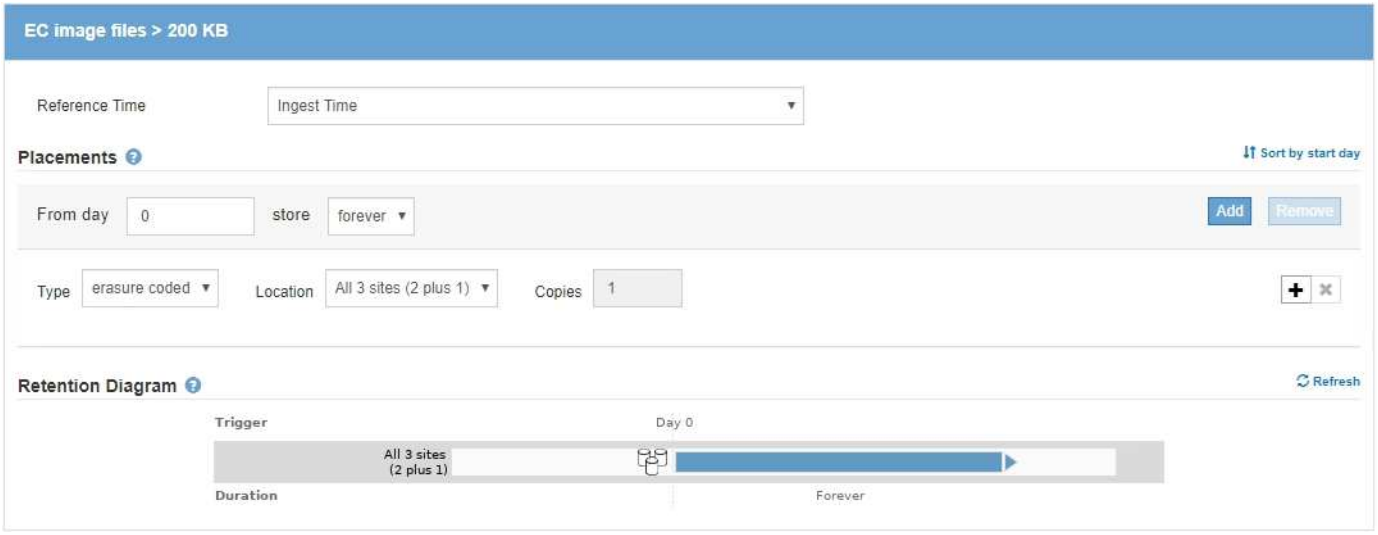
例**3**の**ILM**ルール**1**：**200KB**を超える画像ファイルにイレイジャーコーディングを使用

このILMルールの例では、高度なフィルタリングを使用して、200KBを超えるすべての画像ファイルをイレイジャーコーディングします。

| ルール定義 | 値の例 |
| --- | --- |
| ルール名 | ECイメージファイル>200KB |
| 参照時間 | 取り込み時間 |
| ユーザメタデータの高度なフィルタリング | ユーザメタデータタイプはイメージファイルと同じです |
| オブジェクトサイズの高度なフィルタリング | オブジェクトサイズ（MB）が0.2より大きい |
| コンテンツ配置 | 3 つのサイトを使用して 2+1 のイレイジャーコーディングコピーを作成 |




このルールはポリシー内の最初のルールとして設定されているため、イレイジャーコーディングの配置手順では200KBを超える環境 イメージのみが使用されます。

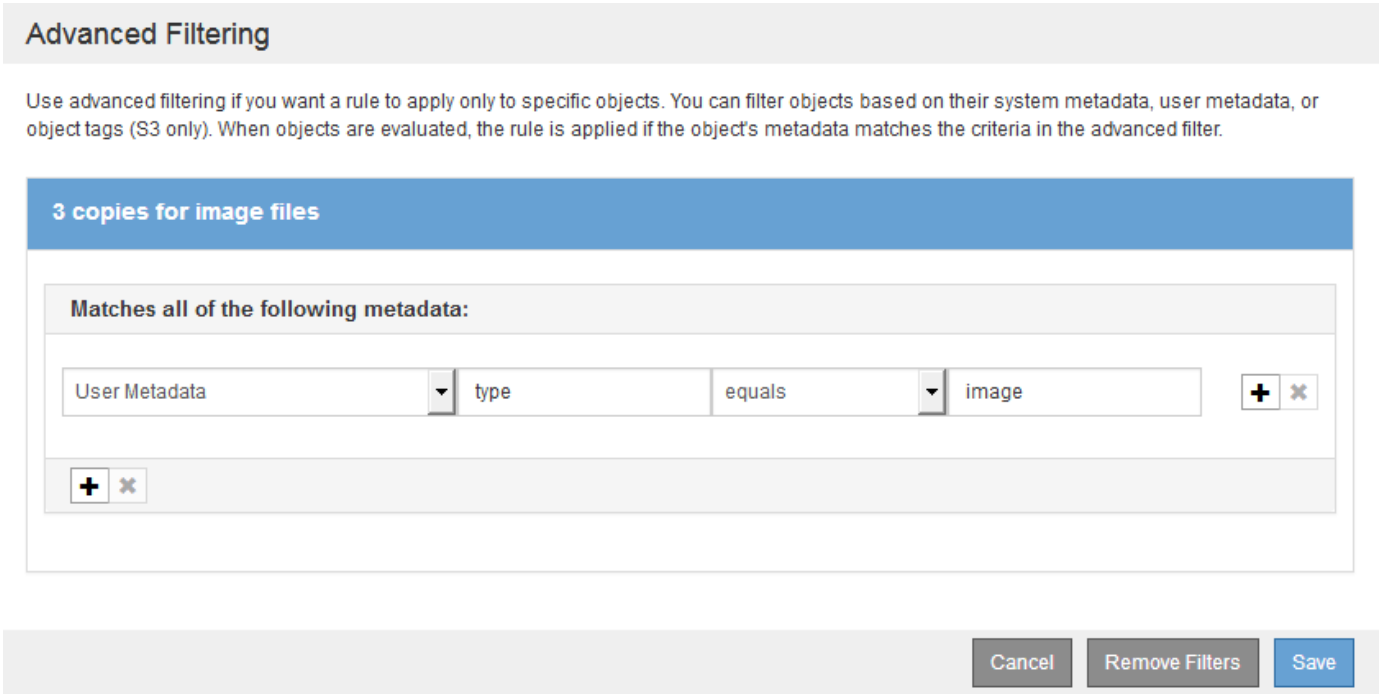



例3のILMルール2：残りのすべてのイメージファイルのコピーを3つレプリケートします

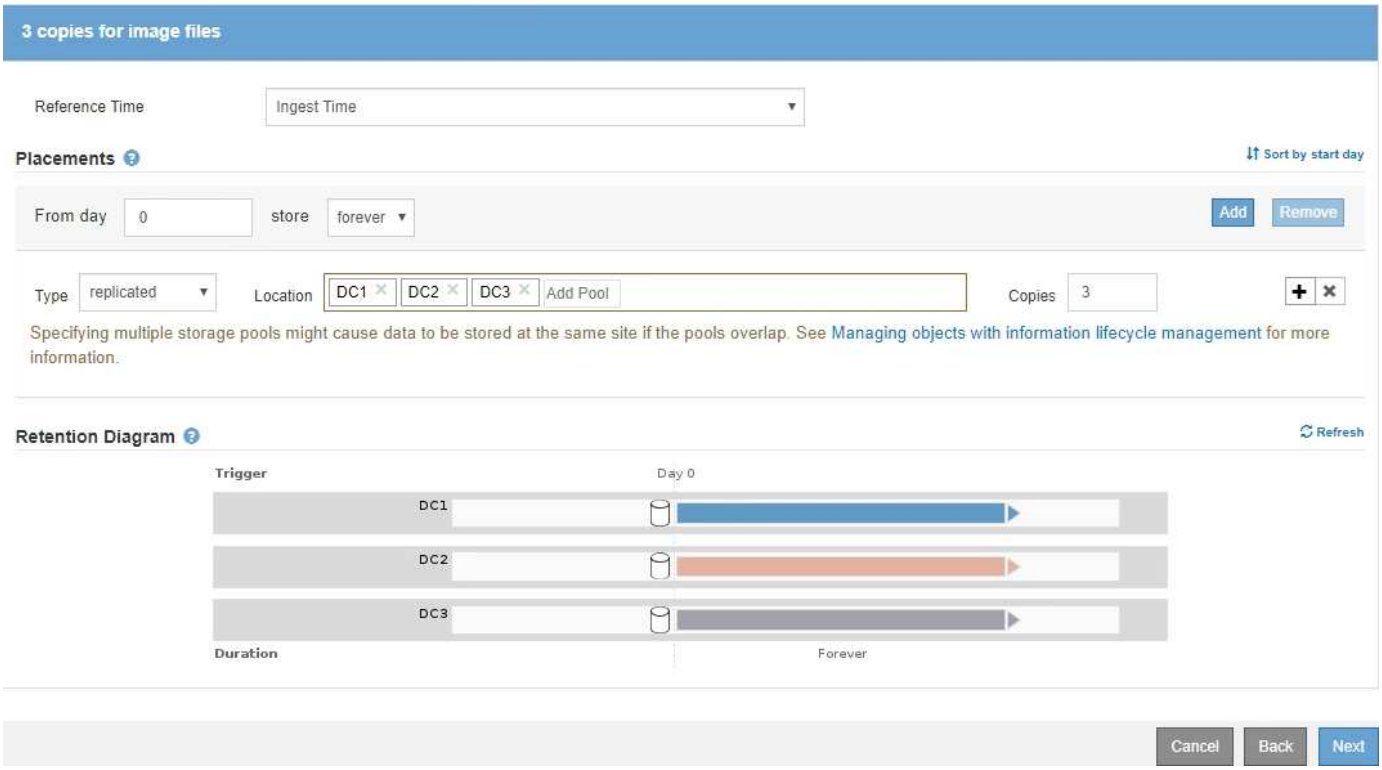
このILMルールの例では、高度なフィルタリングを使用して、イメージファイルをレプリケートするように指定します。

| ルール定義 | 値の例 |
| --- | --- |
| ルール名 | 画像ファイル用に3つのコピー |
| 参照時間 | 取り込み時間 |

| ルール定義 | 値の例 |
| --- | --- |
| ユーザメタデータの高度なフィルタリング | ユーザメタデータタイプはイメージファイルと同じです |
| コンテンツ配置 | レプリケートされたコピーをすべてのストレージノードに3つ作成します |




ポリシー内の最初のルールは200KBを超える画像ファイルにすでに一致しているため、この配置手順は200KB以下の画像ファイルにのみ適用されます。

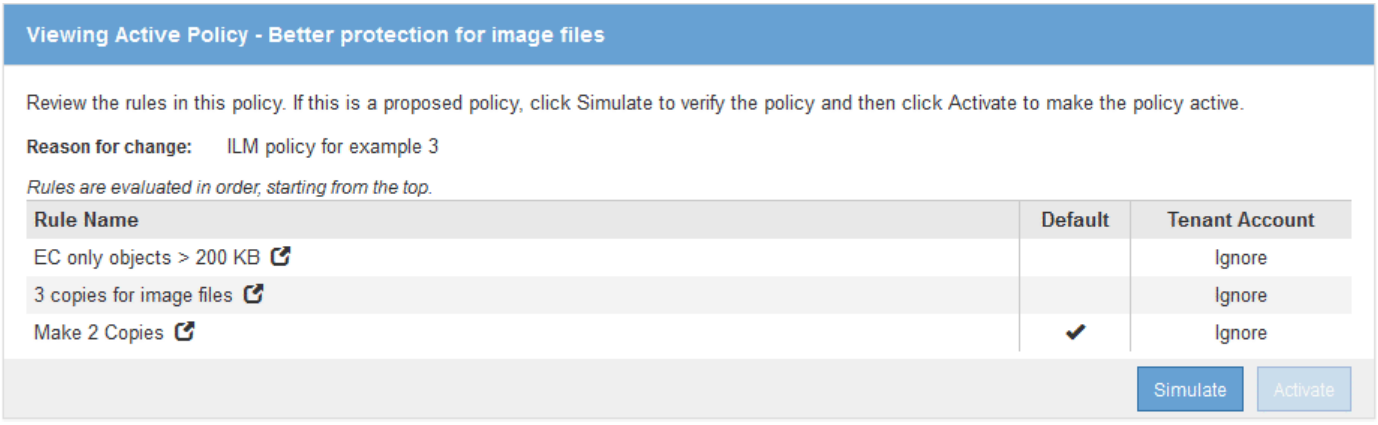



例 **3** の **ILM** ポリシー：画像ファイルの保護の強化

この例では、ILMポリシーで3つのILMルールを使用して、200KB（0.2MB）を超える画像ファイルをイレイジャーコーディングし、200KB以下の画像ファイルのレプリケートコピーを作成し、画像以外のファイルについては2つのレプリケートコピーを作成するポリシーを作成します。

この例のILMポリシーには、次の処理を実行するルールが含まれています。

- 200KBを超えるすべての画像ファイルをイレイジャーコーディングします。
- 残りの（200KB以下の）画像ファイルのコピーを3つ作成します。
- 残りのすべてのオブジェクト（つまり、すべての非イメージファイル）にデフォルトルールを適用します。




例 **4** ： **S3** バージョン管理オブジェクトの **ILM** ルールとポリシー

バージョン管理が有効になっている S3 バケットがある場合は、参照時間として *

## noncurrent time * を使用する ILM ポリシーにルールを含めることで、最新でないオブジェクトバージョンを管理できます。

この例に示すように、バージョン管理オブジェクトで使用されるストレージの量を制御するには、最新でないオブジェクトバージョンに別々の配置手順を使用します。

以下の ILM ルールとポリシーは一例にすぎません。ILM ルールを設定する方法は多数あります。新しいポリシーをアクティブ化する前に、ドラフトポリシーをシミュレートして、コンテンツの損失を防ぐためにドラフトポリシーが想定どおりに機能することを確認してください。

最新でないオブジェクトバージョンを管理するための ILM ポリシーを作成する場合は、ポリシーをシミュレートするためにオブジェクトバージョンの UUID または CBID が必要です。オブジェクトの UUID と CBID を確認するには、オブジェクトが最新の間にオブジェクトメタデータを検索します。

関連情報

"S3 バージョン管理オブジェクトの削除方法"

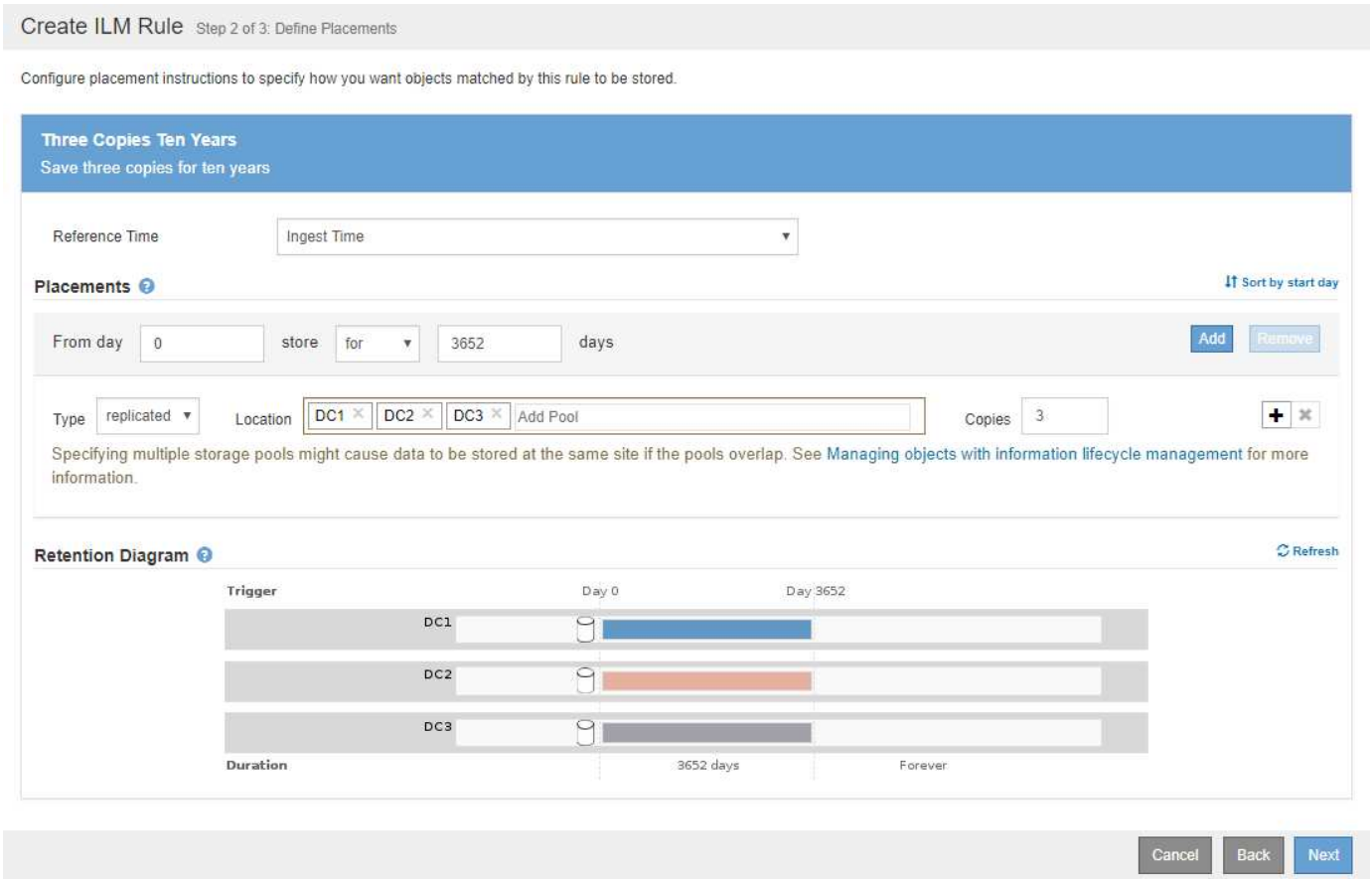
"オブジェクトメタデータの検索によるILMポリシーの検証"

### 例 4 の ILM ルール 1 ：コピーを 3 つ、 10 年間保存します

この例では、 3 つのデータセンターに各オブジェクトのコピーを 10 年間格納します。

このルールは、オブジェクトがバージョン管理されているかどうかに関係なく、すべてのオブジェクトを環境します。

| ルール定義 | 値の例 |
| --- | --- |
| ストレージプール | 別々のデータセンターにある 3 つのストレージプール、 DC1 、 DC2 、 DC3 。 |
| ルール名 | 3 つのコピー 10 年 |
| 参照時間 | 取り込み時間 |
| コンテンツ配置 | 0 日目から、 3 つのレプリケートコピーを 10 年間（ 3 、 652 日）格納（ DC1 、 DC2 、 DC3 に 1 つずつ）。10 年後にオブジェクトのコピーをすべて削除する。 |



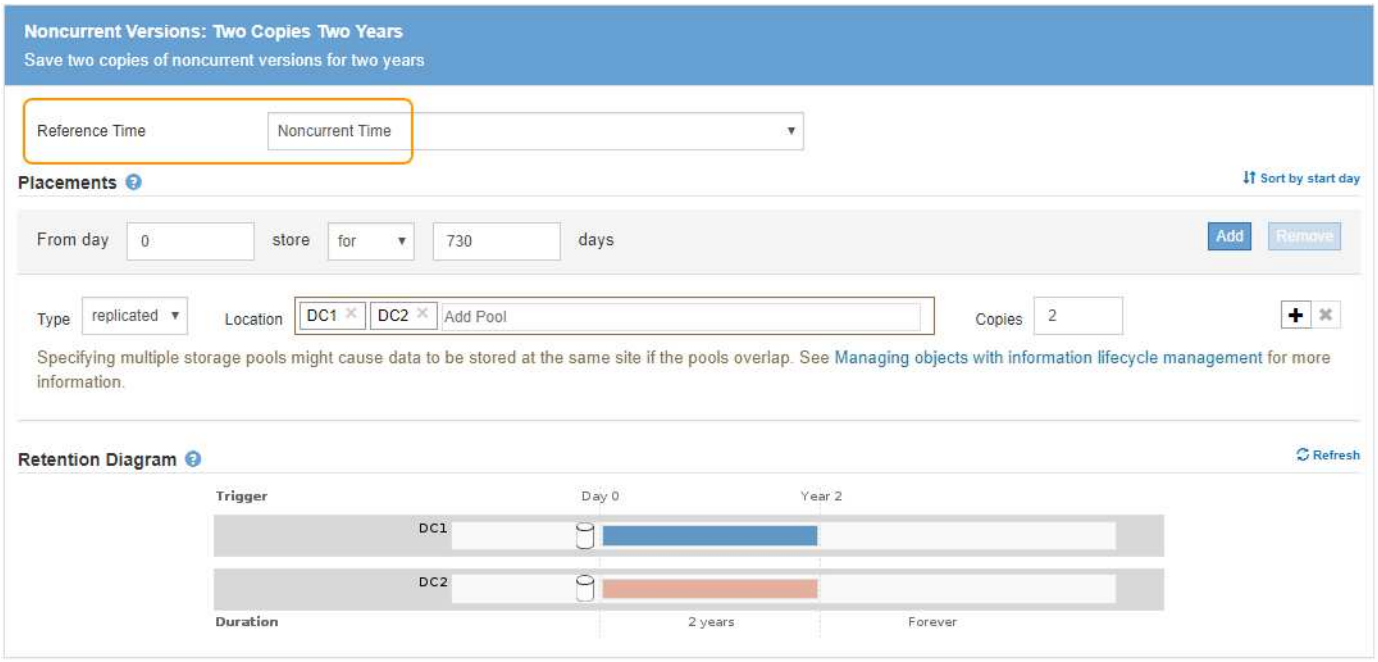

例 **4** の **ILM** ルール **2** ：最新でないバージョンのコピーを **2** つ、 **2** 年間保存します

この例では、最新でないバージョンの S3 バージョン管理オブジェクトのコピーを 2 つ、 2 年間格納します。

ILM ルール 1 ではすべてのバージョンのオブジェクトが環境 されるため、最新でないバージョンをすべて除外する別のルールを作成する必要があります。このルールでは、参照時間に * noncurrent Time * オプションを使用します。

この例では、最新でないバージョンのコピーが 2 つだけ格納され、その期間は 2 年間です。

| ルール定義 | 値の例 |
| --- | --- |
| ストレージプール | 別々のデータセンターにある 2 つのストレージプール、 DC1 および DC2 |
| ルール名 | 最新でないバージョン： 2 コピー 2 年 |
| 参照時間 | 最新でなくなった時間 |
| コンテンツ配置 | 0 日目から最新でない時間（オブジェクトバージョンが最新でないバージョンになる日から）を基準に、最新でないオブジェクトバージョンのレプリケートコピーを 2 つ（ 730 日）保持し、 DC1 と DC2 に 1 つずつ保持します。2 年後に最新でないバージョンを削除します。 |




例 **4** の **ILM** ポリシー： **S3** バージョン管理オブジェクト

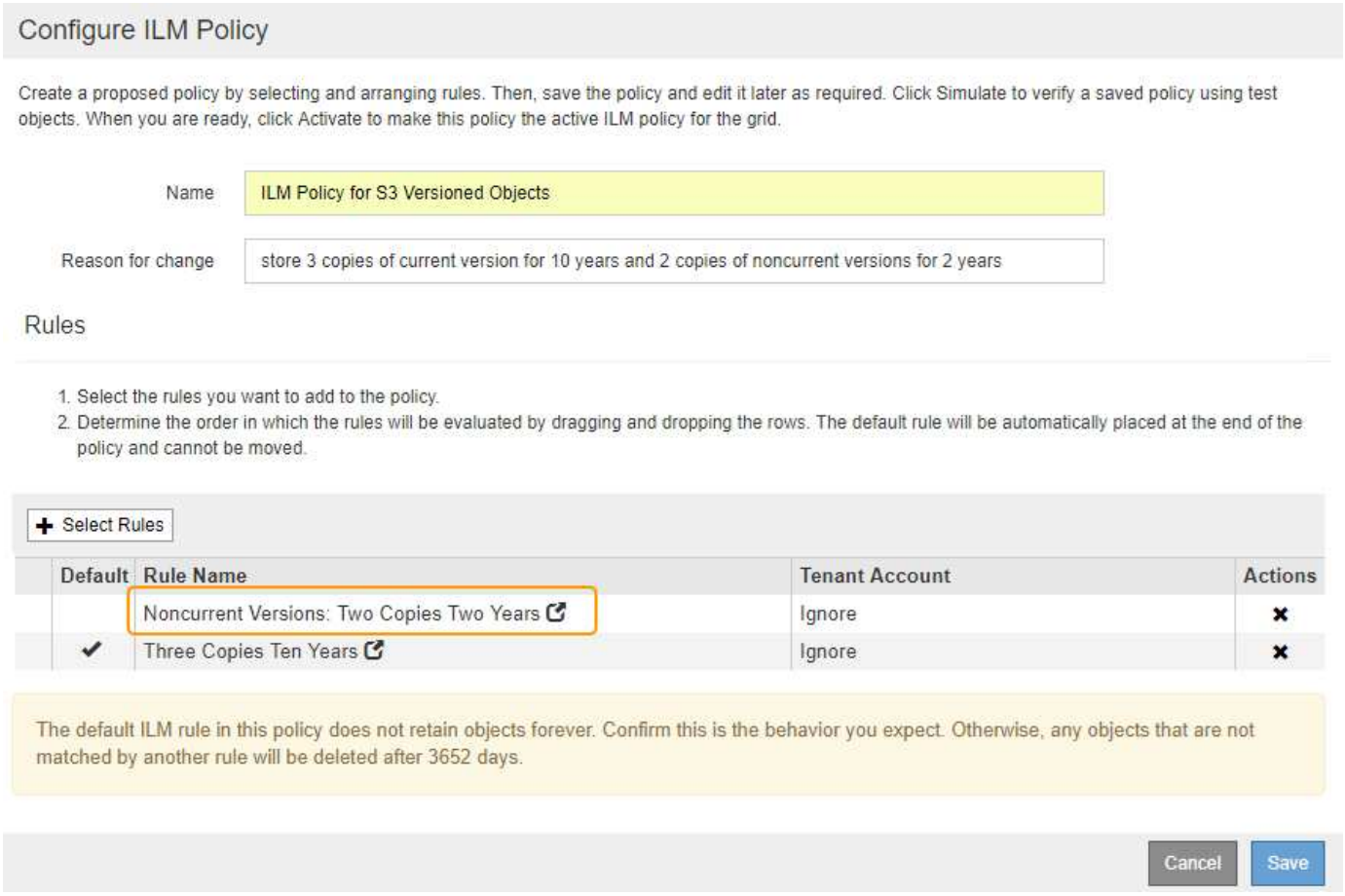
最新バージョンとは異なる古いバージョンのオブジェクトを管理する場合は、現在のオブジェクトバージョンに適用されるルールを開始する前に、参照時間として * noncurrent Time * を使用するルールを ILM ポリシーに含める必要があります。

S3 バージョン管理オブジェクトの ILM ポリシーには、次のような ILM ルールが含まれます。

- 古い（最新でない）バージョンの各オブジェクトを、そのバージョンが最新でなくなった日から 2 年間保持します。

> 最新でない時間ルールは、現在のオブジェクトバージョンに適用されるルールより前にポリシーに表示される必要があります。それ以外の場合、最新でないオブジェクトバージョンは noncurrent Time ルールに一致しません。

- 取り込み時に、レプリケートコピーを 3 つ作成して、 3 つのデータセンターに 1 つずつ格納します。最新のオブジェクトバージョンのコピーを 10 年間保持します。




この例のポリシーをシミュレートすると、テストオブジェクトは次のように評価されます。

- 最新でないオブジェクトバージョンがすべて最初のルールに一致します。最新でないオブジェクトバージョンが 2 年以上経過している場合は、 ILM によって完全に削除されます（最新でないバージョンのコピーがすべてグリッドから削除されます）。

> 最新でないオブジェクトバージョンをシミュレートするには、そのバージョンの UUID または CBID を使用する必要があります。オブジェクトが最新の間であれば、 Object Metadata Lookup を使用して UUID と CBID を検索できます。

- 現在のオブジェクトバージョンが 2 つ目のルールに一致します。最新のオブジェクトバージョンが 10 年間保存されると 'ILM プロセスはオブジェクトの最新バージョンとして削除マーカーを追加し ' 以前のオブジェクトバージョンを「 noncurrent 」にします 次回の ILM 評価では、この最新でないバージョンは最初のルールに一致します。その結果、 DC3 にあるコピーがパージされ、 DC1 と DC2 にある 2 つのコピーがさらに 2 年間格納されます。

関連情報

"オブジェクトメタデータの検索によるILMポリシーの検証"

例 **5** ：取り込み動作が **Strict** の場合の **ILM** ルールとポリシー

## ルールで場所フィルタと Strict 取り込み動作を使用すると、特定のデータセンターの場所にオブジェクトが保存されないようにすることができます。

この例では、規制上の問題により、パリベースのテナントは EU の外部に一部のオブジェクトを格納しないよ

うにしています。他のテナントアカウントのすべてのオブジェクトを含むその他のオブジェクトは、パリデータセンターまたは米国のデータセンターに格納できます。

以下の ILM ルールとポリシーは一例にすぎません。ILM ルールを設定する方法は多数あります。新しいポリシーをアクティブ化する前に、ドラフトポリシーをシミュレートして、コンテンツの損失を防ぐためにドラフトポリシーが想定どおりに機能することを確認してください。

関連情報

"オブジェクトの取り込み方法"

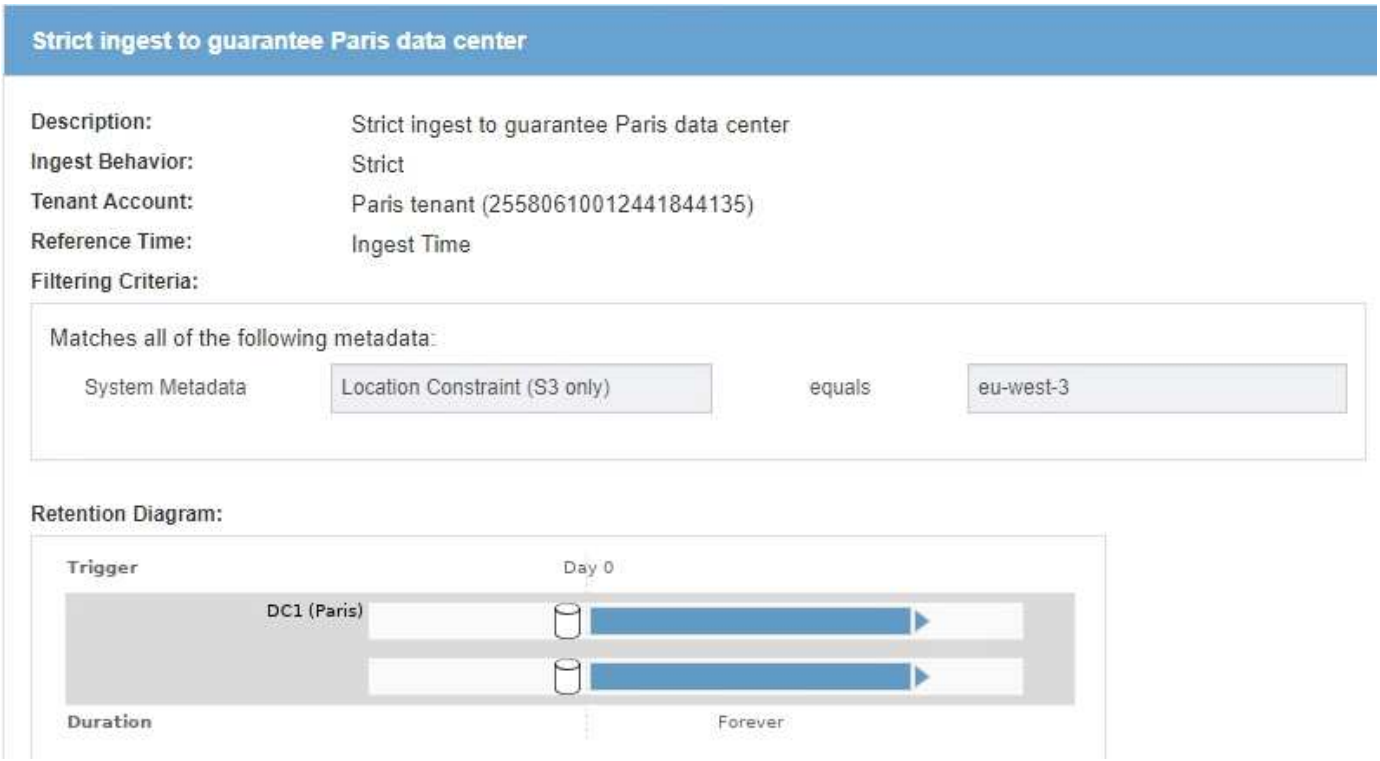
"ステップ 3 / 3 ：取り込み動作を定義する"

例 **5** の **ILM** ルール **1** ：パリデータセンターを確保するための **Strict** 取り込み

この ILM ルールの例では Strict 取り込み動作を使用して、パリベースのテナントによって S3 バケットに保存されたオブジェクトのリージョンが eu-west-3 リージョン（パリ）に設定されたものが米国のデータセンターに格納されないようにします。

このルールは、パリテナントに属し、 S3 バケットリージョンが eu-west-3 （パリ）に設定されている環境 オブジェクトを示します。

| ルール定義 | 値の例 |
| --- | --- |
| テナントアカウント | パリのテナント |
| 高度なフィルタリング | 場所制約は eu-west-3 に相当します |
| ストレージプール | DC1 （パリ） |
| ルール名 | 厳格な取り込みにより、パリのデータセンターを保証します |
| 参照時間 | 取り込み時間 |
| コンテンツ配置 | 0 日目から、 2 つのレプリケートコピーを DC1 （パリ）に保存 |
| 取り込み動作 | strict 。取り込み時に必ずこのルールの配置手順を使用してください。パリデータセンターにオブジェクトのコピーを 2 つ保存できない場合、取り込みは失敗します。 |




例 **5** の **ILM** ルール **2** ：他のオブジェクトに対してバランスのとれた取り込み

この ILM ルールの例では、 Balanced 取り込み動作を使用して、最初のルールに一致しないオブジェクトの ILM 効率が最適化されます。このルールに一致するすべてのオブジェクトのコピーが 2 つ保存されます。 1 つは米国データセンターに、もう 1 つはパリデータセンターに格納されます。ルールをすぐに完了できない場合は、使用可能な任意の場所に中間コピーが格納されます。

このルールは、任意のテナントおよびすべてのリージョンに属する環境 オブジェクトを対象としています。

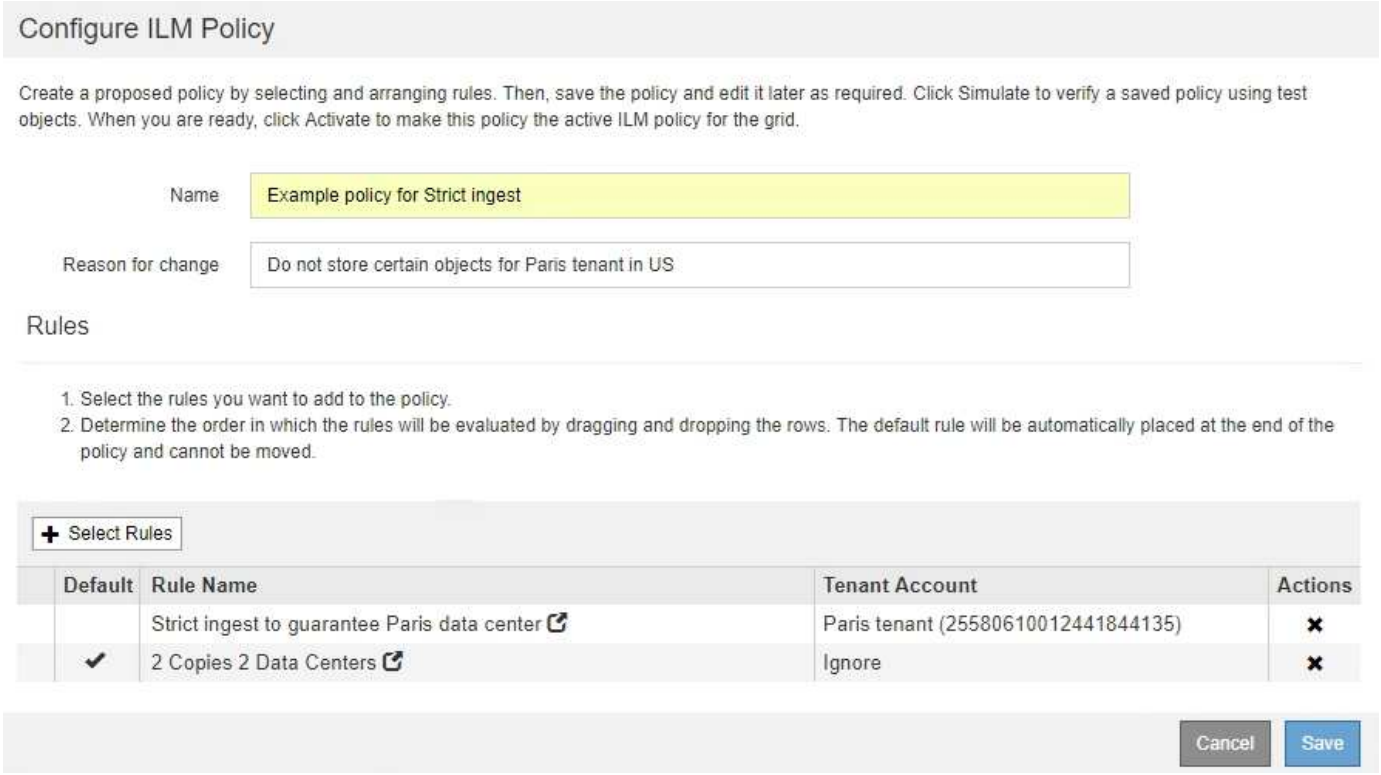
| ルール定義 | 値の例 |
| --- | --- |
| テナントアカウント | 無視します |
| 高度なフィルタリング | _ 指定されていません _ |
| ストレージプール | DC1 （パリ）および DC2 （米国） |
| ルール名 | 2 つのコピーで 2 つのデータセンター |
| 参照時間 | 取り込み時間 |
| コンテンツ配置 | 0 日目から、 2 つのレプリケートコピーを 2 つのデータセンターに無期限に格納します |
| 取り込み動作 | 中間（ Balanced ）：このルールに一致するオブジェクトは、可能であればルールの配置手順に従って配置されます。それ以外の場合、中間コピーは任意の空き場所で作成されます。 |

例 **5** の **ILM** ポリシー：取り込み動作を組み合わせたもの

この例の ILM ポリシーには、取り込み動作が異なる 2 つのルールが含まれています。

2 つの異なる取り込み動作を使用する ILM ポリシーには、次のような ILM ルールが含まれる場合があります。

- パリのテナントに属し、かつ S3 バケットリージョンがパリのデータセンター内でのみ eu-west-3 （パリ）に設定されているオブジェクトを格納します。パリのデータセンターが利用できない場合は取り込みに失敗します。
- その他のすべてのオブジェクト（パリテナントに属しているものの、バケットリージョンが異なるオブジェクトを含む）は、米国のデータセンターとパリのデータセンターの両方に保存します。配置手順を満たすことができない場合は、使用可能な任意の場所に中間コピーを作成します。




この例のポリシーをシミュレートすると、テストオブジェクトは次のように評価されます。

- パリのテナントに属し、 S3 バケットリージョンが eu-west-3 に設定されているオブジェクトはすべて最初のルールに一致し、パリのデータセンターに格納されます。最初のルールでは Strict 取り込みが使用されるため、これらのオブジェクトが米国のデータセンターに格納されることはありません。パリデータセンターのストレージノードを使用できない場合、取り込みは失敗します。
- 他のすべてのオブジェクトは、パリテナントに属するオブジェクトや S3 バケットリージョンが eu-west-3 に設定されていないオブジェクトを含む 2 番目のルールに一致します。各オブジェクトのコピーが各データセンターに 1 つずつ保存されます。ただし、 2 つ目のルールでは Balanced ing( バランスの取れた取り込み ) が使用されるため、 1 つのデータセンターが使用できない場合は、使用可能な任意の場所に 2 つの中間コピーが保存されます。

例 **6** ： **ILM** ポリシーを変更する

## データ保護のニーズが変わった場合や新しいサイトを追加した場合は、新しい ILM ポリシーの作成とアクティブ化が必要になることがあります。

ポリシーを変更する前に、 ILM の配置変更が一時的に StorageGRID システムの全体的なパフォーマンスに及ぼす影響について理解しておく必要があります。

この例では、拡張時に新しい StorageGRID サイトが追加され、新しいサイトにデータを格納するためにアクティブな ILM ポリシーを変更する必要があります。

以下の ILM ルールとポリシーは一例にすぎません。ILM ルールを設定する方法は多数あります。新しいポリシーをアクティブ化する前に、ドラフトポリシーをシミュレートして、コンテンツの損失を防ぐためにドラフトポリシーが想定どおりに機能することを確認してください。

### ILM ポリシーの変更がパフォーマンスに与える影響

新しい ILM ポリシーをアクティブ化すると、特に新しいポリシーの配置手順で多数の既存オブジェクトの新しい場所への移動が必要になった場合には、 StorageGRID システムのパフォーマンスに一時的に影響する可能性があります。

> 新しい ILM ポリシーをアクティブ化すると、 StorageGRID は、そのポリシーを使用して、既存のオブジェクトと新たに取り込まれたオブジェクトを含むすべてのオブジェクトを管理します。新しい ILM ポリシーをアクティブ化する前に、既存のレプリケートオブジェクトとイレイジャーコーディングオブジェクトの配置に対する変更を確認してください。既存のオブジェクトの場所を変更すると、新しい配置が評価されて実装される際に一時的なリソースの問題が発生する可能性があります。

StorageGRID のパフォーマンスに一時的に影響する可能性がある ILM ポリシーの変更には、次のようなものがあります。

- 既存のイレイジャーコーディングオブジェクトへの別のイレイジャーコーディングプロファイルの適用

> StorageGRID では、各イレイジャーコーディングプロファイルは一意とみなされ、新しいプロファイルを使用する場合はイレイジャーコーディングフラグメントが再利用されません。

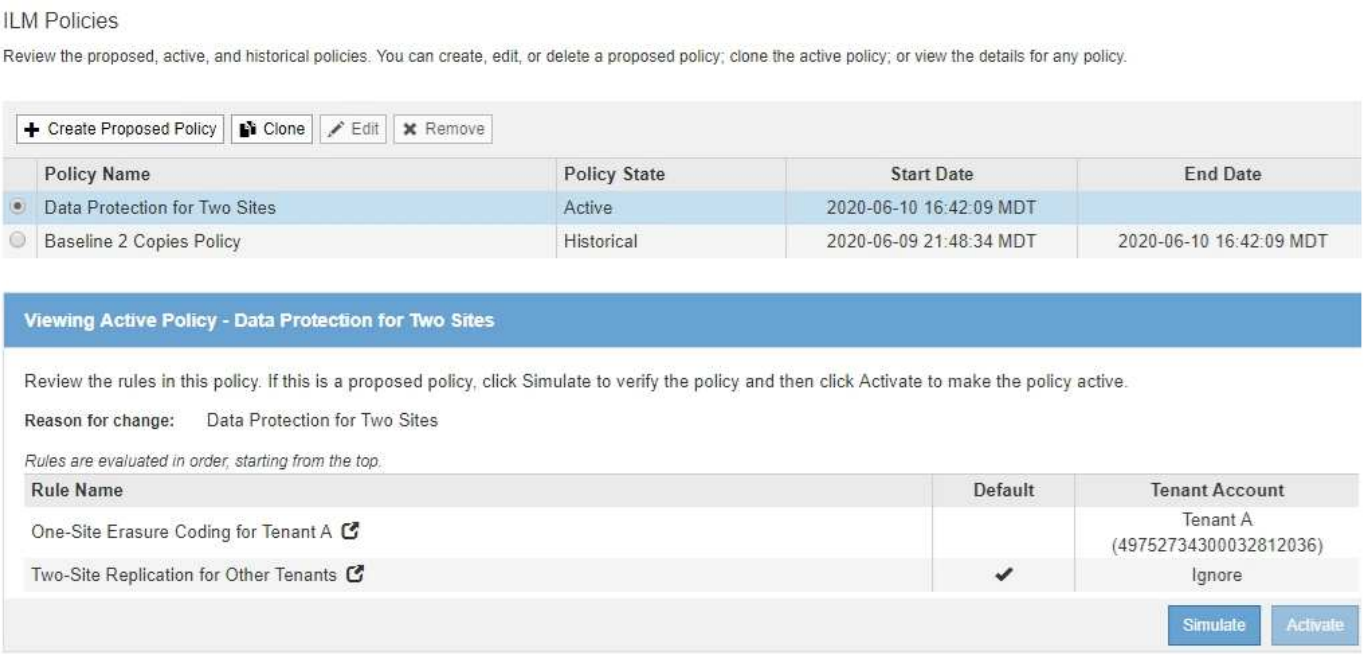
- 既存のオブジェクトに必要なコピーのタイプを変更する。たとえば、大部分のレプリケートオブジェクトをイレイジャーコーディングオブジェクトに変換する場合などです。
- 既存のオブジェクトのコピーをまったく別の場所に移動する。たとえば、クラウドストレージプールとリモートサイトの間で多数のオブジェクトを移動する場合などです。

関連情報

"ILMポリシーを作成する"

#### 例 6 のアクティブな ILM ポリシー： 2 つのサイトでのデータ保護

この例では、アクティブな ILM ポリシーは最初に 2 サイトの StorageGRID システム用に設計され、 2 つの ILM ルールを使用しています。




この ILM ポリシーでは、テナント A に属するオブジェクトが 1 つのサイトで 2+1 のイレイジャーコーディングによって保護され、一方他のすべてのテナントに属するオブジェクトは 2-copy レプリケーションを使用して 2 つのサイト間で保護されます。

> この例の最初のルールでは、高度なフィルタを使用して、イレイジャーコーディングが小さいオブジェクトには使用されないようにしています。200KB未満のテナントAのオブジェクトは、レプリケーションを使用する2つ目のルールによって保護されます。

ルール **1** ：テナント **A** に **1** つのサイトのイレイジャーコーディング

| ルール定義 | 値の例 |
| --- | --- |
| ルール名 | テナント A の 1 サイトのイレイジャーコーディング |
| テナントアカウント | テナント A |
| ストレージプール | データセンター 1 |
| コンテンツ配置 | データセンター 1 の 2+1 イレイジャーコーディングを 0 日目から無期限に実行 |

ルール **2** ：他のテナントに **2** つのサイトをレプリケートする

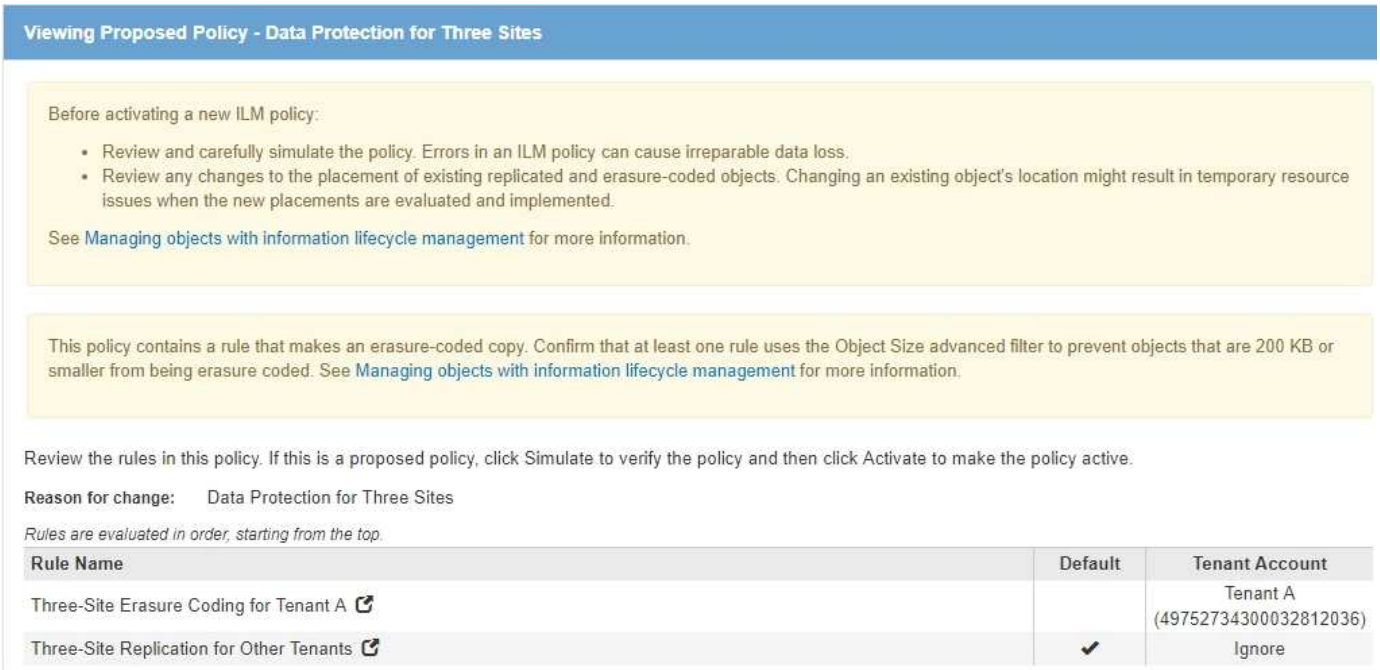
| ルール定義 | 値の例 |
| --- | --- |
| ルール名 | 他のテナント用の 2 サイトレプリケーション |
| テナントアカウント | 無視します |

| ルール定義 | 値の例 |
| --- | --- |
| ストレージプール | データセンター 1 とデータセンター 2 |
| コンテンツ配置 | 0 日目から無期限にレプリケートされたコピー × 2 ：データセンター 1 に 1 つ、データセンター 2 に 1 つ。 |

例 **6** の **ILM** ポリシーとして、 **3** つのサイトのデータ保護が提案されています

この例では、 3 サイトの StorageGRID システムの ILM ポリシーを更新しています。

新しいサイトを追加するための拡張を行ったあと、グリッド管理者は 2 つの新しいストレージプールを作成しました。 1 つは Data Center 3 用のストレージプール、もう 1 つは 3 つのサイトすべてを含むストレージプール（「すべてのストレージノードのデフォルトのストレージプールとは異なる」）です。その後、管理者は 2 つの新しい ILM ルールと、 3 つのサイトすべてのデータを保護するために作成された新しいドラフトの ILM ポリシーを作成しました。




この新しい ILM ポリシーがアクティブ化されると、テナント A に属するオブジェクトが 3 つのサイトで 2+1 イレイジャーコーディングによって保護され、他のテナント（およびテナント A に属する小さいオブジェクト）に属するオブジェクトは 3 つのサイト間で 3 コピーレプリケーションによって保護されるようになります。

ルール **1** ：テナント **A** に **3** サイトイレイジャーコーディング

| ルール定義 | 値の例 |
| --- | --- |
| ルール名 | テナント A の 3 サイトイレイジャーコーディング |
| テナントアカウント | テナント A |

| ルール定義 | 値の例 |
| --- | --- |
| ストレージプール | 3 つのデータセンターすべて（データセンター 1 、データセンター 2 、データセンター 3 を含む） |
| コンテンツ配置 | 0 日目から無期限に 3 つのデータセンターすべてに 2+1 のイレイジャーコーディングを実行 |

ルール **2** ：他のテナントに **3** つのサイトをレプリケーションする

| ルール定義 | 値の例 |
| --- | --- |
| ルール名 | 他のテナント用に 3 つのサイトにレプリケーション |
| テナントアカウント | 無視します |
| ストレージプール | データセンター 1 、データセンター 2 、データセンター 3 |
| コンテンツ配置 | 0 日目から無期限にレプリケートされたコピー 3 つ：データセンター 1 に 1 つ、データセンター 2 に 1 つ、データセンター 3 に 1 つ、 |

例 **6** のドラフト **ILM** ポリシーをアクティブ化しています

新しいドラフト ILM ポリシーをアクティブ化すると、既存のオブジェクトが新しい場所に移動されたり、新規または更新されたルールの配置手順に基づいて既存のオブジェクトの新しいオブジェクトコピーが作成されたりする可能性があります。

原因 ポリシーにエラーがあると、回復不能なデータ損失が発生する可能性があります。ポリシーをアクティブ化する前によく確認およびシミュレートし、想定どおりに機能することを確認してください。

新しい ILM ポリシーをアクティブ化すると、 StorageGRID は、そのポリシーを使用して、既存のオブジェクトと新たに取り込まれたオブジェクトを含むすべてのオブジェクトを管理します。新しい ILM ポリシーをアクティブ化する前に、既存のレプリケートオブジェクトとイレイジャーコーディングオブジェクトの配置に対する変更を確認してください。既存のオブジェクトの場所を変更すると、新しい配置が評価されて実装される際に一時的なリソースの問題が発生する可能性があります。

イレイジャーコーディングの手順が変わったときの動作

この例の現在アクティブな ILM ポリシーでは、テナント A に属するオブジェクトがデータセンター 1 で 2+1 のイレイジャーコーディングを使用して保護されます。新しいドラフトの ILM ポリシーでは、テナント A に属するオブジェクトがデータセンター 1 、 2 、 3 で 2+1 イレイジャーコーディングを使用して保護されます。

新しい ILM ポリシーがアクティブ化されると、次の ILM 処理が実行されます。

- テナント A で取り込まれた新しいオブジェクトは 2 つのデータフラグメントに分割され、 1 つのパリテ

ィフラグメントが追加される。その後、 3 つのフラグメントそれぞれが別々のデータセンターに格納されます。

- テナント A に属する既存のオブジェクトは、実行中の ILM スキャンプロセスで再評価されます。ILM の配置手順では新しいイレイジャーコーディングプロファイルが使用されるため、完全に新しいイレイジャーコーディングされたフラグメントが作成され、 3 つのデータセンターに分散されます。

> データセンター 1 の既存の 2+1 フラグメントは再利用されません。StorageGRID では、各イレイジャーコーディングプロファイルは一意とみなされ、新しいプロファイルを使用する場合はイレイジャーコーディングフラグメントが再利用されません。

レプリケーション手順が変わったときの動作

この例の現在アクティブな ILM ポリシーでは、他のテナントに属するオブジェクトは、データセンター 1 と 2 のストレージプール内の 2 つのレプリケートコピーを使用して保護されます。新しいドラフトの ILM ポリシーでは、他のテナントに属するオブジェクトが、データセンター 1 、 2 、 3 のストレージプール内の 3 つのレプリケートコピーを使用して保護されます。

新しい ILM ポリシーがアクティブ化されると、次の ILM 処理が実行されます。

- テナント A 以外のテナントに新しいオブジェクトが追加されると、 StorageGRID は 3 つのコピーを作成し、各データセンターに 1 つずつコピーを保存します。
- それらの他のテナントに属する既存のオブジェクトは、 ILM のスキャンプロセスの実行中に再評価されます。データセンター 1 とデータセンター 2 にある既存のオブジェクトコピーが新しい ILM ルールのレプリケーション要件を引き続き満たしているため、 StorageGRID はデータセンター 3 にオブジェクトの新しいコピーを 1 つ作成するだけで済みます。

このポリシーをアクティブ化した場合のパフォーマンスへの影響

この例でドラフトの ILM ポリシーをアクティブ化すると、この StorageGRID システムの全体的なパフォーマンスに一時的に影響します。テナント A の既存オブジェクト用に新しいイレイジャーコーディングフラグメントを作成し、他のテナントの既存オブジェクト用にデータセンター 3 に新しいレプリケートコピーを作成するには、通常よりも高いレベルのグリッドリソースが必要になります。

ILM ポリシーが変更されたため、クライアントの読み取り要求と書き込み要求が一時的に通常よりもレイテンシが高くなる可能性があります。配置手順がグリッド全体に完全に実装されたあと、レイテンシは通常レベルに戻ります。

新しい ILM ポリシーをアクティブ化する際のリソースの問題を回避するには、既存のオブジェクトの数が多い場合にルールで取り込み時間の高度なフィルタを使用します。既存のオブジェクトが不必要に移動されないようにするために、新しいポリシーが適用されるおおよその時間よりも長くなるように取り込み時間を設定します。

> ILM ポリシーの変更後にオブジェクトが処理される速度を遅くしたり、上げたりする必要がある場合は、テクニカルサポートにお問い合わせください。

例 **7** ： **S3** オブジェクトロックの準拠 **ILM** ポリシー

S3 オブジェクトのロックが有効なバケット内のオブジェクトの保護および保持の要件を満たす ILM ポリシーを定義する際は、以下の例の S3 バケット、 ILM ルール、 ILM ポリシーをベースとして使用できます。

以前の StorageGRID リリースで従来の準拠機能を使用していた場合、この例を使用して、従来の準拠機能が有効になっている既存のバケットを管理することもできます。

以下の ILM ルールとポリシーは一例にすぎません。ILM ルールを設定する方法は多数あります。新しいポリシーをアクティブ化する前に、ドラフトポリシーをシミュレートして、コンテンツの損失を防ぐためにドラフトポリシーが想定どおりに機能することを確認してください。

関連情報

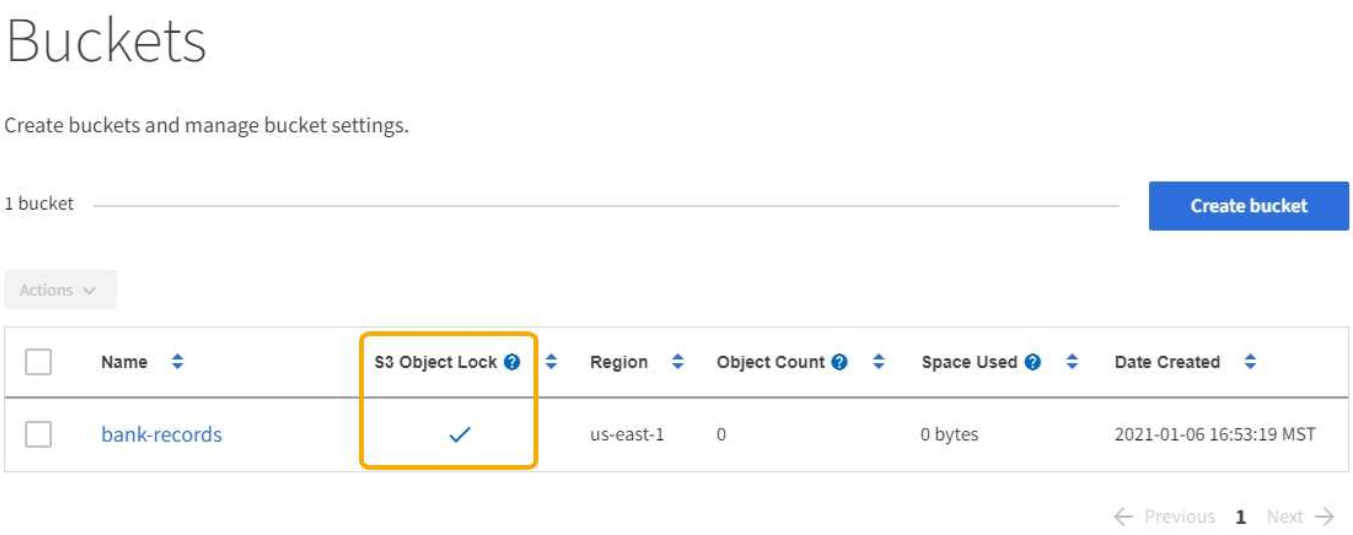
"S3オブジェクトロックでオブジェクトを管理する"

"ILMポリシーを作成する"

**S3** オブジェクトのロックのバケットとオブジェクトの例

次の例では、 Bank of ABC という名前の S3 テナントアカウントで、 Tenant Manager を使用して、重要な銀行記録を格納するために S3 オブジェクトロックを有効にしたバケットを作成しています。

| バケットの定義 | 値の例 |
| --- | --- |
| テナントアカウント名 | ABC 銀行 |
| バケット名 | 銀行記録 |
| バケットのリージョン | us-east-1 （デフォルト） |



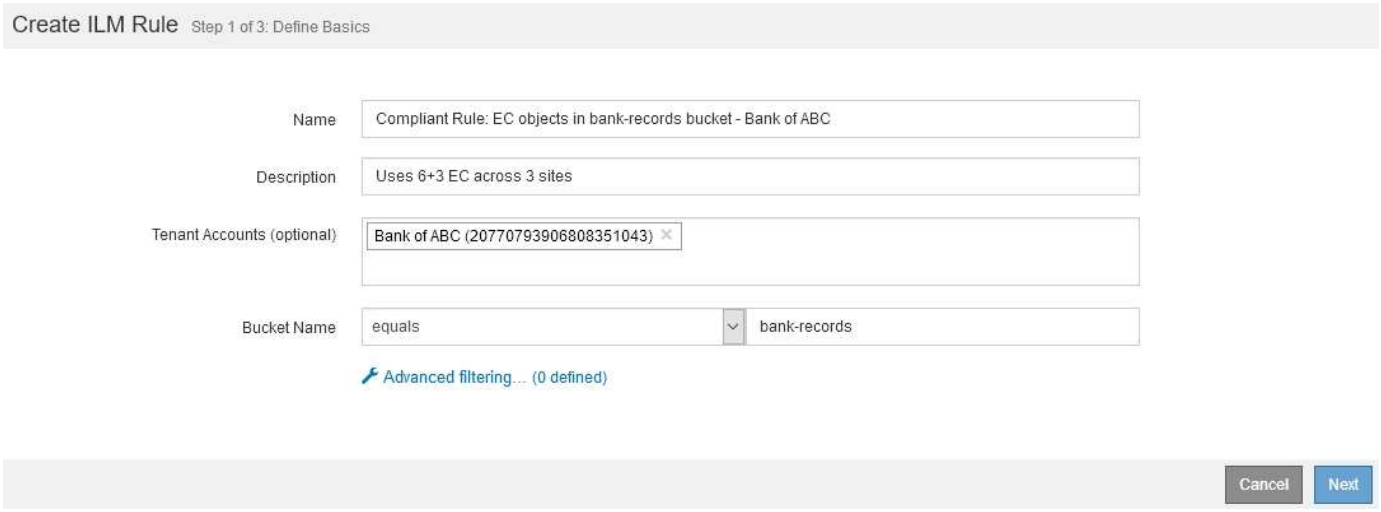

bank-recordsバケットに追加されるオブジェクトとオブジェクトのバージョンには、次の値が使用されます `retain-until-date` および `legal hold` 設定：

| オブジェクトごとに設定します | 値の例 |
| --- | --- |
| `retain-until-date` | `"2030-12-30T23:59:59Z"` （12月30日、2030日）<br><br>各オブジェクトバージョンには独自のバージョンがあります `retain-until-date` 設定：この設定は、上げることはできますが、下げることはできません。 |
| `legal hold` | `"OFF"` （無効）<br><br>リーガルホールドは、保持期間中いつでも任意のオブジェクトバージョンに適用または解除できます。オブジェクトがリーガルホールドの対象になっている場合は、たとえであってもそのオブジェクトを削除することはできません `retain-until-date` に到達しました。 |

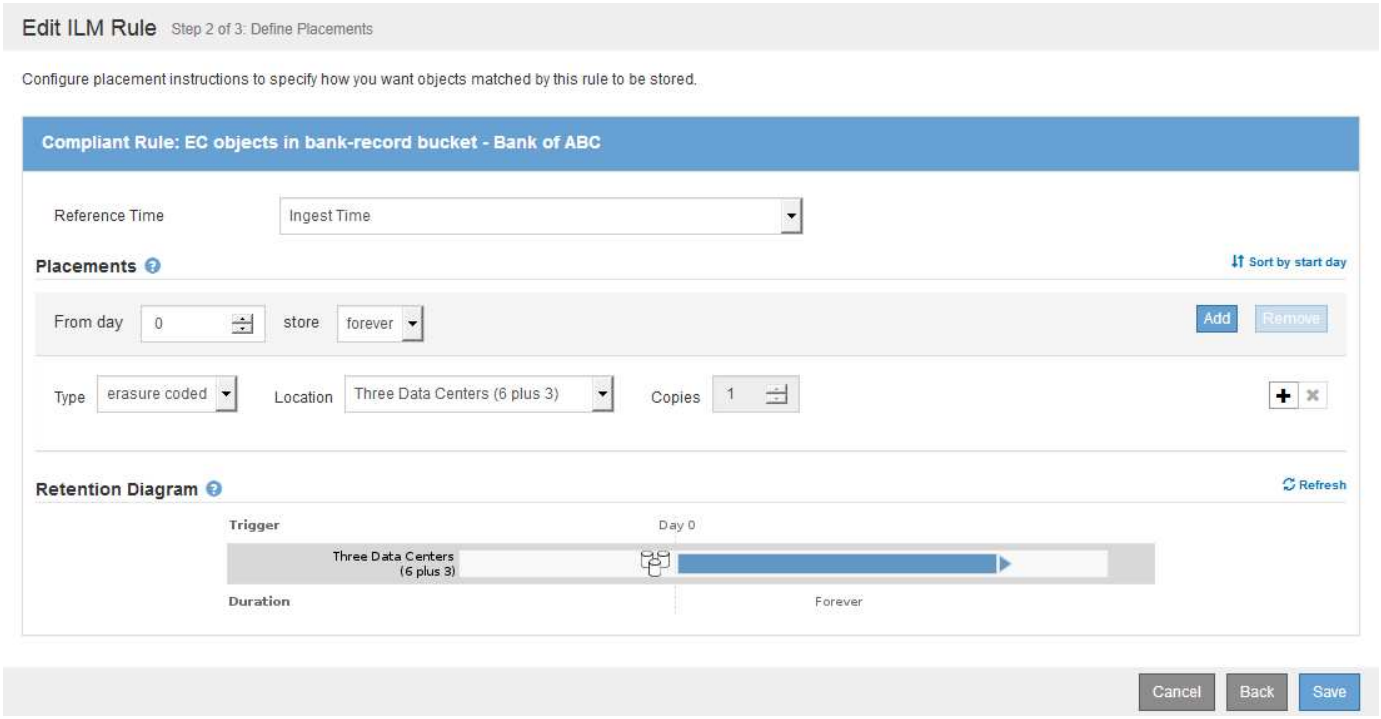
**S3** オブジェクトのロックの **ILM** ルール **1** の例：イレイジャーコーディングプロファイルとバケットの照合

この例の ILM ルールは、 Bank of ABC という名前の S3 テナントアカウントのみに適用されます。内のすべてのオブジェクトに一致します `bank-records` その後、バケットとイレイジャーコーディングを使用して、6+3のイレイジャーコーディングプロファイルを使用して、3つのデータセンターサイトのストレージノードにオブジェクトを格納します。このルールは、 S3 オブジェクトロックが有効なバケットの要件を満たしています。イレイジャーコーディングコピーが 0 日目から無期限にストレージノードに保持され、参照時間として取り込み時間が使用されます。

| ルール定義 | 値の例 |
| --- | --- |
| ルール名 | 準拠ルール： Bank of ABC の銀行記録バケットの EC オブジェクト |
| テナントアカウント | ABC 銀行 |
| バケット名 | `bank-records` |
| 高度なフィルタリング | オブジェクトサイズ（MB）が0.20より大きい<br><br>*注：このフィルタは、200KB以下のオブジェクトにイレイジャーコーディングが使用されないようにします。 |




| ルール定義 | 値の例 |
| --- | --- |
| 参照時間 | 取り込み時間 |
| 配置 | 0 日目のストアから永遠に |
| イレイジャーコーディングプロファイル | • 3 つのデータセンターサイトのストレージノードにイレイジャーコーディングコピーを作成します<br>• 6+3 イレイジャーコーディングスキームを使用 |

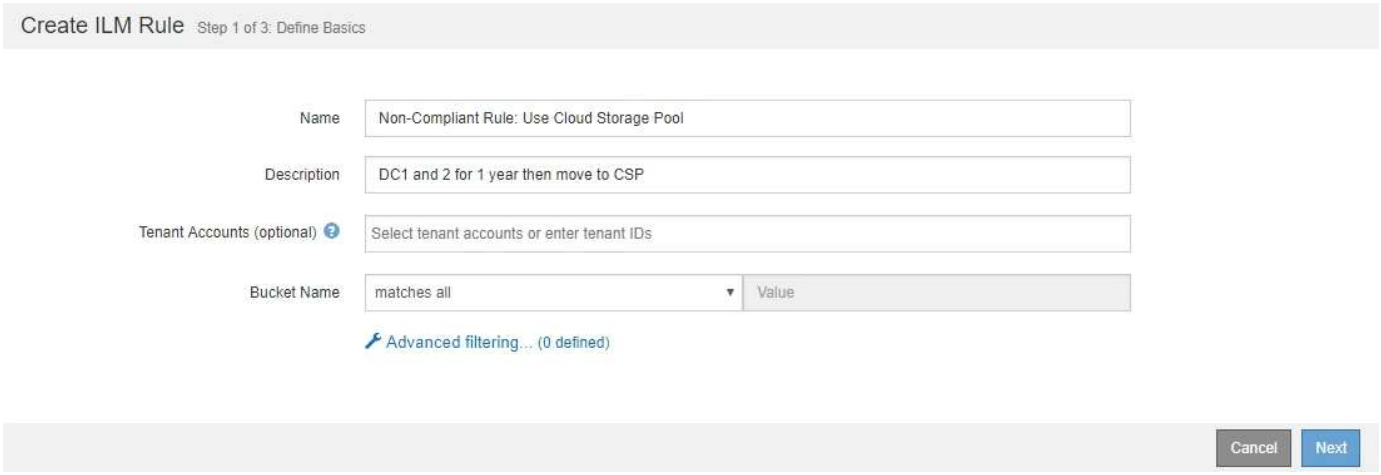



**S3** オブジェクトのロックの例の **ILM** ルール **2** ：非準拠ルール

この例の ILM ルールでは、 2 つのレプリケートオブジェクトコピーをストレージノードに最初に格納します。1 年後、クラウドストレージプールに 1 つのコピーを無期限に格納します。このルールはクラウドストレ

ージプールを使用するため、非準拠となり、 S3 オブジェクトロックが有効になっているバケット内のオブジェクトには適用されません。

| ルール定義 | 値の例 |
| --- | --- |
| ルール名 | 非準拠ルール：クラウドストレージプールを使用 |
| テナントアカウント | 指定されていません |
| バケット名 | 指定されていませんが、 S3 オブジェクトロック（または従来の準拠機能）が有効になっていないバケットのみに適用されます。 |
| 高度なフィルタリング | 指定されていません |



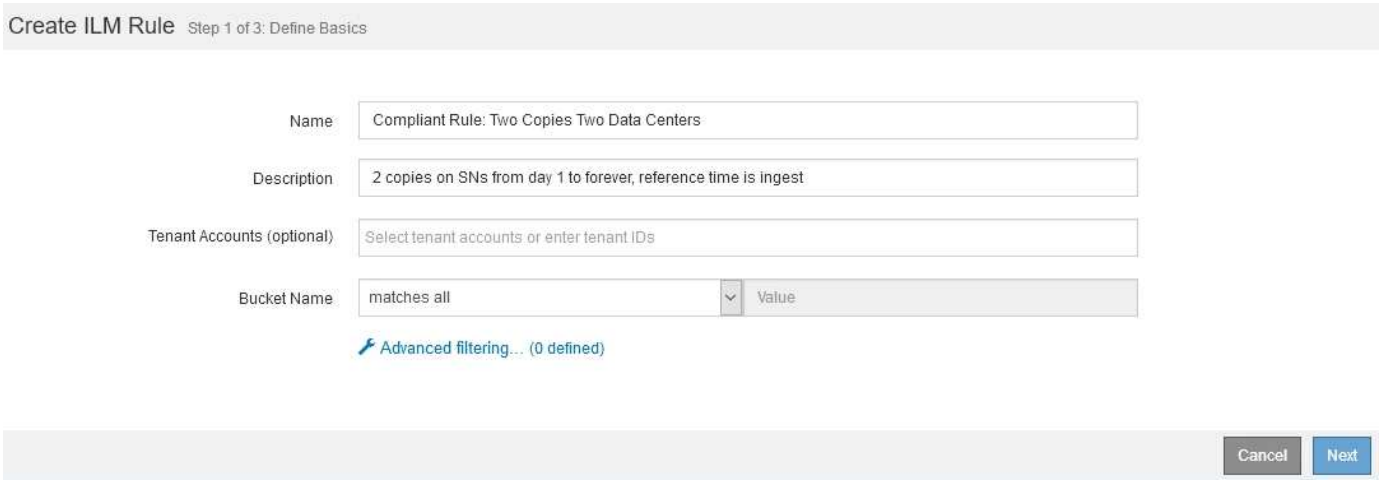

| ルール定義 | 値の例 |
| --- | --- |
| 参照時間 | 取り込み時間 |
| 配置 | • 0 日目から、 2 つのレプリケートコピーをデータセンター 1 とデータセンター 2 のストレージノードに 365 日間格納します<br>• 1 年後、レプリケートコピーを 1 つクラウドストレージプールに無期限に格納します |

**S3** オブジェクトのロックの例の **ILM** ルール **3** ：デフォルトルール

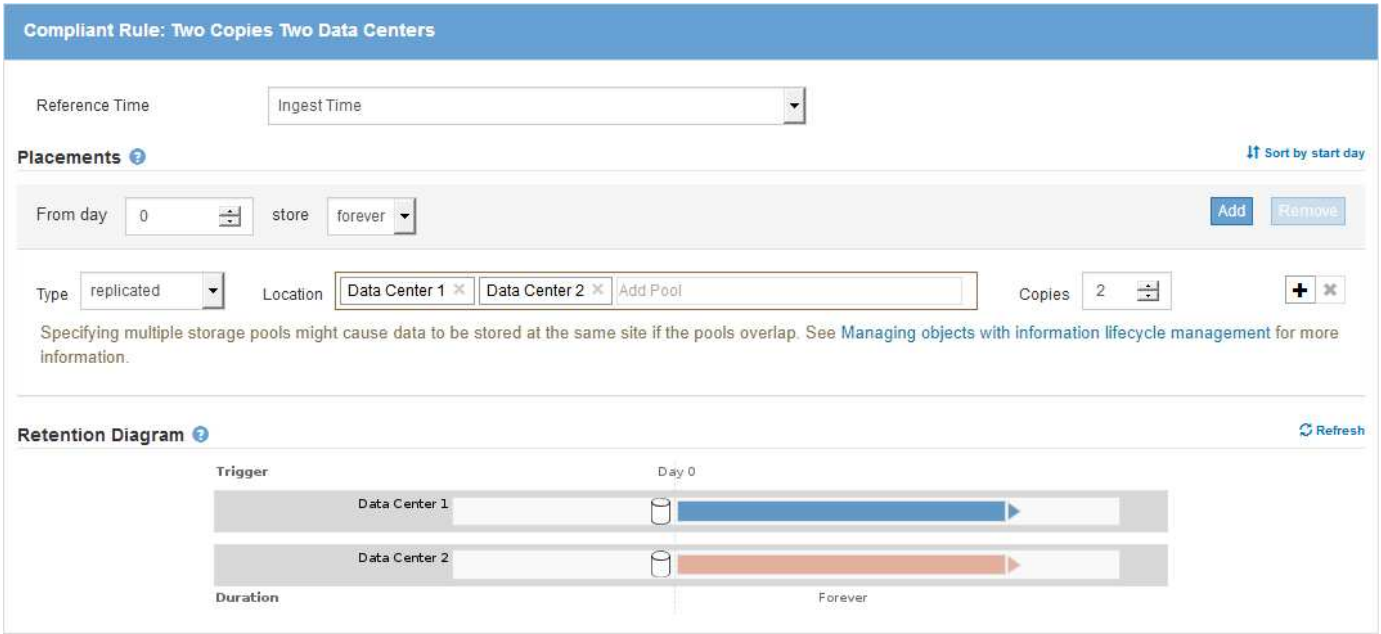
この ILM ルールの例では、 2 つのデータセンター内のストレージプールにオブジェクトデータをコピーします。この準拠ルールは、 ILM ポリシーのデフォルトルールとして設計されています。このルールにはフィルタは含まれておらず、S3オブジェクトロックが有効なバケットの要件を満たしています。参照時間として取り込みを使用して、2つのオブジェクトコピーが0日目から無期限にストレージノードに保持されます。

| ルール定義 | 値の例 |
| --- | --- |
| ルール名 | デフォルトの準拠ルール： 2 つのコピーが 2 つのデータセンターを作成します |

| ルール定義 | 値の例 |
| --- | --- |
| テナントアカウント | 指定されていません |
| バケット名 | 指定されていません |
| 高度なフィルタリング | 指定されていません |




| ルール定義 | 値の例 |
| --- | --- |
| 参照時間 | 取り込み時間 |
| 配置 | 0 日目から無期限に、 2 つのレプリケートコピーを保持します。 1 つはデータセンター 1 のストレージノードに、もう 1 つはデータセンター 2 のストレージノードに保持します。 |

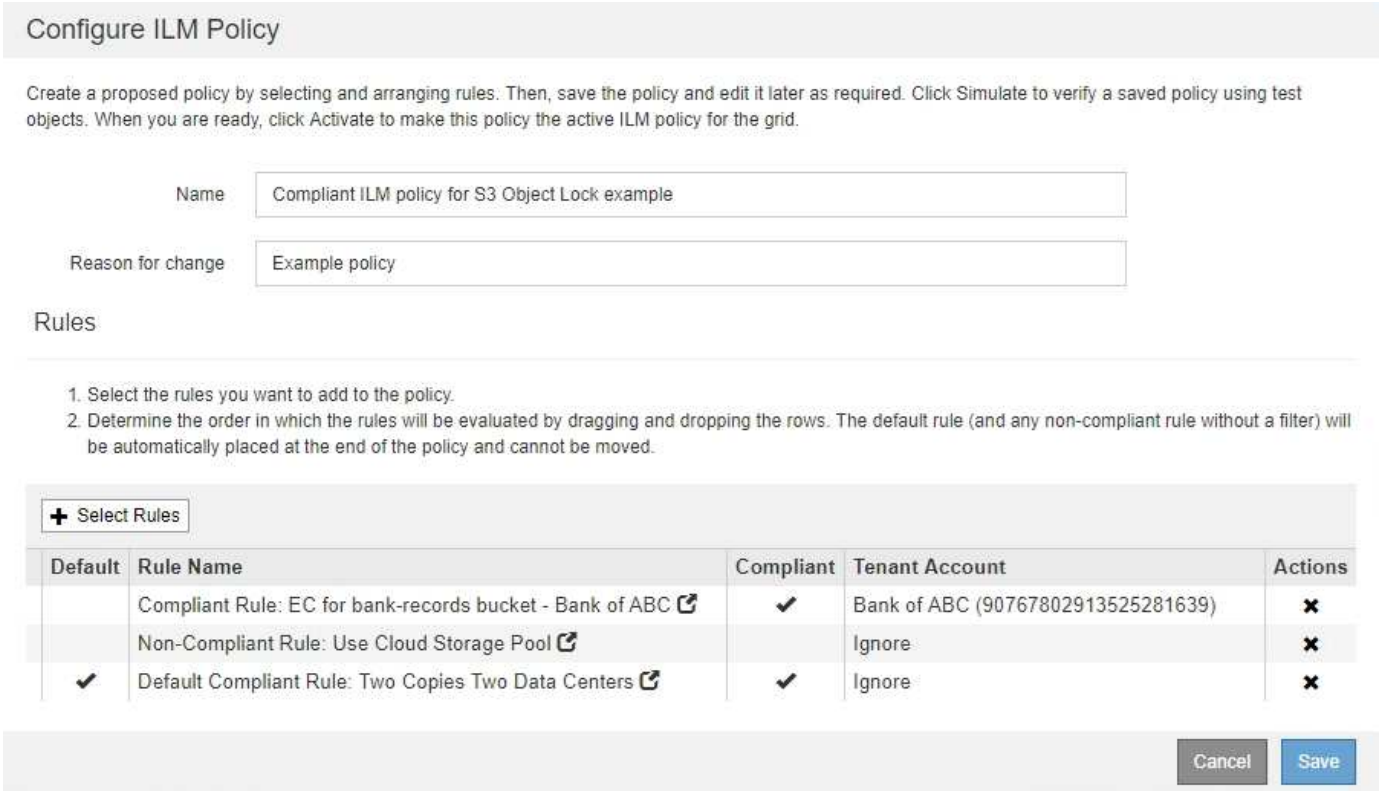


S3 オブジェクトロックが有効になっているバケット内のオブジェクトを含め、システム内のすべてのオブジェクトを効果的に保護する ILM ポリシーを作成するには、すべてのオブジェクトのストレージ要件を満たす ILM ルールを選択する必要があります。その後、ドラフトポリシーをシミュレートしてアクティブ化する必要があります。

ポリシーにルールを追加しています

この例では、 ILM ポリシーに、次の順序で 3 つの ILM ルールが含まれています。

1. S3オブジェクトロックが有効な特定のバケットで、イレイジャーコーディングを使用して200KBを超えるオブジェクトを保護する準拠ルール。オブジェクトは 0 日目から無期限にストレージノードに格納されます。
2. 2 つのレプリケートオブジェクトコピーを作成してストレージノードに 1 年間保存したあと、 1 つのオブジェクトコピーをクラウドストレージプールに無期限に移動する非準拠ルール。S3 オブジェクトロックが有効になっているバケットでは、クラウドストレージプールを使用するため、このルールは適用されません。
3. 2 つのレプリケートオブジェクトコピーを 0 日目からストレージノードに無期限に作成するデフォルトの準拠ルール。




ドラフトポリシーをシミュレートする

ドラフトポリシーにルールを追加してデフォルトの準拠ルールを選択し、他のルールを配置したら、 S3 オブジェクトロックを有効にしたバケットおよび他のバケットのオブジェクトをテストしてポリシーをシミュレートする必要があります。たとえば、この例のポリシーをシミュレートすると、テストオブジェクトは次のように評価されます。

- 最初のルールは、Bank of ABCテナントのバケットバンクレコードで200KBを超えるテストオブジェクト

のみに一致します。

- 2 番目のルールは、他のすべてのテナントアカウントの非準拠バケット内のすべてのオブジェクトに一致します。
- デフォルトのルールは次のオブジェクトに一致します。
  - バケットバンク内の200KB以下のオブジェクト- Bank of ABCテナントのレコード。
  - 他のすべてのテナントアカウントで S3 オブジェクトロックが有効になっている他のバケット内のオブジェクト。

ポリシーをアクティブ化しています

新しいポリシーによってオブジェクトデータが適切に保護されることを確認したら、アクティブ化します。

# システムの保護対策

StorageGRID システムをセキュリティの脅威から保護するためのシステム設定、ベストプラクティス、および推奨事項について説明します。

- "StorageGRID システムのセキュリティ強化"
- "ソフトウェアアップグレードの強化に関するガイドライン"
- "StorageGRID ネットワークのセキュリティ強化のガイドライン"
- "StorageGRID ノードの保護対策のガイドライン"
- "サーバ証明書のセキュリティ強化ガイドライン"
- "その他のセキュリティ強化に関するガイドライン"]

## StorageGRID システムのセキュリティ強化

システムのセキュリティ強化とは、 StorageGRID システムからできるだけ多くのセキュリティリスクを排除するプロセスです。

このドキュメントでは、 StorageGRID 固有の強化ガイドラインの概要を説明します。これらのガイドラインは、システム強化に関する業界標準のベストプラクティスを補足するものです。たとえば、次のガイドラインでは、 StorageGRID に強力なパスワードを使用し、 HTTP ではなく HTTPS を使用し、可能な場合は証明書ベースの認証を有効にすることを前提としています。

StorageGRID をインストールして構成する際に、これらのガイドラインを使用して、情報システムの機密性、整合性、可用性に関する規定のセキュリティ目標を達成できます。

StorageGRID は、 _NetApp 脆弱性処理ポリシー _ に従います。報告された脆弱性は、製品セキュリティインシデント対応プロセスに従って検証および解決されます。

### StorageGRID システムを強化するための一般的な考慮事項

StorageGRID システムを強化する際は、次の点を考慮する必要があります。

- 実装した 3 つの StorageGRID ネットワークのうち、どれですか。すべての StorageGRID システムでグリッドネットワークを使用する必要がありますが、管理ネットワーク、クライアントネットワーク、または

その両方を使用することもできます。ネットワークごとにセキュリティに関する考慮事項が異なります。

- StorageGRID システムの個々のノードで使用するプラットフォームのタイプ。StorageGRID ノードは、VMware仮想マシン、Linuxホスト上のDockerコンテナ内に導入できるほか、専用のハードウェアアプライアンスとして導入することもできます。プラットフォームのタイプごとに、強化に関するベストプラクティスがあります。
- テナントアカウントが信頼されている方法。テナントアカウントを信頼しないサービスプロバイダである場合は、信頼できる社内テナントのみを使用した場合とはセキュリティ上の問題が異なります。
- どのセキュリティ要件および規則に準拠しているか。特定の規制や企業の要件に準拠しなければならない場合があります。

関連情報

"脆弱性対策ポリシー"

## ソフトウェアアップグレードの強化に関するガイドライン

### 攻撃を防御するには、 StorageGRID システムおよび関連サービスを最新の状態に保つ必要があります。

#### **StorageGRID** ソフトウェアへのアップグレード

StorageGRID ソフトウェアは、可能なかぎり、最新のメジャーリリースまたは以前のメジャーリリースにアップグレードする必要があります。StorageGRID を最新の状態に保つことで、既知の脆弱性がアクティブになる時間を短縮し、攻撃対象領域全体を削減できます。また、 StorageGRID の最新リリースには、以前のリリースには含まれていないセキュリティ強化機能が含まれていることがよくあります。

ホットフィックスが必要になったときに、ネットアップは最新リリースの更新プログラムの作成に優先順位を付けます。一部のパッチは、以前のリリースと互換性がない場合があります。

StorageGRID の最新のリリースやホットフィックスをダウンロードするには、 StorageGRID のソフトウェアダウンロードページにアクセスします。StorageGRID ソフトウェアのアップグレード手順については、StorageGRID のアップグレード手順を参照してください。ホットフィックスの適用手順については、リカバリとメンテナンスの手順を参照してください。

#### 外部サービスへのアップグレード

外部サービスには、 StorageGRID に間接的に影響する脆弱性が存在する場合がありますStorageGRID が依存するサービスが最新の状態に保たれていることを確認してください。LDAP 、 KMS （ KMIP サーバ）、 DNS 、 NTP などのサービスを利用できます。

サポートされているバージョンの一覧については、 NetApp Interoperability Matrix Tool を参照してください。

#### ハイパーバイザーのアップグレード

StorageGRID ノードが VMware または別のハイパーバイザーで実行されている場合は、ハイパーバイザーのソフトウェアとファームウェアが最新であることを確認する必要があります。

サポートされているバージョンの一覧については、 NetApp Interoperability Matrix Tool を参照してください。

*** Linuxノードへのアップグレード***

StorageGRID ノードで Linux ホストプラットフォームを使用している場合は、セキュリティ更新とカーネル更新がホスト OS に適用されていることを確認する必要があります。また、これらの更新プログラムが利用可能になった場合は、脆弱なハードウェアにファームウェアの更新プログラムを適用する必要があります。

サポートされているバージョンの一覧については、 NetApp Interoperability Matrix Tool を参照してください。

関連情報

"ネットアップのダウンロード： StorageGRID"

"ソフトウェアをアップグレードする"

""

"NetApp Interoperability Matrix Tool で確認できます"

## StorageGRID ネットワークのセキュリティ強化のガイドライン

StorageGRID システムでは、グリッドノードあたり最大 3 つのネットワークインターフェイスがサポートされ、各グリッドノードのネットワークをセキュリティやアクセスの要件に応じて設定することができます。

グリッドネットワークのガイドライン

グリッドネットワークはすべての内部 StorageGRID トラフィック用に設定する必要があります。グリッドネットワークのグリッドノードは、いずれも他のすべてのノードと通信できなければなりません。

グリッドネットワークを設定する際は、次のガイドラインに従ってください。

- オープンインターネット上のクライアントなど、信頼できないクライアントからネットワークが保護されていることを確認します。
- 可能な場合は、グリッドネットワークを内部トラフィック専用にします。管理ネットワークとクライアントネットワークの両方に、内部サービスへの外部トラフィックをブロックするファイアウォール制限が追加されています。グリッドネットワークを使用した外部クライアントトラフィックの処理はサポートされていますが、この使用によって保護レイヤが少なくなります。
- StorageGRID 環境が複数のデータセンターにまたがっている場合は、仮想プライベートネットワーク（ VPN ）またはグリッドネットワーク上で同等の機能を使用して、内部トラフィックをさらに保護します。
- 一部のメンテナンス手順では、プライマリ管理ノードと他のすべてのグリッドノードの間のポート 22 で Secure Shell （ SSH ）アクセスが必要です。外部ファイアウォールを使用して、信頼できるクライアントへの SSH アクセスを制限します。

管理ネットワークのガイドライン

管理ネットワークは、通常、管理タスク（ Grid Manager または SSH を使用する信頼できる従業員）および LDAP 、 DNS 、 NTP 、 KMS （ KMIP サーバ）などの信頼された他のサービスとの通信に使用します。ただし、 StorageGRID ではこの使用が内部的に適用されることはありません。

管理ネットワークを使用する場合は、次のガイドラインに従ってください。

- 管理ネットワーク上のすべての内部トラフィックポートをブロックします。使用するプラットフォームに対応したインストールガイドの内部ポートの一覧を参照してください。
- 信頼されていないクライアントが管理ネットワークにアクセスできる場合は、外部ファイアウォールで管理ネットワーク上の StorageGRID へのアクセスをブロックします。

クライアントネットワークのガイドライン

クライアントネットワークは、通常、テナント、および CloudMirror レプリケーションサービスや別のプラットフォームサービスなどの外部サービスとの通信に使用されます。ただし、 StorageGRID ではこの使用が内部的に適用されることはありません。

クライアントネットワークを使用する場合は、次のガイドラインに従ってください。

- クライアントネットワーク上のすべての内部トラフィックポートをブロックします。使用するプラットフォームに対応したインストールガイドの内部ポートの一覧を参照してください。
- 明示的に設定されたエンドポイントでのみ、インバウンドクライアントトラフィックを受け入れます。StorageGRID の管理手順の信頼されていないクライアントネットワークの管理に関する情報を参照してください。

関連情報

"ネットワークガイドライン"

"グリッド入門"

"StorageGRID の管理"

"Red Hat Enterprise Linux または CentOS をインストールします"

"Ubuntu または Debian をインストールします"

"VMware をインストールする"

## StorageGRID ノードの保護対策のガイドライン

StorageGRID ノードは、VMware仮想マシン、Linuxホスト上のDockerコンテナ内に導入できるほか、専用のハードウェアアプライアンスとして導入することもできます。プラットフォームのタイプとノードのタイプにはそれぞれ、強化に関するベストプラクティスがあります。

ファイアウォールの設定

システム強化プロセスの一環として、外部ファイアウォールの設定を確認し、 IP アドレスとそれが厳密に必要なポートからのみトラフィックが許可されるように変更する必要があります。

VMwareプラットフォームおよびStorageGRID アプライアンスで実行されるノードは、自動的に管理される内部ファイアウォールを使用します。この内部ファイアウォールは、一部の一般的な脅威に対する追加の保護レイヤを提供しますが、外部ファイアウォールの必要性は排除されません。

StorageGRID で使用されるすべての内部ポートと外部ポートの一覧については、ご使用のプラットフォームのインストールガイドを参照してください。

### 仮想化、コンテナ、共有ハードウェア

すべての StorageGRID ノードで、信頼されていないソフトウェアと同じ物理ハードウェア上で StorageGRID を実行しないでください。StorageGRID とマルウェアの両方が同じ物理ハードウェア上に存在する場合、ハイパーバイザーによる保護によって、 StorageGRID で保護されたデータへのマルウェアのアクセスが防止されるとは限りません。たとえば、 Meltdown と Specter 攻撃は、最新のプロセッサに存在する重要な脆弱性を悪用し、プログラムが同じコンピュータ上のメモリにデータを盗むことを可能にします。

### 未使用のサービスを無効にします

すべての StorageGRID ノードについて、未使用のサービスへのアクセスを無効化またはブロックする必要があります。たとえば、 CIFS または NFS 用の監査共有へのクライアントアクセスを設定しない場合は、これらのサービスへのアクセスをブロックするか無効にします。

### インストール中にノードを保護

信頼されていないユーザが、ノードのインストール時にネットワーク経由で StorageGRID ノードにアクセスすることを許可しないでください。ノードは、グリッドに参加するまで完全にはセキュアではありません。

## 管理ノードのガイドライン

管理ノードは、システムの設定、監視、ロギングなどの管理サービスを提供します。Grid Manager または Tenant Manager にサインインすると、管理ノードに接続されます。

StorageGRID システムで管理ノードを保護するには、次のガイドラインに従います。

- 開いているインターネット上の管理ノードなど、信頼されていないクライアントからすべての管理ノードを保護します。グリッドネットワーク上、管理ネットワーク上、またはクライアントネットワーク上のどの管理ノードにも、信頼されていないクライアントがアクセスできないようにします。
- StorageGRID グループは Grid Manager とテナントマネージャの機能へのアクセスを制御します。各ユーザグループにロールに最低限必要な権限を付与し、読み取り専用アクセスモードを使用してユーザによる設定変更を防止します。
- StorageGRID ロードバランサエンドポイントを使用する場合は、信頼されないクライアントトラフィックに管理ノードの代わりにゲートウェイノードを使用します。
- 信頼されていないテナントがある場合は、テナントマネージャやテナント管理 API に直接アクセスすることを許可しないでください。代わりに、信頼されていないテナントがテナントポータルまたはテナント管理 API と連動する外部テナント管理システムを使用するようにします。
- 必要に応じて、管理ノードからネットアップサポートへの AutoSupport 通信をより細かく制御するために管理プロキシを使用します。StorageGRID の管理手順の管理プロキシの作成手順を参照してください。
- 必要に応じて、制限された 8443 ポートと 9443 ポートを使用して Grid Manager と Tenant Manager の通信を分離します。共有ポート 443 をブロックして、テナント要求をポート 9443 に制限して追加の保護を確保します。
- 必要に応じて、グリッド管理者とテナントユーザには別々の管理ノードを使用します。

詳細については、 StorageGRID の管理手順を参照してください。

## ストレージノードに関するガイドライン

ストレージノードは、オブジェクトデータとメタデータを管理および格納します。StorageGRID システムでストレージノードを保護するには、次のガイドラインに従います。

- 信頼されていないテナントのアウトバウンドサービスは有効にしないでください。たとえば、信頼されていないテナントのアカウントを作成する場合は、テナントが独自のアイデンティティソースを使用することを許可せず、プラットフォームサービスの使用も許可しないでください。StorageGRID の管理手順に従って、テナントアカウントを作成する手順を参照してください。
- 信頼されないクライアントトラフィックには、サードパーティのロードバランサを使用します。サードパーティ製のロードバランシングにより、攻撃に対する制御性が向上し、追加の保護レイヤが提供されます。
- 必要に応じて、ストレージプロキシを使用して、クラウドストレージプールとプラットフォームサービスのストレージノードから外部サービスへの通信をより細かく制御します。StorageGRID の管理手順のストレージプロキシの作成手順を参照してください。
- 必要に応じて、クライアントネットワークを使用して外部サービスに接続します。次に、「* Configuration > Network Settings > Untrusted Client Network *」を選択し、ストレージノード上のクライアントネットワークが信頼されていないことを示します。ストレージノードはクライアントネットワーク上の受信トラフィックを受け入れなくなりますが、プラットフォームサービスへのアウトバウンド要求は引き続き許可します。

### ゲートウェイノードのガイドライン

ゲートウェイノードは、クライアントアプリケーションが StorageGRID への接続に使用できるオプションのロードバランシングインターフェイスです。StorageGRID システムにゲートウェイノードを保護するには、次のガイドラインに従います。

- ゲートウェイノード上の CLB サービスを使用する代わりに、ロードバランサエンドポイントを設定して使用する。StorageGRID の管理手順のロードバランシングの管理手順を参照してください。

  CLB サービスは廃止されました。

- クライアントとゲートウェイノードまたはストレージノードの間で、信頼されていないクライアントトラフィックにサードパーティのロードバランサを使用します。サードパーティ製のロードバランシングにより、攻撃に対する制御性が向上し、追加の保護レイヤが提供されます。サードパーティのロードバランサを使用する場合でも、内部のロードバランサエンドポイントを経由するようにネットワークトラフィックを設定したり、ストレージノードに直接送信したりすることができます。
- ロードバランサエンドポイントを使用している場合は、必要に応じてクライアントネットワーク経由で接続します。次に、「* Configuration > Network Settings > Untrusted Client Network *」を選択し、ゲートウェイノード上のクライアントネットワークが信頼されていないことを示します。ゲートウェイノードは、ロードバランサエンドポイントとして明示的に設定されたポートのインバウンドトラフィックのみを受け入れます。

### ハードウェアアプライアンスノードのガイドライン

StorageGRID ハードウェアアプライアンスは、 StorageGRID システム専用に設計されています。一部のアプライアンスはストレージノードとして使用できます。その他のアプライアンスは、管理ノードまたはゲートウェイノードとして使用できます。アプライアンスノードをソフトウェアベースのノードと組み合わせることも、自社開発の全アプライアンスグリッドを導入することもできます。

StorageGRID システムにハードウェアアプライアンスノードを固定するには、次のガイドラインに従います。

- アプライアンスでストレージコントローラの管理に SANtricity System Manager を使用している場合は、信頼されていないクライアントからネットワーク経由で SANtricity System Manager にアクセスできないようにします。

- アプライアンスに Baseboard Management Controller （ BMC ；ベースボード管理コントローラ）が搭載されている場合は、 BMC 管理ポートで下位レベルのハードウェアアクセスが許可されることに注意してください。BMC 管理ポートは、信頼されているセキュアな内部管理ネットワークにのみ接続してください。該当するネットワークがない場合は、テクニカルサポートから BMC 接続の要請があった場合を除き、 BMC 管理ポートを接続しないか、またはブロックしたままにしてください。
- アプライアンスが Intelligent Platform Management Interface （ IPMI ）標準を使用したイーサネット経由でのコントローラハードウェアのリモート管理をサポートする場合は、ポート 623 での信頼されていないトラフィックをブロックします。
- アプライアンスのストレージコントローラに FDE または FIPS ドライブが搭載されていて、ドライブセキュリティ機能が有効になっている場合は、 SANtricity を使用してドライブセキュリティキーを設定します。
- FDE または FIPS ドライブが搭載されていないアプライアンスの場合は、 Key Management Server （ KMS ）を使用してノード暗号化を有効にします。

使用している StorageGRID ハードウェアアプライアンスのインストールとメンテナンスの手順を参照してください。

関連情報

"Red Hat Enterprise Linux または CentOS をインストールします"

"Ubuntu または Debian をインストールします"

"VMware をインストールする"

"StorageGRID の管理"

"テナントアカウントを使用する"

"SG100 SG1000サービスアプライアンス"

"SG5600 ストレージアプライアンス"

"SG5700 ストレージアプライアンス"

"SG6000 ストレージアプライアンス"

## サーバ証明書のセキュリティ強化ガイドライン

### インストール時に作成されたデフォルトの証明書を独自のカスタム証明書に置き換える必要があります。

多くの組織では、 StorageGRID Web アクセス用の自己署名デジタル証明書が、情報セキュリティポリシーに準拠していません。本番用システムでは、 StorageGRID の認証に使用する CA 署名デジタル証明書をインストールする必要があります。

具体的には、次のデフォルト証明書ではなくカスタムサーバ証明書を使用する必要があります。

- 管理インターフェイスのサーバ証明書：Grid Manager、テナントマネージャ、Grid管理API、テナント管理APIへのアクセスを保護するために使用されます。
- * Object Storage API Service Endpoints Server Certificate *：ストレージノードおよびゲートウェイノード

へのアクセスを保護するために使用します。これらのノードは、S3およびSwiftクライアントアプリケーションがオブジェクトデータをアップロードおよびダウンロードするために使用します。

> StorageGRID では、ロードバランサエンドポイントに使用する証明書は別に管理されます。ロードバランサ証明書を設定するには、 StorageGRID の管理手順でロードバランサエンドポイントの設定手順を参照してください。

カスタムサーバ証明書を使用する場合は、次のガイドラインに従ってください。

- 証明書にはが必要です *subjectAltName* StorageGRID のDNSエントリと同じです。詳細については、のセクション 4.2.1.6 「 Subject Alternative Name 」を参照してください "RFC 5280: PKIX 証明書と CRL プロファイル"。
- 可能であれば、ワイルドカード証明書は使用しないでください。このガイドラインの例外は、 S3 仮想ホスト形式のエンドポイントの証明書です。バケット名が事前に不明な場合は、ワイルドカードを使用する必要があります。
- 証明書にワイルドカードを使用する必要がある場合は、リスクを軽減するために追加の手順を実行する必要があります。などのワイルドカードパターンを使用します `*.s3.example.com`を使用せずに、を使用してください `s3.example.com` その他のアプリケーションのサフィックス。このパターンは、などのパス形式のS3アクセスでも機能します `dc1-s1.s3.example.com/mybucket`。
- 証明書の有効期限を短く（ 2 カ月など）設定し、グリッド管理 API を使用して証明書のローテーションを自動化します。これは、ワイルドカード証明書で特に重要です。

また、クライアントは StorageGRID との通信に厳密なホスト名チェックを使用する必要があります。

## その他のセキュリティ強化に関するガイドライン

### StorageGRID ネットワークおよびノードに対する強化ガイドラインに加えて、StorageGRID システムの他の領域に対する強化ガイドラインに従う必要があります。

ログと監査メッセージ

StorageGRID ログおよび監査メッセージ出力は必ず安全な方法で保護してください。StorageGRID のログと監査メッセージは、サポートやシステム可用性の観点から非常に重要な情報を提供します。また、StorageGRID のログおよび監査メッセージの出力に含まれる情報や詳細情報は、一般に機密性が高いため、

StorageGRID ログの詳細については、監視とトラブルシューティングの手順を参照してください。StorageGRID 監査メッセージの詳細については、監査メッセージに関する手順を参照してください。

**NetApp AutoSupport**

StorageGRID の AutoSupport 機能を使用すると、システムの状態をプロアクティブに監視し、ネットアップテクニカルサポート、組織の社内サポートチーム、またはサポートパートナーにメッセージと詳細を自動的に送信できます。デフォルトでは、 StorageGRID を初めて設定した場合、ネットアップテクニカルサポートへの AutoSupport メッセージが有効になります。

AutoSupport 機能は無効にすることができます。ただし、 StorageGRID システムで問題 に障害が発生した場合には、 AutoSupport を使用して迅速に問題を識別し解決できるため、ネットアップではこの機能を有効にすることを推奨してい

AutoSupport は、転送プロトコルとして HTTPS 、 HTTP 、 SMTP をサポートしています。AutoSupport メッ

セージは機密性が高いため、ネットアップでは、 AutoSupport メッセージをネットアップサポートに送信する際のデフォルト転送プロトコルとして HTTPS を使用することを強く推奨しています。

必要に応じて、管理ノードからネットアップテクニカルサポートへの AutoSupport 通信をより細かく制御するための管理プロキシを設定できます。StorageGRID の管理手順の管理プロキシの作成手順を参照してください。

**Cross-Origin Resource Sharing （ CORS ）**

S3 バケットとバケット内のオブジェクトに他のドメインにある Web アプリケーションからアクセスできるようにする必要がある場合は、そのバケットに Cross-Origin Resource Sharing （ CORS ）を設定できます。一般に、 CORS は必要でないかぎり有効にしないでください。CORS が必要な場合は、信頼できるオリジンに制限します。

テナントアカウントの使用手順の Cross-Origin Resource Sharing （ CORS ）の設定手順を参照してください。

外部セキュリティデバイス

完全なセキュリティ強化解決策 は、 StorageGRID 以外のセキュリティメカニズムに対応する必要があります。StorageGRID へのアクセスをフィルタリングおよび制限するために追加のインフラデバイスを使用すると、厳格なセキュリティ体制を確立し、維持するための効果的な方法となります。これらの外部セキュリティデバイスには、ファイアウォール、 Intrusion Prevention System （ IPS ；侵入防御システム）、およびその他のセキュリティデバイスが含まれます。

信頼されないクライアントトラフィックには、サードパーティのロードバランサを使用することを推奨します。サードパーティ製のロードバランシングにより、攻撃に対する制御性が向上し、追加の保護レイヤが提供されます。

関連情報

"トラブルシューティングを監視します"

"監査ログを確認します"

"テナントアカウントを使用する"

"StorageGRID の管理"

# StorageGRID for FabricPool を設定します

StorageGRID をNetApp FabricPool クラウド階層として設定する方法について説明します。

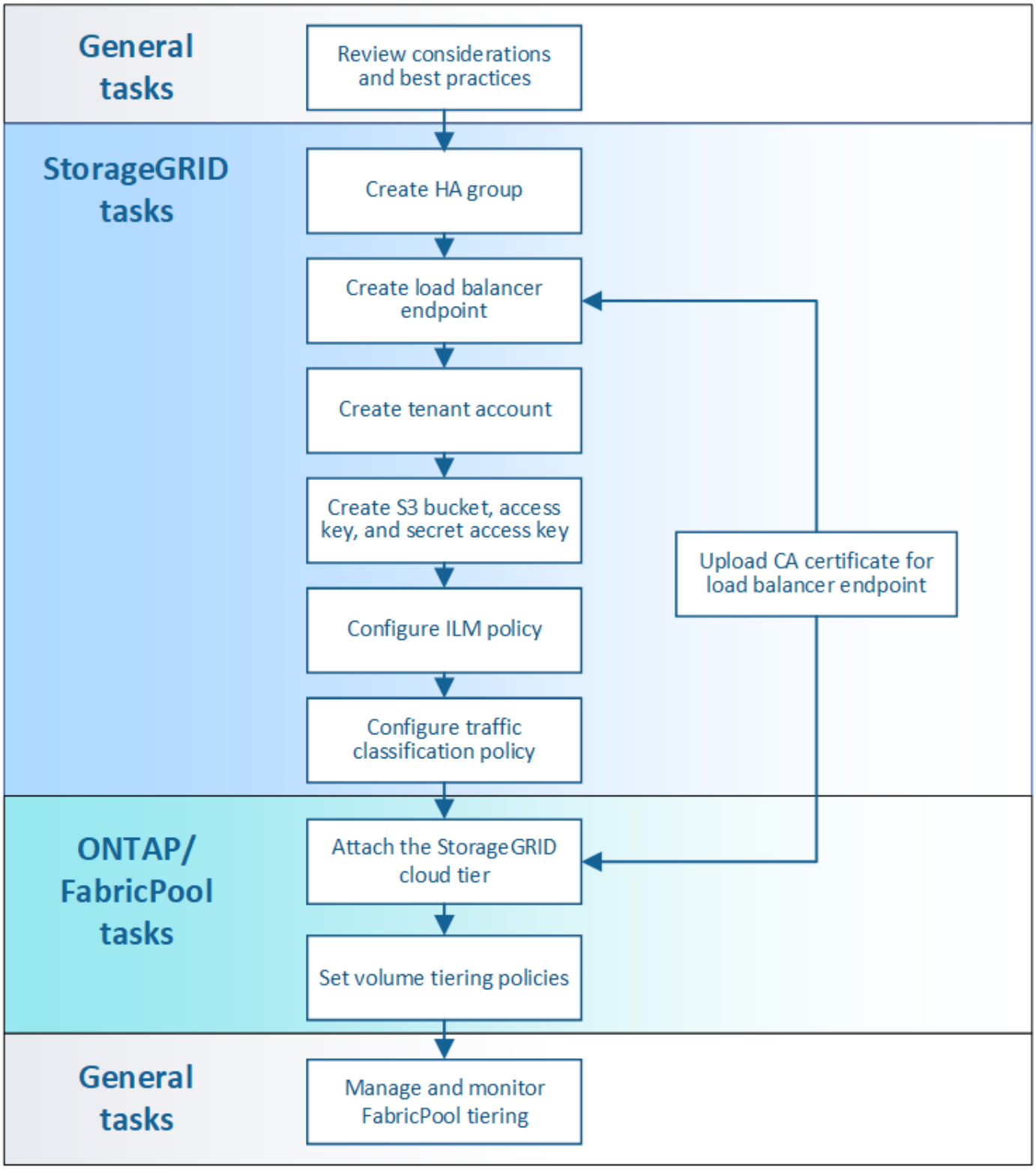
- "StorageGRID for FabricPool を設定しています"
- "StorageGRID をクラウド階層として接続するために必要な情報"
- "StorageGRID の情報ライフサイクル管理とFabricPool のデータを使用する"
- "FabricPool のトラフィック分類ポリシーを作成する"
- "StorageGRID および FabricPool に関するその他のベストプラクティスです"

# StorageGRID for FabricPool を設定しています

NetApp ONTAP ソフトウェアを使用すると、 NetApp FabricPool を使用して、アクセス頻度の低いデータやコールドデータを NetApp StorageGRID オブジェクトストレージシステムに階層化できます。

次の手順に従って、次の操作を行います

- FabricPool で使用する StorageGRID オブジェクトストレージシステムの設定の概要について説明します。
- StorageGRID を FabricPool クラウド階層として接続した場合に ONTAP に入力する情報の入手方法について説明します。
- StorageGRID 情報ライフサイクル管理（ ILM ）ポリシー、 StorageGRID トラフィック分類ポリシー、および FabricPool ワークロードのその他の StorageGRID オプションを設定するためのベストプラクティスについて説明します。




必要なもの

これらの手順を使用する前に、次の

- アクセス頻度の低い ONTAP データを StorageGRID に階層化するときに使用する FabricPool ボリューム階層化ポリシーを決定します。
- ストレージ容量とパフォーマンスのニーズを満たす StorageGRID システムを計画して設置します。
- Grid Manager や Tenant Manager を含む StorageGRID システムソフトウェアの理解

関連情報

- "TR-4598：『FabricPool Best Practices for ONTAP 9.8』"
- "ONTAP 9 ドキュメンテーション・センター"

**FabricPool** とは

FabricPool は、ハイパフォーマンスのフラッシュアグリゲートを高パフォーマンス階層として、オブジェクトストアをクラウド階層として使用する ONTAP ハイブリッドストレージ解決策 です。FabricPool 内のデータは、アクセス頻度に応じてどちらかの階層に格納されます。FabricPool を使用すると、パフォーマンス、効率、保護を犠牲にすることなくストレージコストを削減できます。

アーキテクチャを変更する必要はなく、中央のONTAP ストレージシステムからデータベースとアプリケーションの環境を引き続き管理できます。

オブジェクトストレージとは

オブジェクトストレージは、ファイルストレージやブロックストレージなどの他のストレージアーキテクチャとは対照的に、データをオブジェクトとして管理するストレージアーキテクチャです。オブジェクトは単一のコンテナ（バケットなど）内に保持され、他のディレクトリ内のディレクトリにファイルとしてネストされることはありません。一般にオブジェクトストレージはファイルストレージやブロックストレージよりもパフォーマンスは低くなりますが、拡張性は大幅に向上します。StorageGRID バケットはペタバイト単位のデータを保持できます。

**StorageGRID** を**FabricPool** クラウド階層として使用する

FabricPool では、 ONTAP データを StorageGRID などの多数のオブジェクトストアプロバイダに階層化できます。サポートされる 1 秒あたりの最大入出力処理数（ IOPS ）をバケットレベルまたはコンテナレベルで設定する可能性があるパブリッククラウドとは異なり、 StorageGRID のパフォーマンスはシステム内のノード数に応じて拡張されます。StorageGRID を FabricPool クラウド階層として使用すると、コールドデータをプライベートクラウド内に保持することで、最高のパフォーマンスと完全なデータ管理を実現できます。

また、 StorageGRID をクラウド階層として使用する場合は、 FabricPool ライセンスは必要ありません。

**StorageGRID** で複数の**ONTAP** クラスタを使用する

以下の手順では、 StorageGRID を単一の ONTAP クラスタに接続する方法について説明します。ただし、同じ StorageGRID システムを複数の ONTAP クラスタに接続することができます。

複数の ONTAP クラスタから単一の StorageGRID システムにデータを階層化する場合は、クラスタごとに異なる S3 バケットを使用する必要があります。要件に応じて、すべてのクラスタに同じハイアベイラビリティ（ HA ）グループ、ロードバランサエンドポイント、およびテナントアカウントを使用するか、またはクラスタごとにこれらの項目をそれぞれ設定できます。

## **StorageGRID** をクラウド階層として接続するために必要な情報

StorageGRID をFabricPool のクラウド階層として接続する前に、StorageGRID でいくつかの設定手順を実行して特定の値を取得する必要があります。

このタスクについて

次の表に、 FabricPool のクラウド階層として StorageGRID を接続する場合に ONTAP に入力する必要がある情報を示します。このセクションのトピックでは、 StorageGRID のグリッドマネージャとテナントマネージ

ャを使用して必要な情報を取得する方法について説明します。

表示されるフィールド名と ONTAP で必要な値の入力プロセスは、 ONTAP CLI （ storage aggregate object-store config create ）と ONTAP System Manager （ * Storage * > * Aggregates & Disks * > * Cloud Tier * ）のどちらを使用しているかによって異なります。

詳細については、以下を参照してください。

- "TR-4598：『FabricPool Best Practices for ONTAP 9.8』"
- "ONTAP 9 ドキュメンテーション・センター"

| **ONTAP** フィールド | 説明 |
| --- | --- |
| オブジェクトストア名 | 一意でわかりやすい名前。例： `StorageGRID_Cloud_Tier`。 |
| プロバイダタイプ | StorageGRID （System Manager）または `SGWS` （CLI）。 |
| ポート | FabricPool が StorageGRID に接続するときに使用するポート。StorageGRID ロードバランサエンドポイントを定義する際に使用するポート番号を指定します。<br><br>"FabricPool のロードバランサエンドポイントの作成" |
| サーバ名 | StorageGRID ロードバランサエンドポイントの完全修飾ドメイン名（ FQDN ）。例： `s3.storagegrid.company.com`。<br><br>次の点に注意してください。<br><br>• ここで指定するドメイン名は、 StorageGRID ロードバランサエンドポイント用にアップロードする CA 証明書のドメイン名と一致する必要があります。<br>• このドメイン名の DNS レコードは、 StorageGRID への接続に使用する各 IP アドレスにマッピングする必要があります。<br><br>"StorageGRID IPアドレス用のDNSサーバを設定する" |
| コンテナ名 | この ONTAP クラスタで使用する StorageGRID バケットの名前。例： `fabricpool-bucket`。このバケットはTenant Managerで作成します。<br><br>次の点に注意してください。<br><br>• 設定の作成後にバケット名を変更することはできません。<br>• バケットでバージョン管理を有効にすることはできません。<br>• データを StorageGRID に階層化する ONTAP クラスタごとに異なるバケットを使用する必要があります。<br><br>"S3バケットを作成してアクセスキーを取得する" |

| ONTAP フィールド | 説明 |
| --- | --- |
| アクセスキーとシークレットのパスワード | StorageGRID テナントアカウントのアクセスキーとシークレットアクセスキー。<br><br>これらの値は Tenant Manager で生成します。<br><br>"S3バケットを作成してアクセスキーを取得する" |
| SSL | 有効にする必要があります。 |
| オブジェクトストアの証明書 | StorageGRID ロードバランサエンドポイントの作成時にアップロードした CA 証明書。<br><br>• 注：中間 CA が StorageGRID 証明書を発行した場合は、中間 CA 証明書を指定する必要があります。StorageGRID 証明書がルート CA によって直接発行された場合は、ルート CA 証明書を指定する必要があります。<br><br>"FabricPool のロードバランサエンドポイントの作成" |

完了後

必要な StorageGRID 情報を取得したら、 ONTAP にアクセスしてクラウド階層として StorageGRID を追加し、クラウド階層をアグリゲートとして追加し、ボリューム階層化ポリシーを設定できます。

ロードバランシングのベストプラクティスを参照してください

## StorageGRID をFabricPool クラウド階層として接続する前に、StorageGRID グリッドマネージャを使用して少なくとも1つのロードバランサエンドポイントを設定します。

ロードバランシングとは

データを FabricPool から StorageGRID システムに階層化すると、 StorageGRID はロードバランサを使用して取り込みと読み出しのワークロードを管理します。ロードバランシングは、 FabricPool ワークロードを複数のストレージノードに分散することで、速度と接続容量を最大化します。

StorageGRID ロードバランササービスはすべての管理ノードとすべてのゲートウェイノードにインストールされ、レイヤ 7 のロードバランシングを提供します。クライアント要求の Transport Layer Security （ TLS ）終了を実行し、要求を検査し、ストレージノードへの新しいセキュアな接続を確立します。

各ノード上のロードバランササービスは、クライアントトラフィックをストレージノードに転送する際に独立して動作します。重み付きのプロセスを使用すると、ロードバランササービスは、より多くの要求をより多くの CPU を使用可能なストレージノードにルーティングします。

推奨されるロードバランシングメカニズムは StorageGRID ロードバランササービスですが、代わりにサードパーティのロードバランサを統合することもできます。詳細については、ネットアップのアカウント担当者にお問い合わせいただくか、次のテクニカルレポートを参照してください。

"StorageGRID ロードバランサオプション"

ゲートウェイノード上の別の Connection Load Balancer （ CLB ）サービスは廃止され、FabricPool での使用は推奨されなくなりました。

**StorageGRID** ロードバランシングのベストプラクティスを参照してください

一般的なベストプラクティスとして、 StorageGRID システムの各サイトにロードバランササービスを使用するノードが 2 つ以上必要です。たとえば、サイトには管理ノードとゲートウェイノードの両方、または管理ノードが2つ含まれている場合があります。SG100 または SG100 サービスアプライアンス、ベアメタルノード、仮想マシン（ VM ）ベースのノードのいずれを使用しているかに関係なく、各ロードバランシングノードに適切なネットワーク、ハードウェア、または仮想化インフラがあることを確認します。

StorageGRID ロードバランサエンドポイントを設定して、ゲートウェイノードと管理ノードが FabricPool の受信要求と送信要求に使用するポートを定義する必要があります。

ロードバランサエンドポイント証明書のベストプラクティス

FabricPool で使用するロードバランサエンドポイントを作成する際には、プロトコルとしてHTTPSを使用する必要があります。その後、公開された信頼された証明書またはプライベート認証局（CA）によって署名された証明書をアップロードするか、自己署名証明書を生成できます。この証明書は、 ONTAP が StorageGRID で認証することを許可します。

ベストプラクティスとして、 CA サーバ証明書を使用して接続を保護することを推奨します。CA によって署名された証明書は、無停止でローテーションできます。

ロードバランサエンドポイントで使用する CA 証明書を要求する場合は、証明書のドメイン名が、そのロードバランサエンドポイント用に ONTAP に入力するサーバ名と一致していることを確認してください。可能であれば、ワイルドカード（ * ）を使用して仮想ホスト形式の URL を許可します。例：

```
*.s3.storagegrid.company.com
```

StorageGRID を FabricPool クラウド階層として追加する場合は、 ONTAP クラスタにも同じ証明書をインストールする必要があります。また、ルート証明書と下位の認証局（ CA ）証明書もインストールする必要があります。

StorageGRID では、さまざまな目的でサーバ証明書が使用されます。ロードバランササービスに接続する場合は、Object Storage APIサービスエンドポイントのサーバ証明書をアップロードする必要はありません。

ロードバランシングエンドポイントのサーバ証明書の詳細を確認するには、次の手順を実行します。

- "負荷分散の管理"
- "サーバ証明書のセキュリティ強化ガイドライン"

ハイアベイラビリティグループのベストプラクティス

## StorageGRID をFabricPool クラウド階層として接続する前に、StorageGRID グリッドマネージャを使用してハイアベイラビリティ（HA）グループを設定します。

### ハイアベイラビリティ（**HA**）グループとは

FabricPool データの管理に常にロードバランササービスを使用できるようにするには、複数の管理ノードとゲートウェイノードのネットワークインターフェイスを 1 つのエンティティ（ハイアベイラビリティ（ HA ）グループと呼ばれます）にグループ化します。HA グループのアクティブノードで障害が発生した場合、グループ内の別のノードがワークロードの管理を続行できます。

各 HA グループは、関連付けられたノード上の共有サービスへの可用性の高いアクセスを提供します。たとえば、すべての管理ノードで構成されるHAグループは、一部の管理ノード管理サービスとロードバランササービスへの高可用性アクセスを提供します。ゲートウェイノードのみ、または管理ノードとゲートウェイノードの両方で構成されるHAグループは、共有ロードバランササービスへの可用性の高いアクセスを提供します。

HAグループを作成するときは、グリッドネットワーク（eth0）またはクライアントネットワーク（eth2）に属するネットワークインターフェイスを選択します。HAグループ内のすべてのインターフェイスは、同じネットワークサブネット内に存在する必要があります。

HAグループは、グループ内のアクティブインターフェイスに追加された仮想IPアドレスを1つ以上維持します。アクティブインターフェイスが使用できなくなった場合、仮想IPアドレスは別のインターフェイスに移動します。このフェイルオーバープロセスにかかる時間は通常数秒です。クライアントアプリケーションへの影響はほとんどなく、通常の再試行で処理を続行できます。

ロードバランシングノードのHAグループを設定すると、FabricPool はそのHAグループの仮想IPアドレスに接続します。

### ハイアベイラビリティ（ **HA** ）グループのベストプラクティス

FabricPool 用の StorageGRID HA グループを作成する際のベストプラクティスは、次のワークロードによって異なります。

- プライマリワークロードのデータで FabricPool を使用する場合は、データの取得の中断を回避するために、ロードバランシングノードを少なくとも 2 つ含む HA グループを作成する必要があります。
- FabricPool の snapshot-only のボリューム階層化ポリシーまたは非プライマリのローカルのパフォーマンス階層（ディザスタリカバリ先や NetApp SnapMirror ® デスティネーションなど）を使用する予定の場合は、 1 つのノードだけで HA グループを設定できます。

ここでは、アクティブ / バックアップ HA の HA グループの設定（一方のノードがアクティブでもう一方のノードがバックアップ）について説明します。ただし、 DNS ラウンドロビンまたはアクティブ / アクティブ HA を使用することもできます。これらの他の HA 構成のメリットについては、を参照してください "HA グループの設定オプション"。

### **StorageGRID IP**アドレス用の**DNS**サーバを設定する

ハイアベイラビリティグループとロードバランサエンドポイントを設定したら、 ONTAP システムのドメインネームシステム（ DNS ）に、 FabricPool が接続に使用する IP アドレスに StorageGRID サーバ名（完全修飾ドメイン名）を関連付けるレコードが含まれていることを確認する必要があります。

DNS レコードに入力する IP アドレスは、負荷分散ノードの HA グループを使用しているかどうかによって異なります。

- HA グループを設定している場合、 FabricPool はその HA グループの仮想 IP アドレスに接続します。

- HA グループを使用していない場合、 FabricPool は、任意のゲートウェイノードまたは管理ノードの IP アドレスを使用して StorageGRID ロードバランササービスに接続できます。

また、 DNS レコードが、ワイルドカード名を含む、必要なすべてのエンドポイントドメイン名を参照していることを確認する必要があります。

### FabricPool のハイアベイラビリティ（HA）グループの作成

FabricPool で使用するように StorageGRID を設定する場合は、必要に応じて 1 つ以上のハイアベイラビリティ（ HA ）グループを作成できます。HA グループは、管理ノード、ゲートウェイノード、またはその両方の 1 つ以上のネットワークインターフェイスで構成されます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限が必要です。

このタスクについて

各 HA グループは、仮想 IP アドレス（ VIP ）を使用して、関連付けられたノード上の共有サービスへの可用性の高いアクセスを提供します。

詳細については、を参照してください。を参照してください "ハイアベイラビリティグループの管理"。

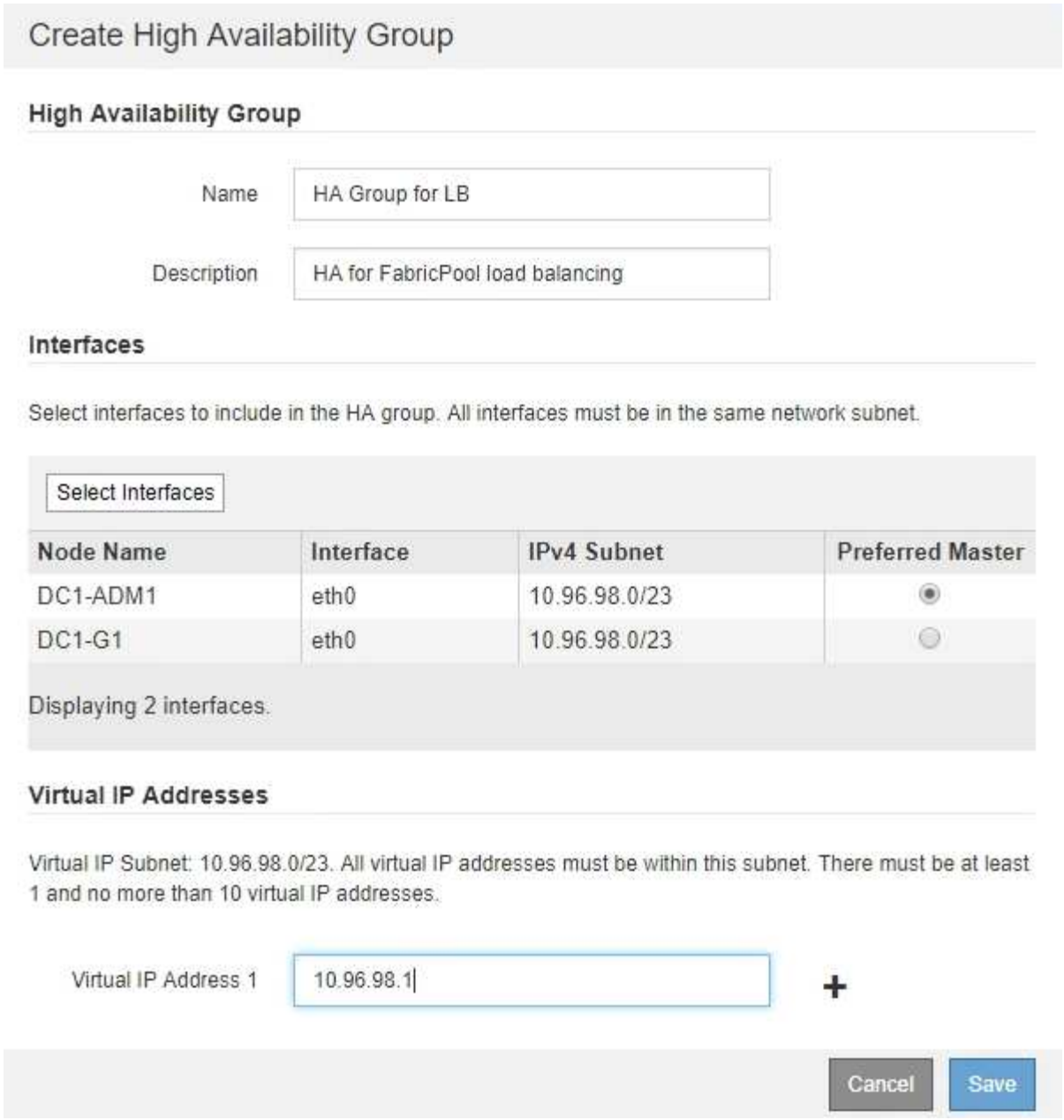
手順

1. * Configuration > Network Settings > High Availability Groups *を選択します。
2. ネットワークインターフェイスを1つ以上選択してください。ネットワークインターフェイスは、グリッドネットワーク（eth0）またはクライアントネットワーク（eth2）上の同じサブネットに属している必要があります。
3. 1つのノードを優先マスターに割り当てます。

   優先マスターは、障害が発生してVIPアドレスがバックアップインターフェイスに再割り当てされない限り、アクティブインターフェイスです。

4. HAグループのIPv4アドレスを10個まで入力します。

   すべてのメンバーインターフェイスで共有するIPv4サブネット内のアドレスを指定する必要があります。




**FabricPool** のロードバランサエンドポイントの作成

FabricPool で使用するStorageGRID を設定する場合は、ロードバランサエンドポイントを設定し、ロードバランサエンドポイント証明書をアップロードします。この証明書は、ONTAP とStorageGRID 間の接続を保護するために使用されます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限が必要です。
- 次のファイルが必要です。
  - Server Certificate ：カスタムサーバ証明書ファイル。
  - Server Certificate Private Key ：カスタムサーバ証明書の秘密鍵ファイル。

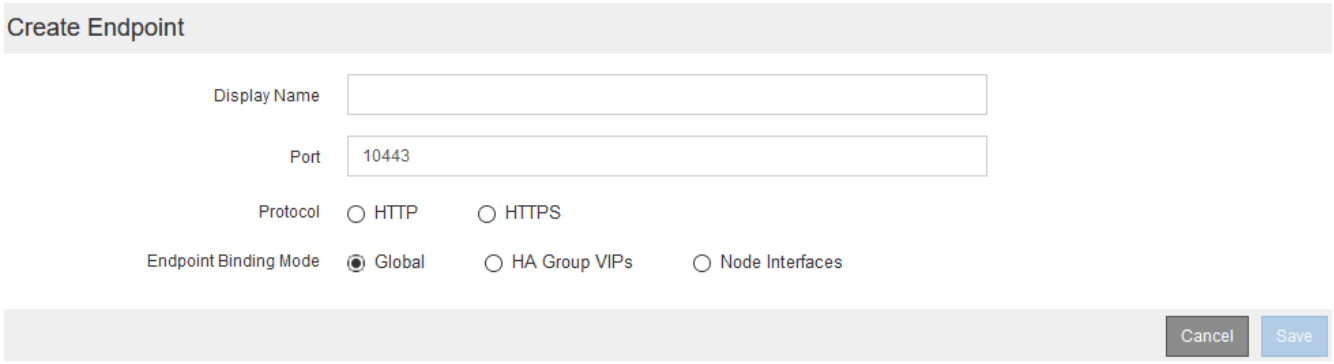
◦ CA Bundle：各中間発行認証局（CA）の証明書を含む単一のファイル。このファイルには、 PEM でエンコードされた各 CA 証明書ファイルが、証明書チェーンの順序で連結して含まれている必要があります。

このタスクについて

このタスクの詳細については、を参照してください "ロードバランサエンドポイントの設定"。

手順

1. [* Configuration > Network Settings > Load Balancer Endpoints *]を選択します。




2. [エンドポイントの追加]を選択します。
3. 次の情報を入力します。

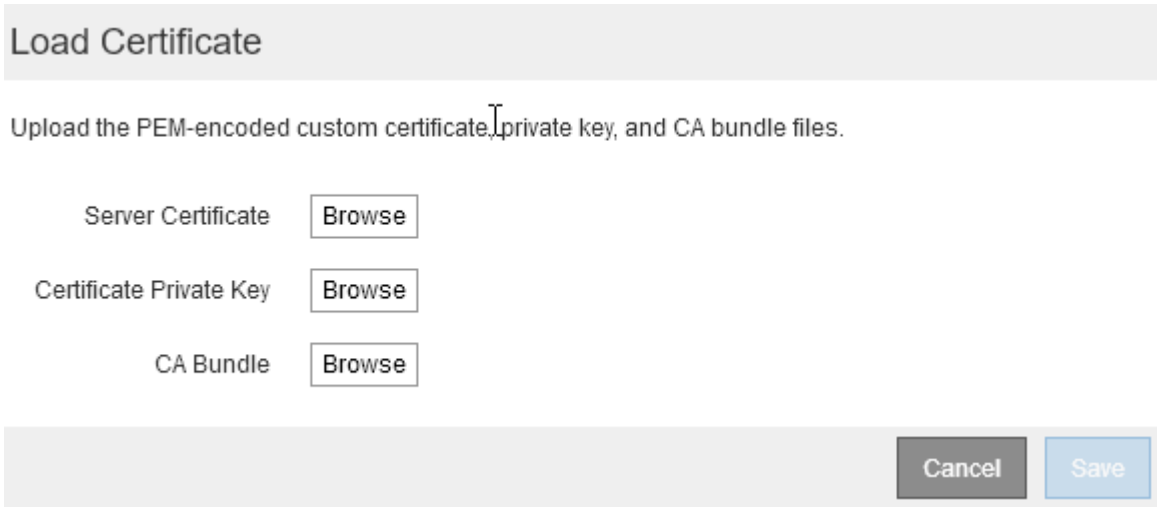
| フィールド | 説明 |
| --- | --- |
| 表示名 | エンドポイントのわかりやすい名前 |
| ポート | ロードバランシングに使用する StorageGRID ポート。このフィールドのデフォルト値は 10433 ですが、未使用の外部ポートを入力することもできます。80 または 443 と入力すると、エンドポイントは管理ノードで予約されているため、ゲートウェイノードにのみ設定されます。<br><br>• 注： * 他のグリッドサービスで使用されているポートは使用できません。内部および外部の通信に使用されるポートのリストを参照してください。<br><br>"ネットワークポートのリファレンス"<br><br>StorageGRID を FabricPool クラウド階層として接続する場合は、 ONTAP に同じポート番号を指定する必要があります。 |
| プロトコル | は* HTTPS *にする必要があります。 |

| フィールド | 説明 |
| --- | --- |
| エンドポイントバインドモード | [ グローバル * （ Global * ） ] 設定を使用するか（推奨）、このエンドポイントのアクセス性を次のいずれかに制限します。<br>• 特定のハイアベイラビリティ（ HA ）仮想 IP アドレス（ VIP ）。このオプションは、ワークロードの分離レベルを大幅に高める必要がある場合にのみ使用してください。<br>• 特定のノードの特定のネットワークインターフェイス。 |

4. [ 保存（ Save ） ] を選択します。

   [Edit Endpoint]ダイアログボックスが表示されます。

5. 「* Endpoint Service Type 」で「 S3 *」を選択します。
6. [証明書のアップロード*(推奨)]を選択し、サーバ証明書、証明書の秘密鍵、およびCAバンドルを参照します。




7. [ 保存（ Save ） ] を選択します。

**FabricPool** のテナントアカウントの作成

## Grid Manager で FabricPool 用のテナントアカウントを作成する必要があります。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

テナントアカウントを使用すると、クライアントアプリケーションで StorageGRID に対してオブジェクトの格納や読み出しを行うことができます。各テナントアカウントには、専用のアカウント ID 、許可されたグループとユーザ、バケット、オブジェクトがあります。

複数の ONTAP クラスタに同じテナントアカウントを使用できます。また、必要に応じて、 ONTAP クラスタごとに専用のテナントアカウントを作成することもできます。

> この手順は、 Grid Manager にシングルサインオン（ SSO ）が設定されていることを前提としています。SSOを使用していない場合は、の手順を使用します "StorageGRID がSSOを使用していない場合のテナントアカウントの作成"。

手順

1. 「* tenants *」を選択します
2. 「 * Create * 」を選択します。
3. FabricPool テナントアカウントの表示名を入力します。
4. S3 を選択します。
5. プラットフォームサービスの使用を有効にするには、[プラットフォームサービスを許可]チェックボックスをオンのままにします。

   プラットフォームサービスが有効になっている場合、テナントは外部サービスにアクセスする CloudMirror レプリケーションなどの機能を使用できます。
6. Storage Quota *フィールドは空白のままにします。
7. [* Root Access Group]フィールドで、テナントに対する最初のRoot Access権限を持つ既存のフェデレーテッドグループをGrid Managerから選択します。
8. [ 保存（ Save ） ] を選択します。

**S3**バケットを作成してアクセスキーを取得する

## FabricPool ワークロードで StorageGRID を使用する前に、 FabricPool データ用の S3 バケットを作成する必要があります。また、 FabricPool に使用するテナントアカウントのアクセスキーとシークレットアクセスキーを取得する必要があります。

必要なもの

- FabricPool で使用するテナントアカウントを作成しておく必要があります。

このタスクについて

ここでは、 StorageGRID テナントマネージャを使用してバケットを作成し、アクセスキーを取得する方法について説明します。テナント管理 API または StorageGRID S3 REST API を使用してこれらのタスクを実行することもできます。

詳細については、以下をご覧ください。

- "テナントアカウントを使用する"
- "S3 を使用する"

手順

1. Tenant Manager にサインインします。

   次のいずれかを実行できます。

- Grid Manager の Tenant Accounts ページで、テナントの * Sign In * リンクを選択し、クレデンシャルを入力します。
- Web ブラウザでテナントアカウントの URL を入力し、クレデンシャルを入力します。

2. FabricPool データ用の S3 バケットを作成する。

   使用する ONTAP クラスタごとに一意のバケットを作成する必要があります。

   a. ストレージ（ S3 ） * > * バケット * を選択します。
   b. [ * バケットの作成 * ] を選択します。
   c. FabricPool で使用する StorageGRID バケットの名前を入力します。例： `fabricpool-bucket`。

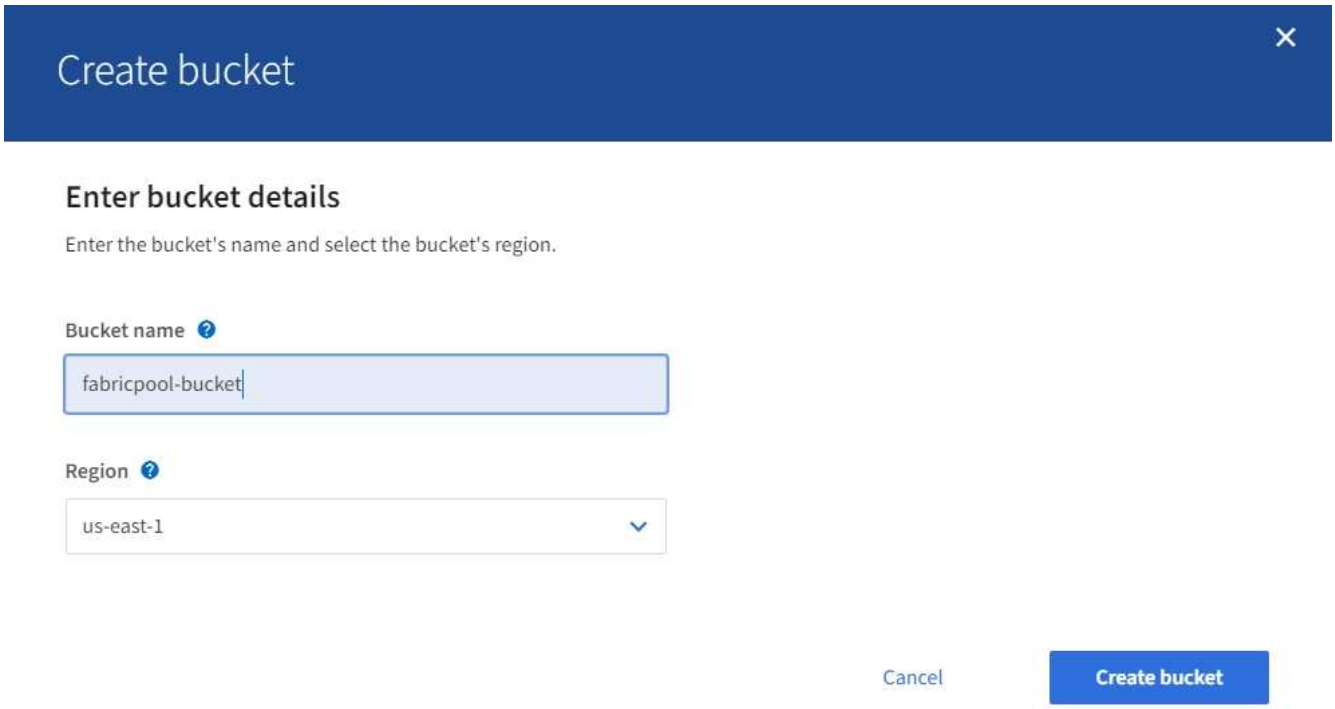
      バケットの作成後にバケット名を変更することはできません。

      バケット名は次のルールを満たす必要があります。

      - StorageGRID システム全体で（テナントアカウント内だけではなく）一意である必要があります。
      - DNS に準拠している必要があります。
      - 3 文字以上 63 文字以下にする必要があります。
      - 1 つ以上のラベルを連続して指定できます。隣接するラベルはピリオドで区切ります。各ラベルの先頭と末尾の文字は小文字のアルファベットか数字にする必要があり、使用できる文字は小文字のアルファベット、数字、ハイフンのみです。
      - テキスト形式の IP アドレスのようにはできません。
      - 仮想ホスト形式の要求でピリオドを使用しないでください。ピリオドを使用すると、サーバワイルドカード証明書の検証で原因 の問題が発生します。

   d. このバケットのリージョンを選択します。

      デフォルトでは、すべてのバケットがに作成されます `us-east-1` リージョン：




a. [ * バケットの作成 * ] を選択します。

3. アクセスキーとシークレットアクセスキーを作成します。

a. 「 * storage （ S3 ） * > * My access keys * 」を選択します。

b. 「 * キーの作成 * 」を選択します。

c. [ アクセスキーの作成 *] を選択します。

d. アクセスキー ID とシークレットアクセスキーを安全な場所にコピーするか、「 * Download.csv * 」を選択してアクセスキー ID とシークレットアクセスキーを含むスプレッドシートファイルを保存します。

これらの値は、 ONTAP で StorageGRID を FabricPool クラウド階層として設定するときに入力します。

今後新しいアクセスキーとシークレットアクセスキー StorageGRID を作成する場合は、 ONTAP がデータの格納と読み出しを中断なく行えるように、 ONTAP で対応する値をただちに更新する必要があります。

## StorageGRID の情報ライフサイクル管理と FabricPool のデータを使用する

FabricPool を使用して StorageGRID にデータを階層化する場合は、 StorageGRID 情報ライフサイクル管理（ ILM ）ルールの作成要件と、 FabricPool データを管理するための ILM ポリシーの作成要件を理解しておく必要があります。FabricPool データに適用される ILM ルールがシステム停止を伴わないようにする必要があります。

FabricPool は、 StorageGRID の ILM ルールやポリシーを認識しません。StorageGRID の ILM ポリシーの設定ミスが原因でデータが失われる可能性があります。

詳細については、以下をご覧ください。 "ILM を使用してオブジェクトを管理する"

**FabricPool** データに関する**ILM**のガイドライン

以下のガイドラインを確認し、 ILM ルールと ILM ポリシーが FabricPool データとビジネス要件に適していることを確認してください。すでに StorageGRID ILM を使用している場合は、次のガイドラインに従って、アクティブな ILM ポリシーの更新が必要になることがあります。

- レプリケーションルールとイレイジャーコーディングルールを任意に組み合わせて、クラウド階層のデータを保護できます。

  コスト効率に優れたデータ保護を実現するために、サイト内で 2+1 のイレイジャーコーディングを使用することを推奨します。イレイジャーコーディングは、レプリケーションよりも多くのCPUを使用しますが、ストレージ容量は大幅に少なくなります。4+1スキームと6+1スキームは2+1よりも少ない容量を使用しますが、グリッド拡張時にストレージノードを追加する場合にスループットが低下し、柔軟性が低下します。

- FabricPool データに適用するルールは、イレイジャーコーディングを使用するか、少なくとも 2 つのレプリケートコピーを作成する必要があります。

  ある期間にレプリケートコピーを 1 つしか作成しない ILM ルールには、データが永続的に失われるリスクがあります。オブジェクトのレプリケートコピーが 1 つしかない場合、ストレージノードに障害が発生したり、重大なエラーが発生すると、そのオブジェクトは失われます。また、アップグレードなどのメンテナンス作業中は、オブジェクトへのアクセスが一時的に失われます。

- FabricPool クラウド階層のデータが期限切れになる、または削除される ILM ルールは使用しないでください。StorageGRID ILM によって FabricPool オブジェクトが削除されないように、各 ILM ルールの保持期間を「 forever 」に設定します。
- FabricPool クラウド階層のデータをバケットから別の場所に移動するルールは作成しないでください。ILMルールを使用して、アーカイブノードを使用してFabricPool データをテープにアーカイブしたり、クラウドストレージプールを使用してFabricPool データをGlacierに移動したりすることはできません。

  クラウドストレージプールターゲットからオブジェクトを読み出すレイテンシが増加しているため、 FabricPool でクラウドストレージプールを使用することはサポートされていません。

- ONTAP 9.8 以降では、オプションでオブジェクトタグを作成して階層化データを分類およびソートし、管理を容易にすることができます。たとえば、タグを設定できるのは、 StorageGRID に接続されている FabricPool ボリュームのみです。次に、 StorageGRID で ILM ルールを作成する際に、高度なフィルタ「オブジェクトタグ」を使用してこのデータを選択し、配置します。

**FabricPool** データ用の **ILM** ポリシーの例

以下に記載するシンプルなポリシーの例をベースに、独自の ILM ルールとポリシーを作成します。

この例では、コロラド州デンバーの 1 つのデータセンターに 4 つのストレージノードがある StorageGRID システムの ILM ルールと ILM ポリシーを設計していることを前提としています。この例のFabricPool データは、というバケットを使用しています `fabricpool-bucket`。

> 以下の ILM ルールとポリシーは一例にすぎません。ILM ルールを設定する方法は多数あります。新しいポリシーをアクティブ化する前に、ドラフトポリシーをシミュレートして、コンテンツの損失を防ぐためにドラフトポリシーが想定どおりに機能することを確認してください。
>
> 詳細については、以下をご覧ください。 "ILM を使用してオブジェクトを管理する"

手順

1. *Den という名前のストレージプールを作成します。Denver サイトを選択します。
2. 2 plus 1 * という名前のイレイジャーコーディングプロファイルを作成します。2+1 イレイジャーコーディングスキームと *Den * ストレージプールを選択します。
3. のデータにのみ適用されるILMルールを作成します `fabricpool-bucket`。次のルール例では、イレイジャーコーディングコピーを作成します。

| ルール定義 | 値の例 |
| --- | --- |
| ルール名 | FabricPool データ用の 2+1 のイレイジャーコーディング |
| バケット名 | `fabricpool-bucket`<br><br>FabricPool テナントアカウントでフィルタリングすることもできます。 |
| 高度なフィルタリング | オブジェクトサイズ（ MB ）が 0.2 MB を超えています。<br><br>• 注： * FabricPool は 4MB のオブジェクトのみを書き込みますが、このルールではイレイジャーコーディングを使用するため、オブジェクトサイズフィルタを追加する必要があります。 |
| 参照時間 | 取り込み時間 |
| 配置 | 0 日目のストアから永遠に |
| を入力します | イレイジャーコーディング |
| 場所 | デン (2 プラス 1) |
| 取り込み動作 | 中間（ Balanced ） |

4. 最初のルールに一致しないオブジェクトのレプリケートコピーを 2 つ作成する ILM ルールを作成します。基本フィルタ（テナントアカウントまたはバケット名）や高度なフィルタは選択しないでください。

| ルール定義 | 値の例 |
| --- | --- |
| ルール名 | 2 つのレプリケートコピー |
| バケット名 | _ なし _ |
| 高度なフィルタリング | _ なし _ |
| 参照時間 | 取り込み時間 |
| 配置 | 0 日目のストアから永遠に |
| を入力します | レプリケート |
| 場所 | デン |
| コピー | 2. |
| 取り込み動作 | 中間（ Balanced ） |

5. ドラフトの ILM ポリシーを作成して 2 つのルールを選択レプリケーションルールではフィルタを使用しないため、ポリシーのデフォルト（最後の）ルールを使用できます。
6. テストオブジェクトをグリッドに取り込みます。
7. ポリシーをテストオブジェクトでシミュレートして動作を確認します。
8. ポリシーをアクティブ化する。

このポリシーをアクティブ化すると、 StorageGRID はオブジェクトデータを次のように配置します。

- のFabricPool から階層化されたデータ `fabricpool-bucket` 2+1イレイジャーコーディングスキームを使用してイレイジャーコーディングされます。2 つのデータフラグメントと 1 つのパリティフラグメントが 3 つの異なるストレージノードに配置されます。
- 他のすべてのバケット内のオブジェクトがレプリケートされます。2 つのコピーが作成され、 2 つの異なるストレージノードに配置されます。
- イレイジャーコーディングコピーとレプリケートコピーは、 S3 クライアントによって削除されるまで StorageGRID に保持されます。StorageGRID ILM によってこれらの項目が削除されることはありません。

## FabricPool のトラフィック分類ポリシーを作成する

必要に応じて、 StorageGRID トラフィック分類ポリシーを設計して、 FabricPool ワークロードのサービス品質を最適化できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

- Root Access 権限が必要です。

このタスクについて

FabricPool のトラフィック分類ポリシーを作成する場合のベストプラクティスは、次のようにワークロードによって異なります。

- FabricPool のプライマリワークロードのデータを StorageGRID に階層化する場合は、 FabricPool ワークロードの帯域幅が大半であることを確認する必要があります。トラフィック分類ポリシーを作成して、他のすべてのワークロードを制限できます。

  一般に、 FabricPool の読み取り処理は、書き込み処理よりも優先順位を付けることが重要です。

  たとえば、他の S3 クライアントがこの StorageGRID システムを使用している場合は、トラフィック分類ポリシーを作成する必要があります。他のバケット、テナント、 IP サブネット、またはロードバランサエンドポイントのネットワークトラフィックを制限できます。

- 原則として、どの FabricPool ワークロードにも QoS 制限を課すべきではなく、他のワークロードに限定するだけです。
- 他のワークロードで設定されている制限は、ワークロードの動作が不明な場合に適用される範囲内である必要があります。また、グリッドのサイジングと機能、および想定される利用率に応じて、制限が適用されます。

詳細については、以下をご覧ください。 "トラフィック分類ポリシーの管理"

手順

1. [* Configuration **]>[** Network Settings **]>[** Traffic Classification]を選択します。
2. 名前と概要 を入力します。
3. [ 一致ルール ] セクションで、少なくとも 1 つのルールを作成します。
   a. 「 * Create * 」を選択します。
   b. [* Endpoint] を選択し、 FabricPool 用に作成したロードバランサエンドポイントを選択します。

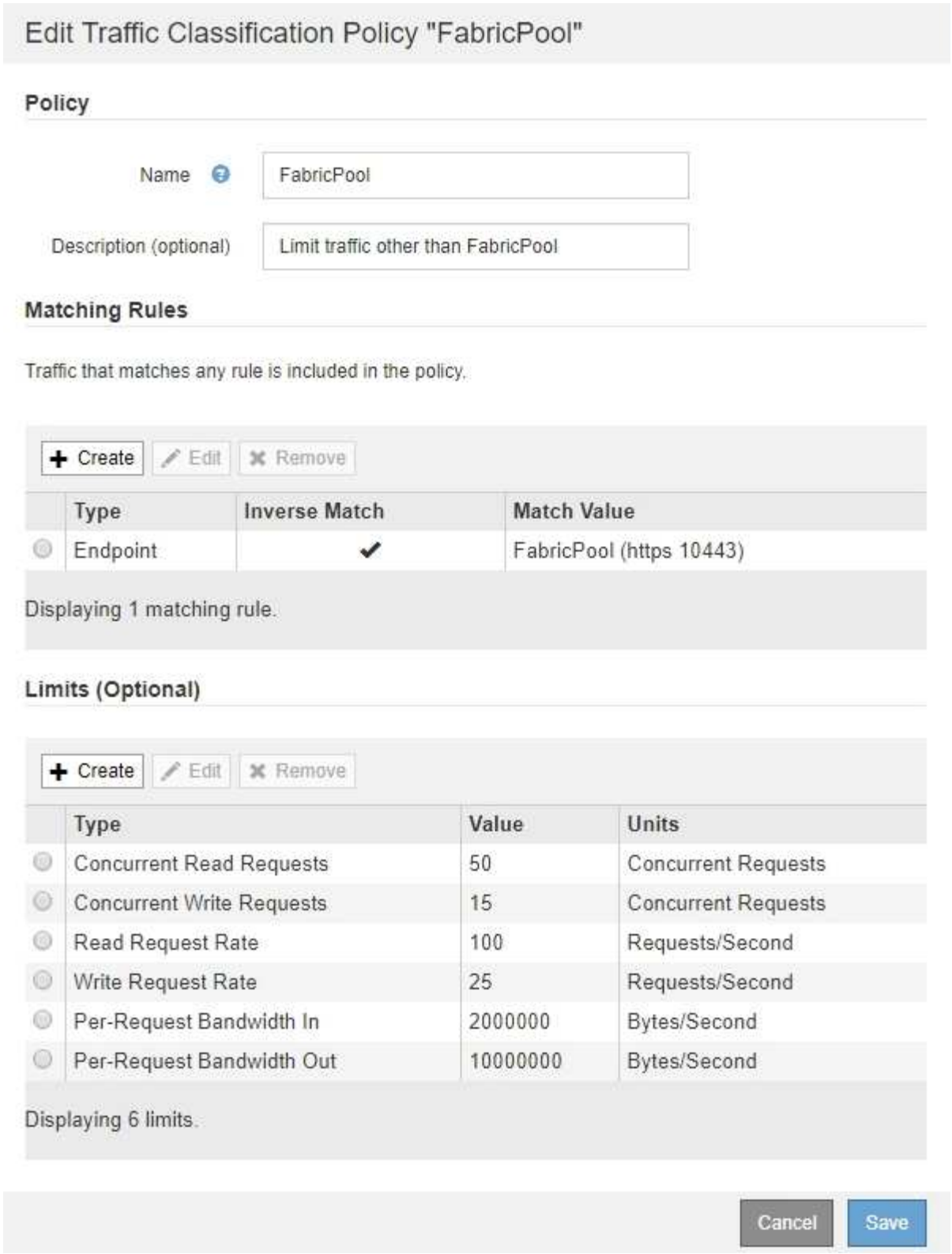
      FabricPool テナントアカウントまたはバケットを選択することもできます。

   c. このトラフィックポリシーで他のエンドポイントのトラフィックを制限する場合は、 [* 逆一致 * （ Inverse match * ） ] を選択します。
4. 必要に応じて、 1 つ以上の制限を作成します。

   トラフィック分類ポリシーに制限が設定されていない場合でも、トラフィックの傾向を把握できるようにメトリックが収集されます。

   a. 「 * Create * 」を選択します。
   b. 制限するトラフィックのタイプと適用する制限を選択します。

      次に、FabricPool トラフィック分類の例では、制限できるネットワークトラフィックのタイプと、選択できる値のタイプを示します。実際のポリシーのトラフィックタイプと値は、固有の要件に基づいています。




5. トラフィック分類ポリシーを作成した後、ポリシーを選択し、 [*Metrics] を選択して、ポリシーがトラフィックを想定どおりに制限しているかどうかを確認します。

## StorageGRID および FabricPool に関するその他のベストプラクティスです

FabricPool で使用する StorageGRID システムを設定する場合は、データの保存方法に影響する可能性があるグローバルオプションを設定しないでください。

### オブジェクトの暗号化

StorageGRID の設定時に、他のStorageGRID クライアント（* Configuration > System Settings > Grid Options *）でデータ暗号化が必要な場合は、グローバル*格納オブジェクト暗号化*設定をオプションで有効にできます。FabricPool から StorageGRID に階層化されたデータはすでに暗号化されているため、StorageGRID 設定を有効にする必要はありません。クライアント側の暗号化キーは ONTAP が所有します。

### オブジェクトの圧縮

StorageGRID を設定する場合は、グローバル*保存オブジェクトの圧縮*設定（構成>*システム設定*>*グリッドオプション*）を有効にしないでください。FabricPool から StorageGRID に階層化されたデータはすでに圧縮されています。「格納オブジェクトの圧縮」を有効にしても、オブジェクトのサイズはこれ以上縮小されません。

### 整合性レベル

FabricPool バケットの場合、推奨されるバケットの整合性レベルは* Read-after-new-write で、新しいバケットのデフォルトの設定です。**FabricPool** バケットを編集して available *やその他の整合性レベルを使用しないでください。

### FabricPool による階層化

StorageGRID ノードが NetApp AFF システムから割り当てられたストレージを使用している場合は、ボリュームで FabricPool 階層化ポリシーが有効になっていないことを確認してください。たとえば、 StorageGRID ノードが VMware ホストで実行されている場合は、 StorageGRID ノードのデータストアの作成元ボリュームで FabricPool 階層化ポリシーが有効になっていないことを確認します。StorageGRID ノードで使用するボリュームで FabricPool による階層化を無効にすることで、トラブルシューティングとストレージの処理がシンプルになります。

StorageGRID を使用して StorageGRID に関連するデータを FabricPool 自体に階層化しないでください。StorageGRID データを StorageGRID に階層化すると、トラブルシューティングと運用がより複雑になります。

# StorageGRID を使用します

## テナントアカウントを使用する

StorageGRID テナントアカウントの使用方法について説明します。

- "Tenant Managerを使用します"
- "テナントユーザのシステムアクセスの管理"
- "S3テナントアカウントの管理"
- "S3プラットフォームサービスの管理"

### Tenant Managerを使用します

Tenant Manager では、 StorageGRID テナントアカウントのすべての要素を管理できます。

Tenant Manager を使用して、テナントアカウントのストレージ使用率を監視したり、アイデンティティフェデレーションを使用するかローカルのグループとユーザを作成してユーザを管理したりできます。S3 テナントアカウントの場合は、 S3 キーの管理、 S3 バケットの管理、プラットフォームサービスの設定も行うことができます。

#### StorageGRID テナントアカウントを使用する

テナントアカウントでは、 Simple Storage Service （ S3 ） REST API または Swift REST API を使用して、StorageGRID システムでオブジェクトの格納や読み出しを行うことができます。

各テナントアカウントには、フェデレーテッド / ローカルグループ、ユーザ、 S3 バケットまたは Swift コンテナ、オブジェクトがあります。

必要に応じて、テナントアカウントを使用して、格納されているオブジェクトをエンティティごとに分離できます。たとえば、次のようなユースケースでは複数のテナントアカウントを使用できます。

- * エンタープライズのユースケース： StorageGRID システムがエンタープライズ内で使用されている場合は、組織の部門ごとにグリッドのオブジェクトストレージを分けることができます。たとえば、マーケティング部門、カスタマーサポート部門、人事部門などのテナントアカウントが存在する場合があります。

> S3 クライアントプロトコルを使用する場合は、 S3 バケットとバケットポリシーを使用してエンタープライズ内の部門間でオブジェクトを分離することもできます。個別のテナントアカウントを作成する必要はありません。S3 クライアントアプリケーションを実装するための手順を参照してください。

- * サービスプロバイダのユースケース： * StorageGRID システムがサービスプロバイダによって使用されている場合は、ストレージをリースするエンティティごとにグリッドのオブジェクトストレージを分けることができます。たとえば、会社 A 、会社 B 、会社 C などのテナントアカウントを作成できます。

##### テナントアカウントの作成

テナントアカウントは、 StorageGRID のグリッド管理者がグリッドマネージャを使用して作成します。グリ

ッド管理者は、テナントアカウントを作成する際に次の情報を指定します。

- テナントの表示名（テナントのアカウント ID は自動的に割り当てられ、変更できません）。
- テナントアカウントが S3 と Swift のどちらを使用するか。
- S3 テナントアカウントの場合：テナントアカウントにプラットフォームサービスの使用を許可するかどうか。プラットフォームサービスの使用が許可されている場合は、グリッドがその使用をサポートするように設定されている必要があります。
- 必要に応じて、テナントアカウントのストレージクォータ — テナントのオブジェクトで使用可能な最大ギガバイト数、テラバイト数、ペタバイト数。テナントのストレージクォータは、物理容量（ディスクのサイズ）ではなく、論理容量（オブジェクトのサイズ）を表します。
- StorageGRID システムでアイデンティティフェデレーションが有効になっている場合は、テナントアカウントを設定するための Root Access 権限が割り当てられているフェデレーテッドグループ。
- StorageGRID システムでシングルサインオン（ SSO ）が使用されていない場合は、テナントアカウントが独自のアイデンティティソースを使用するか、グリッドのアイデンティティソースを共有するか、およびテナントのローカル root ユーザの初期パスワード。

また、 S3 テナントアカウントが規制要件に準拠する必要がある場合は、グリッド管理者が StorageGRID システムに対して S3 オブジェクトロック設定を有効にすることができます。S3 オブジェクトのロックを有効にすると、すべての S3 テナントアカウントで準拠バケットを作成、管理できます。

#### S3テナントを設定する

S3 テナントアカウントが作成されたら、 Tenant Manager にアクセスして次のタスクを実行できます。

- アイデンティティフェデレーションの設定（グリッドとアイデンティティソースを共有する場合を除く）、またはローカルグループおよびユーザの作成
- S3 アクセスキーの管理
- 準拠バケットを含む S3 バケットを作成、管理します
- プラットフォームサービスの使用（有効な場合）
- ストレージ使用状況を監視しています

> Tenant Manager を使用して S3 バケットを作成および管理できますが、オブジェクトを取り込んで管理するには、 S3 アクセスキーを取得し、 S3 REST API を使用する必要があります。

#### Swiftテナントを設定します

Swift テナントアカウントが作成されたら、 Root Access 権限を持つユーザは Tenant Manager にアクセスして、次のようなタスクを実行できます。

- アイデンティティフェデレーションの設定（グリッドとアイデンティティソースを共有する場合を除く）、およびローカルグループとユーザの作成
- ストレージ使用状況を監視しています

> Swift ユーザが Tenant Manager にアクセスするには、 Root Access 権限が必要です。ただし Root Access 権限では、 Swift REST API に認証してコンテナを作成したりオブジェクトを取り込んだりすることはできません。Swift REST API に認証するには、 Swift 管理者の権限が必要です。

関連情報

"StorageGRID の管理"

"S3 を使用する"

"Swift を使用します"

**Web** ブラウザの要件

## サポートされている Web ブラウザを使用する必要があります。

| **Web** ブラウザ | サポートされる最小バージョン |
| --- | --- |
| Google Chrome | 87 |
| Microsoft Edge の場合 | 87 |
| Mozilla Firefox | 84 |

ブラウザウィンドウの幅を推奨される値に設定してください。

| ブラウザの幅 | ピクセル |
| --- | --- |
| 最小（ Minimum ） | 1024 |
| 最適 | 1280 |

**Tenant Manager**にサインインします

## Tenant Manager にアクセスするには、サポート対象の Web ブラウザのアドレスバーにテナントの URL を入力します。

必要なもの

- ログインクレデンシャルが必要です。
- Grid 管理者から提供された Tenant Manager にアクセスするための URL を用意しておく必要があります。URL は次のいずれかの例のようになります。

```
https://FQDN_or_Admin_Node_IP/
```

```
https://FQDN_or_Admin_Node_IP:port/
```

```
https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id
```

```
https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id
```

URL には、管理ノードへのアクセスに使用される完全修飾ドメイン名（ FQDN ）または IP アドレスが必ず含まれ、オプションでポート番号、 20 桁のテナントアカウント ID 、またはその両方が追加されます。

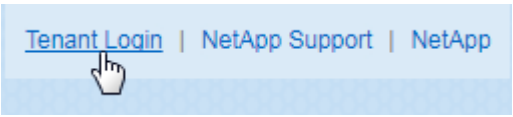
- URL に 20 桁のテナントアカウント ID が含まれていない場合は、このアカウント ID を確認しておく必要があります。
- サポートされているWebブラウザを使用する必要があります。
- Web ブラウザでクッキーが有効になっている必要があります。
- 特定のアクセス権限が必要です。

手順

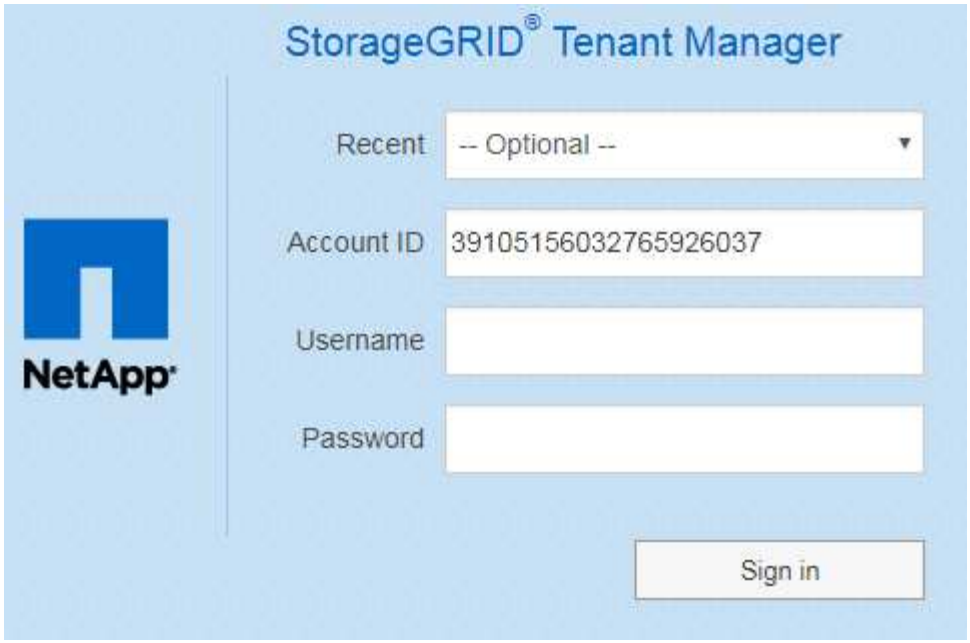
1. サポートされている Web ブラウザを起動します。
2. ブラウザのアドレスバーに、 Tenant Manager にアクセスするための URL を入力します。
3. セキュリティアラートが表示された場合は、ブラウザのインストールウィザードを使用して証明書をインストールします。
4. Tenant Manager にサインインします。

   表示されるサインイン画面は、入力した URL と、組織がシングルサインオン（ SSO ）を使用しているかどうかによって異なります。次のいずれかの画面が表示されます。

   - Grid Manager のサインインページが表示されます。右上の * Tenant Login * リンクをクリックします。

   - Tenant Manager のサインインページが表示されます。以下に示すように、「 * アカウント ID * 」フィールドはすでに入力されている可能性があります。



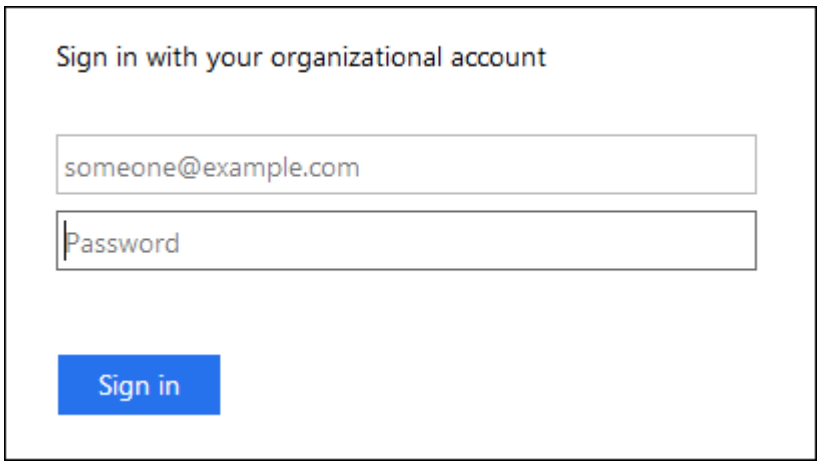

i. テナントの 20 桁のアカウント ID が表示されない場合は、最近のアカウントのリストにテナントアカウントが表示されている場合はその名前を選択するか、アカウント ID を入力します。

ii. ユーザ名とパスワードを入力します。

iii. [ * サインイン * ] をクリックします。

Tenant Manager のダッシュボードが表示されます。

◦ グリッドで SSO が有効になっている場合は、組織の SSO ページ。例：




標準の SSO クレデンシャルを入力し、 * サインイン * をクリックします。

◦ Tenant Manager の SSO サインインページ。

i. テナントの 20 桁のアカウント ID が表示されない場合は、最近のアカウントのリストにテナントアカウントが表示されている場合はその名前を選択するか、アカウント ID を入力します。

ii. [ * サインイン * ] をクリックします。

iii. 組織の SSO サインインページで通常使用している SSO クレデンシャルを使用してサインインします。

Tenant Manager のダッシュボードが表示されます。

5. 他のユーザーから初期パスワードを受け取った場合は、アカウントを保護するためにパスワードを変更してください。[***username***>*Change Password*] を選択します。

> StorageGRID システムで SSO が有効になっている場合は、テナントマネージャからパスワードを変更できません。

関連情報

"StorageGRID の管理"

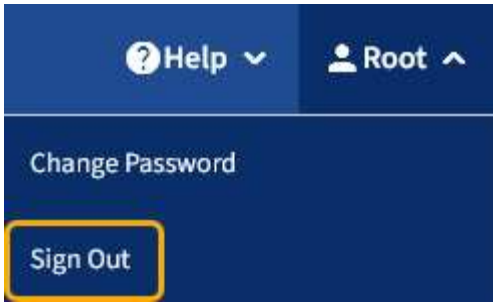
"Web ブラウザの要件"

**Tenant Manager**からサインアウトします

Tenant Manager の使用が完了したら、サインアウトして、権限のないユーザが StorageGRID システムにアクセスできないようにする必要があります。ブラウザのクッキーの設定によっては、ブラウザを閉じてもシステムからサインアウトされない場合があります。

手順

1. ユーザインターフェイスの右上にあるユーザ名ドロップダウンを探します。




2. ユーザー名を選択し、 * サインアウト * を選択します。

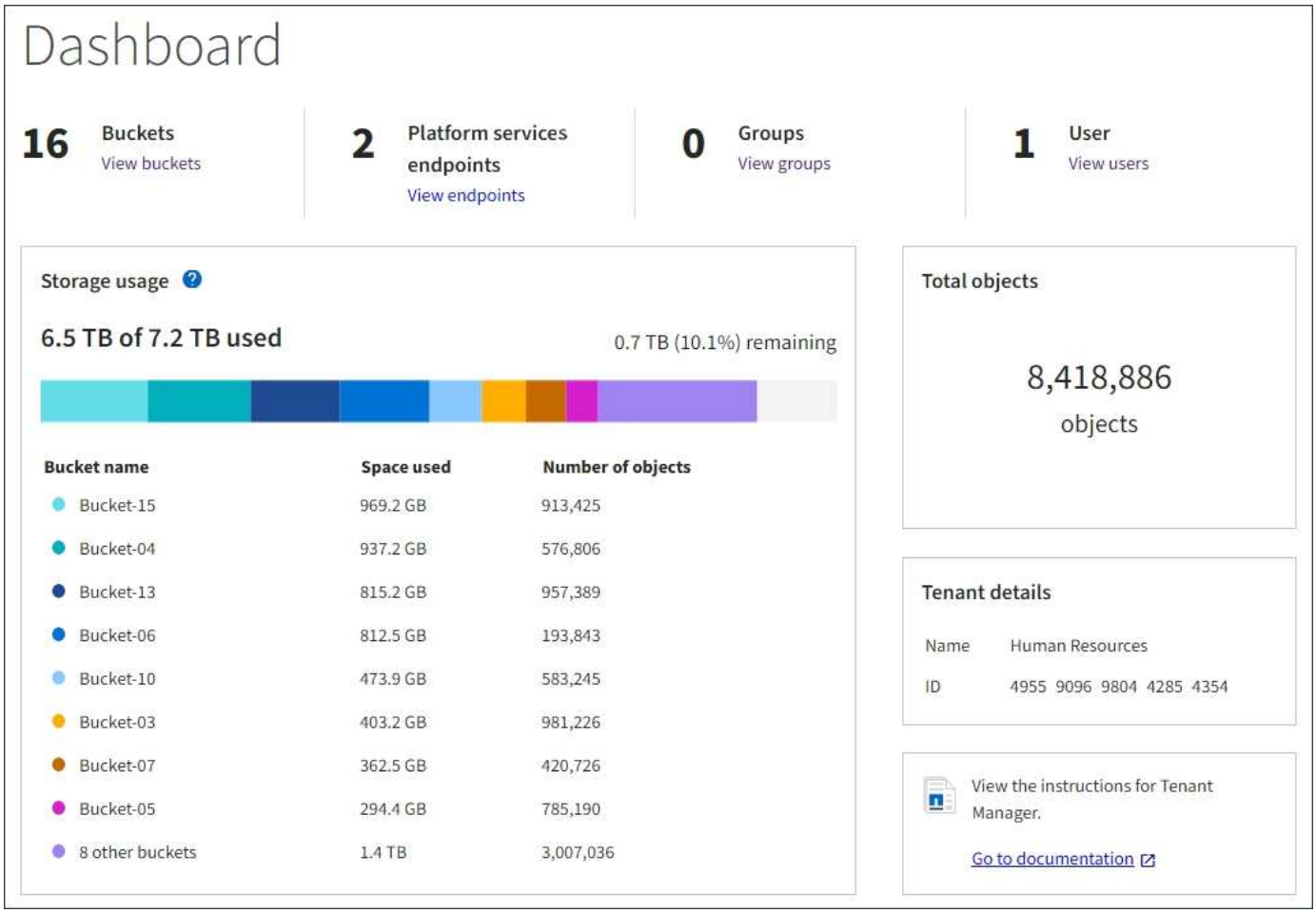
| オプション | 説明 |
| --- | --- |
| SSO は使用されていません | 管理ノードからサインアウトされます。Tenant Manager のサインインページが表示されます。<br><br>• 注： * 複数の管理ノードにサインインした場合、各ノードからサインアウトする必要があります。 |
| SSO が有効です | アクセスしていたすべての管理ノードからサインアウトされます。StorageGRID のサインインページが表示されます。アクセスしたテナントアカウントの名前がデフォルトで「 Recent Accounts * 」ドロップダウンに表示され、テナントの * アカウント ID * が表示されます。<br><br>*注：SSOが有効でGrid Managerにもサインインしている場合は、SSOからサインアウトするためにGrid Managerからもサインアウトする必要があります。 |

**Tenant Manager**のダッシュボードについて

Tenant Manager Dashboard には、テナントアカウントの設定の概要とテナントのバケット（ S3 ）またはコンテナ（ Swift ）でオブジェクトに使用されているスペースの量が表示されます。テナントにクォータがある場合は、クォータの使用量と残りの容量がダッシュボードに表示されます。テナントアカウントに関連するエラーがある場合は、ダッシュボードにそのエラーが表示されます。

使用済みスペースの値は推定値です。これらの推定値は、取り込みのタイミング、ネットワーク接続、ノードのステータスによって左右されます。

オブジェクトがアップロードされると、ダッシュボードは次のようになります。




テナントアカウントの概要

ダッシュボードの上部には、次の情報が表示されます。

- 設定されているバケットまたはコンテナ、グループ、およびユーザの数
- プラットフォームサービスエンドポイントの数（設定されている場合）

リンクを選択すると詳細を確認できます。

ダッシュボードの右側には、次の情報が表示されます。

- テナントのオブジェクトの合計数。

  S3 アカウントでは、オブジェクトが取り込まれておらず、 Root Access 権限がある場合は、オブジェクトの総数ではなく、「 Getting started 」というガイドラインが表示されます。

- テナントアカウントの名前とID。
- StorageGRID のドキュメントへのリンク。

ストレージとクォータの使用状況

ストレージ使用状況パネルには、次の情報が表示されます。

- テナントのオブジェクトデータの量。

アップロードされたオブジェクトデータの合計量を示します。オブジェクトとそのメタデータのコピーを格納するために使用されるスペースは表示されません。

- クォータが設定されている場合は、オブジェクトデータに使用できるスペースの合計容量、および残りのスペースの量と割合。クォータは、取り込むことができるオブジェクトデータの量を制限します。

  クォータ使用率は内部の推定値に基づいており、場合によっては超過することがあります。たとえば、テナントがクォータを超えた場合、 StorageGRID はテナントがオブジェクトのアップロードを開始したときにクォータをチェックし、新しい取り込みを拒否します。ただし、 StorageGRID では、クォータを超過したかどうかを判断する際に、現在のアップロードのサイズは考慮されません。オブジェクトが削除された場合、クォータ使用率が再計算されるまでテナントが一時的に新しいオブジェクトをアップロードできなくなることがあります。クォータ使用率の計算には 10 分以上かかることがあります。

- 最大のバケットまたはコンテナの相対サイズを表す棒グラフ。

  任意のグラフセグメントにカーソルを合わせると、そのバケットまたはコンテナで消費されている合計スペースが表示されます。

- 棒グラフに対応するために、オブジェクトデータの合計量と各バケットまたはコンテナのオブジェクト数を含む最大のバケットまたはコンテナのリスト。

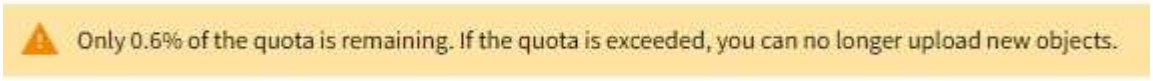
| Bucket name | Space used | Number of objects |
|---|---|---|
| Bucket-02 | 944.7 GB | 7,575 |
| Bucket-09 | 899.6 GB | 589,677 |
| Bucket-15 | 889.6 GB | 623,542 |
| Bucket-06 | 846.4 GB | 648,619 |
| Bucket-07 | 730.8 GB | 808,655 |
| Bucket-04 | 700.8 GB | 420,493 |
| Bucket-11 | 663.5 GB | 993,729 |
| Bucket-03 | 656.9 GB | 379,329 |
| 9 other buckets | 2.3 TB | 5,171,588 |

  テナントに 9 つ以上のバケットまたはコンテナがある場合は、他のすべてのバケットまたはコンテナがリストの一番下にある 1 つのエントリに結合されます。

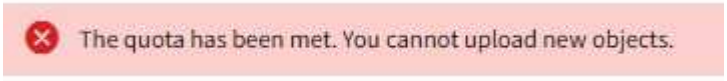
クォータ使用状況アラート

Grid Manager でクォータ使用アラートが有効になっている場合、クォータの下限または超過時に次のように Tenant Manager に表示されます。

テナントのクォータの 90% 以上が使用されると、「テナントクォータ使用率が高い * 」アラートがトリガーされます。詳細については、 StorageGRID の監視とトラブルシューティングの手順にあるアラートリファレンスを参照してください。



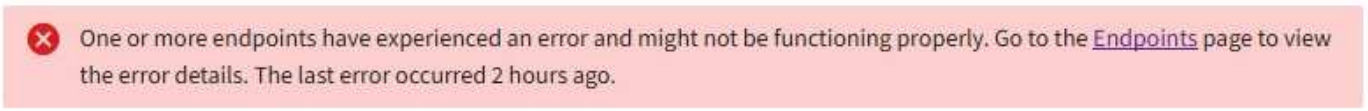

クォータを超えた場合、新しいオブジェクトをアップロードすることはできません。




詳細を表示してアラートのルールと通知を管理するには、 StorageGRID の監視とトラブルシューティングの手順を参照してください。

エンドポイントエラー

Grid Manager を使用して 1 つ以上のエンドポイントをプラットフォームサービスで使用するように設定している場合は、 Tenant Manager のダッシュボードに過去 7 日以内にエンドポイントエラーが発生した場合にアラートが表示されます。




エンドポイントエラーの詳細を表示するには、エンドポイントを選択してエンドポイントページを表示します。

関連情報

"プラットフォームサービスのエンドポイントエラーのトラブルシューティング"

"トラブルシューティングを監視します"

テナント管理**API**について

Tenant Manager のユーザインターフェイスの代わりにテナント管理 REST API を使用してシステム管理タスクを実行できます。たとえば、 API を使用して処理を自動化したり、ユーザなどの複数のエンティティを迅速に作成したりできます。

テナント管理APIでは、SwaggerオープンソースAPIプラットフォームを使用します。Swagger では、開発者でもそうでないユーザでも、わかりやすいユーザインターフェイスを利用して API を操作できます。Swagger のユーザインターフェイスでは、各 API 処理に関する詳細情報とドキュメントを参照できます。

Swagger のテナント管理 API のドキュメントにアクセスするには、次の手順を実行します。

手順

1. Tenant Manager にサインインします。
2. Tenant Managerのヘッダーで* Help > API Documentation *を選択します。

### API 処理

テナント管理 API では、使用可能な API 処理が次のセクションに分類されます。

- **account** — 現在のテナントアカウントに対する処理。ストレージの使用状況情報の取得も含まれます。
- **auth** — ユーザセッション認証を実行するための操作。

  テナント管理 API では、 Bearer トークン認証方式がサポートされています。テナントにログインするには、認証要求（つまり、 `POST /api/v3/authorize`）。ユーザが認証されると、セキュリティトークンが返されます。このトークンは、後続の API 要求（「 Authorization ： Bearer トークン」）のヘッダーで指定する必要があります。

  認証セキュリティの向上については、「クロスサイトリクエストフォージェリに対する保護」を参照してください。

  > StorageGRID システムでシングルサインオン（ SSO ）が有効になっている場合は、別の手順による認証が必要です。StorageGRID の管理手順の「シングルサインオンが有効な場合のAPIへのサインイン」を参照してください。

- *config * — 製品リリースとテナント管理 API のバージョンに関連する操作。製品リリースバージョンおよびそのリリースでサポートされる API のメジャーバージョンを一覧表示できます。
- *containers * — S3 バケットまたは Swift コンテナに対する次の処理。

| プロトコル | 許可するアクセス許可 |
| --- | --- |
| S3 | • 準拠バケットと非準拠バケットを作成する<br>• 古い準拠設定の変更<br>• オブジェクトに対して実行される処理の整合性制御を設定します<br>• バケットのCORS設定を作成、更新、および削除する<br>• オブジェクトの最終アクセス日時の更新の有効化と無効化<br>• CloudMirrorレプリケーション、通知、検索統合（メタデータ通知）などのプラットフォームサービスの構成設定の管理<br>• 空のバケットを削除中 |
| Swift | コンテナに使用する整合性レベルを設定します |

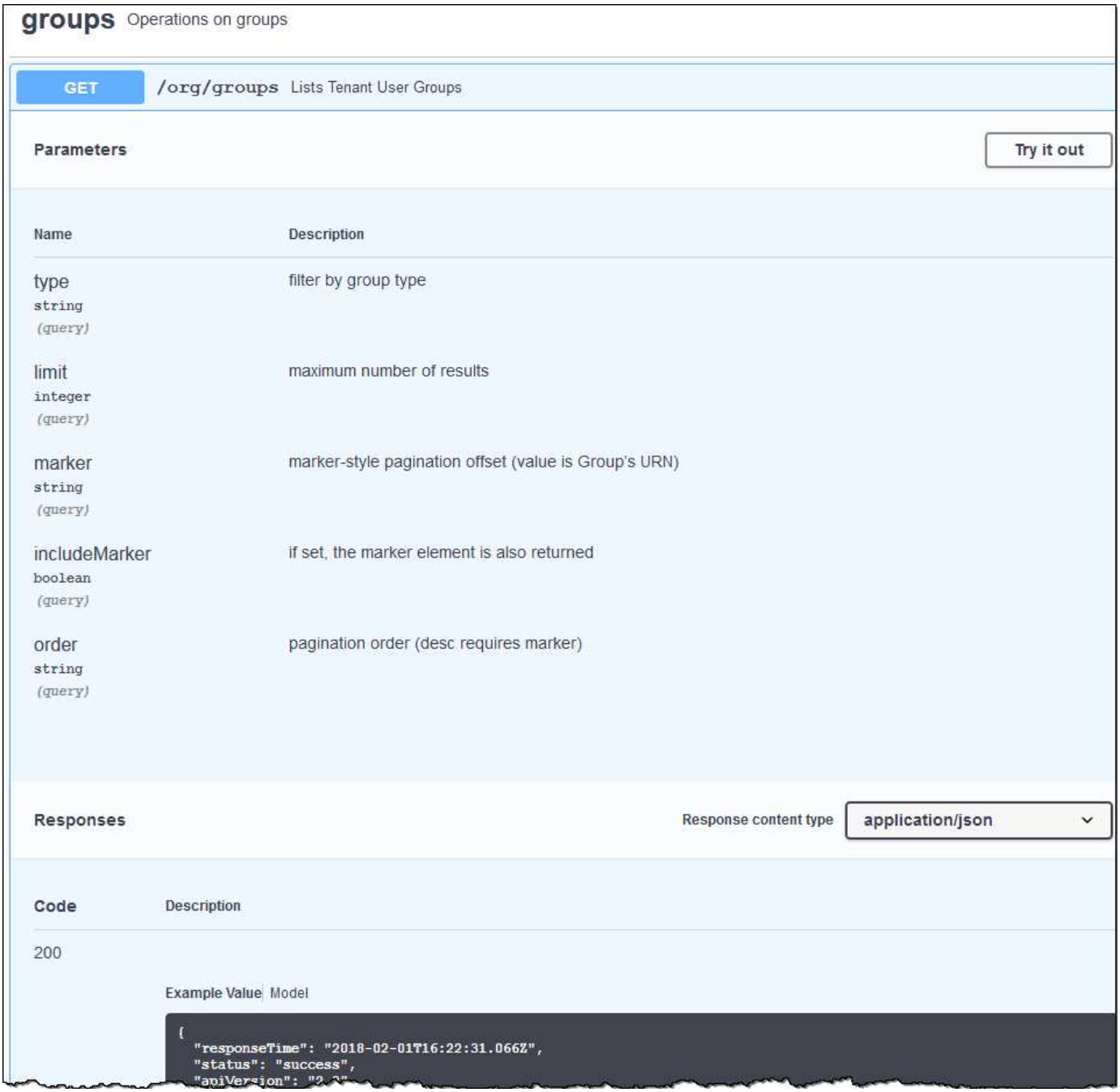
- * deactivated-features * — 非アクティブ化された可能性のある機能を表示する操作。
- * endpoints * — エンドポイントを管理するための処理。エンドポイントを使用することで、 S3 バケットは外部のサービスを StorageGRID CloudMirror レプリケーション、通知、または検索統合に使用できます。
- *groups * — ローカルテナントグループを管理し、外部アイデンティティソースからフェデレーテッドテ

ナントグループを取得するための処理。

- * identity-source * — 外部のアイデンティティソースを設定する処理、およびフェデレーテッドグループとユーザ情報を手動で同期する処理。
- **regions** — StorageGRID システムに設定されているリージョンを判別するための処理。
- * s3 * - テナントユーザの S3 アクセスキーを管理する処理。
- *s3-object-lock *-- StorageGRID システムのグローバルなS3オブジェクトロック（準拠）の構成を確認する処理。
- * users * — テナントユーザーを表示および管理するための操作。

処理の詳細

各 API 処理を展開表示すると、 HTTP アクション、エンドポイント URL 、必須またはオプションのパラメータのリスト、要求の本文の例（必要な場合）、想定される応答を確認できます。




**API**要求の実行

API Docs Web ページを使用して実行する API 処理はすべてその場で実行されます。設定データやその他のデータを誤って作成、更新、または削除しないように注意してください。

手順

1. HTTPアクションをクリックして、要求の詳細を表示します。
2. グループやユーザの ID など、要求で追加のパラメータが必要かどうかを確認します。次に、これらの値を取得します。必要な情報を取得するために、先に別の API 要求の問題 が必要になることがあります。
3. 要求の本文の例を変更する必要があるかどうかを判断します。その場合は、[*Model]をクリックして各フィールドの要件を確認できます。

4. [* 試してみてください * ] をクリックします。
5. 必要なパラメータを指定するか、必要に応じて要求の本文を変更します。
6. [* Execute] をクリックします。
7. 応答コードを確認し、要求が成功したかどうかを判断します。

関連情報

"クロスサイトリクエストフォージェリ（CSRF）の防止"

"StorageGRID の管理"

テナント管理 **API** のバージョン管理

## テナント管理 API では、バージョン管理機能を使用して無停止アップグレードがサポートされます。

たとえば、次の要求 URL ではバージョン 3 の API が指定されています。

```
https://hostname_or_ip_address/api/v3/authorize
```

旧バージョンとの互換性がない *_not compatible _ * の変更が行われると、テナント管理 API のメジャーバージョンが上がります。以前のバージョンと互換性がある _ * の変更を行うと、テナント管理 API のマイナーバージョンが上がります。互換性のある変更には、新しいエンドポイントやプロパティの追加などがあります。次の例は、変更のタイプに基づいて API バージョンがどのように更新されるかを示しています。

| **API** に対する変更のタイプ | 古いバージョン | 新しいバージョン |
|---|---|---|
| 旧バージョンと互換性があります | 2.1 | 2.2. |
| 旧バージョンとの互換性がありません | 2.1 | 3.0 |

StorageGRID ソフトウェアを初めてインストールした場合は、最新バージョンのテナント管理 API のみが有効になります。ただし、 StorageGRID を新しい機能リリースにアップグレードした場合、少なくとも StorageGRID の機能リリース 1 つ分の間は、古い API バージョンにも引き続きアクセスできます。

古い要求は、次の方法で廃止とマークされます。

- 応答ヘッダーが「 Deprecated ： true 」となる。
- JSON 応答の本文に「 deprecated ： true 」が追加される

現在のリリースでサポートされている**API**バージョンを確認します

サポートされている API のメジャーバージョンのリストを返すには、次の API 要求を使用します。

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2019-01-10T20:41:00.845Z",
  "status": "success",
  "apiVersion": "3.0",
  "data": [
    2,
    3
  ]
}
```

要求の**API**バージョンの指定

パスパラメータを使用してAPIバージョンを指定できます (`/api/v3`）またはヘッダー (`Api-Version: 3` ）。両方の値を指定した場合は、ヘッダー値がパス値よりも優先されます。

```
curl https://[IP-Address]/api/v3/grid/accounts

curl -H "Api-Version: 3" https://[IP-Address]/api/grid/accounts
```

クロスサイトリクエストフォージェリ（**CSRF**）の防止

CSRF トークンを使用してクッキーによる認証を強化すると、 StorageGRID に対するクロスサイトリクエストフォージェリ（ CSRF ）攻撃を防ぐことができます。Grid Manager と Tenant Manager はこのセキュリティ機能を自動的に有効にします。他の API クライアントは、サインイン時にこの機能を有効にするかどうかを選択できます。

攻撃者が別のサイト（たとえば、 HTTP フォーム POST を使用して）への要求をトリガーできる場合、サインインしているユーザのクッキーを使用して特定の要求を原因 が送信できます。

StorageGRID では、 CSRF トークンを使用して CSRF 攻撃を防ぐことができます。有効にした場合、特定のクッキーの内容が特定のヘッダーまたは特定の POST パラメータの内容と一致する必要があります。

この機能を有効にするには、を設定します `csrfToken` パラメータの値 `true` 認証中です。デフォルトはです `false`。

```
curl -X POST --header "Content-Type: application/json" --header "Accept:
application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

trueの場合は、Aです `GridCsrfToken` クッキーは、Grid Managerおよびへのサインインにランダムな値を使用して設定されます `AccountCsrfToken` クッキーは、Tenant Managerへのサインインではランダムな値で設定されます。

クッキーが存在する場合は、システムの状態を変更できるすべての要求（ POST 、 PUT 、 PATCH 、 DELETE ）には次のいずれかが含まれている必要があります。

- 。 `X-Csrf-Token` CSRFトークンクッキーの値がヘッダーに設定されています。
- エンドポイントがフォームエンコードされた本文を受け入れる場合：A `csrfToken` フォームエンコードされた要求の本文パラメータ。

その他の例および詳細については、オンラインの API ドキュメントを参照してください。

> CSRFトークンクッキーが設定されている要求では、も適用されます `"Content-Type: application/json"` CSRF攻撃からの保護がさらに強化されるために、JSON要求の本文が必要なすべての要求のヘッダー。

## テナントユーザのシステムアクセスの管理

テナントアカウントへのアクセス権をユーザに付与するには、フェデレーテッドアイデンティティソースからグループをインポートして、管理権限を割り当てます。StorageGRID システム全体でシングルサインオン（SSO）が有効になっていないかぎり、ローカルテナントグループおよびユーザを作成することもできます。

- "アイデンティティフェデレーションを使用する"
- "グループの管理"
- "ローカルユーザの管理"

### アイデンティティフェデレーションを使用する

アイデンティティフェデレーションを使用すると、テナントグループとテナントユーザを迅速に設定できます。またテナントユーザは、使い慣れたクレデンシャルを使用してテナントアカウントにサインインできます。

- "フェデレーテッドアイデンティティソースを設定する"
- "アイデンティティソースとの強制同期"
- "アイデンティティフェデレーションの無効化"

#### フェデレーテッドアイデンティティソースを設定する

テナントグループとユーザをActive Directory、OpenLDAP、Oracle Directory Serverなどの別のシステムで管理する場合は、アイデンティティフェデレーションを設定できます。

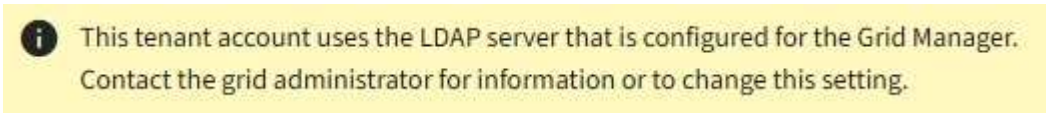
必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。

- 特定のアクセス権限が必要です。
- アイデンティティプロバイダとしてActive Directory、OpenLDAP、またはOracle Directory Serverを使用している必要があります。記載されていないLDAP v3サービスを使用する場合は、テクニカルサポートにお問い合わせください。
- LDAP サーバとの通信に Transport Layer Security （ TLS ）を使用する場合は、アイデンティティプロバイダが TLS 1.2 または 1.3 を使用している必要があります。

このタスクについて

テナントにアイデンティティフェデレーションサービスを設定できるかどうかは、テナントアカウントの設定方法によって異なります。テナントが Grid Manager 用に設定されたアイデンティティフェデレーションサービスを共有する場合があります。アイデンティティフェデレーションページにアクセスしたときにこのメッセージが表示される場合は、このテナント用に別のフェデレーテッドアイデンティティソースを設定することはできません。




手順

1. アクセス管理 * > * アイデンティティフェデレーション * を選択します。
2. ［ * アイデンティティフェデレーションを有効にする * ］ を選択
3. LDAPサービスのタイプセクションで、* Active Directory 、 OpenLDAP 、または Other *を選択します。

   OpenLDAP *を選択した場合は、OpenLDAPサーバを設定します。OpenLDAPサーバの設定に関するガイドラインを参照してください。

   Oracle Directory Server を使用する LDAP サーバーの値を設定するには、 * その他 * を選択します。

4. [* その他 *] を選択した場合は、 [LDAP 属性 ] セクションのフィールドに入力します。
   - * User Unique Name * ： LDAP ユーザの一意な ID が含まれている属性の名前。この属性はと同じです `sAMAccountName` Active Directoryおよびの場合 `uid` OpenLDAPの場合。Oracle Directory Server を設定する場合は、と入力します `uid`。
   - * User UUID * ： LDAP ユーザの永続的な一意な ID が含まれている属性の名前。この属性はと同じです `objectGUID` Active Directoryおよびの場合 `entryUUID` OpenLDAPの場合。Oracle Directory Serverを設定する場合は、と入力します `nsuniqueid`。指定した属性の各ユーザの値は、 16 バイトまたは文字列形式の 32 桁の 16 進数である必要があります。ハイフンは無視されます。
   - * Group Unique name *：LDAPグループの一意なIDが含まれている属性の名前。この属性はと同じです `sAMAccountName` Active Directoryおよびの場合 `cn` OpenLDAPの場合。Oracle Directory Serverを設定する場合は、と入力します `cn`。
   - * グループ UUID * ： LDAP グループの永続的な一意な ID が含まれている属性の名前。この属性はと同じです `objectGUID` Active Directoryおよびの場合 `entryUUID` OpenLDAPの場合。Oracle Directory Serverを設定する場合は、と入力します `nsuniqueid`。指定した属性の各グループの値は、16 バイトまたは文字列形式の 32 桁の 16 進数である必要があります。ハイフンは無視されます。
5. Configure LDAP server（LDAPサーバの設定）セクションで、必要なLDAPサーバおよびネットワーク接続情報を入力します。
   - * Hostname *：LDAPサーバのホスト名またはIPアドレス。

- * Port * ： LDAP サーバへの接続に使用するポート。STARTTLS のデフォルトポートは 389 、 LDAPS のデフォルトポートは 636 です。ただし、ファイアウォールが正しく設定されていれば、任意のポートを使用できます。
- * Username * ： LDAP サーバに接続するユーザの識別名（ DN ）の完全パス。Active Directory の場合は、ダウンレベルログオン名またはユーザープリンシパル名を指定することもできます。

  指定するユーザには、グループおよびユーザを表示する権限、および次の属性にアクセスする権限が必要です。

  - `sAMAccountName` または `uid`
  - `objectGUID`、 `entryUUID`または `nsuniqueid`
  - `cn`
  - `memberOf` または `isMemberOf`
- * Password * ：ユーザ名に関連付けられたパスワード。
- * Group base DN *：グループを検索するLDAPサブツリーの識別名（DN）の完全パス。Active Directory では、ベース DN に対して相対的な識別名（ DC=storagegrid 、 DC=example 、 DC=com など）のグループをすべてフェデレーテッドグループとして使用できます。

  *グループの一意な名前*値は、所属する*グループのベースDN *内で一意である必要があります。
- * User base DN*：ユーザを検索するLDAPサブツリーの識別名（DN）の完全パス。

  *ユーザーの一意な名前*値は、それぞれが属する*ユーザーベースDN *内で一意である必要があります。

6. [* Transport Layer Security（TLS）*]セクションで、セキュリティ設定を選択します。
   - * STARTTLSを使用（推奨）*：STARTTLSを使用してLDAPサーバとの通信を保護します。これが推奨されるオプションです。
   - * LDAPS を使用 * ： LDAPS （ LDAP over SSL ）オプションでは、 TLS を使用して LDAP サーバへの接続を確立します。このオプションは互換性を確保するためにサポートされています。
   - * TLS を使用しないでください * ： StorageGRID システムと LDAP サーバの間のネットワークトラフィックは保護されません。

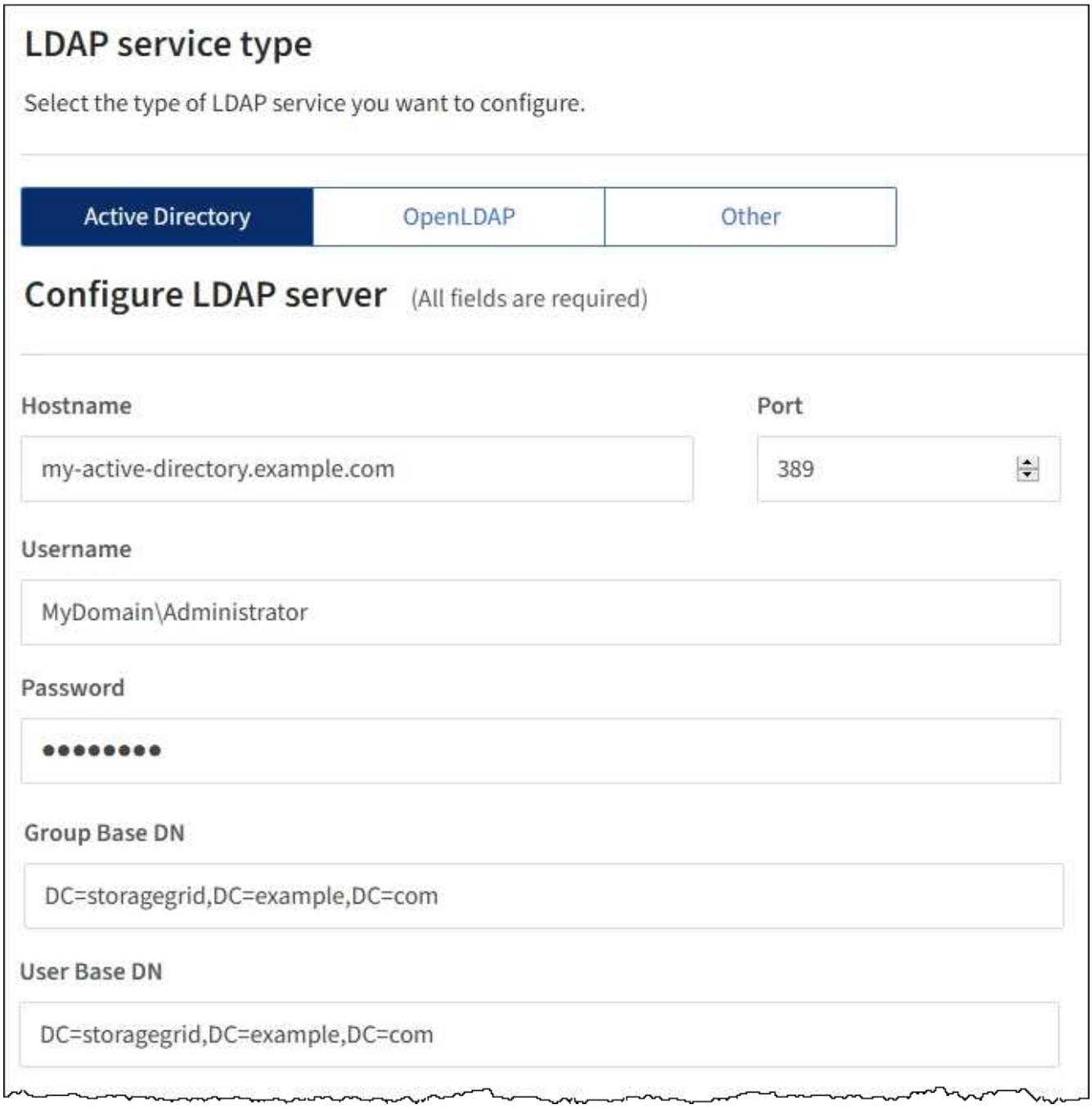
     Active DirectoryサーバでLDAP署名を適用する場合は、このオプションはサポートされていません。STARTTLS または LDAPS を使用する必要があります。
7. STARTTLS または LDAPS を選択した場合は、接続の保護に使用する証明書を選択します。
   - オペレーティング・システムの**CA**証明書を使用：オペレーティング・システムにインストールされているデフォルトのCA証明書を使用して接続を保護します。
   - * カスタム CA 証明書を使用 * ：カスタムセキュリティ証明書を使用します。

     この設定を選択した場合は、カスタムセキュリティ証明書をコピーして CA 証明書テキストボックスに貼り付けます。
8. 「接続のテスト」を選択して、LDAPサーバーの接続設定を検証します。

接続が有効な場合は、ページの右上に確認メッセージが表示されます。

9. 接続が有効な場合は、*保存*を選択します。

   次のスクリーンショットは、Active Directoryを使用するLDAPサーバの設定例を示しています。




関連情報

"テナント管理権限"

"OpenLDAP サーバの設定に関するガイドライン"

**OpenLDAP** サーバの設定に関するガイドライン

アイデンティティフェデレーションに OpenLDAP サーバを使用する場合は、

## OpenLDAP サーバで特定の設定が必要です。

### **memberof** オーバーレイと **refint** オーバーレイ

memberof オーバーレイと refint オーバーレイを有効にする必要があります。詳細については、OpenLDAPの管理者ガイドのリバースグループメンバーシップのメンテナンス手順を参照してください。

### インデックス作成

次の OpenLDAP 属性とインデックスキーワードを設定する必要があります。

```
olcDbIndex: objectClass eq
olcDbIndex: uid eq,pres,sub
olcDbIndex: cn eq,pres,sub
olcDbIndex: entryUUID eq
```

また、パフォーマンスを最適化するには、 Username のヘルプで説明されているフィールドにインデックスを設定してください。

OpenLDAPの管理者ガイドのリバースグループメンバーシップのメンテナンスに関する情報を参照してください。

アイデンティティソースとの強制同期

# StorageGRID システムは、アイデンティティソースからフェデレーテッドグループおよびユーザを定期的に同期します。ユーザの権限をすぐに有効にしたり制限したりする必要がある場合は、同期を強制的に開始できます。

必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- 保存されたアイデンティティソースが有効になっている必要があります。

手順

1. アクセス管理 * > * アイデンティティフェデレーション * を選択します。

   アイデンティティフェデレーションページが表示されます。「サーバーの同期」ボタンは、ページの右上にあります。

   > 保存されているアイデンティティソースが有効になっていない場合、*サーバーの同期*ボタンはアクティブになりません。

2. 「サーバの同期」を選択します。

   同期が開始されたことを示す確認メッセージが表示されます。

関連情報

"テナント管理権限"

アイデンティティフェデレーションの無効化

このテナントにアイデンティティフェデレーションサービスを設定した場合は、テナントグループとユーザのアイデンティティフェデレーションを一時的または永続的に無効にすることができます。アイデンティティフェデレーションを無効にすると、StorageGRID システムとアイデンティティソース間のやり取りは発生しません。ただし、設定は保持されるため、簡単に再度有効にすることができます。

必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

アイデンティティフェデレーションを無効にする前に、次の点に注意してください。

- フェデレーテッドユーザはサインインできなくなります。
- 現在サインインしているフェデレーテッドユーザは、セッションが有効な間はテナントアカウントにアクセスしたままとなりますが、セッションが期限切れになると以降はサインインできなくなります。
- StorageGRID システムとアイデンティティソース間の同期は行われません。

手順

1. アクセス管理 * > * アイデンティティフェデレーション * を選択します。
2. ［アイデンティティフェデレーションを有効にする］チェックボックスをオフにします。
3. [ 保存（ Save ） ] を選択します。

関連情報

"テナント管理権限"

グループの管理

テナントユーザが実行できるタスクを制御するには、ユーザグループに権限を割り当てます。Active Directory や OpenLDAP などのアイデンティティソースからフェデレーテッドグループをインポートすることも、ローカルグループを作成することもできます。

StorageGRID システムでシングルサインオン（ SSO ）が有効になっている場合、ローカルユーザはテナントマネージャにサインインできません。ただし、グループの権限に基づいて S3 リソースと Swift リソースにアクセスすることはできます。

テナント管理権限

テナントグループを作成する前に、そのグループに割り当てる権限を検討してください。テナント管理権限は、 Tenant Manager またはテナント管理 API を使用してユーザが実行できるタスクを決定します。ユーザは 1 つ以上のグループに属することができます。権限は、ユーザが複数のグループに属している場合に累積されます。

Tenant Manager にサインインするには、またはテナント管理 API を使用するには、少なくとも 1 つの権限が割り当てられたグループにユーザが属している必要があります。サインインできるすべてのユーザは、次のタスクを実行できます。

- ダッシュボードを表示します
- 自分のパスワードを変更する（ローカルユーザの場合）

すべての権限について、グループのアクセスモード設定によって、ユーザが設定を変更して処理を実行できるかどうか、またはユーザが関連する設定と機能のみを表示できるかどうかが決まります。

ユーザが複数のグループに属していて、いずれかのグループが読み取り専用に設定されている場合、選択したすべての設定と機能に読み取り専用でアクセスできます。

グループには次の権限を割り当てることができます。S3 テナントと Swift テナントではグループの権限が異なるので注意してください。キャッシングに時間がかかるため変更には最大で 15 分を要します。

| アクセス権 | 説明 |
| --- | --- |
| ルートアクセス（ Root Access ） | Tenant Manager とテナント管理 API へのフルアクセスを提供します。<br>• 注： * Swift ユーザがテナントアカウントにサインインするには、 Root Access 権限が必要です。 |
| 管理者 | Swift テナントのみ。このテナントアカウントの Swift コンテナとオブジェクトへのフルアクセスを提供します<br>• 注： * Swift ユーザが Swift REST API を使用して処理を実行するには、 Swift 管理者の権限が必要です。 |
| 自分の S3 クレデンシャルを管理します | S3 テナントのみ。ユーザに自分の S3 アクセスキーの作成および削除を許可します。この権限を持たないユーザには、「 * storage （ S3 ） * > * My S3 access keys * 」メニューオプションは表示されません。 |
| すべてのバケットを管理します | • S3 テナント： S3 のバケットまたはグループポリシーに関係なく、ユーザに Tenant Manager とテナント管理 API を使用して S3 バケットの作成と削除を許可し、テナントアカウント内のすべての S3 バケットの設定を管理することを許可します。<br>この権限を持たないユーザには、 **Bucket** メニューオプションは表示されません。<br>• Swift テナント： Swift ユーザにテナント管理 API を使用して Swift コンテナの整合性レベルを制御することを許可します。<br>• 注： * テナント管理 API から Swift グループに割り当てることができるのは、 Manage All Buckets 権限だけです。この権限は、 Tenant Manager を使用して Swift グループに割り当てることはできません。 |

| アクセス権 | 説明 |
| --- | --- |
| エンドポイントを管理します | S3 テナントのみ。ユーザが Tenant Manager またはテナント管理 API を使用して、 StorageGRID プラットフォームサービスのデスティネーションとして使用するエンドポイントを作成または編集できるようにします。<br><br>この権限を持たないユーザーには、 * プラットフォームサービスエンドポイント * メニューオプションは表示されません。 |

関連情報

"S3 を使用する"

"Swift を使用します"

**S3**テナント用のグループの作成

# S3 ユーザグループの権限を管理するには、フェデレーテッドグループをインポートするか、ローカルグループを作成します。

必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限を持つユーザグループに属している必要があります。
- フェデレーテッドグループをインポートする場合は、アイデンティティフェデレーションを設定済みで、フェデレーテッドグループが設定済みのアイデンティティソースにすでに存在している必要があります。

手順

1. * access management * > * Groups * を選択します。

2. 「 * グループを作成 * 」を選択します。

3. [ ローカルグループ *] タブを選択してローカルグループを作成するか、または [ フェデレーショングループ *] タブを選択して、以前に設定したアイデンティティソースからグループをインポートします。

   StorageGRID システムでシングルサインオン（ SSO ）が有効になっている場合、ローカルグループに属するユーザは Tenant Manager にサインインできません。ただし、クライアントアプリケーションを使用して、グループの権限に基づいてテナントのリソースを管理することはできます。

4. グループの名前を入力します。

   - * ローカルグループ * ：表示名と一意の名前の両方を入力します。表示名はあとで編集できます。
   - * フェデレーショングループ * ：一意の名前を入力します。Active Directoryの場合、に関連付けられている一意の名前です `sAMAccountName` 属性（Attribute）：OpenLDAPの場合は、に関連付けられている一意の名前です `uid` 属性（Attribute）：

5. 「 * Continue * 」を選択します。
6. アクセスモードを選択します。ユーザが複数のグループに属していて、いずれかのグループが読み取り専用に設定されている場合、選択したすべての設定と機能に読み取り専用でアクセスできます。

   - * Read-Write *（デフォルト）：ユーザは Tenant Manager にログインしてテナントの設定を管理できます。
   - * 読み取り専用 * ：ユーザーは設定と機能のみを表示できます。Tenant Manager またはテナント管理 API では、変更や処理を実行することはできません。ローカルの読み取り専用ユーザは自分のパスワードを変更できます。

7. このグループのグループ権限を選択します。

   テナント管理権限に関する情報を参照してください。

8. 「 * Continue * 」を選択します。
9. グループポリシーを選択して、このグループのメンバーに付与する S3 アクセス権限を決定します。

   - * S3 アクセスなし * ：デフォルト。バケットポリシーでアクセスが許可されていないかぎり、このグループのユーザは S3 リソースにアクセスできません。このオプションを選択すると、デフォルトでは root ユーザにのみ S3 リソースへのアクセスが許可されます。
   - * 読み取り専用アクセス * ：このグループのユーザには、 S3 リソースへの読み取り専用アクセスが許可されます。たとえば、オブジェクトをリストして、オブジェクトデータ、メタデータ、タグを読み取ることができます。このオプションを選択すると、テキストボックスに読み取り専用グループポリシーの JSON 文字列が表示されます。この文字列は編集できません。
   - * フルアクセス * ：このグループのユーザには、バケットを含む S3 リソースへのフルアクセスが許可されます。このオプションを選択すると、テキストボックスにフルアクセスグループポリシーの JSON 文字列が表示されます。この文字列は編集できません。
   - * カスタム * ：グループ内のユーザーには、テキストボックスで指定した権限が付与されます。言語の構文や例など、グループポリシーの詳細については、 S3 クライアントアプリケーションを実装する手順を参照してください。

10. 「 * Custom * 」を選択した場合は、グループポリシーを入力します。各グループポリシーのサイズは 5 、 120 バイトまでに制限されています。有効な JSON 形式の文字列を入力する必要があります。

    この例では、指定したバケット内のユーザ名（キープレフィックス）に一致するフォルダの表示とアクセスのみがグループのメンバーに許可されます。これらのフォルダのプライバシー設定を決めるときは、他のグループポリシーやバケットポリシーのアクセス権限を考慮する必要があります。

11. フェデレーテッドグループとローカルグループのどちらを作成するかに応じて、表示されるボタンを選択します。

    - フェデレーテッドグループ： * グループを作成 *
    - ローカルグループ： * 続行 *

    ローカルグループを作成している場合は、「 * Continue * 」を選択すると、ステップ 4 （ユーザーの追加）が表示されます。この手順は、フェデレーテッドグループに対しては表示されません。

12. グループに追加する各ユーザーのチェックボックスをオンにし、 * グループの作成 * を選択します。

    必要に応じて、ユーザを追加せずにグループを保存することもできます。後でグループにユーザを追加することも、新しいユーザを追加するときにグループを選択することもできます。

13. [ 完了 ] を選択します。

    作成したグループがグループのリストに表示されます。キャッシングに時間がかかるため変更には最大で 15 分を要します。

関連情報

"テナント管理権限"

"S3 を使用する"

**Swift**テナント用のグループの作成

Swift テナントアカウントに対するアクセス権限を管理するには、フェデレーテッドグル

ープをインポートするか、ローカルグループを作成します。Swift テナントアカウントのコンテナとオブジェクトを管理するには、少なくとも 1 つのグループが Swift 管理者権限を持っている必要があります。

必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限を持つユーザグループに属している必要があります。
- フェデレーテッドグループをインポートする場合は、アイデンティティフェデレーションを設定済みで、フェデレーテッドグループが設定済みのアイデンティティソースにすでに存在している必要があります。

手順

1. * access management * > * Groups * を選択します。

2. 「 * グループを作成 * 」を選択します。
3. [ ローカルグループ *] タブを選択してローカルグループを作成するか、または [ フェデレーショングループ *] タブを選択して、以前に設定したアイデンティティソースからグループをインポートします。

   StorageGRID システムでシングルサインオン（ SSO ）が有効になっている場合、ローカルグループに属するユーザは Tenant Manager にサインインできません。ただし、クライアントアプリケーションを使用して、グループの権限に基づいてテナントのリソースを管理することはできます。

4. グループの名前を入力します。
   - * ローカルグループ * ：表示名と一意の名前の両方を入力します。表示名はあとで編集できます。
   - * フェデレーショングループ * ：一意の名前を入力します。Active Directoryの場合、に関連付けられている一意の名前です `sAMAccountName` 属性（Attribute）：OpenLDAPの場合は、に関連付けられている一意の名前です `uid` 属性（Attribute）：
5. 「 * Continue * 」を選択します。
6. アクセスモードを選択します。ユーザが複数のグループに属していて、いずれかのグループが読み取り専

用に設定されている場合、選択したすべての設定と機能に読み取り専用でアクセスできます。

- * Read-Write *（デフォルト）：ユーザは Tenant Manager にログインしてテナントの設定を管理できます。
- * 読み取り専用 * ：ユーザーは設定と機能のみを表示できます。Tenant Manager またはテナント管理 API では、変更や処理を実行することはできません。ローカルの読み取り専用ユーザは自分のパスワードを変更できます。

7. グループ権限を設定します。
   - ユーザが Tenant Manager またはテナント管理 API にサインインする必要がある場合は、 * Root Access * チェックボックスをオンにします。（デフォルト）
   - ユーザが Tenant Manager またはテナント管理 API にアクセスする必要がない場合は、 * Root Access * チェックボックスをオフにします。たとえば、テナントにアクセスする必要がないアプリケーションのチェックボックスをオフにします。次に、 * Swift Administrator * 権限を割り当てて、これらのユーザにコンテナとオブジェクトの管理を許可します。
8. 「 * Continue * 」を選択します。
9. Swift REST API を使用する必要がある場合は、 * Swift 管理者 * チェックボックスを選択します。

   Swift ユーザが Tenant Manager にアクセスするには、 Root Access 権限が必要です。ただし Root Access 権限では、 Swift REST API に認証してコンテナを作成したりオブジェクトを取り込んだりすることはできません。Swift REST API に認証するには、 Swift 管理者の権限が必要です。

10. フェデレーテッドグループとローカルグループのどちらを作成するかに応じて、表示されるボタンを選択します。
    - フェデレーテッドグループ： * グループを作成 *
    - ローカルグループ： * 続行 *

      ローカルグループを作成している場合は、「 * Continue * 」を選択すると、ステップ 4 （ユーザーの追加）が表示されます。この手順は、フェデレーテッドグループに対しては表示されません。

11. グループに追加する各ユーザーのチェックボックスをオンにし、 * グループの作成 * を選択します。

    必要に応じて、ユーザを追加せずにグループを保存することもできます。このグループにあとでユーザを追加することも、新しいユーザを作成するときにグループを選択することもできます。

12. [ 完了 ] を選択します。

    作成したグループがグループのリストに表示されます。キャッシングに時間がかかるため変更には最大で 15 分を要します。

関連情報

"テナント管理権限"

"Swift を使用します"

グループの詳細を表示および編集する

## グループの詳細を表示する際に、グループの表示名、権限、ポリシー、およびグループに属するユーザを変更することができます。

必要なもの

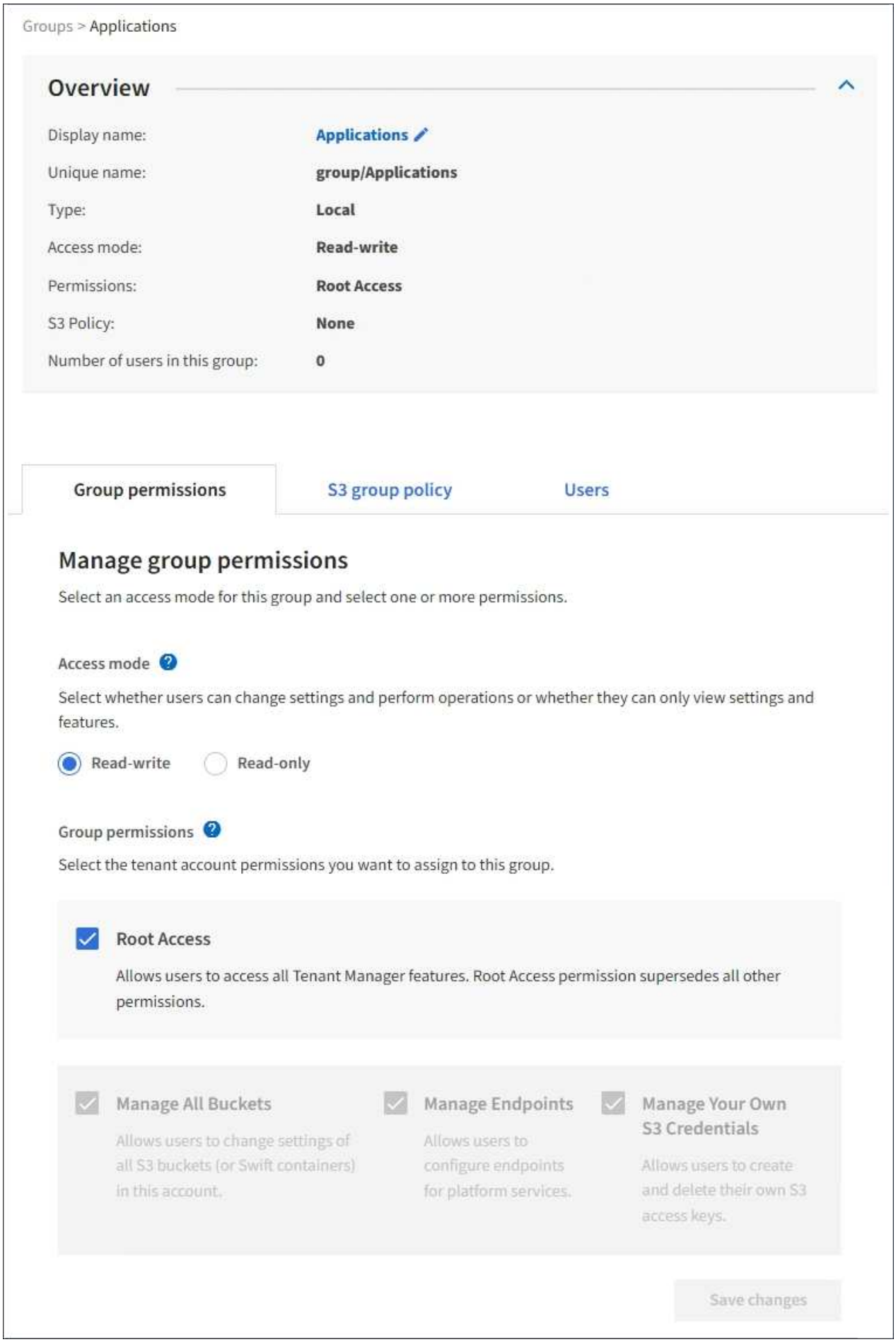
- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限を持つユーザグループに属している必要があります。

手順

1. * access management * > * Groups * を選択します。
2. 詳細を表示または編集するグループの名前を選択します。

   または、 * Actions * > * View group details * を選択します。

   グループの詳細ページが表示されます。次の例は、 S3 グループの詳細ページを表示します。


Groups > Applications
Overview
Display name:
Applications
Unique name:
group/Applications
Type:
Local
Access mode:
Read-write
Permissions:
Root Access
S3 Policy:
None
Number of users in this group:
0
Group permissions
S3 group policy
Users
Manage group permissions
Select an access mode for this group and select one or more permissions.
Access mode
Select whether users can change settings and perform operations or whether they can only view settings and features.
Read-write
Read-only
Group permissions
Select the tenant account permissions you want to assign to this group.
Root Access
Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.
Manage All Buckets
Allows users to change settings of all S3 buckets (or Swift containers) in this account.
Manage Endpoints
Allows users to configure endpoints for platform services.
Manage Your Own S3 Credentials
Allows users to create and delete their own S3 access keys.
Save changes

3. 必要に応じてグループ設定を変更します。

   変更内容を確実に保存するには、各セクションで変更を行った後に「変更を保存」を選択します。変更を保存すると、ページの右上に確認メッセージが表示されます。

   a. 必要に応じて、表示名または編集アイコンを選択します 表示名を更新します。

      グループの一意の名前は変更できません。フェデレーテッドグループの表示名は編集できません。

   b. 必要に応じて、権限を更新します。

   c. グループポリシーの場合は、 S3 または Swift テナントに適した変更を行います。

      - S3 テナントのグループを編集する場合は、必要に応じて別の S3 グループポリシーを選択します。カスタムの S3 ポリシーを選択した場合は、 JSON 文字列を必要に応じて更新します。
      - Swift テナントのグループを編集する場合は、必要に応じて、 * Swift Administrator * チェックボックスをオンまたはオフにします。

        Swift Administrator 権限の詳細については、 Swift テナント用のグループを作成する手順を参照してください。

   d. 必要に応じて、ユーザを追加または削除します。

4. 変更したセクションごとに「変更を保存」を選択したことを確認します。

   キャッシングに時間がかかるため変更には最大で 15 分を要します。

関連情報

"S3テナント用のグループの作成"

"Swiftテナント用のグループの作成"

ローカルグループへのユーザの追加

# 必要に応じて、ローカルグループにユーザを追加できます。

必要なもの

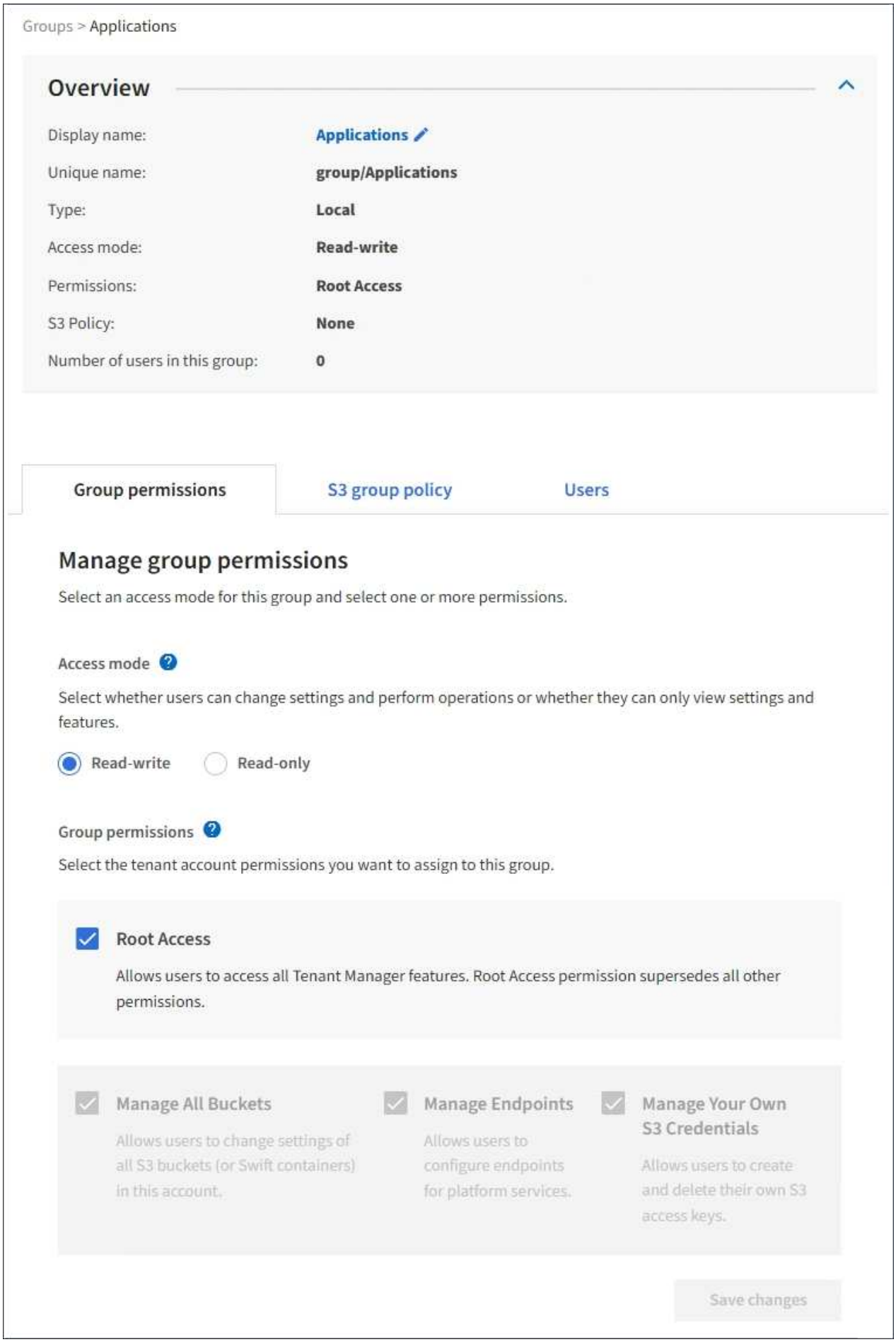
- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限を持つユーザグループに属している必要があります。

手順

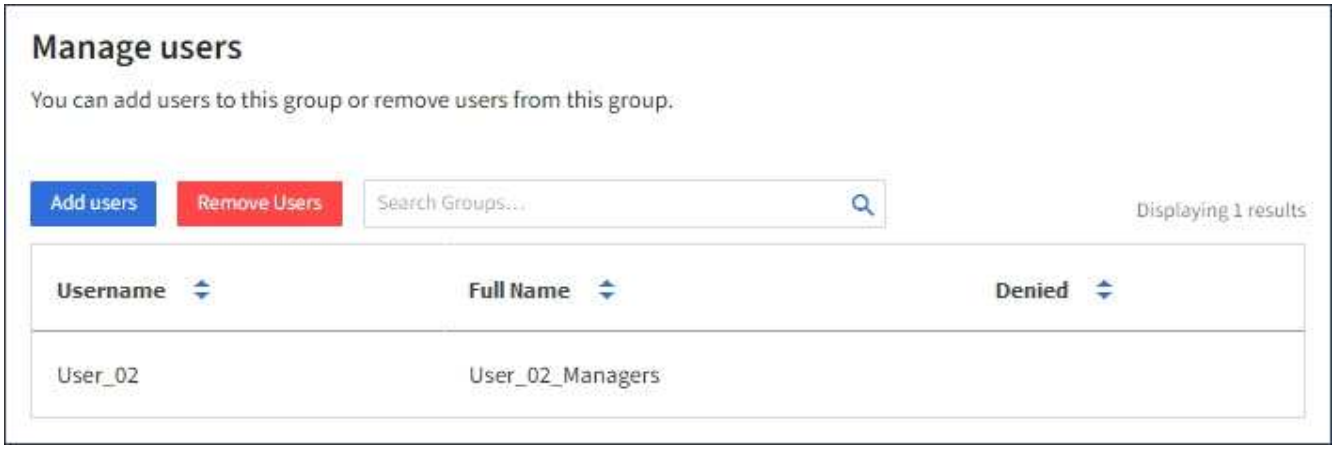
1. * access management * > * Groups * を選択します。
2. ユーザを追加するローカルグループの名前を選択します。

   または、 * Actions * > * View group details * を選択します。

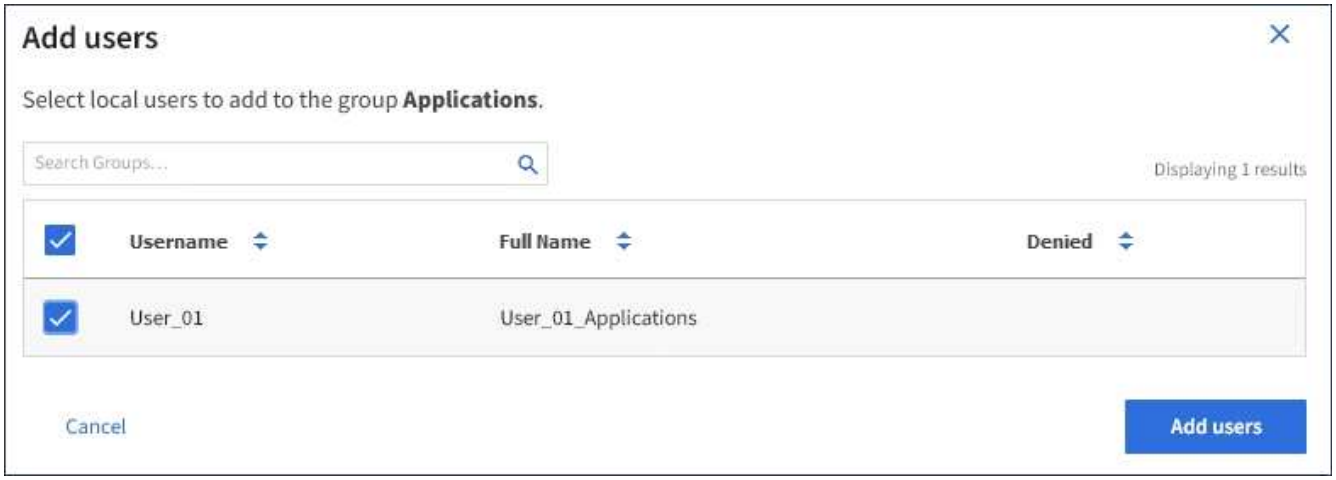
   グループの詳細ページが表示されます。


Groups > Applications
Overview
Display name:
Applications
Unique name:
group/Applications
Type:
Local
Access mode:
Read-write
Permissions:
Root Access
S3 Policy:
None
Number of users in this group:
0
Group permissions
S3 group policy
Users
Manage group permissions
Select an access mode for this group and select one or more permissions.
Access mode
Select whether users can change settings and perform operations or whether they can only view settings and features.
Read-write
Read-only
Group permissions
Select the tenant account permissions you want to assign to this group.
Root Access
Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.
Manage All Buckets
Allows users to change settings of all S3 buckets (or Swift containers) in this account.
Manage Endpoints
Allows users to configure endpoints for platform services.
Manage Your Own S3 Credentials
Allows users to create and delete their own S3 access keys.
Save changes

3. 「ユーザーの管理」を選択し、「ユーザーの追加」を選択します。




4. グループに追加するユーザーを選択し、 * ユーザーの追加 * を選択します。




ページの右上に確認メッセージが表示されます。キャッシングに時間がかかるため変更には最大で 15 分を要します。

グループ名を編集する

## グループの表示名を編集できます。グループの一意の名前は編集できません。

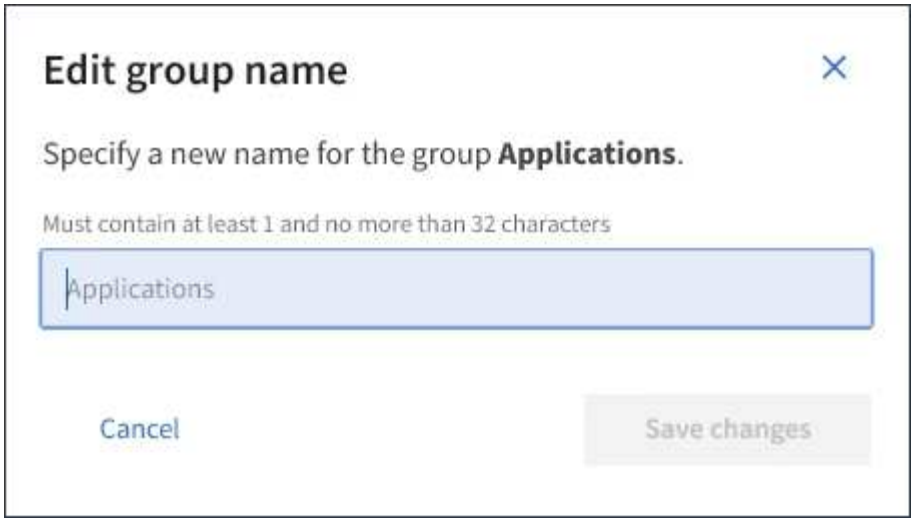
必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限を持つユーザグループに属している必要があります。

手順

1. * access management * > * Groups * を選択します。
2. 表示名を編集するグループのチェックボックスを選択します。
3. [ * アクション * > * グループ名の編集 * ] を選択します。

   Edit group name （グループ名の編集）ダイアログボックスが表示されます。




4. ローカルグループを編集する場合は、必要に応じて表示名を更新します。

   グループの一意の名前は変更できません。フェデレーテッドグループの表示名は編集できません。

5. 「変更を保存」を選択します。

   ページの右上に確認メッセージが表示されます。キャッシングに時間がかかるため変更には最大で 15 分を要します。

関連情報

"テナント管理権限"

グループを複製する

## 既存のグループを複製することで、新しいグループをより迅速に作成できます。

必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限を持つユーザグループに属している必要があります。

手順

1. * access management * > * Groups * を選択します。
2. 複製するグループのチェックボックスをオンにします。
3. 「 * グループを複製 * 」を選択します。グループの作成の詳細については、S3テナントまたはSwiftテナントのグループを作成する手順を参照してください。
4. [ ローカルグループ *] タブを選択してローカルグループを作成するか、または [ フェデレーショングループ *] タブを選択して、以前に設定したアイデンティティソースからグループをインポートします。

   StorageGRID システムでシングルサインオン（ SSO ）が有効になっている場合、ローカルグループに属するユーザは Tenant Manager にサインインできません。ただし、クライアントアプリケーションを使用して、グループの権限に基づいてテナントのリソースを管理することはできます。

5. グループの名前を入力します。

- * ローカルグループ * ：表示名と一意の名前の両方を入力します。表示名はあとで編集できます。
- * フェデレーショングループ * ：一意の名前を入力します。Active Directoryの場合、に関連付けられている一意の名前です `sAMAccountName` 属性（Attribute）：OpenLDAPの場合は、に関連付けられている一意の名前です `uid` 属性（Attribute）：

6. 「 * Continue * 」を選択します。
7. 必要に応じて、このグループの権限を変更します。
8. 「 * Continue * 」を選択します。
9. 必要に応じて、 S3 テナントのグループを複製する場合は、 * S3 ポリシーの追加 * オプションボタンとは別のポリシーを選択します。カスタムポリシーを選択した場合は、 JSON 文字列を必要に応じて更新します。
10. 「 * グループを作成 * 」を選択します。

関連情報

"S3テナント用のグループの作成"

"Swiftテナント用のグループの作成"

"テナント管理権限"

グループを削除しています

## システムからグループを削除できます。そのグループに属するユーザは、 Tenant Manager にサインインしたりテナントアカウントを使用したりすることはできなくなります。

必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限を持つユーザグループに属している必要があります。

手順

1. * access management * > * Groups * を選択します。

2. 削除するグループのチェックボックスを選択します。
3. [ * アクション * > * グループの削除 * ] を選択します。

   確認メッセージが表示されます。

4. ［ * グループの削除 * ］ を選択して、確認メッセージに示されたグループを削除することを確認します。

   ページの右上に確認メッセージが表示されます。キャッシングに時間がかかるため変更には最大で 15 分を要します。

関連情報

"テナント管理権限"

ローカルユーザの管理

ローカルユーザを作成してローカルグループに割り当て、ユーザがアクセスできる機能を決定することができます。Tenant Manager には、「 root 」という名前の事前定義されたローカルユーザが 1 つ含まれています。 ローカルユーザは追加および削除できますが、 root ユーザを削除することはできません。

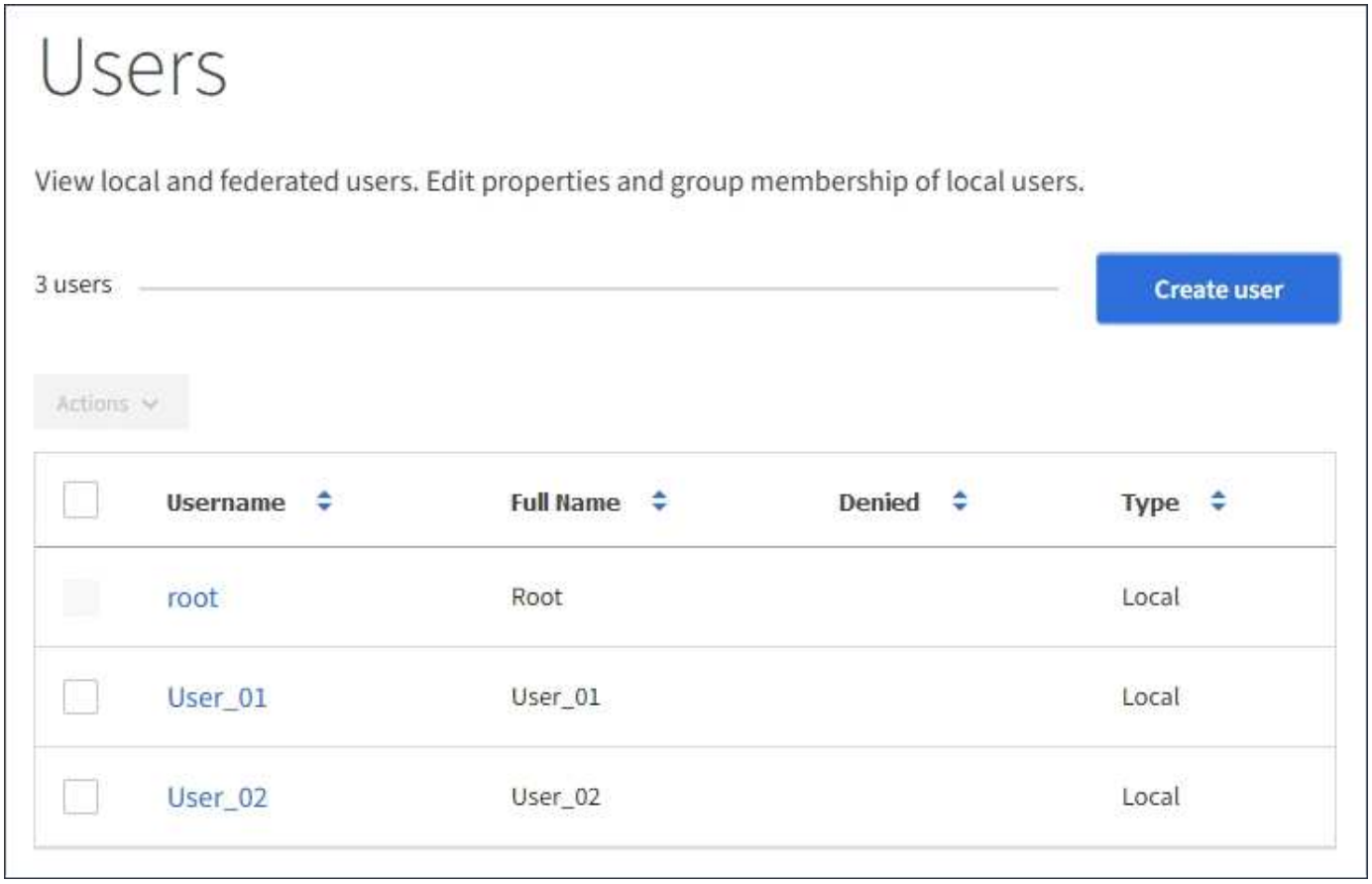
必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限が設定された読み取り / 書き込みユーザグループに属している必要があります。

StorageGRID システムでシングルサインオン（ SSO ）が有効になっている場合、ローカルユーザはテナントマネージャまたはテナント管理 API にサインインできません。ただし、グループの権限に基づいて、 S3 または Swift クライアントアプリケーションを使用してテナントのリソースにアクセスすることはできます。

**Users**ページへのアクセス

アクセス管理 * > * Users * を選択します。




ローカルユーザを作成しています

ローカルユーザを作成して 1 つ以上のローカルグループに割り当て、ユーザのアクセス権限を制御することができます。

いずれのグループにも属していない S3 ユーザには、管理権限または S3 グループポリシーが適用されません。これらのユーザは、バケットポリシーを通じて S3 バケットアクセスを許可されている場合があります。

グループに属していない Swift ユーザには、管理権限または Swift コンテナへのアクセスは付与されません。

手順

1. 「 * ユーザーの作成 * 」を選択します。
2. 次のフィールドに値を入力します。
   - * フルネーム * ：このユーザのフルネーム。たとえば、ユーザの名と姓、またはアプリケーションの名前です。
   - * ユーザ名 * ：このユーザがサインインに使用する名前。ユーザ名は一意である必要があり、変更できません。
   - * Password * ：ユーザがサインイン時に使用するパスワード。
   - * パスワードの確認 * ： [ パスワード ] フィールドに入力したパスワードと同じパスワードを入力します。

◦ * アクセスを拒否 * ：「 * はい」を選択した場合、このユーザはテナントアカウントにサインインできません。これは、ユーザがまだ 1 つ以上のグループに属している可能性がある場合も同様です。

たとえば、この機能を使用すると、ユーザが一時的にサインインできないようにすることができます。

3. 「 * Continue * 」を選択します。
4. 1 つ以上のローカルグループにユーザを割り当てます。

グループに属していないユーザには管理権限は付与されません。アクセス許可は累積的に追加されユーザには、自身が属しているすべてのグループに対するすべての権限が与えられます。

5. 「 * ユーザーの作成 * 」を選択します。

キャッシングに時間がかかるため変更には最大で 15 分を要します。

### ユーザの詳細を編集する

ユーザの詳細を編集する際に、ユーザのフルネームとパスワードを変更したり、ユーザを別のグループに追加したり、ユーザがテナントにアクセスできないようにしたりできます。

手順

1. [ ユーザー ] リストで、詳細を表示または編集するユーザーの名前を選択します。

または、ユーザーのチェックボックスをオンにして、 * アクション * > * ユーザーの詳細を表示 * を選択することもできます。

2. 必要に応じてユーザ設定を変更します。
   a. フルネームまたは編集アイコンを選択して、必要に応じてユーザのフルネームを変更します をクリックします。

ユーザ名は変更できません。

   b. [ パスワード *] タブで、必要に応じてユーザーのパスワードを変更します。
   c. [ * アクセス * ] タブで、ユーザーがサインインすることを許可するか（ [ * いいえ * ] を選択）、ユーザーが必要に応じてサインインしないようにします（ [ * はい * ] を選択）。
   d. [* グループ *] タブで、ユーザーをグループに追加するか、必要に応じてグループから削除します。
   e. 必要に応じて、 [ 変更を保存（ Save Changes ） ] を選択します。

キャッシングに時間がかかるため変更には最大で 15 分を要します。

### ローカルユーザの複製

ローカルユーザを複製して新しいユーザを迅速に作成することができます。

手順

1. [ ユーザー ] リストで、複製するユーザーを選択します。
2. 「 * ユーザーを複製 * 」を選択します。

3. 新しいユーザの次のフィールドを変更します。
   - * フルネーム * ：このユーザのフルネーム。たとえば、ユーザの名と姓、またはアプリケーションの名前です。
   - * ユーザ名 * ：このユーザがサインインに使用する名前。ユーザ名は一意である必要があり、変更できません。
   - * Password * ：ユーザがサインイン時に使用するパスワード。
   - * パスワードの確認 * ：[ パスワード ] フィールドに入力したパスワードと同じパスワードを入力します。
   - * アクセスを拒否 * ：「 * はい」を選択した場合、このユーザはテナントアカウントにサインインできません。これは、ユーザがまだ 1 つ以上のグループに属している可能性がある場合も同様です。

     たとえば、この機能を使用すると、ユーザが一時的にサインインできないようにすることができます。
4. 「 * Continue * 」を選択します。
5. 1 つ以上のローカルグループを選択します。

   グループに属していないユーザには管理権限は付与されません。アクセス許可は累積的に追加されユーザには、自身が属しているすべてのグループに対するすべての権限が与えられます。
6. 「 * ユーザーの作成 * 」を選択します。

   キャッシングに時間がかかるため変更には最大で 15 分を要します。

ローカルユーザを削除しています

StorageGRID テナントアカウントにアクセスする必要がなくなったローカルユーザは、完全に削除できます。

Tenant Manager を使用して、フェデレーテッドユーザは削除できますが、フェデレーテッドユーザは削除できません。フェデレーテッドユーザを削除するには、フェデレーテッドアイデンティティソースを使用する必要があります。

手順

1. [ ユーザ ] リストで、削除するローカルユーザのチェックボックスをオンにします。
2. * アクション * > * ユーザーの削除 * を選択します。
3. 確認ダイアログボックスで、「 * ユーザーの削除 * 」を選択して、システムからユーザーを削除することを確認します。

   キャッシングに時間がかかるため変更には最大で 15 分を要します。

関連情報

"テナント管理権限"

## S3テナントアカウントの管理

Tenant Managerを使用して、S3アクセスキーを管理したり、S3バケットを作成および

管理したりできます。

- "S3 アクセスキーの管理"
- "S3バケットの管理"

**S3** アクセスキーの管理

## S3 テナントアカウントの各ユーザには、 StorageGRID システムでオブジェクトの格納と読み出しを行うためのアクセスキーが必要です。アクセスキーは、アクセスキー ID とシークレットアクセスキーで構成されます。

このタスクについて

S3 アクセスキーは次のように管理できます。

- Manage Your Own S3 Credentials * 権限が設定されたユーザは、自分の S3 アクセスキーを作成または削除できます。
- Root Access * 権限が設定されたユーザは、 S3 root アカウントおよびその他すべてのユーザのアクセスキーを管理できます。root アクセスキーは、バケットポリシーで root アクセスキーが明示的に無効になっていないかぎり、テナントのすべてのバケットとオブジェクトへのフルアクセスを提供します。

StorageGRID では、署名バージョン 2 と署名バージョン 4 の認証がサポートされています。クロスアカウントアクセスは、バケットポリシーで明示的に有効になっていないかぎり、許可されません。

自分の**S3**アクセスキーを作成する

## S3 テナントを使用している場合は、適切な権限があれば、自分の S3 アクセスキーを作成できます。S3 テナントアカウントのバケットとオブジェクトにアクセスするには、アクセスキーが必要です。

必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Manage Your Own S3 Credentials 権限が必要です。

このタスクについて

テナントアカウントのバケットを作成および管理できる S3 アクセスキーを 1 つ以上作成できます。新しいアクセスキーを作成したら、新しいアクセスキー ID とシークレットアクセスキーでアプリケーションを更新します。セキュリティ上の理由から、必要以上の数のキーを作成しないでください。また、使用していないキーは削除してください。キーが 1 つしかなく、有効期限が近づいている場合は、古いキーが期限切れになる前に新しいキーを作成してから、古いキーを削除します。

各キーには、特定の有効期限または有効期限を設定できません。有効期限については、次のガイドラインに従ってください。

- キーの有効期限を設定して、アクセスを特定の期間に制限します。短い有効期限を設定すると、アクセスキー ID とシークレットアクセスキーが誤って公開されるリスクを低減できます。期限切れのキーは自動的に削除されます。
- 環境のセキュリティ・リスクが低く、新しいキーを定期的に作成する必要がない場合は、キーの有効期限を設定する必要はありません。あとで新しいキーを作成する場合は、古いキーを手動で削除します。

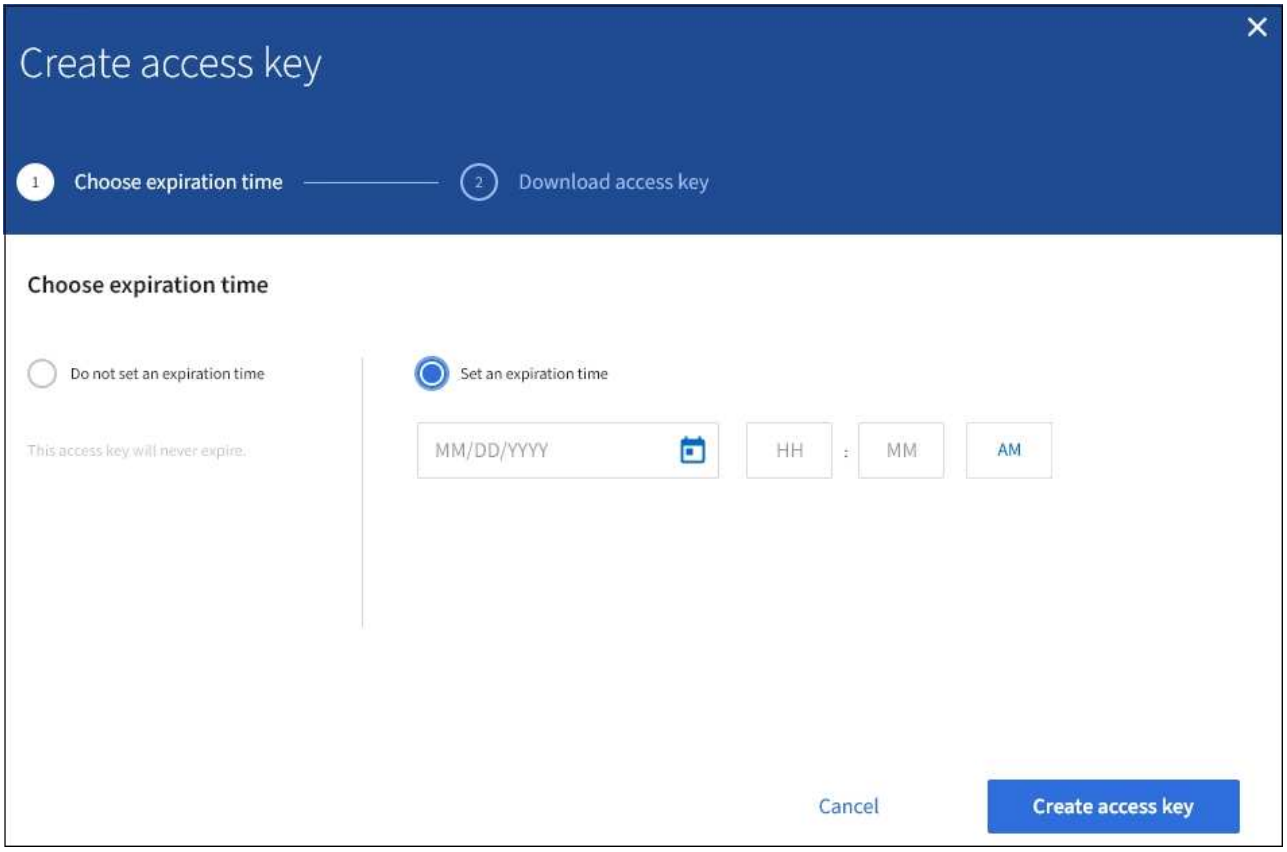
アカウントに属する S3 バケットとオブジェクトには、 Tenant Manager でアカウントに表示されるアクセスキー ID とシークレットアクセスキーを使用してアクセスできます。このため、アクセスキーはパスワードと同じように保護する必要があります。定期的にアクセスキーをローテーションし、使用されていないキーはアカウントから削除します。また、他のユーザとはアクセスキーを共有しないでください。

手順

1. 「 * storage （ S3 ） * > * My access keys * 」を選択します。

   [ マイアクセスキー ] ページが表示され、既存のアクセスキーが一覧表示されます。

2. 「 * キーの作成 * 」を選択します。
3. 次のいずれかを実行します。
   - 有効期限を設定しない * を選択して、有効期限が切れないキーを作成します。（デフォルト）
   - [ 有効期限の設定 *] を選択し、有効期限の日付と時刻を設定します。

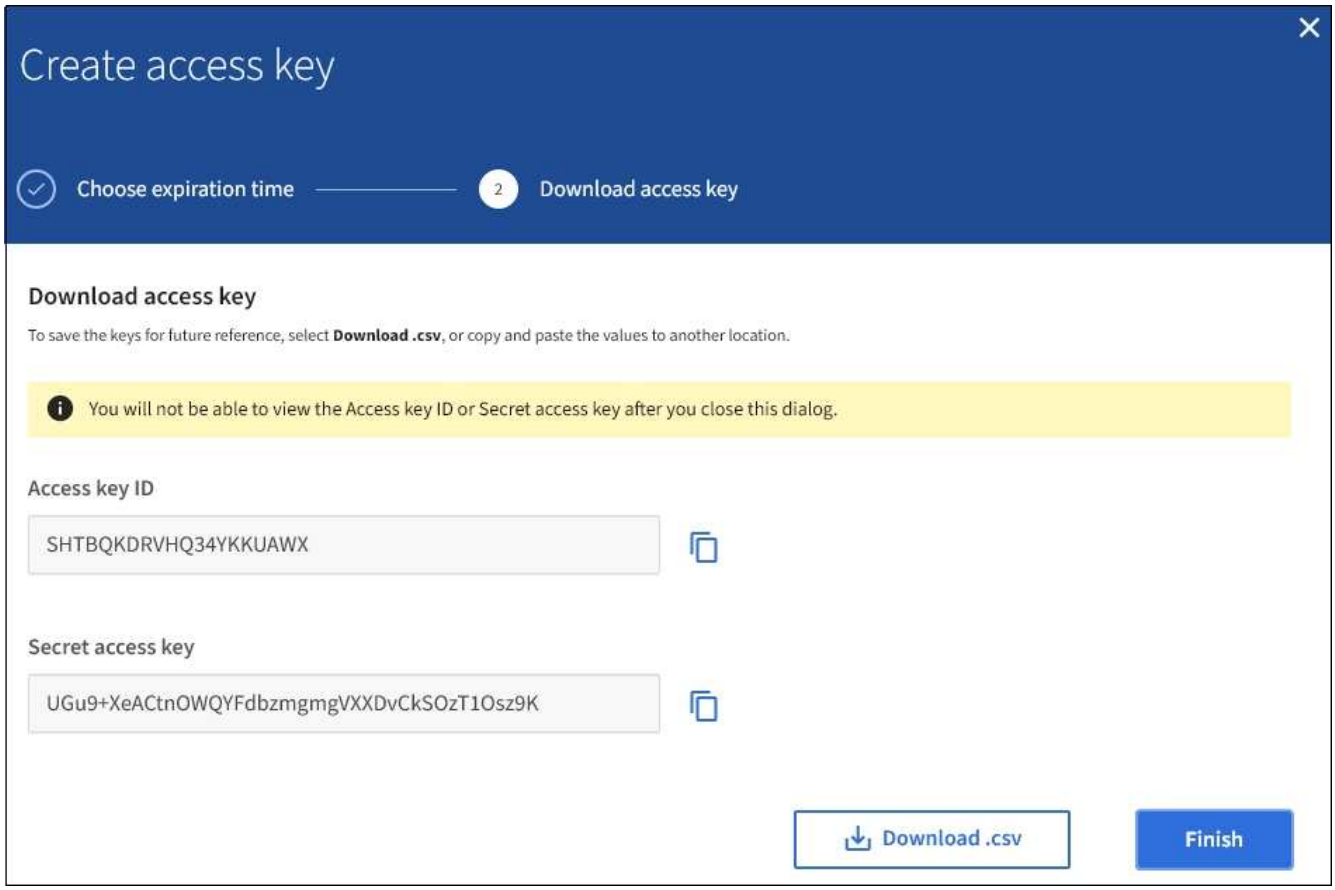



4. [ アクセスキーの作成 *] を選択します。

   Download access key （アクセスキーのダウンロード）ダイアログボックスが表示され、アクセスキー ID とシークレットアクセスキーが一覧表示されます。

5. アクセスキー ID とシークレットアクセスキーを安全な場所にコピーするか、「 * Download.csv * 」を選択してアクセスキー ID とシークレットアクセスキーを含むスプレッドシートファイルを保存します。

この情報をコピーまたはダウンロードするまで、このダイアログボックスを閉じないでください。




6. [ 完了 ] を選択します。

   新しいキーは [ マイアクセスキー ] ページに表示されます。キャッシングに時間がかかるため変更には最大で 15 分を要します。

関連情報

"テナント管理権限"

**S3**アクセスキーを表示します

S3 テナントを使用している場合は、適切な権限があれば、 S3 アクセスキーのリストを表示できます。有効期限でリストをソートすると、まもなく期限切れになるキーを確認できます。必要に応じて、新しいキーを作成したり、使用しなくなったキーを削除したりできます。

必要なもの

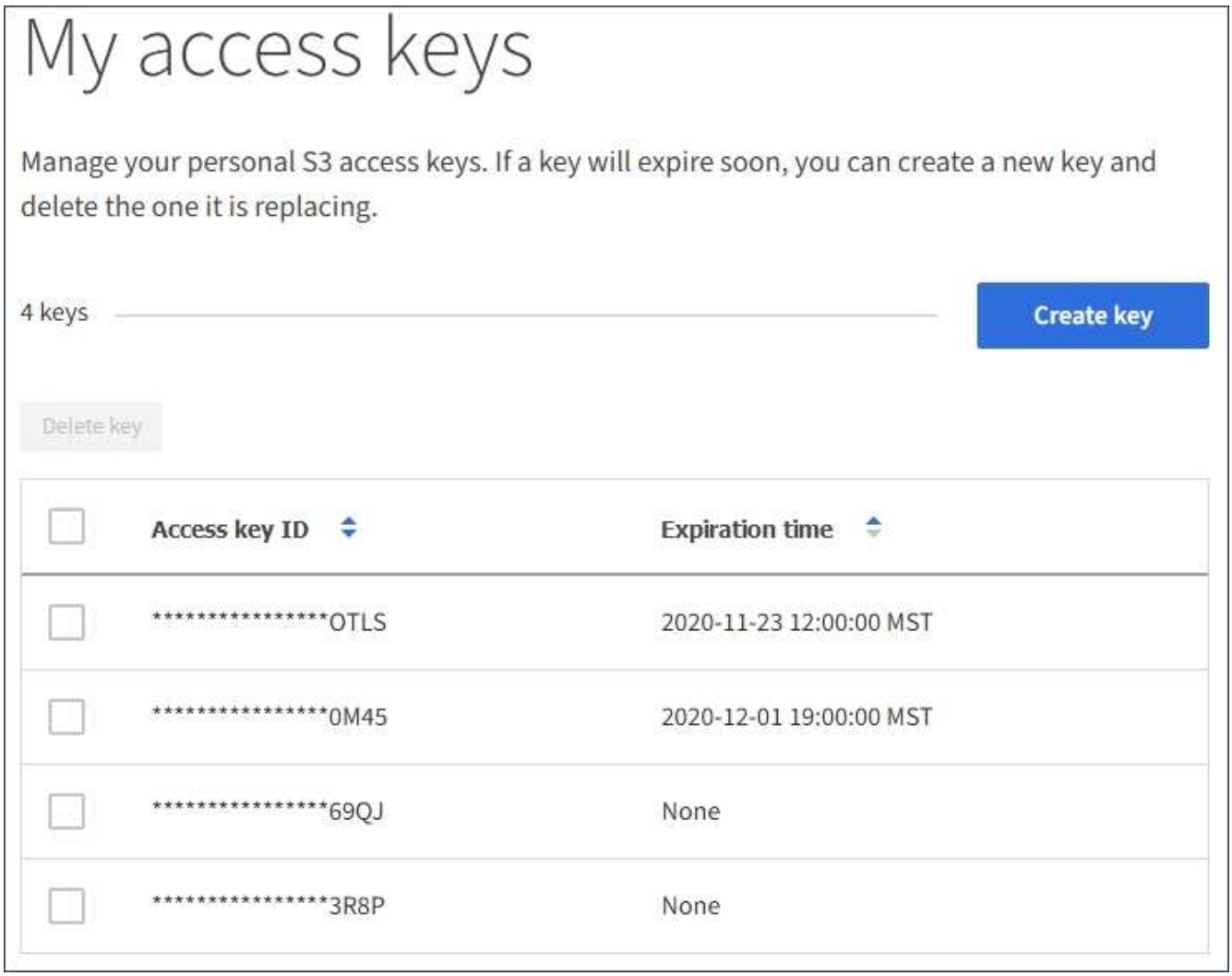
- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Manage Your Own S3 Credentials 権限が必要です。

アカウントに属する S3 バケットとオブジェクトには、 Tenant Manager でアカウントに表示されるアクセスキー ID とシークレットアクセスキーを使用してアクセスできます。このため、アクセスキーはパスワードと同じように保護する必要があります。定期的にアクセスキーをローテーションし、使用されていないキーはアカウントから削除します。また、他のユーザとはアクセスキーを共有しないでください。

手順

1. 「 * storage （ S3 ） * > * My access keys * 」を選択します。

   [ マイアクセスキー ] ページが表示され、既存のアクセスキーが一覧表示されます。




2. キーを * Expiration time * または * Access key ID * でソートします。
3. 必要に応じて、新しいキーを作成し、使用しなくなったキーを手動で削除します。

   既存のキーの有効期限が切れる前に新しいキーを作成した場合は、アカウントのオブジェクトに一時的にアクセスできなくなることなく、新しいキーの使用を開始できます。

   期限切れのキーは自動的に削除されます。

関連情報

"自分のS3アクセスキーを作成する"

"自分のS3アクセスキーを削除する"

自分の**S3**アクセスキーを削除する

S3 テナントを使用している場合は、適切な権限があれば、自分の S3 アクセスキーを削除できます。アクセスキーを削除すると、テナントアカウント内のオブジェクトとバケットにそのアクセスキーでアクセスできなくなります。

必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Manage Your Own S3 Credentials 権限が必要です。

> アカウントに属する S3 バケットとオブジェクトには、 Tenant Manager でアカウントに表示されるアクセスキー ID とシークレットアクセスキーを使用してアクセスできます。このため、アクセスキーはパスワードと同じように保護する必要があります。定期的にアクセスキーをローテーションし、使用されていないキーはアカウントから削除します。また、他のユーザとはアクセスキーを共有しないでください。

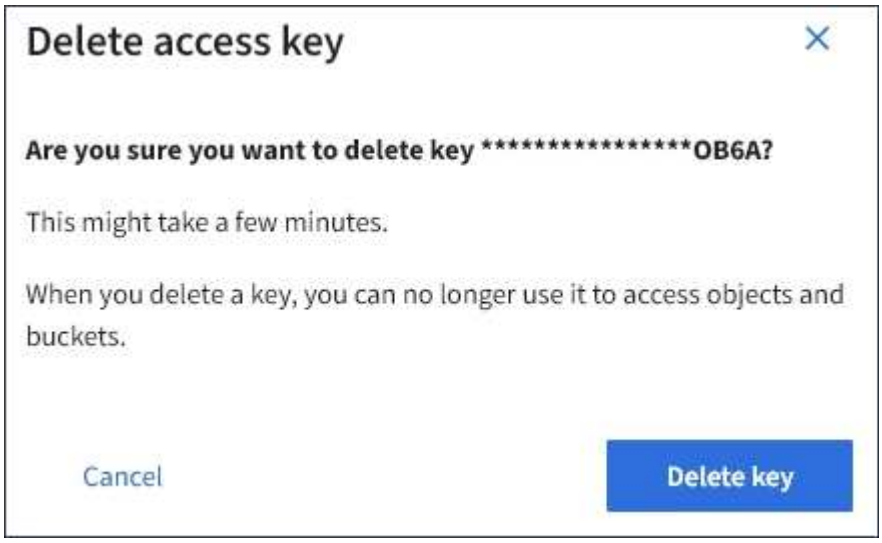
手順

1. 「 * storage （ S3 ） * > * My access keys * 」を選択します。

   [ マイアクセスキー ] ページが表示され、既存のアクセスキーが一覧表示されます。

2. 削除する各アクセスキーのチェックボックスを選択します。
3. 「 * Delete key （キーの削除）」 * を選択

   確認のダイアログボックスが表示されます。




4. 「 * Delete key （キーの削除）」 * を選択

   ページの右上に確認メッセージが表示されます。キャッシングに時間がかかるため変更には最大で 15 分を要します。

関連情報

"テナント管理権限"

別のユーザの**S3**アクセスキーを作成する

# S3 テナントを使用している場合は、適切な権限があれば、バケットやオブジェクトにアクセスする必要があるアプリケーションなど、他のユーザの S3 アクセスキーを作成できます。

必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限が必要です。

このタスクについて

他のユーザがテナントアカウントのバケットを作成および管理できるように、 1 つ以上の S3 アクセスキーを作成できます。新しいアクセスキーを作成したら、新しいアクセスキー ID とシークレットアクセスキーでアプリケーションを更新します。セキュリティ上の理由から、ユーザが必要とする以上のキーは作成しないでください。また、使用されていないキーは削除してください。キーが 1 つしかなく、有効期限が近づいている場合は、古いキーが期限切れになる前に新しいキーを作成してから、古いキーを削除します。

各キーには、特定の有効期限または有効期限を設定できません。有効期限については、次のガイドラインに従ってください。

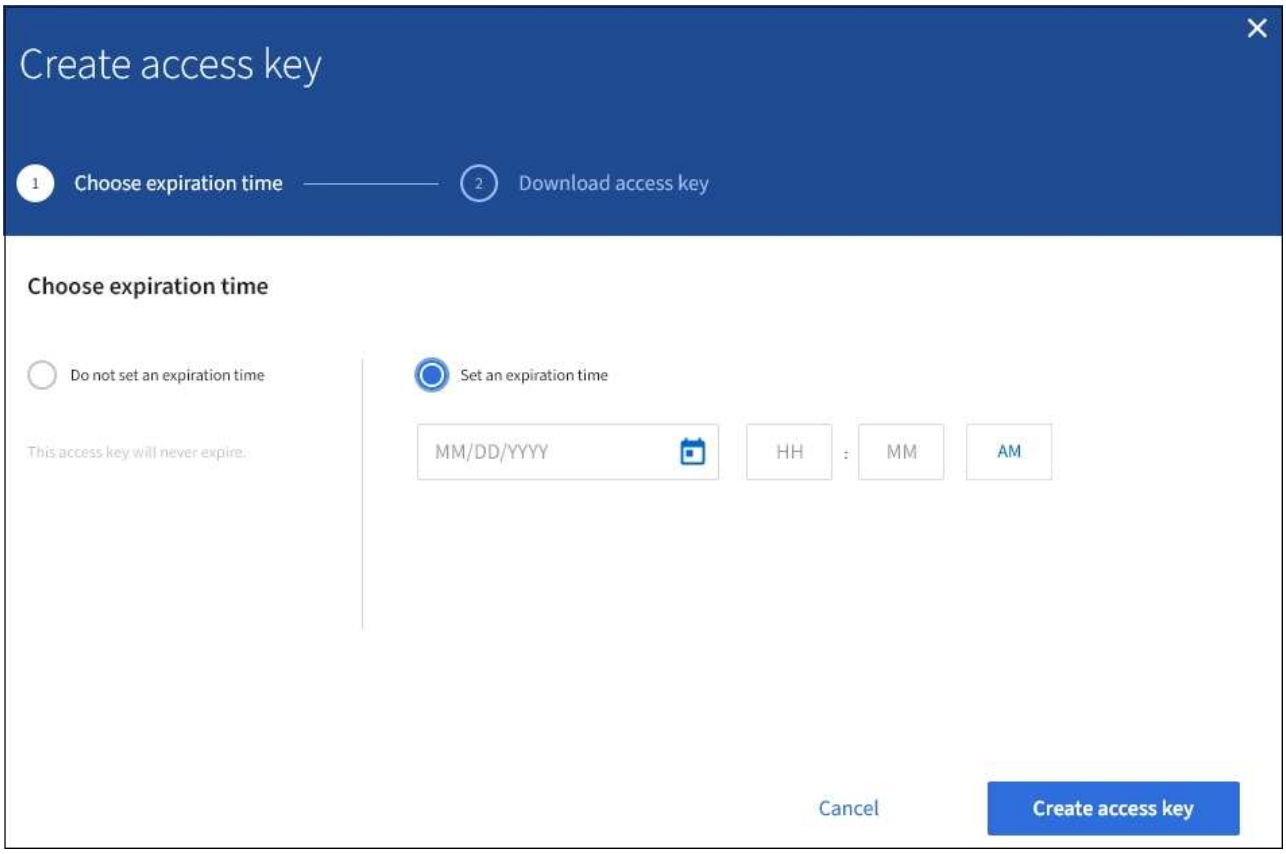
- キーの有効期限を設定して、ユーザのアクセスを一定期間に制限します。短い有効期限を設定すると、アクセスキー ID とシークレットアクセスキーが誤って公開されるリスクを低減できます。期限切れのキーは自動的に削除されます。
- 環境のセキュリティ・リスクが低く、新しいキーを定期的に作成する必要がない場合は、キーの有効期限を設定する必要はありません。あとで新しいキーを作成する場合は、古いキーを手動で削除します。

> ユーザに属する S3 バケットとオブジェクトには、 Tenant Manager でそのユーザに対して表示されるアクセスキー ID とシークレットアクセスキーを使用してアクセスできます。このため、アクセスキーはパスワードと同じように保護する必要があります。定期的にアクセスキーをローテーションし、使用されていないキーはアカウントから削除します。また、他のユーザとはアクセスキーを共有しないでください。

手順

1. アクセス管理 * > * Users * を選択します。
2. S3 アクセスキーを管理するユーザを選択します。

   ユーザーの詳細ページが表示されます。
3. [ * アクセスキー * ] を選択し、 [ * キーの作成 * ] を選択します。
4. 次のいずれかを実行します。
   - 有効期限を設定しない * を選択して、有効期限が切れないキーを作成します。（デフォルト）
   - [ 有効期限の設定 *] を選択し、有効期限の日付と時刻を設定します。

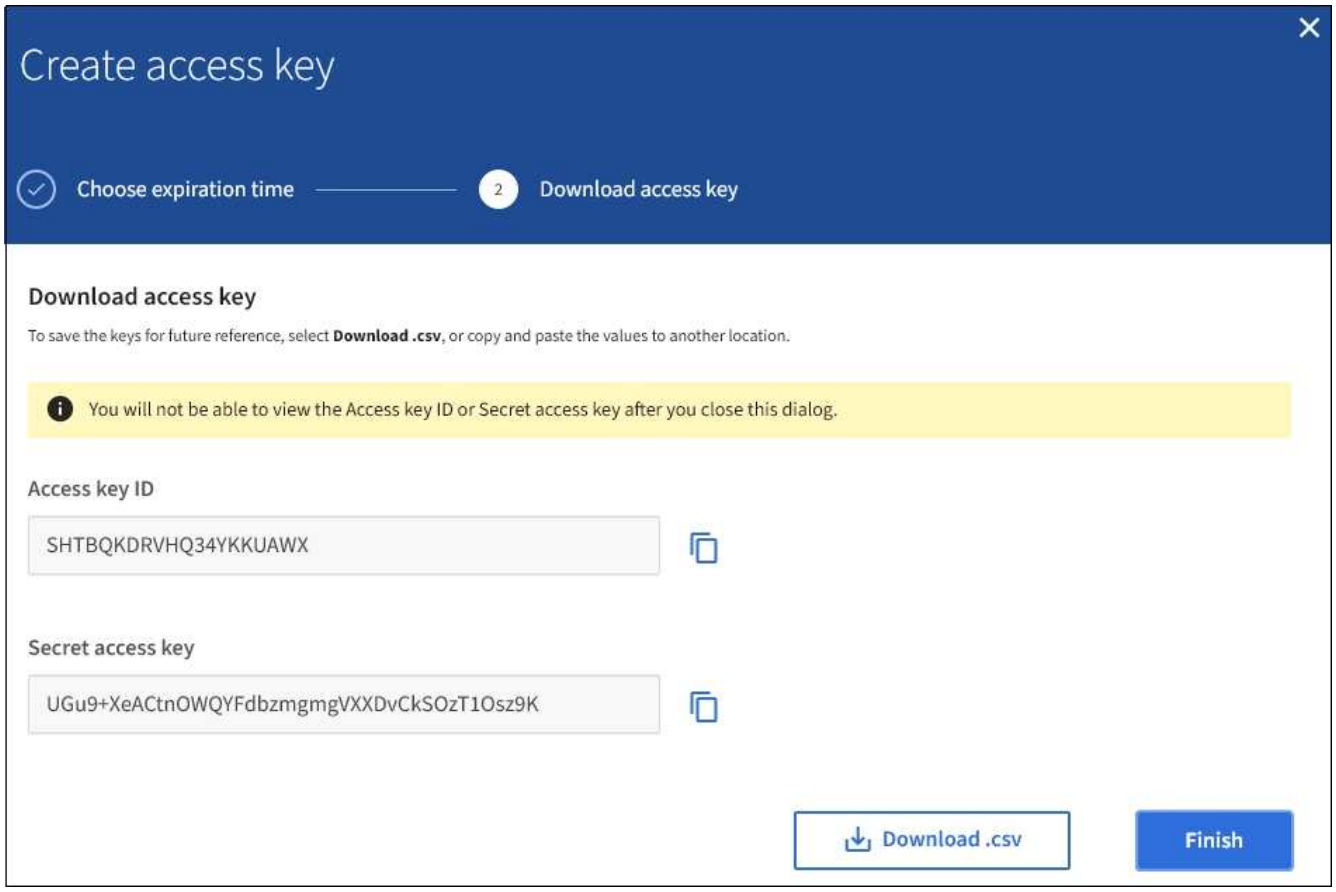



5. [ アクセスキーの作成 *] を選択します。

   Download access key （アクセスキーのダウンロード）ダイアログボックスが表示され、アクセスキー ID とシークレットアクセスキーが一覧表示されます。

6. アクセスキー ID とシークレットアクセスキーを安全な場所にコピーするか、「 * Download.csv * 」を選択してアクセスキー ID とシークレットアクセスキーを含むスプレッドシートファイルを保存します。

   この情報をコピーまたはダウンロードするまで、このダイアログボックスを閉じないでください。




7. [ 完了 ] を選択します。

   新しいキーは、ユーザ詳細ページのアクセスキータブに表示されます。キャッシングに時間がかかるため変更には最大で 15 分を要します。

関連情報

"テナント管理権限"

別のユーザの**S3**アクセスキーを表示しています

S3 テナントを使用している場合は、適切な権限があれば、別のユーザの S3 アクセスキーを表示できます。有効期限でリストをソートすると、まもなく期限切れになるキーを確認できます。必要に応じて、新しいキーを作成したり、使用されなくなったキーを削除したりできます。

必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限が必要です。

ユーザに属する S3 バケットとオブジェクトには、 Tenant Manager でそのユーザに対して表示されるアクセスキー ID とシークレットアクセスキーを使用してアクセスできます。このため、アクセスキーはパスワードと同じように保護する必要があります。定期的にアクセスキーをローテーションし、使用されていないキーはアカウントから削除します。また、他のユーザとはアクセスキーを共有しないでください。

手順

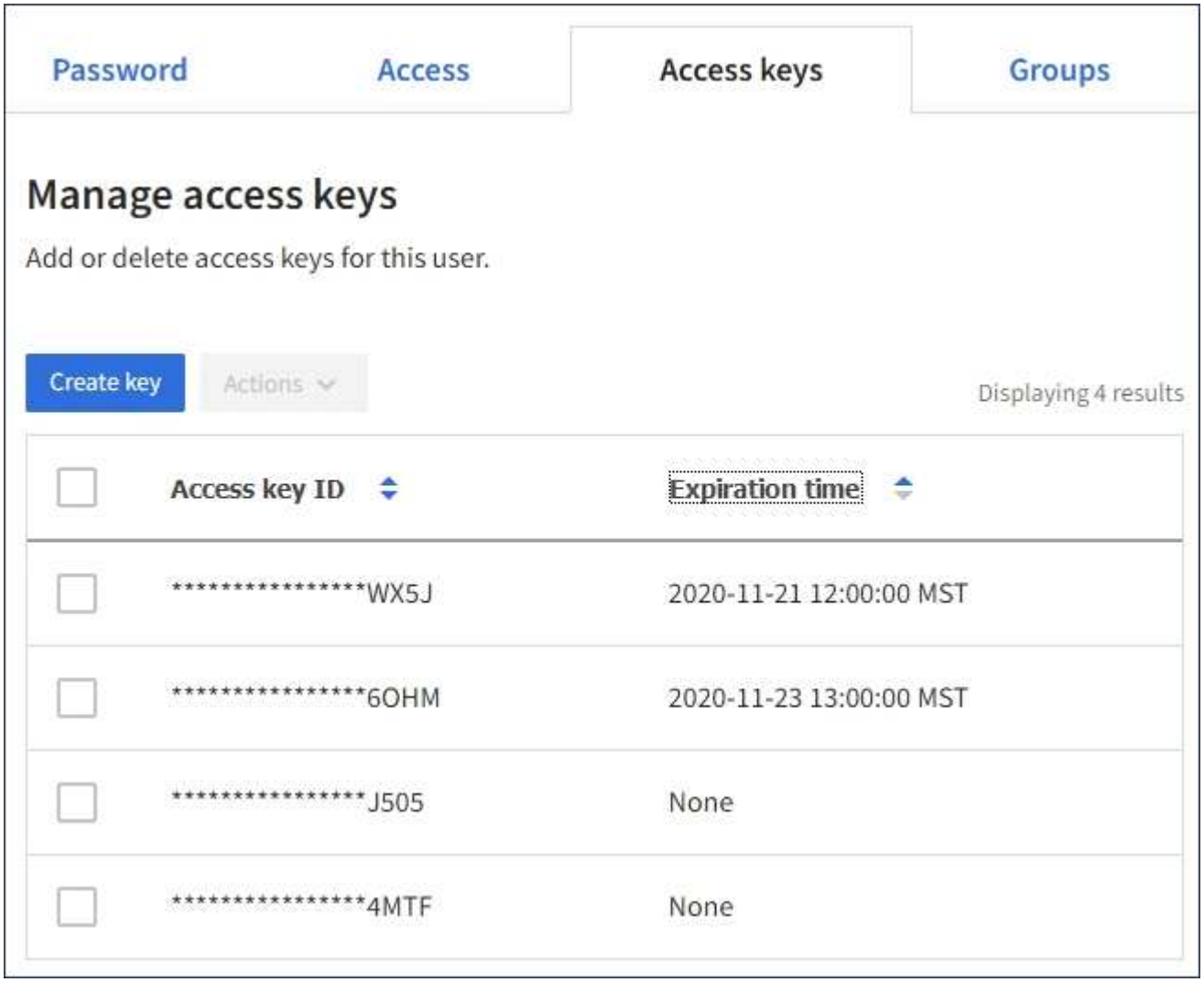
1. アクセス管理 * > * Users * を選択します。

   [ ユーザー ] ページが表示され、既存のユーザーが一覧表示されます。

2. S3 アクセスキーを表示するユーザを選択します。

   ユーザーの詳細ページが表示されます。

3. 「 * アクセスキー * 」を選択します。




4. キーを * Expiration time * または * Access key ID * でソートします。
5. 必要に応じて、新しいキーを作成し、使用しなくなったキーを手動で削除します。

   既存のキーの有効期限が切れる前に新しいキーを作成した場合、ユーザはアカウントのオブジェクトに一時的にアクセスできなくなることなく、新しいキーの使用を開始できます。

   期限切れのキーは自動的に削除されます。

関連情報

"別のユーザのS3アクセスキーを作成しています"

"別のユーザのS3アクセスキーを削除しています"

別のユーザの**S3**アクセスキーを削除しています

S3 テナントを使用している場合は、適切な権限があれば、別のユーザの S3 アクセスキーを削除できます。アクセスキーを削除すると、テナントアカウント内のオブジェクトとバケットにそのアクセスキーでアクセスできなくなります。

必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限が必要です。

> ユーザに属する S3 バケットとオブジェクトには、 Tenant Manager でそのユーザに対して表示されるアクセスキー ID とシークレットアクセスキーを使用してアクセスできます。このため、アクセスキーはパスワードと同じように保護する必要があります。定期的にアクセスキーをローテーションし、使用されていないキーはアカウントから削除します。また、他のユーザとはアクセスキーを共有しないでください。

手順

1. アクセス管理 * > * Users * を選択します。

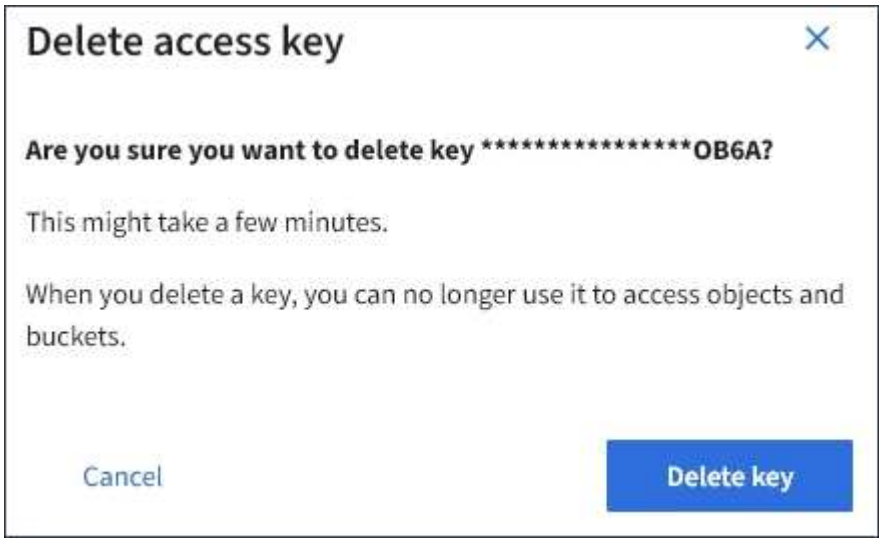
   [ ユーザー ] ページが表示され、既存のユーザーが一覧表示されます。

2. S3 アクセスキーを管理するユーザを選択します。

   ユーザーの詳細ページが表示されます。

3. アクセスキー * を選択し、削除する各アクセスキーのチェックボックスを選択します。
4. * アクション * > * 選択したキーを削除 * を選択します。

   確認のダイアログボックスが表示されます。



5. 「 * Delete key （キーの削除）」 * を選択

   ページの右上に確認メッセージが表示されます。キャッシングに時間がかかるため変更には最大で 15 分を要します。

関連情報

"テナント管理権限"

## S3バケットの管理

S3テナントを適切な権限で使用している場合は、S3バケットの作成、表示、削除、整合性レベルの設定の更新、Cross-Origin Resource Sharing（CORS）の設定、最終アクセス日時の更新の有効化と無効化、S3プラットフォームサービスの管理を実行できます。

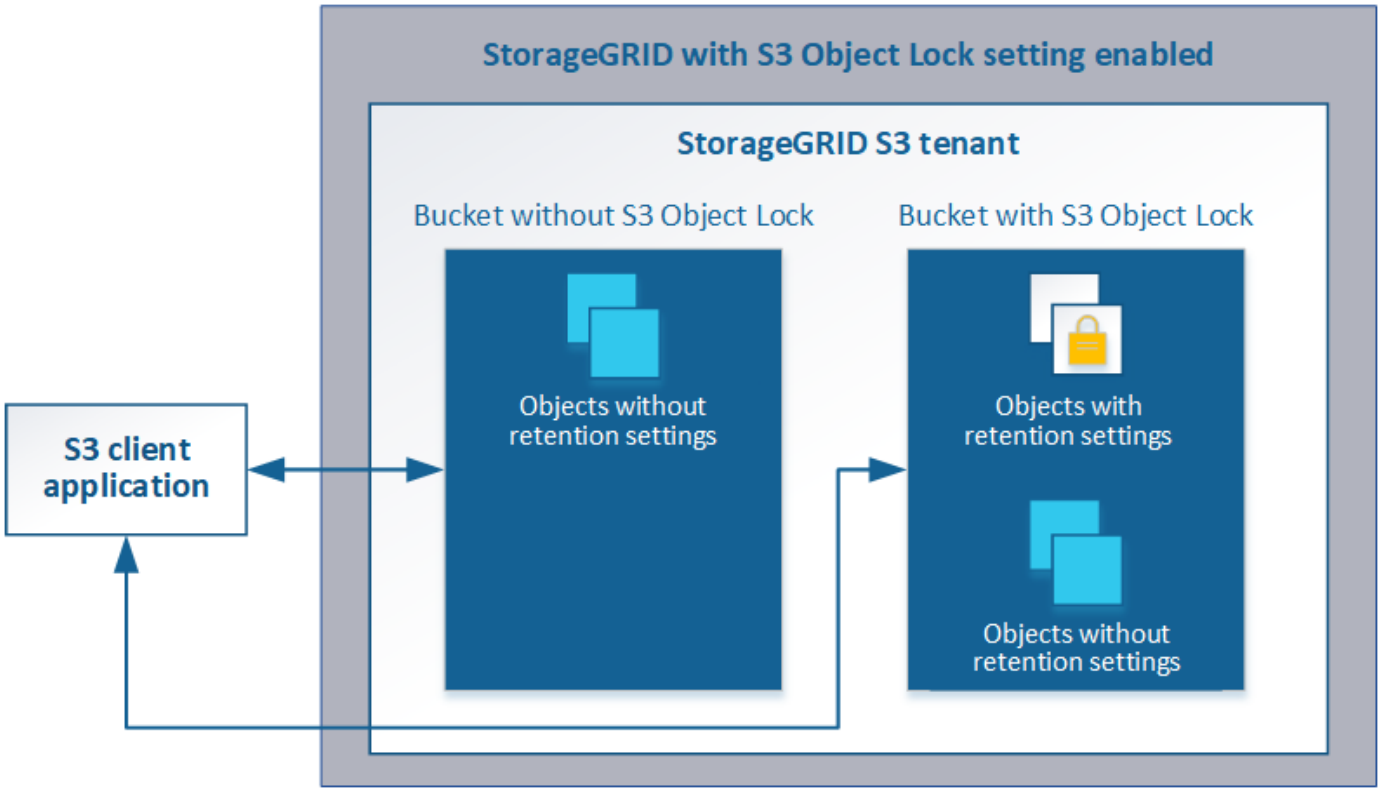
### S3 オブジェクトロックを使用する

オブジェクトが保持に関する規制要件に準拠する必要がある場合は、 StorageGRID で S3 オブジェクトロック機能を使用できます。

#### S3 オブジェクトのロックとは何ですか？

StorageGRID S3 オブジェクトロック機能は、 Amazon Simple Storage Service （ Amazon S3 ）での S3 オブジェクトロックに相当するオブジェクト保護解決策 です。

図に示すように、 StorageGRID システムでグローバルな S3 オブジェクトのロック設定が有効になっている場合、 S3 テナントアカウントでは、 S3 オブジェクトのロックを有効にしているかどうかに関係なくバケットを作成できます。バケットで S3 オブジェクトのロックが有効になっている場合、 S3 クライアントアプリケーションは、そのバケット内の任意のオブジェクトバージョンの保持設定を必要に応じて指定できます。オブジェクトのバージョンには、 S3 オブジェクトロックで保護するように指定された保持設定が必要です。




StorageGRID S3 オブジェクトロック機能は、 Amazon S3 準拠モードと同等の単一の保持モードを提供します。デフォルトでは、保護されたオブジェクトバージョンは、どのユーザーでも上書きまたは削除できません。StorageGRID S3 オブジェクトのロック機能では、ガバナンスモードはサポートされず、特別な権限を持つユーザは保持設定を省略したり保護されたオブジェクトを削除したりすることはできません。

バケットで S3 オブジェクトロックが有効になっている場合、 S3 クライアントアプリケーションは、オブジェクトの作成時または更新時に、次のオブジェクトレベルの保持設定のいずれか、または両方を必要に応じて指定できます。

- **Retain Until - date** ：オブジェクトバージョンの retain-until - date が将来の日付である場合、オブジェクトは読み出し可能ですが、変更または削除することはできません。必要に応じて、オブジェクトの retain-date を増やすことはできますが、この日付を減らすことはできません。
- * リーガルホールド * ：オブジェクトバージョンにリーガルホールドを適用すると、そのオブジェクトがただちにロックされます。たとえば、調査または法的紛争に関連するオブジェクトにリーガルホールドを設定する必要がある場合があります。リーガルホールドには有効期限はありませんが、明示的に削除されるまで保持されます。リーガルホールドは、それまでの保持期間とは関係ありません。

これらの設定の詳細については、の「Using S3 object lock」を参照してください "S3 REST API のサポートされる処理と制限事項"。

従来の準拠バケットの管理

S3 オブジェクトロック機能は、以前のバージョンの StorageGRID で使用されていた準拠機能に代わる機能です。以前のバージョンの StorageGRID を使用して準拠バケットを作成した場合は、引き続きこれらのバケットの設定を管理できますが、新しい準拠バケットは作成できなくなります。手順については、ネットアップの技術情報アーティクルを参照してください。

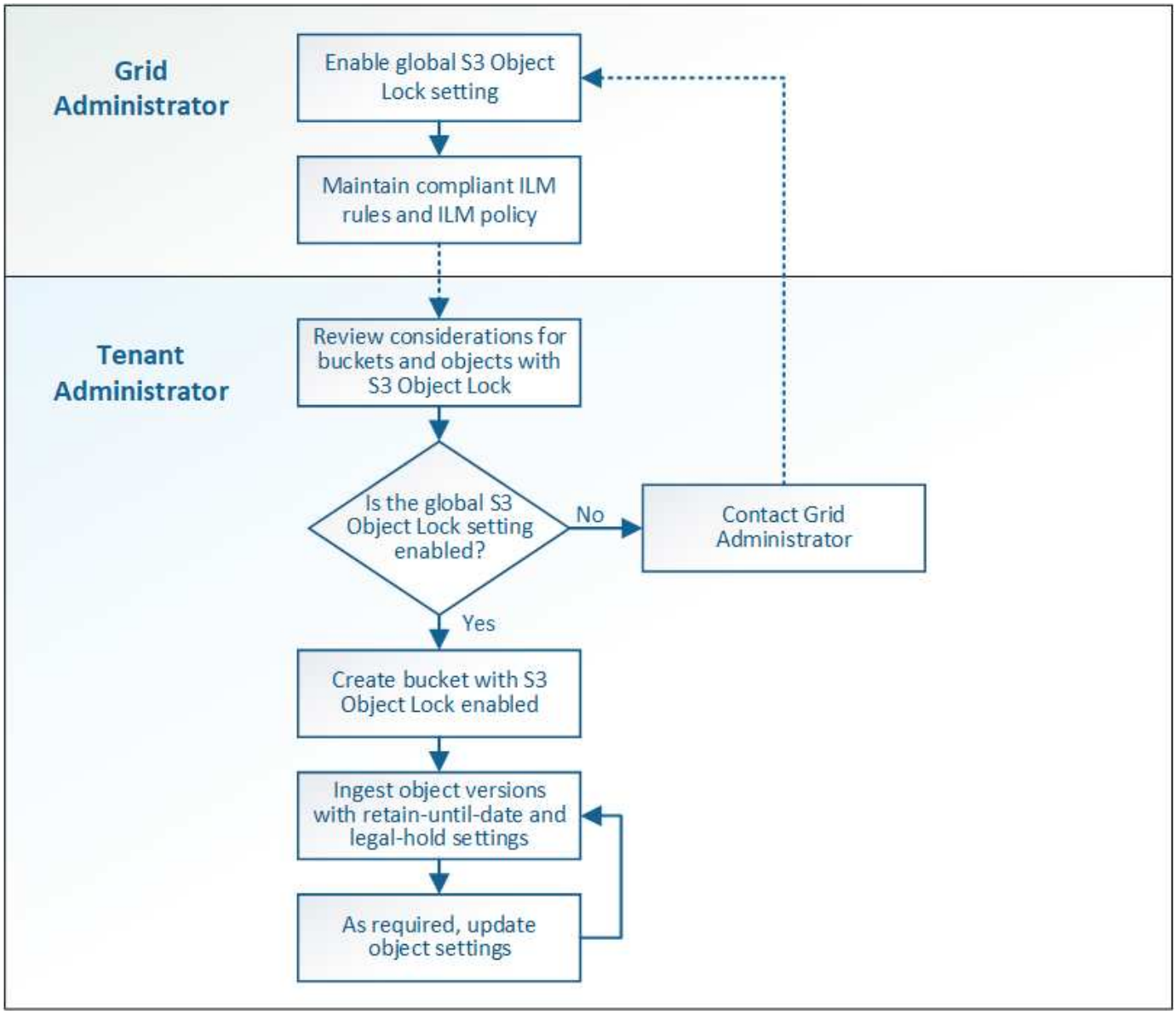
"ネットアップのナレッジベース： StorageGRID 11.5 でレガシー準拠バケットを管理する方法"

**S3** オブジェクトロックのワークフロー

次のワークフロー図は、 StorageGRID で S3 オブジェクトロック機能を使用する場合の大まかな手順を示しています。

S3 オブジェクトのロックを有効にしてバケットを作成する前に、グリッド管理者が StorageGRID システム全体に対してグローバルな S3 オブジェクトのロック設定を有効にする必要があります。また、グリッド管理者は、情報ライフサイクル管理（ILM）ポリシーが「準拠」であることを確認する必要があり、S3オブジェクトロックが有効になっているバケットの要件を満たしている必要があります。詳細については、グリッド管理者に問い合わせるか、情報ライフサイクル管理を使用してオブジェクトを管理する手順を参照してください。

グローバルな S3 オブジェクトのロック設定を有効にしたあと、 S3 オブジェクトのロックを有効にしてバケットを作成できます。その後、 S3 クライアントアプリケーションを使用して、オブジェクトのバージョンごとに保持設定を必要に応じて指定できます。




関連情報

"ILM を使用してオブジェクトを管理する"

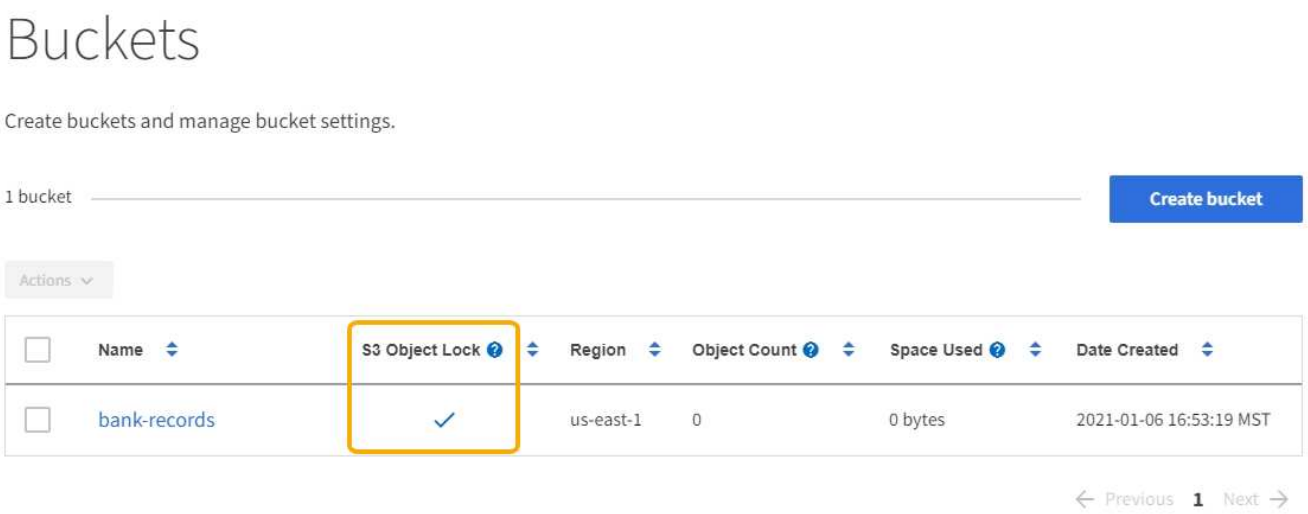
## S3 オブジェクトのロックの要件

バケットで S3 オブジェクトのロックを有効にする前に、 S3 オブジェクトのロックが有効になっているバケットおよびオブジェクトの要件と、バケット内のオブジェクトのライフサイクルを確認します。

### S3 オブジェクトのロックを有効にした場合のバケットの要件

- StorageGRID システムでグローバルな S3 オブジェクトロック設定が有効になっている場合は、テナントマネージャ、テナント管理 API 、または S3 REST API を使用して、 S3 オブジェクトロックを有効にしたバケットを作成できます。

  次の Tenant Manager の例では、 S3 オブジェクトのロックが有効になっているバケットを示しています。




- S3 オブジェクトのロックを使用する場合は、バケットの作成時に S3 オブジェクトのロックを有効にする必要があります。既存のバケットに対して S3 オブジェクトロックを有効にすることはできません。
- S3 オブジェクトロックでは、バケットのバージョン管理が必要です。バケットで S3 オブジェクトのロックが有効になっている場合は、そのバケットのバージョン管理が StorageGRID で自動的に有効になります。
- S3 オブジェクトのロックを有効にしてバケットを作成したあとに、そのバケットの S3 オブジェクトのロックを無効にしたりバージョン管理を一時停止したりすることはできません。
- S3オブジェクトのロックが有効になっているStorageGRID バケットでは、デフォルトの保持期間はありません。代わりに、S3クライアントアプリケーションは、そのバケットに追加されるオブジェクトバージョンごとに保持期限とリーガルホールド設定を指定できます。
- バケットライフサイクル設定は S3 オブジェクトライフサイクルバケットでサポートされます。
- CloudMirror レプリケーションは、 S3 オブジェクトロックが有効になっているバケットではサポートされません。

### S3 オブジェクトのロックが有効になっているバケット内のオブジェクトの要件

- S3クライアントアプリケーションは、S3オブジェクトのロックで保護する必要があるオブジェクトごとに保持設定を指定する必要があります。
- オブジェクトバージョンの retain-until date は増やすことができますが、この値を減らすことはできませ

ん。

- 係争中の訴訟や規制上の調査に関する通知があった場合、オブジェクトバージョンをリーガルホールドの対象にすることで関連情報を保持できます。オブジェクトバージョンがリーガルホールドの対象になっている場合は、それが retain-until 日に達しても、そのオブジェクトを StorageGRID から削除することはできません。リーガルホールドを解除すると、それまで保持期限に達した場合にオブジェクトバージョンを削除できるようになります。
- S3 オブジェクトロックにはバージョン管理されたバケットを使用する必要があります。保持設定はオブジェクトのバージョンごとに適用されます。オブジェクトバージョンには、 retain-until date 設定とリーガルホールド設定の両方を設定できます。ただし、オブジェクトバージョンを保持することはできません。また、どちらも保持することはできません。オブジェクトの retain-une-date 設定またはリーガルホールド設定を指定すると、要求で指定されたバージョンのみが保護されます。オブジェクトの以前のバージョンはロックされたまま、オブジェクトの新しいバージョンを作成できます。

**S3** オブジェクトのロックが有効なバケット内のオブジェクトのライフサイクル

S3 オブジェクトのロックが有効になっているバケットに保存された各オブジェクトは、次の 3 つの段階を経て処理されます。

1. * オブジェクトの取り込み *
    - S3 オブジェクトのロックが有効になっているバケットにオブジェクトのバージョンを追加するときに、 S3 クライアントアプリケーションはオプションでオブジェクトの保持設定を指定できます（ retain-until date 、 legal hold 、または both ）。StorageGRID は、そのオブジェクトのメタデータを生成します。これには、一意のオブジェクト ID （ UUID ）と取り込み日時が含まれます。
    - 保持設定のあるオブジェクトのバージョンが取り込まれたあとに、そのデータと S3 ユーザ定義メタデータを変更することはできません。
    - StorageGRID は、オブジェクトメタデータをオブジェクトデータとは別に格納します。各サイトですべてのオブジェクトメタデータのコピーを 3 つ保持します。
2. * オブジェクト保持 *
    - オブジェクトの複数のコピーが StorageGRID によって格納される。コピーの正確な数、タイプ、格納場所は、アクティブな ILM ポリシーの準拠ルールによって決まります。
3. * オブジェクトの削除 *
    - オブジェクトは、 retain-until - date に到達したときに削除できます。
    - リーガルホールドの対象になっているオブジェクトは削除できません。

**S3**バケットの作成

Tenant Manager を使用して、オブジェクトデータ用の S3 バケットを作成できます。バケットを作成するときは、バケットの名前とリージョンを指定する必要があります。StorageGRID システムでグローバルな S3 オブジェクトのロック設定が有効になっている場合は、必要に応じてバケットで S3 オブジェクトのロックを有効にすることができます。

必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Manage All Buckets 権限または Root Access 権限のあるユーザグループに属している必要があります。これらの権限は、グループまたはバケットポリシーの権限の設定よりも優先されます。

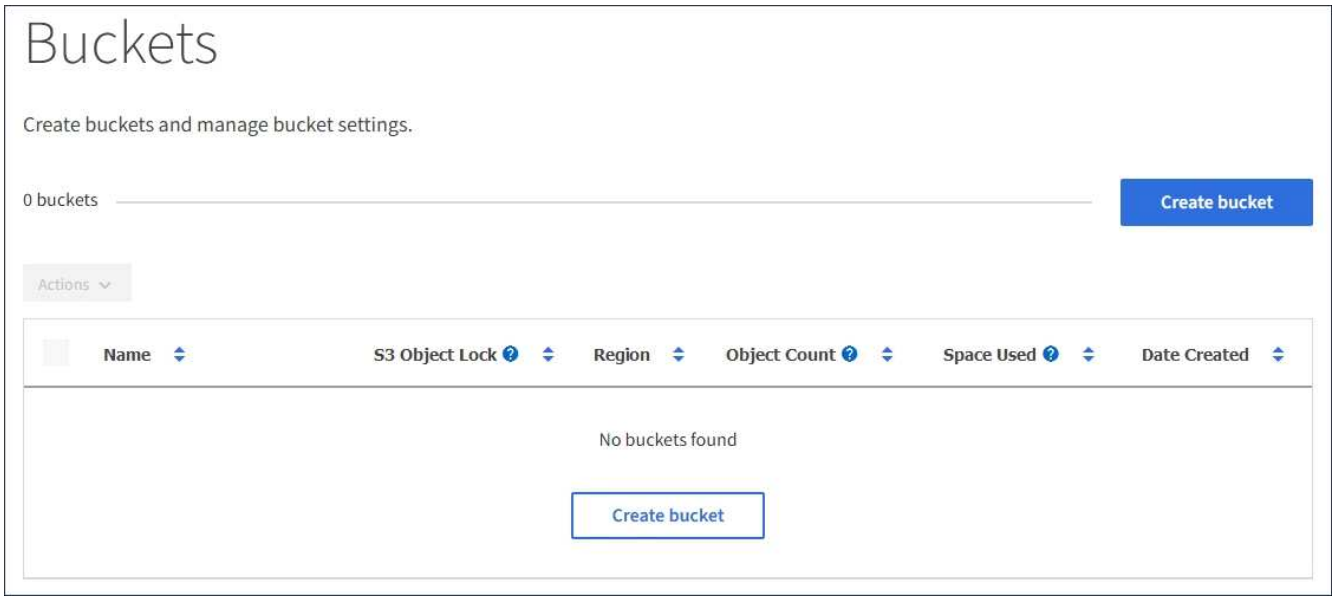
- S3オブジェクトロックを使用してバケットを作成する場合は、StorageGRID システムでグローバルなS3オブジェクトロック設定を有効にしておく必要があります。また、S3オブジェクトロックのバケットとオブジェクトに関する要件を確認しておく必要があります。

  "S3 オブジェクトロックを使用する"

手順

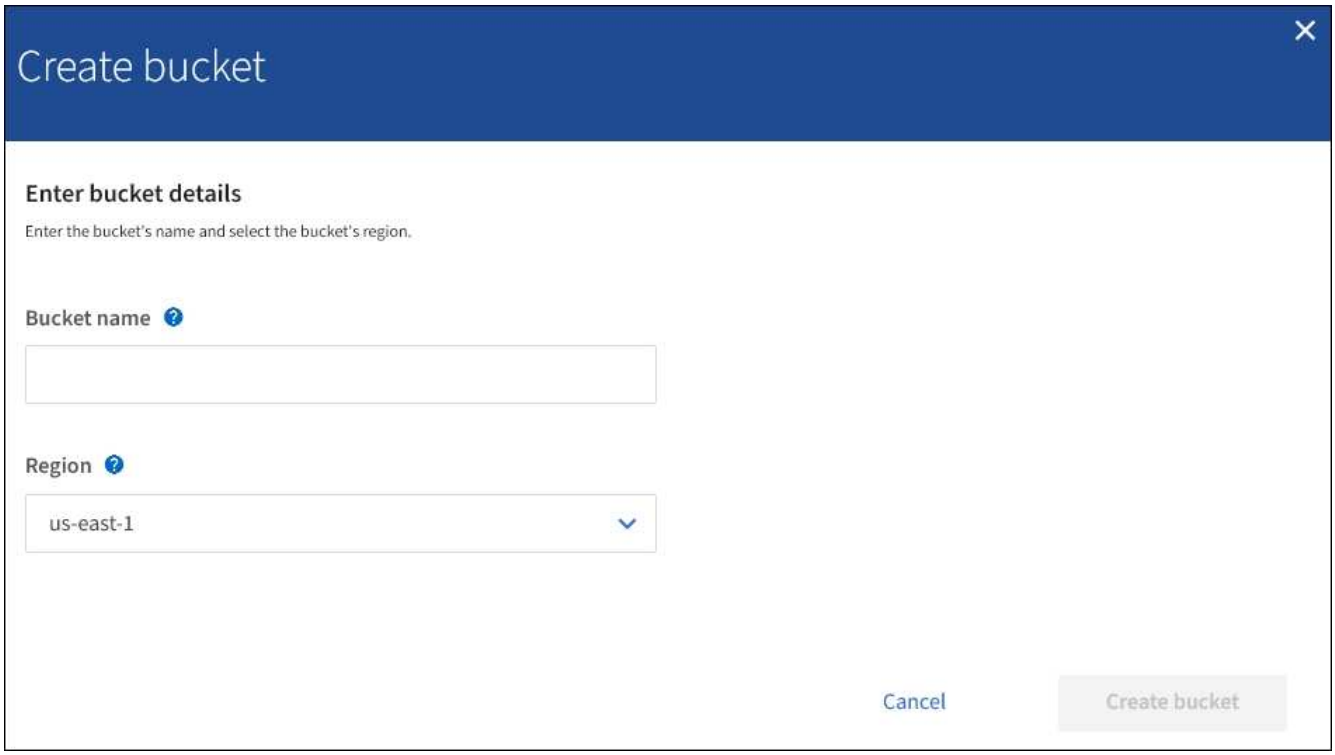
1. ストレージ（ S3 ） * > * バケット * を選択します。

   バケットページが表示され、すでに作成されているバケットが一覧表示されます。




2. [ * バケットの作成 * ] を選択します。

   Create Bucketウィザードが表示されます。




グローバルなS3オブジェクトのロック設定が有効になっている場合、バケットの作成には、バケットのS3オブジェクトのロックを管理するための2つ目の手順が含まれます。

3. バケットの一意の名前を入力します。

バケットの作成後にバケット名を変更することはできません。

バケット名は次のルールを満たす必要があります。

- StorageGRID システム全体で（テナントアカウント内だけではなく）一意である必要があります。
- DNS に準拠している必要があります。
- 3 文字以上 63 文字以下にする必要があります。
- 1 つ以上のラベルを連続して指定できます。隣接するラベルはピリオドで区切ります。各ラベルの先頭と末尾の文字は小文字のアルファベットか数字にする必要があり、使用できる文字は小文字のアルファベット、数字、ハイフンのみです。
- テキスト形式の IP アドレスのようにはできません。
- 仮想ホスト形式の要求でピリオドを使用しないでください。ピリオドを使用すると、サーバワイルドカード証明書の検証で原因 の問題が発生します。

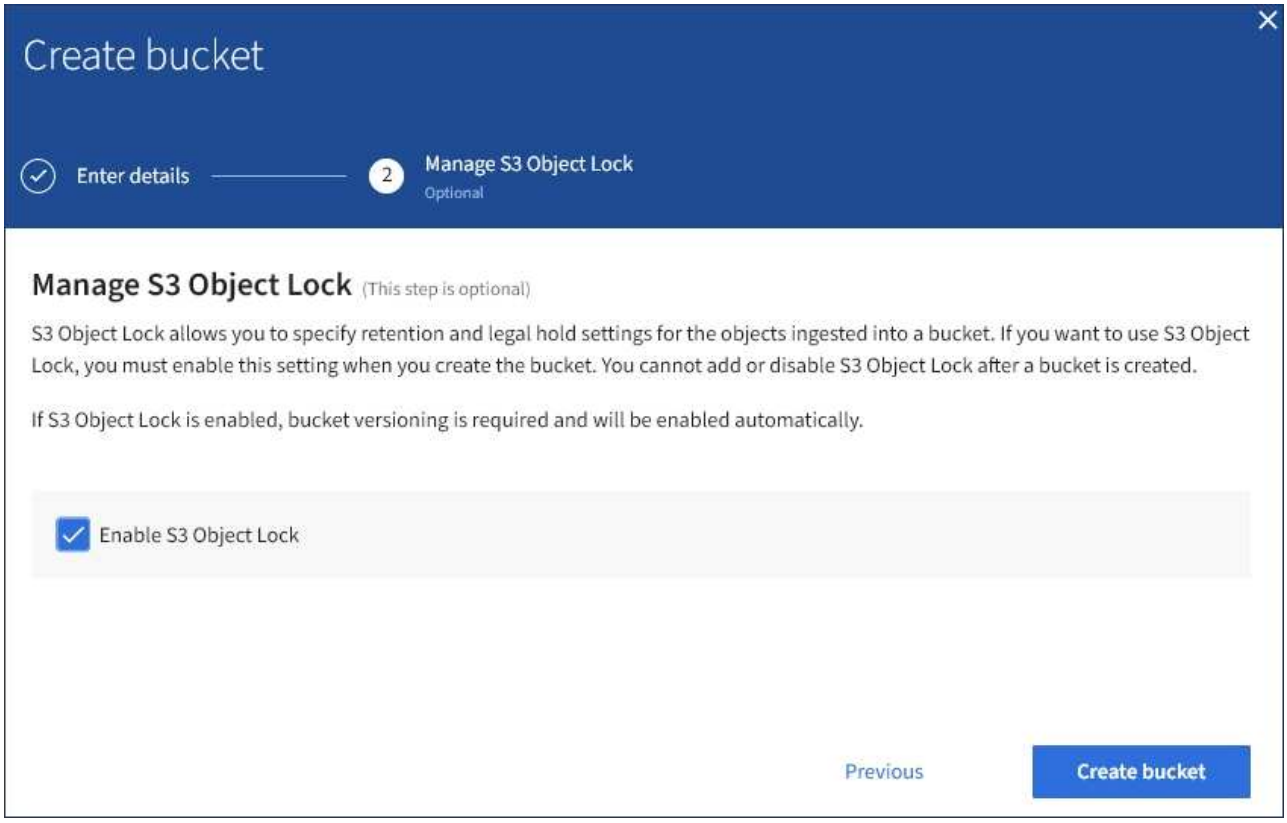
詳細については、Amazon Web Services（AWS）ドキュメントを参照してください。

4. このバケットのリージョンを選択します。

StorageGRID 管理者が利用可能なリージョンを管理します。バケットのリージョンは、オブジェクトに適用されるデータ保護ポリシーに影響する可能性があります。デフォルトでは、すべてのバケットがに作成されます `us-east-1` リージョン：

バケットの作成後にリージョンを変更することはできません。

5. Create bucket または Continue *を選択します。
   - グローバルなS3オブジェクトのロック設定が有効になっていない場合は、*バケットの作成*を選択します。バケットが作成され、バケットページのテーブルに追加されます。
   - グローバルなS3オブジェクトのロック設定が有効になっている場合は、「* Continue *」を選択します。ステップ2：Manage S3 Object Lock（S3オブジェクトのロックの管理）が表示されます。




6. 必要に応じて、このバケットでS3オブジェクトロックを有効にする場合は、チェックボックスを選択します。

   S3 クライアントアプリケーションがバケットに追加されたオブジェクトの最新の保持設定とリーガルホールド設定を指定するには、バケットに対して S3 オブジェクトロックを有効にする必要があります。

   バケットの作成後に S3 オブジェクトのロックを有効または無効にすることはできません。

   バケットで S3 オブジェクトのロックを有効にすると、バケットのバージョン管理が自動的に有効になります。

7. [ * バケットの作成 * ] を選択します。

   バケットが作成され、バケットページのテーブルに追加されます。

関連情報

"ILM を使用してオブジェクトを管理する"

"テナント管理APIについて"

"S3 を使用する"

**S3**バケットの詳細の表示

# テナントアカウントのバケットおよびバケット設定のリストを表示できます。

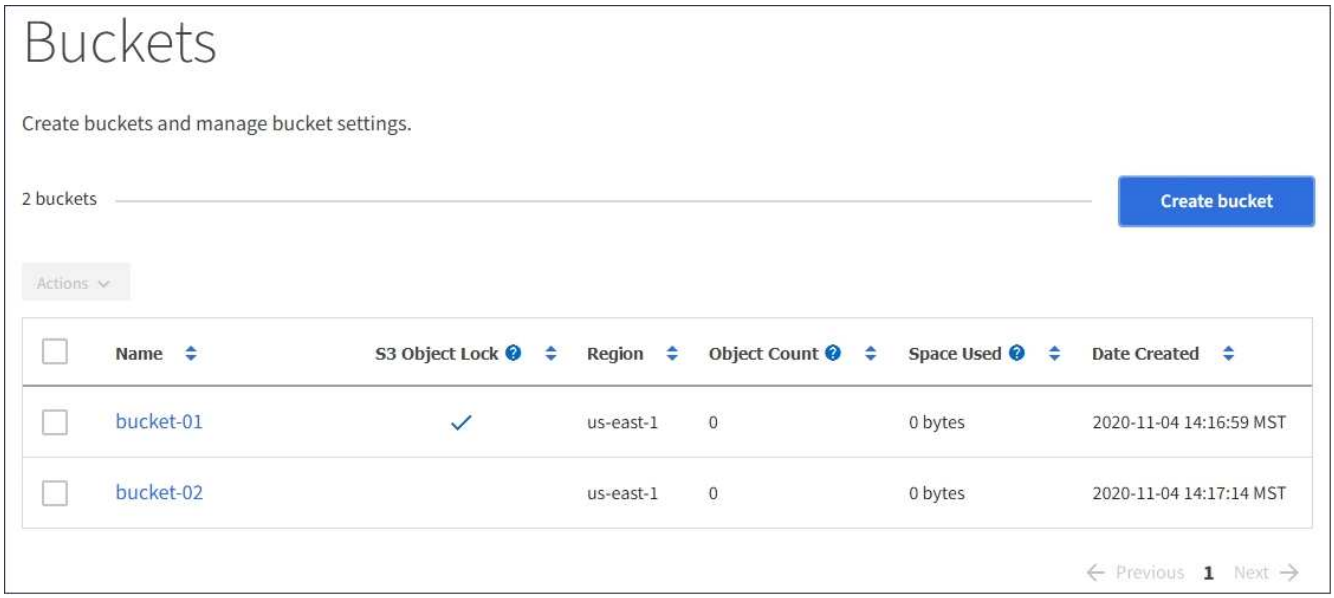
必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。

手順

1. ストレージ（ S3 ） * > * バケット * を選択します。

   バケットページが表示され、テナントアカウントのすべてのバケットがリストされます。




2. 各バケットの情報を確認します。

   必要に応じて、任意の列で情報をソートしたり、リストを前後にページ移動したりできます。

   - Name ：バケットの一意の名前。変更できません。
   - S3 Object Lock ：このバケットで S3 オブジェクトのロックが有効になっているかどうか。

     グローバルな S3 オブジェクトのロック設定が無効になっている場合は、この列は表示されません。この列には、古い準拠バケットの情報も表示されます。

   - Region ：バケットのリージョン。変更できません。
   - Object Count ：このバケット内のオブジェクトの数。
   - Space Used ：このバケット内のすべてのオブジェクトの論理サイズ。論理サイズには、レプリケートコピーやイレイジャーコーディングコピー、またはオブジェクトメタデータに必要な実際のスペースは含まれていません。
   - Date Created ：バケットが作成された日時。

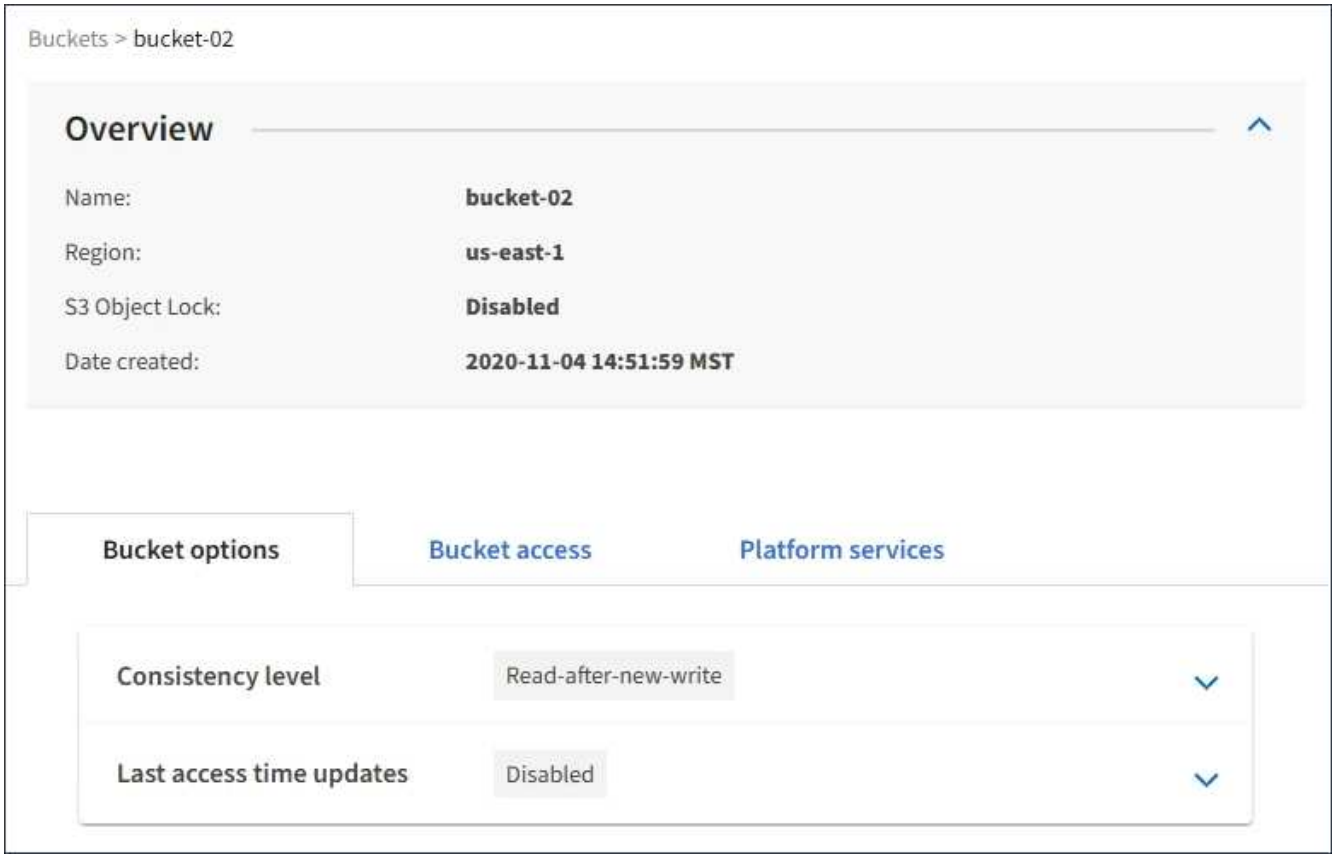
「オブジェクト数」と「使用済みスペース」の値が概算値として表示されます。これらの推定値は、取り込みのタイミング、ネットワーク接続、ノードのステータスによって左右されます。

3. バケットの設定を表示および管理するには、バケット名を選択します。

   バケットの詳細ページが表示されます。

   このページでは、バケットオプション、バケットアクセス、およびプラットフォームサービスの設定を表示および編集できます。

   各設定またはプラットフォームサービスの設定手順を参照してください。




関連情報

"整合性レベルを変更する"

"最終アクセス日時の更新の有効化または無効化"

"Cross-Origin Resource Sharing（CORS）の設定"

"CloudMirrorレプリケーションの設定"

"イベント通知を設定する"

"検索統合サービスの設定"

# S3 テナントを使用している場合は、テナントマネージャまたはテナント管理 API を使用して、 S3 バケット内のオブジェクトに対して実行される処理の整合性制御レベルを変更できます。

必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Manage All Buckets 権限または Root Access 権限のあるユーザグループに属している必要があります。これらの権限は、グループまたはバケットポリシーの権限の設定よりも優先されます。

このタスクについて

整合性レベルを設定する場合は、オブジェクトの可用性と、異なるストレージノードおよびサイト間におけるオブジェクトの整合性のどちらかを犠牲にしなければなりません。通常は、バケットに * Read-after-new-write * 整合性レベルを使用してください。Read-after-new-write *整合性レベルがクライアントアプリケーションの要件を満たさない場合は、バケットの整合性レベルを設定するか、を使用して整合性レベルを変更できます `Consistency-Control` ヘッダー。。 `Consistency-Control` ヘッダーはバケットの整合性レベルよりも優先されます。

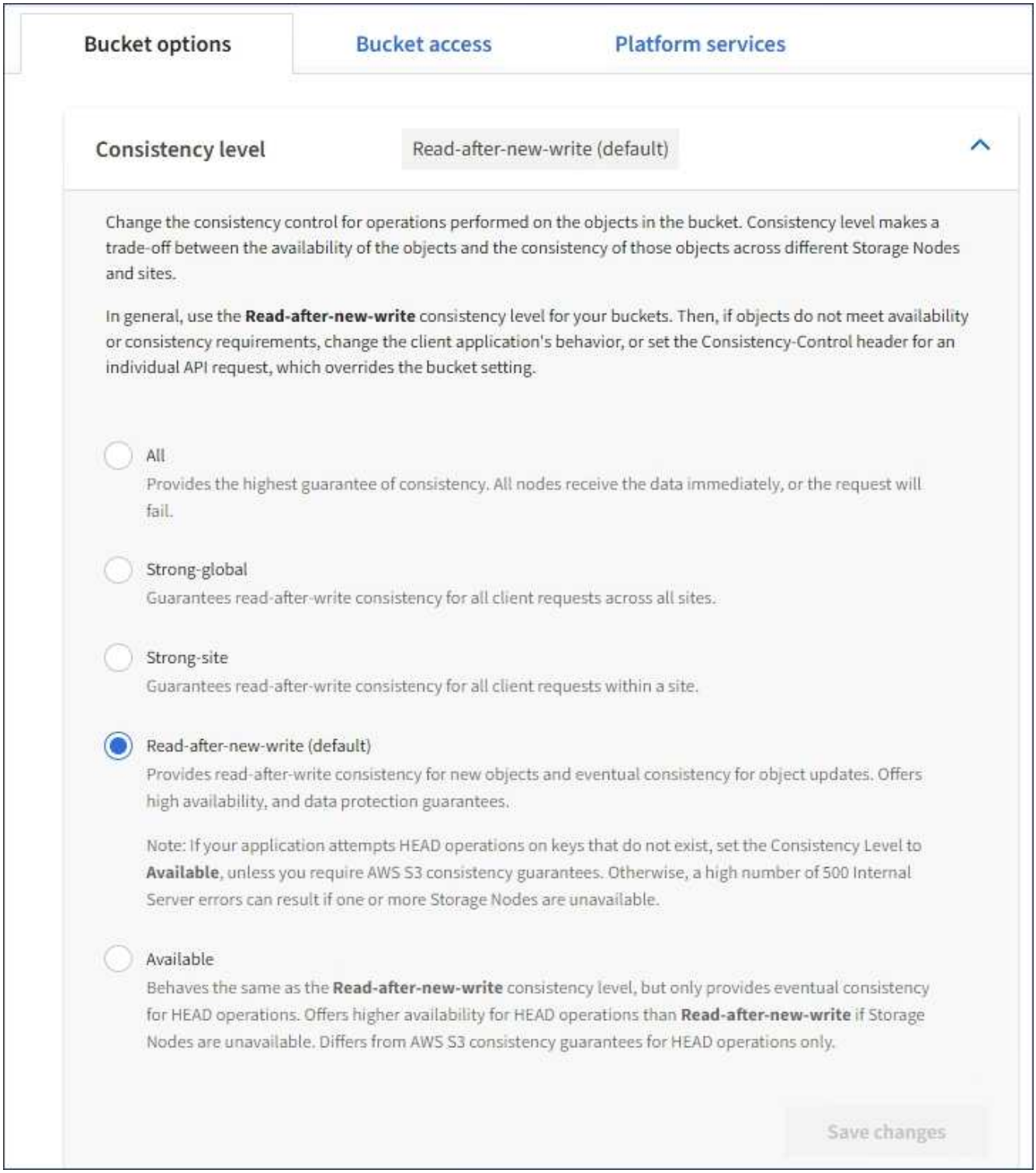
> バケットの整合性レベルを変更した場合、変更後のレベルを満たすことが保証されるのは、変更後に取り込まれたオブジェクトのみです。

手順

1. ストレージ（ S3 ） * > * バケット * を選択します。
2. リストからバケット名を選択します。

   バケットの詳細ページが表示されます。

3. * Bucket options * > * Consistency level * を選択します。




4. このバケット内のオブジェクトに対して実行される処理の整合性レベルを選択します。

| 整合性レベル | 説明 |
| --- | --- |
| すべて | すべてのノードが即座にデータを受け取り、受け取れない場合は要求が失敗します。 |

| 整合性レベル | 説明 |
| --- | --- |
| strong-global | すべてのサイトのすべてのクライアント要求について、リードアフターライト整合性が保証されます。 |
| strong-site | 1 つのサイト内のすべてのクライアント要求について、リードアフターライト整合性が保証されます。 |
| read-after-new-write （デフォルト） | 新規オブジェクトにはリードアフターライト整合性を、オブジェクトの更新には結果整合性を提供します。高可用性が確保され、データ保護が保証されます。Amazon S3の整合性に相当します。<br><br>注：**Amazon S3**の整合性保証が必要な場合を除き、アプリケーションが存在しないキーに対して**HEAD**処理を試行する場合は、整合性レベルを「Available *」に設定してください。そうしないと、使用できないストレージノードがある場合に「 500 Internal Server Error 」が大量に発生する可能性があります。 |
| available（HEAD処理は結果整合性） | read-after-new-write *整合性レベルと動作は同じですが、HEAD処理については結果整合性のみを提供します。ストレージノードを使用できない場合に、HEAD処理に対して「Read-after-new-write」よりも高い可用性が提供される。Amazon S3 の整合性と異なるのは HEAD 処理のみです。 |

5. 「変更を保存」を選択します。

関連情報

"テナント管理権限"

最終アクセス日時の更新の有効化または無効化

グリッド管理者が StorageGRID システムの情報ライフサイクル管理（ ILM ）ルールを作成する際に、オブジェクトを別の格納場所に移動するかどうかを決定する際にオブジェクトの最終アクセス日時を使用するように指定できます。S3 テナントを使用している場合は、 S3 バケット内のオブジェクトに対して最終アクセス日時の更新を有効にすることで、このようなルールを活用できます。

この手順は、配置手順で * Last Access Time * オプションを使用する ILM ルールを 1 つ以上含む StorageGRID システムにのみ適用されます。StorageGRID システムにこのようなルールが含まれていない場合は、この手順を無視してかまいません。

必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Manage All Buckets 権限または Root Access 権限のあるユーザグループに属している必要があります。これらの権限は、グループまたはバケットポリシーの権限の設定よりも優先されます。
- 最終アクセス時間 * は、 ILM ルールの * 参照時間 * 配置手順で使用できるオプションの 1 つです。ルールの参照時間を最終アクセス日時に設定すると、グリッド管理者は、オブジェクトが最後に読み出された（読み取りまたは表示された）タイミングに基づいて特定のストレージの場所にオブジェクトが配置されるように指定できます。

たとえば、最近表示したオブジェクトを高速ストレージに保持するには、次のように指定した ILM ルールを作成できます。

- 過去 1 カ月間に読み出されたオブジェクトは、ローカルストレージノードに保持する。
- 過去 1 カ月間に読み出されなかったオブジェクトは、オフサイトの場所に移動する。

情報ライフサイクル管理を使用してオブジェクトを管理する手順を参照してください。

デフォルトでは、最終アクセス時間の更新は無効です。StorageGRID システムに、 * Last Access Time * オプションを使用する ILM ルールが含まれている場合に、このオプションをこのバケット内のオブジェクトに適用するには、そのルールで指定される S3 バケットで最終アクセス時間の更新を有効にする必要があります。

オブジェクトが読み出されるときに最終アクセス日時を更新すると、特に小さなオブジェクトについては StorageGRID のパフォーマンスが低下する可能性があります。

最終アクセス時間の更新では、オブジェクトが読み出されるたびに StorageGRID で以下の追加手順が実行されるため、パフォーマンスが低下します。

- 新しいタイムスタンプでオブジェクトを更新します
- 現在の ILM ルールとポリシーに照らしてオブジェクトが再評価されるように、 ILM キューにオブジェクトを追加します

次の表に、最終アクセス時間が有効または無効な場合のバケット内のすべてのオブジェクトに適用される動作をまとめます。

| 要求のタイプ | 最終アクセス時間が無効な場合の動作（デフォルト） | | 最終アクセス時間が有効な場合の動作 | |
|---|---|---|---|---|
| | 最終アクセス時間の更新 | ILM 評価キューへのオブジェクトの追加 | 最終アクセス時間の更新 | ILM 評価キューへのオブジェクトの追加 |
| オブジェクト、そのアクセス制御リスト、またはメタデータの読み出し要求 | いいえ | いいえ | はい。 | はい。 |
| オブジェクトメタデータの更新要求 | はい。 | はい。 | はい。 | はい。 |
| バケット間でのオブジェクトのコピー要求 | • ソースコピーに対しては、「いいえ」と指定します<br>• デスティネーションコピーについては、はい | • ソースコピーに対しては、「いいえ」と指定します<br>• デスティネーションコピーについては、はい | • ソースコピーについては、はい<br>• デスティネーションコピーについては、はい | • ソースコピーについては、はい<br>• デスティネーションコピーについては、はい |

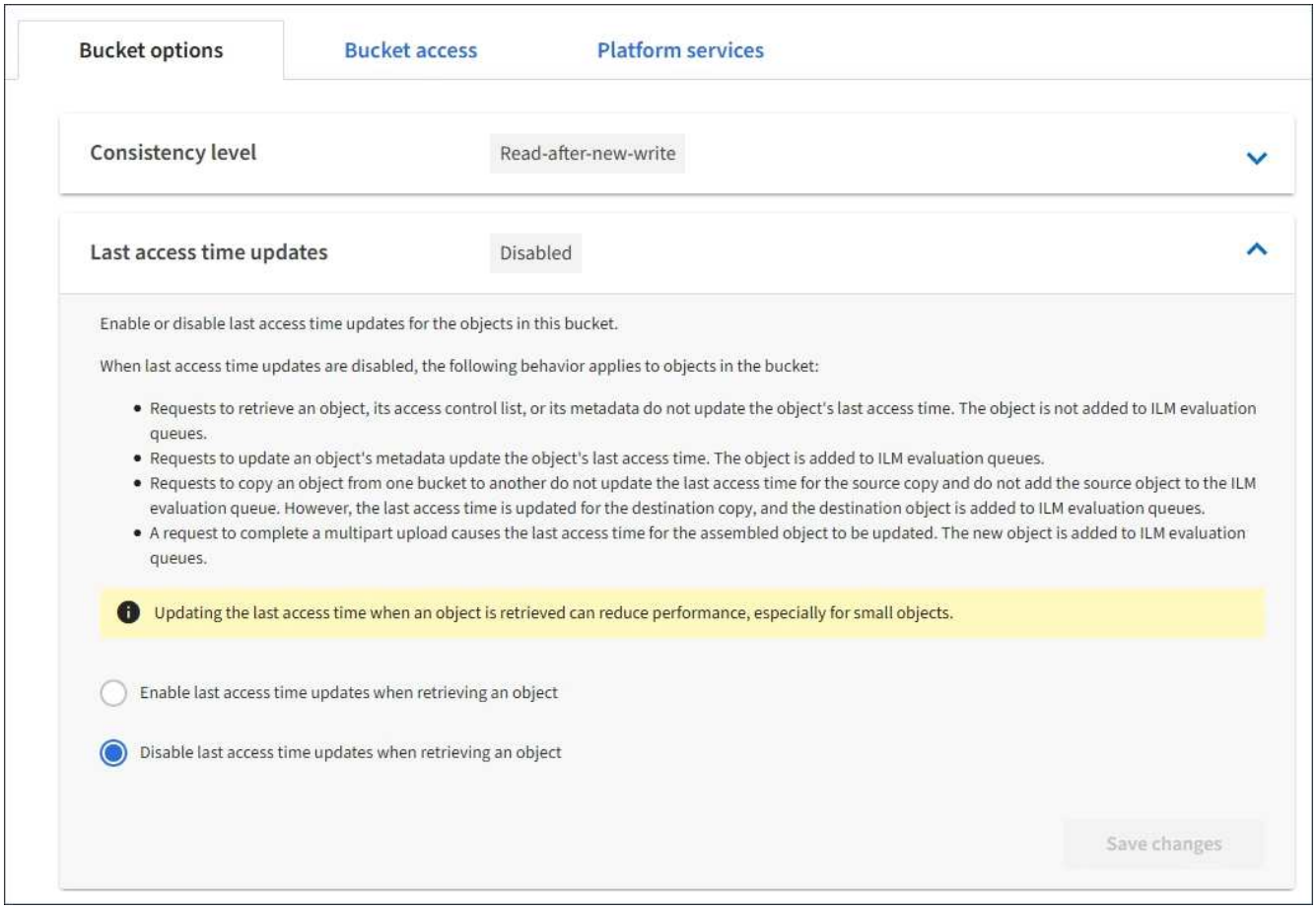
| | | | | |
|---|---|---|---|---|
| マルチパートアップロードの完了要求 | はい、アセンブルされたオブジェクトの場合 | はい、アセンブルされたオブジェクトの場合 | はい、アセンブルされたオブジェクトの場合 | はい、アセンブルされたオブジェクトの場合 |

手順

1. ストレージ（ S3 ） * > * バケット * を選択します。
2. リストからバケット名を選択します。

   バケットの詳細ページが表示されます。

3. 「 * Bucket options * > * Last access time updates * 」を選択します。
4. 適切なオプションボタンを選択して、最終アクセス日時の更新を有効または無効にします。




5. 「変更を保存」を選択します。

関連情報

"テナント管理権限"

"ILM を使用してオブジェクトを管理する"

**Cross-Origin Resource Sharing（CORS）の設定**

## S3 バケットとバケット内のオブジェクトに他のドメインにある Web アプリケーション

## からアクセスできるようにする必要がある場合は、そのバケットに Cross-Origin Resource Sharing （ CORS ）を設定できます。

必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Manage All Buckets 権限または Root Access 権限のあるユーザグループに属している必要があります。これらの権限は、グループまたはバケットポリシーの権限の設定よりも優先されます。

このタスクについて

Cross-Origin Resource Sharing （ CORS ）は、あるドメインのクライアント Web アプリケーションが別のドメインのリソースにアクセスできるようにするセキュリティ機能です。たとえば、というS3バケットを使用するとします `Images` グラフィックを保存します。のCORSを設定する `Images` バケットを使用すると、そのバケット内の画像をWebサイトに表示できます `http://www.example.com`。

手順

1. CORS を有効にするために必要な XML をテキストエディタで作成します。

   次の例は、 S3 バケットの CORS を有効にするために使用される XML を示しています。このXMLでは、すべてのドメインにバケットへのGET要求の送信が許可されていますが、にしか許可されていません `http://www.example.com` POST要求と削除要求を送信するドメイン。要求ヘッダーはすべて許可されます。

   ```
   <CORSConfiguration
       xmlns="http://s3.amazonaws.com/doc/2020-10-22/">
       <CORSRule>
           <AllowedOrigin>*</AllowedOrigin>
           <AllowedMethod>GET</AllowedMethod>
           <AllowedHeader>*</AllowedHeader>
       </CORSRule>
       <CORSRule>
           <AllowedOrigin>http://www.example.com</AllowedOrigin>
           <AllowedMethod>GET</AllowedMethod>
           <AllowedMethod>POST</AllowedMethod>
           <AllowedMethod>DELETE</AllowedMethod>
           <AllowedHeader>*</AllowedHeader>
       </CORSRule>
   </CORSConfiguration>
   ```

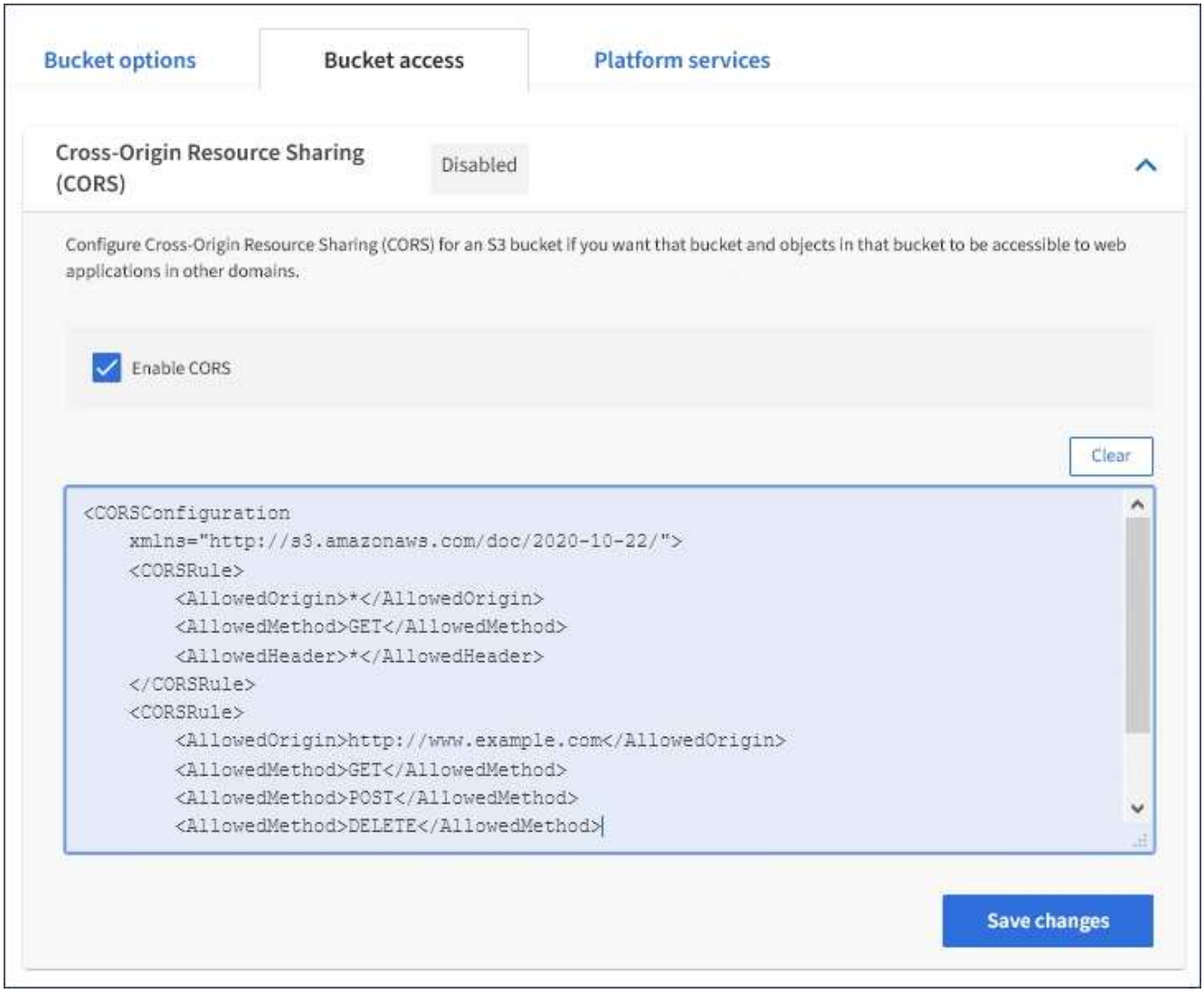
   CORS 設定 XML の詳細については、を参照してください "Amazon Web Services （ AWS ）ドキュメント：「 Amazon Simple Storage Service Developer Guide"。

2. Tenant Manager で、 * Storage （ S3 ） * > * Buckets * を選択します。
3. リストからバケット名を選択します。

   バケットの詳細ページが表示されます。

4. Bucket access * > * Cross-Origin Resource Sharing （ CORS ） * を選択します。

5. ［ * CORS を有効にする * ］ チェックボックスをオンにします。
6. CORS 設定 XML をテキストボックスに貼り付け、 * 変更内容を保存 * を選択します。




7. バケットの CORS 設定を変更するには、テキストボックスで CORS 設定 XML を更新するか、 * Clear * を選択してやり直してください。次に、「変更を保存」を選択します。
8. バケットの CORS を無効にするには、 * CORS を有効にする * チェックボックスの選択を解除し、 * 変更内容を保存 * を選択します。

**S3**バケットを削除しています

## Tenant Manager を使用して、空の S3 バケットを削除できます。

必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Manage All Buckets 権限または Root Access 権限のあるユーザグループに属している必要があります。これらの権限は、グループまたはバケットポリシーの権限の設定よりも優先されます。

このタスクについて

以下の手順では、 Tenant Manager を使用して S3 バケットを削除する方法について説明します。テナント管

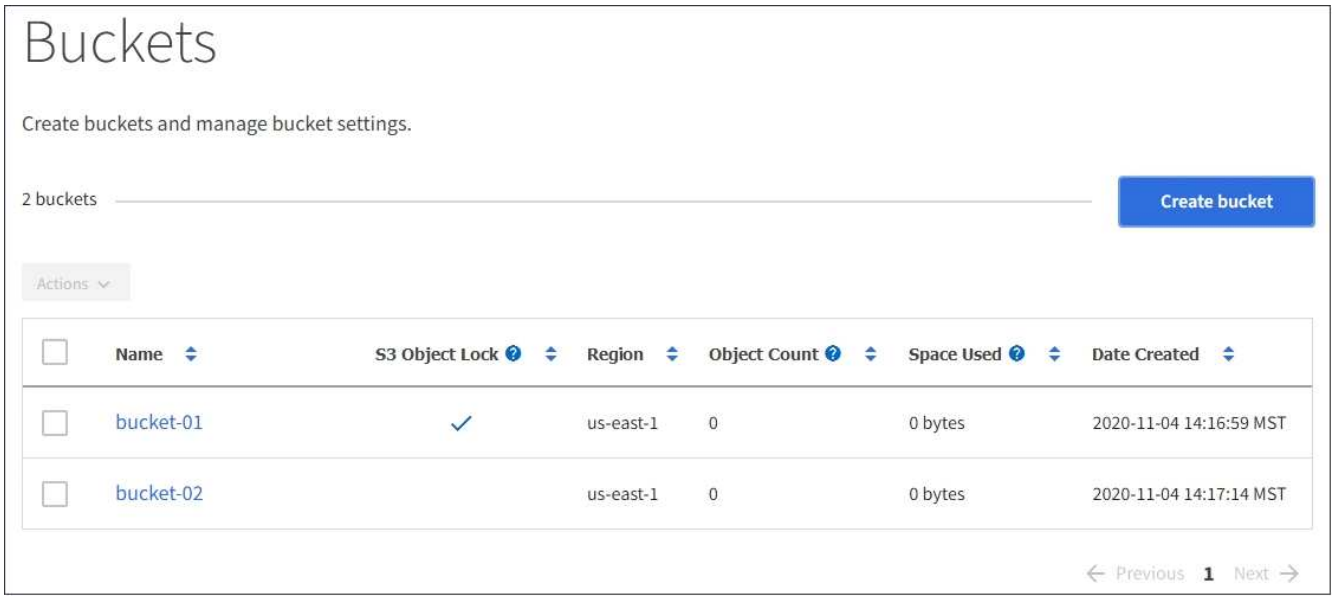
理APIまたはS3 REST APIを使用してS3バケットを削除することもできます。

オブジェクトまたは最新でないオブジェクトバージョンが含まれている S3 バケットは削除できません。S3バージョン管理オブジェクトの削除方法については、情報ライフサイクル管理を使用してオブジェクトを管理する手順を参照してください。

手順

1. ストレージ（ S3 ） * > * バケット * を選択します。

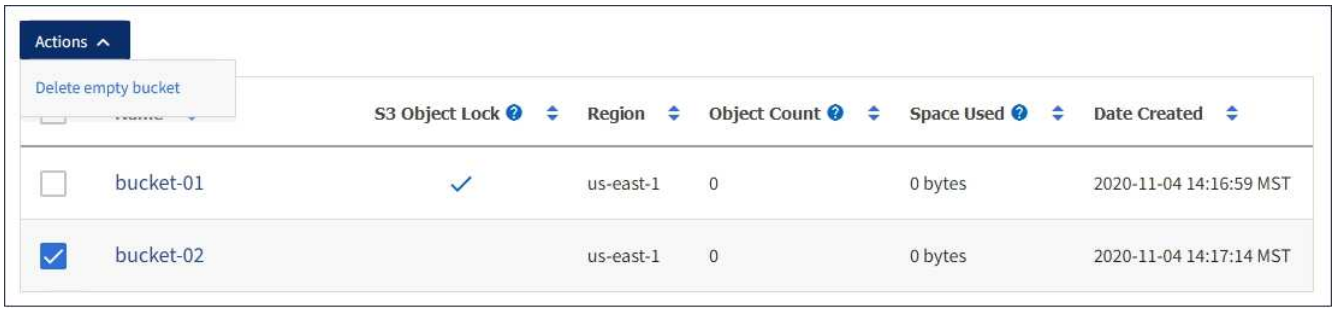
   バケットページが表示され、既存の S3 バケットがすべて表示されます。



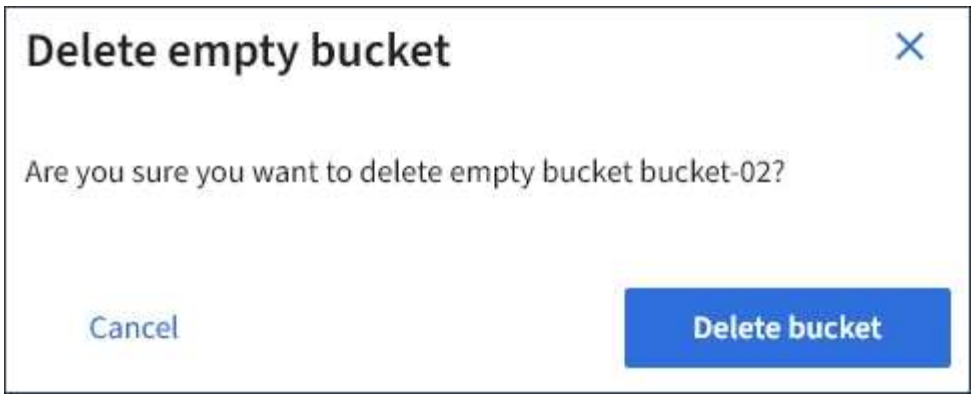

2. 削除する空のバケットのチェックボックスを選択します。

   [ アクション ] メニューが有効になります。

3. アクションメニューから*空のバケットを削除*を選択します。




   確認メッセージが表示されます。




4. バケットを削除してもよろしいですか？*バケットの削除*を選択します。

   StorageGRID は、バケットが空であることを確認してから、バケットを削除します。この処理には数分かかることがあります。

   バケットが空でない場合は、エラーメッセージが表示されます。バケットを削除する前に、すべてのオブジェクトを削除する必要があります。

関連情報

"ILM を使用してオブジェクトを管理する"

## S3プラットフォームサービスの管理

S3テナントアカウントにプラットフォームサービスの使用が許可されている場合は、プラットフォームサービスを使用して外部サービスを利用し、S3バケットに対してCloudMirrorレプリケーション、通知、および検索統合を設定できます。

- "プラットフォームサービスとは"
- "プラットフォームサービスの使用に関する考慮事項"
- "プラットフォームサービスエンドポイントの設定"
- "CloudMirrorレプリケーションの設定"
- "イベント通知を設定する"
- "検索統合サービスを使用する"

プラットフォームサービスとは

StorageGRID プラットフォームサービスは、ハイブリッドクラウドの実装に役立ちます。

テナントアカウントにプラットフォームサービスの使用が許可されている場合は、 S3 バケットに対して次の

サービスを設定できます。

- * CloudMirror レプリケーション * ： StorageGRID CloudMirror レプリケーションサービスは、StorageGRID バケットから指定された外部のデスティネーションに特定のオブジェクトをミラーリングするために使用します。

  たとえば、 CloudMirror レプリケーションを使用して特定の顧客レコードを Amazon S3 にミラーリングし、 AWS サービスを利用してデータを分析することができます。

  ソースバケットで S3 オブジェクトのロックが有効になっている場合、 CloudMirror レプリケーションはサポートされません。

- * 通知 * ：バケット単位のイベント通知は、オブジェクトに対して実行された特定の処理に関する通知を、指定された外部の Amazon Simple Notification Service ™（ SNS ）に送信するために使用します。

  たとえば、バケットに追加された各オブジェクトについてアラートが管理者に送信されるように設定できます。この場合、オブジェクトは重大なシステムイベントに関連付けられているログファイルです。

  S3 オブジェクトのロックが有効になっているバケットでイベント通知を設定することはできますが、オブジェクトの S3 オブジェクトロックメタデータ（ Retain Until Date および Legal Hold のステータスを含む）は通知メッセージに含まれません。

- * 検索統合サービス * ：検索統合サービスは、外部サービスを使用してメタデータを検索または分析できるように、指定された Elasticsearch インデックスに S3 オブジェクトメタデータを送信するために使用します。

  たとえば、リモートの Elasticsearch サービスに S3 オブジェクトメタデータを送信するようにバケットを設定できます。次に、 Elasticsearch を使用してバケット間で検索を実行し、オブジェクトメタデータのパターンに対して高度な分析を実行できます。

  S3 オブジェクトロックが有効なバケットでは Elasticsearch 統合を設定できますが、オブジェクトの S3 オブジェクトロックメタデータ（ Retain Until Date および Legal Hold のステータスを含む）は通知メッセージに含まれません。

通常、プラットフォームサービスのターゲットは StorageGRID 環境の外部にあるため、プラットフォームサービスを使用することで外部ストレージリソース、通知サービス、検索または分析サービスの機能と柔軟性をデータに対して利用できます。

単一の S3 バケットに対して複数のプラットフォームサービスを組み合わせて設定できます。たとえば、StorageGRID S3 バケットに対して CloudMirror サービスと通知の両方を設定して、特定のオブジェクトを Amazon Simple Storage Service にミラーリングし、同時に各オブジェクトに関する通知を他社製の監視アプリケーションに送信して AWS の費用を追跡できます。

プラットフォームサービスの使用は、 StorageGRID 管理者がグリッドマネージャまたはグリッド管理 API を使用してテナントアカウントごとに有効にする必要があります。

### プラットフォームサービスの設定方法

プラットフォームサービスは、 Tenant Manager またはテナント管理 API を使用して、設定した外部エンドポイントと通信します。各エンドポイントは外部のデスティネーション（ StorageGRID S3 バケット、 Amazon Web Services バケット、 Simple Notification Service （ SNS ）トピック、ローカル、 AWS などにホストさ

れる Elasticsearch クラスタなど）です。

エンドポイントを作成したら、バケットに XML 設定を追加してプラットフォームサービスを有効にすることができます。XML 設定は、バケットが処理を実行するオブジェクト、実行する処理、およびサービスに使用するエンドポイントを特定します。

設定するプラットフォームサービスごとに XML 設定を追加する必要があります。例：

1. キーがで始まるすべてのオブジェクトを指定する場合 `/images` Amazon S3バケットにレプリケートするには、ソースバケットにレプリケーション設定を追加する必要があります。
2. これらのオブジェクトがバケットに格納されたときに通知も送信するには、通知設定を追加する必要があります。
3. 最後に、これらのオブジェクトのメタデータのインデックスを作成する場合は、検索統合を実装するためのメタデータ通知設定を追加する必要があります。

設定 XML の形式は、 StorageGRID プラットフォームサービスの実装に使用する S3 REST API に従います。

| プラットフォームサービス | **S3 REST API** |
| --- | --- |
| CloudMirror レプリケーション | • GET Bucket replication<br>• PUT Bucket replication |
| 通知 | • GET Bucket notification<br>• PUT Bucket notification |
| 検索統合 | • GET Bucket metadata notification configuration<br>• PUT Bucket metadata notification configuration のコマンドです<br>これらは StorageGRID 独自の処理です。 |

StorageGRID でのこれらの API の実装方法の詳細については、 S3 クライアントアプリケーションを実装する手順を参照してください。

関連情報

"S3 を使用する"

"CloudMirrorレプリケーションサービスの概要"

"バケットの通知の概要"

"検索統合サービスの概要"

"プラットフォームサービスの使用に関する考慮事項"

**CloudMirror**レプリケーションサービスの概要

StorageGRID で、ある S3 バケットに追加されたオブジェクトを指定して 1 つ以上のデスティネーションバケットにレプリケートする必要がある場合は、そのバケットに対し

て CloudMirror レプリケーションを有効にすることができます。

CloudMirror レプリケーションは、グリッドのアクティブな ILM ポリシーとは別に動作します。CloudMirror サービスは、ソースバケットに格納された時点でオブジェクトをレプリケートし、できるだけ早くデスティネーションバケットに配信します。レプリケートオブジェクトの配信は、オブジェクトの取り込みが成功したときにトリガーされます。

既存のバケットに対して CloudMirror レプリケーションを有効にすると、そのバケットに追加された新しいオブジェクトのみがレプリケートされます。バケット内の既存のオブジェクトはレプリケートされません。既存のオブジェクトのレプリケーションを強制的に実行するには、オブジェクトのコピーを実行して既存のオブジェクトのメタデータを更新します。

CloudMirror レプリケーションを使用して AWS S3 デスティネーションにオブジェクトをコピーする場合は、 Amazon S3 では各 PUT 要求ヘッダー内のユーザ定義メタデータのサイズが 2KB に制限されることに注意してください。オブジェクトのユーザ定義メタデータが 2KB を超える場合、そのオブジェクトはレプリケートされません。

StorageGRID では、 1 つのバケット内のオブジェクトを複数のデスティネーションバケットにレプリケートできます。そのためには、レプリケーション設定 XML で各ルールのデスティネーションを指定します。1 つのオブジェクトを複数のバケットに同時にレプリケートすることはできません。

また、バージョン管理に対応している / していないバケットで CloudMirror レプリケーションを設定することもでき、バージョン管理に対応している / していないバケットをデスティネーションとして指定できます。バージョン管理に対応しているバケットとしていないバケットを組み合わせて使用することができます。たとえば、バージョン管理に対応しているバケットをバージョン管理に対応していないソースバケットのデスティネーションとして指定することも、その逆を指定することもできます。また、バージョン管理に対応していないバケット間でもレプリケートできます。

CloudMirror レプリケーションサービスの削除は、 Amazon S3 が提供する Cross Region Replication （ CRR ；クロスリージョンレプリケーション）サービスの削除と同様に機能します。つまり、ソースバケット内のオブジェクトを削除してもデスティネーションのレプリケートオブジェクトは削除されません。ソースとデスティネーションの両方のバケットがバージョン管理に対応している場合は、削除マーカーがレプリケートされます。デスティネーションバケットがバージョン管理に対応していない場合は、ソースバケット内のオブジェクトを削除しても削除マーカーはデスティネーションバケットにレプリケートされず、デスティネーションオブジェクトも削除されません。

デスティネーションバケットにレプリケートされたオブジェクトは、 StorageGRID によって「 replicas. 」とマークされます。 デスティネーションの StorageGRID バケットはレプリカとしてマークされたオブジェクトを再びレプリケートしないため、意図しないレプリケーションのループが発生することはありません。このレプリカマーキングは StorageGRID の内部処理で、 Amazon S3 バケットをデスティネーションとして使用する際に AWS CRR を使用することには支障はありません。

レプリカのマークに使用されるカスタムヘッダーはです `x-ntap-sg-replica`。このマーキングは ' カスケード・ミラーを防止しますStorageGRID は、 2 つのグリッド間の双方向 CloudMirror をサポートしています。

デスティネーションバケット内ではイベントは一意になるとは限らず、その順序も保証されません。確実に配信することを目的とした処理の結果として、ソースオブジェクトの同一のコピーが複数デスティネーションに配信されることがあります。まれに、複数の異なる StorageGRID サイトから同じオブジェクトが同時に更新された場合、デスティネーションバケットでの処理の順序がソースバケットでのイベントの順序と一致しないことがあります。

通常、 CloudMirror レプリケーションは外部の S3 バケットをデスティネーションとして使用するように設定します。ただし、他の StorageGRID 環境や任意の S3 互換サービスを使用するようにレプリケーションを設定することもできます。

関連情報

"CloudMirrorレプリケーションの設定"

バケットの通知の概要

## S3 バケットに対するイベント通知を有効にすると、指定したイベントに関する通知を StorageGRID からデスティネーションの Amazon Simple Notification Service （ SNS ）に送信できます。

イベント通知を設定するには、通知設定XMLをソースバケットに関連付けます。通知設定 XML には S3 の規則に従ってバケットの通知を設定し、デスティネーションの SNS トピックをエンドポイントの URN として指定します。

イベント通知は通知設定に従ってソースバケットで作成され、デスティネーションに配信されます。オブジェクトに関連付けられているイベントが成功すると、そのイベントに関する通知が作成されて配信のためにキューに登録されます。

一意になるとは限らず、その順序も保証されません。確実に配信することを目的とした処理の結果として、 1 つのイベントに関する通知が複数デスティネーションに配信されることがあります。また配信は非同期で実行されるため、特に異なる StorageGRID サイトで開始された処理の場合、デスティネーションでの通知の時間的順序がソースバケットでのイベントの順序と一致する保証はありません。を使用できます `sequencer` Amazon S3のドキュメントに従って、イベントメッセージを入力して特定のオブジェクトに対するイベントの順序を決定します。

サポートされている通知およびメッセージです

StorageGRID イベント通知は Amazon S3 API に準拠しますが、次の制限事項があります。

- 次のイベントタイプには通知を設定できません。これらのイベントタイプは * サポートされていません。
  - `s3:ReducedRedundancyLostObject`
  - `s3:ObjectRestore:Completed`
- StorageGRID から送信されるイベント通知は標準の JSON 形式を使用しますが、次の表に示すように使用されないキーおよび特定の値が使用されるキーがあります。

| キー名 | **StorageGRID** 値 |
| --- | --- |
| eventSource | `sgws:s3` |
| awsRegion のようになります | 含まれません |
| x-amz-id-2 | 含まれません |
| ARN | `urn:sgws:s3:::bucket_name` |

関連情報

"イベント通知を設定する"

検索統合サービスの概要

# オブジェクトメタデータに外部の検索およびデータ分析サービスを使用する必要がある場合は、 S3 バケットの検索統合を有効にすることができます。

検索統合サービスはカスタムの StorageGRID サービスです。 S3 オブジェクトまたはそのメタデータが更新されるたびに、オブジェクトメタデータを非同期的に自動でデスティネーションエンドポイントに送信します。その後、デスティネーションサービスが提供する高度な検索、データ分析、視覚化、機械学習のツールを使用して、オブジェクトデータを検索、分析し、情報を把握できます。

検索統合サービスはバージョン管理に対応している / していないに関わらずすべてのバケットに対して有効にすることができ検索統合を設定するには、対象のオブジェクトおよびオブジェクトメタデータのデスティネーションを指定したメタデータ通知設定 XML をバケットに関連付けます。

通知は、という名前の JSON ドキュメントの形式で生成されます。バケット名、オブジェクト名、バージョン ID も必要です。各メタデータ通知には、すべてのオブジェクトのタグとユーザメタデータに加えて、オブジェクトのシステムメタデータの標準セットが含まれています。

> タグとユーザメタデータの場合、 StorageGRID は文字列または S3 イベント通知として Elasticsearch に日付と番号を渡します。これらの文字列を日付または数値として解釈するように Elasticsearch を設定するには、動的フィールドマッピングおよびマッピング日付形式に関する Elasticsearch の手順に従ってください。検索統合サービスを設定する前に、インデックスの動的フィールドマッピングを有効にする必要があります。ドキュメントにインデックスを付けた後は、インデックス内のドキュメントのフィールドタイプを編集できません。

通知は次の場合に常に生成され、配信のキューに登録されます

- オブジェクトが作成されます。
- オブジェクトが削除されたとき。グリッドの ILM ポリシーの処理が実行された結果、オブジェクトが削除される場合も含まれます。
- オブジェクトのメタデータまたはタグが追加、更新、または削除されたとき。変更された値だけでなく、すべてのメタデータとタグが常に更新時に送信されます。

バケットにメタデータ通知設定 XML を追加すると、新しく作成したオブジェクトや、データ、ユーザメタデータ、またはタグの更新によって変更したオブジェクトに関する通知が送信されます。ただし、バケット内の既存のオブジェクトに関する通知は送信されません。バケットに含まれるすべてのオブジェクトのオブジェクトメタデータを確実にデスティネーションに送信するには、次のいずれかを行う必要があります。

- バケットの作成後、オブジェクトを追加する前に、検索統合サービスを設定する。
- すでにバケットに含まれているすべてのオブジェクトに対して、メタデータ通知メッセージをデスティネーションに送信するトリガーとなる処理を実行する。

StorageGRID 検索統合サービスは、デスティネーションとして Elasticsearch クラスタをサポートします。他のプラットフォームサービスと同様、 URN がサービスの設定 XML で使用されているエンドポイントにデスティネーションが指定されます。サポートされているElasticsearchのバージョンを確認するには、Interoperability Matrix Toolを使用してください。

関連情報

"NetApp Interoperability Matrix Tool で確認できます"

"検索統合用の XML を設定します"

"メタデータ通知に含まれているオブジェクトメタデータ"

"検索統合サービスで生成される JSON"

"検索統合サービスの設定"

プラットフォームサービスの使用に関する考慮事項

## プラットフォームサービスを実装する前に、これらのサービスの使用に関する推奨事項と考慮事項を確認してください。

プラットフォームサービスの使用に関する考慮事項

| 考慮事項 | 詳細 |
| --- | --- |
| デスティネーションエンドポイントの監視 | 各デスティネーションエンドポイントの可用性を監視する必要があります。長時間にわたってデスティネーションエンドポイントへの接続が失われ、要求のバックログが大量に発生している場合、 StorageGRID に対する以降のクライアント要求（ PUT 要求など）は失敗します。エンドポイントがアクセス可能になったら、失敗した要求を再試行する必要があります。 |
| デスティネーションエンドポイントのスロットル | 要求が送信されるペースがデスティネーションエンドポイントで要求を受信できるペースを超えると、 StorageGRID ソフトウェアはバケットの受信 S3 要求を調整する場合があります。スロットルは、デスティネーションエンドポイントへの送信を待機している要求のバックログが生じている場合にのみ発生します。<br><br>明らかな影響は、受信 S3 要求の実行時間が長くなることだけです。パフォーマンスが大幅に低下していることが検出されるようになった場合は、取り込み速度を下げるか、容量の大きいエンドポイントを使用する必要があります。要求のバックログが増え続けると、クライアント S3 処理（ PUT 要求など）が失敗します。<br><br>通常、 CloudMirror 要求には、検索統合やイベント通知の要求よりも多くのデータ転送が含まれるため、デスティネーションエンドポイントのパフォーマンスによる影響を受ける可能性が高くなります。 |
| 順序保証 | StorageGRID では、 1 つのサイト内のオブジェクトに対する処理の順序が保証されます。あるオブジェクトに対するすべての処理が同じサイト内で実行されるかぎり、最終的なオブジェクトの（レプリケーションの）状態は常に StorageGRID の状態と同じになります。<br><br>StorageGRID は、 StorageGRID サイト間で処理が行われる場合、最善の順序で要求を処理しようと試みます。たとえば、最初にサイト A にオブジェクトを書き込んだあと、サイト B で同じオブジェクトを上書きした場合、 CloudMirror によって最終的にデスティネーションバケットにレプリケートされるオブジェクトが新しいほうのオブジェクトであるとはかぎりません。 |

| 考慮事項 | 詳細 |
| --- | --- |
| ILM ベースのオブジェクト削除 | AWS CRR サービスと SNS サービスの削除動作を一致させるため、StorageGRID の ILM ルールに基づいてソースバケット内のオブジェクトが削除された場合、 CloudMirror 要求とイベント通知要求は送信されません。たとえば、 ILM ルールによって 14 日後にオブジェクトが削除された場合、CloudMirror 要求やイベント通知要求は送信されません。<br><br>一方、 ILM に基づいてオブジェクトが削除された場合、検索統合要求は送信されます。 |

**CloudMirror**レプリケーションサービスの使用に関する考慮事項

| 考慮事項 | 詳細 |
| --- | --- |
| レプリケーションのステータス | StorageGRID ではがサポートされません `x-amz-replication-status` ヘッダー。 |
| オブジェクトのサイズ | CloudMirrorレプリケーションサービスでデスティネーションバケットにレプリケートできるオブジェクトの最大サイズは5TBであり、StorageGRID でサポートされる最大オブジェクトサイズと同じです。 |
| バケットのバージョン管理とバージョン ID | StorageGRID でソース S3 バケットのバージョン管理を有効にした場合、デスティネーションバケットのバージョン管理も有効にする必要があります。<br><br>バージョン管理を使用している場合、 S3 プロトコルの制限事項により、デスティネーションバケットのオブジェクトバージョンの処理はベストエフォートベースで行われ、 CloudMirror サービスによる保証はありません。<br><br>• 注 * ： StorageGRID のソースバケットのバージョン ID は、デスティネーションバケットのバージョン ID とは関連がありません。 |

| | |
|---|---|
| オブジェクトバージョンのタグ付け | CloudMirror サービスでは、 S3 プロトコルの制限事項により、バージョン ID を提供する PUT Object tagging 要求と DELETE Object tagging 要求がレプリケートされません。ソースとデスティネーションのバージョン ID には関連がないため、特定のバージョン ID へのタグの更新を確実にレプリケートする方法はありません。<br><br>一方、バージョン ID を指定しない PUT Object tagging 要求と DELETE Object tagging 要求は、CloudMirror サービスによってレプリケートされます。これらの要求は、最新のキー（バケットがバージョン管理されている場合は最新のバージョン）のタグを更新します。（タグの更新ではなく）タグを使用した通常の取り込みもレプリケートされます。 |
| マルチパートアップロードおよび `ETag` 値 | マルチパートアップロードを使用してアップロードされたオブジェクトをミラーリングした場合、CloudMirror サービスではパートが保持されません。その結果、が表示されます `ETag` ミラーオブジェクトの値は、とは異なります `ETag` 元のオブジェクトの値。 |
| SSE-C （ユーザ指定のキーによるサーバ側の暗号化）で暗号化されたオブジェクト | CloudMirror サービスでは、 SSE-C で暗号化されたオブジェクトがサポートされませんCloudMirror レプリケーションのソースバケットにオブジェクトを取り込む際に、要求に SSE-C 要求ヘッダーが含まれていると、処理が失敗します。 |
| S3 オブジェクトのロックが有効になっているバケット | CloudMirrorレプリケーションのデスティネーションS3バケットでS3オブジェクトロックが有効になっている場合は、レプリケーション処理がAccessDeniedエラーで失敗します。 |

関連情報

"S3 を使用する"

プラットフォームサービスエンドポイントの設定

## バケットのプラットフォームサービスを設定する前に、少なくとも 1 つのエンドポイントをプラットフォームサービスのデスティネーションとして設定する必要があります。

プラットフォームサービスへのアクセスは、 StorageGRID 管理者がテナント単位で有効にします。プラットフォームサービスエンドポイントを作成または使用するには、ストレージノードが外部のエンドポイントリソースにアクセスできるようネットワークが設定されているグリッドで、 Manage Endpoints または Root Access 権限のあるテナントユーザである必要があります。詳細については、 StorageGRID 管理者にお問い合わせください。

プラットフォームサービスエンドポイントとは

プラットフォームサービスエンドポイントを作成するときは、 StorageGRID が外部のデスティネーションにアクセスするために必要な情報を指定します。

たとえば、StorageGRID バケットからS3バケットにオブジェクトをレプリケートする場合は、AWSのデスティネーションバケットにアクセスするためにStorageGRID で必要な情報とクレデンシャルを含むプラットフォームサービスエンドポイントを作成します。

プラットフォームサービスのタイプごとに独自のエンドポイントが必要なため、使用する各プラットフォームサービスについて少なくとも 1 つのエンドポイントを設定する必要があります。プラットフォームサービスエンドポイントの定義が完了したら、サービスを有効にするための設定 XML でエンドポイントの URN をデスティネーションとして指定します。

同じエンドポイントを複数のソースバケットのデスティネーションとして使用できます。たとえば、複数のバケット間で検索を実行できるように、複数のソースバケットが同じ検索統合エンドポイントにオブジェクトメタデータを送信するように設定できます。また、複数のエンドポイントをターゲットとして使用するようにソースバケットを設定することもできます。この方法は、オブジェクトの作成に関する通知をある SNS トピックに送信し、オブジェクトの削除に関する通知を別の SNS トピックに送信する場合などに使用します。

**CloudMirror** レプリケーション用のエンドポイント

StorageGRID は、 S3 バケットを表すレプリケーションエンドポイントをサポートします。このバケットは、 Amazon Web Services 、同一またはリモートの StorageGRID 環境、あるいは別のサービスでホストされている可能性があります。

通知用のエンドポイント

StorageGRID は、 Simple Notification Service （ SNS ）エンドポイントをサポートします。Simple Queue Service （ SQS ）エンドポイントまたは AWS Lambda エンドポイントはサポートされていません。

検索統合サービスのエンドポイント

StorageGRID は、 Elasticsearch クラスタを表す検索統合エンドポイントをサポートします。Elasticsearch クラスタは、ローカルデータセンターにあるか、 AWS クラウドなどの別の場所でホストされている可能性があります。

検索統合エンドポイントは、 Elasticsearch の特定のインデックスとタイプを参照します。StorageGRID でエンドポイントを作成する前に、 Elasticsearch でインデックスを作成しておく必要があります。作成していない場合、エンドポイントの作成に失敗します。タイプはエンドポイントの作成前に作成しておく必要はありません。StorageGRID は、オブジェクトメタデータをエンドポイントに送信するときに必要に応じてタイプを作成します。

関連情報

"StorageGRID の管理"

プラットフォームサービスのエンドポイントの**URN**の指定

プラットフォームサービスエンドポイントを作成するときは、 Unique Resource Name （ URN ）を指定する必要があります。プラットフォームサービスの設定 XML を作成する際、 URN を使用してエンドポイントを参照します。各エンドポイントの URN は一意である必要があります。

プラットフォームサービスエンドポイントは、作成時に StorageGRID で検証されます。プラットフォームサービスエンドポイントを作成する前に、エンドポイントで指定されたリソースが存在し、アクセス可能であることを確認してください。

**URN** 要素

プラットフォームサービスのエンドポイントのURNは、いずれかで開始する必要があります `arn:aws` または `urn:mysite`、次のようにします。

- サービスがAWSでホストされている場合は、を使用します `arn:aws`。
- サービスがローカルでホストされている場合は、を使用します `urn:mysite`

たとえば、StorageGRID でホストされるCloudMirrorエンドポイントのURNを指定する場合、URNはで始まる可能性があります `urn:sgws`。

URN の次の要素では、次のようにプラットフォームサービスのタイプを指定します。

| サービス | を入力します |
| --- | --- |
| CloudMirror レプリケーション | S3 |
| 通知 | SnS |
| 検索統合 | ES |

たとえば、StorageGRID でホストされるCloudMirrorエンドポイントのURNを指定する場合は、と指定します `s3` をダウンロードしてください `urn:sgws:s3`。

URN の最後の要素は、デスティネーション URI の特定のターゲットリソースを識別します。

| サービス | 特定のリソース |
| --- | --- |
| CloudMirror レプリケーション | バケット名 |
| 通知 | sns-topic-name を入力します |
| 検索統合 | `domain-name/index-name/type-name`<br>• 注： Elasticsearch クラスタが * NOT * である場合、インデックスを自動的に作成するように設定されているため、エンドポイントを作成する前にインデックスを手動で作成する必要があります。 |

**AWS**でホストされるサービスの**URN**

AWSのエンティティの場合、完全なURNは有効なAWS ARNです。例：

- CloudMirror レプリケーション：

```
arn:aws:s3:::bucket-name
```

- 通知：

```
arn:aws:sns:region:account-id:topic-name
```

- 検索統合：

```
arn:aws:es:region:account-id:domain/domain-name/index-name/type-name
```

> AWS検索統合エンドポイントの場合は、を参照してください `domain-name` リテラル文字列を含める必要があります `domain/`を参照してください。

ローカルでホストされるサービスの **URN**

クラウド サービス ではなくローカルでホストされるサービスを使用する場合は、 URN の 3 番目と最後の必須要素が含まれていて、有効かつ一意な URN が作成されるのであれば、どのような方法で URN を指定してもかまいません。となっている要素はオプションで空白にすることも、リソースを識別して一意な URN の作成に役立つ任意の情報を指定することもできます。例：

- CloudMirror レプリケーション：

```
urn:mysite:s3:optional:optional:bucket-name
```

StorageGRID でホストされるCloudMirrorエンドポイントの場合は、で始まる有効なURNを指定できます `urn:sgws`：

```
urn:sgws:s3:optional:optional:bucket-name
```

- 通知：

```
urn:mysite:sns:optional:optional:sns-topic-name
```

- 検索統合：

```
urn:mysite:es:optional:optional:domain-name/index-name/type-name
```

ローカルでホストされる検索統合エンドポイントの場合は、を参照してください `domain-name` エンドポイントのURNが一意であるかぎり、Elementには任意の文字列を指定できます。

プラットフォームサービスエンドポイントの作成

# プラットフォームサービスを有効にする前に、正しいタイプのエンドポイントを少なくとも 1 つ作成しておく必要があります。

必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- テナントアカウントのプラットフォームサービスが StorageGRID 管理者によって有効化されている必要があります。
- Manage Endpoints 権限のあるユーザグループに属している必要があります。
- プラットフォームサービスエンドポイントによって参照されるリソースを作成しておく必要があります。
  - CloudMirror レプリケーション： S3 バケット
  - イベント通知： SNS トピック
  - 検索通知：インデックスを自動的に作成するようにデスティネーションクラスタが設定されていない場合、 Elasticsearch インデックス。
- デスティネーションリソースに関する情報を確認しておく必要があります。
  - Uniform Resource Identifier （ URI ）のホストとポート

    StorageGRID システムでホストされているバケットを CloudMirror レプリケーションのエンドポイントとして使用する場合は、グリッド管理者に問い合わせて入力が必要な値を決定してください。

  - Unique Resource Name （ URN ）

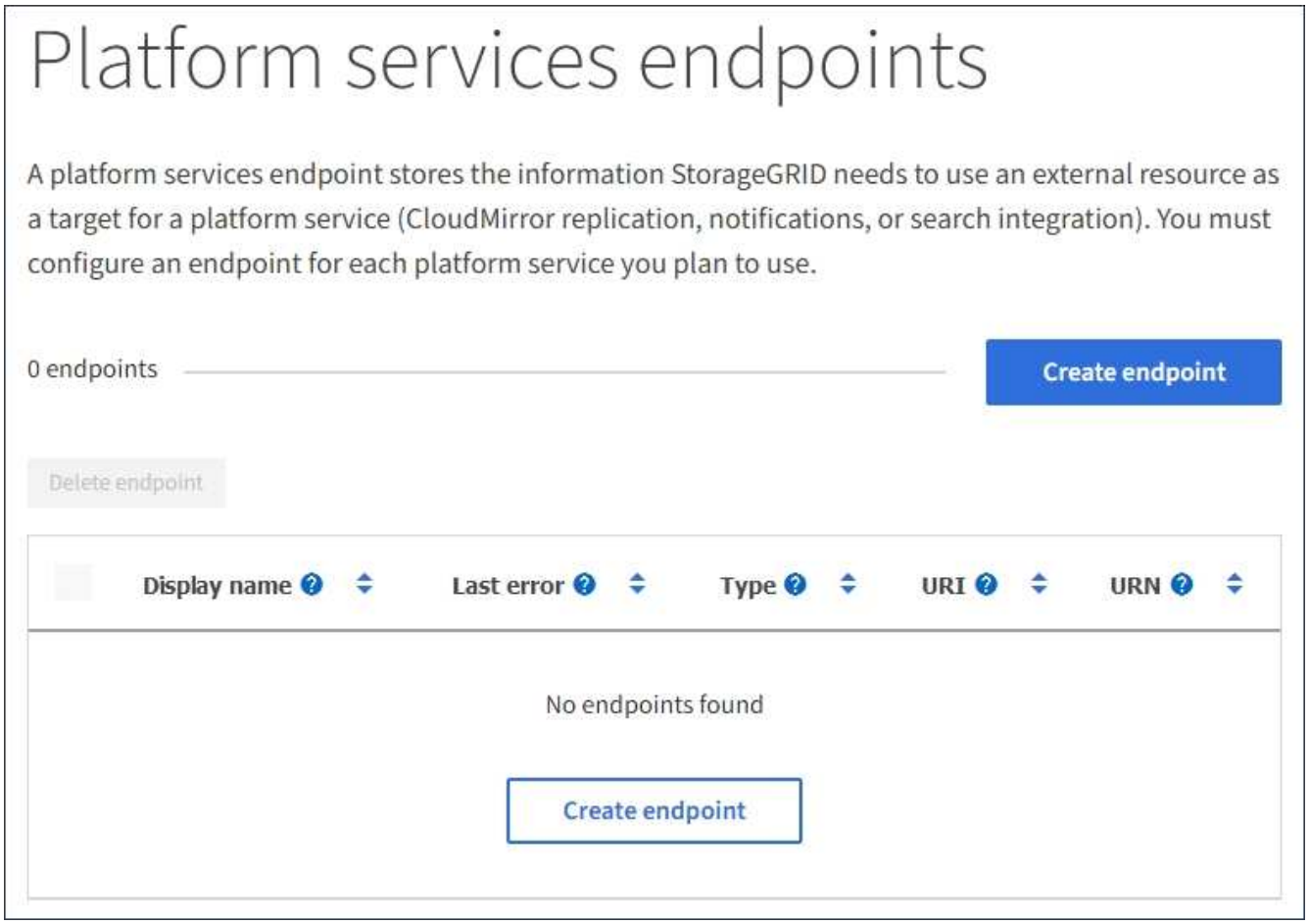
    "プラットフォームサービスのエンドポイントのURNの指定"

  - 認証クレデンシャル（必要な場合）：
    - Access Key ：アクセスキー ID とシークレットアクセスキー
    - 基本 HTTP 認証：ユーザ名とパスワード
  - セキュリティ証明書（カスタム CA 証明書を使用する場合）

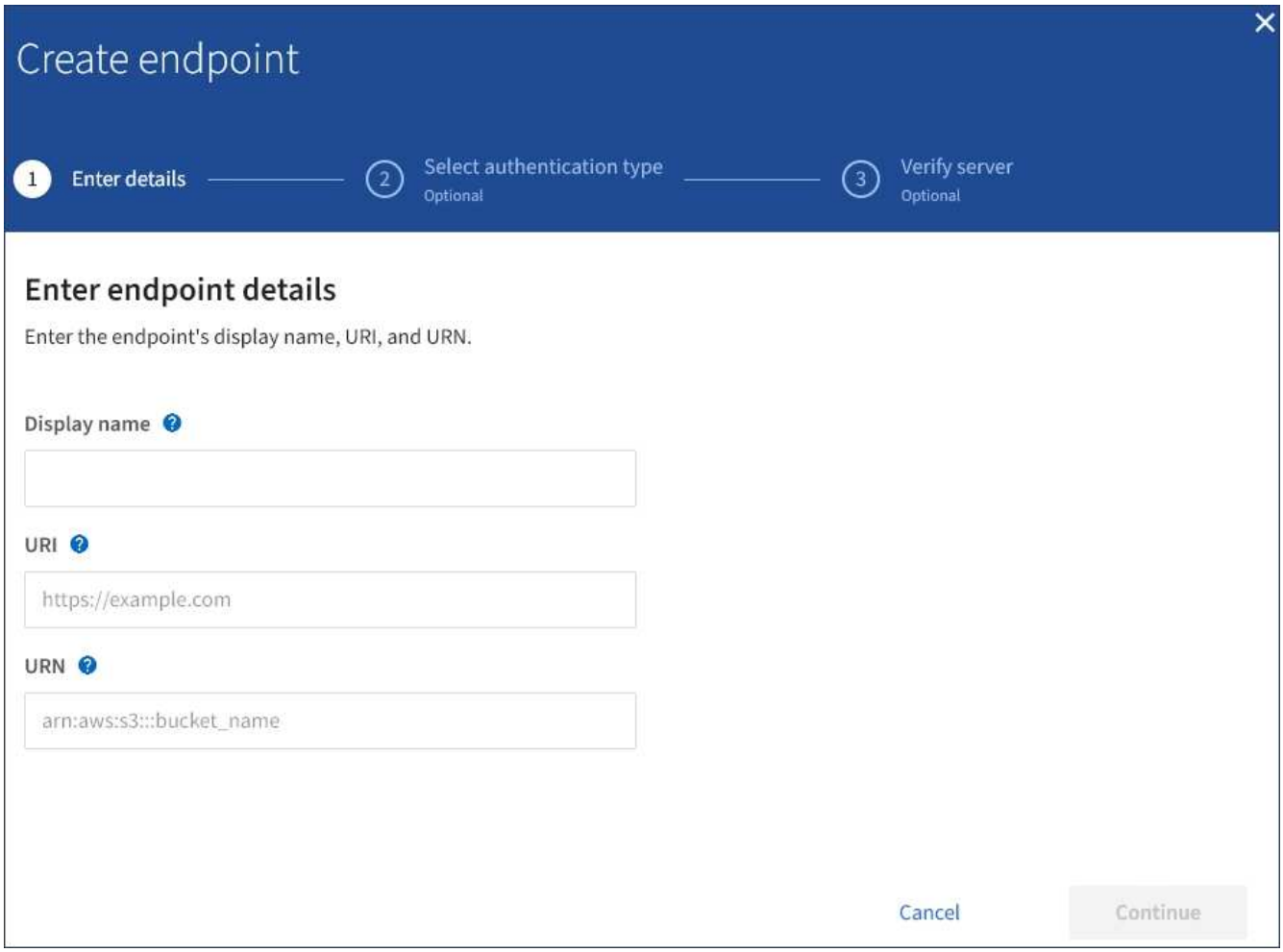
手順

1. ストレージ（ S3 ） * > * プラットフォームサービスのエンドポイント * を選択します。

   プラットフォームサービスエンドポイントページが表示されます。




2. [ * エンドポイントの作成 * ] を選択します。




3. エンドポイントとその目的を簡単に説明する表示名を入力します。

   エンドポイントがサポートするプラットフォームサービスのタイプは、エンドポイントページでその情報を表示するときにエンドポイント名の横に表示されるため、名前にその情報を含める必要はありません。

4. [* URI*] フィールドに、エンドポイントの Unique Resource Identifier （ URI ）を指定します。

   次のいずれかの形式を使用します。

   ```
   https://host:port
   http://host:port
   ```

   ポートを指定しない場合、 HTTPS URI にはポート 443 が、 HTTP URI にはポート 80 が使用されます。

   たとえば、 StorageGRID でホストされているバケットの URI は次のようになります。

   ```
   https://s3.example.com:10443
   ```

   この例では、 `s3.example.com` StorageGRID ハイアベイラビリティ（HA）グループの仮想IP（VIP）のDNSエントリ、およびを表します `10443` ロードバランサエンドポイントで定義されたポートを表します。

単一点障害を回避するには、できるだけ負荷分散ノードの HA グループに接続する必要があります。

同様に、 AWS でホストされているバケットの URI は次のようになります。

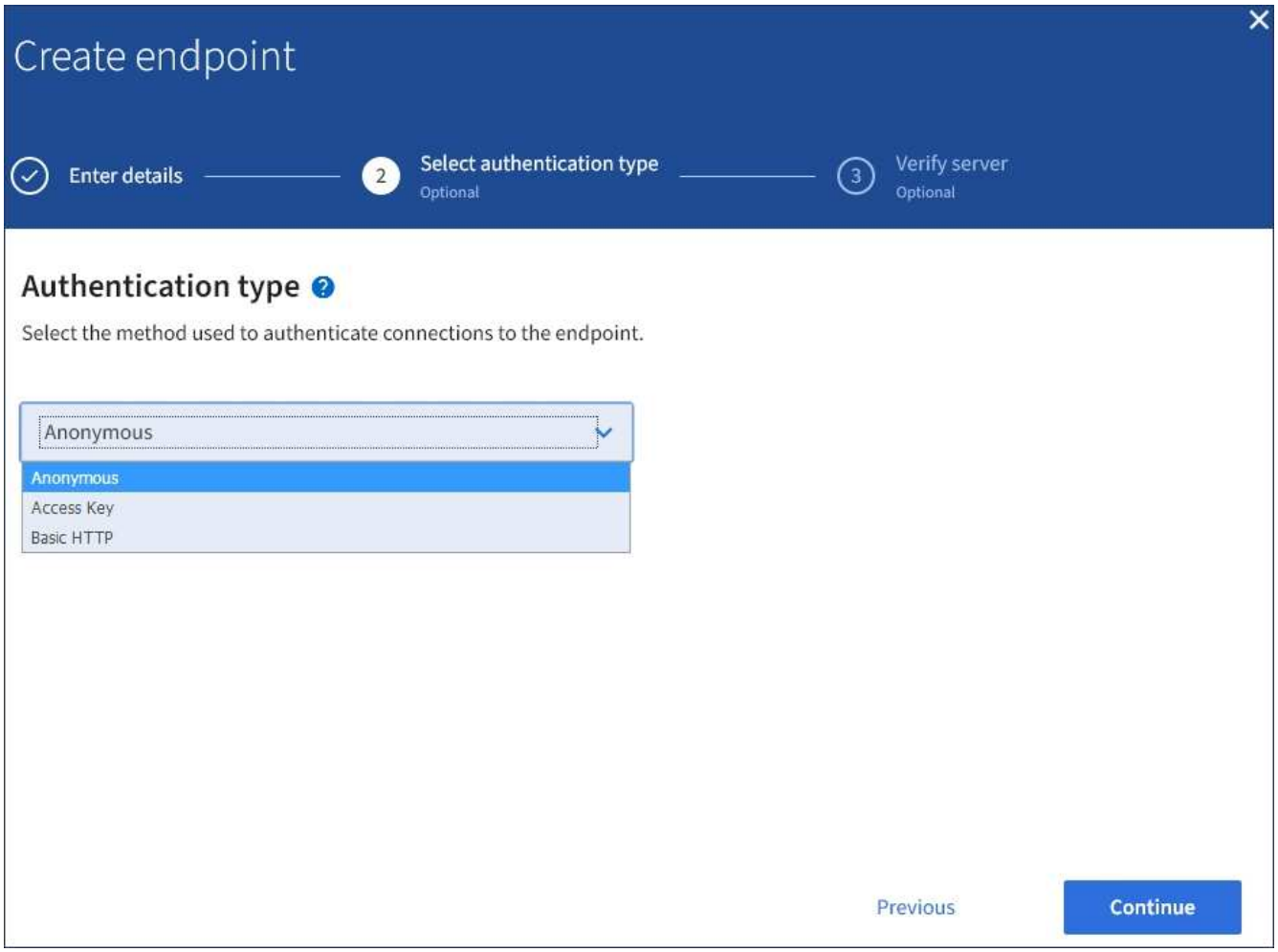
```
https://s3-aws-region.amazonaws.com
```

エンドポイントが CloudMirror レプリケーションサービスで使用される場合は、 URI にバケット名を含めないでください。バケット名は「 * URN * 」フィールドに含める必要があります。

5. エンドポイントの Unique Resource Name （ URN ）を入力します。

エンドポイントの作成後に、エンドポイントの URN を変更することはできません。

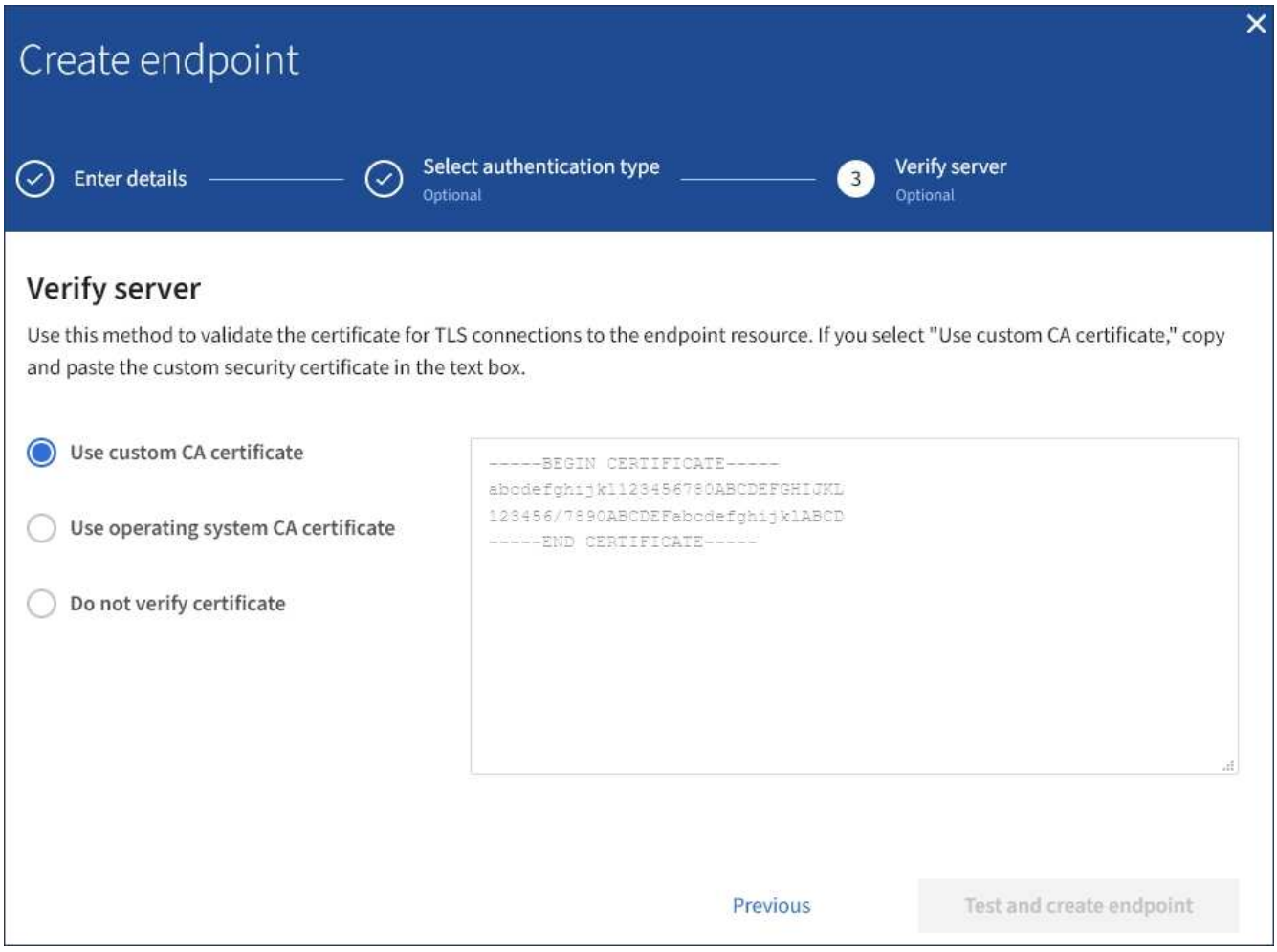
6. 「 * Continue * 」を選択します。
7. 「*認証タイプ」の値を選択し、必要なクレデンシャルを入力します。




指定するクレデンシャルには、デスティネーションリソースに対する書き込み権限が必要です。

| 認証タイプ | 説明 | クレデンシャル |
| --- | --- | --- |
| 匿名 | デスティネーションへの匿名アクセスを許可します。セキュリティが無効になっているエンドポイントでのみ機能します。 | 認証なし。 |
| アクセスキー | AWS 形式のクレデンシャルを使用してデスティネーションとの接続を認証します。 | • アクセスキー ID<br>• シークレットアクセスキー |
| 基本 HTTP | ユーザ名とパスワードを使用して、デスティネーションへの接続を認証します。 | • ユーザ名<br>• パスワード |

8. 「 * Continue * 」を選択します。
9. Verify server * のラジオボタンを選択して、エンドポイントへの TLS 接続の検証方法を選択します。



| 証明書検証のタイプ | 説明 |
| --- | --- |
| カスタム CA 証明書を使用する | カスタムのセキュリティ証明書を使用します。この設定を選択した場合は、カスタムセキュリティ証明書を * CA 証明書 * テキストボックスにコピーして貼り付けます。 |
| オペレーティングシステムの CA 証明書を使用します | オペレーティングシステムにインストールされているデフォルトのCA証明書を使用して接続を保護します。 |
| 証明書を検証しないでください | TLS 接続に使用される証明書は検証されません。このオプションはセキュアではありません。 |

10. [ * テストとエンドポイントの作成 * ] を選択します。
    - 指定したクレデンシャルを使用してエンドポイントにアクセスできた場合は、成功を伝えるメッセージが表示されます。エンドポイントへの接続は、各サイトの 1 つのノードから検証されます。
    - エンドポイントの検証が失敗した場合は、エラーメッセージが表示されます。エラーを修正するためにエンドポイントを変更する必要がある場合は、 * エンドポイントの詳細に戻る * を選択して情報を更新します。次に、「 * Test 」を選択し、エンドポイントを作成します。 *

> テナントアカウントでプラットフォームサービスが有効でない場合は、エンドポイントの作成が失敗します。StorageGRID 管理者にお問い合わせください。

エンドポイントの設定が完了したら、その URN を使用してプラットフォームサービスを設定できます。

関連情報

"プラットフォームサービスのエンドポイントのURNの指定"

"CloudMirrorレプリケーションの設定"

"イベント通知を設定する"

"検索統合サービスの設定"

プラットフォームサービスエンドポイントの接続をテストしています

## プラットフォームサービスへの接続が変更された場合は、エンドポイントへの接続をテストして、デスティネーションリソースが存在すること、および指定したクレデンシャルでアクセスできることを確認できます。

必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Manage Endpoints 権限のあるユーザグループに属している必要があります。

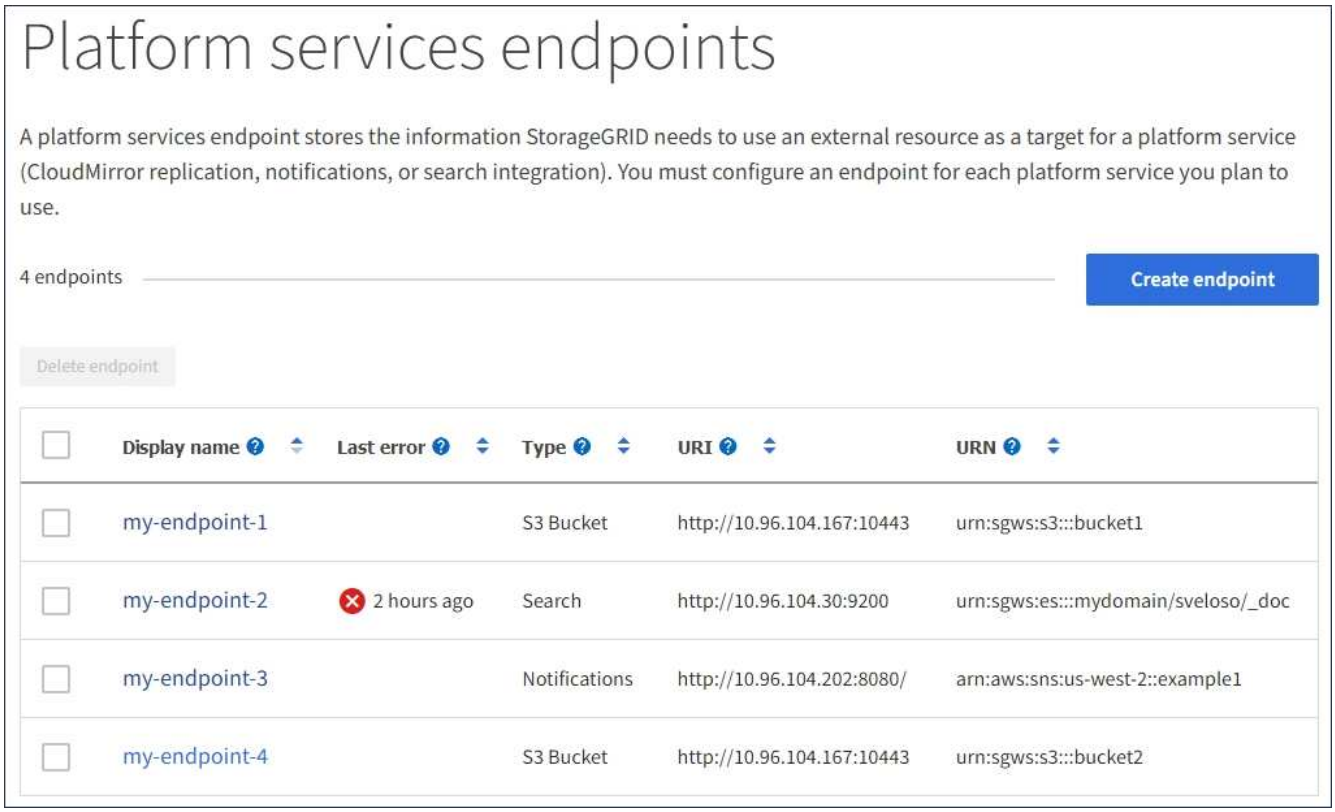
このタスクについて

StorageGRID は、クレデンシャルに正しい権限があるかどうかを検証しません。

手順

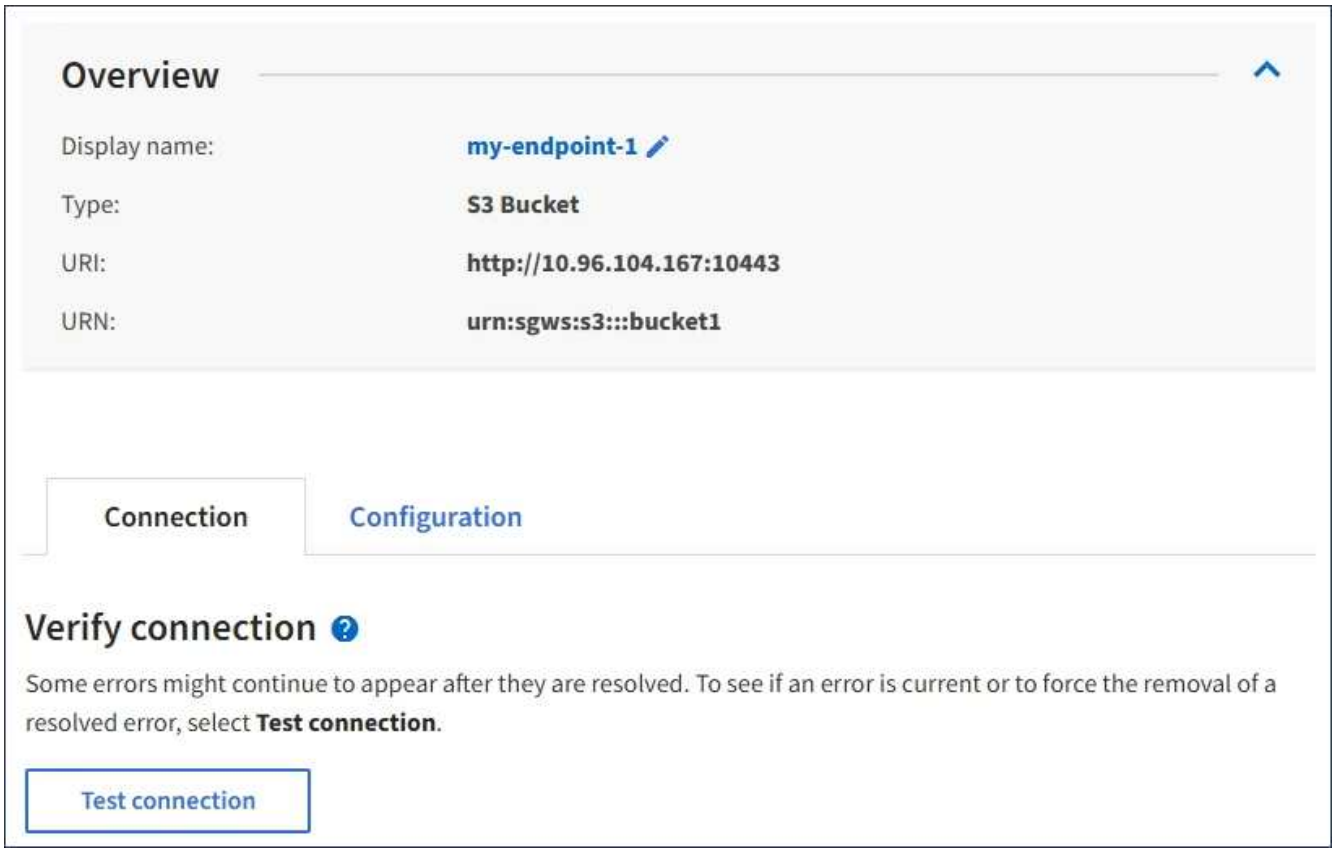
1. ストレージ（ S3 ） * > * プラットフォームサービスのエンドポイント * を選択します。

   Platform services Endpoints ページが表示され、設定済みのプラットフォームサービスエンドポイントのリストが表示されます。




2. 接続をテストするエンドポイントを選択します。

   エンドポイントの詳細ページが表示されます。




3. [ 接続のテスト * ] を選択します。
   - 指定したクレデンシャルを使用してエンドポイントにアクセスできた場合は、成功を伝えるメッセージが表示されます。エンドポイントへの接続は、各サイトの 1 つのノードから検証されます。
   - エンドポイントの検証が失敗した場合は、エラーメッセージが表示されます。エラーを修正するためにエンドポイントを変更する必要がある場合は、「 * Configuration * 」を選択して情報を更新します。次に、 [ テスト ] を選択し、変更を保存します。 *

プラットフォームサービスエンドポイントの編集

プラットフォームサービスエンドポイントの設定を編集して、名前、 URI 、またはその他の詳細を変更できます。たとえば、期限切れのクレデンシャルを更新したり、フェールオーバー用のバックアップ Elasticsearch インデックスを指すように URI を変更したりすることが必要な場合があります。プラットフォームサービスのエンドポイントの URN を変更することはできません。

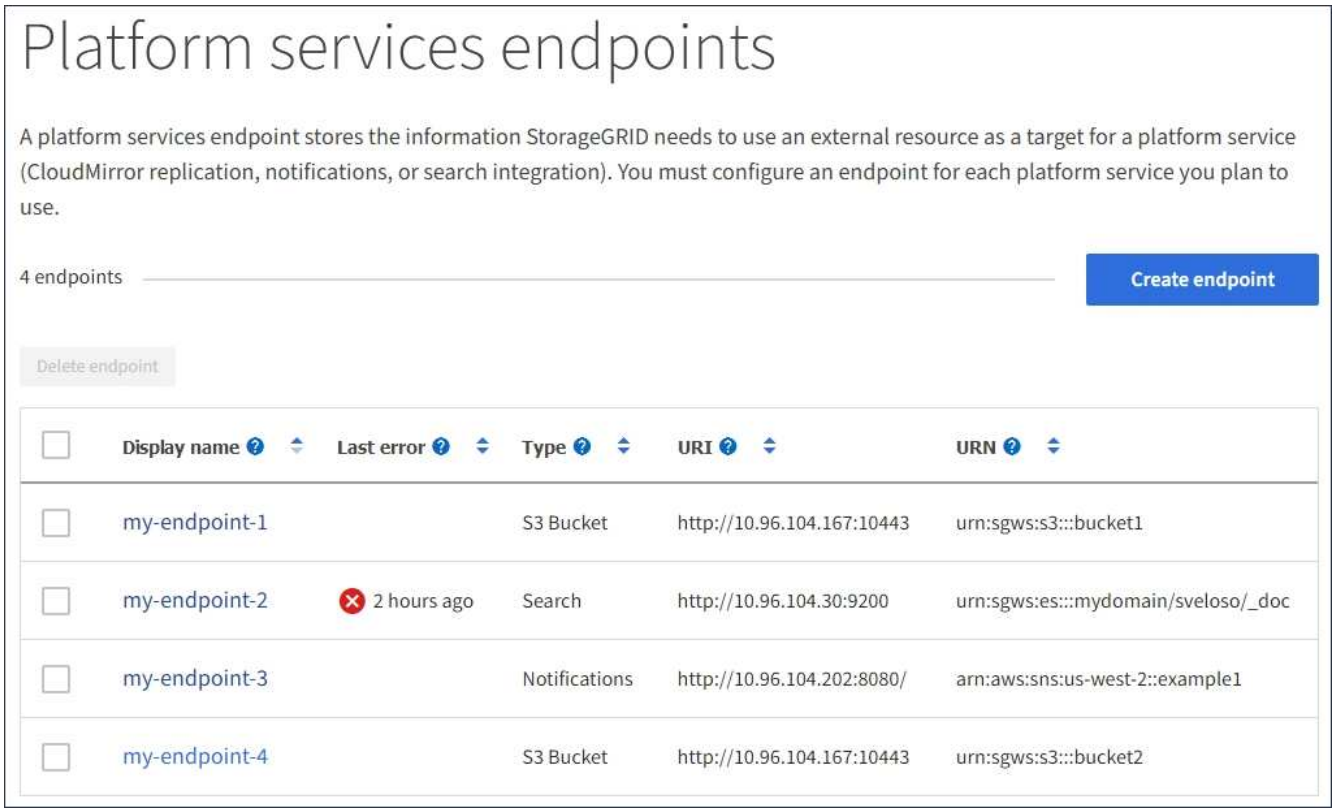
必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Manage Endpoints 権限のあるユーザグループに属している必要があります。

手順

1. ストレージ（ S3 ） * > * プラットフォームサービスのエンドポイント * を選択します。

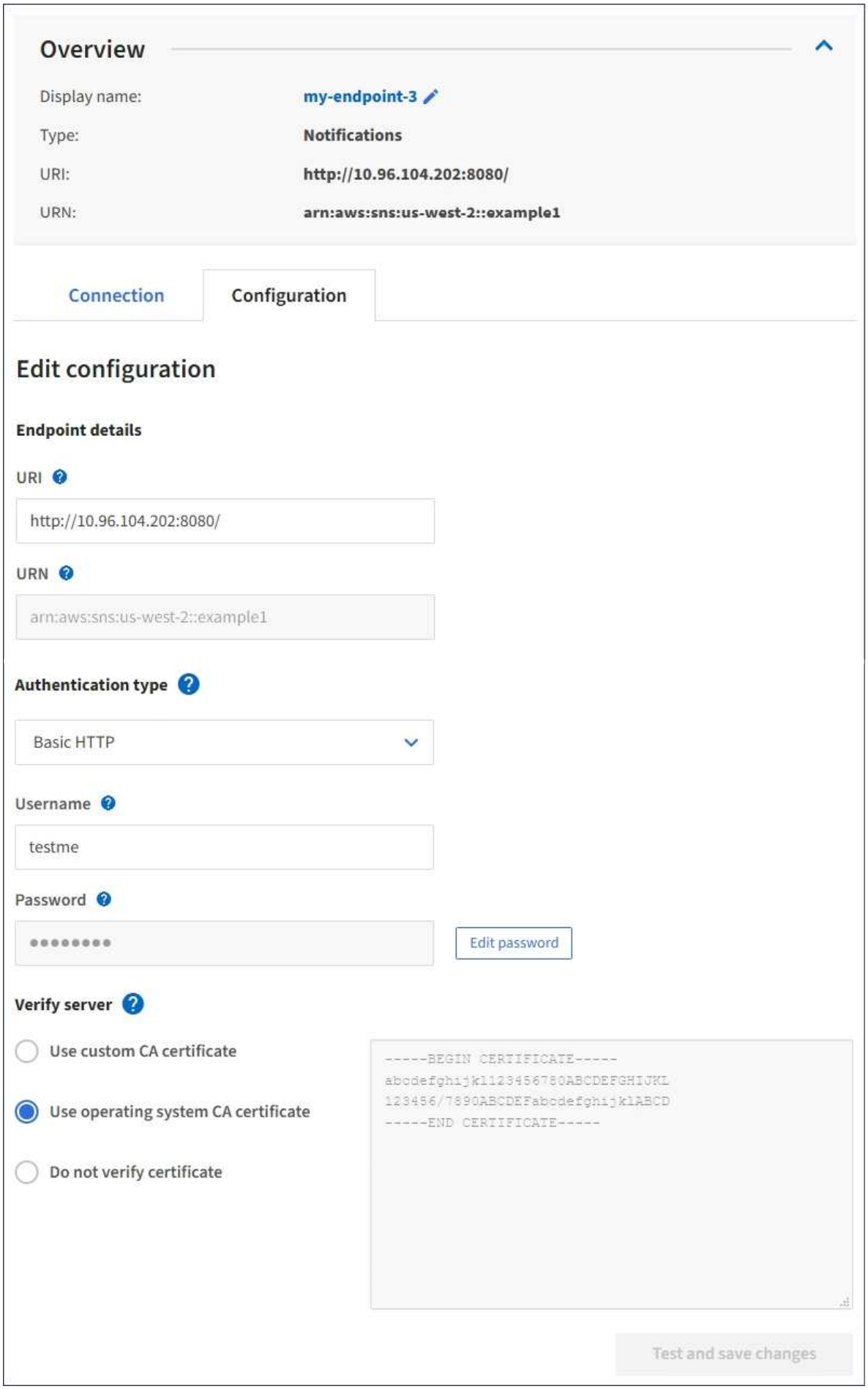
   Platform services Endpoints ページが表示され、設定済みのプラットフォームサービスエンドポイントのリストが表示されます。




2. 編集するエンドポイントを選択します。

   エンドポイントの詳細ページが表示されます。

3. 「 * Configuration * 」を選択します。


Overview
Display name:
my-endpoint-3
Type:
Notifications
URI:
http://10.96.104.202:8080/
URN:
arn:aws:sns:us-west-2::example1
Connection
Configuration
Edit configuration
Endpoint details
URI
http://10.96.104.202:8080/
URN
arn:aws:sns:us-west-2::example1
Authentication type
Basic HTTP
Username
testme
Password
Edit password
Verify server
Use custom CA certificate
Use operating system CA certificate
Do not verify certificate
-----BEGIN CERTIFICATE-----
abcdefghijkl123456780ABCDEFGHIJKL
123456/7890ABCDEFabcdefghijklABCD
-----END CERTIFICATE-----
Test and save changes

4. 必要に応じて、エンドポイントの設定を変更します。

   エンドポイントの作成後に、エンドポイントの URN を変更することはできません。

   a. エンドポイントの表示名を変更するには、編集アイコンを選択します 。
   b. 必要に応じて、 URI を変更します。
   c. 必要に応じて、認証タイプを変更します。
      - Basic HTTP 認証の場合は、必要に応じてユーザ名を変更します。必要に応じてパスワードを変更するには、「 * パスワードを編集」を選択し、新しいパスワードを入力します。変更をキャンセルする必要がある場合は、 * パスワードの編集を元に戻す * を選択します。
      - アクセスキー認証の場合は、必要に応じて「 * S3 キーの編集」を選択し、新しいアクセスキー ID とシークレットアクセスキーを貼り付けることで、キーを変更します。変更をキャンセルする必要がある場合は、 * Revert S3 key edit * を選択します。
   d. 必要に応じて、サーバを検証する方法を変更します。

5. [ 変更のテストと保存 *] を選択します。
   - 指定したクレデンシャルを使用してエンドポイントにアクセスできた場合は、成功を伝えるメッセージが表示されます。エンドポイントへの接続は、各サイトの 1 つのノードから検証されます。
   - エンドポイントの検証が失敗した場合は、エラーメッセージが表示されます。エンドポイントを変更してエラーを修正し、 [ 変更のテストと保存 ] を選択します。

関連情報

"プラットフォームサービスエンドポイントの作成"

プラットフォームサービスエンドポイントを削除しています

# 関連するプラットフォームサービスが不要になった場合は、エンドポイントを削除できます。

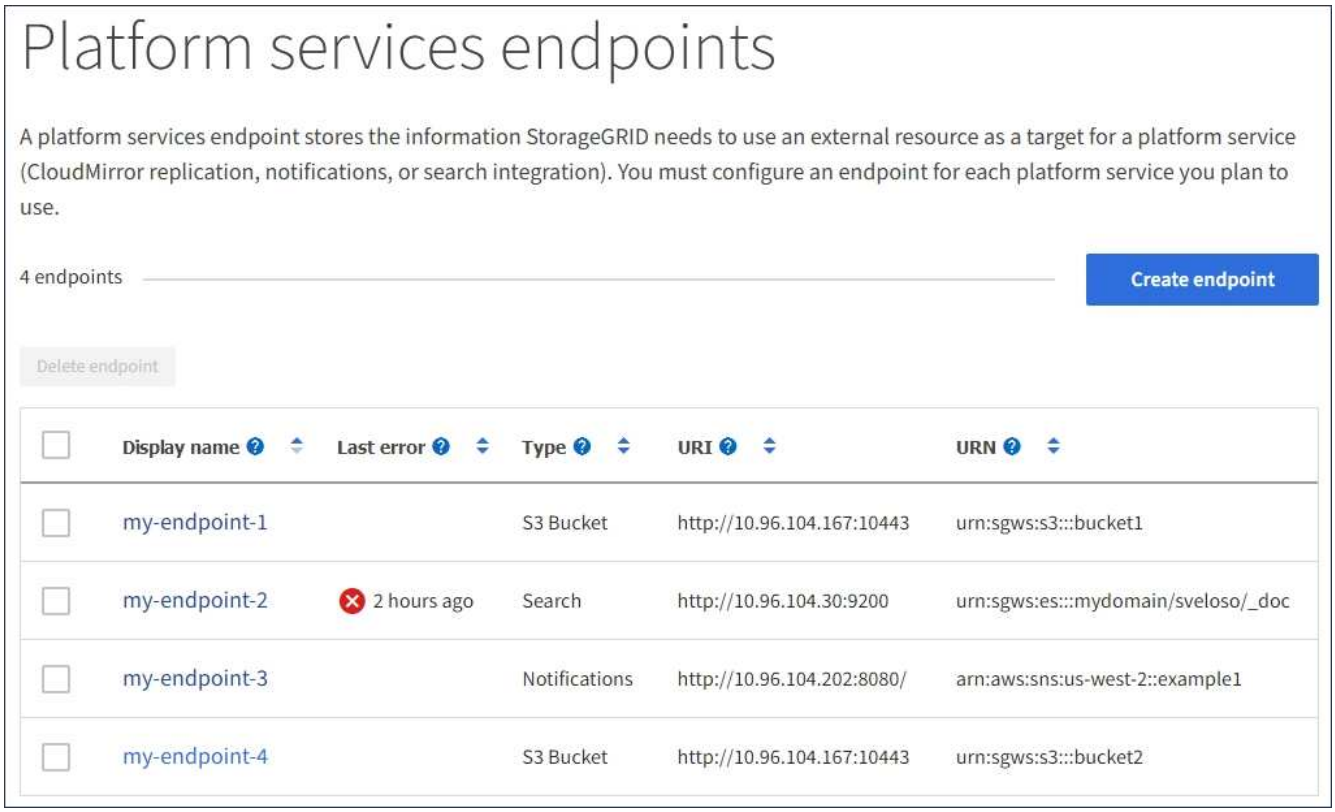
必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Manage Endpoints * 権限のあるユーザグループに属している必要があります。

手順

1. ストレージ（ S3 ） * > * プラットフォームサービスのエンドポイント * を選択します。

   Platform services Endpoints ページが表示され、設定済みのプラットフォームサービスエンドポイントのリストが表示されます。

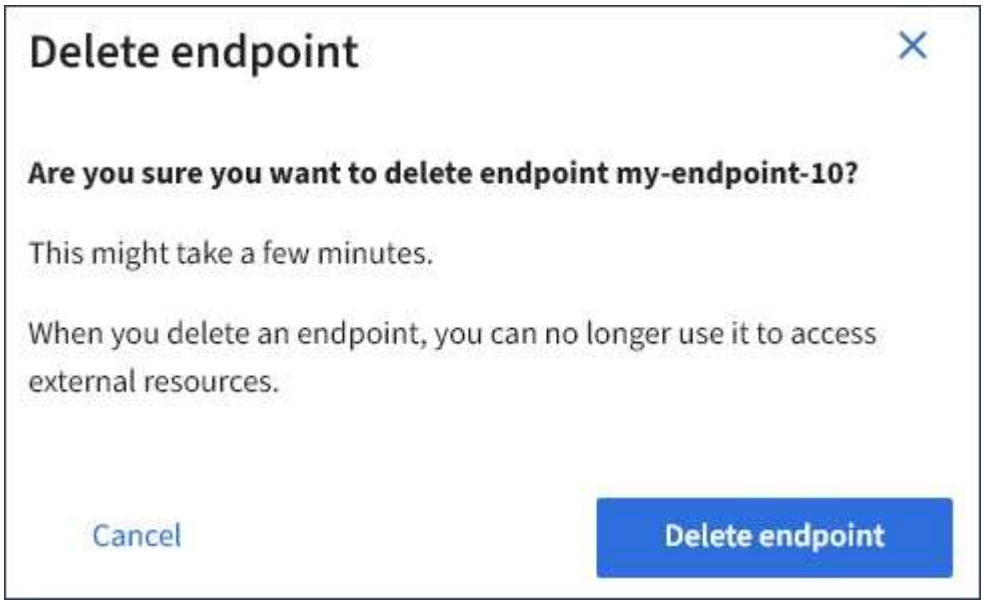



2. 削除する各エンドポイントのチェックボックスを選択します。

> 使用中のプラットフォームサービスエンドポイントを削除すると、エンドポイントを使用するすべてのバケットに対して、関連するプラットフォームサービスが無効になります。完了していない要求はすべて破棄されます。新しい要求は、削除された URN を参照しないようにバケット設定を変更するまで、引き続き生成されます。StorageGRID はこれらの要求を回復不能なエラーとして報告します。

3. [ * アクション * > * エンドポイントの削除 * ] を選択します。

   確認メッセージが表示されます。



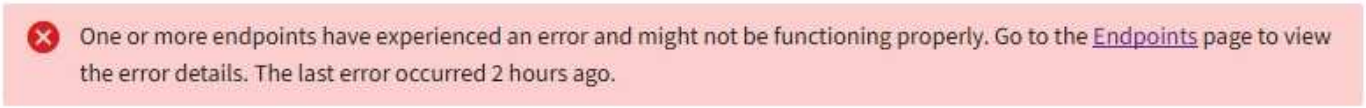
4. [ * エンドポイントの削除 * ] を選択します。

プラットフォームサービスのエンドポイントエラーのトラブルシューティング

StorageGRID がプラットフォームサービスのエンドポイントとの通信を試みたときにエラーが発生した場合は、ダッシュボードにメッセージが表示されます。Platform services Endpoints ページの Last error 列は、エラーが発生してからの時間を示します。エンドポイントのクレデンシャルに関連付けられている権限が正しくない場合は、エラーは表示されません。

エラーが発生したかどうかを確認しています

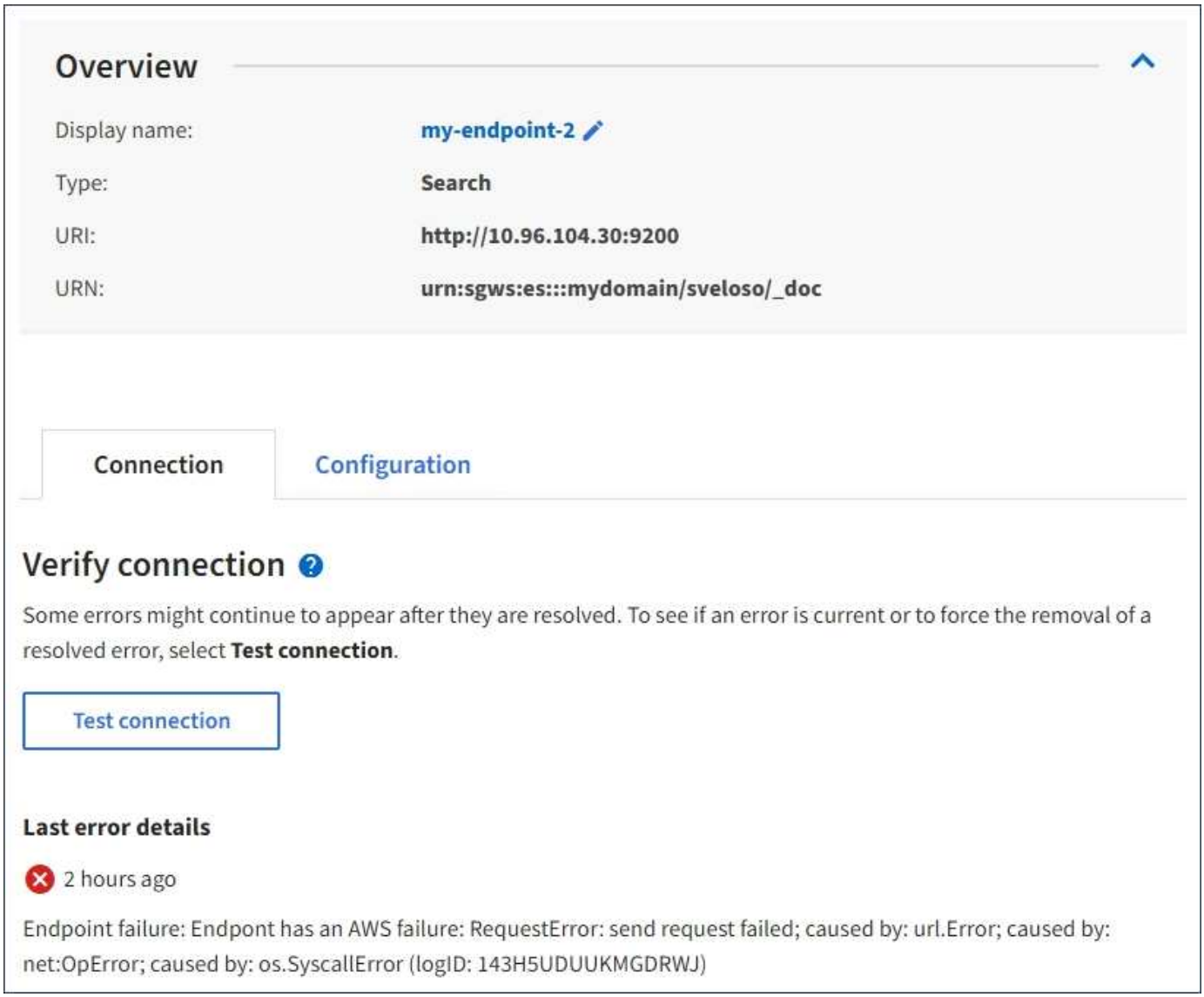
過去 7 日間にプラットフォームサービスエンドポイントでエラーが発生した場合は、 Tenant Manager のダッシュボードにアラートメッセージが表示されます。プラットフォームサービスのエンドポイントページに移動して、エラーの詳細を確認できます。




ダッシュボードに表示されるのと同じエラーは、プラットフォームサービスのエンドポイントページの上部にも表示されます。詳細なエラーメッセージを表示するには、次の手順を実行します

手順

1. エンドポイントのリストで、エラーが発生したエンドポイントを選択します。
2. エンドポイントの詳細ページで、 * 接続 * を選択します。このタブには、エンドポイントの最新のエラーと、エラーが発生してからの経過時間が表示されます。赤の X アイコンを含むエラー 過去 7 日以内に発生しました。




エラーが現在も継続しているかどうかを確認しています

一部のエラーは、解決後も「 * Last error * 」列に引き続き表示される場合があります。エラーが現在発生しているかどうかを確認したり、解決済みのエラーをテーブルから強制的に削除したりするには、次の手順を実行します。

手順

1. エンドポイントを選択します。

   エンドポイントの詳細ページが表示されます。

2. 接続 **>** 接続テスト * を選択します。

[ 接続のテスト * ] を選択すると、 StorageGRID はプラットフォームサービスエンドポイントが存在すること、および現在のクレデンシャルでアクセスできることを検証します。エンドポイントへの接続は、各サイトの 1 つのノードから検証されます。

エンドポイントエラーの解決

エンドポイントの詳細ページの「 * Last error * 」メッセージを使用して、エラーの原因を特定できます。一部のエラーでは、問題 を解決するためにエンドポイントの編集が必要になります。たとえば、 StorageGRID に正しいアクセス権限がないか、アクセスキーが期限切れになっているためにデスティネーションの S3 バケットにアクセスできない場合、 CloudMirror のエラーが発生することがあります。メッセージは ' エンドポイントの資格情報または宛先アクセスを更新する必要があります詳細は 'AccessDenied' または InvalidAccessKeyId' です

エラーを解決するためにエンドポイントを編集する必要がある場合：* Test and save changes *を選択すると、StorageGRID は更新されたエンドポイントを検証し、現在のクレデンシャルでアクセスできることを確認します。エンドポイントへの接続は、各サイトの 1 つのノードから検証されます。

手順

1. エンドポイントを選択します。
2. エンドポイントの詳細ページで、 * 構成 * を選択します。
3. 必要に応じてエンドポイントの設定を編集します。
4. 接続 **>** 接続テスト * を選択します。

必要な権限がないエンドポイントクレデンシャルです

StorageGRID によるプラットフォームサービスエンドポイントの検証では、エンドポイントのクレデンシャルを使用してデスティネーションリソースに接続できること、および基本的な権限チェックを実行できることが確認されます。ただし、 StorageGRID では、特定のプラットフォームサービス処理に必要なすべての権限が検証されるわけではありません。このため、プラットフォームサービスの使用時にエラーが発生した場合（「 403 Forbidden 」など）、エンドポイントのクレデンシャルに関連付けられている権限を確認してください。

その他のプラットフォームサービスのトラブルシューティング

追加情報 プラットフォームサービスのトラブルシューティングについては、 StorageGRID の管理手順を参照してください。

"StorageGRID の管理"

関連情報

"プラットフォームサービスエンドポイントの作成"

"プラットフォームサービスエンドポイントの接続をテストしています"

"プラットフォームサービスエンドポイントの編集"

**CloudMirror**レプリケーションの設定

CloudMirror レプリケーションサービスは、 3 つの StorageGRID プラットフォームサービスのいずれかです。CloudMirror レプリケーションを使用すると、外部の S3 バケットにオブジェクトを自動的にレプリケートできます。

必要なもの

- テナントアカウントのプラットフォームサービスが StorageGRID 管理者によって有効化されている必要

があります。

- レプリケーションのソースとして機能するバケットを作成しておく必要があります。
- CloudMirror レプリケーションのデスティネーションとして使用するエンドポイントを用意しておく必要があります。また、その URN が必要です。
- テナントアカウント内のすべての S3 バケットの設定を管理できるように、 Manage All Buckets 権限または Root Access 権限を持つユーザグループに属している必要があります。これらの権限は、 Tenant Manager を使用してバケットを設定する際にグループポリシーまたはバケットポリシーの権限設定よりも優先されます。

このタスクについて

CloudMirror レプリケーションでは、ソースバケットからエンドポイントで指定されたデスティネーションバケットにオブジェクトがコピーされます。バケットの CloudMirror レプリケーションを有効にするには、有効なバケットレプリケーション設定 XML を作成して適用する必要があります。レプリケーション設定 XML では、各デスティネーションとして S3 バケットエンドポイントの URN を使用する必要があります。

S3 オブジェクトロックが有効なソースバケットまたはデスティネーションバケットでは、レプリケーションはサポートされません。

バケットレプリケーションとその設定方法の一般的な情報については、Amazonのドキュメントのクロスリージョンレプリケーション（CRR）に関する説明を参照してください。StorageGRID がS3バケットのレプリケーション設定APIを実装する方法については、S3クライアントアプリケーションを実装する手順を参照してください。

オブジェクトを含むバケットで CloudMirror レプリケーションを有効にすると、バケットに追加された新しいオブジェクトがレプリケートされますが、バケット内の既存のオブジェクトはレプリケートされません。レプリケーションをトリガーするには、既存のオブジェクトを更新する必要があります。

レプリケーション設定 XML でストレージクラスを指定した場合は、デスティネーション S3 エンドポイントに対して処理を実行する際に StorageGRID でそのクラスが使用されます。指定したストレージクラスは、デスティネーションエンドポイントでもサポートされている必要があります。デスティネーションシステムのベンダーからの推奨事項がある場合は、それに準拠してください。

手順

1. ソースバケットのレプリケーションを有効にします。

   S3 レプリケーション API で指定されているように、レプリケーションを有効にするために必要なレプリケーション設定 XML をテキストエディタで作成します。XML を設定する場合は、次の点に

   - StorageGRID では、 V1 のレプリケーション設定のみがサポートされます。つまり、StorageGRID では、の使用はサポートされていません `Filter` ルールのエレメント。V1の規則に従ってオブジェクトバージョンを削除します。詳細については、レプリケーション設定に関する Amazon のドキュメントを参照してください。
   - デスティネーションとして S3 バケットエンドポイントの URN を使用してください。
   - 必要に応じてを追加します `<StorageClass>` エレメントを選択し、次のいずれかを指定します。
     - `STANDARD`：デフォルトのストレージクラス。オブジェクトをアップロードするときにストレージクラスを指定しない場合は、を参照してください `STANDARD` ストレージクラスが使用されている。
     - `STANDARD_IA`：（標準-アクセス頻度の低いアクセス）このストレージクラスは、アクセス頻度は低いが、必要に応じて高速アクセスが必要なデータに使用します。

- `REDUCED_REDUNDANCY`：重大度が低く、再現可能で、かつ冗長性に劣る状態で保存可能なデータには、このストレージクラスを使用します `STANDARD` ストレージクラス。

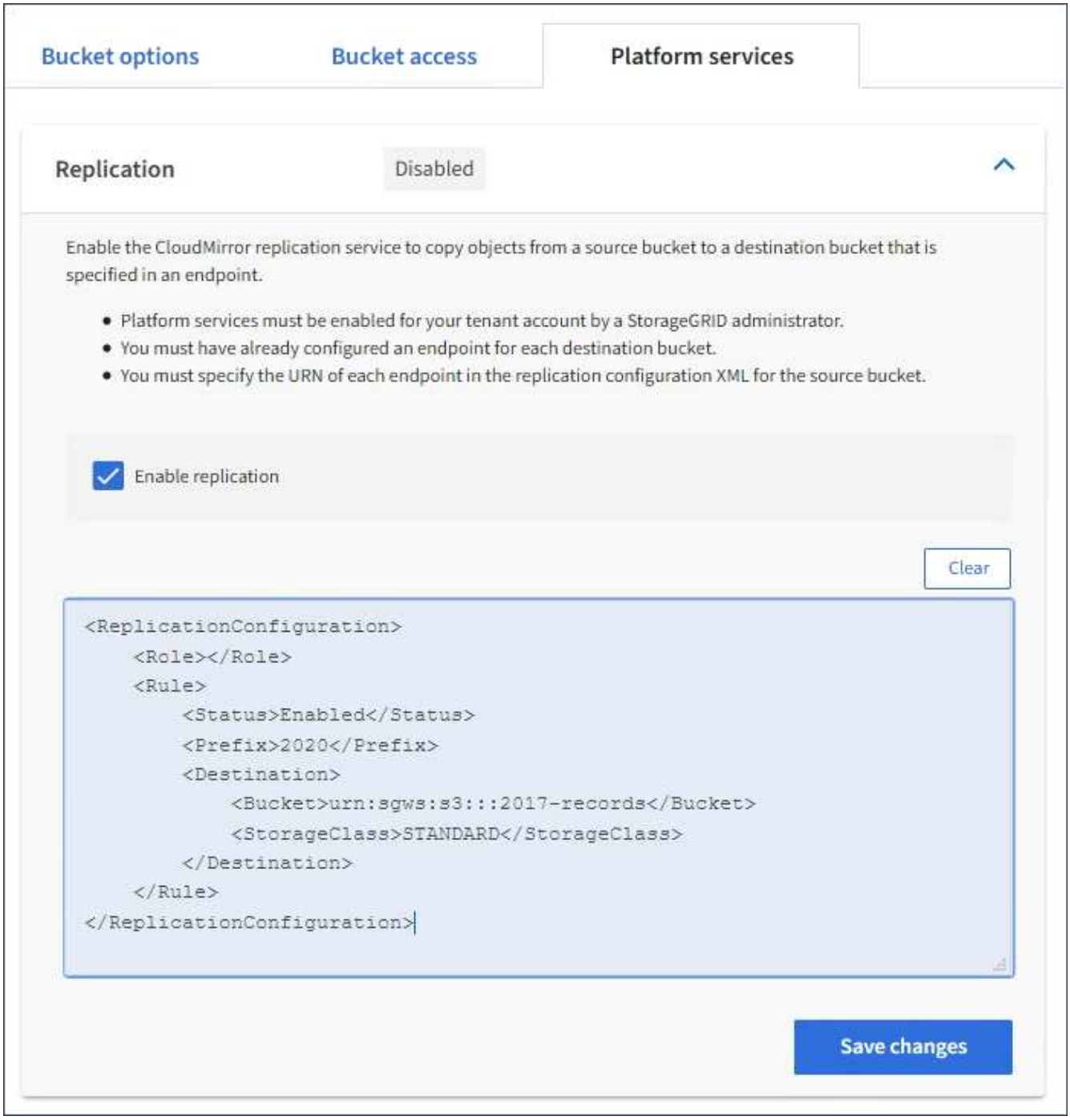
◦ を指定する場合 `Role` 設定XMLでは無視されます。この値は StorageGRID では使用されません。

```
<ReplicationConfiguration>
    <Role></Role>
    <Rule>
        <Status>Enabled</Status>
        <Prefix>2020</Prefix>
        <Destination>
           <Bucket>urn:sgws:s3:::2017-records</Bucket>
           <StorageClass>STANDARD</StorageClass>
         </Destination>
     </Rule>
</ReplicationConfiguration>
```

2. Tenant Manager で、 * Storage （ S3 ） * > * Buckets * を選択します。
3. ソースバケットの名前を選択します。

   バケットの詳細ページが表示されます。

4. プラットフォームサービス * > * レプリケーション * を選択します。
5. [ レプリケーションを有効にする *] チェックボックスをオンにします。
6. レプリケーション設定 XML をテキストボックスに貼り付け、 * 変更を保存 * を選択します。




StorageGRID 管理者がグリッドマネージャまたはグリッド管理 API を使用して各テナントアカウントのプラットフォームサービスを有効にしておく必要があります。設定 XML の保存時にエラーが発生した場合は、 StorageGRID 管理者にお問い合わせください。

7. レプリケーションが正しく設定されていることを確認します。
   a. レプリケーション設定で指定されたレプリケーションの要件を満たすオブジェクトをソースバケットに追加します。

      前述の例では、プレフィックス「 2020 」に一致するオブジェクトがレプリケートされます。

   b. オブジェクトがデスティネーションバケットにレプリケートされたことを確認します。

サイズの小さいオブジェクトについては、レプリケーションの所要時間が短くなります。

関連情報

"CloudMirrorレプリケーションサービスの概要"

"S3 を使用する"

"プラットフォームサービスエンドポイントの作成"

イベント通知を設定する

通知サービスは、 3 つの StorageGRID プラットフォームサービスのうちの 1 つです。バケットの通知を有効にすると、指定したイベントに関する情報を、 AWS Simple Notification Service ™（ SNS ）をサポートするデスティネーションサービスに送信できます。

必要なもの

- テナントアカウントのプラットフォームサービスが StorageGRID 管理者によって有効化されている必要があります。
- 通知のソースとなるバケットを作成しておく必要があります。
- イベント通知のデスティネーションとして使用するエンドポイントが存在し、その URN を把握している必要があります。
- テナントアカウント内のすべての S3 バケットの設定を管理できるように、 Manage All Buckets 権限または Root Access 権限を持つユーザグループに属している必要があります。これらの権限は、 Tenant Manager を使用してバケットを設定する際にグループポリシーまたはバケットポリシーの権限設定よりも優先されます。

このタスクについて

イベント通知を設定すると、ソースバケット内のオブジェクトで指定したイベントが発生するたびに通知が生成され、デスティネーションエンドポイントとして使用される Simple Notification Service （ SNS ）のトピックに送信されます。バケットの通知を有効にするには、有効な通知設定 XML を作成して適用する必要があります。通知設定 XML では、各デスティネーションとしてイベント通知エンドポイントの URN を使用する必要があります。

イベント通知とその設定方法の一般的な情報については、 Amazon のドキュメントを参照してください。StorageGRID が S3 バケットの通知設定 API を実装する方法については、 S3 クライアントアプリケーションを実装する手順を参照してください。

オブジェクトを含むあるバケットのイベント通知を有効にした場合、通知は通知設定の保存後に実行された処理に対してのみ送信されます。

手順

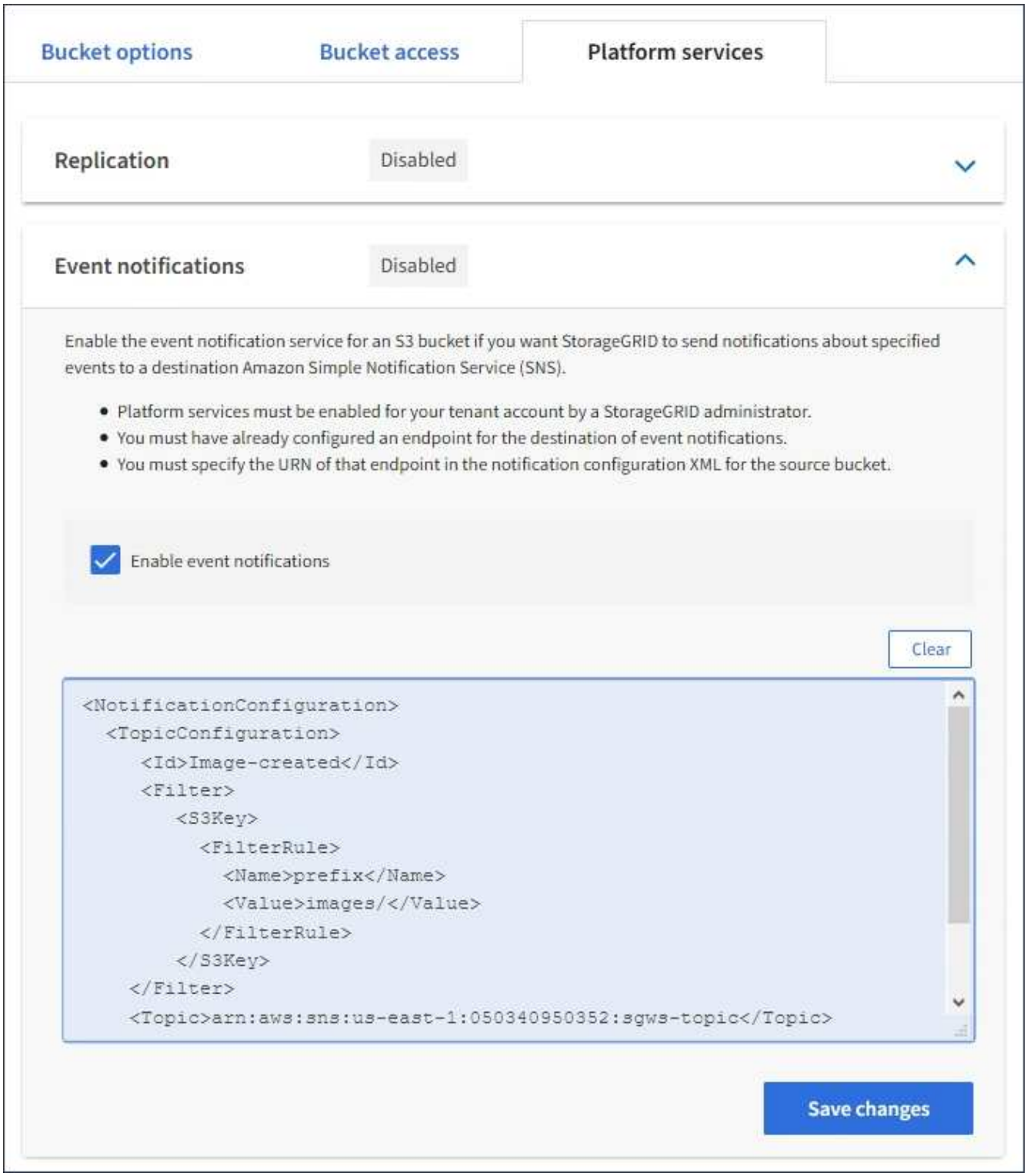
1. ソースバケットの通知を有効にします。
    - イベント通知を有効にするために必要な通知設定 XML を、 S3 通知 API で指定されている内容に従ってテキストエディタで作成します。
    - XML を設定するにあたっては、デスティネーショントピックとしてイベント通知エンドポイントの URN を使用します。

```
<NotificationConfiguration>
  <TopicConfiguration>
     <Id>Image-created</Id>
     <Filter>
        <S3Key>
          <FilterRule>
            <Name>prefix</Name>
            <Value>images/</Value>
          </FilterRule>
        </S3Key>
    </Filter>
    <Topic>arn:aws:sns:us-east-1:050340950352:sgws-topic</Topic>
    <Event>s3:ObjectCreated:*</Event>
   </TopicConfiguration>
 </NotificationConfiguration>
```

2. Tenant Manager で、 * Storage （ S3 ） * > * Buckets * を選択します。
3. ソースバケットの名前を選択します。

   バケットの詳細ページが表示されます。

4. プラットフォームサービス > イベント通知 * を選択します。
5. [ イベント通知を有効にする *] チェックボックスをオンにします。
6. 通知設定 XML をテキストボックスに貼り付け、 * 変更を保存 * を選択します。




StorageGRID 管理者がグリッドマネージャまたはグリッド管理 API を使用して各テナントアカウントのプラットフォームサービスを有効にしておく必要があります。設定 XML の保存時にエラーが発生した場合は、 StorageGRID 管理者にお問い合わせください。

7. イベント通知が正しく設定されていることを確認します。

   a. 設定 XML で設定した通知をトリガーする要件を満たす操作をソースバケット内のオブジェクトに対して実行します。

この例では、を使用してオブジェクトが作成されるたびにイベント通知が送信されます `images/` プレフィックス。

b. デスティネーションの SNS トピックに通知が配信されたことを確認します。

たとえば、デスティネーショントピックが AWS Simple Notification Service （ SNS ）でホストされている場合は、通知が配信されたらユーザに E メールを送信するようにサービスを設定できます。

```
{
   "Records":[
      {
         "eventVersion":"2.0",
         "eventSource":"sgws:s3",
         "eventTime":"2017-08-08T23:52:38Z",
         "eventName":"ObjectCreated:Put",
         "userIdentity":{
            "principalId":"11111111111111111"
         },
         "requestParameters":{
            "sourceIPAddress":"193.51.100.20"
         },
         "responseElements":{
            "x-amz-request-id":"122047343"
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"Image-created",
            "bucket":{
               "name":"test1",
               "ownerIdentity":{
                  "principalId":"11111111111111111"
               },
               "arn":"arn:sgws:s3:::test1"
            },
            "object":{
               "key":"images/cat.jpg",
               "size":0,
               "eTag":"d41d8cd98f00b204e9800998ecf8427e",
               "sequencer":"14D90402421461C7"
            }
         }
      }
   ]
}
```

デスティネーショントピックに通知が届いた場合は、 StorageGRID 通知のソースバケットが正しく設定

されています。

関連情報

"バケットの通知の概要"

"S3 を使用する"

"プラットフォームサービスエンドポイントの作成"

検索統合サービスを使用する

検索統合サービスは、 3 つの StorageGRID プラットフォームサービスのうちの 1 つです。このサービスを有効にすると、オブジェクトが作成、削除されたとき、またはそのメタデータやタグが更新されたときに、デスティネーションの検索インデックスにオブジェクトメタデータを送信できます。

テナントマネージャを使用して検索統合を設定し、カスタム StorageGRID 設定 XML をバケットに適用できます。

検索統合サービスではオブジェクトメタデータがデスティネーションに送信されるため、その設定 XML は _ メタデータ通知設定 xml_ と呼ばれます。この設定 XML は、イベント通知を有効にするための _ 通知設定 xml_ とは異なります。

次のカスタムのStorageGRID S3 REST API処理の詳細については、S3クライアントアプリケーションを実装する手順を参照してください。

- DELETE Bucket metadata notification configuration 要求
- GET Bucket metadata notification configuration 要求
- PUT Bucket metadata notification configuration 要求

関連情報

"検索統合用の XML を設定します"

"メタデータ通知に含まれているオブジェクトメタデータ"

"検索統合サービスで生成される JSON"

"検索統合サービスの設定"

"S3 を使用する"

検索統合用の **XML** を設定します

検索統合サービスは、内に含まれる一連のルールを使用して設定します `<MetadataNotificationConfiguration>` および `</MetadataNotificationConfiguration>` タグ。各ルールは、ルール環境 で指定されたオブジェクト、および StorageGRID からそのオブジェクトのメタデータを送信するデスティネーションを指定します。

オブジェクトはオブジェクト名のプレフィックスでフィルタリングできます。たとえば、というプレフィックスのオブジェクトのメタデータを送信できます `/images` を1つのデスティネーションに、プレフィックスがのオブジェクトのメタデータに追加します `/videos` 別のノードに移動しますプレフィックスが重複している設定は無効で、送信時に拒否されます。たとえば、プレフィックスがのオブジェクトに対するルールを1つ含む設定です `test` プレフィックスが付いたオブジェクトの2番目のルールです `test2` は許可されていません。

デスティネーションは、検索統合サービス用に作成された StorageGRID エンドポイントの URN を使用して指定する必要があります。これらのエンドポイントは、 Elasticsearch クラスタ上に定義されているインデックスとタイプを参照します。

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:region:account-
ID:domain/mydomain/myindex/mytype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

次の表に、メタデータ通知設定 XML の要素を示します。

| 名前 | 説明 | 必須 |
| --- | --- | --- |
| MetadataNotificationConfiguration のページです | メタデータ通知でオブジェクトとデスティネーションの指定に使用されるルール用のコンテナタグ。<br><br>1 つ以上の Rule 要素を含みます。 | はい。 |
| ルール | 指定したインデックスにメタデータを追加する必要があるオブジェクトを特定するルール用のコンテナタグ。<br><br>プレフィックスが重複しているルールは拒否されます。<br><br>MetadataNotificationConfiguration 要素に含まれています。 | はい。 |

| 名前 | 説明 | 必須 |
| --- | --- | --- |
| ID | ルールの一意の識別子。<br><br>Rule 要素に含まれています。 | いいえ |
| ステータス | Status には「 Enabled 」または「 Disabled 」を指定できます。無効になっているルールについては操作が実行されません。<br><br>Rule 要素に含まれています。 | はい。 |
| プレフィックス | プレフィックスと一致するオブジェクトにルールが適用され、そのメタデータが指定したデスティネーションに送信されます。<br><br>すべてのオブジェクトを照合するには、空のプレフィックスを指定します。<br><br>Rule 要素に含まれています。 | はい。 |
| 宛先 | ルールのデスティネーションのコンテナタグ。<br><br>Rule 要素に含まれています。 | はい。 |
| URN | オブジェクトメタデータが送信されるデスティネーションの URN 。次のプロパティを持つ StorageGRID エンドポイントの URN を指定する必要があります。<br><br>• `es` 3番目のエレメントである必要があります。<br>• URNの末尾に、メタデータが格納されるインデックスとタイプを、の形式で指定する必要があります `domain-name/myindex/mytype`。<br><br>エンドポイントは、 Tenant Manager またはテナント管理 API を使用して設定します。形式は次のとおりです。<br><br>• `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype`<br>• `urn:mysite:es:::mydomain/myindex/mytype`<br><br>エンドポイントは設定 XML を送信する前に設定する必要があります。そうしないと、 404 エラーで設定が失敗します。<br><br>Urn は Destination 要素に含まれています。 | はい。 |

サンプルのメタデータ通知設定 XML を使用して、独自の XML を作成する方法を確認できます。

メタデータ通知設定：環境 のすべてのオブジェクトを対象にした設定です

この例では、すべてのオブジェクトのオブジェクトメタデータが同じデスティネーションに送信されます。

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
           <Urn>urn:myes:es:::sgws-notifications/test1/all</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

**2** つのルールを含むメタデータ通知設定

この例では、プレフィックスに一致するオブジェクトのオブジェクトメタデータを指定します `/images` が1つのデスティネーションに送信され、プレフィックスに一致するオブジェクトのオブジェクトメタデータが送信されます `/videos` 2番目の送信先に送信されます。

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Images-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/images</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Videos-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/videos</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

関連情報

"S3 を使用する"

"検索統合サービスで生成される JSON"

"検索統合サービスの設定"

検索統合サービスの設定

# 検索統合サービスでは、オブジェクトが作成、削除、またはそのメタデータ / タグが更新されるたびに、デスティネーションの検索インデックスにオブジェクトメタデータが送信されます。

必要なもの

- テナントアカウントのプラットフォームサービスが StorageGRID 管理者によって有効化されている必要があります。
- コンテンツにインデックスを付ける S3 バケットを作成しておく必要があります。
- 検索統合サービスのデスティネーションとして使用するエンドポイントが存在し、その URN を把握している必要があります。
- テナントアカウント内のすべての S3 バケットの設定を管理できるように、 Manage All Buckets 権限または Root Access 権限を持つユーザグループに属している必要があります。これらの権限は、 Tenant Manager を使用してバケットを設定する際にグループポリシーまたはバケットポリシーの権限設定よりも優先されます。

このタスクについて

ソースバケットに対して検索統合サービスを設定した場合、オブジェクトを作成またはオブジェクトのメタデータ / タグを更新すると、オブジェクトメタデータがデスティネーションエンドポイントに送信されます。オブジェクトをすでに含むバケットで検索統合サービスを有効にすると、既存のオブジェクトに関するメタデータ通知は自動的には送信されません。既存のオブジェクトのメタデータがデスティネーションの検索インデックスに追加されるようにするには、オブジェクトを更新する必要があります。

手順

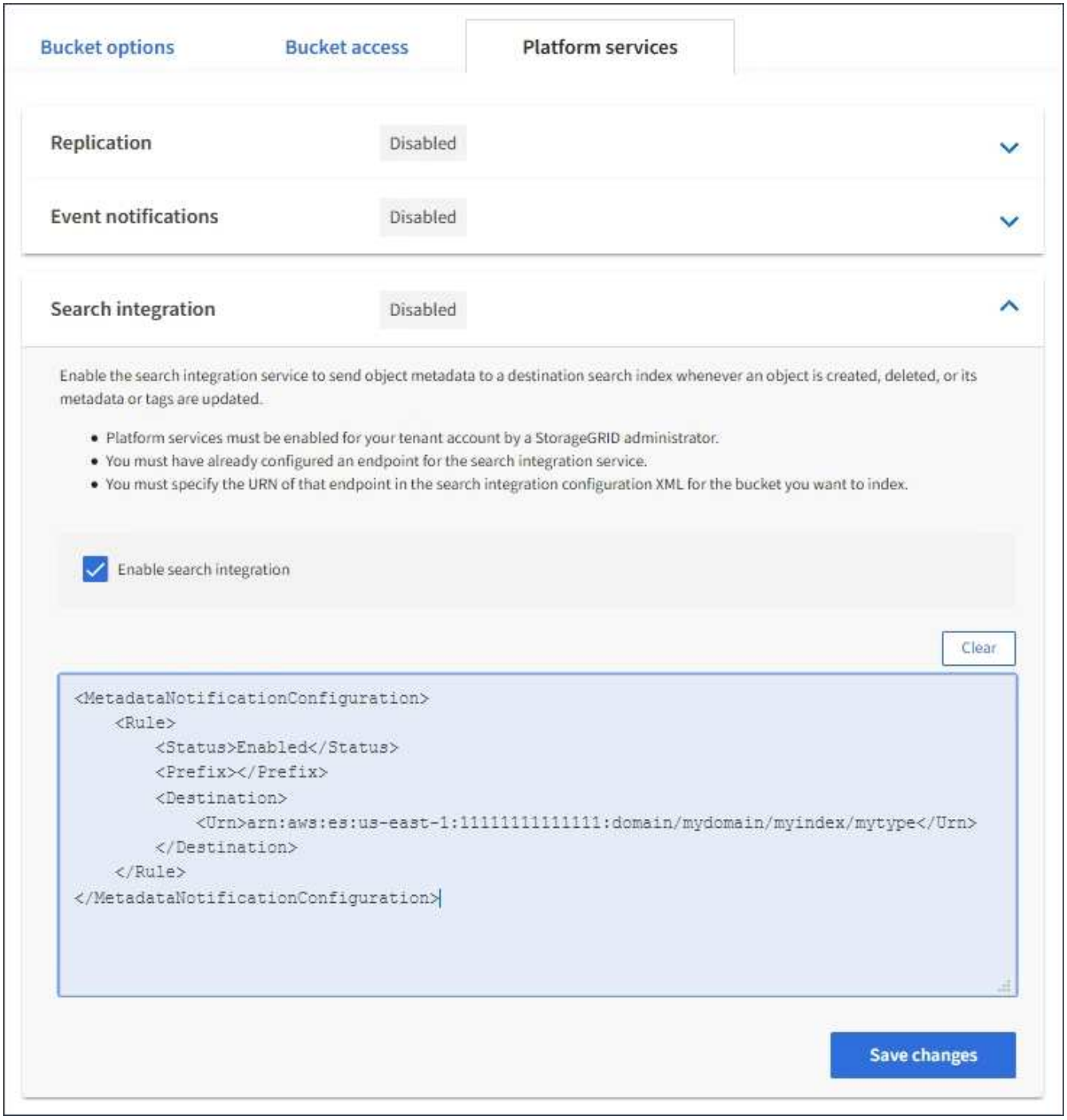
1. 検索統合を有効にするために必要なメタデータ通知 XML をテキストエディタで作成します。
   - 検索統合用の設定 XML に関する情報を参照してください。
   - XML を設定するにあたっては、デスティネーションとして検索統合エンドポイントの URN を使用します。

```
<MetadataNotificationConfiguration>
 <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
       <Urn>arn:aws:es:us-east-
1:11111111111111:domain/mydomain/myindex/mytype</Urn>
       </Destination>
 </Rule>
</MetadataNotificationConfiguration>
```

2. Tenant Manager で、 * Storage （ S3 ） * > * Buckets * を選択します。
3. ソースバケットの名前を選択します。

   バケットの詳細ページが表示されます。

4. プラットフォームサービス > 検索統合 * を選択します
5. 検索統合を有効にする * チェックボックスをオンにします。
6. テキストボックスにメタデータ通知設定を貼り付け、 * 変更を保存 * を選択します。



StorageGRID 管理者がグリッドマネージャまたは管理 API を使用して各テナントアカウントのプラットフォームサービスを有効にしておく必要があります。設定 XML の保存時にエラーが発生した場合は、 StorageGRID 管理者にお問い合わせください。

7. 検索統合サービスが正しく設定されていることを確認します。
   a. 設定 XML で指定されたメタデータ通知をトリガーする要件を満たすオブジェクトをソースバケットに追加します。

      前述の例では、バケットに追加されたすべてのオブジェクトがメタデータ通知をトリガーします。

   b. オブジェクトのメタデータとタグを含む JSON ドキュメントが、エンドポイントで指定された検索インデックスに追加されたことを確認します。

完了後

必要に応じて、次のいずれかの方法でバケットの検索統合を無効にできます。

- Storage （ S3 ） * > * Buckets * を選択し、 * Enable search integration * チェックボックスの選択を解除します。
- S3 API を直接使用している場合は、 DELETE Bucket メタデータ通知要求を使用します。S3 クライアントアプリケーションを実装する手順を参照してください。

関連情報

"検索統合サービスの概要"

"検索統合用の XML を設定します"

"S3 を使用する"

"プラットフォームサービスエンドポイントの作成"

検索統合サービスで生成される **JSON**

バケットで検索統合サービスを有効にすると、オブジェクトのメタデータまたはタグの追加、更新、削除が行われるたびに、 JSON ドキュメントが生成されてデスティネーションエンドポイントに送信されます。

次の例は、キーを含むオブジェクトの場合に生成されるJSONを示しています `SGWS/Tagging.txt` は、という名前のバケットに作成されます `test`。。 `test` バケットはバージョン管理されていないため、を使用します `versionId` タグが空です。

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region":"us-east-1"
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

メタデータ通知に含まれているオブジェクトメタデータ

## 次の表に、検索統合が有効になっている場合にデスティネーションエンドポイントに送信される JSON ドキュメント内のすべてのフィールドを示します。

ドキュメント名には、バケット名、オブジェクト名、バージョン ID （存在する場合）が含まれます。

| を入力します | 項目名と概要 |
| --- | --- |
| バケットとオブジェクトの情報 | `bucket`：バケットの名前 |
| `key`:オブジェクトキー名 | `versionID`：バージョン管理されたバケット内のオブジェクトのオブジェクトバージョン |
| `region`：バケットリージョンなど `us-east-1` | システムメタデータ |
| `size`: HTTPクライアントに表示されるオブジェクトのサイズ(バイト単位) | `md5`:オブジェクトハッシュ |
| ユーザメタデータ | `metadata`：オブジェクトのすべてのユーザメタデータをキーと値のペアとして格納<br><br>`key:value` |

| を入力します | 項目名と概要 |
| --- | --- |
| タグ | `tags`:オブジェクトに定義されているすべてのオブジェクトタグをキーと値のペアとして使用します<br><br>`key:value` |

タグとユーザメタデータの場合、 StorageGRID は文字列または S3 イベント通知として Elasticsearch に日付と番号を渡します。これらの文字列を日付または数値として解釈するように Elasticsearch を設定するには、動的フィールドマッピングおよびマッピング日付形式に関する Elasticsearch の手順に従ってください。検索統合サービスを設定する前に、インデックスの動的フィールドマッピングを有効にする必要があります。ドキュメントにインデックスを付けた後は、インデックス内のドキュメントのフィールドタイプを編集できません。

# S3 を使用する

クライアントアプリケーションでS3 APIを使用して、StorageGRID システムを操作する方法を説明します。

- "S3 REST APIのサポート"
- "テナントアカウントと接続を設定する"
- "StorageGRID でのS3 REST APIの実装"
- "S3 REST API のサポートされる処理と制限事項"
- "StorageGRID の S3 REST API の処理"
- "バケットとグループのアクセスポリシー"
- "REST APIのセキュリティの設定"
- "処理の監視と監査"
- "アクティブ、アイドル、および同時 HTTP 接続のメリット"

## S3 REST APIのサポート

StorageGRID は、 Representational State Transfer （ REST ）の Web サービスのセットとして実装される Simple Storage Service （ S3 ）をサポートします。S3 REST API のサポートにより、 S3 Web サービス用に開発されたサービス指向アプリケーションを、 StorageGRID システムを使用するオンプレミスのオブジェクトストレージと接続できます。クライアントアプリケーションで現在使用している S3 REST API 呼び出しの変更は、最小限しか必要ありません。

- "S3 REST API のサポートに関する変更点"
- "サポートされるバージョン"
- "StorageGRID プラットフォームサービスのサポート"

# StorageGRID システムでの S3 REST API のサポートに関する変更点に注意する必要があります。

| リリース。 | コメント |
| --- | --- |
| 11.5 | • バケットの暗号化の管理のサポートが追加されました。<br>• S3 オブジェクトのロックと廃止された従来の準拠要求のサポートを追加しました。<br>• バージョン管理されたバケットでの DELETE Multiple Objects の使用のサポートが追加されました。<br>• 。 `Content-MD5` 要求ヘッダーが正しくサポートされるようになりました。 |
| 11.4 | • DELETE Bucket tagging 、 GET Bucket tagging 、 PUT Bucket tagging のサポートが追加されました。コスト割り当てタグはサポートされていません。<br>• StorageGRID 11.4 で作成されたバケットでは、オブジェクトキー名がパフォーマンスのベストプラクティスに適合するように制限する必要はなくなりました。<br>• でバケット通知のサポートが追加されました `s3:ObjectRestore:Post` イベントタイプ。<br>• マルチパートの AWS サイズの上限が適用されるようになりました。マルチパートアップロードの各パートのサイズは 5MiB から 5GiB の間にする必要があります。最後の部分は 5MiB より小さくすることができます。<br>• TLS 1.3 のサポートの追加、およびサポートされる TLS 暗号スイートのリストの更新。<br>• CLB サービスは廃止されました。 |

| リリース。 | コメント |
| --- | --- |
| 11.3 | • ユーザ指定のキーによるオブジェクトデータのサーバ側暗号化（ SSE-C ）がサポートされるようになりました。<br>• DELETE Bucket lifecycle、GET Bucket lifecycle、PUT Bucket lifecycleの各処理（Expirationアクションのみ）とがサポートされるようになりました `x-amz-expiration` 応答ヘッダー。<br>• PUT Object 、 PUT Object - Copy 、 Multipart Upload が更新されて、取り込み時に同期配置を使用する ILM ルールの影響を受けるようになりました。<br>• サポートされる TLS 暗号スイートのリストが更新されました。TLS 1.1 暗号はサポートされなくなりました。 |
| 11.2 | クラウドストレージプールで POST Object restore を使用できるようになりました。グループポリシーとバケットポリシーの ARN 、ポリシー条件キー、およびポリシー変数で AWS 構文を使用できるようになりました。StorageGRID 構文を使用する既存のグループポリシーとバケットポリシーは引き続きサポートされます。<br>• 注：カスタム StorageGRID 機能で使用される ARN やその他の構成 JSON / XML での使用に変更はありませんでした。 |
| 11.1 | Cross-Origin Resource Sharing （ CORS ）、グリッドノードへの S3 クライアント接続での HTTP の使用、バケットでの準拠設定がサポートされるようになりました。 |
| 11.0 | バケットでのプラットフォームサービス（ CloudMirror レプリケーション、通知、および Elasticsearch 検索統合）の設定がサポートされるようになりました。また、バケットに対するオブジェクトタグ付け機能の場所の制約、および整合性制御設定「 available 」がサポートされるようになりました。 |
| 10.4. | ILM スキャンのバージョン管理、エンドポイントドメインの名前ページの更新、ポリシーの条件と変数、ポリシーの例、および PutOverwriteObject 権限の変更のサポートが追加されました。 |
| 10.3 | バージョン管理のサポートが追加されました。 |

| リリース。 | コメント |
| --- | --- |
| 10.2 | グループとバケットのアクセスポリシー、およびマルチパートコピー（ Upload Part - Copy ）のサポートが追加されました。 |
| 10.1 | マルチパートアップロード、仮想ホスト形式の要求、および v4 認証のサポートが追加されました。 |
| 10.0 | StorageGRID システムで S3 REST API のサポートが初めて導入されました。現在サポートされているバージョンの _Simple Storage Service API Reference_is 2006-03-01 。 |

サポートされるバージョン

StorageGRID でサポートしている S3 および HTTP のバージョンは次のとおりです。

| 項目 | バージョン |
| --- | --- |
| S3 仕様 | _Simple Storage Service API Reference_2006-03-01 |
| HTTP | 1.1<br><br>HTTP の詳細については、 HTTP/1.1 （ RFC 7230~7235 ）を参照してください。<br><br>• 注： StorageGRID は、 HTTP/1.1 パイプラインをサポートしません。 |

関連情報

"IETF RFC 2616 ：『 Hypertext Transfer Protocol （ HTTP/1.1 ）』"

"Amazon Web Services （ AWS ）ドキュメント：「 Amazon Simple Storage Service API Reference"

**StorageGRID** プラットフォームサービスのサポート

StorageGRID プラットフォームサービスでは、 StorageGRID のテナントアカウントでリモート S3 バケット、 Simple Notification Service （ SNS ）エンドポイント、 Elasticsearch クラスタなどの外部サービスを利用して、グリッドが提供するサービスを拡張できます。

次の表に、使用可能なプラットフォームサービスとその設定に使用する S3 API を示します。

| プラットフォームサービス | 目的 | サービスの設定に使用する **S3 API** |
| --- | --- | --- |
| CloudMirror レプリケーション | ソースの StorageGRID バケットから、設定したリモートの S3 バケットにオブジェクトをレプリケートします。 | PUT Bucket replication |
| 通知 | ソースの StorageGRID バケットでのイベントに関する通知を、設定した Simple Notification Service （ SNS ）エンドポイントに送信します。 | PUT Bucket notification |
| 検索統合 | StorageGRID バケットに格納されているオブジェクトメタデータを、設定した Elasticsearch インデックスに送信します。 | PUT Bucket metadata notification<br>• 注： * これは StorageGRID のカスタム S3 API です。 |

グリッド管理者がテナントアカウントでプラットフォームサービスの使用を有効にするには、事前にプラットフォームサービスを使用できるようにする必要があります。その後、テナント管理者が、テナントアカウントのリモートサービスを表すエンドポイントを作成する必要があります。この手順は、サービスを設定する前に実行する必要があります。

### プラットフォームサービスの使用に関する推奨事項

プラットフォームサービスを使用する前に、次の推奨事項を確認してください。

- CloudMirror のレプリケーション、通知、検索統合を必要とする S3 要求ではアクティブなテナントが 100 個を超えないようにすることを推奨します。アクティブなテナントが 100 を超えると、 S3 クライアントのパフォーマンスが低下する可能性があります。
- StorageGRID システムの S3 バケットで、バージョン管理と CloudMirror レプリケーションの両方が有効になっている場合は、デスティネーションエンドポイントでも S3 バケットのバージョン管理を有効にすることを推奨します。これにより、 CloudMirror レプリケーションでエンドポイントに同様のオブジェクトバージョンを生成できます。
- ソースバケットで S3 オブジェクトのロックが有効になっている場合、 CloudMirror レプリケーションはサポートされません。
- デスティネーションバケットでレガシー準拠が有効になっていると、 CloudMirror レプリケーションは AccessDenied エラーで失敗します。

関連情報

"テナントアカウントを使用する"

"StorageGRID の管理"

"バケットの処理"

"PUT Bucket metadata notification configuration 要求"

# テナントアカウントと接続を設定する

クライアントアプリケーションからの接続を受け入れるように StorageGRID を設定するには、テナントアカウントを 1 つ以上作成し、接続を設定する必要があります。

## S3テナントアカウントを作成および設定する

S3 API クライアントが StorageGRID でオブジェクトの格納や読み出しを行うには、 S3 テナントアカウントが必要です。各テナントアカウントには、専用のアカウント ID 、専用のグループとユーザ、および専用のコンテナとオブジェクトがあります。

S3 テナントアカウントは、 StorageGRID のグリッド管理者がグリッドマネージャまたはグリッド管理 API を使用して作成します。グリッド管理者は、 S3 テナントアカウントを作成する際に次の情報を指定します。

- テナントの表示名（テナントのアカウント ID は自動的に割り当てられ、変更できません）。
- テナントアカウントにプラットフォームサービスの使用を許可するかどうか。プラットフォームサービスの使用が許可されている場合は、グリッドがその使用をサポートするように設定されている必要があります。
- 必要に応じて、テナントアカウントのストレージクォータ — テナントのオブジェクトで使用可能な最大ギガバイト数、テラバイト数、ペタバイト数。テナントのストレージクォータは、物理容量（ディスクのサイズ）ではなく、論理容量（オブジェクトのサイズ）を表します。
- StorageGRID システムでアイデンティティフェデレーションが有効になっている場合は、テナントアカウントを設定するための Root Access 権限が割り当てられているフェデレーテッドグループ。
- StorageGRID システムでシングルサインオン（ SSO ）が使用されていない場合は、テナントアカウントが独自のアイデンティティソースを使用するか、グリッドのアイデンティティソースを共有するか、およびテナントのローカル root ユーザの初期パスワード。

S3 テナントアカウントが作成されたら、テナントユーザは Tenant Manager にアクセスして次のようなタスクを実行できます。

- アイデンティティフェデレーションを設定し（グリッドとアイデンティティソースを共有する場合を除く）、ローカルグループとユーザを作成します
- S3 アクセスキーを管理します
- S3 オブジェクトロックが有効になっているバケットを含む S3 バケットを作成して管理します
- プラットフォームサービスを使用する（有効な場合）
- ストレージの使用状況を監視

> S3 テナントユーザは、 Tenant Manager を使用して S3 バケットを作成および管理できますが、オブジェクトを取り込んで管理するには、 S3 アクセスキーを取得し、 S3 REST API を使用する必要があります。

関連情報

"StorageGRID の管理"

"テナントアカウントを使用する"

クライアント接続の設定方法

グリッド管理者は、 S3 クライアントがデータの格納と読み出しを行うために StorageGRID に接続する方法に関連する設定を行います。接続するために必要な具体的な情報は、選択した設定によって異なります。

クライアントアプリケーションは、次のいずれかに接続することで、オブジェクトを格納または読み出すことができます。

- 管理ノードまたはゲートウェイノード上のロードバランササービス、または必要に応じて、管理ノードまたはゲートウェイノードのハイアベイラビリティ（ HA ）グループの仮想 IP アドレス
- ゲートウェイノード上の CLB サービス、または必要に応じて、ゲートウェイノードのハイアベイラビリティグループの仮想 IP アドレス

> CLB サービスは廃止されました。StorageGRID 11.3 より前に設定されたクライアントは、ゲートウェイノード上の CLB サービスを引き続き使用できます。ロードバランシングに StorageGRID を使用する他のすべてのクライアントアプリケーションは、ロードバランササービスを使用して接続する必要があります。

- 外部ロードバランサを使用するかどうかに関係なく、ストレージノードに追加されます

StorageGRID を設定する場合、グリッド管理者はグリッドマネージャまたはグリッド管理 API を使用して次の手順を実行できます。これらはすべてオプションです。

1. ロードバランササービスのエンドポイントを設定する。

   ロードバランササービスを使用するようにエンドポイントを設定する必要があります。管理ノードまたはゲートウェイノード上のロードバランササービスは、クライアントアプリケーションからの受信ネットワーク接続を複数のストレージノードに分散します。ロードバランサエンドポイントを作成する際、 StorageGRID 管理者は、ポート番号、エンドポイントで HTTP / HTTPS 接続を許可するかどうか、エンドポイントを使用するクライアントのタイプ（ S3 または Swift ）、 HTTPS 接続に使用する証明書（該当する場合）を指定します。

2. 信頼されていないクライアントネットワークを設定する

   StorageGRID 管理者がノードのクライアントネットワークを信頼されていないクライアントネットワークとして設定した場合、ノードはロードバランサエンドポイントとして明示的に設定されたポートでクライアントネットワークのインバウンド接続だけを受け入れます。

3. ハイアベイラビリティグループを設定する。

   管理者が HA グループを作成すると、複数の管理ノードまたはゲートウェイノードのネットワークインターフェイスがアクティブ / バックアップ構成になります。クライアント接続は、 HA グループの仮想 IP アドレスを使用して確立されます。

各オプションの詳細については、 StorageGRID の管理手順を参照してください。

関連情報

"StorageGRID の管理"

**Summary** ：クライアント接続の **IP** アドレスとポート

クライアントアプリケーションは、グリッドノードの IP アドレスおよびそのノード上のサービスのポート番号を使用して StorageGRID に接続します。ハイアベイラビリティ（ HA ）グループが設定されている場合は、 HA グループの仮想 IP アドレスを使用してクライアントアプリケーションを接続できます。

クライアント接続に必要な情報

次の表に、クライアントが StorageGRID に接続できるさまざまな方法、および各接続タイプで使用される IP アドレスとポートを示します。詳細については、 StorageGRID 管理者にお問い合わせください。または、 StorageGRID for a 概要 の管理手順を参照して、グリッドマネージャでこの情報を確認してください。

| 接続が確立される場所 | クライアントが接続するサービス | **IP** アドレス | ポート |
| --- | --- | --- | --- |
| HA グループ | ロードバランサ | HA グループの仮想 IP アドレス | • ロードバランサエンドポイントのポート |
| HA グループ | CLB の機能です<br>• 注： ** CLB サービスは廃止されました。 | HA グループの仮想 IP アドレス | デフォルトの S3 ポート：<br>• HTTPS ： 8082<br>• HTTP ： 8084 |
| 管理ノード | ロードバランサ | 管理ノードの IP アドレス | • ロードバランサエンドポイントのポート |
| ゲートウェイノード | ロードバランサ | ゲートウェイノードの IP アドレス | • ロードバランサエンドポイントのポート |
| ゲートウェイノード | CLB の機能です<br>• 注： ** CLB サービスは廃止されました。 | ゲートウェイノードの IP アドレス<br>• 注： ** CLB および LDR の HTTP ポートはデフォルトでは有効になっていません。 | デフォルトの S3 ポート：<br>• HTTPS ： 8082<br>• HTTP ： 8084 |
| ストレージノード | LDR | ストレージノードの IP アドレス | デフォルトの S3 ポート：<br>• HTTPS ： 18082<br>• HTTP ： 18084 |

例

ゲートウェイノードの HA グループのロードバランサエンドポイントに S3 クライアントを接続するには、次のように構造化された URL を使用します。

- `https://VIP-of-HA-group:_LB-endpoint-port_`

たとえば、 HA グループの仮想 IP アドレスが 192.0.2.5 で S3 ロードバランサエンドポイントのポート番号が 10443 の場合、 S3 クライアントは次の URL を使用して StorageGRID に接続できます。

- `https://192.0.2.5:10443`

クライアントが StorageGRID への接続に使用する IP アドレスに DNS 名を設定できます。ローカルネットワーク管理者にお問い合わせください。

関連情報

"StorageGRID の管理"

#### HTTPS接続とHTTP接続のどちらを使用するかの判断

ロードバランサエンドポイントを使用してクライアント接続を行う場合は、そのエンドポイントに指定されているプロトコル（ HTTP または HTTPS ）を使用して接続を確立する必要があります。ストレージノードへのクライアント接続またはゲートウェイノード上の CLB サービスへのクライアント接続に HTTP を使用する場合は、 HTTP の使用を有効にする必要があります。

デフォルトでは、クライアントアプリケーションがストレージノードまたはゲートウェイノード上の CLB サービスに接続する場合、クライアントアプリケーションはすべての接続に暗号化された HTTPS を使用する必要があります。必要に応じて、 Grid Manager で * Enable HTTP Connection * grid オプションを選択して、セキュアでない HTTP 接続を有効にすることができます。たとえば、非本番環境でストレージノードへの接続をテストする際に、クライアントアプリケーションで HTTP を使用できます。

> 要求が暗号化されずに送信されるため、本番環境のグリッドで HTTP を有効にする場合は注意してください。

> CLB サービスは廃止されました。

[Enable HTTP Connection*] オプションが選択されている場合、クライアントは HTTPS とは異なるポートを HTTP に使用する必要があります。StorageGRID の管理手順を参照してください。

関連情報

"StorageGRID の管理"

"アクティブ、アイドル、および同時 HTTP 接続のメリット"

#### S3 要求のエンドポイントのドメイン名

クライアント要求に S3 ドメイン名を使用できるようにするには、 S3 パス形式と S3 仮想ホスト形式の要求で S3 ドメイン名を使用する接続を受け入れるように StorageGRID 管理者がシステムを設定する必要があります。

このタスクについて

S3 仮想ホスト形式の要求を使用できるようにするには、グリッド管理者が次のタスクを実行する必要があります。

- Grid Manager を使用して、 S3 エンドポイントのドメイン名を StorageGRID システムに追加します。

- クライアントが StorageGRID への HTTPS 接続に使用する証明書が、クライアントが必要とするすべてのドメイン名に対して署名されていることを確認します。

  たとえば、エンドポイントがの場合などです `s3.company.com`、グリッド管理者は、HTTPS接続に使用される証明書にが含まれていることを確認する必要があります `s3.company.com` エンドポイントとエンドポイントのワイルドカードSubject Alternative Name（SAN）： `*.s3.company.com`。

- クライアントが使用する DNS サーバを設定して、必要なワイルドカードレコードを含め、エンドポイントのドメイン名と一致する DNS レコードを含めます。

クライアントがロードバランササービスを使用して接続する場合、グリッド管理者は、クライアントが使用するロードバランサエンドポイントの証明書を設定します。

> 各ロードバランサエンドポイントには独自の証明書があり、異なるエンドポイントドメイン名を認識するように各エンドポイントを設定できます。

クライアントがストレージノードに接続する場合、またはゲートウェイノード上のCLBサービスに接続する場合、グリッド管理者は、グリッドに使用される単一のカスタムサーバ証明書を設定します。

> CLB サービスは廃止されました。

詳細については、 StorageGRID の管理手順を参照してください。

上記の手順が完了したら、仮想ホスト形式の要求（ `bucket.s3.company.com`）。

関連情報

"StorageGRID の管理"

"REST APIのセキュリティの設定"

**S3 REST API**の設定のテスト

Amazon Web Services コマンドラインインターフェイス（ AWS CLI ）を使用してシステムへの接続をテストし、システムに対するオブジェクトの読み取りと書き込みが可能であることを確認できます。

必要なもの

- AWS CLIをからダウンロードしてインストールしておく必要があります "aws.amazon.com/cli"。
- StorageGRID システムでS3テナントアカウントを作成しておく必要があります。

手順

1. Amazon Web Services の設定で、 StorageGRID システムで作成したアカウントを使用するように設定します。
   a. コンフィギュレーションモードを開始します。 `aws configure`
   b. 作成したアカウントの AWS アクセスキー ID を入力します。
   c. 作成したアカウントの AWS シークレットアクセスキーを入力します。
   d. 使用するデフォルトのリージョン（ us-east-1 など）を入力します。
   e. 使用するデフォルトの出力形式を入力するか、 * Enter * キーを押して JSON を選択します。

2. バケットを作成する。

```
aws s3api --endpoint-url https://10.96.101.17:10443
--no-verify-ssl create-bucket --bucket testbucket
```

バケットの作成が完了すると、次の例のようにバケットの場所が返されます。

```
"Location": "/testbucket"
```

3. オブジェクトをアップロードします。

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
put-object --bucket testbucket --key s3.pdf --body C:\s3-
test\upload\s3.pdf
```

オブジェクトのアップロードが完了すると、オブジェクトデータのハッシュである Etag が返されます。

4. バケットの内容をリストして、オブジェクトがアップロードされたことを確認します。

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
list-objects --bucket testbucket
```

5. オブジェクトを削除します。

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-object --bucket testbucket --key s3.pdf
```

6. バケットを削除します。

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-bucket --bucket testbucket
```

## StorageGRID でのS3 REST APIの実装

クライアントアプリケーションは、S3 REST API呼び出しを使用してStorageGRID に接続し、バケットの作成、削除、変更、およびオブジェクトの格納と読み出しを行うことができます。

- "競合するクライアント要求です"
- "整合性制御"
- "StorageGRID の ILM ルールによるオブジェクトの管理"

- "オブジェクトのバージョン管理"
- "S3 REST APIを実装する際の推奨事項"

競合するクライアント要求です

## 同一キーに書き込む2つのクライアントなど'競合するクライアント要求は'最新のWINS形式で解決されます

「latest-wins」評価のタイミングは、S3クライアントが処理を開始するタイミングではなく、StorageGRIDシステムが特定の要求を完了したタイミングに基づいています。

整合性制御

## 整合性制御では、アプリケーションでの必要に応じて、オブジェクトの可用性と、異なるストレージノード間およびサイト間でのオブジェクトの整合性のどちらかを犠牲にしなければなりません。

StorageGRID では、デフォルトで、新しく作成したオブジェクトのリードアフターライト整合性が保証されます。正常に完了した PUT に続く GET では、新しく書き込まれたデータを読み取ることができます。既存のオブジェクトの上書き、メタデータの更新、および削除の整合性レベルは、結果整合性です。上書きは通常、数秒から数分で反映されますが、最大で 15 日かかることがあります。

別の整合性レベルでオブジェクトの処理を実行する場合は、各バケットまたは各 API 処理に対して整合性制御を指定できます。

整合性制御

整合性制御は、 StorageGRID がオブジェクトの追跡に使用するメタデータがノード間に分散される方法、つまりクライアント要求で使用できるオブジェクトの有無に影響します。

バケットまたは API 処理の整合性制御は、次のいずれかの値に設定できます。

| 整合性制御 | 説明 |
| --- | --- |
| すべて | すべてのノードが即座にデータを受け取り、受け取れない場合は要求が失敗します。 |
| strong-global | すべてのサイトのすべてのクライアント要求について、リードアフターライト整合性が保証されます。 |
| strong-site | 1 つのサイト内のすべてのクライアント要求について、リードアフターライト整合性が保証されます。 |

| 整合性制御 | 説明 |
| --- | --- |
| read-after-new-write の場合 | （デフォルト）新規オブジェクトにはリードアフターライト整合性を、オブジェクトの更新には結果整合性を提供します。高可用性が確保され、データ保護が保証されます。Amazon S3の整合性に相当します。<br><br>• 注：存在しないオブジェクトに対してアプリケーションが HEAD 要求を使用すると、使用できないストレージノードがあると「 500 Internal Server Error 」が大量に返される可能性があります。これらのエラーを回避するには、 Amazon S3 と同様の整合性の保証が必要でない限り、整合性制御を「 available 」に設定します。 |
| available （ HEAD 処理は結果整合性） | 「 read-after-new-write 」整合性レベルと動作は同じですが、 HEAD 処理については結果整合性のみを提供します。ストレージ・ノードが使用できない場合 ' リードアフター・新規ライトよりもヘッド操作の可用性が高くなりますAmazon S3 の整合性と異なるのは HEAD 処理のみです。 |

#### 「**read-after-new-write**」および「**available**」整合性制御を使用する

HEAD操作またはGET操作で「read-after-new-write」整合性制御を使用する場合、またはGET操作で「available」整合性制御を使用する場合、StorageGRID は次のように複数の手順で検索を実行します。

- まず、低い整合性レベルを使用してオブジェクトを検索します。
- このルックアップが失敗すると、最も高い整合性レベル「 all 」に到達するまで、次の整合性レベルでルックアップが繰り返されます。このとき、オブジェクトメタデータのすべてのコピーが使用可能になります。

HEAD 操作または GET 操作で「 read-after-new-write 」整合性制御が使用されているが、オブジェクトが存在しない場合、オブジェクトの検索は常に「 all 」整合性レベルに到達します。この整合性レベルでは、オブジェクトのメタデータのすべてのコピーが利用可能である必要があるため、使用できないストレージノードがあると、 500 Internal Server Error が大量に発生する場合があります。

Amazon S3と同様の整合性の保証が必要でない限り、整合性制御を「available」に設定することで、HEAD処理でのこれらのエラーを防ぐことができます。HEAD処理で「available」整合性制御を使用すると、StorageGRID は結果整合性のみを提供します。整合性レベルが「 all 」に達するまで失敗した処理は再試行されないため、オブジェクトメタデータのすべてのコピーが利用可能である必要はありません。

#### **API**処理に対する整合性制御の指定

個々の API 処理に対して整合性制御を設定するには、その処理でサポートされている整合性制御を要求ヘッダーで指定する必要があります。次の例では、 GET Object 処理に対して、整合性制御を「 strong-site 」に設定しています。

```
GET /bucket/object HTTP/1.1
Date: date
Authorization: <em>authorization name</em>
Host: <em>host</em>
Consistency-Control: strong-site
```

PUT Object 処理と GET Object 処理には、同じ整合性制御を使用する必要があります。

バケットの整合性制御の指定

バケットに対して整合性制御を設定するには、 StorageGRID の PUT Bucket 整合性要求および GET Bucket 整合性要求を使用できます。または、 Tenant Manager またはテナント管理 API を使用できます。

バケットの整合性制御を設定する際は、次の点に注意してください。

- バケットの整合性制御を設定することで、バケット内のオブジェクトまたはバケット設定に対して実行される S3 処理に、どの整合性制御を使用するかを指定できます。バケット自体に対する処理には影響しません。
- 個々の API 処理の整合性制御は、バケットの整合性制御よりも優先されます。
- 通常、バケットはデフォルトの整合性制御「 read-after-new-write 」を使用する必要があります。 要求が正しく機能しない場合は、可能であればアプリケーションクライアントの動作を変更します。または、 API 要求ごとに整合性制御を指定するようにクライアントを設定します。バケットレベルの整合性制御は最後の手段と考えてください。

整合性制御と **ILM** ルールの相互作用によるデータ保護への影響

整合性制御と ILM ルールのどちらを選択した場合も、オブジェクトの保護方法に影響します。これらの設定は対話的に操作できます。

たとえば、オブジェクトの格納に使用される整合性制御はオブジェクトメタデータの初期配置に影響し、 ILM ルールで選択される取り込み動作はオブジェクトコピーの初期配置に影響します。StorageGRID では、クライアント要求に対応するためにオブジェクトのメタデータとそのデータの両方にアクセスする必要があるため、整合性レベルと取り込み動作に一致する保護レベルを選択することで、より適切な初期データ保護と予測可能なシステム応答を実現できます。

ILM ルールでは、次の取り込み動作を使用できます。

- * Strict * ： ILM ルールに指定されたすべてのコピーを作成しないと、クライアントに成功が返されません。
- * Balanced * ： StorageGRID は、取り込み時に ILM ルールで指定されたすべてのコピーを作成しようとします。作成できない場合、中間コピーが作成されてクライアントに成功が返されます。可能な場合は、 ILM ルールで指定されたコピーが作成されます。
- * デュアルコミット * ： StorageGRID はオブジェクトの中間コピーをただちに作成し、クライアントに成功を返します。可能な場合は、 ILM ルールで指定されたコピーが作成されます。

ILM ルールの取り込み動作を選択する前に、情報ライフサイクル管理を使用してオブジェクトを管理する手順の設定の完全な概要 を確認してください。

次の ILM ルールと次の整合性レベル設定の 2 サイトグリッドがあるとします。

- * ILM ルール * ：ローカルサイトとリモートサイトに 1 つずつ、 2 つのオブジェクトコピーを作成します。Strict 取り込み動作が選択されています。
- * 整合性レベル *:"Strong-GLOBAL" ( オブジェクトメタデータはすべてのサイトにただちに分散されます )

クライアントがオブジェクトをグリッドに格納すると、 StorageGRID は両方のオブジェクトをコピーし、両方のサイトにメタデータを分散してからクライアントに成功を返します。

オブジェクトは、取り込みが成功したことを示すメッセージが表示された時点で損失から完全に保護されます。たとえば、取り込み直後にローカルサイトが失われた場合、オブジェクトデータとオブジェクトメタデータの両方のコピーがリモートサイトに残っています。オブジェクトを完全に読み出し可能にしている。

代わりに同じILMルールと「strong-site」整合性レベルを使用する場合は、オブジェクトデータがリモートサイトにレプリケートされたあとで、オブジェクトメタデータが分散される前に、クライアントに成功メッセージが送信される可能性があります。この場合、オブジェクトメタデータの保護レベルがオブジェクトデータの保護レベルと一致しません。取り込み直後にローカルサイトが失われると、オブジェクトメタデータが失われます。オブジェクトを読み出すことができません。

整合性レベルと ILM ルールの間の関係は複雑になる可能性があります。サポートが必要な場合は、ネットアップにお問い合わせください。

関連情報

"ILM を使用してオブジェクトを管理する"

"GET Bucket consistency 要求を実行します"

"PUT Bucket consistency 要求"

**StorageGRID** の **ILM** ルールによるオブジェクトの管理

グリッド管理者が情報ライフサイクル管理（ ILM ）ルールを作成して、 S3 REST API クライアントアプリケーションから StorageGRID システムに取り込まれたオブジェクトデータを管理します。これらのルールは、以降のオブジェクトデータを格納する方法と場所を指定するために、 ILM ポリシーに追加されます。

ILM の設定によって、オブジェクトの次の要素が決まります。

- * 地域 *

  StorageGRID システム（ストレージプール）内またはクラウドストレージプール内のオブジェクトのデータの場所。

- * ストレージグレード *

  フラッシュや回転式ディスクなど、オブジェクトデータの格納に使用されるストレージのタイプ。

- * 損失の保護 *

  作成されるコピーの数と作成されるコピーのタイプ（レプリケーション、イレイジャーコーディング、ま

たはその両方）。

- * 保持 *

  オブジェクトのデータの管理方法、格納場所、損失からの保護方法の経過時間に応じて変更が加えられます。

- * 取り込み中の保護 *

  取り込み時にオブジェクトデータを保護する方法。同期配置（取り込み動作に Balanced オプションまたは Strict オプションを使用）または中間コピー作成（ Dual commit オプションを使用）のいずれかです。

ILM ルールではオブジェクトをフィルタして選択できます。S3 を使用して取り込まれたオブジェクトは、ILM ルールによって次のメタデータに基づいてフィルタできます。

- テナントアカウント
- バケット名
- 取り込み時間
- キーを押します
- 最終アクセス時間

> デフォルトでは、すべての S3 バケットで最終アクセス時間の更新が無効になっています。StorageGRID システムに Last Access Time オプションを使用する ILM ルールが含まれている場合は、そのルールで指定される S3 バケットで最終アクセス時間の更新を有効にする必要があります。最終アクセス時間の更新を有効にするには、 Tenant Manager の PUT Bucket last access time 要求、 * S3 * > * Buckets * > * Configure Last Access Time * チェックボックス、またはテナント管理 API を使用します。最終アクセス時間の更新を有効にする場合は、特に小さなオブジェクトを含むシステムで StorageGRID のパフォーマンスが低下する可能性があることに注意してください。

- 場所の制約
- オブジェクトサイズ
- ユーザメタデータ
- オブジェクトタグ

ILM の詳細については、情報ライフサイクル管理を使用してオブジェクトを管理する手順を参照してください。

関連情報

"テナントアカウントを使用する"

"ILM を使用してオブジェクトを管理する"

"PUT Bucket last access time 要求の場合"

オブジェクトのバージョン管理

## バージョン管理の機能を使用してオブジェクトの複数のバージョンを保持することで、

オブジェクトが偶発的に削除される事態に対応したり、以前のバージョンのオブジェクトを読み出してリストアしたりできます。

StorageGRID システムでは、バージョン管理のほとんどの機能をサポートしていますが、いくつかの制限事項があります。StorageGRID では、オブジェクトごとに最大 1 、 000 個のバージョンをサポートしています。

オブジェクトのバージョン管理は、 StorageGRID の情報ライフサイクル管理（ ILM ）または S3 バケットのライフサイクル設定と組み合わせることができます。バケットでバージョン管理機能を有効にするには、各バケットに対して明示的に有効にする必要があります。バケット内の各オブジェクトには、 StorageGRID システムによって生成されるバージョン ID が割り当てられます。

MFA （多要素認証） Delete の使用はサポートされていません。

> バージョン管理は、 StorageGRID バージョン 10.3 以降で作成されたバケットでのみ有効にすることができます。

**ILM** とバージョン管理

ILM ポリシーはオブジェクトの各バージョンに適用されます。ILM のスキャン処理では、すべてのオブジェクトが継続的にスキャンされ、現在の ILM ポリシーに照らして再評価されます。ILM ポリシーに対する変更は、それまでに取り込まれたすべてのオブジェクトに適用されます。バージョン管理が有効になっている場合は、それまでに取り込まれたバージョンも対象にILM のスキャン処理により、過去に取り込まれたオブジェクトに変更後の新しい ILM の内容が適用さ

バージョン管理が有効なバケット内の S3 オブジェクトに対しては、参照時間として noncurrent Time を使用する ILM ルールを作成できます。オブジェクトが更新されると、それまでのバージョンは noncurrent になります。noncurrent の時間フィルタを使用することで、旧バージョンのオブジェクトによるストレージへの影響を軽減するポリシーを作成できます。

> マルチパートアップロード処理を使用してオブジェクトの新しいバージョンをアップロードすると、オブジェクトの元のバージョンの noncurrent の時間には、マルチパートアップロードの完了時ではなく、新しいバージョンのマルチパートアップロードが作成された時点が反映されます。ただし、オリジナルバージョンの最新でない時間は、現行バージョンの時間よりも数時間 ~ 数日早い場合があります。

S3 バージョン管理オブジェクトの ILM ポリシーの例については、情報ライフサイクル管理を使用してオブジェクトを管理する手順を参照してください。

関連情報

"ILM を使用してオブジェクトを管理する"

**S3 REST API**を実装する際の推奨事項

StorageGRID で使用するために S3 REST API を実装する場合は、次の推奨事項を考慮してください。

存在しないオブジェクトに対する **HEAD** の推奨事項

オブジェクトが実際に存在しないと思われるパスにオブジェクトが存在するかどうかをアプリケーションが定期的にチェックする場合は ' 使用可能な整合性制御を使用する必要がありますたとえば ' アプリケーションが

その場所に配置する前にその場所に注意する場合は ' 利用可能な整合性制御を使用する必要があります

そうしないと、使用できないストレージノードがある場合に HEAD 処理でオブジェクトが見つからないと、「 500 Internal Server Error 」が大量に返される可能性があります。

PUT Bucket consistency 要求を使用して各バケットに「 available 」整合性制御を設定するか、または個々の API 処理の要求ヘッダーで整合性制御を指定できます。

#### オブジェクトキーの推奨事項

StorageGRID 11.4 以降で作成されたバケットでは、オブジェクトキー名をパフォーマンスのベストプラクティスに準拠するように制限する必要はなくなりました。たとえば、オブジェクトキー名の最初の 4 文字にランダムな値を使用できるようになりました。

StorageGRID 11.4 より前のリリースで作成されたバケットの場合は、オブジェクトキー名に関する次の推奨事項に進みます。

- オブジェクトキーの最初の 4 文字に、ランダムな値を使用しないでください。これは、 AWS が以前に推奨していたキープレフィックスの推奨事項とは異なります。代わりに、などの一意ではないランダムなプレフィックスを使用してください `image`。
- AWS の以前の推奨事項に従ってキープレフィックスにランダムな一意の文字を使用する場合は、オブジェクトキーの前にディレクトリ名を指定してください。つまり、次の形式を使用します。

  ```
  mybucket/mydir/f8e3-image3132.jpg
  ```

  次の形式は使用しないでください。

  ```
  mybucket/f8e3-image3132.jpg
  ```

#### 「範囲の読み取り」に関する推奨事項

「格納オブジェクトの圧縮」オプション（* Configuration > Grid Options *）を選択した場合、S3クライアントアプリケーションはバイト範囲を指定したGET Object処理を実行しないでください。StorageGRID は要求されたバイトにアクセスするためにオブジェクトを圧縮解除する必要があるため ' これらの “range read” 操作は非効率的です非常に大きなオブジェクトから小さい範囲のバイト数を要求する GET Object 処理は特に効率が悪く、たとえば、 50GB の圧縮オブジェクトから 10MB の範囲を読み取る処理は非常に非効率的です。

圧縮オブジェクトから範囲を読み取ると、クライアント要求がタイムアウトする可能性があります。

> オブジェクトを圧縮する必要があり、クライアントアプリケーションが範囲読み取りを使用する必要がある場合は、アプリケーションの読み取りタイムアウトを増やしてください。

関連情報

"整合性制御"

"PUT Bucket consistency 要求"

"StorageGRID の管理"

# S3 REST API のサポートされる処理と制限事項

StorageGRID システムは Simple Storage Service API （ API バージョン 2006-03-01 ）を実装しており、ほとんどの処理をサポートしていますが、いくつかの制限事項があります。S3 REST API クライアントアプリケーションを統合するときは、実装の詳細を理解しておく必要があります。

StorageGRID システムでは、仮想ホスト形式の要求とパス形式の要求の両方がサポートされます。

- "要求の認証"
- "サービスの処理"
- "バケットの処理"
- "バケットのカスタム処理"
- "オブジェクトの処理"
- "マルチパートアップロードの処理"
- "エラー応答"

## 日付の処理

S3 REST API の StorageGRID 実装では、有効な HTTP の日付形式のみをサポートしています。

StorageGRID システムでは、日付の値を設定できるすべてのヘッダーで、有効な HTTP の日付形式のみがサポートされます。日付の時刻の部分は、 Greenwich Mean Time （ GMT ；グリニッジ標準時）の形式で指定するか、タイムゾーンのオフセットなし（ +0000 を指定）の Universal Coordinated Time （ UTC ；協定世界時）の形式で指定できます。を指定する場合は `x-amz-date` 要求のヘッダー。Date要求ヘッダーで指定された値を上書きします。AWS署名バージョン4を使用している場合は、を参照してください `x-amz-date` 日付ヘッダーがサポートされていないため、署名済み要求にヘッダーが含まれている必要があります。

## 代表的な要求ヘッダー

StorageGRID システムでは、以下の例外を除き、_Simple Storage Service API Reference_で 定義されている共通の要求ヘッダーがサポートされます。

| 要求ヘッダー | 実装 |
| --- | --- |
| 承認 | AWS 署名バージョン 2 は完全にサポートされます<br><br>AWS 署名バージョン 4 は次の例外を除いてサポートされます。<br><br>• 要求の本文の SHA256 の値は計算されません。ユーザが送信した値は、値の場合と同様に、検証なしで受け入れられます `UNSIGNED-PAYLOAD` は用に提供されていた `x-amz-content-sha256` ヘッダー。 |

| 要求ヘッダー | 実装 |
| --- | --- |
| x-amz-security-token を指定します | 実装されていませんを返します `XNotImplemented`。 |

共通の応答ヘッダー

StorageGRID システムでは、以下の例外を除き、 _Simple Storage Service API Reference_で 定義されている共通の応答ヘッダーがすべてサポートされます。

| 応答ヘッダー | 実装 |
| --- | --- |
| x-amz-id-2 | 使用されません |

関連情報

"Amazon Web Services （ AWS ）ドキュメント：「 Amazon Simple Storage Service API Reference"

要求の認証

## StorageGRID システムでは、 S3 API を使用したオブジェクトへのアクセスについて、認証アクセスと匿名アクセスの両方をサポートしています。

S3 API では、 S3 API 要求の認証で署名バージョン 2 と署名バージョン 4 がサポートされます。

認証された要求は、アクセスキー ID とシークレットアクセスキーを使用して署名する必要があります。

StorageGRID システムでは、HTTPという2つの認証方式がサポートされています `Authorization` ヘッダーを使用し、クエリパラメータを使用する。

#### **HTTP Authorization**ヘッダーを使用する

HTTP `Authorization` ヘッダーは、バケットポリシーで許可された匿名の要求を除き、すべてのS3 API処理で使用されます。。 `Authorization` ヘッダーには、要求の認証に必要なすべての署名情報が含まれています。

クエリパラメータを使用する

クエリパラメータを使用すると、 URL に認証情報を追加できます。これは署名付き URL と呼ばれ、特定のリソースへの一時的なアクセスを許可する場合に使用できます。署名付き URL を使用すると、シークレットアクセスキーを知らないユーザでもリソースにアクセスできるため、他のユーザに制限付きアクセスを提供することができます。

サービスの処理

## StorageGRID システムでは、サービスに対して次の処理をサポートしています。

| 操作 | 実装 |
| --- | --- |
| GET Service の略 | Amazon S3 REST API のすべての動作が実装されています。 |
| GET Storage Usage の略 | GET Storage Usage 要求を使用すると、アカウントで使用しているストレージの総容量とアカウントに関連付けられているバケットごとの使用容量を確認できます。これは、パス/とカスタムクエリパラメータを使用したサービスに対する処理です (`?x-ntap-sg-usage`)が追加されました |
| オプション / | クライアントアプリケーションは問題 を実行できます `OPTIONS /` S3認証クレデンシャルを入力せずにストレージノード上のS3ポートに要求し、ストレージノードが使用可能かどうかを確認します。この要求は監視に使用できるほか、外部のロードバランサがストレージノードの停止を特定する目的でも使用できます。 |

関連情報

"GET Storage Usage 要求の略"

バケットの処理

## StorageGRID システムでは、 S3 テナントアカウントあたり最大 1 、 000 個のバケットがサポートされます。

バケット名については、 AWS US Standard リージョンの制限が適用されますが、 S3 仮想ホスト形式の要求をサポートするために DNS の命名規則にも従う必要があります。

"Amazon Web Services （ AWS ）ドキュメント：「 Bucket Restrictions and Limitations"

"S3要求のエンドポイントのドメイン名"

GET Bucket （ List Objects ）処理と GET Bucket versions 処理では、 StorageGRID の整合性制御がサポートされます。

最終アクセス時間の更新が個々のバケットで有効になっているか無効になっているかを確認することができます。

次の表に、 StorageGRID での S3 REST API バケット処理の実装方法を示します。これらの処理を実行するには、アカウントに必要なアクセスクレデンシャルが付与されている必要があります。

| 操作 | 実装 |
| --- | --- |
| バケットを削除します | Amazon S3 REST API のすべての動作が実装されています。 |

| 操作 | 実装 |
| --- | --- |
| バケットの CORS を削除します | この処理は、バケットの CORS 設定を削除します。 |
| バケットの暗号化を削除 | この処理は、バケットからデフォルトの暗号化を削除します。既存の暗号化オブジェクトは暗号化されたままですが、バケットに追加された新しいオブジェクトは暗号化されません。 |
| バケットライフサイクルを削除 | この処理は、バケットからライフサイクル設定を削除します。 |
| バケットポリシーを削除 | この処理は、バケットに関連付けられているポリシーを削除します。 |
| バケットレプリケーションを削除します | この処理は、バケットに関連付けられているレプリケーション設定を削除します。 |
| バケットのタグ付けを削除します | この処理にはを使用します `tagging` サブリソース：バケットからすべてのタグを削除します。 |
| GET Bucket （ List Objects ）、バージョン 1 およびバージョン 2 | この処理は、バケット内のオブジェクトの一部またはすべて（最大 1 、 000 ）を返します。を使用してオブジェクトを取り込んだ場合でも、オブジェクトのストレージクラスには2つの値が設定されます `REDUCED_REDUNDANCY` ストレージクラスのオプション：<br>• `STANDARD`を指定します。このオブジェクトは、ストレージノードで構成されるストレージプールに格納されます。<br>• `GLACIER`を指定します。このオブジェクトは、クラウドストレージプールで指定された外部バケットに移動されています。<br>バケットに同じプレフィックスを持つ削除済みキーが多数含まれている場合、応答に一部のキーが含まれることがあります `CommonPrefixes` キーが含まれていないもの。 |
| GET Bucket ACL の場合 | この処理では、バケットの所有者にバケットに対するフルアクセスがあることを示す応答が返され、所有者の ID 、表示名、および権限が表示されます。 |
| GET Bucket CORS | この処理を実行するとが返されます `cors` バケットの設定。 |

| 操作 | 実装 |
| --- | --- |
| GET Bucket encryption | この処理は、バケットのデフォルトの暗号化設定を返します。 |
| GET Bucket lifecycle | この処理は、バケットのライフサイクル設定を返します。 |
| GET Bucket location の各ノードで使用でき | この操作は、を使用して設定されたリージョンを返します `LocationConstraint` PUT Bucket要求の要素。バケットのリージョンがの場合 `us-east-1`を指定すると、リージョンに対して空の文字列が返されます。 |
| GET Bucket notification | この処理は、バケットに関連付けられている通知設定を返します。 |
| GET Bucket Object versions | バケットに対する読み取りアクセスで、を使用した処理 `versions` サブリソースには、バケット内のオブジェクトのすべてのバージョンのメタデータが表示されます。 |
| GET Bucket policy の場合 | この処理は、バケットに関連付けられているポリシーを返します。 |
| GET Bucket replication | この処理は、バケットに関連付けられているレプリケーション設定を返します。 |
| GET Bucket tagging | この処理にはを使用します `tagging` サブリソース：バケットのすべてのタグを返す |
| GET Bucket versioning | この実装ではを使用します `versioning` サブリソース：バケットのバージョン管理の状態を返します。返されるバージョン管理状態は'バケットがバージョン管理されていないか'バケットがバージョン管理されているか'または一時停止されているかを示します |
| オブジェクトロック設定の取得 | この処理は、バケットでS3オブジェクトのロックが有効になっているかどうかを判断します。 "S3 オブジェクトロックを使用する" |
| HEAD Bucket （ヘッドバケット） | この処理は、バケットが存在し、そのバケットへのアクセス権限があるかどうかを判断します。 |

| 操作 | 実装 |
| --- | --- |
| PUT Bucket の場合 | この処理は、新しいバケットを作成します。バケットを作成すると、そのバケットの所有者になります。<br><br>• バケット名は次のルールを満たす必要があります。<br>◦ StorageGRID システム全体で（テナントアカウント内だけではなく）一意である必要があります。<br>◦ DNS に準拠している必要があります。<br>◦ 3 文字以上 63 文字以下にする必要があります。<br>◦ 1 つ以上のラベルを連続して指定できます。隣接するラベルはピリオドで区切ります。各ラベルの先頭と末尾の文字は小文字のアルファベットか数字にする必要があり、使用できる文字は小文字のアルファベット、数字、ハイフンのみです。<br>◦ テキスト形式の IP アドレスのようにはできません。<br>◦ 仮想ホスト形式の要求でピリオドを使用しないでください。ピリオドを使用すると、サーバワイルドカード証明書の検証で原因 の問題が発生します。<br>• デフォルトでは、バケットはに作成されます `us-east-1` リージョン。ただし、を使用することはできます `LocationConstraint` 別のリージョンを指定するように要求本文内の要求要素。を使用する場合 `LocationConstraint` 要素：Grid Managerまたはグリッド管理APIを使用して定義されているリージョンの正確な名前を指定する必要があります。使用すべきリージョン名がわからない場合は、システム管理者にお問い合わせください。* 注： StorageGRID で定義されていないリージョンを PUT Bucket 要求で使用すると、エラーが発生します。<br>• を含めることができます `x-amz-bucket-object-lock-enabled` S3オブジェクトのロックを有効にしてバケットを作成する要求ヘッダー。<br><br>バケットの作成時に S3 オブジェクトのロックを有効にする必要があります。バケットの作成後に S3 オブジェクトのロックを追加または無効にすることはできません。S3 オブジェクトロックにはバケットのバージョン管理が必要です。バケットの作成時に自動的に有効になります。<br><br>"S3 オブジェクトロックを使用する" |

| 操作 | 実装 |
| --- | --- |
| PUT Bucket CORS | この処理は、バケットの CORS 設定を指定し、クロスオリジン要求を処理できるようにします。Cross-Origin Resource Sharing （ CORS ）は、あるドメインのクライアント Web アプリケーションが別のドメインのリソースにアクセスできるようにするセキュリティ機能です。たとえば、というS3バケットを使用するとします `images` グラフィックを保存します。のCORS設定を指定します `images` バケットを使用すると、そのバケット内の画像をWebサイトに表示できます `http://www.example.com`。 |
| PUT Bucket encryption | この処理は、既存のバケットのデフォルトの暗号化状態を設定します。バケットレベルの暗号化が有効な場合は、バケットに追加されたすべての新しいオブジェクトが暗号化されます。 StorageGRID では、StorageGRID で管理されるキーによるサーバ側の暗号化がサポートされます。サーバ側の暗号化設定ルールを指定する場合は、を設定します `SSEAlgorithm` パラメータの値 `AES256`を使用せずに、を使用してください `KMSMasterKeyID` パラメータ<br><br>バケットのデフォルトの暗号化設定は、オブジェクトのアップロード要求ですでに暗号化が指定されている場合（要求にが含まれている場合）は無視されます `x-amz-server-side-encryption-*` 要求ヘッダー）。 |

| 操作 | 実装 |
| --- | --- |
| PUT Bucket lifecycle の場合 | この処理は、バケットの新しいライフサイクル設定を作成するか、既存のライフサイクル設定を置き換えます。StorageGRID では、 1 つのライフサイクル設定で最大 1 、 000 個のライフサイクルルールがサポートされます。各ルールには、次の XML 要素を含めることができます。<br><br>• 有効期限（日数、日付）<br>• NoncurrentVersionExpiration （ NoncurrentDays ）<br>• フィルタ（プレフィックス、タグ）<br>• ステータス<br>• ID<br><br>StorageGRID では、次のアクションはサポートされません。<br><br>• AbortIncompleteMultipartUpload の略<br>• ExpiredObjectDeleteMarker<br>• 移行<br><br>バケット・ライフサイクルの Expiration アクションと ILM 配置手順の相互作用については ' 情報ライフサイクル管理を使用してオブジェクトを管理する手順のオブジェクトのライフサイクル全体にわたる ILM の動作を参照してください<br><br>• 注：バケットライフサイクル設定は S3 オブジェクトロックが有効なバケットで使用できますが、従来の準拠バケットではバケットライフサイクル設定がサポートされません。 |

| 操作 | 実装 |
| --- | --- |
| PUT Bucket notification | この処理は、要求の本文に含まれる通知設定 XML を使用してバケットの通知を設定します。実装に関する次の詳細事項に注意してください。<br><br>• StorageGRID では、 Simple Notification Service （ SNS ）のトピックがデスティネーションとしてサポートされます。Simple Queue Service （ SQS ）エンドポイントまたは Amazon Lambda エンドポイントはサポートされていません。<br>• 通知のデスティネーションは、 StorageGRID エンドポイントの URN として指定する必要があります。エンドポイントは、 Tenant Manager またはテナント管理 API を使用して作成できます。<br><br>通知設定が機能するためには、エンドポイントが存在している必要があります。エンドポイントが存在しない場合は、 `400 Bad Request` エラーがコードとともに返されます `InvalidArgument`。<br><br>• 次のイベントタイプには通知を設定できません。これらのイベントタイプは * サポートされていません。<br><br>◦ `s3:ReducedRedundancyLostObject`<br><br>◦ `s3:ObjectRestore:Completed`<br><br>• StorageGRID から送信されるイベント通知は標準の JSON 形式を使用しますが、次のように使用されないキーおよび特定の値が使用されるキーがあります。<br>• * eventSource*<br><br>`sgws:s3`<br><br>• * awsRegion *<br><br>含まれません<br><br>• * x-amz-id-2 *<br><br>含まれません<br><br>• * arn *<br><br>`urn:sgws:s3:::bucket_name` |
| PUT Bucket policy の場合 | この処理は、バケットに関連付けられているポリシーを設定します。 |

| 操作 | 実装 |
| --- | --- |
| PUT Bucket replication | この処理では、要求の本文に含まれるレプリケーション設定 XML を使用して、バケットの StorageGRID CloudMirror レプリケーションが設定されます。CloudMirror レプリケーションについては、実装に関する次の詳細事項に注意してください。<br><br>• StorageGRID では、 V1 のレプリケーション設定のみがサポートされます。つまり、StorageGRID では、の使用はサポートされていません `Filter` ルールのエレメント。V1の規則に従ってオブジェクトバージョンを削除します。詳細については、レプリケーション設定に関する Amazon のドキュメントを参照してください。<br>• バケットレプリケーションは、バージョン管理されているバケットでもバージョン管理されていないバケットでも設定でき<br>• レプリケーション設定 XML の各ルールで異なるデスティネーションバケットを指定できます。1 つのソースバケットを複数のデスティネーションバケットにレプリケートできます。<br>• デスティネーションバケットは、テナントマネージャまたはテナント管理 API で指定された StorageGRID エンドポイントの URN として指定する必要があります。<br><br>レプリケーション設定が機能するためには、エンドポイントが存在している必要があります。エンドポイントが存在しない場合は、として要求が失敗します `400 Bad Request`。エラーメッセージ： `Unable to save the replication policy. The specified endpoint URN does not exist: URN`.<br><br>• を指定する必要はありません `Role` 設定XMLを使用します。この値は StorageGRID では使用されず、送信されても無視されます。<br>• 設定XMLでストレージクラスを省略した場合、StorageGRID ではを使用します `STANDARD` デフォルトのストレージクラス。<br>• ソースバケットからオブジェクトを削除する場合、またはソースバケット自体を削除する場合、クロスリージョンレプリケーションは次のように動作します。<br>◦ レプリケートの前にオブジェクトまたはバケットを削除すると、オブジェクトまたはバケットはレプリケートされず、通知は届きません。<br>◦ レプリケートのあとにオブジェクトまたはバケットを削除すると、 StorageGRID は、 V1 のクロスリージョンレプリケーションに対する Amazon S3 の通常の削除動作に従います。 |

| 操作 | 実装 |
| --- | --- |
| PUT Bucket tagging | この処理にはを使用します `tagging` サブリソース：バケットの一連のタグを追加または更新できます。バケットタグを追加する場合は、次の制限事項に注意してください。<br><br>• StorageGRID と Amazon S3 はどちらもバケットごとに最大 50 個のタグをサポートします。<br>• バケットに関連付けられているタグには、一意のタグキーが必要です。タグキーには Unicode 文字を 128 文字まで使用できます。<br>• タグ値には、 Unicode 文字を 256 文字以内で指定します。<br>• キーと値では大文字と小文字が区別されます。 |
| PUT Bucket versioning の場合 | この実装ではを使用します `versioning` サブリソース：既存のバケットのバージョン管理の状態を設定できます。バージョン管理の状態は、次のいずれかの値に設定できます。<br><br>• Enabled ：バケット内のオブジェクトに対してバージョン管理を有効にします。バケットに追加されるすべてのオブジェクトに、一意のバージョン ID が割り当てられます。<br>• Suspended ：バケット内のオブジェクトに対してバージョン管理を無効にします。バケットに追加されるすべてのオブジェクトに、バージョンIDが割り当てられます `null`。 |

関連情報

"Amazon Web Services（AWS）ドキュメント：「Cross-Region Replication"

"整合性制御"

"GET Bucket last access time 要求"

"バケットとグループのアクセスポリシー"

"S3 オブジェクトロックを使用する"

"監査ログで追跡される S3 処理"

"ILM を使用してオブジェクトを管理する"

"テナントアカウントを使用する"

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

このセクションの簡単な例では、 S3 ライフサイクル設定で特定のオブジェクトが特定の S3 バケットから削除（期限切れ）されるタイミングを制御する方法を示します。このセクションの例は、説明のみを目的としています。S3ライフサイクル設定の作成の詳細については、Amazon Simple Storage Service Developer Guide _のオブジェクトライフサイクル管理に関するセクションを参照してください。StorageGRID では、 Expiration アクションのみがサポートされ、移行アクションはサポートされません。

"Amazon Simple Storage Service Developer Guide ： Object lifecycle management"

ライフサイクル構成とは

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

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

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

バケットにライフサイクル設定を適用する場合、バケットのライフサイクル設定は常に StorageGRID の ILM 設定よりも優先されます。StorageGRID は、 ILM ではなくバケットの Expiration 設定を使用して、特定のオブジェクトを削除するか保持するかを決定します。

そのため、 ILM ルールの配置手順がオブジェクトに引き続き適用されていても、オブジェクトがグリッドから削除されることがあります。あるいは、 ILM 配置手順がすべて終了したあとも、オブジェクトがグリッドに保持される場合があります。詳細については'情報ライフサイクル管理を使用してオブジェクトを管理する手順のオブジェクトのライフサイクル全体にわたるILMの動作を参照してください

> バケットライフサイクル設定は S3 オブジェクトロックが有効になっているバケットで使用できますが、従来の準拠バケットではバケットライフサイクル設定がサポートされません。

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

- バケットライフサイクルを削除
- GET Bucket lifecycle
- PUT Bucket lifecycle の場合

ライフサイクル構成を作成します

ライフサイクル設定を作成するための最初の手順として、 1 つ以上のルールを含む JSON ファイルを作成します。たとえば、この JSON ファイルには次の 3 つのルールが含まれています。

1. ルール1は、プレフィックスに一致するオブジェクトにのみ適用されます `category1/`とそれにはがあります `key2` の値 `tag2`。。 `Expiration` パラメータは、フィルタに一致するオブジェクトの有効期限が2020年8月22日の午前0時に切れるように指定します。
2. ルール2は、プレフィックスに一致するオブジェクトにのみ適用されます `category2/`。。 `Expiration` パラメータは、フィルタに一致するオブジェクトの取り込みから100日後に期限切れにするを指定します。

   日数を指定するルールは、オブジェクトが取り込まれた時点を基準とした相対的なルールです。現在の日付が取り込み日と日数を超えている場合は、ライフサイクル設定の適用後すぐに一部のオブジェクトがバケットから削除される可能性があります。

3. ルール3は、プレフィックスに一致するオブジェクトにのみ適用されます `category3/`。。 `Expiration` パラメータは、最新でないバージョンの一致オブジェクトが最新でなくなったあと50日で期限切れになるように指定します。

```
{
    "Rules": [
        {
            "ID": "rule1",
            "Filter": {
                "And": {
                    "Prefix": "category1/",
                    "Tags": [
                        {
                            "Key": "key2",
                            "Value": "tag2"
                        }
                    ]
                }
            },
            "Expiration": {
                "Date": "2020-08-22T00:00:00Z"
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule2",
            "Filter": {
                "Prefix": "category2/"
            },
            "Expiration": {
                "Days": 100
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule3",
            "Filter": {
                "Prefix": "category3/"
            },
            "NoncurrentVersionExpiration": {
                "NoncurrentDays": 50
            },
            "Status": "Enabled"
        }
    ]
}
```

バケットへのライフサイクル設定の適用

ライフサイクル設定ファイルを作成したら、 PUT Bucket lifecycle 要求を発行してバケットに適用します。

次の要求は、サンプルファイル内のライフサイクル設定を、という名前のバケット内のオブジェクトに適用します `testbucket`：バケット

```
aws s3api --endpoint-url <StorageGRID endpoint> put-bucket-lifecycle-
configuration
--bucket testbucket --lifecycle-configuration file://bktjson.json
```

ライフサイクル設定がバケットに正常に適用されたことを検証するために、問題 には GET Bucket lifecycle 要求があります。例：

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-
configuration
 --bucket testbucket
```

成功応答には、適用したライフサイクル設定が表示されます。

バケットライフサイクルの有効期限を検証すると、オブジェクトが環境 に期限切れになります

PUT Object 、 HEAD Object 、または GET Object 要求の発行時に、ライフサイクル設定の有効期限ルールが環境 の特定のオブジェクトかどうかを確認できます。ルールが適用される場合、応答にはが含まれます `Expiration` オブジェクトの有効期限と一致する有効期限を示すパラメータ。

> バケットライフサイクルはILMよりも優先されるため、を参照してください `expiry-date` 表示されているのは、オブジェクトが削除される実際の日付です。詳細については、StorageGRID 管理の実行手順の「オブジェクト保持の決定方法」を参照してください。

たとえば、このPUT Object要求は2020年6月22日に実行され、にオブジェクトが配置されます `testbucket` バケット。

```
aws s3api --endpoint-url <StorageGRID endpoint> put-object
--bucket testbucket --key obj2test2 --body bktjson.json
```

成功の応答は、オブジェクトの有効期限が 100 日（ 2020 年 10 月 1 日）に切れ、ライフサイクル設定のルール 2 に一致したことを示します。

```
{
      *"Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:49 GMT\", rule-
id=\"rule2\"",
      "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
}
```

たとえば、この HEAD Object 要求を使用して、 testbucket バケット内の同じオブジェクトのメタデータを取得しました。

```
aws s3api --endpoint-url <StorageGRID endpoint> head-object
--bucket testbucket --key obj2test2
```

成功の応答にはオブジェクトのメタデータが含まれ、オブジェクトが 100 日で期限切れになり、ルール 2 に一致したことが示されます。

```
{
      "AcceptRanges": "bytes",
      *"Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:48 GMT\", rule-
id=\"rule2\"",
      "LastModified": "2020-06-23T09:07:48+00:00",
      "ContentLength": 921,
      "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
      "ContentType": "binary/octet-stream",
      "Metadata": {}
}
```

関連情報

"バケットの処理"

"ILM を使用してオブジェクトを管理する"

バケットのカスタム処理

## StorageGRID システムでは、 S3 REST API に追加されたシステム固有のカスタムバケット処理をサポートしています。

次の表に、 StorageGRID でサポートされるカスタムバケット処理を示します。

| 操作 | 説明 | を参照してください。 |
| --- | --- | --- |
| GET Bucket consistency | 特定のバケットに適用されている整合性レベルを返します。 | "GET Bucket consistency 要求を実行します" |
| PUT Bucket consistency | 特定のバケットに適用される整合性レベルを設定します。 | "PUT Bucket consistency 要求" |
| GET Bucket last access time の場合 | 特定のバケットで最終アクセス時間の更新が有効になっているか無効になっているかを返します。 | "GET Bucket last access time 要求" |

| 操作 | 説明 | を参照してください。 |
| --- | --- | --- |
| PUT Bucket last access time のように指定します | 特定のバケットの最終アクセス時間の更新を有効または無効にできます。 | "PUT Bucket last access time 要求の場合" |
| バケットのメタデータ通知設定を削除します | 特定のバケットに関連付けられているメタデータ通知設定 XML を削除します。 | "DELETE Bucket metadata notification configuration 要求" |
| GET Bucket metadata notification configuration | 特定のバケットに関連付けられているメタデータ通知設定 XML を返します。 | "GET Bucket metadata notification configuration 要求" |
| PUT Bucket metadata notification configuration のコマンドです | バケットのメタデータ通知サービスを設定します。 | "PUT Bucket metadata notification configuration 要求" |
| 準拠のためのPUT Bucketの変更 | 廃止およびサポート終了：準拠を有効にした新しいバケットを作成できなくなりました。 | "廃止：準拠のための PUT Bucket 要求の変更" |
| GET Bucket compliance で確認します | 廃止されましたがサポートされています：既存の古い準拠バケットに対して現在有効な準拠設定を返します。 | "廃止予定： GET Bucket compliance 要求" |
| PUT Bucket compliance で確認してください | 廃止されましたがサポートされています：既存の古い準拠バケットの準拠設定を変更できます。 | "廃止予定： PUT Bucket compliance 要求" |

関連情報

"監査ログで追跡される S3 処理"

オブジェクトの処理

## このセクションでは、 StorageGRID システムでオブジェクトの S3 REST API 処理を実装する方法について説明します。

- "S3 オブジェクトロックを使用する"
- "サーバ側の暗号化を使用する"
- "オブジェクトの取得"
- "HEAD Object の実行"
- "POST Object restore の実行"
- "PUT Object の場合"
- "PUT Object - Copy の各コマンドを実行します"

すべてのオブジェクトの処理に次の条件が適用されます。

- StorageGRID 整合性制御は、次の点を除いて、オブジェクトに対するすべての処理でサポートされます。
  - GET Object ACL の場合
  - `OPTIONS /`
  - オブジェクトのリーガルホールドを適用します
  - PUT Object retention のことです
- 同一キーに書き込む2つのクライアントなど'競合するクライアント要求は'最新のWINS形式で解決されます「latest-wins」評価のタイミングは、S3クライアントが処理を開始するタイミングではなく、StorageGRID システムが特定の要求を完了したタイミングに基づいています。
- StorageGRID バケット内のオブジェクトは、匿名ユーザまたは別のアカウントが作成したオブジェクトも含めて、すべてバケット所有者によって所有されます。
- Swift を使用して StorageGRID システムに取り込まれたデータオブジェクトに S3 を使用してアクセスすることはできません。

次の表に、 StorageGRID での S3 REST API オブジェクト処理の実装方法を示します。

| 操作 | 実装 |
| --- | --- |
| オブジェクトを削除します | 多要素認証（MFA）と応答ヘッダー `x-amz-mfa` はサポートされていません。<br><br>StorageGRID は、 DELETE Object 要求を処理する際に、オブジェクトのすべてのコピーをすべての格納場所からただちに削除しようとします。成功すると、 StorageGRID はただちにクライアントに応答を返します。30 秒以内にすべてのコピーを削除できなかった場合（格納場所が一時的に使用不能などの理由で）、 StorageGRID は削除対象のコピーをキューに登録し、クライアントに処理が成功したことを通知します。<br><br>• バージョン管理 *<br><br>特定のバージョンを削除するには、バケットの所有者を要求元にしてを使用する必要があります `versionId` サブリソース：このサブリソースを使用すると、バージョンが完全に削除されます。状況に応じて `versionId` 削除マーカー、応答ヘッダーに対応します `x-amz-delete-marker` はに設定されています `true`。<br><br>• を使用せずにオブジェクトが削除された場合 `versionId` バージョンが有効になっているバケットのサブリソースが表示されると、削除マーカーが生成されます。。 `versionId` 削除マーカーの場合は、を使用して戻ります `x-amz-version-id` 応答ヘッダー、および `x-amz-delete-marker` 応答ヘッダーがに設定されて返されます `true`。<br>• を使用せずにオブジェクトが削除された場合 `versionId` バージョンが一時停止中のバケットについて、既存の「null」バージョンまたは「null」削除マーカーが完全に削除され、新しい「null」削除マーカーが生成されます。。 `x-amz-delete-marker` 応答ヘッダーがに設定されて返されます `true`。<br>• 注 * ：特定の場合、 1 つのオブジェクトに複数の削除マーカーが存在することがあります。 |
| 複数のオブジェクトを削除します | 多要素認証（MFA）と応答ヘッダー `x-amz-mfa` はサポートされていません。<br><br>同じ要求メッセージで複数のオブジェクトを削除できます。 |

| 操作 | 実装 |
| --- | --- |
| オブジェクトのタグ付けを削除します | を使用します `tagging` サブリソース：オブジェクトからすべてのタグを削除します。Amazon S3 REST API のすべての動作が実装されています。<br><br>• バージョン管理 *<br><br>状況に応じて `versionId` クエリパラメータが要求で指定されていない場合、バージョン管理されたバケット内のオブジェクトの最新バージョンからすべてのタグが削除されます。オブジェクトの現在のバージョンが削除マーカーの場合は、"MethodNotAllowed`"ステータスがとともに返されます `x-amz-delete-marker` 応答ヘッダーをに設定しました `true`。 |
| オブジェクトの取得 | "オブジェクトの取得" |
| GET Object ACL の場合 | アカウントに必要なアクセスクレデンシャルがある場合、オブジェクトの所有者にオブジェクトに対するフルアクセスがあることを示す応答が返され、所有者の ID 、表示名、および権限が表示されます。 |
| オブジェクトのリーガルホールドを取得します | "S3 オブジェクトロックを使用する" |
| GET Object retention のことです | "S3 オブジェクトロックを使用する" |
| GET Object tagging | を使用します `tagging` サブリソース：オブジェクトのすべてのタグを返すために使用します。Amazon S3 REST API のすべての動作が実装されています<br><br>• バージョン管理 *<br><br>状況に応じて `versionId` クエリパラメータが要求で指定されていない場合、バージョン管理されたバケット内のオブジェクトの最新バージョンからすべてのタグが返されます。オブジェクトの現在のバージョンが削除マーカーの場合は、"MethodNotAllowed`"ステータスがとともに返されます `x-amz-delete-marker` 応答ヘッダーをに設定しました `true`。 |
| HEAD Object の実行 | "HEAD Object の実行" |
| POST Object restore の実行 | "POST Object restore の実行" |
| PUT Object の場合 | "PUT Object の場合" |

| 操作 | 実装 |
| --- | --- |
| PUT Object - Copy の各コマンドを実行します | "PUT Object - Copy の各コマンドを実行します" |
| オブジェクトのリーガルホールドを適用します | "S3 オブジェクトロックを使用する" |
| PUT Object retention のことです | "S3 オブジェクトロックを使用する" |
| PUT Object tagging | を使用します `tagging` サブリソース：既存のオブジェクトに一連のタグを追加します。Amazon S3 REST API のすべての動作が実装されています<br><br>• タグの更新と取り込み動作 *<br><br>PUT Object tagging を使用してオブジェクトのタグを更新した場合、 StorageGRID はオブジェクトを再取り込みしません。これは、一致する ILM ルールで指定されている取り込み動作が使用されないことを意味します。更新によって発生したオブジェクト配置の変更は、通常のバックグラウンド ILM プロセスで ILM が再評価されるときに実施されます。<br><br>このため、 ILM ルールの取り込み動作に Strict オプションが指定されている場合、必要なオブジェクト配置を実行できないと（たとえば、新たに必要となった場所を使用できない場合）、アクションは実行されません。更新されたオブジェクトは、必要な配置を実行可能になるまで現在の配置が維持されます。<br><br>• 衝突の解決 *<br><br>同一キーに書き込む2つのクライアントなど'競合するクライアント要求は'最新のWINS形式で解決されます「latest-wins」評価のタイミングは、S3クライアントが処理を開始するタイミングではなく、StorageGRID システムが特定の要求を完了したタイミングに基づいています。<br><br>• バージョン管理 *<br><br>状況に応じて `versionId` クエリパラメータが要求で指定されていません。処理は、バージョン管理されたバケット内のオブジェクトの最新バージョンにタグを追加します。オブジェクトの現在のバージョンが削除マーカーの場合は、"MethodNotAllowed`"ステータスがとともに返されます `x-amz-delete-marker` 応答ヘッダーをに設定しました `true`。 |

関連情報

"整合性制御"

"監査ログで追跡される S3 処理"

**S3** オブジェクトロックを使用する

# StorageGRID システムでグローバルな S3 オブジェクトのロック設定が有効になっている場合は、 S3 オブジェクトのロックを有効にしたバケットを作成し、そのバケットに追加するオブジェクトのバージョンごとに retain-until date および legal hold 設定を指定できます。

S3 オブジェクトロックでは、オブジェクトレベルの設定を指定して、一定期間または無期限にオブジェクトが削除または上書きされないようにすることができます。

StorageGRID S3 オブジェクトロック機能は、 Amazon S3 準拠モードと同等の単一の保持モードを提供します。デフォルトでは、保護されたオブジェクトバージョンは、どのユーザーでも上書きまたは削除できません。StorageGRID S3 オブジェクトのロック機能では、ガバナンスモードはサポートされず、特別な権限を持つユーザは保持設定を省略したり保護されたオブジェクトを削除したりすることはできません。

## バケットで**S3**オブジェクトのロックを有効にする

StorageGRID システムでグローバルな S3 オブジェクトのロック設定が有効になっている場合は、各バケットの作成時に S3 オブジェクトのロックを必要に応じて有効にすることができます。次のいずれかの方法を使用できます。

- Tenant Manager を使用してバケットを作成します。

  "テナントアカウントを使用する"

- を指定したPUT Bucket要求を使用してバケットを作成します `x-amz-bucket-object-lock_enabled` 要求ヘッダー。

  "バケットの処理"

バケットの作成後に S3 オブジェクトのロックを追加または無効にすることはできません。S3 オブジェクトロックにはバケットのバージョン管理が必要です。バケットの作成時に自動的に有効になります。

S3 オブジェクトのロックが有効になっているバケットには、 S3 オブジェクトのロック設定があるオブジェクトとなっていないオブジェクトを組み合わせて含めることができます。StorageGRID では、S3オブジェクトロックバケット内のオブジェクトのデフォルトの保持はサポートされないため、PUT Object Lock Configurationバケットの処理はサポートされません。

## バケットで**S3**オブジェクトのロックが有効になっているかどうかを確認しています

S3オブジェクトロックが有効になっているかどうかを確認するには、GET Object Lock Configuration要求を使用します。

"バケットの処理"

## **S3**オブジェクトのロック設定を使用してオブジェクトを作成する

S3 オブジェクトロックが有効に問題 なっているバケットにオブジェクトのバージョンを追加するときに S3 オブジェクトのロック設定を指定するには、 PUT Object 、 PUT Object - Copy 、 Initiate Multipart Upload 要

求のいずれかを実行します。次の要求ヘッダーを使用します。

> バケットの作成時に S3 オブジェクトのロックを有効にする必要があります。バケットの作成後に S3 オブジェクトのロックを追加または無効にすることはできません。

- `x-amz-object-lock-mode`は、コンプライアンスに準拠している必要があります（大文字と小文字が区別されます

  > を指定する場合 `x-amz-object-lock-mode`、も指定する必要があります `x-amz-object-lock-retain-until-date`。

- `x-amz-object-lock-retain-until-date`
  - retain-une-dateの値は、の形式で指定する必要があります `2020-08-10T21:46:00Z`。秒数には分数を指定できますが、保持される 10 進数は 3 桁（ミリ秒単位）だけです。それ以外の ISO 8601 形式はサポートされません。
  - retain-une-date は将来の日付にする必要があります。
- `x-amz-object-lock-legal-hold`

  リーガルホールドがオン（大文字と小文字が区別される）の場合、オブジェクトはリーガルホールドの対象になります。リーガルホールドがオフの場合、リーガルホールドは適用されません。それ以外の値を指定すると、 400 Bad Request （ InvalidArgument ）エラーが発生します。

次のいずれかの要求ヘッダーを使用する場合は、次の制限事項に注意してください。

- 。 `Content-MD5` 要求ヘッダーがある場合は必須です `x-amz-object-lock-*` 要求ヘッダーがPUT Object要求に含まれています。 `Content-MD5` PUT Object - CopyまたはInitiate Multipart Uploadには必要ありません。
- バケットでS3オブジェクトロックが有効になっていない場合は、とをクリックします `x-amz-object-lock-*` 要求ヘッダーが存在し、400 Bad Request（InvalidRequest）エラーが返されます。
- PUT Object要求では、の使用がサポートされます `x-amz-storage-class: REDUCED_REDUNDANCY` AWSの動作に合わせて調整できます。ただし、 S3 オブジェクトのロックが有効になっているバケットにオブジェクトが取り込まれると、 StorageGRID は常にデュアルコミットの取り込みを実行します。
- 後続のGETまたはHEAD Objectバージョンの応答では、ヘッダーが含まれます `x-amz-object-lock-mode`、 `x-amz-object-lock-retain-until-date`および `x-amz-object-lock-legal-hold` が設定されている場合、および要求の送信者が正しいかどうか `s3:Get*` 権限：
- それ以降の DELETE Object version 要求または DELETE Objects versions 要求は、 retain-until 日の前であるか、リーガルホールドがオンの場合には失敗します。

**S3**オブジェクトのロック設定を更新しています

既存のオブジェクトのバージョンのリーガルホールドや保持の設定を更新する必要がある場合、次のオブジェクトサブリソース処理を実行できます。

- `PUT Object legal-hold`

  新しいリーガルホールドの値が on の場合、オブジェクトはリーガルホールドの対象になります。リーガルホールドの値がオフの場合、リーガルホールドは解除されます。

- `PUT Object retention`
  - モード値は準拠している必要があります（大文字と小文字が区別されます）。
  - retain-une-dateの値は、の形式で指定する必要があります `2020-08-10T21:46:00Z`。秒数には分数を指定できますが、保持される 10 進数は 3 桁（ミリ秒単位）だけです。それ以外の ISO 8601 形式はサポートされません。
  - オブジェクトバージョンに既存の retain-until がある場合は、オブジェクトバージョンを増やすことはできますが、増やすことはできません。新しい値は将来の必要があります。

関連情報

"ILM を使用してオブジェクトを管理する"

"テナントアカウントを使用する"

"PUT Object の場合"

"PUT Object - Copy の各コマンドを実行します"

"マルチパートアップロードを開始します"

"オブジェクトのバージョン管理"

"Amazon Simple Storage Service User Guide ： Using S3 Object Lock"

サーバ側の暗号化を使用

## サーバ側の暗号化を使用して、保存中のオブジェクトデータを保護できます。StorageGRID は、オブジェクトを書き込む際にデータを暗号化し、ユーザがオブジェクトにアクセスする際にデータを復号化します。

サーバ側の暗号化を使用する場合は、暗号化キーの管理方法に基づいて、次の 2 つのオプションを同時に選択できます。

- * SSE （ StorageGRID で管理されるキーによるサーバ側の暗号化） * ：オブジェクトを格納する S3 要求を問題 で暗号化すると、 StorageGRID は一意のキーでオブジェクトを暗号化します。オブジェクトを読み出す S3 要求を問題 で実行すると、 StorageGRID は格納されているキーを使用してオブジェクトを復号化します。
- * SSE-C （ユーザ指定のキーによるサーバ側の暗号化） * ：オブジェクトを格納する S3 要求を問題 で処理するときに、独自の暗号化キーを指定します。オブジェクトを読み出すときは、同じ暗号化キーを要求に指定します。2 つの暗号化キーが一致すると、オブジェクトが復号化されてオブジェクトデータが返されます。

  オブジェクトの暗号化処理と復号化処理はすべて StorageGRID で管理されますが、指定する暗号化キーはユーザが管理する必要があります。

  指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。

  SSE または SSE-C で暗号化されたオブジェクトは、バケットレベルまたはグリッドレベルの暗号化設定が無視されます。

**SSE**を使用します

StorageGRID で管理される一意のキーでオブジェクトを暗号化する場合は、次の要求ヘッダーを使用します。

```
x-amz-server-side-encryption
```

SSE 要求ヘッダーは、次のオブジェクト処理でサポートされます。

- PUT Object の場合
- PUT Object - Copy の各コマンドを実行します
- マルチパートアップロードを開始します

**SSE-C**を使用する

ユーザが管理する一意のキーでオブジェクトを暗号化する場合は、次の 3 つの要求ヘッダーを使用します。

| 要求ヘッダー | 説明 |
| --- | --- |
| `x-amz-server-side-encryption-customer-algorithm` | 暗号化アルゴリズムを指定します。ヘッダー値はである必要があります `AES256`。 |
| `x-amz-server-side-encryption-customer-key` | オブジェクトの暗号化と復号化に使用する暗号化キーを指定します。キーの値は、 Base64 でエンコードされた 256 ビットであることが必要です。 |
| `x-amz-server-side-encryption-customer-key-MD5` | RFC 1321 に従って暗号化キーの MD5 ダイジェストを指定します。これは、暗号化キーがエラーなしで送信されたことを確認するために使用されます。MD5 ダイジェストの値は、 Base64 でエンコードされた 128 ビットであることが必要です。 |

SSE-C 要求ヘッダーは、次のオブジェクト処理でサポートされます。

- オブジェクトの取得
- HEAD Object の実行
- PUT Object の場合
- PUT Object - Copy の各コマンドを実行します
- マルチパートアップロードを開始します
- パーツをアップロードします
- パーツのアップロード - コピー

ユーザ指定のキーによるサーバ側の暗号化（ **SSE-C** ）を使用する場合の考慮事項

SSE-C を使用する場合は、次の考慮事項に注意してください。

- HTTPS を使用する必要があります。

SSE-C を使用すると、 http 経由の要求が StorageGRID ですべて拒否されますセキュリティ上の理由から、誤って http を使用して送信したキーは漏洩する可能性があります。キーを破棄し、必要に応じてローテーションします。

- 応答内の ETag は、オブジェクトデータの MD5 ではありません。
- 暗号化キーとオブジェクトの対応関係を管理する必要があります。StorageGRID では暗号化キーは格納されません。各オブジェクトに対して指定した暗号化キーを管理する責任はユーザにあります。
- バケットのバージョン管理が有効になっている場合は、オブジェクトのバージョンごとに固有の暗号化キーが必要です。各オブジェクトバージョンで使用される暗号化キーを管理する責任はユーザにあります。
- 暗号化キーはクライアント側で管理するため、キーローテーションなどの追加の防護策もクライアント側で管理する必要があります。

指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。

- バケットに CloudMirror レプリケーションが設定されている場合は、 SSE-C オブジェクトを取り込むことができません。取り込み処理は失敗します。

関連情報

"オブジェクトの取得"

"HEAD Object の実行"

"PUT Object の場合"

"PUT Object - Copy の各コマンドを実行します"

"マルチパートアップロードを開始します"

"パーツをアップロードします"

"パーツのアップロード - コピー"

"Amazon S3 開発者ガイド：「お客様が用意した暗号化キーによるサーバ側の暗号化（ SSE-C ）を使用したデータの保護」"

オブジェクトの取得

# S3 GET Object 要求を使用して、 S3 バケットからオブジェクトを読み出すことができます。

**PartNumber**要求パラメータはサポートされていません

。 `partNumber` 要求パラメータはGET Object要求ではサポートされません。マルチパートオブジェクトの特定のパートを読み出すGET要求は実行できません。501 Not Implementedエラーが返され、次のメッセージが表示されます。

```
GET Object by partNumber is not implemented
```

ユーザ指定の暗号化キーによるサーバ側の暗号化（ **SSE-C** ）の要求ヘッダー

指定した一意のキーでオブジェクトが暗号化されている場合は、 3 つのヘッダーをすべて使用します。

- `x-amz-server-side-encryption-customer-algorithm`:指定します `AES256`。
- `x-amz-server-side-encryption-customer-key`:オブジェクトの暗号化キーを指定します
- `x-amz-server-side-encryption-customer-key-MD5`:オブジェクトの暗号化キーのMD5ダイジェストを指定します。

> 指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。お客様提供の鍵を使用してオブジェクト・データを保護する前に'サーバ側の暗号化の使用に関する考慮事項を確認してください

ユーザメタデータ内の **UTF-8** 文字

StorageGRID は、ユーザ定義メタデータ内のエスケープされた UTF-8 文字を解析も解釈もしません。ユーザ定義メタデータにエスケープされたUTF-8文字が含まれているオブジェクトに対してGET要求を実行した場合、からは返されません `x-amz-missing-meta` キーの名前または値に印刷できない文字が含まれている場合は、ヘッダーを指定します。

サポートされない要求ヘッダーです

次の要求ヘッダーはサポートされていません `XNotImplemented`：

- `x-amz-website-redirect-location`

バージョン管理

の場合 `versionId` サブリソースが指定されていません。バージョン管理されたバケット内のオブジェクトの最新バージョンが取得されます。オブジェクトの現在のバージョンが削除マーカーの場合は、「見つからない」ステータスがとともに返されます `x-amz-delete-marker` 応答ヘッダーをに設定しました `true`。

クラウドストレージプールオブジェクトに対する **GET Object** の動作

オブジェクトがクラウドストレージプールに格納されている場合（情報ライフサイクル管理を使用してオブジェクトを管理する手順を参照）、 GET Object 要求の動作はオブジェクトの状態によって異なります。詳細については、「 head Object 」を参照してください。

> オブジェクトがクラウドストレージプールに格納され、かつそのオブジェクトのコピーがグリッドに 1 つ以上存在する場合、 GET Object 要求はクラウドストレージプールからデータを読み出す前に、グリッドからデータを読み出そうとします。

| オブジェクトの状態 | **GET Object** の動作 |
| --- | --- |
| StorageGRID に取り込まれているがまだ ILM によって評価されていないオブジェクト、または従来のストレージプールに格納されているオブジェクト、またはイレイジャーコーディングを使用しているオブジェクト | `200 OK`<br><br>オブジェクトのコピーが読み出されます。 |

| オブジェクトの状態 | **GET Object** の動作 |
| --- | --- |
| クラウドストレージプール内にあるが、まだ読み出し不可能な状態に移行していない | `200 OK`<br><br>オブジェクトのコピーが読み出されます。 |
| オブジェクトを読み出し不可能な状態に移行した | `403 Forbidden、 InvalidObjectState`<br><br>POST Object restore 要求を使用して、オブジェクトを読み出し可能な状態にリストアします。 |
| 読み出し不可能な状態からリストア中である | `403 Forbidden、 InvalidObjectState`<br><br>POST Object restore 要求が完了するまで待ちます。 |
| クラウドストレージプールへのリストアが完了している | `200 OK`<br><br>オブジェクトのコピーが読み出されます。 |

クラウドストレージプール内のマルチパートオブジェクトまたはセグメント化されたオブジェクト

マルチパートオブジェクトをアップロードした場合や StorageGRID が大きなオブジェクトをセグメントに分割した場合、 StorageGRID はオブジェクトのパーツまたはセグメントのサブセットをサンプリングすることでクラウドストレージプール内のオブジェクトが使用可能かどうかを判断します。GET Object要求が誤って返されることがあります `200 OK` オブジェクトの一部のパートがすでに読み出し不可能な状態に移行されている場合や、オブジェクトの一部のパートがまだリストアされていない場合。

このような場合は、次のよう

- GET Object 要求がデータの一部を返し、転送の途中で停止することがあります。
- 後続のGET Object要求が返されることがあります `403 Forbidden`。

関連情報

"サーバ側の暗号化を使用"

"ILM を使用してオブジェクトを管理する"

"POST Object restore の実行"

"監査ログで追跡される S3 処理"

#### **HEAD Object** の実行

S3 HEAD Object 要求を使用すると、オブジェクト自体を返さずにオブジェクトからメタデータを読み出すことができます。オブジェクトがクラウドストレージプールに格納されている場合は、 HEAD Object を使用してオブジェクトの移行状態を特定できます。

ユーザ指定の暗号化キーによるサーバ側の暗号化（ **SSE-C** ）の要求ヘッダー

指定した一意のキーでオブジェクトが暗号化されている場合は、次の 3 つのヘッダーをすべて使用します。

- `x-amz-server-side-encryption-customer-algorithm`:指定します `AES256`。
- `x-amz-server-side-encryption-customer-key`:オブジェクトの暗号化キーを指定します
- `x-amz-server-side-encryption-customer-key-MD5`:オブジェクトの暗号化キーのMD5ダイジェストを指定します。

> 指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。お客様提供の鍵を使用してオブジェクト・データを保護する前に'サーバ側の暗号化の使用に関する考慮事項を確認してください

ユーザメタデータ内の **UTF-8** 文字

StorageGRID は、ユーザ定義メタデータ内のエスケープされた UTF-8 文字を解析も解釈もしません。ユーザ定義メタデータにエスケープされたUTF-8文字が含まれているオブジェクトに対してHEAD要求を実行しても、は返されません `x-amz-missing-meta` キーの名前または値に印刷できない文字が含まれている場合は、ヘッダーを指定します。

サポートされない要求ヘッダーです

次の要求ヘッダーはサポートされていません `XNotImplemented`：

- `x-amz-website-redirect-location`

クラウドストレージプールオブジェクトの応答ヘッダー

オブジェクトがクラウドストレージプールに格納されている場合（情報ライフサイクル管理を使用してオブジェクトを管理する手順を参照）、次の応答ヘッダーが返されます。

- `x-amz-storage-class: GLACIER`
- `x-amz-restore`

応答ヘッダーは、オブジェクトがクラウドストレージプールに移動され、必要に応じて読み出し不可能な状態に移行されてリストアされるときの状態に関する情報を提供します。

| オブジェクトの状態 | **HEAD Object** への応答 |
| --- | --- |
| StorageGRID に取り込まれているがまだ ILM によって評価されていないオブジェクト、または従来のストレージプールに格納されているオブジェクト、またはイレイジャーコーディングを使用しているオブジェクト | `200 OK` （特別な応答ヘッダーは返されません）。 |

| オブジェクトの状態 | **HEAD Object** への応答 |
| --- | --- |
| クラウドストレージプール内にあるが、まだ読み出し不可能な状態に移行していない | `200 OK`<br><br>`x-amz-storage-class: GLACIER`<br><br>`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`<br><br>オブジェクトが読み出し不可能な状態に移行されるまでの間、の値 `expiry-date` は、将来の特定の日時に設定されます。移行の正確な時間は、StorageGRID システムでは制御されません。 |
| オブジェクトが読み出し不可能な状態に移行したが、少なくとも 1 つのコピーがグリッドに存在する | `200 OK`<br><br>`x-amz-storage-class: GLACIER`<br><br>`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`<br><br>の値 `expiry-date` は、将来の特定の日時に設定されます。<br><br>• 注：グリッド上のコピーを取得できない場合（ストレージノードが停止している場合など）は、オブジェクトを読み出す前に、問題 a POST Object restore 要求を実行してクラウドストレージプールからコピーをリストアする必要があります。 |
| 読み出し不可能な状態に移行しており、グリッドにコピーが存在しない | `200 OK`<br><br>`x-amz-storage-class: GLACIER` |
| 読み出し不可能な状態からリストア中である | `200 OK`<br><br>`x-amz-storage-class: GLACIER`<br><br>`x-amz-restore: ongoing-request="true"` |

| オブジェクトの状態 | **HEAD Object** への応答 |
| --- | --- |
| クラウドストレージプールへのリストアが完了している | `200 OK`<br><br>`x-amz-storage-class: GLACIER`<br><br>`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2018 00:00:00 GMT"`<br><br>。 `expiry-date` クラウドストレージプール内のオブジェクトが読み出し不可能な状態に戻るタイミングを示します。 |

クラウドストレージプール内のマルチパートオブジェクトまたはセグメント化されたオブジェクト

マルチパートオブジェクトをアップロードした場合や StorageGRID が大きなオブジェクトをセグメントに分割した場合、 StorageGRID はオブジェクトのパーツまたはセグメントのサブセットをサンプリングすることでクラウドストレージプール内のオブジェクトが使用可能かどうかを判断します。HEAD Object要求が誤って返されることがあります `x-amz-restore: ongoing-request="false"` オブジェクトの一部のパートがすでに読み出し不可能な状態に移行されている場合や、オブジェクトの一部のパートがまだリストアされていない場合。

バージョン管理

の場合 `versionId` サブリソースが指定されていません。バージョン管理されたバケット内のオブジェクトの最新バージョンが取得されます。オブジェクトの現在のバージョンが削除マーカーの場合は、「見つからない」ステータスがとともに返されます `x-amz-delete-marker` 応答ヘッダーをに設定しました `true`。

関連情報

"サーバ側の暗号化を使用"

"ILM を使用してオブジェクトを管理する"

"POST Object restore の実行"

"監査ログで追跡される S3 処理"

**POST Object restore** の実行

## S3 POST Object restore 要求を使用して、クラウドストレージプールに格納されているオブジェクトをリストアできます。

サポートされている要求タイプ

StorageGRID では、オブジェクトのリストアに POST Object restore 要求のみがサポートされます。ではサポートされません `SELECT` リストアのタイプ。戻り要求を選択してください `XNotImplemented`。

バージョン管理

必要に応じて、と指定します `versionId` バージョン管理されたバケット内のオブジェクトの特定のバージョンをリストアする。指定しない場合は `versionId`オブジェクトの最新バージョンがリストアされます

クラウドストレージプールオブジェクトでの **POST Object restore** の動作

オブジェクトがクラウドストレージプールに格納されている場合（情報ライフサイクル管理を使用してオブジェクトを管理する手順を参照）、 POST Object restore 要求はオブジェクトの状態に基づいて次のように動作します。詳細については、「 head Object 」を参照してください。

> オブジェクトがクラウドストレージプールに格納され、かつそのオブジェクトのコピーがグリッドに 1 つ以上存在する場合は、 POST Object restore 要求を実行してオブジェクトをリストアする必要はありません。GET Object 要求を使用してローカルコピーを直接読み出すことができます。

| オブジェクトの状態 | **POST Object restore** の動作 |
| --- | --- |
| StorageGRID に取り込まれているがまだ ILM によって評価されていない、またはオブジェクトがクラウドストレージプールにない | `403 Forbidden、 InvalidObjectState` |
| クラウドストレージプール内にあるが、まだ読み出し不可能な状態に移行していない | `200 OK` 変更は行われません。<br><br>*注：読み出し不可能な状態に移行する前に、オブジェクトを変更することはできません `expiry-date`。 |
| オブジェクトを読み出し不可能な状態に移行した | `202 Accepted` 要求の本文で指定されている日数、オブジェクトの読み出し可能なコピーをクラウドストレージプールにリストアします。この期間が終了すると、オブジェクトは読み出し不可能な状態に戻ります。<br><br>必要に応じて、を使用します `Tier` リストアジョブの完了までにかかる時間を確認するための要求要素 (`Expedited`、 `Standard`または `Bulk`）。指定しない場合は `Tier`、 `Standard` 階層を使用しています。<br><br>*注意：S3 Glacier Deep Archiveまたはクラウドストレージプールに移行されたオブジェクトや、Azure Blob Storageを使用するクラウドストレージは、を使用してリストアできません `Expedited` 階層：次のエラーが返されます `403 Forbidden、 InvalidTier：Retrieval option is not supported by this storage class`。 |
| 読み出し不可能な状態からリストア中である | `409 Conflict、 RestoreAlreadyInProgress` |

| オブジェクトの状態 | **POST Object restore** の動作 |
| --- | --- |
| クラウドストレージプールへのリストアが完了している | `200 OK`<br><br>*注：*オブジェクトが読み出し可能な状態にリストアされている場合は、オブジェクトを変更できます `expiry-date` 用の新しい値を指定してPOST Object restore要求を再発行する `Days`。要求が実行された日時に基づいてリストア日が更新されます。 |

関連情報

"ILM を使用してオブジェクトを管理する"

"HEAD Object の実行"

"監査ログで追跡される S3 処理"

**PUT Object** の場合

## S3 PUT Object 要求を使用すると、オブジェクトをバケットに追加できます。

競合の解決

同一キーに書き込む2つのクライアントなど'競合するクライアント要求は'最新のWINS形式で解決されます「latest-wins」評価のタイミングは、S3クライアントが処理を開始するタイミングではなく、StorageGRIDシステムが特定の要求を完了したタイミングに基づいています。

オブジェクトのサイズ

StorageGRID は、サイズが最大5TBのオブジェクトをサポートします。

ユーザメタデータのサイズ

Amazon S3 では、各 PUT 要求ヘッダー内のユーザ定義メタデータのサイズが 2KB に制限されます。StorageGRID では、ユーザメタデータが 24KiB に制限されます。ユーザ定義のメタデータのサイズは、各キーと値の UTF-8 エンコードでのバイト数の合計で測定されます。

ユーザメタデータ内の **UTF-8** 文字

要求のユーザ定義メタデータのキー名または値に（エスケープされていない） UTF-8 文字が含まれている場合、 StorageGRID の動作は定義されていません。

ユーザ定義メタデータのキー名または値に含まれているエスケープされた UTF-8 文字は、 StorageGRID で解析も解釈もされません。エスケープされた UTF-8 文字は ASCII 文字として扱われます。

- ユーザ定義メタデータにエスケープされた UTF-8 文字が含まれている場合、 PUT 、 PUT Object-Copy 、 GET 、 HEAD の各要求は正常に実行されます。
- StorageGRID からが返されない `x-amz-missing-meta` キーの名前または値の解釈後の値に印刷不能文字が含まれている場合は、ヘッダー。

### オブジェクトタグの制限

タグは、新しいオブジェクトをアップロードするときに追加することも、既存のオブジェクトに追加することもできます。StorageGRID と Amazon S3 はどちらも、オブジェクトごとに最大 10 個のタグをサポートします。オブジェクトに関連付けられたタグには、一意のタグキーが必要です。タグキーには Unicode 文字を 128 文字まで、タグ値には Unicode 文字を 256 文字まで使用できます。キーと値では大文字と小文字が区別されます。

### オブジェクトの所有権

StorageGRID では、非所有者アカウントまたは匿名ユーザによって作成されたオブジェクトを含むすべてのオブジェクトが、バケット所有者アカウントによって所有されます。

### サポートされる要求ヘッダー

次の要求ヘッダーがサポートされています。

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`

  を指定する場合 `aws-chunked` の場合 `Content-Encoding`StorageGRID では、次の項目は検証されません。

  - StorageGRID ではが検証されません `chunk-signature` チャンクデータに対して。
  - StorageGRID は、ユーザが指定した値を検証しません `x-amz-decoded-content-length` をクリックします。
- `Content-Language`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Expires`
- `Transfer-Encoding`

  チャンク転送エンコードは、の場合にサポートされます `aws-chunked` ペイロード署名も使用されます。

- `x-amz-meta-`をクリックし、続けてユーザ定義のメタデータを含む名前と値のペアを作成します。

  ユーザ定義メタデータの名前と値のペアを指定する場合、一般的な形式は次のとおりです。

  ```
  x-amz-meta-<em>name</em>: <em>value</em>
  ```

  ILMルールの参照時間として* User Defined Creation Time *オプションを使用する場合は、を使用する必要があります `creation-time` を、オブジェクトの作成時に記録されたメタデータの名前として指定します。例：

```
x-amz-meta-creation-time: 1443399726
```

の値 `creation-time` は、1970年1月1日からの秒数として評価されます。

> ILM ルールで、参照時間に * User Defined Creation Time * と取り込み動作に Balanced オプションまたは Strict オプションの両方を使用することはできません。ILM ルールの作成時にエラーが返されます。

- `x-amz-tagging`
- S3 Object Lock 要求のヘッダー
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

"S3 オブジェクトロックを使用する"

- SSE 要求ヘッダー：
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

"S3 REST API のサポートされる処理と制限事項"

サポートされない要求ヘッダーです

次の要求ヘッダーはサポートされていません。

- 。 `x-amz-acl` 要求ヘッダーはサポートされていません。
- 。 `x-amz-website-redirect-location` 要求ヘッダーはサポートされておらず、返されます `XNotImplemented`。

ストレージクラスのオプション

。 `x-amz-storage-class` 要求ヘッダーがサポートされています。に送信された値 `x-amz-storage-class` StorageGRID が取り込み中にオブジェクトデータを保護する方法に影響し、StorageGRID システム（ILMで決定）に格納されるオブジェクトの永続的コピーの数には影響しません。

取り込まれたオブジェクトに一致するILMルールの取り込み動作がStrictオプションに指定されている場合、はを使用します `x-amz-storage-class` ヘッダーに影響はありません。

には次の値を使用できます `x-amz-storage-class`：

- `STANDARD` （デフォルト）

- * Dual commit * ： ILM ルールの取り込み動作が Dual commit オプションに指定されている場合は、オブジェクトの取り込み直後にオブジェクトの 2 つ目のコピーが作成されて別のストレージノードに配置されます（デュアルコミット）。ILM が評価されると、この初期中間コピーがルールの配置手順を満たしているかどうかを StorageGRID が判断します。満たしていない場合は、新しいオブジェクトコピーを別の場所に作成し、初期中間コピーを削除することが必要になる可能性があります。
- * Balanced * ： ILM ルールで Balanced オプションが指定されていて、ルールで指定されたすべてのコピーを StorageGRID がただちに作成できない場合、 StorageGRID は 2 つの中間コピーを別々のストレージノードに作成します。

  StorageGRID がILMルールに指定されたすべてのオブジェクトコピーをただちに作成できる場合（同期配置）は、を参照してください `x-amz-storage-class` ヘッダーに影響はありません。

- `REDUCED_REDUNDANCY`
  - * Dual commit * ： ILM ルールの取り込み動作が Dual commit オプションに指定されている場合は、オブジェクトの取り込み時に StorageGRID が中間コピーを 1 つ作成します（シングルコミット）。
  - * Balanced * ： ILM ルールで Balanced オプションが指定されている場合、 StorageGRID は、ルールで指定されたすべてのコピーをただちに作成できない場合にのみ、中間コピーを 1 つ作成します。StorageGRID で同期配置を実行できる場合、このヘッダーは効果がありません。。 `REDUCED_REDUNDANCY` オプションは、オブジェクトに一致するILMルールで単一のレプリケートコピーが作成される場合に最適です。この場合は、を使用します `REDUCED_REDUNDANCY` 取り込み処理のたびに追加のオブジェクトコピーを不要に作成および削除する必要がなくなります。

  を使用する `REDUCED_REDUNDANCY` それ以外の場合は、このオプションは推奨されません。 `REDUCED_REDUNDANCY` 取り込み中にオブジェクトデータが失われるリスクが高まります。たとえば、 ILM 評価の前にコピーが 1 つだけ格納されていたストレージノードに障害が発生すると、データが失われる可能性があります。

- 注意 * ：一定期間にレプリケートされたコピーを 1 つだけ保持すると、データが永久に失われる危険があります。オブジェクトのレプリケートコピーが 1 つしかない場合、ストレージノードに障害が発生したり、重大なエラーが発生すると、そのオブジェクトは失われます。また、アップグレードなどのメンテナンス作業中は、オブジェクトへのアクセスが一時的に失われます。

を指定します `REDUCED_REDUNDANCY` オブジェクトの初回取り込み時に作成されるコピー数のみに影響します。オブジェクトがアクティブな ILM ポリシーで評価される際に作成されるオブジェクトのコピー数には影響せず、 StorageGRID システムでデータが格納されるときの冗長性レベルが低下することもありません。

*注：S3オブジェクトロックが有効な状態でオブジェクトをバケットに取り込む場合は、を使用します `REDUCED_REDUNDANCY` オプションは無視されます。古い準拠バケットにオブジェクトを取り込む場合は、を参照してください `REDUCED_REDUNDANCY` オプションを指定するとエラーが返されます。StorageGRID では、常にデュアルコミットの取り込みが実行され、コンプライアンス要件が満たされます。

サーバ側の暗号化を行うための要求ヘッダー

オブジェクトをサーバ側の暗号化で暗号化するには、次の要求ヘッダーを使用します。SSE オプションと SSE-C オプションを同時に指定することはできません。

- * SSE * ： StorageGRID で管理される一意のキーでオブジェクトを暗号化するには、次のヘッダーを使用します。
  - `x-amz-server-side-encryption`
- * SSE-C * ：ユーザが指定および管理する一意のキーでオブジェクトを暗号化する場合は、次の 3 つのヘ

ッダーをすべて使用します。

- `x-amz-server-side-encryption-customer-algorithm`:指定します `AES256`。
- `x-amz-server-side-encryption-customer-key`:新しいオブジェクトの暗号化キーを指定します。
- `x-amz-server-side-encryption-customer-key-MD5`:新しいオブジェクトの暗号化キーのMD5ダイジェストを指定します。

- 注意： * 指定した暗号化キーは保存されません。暗号化キーを紛失すると、対応するオブジェクトが失われます。お客様提供の鍵を使用してオブジェクト・データを保護する前に'サーバ側の暗号化の使用に関する考慮事項を確認してください

*注：SSEまたはSSE-Cで暗号化されたオブジェクトは、バケットレベルまたはグリッドレベルの暗号化設定が無視されます。

バージョン管理

バケットでバージョン管理が有効になっている場合は、一意です `versionId` は、格納されているオブジェクトのバージョンに対して自動的に生成されます。これ `versionId` は、を使用して応答としても返されます `x-amz-version-id` 応答ヘッダー。

バージョン管理が一時停止中の場合は、オブジェクトバージョンはnullで格納されます `versionId` また、nullバージョンがすでに存在する場合は上書きされます。

関連情報

"ILM を使用してオブジェクトを管理する"

"バケットの処理"

"監査ログで追跡される S3 処理"

"サーバ側の暗号化を使用"

"クライアント接続の設定方法"

**PUT Object - Copy** の各コマンドを実行します

S3 PUT Object - Copy 要求を使用すると、すでに S3 に格納されているオブジェクトのコピーを作成できます。PUT Object - Copy 処理は、 GET を実行してから PUT を実行する処理と同じです。

競合の解決

同一キーに書き込む2つのクライアントなど'競合するクライアント要求は'最新のWINS形式で解決されます「latest-wins」評価のタイミングは、S3クライアントが処理を開始するタイミングではなく、StorageGRIDシステムが特定の要求を完了したタイミングに基づいています。

オブジェクトのサイズ

StorageGRID は、サイズが最大5TBのオブジェクトをサポートします。

ユーザメタデータ内の **UTF-8** 文字

要求のユーザ定義メタデータのキー名または値に（エスケープされていない） UTF-8 文字が含まれている場合、 StorageGRID の動作は定義されていません。

ユーザ定義メタデータのキー名または値に含まれているエスケープされた UTF-8 文字は、 StorageGRID で解析も解釈もされません。エスケープされた UTF-8 文字は ASCII 文字として扱われます。

- ユーザ定義メタデータにエスケープされた UTF-8 文字が含まれている場合、要求は正常に実行されます。
- StorageGRID からが返されない `x-amz-missing-meta` キーの名前または値の解釈後の値に印刷不能文字が含まれている場合は、ヘッダー。

サポートされる要求ヘッダー

次の要求ヘッダーがサポートされています。

- `Content-Type`
- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`
- `x-amz-meta-`をクリックし、続けてユーザ定義のメタデータを含む名前と値のペアを作成します
- `x-amz-metadata-directive`:デフォルト値はです `COPY`をクリックすると、オブジェクトおよび関連するメタデータをコピーできます。

  を指定できます `REPLACE` オブジェクトのコピー時に既存のメタデータを上書きする場合、またはオブジェクトメタデータを更新する場合。

- `x-amz-storage-class`
- `x-amz-tagging-directive`:デフォルト値はです `COPY`をクリックすると、オブジェクトとすべてのタグをコピーできます。

  を指定できます `REPLACE` オブジェクトのコピー時に既存のタグを上書きする場合、またはタグを更新する場合。

- S3 オブジェクトロック要求のヘッダー：
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

"S3 オブジェクトロックを使用する"

- SSE 要求ヘッダー：
  - `x-amz-copy-source-server-side-encryption-customer-algorithm`

- x-amz-copy-source-server-side-encryption-customer-key
- x-amz-copy-source-server-side-encryption-customer-key-MD5
- x-amz-server-side-encryption
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-algorithm

"サーバ側の暗号化を行うための要求ヘッダー"

サポートされない要求ヘッダーです

次の要求ヘッダーはサポートされていません。

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- x-amz-website-redirect-location

ストレージクラスのオプション

。 x-amz-storage-class 要求ヘッダーがサポートされ、一致するILMルールで取り込み動作にDual commitまたはBalancedが指定されている場合にStorageGRID で作成されるオブジェクトコピーの数に影響します。

- STANDARD

  （デフォルト） ILM ルールで Dual commit オプションが使用されている場合、または Balanced オプションによって中間コピーが作成される場合に、デュアルコミットの取り込み処理を指定します。

- REDUCED_REDUNDANCY

  ILM ルールで Dual commit オプションが使用されている場合、または Balanced オプションによって中間コピーが作成される場合に、シングルコミットの取り込み処理を指定します。

> S3オブジェクトロックを有効にしてオブジェクトをバケットに取り込む場合は、を使用します REDUCED_REDUNDANCY オプションは無視されます。古い準拠バケットにオブジェクトを取り込む場合は、を参照してください REDUCED_REDUNDANCY オプションを指定するとエラーが返されます。StorageGRID では、常にデュアルコミットの取り込みが実行され、コンプライアンス要件が満たされます。

**PUT Object - Copy** で **x-amz-copy-source** を使用しています

ソースのバケットとキーの場合は、で指定します x-amz-copy-source ヘッダーはデスティネーションのバケットおよびキーとは異なり、ソースオブジェクトデータのコピーがデスティネーションに書き込まれます。

送信元と宛先が一致している場合は、および x-amz-metadata-directive ヘッダーはのように指定します `REPLACE`では、要求で指定されたメタデータの値に基づいてオブジェクトのメタデータが更新されます。この場合、 StorageGRID はオブジェクトを再取り込みしません。これには 2 つの重要な結果があります。

- PUT Object - Copy を使用して既存のオブジェクトを暗号化したり、既存のオブジェクトの暗号化を変更したりすることはできません。を用意する場合は x-amz-server-side-encryption ヘッダーまたは x-amz-server-side-encryption-customer-algorithm ヘッダー。StorageGRID は要求を拒否し、戻ります XNotImplemented。
- 一致する ILM ルールで指定されている取り込み動作のオプションが使用されません。更新によって発生したオブジェクト配置の変更は、通常のバックグラウンド ILM プロセスで ILM が再評価されるときに実施されます。

  このため、 ILM ルールの取り込み動作に Strict オプションが指定されている場合、必要なオブジェクト配置を実行できないと（たとえば、新たに必要となった場所を使用できない場合）、アクションは実行されません。更新されたオブジェクトは、必要な配置を実行可能になるまで現在の配置が維持されます。

サーバ側の暗号化を行うための要求ヘッダー

サーバ側の暗号化を使用する場合は、ソースオブジェクトが暗号化されているかどうか、およびターゲットオブジェクトを暗号化するかどうかによって、指定する要求ヘッダーが異なります。

- ソースオブジェクトがユーザ指定のキーを使用して暗号化されている場合（ SSE-C ）は、オブジェクトを復号化してコピーできるように、 PUT Object - Copy 要求に次の 3 つのヘッダーを含める必要があります。
  - x-amz-copy-source-server-side-encryption-customer-algorithm を指定します AES256。
  - x-amz-copy-source-server-side-encryption-customer-key ソースオブジェクトの作成時に指定した暗号化キーを指定します。
  - x-amz-copy-source-server-side-encryption-customer-key-MD5:ソースオブジェクトの作成時に指定したMD5ダイジェストを指定します。
- ユーザが指定および管理する一意のキーでターゲットオブジェクト（コピー）を暗号化する場合は、次の 3 つのヘッダーを含めます。
  - x-amz-server-side-encryption-customer-algorithm:指定します AES256。
  - x-amz-server-side-encryption-customer-key:ターゲットオブジェクトの新しい暗号化キーを指定します
  - x-amz-server-side-encryption-customer-key-MD5:新しい暗号化キーのMD5ダイジェストを指定します。
- 注意： * 指定した暗号化キーは保存されません。暗号化キーを紛失すると、対応するオブジェクトが失われます。お客様提供の鍵を使用してオブジェクト・データを保護する前に'サーバ側の暗号化の使用に関する考慮事項を確認してください
- StorageGRID で管理される一意のキーでターゲットオブジェクト（コピー）を暗号化する（ SSE ）には、 PUT Object - Copy 要求に次のヘッダーを含めます。
  - x-amz-server-side-encryption

注： server-side-encryption オブジェクトの値を更新できません。代わりに、新しいを使用してコピーを作成します server-side-encryption を使用した値 x-amz-metadata-directive： REPLACE。

バージョン管理

ソースバケットがバージョン管理に対応している場合は、を使用できます `x-amz-copy-source` オブジェクトの最新バージョンをコピーするヘッダー。オブジェクトの特定のバージョンをコピーするには、を使用してコピーするバージョンを明示的に指定する必要があります `versionId` サブリソース：デスティネーションバケットがバージョン管理に対応している場合は、で生成されたバージョンが返されます `x-amz-version-id` 応答ヘッダー。ターゲットバケットのバージョン管理が一時停止中の場合は、を実行します `x-amz-version-id` 「null」値を返します。

関連情報

"ILM を使用してオブジェクトを管理する"

"サーバ側の暗号化を使用"

"監査ログで追跡される S3 処理"

"PUT Object の場合"

マルチパートアップロードの処理

このセクションでは、 StorageGRID でのマルチパートアップロードの処理のサポートについて説明します。

- "マルチパートアップロードを表示します"
- "マルチパートアップロードを開始します"
- "パーツをアップロードします"
- "パーツのアップロード - コピー"
- "Complete Multipart Upload の実行"

マルチパートアップロードのすべての処理に、次の条件と注意事項が適用されます。

- 1 つのバケットに対して同時に実行するマルチパートアップロードが 1 、 000 件を超えないようにしてください。 1 、 000 件を超えると、そのバケットに対する List Multipart Uploads のクエリで完全な結果が返されないことがあります。
- StorageGRID は、マルチパートに AWS のサイズ制限を適用します。S3 クライアントは次のガイドラインに従う必要があります。
  - マルチパートアップロードの各パートのサイズは 5MiB （ 5 、 242 、 880 バイト）と 5GiB （ 5 、 368 、 709 、 120 バイト）の間にする必要があります。
  - 最後の部分は 5MiB （ 5,242,880 バイト）より小さくできます。
  - 一般に、パーツサイズはできるだけ大きくする必要があります。たとえば、 100GiB オブジェクトの場合、 5GB のパートサイズを使用します。各パートは固有のオブジェクトとみなされるため、大きなパートサイズを使用すると、 StorageGRID のメタデータのオーバーヘッドが軽減されます。
  - 5GB 未満のオブジェクトでは、マルチパートではないアップロードの使用を検討してください。
- ILM ルールの取り込み動作が Strict または Balanced に指定されている場合は、マルチパートオブジェクトの各パートが取り込まれるときに ILM が評価され、マルチパートアップロードが完了したときにオブジェクト全体に対して ILM が評価されます。これがオブジェクトとパートの配置にどのように影響するかに注意する必要があります。

- S3 マルチパートアップロードの進行中に ILM が変更されると、マルチパートアップロードが完了した時点でオブジェクトの一部のパートが現在の ILM 要件を満たしていないことがあります。正しく配置されていないパートは ILM ルールによる再評価の対象としてキューに登録され、あとで正しい場所に移動されます。
- パートに対して ILM を評価する際、 StorageGRID はオブジェクトのサイズではなくパートのサイズでフィルタリングします。つまり、オブジェクト全体としては ILM 要件を満たしていない場所にオブジェクトのパーツが格納される可能性があります。たとえば、 10GB 以上のオブジェクトをすべて DC1 に格納し、それより小さいオブジェクトをすべて DC2 に格納するルールの場合、 10 パートからなるマルチパートアップロードの 1GB の各パートは取り込み時に DC2 に格納されます。オブジェクト全体に対して ILM が評価されると、オブジェクトのすべてのパートが DC1 に移動されます。

- マルチパートアップロードでは、すべての処理で StorageGRID の整合性制御がサポートされます。
- マルチパートアップロードでは、必要に応じてサーバ側の暗号化を使用できます。SSE（StorageGRIDで管理されるキーによるサーバ側の暗号化）を使用するには、を指定します `x-amz-server-side-encryption` Initiate Multipart Upload要求のみの要求ヘッダー。SSE-C （ユーザ指定のキーによるサーバ側の暗号化）を使用する場合は、 Initiate Multipart Upload 要求と後続の各 Upload Part 要求に、同じ 3 つの暗号化キー要求ヘッダーを指定します。

| 操作 | 実装 |
| --- | --- |
| マルチパートアップロードをリストします | を参照してください "マルチパートアップロードをリストします" |
| マルチパートアップロードを開始します | を参照してください "マルチパートアップロードを開始します" |
| パーツをアップロードします | を参照してください "パーツをアップロードします" |
| パーツのアップロード - コピー | を参照してください "パーツのアップロード - コピー" |
| Complete Multipart Upload の実行 | を参照してください "Complete Multipart Upload の実行" |
| マルチパートアップロードを中止します | Amazon S3 REST API のすべての動作が実装されています |
| パーツをリストします | Amazon S3 REST API のすべての動作が実装されています |

関連情報

"整合性制御"

"サーバ側の暗号化を使用"

マルチパートアップロードをリストします

## List Multipart Uploads 処理では、バケットの進行中のマルチパートアップロードがリストされます。

次の要求パラメータがサポートされています。

- encoding-type
- max-uploads
- key-marker
- prefix
- upload-id-marker

。 delimiter 要求パラメータはサポートされません。

バージョン管理

マルチパートアップロードは、アップロードの開始、アップロードのリストの表示、パートのアップロード、アップロードしたパートのアセンブル、およびアップロードの完了の個別の処理に分けられます。Complete Multipart Upload 処理が実行されると、オブジェクトが作成される時点（およびバージョン管理されている場合）になります。

マルチパートアップロードを開始します

## Initiate Multipart Upload 処理は、オブジェクトのマルチパートアップロードを開始し、アップロード ID を返します。

。 x-amz-storage-class 要求ヘッダーがサポートされています。に送信された値 x-amz-storage-class StorageGRID が取り込み中にオブジェクトデータを保護する方法に影響し、StorageGRID システム（ILMで決定）に格納されるオブジェクトの永続的コピーの数には影響しません。

取り込まれたオブジェクトに一致するILMルールの取り込み動作がStrictオプションに指定されている場合、はを使用します x-amz-storage-class ヘッダーに影響はありません。

には次の値を使用できます x-amz-storage-class：

- STANDARD （デフォルト）
  - * Dual commit * ： ILM ルールの取り込み動作が Dual commit オプションに指定されている場合は、オブジェクトの取り込み直後にオブジェクトの 2 つ目のコピーが作成されて別のストレージノードに配置されます（デュアルコミット）。ILM が評価されると、この初期中間コピーがルールの配置手順を満たしているかどうかを StorageGRID が判断します。満たしていない場合は、新しいオブジェクトコピーを別の場所に作成し、初期中間コピーを削除することが必要になる可能性があります。
  - * Balanced * ： ILM ルールで Balanced オプションが指定されていて、ルールで指定されたすべてのコピーを StorageGRID がただちに作成できない場合、 StorageGRID は 2 つの中間コピーを別々のストレージノードに作成します。

    StorageGRID がILMルールに指定されたすべてのオブジェクトコピーをただちに作成できる場合（同期配置）は、を参照してください x-amz-storage-class ヘッダーに影響はありません。
- REDUCED_REDUNDANCY
  - * Dual commit * ： ILM ルールの取り込み動作が Dual commit オプションに指定されている場合は、オブジェクトの取り込み時に StorageGRID が中間コピーを 1 つ作成します（シングルコミット）。

◦ * Balanced * ： ILM ルールで Balanced オプションが指定されている場合、 StorageGRID は、ルールで指定されたすべてのコピーをただちに作成できない場合にのみ、中間コピーを 1 つ作成します。StorageGRID で同期配置を実行できる場合、このヘッダーは効果がありません。。 `REDUCED_REDUNDANCY` オプションは、オブジェクトに一致するILMルールで単一のレプリケートコピーが作成される場合に最適です。この場合は、を使用します `REDUCED_REDUNDANCY` 取り込み処理のたびに追加のオブジェクトコピーを不要に作成および削除する必要がなくなります。

を使用する `REDUCED_REDUNDANCY` それ以外の場合は、このオプションは推奨されません。 `REDUCED_REDUNDANCY` 取り込み中にオブジェクトデータが失われるリスクが高まります。たとえば、 ILM 評価の前にコピーが 1 つだけ格納されていたストレージノードに障害が発生すると、データが失われる可能性があります。

- 注意 * ：一定期間にレプリケートされたコピーを 1 つだけ保持すると、データが永久に失われる危険があります。オブジェクトのレプリケートコピーが 1 つしかない場合、ストレージノードに障害が発生したり、重大なエラーが発生すると、そのオブジェクトは失われます。また、アップグレードなどのメンテナンス作業中は、オブジェクトへのアクセスが一時的に失われます。

を指定します `REDUCED_REDUNDANCY` オブジェクトの初回取り込み時に作成されるコピー数のみに影響します。オブジェクトがアクティブな ILM ポリシーで評価される際に作成されるオブジェクトのコピー数には影響せず、 StorageGRID システムでデータが格納されるときの冗長性レベルが低下することもありません。

*注：S3オブジェクトロックが有効な状態でオブジェクトをバケットに取り込む場合は、を使用します `REDUCED_REDUNDANCY` オプションは無視されます。古い準拠バケットにオブジェクトを取り込む場合は、を参照してください `REDUCED_REDUNDANCY` オプションを指定するとエラーが返されます。StorageGRID では、常にデュアルコミットの取り込みが実行され、コンプライアンス要件が満たされます。

次の要求ヘッダーがサポートされています。

- `Content-Type`
- `x-amz-meta-`をクリックし、続けてユーザ定義のメタデータを含む名前と値のペアを作成します

  ユーザ定義メタデータの名前と値のペアを指定する場合、一般的な形式は次のとおりです。

  ```
  x-amz-meta-_name_: `value`
  ```

  ILMルールの参照時間として* User Defined Creation Time *オプションを使用する場合は、を使用する必要があります `creation-time` を、オブジェクトの作成時に記録されたメタデータの名前として指定します。例：

  ```
  x-amz-meta-creation-time: 1443399726
  ```

  の値 `creation-time` は、1970年1月1日からの秒数として評価されます。

  追加中です `creation-time` レガシー準拠が有効になっているバケットにオブジェクトを追加する場合、ユーザ定義メタデータは許可されません。エラーが返されます。

- S3 オブジェクトロック要求のヘッダー：
  - `x-amz-object-lock-mode`

- x-amz-object-lock-retain-until-date
- x-amz-object-lock-legal-hold

"S3 オブジェクトロックを使用する"

- SSE 要求ヘッダー：
  - x-amz-server-side-encryption
  - x-amz-server-side-encryption-customer-key-MD5
  - x-amz-server-side-encryption-customer-key
  - x-amz-server-side-encryption-customer-algorithm

"S3 REST API のサポートされる処理と制限事項"

StorageGRID での UTF-8 文字の処理については、 PUT Object に関するドキュメントを参照してください。

サーバ側の暗号化を行うための要求ヘッダー

マルチパートオブジェクトをサーバ側の暗号化で暗号化するには、次の要求ヘッダーを使用します。SSE オプションと SSE-C オプションを同時に指定することはできません。

- * SSE * ： StorageGRID で管理される一意のキーでオブジェクトを暗号化する場合は、 Initiate Multipart Upload 要求で次のヘッダーを使用します。Upload Part 要求ではこのヘッダーを指定しないでください。
  - x-amz-server-side-encryption
- * SSE-C * ：ユーザが指定および管理する一意のキーでオブジェクトを暗号化する場合は、 Initiate Multipart Upload 要求（および後続の各 Upload Part 要求）で、次の 3 つのヘッダーをすべて使用します。
  - x-amz-server-side-encryption-customer-algorithm:指定します AES256。
  - x-amz-server-side-encryption-customer-key:新しいオブジェクトの暗号化キーを指定します。
  - x-amz-server-side-encryption-customer-key-MD5:新しいオブジェクトの暗号化キーのMD5ダイジェストを指定します。
- 注意： * 指定した暗号化キーは保存されません。暗号化キーを紛失すると、対応するオブジェクトが失われます。お客様提供の鍵を使用してオブジェクト・データを保護する前に'サーバ側の暗号化の使用に関する考慮事項を確認してください

サポートされない要求ヘッダーです

次の要求ヘッダーはサポートされていません XNotImplemented

- x-amz-website-redirect-location

バージョン管理

マルチパートアップロードは、アップロードの開始、アップロードのリストの表示、パートのアップロード、アップロードしたパートのアセンブル、およびアップロードの完了の個別の処理に分けられます。Complete

Multipart Upload 処理が実行されると、オブジェクトが作成されます（該当する場合はバージョン管理されます）。

関連情報

"ILM を使用してオブジェクトを管理する"

"サーバ側の暗号化を使用"

"PUT Object の場合"

パーツをアップロードします

## Upload Part 処理では、オブジェクトのマルチパートアップロード内のパートがアップロードされます。

サポートされる要求ヘッダー

次の要求ヘッダーがサポートされています。

- `Content-Length`
- `Content-MD5`

サーバ側の暗号化を行うための要求ヘッダー

Initiate Multipart Upload 要求に SSE-C 暗号化を指定した場合は、各 Upload Part 要求に次の要求ヘッダーも含める必要があります。

- `x-amz-server-side-encryption-customer-algorithm`:指定します `AES256`。
- `x-amz-server-side-encryption-customer-key`：Initiate Multipart Upload要求で指定した暗号化キーを指定します。
- `x-amz-server-side-encryption-customer-key-MD5`：Initiate Multipart Upload要求で指定したMD5ダイジェストを指定します。

> 指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。お客様提供の鍵を使用してオブジェクト・データを保護する前に'サーバ側の暗号化の使用に関する考慮事項を確認してください

バージョン管理

マルチパートアップロードは、アップロードの開始、アップロードのリストの表示、パートのアップロード、アップロードしたパートのアセンブル、およびアップロードの完了の個別の処理に分けられます。Complete Multipart Upload 処理が実行されると、オブジェクトが作成されます（該当する場合はバージョン管理されます）。

関連情報

"サーバ側の暗号化を使用"

# Upload Part - Copy 処理は、データソースとしての既存のオブジェクトからデータをコピーすることで、オブジェクトのパートをアップロードします。

Upload Part - Copy 処理には、すべての Amazon S3 REST API の動作が実装されています。

この要求は、で指定されたオブジェクトデータの読み取りと書き込みを行います `x-amz-copy-source-range` StorageGRID システム内で実行する。

次の要求ヘッダーがサポートされています。

- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`

サーバ側の暗号化を行うための要求ヘッダー

Initiate Multipart Upload 要求に SSE-C 暗号化を指定した場合は、各 Upload Part - Copy 要求に次の要求ヘッダーも含める必要があります。

- `x-amz-server-side-encryption-customer-algorithm`:指定します `AES256`。
- `x-amz-server-side-encryption-customer-key`：Initiate Multipart Upload要求で指定した暗号化キーを指定します。
- `x-amz-server-side-encryption-customer-key-MD5`：Initiate Multipart Upload要求で指定したMD5ダイジェストを指定します。

ソースオブジェクトがユーザ指定のキーを使用して暗号化されている場合（ SSE-C ）は、オブジェクトを復号化してコピーできるように、 Upload Part - Copy 要求に次の 3 つのヘッダーを含める必要があります。

- `x-amz-copy-source-server-side-encryption-customer-algorithm`:指定します `AES256`。
- `x-amz-copy-source-server-side-encryption-customer-key`:ソースオブジェクトの作成時に指定した暗号化キーを指定します
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`:ソースオブジェクトの作成時に指定したMD5ダイジェストを指定します。

> 指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。お客様提供の鍵を使用してオブジェクト・データを保護する前に'サーバ側の暗号化の使用に関する考慮事項を確認してください

バージョン管理

マルチパートアップロードは、アップロードの開始、アップロードのリストの表示、パートのアップロード、アップロードしたパートのアセンブル、およびアップロードの完了の個別の処理に分けられます。Complete Multipart Upload 処理が実行されると、オブジェクトが作成されます（該当する場合はバージョン管理されます）。

# Complete Multipart Upload 処理では、以前にアップロードされたパートをアセンブルすることで、オブジェクトのマルチパートアップロードを完了します。

## 競合の解決

同一キーに書き込む2つのクライアントなど'競合するクライアント要求は'最新のWINS形式で解決されます「latest-wins」評価のタイミングは、S3クライアントが処理を開始するタイミングではなく、StorageGRIDシステムが特定の要求を完了したタイミングに基づいています。

## オブジェクトのサイズ

StorageGRID は、サイズが最大5TBのオブジェクトをサポートします。

## 要求ヘッダー

。 `x-amz-storage-class` 要求ヘッダーがサポートされ、一致するILMルールで取り込み動作にDual commitまたはBalancedが指定されている場合にStorageGRID で作成されるオブジェクトコピーの数に影響します。

- `STANDARD`

  （デフォルト） ILM ルールで Dual commit オプションが使用されている場合、または Balanced オプションによって中間コピーが作成される場合に、デュアルコミットの取り込み処理を指定します。

- `REDUCED_REDUNDANCY`

  ILM ルールで Dual commit オプションが使用されている場合、または Balanced オプションによって中間コピーが作成される場合に、シングルコミットの取り込み処理を指定します。

  S3オブジェクトロックを有効にしてオブジェクトをバケットに取り込む場合は、を使用します `REDUCED_REDUNDANCY` オプションは無視されます。古い準拠バケットにオブジェクトを取り込む場合は、を参照してください `REDUCED_REDUNDANCY` オプションを指定するとエラーが返されます。StorageGRID では、常にデュアルコミットの取り込みが実行され、コンプライアンス要件が満たされます。

マルチパートアップロードが 15 日以内に完了しないと、非アクティブな処理としてマークされ、関連するすべてのデータがシステムから削除されます。

。 `ETag` 返される値はデータのMD5サムではなく、のAmazon S3 APIの実装に従います `ETag` マルチパートオブジェクトの値。

## バージョン管理

マルチパートアップロードは、この処理で完了します。バケットでバージョン管理が有効になっている場合は、マルチパートアップロードの完了時にオブジェクトのバージョンが作成されます。

バケットでバージョン管理が有効になっている場合は、一意です `versionId` は、格納されているオブジェクトのバージョンに対して自動的に生成されます。これ `versionId` は、を使用して応答としても返されます

`x-amz-version-id` 応答ヘッダー。

バージョン管理が一時停止中の場合は、オブジェクトバージョンはnullで格納されます `versionId` また、null バージョンがすでに存在する場合は上書きされます。

> バケットでバージョン管理が有効になっているときは、同じオブジェクトキーで同時に複数のマルチパートアップロードが実行されている場合でも、マルチパートアップロードが完了するたびに常に新しいバージョンが作成されます。バケットでバージョン管理が有効になっていないときは、マルチパートアップロードの開始後に、同じオブジェクトキーで別のマルチパートアップロードが開始されて先に完了することがあります。バージョン管理が有効になっていないバケットでは、最後に完了したマルチパートアップロードが優先されます。

レプリケーション、通知、またはメタデータ通知に失敗しました

マルチパートアップロードが行われるバケットでプラットフォームサービスが設定されている場合、関連するレプリケーション操作や通知操作が失敗してもマルチパートアップロードは正常に実行されます。

この状況が発生すると、 Total Events （ SMTT ）のアラームがグリッドマネージャで生成されます。Last Event メッセージに、通知が失敗した最後のオブジェクトについて、「 Failed to publish notifications for bucket-name object key 」と表示されます。（このメッセージを表示するには、* Nodes **>*_ Storage Node_**>* Events *を選択します。表の一番上にLast Eventが表示されます）。イベントメッセージは、にも表示されます `/var/local/log/bycast-err.log`。

テナントでは、オブジェクトのメタデータまたはタグを更新することで、失敗したレプリケーションまたは通知をトリガーできます。テナントでは、既存の値を再送信し、不要な変更を回避できます。

関連情報

"ILM を使用してオブジェクトを管理する"

エラー応答

StorageGRID システムでは、該当する S3 REST API の標準のエラー応答をすべてサポートしています。また、 StorageGRID の実装では、カスタム応答もいくつか追加されています。

サポートされている **S3 API** のエラーコード

| 名前 | **HTTP** ステータス |
| --- | --- |
| アクセスが拒否されました | 403 禁止 |
| BadDigest の略 | 400 不正な要求です |
| BucketAlreadyExists のようになりました | 409 競合 |
| BucketNotEmpty のように入力します | 409 競合 |
| IncompleteBody | 400 不正な要求です |

| 名前 | **HTTP** ステータス |
| --- | --- |
| 内部エラー | 500 Internal Server Error （内部サーバエラー） |
| InvalidAccessKeyId | 403 禁止 |
| アンヴァリッドドキュメント | 400 不正な要求です |
| InvalidBucketName の略 | 400 不正な要求です |
| InvalidBucketState の場合 | 409 競合 |
| InvalidDigest の略 | 400 不正な要求です |
| InvalidEncryptionAlgorithmError | 400 不正な要求です |
| InvalidPart | 400 不正な要求です |
| InvalidPartOrder | 400 不正な要求です |
| InvalidRange ：無効な範囲 | 416 リクエストされた範囲が適合しません |
| InvalidRequest | 400 不正な要求です |
| InvalidStorageClass | 400 不正な要求です |
| InvalidTag | 400 不正な要求です |
| InvalidURI | 400 不正な要求です |
| KeyTooLong の 2 つのグループがあります | 400 不正な要求です |
| MalformedXML の場合 | 400 不正な要求です |
| MetadataTooLarge | 400 不正な要求です |
| MethodNotAllowed のように入力します | 405 メソッドは許可されていません |
| MissingContentLength （ MissingContentLength ） | 411 長さが必要です |
| MissingRequestBodyError | 400 不正な要求です |
| MissingSecurityHeader | 400 不正な要求です |

| 名前 | **HTTP** ステータス |
| --- | --- |
| NoSuchBucket | 404 が見つかりません |
| NoSuchKey | 404 が見つかりません |
| NoSuchUpload | 404 が見つかりません |
| 実装なし | 501 は実装されていません |
| NoSuchBucketPolicy のようになります | 404 が見つかりません |
| ObjectLockConfigurationNotFoundError | 404 が見つかりません |
| PreconditionalFailed | 412 事前条件が失敗しました |
| RequestTimeTooSkewed | 403 禁止 |
| サービスを利用できません | 503 Service Unavailable （ 503 サービスが利用でき |
| SignatureDoesNotMatch のように指定します | 403 禁止 |
| TooManyBuckets | 400 不正な要求です |
| UserKeyMustBeSpecified | 400 不正な要求です |

**StorageGRID** カスタムのエラーコード

| 名前 | 説明 | **HTTP** ステータス |
| --- | --- | --- |
| XBucketLifecycleNotAllowed のようになりました | バケットライフサイクル設定は従来の準拠バケットには適用されません | 400 不正な要求です |
| XBucketPolicyParseException | 受信したバケットポリシー JSON を解析できませんでした。 | 400 不正な要求です |
| XCompliConflict | 準拠設定が古いため、処理が拒否されました。 | 403 禁止 |
| XCompliReducedRedundancyForbidden | レガシー準拠バケットでは冗長性の低下は許可されません | 400 不正な要求です |

| 名前 | 説明 | HTTP ステータス |
| --- | --- | --- |
| XMaxBucketPolicyLengthExceeded （ XMaxBucketLengthExceeded ） | ポリシーが許容される最大バケットポリシー長を超えています。 | 400 不正な要求です |
| XMissingInternalRequestHeader | 内部要求のヘッダーがありません。 | 400 不正な要求です |
| XNoSuchBucketCompliance です | 指定したバケットで従来の準拠が有効になっていません。 | 404 が見つかりません |
| XNotAcceptable | 要求に含まれている Accept ヘッダーの 1 つ以上を満たすことができませんでした。 | 406 は許容されません |
| XNotImplemented | 指定した要求の処理には、実装されていない機能が含まれます。 | 501 は実装されていません |

## StorageGRID の S3 REST API の処理

StorageGRID システム固有の処理が S3 REST API に追加されています。

### GET Bucket consistency 要求を実行します

GET Bucket consistency 要求を使用すると、特定のバケットに適用されている整合性レベルを確認できます。

新たに作成したオブジェクトに対しては、リードアフターライト整合性を保証するようにデフォルトの整合性制御が設定されます。

この処理を完了するには、s3：GetBucketConsistency権限またはrootアカウントが必要です。

要求例

```
GET /bucket?x-ntap-sg-consistency HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

応答

応答XMLで、 `<Consistency>` は次のいずれかの値を返します。

| 整合性制御 | 説明 |
| --- | --- |
| すべて | すべてのノードが即座にデータを受け取り、受け取れない場合は要求が失敗します。 |

| 整合性制御 | 説明 |
| --- | --- |
| strong-global | すべてのサイトのすべてのクライアント要求について、リードアフターライト整合性が保証されます。 |
| strong-site | 1 つのサイト内のすべてのクライアント要求について、リードアフターライト整合性が保証されます。 |
| read-after-new-write の場合 | （デフォルト）新規オブジェクトにはリードアフターライト整合性を、オブジェクトの更新には結果整合性を提供します。高可用性が確保され、データ保護が保証されます。Amazon S3の整合性に相当します。<br><br>• 注：存在しないオブジェクトに対してアプリケーションが HEAD 要求を使用すると、使用できないストレージノードがあると「 500 Internal Server Error 」が大量に返される可能性があります。これらのエラーを回避するには、 Amazon S3 と同様の整合性の保証が必要でない限り、整合性制御を「 available 」に設定します。 |
| available （ HEAD 処理は結果整合性） | 「 read-after-new-write 」整合性レベルと動作は同じですが、 HEAD 処理については結果整合性のみを提供します。ストレージ・ノードが使用できない場合 ' リードアフター・新規ライトよりもヘッド操作の可用性が高くなりますAmazon S3 の整合性と異なるのは HEAD 処理のみです。 |

応答例

```
HTTP/1.1 200 OK
Date: Fri, 18 Sep 2020 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/11.5.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<Consistency xmlns="http://s3.storagegrid.com/doc/2015-02-01/">read-after-
new-write</Consistency>
```

関連情報

"整合性制御"

### PUT Bucket consistency 要求

PUT Bucket consistency 要求を使用すると、バケットで実行される処理に適用する整合性レベルを指定できます。

新たに作成したオブジェクトに対しては、リードアフターライト整合性を保証するようにデフォルトの整合性制御が設定されます。

この処理を完了するには、s3：PutBucketConsistency権限またはrootアカウントが必要です。

リクエスト

。 `x-ntap-sg-consistency` パラメータには次のいずれかの値を指定する必要があります。

| 整合性制御 | 説明 |
| --- | --- |
| すべて | すべてのノードが即座にデータを受け取り、受け取れない場合は要求が失敗します。 |
| strong-global | すべてのサイトのすべてのクライアント要求について、リードアフターライト整合性が保証されます。 |
| strong-site | 1 つのサイト内のすべてのクライアント要求について、リードアフターライト整合性が保証されます。 |
| read-after-new-write の場合 | （デフォルト）新規オブジェクトにはリードアフターライト整合性を、オブジェクトの更新には結果整合性を提供します。高可用性が確保され、データ保護が保証されます。Amazon S3の整合性に相当します。<br>• 注：存在しないオブジェクトに対してアプリケーションが HEAD 要求を使用すると、使用できないストレージノードがあると「 500 Internal Server Error 」が大量に返される可能性があります。これらのエラーを回避するには、 Amazon S3 と同様の整合性の保証が必要でない限り、整合性制御を「 available 」に設定します。 |
| available （ HEAD 処理は結果整合性） | 「 read-after-new-write 」整合性レベルと動作は同じですが、 HEAD 処理については結果整合性のみを提供します。ストレージ・ノードが使用できない場合 ' リードアフター・新規ライトよりもヘッド操作の可用性が高くなりますAmazon S3 の整合性と異なるのは HEAD 処理のみです。 |

- 注： * 一般的には、「 read-after-new-write 」整合性制御値を使用する必要があります。要求が正しく機能しない場合は、可能であればアプリケーションクライアントの動作を変更します。または、 API 要求ごとに整合性制御を指定するようにクライアントを設定します。バケットレベルの整合性制御は最後の手段と考えてください。

要求例

```
PUT /bucket?x-ntap-sg-consistency=strong-global HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

関連情報

"整合性制御"

### GET Bucket last access time 要求

GET Bucket last access time 要求を使用すると、最終アクセス時間の更新が個々のバケットで有効になっているか無効になっているかを確認できます。

この処理を完了するには、s3：GetBucketLastAccessTime権限またはrootアカウントが必要です。

要求例

```
GET /bucket?x-ntap-sg-lastaccesstime HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

応答例

次の例では、バケットの最終アクセス時間の更新が有効になっています。

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/10.3.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<LastAccessTime xmlns="http://s3.storagegrid.com/doc/2015-02-01/">enabled
</LastAccessTime>
```

### PUT Bucket last access time 要求の場合

PUT Bucket last access time 要求を使用すると、最終アクセス時間の更新を個々のバケットで有効または無効にできます。最終アクセス時間の更新を無効にするとパフォーマンスが向上します。バージョン 10.3.0 以降で作成されたバケットに対しては、いずれもデフォルトで無効になります。

この処理を完了するには、バケットのs3：PutBucketLastAccessTime権限またはrootアカウントが必要です。

> StorageGRID バージョン 10.3 以降では、すべての新規バケットで最終アクセス時間の更新がデフォルトで無効になります。以前のバージョンの StorageGRID で作成されたバケットにこの新たなデフォルトの動作を適用する場合は、対象となるバケットごとに最終アクセス時間の更新を無効にする必要があります。Tenant Manager またはテナント管理 API の PUT Bucket last access time 要求、 * S3 * > * Buckets * > * Change Last Access Setting * チェックボックスを使用して、最終アクセス時間の更新を有効または無効にできます。

バケットで最終アクセス時間の更新が無効になっている場合、バケットの処理の動作は次のようになります。

- GET Object 、 GET Object ACL 、 GET Object Tagging 、 HEAD Object の各要求では、最終アクセス時間が更新されません。オブジェクトは、情報ライフサイクル管理（ ILM ）評価のキューに追加されません。
- メタデータのみを更新する PUT Object - Copy 要求と PUT Object Tagging 要求では、最終アクセス時間も更新されます。オブジェクトは ILM 評価のキューに追加されます。
- ソースバケットで最終アクセス時間の更新が無効になっている場合は、 PUT Object - Copy 要求でソースバケットの最終アクセス時間が更新されません。コピーされたオブジェクトは、ソースバケットの ILM 評価のキューに追加されません。ただし、デスティネーションについては、 PUT Object - Copy 要求で常に最終アクセス時間が更新されます。オブジェクトのコピーは、 ILM 評価のキューに追加されます。
- Complete Multipart Upload 要求では、最終アクセス時間が更新されます。完了したオブジェクトは、 ILM 評価のキューに追加されます。

例をリクエストする

この例では、バケットの最終アクセス時間を有効にしています。

```
PUT /bucket?x-ntap-sg-lastaccesstime=enabled HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

この例では、バケットの最終アクセス時間を無効にしています。

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

関連情報

"テナントアカウントを使用する"

### DELETE Bucket metadata notification configuration 要求

DELETE Bucket metadata notification configuration 要求では、設定 XML を削除することで、個々のバケットで検索統合サービスを無効化できます。

この処理を完了するには、バケットのs3：DeleteBucketMetadataNotification権限またはrootアカウントが必要です。

要求例

次の例は、バケットの検索統合サービスを無効にする方法を示しています。

```
DELETE /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

### GET Bucket metadata notification configuration 要求

GET Bucket metadata notification configuration 要求では、個々のバケットで検索統合を設定するために使用する設定 XML を読み出すことができます。

この処理を完了するには、s3：GetBucketMetadataNotification権限またはrootアカウントが必要です。

要求例

次の要求は、というバケットのメタデータ通知設定を読み出します `bucket`。

```
GET /bucket?x-ntap-sg-metadata-notification HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

応答

応答の本文には、バケットのメタデータ通知設定が含まれます。メタデータ通知設定では、バケットでの検索統合の設定を確認できます。つまり、どのオブジェクトにインデックスが付けられ、そのオブジェクトメタデータがどのエンドポイントに送信されるかを確認できます。

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:_region:account-
ID_:domain/_mydomain/myindex/mytype_</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

各メタデータ通知設定には、 1 つ以上のルールが含まれています。各ルールは、環境 がオブジェクトを指定し、 StorageGRID がオブジェクトメタデータを送信するデスティネーションを指定します。デスティネーションは、 StorageGRID エンドポイントの URN を使用して指定する必要があります。

| 名前 | 説明 | 必須 |
| --- | --- | --- |
| MetadataNotificationConfiguration のページです | メタデータ通知でオブジェクトとデスティネーションの指定に使用されるルール用のコンテナタグ。<br><br>1 つ以上の Rule 要素を含みます。 | はい。 |
| ルール | 指定したインデックスにメタデータを追加する必要があるオブジェクトを特定するルール用のコンテナタグ。<br><br>プレフィックスが重複しているルールは拒否されます。<br><br>MetadataNotificationConfiguration 要素に含まれています。 | はい。 |
| ID | ルールの一意の識別子。<br><br>Rule 要素に含まれています。 | いいえ |

| 名前 | 説明 | 必須 |
| --- | --- | --- |
| ステータス | Status には「 Enabled 」または「 Disabled 」を指定できます。無効になっているルールについては操作が実行されません。<br><br>Rule 要素に含まれています。 | はい。 |
| プレフィックス | プレフィックスと一致するオブジェクトにルールが適用され、そのメタデータが指定したデスティネーションに送信されます。<br><br>すべてのオブジェクトを照合するには、空のプレフィックスを指定します。<br><br>Rule 要素に含まれています。 | はい。 |
| 宛先 | ルールのデスティネーションのコンテナタグ。<br><br>Rule 要素に含まれています。 | はい。 |

| 名前 | 説明 | 必須 |
| --- | --- | --- |
| URN | オブジェクトメタデータが送信されるデスティネーションの URN 。次のプロパティを持つ StorageGRID エンドポイントの URN を指定する必要があります。<br><br>• `es` 3番目のエレメントである必要があります。<br>• URNの末尾に、メタデータが格納されるインデックスとタイプを、の形式で指定する必要があります `domain-name/myindex/mytype`。<br><br>エンドポイントは、 Tenant Manager またはテナント管理 API を使用して設定します。形式は次のとおりです。<br><br>• `arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype`<br>• `urn:mysite:es:::mydomain/myindex/mytype`<br><br>エンドポイントは設定 XML を送信する前に設定する必要があります。そうしないと、 404 エラーで設定が失敗します。<br><br>Urn は Destination 要素に含まれています。 | はい。 |

応答例

間に含まれるXML
`<MetadataNotificationConfiguration></MetadataNotificationConfiguration>` タグは、バケットに対して検索統合エンドポイントとの統合がどのように設定されているかを示します。次の例では、という名前のElasticsearchインデックスにオブジェクトメタデータが送信されています `current` と入力します `2017` という名前のAWSドメインでホストされている `records`。

```
HTTP/1.1 200 OK
Date: Thu, 20 Jul 2017 18:24:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/11.0.0
x-amz-request-id: 3832973499
Content-Length: 264
Content-Type: application/xml

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix>2017</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-
1:3333333:domain/records/current/2017</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

関連情報

"テナントアカウントを使用する"

### PUT Bucket metadata notification configuration 要求

PUT Bucket metadata notification configuration 要求を使用すると、個々のバケットで検索統合サービスを有効化できます。要求の本文に含めるメタデータ通知設定 XML では、デスティネーション検索インデックスにメタデータを送信するオブジェクトを指定します。

この処理を完了するには、バケットのs3：PutBucketMetadataNotification権限またはrootアカウントが必要です。

リクエスト

要求の本文にメタデータ通知設定が含まれている必要があります。各メタデータ通知設定には、 1 つ以上のルールが含まれています。各ルールは、環境 がオブジェクトを指定し、 StorageGRID がオブジェクトメタデータを送信するデスティネーションを指定します。

オブジェクトはオブジェクト名のプレフィックスでフィルタリングできます。たとえば、というプレフィックスのオブジェクトのメタデータを送信できます `/images` を1つのデスティネーションに、プレフィックスがのオブジェクトに追加します `/videos` 別のノードに移動します

プレフィックスが重複している設定は無効で、送信時に拒否されます。たとえば、プレフィックスがのオブジェクト用のルールを1つ含む設定などです `test` プレフィックスが付いたオブジェクトの2番目のルールです `test2` 許可されません。

デスティネーションは、 StorageGRID エンドポイントの URN を使用して指定する必要があります。エンドポイントは、メタデータ通知設定が送信されたときに存在している必要があります。存在していない場合、要

求がとして失敗します `400 Bad Request`。エラーメッセージ：`Unable to save the metadata notification (search) policy. The specified endpoint URN does not exist: URN.`

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:region:account-
ID:domain/mydomain/myindex/mytype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

次の表に、メタデータ通知設定 XML の要素を示します。

| 名前 | 説明 | 必須 |
| --- | --- | --- |
| MetadataNotificationConfiguration のページです | メタデータ通知でオブジェクトとデスティネーションの指定に使用されるルール用のコンテナタグ。<br><br>1 つ以上の Rule 要素を含みます。 | はい。 |
| ルール | 指定したインデックスにメタデータを追加する必要があるオブジェクトを特定するルール用のコンテナタグ。<br><br>プレフィックスが重複しているルールは拒否されます。<br><br>MetadataNotificationConfiguration 要素に含まれています。 | はい。 |
| ID | ルールの一意の識別子。<br><br>Rule 要素に含まれています。 | いいえ |

| 名前 | 説明 | 必須 |
| --- | --- | --- |
| ステータス | Status には「 Enabled 」または「 Disabled 」を指定できます。無効になっているルールについては操作が実行されません。<br><br>Rule 要素に含まれています。 | はい。 |
| プレフィックス | プレフィックスと一致するオブジェクトにルールが適用され、そのメタデータが指定したデスティネーションに送信されます。<br><br>すべてのオブジェクトを照合するには、空のプレフィックスを指定します。<br><br>Rule 要素に含まれています。 | はい。 |
| 宛先 | ルールのデスティネーションのコンテナタグ。<br><br>Rule 要素に含まれています。 | はい。 |

| 名前 | 説明 | 必須 |
| --- | --- | --- |
| URN | オブジェクトメタデータが送信されるデスティネーションの URN 。次のプロパティを持つ StorageGRID エンドポイントの URN を指定する必要があります。<br><br>• `es` 3番目のエレメントである必要があります。<br>• URNの末尾に、メタデータが格納されるインデックスとタイプを、の形式で指定する必要があります `domain-name/myindex/mytype`。<br><br>エンドポイントは、 Tenant Manager またはテナント管理 API を使用して設定します。形式は次のとおりです。<br><br>• `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype`<br>• `urn:mysite:es:::mydomain/myindex/mytype`<br><br>エンドポイントは設定 XML を送信する前に設定する必要があります。そうしないと、 404 エラーで設定が失敗します。<br><br>Urn は Destination 要素に含まれています。 | はい。 |

例をリクエストする

次の例は、バケットの検索統合を有効にする方法を示しています。この例では、すべてのオブジェクトのオブジェクトメタデータが同じデスティネーションに送信されます。

```
PUT /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
           <Urn>urn:sgws:es:::sgws-notifications/test1/all</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

この例では、プレフィックスに一致するオブジェクトのオブジェクトメタデータを指定します `/images` が1つのデスティネーションに送信され、プレフィックスに一致するオブジェクトのオブジェクトメタデータが送信されます `/videos` 2番目の送信先に送信されます。

```
PUT /graphics?x-ntap-sg-metadata-notification HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Images-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/images</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Videos-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/videos</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

関連情報

"テナントアカウントを使用する"

#### 検索統合サービスで生成される **JSON**

バケットで検索統合サービスを有効にすると、オブジェクトのメタデータまたはタグの追加、更新、削除が行われるたびに、 JSON ドキュメントが生成されてデスティネーションエンドポイントに送信されます。

次の例は、キーを含むオブジェクトの場合に生成されるJSONを示しています `SGWS/Tagging.txt` は、という名前のバケットに作成されます `test`。。 `test` バケットはバージョン管理されていないため、を使用します `versionId` タグが空です。

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region":"us-east-1"
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

メタデータ通知に含まれているオブジェクトメタデータ

次の表に、検索統合が有効になっている場合にデスティネーションエンドポイントに送信される JSON ドキュメント内のすべてのフィールドを示します。

ドキュメント名には、バケット名、オブジェクト名、バージョン ID （存在する場合）が含まれます。

| を入力します | 項目名 | 説明 |
| --- | --- | --- |
| バケットとオブジェクトの情報 | バケット | バケットの名前 |
| バケットとオブジェクトの情報 | キーを押します | オブジェクトキーの名前 |
| バケットとオブジェクトの情報 | versionId | バージョン管理されたバケット内のオブジェクトのオブジェクトバージョン |
| バケットとオブジェクトの情報 | リージョン | たとえば、バケットのリージョンのように指定します `us-east-1` |
| システムメタデータ | サイズ | HTTP クライアントから認識できるオブジェクトのサイズ（バイト） |
| システムメタデータ | MD5 | オブジェクトのハッシュ |
| ユーザメタデータ | メタデータ<br>*`key:value`* | オブジェクトのすべてのユーザメタデータをキーと値のペアとして格納 |

| を入力します | 項目名 | 説明 |
| --- | --- | --- |
| タグ | タグ<br>*key:value* | オブジェクトに対して定義されたすべてのオブジェクトタグをキーと値のペアとして使用します |

- 注： StorageGRID は、タグとユーザメタデータに対して、文字列または S3 イベント通知として Elasticsearch に日付と番号を渡します。これらの文字列を日付または数値として解釈するように Elasticsearch を設定するには、動的フィールドマッピングおよびマッピング日付形式に関する Elasticsearch の手順に従ってください。検索統合サービスを設定する前に、インデックスの動的フィールドマッピングを有効にする必要があります。ドキュメントにインデックスを付けた後は、インデックス内のドキュメントのフィールドタイプを編集できません。

**GET Storage Usage** 要求の略

GET Storage Usage 要求を使用すると、アカウントで使用しているストレージの総容量とアカウントに関連付けられているバケットごとの使用容量を確認できます。

アカウントとそのバケットで使用されているストレージの量は、でGET Service要求を変更して取得できます `x-ntap-sg-usage` クエリパラメータ。バケットによるストレージの使用量は、システムで処理される PUT 要求や DELETE 要求とは別に追跡されます。特にシステムの負荷が高い場合などは、使用量の値が要求の処理に基づく想定値と同じになるまでに少し時間がかかることがあります。

デフォルトでは、 StorageGRID は strong-global 整合性を使用して、使用状況の情報を取得します。strong-global 整合性が保証されていない場合、 StorageGRID は、強いサイトで整合性のある使用状況情報を取得しようとします。

この処理を完了するには、s3：ListAllMyBuckets権限またはrootアカウントが必要です。

要求例

```
GET /?x-ntap-sg-usage HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

応答例

次の例は、 2 つのバケットに 4 つのオブジェクトと 12 バイトのデータが格納されたアカウントです。各バケットには、 2 つのオブジェクトと 6 バイトのデータが格納されています。

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 00:49:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/10.2.0
x-amz-request-id: 727237123
Content-Length: 427
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<UsageResult xmlns="http://s3.storagegrid.com/doc/2015-02-01">
<CalculationTime>2014-11-19T05:30:11.000000Z</CalculationTime>
<ObjectCount>4</ObjectCount>
<DataBytes>12</DataBytes>
<Buckets>
<Bucket>
<Name>bucket1</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
<Bucket>
<Name>bucket2</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
</Buckets>
</UsageResult>
```

#### バージョン管理

には、格納されているすべてのオブジェクトバージョンが関連します `ObjectCount` および `DataBytes` 応答の値。削除マーカーはに追加されません `ObjectCount` 合計。

#### 関連情報

"整合性制御"

### 従来の準拠のためのバケット要求が廃止されました

従来の準拠機能で作成されたバケットの管理には、 StorageGRID S3 REST API の使用が必要になる場合があります。

#### コンプライアンス機能は廃止されました

以前のバージョンの StorageGRID で提供されていた StorageGRID 準拠機能は廃止され、 S3 オブジェクトロックに置き換えられました。

グローバル準拠設定を有効にしている場合は、StorageGRID 11.5にアップグレードすると、グローバルなS3オブジェクトロック設定が自動的に有効になります。準拠を有効にした新しいバケットは作成できなくなりま

した。ただし、必要に応じて、 StorageGRID S3 REST API を使用して、従来の準拠バケットを管理できます。

"S3 オブジェクトロックを使用する"

"ILM を使用してオブジェクトを管理する"

"ネットアップのナレッジベース： StorageGRID 11.5 でレガシー準拠バケットを管理する方法"

#### 廃止：準拠のための **PUT Bucket** 要求の変更

SGCompliance XML 要素は廃止されました。これまでは、この StorageGRID カスタム要素を PUT Bucket 要求のオプションの XML 要求の本文に含めて準拠バケットを作成できました。

> 以前のバージョンの StorageGRID で提供されていた StorageGRID 準拠機能は廃止され、 S3 オブジェクトロックに置き換えられました。

"S3 オブジェクトロックを使用する"

"ILM を使用してオブジェクトを管理する"

"ネットアップのナレッジベース： StorageGRID 11.5 でレガシー準拠バケットを管理する方法"

準拠を有効にした新しいバケットを作成することはできなくなりました。準拠バケットを新しく作成するために PUT Bucket 要求の変更を使用しようとすると、次のエラーメッセージが返されます。

```
The Compliance feature is deprecated.
Contact your StorageGRID administrator if you need to create new Compliant
buckets.
```

関連情報

"ILM を使用してオブジェクトを管理する"

"テナントアカウントを使用する"

#### 廃止予定： **GET Bucket compliance** 要求

GET Bucket compliance 要求は廃止されました。ただし、既存のレガシー準拠バケットに対して現在有効な準拠設定を引き続き確認することができます。

> 以前のバージョンの StorageGRID で提供されていた StorageGRID 準拠機能は廃止され、 S3 オブジェクトロックに置き換えられました。

"S3 オブジェクトロックを使用する"

"ILM を使用してオブジェクトを管理する"

"ネットアップのナレッジベース： StorageGRID 11.5 でレガシー準拠バケットを管理する方法"

この処理を完了するには、s3：GetBucketCompliance権限またはrootアカウントが必要です。

要求例

次の要求例では、という名前のバケットの準拠設定を確認できます `mybucket`。

```
GET /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

応答例

応答XMLで、 `<SGCompliance>` バケットで有効な準拠設定が表示されます。次の応答例では、バケットの準拠設定が示されており、各オブジェクトはグリッドに取り込まれてから 1 年間（ 525 、 600 分）保持されます。このバケットには現在リーガルホールドはありません。各オブジェクトは 1 年後に自動的に削除されます。

```
HTTP/1.1 200 OK
Date: <em>date</em>
Connection: <em>connection</em>
Server: StorageGRID/11.1.0
x-amz-request-id: <em>request ID</em>
Content-Length: <em>length</em>
Content-Type: application/xml

<SGCompliance>
  <RetentionPeriodMinutes>525600</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

| 名前 | 説明 |
| --- | --- |
| RetentionPeriodMinutes です | このバケットに追加されたオブジェクトの保持期間を分で指定します。保持期間は、オブジェクトがグリッドに取り込まれたときからの期間です。 |
| LegalHold のようになります | • True ：このバケットは、現在リーガルホールドの対象です。このバケット内のオブジェクトは、保持期間が過ぎたあとも、リーガルホールドが解除されるまで削除できません。<br>• False ：このバケットは、現在リーガルホールドの対象ではありません。このバケット内のオブジェクトは、保持期間が過ぎたら削除できます。 |

| 名前 | 説明 |
| --- | --- |
| 自動削除 | • True ：このバケット内のオブジェクトは、バケットがリーガルホールドの対象である場合を除き、保持期間が過ぎると自動的に削除されます。<br>• false ：このバケット内のオブジェクトは、保持期間が過ぎても自動的には削除されません。これらのオブジェクトを削除する必要がある場合は、手動で削除する必要があります。 |

エラー応答

バケットが準拠バケットとして作成されていない場合、応答のHTTPステータスコードはになります `404 Not Found`を返します `XNoSuchBucketCompliance`。

関連情報

"ILM を使用してオブジェクトを管理する"

"テナントアカウントを使用する"

廃止予定： **PUT Bucket compliance** 要求

PUT Bucket compliance 要求は廃止されました。ただし、この要求を引き続き使用して、既存のレガシー準拠バケットの準拠設定を変更できます。たとえば、既存のバケットをリーガルホールドの対象にしたり、バケットの保持期間を長くしたりできます。

以前のバージョンの StorageGRID で提供されていた StorageGRID 準拠機能は廃止され、 S3 オブジェクトロックに置き換えられました。

"S3 オブジェクトロックを使用する"

"ILM を使用してオブジェクトを管理する"

"ネットアップのナレッジベース： StorageGRID 11.5 でレガシー準拠バケットを管理する方法"

この処理を完了するには、s3：PutBucketCompliance権限またはrootアカウントが必要です。

PUT Bucket compliance 要求を発行する際は、準拠設定のすべてのフィールドに値を指定する必要があります。

要求例

次の要求例では、という名前のバケットの準拠設定を変更します `mybucket`。この例では、のオブジェクトが表示されています `mybucket` オブジェクトがグリッドに取り込まれてから1年間ではなく2年間（1、051、200分）保持されます。このバケットにリーガルホールドはありません。各オブジェクトは 2 年後に自動的に削除されます。

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization name</em>
Host: <em>host</em>
Content-Length: 152

<SGCompliance>
  <RetentionPeriodMinutes>1051200</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

| 名前 | 説明 |
| --- | --- |
| RetentionPeriodMinutes です | このバケットに追加されたオブジェクトの保持期間を分で指定します。保持期間は、オブジェクトがグリッドに取り込まれたときからの期間です。<br>• 注意： RetentionPeriodMinutes に新しい値を指定する場合は、バケットの現在の保持期間以上の値を指定する必要があります。設定したバケットの保持期間は、増やすことはできますが減らすことはできません。 |
| LegalHold のようになります | • True ：このバケットは、現在リーガルホールドの対象です。このバケット内のオブジェクトは、保持期間が過ぎたあとも、リーガルホールドが解除されるまで削除できません。<br>• False ：このバケットは、現在リーガルホールドの対象ではありません。このバケット内のオブジェクトは、保持期間が過ぎたら削除できます。 |
| 自動削除 | • True ：このバケット内のオブジェクトは、バケットがリーガルホールドの対象である場合を除き、保持期間が過ぎると自動的に削除されます。<br>• false ：このバケット内のオブジェクトは、保持期間が過ぎても自動的には削除されません。これらのオブジェクトを削除する必要がある場合は、手動で削除する必要があります。 |

準拠設定の整合性レベル

PUT Bucket compliance 要求によって S3 バケットの準拠設定を更新すると、 StorageGRID は、グリッド全体のバケットのメタデータを更新しようとします。デフォルトでは、 StorageGRID は * strong-global * 整合性レベルを使用し、バケットのメタデータを含むすべてのデータセンターサイトおよびストレージノードで、変更された準拠設定のリードアフターライト整合性を保証します。

データセンターサイトまたはサイトの複数のストレージノードが利用できないために、StorageGRIDが「strong-global」の整合性レベルを保証できない場合は、応答のHTTPステータスコードがになります `503 Service Unavailable.`

この応答を受け取った場合は、必要なストレージサービスをできるだけ早く利用可能にするために、グリッド管理者に問い合わせる必要があります。グリッド管理者が各サイトで十分な数のストレージノードを利用可能にできない場合は、テクニカルサポートから、 * strong-site * 整合性レベルを強制的に適用することで、失敗した要求を再試行するよう指示される場合があります。

> テクニカルサポートから指示があった場合や、このレベルを使用した場合の影響を理解している場合を除き、 PUT Bucket compliance で * strong-site * 整合性レベルを強制的に適用することは避けてください。

整合性レベルを * strong-site * 」に下げると、 StorageGRID は、サイト内のクライアント要求に対してのみ、更新された準拠設定のリードアフターライト整合性を保証します。そのため、すべてのサイトおよびストレージノードが利用可能になるまでの間、 StorageGRID システムにはこのバケットに対して複数の異なる設定が一時的に存在することになる場合があります。整合性のない設定を使用すると、予期せぬ望ましくない動作が生じる可能性がありますたとえば、あるバケットをリーガルホールドの対象にして、低い整合性レベルを強制的に適用すると、一部のデータセンターサイトでバケットの以前の準拠設定（つまり、リーガルホールドの対象外の状態）が引き続き適用される場合があります。したがって、リーガルホールドの対象と思われるオブジェクトは、保持期間が経過すると、ユーザによって削除される場合と、 AutoDelete によって削除される場合があります。

strong-site *整合性レベルを強制的に適用するには、PUT Bucket compliance要求を再発行し、を含めてください `Consistency-Control` HTTP要求ヘッダー。

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Consistency-Control: strong-site
```

エラー応答

- バケットが準拠バケットとして作成されていない場合、応答のHTTPステータスコードはになります `404 Not Found`。
- 状況 `RetentionPeriodMinutes` 要求がバケットの現在の保持期間よりも短い場合、HTTPステータスコードはになります `400 Bad Request`。

関連情報

"廃止：準拠のための PUT Bucket 要求の変更"

"テナントアカウントを使用する"

"ILM を使用してオブジェクトを管理する"

## バケットとグループのアクセスポリシー

StorageGRID では、 Amazon Web Services （ AWS ）ポリシー言語を使用して、 S3 テナントによるバケットおよびバケット内のオブジェクトへのアクセスを制御できます。StorageGRID システムには、 S3 REST API ポリシー言語のサブセットが実装され

ています。S3 API のアクセスポリシーは JSON 形式で記述されます。

アクセスポリシーの概要

StorageGRID では 2 種類のアクセスポリシーがサポートされています。

- * バケットポリシー * 。 GET Bucket policy 、 PUT Bucket policy 、 DELETE Bucket policy の各 S3 API 処理を使用して設定します。バケットポリシーはバケットに関連付けられ、バケットとそのオブジェクトへのバケット所有者アカウントやその他のアカウントのユーザによるアクセスを制御するために使用されます。バケットポリシー環境 は 1 つのバケットのみで、場合によっては複数のグループに分かれています。
- * グループポリシー * 。 Tenant Manager またはテナント管理 API を使用して設定します。グループポリシーはアカウントのグループに関連付けられ、そのアカウントが所有する特定のリソースにそのグループがアクセスできるように設定されます。グループポリシー環境 は 1 つのグループに限定され、場合によっては複数のバケットに適用されます。

StorageGRID のバケットとグループのポリシーは、 Amazon が定義している特定の文法に従って記述されます。各ポリシーは一連のステートメントからなり、各ステートメントは次の要素で構成されます。

- ステートメント ID （ SID ）（オプション）
- 効果
- プリンシパル / NotPrincipal
- リソース / メモリソース
- アクション / NotAction
- Condition （オプション）

次の構造を使用して、権限を指定するポリシーステートメントが構築されます。 <Effect> を付与して、 <Condition> に該当する場合に <Principal> に <Resource> に対する <Action> の実行を許可または拒否します。

各ポリシー要素は、特定の機能に使用されます。

| 要素（ **Element** ） | 説明 |
| --- | --- |
| SID | Sid 要素はオプションです。SID は、ユーザの概要 としてのみ使用されます。StorageGRID システムに格納はされますが、システムで解釈されません。 |
| 効果 | Effect 要素では、指定した処理を許可するか拒否するかを指定します。Action 要素でサポートされるキーワードを使用して、バケットやオブジェクトで許可（または拒否）する処理を指定する必要があります。 |

| 要素（ **Element** ） | 説明 |
| --- | --- |
| プリンシパル / NotPrincipal | ユーザ、グループ、およびアカウントに特定のリソースへのアクセスと特定の操作の実行を許可できます。要求に S3 の署名が含まれていない場合は、ワイルドカード文字（ * ）をプリンシパルとして指定することで匿名アクセスが許可されます。デフォルトでは、アカウントが所有するリソースへのアクセスは root アカウントにのみ許可されます。<br><br>Principal 要素を指定する必要があるのはバケットポリシーだけです。グループポリシーの場合は、ポリシーが関連付けられたグループが暗黙的にプリンシパルになります。 |
| リソース / メモリソース | Resource 要素では、バケットとオブジェクトを指定します。Amazon リソースネーム（ ARN ）を使用してリソースを指定し、バケットやオブジェクトに対する権限を許可または拒否することができます。 |
| アクション / NotAction | 権限は Action 要素と Effect 要素の 2 つで構成されます。グループがリソースを要求すると、リソースへのアクセスが許可または拒否されます。権限を明示的に割り当てていないかぎりアクセスは拒否されますが、明示的な拒否を使用して別のポリシーで付与された権限を上書きすることもできます。 |
| 条件 | Condition 要素はオプションです。条件を使用すると、ポリシーを適用する条件を示す式を作成できます。 |

Action 要素では、ワイルドカード文字（ * ）を使用してすべての処理または処理のサブセットを指定できます。たとえば、次の Action の値は、 s3 ： GetObject 、 s3 ： PutObject 、 s3 ： DeleteObject などの権限に一致します。

```
s3:*Object
```

Resource 要素では、ワイルドカード文字（ \ * ）および（？）を使用できます。アスタリスク（ * ）は 0 文字以上の文字に一致し、疑問符（？）は 0 文字以上の文字に一致します。 任意の 1 文字に一致します。

Principal 要素では、匿名アクセスを設定してすべてのユーザに権限を付与する場合を除き、ワイルドカード文字はサポートされません。たとえば、 Principal の値としてワイルドカード（ * ）を設定します。

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

次の例では、 Effect 、 Principal 、 Action 、および Resource の各要素を使用して記述します。次の例は、「許可」の効果を使用してプリンシパル、adminグループを指定したバケットポリシーのステートメントを示しています `federated-group/admin` 財務グループなどです `federated-group/finance`、アクションを

実行する権限 `s3:ListBucket` をバケットにインストールします `mybucket` そしてアクション `s3:GetObject` そのバケット内のすべてのオブジェクト。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::27233906934684427525:federated-group/admin",
          "arn:aws:iam::27233906934684427525:federated-group/finance"
        ]
      },
      "Action": [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:iam:s3:::mybucket",
        "arn:aws:iam:s3:::mybucket/*"
      ]
    }
  ]
}
```

バケットポリシーのサイズの上限は 20 、 480 バイトで、グループポリシーのサイズの上限は 5 、 120 バイトです。

関連情報

"テナントアカウントを使用する"

ポリシーの整合性制御設定

デフォルトでは、グループポリシーに対するすべての更新の整合性レベルは結果整合性です。グループポリシーが整合した状態になっても、ポリシーキャッシュのために、変更が有効になるまでさらに 15 分を要することがあります。デフォルトでは、バケットポリシーに対するすべての更新の整合性レベルも結果整合性です。

バケットポリシーの更新の整合性保証は必要に応じて変更できます。たとえば、セキュリティ上の理由から、できるだけ早くバケットポリシーの変更を有効にしなければならない場合があります。

この場合は、を設定できます `Consistency-Control` PUT Bucket policy要求のヘッダーを指定するか、PUT Bucket整合性要求を使用できます。この要求で整合性制御を変更する場合は、値「 * all * 」を使用して最高レベルのリードアフターライト整合性を保証する必要があります。それ以外の整合性制御値を PUT Bucket consistency 要求のヘッダーで指定すると、要求は拒否されます。PUT Bucket policy 要求でそれ以外の値を指定した場合は、値が無視されます。バケットポリシーが整合した状態になっても、ポリシーキャッシュのために、変更が有効になるまでさらに 8 秒を要することがあります。

新しいバケットポリシーを速やかに有効にするために整合性レベルを * all * に設定する場合は、処理が完了したあとに必ずバケットレベルの制御を元の値に戻してください。そうしないと、それ以降のすべてのバケット要求で * all * 設定が使用されます。

ポリシーステートメントで**ARN**を使用する

ポリシーステートメントでは、 Principal 要素と Resource 要素で ARN を使用します。

- S3 リソースの ARN の指定には次の構文を使用します。

```
arn:aws:s3:::bucket-name
arn:aws:s3:::bucket-name/object_key
```

- アイデンティティリソースの ARN （ユーザおよびグループ）の指定には次の構文を使用します。

```
arn:aws:iam::account_id:root
arn:aws:iam::account_id:user/user_name
arn:aws:iam::account_id:group/group_name
arn:aws:iam::account_id:federated-user/user_name
arn:aws:iam::account_id:federated-group/group_name
```

その他の考慮事項：

- オブジェクトキーの一部にワイルドカードとしてアスタリスク（ * ）を使用すると、 0 文字以上の文字に一致します。
- オブジェクトキーで指定できる国際文字は、 JSON UTF-8 形式または JSON \u エスケープシーケンスを使用してエンコードする必要があります。パーセントエンコーディングはサポートされていません。

  "RFC 2141 の URN 構文"

  PUT Bucket policy 処理の HTTP 要求の本文は、 charset=UTF-8 でエンコードする必要があります。

ポリシーでのリソースの指定

ポリシーステートメントでは、 Resource 要素を使用して、権限を許可または拒否するバケットやオブジェクトを指定できます。

- Resource 要素はポリシーの各ステートメントに必要です。ポリシーでは、リソースは要素で示されます `Resource`または、 `NotResource` 除外のため。
- リソースは S3 リソースの ARN で指定します。例：

```
"Resource": "arn:aws:s3:::mybucket/*"
```

- オブジェクトキーの内部でポリシー変数を使用することもできます。例：

```
"Resource": "arn:aws:s3:::mybucket/home/${aws:username}/*"
```

- グループポリシーの作成時は、まだ存在しないバケットもリソースの値で指定することができます。

関連情報

"ポリシーでの変数の指定"

ポリシーでのプリンシパルの指定

ポリシーステートメントでリソースへのアクセスを許可または拒否するユーザ、グループ、またはテナントアカウントを指定するには、 Principal 要素を使用します。

- バケットポリシーの各ポリシーステートメントには、 Principal 要素を含める必要があります。グループはプリンシパルとみなされるため、グループポリシーのポリシーステートメントには Principal 要素は不要です。
- ポリシーでは ' 主体は ' 主 (Principal)' または除外のためにもう 1 つの "NotPrincipal" という要素によって示されます
- ID または ARN を使用してアカウントベースのアイデンティティを指定する必要があります。

```
"Principal": { "AWS": "account_id"}
"Principal": { "AWS": "identity_arn" }
```

- 次の例では、テナントアカウント ID 27233906934684427525 を使用しています。この場合、 root アカウントとそのすべてのユーザが含まれます。

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

- root アカウントのみを指定する場合は次のようになります。

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:root" }
```

- 特定のフェデレーテッドユーザ（「 Alex 」）を指定する場合は次のようになります。

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

- 特定のフェデレーテッドグループ（「 Managers 」）のみを指定する場合は次のようになります。

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

- 匿名プリンシパルを指定する場合は次のようになります。

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

- あいまいさを排除するために、ユーザ名の代わりに UUID を使用できます。

```
arn:aws:iam::27233906934684427525:user-uuid/de305d54-75b4-431b-adb2-
eb6b9e546013
```

  たとえば、Alexが組織とユーザ名を退職するとします `Alex` が削除されました。新しいAlexが組織に参加し、同じが割り当てられている場合 `Alex` ユーザ名。元のユーザに付与された権限が、新しいユーザに意図せず継承されることがあります。

- バケットポリシーの作成時は、まだ存在しないグループ / ユーザの名前もプリンシパルの値で指定することができます。

ポリシーで権限を指定する

ポリシーでは、 Action 要素を使用してリソースに対する権限を許可または拒否します。ポリシーには、「 Action 」要素で示される一連の権限、または除外する「 NotAction 」要素で指定できる一連の権限があります。それぞれが特定の S3 REST API 処理に対応しています。

次の表に、バケットに適用される権限とオブジェクトに適用される権限を示します。

Amazon S3 では、 PUT と DELETE Bucket の両方のレプリケーション処理に s3 ： PutReplicationConfiguration 権限が使用されるようになりました。StorageGRID では、元の Amazon S3 仕様に一致する個別の権限が各アクションに使用されます。

DELETE は、 PUT を使用して既存の値を上書きするときに実行されます。

バケットに適用される権限

| 権限 | **S3 REST API** の処理 | **StorageGRID** のカスタム |
|---|---|---|
| S3 ： CreateBucket を指定します | PUT Bucket の場合 | |
| S3 ： DeleteBucket | バケットを削除します | |
| S3 ： DeleteBucketMetadataNotification | バケットのメタデータ通知設定を削除します | はい。 |
| S3 ： DeleteBucketPolicy | バケットポリシーを削除 | |
| S3 ： DeleteReplicationConfiguration | バケットレプリケーションを削除します | はい。 PUT および DELETE の権限は分離されています |

| 権限 | **S3 REST API** の処理 | **StorageGRID** のカスタム |
| --- | --- | --- |
| S3 ： GetBucketAcl | GET Bucket ACL の場合 | |
| S3 ： GetBucketCompliance | GET Bucket compliance （廃止） | はい。 |
| S3 ： GetBucketConsistency | GET Bucket consistency | はい。 |
| S3 ： GetBucketCORS | GET Bucket CORS | |
| S3 ： GetEncryptionConfiguration | GET Bucket encryption | |
| S3 ： GetBucketLastAccessTime | GET Bucket last access time の場合 | はい。 |
| S3 ： GetBucketLocation | GET Bucket location の各ノードで使用でき | |
| S3 ： GetBucketMetadataNotification | GET Bucket metadata notification configuration | はい。 |
| S3 ： GetBucketNotification | GET Bucket notification | |
| S3 ： GetBucketObjectLockConfiguration | オブジェクトロック設定の取得 | |
| S3 ： GetBucketPolicy | GET Bucket policy の場合 | |
| S3 ： GetBucketTagging | GET Bucket tagging | |
| S3 ： GetBucketVersioning | GET Bucket versioning | |
| S3 ： GetLifecycleConfiguration | GET Bucket lifecycle | |
| S3 ： GetReplicationConfiguration | GET Bucket replication | |
| S3 ： ListAllMyBuckets | • GET Service の略<br>• GET Storage Usage の略 | GET Storage Usage の場合は、はい |
| S3 ： ListBucket | • GET Bucket （ List Objects ）<br>• HEAD Bucket （ヘッドバケット）<br>• POST Object restore の実行 | |

| 権限 | **S3 REST API** の処理 | **StorageGRID** のカスタム |
| --- | --- | --- |
| S3 ： ListBucketMultipartUploads | • マルチパートアップロードをリストします<br>• POST Object restore の実行 | |
| S3 ： ListBucketVersions | GET Bucket versions （バケットバージョンの取得 | |
| S3 ： PutBucketCompliance | PUT Bucket compliance （廃止） | はい。 |
| S3 ： PutBucketConsistency | PUT Bucket consistency | はい。 |
| S3 ： PutBucketCORS | • バケットの CORS を削除†<br>• PUT Bucket CORS | |
| S3 ： PutEncryptionConfiguration | • バケットの暗号化を削除<br>• PUT Bucket encryption | |
| S3 ： PutBucketLastAccessTime | PUT Bucket last access time のように指定します | はい。 |
| S3 ： PutBucketMetadataNotification | PUT Bucket metadata notification configuration のコマンドです | はい。 |
| S3 ： PutBucketNotification | PUT Bucket notification | |
| S3 ： PutBucketObjectLockConfiguration | PUT Bucketにで接続します `x-amz-bucket-object-lock-enabled: true` 要求ヘッダー（s3：CreateBucket権限も必要） | |
| S3 ： PutBucketPolicy | PUT Bucket policy の場合 | |
| S3 ： PutBucketTagging | • バケットタグを削除†<br>• PUT Bucket tagging | |
| S3 ： PutBucketVersioning | PUT Bucket versioning の場合 | |
| S3 ： PutLifecycleConfiguration | • バケットライフサイクルを削除†<br>• PUT Bucket lifecycle の場合 | |

| 権限 | **S3 REST API** の処理 | **StorageGRID** のカスタム |
| --- | --- | --- |
| S3 ： PutReplicationConfiguration | PUT Bucket replication | はい。 PUT および DELETE の権限は分離されています |

オブジェクトに適用される権限

| 権限 | **S3 REST API** の処理 | **StorageGRID** のカスタム |
| --- | --- | --- |
| S3 ： AbortMultipartUpload | • マルチパートアップロードを中止します<br>• POST Object restore の実行 | |
| S3 ： DeleteObject | • オブジェクトを削除します<br>• 複数のオブジェクトを削除します<br>• POST Object restore の実行 | |
| S3 ： DeleteObjectTagging | オブジェクトのタグ付けを削除します | |
| S3 ： DeleteObjectVersionTagging | DELETE Object Tagging （オブジェクトの特定のバージョン） | |
| S3 ： DeleteObjectVersion | DELETE Object （オブジェクトの特定のバージョン） | |
| S3 ： GetObject | • オブジェクトの取得<br>• HEAD Object の実行<br>• POST Object restore の実行 | |
| S3 ： GetObjectAcl | GET Object ACL の場合 | |
| S3 ： GetObjectLegalHold | オブジェクトのリーガルホールドを取得します | |
| S3 ： GetObjectRetention | GET Object retention のことです | |
| S3 ： GetObjectTagging | GET Object Tagging の場合 | |
| S3 ： GetObjectVersionTagging | GET Object Tagging （オブジェクトの特定のバージョン） | |

| 権限 | **S3 REST API** の処理 | **StorageGRID** のカスタム |
| --- | --- | --- |
| S3 ： GetObjectVersion | GET Object （オブジェクトの特定のバージョン） | |
| S3 ： ListMultipartUploadParts | パーツを表示し、 POST Object restore を実行します | |
| S3 ： PutObject | • PUT Object の場合<br>• PUT Object - Copy の各コマンドを実行します<br>• POST Object restore の実行<br>• マルチパートアップロードを開始します<br>• Complete Multipart Upload の実行<br>• パーツをアップロードします<br>• パーツのアップロード - コピー | |
| S3 ： PutObjectLegalHold | オブジェクトのリーガルホールドを適用します | |
| S3 ： PutObjectRetention | PUT Object retention のことです | |
| S3 ： PutObjectTagging | PUT Object Tagging の場合 | |
| S3 ： PutObjectVersionTagging | PUT Object Tagging （オブジェクトの特定のバージョン） | |
| S3 ： PutOverwriteObject | • PUT Object の場合<br>• PUT Object - Copy の各コマンドを実行します<br>• PUT Object tagging<br>• オブジェクトのタグ付けを削除します<br>• Complete Multipart Upload の実行 | はい。 |
| S3 ： RestoreObject | POST Object restore の実行 | |

**PutOverwriteObject**権限の使用

s3 ： PutOverwriteObject 権限は、オブジェクトの作成または更新を行う環境 処理のカスタムの

StorageGRID 権限です。この権限の設定により、オブジェクトのデータ、ユーザ定義メタデータ、または S3 オブジェクトのタグをクライアントが上書きできるかどうかが決まります。

この権限で可能な設定は次のとおりです。

- * allow * ：クライアントはオブジェクトを上書きできます。これがデフォルト設定です。
- * Deny * ：クライアントはオブジェクトを上書きできません。PutOverwriteObject 権限が Deny に設定されている場合の動作は次のとおりです。
  - 同じパスで既存のオブジェクトが見つかった場合は、次の手順を実行します。
    - オブジェクトのデータ、ユーザ定義メタデータ、または S3 オブジェクトのタグを上書きすることはできません。
    - 実行中の取り込み処理はすべてキャンセルされ、エラーが返されます。
    - S3 バージョン管理が有効になっている場合は、 Deny に設定すると、 PUT Object tagging 処理または DELETE Object tagging 処理によって、オブジェクトとその最新ではないバージョンの TagSet が変更されなくなります。
  - 既存のオブジェクトが見つからない場合は、この権限の設定は影響しません。
- この権限がない場合、 Allow が設定されたものと同じ結果になります。

> 現在の S3 ポリシーで上書きが許可されていても、 PutOverwriteObject 権限が Deny に設定されている場合は、オブジェクトのデータ、ユーザ定義メタデータ、またはオブジェクトのタグをクライアントが上書きすることはできません。また、[クライアントの変更を禁止する*]チェックボックス（構成>*グリッドオプション*）がオンになっている場合は、この設定がPutOverwriteObject権限の設定よりも優先されます。

関連情報

"S3 グループポリシーの例"

ポリシーで条件を指定する

条件は、ポリシーが有効になるタイミングを定義します。条件は演算子とキーと値のペアで構成されます。

条件はキーと値のペアを使用して評価されます。Condition 要素には複数の条件を指定でき、各条件には複数のキーと値のペアを含めることができます。条件ブロックの形式は次のとおりです。

```
Condition: {
     <em>condition_type</em>: {
          <em>condition_key</em>: <em>condition_values</em>
```

次の例では、 IpAddress 条件で SourceIp 条件キーを使用しています。

```
"Condition": {
    "IpAddress": {
      "aws:SourceIp": "54.240.143.0/24"
        ...
},
        ...
```

サポートされる条件演算子は次の

条件演算子は次のように分類されます。

- 文字列
- 数値
- ブール値
- IP アドレス
- Null チェック

| 条件演算子 | 説明 |
| --- | --- |
| StringEquals | キーを文字列値と比較し、完全一致であるかを確認します（大文字と小文字の区別あり）。 |
| StringNotEquals | キーを文字列値と比較し、不一致であるかを確認します（大文字と小文字の区別あり）。 |
| StringEqualsIgnoreCase | キーを文字列値と比較し、完全一致であるかを確認します（大文字と小文字の区別なし）。 |
| StringNotEqualsIgnoreCase | キーを文字列値と比較し、不一致であるかを確認します（大文字と小文字の区別なし）。 |
| StringLike | キーを文字列値と比較し、完全一致であるかを確認します（大文字と小文字の区別あり）。含めることができる * と？ワイルドカード文字を使用できます。 |
| StringNotLike | キーを文字列値と比較し、不一致であるかを確認します（大文字と小文字の区別あり）。含めることができる * と？ワイルドカード文字を使用できます。 |
| NumericEquals （数値機器） | キーを数値と比較し、完全一致であるかを確認します。 |
| NumericNotEquals | キーを数値と比較し、不一致であるかを確認します。 |

| 条件演算子 | 説明 |
| --- | --- |
| NumericGreaterThan | キーを数値と比較し、「大なり」の一致であるかを確認します。 |
| NumericGreaterThanEquals | キーを数値と比較し、「大なり」または「等しい」の一致であるかを確認します。 |
| NumericLessThan | キーを数値と比較し、「より小さい」の一致であるかを確認します。 |
| NumericLessThanEquals | キーを数値と比較し、「より小さい」または「等しい」の一致であるかを確認します。 |
| ブール値 | キーをブール値と比較し、「 true 」または「 false 」の一致であるかを確認します。 |
| IP アドレス | キーを IP アドレスまたは IP アドレスの範囲と比較します。 |
| NotIpAddress | キーを IP アドレスまたは IP アドレスの範囲と比較し、不一致であるかを確認します。 |
| null | 現在の要求コンテキストに条件キーが存在するかどうかを確認します。 |

サポートされている条件キー

| カテゴリ | 適用される条件キー | 説明 |
| --- | --- | --- |
| IP 演算子 | AWS ： sourceIP | 要求の送信元の IP アドレスと比較します。バケットまたはオブジェクトの処理に使用できます。<br>• 注： S3 要求が管理ノードおよびゲートウェイノード上のロードバランササービスを介して送信された場合は、ロードバランササービスのアップストリームの IP アドレスと比較します。<br>• 注 * ：サードパーティ製の非透過型ロードバランサを使用する場合は、そのロードバランサの IP アドレスと比較します。任意 `X-Forwarded-For` 有効性を確認できないため、ヘッダーは無視されます。 |

| カテゴリ | 適用される条件キー | 説明 |
| --- | --- | --- |
| リソース / ID | AWS ：ユーザ名 | 要求の送信者のユーザ名と比較します。バケットまたはオブジェクトの処理に使用できます。 |
| S3：ListBucketと<br><br>S3：ListBucketVersions権限 | S3 ：デリミタ | GET Bucket 要求または GET Bucket Object versions 要求で指定された delimiter パラメータと比較します。 |
| S3：ListBucketと<br><br>S3：ListBucketVersions権限 | S3 ： max-keys | GET Bucket 要求または GET Bucket Object versions 要求で指定された max-keys パラメータと比較します。 |
| S3：ListBucketと<br><br>S3：ListBucketVersions権限 | S3 ：プレフィックス | GET Bucket 要求または GET Bucket Object versions 要求で指定された prefix パラメータと比較します。 |

ポリシーでの変数の指定

ポリシーで変数を使用すると、該当するポリシーの情報を設定できます。でポリシー変数を使用できます `Resource` の要素と文字列比較 `Condition` 要素（Element）：

この例では、変数を使用しています `${aws:username}` はResource要素の一部です。

```
"Resource": "arn:aws:s3:::_bucket-name/home_/${aws:username}/*"
```

この例では、変数を使用しています `${aws:username}` は、条件ブロックの条件値の一部です。

```
"Condition": {
    "StringLike": {
      "s3:prefix": "${aws:username}/*"
        ...
},
        ...
```

| 変数（ **Variable** ） | 説明 |
| --- | --- |
| `${aws:SourceIp}` | SourceIp キーを指定の変数として使用します。 |
| `${aws:username}` | username キーを指定の変数として使用します。 |

| 変数（ **Variable** ） | 説明 |
| --- | --- |
| `${s3:prefix}` | サービス固有のプレフィックスキーを指定の変数として使用します。 |
| `${s3:max-keys}` | サービス固有の max-keys キーを指定の変数として使用します。 |
| `${*}` | 特殊文字です。文字をリテラル * 文字として使用します。 |
| `${?}` | 特殊文字です。文字をリテラル文字として使用しますか？を押します。 |
| `${$}` | 特殊文字です。文字「 $ 」をリテラル文字として使用します。 |

特別な処理を必要とするポリシーの作成

ポリシーで付与される権限によって、アカウントの root ユーザがロックアウトされるなど、セキュリティや継続的な運用に支障が生じることがあります。StorageGRID の S3 REST API の実装では、ポリシーの検証時の制限は Amazon よりも厳しくありませんが、評価時は同等の制限が適用されます。

| **Policy** 概要 の略 | ポリシータイプ | **Amazon** の動作 | **StorageGRID** の動作 |
| --- | --- | --- | --- |
| 自身に対し、 root アカウントに対するすべての権限を拒否する | バケット | 有効で適用されるが、 S3 バケットのすべてのポリシー処理に対する権限は引き続き root ユーザアカウントに付与される | 同じ |
| 自身に対しユーザ / グループに対するすべての権限を拒否する | グループ | 有効で適用されます | 同じ |
| 外部アカウントグループに対し任意の権限を許可します | バケット | 無効なプリンシパルです | 有効だが、 S3 バケットのすべてのポリシー処理に対する権限をポリシーで許可すると 405 Method Not Allowed エラーが返されます |
| 外部アカウントの root またはユーザに任意の権限を許可します | バケット | 有効だが、 S3 バケットのすべてのポリシー処理に対する権限をポリシーで許可すると 405 Method Not Allowed エラーが返されます | 同じ |

| Policy 概要 の略 | ポリシータイプ | Amazon の動作 | StorageGRID の動作 |
| --- | --- | --- | --- |
| すべてのユーザにすべての処理に対する権限を許可します | バケット | 有効だが、外部アカウントの root およびユーザについては、 S3 バケットのすべてのポリシー処理に対する権限で 405 Method Not Allowed エラーが返されます | 同じ |
| すべてのユーザに対してすべての処理に対する権限を拒否する | バケット | 有効で適用されるが、 S3 バケットのすべてのポリシー処理に対する権限は引き続き root ユーザアカウントに付与される | 同じ |
| プリンシパルとして新規のユーザまたはグループを指定します | バケット | 無効なプリンシパルです | 有効 |
| リソースとして新規の S3 バケットを指定する必要があります | グループ | 有効 | 同じ |
| プリンシパルとしてローカルグループを指定します | バケット | 無効なプリンシパルです | 有効 |
| ポリシーでは、非所有者アカウント（匿名アカウントを含む）にオブジェクトを PUT する権限が付与されます | バケット | 有効。オブジェクトは作成者アカウントによって所有され、バケットポリシーは適用されません。作成者アカウントは、オブジェクトの ACL を使用してオブジェクトにアクセス権限を付与する必要があります。 | 有効。オブジェクトはバケット所有者アカウントによって所有され、バケットポリシーが適用される。 |

### Write-Once-Read-Many （ WORM ）による保護

データ、ユーザ定義オブジェクトのメタデータ、 S3 オブジェクトのタグを保護するために、 Write-Once-Read-Many （ WORM ）バケットを作成することができます。新しいオブジェクトの作成を許可し、既存のコンテンツの上書きや削除を防止するように WORM バケットを設定します。ここで説明するいずれかの方法を使用します。

上書きを常に拒否するには、次の操作を実行します。

- Grid Managerから* Configuration > Grid Options の順に選択し、 Prevent Client Modification *チェックボックスを選択します。
- 次のルールと S3 ポリシーを適用します。

- S3 ポリシーに PutOverwriteObject DENY 処理を追加します。
- S3 ポリシーに DeleteObject DENY 処理を追加します。
- S3 ポリシーに PUT Object ALLOW 処理を追加します。

S3 ポリシーで DeleteObject を DENY に設定しても、「 zero copies after 30 days 」のようなルールに基づく ILM によるオブジェクトの削除は実行されます。

これらのルールとポリシーがすべて適用されても、同時書き込みからは保護されません（状況 A を参照）。保護の対象になるのはシーケンシャルな上書きです（状況 B を参照）。

- 状況 A * ：同時書き込み（保護対象外）

```
/mybucket/important.doc
PUT#1 ---> OK
PUT#2 -------> OK
```

- 状況 B * ：シーケンシャルな上書き（保護対象）

```
/mybucket/important.doc
PUT#1 -------> PUT#2 ---X (denied)
```

関連情報

"ILM を使用してオブジェクトを管理する"

"特別な処理を必要とするポリシーの作成"

"StorageGRID の ILM ルールによるオブジェクトの管理"

"S3 グループポリシーの例"

**S3** ポリシーの例

このセクションでは、バケットとグループの StorageGRID アクセスポリシーを作成する例を示します。

**S3** バケットポリシーの例

バケットポリシーでは、そのポリシーが関連付けられたバケットに対するアクセス権限を指定します。バケットポリシーは、 S3 PutBucketPolicy API を使用して設定します。

バケットポリシーを設定するには、 AWS CLI で次のコマンドを使用します。

```
> aws s3api put-bucket-policy --bucket examplebucket --policy
<em>file://policy.json</em>
```

例：すべてのユーザにバケットへの読み取り専用アクセスを許可する

この例では、匿名ユーザを含むすべてのユーザにバケット内のオブジェクトのリストとバケット内のすべてのオブジェクトの GET Object 処理を許可しています。それ以外の処理はすべて拒否されます。バケットへの書き込みが root アカウントにしか許可されないため、このポリシーは限定的な状況でしか使用されないことに注意してください。

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadOnlyAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:GetObject", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"]
    }
  ]
}
```

例：あるアカウントのすべてのユーザにフルアクセスを許可し、別のアカウントのすべてのユーザにバケットへの読み取り専用アクセスを許可する

この例では、指定したアカウントのすべてのユーザにバケットへのフルアクセスを許可しています。さらに、アカウントをもう1つ指定し、そのアカウントのすべてのユーザには、で始まるバケットのオブジェクトのList処理とGetObject処理のみを許可しています `shared/` オブジェクトキープレフィックス。

> StorageGRID では、非所有者アカウント（匿名アカウントを含む）によって作成されたオブジェクトが、バケット所有者アカウントによって所有されます。バケットポリシーで、これらのオブジェクトの環境 を設定します。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "95390887230002558202"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::examplebucket/shared/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::examplebucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "shared/*"
        }
      }
    }
  ]
}
```

例：すべてのユーザにバケットへの読み取り専用アクセスを許可し、指定したグループにフルアクセスを許可する

この例では、匿名ユーザを含むすべてのユーザにバケットのList処理とバケット内のすべてのオブジェクトのGET Object処理を許可し、グループに属するユーザのみを許可しています `Marketing` 指定したアカウントでは、フルアクセスが許可されています。

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

例：クライアントの **IP** 範囲を限定して、すべてのユーザにバケットへの読み取り **/** 書き込みアクセスを許可する

この例では、指定した IP 範囲（ 54.240.143.0~54.240.143.255 で 54.240.143.188 を除く）からの要求についてのみ、匿名ユーザを含むすべてのユーザにバケットの List 処理とバケット内のすべてのオブジェクトの全処理を許可しています。それ以外の処理はすべて拒否され、 IP 範囲外の要求はすべて拒否されます。

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadWriteAccessIfInSourceIpRange",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:*Object", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"],
      "Condition": {
        "IpAddress": {"aws:SourceIp": "54.240.143.0/24"},
        "NotIpAddress": {"aws:SourceIp": "54.240.143.188"}
      }
    }
  ]
}
```

例：指定したフェデレーテッドユーザにのみバケットへのフルアクセスを許可します

この例では、フェデレーテッドユーザのAlexがへのフルアクセスを許可しています `examplebucket` バケットとそのオブジェクト。'root' を含む他のすべてのユーザは ' すべての操作を明示的に拒否されますただし、「 root 」による Put/Get/DeleteBucketPolicy は拒否されません。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Deny",
      "NotPrincipal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

例： **PutOverwriteObject** 権限

この例では、を使用しています `Deny` PutOverwriteObjectとDeleteObjectの効果は、オブジェクトのデータ、ユーザ定義メタデータ、S3オブジェクトのタグを上書きまたは削除できないようにします。

```
{
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3:PutOverwriteObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": "arn:aws:s3:::wormbucket/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::wormbucket"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::wormbucket/*"
    }
  ]
}
```

関連情報

"バケットの処理"

#### S3 グループポリシーの例

グループポリシーは、そのポリシーが関連付けられたグループに対するアクセス権限を指定します。はいません `Principal` ポリシーは暗黙的な要素であるため、ポリシー内の要素。グループポリシーは Tenant Manager または API を使用して設定します。

例：**Tenant Manager**を使用してグループポリシーを設定します

Tenant Manager を使用してグループを追加または編集するときは、このグループのメンバーに付与する S3 アクセス権限を定義するグループポリシーの作成方法を次の中から選択できます。

- * No S3 Access * ：デフォルトオプション。バケットポリシーでアクセスが許可されていないかぎり、このグループのユーザは S3 リソースにアクセスできません。このオプションを選択すると、デフォルトでは root ユーザにのみ S3 リソースへのアクセスが許可されます。
- * 読み取り専用アクセス * ：このグループのユーザには、 S3 リソースへの読み取り専用アクセスが許可されます。たとえば、オブジェクトをリストして、オブジェクトデータ、メタデータ、タグを読み取ることができます。このオプションを選択すると、テキストボックスに読み取り専用グループポリシーの JSON 文字列が表示されます。この文字列は編集できません。
- * フルアクセス * ：このグループのユーザには、バケットを含む S3 リソースへのフルアクセスが許可されます。このオプションを選択すると、テキストボックスにフルアクセスグループポリシーの JSON 文字列が表示されます。この文字列は編集できません。
- * カスタム * ：グループ内のユーザーには、テキストボックスで指定した権限が付与されます。

  この例では、指定したバケット内の特定のフォルダ（キープレフィックス）のリストおよびアクセスのみがグループのメンバーに許可されます。

例：グループにすべてのバケットへのフルアクセスを許可する

この例では、バケットポリシーで明示的に拒否されている場合を除き、グループのすべてのメンバーにテナントアカウントが所有するすべてのバケットへのフルアクセスが許可されます。

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

例：グループにすべてのバケットへの読み取り専用アクセスを許可する

この例では、バケットポリシーで明示的に拒否されている場合を除き、グループのすべてのメンバーに S3 リソースへの読み取り専用アクセスが許可されます。たとえば、オブジェクトをリストして、オブジェクトデータ、メタデータ、タグを読み取ることができます。

```
{
  "Statement": [
    {
      "Sid": "AllowGroupReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

例：グループメンバーにバケット内の各自の「フォルダ」のみへのフルアクセスを許可します

この例では、指定したバケット内の特定のフォルダ（キープレフィックス）のリストおよびアクセスのみがグループのメンバーに許可されます。これらのフォルダのプライバシー設定を決めるときは、他のグループポリシーやバケットポリシーのアクセス権限を考慮する必要があります。

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

関連情報

"テナントアカウントを使用する"

"PutOverwriteObject権限の使用"

"Write-Once-Read-Many （ WORM ）による保護"

## REST APIのセキュリティの設定

REST API のセキュリティの実装を確認し、システムの保護方法について理解しておく必要があります。

### StorageGRID がREST APIのセキュリティを提供する仕組み

StorageGRID システムで REST API のセキュリティ、認証、および許可がどのように実装されるかを理解しておく必要があります。

StorageGRID では、次のセキュリティ対策が使用されます。

- ロードバランサエンドポイントで HTTPS が設定されている場合は、ロードバランササービスとのクライアント通信に HTTPS が使用されます。

  ロードバランサエンドポイントを設定する際に、オプションで HTTP を有効にすることができます。たとえば、非本番環境でのテストなどに HTTP を使用できます。詳細については、 StorageGRID の管理手順を参照してください。

- StorageGRID は、ストレージノードとのクライアント通信およびゲートウェイノード上の CLB サービスとのクライアント通信に、デフォルトで HTTPS を使用します。

  これらの接続に対して HTTP を有効にすることもできます。たとえば、非本番環境でのテストなどに HTTP を使用できます。詳細については、 StorageGRID の管理手順を参照してください。

  CLB サービスは廃止されました。

- StorageGRID とクライアント間の通信は、 TLS を使用して暗号化されます。
- ロードバランササービスとグリッド内のストレージノードの間の通信は、ロードバランサエンドポイントが HTTP と HTTPS どちらの接続を受け入れるように設定されているかに関係なく暗号化されます。
- REST API 処理を実行するには、クライアントが StorageGRID に HTTP 認証ヘッダーを提供する必要があります。

セキュリティ証明書とクライアントアプリケーション

クライアントは、ゲートウェイノードまたは管理ノード上のロードバランササービスに接続するか、ストレージノードに直接接続するか、またはゲートウェイノード上の CLB サービスに直接接続することができます。

いずれの場合も、クライアントアプリケーションは、グリッド管理者がアップロードしたカスタムサーバ証明書または StorageGRID システムが生成した証明書を使用して、 TLS 接続を確立できます。

- ロードバランササービスに接続する場合、クライアントアプリケーションは、接続に使用するロードバランサエンドポイント用に設定された証明書を使用します。各エンドポイントには独自の証明書があり、グリッド管理者がアップロードしたカスタムサーバ証明書か、グリッド管理者がエンドポイントの設定時に StorageGRID で生成した証明書のいずれかです。
- クライアントアプリケーションをストレージノードまたはゲートウェイノード上の CLB サービスに直接接続する場合、 StorageGRID システムのインストール時に生成されたシステム生成のサーバ証明書（システム認証局によって署名された証明書）を使用します。 グリッド管理者がグリッド用に指定した単一のカスタムサーバ証明書。

TLS 接続の確立に使用する証明書に署名した認証局を信頼するよう、クライアントを設定する必要があります。

ロードバランサエンドポイントの設定に関する情報や、ストレージノードまたはゲートウェイノード上の CLB サービスへの直接 TLS 接続に使用する単一のカスタムサーバ証明書を追加する方法については、 StorageGRID の管理手順を参照してください。

まとめ

次の表に、 S3 および Swift の REST API におけるセキュリティの問題に対する実装を示します。

| **Security** 問題 の略 | **REST API** の実装 |
| --- | --- |
| 接続のセキュリティ | TLS |
| サーバ認証 | システム CA によって署名された X.509 サーバ証明書、または管理者から提供されたカスタムサーバ証明書 |

| Security 問題 の略 | REST API の実装 |
| --- | --- |
| クライアント認証 | • S3 ： S3 アカウント（アクセスキー ID とシークレットアクセスキー）<br>• Swift ： Swift アカウント（ユーザ名とパスワード） |
| クライアント許可 | • S3 ：バケットの所有権と適用可能なすべてのアクセス制御ポリシー<br>• Swift ：管理者ロールのアクセス |

関連情報

"StorageGRID の管理"

**TLS** ライブラリのハッシュアルゴリズムと暗号化アルゴリズムがサポートされます

StorageGRID システムでは、クライアントアプリケーションが Transport Layer Security （ TLS ）セッションを確立する際に使用できる暗号スイートに制限があります。

サポートされる **TLS** のバージョン

StorageGRID では、 TLS 1.2 と TLS 1.3 がサポートされています。

SSLv3 と TLS 1.1 （またはそれ以前のバージョン）はサポートされなくなりました。

サポートされている暗号スイート

| TLS バージョン | IANA 暗号スイートの名前 |
| --- | --- |
| 1/2 | TLS_ECDHE_RSA_with _AES_256_GCM_SHA384 |
| 1/2 | TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 |
| 1/2 | TLS_ECDHE_RSA_With _AES_128_GCM_SHA256 |
| 1.3 | TLS_AES_256_GCM_SHA384 |
| 1.3 | TLS_CHACHA20_POLY1305_SHA256 |
| 1.3 | TLS_AES_128_GCM _SHA256 |

廃止された暗号スイート

次の暗号スイートは廃止されました。これらの暗号のサポートは今後のリリースで廃止される予定です。

| IANA 名 |
| --- |
| TLS_RSA_With _AES_128_GCM _SHA256 |
| TLS_RSA_With _AES_256_GCM_SHA384 |

関連情報

"クライアント接続の設定方法"

## 処理の監視と監査

グリッド全体または特定のノードのトランザクションの傾向を確認することで、クライアント処理のワークロードと効率を監視できます。監査メッセージを使用して、クライアント処理とトランザクションを監視できます。

- "オブジェクトの取り込み速度と読み出し速度を監視する"
- "監査ログへのアクセスと確認"

### オブジェクトの取り込み速度と読み出し速度を監視する

オブジェクトの取り込み速度と読み出し速度、およびオブジェクト数、クエリ、検証関連の指標を監視できます。StorageGRID システムのオブジェクトに対してクライアントアプリケーションが試みた読み取り、書き込み、変更の各処理について、成功した回数と失敗した回数を表示できます。

手順

1. サポートされているブラウザを使用してGrid Managerにサインインします。
2. ダッシュボードで、プロトコル操作セクションを探します。

   このセクションには、 StorageGRID システムによって実行されたクライアント処理の回数に関する概要が表示されます。プロトコル速度は過去 2 分間の平均値です。

3. [ノード（ Nodes）]を選択し
4. ノードのホームページ（導入レベル）で、 * ロードバランサ * タブをクリックします。

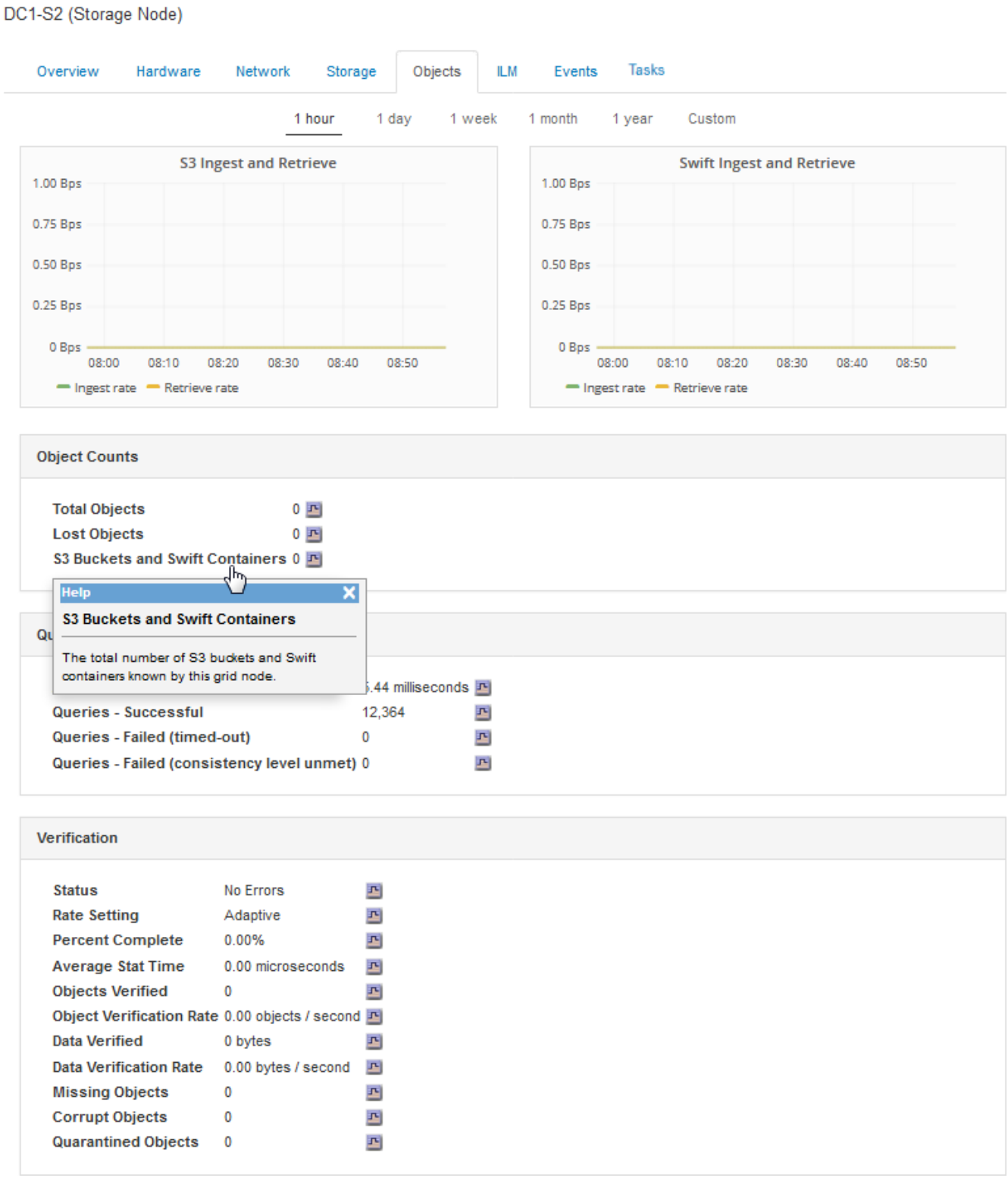
   このグラフには、グリッド内でロードバランサエンドポイントに送信されるすべてのクライアントトラフィックの傾向が表示されます。時間、日、週、月、年単位の間隔を選択できます。 または、カスタムの間隔を適用することもできます。

5. ノードのホームページ（導入レベル）で、 * Objects * タブをクリックします。

   グラフには、 StorageGRID システム全体の取り込み速度と読み出し速度が、 1 秒あたりのバイト数と合計バイト数で表示されます。時間、日、週、月、年単位の間隔を選択できます。 または、カスタムの間隔を適用することもできます。

6. 特定のストレージノードに関する情報を表示するには、左側のリストからノードを選択し、 * Objects * タブをクリックします。

グラフには、このストレージノードのオブジェクトの取り込み速度と読み出し速度が表示されます。このタブには、オブジェクト数、クエリ、検証関連の指標も表示されます。ラベルをクリックすると、これらの指標の定義を確認できます。




7. さらに詳細な情報が必要な場合は、次の手順に従います
   a. Support **>** Tools **>** Grid Topology *を選択します。
   b. [**_site *>] > [** Overview **] > [** Main*] を選択します。

API Operations セクションには、グリッド全体の概要情報が表示されます。

c. 「 * _ ストレージノード _ * > * LDR * > * _ クライアントアプリケーション _ * > * 概要 * > * Main * 」を選択します

Operations セクションには、選択したストレージノードに関する概要情報が表示されます。

監査ログへのアクセスと確認

## 監査メッセージは StorageGRID サービスによって生成され、テキスト形式のログファイルに保存されます。監査ログの API 固有の監査メッセージにより、セキュリティ、運用、およびパフォーマンスについて、システムの健全性の評価に役立つ重要な監視データが提供されます。

必要なもの

- 特定のアクセス権限が必要です。
- を用意しておく必要があります `Passwords.txt` ファイル。
- 管理ノードの IP アドレスを確認しておく必要があります。

このタスクについて

アクティブな監査ログファイルの名前はです `audit.log`をクリックし、を管理ノードに格納します。

1日に1回、アクティブなaudit.logファイルが保存され、新しいファイルが作成されます `audit.log` ファイルが開始されました。保存されたファイルの名前は、保存された日時をの形式で示しています *`yyyy-mm-dd.txt`*。

1日後、保存されたファイルは圧縮され、という形式で名前が変更されます `*yyyy-mm-dd.txt.gz*`元の日付を保持します。

この例は、アクティブを示しています `audit.log` ファイル。前日のファイルです (`2018-04-15.txt`）、および前日の圧縮ファイルです (`2018-04-14.txt.gz`）。

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

手順

1. 管理ノードにログインします。
   a. 次のコマンドを入力します。+
   `ssh admin@primary_Admin_Node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
2. 監査ログファイルが保存されているディレクトリに移動します。

   ```
   cd /var/local/audit/export
   ```

3. 必要に応じて、現在の監査ログファイルまたは保存された監査ログファイルを表示します。

監査ログで追跡される **S3** 処理

# バケットおよびオブジェクトのいくつかの処理は、 StorageGRID の監査ログで追跡されます。

監査ログで追跡されるバケットの処理

- バケットを削除します
- バケットのタグ付けを削除します
- 複数のオブジェクトを削除します
- GET Bucket （ List Objects ）
- GET Bucket Object versions
- GET Bucket tagging
- HEAD Bucket （ヘッドバケット）
- PUT Bucket の場合
- PUT Bucket compliance で確認してください
- PUT Bucket tagging
- PUT Bucket versioning の場合

監査ログで追跡されるオブジェクトの処理

- Complete Multipart Upload の実行
- Upload Part （ ILM ルールの取り込み動作が Strict または Balanced に指定されている場合）
- Upload Part - Copy （ ILM ルールの取り込み動作が Strict または Balanced に指定されている場合）
- オブジェクトを削除します
- オブジェクトの取得
- HEAD Object の実行
- POST Object restore の実行
- PUT Object の場合
- PUT Object - Copy の各コマンドを実行します

関連情報

"バケットの処理"

"オブジェクトの処理"

# アクティブ、アイドル、および同時 **HTTP** 接続のメリット

StorageGRID システムのパフォーマンスに影響するのは、 HTTP 接続の設定方法です。

設定は、 HTTP 接続がアクティブであるかアイドルであるか、同時に複数の接続を使用するかによって異なります。

次の種類の HTTP 接続について、パフォーマンスのメリットを特定することができます。

- アイドル HTTP 接続
- アクティブ HTTP 接続
- 同時 HTTP 接続

関連情報

- "アイドル HTTP 接続を開いておくメリット"
- "アクティブ HTTP 接続のメリット"
- "同時 HTTP 接続のメリット"
- "読み取り処理用と書き込み処理用に別々の HTTP 接続プールを使用する"

アイドル **HTTP** 接続を開いておくメリット

クライアントアプリケーションがアイドル状態のときも HTTP 接続を開いておくと、クライアントアプリケーションで以降のトランザクションが発生したときに、それらの開いている接続を使用して実行することができます。ネットアップでは、アイドル HTTP 接続を開いておく時間を 10 分までにすることを推奨します。HTTP 接続をアイドル状態のまま 10 分以上開いていると、 StorageGRID によって自動的に閉じられることがあります。

アイドル HTTP 接続を開いておくと、次のようなメリットがあります。

- HTTP トランザクションの実行が StorageGRID 必要と判断されてから StorageGRID システムでトランザクションが実行されるまでのレイテンシが短縮されます

  レイテンシの短縮は、特に TCP / IP 接続と TLS 接続の確立に時間がかかる場合に大きなメリットとなります。

- 実行済みの転送が増えるにしたがって TCP / IP のスロースタートアルゴリズムによってデータ転送速度が向上します
- クライアントアプリケーションと StorageGRID システムの間の接続が中断された、複数の障害状況の瞬時通知

アイドル接続を開いておく適切な時間は、既存の接続のスロースタートから得られるメリットと、内部システムリソースへの理想的な接続の割り当てとのバランスによって決まります。

アクティブ **HTTP** 接続のメリット

ストレージノードへの直接接続、またはゲートウェイノード上の CLB サービス（廃止）への直接接続を行う場合は、 HTTP 接続でトランザクションを継続的に実行する場合でも、アクティブ HTTP 接続の継続時間を 10 分までに制限することを推奨します。

接続を開いておく最大継続時間は、接続を維持することで得られるメリットと内部システムリソースへの理想

的な接続の割り当てとのバランスによって決まります。

ストレージノードまたは CLB サービスへのクライアント接続でアクティブ HTTP 接続を制限する利点は次のとおりです。

- StorageGRID システム全体で負荷を最適に分散できます。

  CLB サービスを使用する場合に StorageGRID システム全体で負荷を最適に分散するには、 TCP / IP 接続を長時間維持しないようにすることが重要です。それぞれの HTTP 接続の継続時間をクライアントアプリケーションで追跡し、設定した時間が経過したら HTTP 接続を閉じるように設定します。これにより、 HTTP 接続を再確立して負荷を再分散できます。

  CLB サービスは、クライアントアプリケーションが HTTP 接続を確立したときに、 StorageGRID システム全体で負荷を分散します。時間の経過とともに負荷分散の要件が変わったため、 HTTP 接続が最適な状態でなくなることがあります。クライアントアプリケーションでトランザクションごとに別の HTTP 接続を確立すれば、システムによる負荷分散は最適になりますが、この場合、接続を維持することで得られるより大きなメリットを失うことになります。

  CLB サービスは廃止されました。

- クライアントアプリケーションからの HTTP トランザクションを使用可能な空きスペースがある LDR サービスに転送できる
- メンテナンス手順を開始できます。

  メンテナンス手順の中には、実行中のすべての HTTP 接続が完了してからでないと開始されないものがあります。

ロードバランササービスへのクライアント接続では、接続時間を制限することで一部のメンテナンス手順をすぐに開始できます。クライアント接続の継続時間が制限されていない場合は、アクティブな接続が自動的に終了するまでに数分かかることがあります。

同時 **HTTP** 接続のメリット

## StorageGRID システムへの TCP / IP 接続を複数開いて並列処理を可能にしておくと、パフォーマンスが向上します。最適な並列接続数は、さまざまな要因によって異なります。

同時 HTTP 接続には、次のようなメリットがあります。

- レイテンシが短縮されます

  他のトランザクションが完了するのを待たずに、トランザクションをすぐに開始できます。

- スループットの向上

  StorageGRID システムでは、トランザクションの並列処理が可能なため、全体的なトランザクションのスループットが向上します。

クライアントアプリケーションで複数の HTTP 接続を確立する必要があります。クライアントアプリケーションでトランザクションの実行が必要になったときは、確立された接続の中からトランザクションの処理に現在使用されていない接続を選択してすぐに使用することができます。

同時トランザクションや同時接続の最大スループットは StorageGRID システムのトポロジごとに異なり、それを超えるとパフォーマンスが低下し始めます。最大スループットは、コンピューティングリソース、ネットワークリソース、ストレージリソース、 WAN リンクなどの要因によって決まります。また、サーバやサービスの数、 StorageGRID システムでサポートするアプリケーションの数も影響します。

StorageGRID システムでは、複数のクライアントアプリケーションをサポートすることがよくありますクライアントアプリケーションで使用する同時接続の最大数を決定する場合は、この点に注意してください。クライアントアプリケーションを構成する複数のソフトウェアエンティティのそれぞれで StorageGRID システムへの接続を確立する場合は、それらのエンティティのすべての接続を合計して考慮する必要があります。次のような場合は、同時接続の最大数の調整が必要になることがあります。

- StorageGRID システムのトポロジによって、システムでサポートできる同時トランザクションや同時接続の最大数が異なります。
- クライアントアプリケーションがネットワークの限られた帯域幅で StorageGRID システムと通信する場合は、個々のトランザクションが妥当な時間で完了するように、必要に応じて同時実行の数を少なくします。
- 多くのクライアントアプリケーションで StorageGRID システムを共有する場合は、システムの制限を超えないように、同時実行の数を少なくする必要があります。

読み取り処理用と書き込み処理用に別々の **HTTP** 接続プールを使用する

読み取り処理と書き込み処理に別々の HTTP 接続プールを使用して、それぞれに使用するプールの容量を制御できます。HTTP 接続のプールを分けることで、トランザクションや負荷分散をより細かく制御できます。

クライアントアプリケーションで生成される負荷には、読み出し中心（読み取り）の負荷と格納中心（書き込み）の負荷があります。読み取りと書き込みで HTTP 接続プールを分けることで、各プールの量を調整してそれぞれのトランザクション専用に使用することができます。

# Swift を使用します

クライアントアプリケーションでOpenStack Swift APIを使用して、StorageGRID システムを操作する方法について説明します。

- "StorageGRID でのOpenStack Swift APIのサポート"
- "テナントアカウントと接続を設定する"
- "Swift REST API でサポートされている処理"
- "StorageGRID の Swift REST API 処理"
- "REST APIのセキュリティの設定"
- "処理の監視と監査"

## StorageGRID でのOpenStack Swift APIのサポート

StorageGRID でサポートしている Swift および HTTP のバージョンは次のとおりです。

| 項目 | バージョン |
| --- | --- |
| Swift の仕様 | 2015 年 11 月時点の OpenStack Swift Object Storage API v1 |
| HTTP | 1.1 HTTP の詳細については、 HTTP/1.1 （ RFC 7230~7235 ）を参照してください。<br><br>• 注： StorageGRID は、 HTTP/1.1 パイプラインをサポートしません。 |

関連情報

"OpenStack ：オブジェクトストレージ API"

**StorageGRID** での **Swift API** サポートの履歴

StorageGRID システムでの Swift REST API のサポートに関する変更点に注意する必要があります。

| リリース。 | コメント |
| --- | --- |
| 11.5 | 弱い整合性制御を削除しました。代わりに、 available 整合性レベルが使用されます。 |
| 11.4 | TLS 1.3 のサポートの追加と、サポートされる TLS 暗号スイートのリストの更新CLB は廃止されました。ILM と整合性設定の間の相互関係の概要 が追加されました。 |
| 11.3 | PUT Object 処理が更新され、取り込み時に同期配置を使用する ILM ルールの影響（取り込み動作の Balanced オプションと Strict オプション）が記述されるようになりました。ロードバランサエンドポイントまたはハイアベイラビリティグループを使用するクライアント接続の概要 が追加されました。サポートされる TLS 暗号スイートのリストが更新されました。TLS 1.1 暗号はサポートされなくなりました。 |
| 11.2 | ドキュメントに対する編集上の変更がいくつかあります。 |
| 11.1 | グリッドノードへの Swift クライアント接続での HTTP の使用のサポートが追加されました。整合性制御の定義が更新されました。 |
| 11.0 | テナントアカウントにつき 1 、 000 個のコンテナのサポートが追加されました。 |

| リリース。 | コメント |
| --- | --- |
| 10.3 | ドキュメントの管理に関する記述の更新と修正カスタムサーバ証明書の設定に関するセクションが削除されました。 |
| 10.2 | StorageGRID システムで Swift API が初めてサポートされました。現在サポートされているバージョンは、 OpenStack Swift Object Storage API v1 です。 |

**StorageGRID** での**Swift REST API**の実装

クライアントアプリケーションは、 Swift REST API 呼び出しを使用してストレージノードやゲートウェイノードに接続し、コンテナの作成やオブジェクトの格納と読み出しを行うことができます。これを利用して、 OpenStack Swift 向けに開発されたサービス指向アプリケーションを、 StorageGRID システムで利用できるオンプレミスのオブジェクトストレージに接続することができます。

**Swift** オブジェクトの管理

StorageGRID システムに取り込まれた Swift オブジェクトは、システムのアクティブな ILM ポリシー内の情報ライフサイクル管理（ ILM ）ルールによって管理されます。ILM ルールとポリシーは、 StorageGRID がオブジェクトデータのコピーを作成および分散し、一定の期間にわたって管理する方法を決定します。たとえば、 ILM ルールを特定の Swift コンテナ内のオブジェクトに適用し、複数のオブジェクトコピーを複数のデータセンターに一定期間保存するように指定できます。

グリッドの ILM ルールとポリシーが Swift テナントアカウントのオブジェクトに与える影響については、 StorageGRID 管理者にお問い合わせください。

競合するクライアント要求です

同一キーに書き込む2つのクライアントなど'競合するクライアント要求は'最新のWINS形式で解決されます「latest-wins」評価のタイミングは、Swiftクライアントが処理を開始するタイミングではなく、StorageGRID システムが特定の要求を完了したタイミングに基づいています。

整合性の保証と制御

デフォルトでは、 StorageGRID は、新規作成されたオブジェクトにはリードアフターライト整合性を、オブジェクトの更新と HEAD 処理には結果整合性を提供します。正常に完了した PUT に続く GET では、新しく書き込まれたデータを読み取ることができます。既存のオブジェクトの上書き、メタデータの更新、および削除の整合性レベルは、結果整合性です。上書きは通常、数秒から数分で反映されますが、最大で 15 日かかることがあります。

StorageGRID では、コンテナごとに整合性を制御することもできます。アプリケーションでの必要に応じて、ストレージノード間およびサイト間でオブジェクトの可用性と整合性のトレードオフを行うために、整合性制御を変更できます。

関連情報

"ILM を使用してオブジェクトを管理する"

"GET コンテナセイコウセイヨウキユウ"

"PUT コンテナセイコウセイヨウキユウ"

**Swift REST API**を実装する際の推奨事項

## StorageGRID で使用するために Swift REST API を実装する場合は、次の推奨事項を考慮してください。

存在しないオブジェクトに対する **HEAD** の推奨事項

オブジェクトが実際に存在しないと思われるパスにオブジェクトが存在するかどうかをアプリケーションが定期的にチェックする場合は ' 使用可能な整合性制御を使用する必要がありますたとえば ' アプリケーションがそのロケーションに対して PUT 操作を実行する前に ' そのロケーションに対して HEAD 操作を実行する場合は ' Available 整合性制御を使用する必要があります

そうしないと、使用できないストレージノードがある場合に HEAD 処理でオブジェクトが見つからないと、「 500 Internal Server Error 」が大量に返される可能性があります。

PUT コンテナ整合性要求を使用して、各コンテナに「 available 」整合性制御を設定できます。

オブジェクト名の推奨事項

オブジェクト名の最初の 4 文字に、ランダムな値を使用しないでください。代わりに、イメージなど、ランダムで一意でないプレフィックスを使用してください。

オブジェクト名のプレフィックスにランダムな一意の文字を使用する必要がある場合は、オブジェクト名の前にディレクトリ名を指定してください。つまり、次の形式を使用します。

```
mycontainer/mydir/f8e3-image3132.jpg
```

次の形式は使用しないでください。

```
mycontainer/f8e3-image3132.jpg
```

「範囲の読み取り」に関する推奨事項

「格納オブジェクトの圧縮」オプション（* Configuration > System Settings > Grid Options *）を選択した場合、Swiftクライアントアプリケーションでは、バイト範囲を指定したGET object処理を実行しないでください。StorageGRID は要求されたバイトにアクセスするためにオブジェクトを圧縮解除する必要があるため ' これらの “range read” 操作は非効率的です非常に大きなオブジェクトから小さい範囲のバイト数を要求する GET Object 処理は特に効率が悪く、たとえば、 50GB の圧縮オブジェクトから 10MB の範囲を読み取る処理は非常に非効率的です。

圧縮オブジェクトから範囲を読み取ると、クライアント要求がタイムアウトする可能性があります。

> オブジェクトを圧縮する必要があり、クライアントアプリケーションが範囲読み取りを使用する必要がある場合は、アプリケーションの読み取りタイムアウトを増やしてください。

関連情報

"GET コンテナセイコウセイヨウキユウ"

"PUT コンテナセイコウセイヨウキユウ"

"StorageGRID の管理"

## テナントアカウントと接続を設定する

クライアントアプリケーションからの接続を受け入れるように StorageGRID を設定するには、テナントアカウントを 1 つ以上作成し、接続を設定する必要があります。

### **Swift**テナントアカウントを作成および設定します

Swift API クライアントで StorageGRID に対してオブジェクトの格納や読み出しを行うには、 Swift テナントアカウントが必要です。各テナントアカウントには、専用のアカウント ID 、専用のグループとユーザ、および専用のコンテナとオブジェクトがあります。

Swift テナントアカウントは、 StorageGRID のグリッド管理者がグリッドマネージャまたはグリッド管理 API を使用して作成します。

グリッド管理者は、 Swift テナントアカウントを作成する際に次の情報を指定します。

- テナントの表示名（テナントのアカウント ID は自動的に割り当てられ、変更できません）
- 必要に応じて、テナントアカウントのストレージクォータ — テナントのオブジェクトで使用可能な最大ギガバイト数、テラバイト数、ペタバイト数。テナントのストレージクォータは、物理容量（ディスクのサイズ）ではなく、論理容量（オブジェクトのサイズ）を表します。
- StorageGRID システムでシングルサインオン（ SSO ）が使用されていない場合は、テナントアカウントが独自のアイデンティティソースを使用するか、グリッドのアイデンティティソースを共有するか、およびテナントのローカル root ユーザの初期パスワード。
- SSO が有効になっている場合は、テナントアカウントを設定するための Root Access 権限が割り当てられているフェデレーテッドグループ。

Swift テナントアカウントが作成されたら、 Root Access 権限を持つユーザは Tenant Manager にアクセスして、次のようなタスクを実行できます。

- アイデンティティフェデレーションの設定（グリッドとアイデンティティソースを共有する場合を除く）、およびローカルグループとユーザの作成
- ストレージ使用状況を監視しています

> Swift ユーザが Tenant Manager にアクセスするには、 Root Access 権限が必要です。ただし Root Access 権限では、 Swift REST API に認証してコンテナを作成したりオブジェクトを取り込んだりすることはできません。Swift REST API に認証するには、 Swift 管理者の権限が必要です。

関連情報

"StorageGRID の管理"

"テナントアカウントを使用する"

"サポートされている Swift API エンドポイント"

クライアント接続の設定方法

グリッド管理者は、 Swift クライアントがデータの格納と読み出しを行うために StorageGRID に接続する方法に関連する設定を行います。接続するために必要な具体的な情報は、選択した設定によって異なります。

クライアントアプリケーションは、次のいずれかに接続することで、オブジェクトを格納または読み出すことができます。

- 管理ノードまたはゲートウェイノード上のロードバランササービス、または必要に応じて、管理ノードまたはゲートウェイノードのハイアベイラビリティ（ HA ）グループの仮想 IP アドレス
- ゲートウェイノード上の CLB サービス、または必要に応じて、ゲートウェイノードのハイアベイラビリティグループの仮想 IP アドレス

> CLB サービスは廃止されました。StorageGRID 11.3 より前に設定されたクライアントは、ゲートウェイノード上の CLB サービスを引き続き使用できます。ロードバランシングに StorageGRID を使用する他のすべてのクライアントアプリケーションは、ロードバランササービスを使用して接続する必要があります。

- 外部ロードバランサを使用するかどうかに関係なく、ストレージノードに追加されます

StorageGRID を設定する場合、グリッド管理者はグリッドマネージャまたはグリッド管理 API を使用して次の手順を実行できます。これらはすべてオプションです。

1. ロードバランササービスのエンドポイントを設定する。

   ロードバランササービスを使用するようにエンドポイントを設定する必要があります。管理ノードまたはゲートウェイノード上のロードバランササービスは、クライアントアプリケーションからの受信ネットワーク接続を複数のストレージノードに分散します。ロードバランサエンドポイントを作成する際、 StorageGRID 管理者は、ポート番号、エンドポイントで HTTP / HTTPS 接続を許可するかどうか、エンドポイントを使用するクライアントのタイプ（ S3 または Swift ）、 HTTPS 接続に使用する証明書（該当する場合）を指定します。

2. 信頼されていないクライアントネットワークを設定する

   StorageGRID 管理者がノードのクライアントネットワークを信頼されていないクライアントネットワークとして設定した場合、ノードはロードバランサエンドポイントとして明示的に設定されたポートでクライアントネットワークのインバウンド接続だけを受け入れます。

3. ハイアベイラビリティグループを設定する。

   管理者が HA グループを作成すると、複数の管理ノードまたはゲートウェイノードのネットワークインターフェイスがアクティブ / バックアップ構成になります。クライアント接続は、 HA グループの仮想 IP アドレスを使用して確立されます。

各オプションの詳細については、 StorageGRID の管理手順を参照してください。

**Summary** ：クライアント接続の **IP** アドレスとポート

クライアントアプリケーションは、グリッドノードの IP アドレスおよびそのノード上のサービスのポート番号を使用して StorageGRID に接続します。ハイアベイラビリティ（ HA ）グループが設定されている場合

は、 HA グループの仮想 IP アドレスを使用してクライアントアプリケーションを接続できます。

クライアント接続に必要な情報

次の表に、クライアントが StorageGRID に接続できるさまざまな方法、および各接続タイプで使用される IP アドレスとポートを示します。詳細については、 StorageGRID 管理者にお問い合わせください。または、 StorageGRID for a 概要 の管理手順を参照して、グリッドマネージャでこの情報を確認してください。

| 接続が確立される場所 | クライアントが接続するサービス | **IP** アドレス | ポート |
| --- | --- | --- | --- |
| HA グループ | ロードバランサ | HA グループの仮想 IP アドレス | • ロードバランサエンドポイントのポート |
| HA グループ | CLB の機能です<br>• 注： * CLB サービスは廃止されました。 | HA グループの仮想 IP アドレス | デフォルトの Swift ポート：<br>• HTTPS ： 8083<br>• HTTP ： 8085 |
| 管理ノード | ロードバランサ | 管理ノードの IP アドレス | • ロードバランサエンドポイントのポート |
| ゲートウェイノード | ロードバランサ | ゲートウェイノードの IP アドレス | • ロードバランサエンドポイントのポート |
| ゲートウェイノード | CLB の機能です<br>• 注： * CLB サービスは廃止されました。 | ゲートウェイノードの IP アドレス<br>• 注：デフォルトでは、 CLB および LDR の HTTP ポートは有効になっていません。 | デフォルトの Swift ポート：<br>• HTTPS ： 8083<br>• HTTP ： 8085 |
| ストレージノード | LDR | ストレージノードの IP アドレス | デフォルトの Swift ポート：<br>• HTTPS ： 18083<br>• HTTP ： 18085 |

例

Swift クライアントをゲートウェイノードの HA グループのロードバランサエンドポイントに接続するには、次のように構造化された URL を使用します。

- `https://VIP-of-HA-group:LB-endpoint-port`

たとえば、 HA グループの仮想 IP アドレスが 192.0.2.6 で、 Swift ロードバランサエンドポイントのポート番

号が 10444 の場合、 Swift クライアントは次の URL を使用して StorageGRID に接続できます。

- `https://192.0.2.6:10444`

クライアントが StorageGRID への接続に使用する IP アドレスに DNS 名を設定できます。ローカルネットワーク管理者にお問い合わせください。

#### HTTPS接続とHTTP接続のどちらを使用するかの判断

ロードバランサエンドポイントを使用してクライアント接続を行う場合は、そのエンドポイントに指定されているプロトコル（ HTTP または HTTPS ）を使用して接続を確立する必要があります。ストレージノードへのクライアント接続またはゲートウェイノード上の CLB サービスへのクライアント接続に HTTP を使用する場合は、 HTTP の使用を有効にする必要があります。

デフォルトでは、クライアントアプリケーションがストレージノードまたはゲートウェイノード上の CLB サービスに接続する場合、クライアントアプリケーションはすべての接続に暗号化された HTTPS を使用する必要があります。必要に応じて、 Grid Manager で * Enable HTTP Connection * grid オプションを選択して、セキュアでない HTTP 接続を有効にすることができます。たとえば、非本番環境でストレージノードへの接続をテストする際に、クライアントアプリケーションで HTTP を使用できます。

> 要求が暗号化されずに送信されるため、本番環境のグリッドで HTTP を有効にする場合は注意してください。

> CLB サービスは廃止されました。

[Enable HTTP Connection*] オプションが選択されている場合、クライアントは HTTPS とは異なるポートを HTTP に使用する必要があります。StorageGRID の管理手順を参照してください。

関連情報

"StorageGRID の管理"

### Swift API設定で接続をテストします

Swift の CLI を使用して、 StorageGRID システムへの接続をテストし、システムに対するオブジェクトの読み取りと書き込みが可能であることを確認できます。

必要なもの

- Swift のコマンドラインクライアント python-swiftclient をダウンロードしてインストールしておく必要があります。
- StorageGRID システムに Swift テナントアカウントが必要です。

このタスクについて

セキュリティを設定していない場合は、を追加する必要があります `--insecure` これらの各コマンドにフラグを設定します。

手順

1. StorageGRID Swift 環境の情報 URL を照会します。

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/info
capabilities
```

この手順で、 Swift 環境が機能することをテストできます。オブジェクトを格納してアカウント設定をさらにテストするには、以降の手順を実行します。

2. オブジェクトをコンテナに配置します。

```
touch test_object
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
upload test_container test_object
--object-name test_object
```

3. コンテナを取得してオブジェクトを確認します。

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
list test_container
```

4. オブジェクトを削除します。

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
delete test_container test_object
```

5. コンテナを削除します。

```
swift
-U `<_Tenant_Account_ID:Account_User_Name_>`
-K `<_User_Password_>`
-A `\https://<_FQDN_ | _IP_>:<_Port_>/auth/v1.0'
delete test_container
```

関連情報

"Swiftテナントアカウントを作成および設定します"

"REST APIのセキュリティの設定"

## Swift REST API でサポートされている処理

StorageGRID システムは、 OpenStack Swift API のほとんどの処理をサポートしています。Swift REST API クライアントを StorageGRID に統合する前に、アカウント、コンテナ、およびオブジェクトの処理の実装に関する詳細を確認します。

### StorageGRID でサポートされている操作

次の Swift API 処理がサポートされています。

- "アカウントの処理"
- "コンテナの処理"
- "オブジェクトの処理"

### すべての処理に共通の応答ヘッダー

StorageGRID システムでは、 OpenStack Swift Object Storage API v1 の定義に従って、サポートされるすべての処理に共通のヘッダーが実装されます。

関連情報

"OpenStack ：オブジェクトストレージ API"

### サポートされている Swift API エンドポイント

StorageGRID でサポートされている Swift API エンドポイントは、情報 URL 、認証 URL 、およびストレージ URL です。

#### 情報 URL

StorageGRID Swift 実装の機能と制限事項については、 Swift のベース URL に /info パスを付加して GET 要求を発行することで確認できます。

```
https://FQDN | Node IP:Swift Port/info/
```

要求の内容は次のとおりです。

- *FQDN* は完全修飾ドメイン名です。
- *Node IP* は、StorageGRID ネットワークのストレージノードまたはゲートウェイノードのIPアドレスです。
- *Swift Port* は、ストレージノードまたはゲートウェイノードのSwift API接続に使用するポート番号です。

たとえば、次の情報 URL は、 IP アドレスが 10.99.106.103 でポート 18083 を使用しているストレージノードから情報を要求します。

```
https://10.99.106.103:18083/info/
```

応答には、 Swift 実装の機能が JSON ディクショナリとして含まれます。クライアントツールは、 JSON 応答を解析して実装の機能を特定し、後続のストレージ処理で制約として使用できます。

StorageGRID 実装の Swift では、情報 URL への認証されていないアクセスが許可されます。

#### 認証 URL

クライアントは、 Swift 認証 URL を使用してテナントアカウントユーザとして認証できます。

```
https://FQDN | Node IP:Swift Port/auth/v1.0/
```

で、テナントアカウントID、ユーザ名、およびパスワードをパラメータとして指定する必要があります `X-Auth-User` および `X-Auth-Key` 次のように要求ヘッダー

```
X-Auth-User: Tenant_Account_ID:Username
```

```
X-Auth-Key: Password
```

要求ヘッダーは次のようになります。

- *Tenant_Account_ID* は、Swiftテナントの作成時にStorageGRID によって割り当てられたアカウントIDです。Tenant Manager のサインインページで使用するテナントアカウント ID と同じです。
- *Username* は、Tenant Managerで作成されたテナントユーザの名前です。このユーザは、 Swift 管理者権限を持つグループに属している必要があります。テナントの root ユーザを、 Swift REST API を使用するように設定することはできません。

  テナントアカウントに対してアイデンティティフェデレーションが有効になっている場合は、 LDAP サーバからのフェデレーテッドユーザのユーザ名とパスワードを指定します。または、 LDAP ユーザのドメイン名を指定します。例：

  ```
  X-Auth-User: Tenant_Account_ID:Username@Domain_Name
  ```

- *Password* は、テナントユーザのパスワードです。ユーザパスワードは Tenant Manager で作成および管理します。

認証要求が成功すると、ストレージ URL と認証トークンが次のように返されます。

```
X-Storage-Url: https://FQDN | Node_IP:Swift_Port/v1/Tenant_Account_ID
```

```
X-Auth-Token: token
```

```
X-Storage-Token: token
```

デフォルトでは、トークンの有効期間は生成時刻から 24 時間です。

トークンは特定のテナントアカウントに対して生成されます。あるアカウントに対して有効なトークンで、別のアカウントにアクセスするユーザを許可することはできません。

#### ストレージ **URL**

クライアントアプリケーションは、ゲートウェイノードまたはストレージノードに対して、問題 の Swift REST API 呼び出しを使用して、アカウント、コンテナ、オブジェクトのサポートされる処理を実行できます。ストレージ要求は、認証応答で返されたストレージ URL にアドレスが指定されます。要求には、認証要求から返された X-Auth-Token ヘッダーと値も含める必要があります。

```
https://FQDN | IP:Swift_Port/v1/Tenant_Account_ID

[/container][/object]

X-Auth-Token: token
```

使用状況の統計が含まれるストレージ応答ヘッダーに、最近変更されたオブジェクトの正確な数が反映されない場合があります。このヘッダーに正確な数値が表示されるまでに数分かかることがあります。

使用状況の統計が含まれているアカウントおよびコンテナ処理の応答ヘッダーの例を次に示します。

- `X-Account-Bytes-Used`
- `X-Account-Object-Count`
- `X-Container-Bytes-Used`
- `X-Container-Object-Count`

関連情報

"クライアント接続の設定方法"

"Swiftテナントアカウントを作成および設定します"

"アカウントの処理"

"コンテナの処理"

"オブジェクトの処理"

アカウントの処理

## アカウントに対して実行する Swift API 処理を次に示します。

#### **GET** アカウント

この処理は、アカウントに関連付けられているコンテナリストおよびアカウントの使用状況を示す統計を取得します。

次の要求パラメータが必要です。

- Account

次の要求ヘッダーが必要です。

- X-Auth-Token

次のサポートされている要求クエリパラメータはオプションです。

- Delimiter
- End_marker
- Format
- Limit
- Marker
- Prefix

実行が成功すると ' アカウントが見つかってコンテナがないかコンテナリストが空である場合 ' またはアカウントが見つかってコンテナリストが空でない場合には 'HTTP/1.1 204 No Content' の応答とともに ' 次のヘッダーが返され ' コンテナリストが空でない場合は 'HTTP/1.1 200 OK' の応答が返されます

- Accept-Ranges
- Content-Length
- Content-Type
- Date
- X-Account-Bytes-Used
- X-Account-Container-Count
- X-Account-Object-Count
- X-Timestamp
- X-Trans-Id

#### HEAD アカウント

この処理は、 Swift アカウントからアカウント情報と統計情報を取得します。

次の要求パラメータが必要です。

- Account

次の要求ヘッダーが必要です。

- X-Auth-Token

実行が成功すると、「 HTTP/1.1 204 No Content 」の応答とともに次のヘッダーが返されます。

- `Accept-Ranges`
- `Content-Length`
- `Date`
- `X-Account-Bytes-Used`
- `X-Account-Container-Count`
- `X-Account-Object-Count`
- `X-Timestamp`
- `X-Trans-Id`

関連情報

"監査ログで追跡される Swift 処理"

コンテナの処理

StorageGRID では、 Swift アカウントあたり最大で 1 、 000 個のコンテナがサポートされます。コンテナに対して実行する Swift API 処理を次に示します。

コンテナを削除します

この処理は、 StorageGRID システムの Swift アカウントから空のコンテナを削除します。

次の要求パラメータが必要です。

- `Account`
- `Container`

次の要求ヘッダーが必要です。

- `X-Auth-Token`

実行が成功すると、「 HTTP/1.1 204 No Content 」の応答とともに次のヘッダーが返されます。

- `Content-Length`
- `Content-Type`
- `Date`
- `X-Trans-Id`

**GET** コンテナ

この処理は、コンテナに関連付けられているオブジェクトリストを、 StorageGRID システム内のコンテナの統計情報およびメタデータとともに読み出します。

次の要求パラメータが必要です。

- `Account`

- Container

次の要求ヘッダーが必要です。

- X-Auth-Token

次のサポートされている要求クエリパラメータはオプションです。

- Delimiter
- End_marker
- Format
- Limit
- Marker
- Path
- Prefix

実行が成功すると、「 HTTP/1.1 200 Success 」または「 HTTP/1.1 204 No Content 」の応答とともに次のヘッダーが返されます。

- Accept-Ranges
- Content-Length
- Content-Type
- Date
- X-Container-Bytes-Used
- X-Container-Object-Count
- X-Timestamp
- X-Trans-Id

#### HEAD コンテナ

この処理は、 StorageGRID システムからコンテナの統計情報とメタデータを読み出します。

次の要求パラメータが必要です。

- Account
- Container

次の要求ヘッダーが必要です。

- X-Auth-Token

実行が成功すると、「 HTTP/1.1 204 No Content 」の応答とともに次のヘッダーが返されます。

- Accept-Ranges

- `Content-Length`
- `Date`
- `X-Container-Bytes-Used`
- `X-Container-Object-Count`
- `X-Timestamp`
- `X-Trans-Id`

#### PUT コンテナ

この処理は、 StorageGRID システムのアカウントにコンテナを作成します。

次の要求パラメータが必要です。

- `Account`
- `Container`

次の要求ヘッダーが必要です。

- `X-Auth-Token`

実行が成功すると、「 HTTP/1.1 201 Created 」または「 HTTP/1.1 202 Accepted 」の応答（このアカウントにコンテナがすでに存在する場合）とともに次のヘッダーが返されます。

- `Content-Length`
- `Date`
- `X-Timestamp`
- `X-Trans-Id`

コンテナ名は StorageGRID ネームスペース内で一意である必要があります。このコンテナが別のアカウントの下に存在する場合は、ヘッダー「 HTTP/1.1 409 Conflict 」が返されます。

#### 関連情報

"監査ログで追跡される Swift 処理"

### オブジェクトの処理

## オブジェクトに対して実行する Swift API 処理を次に示します。

#### オブジェクトを削除します

この処理は、オブジェクトのコンテンツとメタデータを StorageGRID システムから削除します。

次の要求パラメータが必要です。

- `Account`
- `Container`

- `Object`

次の要求ヘッダーが必要です。

- `X-Auth-Token`

実行が成功すると、が指定された次の応答ヘッダーが返されます `HTTP/1.1 204 No Content` 対応：

- `Content-Length`
- `Content-Type`
- `Date`
- `X-Trans-Id`

StorageGRID は、 DELETE Object 要求を処理する際に、オブジェクトのすべてのコピーをすべての格納場所からただちに削除しようとします。成功すると、 StorageGRID はただちにクライアントに応答を返します。30 秒以内にすべてのコピーを削除できなかった場合（格納場所が一時的に使用不能などの理由で）、StorageGRID は削除対象のコピーをキューに登録し、クライアントに処理が成功したことを通知します。

オブジェクトの削除方法の詳細については、情報ライフサイクル管理を使用してオブジェクトを管理する手順を参照してください。

#### GET オブジェクト

この処理は、 StorageGRID から、オブジェクトのコンテンツを読み出し、オブジェクトメタデータを取得します。

次の要求パラメータが必要です。

- `Account`
- `Container`
- `Object`

次の要求ヘッダーが必要です。

- `X-Auth-Token`

次の要求ヘッダーはオプションです。

- `Accept-Encoding`
- `If-Match`
- `If-Modified-Since`
- `If-None-Match`
- `If-Unmodified-Since`
- `Range`

実行が成功すると、が指定された次のヘッダーが返されます `HTTP/1.1 200 OK` 対応：

- Accept-Ranges
- Content-Disposition`の場合にのみ返されます `Content-Disposition メタデータが設定されました
- Content-Encoding`の場合にのみ返されます `Content-Encoding メタデータが設定されました
- Content-Length
- Content-Type
- Date
- ETag
- Last-Modified
- X-Timestamp
- X-Trans-Id

#### HEAD オブジェクト

この処理は、取り込まれたオブジェクトのメタデータとプロパティを StorageGRID システムから読み出します。

次の要求パラメータが必要です。

- Account
- Container
- Object

次の要求ヘッダーが必要です。

- X-Auth-Token

実行が成功すると、「 HTTP/1.1 200 OK 」の応答とともに次のヘッダーが返されます。

- Accept-Ranges
- Content-Disposition`の場合にのみ返されます `Content-Disposition メタデータが設定されました
- Content-Encoding`の場合にのみ返されます `Content-Encoding メタデータが設定されました
- Content-Length
- Content-Type
- Date
- ETag
- Last-Modified
- X-Timestamp
- X-Trans-Id

この処理は、 StorageGRID システムで、データとメタデータを含む新しいオブジェクトを作成するか、データとメタデータを含む既存のオブジェクトを置換します。

StorageGRID は、サイズが最大5TBのオブジェクトをサポートします。

> 同一キーに書き込む2つのクライアントなど'競合するクライアント要求は'最新のWINS形式で解決されます「latest-wins」評価のタイミングは、Swiftクライアントが処理を開始するタイミングではなく、StorageGRID システムが特定の要求を完了したタイミングに基づいています。

次の要求パラメータが必要です。

- `Account`
- `Container`
- `Object`

次の要求ヘッダーが必要です。

- `X-Auth-Token`

次の要求ヘッダーはオプションです。

- `Content-Disposition`
- `Content-Encoding`

  チャンクを使用しないでください `Content-Encoding` 環境 オブジェクトがサイズに基づいてオブジェクトをフィルタリングし、取り込み時に同期配置を使用するILMルール（取り込み動作にBalancedオプションまたはStrictオプション）の場合。

- `Transfer-Encoding`

  圧縮またはチャンクを使用しないでください `Transfer-Encoding` 環境 オブジェクトがサイズに基づいてオブジェクトをフィルタリングし、取り込み時に同期配置を使用するILMルール（取り込み動作にBalancedオプションまたはStrictオプション）の場合。

- `Content-Length`

  ILMルールで、オブジェクトがサイズでフィルタリングされ、取り込み時に同期配置が使用される場合は、を指定する必要があります `Content-Length`。

  > でこれらのガイドラインに従っていない場合は、を参照してください `Content-Encoding`、 `Transfer-Encoding`および `Content-Length`ではStorageGRID 、オブジェクトのサイズを確認してILMルールを適用する前に、オブジェクトを保存しておく必要があります。つまり、 StorageGRID で取り込み時にデフォルトでオブジェクトの中間コピーを作成する必要があります。つまり、 StorageGRID での取り込み動作には Dual Commit オプションを使用する必要があります。

  同期配置と ILM ルールの詳細については、情報ライフサイクル管理を使用してオブジェクトを管理する手順を参照してください。

- `Content-Type`
- `ETag`
- `X-Object-Meta-<name\>` （オブジェクト関連のメタデータ）

  ILMルールの参照時間として* User Defined Creation Time *オプションを使用する場合は、という名前のユーザ定義のヘッダーに値を格納する必要があります `X-Object-Meta-Creation-Time`。例：

  ```
  X-Object-Meta-Creation-Time: 1443399726
  ```

  このフィールドの値は、 1970 年 1 月 1 日からの秒数となります。

- `X-Storage-Class: reduced_redundancy`

  このヘッダーは、取り込まれたオブジェクトに一致する ILM ルールで取り込み動作に Dual Commit または Balanced が指定されている場合に StorageGRID で作成されるオブジェクトコピーの数に影響します。

  - * Dual commit * ： ILM ルールの取り込み動作が Dual commit オプションに指定されている場合は、オブジェクトの取り込み時に StorageGRID が中間コピーを 1 つ作成します（シングルコミット）。
  - * Balanced * ： ILM ルールで Balanced オプションが指定されている場合、 StorageGRID は、ルールで指定されたすべてのコピーをただちに作成できない場合にのみ、中間コピーを 1 つ作成します。StorageGRID で同期配置を実行できる場合、このヘッダーは効果がありません。

    。 `reduced_redundancy` ヘッダーは、オブジェクトに一致するILMルールで単一のレプリケートコピーが作成される場合に最も適しています。この場合は、を使用します `reduced_redundancy` 取り込み処理のたびに追加のオブジェクトコピーを不要に作成および削除する必要がなくなります。

    を使用する `reduced_redundancy` 取り込み中にオブジェクトデータが失われるリスクが高まるため、他の状況ではヘッダーを使用することは推奨されません。たとえば、 ILM 評価の前にコピーが 1 つだけ格納されていたストレージノードに障害が発生すると、データが失われる可能性があります。

    > ⓘ レプリケートコピーを一定期間に 1 つだけ作成すると、データが永続的に失われるリスクがあります。オブジェクトのレプリケートコピーが 1 つしかない場合、ストレージノードに障害が発生したり、重大なエラーが発生すると、そのオブジェクトは失われます。また、アップグレードなどのメンテナンス作業中は、オブジェクトへのアクセスが一時的に失われます。

  を指定することに注意してください `reduced_redundancy` オブジェクトの初回取り込み時に作成されるコピー数のみに影響します。オブジェクトがアクティブな ILM ポリシーで評価される際に作成されるオブジェクトのコピー数には影響せず、 StorageGRID システムでデータが格納されるときの冗長性レベルが低下することもありません。

実行が成功すると、「 HTTP/1.1 201 Created 」の応答とともに次のヘッダーが返されます。

- `Content-Length`
- `Content-Type`
- `Date`
- `ETag`

- `Last-Modified`
- `X-Trans-Id`

関連情報

"ILM を使用してオブジェクトを管理する"

"監査ログで追跡される Swift 処理"

### OPTIONS 要求

OPTIONS 要求は、個々の Swift サービスが使用可能かどうかを確認します。OPTIONS 要求は、 URL で指定されたストレージノードまたはゲートウェイノードによって処理されます。

#### OPTIONS メソッド

たとえば、クライアントアプリケーションでは、 Swift 認証クレデンシャルを入力することなく、ストレージノード上の Swift ポートに OPTIONS 要求を問題 で送信して、ストレージノードが使用可能かどうかを判別できます。この要求は、監視に使用できるほか、外部のロードバランサがストレージノードの停止を特定する目的でも使用できます。

情報（ info ） URL またはストレージ（ storage ） URL と併用する場合、 OPTIONS メソッドは、 HEAD 、 GET 、 OPTIONS 、 PUT など、指定された URL でサポートされる動詞のリストを返します。AUTH URL にはオプションを使用できません。

次の要求パラメータが必要です。

- `Account`

次の要求パラメータはオプションです。

- `Container`
- `Object`

実行が成功すると、「 HTTP/1.1 204 No Content 」の応答とともに次のヘッダーが返されます。ストレージ URL への OPTIONS 要求には、ターゲットが存在する必要はありません。

- `Allow` （HEAD、GET、OPTIONSなど、指定されたURLでサポートされる動詞のリスト）およびPUT）
- `Content-Length`
- `Content-Type`
- `Date`
- `X-Trans-Id`

関連情報

"サポートされている Swift API エンドポイント"

エラー応答について理解しておくと、処理をトラブルシューティングする際に役立ちます。

処理中にエラーが発生した場合に返される HTTP ステータスコードを次に示します。

| Swift エラーの名前 | HTTP ステータス |
| --- | --- |
| AccountNameTooLong 、 ContainerNameTooLong 、 HeaderTooBig 、 InvalidContainerName 、 InvalidRequest 、 InvalidURI 、 MetadataNameTooLong 、 MetadataValueTooBig 、 MissingSecurityHeader 、 ObjectNameTooLong 、 TooManyContainers 、 TooManyMetadataItems 、 TotalMetadataTooLarge | 400 不正な要求です |
| アクセスが拒否されました | 403 禁止 |
| ContainerNotEmpty 、 ContainerAlreadyExists です | 409 競合 |
| 内部エラー | 500 Internal Server Error （内部サーバエラー） |
| InvalidRange ：無効な範囲 | 416 リクエストされた範囲が適合しません |
| MethodNotAllowed のように入力します | 405 メソッドは許可されていません |
| MissingContentLength （ MissingContentLength ） | 411 長さが必要です |
| NOTFOUND | 404 が見つかりません |
| 実装なし | 501 は実装されていません |
| PreconditionalFailed | 412 事前条件が失敗しました |
| resourceNotFound です | 404 が見つかりません |
| 権限がありません | 401 認証なし |
| UnprocessableEntity の場合 | 422 加工不能エンティティ |

## StorageGRID の Swift REST API 処理

StorageGRID システム固有の処理が Swift REST API に追加されています。

### GET コンテナセイコウセイヨウキユウ

整合性レベルを設定する場合は、オブジェクトの可用性と、異なるストレージノードおよびサイト間におけるオブジェクトの整合性のどちらかを犠牲にしなければなりません。GET コンテナ整合性要求では、特定のコンテナに適用されている整合性レベルを確認できます。

リクエスト

| 要求の **HTTP** ヘッダー | 説明 |
| --- | --- |
| `X-Auth-Token` | 要求に使用するアカウントの Swift 認証トークンを指定します。 |
| `x-ntap-sg-consistency` | 要求のタイプを指定します `true` = GETコンテナconsistency、および `false` =コンテナを取得します。 |
| `Host` | 要求の転送先のホスト名。 |

要求例

```
GET /v1/28544923908243208806/Swift container
X-Auth-Token: SGRD_3a877009a2d24cb1801587bfa9050f29
x-ntap-sg-consistency: true
Host: test.com
```

応答

| 応答の **HTTP** ヘッダー | 説明 |
| --- | --- |
| `Date` | 応答の日時。 |
| `Connection` | サーバへの接続が開いているかどうか。 |
| `X-Trans-Id` | 要求の一意のトランザクション ID 。 |
| `Content-Length` | 応答の本文の長さ。 |

| 応答の **HTTP** ヘッダー | 説明 |
| --- | --- |
| `x-ntap-sg-consistency` | コンテナに適用されている整合性制御レベルです。次の値がサポートされています。<br>• * all * ：すべてのノードが即座にデータを受け取り、受け取れない場合は要求が失敗します。<br>• * strong-global * ：すべてのサイトにおけるすべてのクライアント要求について、リードアフターライト整合性が保証されます。<br>• * strong-site * ： 1 つのサイトにおけるすべてのクライアント要求について、リードアフターライト整合性が保証されます。<br>• * read-after-new-write * ：新規オブジェクトについてはリードアフターライト整合性が提供され、オブジェクトの更新については結果整合性が提供されます。高可用性が確保され、データ保護が保証されます。<br>• 注：存在しないオブジェクトに対してアプリケーションが HEAD 要求を使用すると、使用できないストレージノードがあると「 500 Internal Server Error 」が大量に返される可能性があります。これらのエラーを防ぐには、「 available 」レベルを使用します。<br>• * available * （ HEAD オペレーションについては結果整合性）：「 read-after-new-write 」整合性レベルと動作は同じですが、 HEAD オペレーションについては結果整合性のみを提供します。ストレージ・ノードが使用できない場合 ' リードアフター・新規ライトよりもヘッド操作の可用性が高くなります |

応答例

```
HTTP/1.1 204 No Content
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
X-Trans-Id: 1936575373
Content-Length: 0
x-ntap-sg-consistency: strong-site
```

関連情報

"テナントアカウントを使用する"

**PUT** コンテナセイコウセイヨウキユウ

PUT コンテナ整合性要求では、コンテナに対して実行される処理に適用する整合性レベルを指定できます。デフォルトでは ' 新しいコンテナは ' リードアフター・ア・ニュー・ライトの整合性レベルを使用して作成されます

リクエスト

| 要求の **HTTP** ヘッダー | 説明 |
| --- | --- |
| `X-Auth-Token` | 要求に使用するアカウントの Swift 認証トークンです。 |
| `x-ntap-sg-consistency` | コンテナに対する処理に適用される整合性制御レベルです。次の値がサポートされています。<br>• * all * ：すべてのノードが即座にデータを受け取り、受け取れない場合は要求が失敗します。<br>• * strong-global * ：すべてのサイトにおけるすべてのクライアント要求について、リードアフターライト整合性が保証されます。<br>• * strong-site * ： 1 つのサイトにおけるすべてのクライアント要求について、リードアフターライト整合性が保証されます。<br>• * read-after-new-write * ：新規オブジェクトについてはリードアフターライト整合性が提供され、オブジェクトの更新については結果整合性が提供されます。高可用性が確保され、データ保護が保証されます。<br>• 注：存在しないオブジェクトに対してアプリケーションが HEAD 要求を使用すると、使用できないストレージノードがあると「 500 Internal Server Error 」が大量に返される可能性があります。これらのエラーを防ぐには、「 available 」レベルを使用します。<br>• * available * （ HEAD オペレーションについては結果整合性）：「 read-after-new-write 」整合性レベルと動作は同じですが、 HEAD オペレーションについては結果整合性のみを提供します。ストレージ・ノードが使用できない場合 ' リードアフター・新規ライトよりもヘッド操作の可用性が高くなります |
| `Host` | 要求の転送先のホスト名。 |

整合性制御と **ILM** ルールの相互作用によるデータ保護への影響

整合性制御と ILM ルールのどちらを選択した場合も、オブジェクトの保護方法に影響します。これらの設定は対話的に操作できます。

たとえば、オブジェクトの格納に使用される整合性制御はオブジェクトメタデータの初期配置に影響し、 ILM ルールで選択される取り込み動作はオブジェクトコピーの初期配置に影響します。StorageGRID では、クライアント要求に対応するためにオブジェクトのメタデータとそのデータの両方にアクセスする必要があるため、整合性レベルと取り込み動作に一致する保護レベルを選択することで、より適切な初期データ保護と予測可能なシステム応答を実現できます。

ILM ルールでは、次の取り込み動作を使用できます。

- * Strict * ： ILM ルールに指定されたすべてのコピーを作成しないと、クライアントに成功が返されません。
- * Balanced * ： StorageGRID は、取り込み時に ILM ルールで指定されたすべてのコピーを作成しようとします。作成できない場合、中間コピーが作成されてクライアントに成功が返されます。可能な場合は、 ILM ルールで指定されたコピーが作成されます。
- * デュアルコミット * ： StorageGRID はオブジェクトの中間コピーをただちに作成し、クライアントに成功を返します。可能な場合は、 ILM ルールで指定されたコピーが作成されます。

ILM ルールの取り込み動作を選択する前に、情報ライフサイクル管理を使用してオブジェクトを管理する手順の設定の完全な概要 を確認してください。

整合性制御と **ILM** ルールの連動の例

次の ILM ルールと次の整合性レベル設定の 2 サイトグリッドがあるとします。

- * ILM ルール * ：ローカルサイトとリモートサイトに 1 つずつ、 2 つのオブジェクトコピーを作成します。Strict 取り込み動作が選択されています。
- * 整合性レベル *:"Strong-GLOBAL" ( オブジェクトメタデータはすべてのサイトにただちに分散されます )

クライアントがオブジェクトをグリッドに格納すると、 StorageGRID は両方のオブジェクトをコピーし、両方のサイトにメタデータを分散してからクライアントに成功を返します。

オブジェクトは、取り込みが成功したことを示すメッセージが表示された時点で損失から完全に保護されます。たとえば、取り込み直後にローカルサイトが失われた場合、オブジェクトデータとオブジェクトメタデータの両方のコピーがリモートサイトに残っています。オブジェクトを完全に読み出し可能にしている。

代わりに同じ ILM ルールと「 strong-site 」整合性レベルを使用する場合は、オブジェクトデータがリモートサイトにレプリケートされたあとで、オブジェクトメタデータがそこに分散される前に、クライアントに成功メッセージが送信される可能性があります。この場合、オブジェクトメタデータの保護レベルがオブジェクトデータの保護レベルと一致しません。取り込み直後にローカルサイトが失われると、オブジェクトメタデータが失われます。オブジェクトを読み出すことができません。

整合性レベルと ILM ルールの間の関係は複雑になる可能性があります。サポートが必要な場合は、ネットアップにお問い合わせください。

要求例

```
PUT /v1/28544923908243208806/_Swift container_
X-Auth-Token: SGRD_3a877009a2d24cb1801587bfa9050f29
x-ntap-sg-consistency: strong-site
Host: test.com
```

応答

| 応答の **HTTP** ヘッダー | 説明 |
| --- | --- |
| `Date` | 応答の日時。 |
| `Connection` | サーバへの接続が開いているかどうか。 |
| `X-Trans-Id` | 要求の一意のトランザクション ID 。 |
| `Content-Length` | 応答の本文の長さ。 |

応答例

```
HTTP/1.1 204 No Content
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
X-Trans-Id: 1936575373
Content-Length: 0
```

関連情報

"テナントアカウントを使用する"

# REST APIのセキュリティの設定

REST API のセキュリティの実装を確認し、システムの保護方法について理解しておく必要があります。

## StorageGRID がREST APIのセキュリティを提供する仕組み

StorageGRID システムで REST API のセキュリティ、認証、および許可がどのように実装されるかを理解しておく必要があります。

StorageGRID では、次のセキュリティ対策が使用されます。

- ロードバランサエンドポイントで HTTPS が設定されている場合は、ロードバランササービスとのクライアント通信に HTTPS が使用されます。

  ロードバランサエンドポイントを設定する際に、オプションで HTTP を有効にすることができます。たとえば、非本番環境でのテストなどに HTTP を使用できます。詳細については、 StorageGRID の管理手順を参照してください。

- StorageGRID は、ストレージノードとのクライアント通信およびゲートウェイノード上の CLB サービスとのクライアント通信に、デフォルトで HTTPS を使用します。

  これらの接続に対して HTTP を有効にすることもできます。たとえば、非本番環境でのテストなどに HTTP を使用できます。詳細については、 StorageGRID の管理手順を参照してください。

CLB サービスは廃止されました。

- StorageGRID とクライアント間の通信は、 TLS を使用して暗号化されます。
- ロードバランササービスとグリッド内のストレージノードの間の通信は、ロードバランサエンドポイントが HTTP と HTTPS どちらの接続を受け入れるように設定されているかに関係なく暗号化されます。
- REST API 処理を実行するには、クライアントが StorageGRID に HTTP 認証ヘッダーを提供する必要があります。

セキュリティ証明書とクライアントアプリケーション

クライアントは、ゲートウェイノードまたは管理ノード上のロードバランササービスに接続するか、ストレージノードに直接接続するか、またはゲートウェイノード上の CLB サービスに直接接続することができます。

いずれの場合も、クライアントアプリケーションは、グリッド管理者がアップロードしたカスタムサーバ証明書または StorageGRID システムが生成した証明書を使用して、 TLS 接続を確立できます。

- ロードバランササービスに接続する場合、クライアントアプリケーションは、接続に使用するロードバランサエンドポイント用に設定された証明書を使用します。各エンドポイントには独自の証明書があり、グリッド管理者がアップロードしたカスタムサーバ証明書か、グリッド管理者がエンドポイントの設定時に StorageGRID で生成した証明書のいずれかです。
- クライアントアプリケーションをストレージノードまたはゲートウェイノード上の CLB サービスに直接接続する場合、 StorageGRID システムのインストール時に生成されたシステム生成のサーバ証明書（システム認証局によって署名された証明書）を使用します。 グリッド管理者がグリッド用に指定した単一のカスタムサーバ証明書。

TLS 接続の確立に使用する証明書に署名した認証局を信頼するよう、クライアントを設定する必要があります。

ロードバランサエンドポイントの設定に関する情報や、ストレージノードまたはゲートウェイノード上の CLB サービスへの直接 TLS 接続に使用する単一のカスタムサーバ証明書を追加する方法については、 StorageGRID の管理手順を参照してください。

まとめ

次の表に、 S3 および Swift の REST API におけるセキュリティの問題に対する実装を示します。

| **Security** 問題 の略 | **REST API** の実装 |
| --- | --- |
| 接続のセキュリティ | TLS |
| サーバ認証 | システム CA によって署名された X.509 サーバ証明書、または管理者から提供されたカスタムサーバ証明書 |
| クライアント認証 | • S3 ： S3 アカウント（アクセスキー ID とシークレットアクセスキー）<br>• Swift ： Swift アカウント（ユーザ名とパスワード） |

| Security 問題 の略 | REST API の実装 |
| --- | --- |
| クライアント許可 | • S3 ：バケットの所有権と適用可能なすべてのアクセス制御ポリシー<br>• Swift ：管理者ロールのアクセス |

関連情報

"StorageGRID の管理"

### TLS ライブラリのハッシュアルゴリズムと暗号化アルゴリズムがサポートされます

StorageGRID システムでは、クライアントアプリケーションが Transport Layer Security （ TLS ）セッションを確立する際に使用できる暗号スイートに制限があります。

#### サポートされる TLS のバージョン

StorageGRID では、 TLS 1.2 と TLS 1.3 がサポートされています。

SSLv3 と TLS 1.1 （またはそれ以前のバージョン）はサポートされなくなりました。

#### サポートされている暗号スイート

| TLS バージョン | IANA 暗号スイートの名前 |
| --- | --- |
| 1/2 | TLS_ECDHE_RSA_with _AES_256_GCM_SHA384 |
| TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 | TLS_ECDHE_RSA_With _AES_128_GCM_SHA256 |
| 1.3 | TLS_AES_256_GCM_SHA384 |
| TLS_CHACHA20_POLY1305_SHA256 | TLS_AES_128_GCM _SHA256 |

#### 廃止された暗号スイート

次の暗号スイートは廃止されました。これらの暗号のサポートは今後のリリースで廃止される予定です。

| IANA 名 |
| --- |
| TLS_RSA_With _AES_128_GCM _SHA256 |
| TLS_RSA_With _AES_256_GCM_SHA384 |

関連情報

"クライアント接続の設定方法"

# 処理の監視と監査

グリッド全体または特定のノードのトランザクションの傾向を確認することで、クライアント処理のワークロードと効率を監視できます。監査メッセージを使用して、クライアント処理とトランザクションを監視できます。

## オブジェクトの取り込み速度と読み出し速度を監視する

オブジェクトの取り込み速度と読み出し速度、およびオブジェクト数、クエリ、検証関連の指標を監視できます。StorageGRID システムのオブジェクトに対してクライアントアプリケーションが試みた読み取り、書き込み、変更の各処理について、成功した回数と失敗した回数を表示できます。

手順

1. サポートされているブラウザを使用してGrid Managerにサインインします。
2. ダッシュボードで、プロトコル操作セクションを探します。

   このセクションには、 StorageGRID システムによって実行されたクライアント処理の回数に関する概要が表示されます。プロトコル速度は過去 2 分間の平均値です。

3. [ノード（ Nodes）]を選択し
4. ノードのホームページ（導入レベル）で、 * ロードバランサ * タブをクリックします。

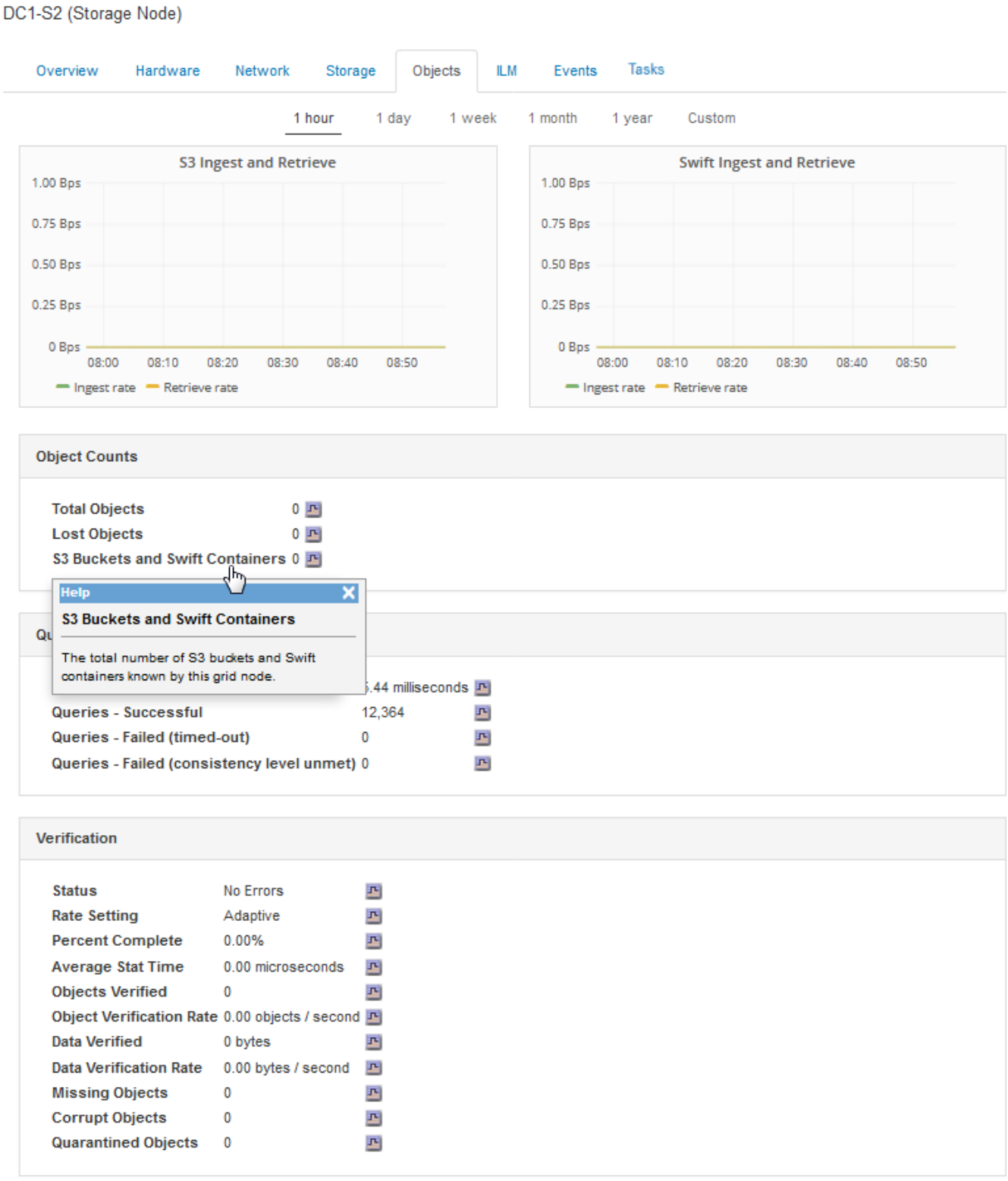
   このグラフには、グリッド内でロードバランサエンドポイントに送信されるすべてのクライアントトラフィックの傾向が表示されます。時間、日、週、月、年単位の間隔を選択できます。 または、カスタムの間隔を適用することもできます。

5. ノードのホームページ（導入レベル）で、 * Objects * タブをクリックします。

   グラフには、 StorageGRID システム全体の取り込み速度と読み出し速度が、 1 秒あたりのバイト数と合計バイト数で表示されます。時間、日、週、月、年単位の間隔を選択できます。 または、カスタムの間隔を適用することもできます。

6. 特定のストレージノードに関する情報を表示するには、左側のリストからノードを選択し、 * Objects * タブをクリックします。

   グラフには、このストレージノードのオブジェクトの取り込み速度と読み出し速度が表示されます。このタブには、オブジェクト数、クエリ、検証関連の指標も表示されます。ラベルをクリックすると、これらの指標の定義を確認できます。




7. さらに詳細な情報が必要な場合は、次の手順に従います
   a. Support **>** Tools **>** Grid Topology *を選択します。
   b. [**_site *>] > [** Overview **] > [** Main*] を選択します。

      API Operations セクションには、グリッド全体の概要情報が表示されます。

c. 「 * _ ストレージノード _ * > * LDR * > * _ クライアントアプリケーション _ * > * 概要 * > * Main * 」を選択します

Operations セクションには、選択したストレージノードに関する概要情報が表示されます。

監査ログへのアクセスと確認

監査メッセージは StorageGRID サービスによって生成され、テキスト形式のログファイルに保存されます。監査ログの API 固有の監査メッセージにより、セキュリティ、運用、およびパフォーマンスについて、システムの健全性の評価に役立つ重要な監視データが提供されます。

必要なもの

- 特定のアクセス権限が必要です。
- を用意しておく必要があります `Passwords.txt` ファイル。
- 管理ノードの IP アドレスを確認しておく必要があります。

このタスクについて

アクティブな監査ログファイルの名前はです `audit.log`をクリックし、を管理ノードに格納します。

1 日に 1 回、アクティブな audit.log ファイルが保存され、新しい audit.log ファイルが開始されます。保存されたファイルの名前は、保存された日時をの形式で示しています `yyyy-mm-dd.txt`。

1日後、保存されたファイルは圧縮され、という形式で名前が変更されます `yyyy-mm-dd.txt.gz`元の日付を保持します。

次の例は、アクティブなaudit.logファイル、前日のファイル（2018-04-15.txt）、および前日の圧縮されたファイルを示しています (`2018-04-14.txt.gz`）。

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

手順

1. 管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
2. 監査ログファイルが保存されているディレクトリに移動します。`cd /var/local/audit/export`
3. 必要に応じて、現在の監査ログファイルまたは保存された監査ログファイルを表示します。

関連情報

"監査ログを確認します"

監査ログで追跡される **Swift** 処理

ストレージに対する成功した DELETE 、 GET 、 HEAD 、 POST 、 PUT の各処理は、 StorageGRID 監査ロ

グで追跡されます。エラーはログに記録されず、情報、認証、オプションの要求も記録されません。

次の Swift 処理で追跡される情報の詳細については、「監査メッセージの概要」を参照してください。

アカウントの処理

- GET アカウント
- HEAD アカウント

コンテナの処理

- コンテナを削除します
- GET コンテナ
- HEAD コンテナ
- PUT コンテナ

オブジェクトの処理

- オブジェクトを削除します
- GET オブジェクト
- HEAD オブジェクト
- PUT オブジェクト

関連情報

"監査ログを確認します"

"アカウントの処理"

"コンテナの処理"

"オブジェクトの処理"

# 監視とトラブルシューティング

## StorageGRID システムを監視する

StorageGRID システムを監視する方法と、発生する可能性のある問題を評価する方法について説明します。すべてのシステムアラートを一覧表示します。

- "Grid Managerを使用して監視する"
- "定期的に監視する必要がある情報"
- "アラートとアラームの管理"
- "SNMPによる監視を使用する"
- "追加のStorageGRID データを収集しています"
- "StorageGRID システムのトラブルシューティング"
- "アラート一覧"
- "アラーム一覧（従来のシステム）"
- "ログファイル参照"

### Grid Managerを使用して監視する

Grid Managerは、StorageGRID システムの監視に最も重要なツールです。このセクションでは、Grid Managerダッシュボードの概要を紹介し、ノードページに関する詳細情報を提供します。

- "Web ブラウザの要件"
- "ダッシュボードの表示"
- "Nodesページを表示します"

#### Web ブラウザの要件

サポートされている Web ブラウザを使用する必要があります。

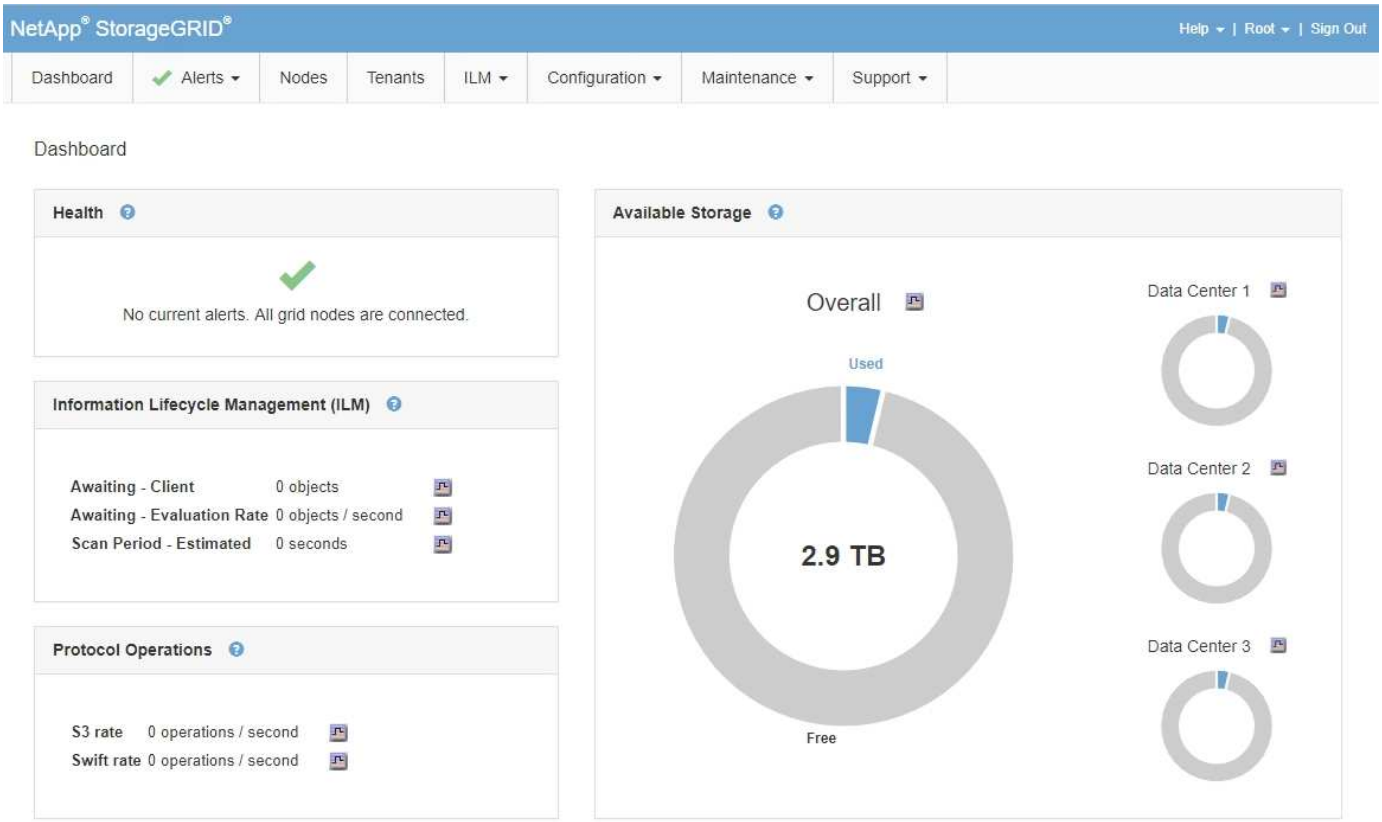
| Web ブラウザ | サポートされる最小バージョン |
| --- | --- |
| Google Chrome | 87 |
| Microsoft Edge の場合 | 87 |
| Mozilla Firefox | 84 |

ブラウザウィンドウの幅を推奨される値に設定してください。

| ブラウザの幅 | ピクセル |
| --- | --- |
| 最小（ Minimum ） | 1024 |
| 最適 | 1280 |

ダッシュボードの表示

Grid Manager に初めてサインインするときは、ダッシュボードを使用してシステムのアクティビティを一目で監視できます。ダッシュボードには、システムの健全性、使用状況、および処理の傾向とグラフに関する情報が表示されます。




正常性パネル

| 説明 | 詳細を確認します | 詳細はこちら。 |
| --- | --- | --- |
| システムの健常性をまとめたものです。緑のチェックマークは、現在のアラートがなく、すべてのグリッドノードが接続されていることを示します。その他のアイコンは、現在のアラートまたは切断されているノードが少なくとも 1 つあることを示します。 | 次のリンクが 1 つ以上表示されることがあります。<br>• * Grid details * ：切断されているノード（接続状態が「 Unknown 」または「 Administratively Down 」）があります。リンクをクリックするか、青またはグレーのアイコンをクリックして、影響を受けるノードを特定します。<br>• * 現在のアラート * ：現在アクティブなアラートがある場合に表示されます。リンクをクリックするか、クリティカル、メジャー、または*マイナー*をクリックして、アラート>*現在の*ページの詳細を表示します。<br>• * Recently Resolved alerts * ：過去 1 週間にトリガーされたアラートが解決されると表示されます。リンクをクリックすると、[* Alerts > Resolved （*アラート>*解決済み*）]ページに詳細が表示されます。<br>• * レガシーアラーム * ：現在アクティブなアラーム（レガシーシステム）がある場合に表示されます。リンクをクリックすると、* Support > Alarms （Legacy）> Current Alarms * ページで詳細が表示されます。<br>• * ライセンス * ：この StorageGRID システムのソフトウェアライセンスを含む問題がある場合に表示されます。リンクをクリックして、[* Maintenance （メンテナンス）]>[ System （*システム）]>[* License （ライセンス）]ページで詳細を確認します。 | • "ノードの接続状態を監視しています"<br>• "現在のアラートの表示"<br>• "解決済みのアラートの表示"<br>• "古いアラームの表示"<br>• "StorageGRID の管理" |

**Available Storage** （使用可能なストレージ）パネル

| 説明 | 詳細を確認します | 詳細はこちら。 |
| --- | --- | --- |
| グリッド全体の使用可能および使用済みのストレージ容量が表示されます。アーカイブメディアは表示されません。<br><br>グラフ全体には、グリッド全体の合計が表示されます。複数サイトのグリッドの場合は、各データセンターサイトのグラフが追加で表示されます。<br><br>この情報から、使用済みのストレージと使用可能なストレージを比較できます。マルチサイトグリッドを使用している場合は、より多くのストレージを消費しているサイトを特定できます。 | • 容量を確認するには、グラフ上の使用可能容量と使用済み容量のセクションにカーソルを合わせます。<br>• ある期間の容量のトレンドを確認するには、グラフアイコンをクリックします をクリックします。<br>• 詳細を表示するには、*ノード*を選択します。次に、グリッド全体、サイト全体、または単一のストレージノードについて、ストレージタブを表示します。 | • "Storage（ストレージ）タブを表示します"<br>• "ストレージ容量を監視しています" |

情報ライフサイクル管理（**ILM**）パネル

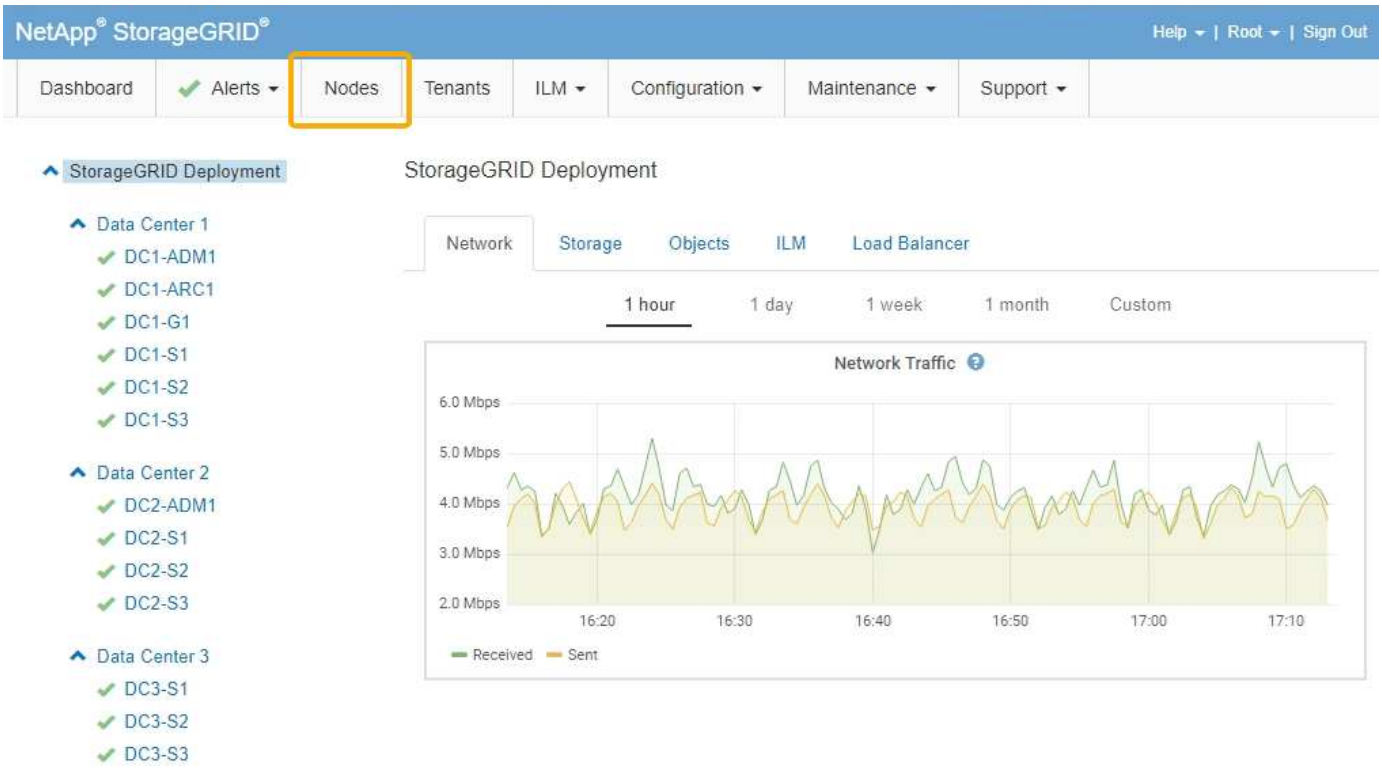
| 説明 | 詳細を確認します | 詳細はこちら。 |
| --- | --- | --- |
| システムの現在の ILM 処理と ILM キューの状況が表示されます。この情報から、システムのワークロードを監視できます。<br><br>• * Awaiting - Client * ：クライアント処理（取り込みなど）から ILM による評価を待機しているオブジェクトの合計数です。<br>• * 待機中 - 評価速度 * ：グリッド内の ILM ポリシーに照らしてオブジェクトが評価されている現在の速度です。<br>• * スキャン期間 - 推定 * ： ILM によるすべてのオブジェクトのフルスキャンが完了するまでの推定時間。* 注： * フルスキャンが完了しても、 ILM がすべてのオブジェクトに適用されるとは限りません。 | • 詳細を表示するには、*ノード*を選択します。次に、グリッド全体、サイト全体、または単一のストレージノードについて、 ILM のタブを表示します。<br>• 既存の ILM ルールを表示するには、 * ILM * > * Rules * を選択します。<br>• 既存の ILM ポリシーを表示するには、 * ILM * > * Policies * を選択します。 | • "ILMタブの表示"<br>• "StorageGRID の管理"。 |

プロトコル操作パネル

| 説明 | 詳細を確認します | 詳細はこちら。 |
| --- | --- | --- |
| システムで実行されたプロトコル固有の処理（ S3 および Swift ）の数が表示されます。<br><br>この情報から、システムのワークロードと効率性を監視できます。プロトコル速度は過去 2 分間の平均値です。 | • 詳細を表示するには、*ノード*を選択します。次に、グリッド全体、サイト全体、または単一のストレージノードについて、Objects タブを表示します。<br>• 特定の期間の傾向を表示するには、グラフアイコンをクリックします をクリックします。 | • "[オブジェクト（Objects）タブの表示"]<br>• "S3 を使用する"<br>• "Swift を使用します" |

**Nodes**ページを表示します

StorageGRID システムに関する詳しい情報がダッシュボードに表示されるよりも必要な場合は、ノードページを使用して、グリッド全体、グリッド内の各サイト、およびサイトの各ノードの指標を表示できます。




左側のツリービューには、StorageGRID システム内のすべてのサイトおよびすべてのノードが表示されます。各ノードのアイコンは、ノードが接続されているかどうか、またはアクティブなアラートがあるかどうかを示します。

接続状態アイコン

ノードがグリッドから切断されている場合、ツリービューには、基盤となるアラートのアイコンではなく、青またはグレーの接続状態アイコンが表示されます。

- * 接続されていません - 不明 * ：不明な理由でノードがグリッドに接続されていません。たとえば、ノード間のネットワーク接続が失われた、電源が切れたなどの原因が考えられます。* Unable to

communicate with node * アラートがトリガーされる場合もあります。他のアラートもアクティブになる可能性があります。この状況にはすぐに対処する必要があります。

> 管理されたシャットダウン処理の実行中に、ノードが Unknown と表示されることがありますこのような場合、 Unknown 状態は無視してかまいません。

- * 接続されていません - 管理上の理由により停止して：ノードが想定される理由でグリッドに接続されていません。たとえば、ノードまたはノード上のサービスが正常にシャットダウンされた、ノードがリブート中である、ソフトウェアのアップグレード中であるなどの原因が考えられます。1 つ以上のアラートがアクティブになっている可能性もあります。

警告アイコン

ノードがグリッドに接続されている場合、ノードに現在アラートがあるかどうかに応じて、ツリービューには次のアイコンのいずれかが表示されます。

- * 重要 *：異常な状態で、 StorageGRID のノードやサービスの通常の動作が停止しています。基盤となる問題 にすぐに対処する必要があります。問題 が解決されないと、サービスの停止やデータの損失を招くおそれがあります。
- * メジャー *：異常な状態で、現在の処理に影響しているか、重大アラートのしきい値に近づいています。Major アラートを調査し、根本的な問題に対処して、異常な状態が発生した場合に StorageGRID のノードやサービスが正常に動作しなくなる事態を防ぐ必要があります。
- * マイナー *：システムは正常に動作していますが、継続するとシステムの動作に影響する可能性がある異常な状態が発生しています。自動的にクリアされない Minor アラートを監視し、解決して、深刻な問題が生じないようにする必要があります。
- * 標準 *：アクティブなアラートはなく、ノードがグリッドに接続されています。

システム、サイト、またはノードの詳細を表示する

利用可能な情報を表示するには、左側の該当するリンクをクリックします。

- グリッド名を選択すると、 StorageGRID システム全体の統計が要約して表示されます。（スクリーンショットには、 StorageGRID Deployment という名前のシステムが示されています）。
- 特定のデータセンターサイトを選択すると、そのサイトのすべてのノードの統計が要約して表示されます。
- 特定のノードを選択すると、そのノードの詳細情報が表示されます。

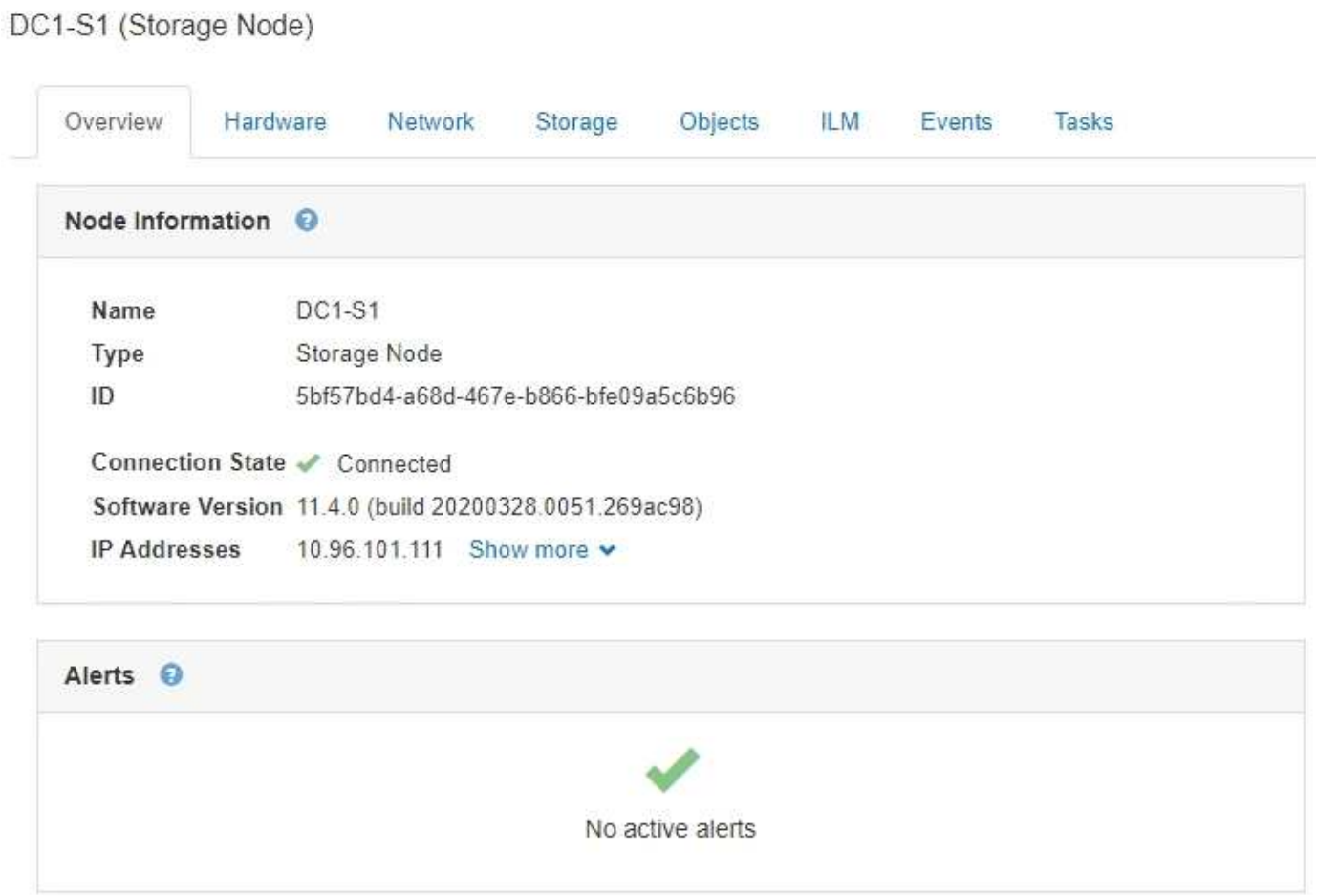
概要タブを表示します

## Overview タブには ' 各ノードに関する基本的な情報が表示されますまた、ノードに現在影響しているアラートも表示されます。

すべてのノードの Overview （概要）タブが表示されます。

ノード情報

Overview （概要）タブの Node Information （ノード情報）セクションには、グリッドノードに関する基本情報が表示されます。



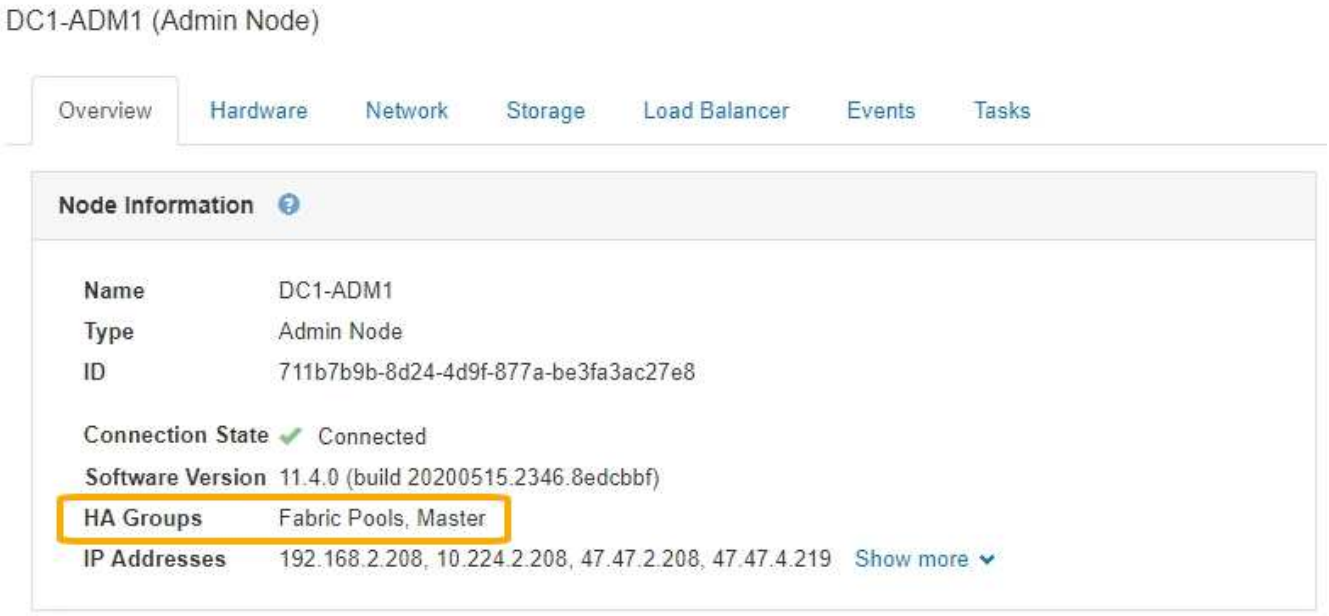

ノードの概要情報には次のものがあります。

- * Name * ：ノードに割り当てられたホスト名で、 Grid Manager に表示されます。
- タイプ：ノードのタイプ-管理ノード、ストレージノード、ゲートウェイノード、またはアーカイブノード。
- * ID * ：ノードの一意の識別子。 UUID とも呼ばれます。
- 接続状態：3つの状態のいずれか。最も重大な状態のアイコンが表示されます。
  - * 接続されていません - 不明 * ：不明な理由でノードがグリッドに接続されていません。たとえば、ノード間のネットワーク接続が失われた、電源が切れたなどの原因が考えられます。* Unable to communicate with node * アラートがトリガーされる場合もあります。他のアラートもアクティブになる可能性があります。この状況にはすぐに対処する必要があります。

    管理されたシャットダウン処理の実行中に、ノードが Unknown と表示されることがありますこのような場合、 Unknown 状態は無視してかまいません。

  - * 接続されていません - 管理上の理由により停止して ：ノードが想定される理由でグリッドに接続されていません。たとえば、ノードまたはノード上のサービスが正常にシャットダウンされた、ノードがリブート中である、ソフトウェアのアップグレード中であるなどの原因が考えられます。1 つ以上のアラートがアクティブになっている可能性もあります。
  - * 接続済み * ：ノードがグリッドに接続されています。
- * Software Version * ：ノードにインストールされているStorageGRID のバージョン。

- * HAグループ*：管理ノードとゲートウェイノードのみ。ノードのネットワークインターフェイスがハイアベイラビリティグループに含まれている場合、およびそのインターフェイスがマスターかバックアップかが表示されます。




- * ip addresses *：ノードのIPアドレス。Show More *をクリックして、ノードのIPv4およびIPv6アドレスとインターフェイスマッピングを表示します。
  - eth0：グリッドネットワーク
  - eth1：管理ネットワーク
  - eth2：クライアントネットワーク

アラート

Overview （概要）タブの Alerts （アラート）セクションには、サイレント化されていないこのノードに現在影響しているアラートがすべて表示されます。アラート名をクリックすると、その他の詳細情報や推奨される対処方法が表示されます。

関連情報

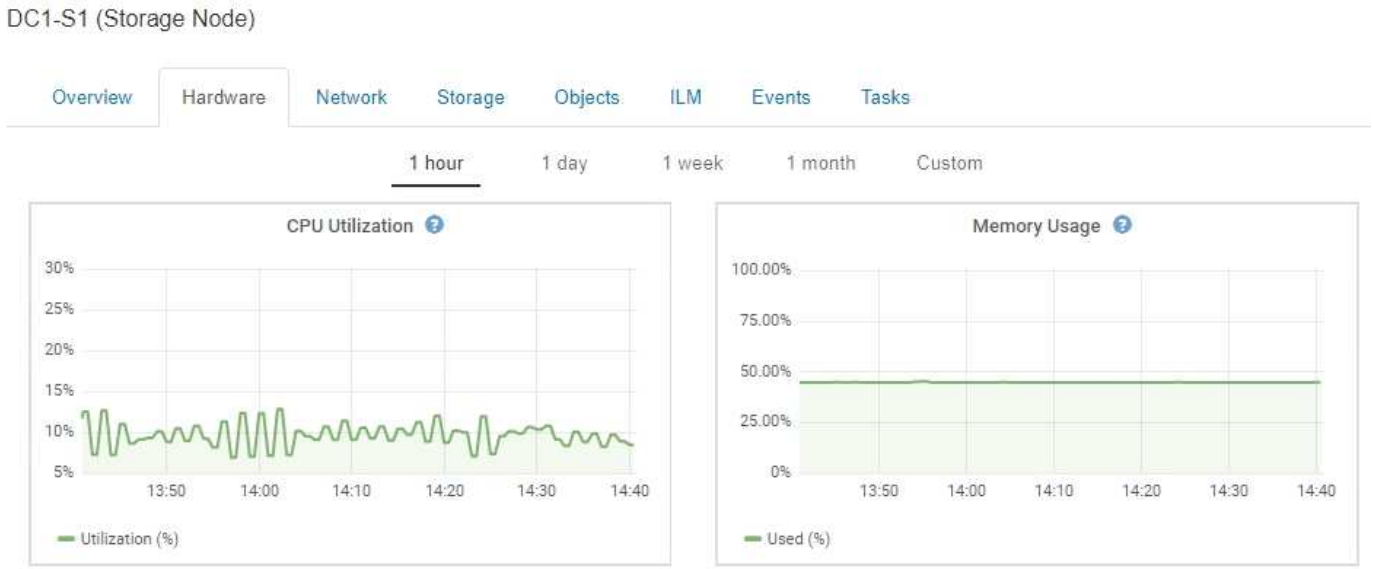
"ノードの接続状態を監視しています"

"現在のアラートの表示"

"特定のアラートの表示"

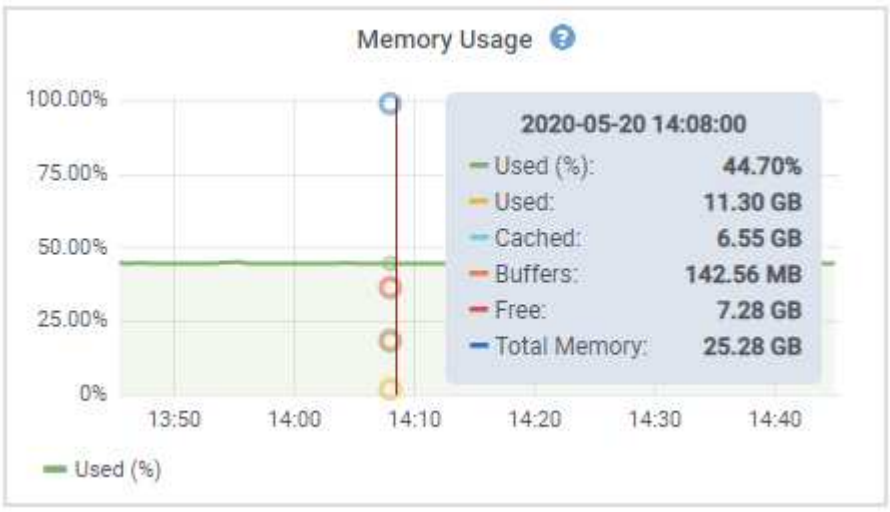
# Hardware タブには、各ノードの CPU 利用率とメモリ使用量、およびアプライアンスに関する追加のハードウェア情報が表示されます。

すべてのノードの Hardware （ハードウェア）タブが表示されます。




別の期間を表示するには、グラフまたはグラフの上にあるコントロールのいずれかを選択します。1 時間、 1 日、 1 週間、または 1 カ月の期間の情報を表示できます。また、カスタムの間隔を設定して、日時の範囲を指定することもできます。

CPU とメモリの使用率に関する詳細を表示するには、各グラフにカーソルを合わせます。




ノードがアプライアンスノードの場合は、アプライアンスハードウェアに関する詳細情報を含むセクションも表示されます。

関連情報

"アプライアンスストレージノードに関する情報の表示"

"アプライアンスの管理ノードとゲートウェイノードに関する情報の表示"

# Network タブには、ノード、サイト、またはグリッド上のすべてのネットワークインターフェイスで送受信されたネットワークトラフィックがグラフで表示されます。

ネットワークタブは、すべてのノード、各サイト、およびグリッド全体に対して表示されます。

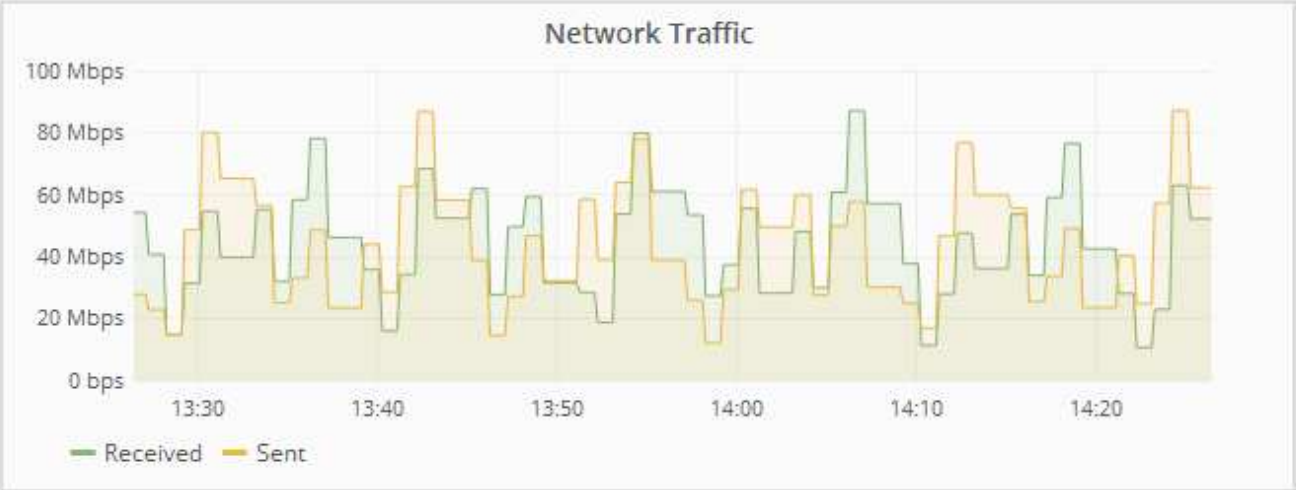
別の期間を表示するには、グラフまたはグラフの上にあるコントロールのいずれかを選択します。1 時間、 1 日、 1 週間、または 1 カ月の期間の情報を表示できます。また、カスタムの間隔を設定して、日時の範囲を指定することもできます。

ノードの場合、各ノードの物理ネットワークポートに関する情報がネットワークインターフェイスの表に表示されます。Network Communicationsテーブルには、各ノードの送受信操作の詳細と、ドライバから報告された障害カウンタが表示されます。

DC1-S1-226 (Storage Node)

Overview | Hardware | Network | Storage | Objects | ILM | Events

1 hour | 1 day | 1 week | 1 month | 1 year | Custom




## Network Interfaces

| Name | Hardware Address | Speed | Duplex | Auto Negotiate | Link Status |
|---|---|---|---|---|---|
| eth0 | 00:50:56:A8:2A:75 | 10 Gigabit | Full | Off | Up |

## Network Communication

### Receive

| Interface | Data | Packets | Errors | Dropped | Frame Overruns | Frames |
|---|---|---|---|---|---|---|
| eth0 | 738.858 GB | 904,587,345 | 0 | 14,340 | 0 | 0 |

### Transmit

| Interface | Data | Packets | Errors | Dropped | Collisions | Carrier |
|---|---|---|---|---|---|---|
| eth0 | 677.555 GB | 465,715,998 | 0 | 0 | 0 | 0 |

関連情報

"ネットワーク接続およびパフォーマンスの監視"

**Storage**（ストレージ）タブを表示します

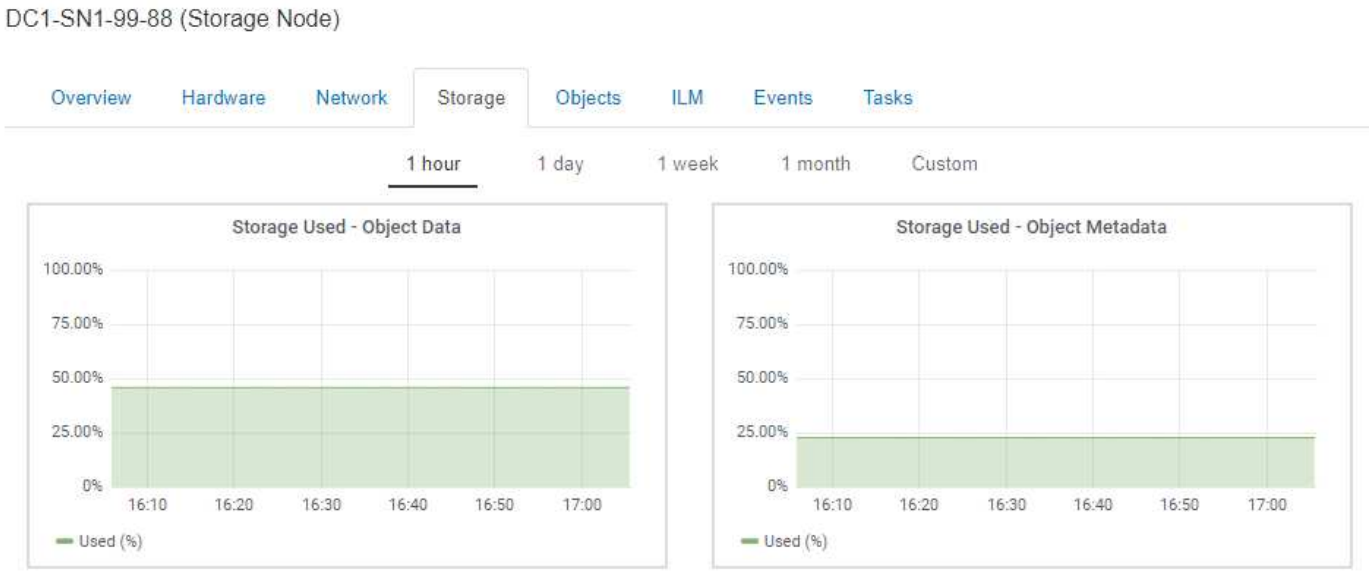
# ストレージタブには、ストレージの可用性やその他のストレージ指標が表示されます。

ストレージタブは、すべてのノード、各サイト、およびグリッド全体に対して表示されます。

## Storage Usedグラフ

ストレージノード、各サイト、およびグリッド全体が対象である場合は、オブジェクトデータとオブジェクトメタデータで一定期間にわたって使用されているストレージの量を示すグラフがストレージタブに表示されます。

サイトまたはグリッドの合計値には、オフラインノードなど、指標が報告されていないノードは 5 分以上含まれません。




## Disk Devices, Volumes, and Object Storeの各テーブルに格納されています

すべてのノードが対象である場合は、ノード上のディスクデバイスとボリュームの詳細が表示されます。ストレージノードの場合、 Object Stores テーブルに各ストレージボリュームの情報が表示されます。

**Disk Devices**

| Name | World Wide Name | I/O Load | Read Rate | Write Rate |
|---|---|---|---|---|
| croot(8:1,sda1) | N/A | 0.03% | 0 bytes/s | 3 KB/s |
| cvloc(8:2,sda2) | N/A | 0.85% | 0 bytes/s | 58 KB/s |
| sdc(8:16,sdb) | N/A | 0.00% | 0 bytes/s | 81 bytes/s |
| sdd(8:32,sdc) | N/A | 0.00% | 0 bytes/s | 82 bytes/s |
| sde(8:48,sdd) | N/A | 0.00% | 0 bytes/s | 82 bytes/s |

**Volumes**

| Mount Point | Device | Status | Size | Available | Write Cache Status |
|---|---|---|---|---|---|
| / | croot | Online | 21.00 GB | 14.90 GB | Unknown |
| /var/local | cvloc | Online | 85.86 GB | 84.10 GB | Unknown |
| /var/local/rangedb/0 | sdc | Online | 107.32 GB | 107.18 GB | Enabled |
| /var/local/rangedb/1 | sdd | Online | 107.32 GB | 107.18 GB | Enabled |
| /var/local/rangedb/2 | sde | Online | 107.32 GB | 107.18 GB | Enabled |

**Object Stores**

| ID | Size | Available | Replicated Data | EC Data | Object Data (%) | Health |
|---|---|---|---|---|---|---|
| 0000 | 107.32 GB | 96.45 GB | 250.90 KB | 0 bytes | 0.00% | No Errors |
| 0001 | 107.32 GB | 107.18 GB | 0 bytes | 0 bytes | 0.00% | No Errors |
| 0002 | 107.32 GB | 107.18 GB | 0 bytes | 0 bytes | 0.00% | No Errors |

関連情報

"グリッド全体のストレージ容量を監視する"

"各ストレージノードのストレージ容量を監視しています"

"各ストレージノードのオブジェクトメタデータ容量を監視します"

[イベント]タブを表示します

## Eventsタブには、ノードのシステムエラーまたは障害イベントの数が表示されます。これには、ネットワークエラーなどのエラーも含まれます。

すべてのノードのEventsタブが表示されます。

特定のノードで問題が発生した場合は、Eventsタブで問題 の詳細を確認できます。テクニカルサポートは、[Events]タブの情報をトラブルシューティングに使用することもできます。

[イベント]タブでは、次のタスクを実行できます。

- 表の上部にある「* Last Event *」フィールドに表示される情報を使用して、最近発生したイベントを特定します。
- グラフアイコンをクリックします をクリックして、そのイベントがいつ発生したかを確認します。

- 問題解決後にイベントの数をゼロにリセットする。

関連情報

"イベントの監視"

"グラフやグラフの表示"

"イベント数のリセット"

**Task**タブを使用して、グリッドノードをリブートします

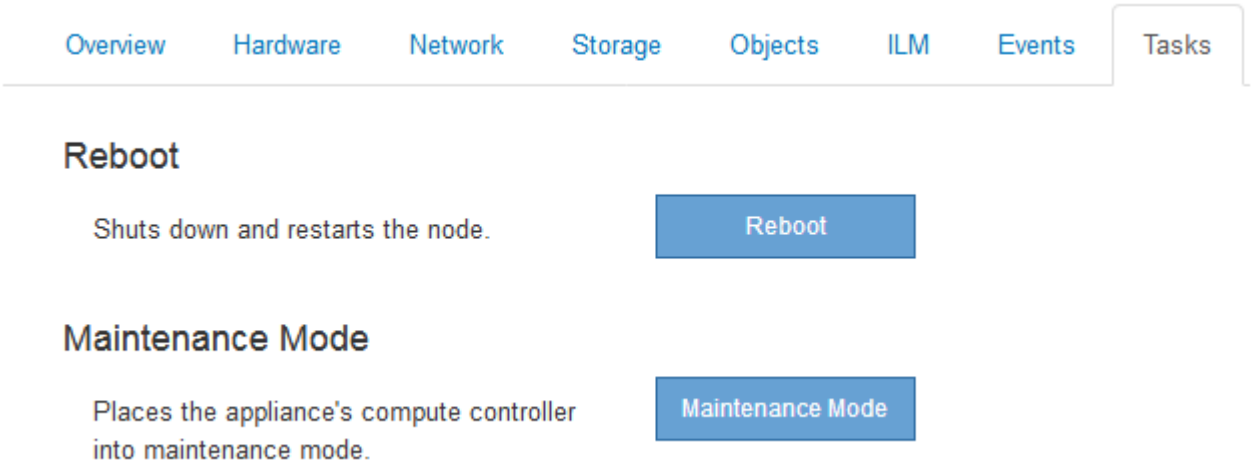
Task タブでは ' 選択したノードを再起動できますすべてのノードの [ タスク ] タブが表示されます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Maintenance または Root Access 権限が必要です。
- プロビジョニングパスフレーズが必要です。

このタスクについて

[ タスク ] タブを使用して、ノードをリブートできます。アプライアンスノードの場合は、 Task タブを使用して、アプライアンスをメンテナンスモードにすることもできます。




- Task タブからグリッドノードをリブートすると、ターゲットノードで reboot コマンドが実行されます。ノードをリブートすると、ノードがシャットダウンして再起動します。すべてのサービスが自動的に再開されます。

  ストレージノードをリブートする場合は、次の点に注意してください。

  - ILM ルールに取り込み動作に Dual commit が指定されている場合、またはルールで Balanced が指定されていて、必要なすべてのコピーをただちに作成できない場合は、 StorageGRID は新たに取り込まれたオブジェクトをただちに同じサイトの 2 つのストレージノードにコミットしてあとから ILM を評価します。1 つのサイトで複数のストレージノードをリブートすると、リブート中はこれらのオブジェクトにアクセスできない場合があります。

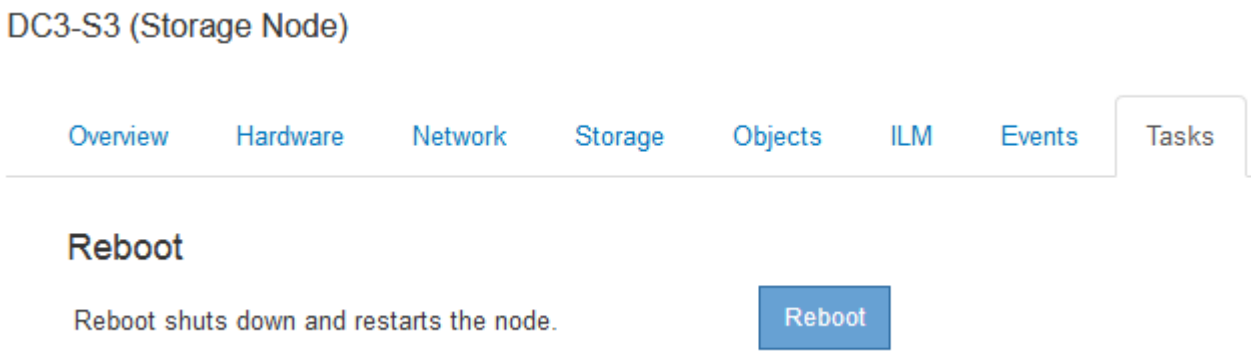
◦ ストレージノードのリブート中もすべてのオブジェクトにアクセスできるようにするには、ノードをリブートする前に、サイトでのオブジェクトの取り込みを約 1 時間停止します。

- リンク設定の変更やストレージコントローラの交換など、特定の手順を実行するために StorageGRID アプライアンスのメンテナンスモードへの切り替えが必要になる場合があります。手順については、アプライアンスのハードウェアの設置とメンテナンスの手順を参照してください。

> アプライアンスをメンテナンスモードにすると、アプライアンスにリモートアクセスできなくなることがあります。

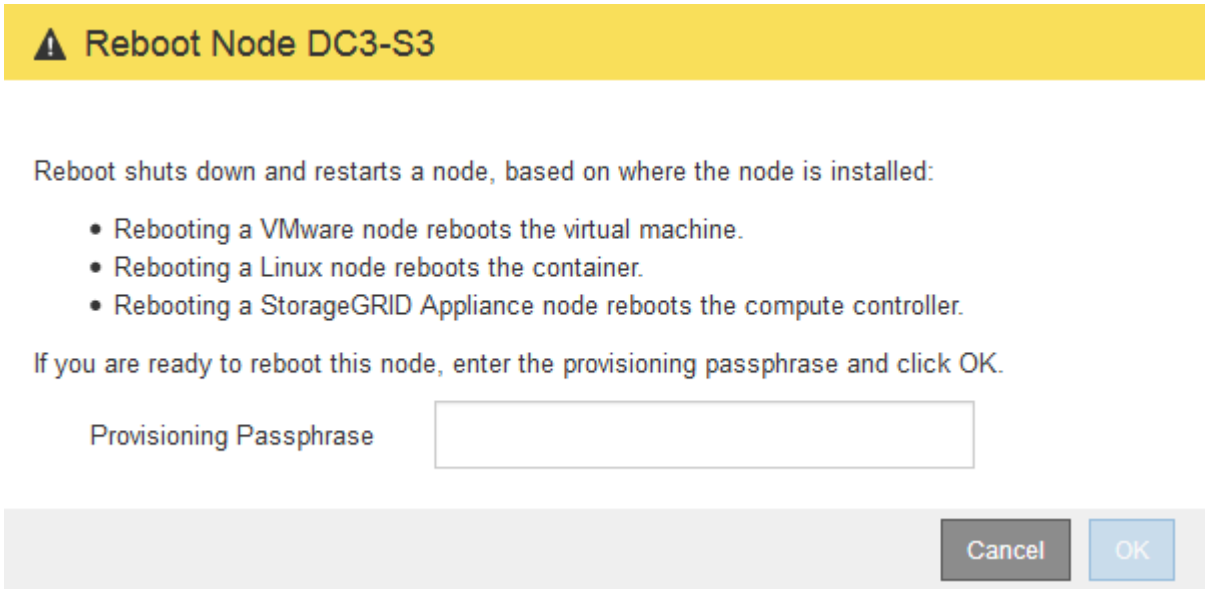
手順

1. [ノード（ Nodes）]を選択し
2. リブートするグリッドノードを選択します。
3. [* タスク * （ Tasks * ） ] タブを選択します。




4. [Reboot]をクリックします。

確認のダイアログボックスが表示されます。




> プライマリ管理ノードをリブートすると、サービスの停止中はブラウザと Grid Manager の接続が一時的に失われることを知らせる確認ダイアログボックスが表示されます。

5. プロビジョニングパスフレーズを入力し、 * OK * をクリックします。
6. ノードがリブートするまで待ちます。

   サービスがシャットダウンするまでに時間がかかる場合があります。

   ノードのリブート中は、Nodesページの左側にグレーのアイコン（Administratively Down）が表示されます。すべてのサービスが再び開始されると、アイコンは元の色に戻ります。

関連情報

"SG6000 ストレージアプライアンス"

"SG5700 ストレージアプライアンス"

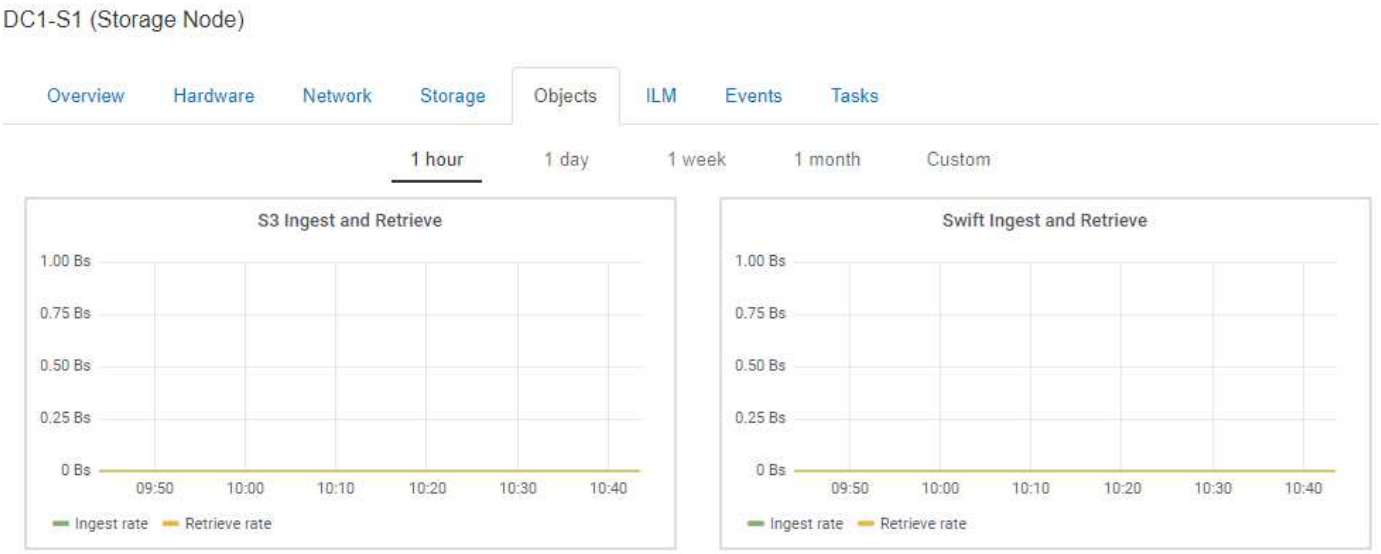
"SG5600 ストレージアプライアンス"

"SG100 SG1000サービスアプライアンス"

**[**オブジェクト（**Objects**）**]**タブの表示

## Objects タブには、 S3 および Swift の取り込み速度と読み出し速度に関する情報が表示されます。

各ストレージノード、各サイト、およびグリッド全体のオブジェクトタブが表示されます。ストレージノードが対象である場合は、オブジェクト数や、メタデータクエリやバックグラウンド検証に関する情報も表示されます。




**Object Counts**

| | |
|---|---|
| Total Objects | 0 |
| Lost Objects | 0 |
| S3 Buckets and Swift Containers | 0 |

**Queries**

| | |
|---|---|
| Average Latency | 5.74 milliseconds |
| Queries - Successful | 12,403 |
| Queries - Failed (timed-out) | 0 |
| Queries - Failed (consistency level unmet) | 0 |

**Verification**

| | |
|---|---|
| Status | No Errors |
| Rate Setting | Adaptive |
| Percent Complete | 0.00% |
| Average Stat Time | 0.00 microseconds |
| Objects Verified | 0 |
| Object Verification Rate | 0.00 objects / second |
| Data Verified | 0 bytes |
| Data Verification Rate | 0.00 bytes / second |
| Missing Objects | 0 |
| Corrupt Objects | 0 |
| Corrupt Objects Unidentified | 0 |
| Quarantined Objects | 0 |

関連情報

"S3 を使用する"

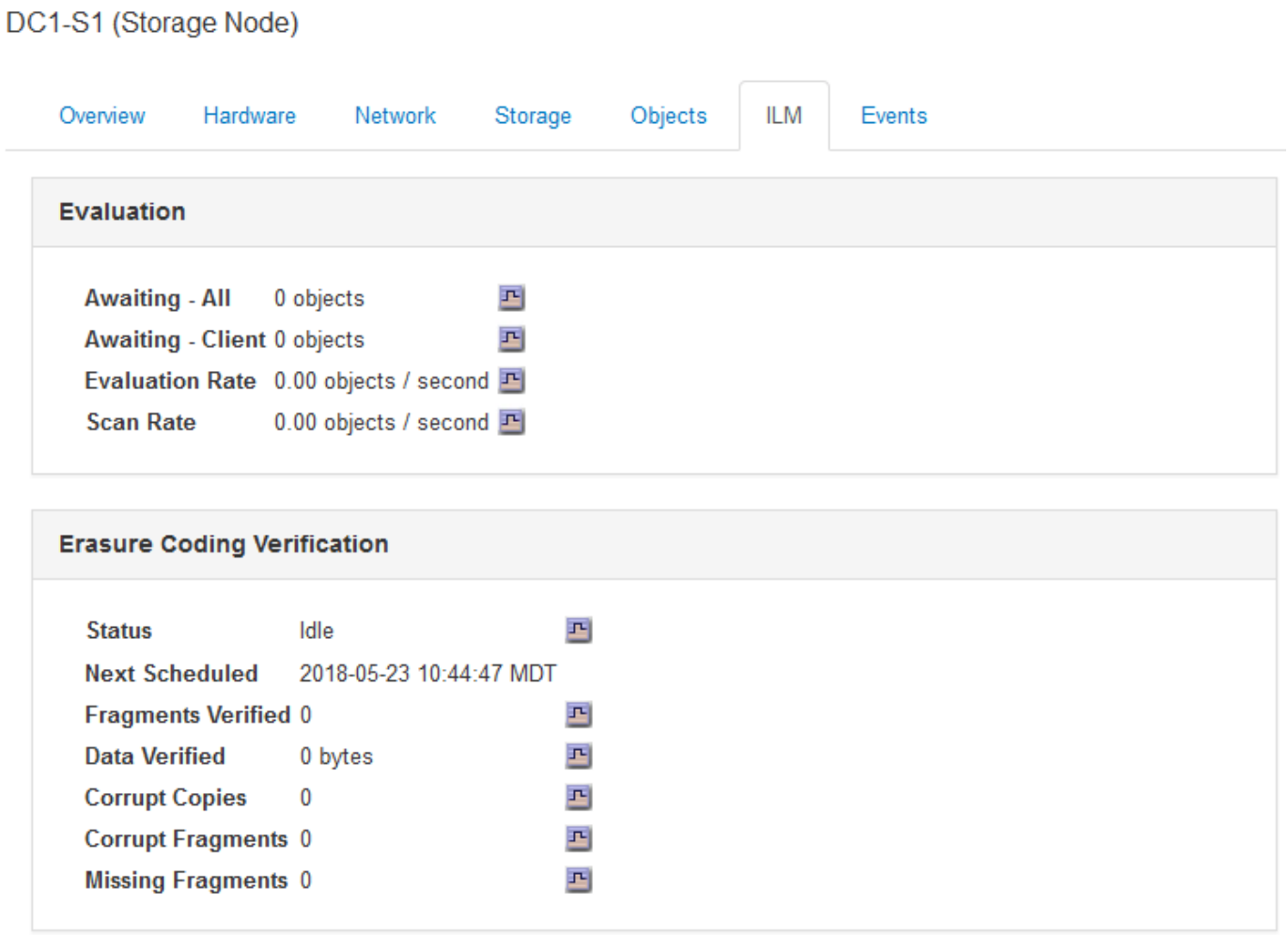
"Swift を使用します"

**ILM**タブの表示

## ILM タブには、情報ライフサイクル管理（ ILM ）処理に関する情報が表示されます。

各ストレージノード、各サイト、およびグリッド全体に対して ILM タブが表示されます。各サイトおよびグリッドが対象である場合は、 ILM キューの状況の推移を示すグラフがこのタブに表示されます。グリッドが対象である場合は、 ILM によるすべてのオブジェクトのフルスキャンが完了するまでの推定時間も表示されます。

ストレージノードが対象である場合は、 ILM 評価およびイレイジャーコーディングオブジェクトのバックグラウンド検証に関する詳細が表示されます。




関連情報

"情報ライフサイクル管理の監視"

"StorageGRID の管理"

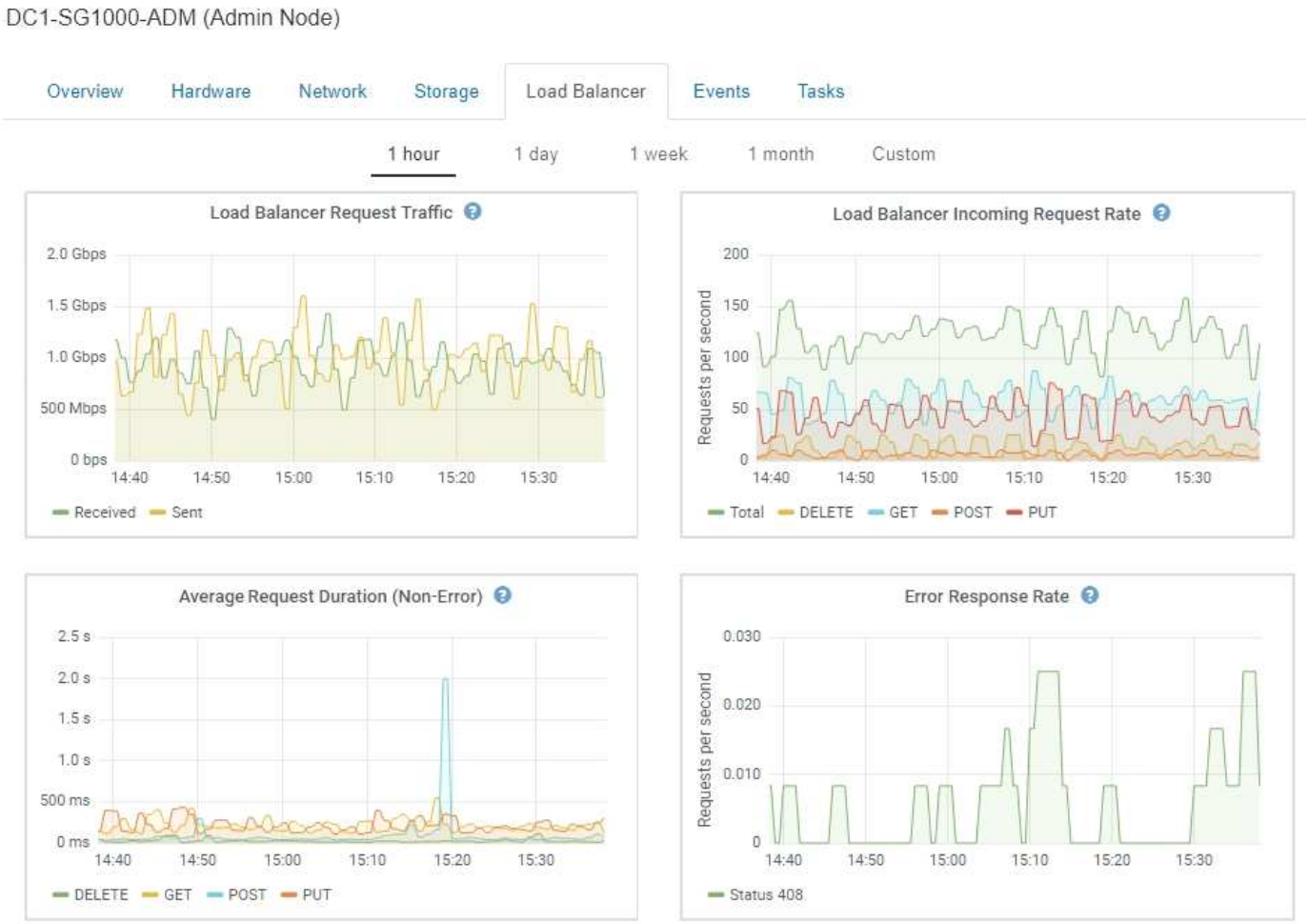
**Load Balancer**タブの表示

## ロードバランサのタブには、ロードバランササービスの動作に関連するパフォーマンスグラフと診断グラフが表示されます。

管理ノードとゲートウェイノード、各サイト、およびグリッド全体が対象の場合は、ロードバランサのタブが

表示されます。各サイトが対象である場合は、そのサイトのすべてのノードの統計が要約して表示されます。グリッド全体が対象である場合は、すべてのサイトの統計が要約して表示されます。

ロードバランササービスで実行されている I/O がない場合、またはロードバランサが設定されていない場合は、グラフに「 No data. 」と表示されます。




ロードバランサ要求のトラフィック

このグラフには、ロードバランサエンドポイントと要求を行っているクライアントの間に送信されたデータのスループットの 3 分間の移動平均が、 1 秒あたりのビット数で示されます。

この値は、各要求が完了した時点で更新されます。そのため、要求数が少ない場合や要求の実行時間が非常に長い場合は、リアルタイムのスループットと異なる場合があります。[ ネットワーク ] タブを見ると、現在のネットワーク動作をよりリアルに表示できます。

ロードバランサの着信要求レート

このグラフには、 1 秒あたりの新しい要求数の 3 分間の移動平均が、要求タイプ（ GET 、 PUT 、 HEAD 、 DELETE ）別に示されます。この値は、新しい要求のヘッダーが検証されると更新されます。

平均リクエスト時間（エラーなし）

このグラフには、要求期間の 3 分間の移動平均が、要求タイプ（ GET 、 PUT 、 HEAD 、 DELETE ）別に示

されます。要求期間は、要求ヘッダーがロードバランササービスによって解析された時点から始まり、完全な応答本文がクライアントに返された時点で終了します。

エラー応答速度

このグラフには、 1 秒あたりにクライアントに返されたエラー応答数の 3 分間の移動平均が、エラー応答コード別に示されます。

関連情報

"ロードバランシング処理の監視"

"StorageGRID の管理"

プラットフォームサービスタブの表示

## プラットフォームサービスタブには、サイトでのS3プラットフォームサービスの処理に関する情報が表示されます。

各サイトの[プラットフォームサービス]タブが表示されます。このタブには、 CloudMirror レプリケーションや検索統合サービスなどの S3 プラットフォームサービスに関する情報が表示されます。このタブのグラフには、保留中の要求数、要求の完了率、要求の失敗率などの指標が表示されます。

トラブルシューティングの詳細など、S3プラットフォームサービスの詳細については、StorageGRID の管理手順を参照してください。

関連情報

"StorageGRID の管理"

アプライアンスストレージノードに関する情報の表示

ノードページには、各アプライアンスストレージノードのサービスの健常性と、すべてのコンピューティング、ディスクデバイス、およびネットワークリソースに関する情報が表示されます。メモリ、ストレージハードウェア、コントローラファームウェアのバ

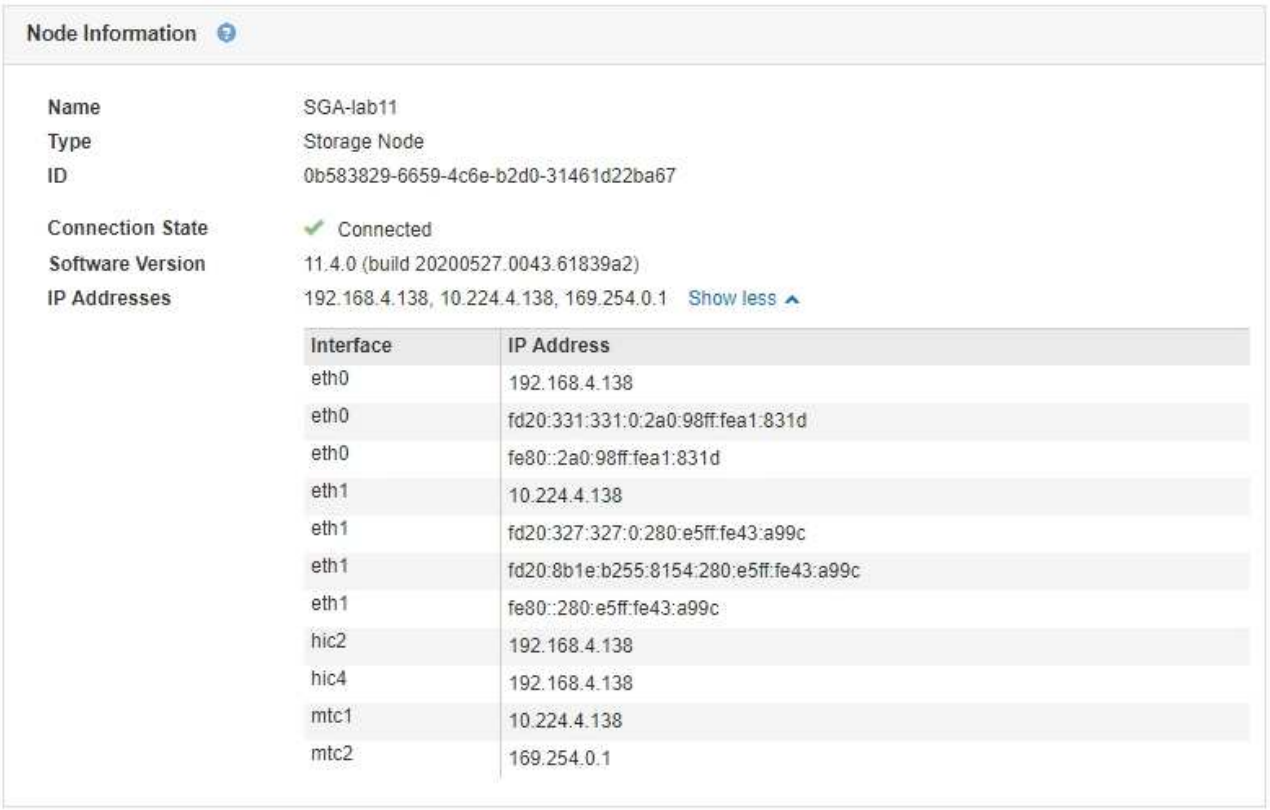
ージョン、ネットワークリソース、ネットワークインターフェイスも表示されます。ネットワークアドレス、およびデータの送受信。

手順

1. ノードページで、アプライアンスストレージノードを選択します。
2. 「 * 概要 * 」を選択します。

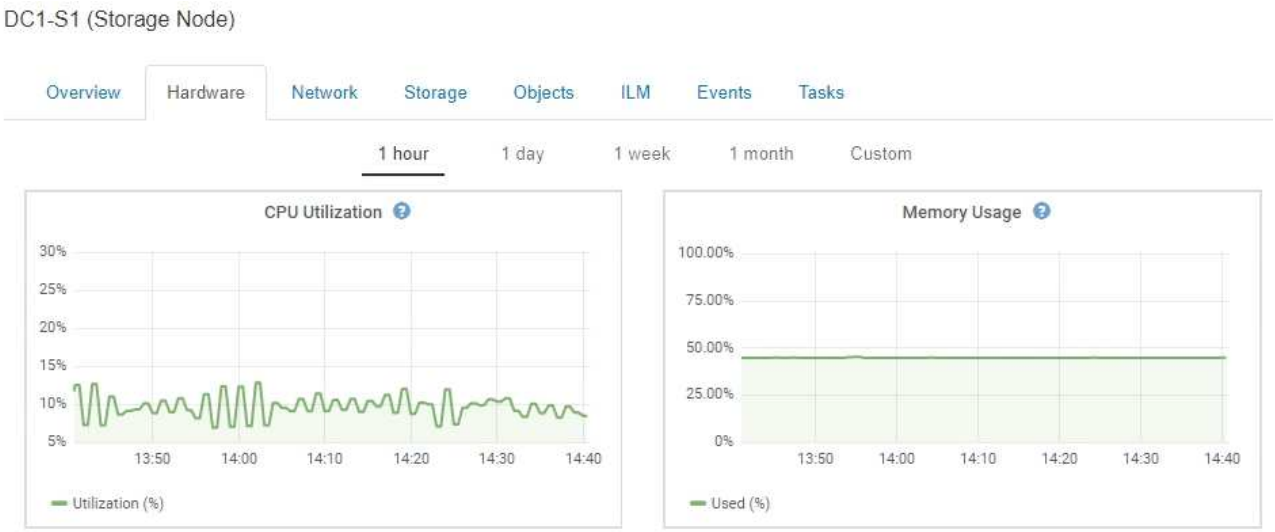
   OverviewタブのNode Informationテーブルには'ノードのIDと名前'ノードのタイプ'インストールされているソフトウェアのバージョン'およびノードに関連付けられているIPアドレスが表示されます[Interface]列には、次のようにインターフェイスの名前が表示されます。

   - * eth * ：グリッドネットワーク、管理ネットワーク、またはクライアントネットワーク。
   - * HIC * ：アプライアンスの 10 、 25 、または 100GbE の物理ポートの 1 つ。これらのポートをボンディングして、 StorageGRID のグリッドネットワーク（ eth0 ）とクライアントネットワーク（ eth2 ）に接続できます。
   - * mtc * ：アプライアンス上の物理1GbEポートの1つ。ボンディングまたはエイリアスを設定し、StorageGRID 管理ネットワーク（eth1）に接続できます。




3. アプライアンスの詳細情報を表示するには、「 * Hardware * 」を選択します。

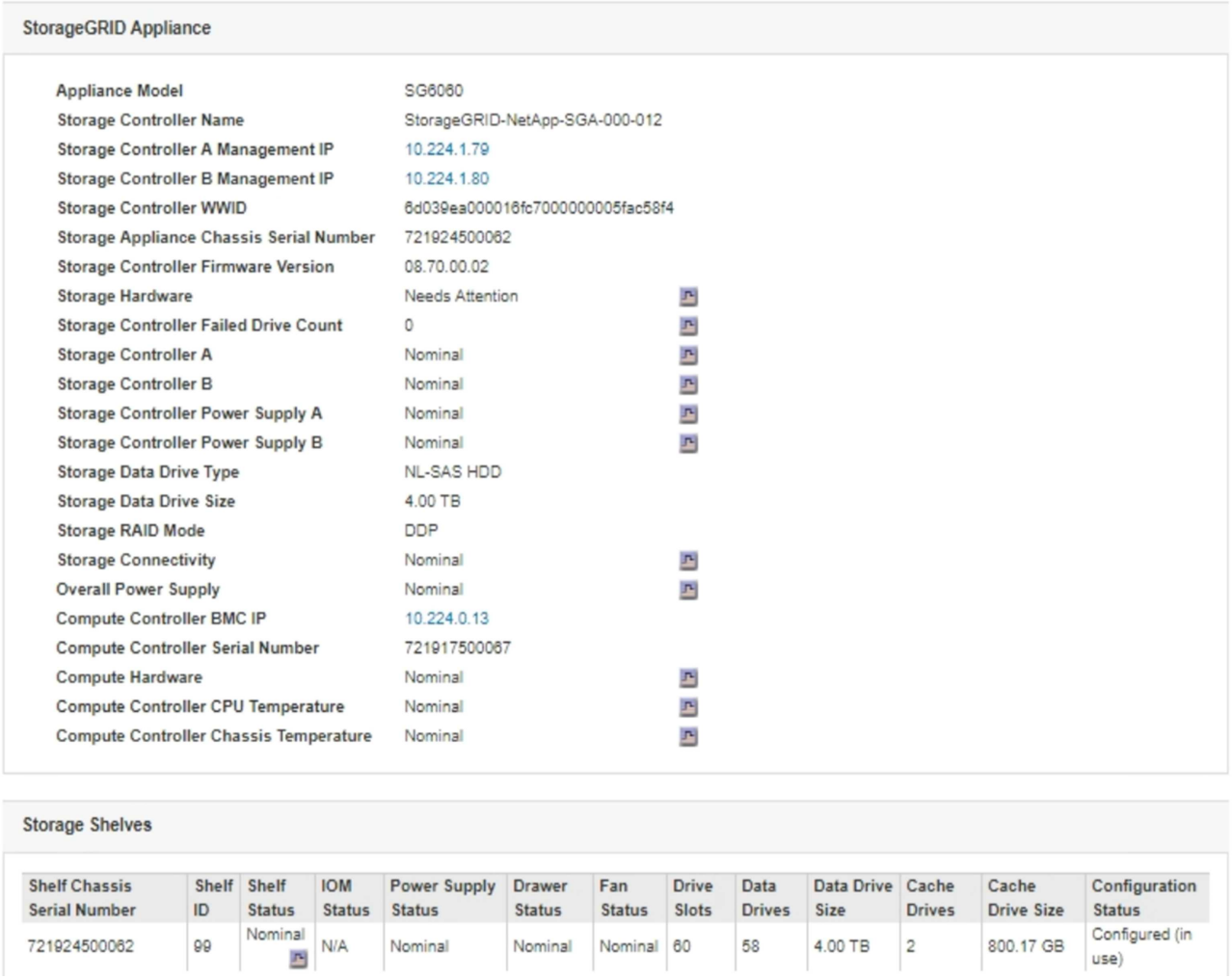
   a. CPU Utilization および Memory のグラフで、一定期間の CPU およびメモリ使用量の割合を確認します。別の期間を表示するには、グラフまたはグラフの上にあるコントロールのいずれかを選択します。1 時間、 1 日、 1 週間、または 1 カ月の期間の情報を表示できます。また、カスタムの間隔を設定して、日時の範囲を指定することもできます。




b. 下にスクロールして、アプライアンスのコンポーネントの表を表示します。この表には、アプライアンスのモデル名、コントローラ名、シリアル番号、 IP アドレス、各コンポーネントのステータスなどの情報が含まれています。

> Compute Controller BMC IPやCompute Hardwareなどの一部のフィールドは、その機能を持つアプライアンスに対してのみ表示されます。

ストレージシェルフのコンポーネントと拡張シェルフが設置に含まれている場合は、アプライアンステーブルの下の個別のテーブルに表示されます。




| **Appliance** テーブルのフィールド | 説明 |
| --- | --- |
| アプライアンスモデル | SANtricity ソフトウェアに表示されるこの StorageGRID アプライアンスのモデル番号。 |
| ストレージコントローラ名 | SANtricity ソフトウェアに表示されるこの StorageGRID アプライアンスの名前。 |
| ストレージコントローラAの管理IP | ストレージコントローラ A 上の管理ポート 1 の IP アドレスストレージの問題をトラブルシューティングするには、この IP を使用して SANtricity ソフトウェアにアクセスします。 |
| ストレージコントローラBの管理IP | ストレージコントローラ B 上の管理ポート 1 の IP アドレスストレージの問題をトラブルシューティングするには、この IP を使用して SANtricity ソフトウェアにアクセスします。<br><br>一部のアプライアンスモデルには、ストレージコントローラ B がありません |

| **Appliance** テーブルのフィールド | 説明 |
| --- | --- |
| ストレージコントローラWWID | SANtricity ソフトウェアに表示されるストレージコントローラの World-Wide Identifier 。 |
| ストレージアプライアンスのシャーシのシリアル番号 | アプライアンスのシャーシのシリアル番号。 |
| ストレージコントローラのファームウェアバージョン | このアプライアンスのストレージコントローラ上のファームウェアのバージョン。 |
| ストレージハードウェア | ストレージコントローラハードウェアの全体的なステータス。SANtricity System Manager からストレージハードウェアの要注意のステータスが報告された場合、 StorageGRID システムからも報告されます。<br><br>ステータスが「 Needs Attention 」の場合は、まず SANtricity ソフトウェアを使用してストレージコントローラをチェックします。次に、コンピューティングコントローラに関するアラームが他にないことを確認します。 |
| ストレージコントローラ障害ドライブ数 | 最適な状態でないドライブの数。 |
| ストレージコントローラ A | ストレージコントローラ A のステータス |
| ストレージコントローラ B | ストレージコントローラ B のステータス一部のアプライアンスモデルには、ストレージコントローラ B がありません |
| ストレージコントローラの電源装置A | ストレージコントローラの電源装置 A のステータス。 |
| ストレージコントローラの電源装置B | ストレージコントローラの電源装置 B のステータス。 |
| ストレージデータドライブタイプ | アプライアンスのドライブのタイプ。 HDD （ハードディスクドライブ）や SSD （ソリッドステートドライブ）など。 |
| ストレージデータドライブサイズ | アプライアンス内のすべてのデータドライブの合計容量。 |
| Storage RAID Mode（ストレージRAIDモード） | アプライアンスに設定されている RAID モード。 |
| ストレージ接続 | ストレージ接続の状態。 |

| **Appliance** テーブルのフィールド | 説明 |
| --- | --- |
| 全体的な電源装置 | アプライアンスのすべての電源装置のステータス。 |
| Compute Controller BMC IPの略 | コンピューティングコントローラ内の Baseboard Management Controller （ BMC ；ベースボード管理コントローラ）ポートの IP アドレス。この IP を使用して BMC インターフェイスに接続し、アプライアンスハードウェアを監視および診断します。<br><br>このフィールドは、 BMC が含まれないアプライアンスモデルに対しては表示されません。 |
| コンピューティングコントローラのシリアル番号 | コンピューティングコントローラのシリアル番号。 |
| コンピューティングハードウェア | コンピューティングコントローラハードウェアのステータス。このフィールドは、コンピューティングハードウェアとストレージハードウェアが個別に用意されていないアプライアンスモデルに対しては表示されません。 |
| コンピューティングコントローラの CPU 温度 | コンピューティングコントローラの CPU の温度ステータス。 |
| コンピューティングコントローラシャーシの温度 | コンピューティングコントローラの温度ステータス。 |

+

| ストレージシェルフテーブルの列 | 説明 |
| --- | --- |
| シェルフシャーシのシリアル番号 | ストレージシェルフシャーシのシリアル番号。 |
| シェルフ ID | ストレージシェルフの数値識別子。<br><br>• 99 ：ストレージコントローラシェルフ<br>• 0 ：最初の拡張シェルフ<br>• 1 ： 2 台目の拡張シェルフ<br>◦ 注： * 拡張シェルフは SG6060 にのみ適用されます。 |
| シェルフステータス | ストレージシェルフの全体的なステータス。 |
| IOMのステータス | 拡張シェルフの入出力モジュール（ IOM ）のステータス。拡張シェルフでない場合は N/A 。 |

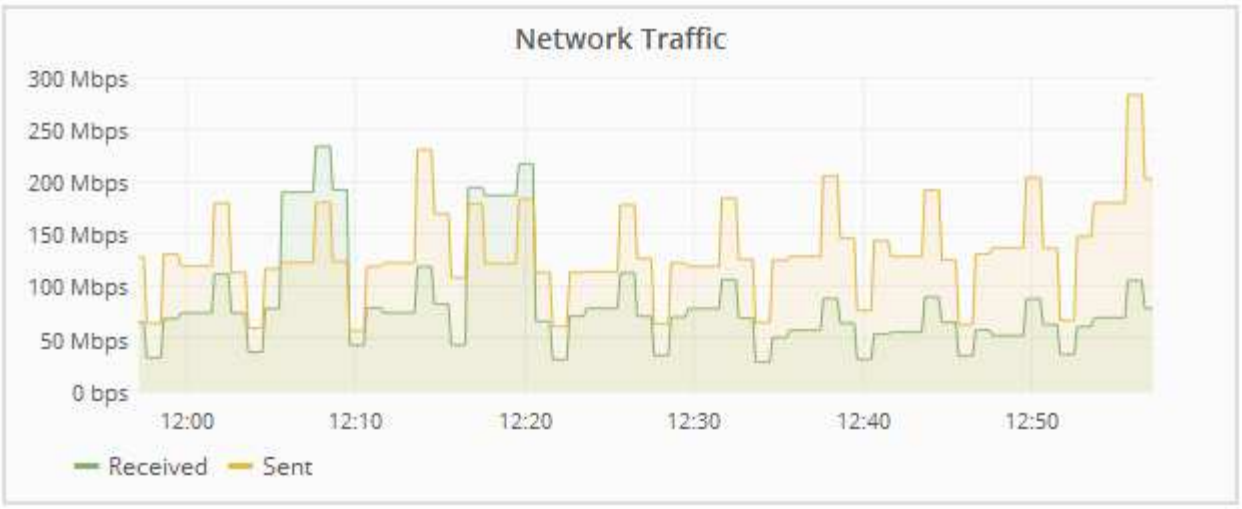
| ストレージシェルフテーブルの列 | 説明 |
| --- | --- |
| 電源装置ステータス | ストレージシェルフの電源装置の全体的なステータス。 |
| ドロワーステータス | ストレージシェルフのドロワーのステータス。N/A は、シェルフにドロワーが搭載されていない場合。 |
| ファンのステータス | ストレージシェルフの冷却ファンの全体的なステータス。 |
| ドライブスロット | ストレージシェルフ内のドライブスロットの総数。 |
| データドライブ | ストレージシェルフ内の、データストレージに使用されるドライブの数。 |
| データドライブサイズ | ストレージシェルフ内の 1 つのデータドライブの実効サイズ。 |
| キャッシュドライブ | ストレージシェルフ内のキャッシュとして使用されるドライブの数。 |
| キャッシュドライブサイズ | ストレージシェルフ内で最小のキャッシュドライブのサイズ。通常、キャッシュドライブのサイズはすべて同じです。 |
| 構成ステータス | ストレージシェルフの設定ステータス。 |

4. すべてのステータスが「 Nominal 」であることを確認します。

   ステータスが「公称」でない場合は、現在のアラートを確認します。SANtricity System Manager を使用して、これらのハードウェアの値の一部を確認することもできます。アプライアンスの設置とメンテナンスの手順を参照してください。

5. 各ネットワークの情報を表示するには、「 * ネットワーク * 」を選択します。

   Network Traffic グラフには、ネットワークトラフィック全体のサマリが表示されます。




a. ネットワークインターフェイスセクションを確認します。

**Network Interfaces**

| Name | Hardware Address | Speed | Duplex | Auto Negotiate | Link Status |
|---|---|---|---|---|---|
| eth0 | 50:6B:4B:42:D7:11 | 100 Gigabit | Full | Off | Up |
| eth1 | D8:C4:97:2A:E4:9E | Gigabit | Full | Off | Up |
| eth2 | 50:6B:4B:42:D7:11 | 100 Gigabit | Full | Off | Up |
| hic1 | 50:6B:4B:42:D7:11 | 25 Gigabit | Full | Off | Up |
| hic2 | 50:6B:4B:42:D7:11 | 25 Gigabit | Full | Off | Up |
| hic3 | 50:6B:4B:42:D7:11 | 25 Gigabit | Full | Off | Up |
| hic4 | 50:6B:4B:42:D7:11 | 25 Gigabit | Full | Off | Up |
| mtc1 | D8:C4:97:2A:E4:9E | Gigabit | Full | On | Up |
| mtc2 | D8:C4:97:2A:E4:9F | Gigabit | Full | On | Up |

次の表に、 Network Interfaces テーブルの * Speed * 列の値を記載した値を使用して、アプライアンス上の 10 / 25GbE ネットワークポートがアクティブ / バックアップモードと LACP モードのどちらを使用するように設定されているかを判断します。

この表の値は、 4 つのリンクがすべて使用されていることを前提としています。

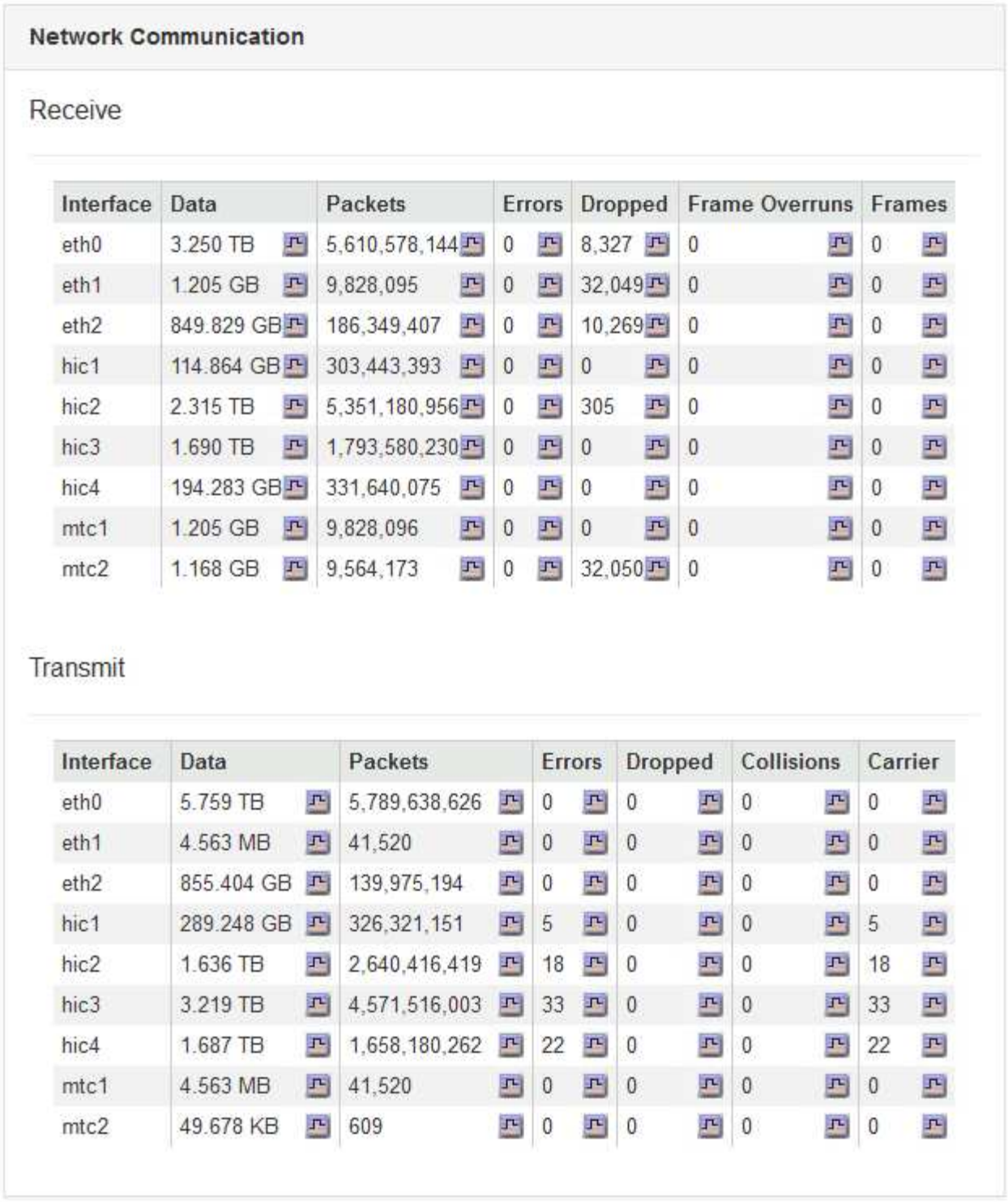
| リンクモード | ボンディングモード | 個々の **HIC** リンク速度（ **hic1** 、 **hic2** 、 **hic3** 、 **hic4** ） | 想定されるグリッド / クライアントネットワーク速度（ **eth0** 、 **eth2** ） |
|---|---|---|---|
| アグリゲート | LACP | 25 | 100 |
| 固定（ Fixed ） | LACP | 25 | 50 |

| リンクモード | ボンディングモード | 個々の **HIC** リンク速度（ **hic1** 、 **hic2** 、 **hic3** 、 **hic4** ） | 想定されるグリッド / クライアントネットワーク速度（ **eth0** 、 **eth2** ） |
| --- | --- | --- | --- |
| 固定（ Fixed ） | アクティブ / バックアップ | 25 | 25 |
| アグリゲート | LACP | 10. | 40 |
| 固定（ Fixed ） | LACP | 10. | 20 |
| 固定（ Fixed ） | アクティブ / バックアップ | 10. | 10. |

10 / 25GbE ポートの設定の詳細については、ご使用のアプライアンスのインストールおよびメンテナンスの手順を参照してください。

b. 「ネットワーク通信」セクションを確認します。

Receive テーブルと Transmit テーブルには、各ネットワークで送受信されたバイト数とパケット数、およびその他の送受信メトリックが表示されます。



**Network Communication**

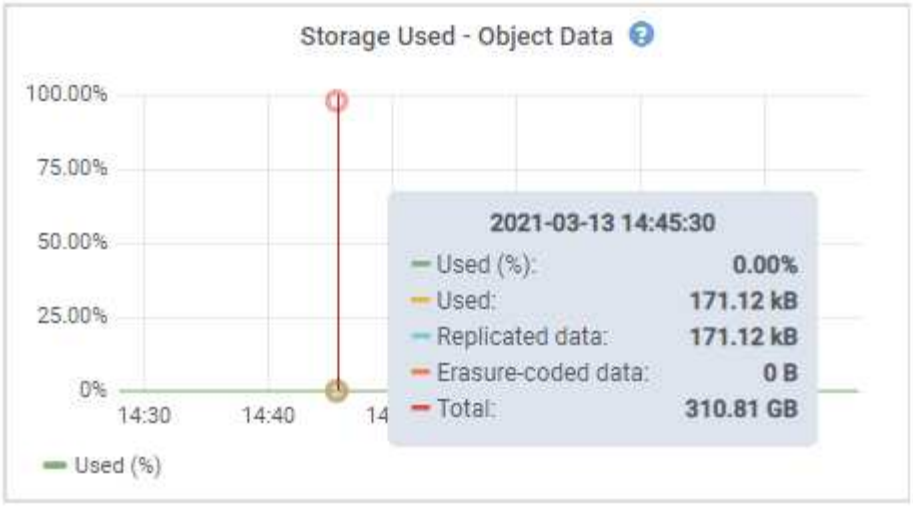
Receive

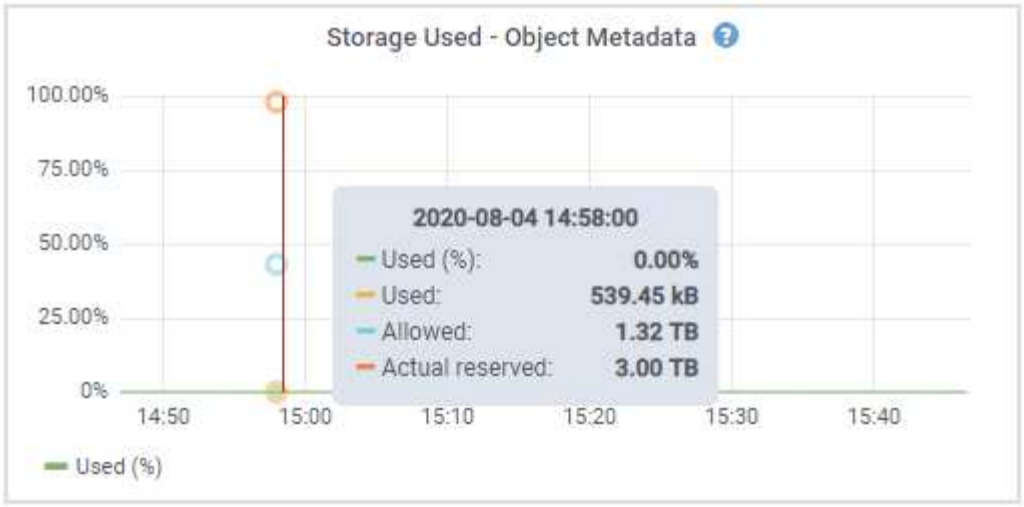
| Interface | Data | Packets | Errors | Dropped | Frame Overruns | Frames |
|---|---|---|---|---|---|---|
| eth0 | 3.250 TB | 5,610,578,144 | 0 | 8,327 | 0 | 0 |
| eth1 | 1.205 GB | 9,828,095 | 0 | 32,049 | 0 | 0 |
| eth2 | 849.829 GB | 186,349,407 | 0 | 10,269 | 0 | 0 |
| hic1 | 114.864 GB | 303,443,393 | 0 | 0 | 0 | 0 |
| hic2 | 2.315 TB | 5,351,180,956 | 0 | 305 | 0 | 0 |
| hic3 | 1.690 TB | 1,793,580,230 | 0 | 0 | 0 | 0 |
| hic4 | 194.283 GB | 331,640,075 | 0 | 0 | 0 | 0 |
| mtc1 | 1.205 GB | 9,828,096 | 0 | 0 | 0 | 0 |
| mtc2 | 1.168 GB | 9,564,173 | 0 | 32,050 | 0 | 0 |

Transmit

| Interface | Data | Packets | Errors | Dropped | Collisions | Carrier |
|---|---|---|---|---|---|---|
| eth0 | 5.759 TB | 5,789,638,626 | 0 | 0 | 0 | 0 |
| eth1 | 4.563 MB | 41,520 | 0 | 0 | 0 | 0 |
| eth2 | 855.404 GB | 139,975,194 | 0 | 0 | 0 | 0 |
| hic1 | 289.248 GB | 326,321,151 | 5 | 0 | 0 | 5 |
| hic2 | 1.636 TB | 2,640,416,419 | 18 | 0 | 0 | 18 |
| hic3 | 3.219 TB | 4,571,516,003 | 33 | 0 | 0 | 33 |
| hic4 | 1.687 TB | 1,658,180,262 | 22 | 0 | 0 | 22 |
| mtc1 | 4.563 MB | 41,520 | 0 | 0 | 0 | 0 |
| mtc2 | 49.678 KB | 609 | 0 | 0 | 0 | 0 |

6. 「 * Storage * 」を選択すると、オブジェクトデータとオブジェクトメタデータに使用されているストレージの割合、およびディスクデバイス、ボリューム、オブジェクトストアに関する情報がグラフに表示されます。




a. 下にスクロールして、各ボリュームとオブジェクトストアに使用可能なストレージ容量を表示します。

   各ディスクの Worldwide Name は、 SANtricity ソフトウェア（アプライアンスのストレージコントローラに接続される管理ソフトウェア）で標準のボリュームプロパティとして表示される、ボリュームの World-Wide Identifier （ WWID ）と同じです。

   ボリュームマウントポイントに関連するディスクの読み取りと書き込みの統計情報を解釈できるように、 Disk Devices テーブルの * Name * 列に表示される名前の最初の部分（つまり、 *sdc_sd*,*sde* ）が Volumes テーブルの * Device * 列に表示される値と一致していることを確認します。

**Disk Devices**

| Name | World Wide Name | I/O Load | Read Rate | Write Rate |
|---|---|---|---|---|
| croot(8:1,sda1) | N/A | 0.03% | 0 bytes/s | 3 KB/s |
| cvloc(8:2,sda2) | N/A | 0.85% | 0 bytes/s | 58 KB/s |
| sdc(8:16,sdb) | N/A | 0.00% | 0 bytes/s | 81 bytes/s |
| sdd(8:32,sdc) | N/A | 0.00% | 0 bytes/s | 82 bytes/s |
| sde(8:48,sdd) | N/A | 0.00% | 0 bytes/s | 82 bytes/s |

**Volumes**

| Mount Point | Device | Status | Size | Available | Write Cache Status |
|---|---|---|---|---|---|
| / | croot | Online | 21.00 GB | 14.90 GB | Unknown |
| /var/local | cvloc | Online | 85.86 GB | 84.10 GB | Unknown |
| /var/local/rangedb/0 | sdc | Online | 107.32 GB | 107.18 GB | Enabled |
| /var/local/rangedb/1 | sdd | Online | 107.32 GB | 107.18 GB | Enabled |
| /var/local/rangedb/2 | sde | Online | 107.32 GB | 107.18 GB | Enabled |

**Object Stores**

| ID | Size | Available | Replicated Data | EC Data | Object Data (%) | Health |
|---|---|---|---|---|---|---|
| 0000 | 107.32 GB | 96.45 GB | 250.90 KB | 0 bytes | 0.00% | No Errors |
| 0001 | 107.32 GB | 107.18 GB | 0 bytes | 0 bytes | 0.00% | No Errors |
| 0002 | 107.32 GB | 107.18 GB | 0 bytes | 0 bytes | 0.00% | No Errors |

関連情報

"SG6000 ストレージアプライアンス"

"SG5700 ストレージアプライアンス"

"SG5600 ストレージアプライアンス"

**SANtricity のSystem Managerタブの表示**

SANtricity の System Manager タブから、ストレージアプライアンスの管理ポートを設定したり接続したりしなくても、 SANtricity の System Manager にアクセスできます。このタブでは、ハードウェア診断と環境情報、およびドライブに関連する問題を確認できます。

ストレージアプライアンスノードの SANtricity System Manager タブが表示されます。

SANtricity システムマネージャを使用すると、次の操作を実行できます。

- ストレージアレイレベルのパフォーマンス、 I/O レイテンシ、ストレージコントローラの CPU 利用率、スループットなどのパフォーマンスデータを表示します
- ハードウェアコンポーネントのステータスを確認します
- 診断データの表示や E シリーズ AutoSupport の設定など、サポート機能を実行

SANtricity システムマネージャを使用して E シリーズ AutoSupport のプロキシを設定するには、管理 StorageGRID の手順を参照してください。

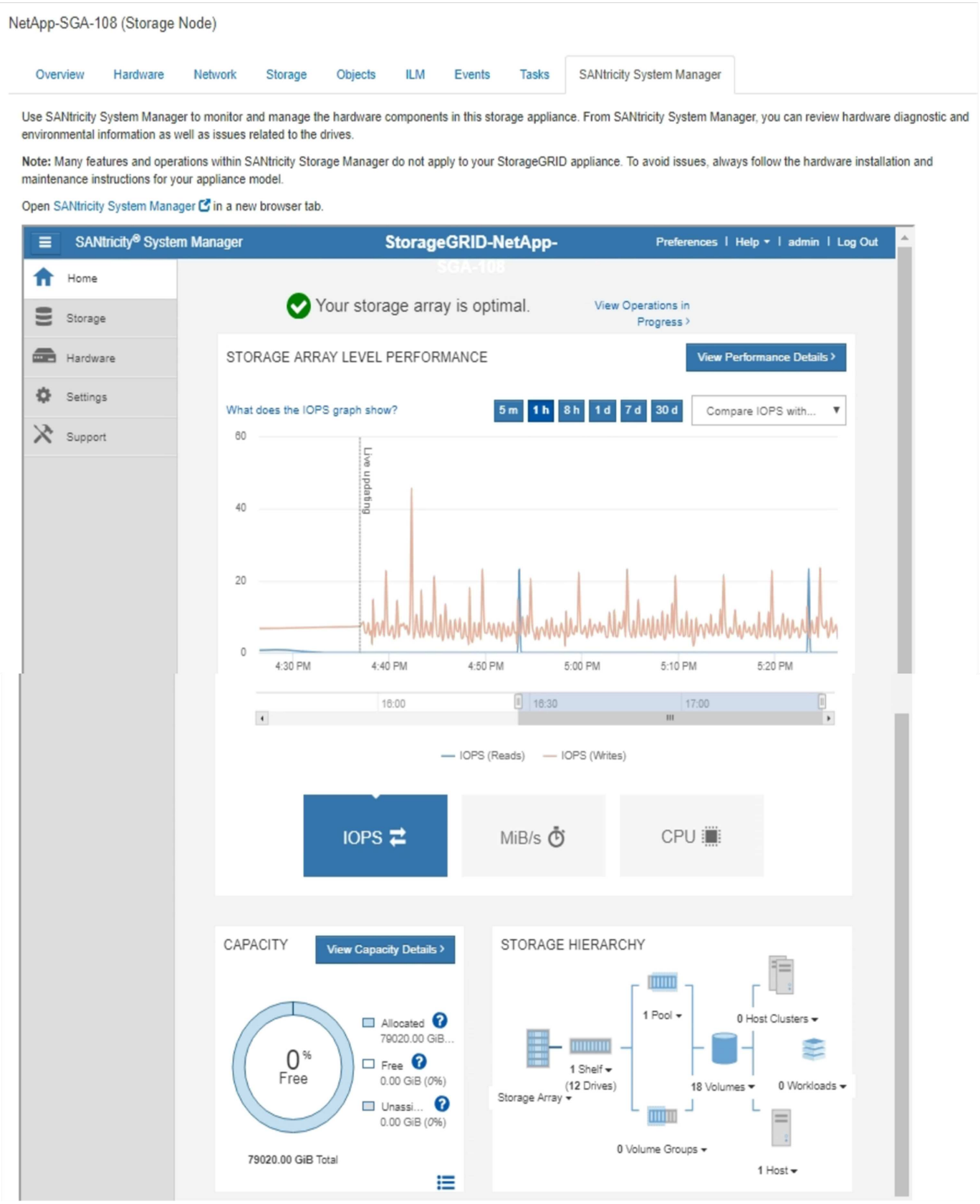
"StorageGRID の管理"

グリッドマネージャを介して SANtricity システムマネージャにアクセスするには、ストレージアプライアンス管理者の権限またはルートアクセス権限が必要です。

Grid Manager を使用して SANtricity System Manager にアクセスするには、 SANtricity ファームウェア 8.70 以降が必要です。

グリッドマネージャから SANtricity システムマネージャにアクセスする手順は、通常、アプライアンスのハードウェアを監視し、 E シリーズ AutoSupport を設定することだけを目的としています。ファームウェアのアップグレードなど、 SANtricity System Manager 内の多くの機能や操作は、 StorageGRID アプライアンスの監視には適用されません。問題を回避するには、アプライアンスのハードウェアの設置とメンテナンスの手順に必ず従ってください。

このタブには、SANtricity システムマネージャのホームページが表示されます




SANtricity System Manager のリンクを使用すると、 SANtricity System Manager を新しいブラウザウィンドウで開いて確認しやすくなります。

ストレージアレイレベルのパフォーマンスと使用容量の詳細を表示するには、各グラフにカーソルを合わせま

す。

SANtricity のSystem Managerタブからアクセスできる情報の表示の詳細については、の情報を参照してください "NetApp Eシリーズシステムのドキュメントセンター"

アプライアンスの管理ノードとゲートウェイノードに関する情報の表示

ノードページには、管理ノードまたはゲートウェイノードに使用される各サービスアプライアンスのサービスの健常性とすべてのコンピューティング、ディスクデバイス、およびネットワークリソースに関する情報が表示されます。メモリ、ストレージハードウェア、ネットワークリソース、ネットワークインターフェイス、ネットワークアドレスも表示できます。 データを送受信します。

手順

1. Nodes ページで、アプライアンスの管理ノードまたはアプライアンスのゲートウェイノードを選択します。
2. 「 * 概要 * 」を選択します。

   OverviewタブのNode Informationテーブルには'ノードのIDと名前'ノードのタイプ'インストールされているソフトウェアのバージョン'およびノードに関連付けられているIPアドレスが表示されます[Interface]列には、次のようにインターフェイスの名前が表示されます。

   - * adllb * および * adlli * ：管理ネットワーク・インターフェイスでアクティブ / バックアップ・ボンディングが使用されている場合に表示されます
   - * eth * ：グリッドネットワーク、管理ネットワーク、またはクライアントネットワーク。
   - * HIC * ：アプライアンスの 10 、 25 、または 100GbE の物理ポートの 1 つ。これらのポートをボンディングして、 StorageGRID のグリッドネットワーク（ eth0 ）とクライアントネットワーク（ eth2 ）に接続できます。
   - * mtc * ：アプライアンス上の物理1GbEポートの1つ。ボンディングまたはエイリアスを設定し、StorageGRID 管理ネットワーク（eth1）に接続できます。

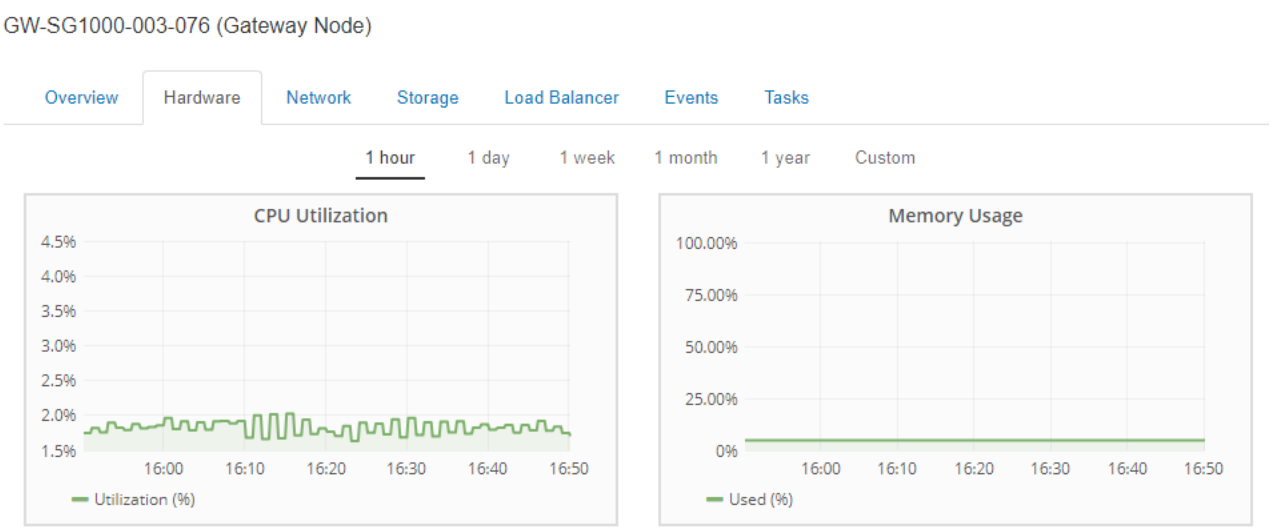
**Node Information**

| | |
|---|---|
| ID | 46702fe0-2bca-4097-8f61-f3fe6b22ed75 |
| Name | GW-SG1000-003-076 |
| Type | Gateway Node |
| Software Version | 11.3.0 (build 20190708.2304.71ba19a) |
| IP Addresses | 169.254.0.1, 172.16.3.76, 10.224.3.76, 47.47.3.76 Show less |

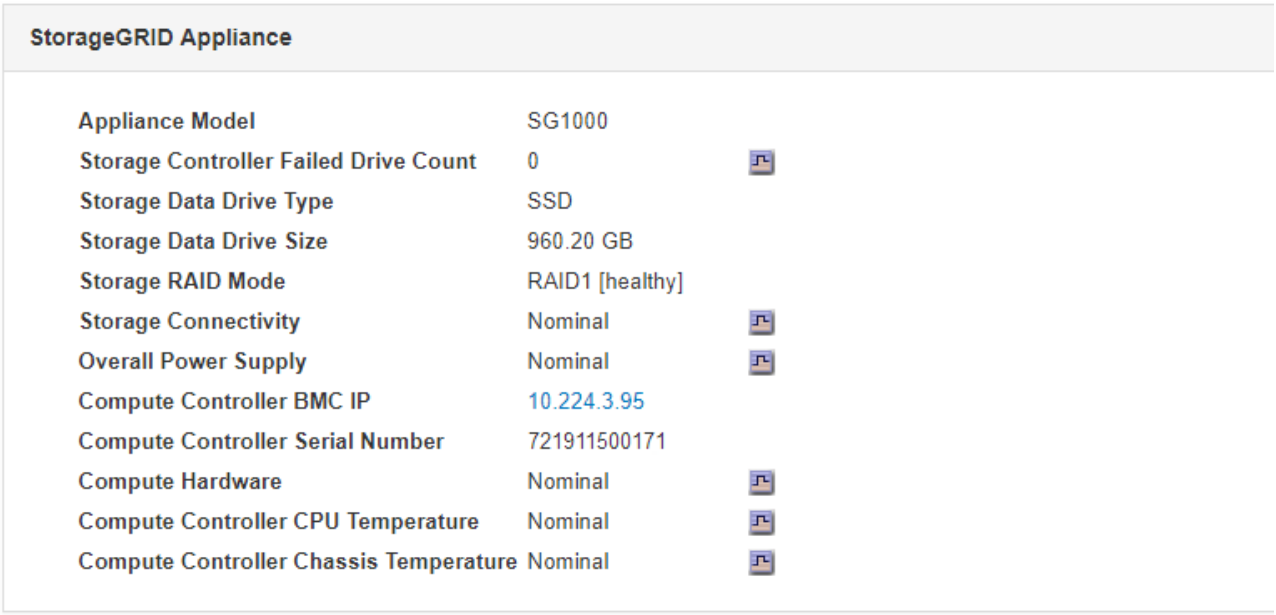
| Interface | IP Address |
|---|---|
| adllb | fe80::c020:17ff:fe59:1cf3 |
| adlli | 169.254.0.1 |
| adlli | fd20:327:327:0:408f:84ff:fe80:a9 |
| adlli | fd20:8b1e:b255:8154:408f:84ff:fe80:a9 |
| adlli | fe80::408f:84ff:fe80:a9 |
| eth0 | 172.16.3.76 |
| eth0 | fd20:328:328:0:9a03:9bff:fe98:a272 |
| eth0 | fe80::9a03:9bff:fe98:a272 |
| eth1 | 10.224.3.76 |
| eth1 | fd20:327:327:0:b6a9:fcff:fe08:4e49 |
| eth1 | fd20:8b1e:b255:8154:b6a9:fcff:fe08:4e49 |
| eth1 | fe80::b6a9:fcff:fe08:4e49 |
| eth2 | 47.47.3.76 |
| eth2 | fd20:332:332:0:9a03:9bff:fe98:a272 |
| eth2 | fe80::9a03:9bff:fe98:a272 |
| hic1 | 47.47.3.76 |
| hic2 | 47.47.3.76 |
| hic3 | 47.47.3.76 |
| hic4 | 47.47.3.76 |
| mtc1 | 10.224.3.76 |
| mtc2 | 10.224.3.76 |

3. アプライアンスの詳細情報を表示するには、「 * Hardware * 」を選択します。

   a. CPU Utilization および Memory のグラフで、一定期間の CPU およびメモリ使用量の割合を確認します。別の期間を表示するには、グラフまたはグラフの上にあるコントロールのいずれかを選択します。1 時間、 1 日、 1 週間、または 1 カ月の期間の情報を表示できます。また、カスタムの間隔を設定して、日時の範囲を指定することもできます。




b. 下にスクロールして、アプライアンスのコンポーネントの表を表示します。この表には、モデル名、シリアル番号、コントローラファームウェアのバージョン、各コンポーネントのステータスなどの情報が含まれています。



**StorageGRID Appliance**

| | |
|---|---|
| **Appliance Model** | SG1000 |
| **Storage Controller Failed Drive Count** | 0 |
| **Storage Data Drive Type** | SSD |
| **Storage Data Drive Size** | 960.20 GB |
| **Storage RAID Mode** | RAID1 [healthy] |
| **Storage Connectivity** | Nominal |
| **Overall Power Supply** | Nominal |
| **Compute Controller BMC IP** | 10.224.3.95 |
| **Compute Controller Serial Number** | 721911500171 |
| **Compute Hardware** | Nominal |
| **Compute Controller CPU Temperature** | Nominal |
| **Compute Controller Chassis Temperature** | Nominal |

| **Appliance** テーブルのフィールド | 説明 |
|---|---|
| アプライアンスモデル | この StorageGRID アプライアンスのモデル番号。 |
| ストレージコントローラ障害ドライブ数 | 最適な状態でないドライブの数。 |
| ストレージデータドライブタイプ | アプライアンスのドライブのタイプ。 HDD （ハードディスクドライブ）や SSD （ソリッドステートドライブ）など。 |
| ストレージデータドライブサイズ | アプライアンス内のすべてのデータドライブの合計容量。 |

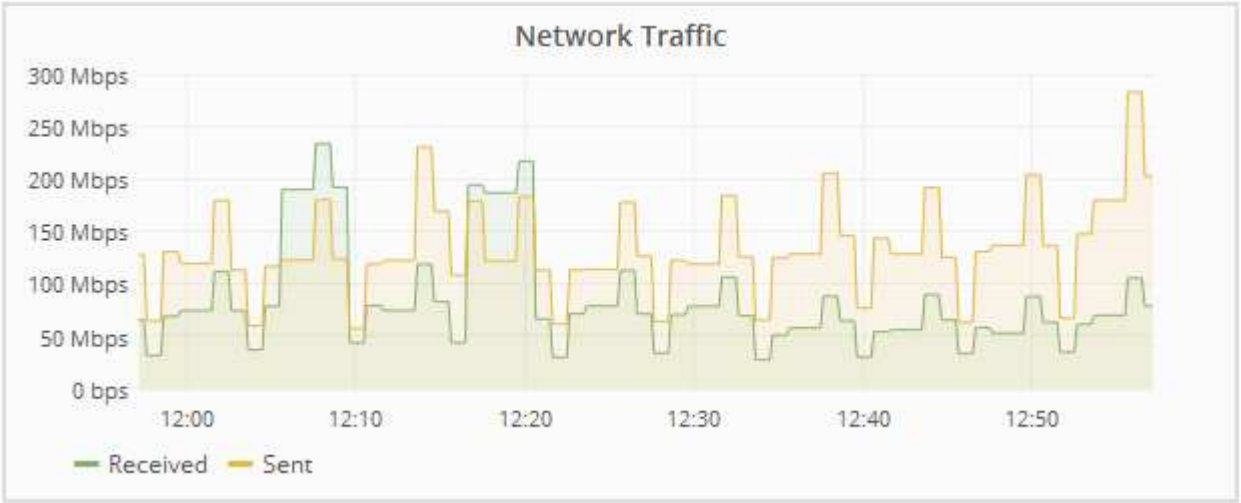
| **Appliance** テーブルのフィールド | 説明 |
| --- | --- |
| Storage RAID Mode（ストレージRAIDモード） | アプライアンスの RAID モード。 |
| 全体的な電源装置 | アプライアンスのすべての電源装置のステータス。 |
| Compute Controller BMC IPの略 | コンピューティングコントローラ内の Baseboard Management Controller （ BMC ；ベースボード管理コントローラ）ポートの IP アドレス。この IP を使用して BMC インターフェイスに接続し、アプライアンスハードウェアを監視および診断することができます。<br><br>このフィールドは、 BMC が含まれないアプライアンスモデルに対しては表示されません。 |
| コンピューティングコントローラのシリアル番号 | コンピューティングコントローラのシリアル番号。 |
| コンピューティングハードウェア | コンピューティングコントローラハードウェアのステータス。 |
| コンピューティングコントローラの CPU 温度 | コンピューティングコントローラの CPU の温度ステータス。 |
| コンピューティングコントローラシャーシの温度 | コンピューティングコントローラの温度ステータス。 |

a. すべてのステータスが「 Nominal 」であることを確認します。

ステータスが「公称」でない場合は、現在のアラートを確認します。

4. 各ネットワークの情報を表示するには、「 * ネットワーク * 」を選択します。

Network Traffic グラフには、ネットワークトラフィック全体のサマリが表示されます。



a. ネットワークインターフェイスセクションを確認します。

**Network Interfaces**

| Name | Hardware Address | Speed | Duplex | Auto Negotiate | Link Status |
|---|---|---|---|---|---|
| adllb | C2:20:17:59:1C:F3 | 10 Gigabit | Full | Off | Up |
| adlli | 42:8F:84:80:00:A9 | 10 Gigabit | Full | Off | Up |
| eth0 | 98:03:9B:98:A2:72 | 400 Gigabit | Full | Off | Up |
| eth1 | B4:A9:FC:08:4E:49 | 10 Gigabit | Full | Off | Up |
| eth2 | 98:03:9B:98:A2:72 | 400 Gigabit | Full | Off | Up |
| hic1 | 98:03:9B:98:A2:72 | 100 Gigabit | Full | On | Up |
| hic2 | 98:03:9B:98:A2:72 | 100 Gigabit | Full | On | Up |
| hic3 | 98:03:9B:98:A2:72 | 100 Gigabit | Full | On | Up |
| hic4 | 98:03:9B:98:A2:72 | 100 Gigabit | Full | On | Up |
| mtc1 | B4:A9:FC:08:4E:49 | Gigabit | Full | On | Up |
| mtc2 | B4:A9:FC:08:4E:49 | Gigabit | Full | On | Up |

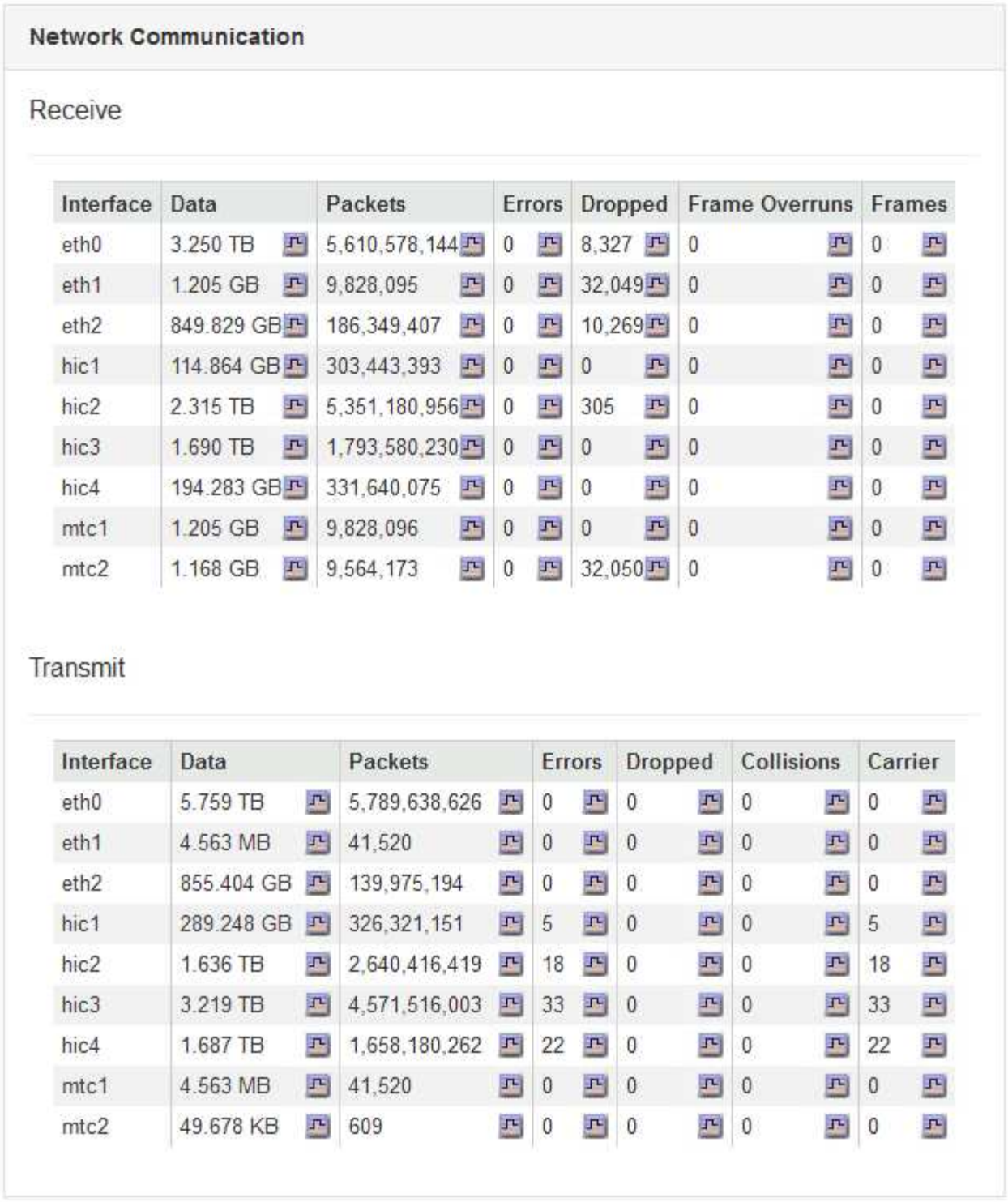
次の表のネットワークインターフェイスの表の「 * Speed * 」列の値を使用して、アプライアンス上の 4 つの 40 / 100GbE ネットワークポートがアクティブ / バックアップモードと LACP モードのどちらを使用するように設定されているかを確認してください。

この表の値は、 4 つのリンクがすべて使用されていることを前提としています。

| リンクモード | ボンディングモード | 個々の **HIC** リンク速度（ **hic1** 、 **hic2** 、 **hic3** 、 **hic4** ） | 想定されるグリッド / クライアントネットワーク速度（ **eth0** 、 **eth2** ） |
|---|---|---|---|
| アグリゲート | LACP | 100 | 400 |
| 固定（ Fixed ） | LACP | 100 | 200 |
| 固定（ Fixed ） | アクティブ / バックアップ | 100 | 100 |
| アグリゲート | LACP | 40 | 160 |
| 固定（ Fixed ） | LACP | 40 | 80 |
| 固定（ Fixed ） | アクティブ / バックアップ | 40 | 40 |

b. 「ネットワーク通信」セクションを確認します。

受信および送信テーブルには、各ネットワークで送受信されたバイト数とパケット数、およびその他の受信および送信メトリックが表示されます。



**Network Communication**

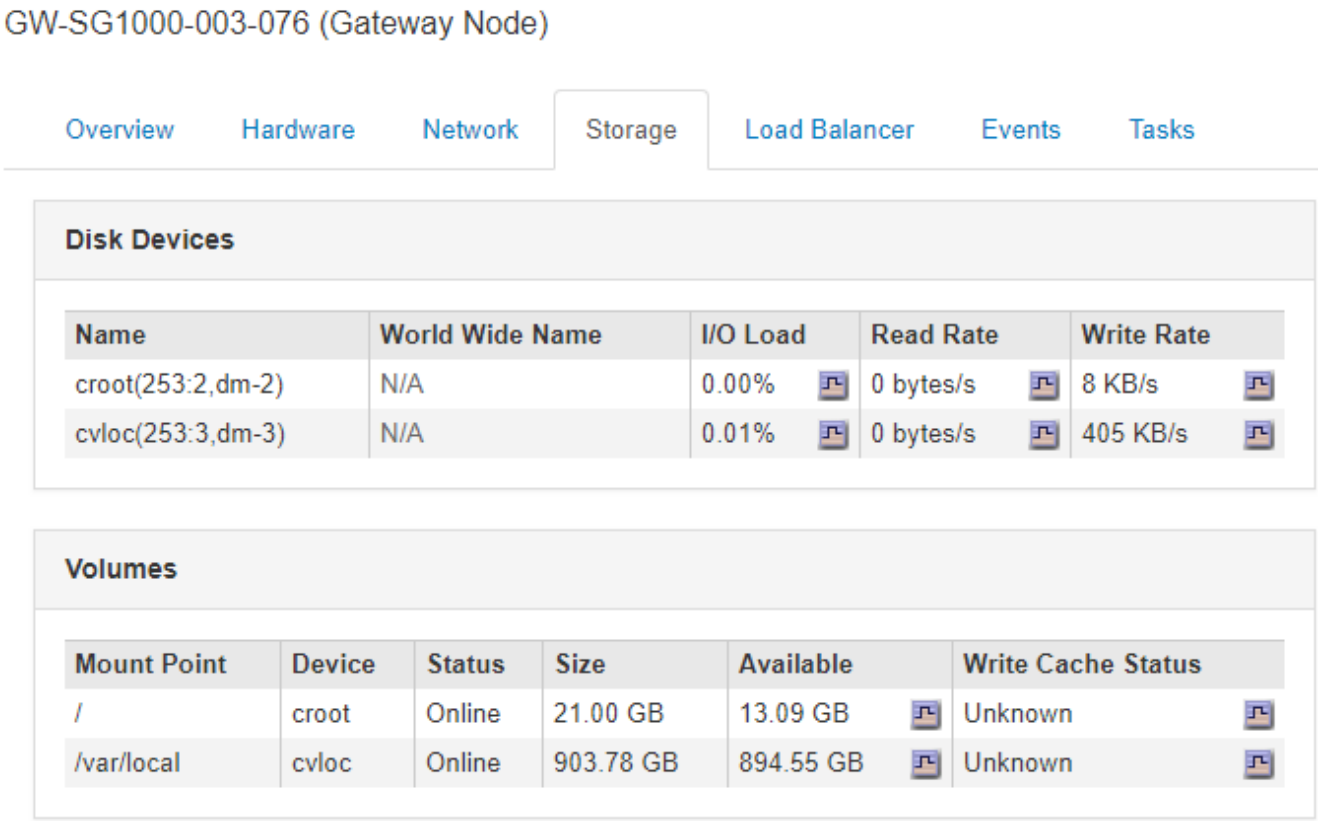
Receive

| Interface | Data | Packets | Errors | Dropped | Frame Overruns | Frames |
|---|---|---|---|---|---|---|
| eth0 | 3.250 TB | 5,610,578,144 | 0 | 8,327 | 0 | 0 |
| eth1 | 1.205 GB | 9,828,095 | 0 | 32,049 | 0 | 0 |
| eth2 | 849.829 GB | 186,349,407 | 0 | 10,269 | 0 | 0 |
| hic1 | 114.864 GB | 303,443,393 | 0 | 0 | 0 | 0 |
| hic2 | 2.315 TB | 5,351,180,956 | 0 | 305 | 0 | 0 |
| hic3 | 1.690 TB | 1,793,580,230 | 0 | 0 | 0 | 0 |
| hic4 | 194.283 GB | 331,640,075 | 0 | 0 | 0 | 0 |
| mtc1 | 1.205 GB | 9,828,096 | 0 | 0 | 0 | 0 |
| mtc2 | 1.168 GB | 9,564,173 | 0 | 32,050 | 0 | 0 |

Transmit

| Interface | Data | Packets | Errors | Dropped | Collisions | Carrier |
|---|---|---|---|---|---|---|
| eth0 | 5.759 TB | 5,789,638,626 | 0 | 0 | 0 | 0 |
| eth1 | 4.563 MB | 41,520 | 0 | 0 | 0 | 0 |
| eth2 | 855.404 GB | 139,975,194 | 0 | 0 | 0 | 0 |
| hic1 | 289.248 GB | 326,321,151 | 5 | 0 | 0 | 5 |
| hic2 | 1.636 TB | 2,640,416,419 | 18 | 0 | 0 | 18 |
| hic3 | 3.219 TB | 4,571,516,003 | 33 | 0 | 0 | 33 |
| hic4 | 1.687 TB | 1,658,180,262 | 22 | 0 | 0 | 22 |
| mtc1 | 4.563 MB | 41,520 | 0 | 0 | 0 | 0 |
| mtc2 | 49.678 KB | 609 | 0 | 0 | 0 | 0 |

5. サービス・アプライアンス上のディスク・デバイスおよびボリュームに関する情報を表示するには、「 * Storage * 」を選択します。




関連情報

"SG100 SG1000サービスアプライアンス"

## 定期的に監視する必要がある情報

StorageGRID は、フォールトトレラントな分散ストレージシステムで、エラーが発生した場合やノードやサイトを使用できない場合でも、継続して動作するように設計されています。システムの健全性、ワークロード、および使用状況の統計をプロアクティブに監視して、潜在的な問題にグリッドの効率性または可用性に影響が及ぶ前に対処できるようにする必要があります。

ビジーシステムでは大量の情報が生成されます。このセクションでは、継続的に監視する必要がある最も重要な情報についてガイダンスを提供します。ここでは、次のサブセクションについて説明します。

- "システムヘルスを監視しています"
- "ストレージ容量を監視しています"
- "情報ライフサイクル管理の監視"
- "パフォーマンス、ネットワーク、およびシステムリソースの監視"
- "テナントアクティビティの監視"
- "アーカイブ容量を監視しています"
- "ロードバランシング処理の監視"
- "必要に応じてホットフィックスの適用またはソフトウェアのアップグレードを行います"

| 監視対象 | 頻度 |
| --- | --- |
| Grid Managerのダッシュボードに表示されるシステム健全性データ。前日から変更があった場合はメモします。 | 毎日 |
| ストレージノードのオブジェクトとメタデータの容量が消費されている速度です | 毎週 |
| 情報ライフサイクル管理のオペレーション | 毎週 |
| パフォーマンス、ネットワーク、システムリソース：<br>• クエリのレイテンシ<br>• 接続とネットワーク<br>• ノードレベルのリソース | 毎週 |
| テナントのアクティビティ | 毎週 |
| 外部アーカイブストレージシステムの容量 | 毎週 |
| ロードバランシング操作 | 初期設定後と設定の変更後 |
| ソフトウェアのホットフィックスおよびソフトウェアのアップグレードの可用性 | 毎月 |

システムヘルスを監視しています

## StorageGRID システムの全体的なヘルスは日単位で監視する必要があります。

StorageGRID システムはフォールトトレラントであり、グリッドの一部が使用できない場合でも動作を継続できます。StorageGRID システムに搭載されている可能性がある問題 の最初の署名は、アラートまたはアラーム（従来のシステム）である可能性があり、問題 にシステム処理が含まれているとは限りません。システムヘルスに注意することで、運用やグリッドの効率に影響が及ぶ前に小さな問題を検出できます。

Grid Manager のダッシュボードの健全性パネルには、システムに影響している可能性がある問題の概要が表示されます。ダッシュボードに表示された問題を調査する必要があります。

アラートがトリガーされたときにすぐに通知されるようにするには、アラートの E メール通知を設定するか、 SNMP トラップを設定します。

1. Grid Manager にサインインしてダッシュボードを表示します。
2. 正常性パネルの情報を確認します。

問題が発生している場合は、詳細を確認できるリンクが表示されます。

| リンク | を示します |
| --- | --- |
| グリッドの詳細 | 切断されているノード（接続状態が「 Unknown 」または「 Administratively Down 」）がある場合に表示されます。リンクをクリックするか、青またはグレーのアイコンをクリックして、影響を受けるノードを特定します。 |
| 現在のアラート | 現在アクティブなアラートがある場合に表示されます。リンクをクリックするか、クリティカル、メジャー、または*マイナー*をクリックして、アラート>*現在の*ページの詳細を表示します。 |
| 最近解決したアラート | 過去 1 週間にトリガーされたアラートが解決された場合に表示されます。リンクをクリックすると、[* Alerts > Resolved （*アラート>*解決済み*）]ページに詳細が表示されます。 |
| 従来のアラームです | 現在アクティブなアラーム（レガシーシステム）がある場合に表示されます。リンクをクリックすると、* Support > Alarms（レガシー）> Current Alarms *ページで詳細が表示されます。<br><br>*注：*従来のアラームシステムは引き続きサポートされていますが、アラートシステムには大きな利点があり、使いやすくなっています。 |
| 使用許諾 | この StorageGRID システムのソフトウェアライセンスを含む問題 がある場合に表示されます。リンクをクリックして、[* Maintenance （メンテナンス）]>[ System （*システム）]>[* License （ライセンス）]ページで詳細を確認します。 |

関連情報

"StorageGRID の管理"

"アラート用のEメール通知の設定"

"SNMPによる監視を使用する"

ノードの接続状態を監視しています

# 1 つ以上のノードがグリッドから切断されると、重要な StorageGRID 処理に影響する可能性があります。ノードの接続状態を監視し、速やかに問題に対処する必要があります。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

このタスクについて

ノードには、次の 3 つのいずれかの接続状態があります。

- * 接続されていません - 不明 * ：不明な理由でノードがグリッドに接続されていません。たとえば、ノード間のネットワーク接続が失われた、電源が切れたなどの原因が考えられます。* Unable to communicate with node * アラートがトリガーされる場合もあります。他のアラートもアクティブになる可能性があります。この状況にはすぐに対処する必要があります。

  管理されたシャットダウン処理の実行中に、ノードが Unknown と表示されることがありますこのような場合、 Unknown 状態は無視してかまいません。

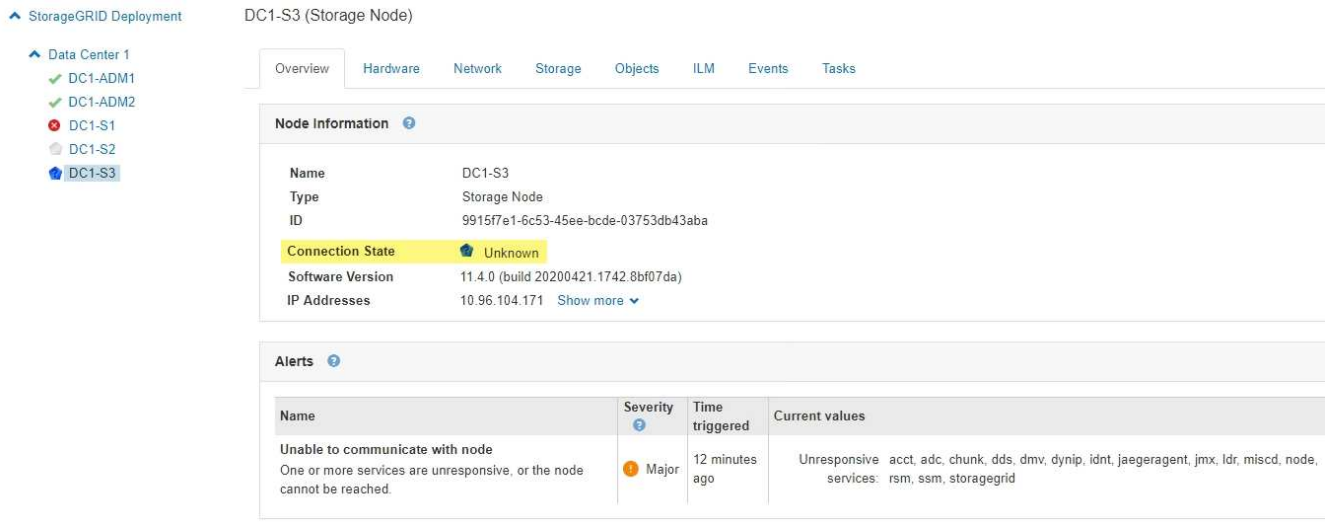
- * 接続されていません - 管理上の理由により停止して ：ノードが想定される理由でグリッドに接続されていません。たとえば、ノードまたはノード上のサービスが正常にシャットダウンされた、ノードがリブート中である、ソフトウェアのアップグレード中であるなどの原因が考えられます。1 つ以上のアラートがアクティブになっている可能性もあります。
- * 接続済み * ：ノードがグリッドに接続されています。

手順

1. ダッシュボードのヘルスパネルに青またはグレーのアイコンが表示されている場合は、そのアイコンをクリックするか、 * グリッドの詳細 * をクリックします。（青またはグレーのアイコンと * グリッドの詳細 * リンクは、少なくとも 1 つのノードがグリッドから切断されている場合にのみ表示されます）。

   ノードツリーの最初の青いノードの [ 概要（ Overview ） ] ページが表示されます。青色のノードがない場合は、ツリーの最初のグレーのノードの [ 概要（ Overview ） ] ページが表示されます。

   この例では、 DC1-S3 という名前のストレージノードに青いアイコンが表示されています。ノード情報パネルの * 接続状態 * が * 不明 * で、 * ノードと通信できません * アラートがアクティブです。アラートには、 1 つ以上のサービスが応答していないか、ノードに到達できないことが示されます。




2. ノードのアイコンが青色の場合は、次の手順を実行します。
   a. 表で各アラートを選択し、推奨される対処方法に従います。

      たとえば、ノードのホストを停止または再起動したサービスの再起動が必要になることがあります。

   b. ノードをオンラインに戻すことができない場合は、テクニカルサポートにお問い合わせください。
3. ノードのグレーのアイコンが表示されている場合は、次の手順を実行します。

   グレーのノードはメンテナンス時の手順で、 1 つ以上のアラートに関連付けられることがあります。基盤となる問題 に基づいて ' これらのノードは頻繁に管理上のダウン状態になり ' 介入なしでオンラインに戻ります

   a. アラートセクションを確認して、このノードに影響しているアラートがないかどうかを確認します。
   b. 1 つ以上のアラートがアクティブな場合は、表内の各アラートを選択し、推奨される対処方法に従います。
   c. ノードをオンラインに戻すことができない場合は、テクニカルサポートにお問い合わせください。

関連情報

"アラート一覧"

""

現在のアラートの表示

アラートがトリガーされると、ダッシュボードにアラートアイコンが表示されます。ノードに関するアラートアイコンは、ノードページにも表示されます。アラートをサイレント化しないかぎり、 E メール通知も送信される場合があります。

必要なもの

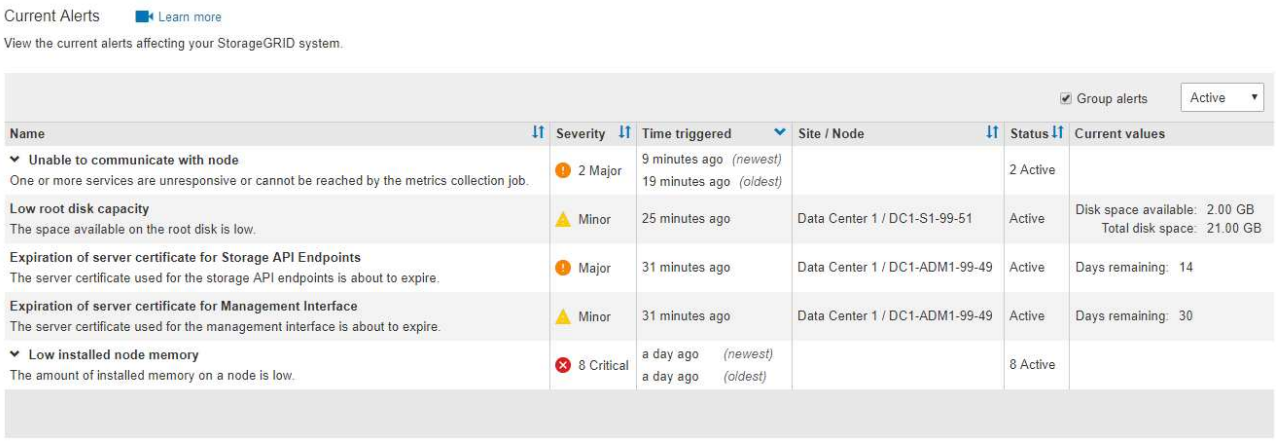
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

手順

1. アクティブなアラートが 1 つ以上ある場合は、次のいずれかを実行します。

- ダッシュボードのヘルスパネルで、アラートアイコンをクリックするか、 * 現在のアラート * をクリックします。（警告アイコンと * 現在のアラート * リンクは、少なくとも 1 つのアラートが現在アクティブである場合にのみ表示されます）。
- [* Alerts*>*current*]を選択します。

  [Current Alerts] ページが表示されます。StorageGRID システムに現在影響しているすべてのアラートが表示されます。




  デフォルトでは、アラートは次のように表示されます。

  - 最後にトリガーされたアラートが最初に表示されます。
  - 同じタイプの複数のアラートが 1 つのグループとして表示されます。
  - サイレント化されているアラートは表示されません。
  - 特定のノードの特定のアラートが複数の重大度のしきい値に達した場合は、最も重大度の高いアラートのみが表示されます。つまり、アラートが Minor 、 Major 、 Critical の各重大度のしきい値に達した場合は、 Critical アラートのみが表示されます。

    現在のアラートページは 2 分ごとに更新されます。

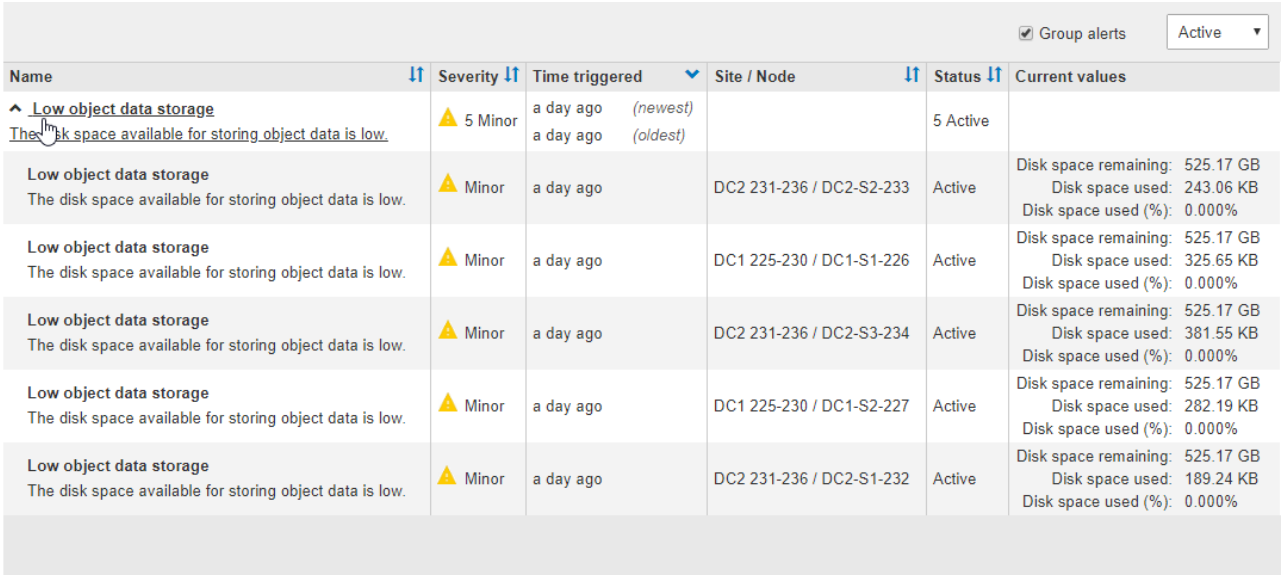
2. 表内の情報を確認します。

| 列ヘッダー | 説明 |
| --- | --- |
| 名前 | アラートの名前と概要 。 |

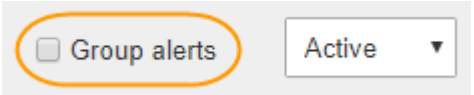
| 列ヘッダー | 説明 |
| --- | --- |
| 重大度 | アラートの重大度。複数のアラートがグループ化されている場合は、各重大度で発生しているアラートのインスタンスの数がタイトル行に表示されます。<br><br>• * 重要 * ：異常な状態で、 StorageGRID のノードやサービスの通常の動作が停止しています。基盤となる問題 にすぐに対処する必要があります。問題 が解決されないと、サービスの停止やデータの損失を招くおそれがあります。<br>• * メジャー * ：異常な状態で、現在の処理に影響しているか、重大アラートのしきい値に近づいています。Major アラートを調査し、根本的な問題に対処して、異常な状態が発生した場合に StorageGRID のノードやサービスが正常に動作しなくなる事態を防ぐ必要があります。<br>• * マイナー * ：システムは正常に動作していますが、継続するとシステムの動作に影響する可能性がある異常な状態が発生しています。自動的にクリアされない Minor アラートを監視し、解決して、深刻な問題が生じないようにする必要があります。 |
| トリガーされた時刻 | アラートがトリガーされてからの時間。複数のアラートがグループ化されている場合は、タイトル行にアラートの最新のインスタンス（ _newnewest _ ）と最も古いインスタンス（ _oldest _ ）の時間が表示されます。 |
| サイト / ノード | アラートが発生しているサイトとノードの名前。複数のアラートがグループ化されている場合、サイト名とノード名はタイトル行に表示されません。 |
| ステータス | アラートがアクティブであるか、またはサイレント化されているか。複数のアラートがグループ化され、ドロップダウンですべてのアラート * が選択されている場合、タイトル行には、そのアラートのアクティブなインスタンスの数と、サイレント化されたインスタンスの数が表示されます。 |

| 列ヘッダー | 説明 |
| --- | --- |
| 現在の値 | アラートをトリガーした指標の現在の値。一部のアラートでは、アラートの理解と調査に役立つ値が追加で表示されます。たとえば、 Low object data storage * アラートには、使用されているディスクスペースの割合、ディスクスペースの総容量、使用されているディスクスペースの容量の値が表示されます。<br>• 注：複数のアラートがグループ化されている場合、現在の値はタイトル行に表示されません。 |

3. アラートのグループを展開または折りたたむには、次の手順を実行します
   - グループ内の個々のアラートを表示するには、見出しの下キャレットをクリックします をクリックするか、グループの名前をクリックします。
   - グループ内の個々のアラートを非表示にするには、見出しの上キャレットをクリックします をクリックするか、グループの名前をクリックします。




4. アラートのグループではなく個々のアラートを表示するには、テーブルの上部にある ［ * グループアラート * ］ チェックボックスの選択を解除します。




5. アラートまたはアラートグループをソートするには、上下の矢印をクリックします をクリックします。
   - グループアラート * を選択すると、アラートグループと各グループ内の個々のアラートの両方がソートされます。たとえば、グループ内のアラートを「時間トリガー」でソートして、特定のアラートの最新のインスタンスを確認できます。
   - グループアラート * が選択されていない場合は、アラートのリスト全体がソートされます。たとえば、すべてのアラートを * Node/Site * でソートして、特定のノードに影響しているすべてのアラートを表示できます。

6. アラートをステータスでフィルタリングするには、テーブルの上部にあるドロップダウンメニューを使用します。

   - 現在のすべてのアラート（アクティブなアラートとサイレント化されたアラートの両方）を表示するには、 * All alerts * を選択します。
   - アクティブな現在のアラートだけを表示するには、「 * アクティブ * 」を選択します。
   - サイレント化されている現在のアラートだけを表示するには、「 * Silented * 」を選択します。

7. 特定のアラートの詳細を表示するには、テーブルでアラートを選択します。

   アラートのダイアログボックスが表示されます。特定のアラートを表示する手順を参照してください。

関連情報

"特定のアラートの表示"

"アラート通知のサイレント化"

解決済みのアラートの表示

# 解決済みのアラートの履歴を検索して確認できます。

必要なもの

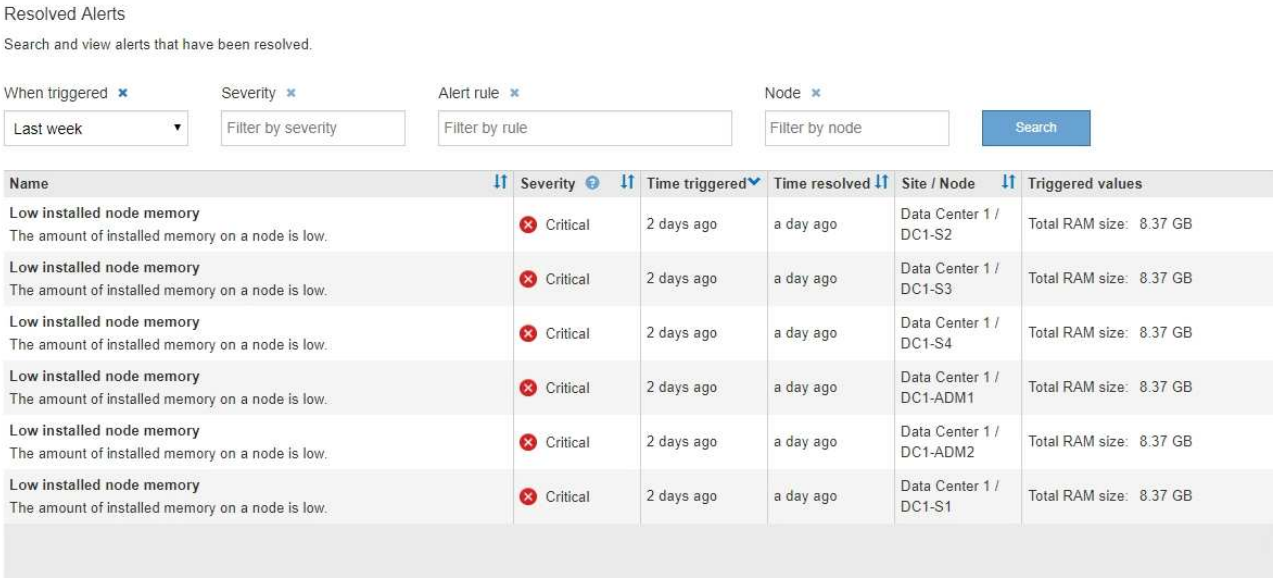
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

手順

1. 解決済みのアラートを表示するには、次のいずれかを実行します。
   - ダッシュボードのヘルスパネルで、 * 最近解決したアラート * をクリックします。

     Recently Resolved alerts * リンクは、 1 つ以上のアラートが過去 1 週間にトリガーされ、現在解決された場合にのみ表示されます。

   - [* Alerts*>]>[* Resolved *]を選択します。[Resolved Alerts] ページが表示されます。デフォルトでは、過去 1 週間にトリガーされた解決済みのアラートが表示され、最後にトリガーされたアラートが最初に表示されます。このページのアラートは、以前は現在のアラートページまたは E メール通知に表示されていました。




2. 表内の情報を確認します。

| 列ヘッダー | 説明 |
| --- | --- |
| 名前 | アラートの名前と概要 。 |
| 重大度 | アラートの重大度。<br>• * 重要 * ：異常な状態で、 StorageGRID のノードやサービスの通常の動作が停止しています。基盤となる問題 にすぐに対処する必要があります。問題 が解決されないと、サービスの停止やデータの損失を招くおそれがあります。<br>• * メジャー * ：異常な状態で、現在の処理に影響しているか、重大アラートのしきい値に近づいています。Major アラートを調査し、根本的な問題に対処して、異常な状態が発生した場合に StorageGRID のノードやサービスが正常に動作しなくなる事態を防ぐ必要があります。<br>• * マイナー * ：システムは正常に動作していますが、継続するとシステムの動作に影響する可能性がある異常な状態が発生しています。自動的にクリアされない Minor アラートを監視し、解決して、深刻な問題が生じないようにする必要があります。 |
| トリガーされた時刻 | アラートがトリガーされてからの時間。 |
| 解決時刻 | アラートが解決されてからの時間。 |
| サイト / ノード | アラートが発生したサイトとノードの名前。 |

| 列ヘッダー | 説明 |
| --- | --- |
| トリガーされた値 | アラートをトリガーした指標の値。一部のアラートでは、アラートの理解と調査に役立つ値が追加で表示されます。たとえば、 Low object data storage * アラートには、使用されているディスクスペースの割合、ディスクスペースの総容量、使用されているディスクスペースの容量の値が表示されます。 |

3. 解決済みアラートのリスト全体をソートするには、上 / 下矢印をクリックします をクリックします。

   たとえば、解決済みのアラートを * Site/Node * でソートして、特定のノードに影響するアラートを確認できます。

4. 必要に応じて、テーブルの上部にあるドロップダウンメニューを使用して、解決済みのアラートのリストをフィルタリングします。

   a. [*When Triggered *] ドロップダウンメニューから期間を選択し、トリガーされた時間に基づいて解決済みのアラートを表示します。

      次の期間内にトリガーされたアラートを検索することができます。

      - 過去 1 時間
      - 最終日
      - 先週（デフォルトビュー）
      - 先月
      - 任意の期間
      - Custom （期間の開始日と終了日を指定できます）

   b. 特定の重大度の解決済みアラートをフィルタリングするには、 **Severity** ドロップダウンメニューから 1 つ以上の重大度を選択します。

   c. [* アラートルール * （ * Alert rule * ） ] ドロップダウンメニューから 1 つ以上のデフォルトまたはカスタムのアラートルールを選択して、特定のアラートルールに関連する解決済みのアラートをフィルタリングします。

   d. ノード * ドロップダウンメニューから 1 つ以上のノードを選択して、特定のノードに関連する解決済みアラートをフィルタします。

   e. [* 検索（ Search ） ] をクリックする。

5. 特定の解決済みアラートの詳細を表示するには、テーブルでアラートを選択します。

   アラートのダイアログボックスが表示されます。特定のアラートを表示する手順を参照してください。

関連情報

"特定のアラートの表示"

特定のアラートの表示

## StorageGRID システムに現在影響しているアラートや解決されたアラートに関する詳細

情報を表示できます。これには、推奨される対処方法、アラートがトリガーされた時間、アラートに関連する指標の現在の値などの情報が含まれます。必要に応じて、現在のアラートをサイレント化したり、アラートルールを更新したりできます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

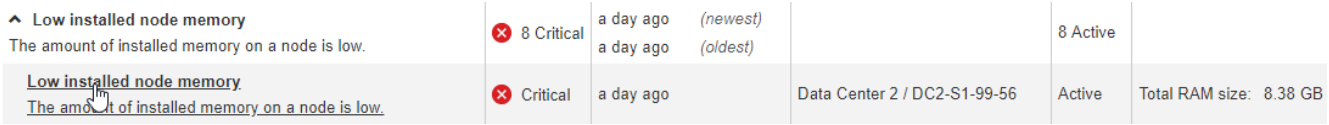
手順

1. 現在のアラートと解決済みのアラートのどちらを表示するかに基づいて、次のいずれかを実行します。

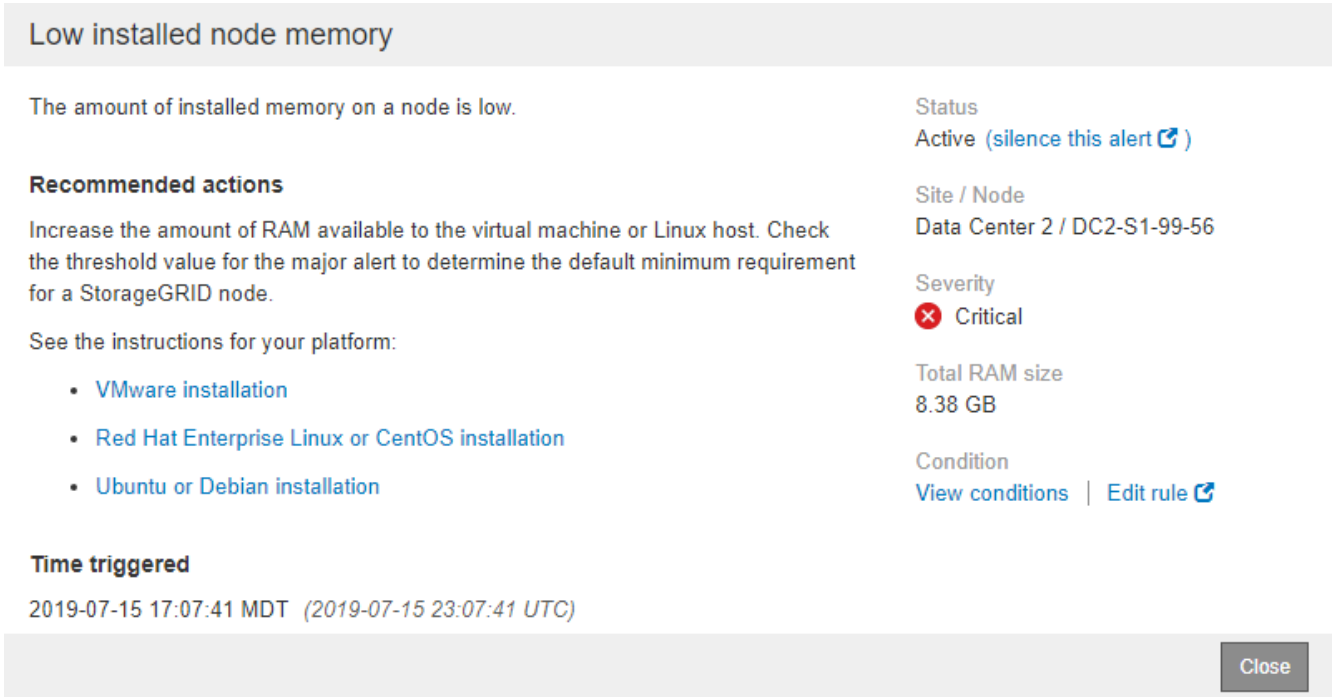
| 列ヘッダー | 説明 |
| --- | --- |
| 現在の警告 | • ダッシュボードのヘルスパネルで、 * 現在のアラート * リンクをクリックします。このリンクは、少なくとも 1 つのアラートが現在アクティブである場合にのみ表示されます。このリンクは、現在のアラートがない場合、または現在のすべてのアラートがサイレント化されている場合は表示されません。<br>• [* Alerts*>*current*]を選択します。<br>• [ノード（* Nodes ）]ページで、警告アイコンが表示されているノードの**[***概要（* Overview * ）]タブを選択します。次に、 [Alerts] セクションでアラート名をクリックします。 |
| 解決済みアラート | • ダッシュボードのヘルスパネルで、最近解決したアラート * リンクをクリックします。（このリンクは、過去 1 週間に 1 つ以上のアラートがトリガーされ、解決された場合にのみ表示されます。過去 1 週間にトリガーされて解決されたアラートがない場合は、このリンクが非表示になります）。<br>• [* Alerts*>]>[* Resolved *]を選択します。 |

2. 必要に応じて、アラートのグループを展開し、表示するアラートを選択します。

アラートグループの見出しではなく、アラートを選択します。




ダイアログボックスが表示され、選択したアラートの詳細が表示されます。




3. アラートの詳細を確認します。

| 情報 | 説明 |
| --- | --- |
| *TITLE* | アラートの名前。 |
| _ 最初の段落 _ | アラートの概要 。 |
| 推奨される対処方法 | このアラートの推奨される対処方法。 |
| トリガーされた時刻 | アラートがローカルの時刻と UTC でトリガーされた日時。 |
| 解決時刻 | 解決済みのアラートの場合のみ、アラートがローカルの時刻と UTC で解決された日時。 |
| ステータス | アラートのステータス。 Active 、 Silved 、または Resolved です。 |
| サイト / ノード | アラートの影響を受けるサイトとノードの名前。 |

| 情報 | 説明 |
| --- | --- |
| 重大度 | アラートの重大度。<br>• * 重要 * ：異常な状態で、 StorageGRID のノードやサービスの通常の動作が停止しています。基盤となる問題 にすぐに対処する必要があります。問題 が解決されないと、サービスの停止やデータの損失を招くおそれがあります。<br>• * メジャー * ：異常な状態で、現在の処理に影響しているか、重大アラートのしきい値に近づいています。Major アラートを調査し、根本的な問題に対処して、異常な状態が発生した場合に StorageGRID のノードやサービスが正常に動作しなくなる事態を防ぐ必要があります。<br>• * マイナー * ：システムは正常に動作していますが、継続するとシステムの動作に影響する可能性がある異常な状態が発生しています。自動的にクリアされない Minor アラートを監視し、解決して、深刻な問題が生じないようにする必要があります。 |
| データ値 _ | このアラートに関する指標の現在の値。一部のアラートでは、アラートの理解と調査に役立つ値が追加で表示されます。たとえば、「 Low metadata storage * 」アラートには、使用されているディスクスペースの割合、ディスクスペースの総容量、使用されているディスクスペースの容量の値が表示されます。 |

4. 必要に応じて、 * silence this alert * をクリックして、このアラートをトリガーしたアラートルールをサイレント化します。

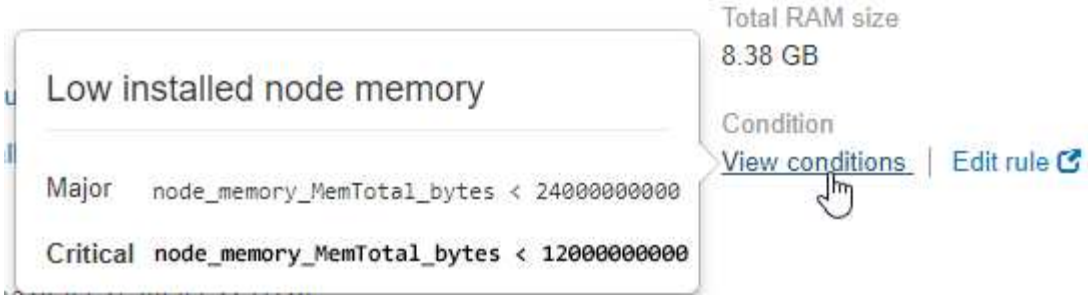
   アラートルールをサイレント化するには、 Manage Alerts または Root アクセス権限が必要です。

   > アラートルールをサイレント化する場合は注意が必要です。アラートルールがサイレント化されている場合、重大な処理が完了しないかぎり、根本的な問題が検出されないことがあります。

5. アラートルールの現在の条件を表示するには、次の手順を実行します。

   a. アラートの詳細から、 * 状態の表示 * をクリックします。

      定義されている各重大度の Prometheus 式がポップアップに表示されます。




a. ポップアップを閉じるには、ポップアップの外側をクリックします。

6. 必要に応じて、 * Edit rule * をクリックして、このアラートをトリガーしたアラートルールを編集します。

   アラートルールを編集するには、 Manage Alerts または Root アクセス権限が必要です。

   アラートルールを編集する場合は注意が必要です。トリガー値を変更した場合、重大な処理を完了できなくなるまで、根本的な問題が検出されないことがあります。

7. 警告の詳細を閉じるには、 * 閉じる * をクリックします。

関連情報

"アラート通知のサイレント化"

"アラートルールを編集する"

古いアラームの表示

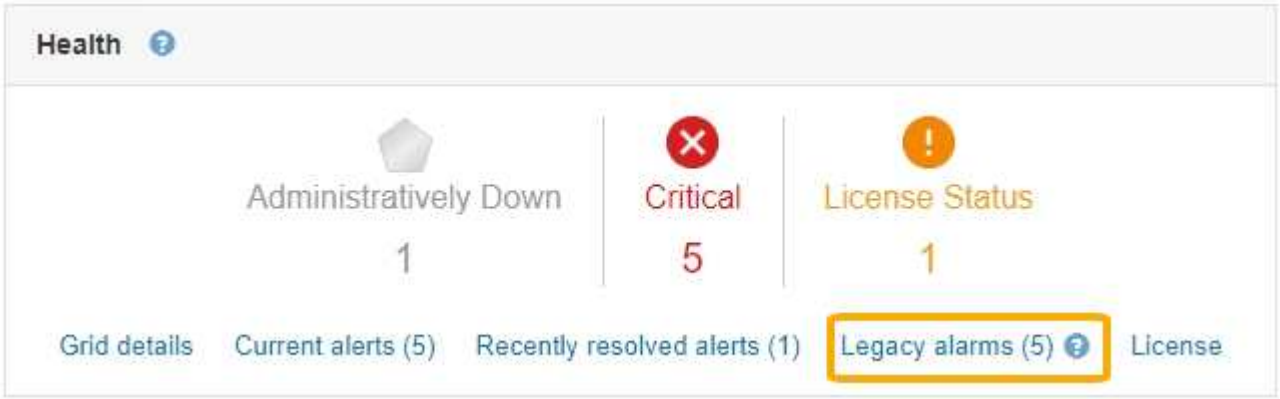
## システム属性がアラームのしきい値に達すると、アラーム（従来のシステム）がトリガーされます。現在アクティブなアラームは、DashboardまたはCurrent Alarmsページで表示できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

このタスクについて

1つまたは複数のレガシーアラームが現在アクティブな場合、ダッシュボードのヘルスパネルには*レガシーアラーム*リンクが含まれます。かっこ内の数字は、現在アクティブなアラームの数を示します。



Dashboardの* Legacy alarms *カウントは、レガシーアラームがトリガーされるたびに増分されます。アラームのEメール通知を無効にしていても、この数が増分します。通常はこの数値を無視するか（アラートによってシステムがより正確に把握されるため）、現在アクティブなアラームを表示することができます。

従来のアラームシステムは引き続きサポートされますが、アラートシステムには大きなメリットがあり、使いやすくなっています。

手順

1. 現在アクティブなレガシーアラームを表示するには、次のいずれかを実行します。
   - ダッシュボードの正常性パネルで、*レガシーアラーム*をクリックします。このリンクは、少なくとも1つのアラームが現在アクティブである場合にのみ表示されます。
   - [**Support**>]>[* Alarms (legac)**>]>[** Current Alarms]を選択します。[Current Alarms]ページが表示されます。

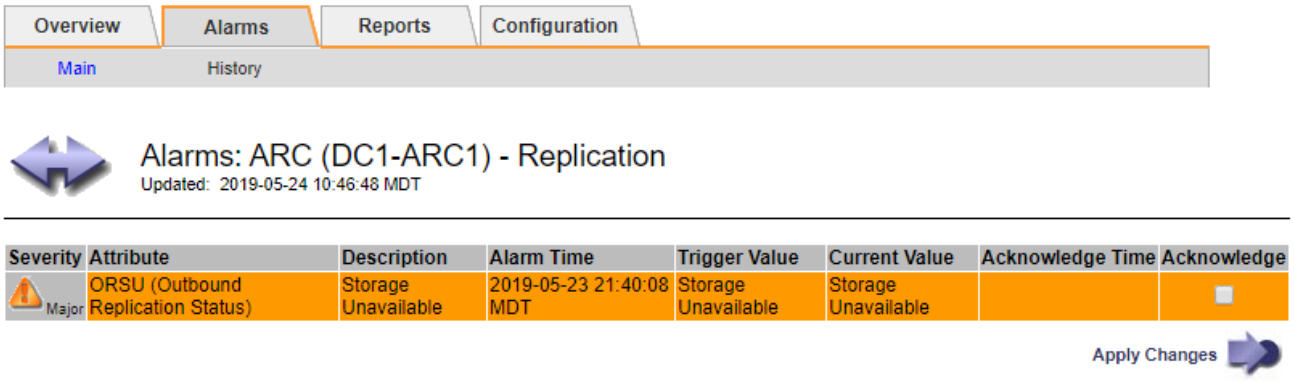
アラームアイコンは、各アラームの重大度を次のように示します。

| をクリックします。 | 色（ **Color** ） | アラームの重大度 | 意味 |
|---|---|---|---|
| | 黄色 | 注意 | ノードはグリッドに接続されていますが、正常な状態ではありません。通常の動作に影響はありません。 |
| | 薄いオレンジ | マイナー | ノードはグリッドに接続されていますが、正常な状態ではありません。将来的に動作に影響する可能性があります。さらに重大な問題にならないように調査が必要です。 |

| をクリックします。 | 色（ **Color** ） | アラームの重大度 | 意味 |
| --- | --- | --- | --- |
| | 濃いオレンジ | メジャー（ Major ） | ノードはグリッドに接続されていますが、正常な状態ではありません。すでに動作に影響が及んでいます。エスカレーションを防ぐために早急な対応が必要です。 |
| | 赤 | 重要 | ノードはグリッドに接続されていますが、正常な状態ではありません。正常に動作しなくなっています。問題 にはすぐに対処する必要があります。 |

1. アラームをトリガーした原因となった属性を確認するには、テーブルで属性名を右クリックします。
2. アラームのその他の詳細情報を表示するには、テーブルでサービス名をクリックします。

   選択したサービスのAlarmsタブが表示されます（* Support **>** Tools **>** Grid Topology ***>*Grid Node*** >**Service*>* Alarms *）。




3. 現在のアラームの数を消去するには、必要に応じて次の操作を行います。
   - アラームを確認します。確認済みのアラームは、重大度レベルが次のレベルでトリガーされるか、解決されてから再度発生するまで、レガシーアラームの数に含まれなくなります。
   - システム全体で特定のデフォルトアラームまたはグローバルカスタムアラームを無効にして、再度トリガーされないようにします。

関連情報

"アラーム一覧（従来のシステム）"

"現在のアラームの確認応答（従来のシステム）"

"アラームの無効化（従来のシステム）"

# StorageGRID システムでオブジェクトまたはオブジェクトメタデータのストレージスペースが不足しないように、ストレージノードの使用可能な合計スペースを監視する必要があります。

StorageGRID は、オブジェクトデータとオブジェクトメタデータを別々に格納し、オブジェクトメタデータを含む分散 Cassandra データベース用に一定量のスペースをリザーブします。オブジェクトとオブジェクトメタデータ用に消費されるスペースの合計量のほか、それぞれので消費されるスペースの傾向を監視します。これにより、ノードの追加を事前に計画し、サービスの停止を回避できます。

StorageGRID システムのグリッド全体、サイト、およびストレージノードごとに、ストレージ容量の情報を表示できます。

関連情報

"Storage（ストレージ）タブを表示します"

## グリッド全体のストレージ容量を監視する

# グリッドの全体的なストレージ容量を監視して、オブジェクトデータおよびオブジェクトメタデータ用に十分な空きスペースが残っていることを確認する必要があります。時間の経過に伴うストレージ容量の変化を理解しておくと、グリッドの使用可能なストレージ容量が消費される前にストレージノードまたはストレージボリュームを追加する際に役立ちます。

必要なもの

Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

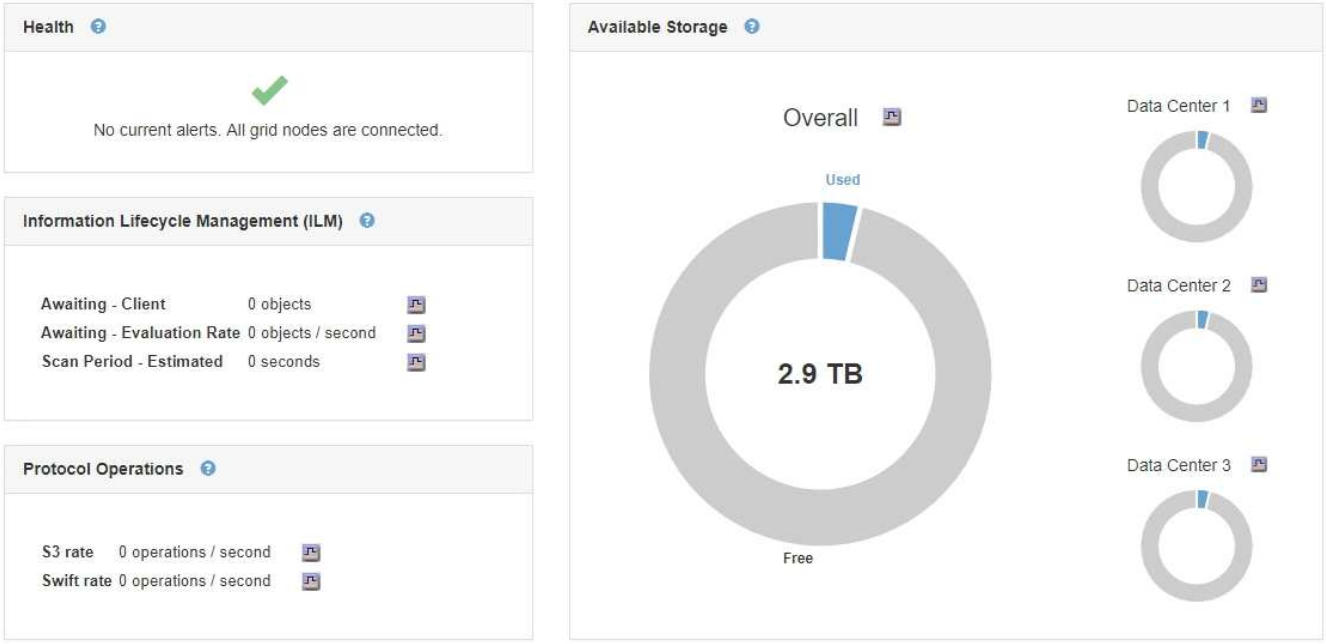
このタスクについて

Grid Manager のダッシュボードを使用して、グリッド全体および各データセンターで使用可能なストレージの量を簡単に評価できます。ノードページには、オブジェクトデータとオブジェクトメタデータの詳細な値が表示されます。

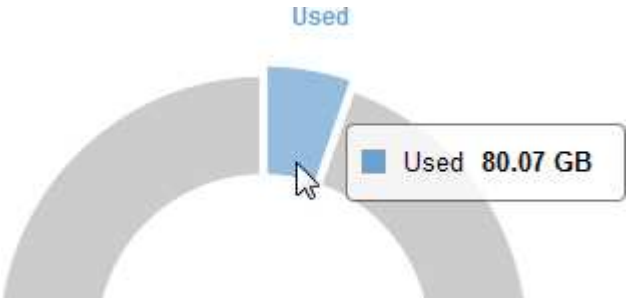
手順

1. グリッド全体および各データセンターで使用可能なストレージ容量を評価します。
   a. 「 * ダッシュボード * 」を選択します。
   b. Available Storage （使用可能なストレージ）パネルで、空きストレージ容量と使用済みストレージ容量の概要を確認します。

      アーカイブメディアはこの概要に含まれません。




a. グラフの「 Free 」または「 Used 」セクションにカーソルを合わせて、正確な空きスペース量または使用済みスペース量を確認します。




b. マルチサイトグリッドの場合は、各データセンターのグラフを確認します。

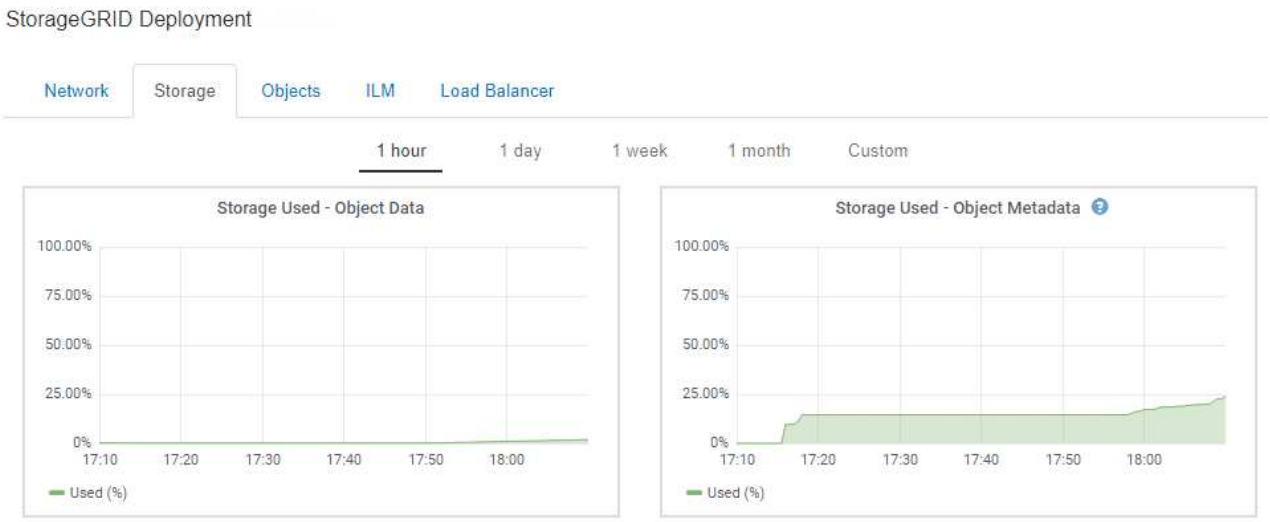
c. グラフアイコンをクリックします をクリックして、使用容量の推移を示すグラフを表示します。

使用済みストレージ容量の割合（ % ）と時刻が表示されます。

2. ストレージの使用済み容量と、オブジェクトデータおよびオブジェクトメタデータに使用可能な残りのストレージ容量を確認します。

a. [ノード（ Nodes）]を選択し

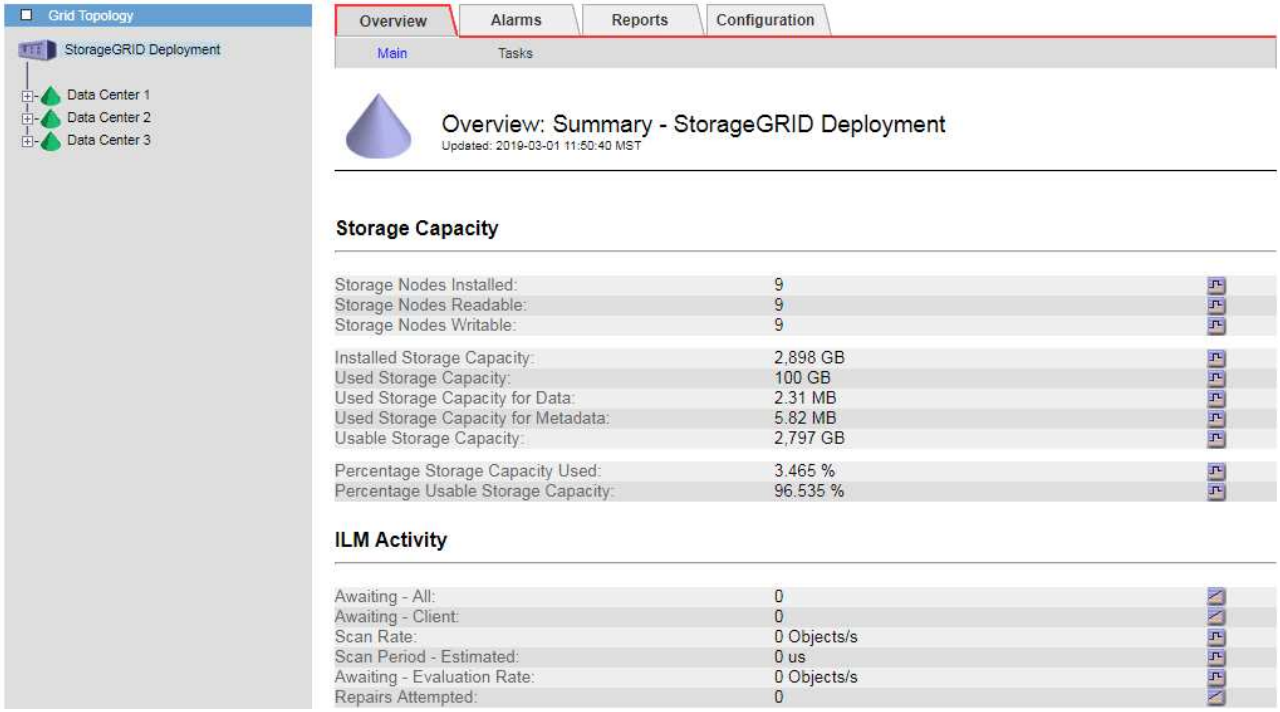
b. [***grid***>*Storage*] を選択します。




c. Storage Used - Object DataチャートとStorage Used - Object Metadataチャートにカーソルを合わせ、グリッド全体で使用可能なオブジェクトストレージとオブジェクトメタデータストレージの量、および一定の期間にわたって使用済みの容量を確認します。

> ⓘ サイトまたはグリッドの合計値には、オフラインノードなど、指標が報告されていないノードは 5 分以上含まれません。

3. テクニカルサポートからの指示に従って、グリッドのストレージ容量に関する追加の詳細を表示します。
   a. Support **>** Tools **>** Grid Topology *を選択します。
   b. ***grid***>* Overview **>** Main *を選択します。




4. グリッドの使用可能なストレージ容量がすべて使用される前に、ストレージノードまたはストレージボリュームを追加する拡張を実行します。

拡張のタイミングを計画する際には、追加のストレージを調達して設置するのにどれくらいの時間がかかるかを検討します。

> ILM ポリシーでイレイジャーコーディングを使用している場合は、既存のストレージノードの使用率が約 70% のときに拡張して、追加する必要のあるノードの数を減らすことができます。

ストレージの拡張計画の詳細については、 StorageGRID の拡張手順を参照してください。

関連情報

"グリッドを展開します"

各ストレージノードのストレージ容量を監視しています

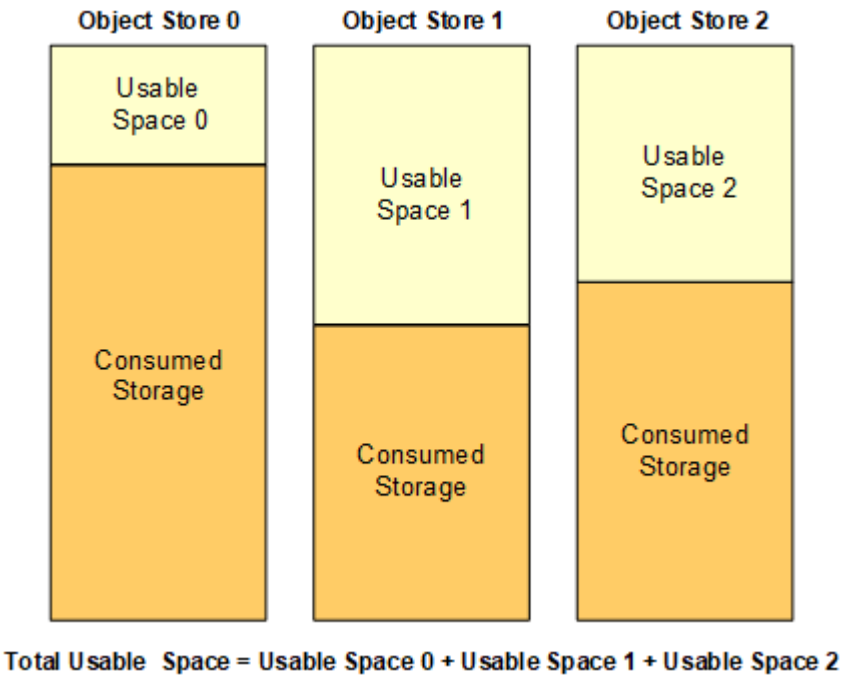
# 各ストレージノードの使用可能な合計スペースを監視して、ノードに新しいオブジェクトデータ用の十分なスペースがあることを確認する必要があります。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

このタスクについて

使用可能なスペースは、オブジェクトの格納に使用できるストレージスペースの量です。ストレージノードの使用可能な合計スペースは、ノード内のすべてのオブジェクトストアの使用可能なスペースの合計です。




手順

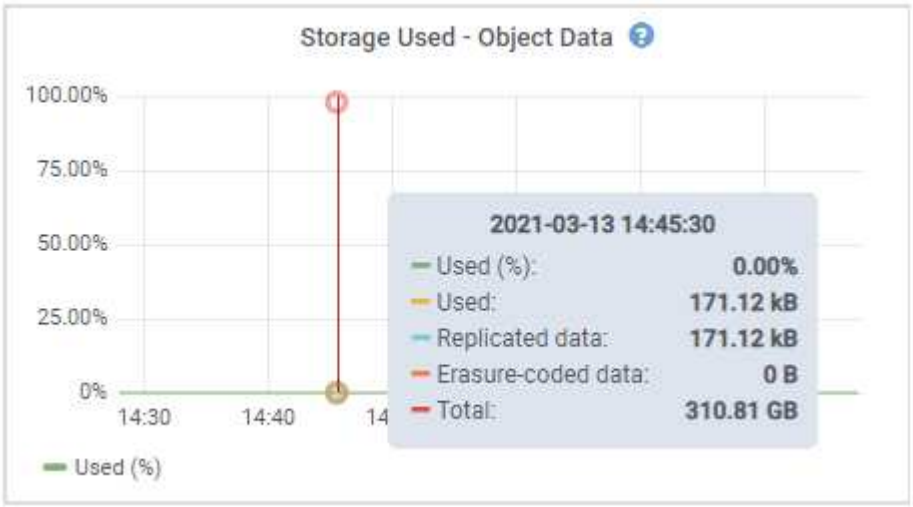
1. ノード*>*ストレージノード*>*ストレージ*を選択します。

   ノードのグラフと表が表示されます。

2. Storage Used - Object Data グラフにカーソルを合わせます。

次の値が表示されます。

- * Used （ % ） * ：オブジェクトデータに使用されている合計使用可能スペースの割合。
- * Used * ：オブジェクトデータに使用されている合計使用可能スペースの量。
- * Replicated data * ：このノード、サイト、またはグリッド上のレプリケートオブジェクトデータの推定量。
- * イレイジャーコーディングデータ * ：このノード、サイト、またはグリッドにあるイレイジャーコーディングオブジェクトデータの推定量。
- * Total * ：このノード、サイト、またはグリッドで使用可能なスペースの総容量。使用済みの値はです `storagegrid_storage_utilization_data_bytes` メートル法。




3. グラフの下のVolumesテーブルとObject Storesテーブルで使用可能な値を確認します。

> これらの値のグラフを表示するには、グラフアイコンをクリックします をクリックします。

**Disk Devices**

| Name | World Wide Name | I/O Load | Read Rate | Write Rate |
|---|---|---|---|---|
| croot(8:1,sda1) | N/A | 0.03% | 0 bytes/s | 3 KB/s |
| cvloc(8:2,sda2) | N/A | 0.85% | 0 bytes/s | 58 KB/s |
| sdc(8:16,sdb) | N/A | 0.00% | 0 bytes/s | 81 bytes/s |
| sdd(8:32,sdc) | N/A | 0.00% | 0 bytes/s | 82 bytes/s |
| sde(8:48,sdd) | N/A | 0.00% | 0 bytes/s | 82 bytes/s |

**Volumes**

| Mount Point | Device | Status | Size | Available | Write Cache Status |
|---|---|---|---|---|---|
| / | croot | Online | 21.00 GB | 14.90 GB | Unknown |
| /var/local | cvloc | Online | 85.86 GB | 84.10 GB | Unknown |
| /var/local/rangedb/0 | sdc | Online | 107.32 GB | 107.18 GB | Enabled |
| /var/local/rangedb/1 | sdd | Online | 107.32 GB | 107.18 GB | Enabled |
| /var/local/rangedb/2 | sde | Online | 107.32 GB | 107.18 GB | Enabled |

**Object Stores**

| ID | Size | Available | Replicated Data | EC Data | Object Data (%) | Health |
|---|---|---|---|---|---|---|
| 0000 | 107.32 GB | 96.45 GB | 250.90 KB | 0 bytes | 0.00% | No Errors |
| 0001 | 107.32 GB | 107.18 GB | 0 bytes | 0 bytes | 0.00% | No Errors |
| 0002 | 107.32 GB | 107.18 GB | 0 bytes | 0 bytes | 0.00% | No Errors |

4. 一定期間の値を監視して、使用可能なストレージスペースが消費される速度を見積もります。
5. システムの正常な運用を維持するには、使用可能なスペースを使い切る前に、ストレージノードを追加するか、ストレージボリュームを追加するか、オブジェクトデータをアーカイブします。

   拡張のタイミングを計画する際には、追加のストレージを調達して設置するのにどれくらいの時間がかかるかを検討します。

   > ILM ポリシーでイレイジャーコーディングを使用している場合は、既存のストレージノードの使用率が約 70% のときに拡張して、追加する必要のあるノードの数を減らすことができます。

   ストレージの拡張計画の詳細については、 StorageGRID の拡張手順を参照してください。

   Low object data storage *アラートと従来のStorage Status（SSTS）アラームは、ストレージノードにオブジェクトデータを格納するための十分なスペースが残っていない場合にトリガーされます。

関連情報

"StorageGRID の管理"

"Low object data storageアラートのトラブルシューティング"

"グリッドを展開します"

# 各ストレージノードのメタデータの使用量を監視して、重要なデータベース処理に使用できるスペースが十分に残っていることを確認する必要があります。オブジェクトメタデータが許容されるメタデータスペースの 100% を超える前に、各サイトに新しいストレージノードを追加する必要があります。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

このタスクについて

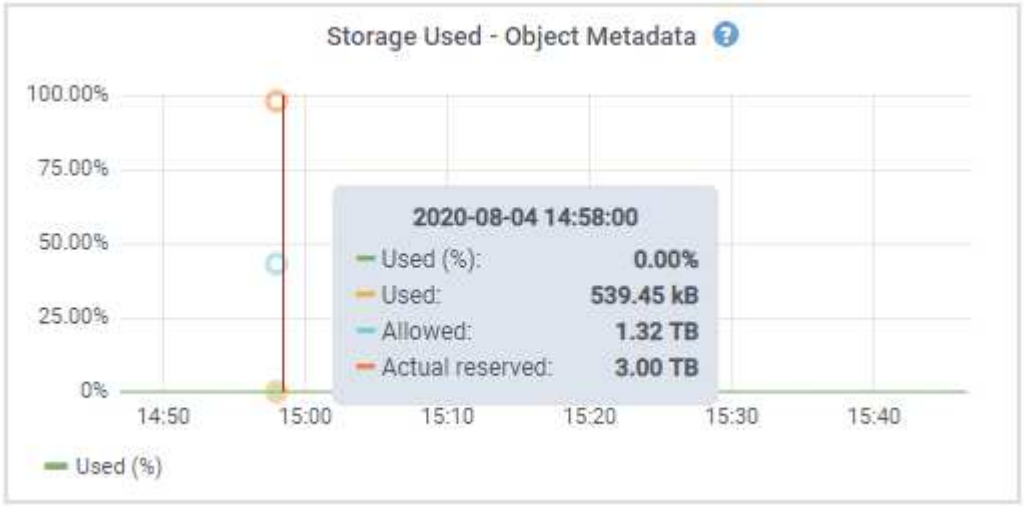
StorageGRID は、冗長性を確保し、オブジェクトメタデータを損失から保護するために、各サイトでオブジェクトメタデータのコピーを 3 つ保持します。3 つのコピーは、各ストレージノードのストレージボリューム 0 でメタデータ用にリザーブされたスペースを使用して、各サイトのすべてのストレージノードに均等に分散されます。

場合によっては、グリッドのオブジェクトメタデータ容量がオブジェクトのストレージ容量よりも早く消費されることがあります。たとえば、一般に大量の小さいオブジェクトを取り込む場合は、オブジェクトストレージの容量が十分に残っている場合でも、ストレージノードを追加してメタデータ容量を増やす必要があります。

メタデータの使用量を増やすことができる要因には、ユーザのメタデータとタグのサイズと数、マルチパートアップロードのパートの合計数、 ILM のストレージの場所に対する変更の頻度などがあります。

手順

1. ノード*>*ストレージノード*>*ストレージ*を選択します。
2. 「Storage Used - Object Metadata」グラフにカーソルを合わせると、特定の時間の値が表示されます。




| 価値 | 説明 | **Prometheus** 指標 |
| --- | --- | --- |
| 使用済み（ % ） | このストレージノードで使用されている使用可能なメタデータスペースの割合。 | `storagegrid_storage_utilization_metadata_bytes/ storagegrid_storage_utilization_metadata_allowed_bytes` |

| 価値 | 説明 | Prometheus 指標 |
| --- | --- | --- |
| 使用済み | このストレージノードで使用されている使用可能なメタデータスペースのバイト数。 | `storagegrid_storage_utilization_metadata_bytes` |
| 許可されます | このストレージノードでオブジェクトメタデータに使用できるスペース。各ストレージノードのこの値がどのように判断されるかについては、StorageGRID の管理手順を参照してください。 | `storagegrid_storage_utilization_metadata_allowed_bytes` |
| 実際の予約 | このストレージノードでメタデータ用にリザーブされている実際のスペース。使用可能なスペースと重要なメタデータ処理に必要なスペースが含まれます。各ストレージノードのこの値の計算方法については、StorageGRID の管理手順を参照してください。 | `storagegrid_storage_utilization_metadata_reserved_bytes` |

サイトまたはグリッドの合計値に、指標が報告されていないノード（オフラインノードなど）は含まれません。

3. Used （ % ） * 値が 70% 以上の場合は、各サイトにストレージノードを追加して StorageGRID システムを拡張します。

Low metadata storage * アラートは、「 Used （ % ）」の値が特定のしきい値に達するとトリガーされます。オブジェクトメタデータの使用スペースが使用可能なスペースの 100% を超えている場合、望ましくない結果が生じる可能性があります。

新しいノードを追加すると、サイト内のすべてのストレージノード間でオブジェクトメタデータが自動的にリバランシングされます。StorageGRID システムの拡張手順を参照してください。

関連情報

"Low metadata storageアラートのトラブルシューティング"

"StorageGRID の管理"

"グリッドを展開します"

情報ライフサイクル管理の監視

Information Lifecycle Management （ ILM ；情報ライフサイクル管理）システムは、グリッドに格納されているすべてのオブジェクトのデータ管理を提供します。ILM 処理を監視して、グリッドが現在の負荷を処理できるかどうか、またはリソースの追加が必要かどうかを判断する必要があります。

必要なもの

Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

このタスクについて

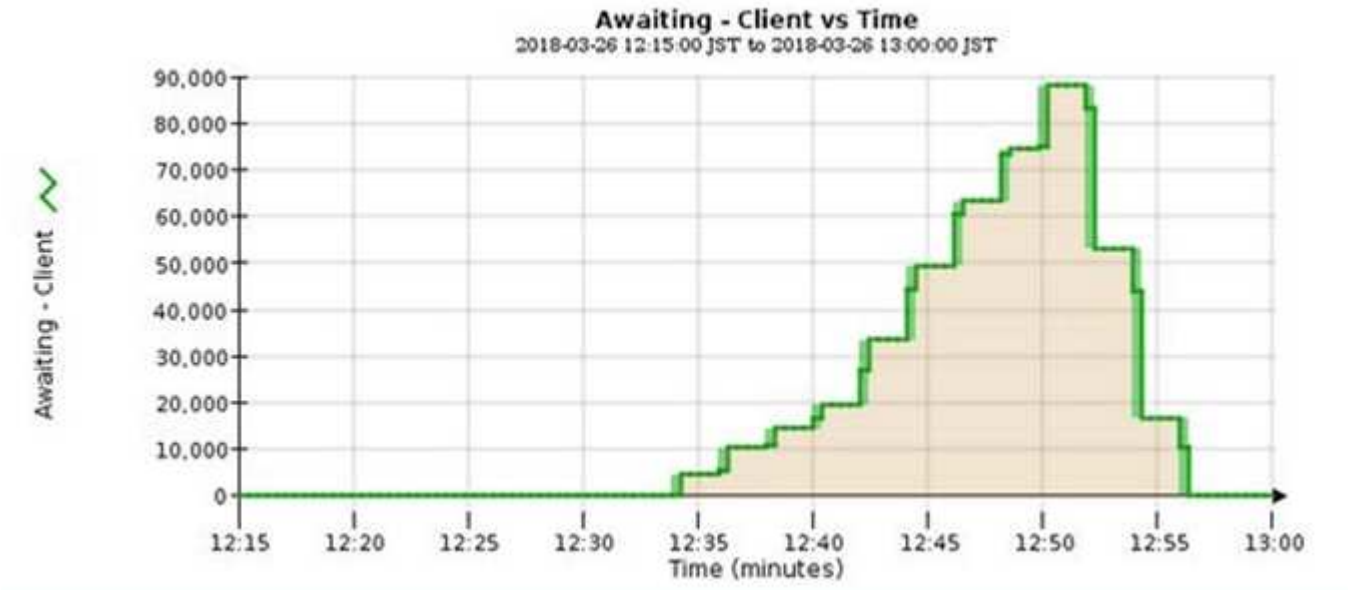
StorageGRID システムは、アクティブな ILM ポリシーを適用することでオブジェクトを管理します。ILM ポリシーとそれに関連付けられた ILM ルールによって、作成されるコピーの数、作成先、コピーの配置場所、各コピーの保持期間が決まります。

オブジェクトの取り込みやその他のオブジェクト関連アクティビティが StorageGRID で評価される速度を超えると、 ILM 配置手順をほぼリアルタイムで実行できないオブジェクトがキューに登録される可能性があります。StorageGRID がクライアント処理に対応しているかどうかを監視するには、 Awaiting - Client 属性をグラフ化します。

この属性をグラフ化するには：

1. Grid Manager にサインインします。
2. ダッシュボードで、 Information Lifecycle Management （ ILM ；情報ライフサイクル管理）パネルの * Awaiting - Client * エントリを探します。
3. グラフアイコンをクリックします 。

次の例のグラフは、 ILM 評価を待機しているオブジェクトの数が一時的に増加したあと、最終的に減少したことを示しています。このような傾向は、 ILM をほぼリアルタイムで処理することが一時的に不可能になったことを示しています。




Awaiting - Client のグラフで一時的な急増が予想されます。ただし、グラフに表示される値が増え続ける一方で低下しない場合は、より多くのリソースを効率的に運用する必要があります。追加のストレージノードがある場合や、 ILM ポリシーによってオブジェクトがリモートサイトに配置される場合は、より多くのネットワーク帯域幅が必要になります。

Nodes *ページを使用すると、ILMキューをさらに調査できます。

手順

1. [ノード（ Nodes）]を選択し

2. ***grid name***>*ilm * を選択します。
3. ILM キューのグラフにカーソルを合わせると、特定の時点における次の属性の値が表示されます。
   - * Objects queued （ from client operations ） * ：クライアント処理（取り込みなど）のために ILM による評価を待機しているオブジェクトの総数。
   - * Objects queued （ from all operations ） * ： ILM による評価を待機しているオブジェクトの総数。
   - * Scan rate （ objects/sec ） * ：グリッドのオブジェクトがスキャンされて ILM のキューに登録される速度。
   - * 評価速度（オブジェクト数 / 秒） * ：グリッド内の ILM ポリシーに照らしてオブジェクトが評価されている現在の速度。
4. ILM キューセクションで、次の属性を確認します。

   ILM キューのセクションはグリッドのみを対象としています。この情報は、サイトまたはストレージノードの ILM タブには表示されません。

   - * スキャン期間 - 推定 * ： ILM によるすべてのオブジェクトのフルスキャンが完了するまでの推定時間。

     フルスキャンが完了しても、 ILM がすべてのオブジェクトに適用されるとは限りません。

   - * Repairs Attempted * ：レプリケートデータの修復処理が試行されたオブジェクトの総数。この数は、ストレージノードがハイリスクオブジェクトの修復を試みるたびに増分します。グリッドがビジー状態になった場合は、リスクの高い ILM の修復が優先されます。

     修復後にレプリケーションに失敗した場合は、同じオブジェクトの修復で再び増分される可能性があります。

   これらの属性は、ストレージノードのボリュームリカバリの進捗状況を監視する場合に役立ちます。試行された修理の回数が増えなくなり、完全スキャンが完了した場合は、修理が完了している可能性があります。

パフォーマンス、ネットワーク、およびシステムリソースの監視

# パフォーマンス、ネットワーク、およびシステムのリソースを監視して、StorageGRIDが現在の負荷を処理できるかどうかを判断し、クライアントのパフォーマンスが時間とともに低下しないようにする必要があります。

クエリのレイテンシを監視しています

## オブジェクトの格納、読み出し、削除などのクライアント操作を実行すると、グリッドの分散データベースであるオブジェクトメタデータへのクエリが作成されます。クエリレイテンシの傾向を監視して、グリッドリソースが現在の負荷に適していることを確認する必要があります。

必要なもの

Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

このタスクについて

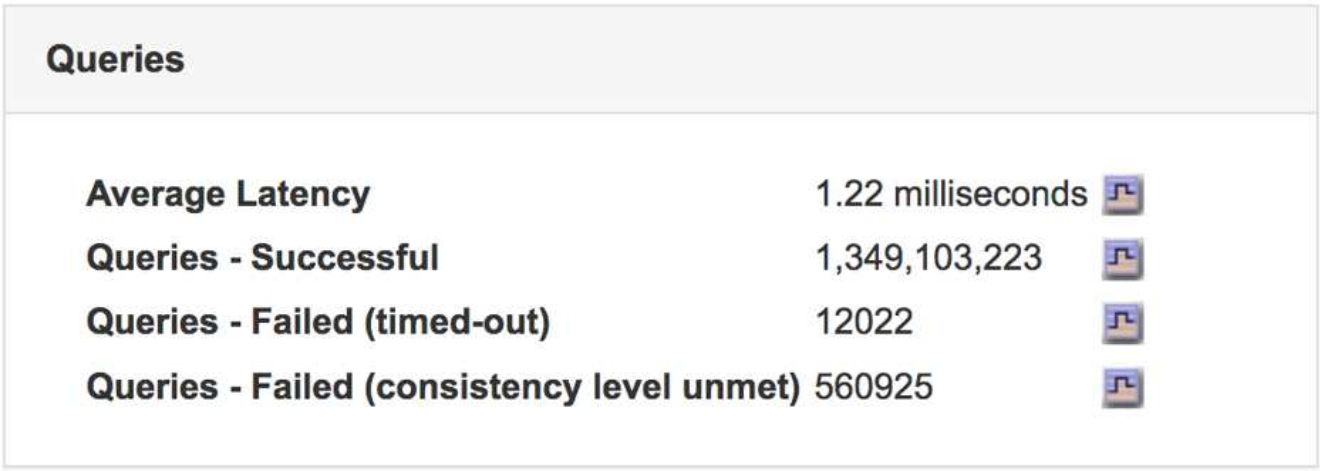
クエリのレイテンシが一時的に上昇するのは正常な状態であり、取り込み要求の急増が原因である可能性があります。失敗したクエリも正常な状態であり、一時的なネットワークの問題や一時的に使用できないノードが原因で発生する可能性があります。ただし、クエリの平均実行時間が長くなると、グリッドの全体的なパフォーマンスは低下します。

クエリのレイテンシが時間の経過に伴って増加している場合は、将来のワークロードに対応できるように拡張手順 にストレージノードを追加することを検討してください。

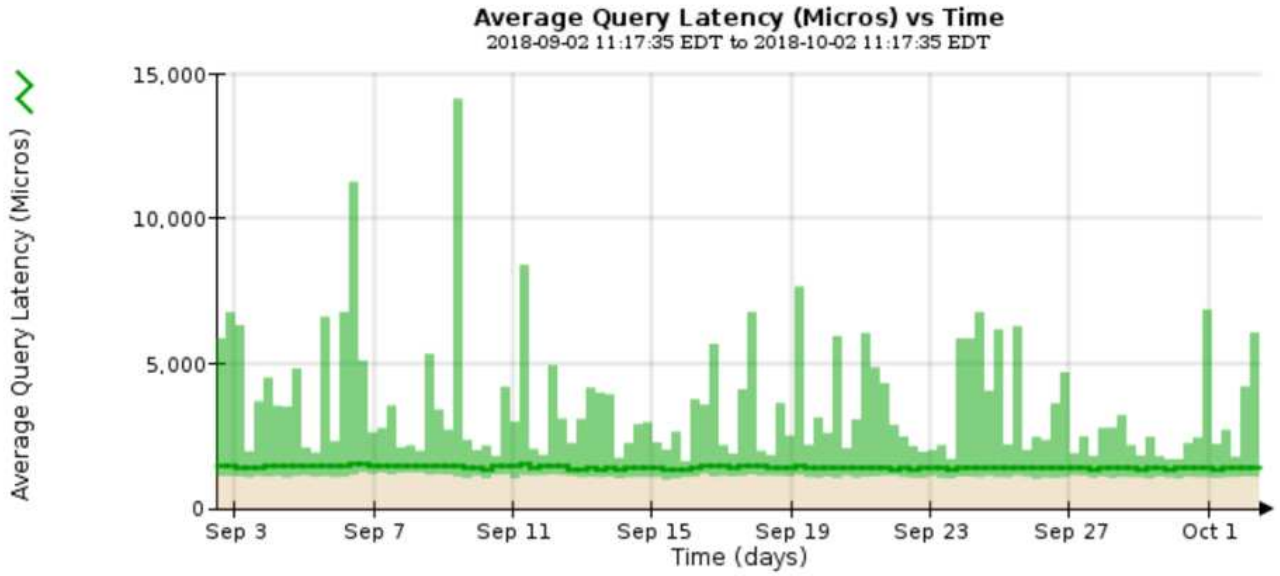
クエリの平均時間が長すぎると、「メタデータクエリの高レイテンシ*」アラートがトリガーされます。

手順

1. ノード*>*ストレージノード*>*オブジェクト*を選択します。
2. クエリの表までスクロールし、平均レイテンシの値を確認します。




3. グラフアイコンをクリックします 時間の経過に伴う値をグラフ化します。




この例のグラフは、グリッドの通常運用時のクエリレイテンシの急増を示しています。

関連情報

"グリッドを展開します"

ネットワーク接続およびパフォーマンスの監視

# グリッドの動作を許可するには、グリッドノードが相互に通信できる必要があります。ノードとサイト間のネットワークの整合性、およびサイト間のネットワーク帯域幅は、効率的な運用に不可欠です。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

ネットワーク接続と帯域幅は、情報ライフサイクル管理（ ILM ）ポリシーでサイト間のレプリケートオブジェクトをコピーする場合や、サイト障害からの保護を提供するスキームを使用してイレイジャーコーディングオブジェクトを格納する場合に特に重要になります。サイト間のネットワークを使用できない場合、ネットワークレイテンシが高すぎる場合、またはネットワーク帯域幅が不十分な場合、一部の ILM ルールでオブジェクトが想定どおりに配置されない可能性があります。その結果、取り込みエラーが発生する（ ILM ルールに対して Strict ingest option が選択されている場合）か、あるいは取り込みパフォーマンスの低下や ILM バックログが発生する可能性があります。

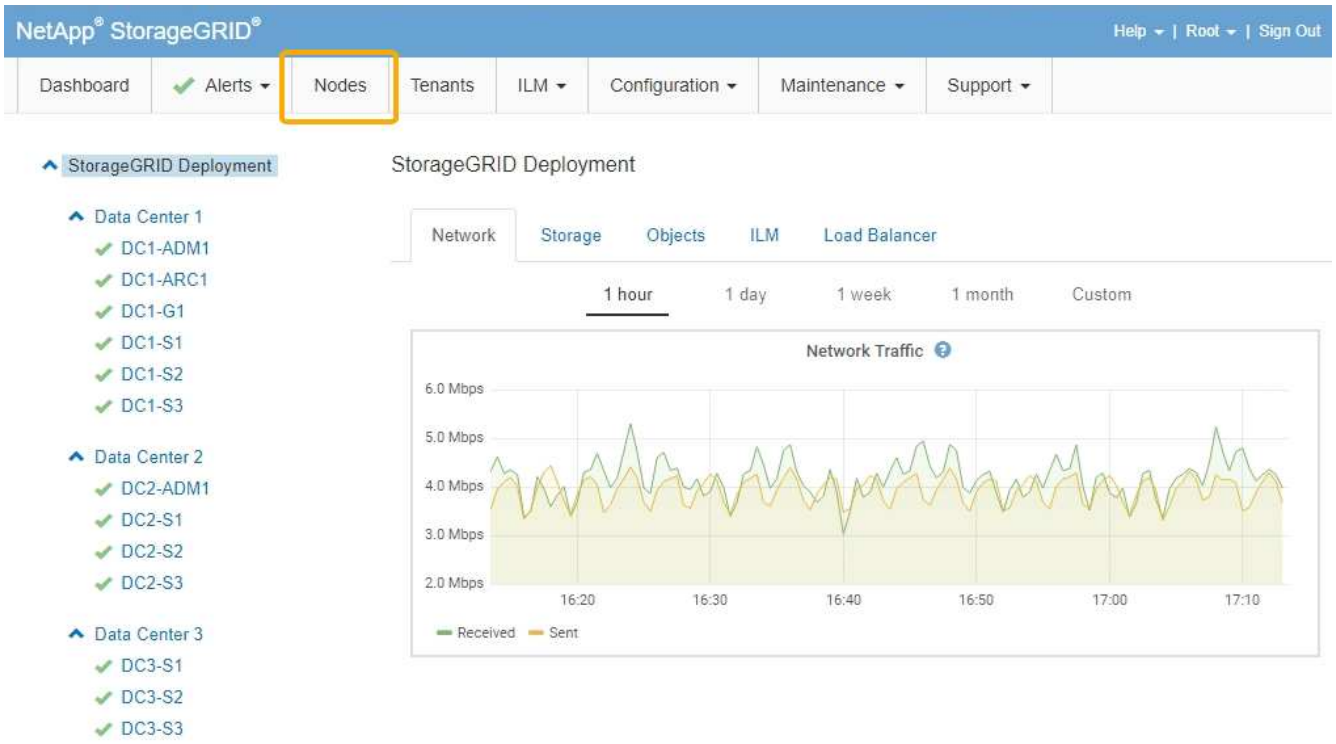
グリッドマネージャを使用して接続とネットワークのパフォーマンスを監視できるため、何らかの問題に迅速に対処できます。

また、ネットワークトラフィック分類ポリシーを作成して、特定のテナント、バケット、サブネット、またはロードバランサエンドポイントに関連するトラフィックを監視および制限することを検討してください。StorageGRID の管理手順を参照してください。

手順

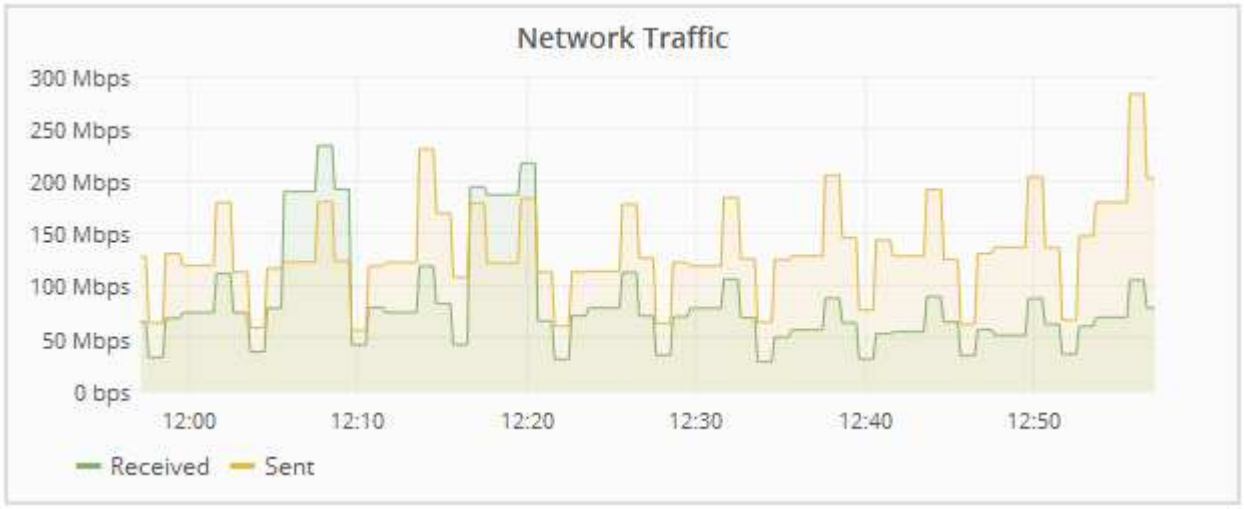
1. [ノード（ Nodes）]を選択し

   Nodes ページが表示されます。ノードアイコンは、接続されているノード（緑のチェックマークアイコン）と切断されているノード（青またはグレーのアイコン）を一目で示します。




2. グリッド名、特定のデータセンターサイト、またはグリッドノードを選択し、 * ネットワーク * タブを選択します。

   このネットワークトラフィックのグラフには、グリッド全体、データセンターサイト、またはノードのネットワークトラフィックの概要が表示されます。




   a. グリッドノードを選択した場合は、ページの「 * ネットワークインターフェイス * 」セクションまでスクロールします。

**Network Interfaces**

| Name | Hardware Address | Speed | Duplex | Auto Negotiate | Link Status |
|---|---|---|---|---|---|
| eth0 | 50:6B:4B:42:D7:11 | 100 Gigabit | Full | Off | Up |
| eth1 | D8:C4:97:2A:E4:9E | Gigabit | Full | Off | Up |
| eth2 | 50:6B:4B:42:D7:11 | 100 Gigabit | Full | Off | Up |
| hic1 | 50:6B:4B:42:D7:11 | 25 Gigabit | Full | Off | Up |
| hic2 | 50:6B:4B:42:D7:11 | 25 Gigabit | Full | Off | Up |
| hic3 | 50:6B:4B:42:D7:11 | 25 Gigabit | Full | Off | Up |
| hic4 | 50:6B:4B:42:D7:11 | 25 Gigabit | Full | Off | Up |
| mtc1 | D8:C4:97:2A:E4:9E | Gigabit | Full | On | Up |
| mtc2 | D8:C4:97:2A:E4:9F | Gigabit | Full | On | Up |

b. グリッドノードがある場合は、下にスクロールしてページの「 * ネットワーク通信 * 」セクションを確認します。

受信および送信テーブルには、各ネットワークで送受信されたバイト数とパケット数、およびその他の受信および送信メトリックが表示されます。

**Network Communication**

Receive

| Interface | Data | Packets | Errors | Dropped | Frame Overruns | Frames |
|---|---|---|---|---|---|---|
| eth0 | 3.250 TB | 5,610,578,144 | 0 | 8,327 | 0 | 0 |
| eth1 | 1.205 GB | 9,828,095 | 0 | 32,049 | 0 | 0 |
| eth2 | 849.829 GB | 186,349,407 | 0 | 10,269 | 0 | 0 |
| hic1 | 114.864 GB | 303,443,393 | 0 | 0 | 0 | 0 |
| hic2 | 2.315 TB | 5,351,180,956 | 0 | 305 | 0 | 0 |
| hic3 | 1.690 TB | 1,793,580,230 | 0 | 0 | 0 | 0 |
| hic4 | 194.283 GB | 331,640,075 | 0 | 0 | 0 | 0 |
| mtc1 | 1.205 GB | 9,828,096 | 0 | 0 | 0 | 0 |
| mtc2 | 1.168 GB | 9,564,173 | 0 | 32,050 | 0 | 0 |

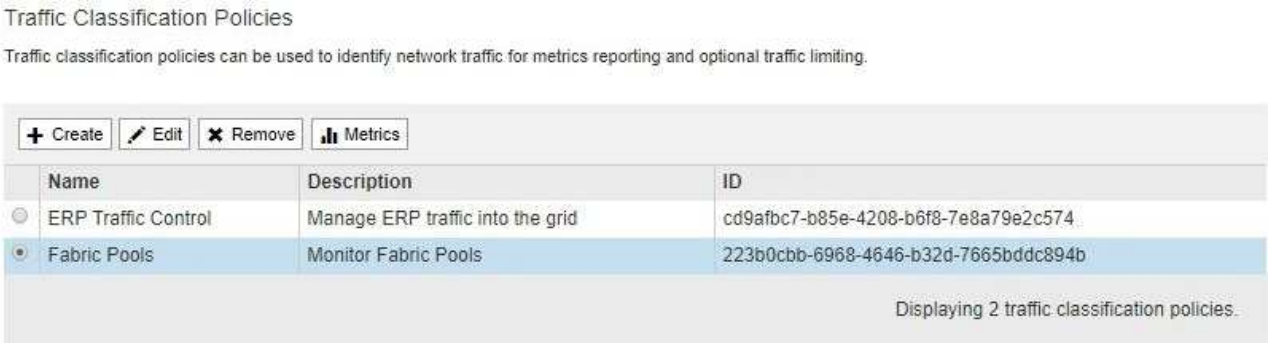
Transmit

| Interface | Data | Packets | Errors | Dropped | Collisions | Carrier |
|---|---|---|---|---|---|---|
| eth0 | 5.759 TB | 5,789,638,626 | 0 | 0 | 0 | 0 |
| eth1 | 4.563 MB | 41,520 | 0 | 0 | 0 | 0 |
| eth2 | 855.404 GB | 139,975,194 | 0 | 0 | 0 | 0 |
| hic1 | 289.248 GB | 326,321,151 | 5 | 0 | 0 | 5 |
| hic2 | 1.636 TB | 2,640,416,419 | 18 | 0 | 0 | 18 |
| hic3 | 3.219 TB | 4,571,516,003 | 33 | 0 | 0 | 33 |
| hic4 | 1.687 TB | 1,658,180,262 | 22 | 0 | 0 | 22 |
| mtc1 | 4.563 MB | 41,520 | 0 | 0 | 0 | 0 |
| mtc2 | 49.678 KB | 609 | 0 | 0 | 0 | 0 |

3. トラフィック分類ポリシーに関連付けられたメトリックを使用して、ネットワークトラフィックを監視します。

   a. [* Configuration **]>[** Network Settings **]>[** Traffic Classification]を選択します。

      [Traffic Classification Policies] ページが表示され、既存のポリシーがテーブルにリストされます。




b. ポリシーに関連付けられているネットワーク指標を示すグラフを表示するには、ポリシーの左側にあるオプションボタンを選択し、 [*Metrics] をクリックします。

c. グラフを確認して、ポリシーに関連付けられているネットワークトラフィックを把握します。

トラフィック分類ポリシーがネットワークトラフィックを制限するように設計されている場合は、トラフィックが制限される頻度を分析し、ポリシーがニーズを満たし続けるかどうかを判断します。時間をかけて、必要に応じて各トラフィック分類ポリシーを調整します。

トラフィック分類ポリシーを作成、編集、または削除するには、 StorageGRID の管理手順を参照してください。

関連情報

"[ネットワークタブを表示します"]

"ノードの接続状態を監視しています"

"StorageGRID の管理"

ノードレベルのリソースを監視しています

# 個々のグリッドノードを監視して、そのリソース利用率レベルを確認する必要があります。

必要なもの

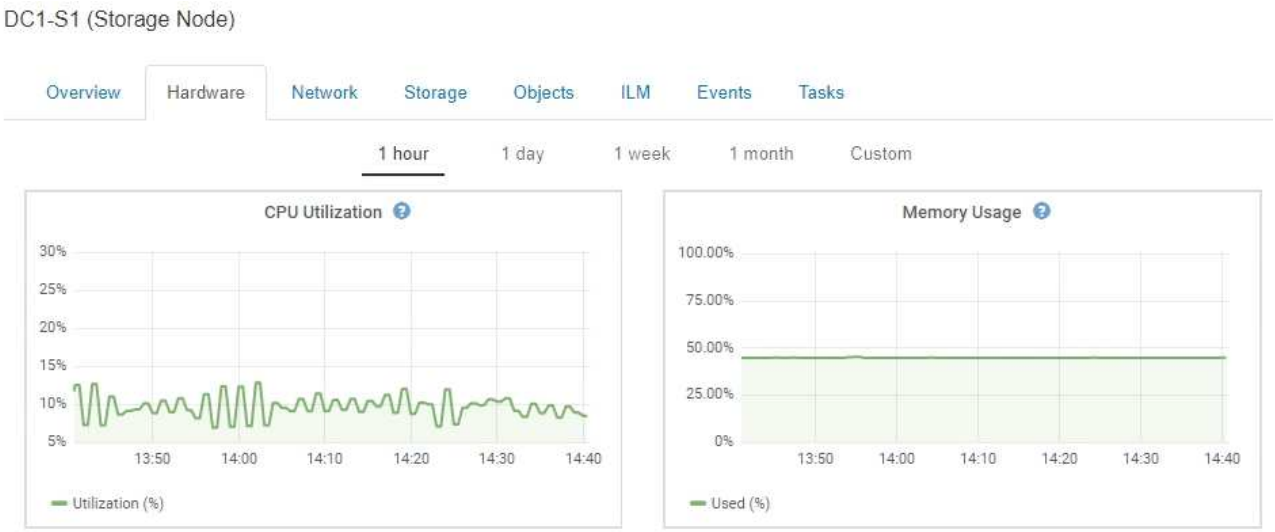
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

このタスクについて

ノードが常に過負荷状態になっていると、効率的な処理に必要なノードの数が増えます。

手順

1. グリッドノードのハードウェア利用率に関する情報を表示するには、次の手順を実行します。
   a. [* Nodes （ノード）]ページで、ノードを選択します。
   b. [**Hardware**] タブを選択して、 CPU 使用率とメモリ使用率のグラフを表示します。




c. 別の期間を表示するには、グラフまたはグラフの上にあるコントロールのいずれかを選択します。1 時間、 1 日、 1 週間、または 1 カ月の期間の情報を表示できます。また、カスタムの間隔を設定して、日時の範囲を指定することもできます。

d. ノードがストレージアプライアンスまたはサービスアプライアンスでホストされている場合は、下にスクロールしてコンポーネントの表を表示します。すべてのコンポーネントのステータスは "Nominal .`" である必要があります その他のステータスのコンポーネントを調査します。

関連情報

"アプライアンスストレージノードに関する情報の表示"

"アプライアンスの管理ノードとゲートウェイノードに関する情報の表示"

テナントアクティビティの監視

すべてのクライアントアクティビティがテナントアカウントに関連付けられている。Grid Manager を使用してテナントのストレージ使用状況やネットワークトラフィックを監視できます。または、監査ログまたは Grafana ダッシュボードを使用して、テナントが StorageGRID を使用している状況に関する詳細情報を収集できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access権限またはAdministrator権限が必要です。

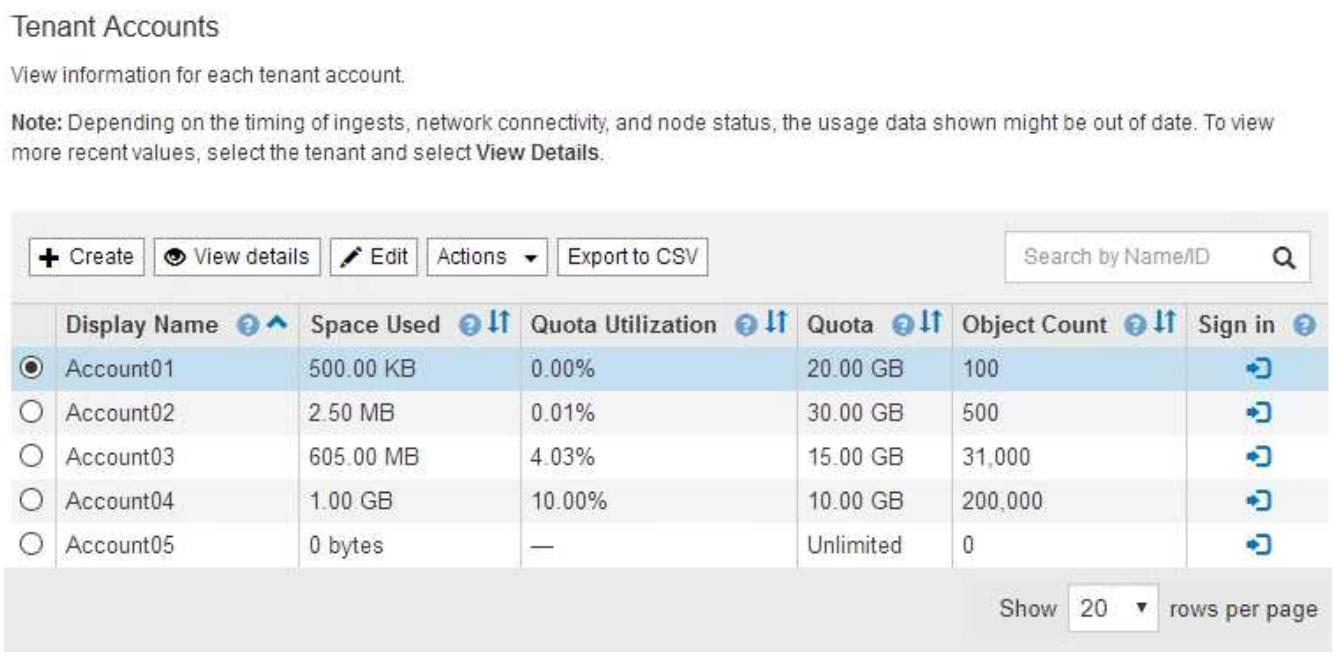
このタスクについて

使用済みスペースの値は推定値です。これらの推定値は、取り込みのタイミング、ネットワーク接続、ノードのステータスによって左右されます。

手順

1. すべてのテナントで使用されているストレージの量を確認するには、「* tenants *」を選択します。

   テナントごとに、使用済みスペース、クォータ利用率、クォータ、オブジェクト数が表示されます。テナントにクォータが設定されていない場合は'[Quota Utilization]フィールドにダッシュ（-）が表示され'Quotaフィールドには[Unlimited]と表示されます




システムに20個を超えるアイテムが含まれている場合は、各ページに一度に表示する行数を指定できます。検索ボックスを使用して、表示名またはテナントIDでテナントアカウントを検索します。

テナントアカウントにサインインするには、テーブルの*サインイン*列でリンクを選択します。

2. 必要に応じて、 * Export to CSV * を選択し、すべてのテナントの使用量の値を含む .csv ファイルを表示およびエクスポートします。

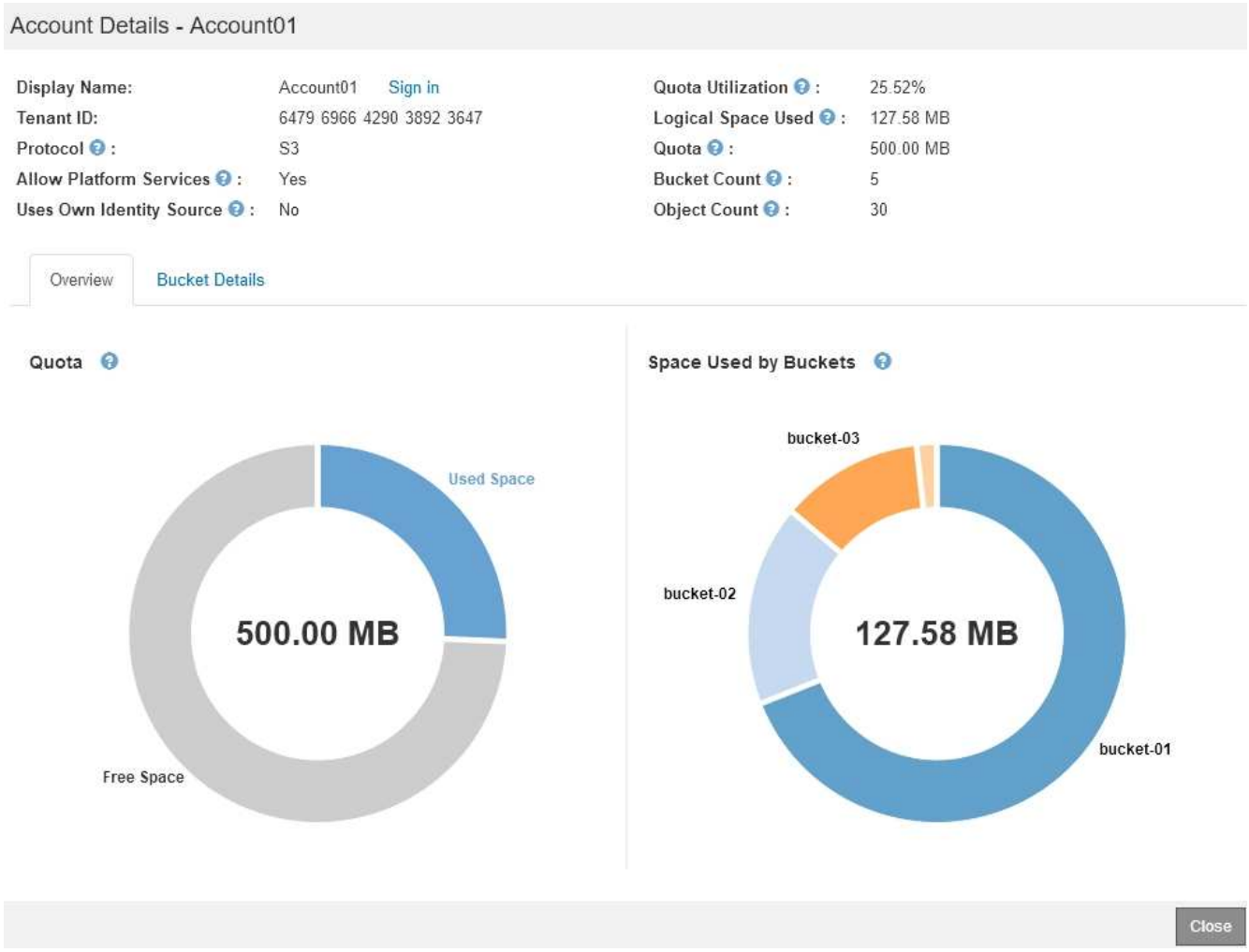
   を開くか保存するかを確認するメッセージが表示されます `.csv` ファイル。

| Tenant ID | Display Name | Space Used (Bytes) | Quota utilization (%) | Quota (Bytes) | Object Count | Protocol |
|---|---|---|---|---|---|---|
| 56243391454153665591 | Account01 | 500000 | 0 | 20000000000 | 100 | S3 |
| 82457136581801590515 | Account02 | 2500000 | 0.01 | 30000000000 | 500 | S3 |
| 04489086912300179118 | Account03 | 605000000 | 4.03 | 15000000000 | 31000 | S3 |
| 26417581662098345719 | Account04 | 1000000000 | 10 | 10000000000 | 200000 | S3 |
| 78472447501213318575 | Account05 | 0 | | | 0 | S3 |

図 **1. csv** ファイルの内容は次の例のようになります。

3. 使用状況グラフなど、特定のテナントの詳細を表示するには、テナントアカウントページでテナントアカウントを選択し、*詳細を表示*を選択します。

   Account Detailsページが表示され、概要情報、使用済みクォータと残りのクォータの量を示すグラフ、およびバケット（S3）またはコンテナ（Swift）内のオブジェクトデータの量を表すグラフが表示されます。




◦ クォータ

このテナントにクォータが設定されている場合は、* Quota *チャートに、このテナントが使用したクォータの量とまだ使用可能なクォータの量が表示されます。クォータが設定されていない場合、テナントのクォータは無制限となり、情報メッセージが表示されます。テナントがストレージクォータを 1% 以上かつ 1GB 以上超過した場合は、クォータの総容量と超過容量がグラフに表示されます。

使用済みスペースセグメントにカーソルを合わせると、格納されているオブジェクトの数と使用されている合計バイト数を確認できます。空きスペースセグメントにカーソルを合わせると、使用可能なストレージクォータのバイト数を確認できます。

クォータ使用率は内部の推定値に基づいており、場合によっては超過することがあります。たとえば、テナントがクォータを超えた場合、 StorageGRID はテナントがオブジェクトのアップロードを開始したときにクォータをチェックし、新しい取り込みを拒否します。ただし、 StorageGRID では、クォータを超過したかどうかを判断する際に、現在のアップロードのサイズは考慮されません。オブジェクトが削除された場合、クォータ使用率が再計算されるまでテナントが一時的に新しいオブジェクトをアップロードできなくなることがあります。クォータ使用率の計算には 10 分以上かかることがあります。

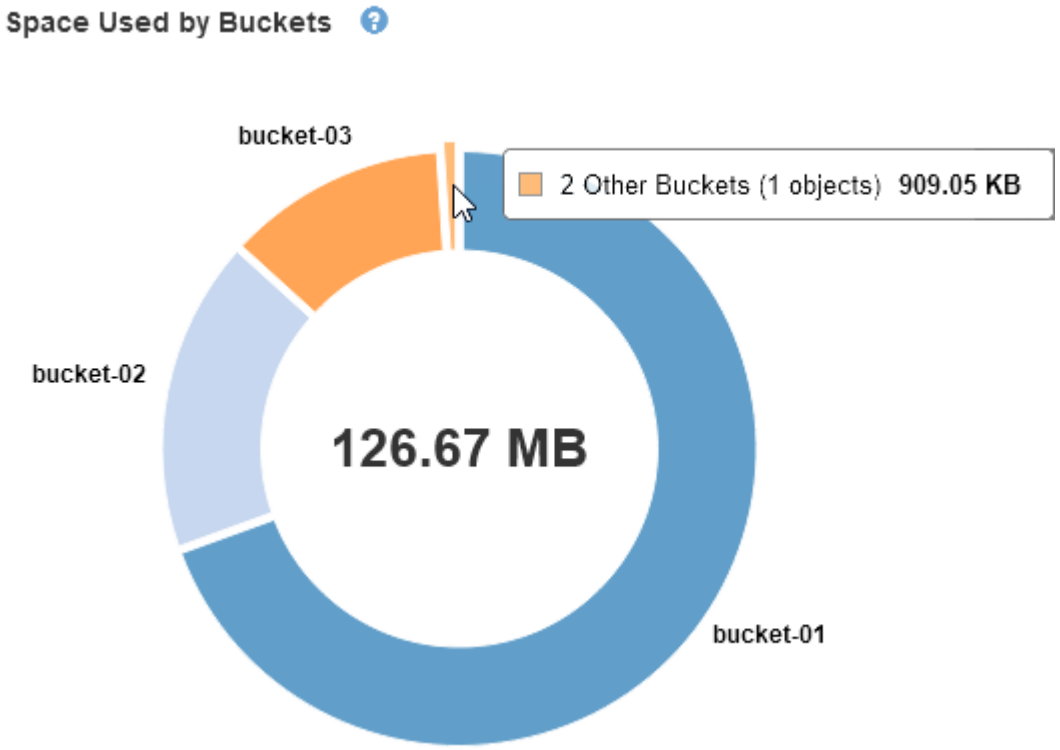
テナントのクォータ利用率は、テナントが StorageGRID にアップロードしたオブジェクトデータの総容量（論理サイズ）を示します。クォータ利用率は、これらのオブジェクトおよびそのメタデータのコピーを格納するために使用されるスペース（物理サイズ）を表していません。

テナントのクォータ使用率が高い * アラートを有効にすると、テナントがそのクォータを消費しているかどうかを確認できます。有効にすると、テナントのクォータの 90% が使用されたときにこのアラートがトリガーされます。詳細については、アラートリファレンスを参照してください。

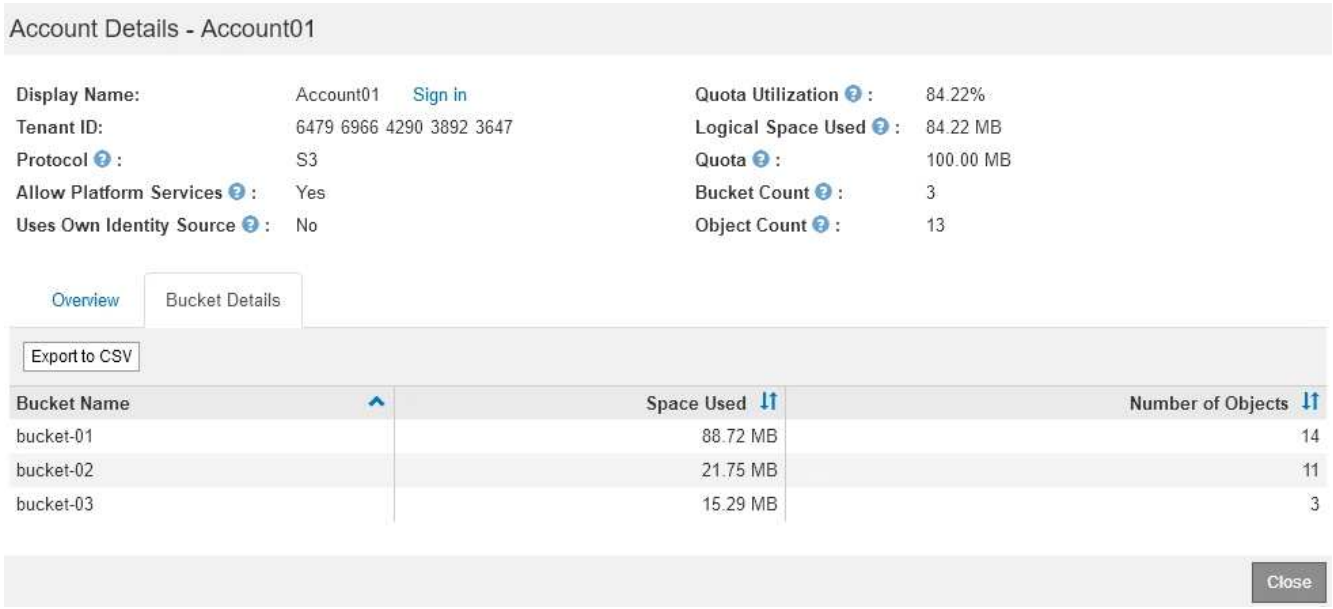
- 使用済みスペース

  バケットで使用されているスペース*（S3）またはコンテナで使用されているスペース*（Swift）グラフには、テナントの最大バケットが表示されます。使用済みスペースは、バケット内のオブジェクトデータの総容量です。この値は、 ILM コピーとオブジェクトメタデータに必要なストレージスペースを表しているわけではありません。

  テナントに含まれているバケットまたはコンテナが9つを超える場合は、それらのバケットが「Other」というセグメントに結合されます。一部のグラフセグメントは小さすぎてラベルを含めることができません。任意のセグメントにカーソルを合わせると、ラベルが表示され、格納されているオブジェクトの数や各バケットまたはコンテナの合計バイト数などの詳細情報を確認できます。




4. 「* Bucket Details （**S3**）」または「 Container Details *（Swift）」を選択して、各テナントのバケットまたはコンテナのスペース使用済みオブジェクトとオブジェクト数のリストを表示します。




5. 必要に応じて、「 * Export to CSV * 」を選択し、各バケットまたはコンテナの使用量の値を含む .csv ファイルを表示してエクスポートします。

   **csv**ファイルを開くか保存するように求められます。

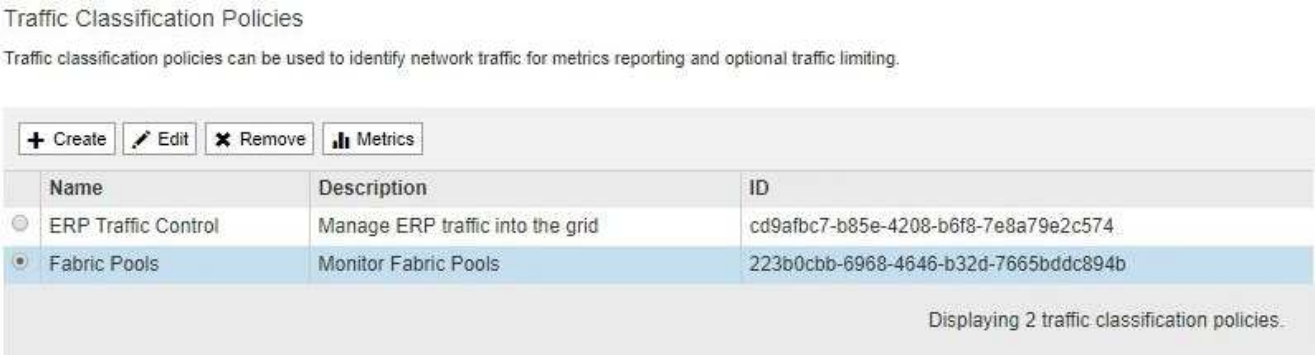
   個々の S3 テナントの .csv ファイルの内容は、次の例のようになります。

| Tenant ID | Bucket Name | Space Used (Bytes) | Number of Objects |
|---|---|---|---|
| 64796966429038923647 | bucket-01 | 88717711 | 14 |
| 64796966429038923647 | bucket-02 | 21747507 | 11 |
| 64796966429038923647 | bucket-03 | 15294070 | 3 |

6. テナントにトラフィック分類ポリシーが設定されている場合は、そのテナントのネットワークトラフィックを確認します。

   a. [* Configuration **]>[** Network Settings **]>[** Traffic Classification]を選択します。

      [Traffic Classification Policies] ページが表示され、既存のポリシーがテーブルにリストされます。




   a. ポリシーのリストを確認して、特定のテナントに適用されるポリシーを特定します。

   b. ポリシーに関連付けられている指標を表示するには、ポリシーの左側にあるオプションボタンを選択し、 [*Metrics] をクリックします。

   c. グラフを分析して、ポリシーがトラフィックを制限している頻度と、ポリシーを調整する必要がある

かどうかを判断します。

トラフィック分類ポリシーを作成、編集、または削除するには、 StorageGRID の管理手順を参照してください。

7. 必要に応じて、監査ログを使用してテナントのアクティビティをより詳細に監視できます。

   たとえば、次の種類の情報を監視できます。

   - PUT 、 GET 、 DELETE など、特定のクライアント処理
   - オブジェクトサイズ
   - オブジェクトに適用されている ILM ルール
   - クライアント要求の送信元 IP

   監査ログは、選択したログ分析ツールを使用して分析可能なテキストファイルに書き込まれます。これにより、クライアントアクティビティをよりよく理解したり、高度なチャージバックおよび課金モデルを実装したりできます。詳細については、監査メッセージを確認する手順を参照してください。

8. 必要に応じて、 Prometheus 指標を使用してテナントのアクティビティをレポートします。

   - Grid Managerで、* Support > Tools > Metrics *を選択します。S3 の概要など、既存のダッシュボードを使用してクライアントのアクティビティを確認できます。

     Metrics ページで使用できるツールは、主にテクニカルサポートが使用することを目的としています。これらのツールの一部の機能およびメニュー項目は、意図的に機能しないようになっています。

   - ヘルプ*>* APIドキュメント*を選択します。グリッド管理 API の指標セクションの指標を使用して、テナントアクティビティ用のカスタムのアラートルールとダッシュボードを作成できます。

関連情報

"アラート一覧"

"監査ログを確認します"

"StorageGRID の管理"

"サポート指標の確認"

アーカイブ容量を監視しています

外部アーカイブストレージシステムの容量を StorageGRID システムで直接監視することはできません。ただし、アーカイブノードからアーカイブ先にまだオブジェクトデータを送信できるかを監視することで、アーカイブメディアの拡張が必要かどうかを確認できます。

必要なもの

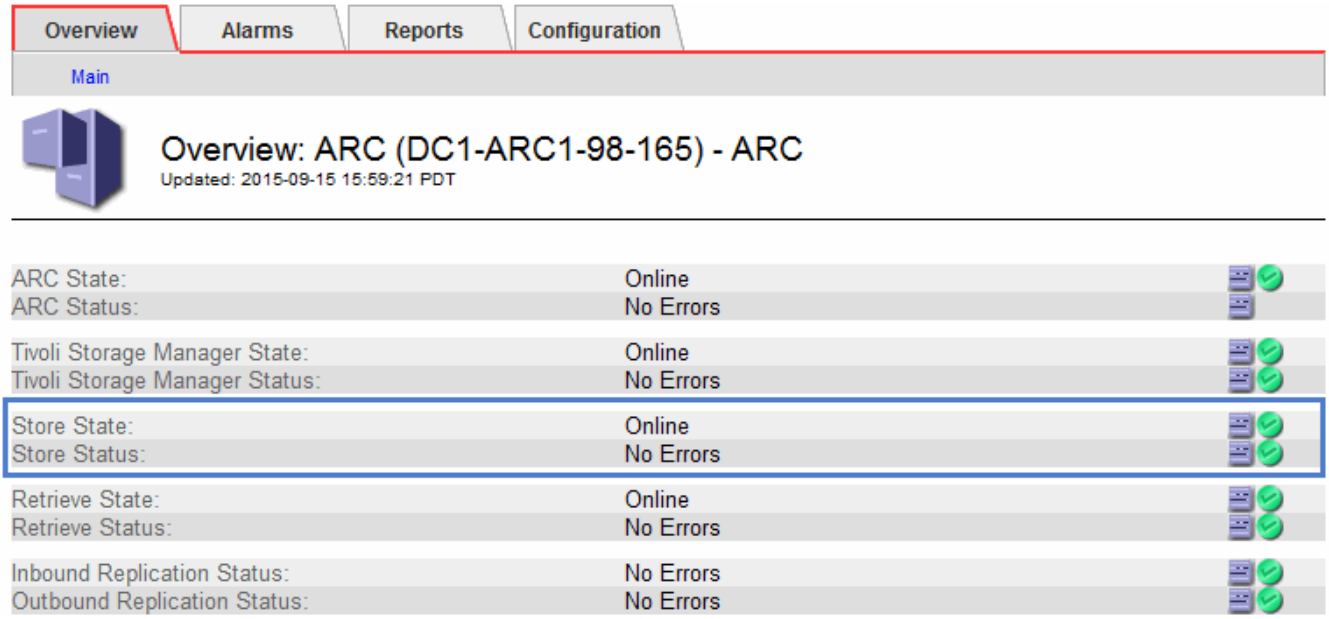
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

Store コンポーネントを監視することにより、アーカイブノードから対象のアーカイブストレージシステムにまだオブジェクトデータを送信できるかどうかを確認できます。また、 Store Failures （ ARVF ）アラームがトリガーされた場合、対象のアーカイブストレージシステムが容量に達し、オブジェクトデータをそれ以上受け入れられない状態になっている可能性があります。

手順

1. Support **>** Tools **>** Grid Topology *を選択します。
2. [***Archive Node***>*ARC **>Overview**>Main*] を選択します。
3. Store State 属性と Store Status 属性をチェックして、 Store コンポーネントが Online with No Errors であることを確認します。




Store コンポーネントがオフラインになっている場合やエラーがある場合は、対象のアーカイブストレージシステムの容量に達したためにオブジェクトデータをそれ以上受け入れられない状態になっている可能性があります。

関連情報

"StorageGRID の管理"

ロードバランシング処理の監視

ロードバランサを使用して StorageGRID へのクライアント接続を管理している場合は、システムを最初に設定したあとと、設定を変更したり拡張を行ったあとに、ロードバランシング処理を監視する必要があります。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

管理ノードまたはゲートウェイノード上のロードバランササービス、外部のサードパーティのロードバランサ、またはゲートウェイノード上の CLB サービスを使用して、複数のストレージノードにクライアント要求を分散することができます。

CLB サービスは廃止されました。

ロードバランシングを設定したら、オブジェクトの取り込みと読み出しの処理がストレージノード間で均等に分散されていることを確認する必要があります。要求が均等に分散されるため、 StorageGRID は負荷がかかっているクライアント要求への応答性を維持し、クライアントのパフォーマンスを維持できます。

ゲートウェイノードまたは管理ノードのハイアベイラビリティ（ HA ）グループをアクティブ / バックアップモードで設定した場合、グループ内の 1 つのノードだけがクライアント要求をアクティブに分散します。

StorageGRID の管理手順のクライアント接続の設定に関するセクションを参照してください。

手順

1. S3 または Swift クライアントがロードバランササービスを使用して接続する場合は、管理ノードまたはゲートウェイノードが想定どおりにトラフィックをアクティブに分散していることを確認します。
   a. [ノード（ Nodes）]を選択し
   b. ゲートウェイノードまたは管理ノードを選択します。
   c. 概要 * タブで、ノードインターフェイスが HA グループに含まれているかどうか、およびノードインターフェイスのロールがマスターであるかどうかを確認します。

      マスターのロールがノードで、 HA グループにないノードがクライアントに要求をアクティブに分散している必要があります。

   d. クライアント要求をアクティブに分散するノードごとに、 * ロードバランサ * タブを選択します。
   e. 過去 1 週間のロードバランサ要求トラフィックのチャートを確認して、ノードが要求をアクティブに分散していることを確認します。

      アクティブ / バックアップ HA グループのノードでは、 Backup ロールが随時割り当てられる場合があります。この間、ノードはクライアント要求を分散しません。

   f. ノードのオブジェクトスループットを確認するには、過去 1 週間のロードバランサの受信要求速度のグラフを確認します。
   g. StorageGRID システムの管理ノードまたはゲートウェイノードごとに上記の手順を繰り返します。
   h. 任意で、トラフィック分類ポリシーを使用して、ロードバランササービスが処理するトラフィックの詳細な内訳を表示できます。
2. S3 または Swift クライアントが CLB サービス（廃止）を使用して接続する場合は、次のチェックを実行します。
   a. [ノード（ Nodes）]を選択し
   b. ゲートウェイノードを選択します。
   c. 概要 * タブで、ノードインターフェイスが HA グループに含まれているかどうか、およびノードインターフェイスのロールがマスターであるかどうかを確認します。

      マスターのロールがノードで、 HA グループにないノードがクライアントに要求をアクティブに分散している必要があります。

d. クライアント要求をアクティブに分散するゲートウェイノードごとに、* Support > Tools > Grid Topology *を選択します。

e. [***Gateway Node***>*CLB*>*HTTP*>*Overview*>*Main*] を選択します。

f. ゲートウェイノードが要求をアクティブに処理していることを確認するために、受信セッション - ESTABLISHED * の数を確認します。

3. これらの要求がストレージノードに均等に分散されていることを確認します。

a. 「 * _ ストレージノード _ * > * LDR * > * HTTP * 」を選択します。

b. 現在確立されている受信セッション数 * を確認します。

c. グリッド内のストレージノードごとにこの手順を繰り返します。

セッションの数はすべてのストレージノードでほぼ同じにします。

関連情報

"StorageGRID の管理"

"Load Balancerタブの表示"

必要に応じてホットフィックスの適用またはソフトウェアのアップグレードを行います

## ホットフィックスや新しいバージョンの StorageGRID ソフトウェアが入手可能な場合は、その更新がシステムに適しているかどうかを評価し、必要に応じてインストールしてください。

このタスクについて

StorageGRID のホットフィックスには、フィーチャーパックまたはフィーチャーパックに含まれないソフトウェアの変更が含まれます。今後のリリースにも同じ変更が含まれます。

手順

1. ネットアップの StorageGRID ダウンロードページにアクセスします。

"ネットアップのダウンロード： StorageGRID"

2. [* タイプ / バージョンの選択 *] フィールドの下矢印を選択して、ダウンロード可能なアップデートのリストを表示します。

◦ * StorageGRID ソフトウェアのバージョン * ： 11.*x.y*

◦ * StorageGRID ホットフィックス * ： 11._x.y.z _

3. 更新に含まれている変更を確認します。

a. プルダウンメニューからバージョンを選択し、 * Go * をクリックします。

b. ネットアップアカウントのユーザ名とパスワードを使用してサインインします。

c. エンドユーザライセンス契約を読み、チェックボックスをオンにして、「 * 同意して続行 * 」を選択します。

選択したバージョンのダウンロードページが表示されます。

4. ソフトウェアバージョンまたはホットフィックスに含まれる変更点について説明します。
    - 新しいソフトウェア・バージョンについては、 StorageGRID のアップグレード手順の「新機能」を参照してください。
    - ホットフィックスの場合は、 README ファイルをダウンロードして、ホットフィックスに含まれている変更の概要を確認します。
5. ソフトウェアの更新が必要と判断した場合は、続行する前にその手順を確認してください。
    - 新しいソフトウェアバージョンについては、 StorageGRID のアップグレード手順に慎重に従ってください。
    - ホットフィックスの場合は、リカバリとメンテナンスの手順にあるホットフィックス手順 を探します
        - 関連情報 *

"ソフトウェアをアップグレードする"

""

## アラートとアラームの管理

StorageGRID アラートシステムは、注意が必要な運用上の問題について通知するように設計されています。必要に応じて、従来のアラームシステムを使用してシステムを監視することもできます。ここでは、次のサブセクションについて説明します。

- "アラートとアラームの比較"
- "アラートの管理"
- "アラームの管理（従来のシステム）"

StorageGRID には、問題について通知するための2つのシステムが含まれています。

アラートシステム

アラートシステムは、 StorageGRID システムで発生する可能性のある問題を監視する主要なツールです。アラートシステムは、問題を検出、評価、解決するための使いやすいインターフェイスを提供します。

アラートルールの条件が true と評価されると、特定の重大度レベルでアラートがトリガーされます。アラートがトリガーされると、次の処理が行われます。

- アラートの重大度アイコンはグリッドマネージャのダッシュボードに表示され、現在のアラートの数が増えます。
- このアラートはノード*>*_node_name >* Overview *タブに表示されます。
- SMTP サーバを設定し、受信者に E メールアドレスを提供している場合は、 E メール通知が送信されます。
- StorageGRID SNMP エージェントが設定されている場合は、簡易ネットワーク管理プロトコル（ SNMP ）通知が送信されます。

レガシーアラームシステム

アラームシステムはサポートされていますが、従来型システムとみなされます。アラートと同様に、属性が定

義されたしきい値に達すると、特定の重大度レベルでアラームがトリガーされます。ただし、アラートとは異なり、無視しても問題なくアラートがトリガーされるアラームが多数あるため、 E メールや SNMP 通知が大量に送信されることがあります。

アラームがトリガーされると、次の処理が行われます。

- ダッシュボードに表示されていた古いアラームの数が増えます。
- このアラームは、[**Support**>*Alarms (legac)*>*Current Alarms]ページに表示されます。
- SMTP サーバを設定して 1 つ以上のメーリングリストを設定している場合は、 E メール通知が送信されます。
- StorageGRID SNMP エージェントを設定している場合は、 SNMP 通知が送信されることがあります。（ SNMP 通知は、すべてのアラームまたはアラームの重大度について送信されるわけではありません）。

アラートとアラームの比較

## アラートシステムと従来のアラームシステムにはいくつかの類似点がありますが、アラートシステムには大きなメリットがあり、使いやすくなっています。

同様の処理を実行する方法については、次の表を参照してください。

| | アラート | アラーム（レガシーシステム） |
|---|---|---|
| アクティブなアラートまたはアラームを確認するにはどうすればよいですか？ | • ダッシュボードの* Current alerts *リンクをクリックします。<br>• ノード*>*概要*ページで警告をクリックします。<br>• [* Alerts*>*current*]を選択します。<br><br>"現在のアラートの表示" | • ダッシュボードの*レガシーアラーム*リンクをクリックします。<br>• [**Support**>]>[* Alarms (legac)**>]>[** Current Alarms]を選択します。<br><br>"古いアラームの表示" |
| アラートまたはアラートがトリガーされる原因 | アラートは、アラートルールの Prometheus 式で特定のトリガー条件と期間について true と評価されたときにトリガーされます。<br><br>"アラートルールを表示しています" | StorageGRID 属性がしきい値に達すると、アラームがトリガーされます。<br><br>"アラームトリガーロジック（レガシーシステム）" |
| アラートまたはアラームがトリガーされた場合、原因となっている問題をどのように解決すればよいですか？ | アラートの推奨される対処方法は E メール通知に含まれており、 Grid Manager のアラートページから確認できます。<br><br>追加情報 は、必要に応じて StorageGRID のドキュメントに記載されています。<br><br>"アラート一覧" | アラームの詳細については、属性名をクリックするか、StorageGRID のドキュメントでアラームコードを検索して確認できます。<br><br>"アラーム一覧（従来のシステム）" |

| | アラート | アラーム（レガシーシステム） |
|---|---|---|
| アラートまたはアラームのリストはどこで確認できますか？ | • ダッシュボードの最近解決したアラート*リンクをクリックします。<br>• [* Alerts*>]>[* Resolved *]を選択します。<br><br>"解決済みのアラートの表示" | [**Support**>]>[* Alarms (legac)**>]>[** Historical Alarms]を選択します。<br><br>"アラーム履歴とアラーム頻度の確認（従来のシステム）" |
| 設定を管理する場所 | [Alerts（アラート）]を選択します。次に、[Alerts]メニューのオプションを使用します。<br><br>"アラートの管理" | [ サポート ] を選択します。次に、メニューの * Alarms （レガシー）* セクションのオプションを使用します。<br><br>"アラームの管理（従来のシステム）" |
| どのようなユーザグループ権限が必要ですか？ | • Grid Manager にサインインできるユーザは、現在のアラートと解決済みのアラートを表示できます。<br>• サイレンス、アラート通知、およびアラートルールを管理するには、 Manage Alerts 権限が必要です。<br><br>"StorageGRID の管理" | • Grid Manager にサインインできるすべてのユーザがレガシーアラームを表示できます。<br>• アラームを確認するには、 Acknowledge Alarms 権限が必要です。<br>• グローバルなアラームと E メール通知を管理するには、 Grid Topology Page Configuration 権限と Other Grid Configuration 権限の両方が必要です。<br><br>"StorageGRID の管理" |
| 電子メール通知の管理方法を教えてください。 | [* Alerts*>*Email Setup*]を選択します。<br><br>• 注：* アラームとアラートは独立したシステムなので、アラームと AutoSupport 通知に使用されるメール設定は、アラート通知には使用されません。ただし、すべての通知に同じメールサーバを使用できます。<br><br>"アラート通知の管理" | [**Support**>]>[* Alarms (legacy]**>[** Legacy Email Setup*]を選択します。 "アラームの通知の設定（従来のシステム）" |

| | アラート | アラーム（レガシーシステム） |
|---|---|---|
| SNMP 通知の管理方法を教えてください。 | • Configuration > Monitoring > SNMP Agent *を選択します。 "SNMPによる監視を使用する" | • Configuration > Monitoring > SNMP Agent *を選択します。 "SNMPによる監視を使用する"<br>• 注 * ： SNMP 通知は、すべてのアラームまたはアラーム重大度について送信されるわけではありません。<br>"SNMP 通知を生成するアラーム（従来のシステム）" |
| 通知の受信者を制御するにはどうすればよいですか？ | 1. [* Alerts*>*Email Setup*]を選択します。<br>2. [ 受信者 * ] セクションで、電子メールリストごと、またはアラート発生時に電子メールを受信する必要があるユーザーごとに電子メールアドレスを入力します。<br>"アラート用のEメール通知の設定" | 1. [**Support**>]>[* Alarms (legacy)**>[** Legacy Email Setup*]を選択します。<br>2. メーリングリストを作成しています。<br>3. [*Notifications] を選択します。<br>4. メーリングリストを選択します。<br>"アラーム通知のメーリングリストの作成（従来のシステム）"<br>"アラームのEメール通知の設定（従来のシステム）" |
| 通知を送信する管理ノードはどれですか？ | 1 つの管理ノード（「優先送信者」）。<br>"StorageGRID の管理" | 1 つの管理ノード（「優先送信者」）。<br>"StorageGRID の管理" |

| | アラート | アラーム（レガシーシステム） |
|---|---|---|
| 一部の通知を停止する方法を教えてください。 | 1. [アラート>]>[サイレンス]を選択します。<br>2. サイレント化するアラートルールを選択します。<br>3. サイレンスの期間を指定します。<br>4. サイレント化するアラートの重大度を選択します。<br>5. を選択して、グリッド全体、単一サイト、または単一ノードにサイレンスを適用します。<br>◦ 注： SNMP エージェントを有効にした場合、サイレンスは SNMP トラップおよびインフォームも抑制します。<br>"アラート通知のサイレント化" | 1. [**Support**>]>[* Alarms (legacy)**>[** Legacy Email Setup*]を選択します。<br>2. [*Notifications] を選択します。<br>3. メーリングリストを選択し、 * 抑制 * を選択します。<br>"メーリングリストでのアラーム通知の停止（従来のシステム）" |
| すべての通知を停止するにはどうすればよいですか？ | [アラート>*サイレンス*]を選択します。次に、[すべてのルール]を選択します。<br>• 注： SNMP エージェントを有効にした場合、サイレンスは SNMP トラップおよびインフォームも抑制します。<br>"アラート通知のサイレント化" | 1. * Configuration **>** System Settings **>** Display Options *を選択します。<br>2. [* 通知 - すべてを抑制 * ] チェックボックスをオンにします。<br>◦ 注：システム全体で E メール通知を無効にすることで、イベントトリガー型 AutoSupport E メールも抑制されます。<br>"システム全体でのEメール通知の停止" |
| 条件とトリガーをカスタマイズする方法を教えてください。 | 1. [アラート>]>[アラートルール]を選択します。<br>2. 編集するデフォルトルールを選択するか、 * カスタムルールの作成 * を選択します。<br>"アラートルールを編集する"<br>"カスタムのアラートルールを作成する" | 1. [**Support**>]>[* Alarms (legac)**>]>[** Global Alarms]を選択します。<br>2. グローバルカスタムアラームを作成して、デフォルトアラームを上書きしたり、デフォルトアラームのない属性を監視したりします。<br>"グローバルカスタムアラームの作成（従来のシステム）" |

| | アラート | アラーム（レガシーシステム） |
|---|---|---|
| 個々のアラートまたはアラームを無効にする方法を教えてください。 | 1. [アラート>]>[アラートルール]を選択します。<br>2. ルールを選択し、*ルールの編集*をクリックします。<br>3. [ 有効 *] チェックボックスの選択を解除します。<br><br>"アラートルールを無効にします" | 1. [**Support**>]>[* Alarms (legac)**>]>[** Global Alarms]を選択します。<br>2. ルールを選択し、[編集]アイコンをクリックします。<br>3. [ 有効 *] チェックボックスの選択を解除します。<br><br>"デフォルトアラームの無効化（レガシーシステム）"<br><br>"グローバルカスタムアラームの無効化（従来のシステム）" |

アラートの管理

## アラートを使用すると、 StorageGRID システム内のさまざまなイベントや状態を監視できます。アラートの管理では、カスタムアラートの作成、デフォルトアラートの編集または無効化、アラート用の E メール通知の設定、アラート通知のサイレント化を行うことができます。

関連情報

"現在のアラートの表示"

"解決済みのアラートの表示"

"特定のアラートの表示"

"アラート一覧"

アラートとは

アラートシステムでは、 StorageGRID の運用中に発生する問題を、使いやすいインターフェイスを通じて検出し、評価し、解決することができます。

- アラートシステムは、システムで実行可能な問題に焦点を当てます。従来のシステムのアラームとは異なり、無視しても安全なイベントではアラートはトリガーされず、すぐに対処が必要なイベントに対してトリガーされます。
- Current Alerts （現在のアラート）ページには、現在の問題を表示するための使いやすいインターフェイスが用意されています。リストは、個々のアラートやアラートグループでソートできます。たとえば、すべてのアラートをノード / サイトでソートして、特定のノードに影響しているアラートを確認できます。または、グループ内のアラートを時間でソートして、特定のアラートの最新のインスタンスを確認することもできます。
- 解決済みアラートページには、現在のアラートページと同様の情報が表示されますが、アラートがトリガーされた日時や解決された日時など、解決済みのアラートの履歴を検索して表示することができます。
- 同じ種類の複数のアラートが 1 つの E メールにグループ化され、通知の数が削減されます。また、同じタ

イプの複数のアラートが [Alerts] ページにグループとして表示されます。アラートグループを展開または縮小すると、個々のアラートの表示と非表示を切り替えることができます。たとえば、複数のノードから「 Unable to communicate with node * 」アラートがほぼ同時に報告された場合、送信される E メールは 1 通だけで、アラートは Alerts ページのグループとして表示されます。

- アラートには、問題をすばやく把握できるように、わかりやすい名前と説明が使用されています。アラート通知には、影響を受けるノードとサイトに関する詳細、アラートの重大度、アラートルールがトリガーされた時刻、およびアラートに関連する指標の現在の値が含まれます。
- アラート E メール通知および現在のアラートおよび解決済みアラートのページに表示されるアラートリストは、アラートを解決するための推奨される対処方法を提供します。これらの対処方法には、StorageGRID ドキュメントセンターへの直接リンクが含まれていることが多く、より詳細なトラブルシューティング手順を見つけてアクセスしやすくなっています。
- 1 つ以上の重大度のアラートの通知を一時的に停止する必要がある場合は、特定のアラートルールを簡単に一定期間、およびグリッド全体、単一サイト、または単一ノードでサイレント化することができます。また、ソフトウェアアップグレードなどの計画的なメンテナンス手順 の実行中など、すべてのアラートルールをサイレント化することもできます。
- 必要に応じてデフォルトのアラートルールを編集できます。アラートルールは完全に無効にすることも、トリガー条件と期間を変更することもできます。
- 環境に応じた特定の条件を対象にカスタムのアラートルールを作成して、独自の対処方法を提供できます。カスタムアラートの条件を定義するには、グリッド管理 API の指標セクションで使用できる Prometheus 指標を使用して式を作成します。

アラートルールの管理

アラートルールは、特定のアラートをトリガーする条件を定義します。StorageGRID には一連のデフォルトアラートルールが用意されており、そのまま使用したり変更したりすることができます。また、カスタムのアラートルールを作成することもできます。

## アラートルールを表示しています

デフォルトとカスタムのアラートルールをすべて表示して、各アラートをトリガーする条件を確認したり、アラートが無効になっているかどうかを確認したりできます。

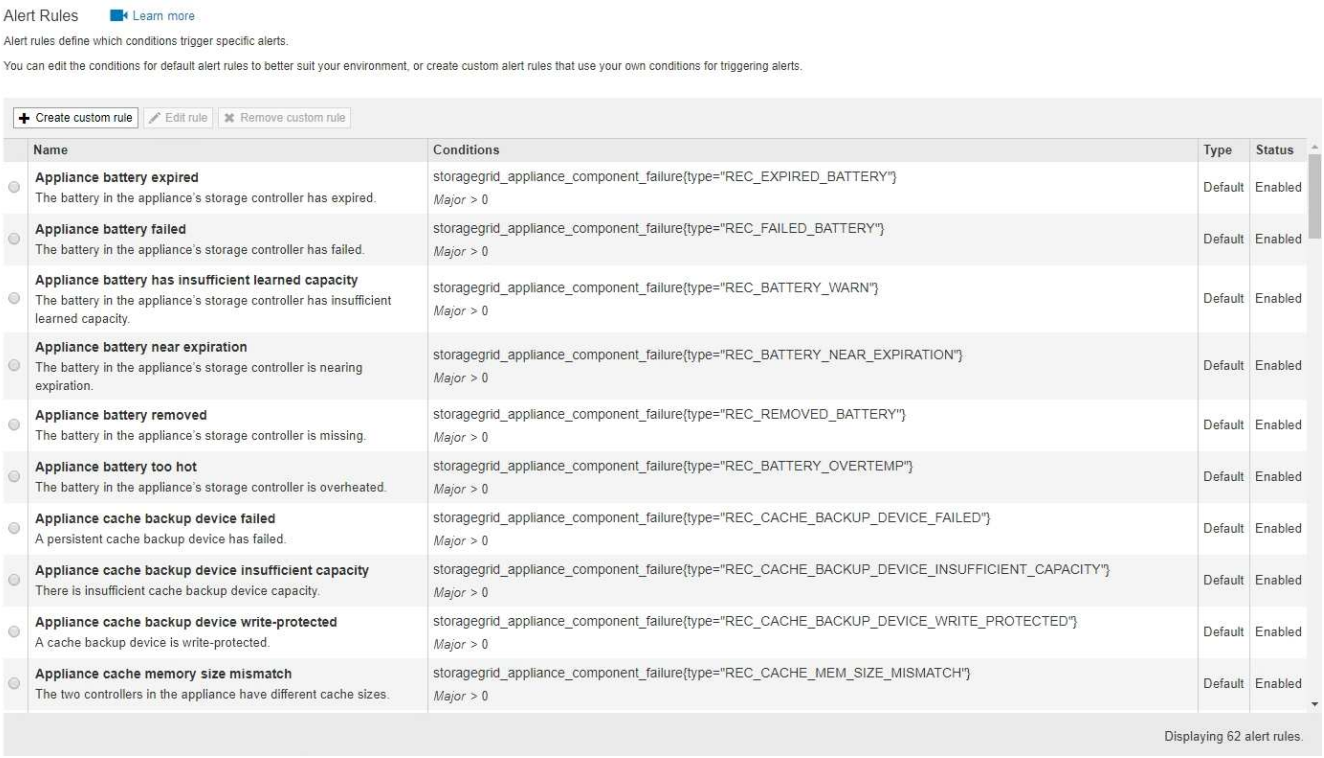
### 必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Manage AlertsまたはRoot Access権限が必要です。

### 手順

1. [アラート>]>[アラートルール]を選択します。

   [Alert Rules] ページが表示されます。




2. アラートルールのテーブルの情報を確認します。

| 列ヘッダー | 説明 |
| --- | --- |
| 名前 | アラートルールの一意の名前と概要 。カスタムのアラートルールが最初に表示され、そのあとにデフォルトのアラートルールが表示されます。アラートルール名は E メール通知の件名となります。 |

| 列ヘッダー | 説明 |
| --- | --- |
| 条件： | このアラートがトリガーされるタイミングを決定する Prometheus 式。アラートは次の 1 つ以上の重大度レベルでトリガーできますが、重大度ごとの条件は不要です。<br><br>• * 重要 * ：異常な状態で、 StorageGRID のノードやサービスの通常の動作が停止しています。基盤となる問題 にすぐに対処する必要があります。問題 が解決されないと、サービスの停止やデータの損失を招くおそれがあります。<br>• * メジャー * ：異常な状態で、現在の処理に影響しているか、重大アラートのしきい値に近づいています。Major アラートを調査し、根本的な問題に対処して、異常な状態が発生した場合に StorageGRID のノードやサービスが正常に動作しなくなる事態を防ぐ必要があります。<br>• * マイナー * ：システムは正常に動作していますが、継続するとシステムの動作に影響する可能性がある異常な状態が発生しています。自動的にクリアされない Minor アラートを監視し、解決して、深刻な問題が生じないようにする必要があります。 |
| を入力します | アラートルールのタイプ。<br><br>• * デフォルト * ：システムに付属のアラートルール。デフォルトのアラートルールは、無効にするか、条件と期間を編集できます。デフォルトのアラートルールは削除できません。<br>• * デフォルト ** ：条件または期間が編集されたデフォルトのアラートルール。必要に応じて、変更した条件を元のデフォルトに戻すことができます。<br>• * Custom * ：ユーザが作成したアラートルール。カスタムのアラートルールは、無効化、編集、削除することができます。 |
| ステータス | このアラートルールが現在有効になっているか無効になっているか。アラートルールが無効になっている場合は、条件が評価されないため、アラートはトリガーされません。 |

関連情報

"アラート一覧"

## カスタムのアラートルールを作成する

カスタムのアラートルールを作成して、アラートをトリガーする条件を独自に定義することができます。

### 必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Manage AlertsまたはRoot Access権限が必要です。

### このタスクについて

StorageGRID はカスタムアラートを検証しません。カスタムのアラートルールを作成する場合は、次の一般的なガイドラインに従ってください。

- デフォルトのアラートルールの条件を参考に、カスタムのアラートルールを作成します。
- アラートルールに複数の条件を定義する場合は、すべての条件に同じ式を使用します。その後、各条件のしきい値を変更します。
- 各条件に入力ミスやロジックエラーがないか、慎重にチェックしてください。
- Grid 管理 API にリストされている指標のみを使用してください。
- Grid Management API を使用して式をテストする場合、「 Successful 」応答は単に空の応答本文になる場合があります（アラートはトリガーされません）。アラートが実際にトリガーされるかどうかを確認するには、現在 true になるしきい値を一時的に設定します。

  たとえば、式をテストする場合などです `node_memory_MemTotal_bytes < 24000000000`を実行します `node_memory_MemTotal_bytes >= 0` また、想定される結果を確認します（すべてのノードが値を返します）。次に、演算子としきい値を目的の値に戻して再実行します。結果がない場合は、この式に対するアラートが現在発生していません。

- 想定どおりにトリガーされることを確認するまでは、カスタムアラートが機能していると判断しないでください。

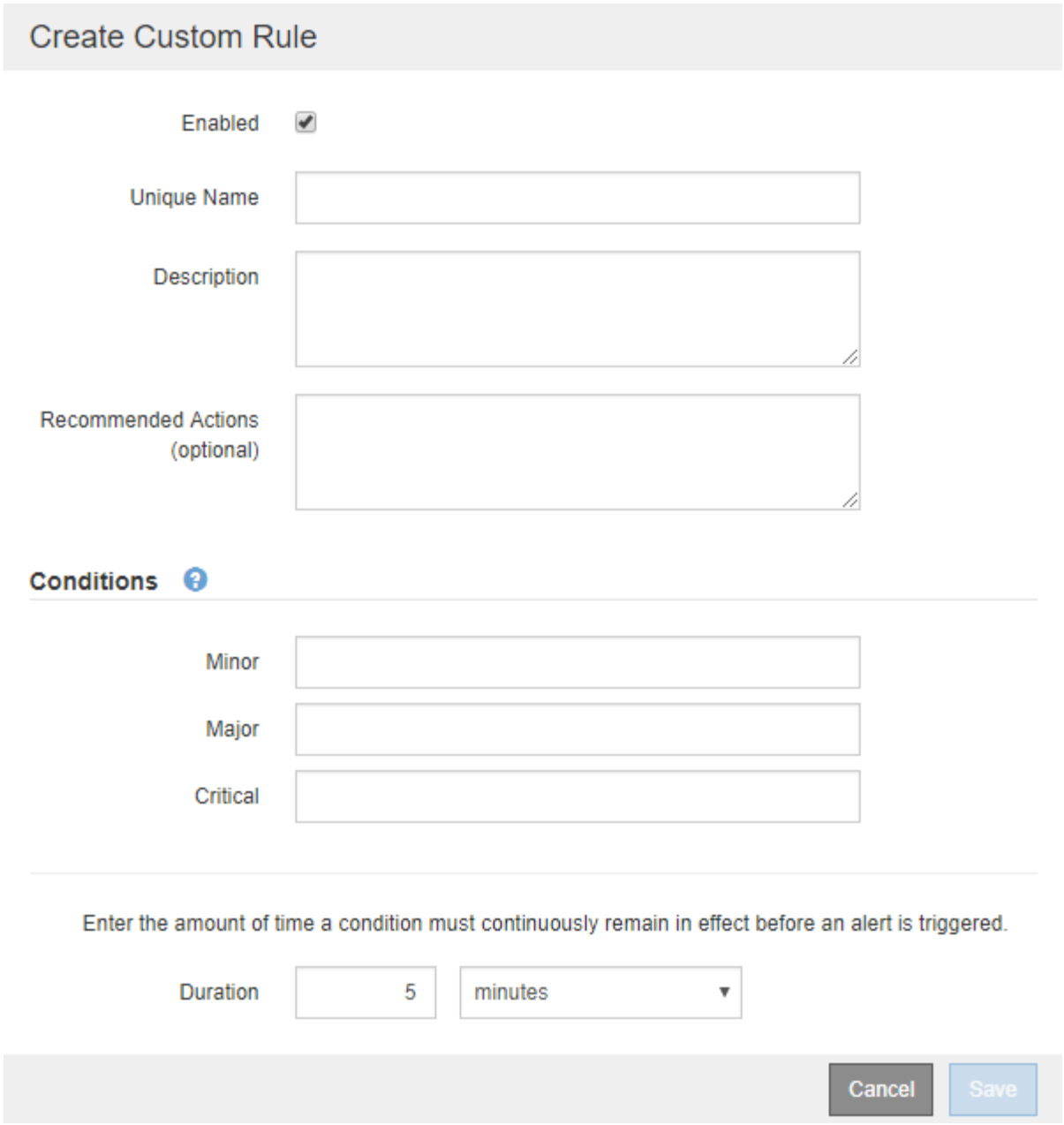
### 手順

1. [アラート>]>[アラートルール]を選択します。

   [Alert Rules] ページが表示されます。

2. [ * カスタムルールの作成 * ] を選択します。

   [Create Custom Rule] ダイアログボックスが表示されます。




3. このアラートルールが現在有効になっているかどうかを確認するには、 [ 有効 *] チェックボックスをオンまたはオフにします。

   アラートルールを無効にすると、ルールの式は評価されず、アラートはトリガーされません。

4. 次の情報を入力します。

| フィールド | 説明 |
| --- | --- |
| 一意の名前 | このルールの一意の名前。アラートルール名は、[Alerts] ページに表示され、電子メール通知の件名にもなります。アラートルールの名前は 1~64 文字で指定できます。 |

| フィールド | 説明 |
| --- | --- |
| 説明 | 発生している問題の概要 。概要 は、アラートページおよび E メール通知に表示されるアラートメッセージです。アラートルールの説明は、 1~128 文字で指定できます。 |
| 推奨される対処方法 | 必要に応じて、このアラートがトリガーされたときに実行する推奨される対処方法を指定します。推奨される対処方法をプレーンテキスト（書式コードなし）で入力します。アラートルールの推奨される対処方法は、 0~1 、 024 文字で指定できます。 |

5. Conditions セクションで、アラートの重大度レベルを 1 つ以上指定する Prometheus 式を入力します。

   基本式は、通常、次の形式で指定します。

   ```
   [metric] [operator] [value]
   ```

   式の文字数に制限はありませんが、ユーザインターフェイスでは 1 行で表示されます。少なくとも 1 つの式が必要です。

   使用可能な指標を確認したり、Prometheus式をテストしたりするには、ヘルプアイコンをクリックします グリッド管理 API のメトリクスセクションへのリンクをクリックします。

   グリッド管理APIの使用方法については、StorageGRID の管理手順を参照してください。Prometheusクエリの構文の詳細については、Prometheusのドキュメントを参照してください。

   次の式では、あるノードに搭載された RAM の容量が 24 、 000 、 000 、 000 バイト（ 24GB ）未満である場合にアラートがトリガーされます。

   ```
   node_memory_MemTotal_bytes < 24000000000
   ```

6. [ * 期間 * ] フィールドに、アラートがトリガーされるまでに条件を継続的に有効にしておく必要がある期間を入力し、時間の単位を選択します。

   条件が true になったときにすぐにアラートをトリガーするには、「 * 0 * 」と入力します。一時的な状況でアラートがトリガーされないようにするには、この値を大きくし

   デフォルトは 5 分です。

7. [ 保存（ Save ） ] をクリックします。

   ダイアログボックスが閉じ、新しいカスタムアラートルールがアラートルールテーブルに表示されます。

関連情報

"StorageGRID の管理"

"よく使用される Prometheus 指標"

"Prometheus：クエリの基本"

## アラートルールを編集する

アラートルールを編集してトリガー条件を変更したり、カスタムのアラートルールを使用してルール名、概要、および推奨される対処方法を更新したりできます。

### 必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Manage AlertsまたはRoot Access権限が必要です。

### このタスクについて

デフォルトのアラートルールを編集する場合は、 Minor 、 Major 、 Critical の各アラートの条件と期間を変更できます。カスタムのアラートルールを編集する際に、ルールの名前、概要 、および推奨される対処方法を編集することもできます。

> アラートルールを編集する場合は注意が必要です。トリガー値を変更した場合、重大な処理を完了できなくなるまで、根本的な問題が検出されないことがあります。

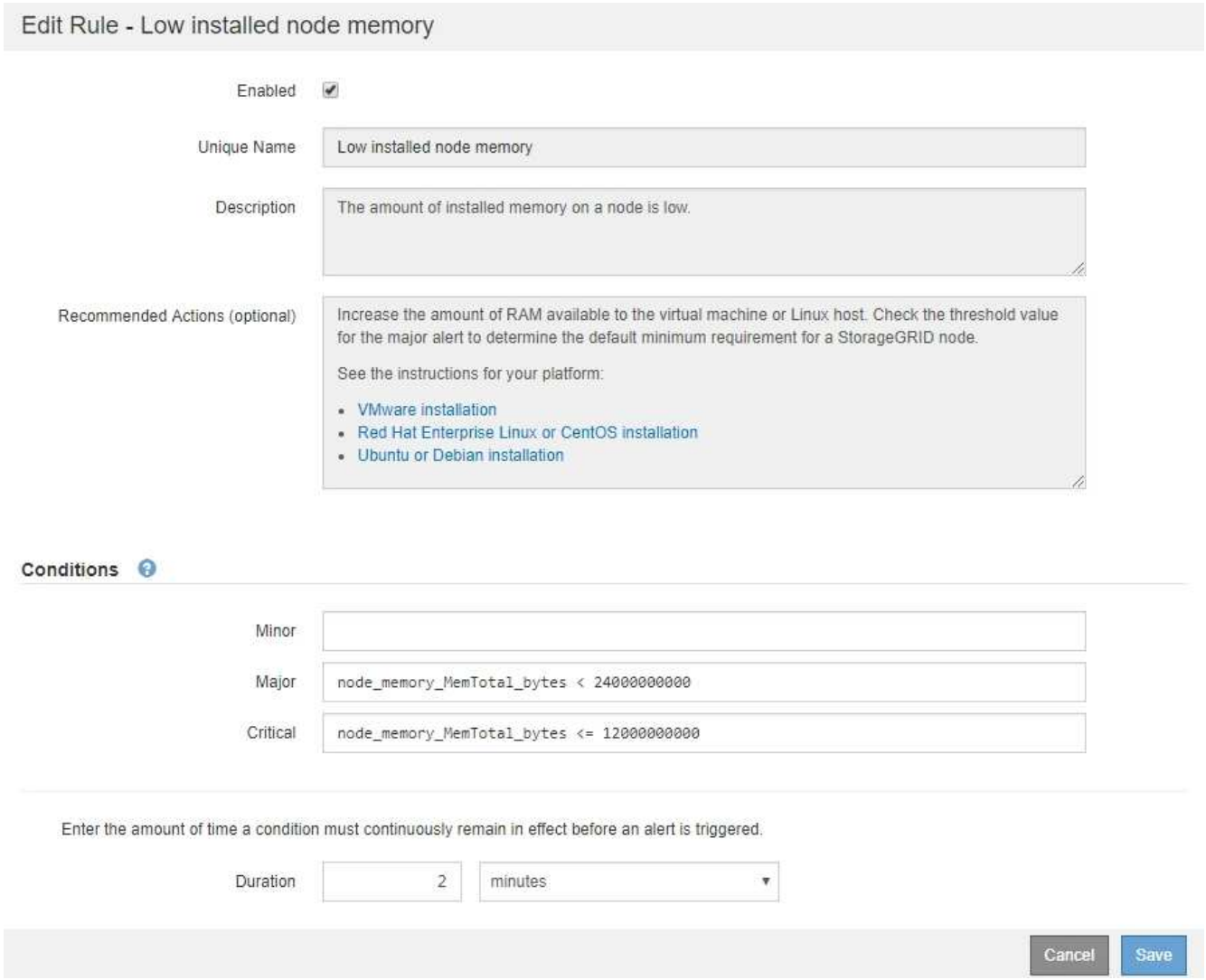
### 手順

1. [アラート>]>[アラートルール]を選択します。

   [Alert Rules] ページが表示されます。

2. 編集するアラートルールのラジオボタンを選択します。
3. [ * ルールの編集 * ] を選択します。

   Edit Rule ダイアログボックスが表示されます。この例はデフォルトのアラートルールを示しています。一意の名前、概要 、および推奨されるアクションフィールドは無効になっており、編集することはできません。




4. このアラートルールが現在有効になっているかどうかを確認するには、 [ 有効 *] チェックボックスをオンまたはオフにします。

   アラートルールを無効にすると、ルールの式は評価されず、アラートはトリガーされません。

   現在のアラートのアラートルールを無効にした場合は、アラートがアクティブなアラートとして表示されなくなるまで数分待つ必要があります。

   通常は、デフォルトのアラートルールを無効にすることは推奨されません。アラートルールが無効になっている場合は、重大な処理を完了できなくなるまで、根本的な問題が検出されない可能性があります。

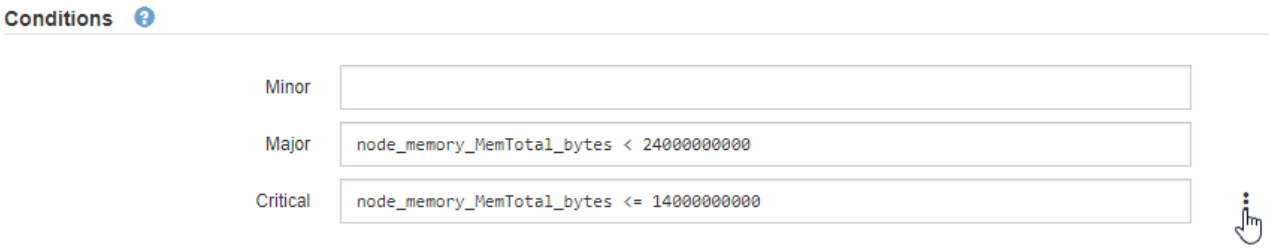
5. カスタムのアラートルールの場合は、次の情報を必要に応じて更新します。

   この情報はデフォルトのアラートルールでは編集できません。

| フィールド | 説明 |
| --- | --- |
| 一意の名前 | このルールの一意の名前。アラートルール名は、[Alerts] ページに表示され、電子メール通知の件名にもなります。アラートルールの名前は 1~64 文字で指定できます。 |
| 説明 | 発生している問題の概要 。概要 は、アラートページおよび E メール通知に表示されるアラートメッセージです。アラートルールの説明は、 1~128 文字で指定できます。 |
| 推奨される対処方法 | 必要に応じて、このアラートがトリガーされたときに実行する推奨される対処方法を指定します。推奨される対処方法をプレーンテキスト（書式コードなし）で入力します。アラートルールの推奨される対処方法は、 0~1 、 024 文字で指定できます。 |

6. Conditions セクションで、 1 つ以上のアラート重大度レベルの Prometheus 式を入力または更新します。

編集したデフォルトのアラートルールの条件を元の値に戻すには、変更した条件の右側にある3つの点をクリックします。




現在のアラートの条件を更新した場合は、更新前の条件が解決されるまで変更が適用されないことがあります。ルールのいずれかの条件が次回満たされた時点で、更新された値がアラートに反映されます。

基本式は、通常、次の形式で指定します。

```
[metric] [operator] [value]
```

式の文字数に制限はありませんが、ユーザインターフェイスでは 1 行で表示されます。少なくとも 1 つの式が必要です。

使用可能な指標を確認したり、Prometheus式をテストしたりするには、ヘルプアイコンをクリックします グリッド管理 API のメトリクスセクションへのリンクをクリックします。

グリッド管理APIの使用方法については、StorageGRID の管理手順を参照してください。Prometheusクエリの構文の詳細については、Prometheusのドキュメントを参照してください。

次の式では、あるノードに搭載された RAM の容量が 24 、 000 、 000 、 000 バイト（ 24GB ）未満である場合にアラートがトリガーされます。

```
node_memory_MemTotal_bytes < 24000000000
```

7. [* Duration * （時間 * ） ] フィールドに、アラートがトリガーされるまでに条件が継続的に有効である必要がある時間を入力し、時間の単位を選択します。

   条件が true になったときにすぐにアラートをトリガーするには、「 * 0 * 」と入力します。一時的な状況でアラートがトリガーされないようにするには、この値を大きくし

   デフォルトは 5 分です。

8. [ 保存（ Save ） ] をクリックします。

   デフォルトのアラート・ルールを編集した場合は ' ［ タイプ ］ カラムに **Default*** と表示されますデフォルトまたはカスタムのアラートルールを無効にした場合は、 * Status * 列に * Disabled * と表示されます。

関連情報

"StorageGRID の管理"

"よく使用される Prometheus 指標"

"Prometheus：クエリの基本"

アラートルールを無効にします

デフォルトまたはカスタムのアラートルールの有効 / 無効の状態を変更できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Manage AlertsまたはRoot Access権限が必要です。

このタスクについて

アラートルールを無効にすると、ルールの式は評価されず、アラートはトリガーされません。

> 通常は、デフォルトのアラートルールを無効にすることは推奨されません。アラートルールが無効になっている場合は、重大な処理を完了できなくなるまで、根本的な問題が検出されない可能性があります。

手順

1. [アラート>]>[アラートルール]を選択します。

   [Alert Rules] ページが表示されます。

2. 無効または有効にするアラートルールのラジオボタンを選択します。
3. [ * ルールの編集 * ] を選択します。

Edit Rule ダイアログボックスが表示されます。

4. このアラートルールが現在有効になっているかどうかを確認するには、 [ 有効 *] チェックボックスをオンまたはオフにします。

   アラートルールを無効にすると、ルールの式は評価されず、アラートはトリガーされません。

   > 現在のアラートのアラートルールを無効にした場合は、アラートがアクティブなアラートとして表示されなくなるまで数分待つ必要があります。

5. [ 保存（ Save ） ] をクリックします。
   - 無効 * は、 * ステータス * 列に表示されます。

カスタムのアラートルールを削除する

不要となったカスタムのアラートルールは削除できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Manage AlertsまたはRoot Access権限が必要です。

手順

1. [アラート>]>[アラートルール]を選択します。

   [Alert Rules] ページが表示されます。

2. 削除するカスタムのアラートルールのラジオボタンを選択します。

   デフォルトのアラートルールは削除できません。

3. [カスタムルールの削除]をクリックします。

   確認のダイアログボックスが表示されます。

4. [OK]をクリックして、アラートルールを削除します。

   アラートのアクティブなインスタンスがあった場合、 10 分以内に解決されます。

アラート通知の管理

アラートがトリガーされると、StorageGRID からEメール通知および簡易ネットワーク管理プロトコル（SNMP）通知（トラップ）を送信できます。

アラートの**SNMP**通知の設定

アラート発生時に StorageGRID から SNMP 通知を送信するには、 StorageGRID SNMP エージェントを有効にし、 1 つ以上のトラップ送信先を設定する必要があります。

このタスクについて

Grid ManagerまたはグリッドAPIのSNMPエンドポイントで* Configuration > Monitoring > SNMP Agent *オプションを使用して、StorageGRID SNMPエージェントを有効にして設定できます。SNMP エージェントは、 3 つのバージョンの SNMP プロトコルをすべてサポートします。

SNMPエージェントの設定方法については、SNMPモニタリングの使用に関するセクションを参照してください。

StorageGRID SNMP エージェントの設定後に、次の 2 種類のイベントベースの通知を送信できます。

- トラップは、 SNMP エージェントから送信される通知であり、管理システムによる確認応答は必要ありません。トラップは、アラートがトリガーされているなど、 StorageGRID 内で何らかの問題が発生したことを管理システムに通知するために使用されます。トラップは、SNMPの3つのバージョンすべてでサポートされています
- 通知はトラップと似ていますが、管理システムによる確認応答が必要です。SNMP エージェントが一定時間内に確認応答を受信しなかった場合、確認応答を受信するか、最大再試行値に達するまで、通知を再送信します。インフォームは SNMPv2c および SNMPv3 でサポートされます。

トラップ通知およびインフォーム通知は、デフォルトまたはカスタムアラートがいずれかの重大度レベルでトリガーされたときに送信されます。アラートの SNMP 通知を停止するには、アラートのサイレンスを設定する必要があります。アラート通知は、優先送信者として設定された管理ノードから送信されます。デフォルトでは、プライマリ管理ノードが選択されます。詳細については、 StorageGRID の管理手順を参照してください。

> トラップ通知およびインフォーム通知は、指定された重大度レベル以上で特定のアラーム（レガシーシステム）がトリガーされたときにも送信されますが、 SNMP 通知はすべてのアラームまたはすべてのアラーム重大度に対して送信されるわけではありません。

関連情報

"SNMPによる監視を使用する"

"アラート通知のサイレント化"

"StorageGRID の管理"

"SNMP 通知を生成するアラーム（従来のシステム）"

アラート用のEメール通知の設定

アラート発生時に E メール通知が送信されるようにするには、 SMTP サーバに関する情報を指定する必要があります。また、アラート通知の受信者の E メールアドレスを入力する必要があります。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Manage AlertsまたはRoot Access権限が必要です。

必要なもの

アラームとアラートは別々のシステムであるため、アラート通知に使用される E メール設定は、アラーム通知と AutoSupport メッセージには使用されません。ただし、すべての通知に同じ E メールサーバを使用できます。

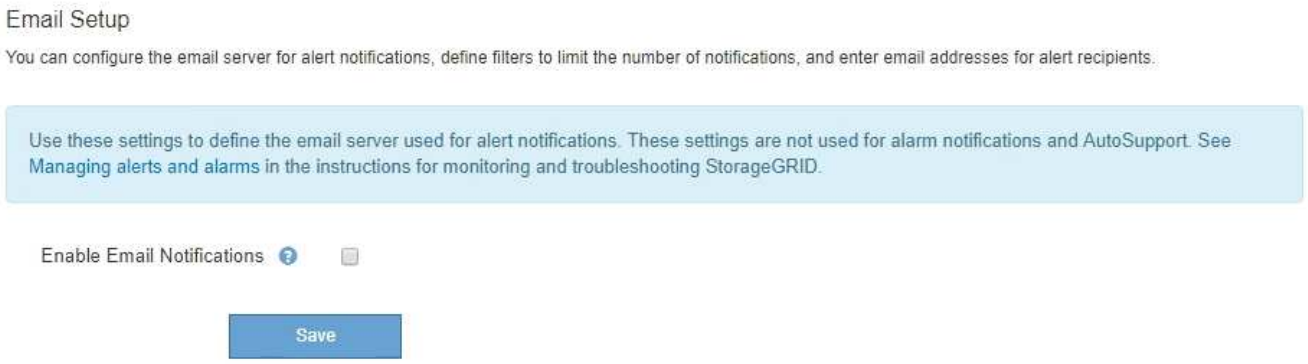
StorageGRID 環境に複数の管理ノードが含まれている場合は、アラート通知の優先送信者となる管理ノード

を選択できます。同じ「優先送信者」は、アラーム通知と AutoSupport メッセージにも使用されます。デフォルトでは、プライマリ管理ノードが選択されます。詳細については、 StorageGRID の管理手順を参照してください。

手順

1. [* Alerts*>*Email Setup*]を選択します。

   [ 電子メールの設定 ] ページが表示されます。




2. [ 電子メール通知を有効にする *] チェックボックスをオンにして、アラートが設定されたしきい値に達したときに通知電子メールを送信するように指定します。

   電子メール（ SMTP ）サーバー、 Transport Layer Security （ TLS ）、電子メールアドレス、およびフィルタセクションが表示されます。

3. 電子メール（ SMTP ）サーバーセクションで、 StorageGRID が SMTP サーバーにアクセスするために必要な情報を入力します。

   SMTP サーバで認証が必要な場合は、ユーザ名とパスワードの両方を指定する必要があります。TLSも必要で、CA証明書を指定する必要があります。

| フィールド | 入力するコマンド |
| --- | --- |
| メールサーバ | SMTP サーバの完全修飾ドメイン名（ FQDN ）または IP アドレス。 |
| ポート | SMTP サーバへのアクセスに使用するポート。1~65535 の範囲で指定する必要があります。 |
| ユーザ名（オプション） | SMTP サーバで認証が必要な場合は、認証に使用するユーザ名を入力します。 |
| パスワード（オプション） | SMTP サーバで認証が必要な場合は、で認証するためのパスワードを入力します。 |

4. [ 電子メールアドレス ] セクションで、送信者と各受信者の電子メールアドレスを入力します。

   a. * 送信者電子メールアドレス * には、アラート通知の送信元アドレスとして使用する有効な電子メールアドレスを指定します。

      例： `storagegrid-alerts@example.com`

   b. [ 受信者 ] セクションで、電子メールリストごとに電子メールアドレスを入力するか、アラートが発生したときに電子メールを受信する必要があるユーザーを入力します。

      プラスアイコンをクリックします ✚ をクリックします。

5. SMTPサーバとの通信にTransport Layer Security（TLS）が必要な場合は、Transport Layer Security（TLS）セクションで、* Require TLS *チェックボックスをオンにします。

   a. [CA 証明書 *] フィールドに、 SMTP サーバの識別に使用する CA 証明書を入力します。

      このフィールドに内容をコピーして貼り付けるか、*参照*をクリックしてファイルを選択します。

      各中間発行認証局（ CA ）の証明書を含む単一のファイルを指定する必要があります。このファイルには、 PEM でエンコードされた各 CA 証明書ファイルが、証明書チェーンの順序で連結して含まれている必要があります。

   b. SMTP 電子メールサーバーが認証用のクライアント証明書を提供するために電子メール送信者を必要とする場合は、 [ クライアント証明書の送信 *] チェックボックスをオンにします。

   c. [ * クライアント証明書 * ] フィールドに、 SMTP サーバに送信する PEM でエンコードされたクライアント証明書を入力します。

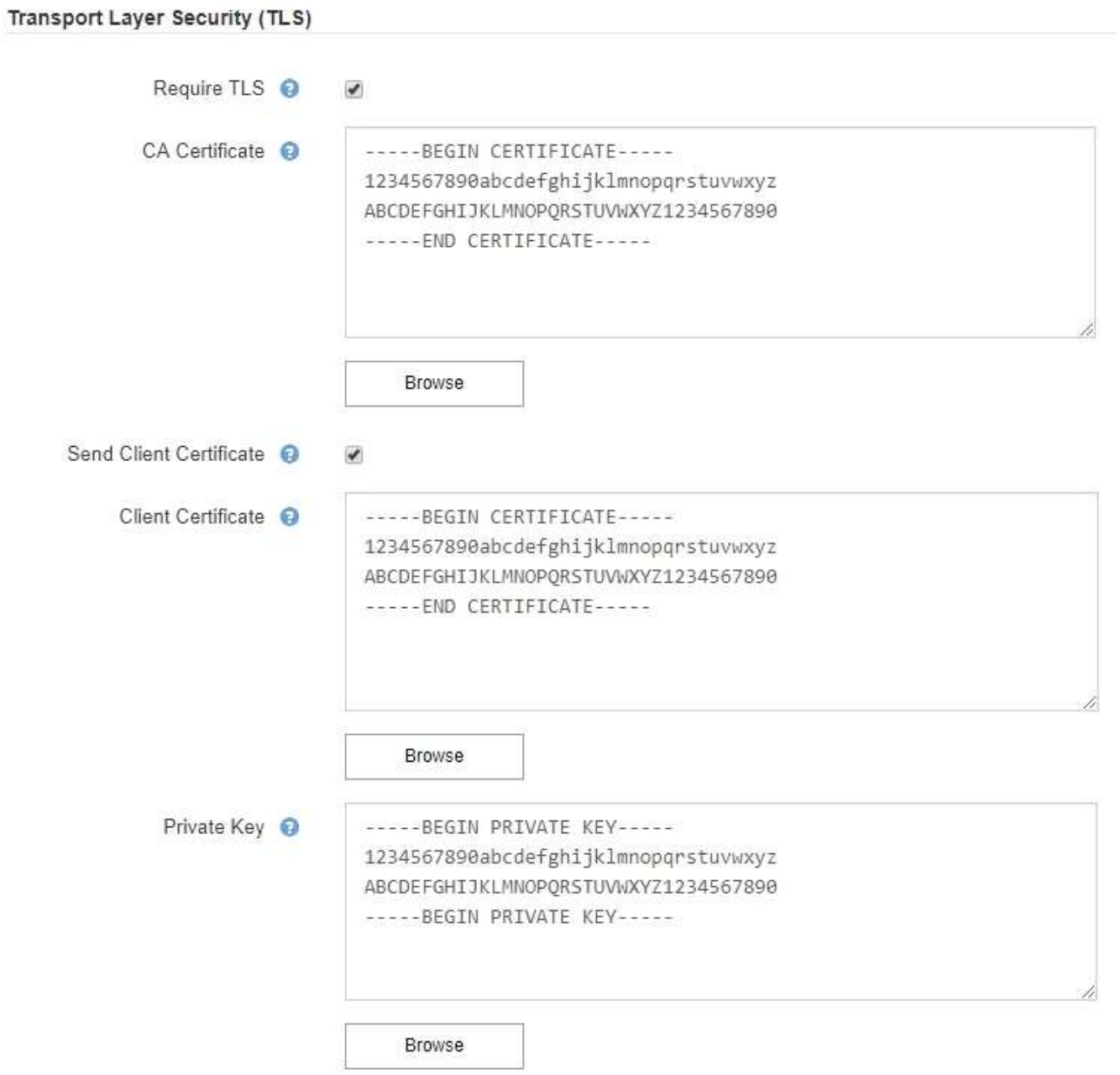
      このフィールドに内容をコピーして貼り付けるか、*参照*をクリックしてファイルを選択します。

   d. [**Private Key**] フィールドに、クライアント証明書の秘密鍵を暗号化されていない PEM エンコードで

入力します。

このフィールドに内容をコピーして貼り付けるか、*参照*をクリックしてファイルを選択します。

> Eメールのセットアップを編集する必要がある場合は、鉛筆のアイコンをクリックしてこのフィールドを更新します。




6. [ フィルタ ] セクションで、特定のアラートのルールがサイレント化されていない限り、電子メール通知を行うアラート重大度レベルを選択します。

| 重大度 | 説明 |
| --- | --- |
| マイナー、メジャー、クリティカルです | アラートルールの Minor 、 Major 、 Critical のいずれかの条件が満たされたときに、 E メール通知が送信されます。 |
| メジャー、クリティカルです | アラートルールの Major または Critical の条件が満たされたときに、 E メール通知が送信されます。Minor アラートの場合、通知は送信されません。 |
| 重大な問題のみ | アラートルールの Critical 条件が満たされたときにのみ、 E メール通知が送信されます。Minor または Major アラートの場合、通知は送信されません。 |

7. E メールの設定をテストする準備ができたら、次の手順を実行します。
   a. [テストメールの送信]をクリックします。

      テスト用 E メールが送信されたことを示す確認メッセージが表示されます。

   b. すべての E メール受信者の受信ボックスを調べて、テスト用 E メールが受信されたことを確認します。

      数分以内に電子メールが受信されない場合、または * 電子メール通知エラー * アラートがトリガーされた場合は、設定を確認してから再試行してください。

   c. 他の管理ノードにサインインし、テスト用 E メールを送信してすべてのサイトからの接続を確認します。

      アラート通知をテストするときは、すべての管理ノードにサインインして接続を確認する必要があります。これは、すべての管理ノードがテスト E メールを送信する、アラーム通知と AutoSupport メッセージをテストするのとは異なります。

8. [ 保存（ Save ） ] をクリックします。

   テスト用 E メールを送信しても設定は保存されません。[保存（Save）]をクリックする必要があります。

   E メール設定が保存されます。

関連情報

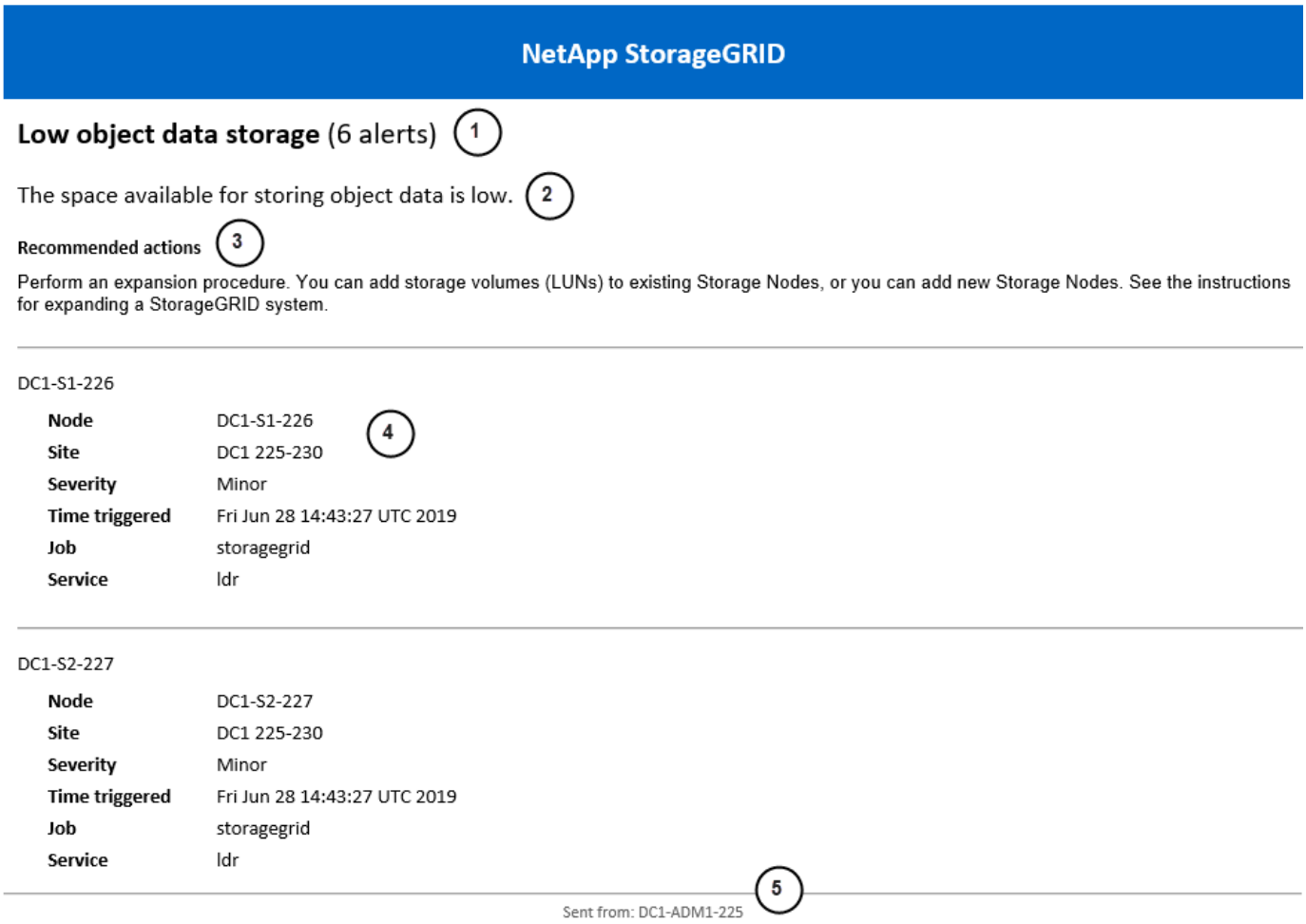
"アラートEメール通知のトラブルシューティング"

""

アラート **E** メール通知に記載される情報

SMTP E メールサーバを設定すると、アラートルールがサイレンスによって停止されていないかぎり、アラートがトリガーされたときに E メール通知が指定の受信者に送信されます。

E メール通知には次の情報が含まれます。




| | 説明 |
|---|---|
| 1. | アラートの名前と、そのアラートのアクティブなインスタンスの数。 |
| 2. | アラートの概要 。 |
| 3. | アラートの推奨される対処方法。 |
| 4. | アラートのアクティブな各インスタンスに関する詳細情報。対象となるノードとサイト、アラートの重大度、アラートルールがトリガーされた UTC 時間、影響を受けるジョブとサービスの名前などが含まれます。 |
| 5. | 通知を送信した管理ノードのホスト名。 |

関連情報

"アラート通知のサイレント化"

**StorageGRID** でのEメール通知でのアラートのグループ化

StorageGRID は、アラートがトリガーされたときに大量の E メール通知が送信されないように、複数のアラートを同じ通知にまとめます。

StorageGRID で複数のアラートを E メール通知でグループ化する例については、次の表を参照してください。

| 動作 | 例 |
| --- | --- |
| 各アラート通知は、同じ名前のアラートにのみ適用されます。名前が異なる 2 つのアラートが同時にトリガーされると、 2 つの E メール通知が送信されます。 | • アラート A は 2 つのノードで同時にトリガーされます。1 つの通知のみが送信されます。<br>• アラート A はノード 1 でトリガーされ、アラート B はノード 2 で同時にトリガーされます。2 つの通知が送信されます各アラートに 1 つずつ送信されます |
| 特定のノードの特定のアラートが複数の重大度のしきい値に達した場合は、最も重大度の高いアラートに関してのみ通知が送信されます。 | • アラート A がトリガーされ、 Minor 、 Major 、 Critical の各アラートしきい値に達した場合重大アラートに対して 1 つの通知が送信されます。 |
| あるアラートが初めてトリガーされた場合、 StorageGRID は 2 分待ってから通知を送信します。この時間内に同じ名前のアラートがほかにもトリガーされた場合、 StorageGRID はすべてのアラートを最初の通知の最初のグループにまとめます | 1. アラート A は、ノード 1 で 08 ： 00 にトリガーされます。通知は送信されません。<br>2. ノード 2 の 08 ： 01 でアラート A がトリガーされます。通知は送信されません。<br>3. 08:02 で、アラートの両方のインスタンスを報告する通知が送信されます。 |
| 同じ名前の別のアラートがトリガーされた場合、 StorageGRID は 10 分待ってから新しい通知を送信します。新しい通知では、以前に報告されたものも含めて、アクティブなアラート（サイレント化されていない現在のアラート）がすべて報告されます。 | 1. アラート A は、ノード 1 で 08 ： 00 にトリガーされます。通知が 08:02 に送信されます。<br>2. アラート A は、ノード 2 の 08 ： 05 でトリガーされます。2 回目の通知は 8 ： 15 （ 10 分後）に送信されます。両方のノードが報告されます。 |
| 同じ名前の現在のアラートが複数あり、そのうちの 1 つのアラートが解決された場合、そのアラートが解決されたノードでアラートが再度発生しても新しい通知は送信されません。 | 1. アラート A はノード 1 に対してトリガーされます。通知が送信されます。<br>2. アラート A がノード 2 に対してトリガーされます。2 回目の通知が送信されます。<br>3. アラート A はノード 2 について解決されましたが、ノード 1 に対してはアクティブなままです。<br>4. アラート A がノード 2 に対して再度トリガーされます。ノード 1 のアラートがまだアクティブなため、新しい通知は送信されません。 |

| 動作 | 例 |
| --- | --- |
| StorageGRID は、アラートのすべてのインスタンスが解決されるか、アラートルールがサイレント化されるまで、 7 日ごとに E メール通知を送信します。 | 1. 3 月 8 日にノード 1 のアラート A がトリガーされます。通知が送信されます。<br>2. アラート A が解決されていないか、サイレント化されていその他の通知は 3 月 15 日、 3 月 22 日、 3 月 29 日などに送信されます。 |

アラート**E**メール通知のトラブルシューティング

- Email notification failure * アラートがトリガーされた場合、またはテストアラート E メール通知を受信できない場合は、次の手順に従って問題 を解決します。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Manage AlertsまたはRoot Access権限が必要です。

手順

1. 設定を確認します。
   a. [* Alerts*>*Email Setup*]を選択します。
   b. E メール（ SMTP ）サーバの設定が正しいことを確認します。
   c. 受信者の有効な E メールアドレスが指定されていることを確認します。
2. スパムフィルタを確認し、 E メールが迷惑メールフォルダに送信されていないことを確認します。
3. E メール管理者に依頼して、送信者アドレスからの E メールがブロックされていないことを確認します。
4. 管理ノードのログファイルを収集し、テクニカルサポートに連絡します。

   テクニカルサポートは、ログの情報を参考に問題の原因を特定します。たとえば、指定したサーバに接続するときに、 prometheus.log ファイルにエラーが表示されることがあります。

関連情報

"ログファイルとシステムデータを収集しています"

アラート通知のサイレント化

必要に応じて、サイレンスを設定してアラート通知を一時的に停止することができます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Manage AlertsまたはRoot Access権限が必要です。

このタスクについて

アラートルールは、グリッド全体、単一サイト、または単一ノードと、 1 つ以上の重大度に対してサイレント化できます。各サイレンスは、 1 つのアラートルールまたはすべてのアラートルールのすべての通知を停止します。

SNMP エージェントを有効にすると、サイレンスは SNMP トラップおよびインフォームも抑制します。

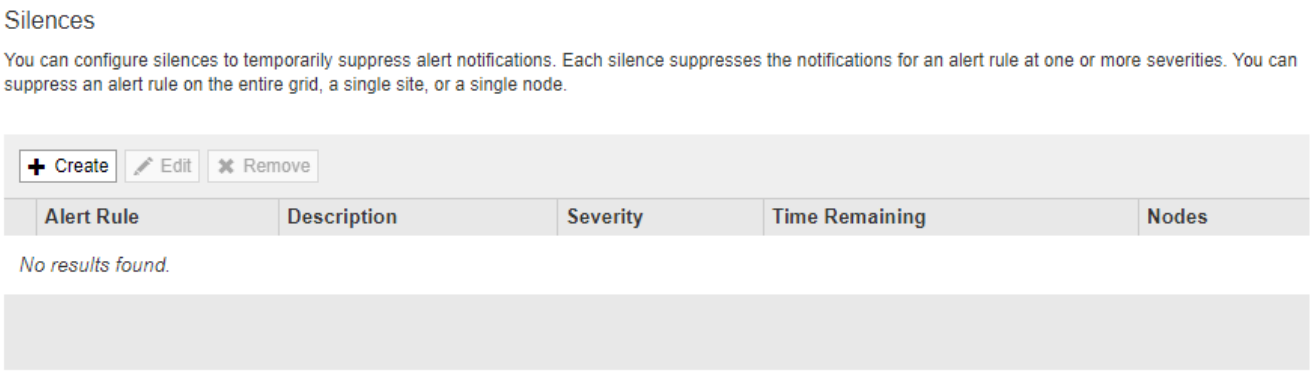
アラートルールをサイレント化する場合は注意が必要です。アラートをサイレント化すると、重大な処理を完了できなくなるまで、原因となっている問題が検出されない可能性があります。

アラームとアラートは別々のシステムであるため、この機能を使用してアラーム通知を停止することはできません。

手順

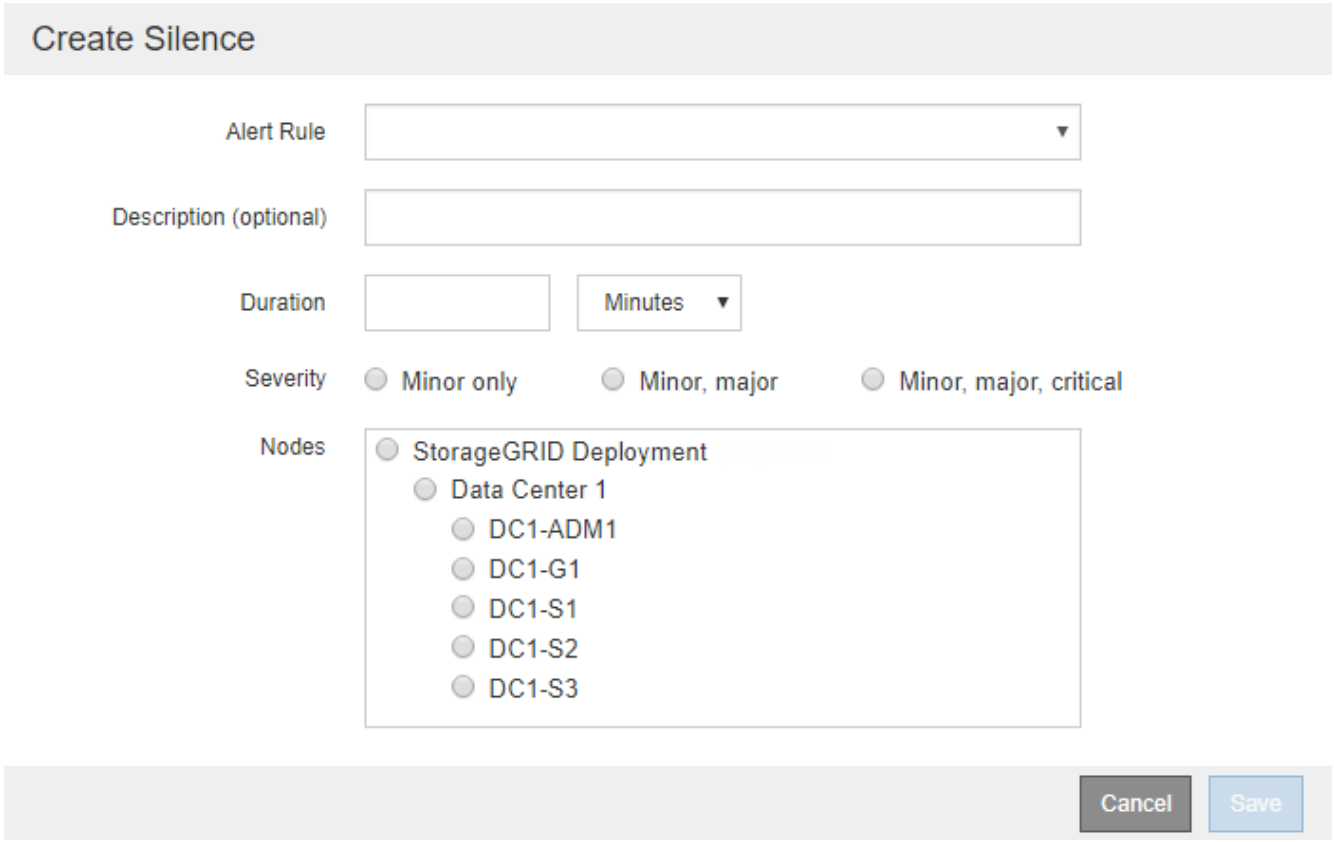
1. [アラート>]>[サイレンス]を選択します。

   [Silences] ページが表示されます。




2. 「 * Create * 」を選択します。

   [ 無音の作成 ] ダイアログボックスが表示されます。




3. 次の情報を選択または入力します。

| フィールド | 説明 |
| --- | --- |
| アラートルール | サイレント化するアラートルールの名前。アラートルールが無効になっている場合でも、任意のデフォルトまたはカスタムのアラートルールを選択できます。<br><br>• 注：このダイアログボックスで指定した条件を使用してすべてのアラートルールをサイレント化する場合は、「 * すべてのルール * 」を選択します。 |
| 説明 | 必要に応じて、サイレンスの概要 。たとえば、このサイレンスの目的を入力します。 |
| 期間 | このサイレンスを有効にしておく期間（分、時間、または日数）。サイレンスを有効にできる期間は、 5 分から 1 、 825 日（ 5 年）です。<br><br>• 注： * アラートルールを長時間サイレント化しないでください。アラートルールがサイレント化されている場合、重大な処理が完了しないかぎり、根本的な問題が検出されないことがあります。ただし、 * サービスアプライアンスリンク停止 * アラートや * ストレージアプライアンスリンク停止 * アラートなど、特定の意図的な設定によってアラートがトリガーされた場合は、拡張サイレンスを使用する必要があります。 |
| 重大度 | サイレント化するアラートの重大度。選択した重大度のいずれかでアラートがトリガーされた場合、通知は送信されません。 |

| フィールド | 説明 |
| --- | --- |
| ノード | このサイレンスを適用するノード。アラートルール、またはグリッド全体、単一サイト、または単一ノード上のすべてのルールを抑制することができます。グリッド全体を選択環境 する場合は、すべてのサイトとすべてのノードをサイレント化します。サイトを選択すると、そのサイトのノードにのみサイレンスが適用されます。<br>• 注： * 1 つのサイレンスで複数のノードまたは複数のサイトを選択することはできません。同じアラートルールを複数のノードまたは複数のサイトで一度に停止するには、追加のサイレンスを作成する必要があります。 |

4. [ 保存（ Save ） ] をクリックします。
5. 期限が切れる前に変更または終了するには、サイレンスを編集または削除できます。

| オプション | 説明 |
| --- | --- |
| サイレンスを編集する | a. [アラート>]>[サイレンス]を選択します。<br>b. テーブルで、編集するサイレンスのラジオボタンを選択します。<br>c. [ 編集（ Edit ） ] をクリックします。<br>d. 概要 、残り時間、選択した重大度、または対象となるノードを変更します。<br>e. [ 保存（ Save ） ] をクリックします。 |
| サイレンスを削除する | a. [アラート>]>[サイレンス]を選択します。<br>b. テーブルで、削除するサイレンスのラジオボタンを選択します。<br>c. [ 削除（ Remove ） ] をクリックします。<br>d. [OK]をクリックして、このサイレンスを削除することを確定します。<br>◦ 注 * ：このアラートがトリガーされると（別のサイレンスで停止されていないかぎり）通知が送信されるようになりました。このアラートが現在トリガーされている場合は、 E メールまたは SNMP 通知の送信やアラートページの更新に数分かかることがあります。 |

関連情報

"SNMPエージェントの設定"

アラームの管理（従来のシステム）

## StorageGRID アラームシステムは、通常の動作中に発生することがある問題点を特定するために使用される従来のシステムです。

従来のアラームシステムは引き続きサポートされますが、アラートシステムには大きなメリットがあり、使いやすくなっています。

関連情報

"アラーム一覧（従来のシステム）"

"古いアラームの表示"

"StorageGRID の管理"

### アラームクラス（レガシーシステム）

レガシーアラームは、相互に排他的な 2 つのアラームクラスのいずれかに属することができます。

#### デフォルトアラーム

各 StorageGRID システムにはデフォルトアラームが用意されており、変更することはできません。ただし、グローバルカスタムアラームを定義して、デフォルトアラームを無効にしたり上書きしたりすることができます。

#### グローバルカスタムアラーム

グローバルカスタムアラームは、 StorageGRID システムの特定のタイプのサービスすべてのステータスを監視します。グローバルカスタムアラームを作成して、デフォルトアラームを上書きすることができます。新しいグローバルカスタムアラームを作成することもできます。これは、 StorageGRID システムについて独自の状況を監視する場合に役立ちます。

関連情報

"デフォルトアラームの表示（従来のシステム）"

"デフォルトアラームの無効化（レガシーシステム）"

"グローバルカスタムアラームの作成（従来のシステム）"

"グローバルカスタムアラームの無効化（従来のシステム）"

### アラームトリガーロジック（レガシーシステム）

StorageGRID 属性が、あるアラームクラス（デフォルトまたはグローバルカスタム）とアラームの重大度レベルの組み合わせに対して true と評価されるしきい値に達すると、それまでのアラームがトリガーされます。

| をクリックします。 | 色（ **Color** ） | アラームの重大度 | 意味 |
| --- | --- | --- | --- |
| | 黄色 | 注意 | ノードはグリッドに接続されていますが、正常な状態ではありません。通常の動作に影響はありません。 |

| をクリックします。 | 色（ **Color** ） | アラームの重大度 | 意味 |
| --- | --- | --- | --- |
| | 薄いオレンジ | マイナー | ノードはグリッドに接続されていますが、正常な状態ではありません。将来的に動作に影響する可能性があります。さらに重大な問題にならないように調査が必要です。 |
| | 濃いオレンジ | メジャー（ Major ） | ノードはグリッドに接続されていますが、正常な状態ではありません。すでに動作に影響が及んでいます。エスカレーションを防ぐために早急な対応が必要です。 |
| | 赤 | 重要 | ノードはグリッドに接続されていますが、正常な状態ではありません。正常に動作しなくなっています。問題 にはすぐに対処する必要があります。 |

アラームの重大度と対応するしきい値は、すべての数値属性に設定できます。各管理ノード上の NMS サービスは、設定されたしきい値に照らして現在の属性値を継続的に監視します。アラームがトリガーされると、指定した担当者全員に通知が送信されます。

重大度レベルが「 Normal 」の場合、アラームはトリガーされません。

属性値は、その属性に対して定義されている有効なアラームのリストに照らして評価されます。アラームのリストは次の順序でチェックされ、属性に対して定義された有効なアラームを含む最初のアラームクラスが特定されます。

1. アラームの重大度が「 Critical 」から「 Notice 」までのグローバルカスタムアラーム
2. アラームの重大度が「 Critical Down 」から「 Notice 」に設定されているデフォルトアラームです。

NMS サービスは、上位のアラームクラスで属性に対する有効なアラームを検出すると、そのクラス内でのみ評価し、NMS サービスは、他の優先順位の低いクラスとは比較しません。つまり、ある属性に対してグローバルカスタムアラームが有効になっている場合、 NMS サービスはグローバルカスタムアラームに対してのみ属性値を評価します。デフォルトアラームは評価されません。したがって、ある属性の有効なデフォルトアラームがアラームのトリガーに必要な条件を満たしていても、同じ属性の（指定した条件を満たさない）グローバルカスタムアラームが有効な場合はトリガーされません。アラームはトリガーされず、通知は送信されません。

アラームのトリガー例

次の例を参考に、グローバルカスタムアラームとデフォルトアラームのトリガー方法について理解してください。

次の例では、次の表に示すように、ある属性に対してグローバルカスタムアラームとデフォルトアラームが定義されて有効になっています。

| | グローバルカスタムアラームしきい値（有効） | デフォルトのアラームしきい値（有効） |
|---|---|---|
| 注意 | 1500 以上 | >=1000 |
| マイナー | 15 、 000 以上 | >=1000 |
| メジャー（ Major ） | 15 、 000 以上 | >=250,000 |

値が 1000 のときにこの属性が評価されると、アラームはトリガーされず、通知は送信されません。

グローバルカスタムアラームはデフォルトアラームより優先されます。1000 という値は、グローバルカスタムアラームのどの重大度レベルのしきい値にも達していません。その結果、アラームレベルは Normal と評価されます。

このシナリオのあとでグローバルカスタムアラームを無効にしても、何も変わりません。新しいアラームレベルがトリガーされるためには、属性値が再評価される必要があります。

グローバルカスタムアラームが無効な状態で属性値が再評価されると、属性値はデフォルトアラームのしきい値に照らして評価されます。その結果 Notice レベルのアラームがトリガーされ、指定した担当者に E メール通知が送信されます。

同じ重大度のアラームです

同じ属性の 2 つのグローバルカスタムアラームの重大度が同じ場合、アラームは「上から下」の優先度で評価されます。

たとえば、 UMEM が 50MB に下がった場合、最初のアラーム（ = 50000000 ）はトリガーされますが、その下のアラーム（ <= 100000000 ）はトリガーされません。

Global Alarms

Updated: 2016-03-17 16:05:31 PDT

**Global Custom Alarms** (0 Result(s))

| Enabled | Service | Attribute | Severity | Message | Operator | Value | Additional Recipients | Actions |
|---|---|---|---|---|---|---|---|---|
| ☑ | SSM | UMEM (Available Memory) | Minor | Under 50 | = | 5000 | | |
| ☑ | SSM | UMEM (Available Memory) | Minor | under10 | <= | 1000 | | |

アラームの順序を逆にした場合、 UMEM が 100MB に下がると、最初のアラーム（ <= 100000000 ）はトリガーされますが、その下のアラーム（ = 50000000 ）はトリガーされません。

Global Alarms
Updated: 2016-03-17 16:05:31 PDT

**Global Custom Alarms** (0 Result(s))

| Enabled | Service | Attribute | Severity | Message | Operator | Value | Additional Recipients | Actions |
|---|---|---|---|---|---|---|---|---|
| ☑ | SSM | UMEM (Available Memory) | Minor | under10 | <= | 1000 | | |
| ☑ | SSM | UMEM (Available Memory) | Minor | Under 50 | = | 5000 | | |

**Default Alarms**

Filter by Disabled Defaults

0 Result(s)

| Enabled | Service | Attribute | Severity | Message | Operator | Value | Actions |
|---|---|---|---|---|---|---|---|

Apply Changes

通知

通知には、アラームの発生またはサービスの状態の変更が報告されます。アラーム通知は E メールまたは SNMP で送信できます。

あるアラームしきい値に達したときに複数のアラームと通知が送信されないようにするために、アラームの重大度が属性の現在のアラームの重大度に照らしてチェックされます。変更がない場合、それ以上のアクションは実行されません。つまり、 NMS サービスは、システムの監視を継続するにあたり、ある属性のアラーム状態を初めて検出したときにのみアラームを生成して通知を送信します。属性の新しいしきい値に達したことが検出された場合は、アラームの重大度が変わり、新しい通知が送信されます。条件が Normal レベルに戻ると、アラームはクリアされます。

アラーム状態の通知に表示されるトリガー値は、小数点以下 3 桁に四捨五入されます。したがって、 1.9999 の属性値はしきい値が「 2.0 未満」のアラームをトリガーしますが、アラーム通知にはトリガー値が 2.0 と表示されます。

新しいサービス

新しいグリッドノードまたはサイトの追加によって新しいサービスが追加されると、そのサービスにはデフォルトアラームとグローバルカスタムアラームが継承されます。

アラームとテーブル

テーブルに表示されるアラーム属性は、システムレベルで無効にすることができます。テーブル内の個々の行に対してアラームを無効にすることはできません。

たとえば、次の表に、 Critical レベルの VMFI （ Entries Available ）アラームを 2 つ示します。（* Support > Tools > Grid Topology *を選択します。次に、「 * _ ストレージノード _ * > * SSM * > * リソース * 」を選択します。）

VMFI アラームを無効にして、 Critical レベルの VMFI アラームがトリガーされないようにすることができます（現在、 Critical レベルの両方のアラームがテーブルに緑で表示されます）。 ただし、テーブルの行の 1 つのアラームを無効にして、一方の VMFI アラームがクリティカルレベルのアラームとして表示され、もう一方の VMFI アラームは緑のままになるようにすることはできません。

**Volumes**

| Mount Point | Device | Status | Size | Space Available | Total Entries | Entries Available | Write Cache |
|---|---|---|---|---|---|---|---|
| / | sda1 | Online | 10.6 GB | 7.46 GB | 655,360 | 559,263 | Enabled |
| /var/local | sda3 | Online | 63.4 GB | 59.4 GB | 3,932,160 | 3,931,842 | Unknown |
| /var/local/rangedb/0 | sdb | Online | 53.4 GB | 53.4 GB | 52,428,800 | 52,427,856 | Enabled |
| /var/local/rangedb/1 | sdc | Online | 53.4 GB | 53.4 GB | 52,428,800 | 52,427,848 | Enabled |
| /var/local/rangedb/2 | sdd | Online | 53.4 GB | 53.4 GB | 52,428,800 | 52,427,856 | Enabled |

現在のアラームの確認応答（従来のシステム）

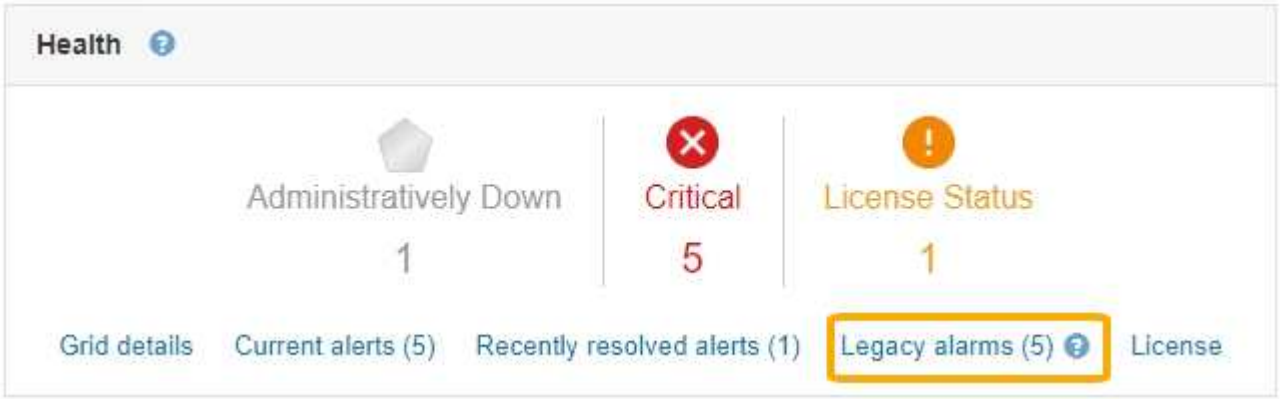
システム属性がアラームのしきい値に達すると、従来のアラームがトリガーされます。ダッシュボードでの古いアラームの数を減らすかクリアするには、アラームを確認します。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Acknowledge Alarms 権限が必要です。

このタスクについて

従来のシステムのアラームが現在アクティブな場合は、ダッシュボードのヘルスパネルに*レガシーアラーム*リンクが表示されます。かっこ内の数字は、現在アクティブなレガシーアラームの数を示します。




従来のアラームシステムは引き続きサポートされるため、新しいアラームが発生するたびに、ダッシュボードに表示される従来のアラームの数が増えます。この数は、アラームのEメール通知が送信されなくなった場合でも増分します。通常はこの数値を無視するか（アラートによってシステムがより正確に把握されるため）、アラームを確認することができます。

必要に応じて、アラートシステムに完全に移行した場合は、各レガシーアラームを無効にして、アラームがトリガーされないようにしたり、レガシーアラームの数に追加されたりしないようにすることができます。

確認応答したアラームは、重大度レベルが次のレベルでトリガーされるか、解決されて再度発生しないかぎり、レガシーアラームの数に含まれなくなります。

> 従来のアラームシステムは引き続きサポートされますが、アラートシステムには大きなメリットがあり、使いやすくなっています。

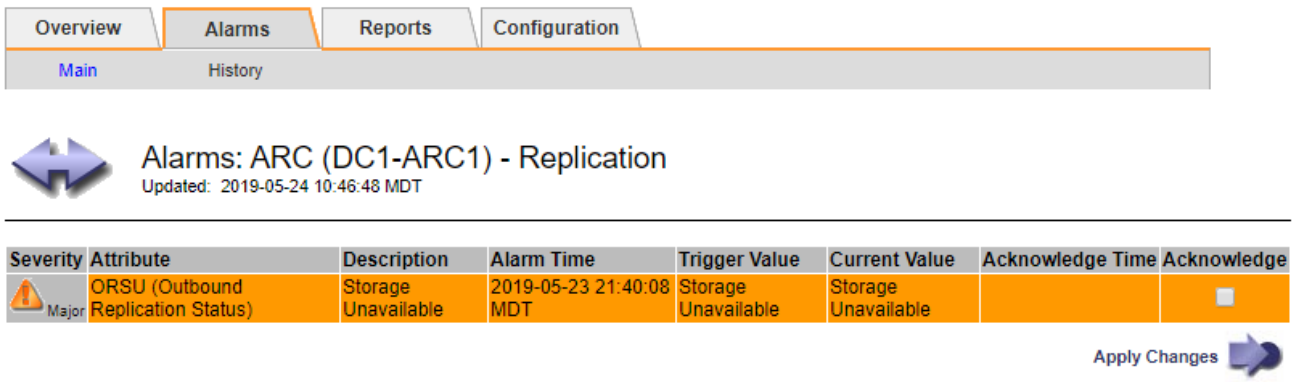
手順

1. アラームを表示するには、次のいずれかの操作を行います。

   - ダッシュボードの正常性パネルで、*レガシーアラーム*をクリックします。このリンクは、少なくとも1つのアラームが現在アクティブである場合にのみ表示されます。
   - [**Support**>]>[* Alarms (legac)**>]>[** Current Alarms]を選択します。[Current Alarms]ページが表示されます。

2. テーブルでサービス名をクリックします。

   選択したサービスのAlarmsタブが表示されます（* Support **>** Tools **>** Grid Topology **>*Grid Node** >**Service**>* Alarms *）。




3. アラームの * Acknowledge * （確認）チェックボックスを選択し、 * Apply Changes （変更の適用） * をクリックします。

   ダッシュボードまたは現在のアラームページにアラームが表示されなくなります。

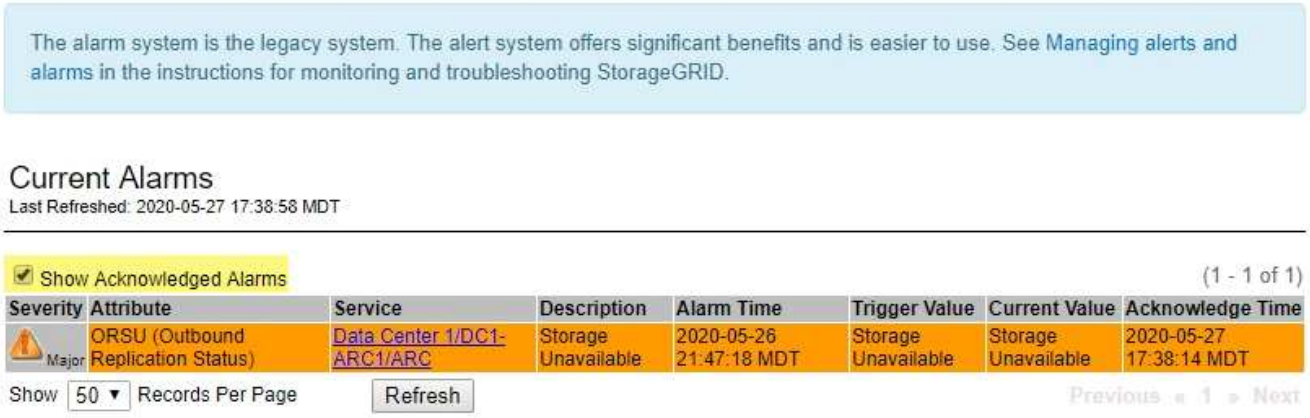
> アラームを確認しても、他の管理ノードには通知されません。このため、別の管理ノードのダッシュボードを表示してもアクティブなアラームが引き続き表示される場合があります。

4. 必要に応じて、確認済みのアラームを表示します。

a. [**Support**>]>[* Alarms (legac)**>]>[** Current Alarms]を選択します。

b. 「 * 確認済みアラームを表示」を選択します。

確認済みのアラームが表示されます。




関連情報

"アラーム一覧（従来のシステム）"

デフォルトアラームの表示（従来のシステム）

すべてのデフォルトのレガシーアラームのリストを表示できます。

必要なもの

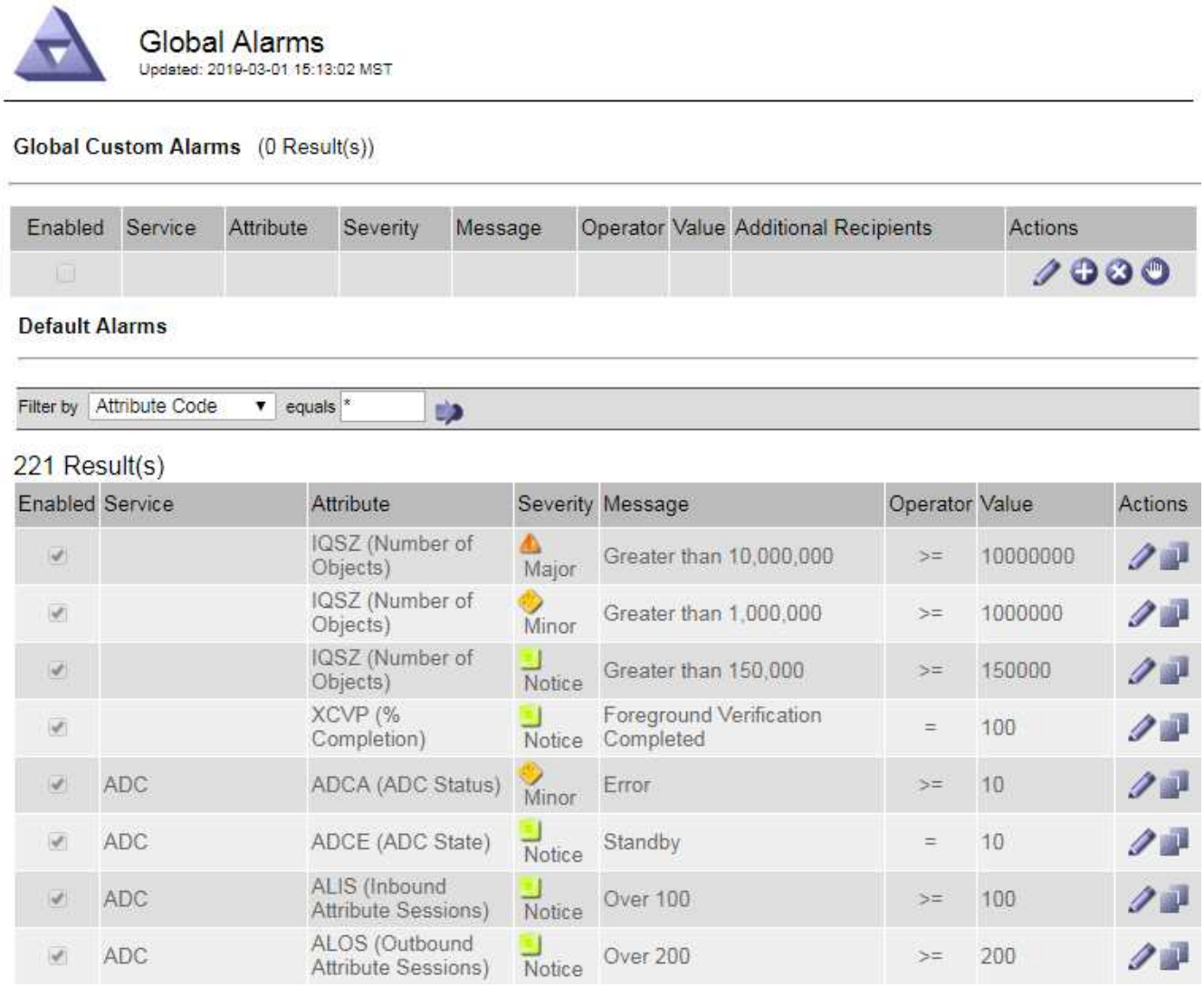
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

従来のアラームシステムは引き続きサポートされますが、アラートシステムには大きなメリットがあり、使いやすくなっています。

手順

1. [**Support**>]>[* Alarms (legac)**>]>[** Global Alarms]を選択します。
2. [ フィルタ条件 ] で、 [ * 属性コード * ] または [ * 属性名 * ] を選択します。
3. [等しい]には、アスタリスクを入力します。 *
4. 矢印をクリックします または、 **Enter** キーを押します。

すべてのデフォルトアラームが表示されます。




アラーム履歴とアラーム頻度の確認（従来のシステム）

問題 のトラブルシューティングでは、過去に過去のアラームがトリガーされた頻度を確認できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

従来のアラームシステムは引き続きサポートされますが、アラートシステムには大きなメリットがあり、使いやすくなっています。

手順

1. 一定の期間にトリガーされたすべてのアラームのリストを表示する手順は、次のとおりです。
   a. [**Support**>]>[* Alarms (legac)**>]>[** Historical Alarms]を選択します。
   b. 次のいずれかを実行します。
      - いずれかの期間をクリックします。
      - カスタム範囲を入力し、 * カスタムクエリ * をクリックします。

2. 特定の属性に対してアラームがトリガーされた頻度を確認するには、次の手順を実行します。
   a. Support **>** Tools **>** Grid Topology *を選択します。
   b. ***grid node***>**service* または *component**>* Alarms **>** History * を選択します
   c. リストから属性を選択します。
   d. 次のいずれかを実行します。
      - いずれかの期間をクリックします。
      - カスタム範囲を入力し、 * カスタムクエリ * をクリックします。

      アラームは新しいものから順番に表示されます。
   e. ［ ALARMS HISTORY REQUEST ］ フォームに戻るには、 ［ * 履歴 * ］ をクリックします。

関連情報

"アラーム一覧（従来のシステム）"

グローバルカスタムアラームの作成（従来のシステム）

従来のシステムでグローバルカスタムアラームを使用して特定の監視要件に対処している場合があります。グローバルカスタムアラームには、デフォルトアラームを上書きするアラームレベルが設定されている場合や、デフォルトアラームのない属性を監視する場合があります。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

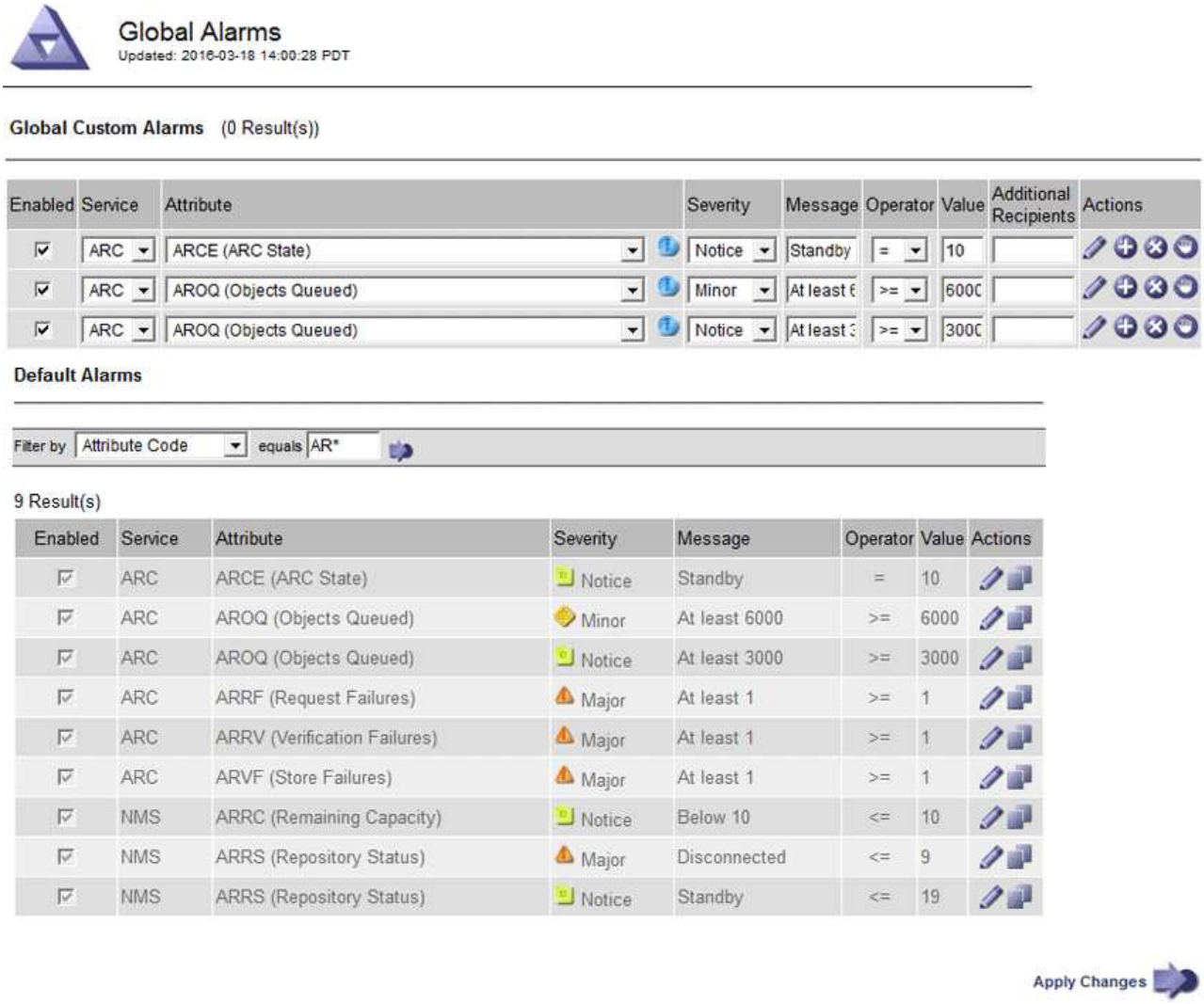
> 従来のアラームシステムは引き続きサポートされますが、アラートシステムには大きなメリットがあり、使いやすくなっています。

グローバルカスタムアラームはデフォルトアラームを上書きします。デフォルトアラームの値は、どうしても必要な場合以外は変更しないでください。デフォルトアラームを変更すると、アラームとなるはずの問題が発覚しなくなる危険があります。

> アラーム設定を変更する場合は十分に注意してください。たとえば、あるアラームのしきい値を引き上げると、根本的な問題が検出されない可能性があります。アラームの設定を変更する前に、変更案についてテクニカルサポートと検討してください。

手順

1. [**Support**>]>[* Alarms (legac)**>]>[** Global Alarms]を選択します。
2. グローバルカスタムアラームのテーブルに新しい行を追加します。
   - 新しいアラームを追加するには、 * Edit * をクリックします （最初のエントリの場合）または * Insert * を入力します アイコン"]。




◦ デフォルトアラームを変更するには、デフォルトアラームを検索します。

i. [ フィルタ条件 ] で、 [ * 属性コード * ] または [ * 属性名 * ] を選択します。

ii. 検索文字列を入力します。

4 文字を指定するか、ワイルドカードを使用します（例： a ？？？？または AB* ）。アスタリスク（ * ）は複数の文字を表し、疑問符（？）は 単一の文字を表します。

iii. 矢印をクリックします を押すか、 * Enter * を押します。

iv. 結果のリストで、 * コピー * をクリックします をクリックします。

デフォルトアラームがグローバルカスタムアラームのテーブルにコピーされます。

3. グローバルカスタムアラームの設定に必要な変更を加えます。

| 見出し | 説明 |
| --- | --- |
| 有効 | このチェックボックスをオンまたはオフにすると、アラームが有効または無効になります。 |

| 見出し | 説明 |
| --- | --- |
| 属性 | 選択したサービスまたはコンポーネントに該当するすべての属性のリストから、監視対象の属性の名前とコードを選択します。<br><br>属性に関する情報を表示するには、 * 情報 * をクリックします をクリックします。 |
| 重大度 | アラームのレベルを示すアイコンとテキスト。 |
| メッセージ | アラームの理由です（例： connection lost 、 storage space below 10% ）。 |
| 演算子 | 値のしきい値に対して現在の属性値をテストするための演算子：<br><br>• = 等しい<br>• > より大きい<br>• < より小さい<br>• >= より大きいか等しい<br>• <= 以下<br>• ≠等しくありません |
| 価値 | アラームのしきい値。演算子を使用して属性の実際の値に対してテストします。1 つの数値、コロンで指定した数値範囲（ 1 ： 3 ）、または数値と範囲をカンマで区切ったリストを入力できます。 |
| 受信者の追加 | アラームがトリガーされたときに通知を受け取る E メールアドレスの追加リストです。これは、 [**Alarms**>*Email Setup*] ページに設定されているメーリングリストに加えて行われます。カンマで区切って指定します。<br><br>• 注意： * メーリングリストを利用するには、 SMTP サーバーを設定する必要があります。メーリングリストを追加する前に、 SMTP が設定されていることを確認してください。カスタムアラームの通知で、グローバルカスタムアラームまたはデフォルトアラームの通知を上書きすることができます。 |
| アクション | 次の操作を行うためのコントロールボタン<br><br>行を編集します<br><br>アイコン"] 行を挿入します<br><br>行を削除します<br><br>行を上下にドラッグアンドドロップします<br><br>行をコピーします |

4. [ 変更の適用 *] をクリックします。

関連情報

"アラーム用Eメールサーバの設定（従来のシステム）"

### アラームの無効化（従来のシステム）

従来のアラームシステムのアラームはデフォルトで有効になっていますが、不要なアラームは無効にすることができます。新しいアラートシステムに完全に移行したあとに、古いアラームを無効にすることもできます。

> 従来のアラームシステムは引き続きサポートされますが、アラートシステムには大きなメリットがあり、使いやすくなっています。

### デフォルトアラームの無効化（レガシーシステム）

システム全体でいずれかの従来のデフォルトアラームを無効にすることができます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

現在アラームがトリガーされている属性のアラームを無効にしても、現在のアラームはクリアされません。次回その属性がアラームのしきい値を超えるとアラームが無効になります。または、トリガーされたアラームをクリアできます。

> 新しいアラートシステムに完全に移行するまでは、古いアラームを無効にしないでください。そうしないと、重大な処理を完了できなくなるまで、根本的な問題が検出されない可能性があります。

手順

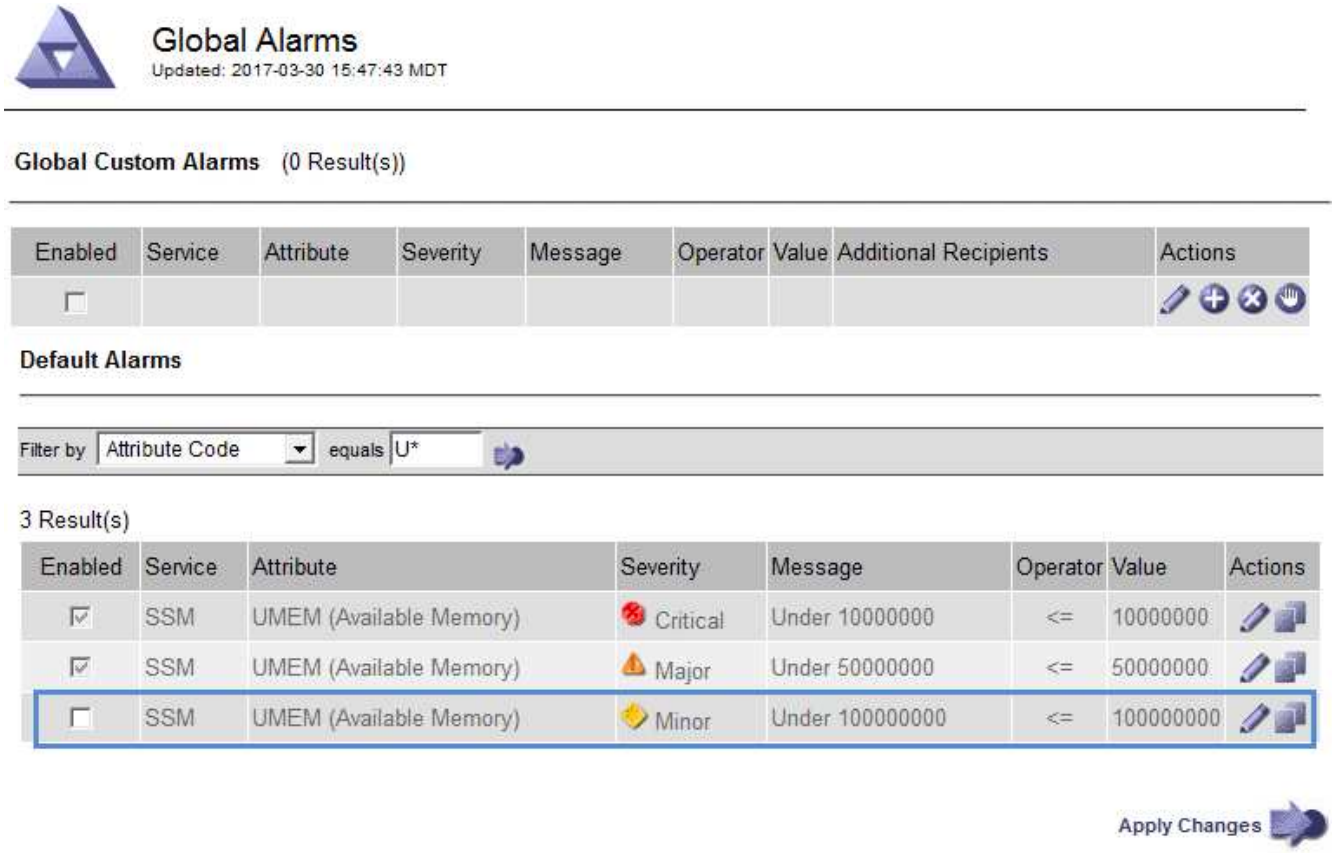
1. [**Support**>]>[* Alarms (legac)**>]>[** Global Alarms]を選択します。
2. 無効にするデフォルトアラームを検索します。
   a. [ デフォルトアラーム ] セクションで、 [* フィルタを * > * 属性コード * でフィルタ ] または [ * 属性名 * ] を選択します。
   b. 検索文字列を入力します。

      4 文字を指定するか、ワイルドカードを使用します（例： a ？？？？または AB* ）。アスタリスク（ * ）は複数の文字を表し、疑問符（？）は 単一の文字を表します。

   c. 矢印をクリックします を押すか、 * Enter * を押します。

      > [*Disabled Defaults] を選択すると、現在無効になっているすべてのデフォルトアラームのリストが表示されます。

3. 検索結果リストから、 [ 編集 ] アイコンをクリックします をクリックします。




選択したアラームの * Enabled * チェックボックスがアクティブになります。

4. [ 有効 *] チェックボックスの選択を解除します。
5. [ 変更の適用 *] をクリックします。

   デフォルトアラームは無効です。

## グローバルカスタムアラームの無効化（従来のシステム）

システム全体で従来のグローバルカスタムアラームを無効にすることができます。

### 必要なもの

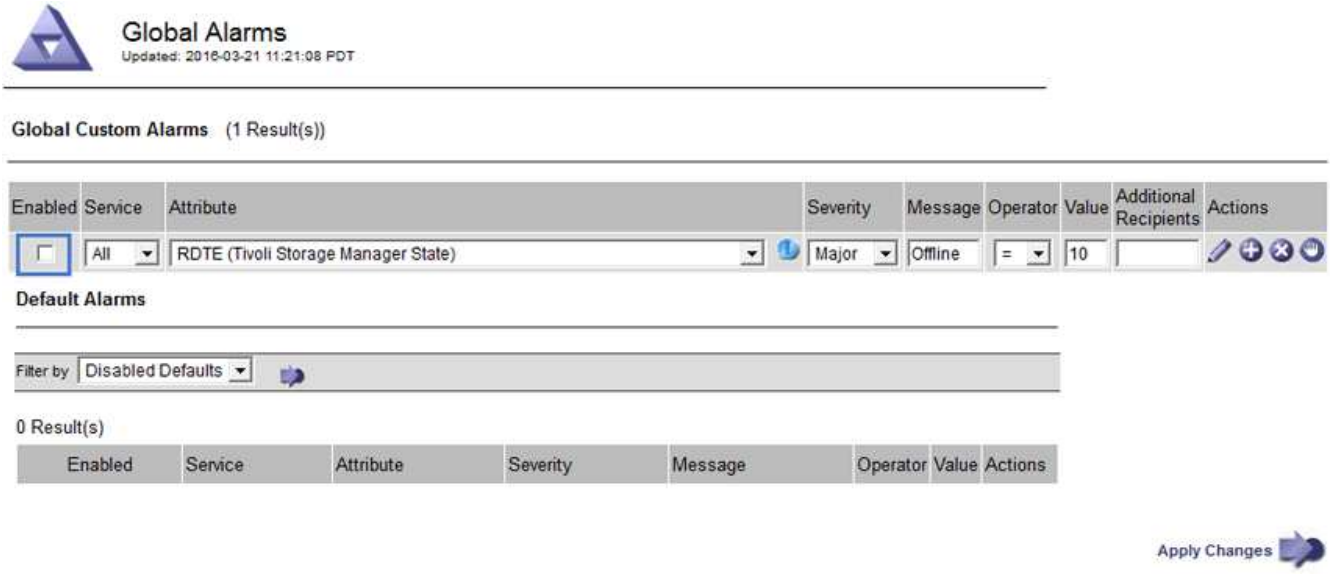
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

### このタスクについて

現在アラームがトリガーされている属性のアラームを無効にしても、現在のアラームはクリアされません。次回その属性がアラームのしきい値を超えるとアラームが無効になります。または、トリガーされたアラームをクリアできます。

### 手順

1. [**Support**>]>[* Alarms (legac)**>]>[** Global Alarms]を選択します。
2. Global Custom Alarms テーブルで、 * Edit * をクリックします をクリックします。
3. [ 有効 *] チェックボックスの選択を解除します。




4. [ 変更の適用 *] をクリックします。

   グローバルカスタムアラームは無効になっています。

## トリガーされたアラームのクリア（従来のシステム）

古いアラームがトリガーされた場合は、確認せずにクリアできます。

必要なもの

- を用意しておく必要があります `Passwords.txt` ファイル。

現在アラームがトリガーされている属性のアラームを無効にしても、アラームはクリアされません。このアラームは、属性が変わったときに無効になります。アラームを確認することも、属性値の変化（アラームの状態の変化）を待たずにアラームをすぐにクリアしたい場合は、トリガーされたアラームをクリアできます。これは、値があまり変化しない属性（状態属性など）に対してアラームをすぐにクリアしたい場合に便利です。

1. アラームを無効にします。
2. プライマリ管理ノードにログインします。
   a. 次のコマンドを入力します。 *`ssh admin@primary_Admin_Node_IP`*
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

      rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。
3. NMSサービスを再開します。 `service nms restart`
4. 管理ノードからログアウトします。 `exit`

   アラームが解除されます。

関連情報

"アラームの無効化（従来のシステム）"

アラームの通知の設定（従来のシステム）

StorageGRID システムでは、アラームがトリガーされたときやサービスの状態が変わったときに、Eメール通知やSNMP通知を自動的に送信できます。

デフォルトでは、アラームの E メール通知は送信されません。E メール通知の場合は、 E メールサーバを設定し、 E メール受信者を指定する必要があります。SNMP 通知の場合は、 SNMP エージェントを設定する必要があります。

関連情報

"SNMPによる監視を使用する"

アラーム通知のタイプ（従来のシステム）

レガシーアラームがトリガーされると、 StorageGRID システムは重大度レベルとサービス状態の 2 種類のアラーム通知を送信します。

重大度レベルの通知

選択した重大度レベルのレガシーアラームがトリガーされると、アラーム E メール通知が送信されます。

- 注意
- マイナー
- メジャー（ Major ）
- 重要

メーリングリストは、選択した重大度のアラームに関連するすべての通知を受信します。また、アラームが解決されたか、別の重大度レベルになったことによって、アラームレベルが解除されたときにも通知が送信されます。

サービス状態の通知

サービス状態の通知は、サービス（ LDR サービスや NMS サービスなど）が選択したサービス状態になったとき、および選択したサービス状態でなくなったときに送信されます。サービス状態通知は、サービスが次のサービス状態になったとき、またはその状態になったときに送信されます。

- 不明です
- 意図的な停止

メーリングリストは、選択した状態の変更に関連するすべての通知を受信します。

関連情報

"アラームのEメール通知の設定（従来のシステム）"

アラーム用**E**メールサーバの設定（従来のシステム）

従来のアラームがトリガーされたときに StorageGRID から E メール通知を送信するには、 SMTP メールサーバ設定を指定する必要があります。StorageGRID システムは E メールを送信するだけで、 E メールを受信

することはできません。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

以下の設定を使用して、従来のアラーム E メール通知と AutoSupport E メールメッセージに使用する SMTP サーバを定義します。これらの設定は、アラート通知には使用されません。

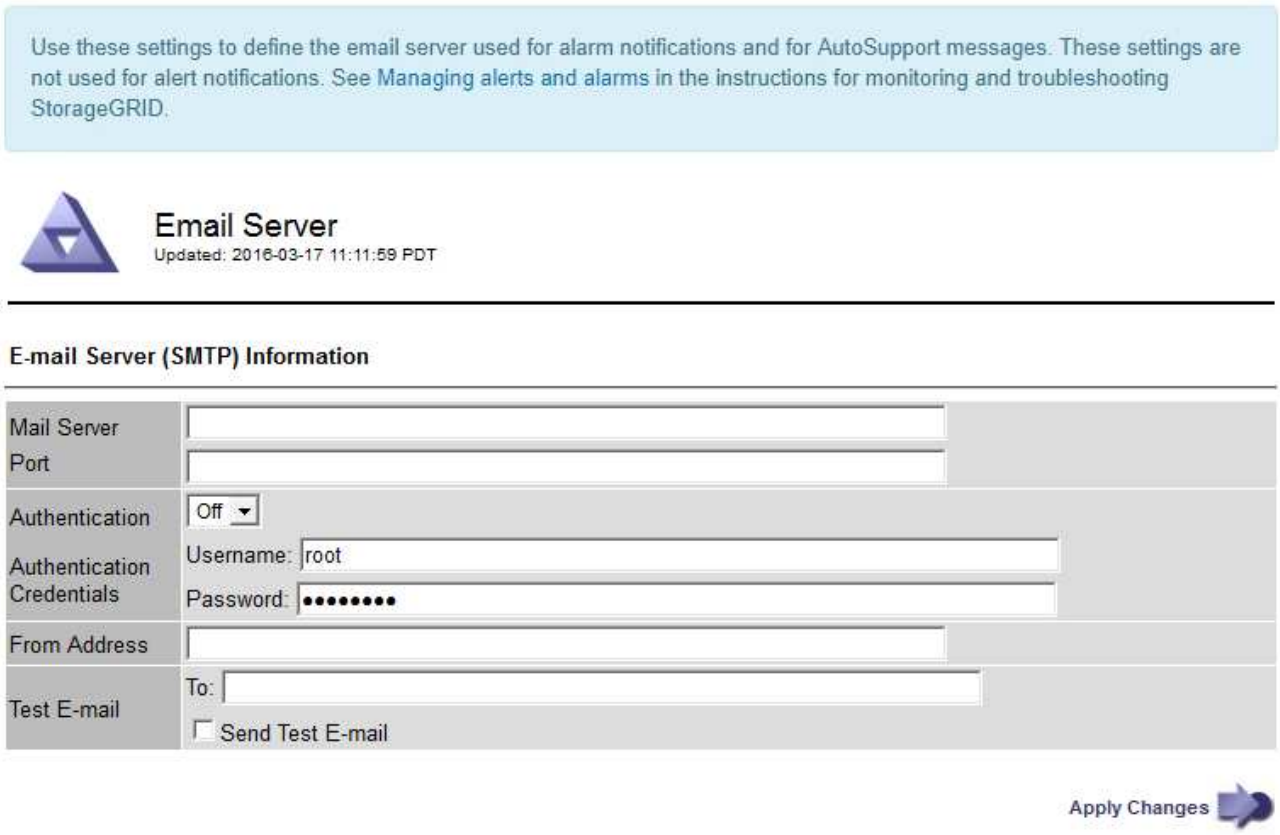
SMTP を AutoSupport メッセージのプロトコルとして使用する場合は、 SMTP メールサーバを設定済みの可能性があります。アラームの E メール通知には同じ SMTP サーバが使用されるため、この手順 はスキップしてかまいません。StorageGRID の管理手順を参照してください。

SMTP は、 E メールの送信用にサポートされている唯一のプロトコルです。

手順

1. [**Support**>]>[* Alarms (legacy]**>[** Legacy Email Setup*]を選択します。
2. [ 電子メール ] メニューから、 [**Server** ] を選択します。

   [Email Server] ページが表示されます。このページは、 AutoSupport メッセージ用の E メールサーバの設定にも使用されます。




3. 次の SMTP メールサーバ設定を追加します。

| 項目 | 説明 |
| --- | --- |
| メールサーバ | SMTP メールサーバの IP アドレス。以前に管理ノードで DNS を設定している場合は、 IP アドレスではなくホスト名を入力できます。 |
| ポート | SMTP メールサーバにアクセスするためのポート番号。 |
| 認証 | SMTP メールサーバの認証を許可します。デフォルトでは、認証はオフです。 |
| 認証クレデンシャル | SMTP メールサーバのユーザ名とパスワード。認証がオンに設定されている場合は、 SMTP メールサーバにアクセスするためのユーザ名とパスワードを指定する必要があります。 |

4. [ 送信元アドレス * ] に、 SMTP サーバーが送信元電子メールアドレスとして認識する有効な電子メールアドレスを入力します。これは、 E メールメッセージの送信元となる公式な E メールアドレスです。
5. 必要に応じて、テスト用 E メールを送信して SMTP メールサーバの設定が正しいことを確認します。
   a. [ 電子メールのテスト > 宛先 *] ボックスに、アクセスできるアドレスを 1 つ以上追加します。

      1 つの E メールアドレスまたは E メールアドレスのカンマ区切りのリストを入力できます。テスト用 E メールを送信しても NMS サービスでは成功したかどうかが確認されないため、テスト受信者の受信ボックスを確認できる必要があります。

   b. [ テスト電子メールの送信 *] を選択します。
6. [ 変更の適用 *] をクリックします。

   SMTP メールサーバの設定が保存されます。テスト用 E メールの情報を入力した場合は、その E メールが送信されます。テスト用 E メールは、すぐにメールサーバに送信され、通知キュー経由では送信されません。複数の管理ノードがあるシステムでは、各管理ノードから E メールが送信されます。テスト用 E メールが届けば、 SMTP メールサーバの設定は正しく、 NMS サービスはメールサーバに正常に接続しています。NMS サービスとメールサーバの接続に問題がある場合は、 Minor 重大度レベルの Legacy MINS （ NMS Notification Status ）アラームがトリガーされます。

関連情報

"StorageGRID の管理"

アラーム**E**メールテンプレートの作成（従来のシステム）

E メールテンプレートを使用して、従来のアラーム E メール通知のヘッダー、フッター、および件名をカスタマイズできます。E メールテンプレートを使用すると、本文に同じ内容を含む一意の通知をさまざまなメーリングリストに送信できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

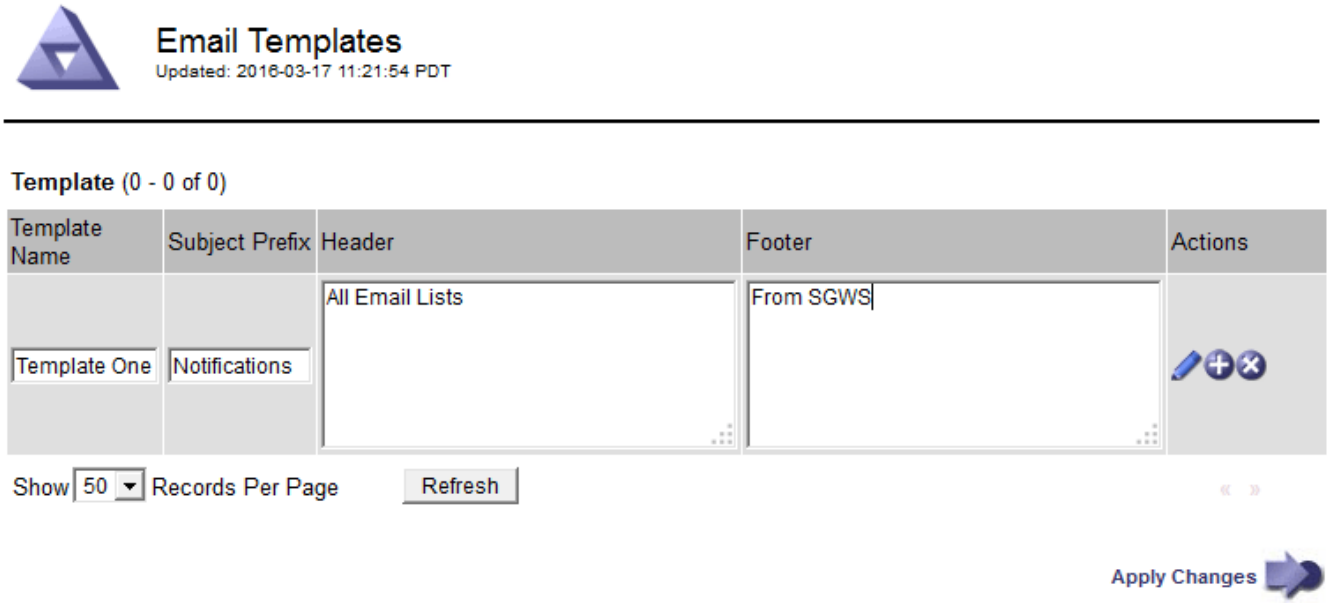
このタスクについて

以下の設定を使用して、従来のアラーム通知に使用する E メールテンプレートを定義します。これらの設定は、アラート通知には使用されません。

メーリングリストごとに異なる連絡先情報が必要になる場合があります。テンプレートには、電子メールメッセージの本文は含まれません。

手順

1. [**Support**>]>[* Alarms (legacy]**>[** Legacy Email Setup*]を選択します。
2. [ 電子メール ] メニューから、 [**Templates**] を選択します。
3. [ 編集（ Edit ） ] をクリックします。 （または * Insert * ） アイコン"] 最初のテンプレートではない場合）をクリックします。




4. 新しい行に次の項目を追加します。

| 項目 | 説明 |
| --- | --- |
| テンプレート名 | テンプレートの識別に使用する一意の名前。重複するテンプレート名は使用できません。 |
| 件名の接頭辞 | 任意。E メールの件名の先頭に表示されるプレフィックスです。プレフィックスを使用すると、メールフィルタを簡単に設定し、通知を整理できます。 |
| ヘッダー | 任意。メール本文の先頭に表示されるヘッダーテキストです。ヘッダーテキストを使用すると、会社名や住所などの情報を本文の前に配置できます。 |

| 項目 | 説明 |
| --- | --- |
| フッター | 任意。メッセージ本文の末尾に表示されるフッターテキストです。フッターテキストを使用すると、連絡先の電話番号や Web サイトへのリンクなどのリマインダ情報を本文の末尾に配置できます。 |

5. [ 変更の適用 *] をクリックします。

   通知の新しいテンプレートが追加されます。

## アラーム通知のメーリングリストの作成（従来のシステム）

メーリングリストを使用すると、古いアラームがトリガーされたときやサービスの状態が変わったときに通知を送信することができます。アラームの E メール通知を送信するには、少なくとも 1 つのメーリングリストを作成する必要があります。1 人の受信者に通知を送信するには、 1 つの E メールアドレスを含むメーリングリストを作成します。

### 必要なもの

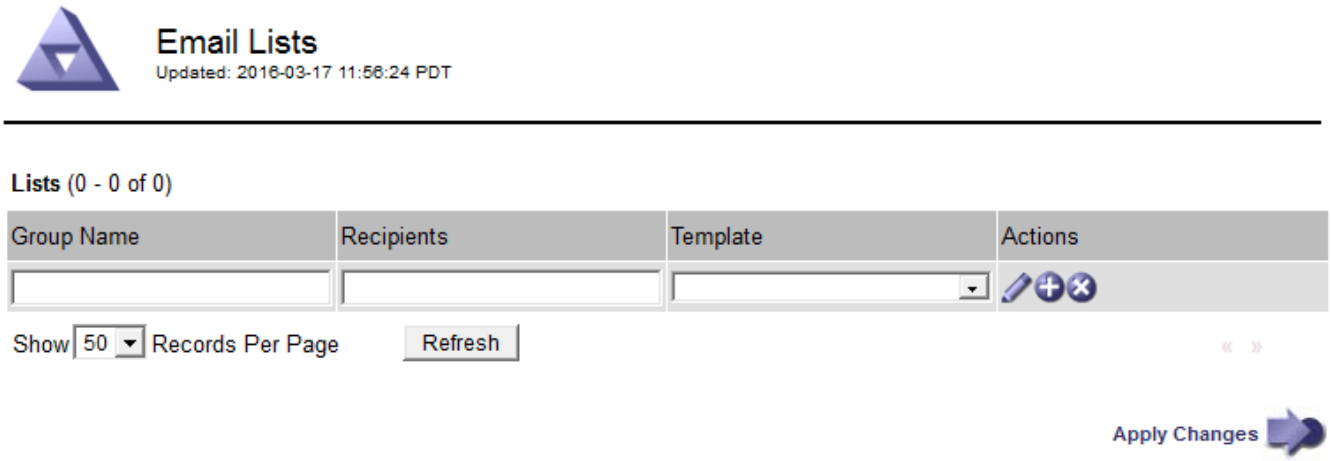
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- メーリングリストに E メールテンプレート（カスタムのヘッダー、フッター、件名）を指定する場合は、テンプレートを作成しておく必要があります。

### このタスクについて

以下の設定を使用して、従来のアラーム E メール通知に使用するメーリングリストを定義します。これらの設定は、アラート通知には使用されません。

### 手順

1. [**Support**>]>[* Alarms (legacy]**>[** Legacy Email Setup*]を選択します。
2. ［ E メール ］ メニューから ［ * リスト * ］ を選択します。
3. [ 編集（ Edit ） ] をクリックします。 （または * Insert * ） アイコン"] 最初のメーリングリストではない場合）をクリックします。



4. 新しい行に次の項目を追加します。

| 項目 | 説明 |
| --- | --- |
| グループ名 | メーリングリストを識別する一意の名前。重複するメーリングリスト名は使用できません。<br><br>• 注意：* メーリングリストの名前を変更しても、そのメーリングリスト名を使用する他の場所に変更は反映されません。新しいメーリングリスト名を使用するように、設定済みの通知をすべて手動で更新する必要があります。 |
| 受信者 | 通知の送信先となる単独の E メールアドレス、設定済みのメーリングリスト、または E メールアドレスおよびメーリングリストをカンマで区切って指定します。<br><br>• 注意：* 電子メールアドレスが複数のメーリングリストに属している場合は、通知をトリガーするイベントが発生すると、 1 通の電子メール通知のみが送信されます。 |
| テンプレート | 必要に応じて、 E メールテンプレートを選択し、このメーリングリストのすべての受信者に送信される通知に一意のヘッダー、フッター、および件名を追加します。 |

5. [ 変更の適用 *] をクリックします。

   新しいメーリングリストが作成されます。

関連情報

"アラームEメールテンプレートの作成（従来のシステム）"

## アラームのEメール通知の設定（従来のシステム）

従来のアラームシステムの E メール通知を受信するには、受信者がメーリングリストのメンバーであり、そのリストを通知ページに追加する必要があります。通知は、指定した重大度レベルのアラームがトリガーされた場合やサービスの状態が変わった場合にのみ、受信者に E メールを送信するように設定されています。このため、受信者は受信する必要がある通知のみを受信します。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- 設定済みの E メールリストが必要です。

このタスクについて

以下の設定を使用して、従来のアラームの通知を設定します。これらの設定は、アラート通知には使用されま

せん。

E メールアドレス（またはリスト）が複数のメーリングリストに属している場合、通知をトリガーするイベントが発生すると E メール通知は 1 通だけ送信されます。たとえば、重大度に関係なくすべてのアラームの通知を受信するように、組織内の 1 つの管理者グループを設定できます。また、別のグループは、重大度が Critical のアラームの通知のみ必要とします。両方のリストに所属できます。Critical レベルのアラームがトリガーされると通知が 1 通だけ送信されます。

手順

1. [**Support**>]>[* Alarms (legacy]**>[** Legacy Email Setup*]を選択します。
2. [ 電子メール ] メニューから、 [**Notifications**] を選択します。
3. [ 編集（ Edit ） ] をクリックします。 （または * Insert * ） アイコン"] 最初の通知ではない場合）をクリックします。
4. [ 電子メールリスト ] でメーリングリストを選択します。
5. 1 つ以上のアラーム重大度レベルとサービス状態を選択します。
6. [ 変更の適用 *] をクリックします。

   選択したアラーム重大度レベルまたはサービス状態のアラームがトリガーまたは変更されると、メーリングリストに通知が送信されます。

関連情報

"アラーム通知のメーリングリストの作成（従来のシステム）"

"アラーム通知のタイプ（従来のシステム）"

メーリングリストでのアラーム通知の停止（従来のシステム）

メーリングリストでアラームに関する通知を受信しないようにするには、メーリングリストのアラーム通知を停止します。たとえば、に移行したあとに、古いアラームに関する通知をアラート E メール通知を停止することができます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

以下の設定を使用して、レガシーアラームシステムの E メール通知を停止します。これらの設定は、アラート E メール通知には適用されません。

従来のアラームシステムは引き続きサポートされますが、アラートシステムには大きなメリットがあり、使いやすくなっています。

手順

1. [**Support**>]>[* Alarms (legacy]**>[** Legacy Email Setup*]を選択します。
2. [ 電子メール ] メニューから、 [**Notifications**] を選択します。
3. [ 編集（ Edit ） ] をクリックします。 をクリックします。
4. 抑制 (Suppress) で ' 抑制するメーリングリストの横にあるチェックボックスをオンにするか ' 列の上部に

ある **Suppress** を選択してすべてのメーリングリストを抑制します

5. [ 変更の適用 *] をクリックします。

   選択したメーリングリストに対して古いアラーム通知が停止されます。

## システム全体での**E**メール通知の停止

従来のアラームやイベントトリガー型 AutoSupport メッセージについて、 StorageGRID システムから E メール通知を送信する機能をブロックできます。

### 必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

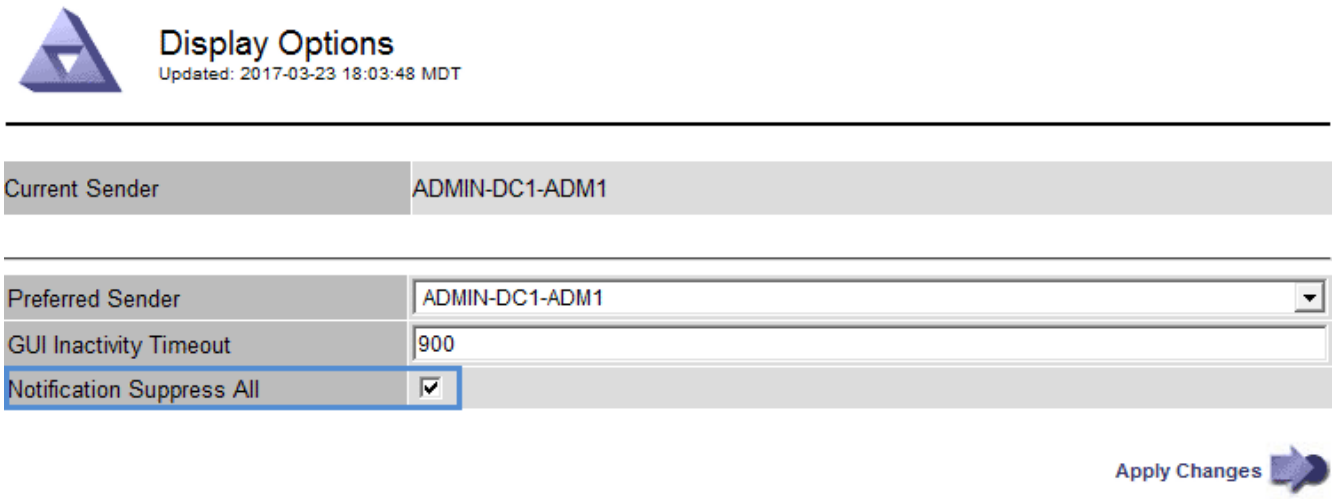
### このタスクについて

このオプションを使用して、従来のアラームやイベントトリガー型 AutoSupport メッセージの E メール通知を停止します。

> このオプションではアラート E メール通知は停止されません。週次またはユーザトリガー型の AutoSupport メッセージも停止されません。

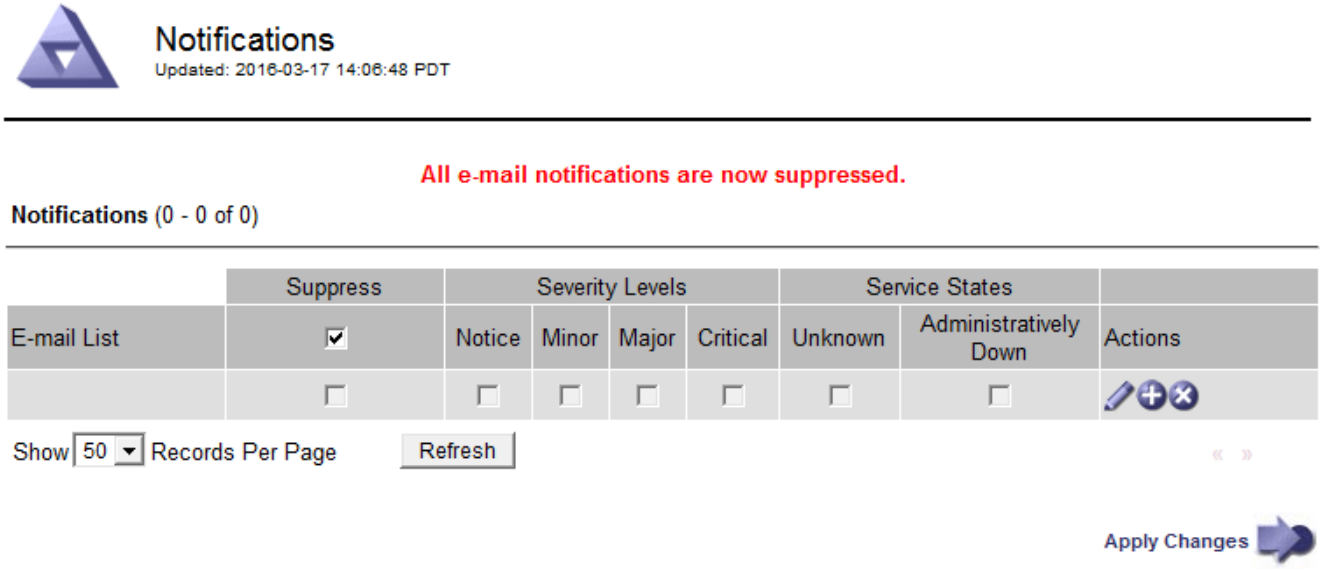
### 手順

1. * Configuration **>** System Settings **>** Display Options *を選択します。
2. [ 表示オプション ] メニューから、 [ * オプション * ] を選択します。
3. 通知 (Notification Suppress All) を選択します *




4. [ 変更の適用 *] をクリックします。

   通知ページ（ * 構成 * > * 通知 * ）には、次のメッセージが表示されます。




関連情報

"StorageGRID の管理"

# SNMPによる監視を使用する

簡易ネットワーク管理プロトコル（ SNMP ）を使用して StorageGRID を監視する場合は、 StorageGRID に含まれる SNMP エージェントを設定する必要があります。

- "SNMPエージェントの設定"
- "SNMPエージェントを更新しています"

機能

各 StorageGRID ノードは、管理情報ベース（ MIB ）を提供する SNMP エージェントまたはデーモンを実行します。StorageGRID の MIB には、アラートおよびアラームのテーブルおよび通知定義が含まれています。この MIB には、各ノードのプラットフォームやモデル番号など、システムの概要 情報も含まれています。各 StorageGRID ノードは MIB-II オブジェクトのサブセットもサポートしています。

最初は、すべてのノードで SNMP が無効になっています。SNMP エージェントを設定すると、すべての StorageGRID ノードに同じ設定が適用されます。

StorageGRID SNMP エージェントは、 3 つのバージョンの SNMP プロトコルをすべてサポートします。クエリに読み取り専用 MIB アクセスを提供し、次の 2 種類のイベントベース通知を管理システムに送信できます。

- * トラップ * は、管理システムによる確認応答を必要としない SNMP エージェントによって送信される通知です。トラップは、アラートがトリガーされているなど、 StorageGRID 内で何らかの問題が発生したことを管理システムに通知するために使用されます。

  トラップは、 SNMP の 3 つのバージョンすべてでサポートされています。

- * informs * はトラップに似ていますが、管理システムからの確認応答が必要です。SNMP エージェントが一定時間内に確認応答を受信しなかった場合、確認応答を受信するか、最大再試行値に達するまで、通知を再送信します。

インフォームは SNMPv2c および SNMPv3 でサポートされます。

トラップ通知およびインフォーム通知は、次の場合に送信されます。

- デフォルトまたはカスタムのアラートはいずれかの重大度レベルでトリガーされます。アラートの SNMP 通知を停止するには、アラートのサイレンスを設定する必要があります。アラート通知は、優先送信者として設定された管理ノードから送信されます。
- 特定のアラーム（従来型システム）は、指定した重大度レベル以上でトリガーされます。

> SNMP 通知は、すべてのアラームまたはすべてのアラーム重大度について送信されるわけではありません。

**SNMP** バージョンサポート

次の表に、各 SNMP バージョンでサポートされる内容の概要を示します。

| | **SNMPv1** | **SNMPv2c** の場合 | **SNMPv3** |
|---|---|---|---|
| クエリ | 読み取り専用 MIB クエリ | 読み取り専用 MIB クエリ | 読み取り専用 MIB クエリ |
| クエリ認証 | コミュニティストリング | コミュニティストリング | ユーザベースのセキュリティモデル（ USM ）ユーザ |
| 通知 | トラップのみ | トラップおよびインフォーム | トラップおよびインフォーム |
| 通知認証 | トラップの送信先ごとに、デフォルトのトラップコミュニティまたはカスタムのコミュニティストリングを指定します | トラップの送信先ごとに、デフォルトのトラップコミュニティまたはカスタムのコミュニティストリングを指定します | トラップの送信先ごとの USM ユーザ |

制限

- StorageGRID は、読み取り専用 MIB アクセスをサポートしています。読み取り / 書き込みアクセスはサポートされていません。
- グリッド内のすべてのノードが同じ設定を受信します。
- SNMPv3 ： StorageGRID は TSM （ Transport Support Mode ）をサポートしていません。
- SNMPv3 ： SHA （ HMAC-SHA-96 ）だけがサポートされています。
- SNMPv3 ： AES のみがサポートされています。

**MIB**へのアクセス

MIB 定義ファイルには、任意の StorageGRID ノードの次の場所からアクセスできます。

/usr/share/snmp/mibs/NETAPP-STORAGEGRID-MIB.txt

関連情報

"アラート一覧"

"アラーム一覧（従来のシステム）"

"SNMP 通知を生成するアラーム（従来のシステム）"

"アラート通知のサイレント化"

**SNMP**エージェントの設定

## 読み取り専用 MIB アクセスおよび通知にサードパーティ製 SNMP 管理システムを使用する場合は、 StorageGRID SNMP エージェントを設定できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限が必要です。

このタスクについて

StorageGRID SNMP エージェントは、 3 つのバージョンの SNMP プロトコルをすべてサポートします。エージェントは 1 つ以上のバージョンに設定できます。

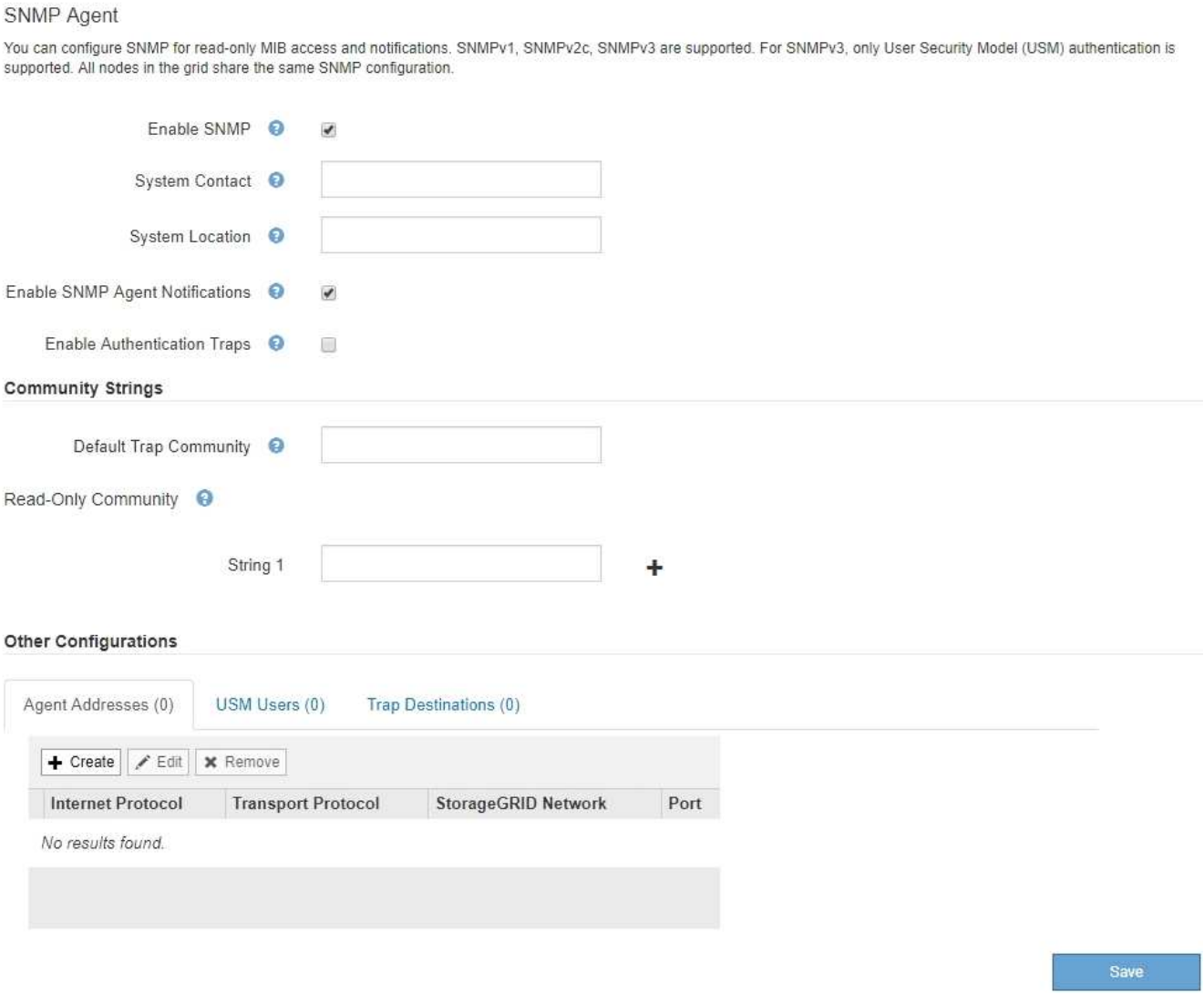
手順

1. * Configuration > Monitoring > SNMP Agent *を選択します。

   SNMP Agent ページが表示されます。

2. すべてのグリッドノードで SNMP エージェントを有効にするには、 * SNMP を有効にする * チェックボックスをオンにします。

   SNMP エージェントを設定するためのフィールドが表示されます。




3. **System Contact** フィールドに、 sysContact の SNMP メッセージで StorageGRID が提供する値を入力します。

   システムの連絡先は通常、電子メールアドレスです。StorageGRID システムで環境 のすべてのノードを指定する値。* システム連絡先 * は最大 255 文字です。

4. [ システムロケーション *] フィールドに、 StorageGRID が sysLocation の SNMP メッセージに提供する値を入力します。

   システムの場所は、 StorageGRID システムの場所を特定するのに役立つ情報で、任意に指定できます。たとえば、施設の住所を使用できます。StorageGRID システムで環境 のすべてのノードを指定する値。* システムの場所 * は最大 255 文字です。

5. StorageGRID SNMP エージェントがトラップおよびインフォーム通知を送信する場合は、 [SNMP エージェント通知を有効にする *] チェックボックスをオンのままにします。

   このチェックボックスがオフの場合、 SNMP エージェントは読み取り専用 MIB アクセスをサポートしますが、 SNMP 通知は送信しません。

6. StorageGRID SNMP エージェントが不適切に認証されたプロトコルメッセージを受信した場合に認証トラップを送信するには、 [ 認証トラップを有効にする *] チェックボックスをオンにします。

7. SNMPv1 または SNMPv2c を使用する場合は、コミュニティストリングセクションに必要事項を記入します。

   このセクションのフィールドは、 SNMPv1 または SNMPv2c でのコミュニティベースの認証に使用されます。これらのフィールドは SNMPv3 には適用されません。

   a. [ デフォルトトラップコミュニティ *] フィールドに、トラップ送信先に使用するデフォルトのコミュニティストリングを任意で入力します。

      必要に応じて ' 別の ( カスタム ) コミュニティ文字列を指定できます 特定のトラップ送信先を定義します。

      - デフォルトのトラップコミュニティ * は 32 文字以内で、空白文字を含めることはできません。

   b. * 読み取り専用コミュニティ * には、 1 つ以上のコミュニティストリングを入力して、 IPv4 および IPv6 エージェントアドレスでの読み取り専用 MIB アクセスを許可します。プラス記号をクリックします ➕ 複数の文字列を追加します。

      管理システムが StorageGRID MIB を照会すると、コミュニティストリングが送信されます。コミュニティストリングがここで指定した値のいずれかと一致すると、 SNMP エージェントは管理システムに応答を送信します。

      各コミュニティストリングの最大文字数は 32 文字で、空白文字は使用できません。最大 5 つの文字列を指定できます。

      > ⓘ StorageGRID システムのセキュリティを確保するために、コミュニティストリングとして「 public 」を使用しないでください。コミュニティストリングを入力しない場合、 SNMP エージェントは StorageGRID システムのグリッド ID をコミュニティストリングとして使用します。

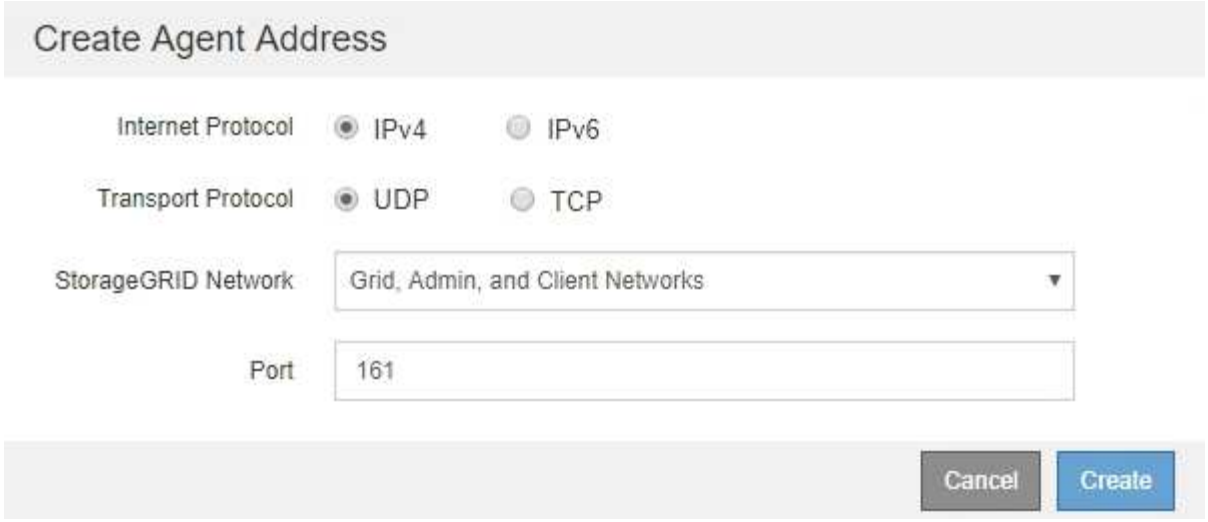
8. 必要に応じて、 Other Configurations セクションの Agent Addresses タブを選択します。

   このタブを使用して '1 つまたは複数の " リスニング・アドレス " を指定します これらは、 SNMP エージェントがクエリを受信できる StorageGRID アドレスです。各エージェントアドレスには、インターネットプロトコル、転送プロトコル、 StorageGRID ネットワーク、およびオプションでポートが含まれます。

   エージェントアドレスを設定しない場合、すべての StorageGRID ネットワーク上のデフォルトのリスニングアドレスは UDP ポート 161 です。

   a. [ 作成（ Create ） ] をクリックします。

      Create Agent Address ダイアログボックスが表示されます。




b. インターネットプロトコル * の場合は、このアドレスに IPv4 と IPv6 のどちらを使用するかを選択します。

デフォルトでは、 SNMP は IPv4 を使用します。

c. [*Transport Protocol] には、このアドレスで UDP と TCP のどちらを使用するかを選択します。

デフォルトでは、 SNMP は UDP を使用します。

d. StorageGRID Network*] フィールドで、クエリーを受信する StorageGRID ネットワークを選択します。

- グリッドネットワーク、管理ネットワーク、クライアントネットワーク： StorageGRID は、 3 つのネットワークすべてで SNMP クエリをリスンする必要があります。
- Grid ネットワーク
- 管理ネットワーク
- クライアントネットワーク

> StorageGRID とのクライアント通信のセキュリティを確保するために、クライアントネットワーク用のエージェントアドレスを作成しないでください。

e. **[Port]** フィールドには、オプションで、 SNMP エージェントがリッスンするポート番号を入力します。

SNMP エージェントのデフォルトの UDP ポートは 161 ですが、未使用のポート番号は任意に入力できます。

> SNMP エージェントを保存すると、 StorageGRID によって内部ファイアウォールのエージェントアドレスポートが自動的に開きます。これらのポートへのアクセスが外部ファイアウォールで許可されていることを確認してください。

f. [ 作成（ Create ） ] をクリックします。

エージェントアドレスが作成され、テーブルに追加されます。

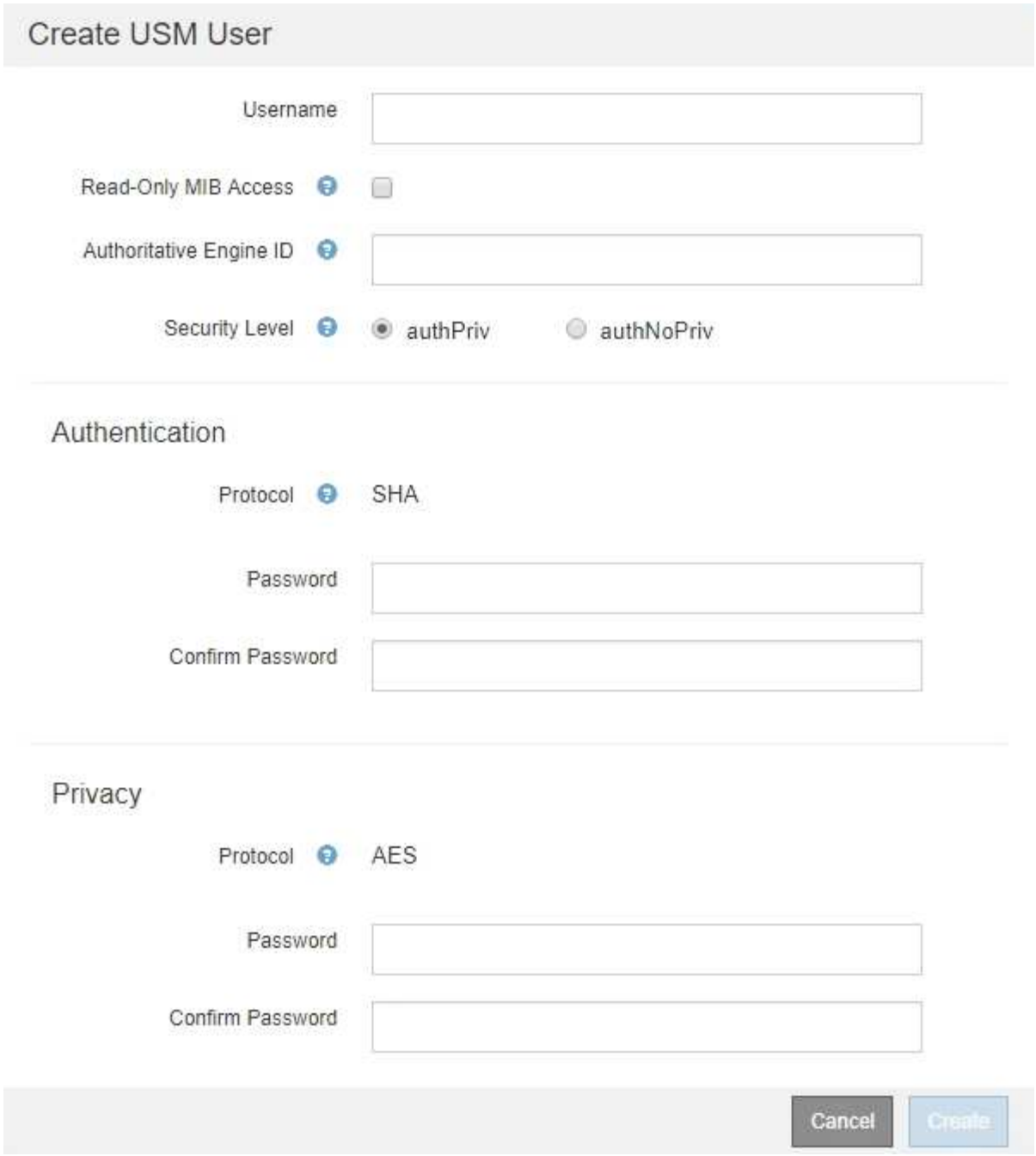
9. SNMPv3 を使用している場合は、 Other Configurations セクションの USM Users タブを選択します。

   このタブを使用して、 MIB の照会またはトラップおよびインフォームの受信を許可されている USM ユーザを定義します。

   この手順は、 SNMPv1 または SNMPv2c のみを使用している場合は適用されません。

   a. [ 作成（ Create ） ] をクリックします。

      [Create USM User] ダイアログボックスが表示されます。




b. この USM ユーザの一意の * ユーザ名 * を入力します。

ユーザ名の最大文字数は 32 文字で、空白文字は使用できません。ユーザ名は作成後に変更することはできません。

c. このユーザに MIB への読み取り専用アクセス権が必要な場合は、 [* Read-Only MIB Access] チェックボックスをオンにします。

[**Read-Only MIB Access**] を選択すると、 [**Authoritative Engine ID**] フィールドは無効になります。

読み取り専用 MIB アクセスが設定された USM ユーザは、エンジン ID を取得できません。

d. このユーザを INFORM 宛先で使用する場合は、このユーザの権限のあるエンジン ID * を入力しま

す。

SNMPv3 インフォームの送信先には、エンジン ID を持つユーザが必要です。SNMPv3 トラップの送信先にエンジン ID を持つユーザを含めることはできません。

信頼できるエンジン ID は、 16 進数で 5 ～ 32 バイトです。

e. USM ユーザのセキュリティレベルを選択します。

- * authPriv * ：認証とプライバシー（暗号化）と通信します。認証プロトコルとパスワード、およびプライバシープロトコルとパスワードを指定する必要があります。
- * authNoPriv * ：このユーザは認証と通信し、プライバシーはありません（暗号化なし）。認証プロトコルとパスワードを指定する必要があります。

f. このユーザが認証に使用するパスワードを入力し、確認のためにもう一度入力します。

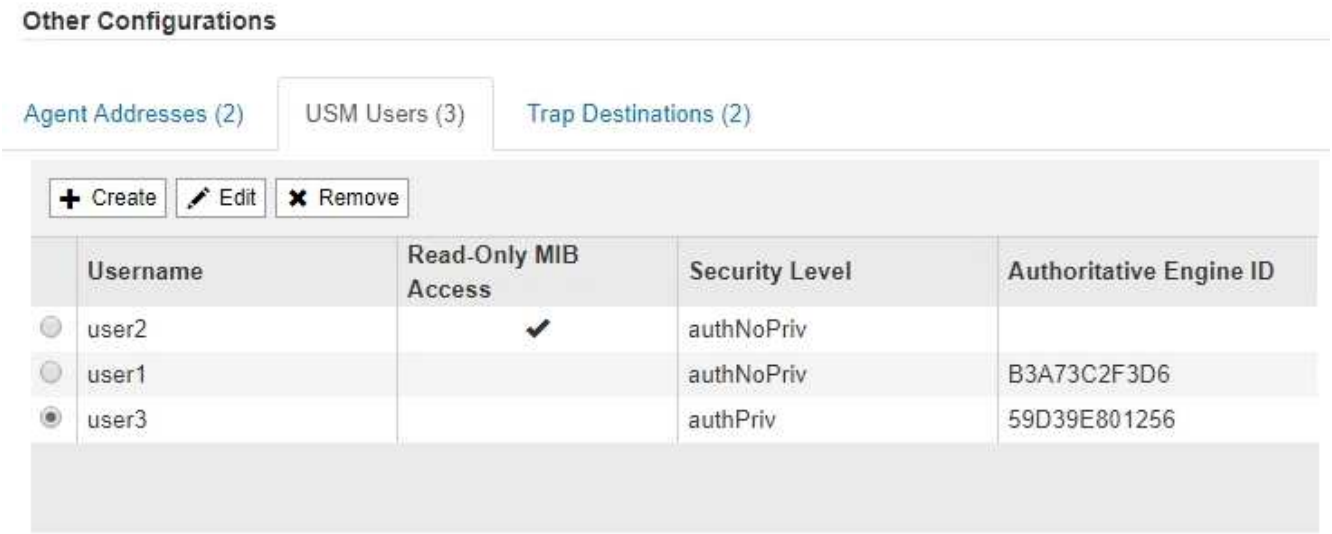
サポートされている認証プロトコルは SHA （ HMAC-SHA-96 ）だけです。

g. [**authPriv**] を選択した場合は、このユーザがプライバシーに使用するパスワードを入力し、確認します。

サポートされているプライバシープロトコルは AES のみです。

h. [ 作成（ Create ） ] をクリックします。

USM ユーザが作成され、テーブルに追加されます。

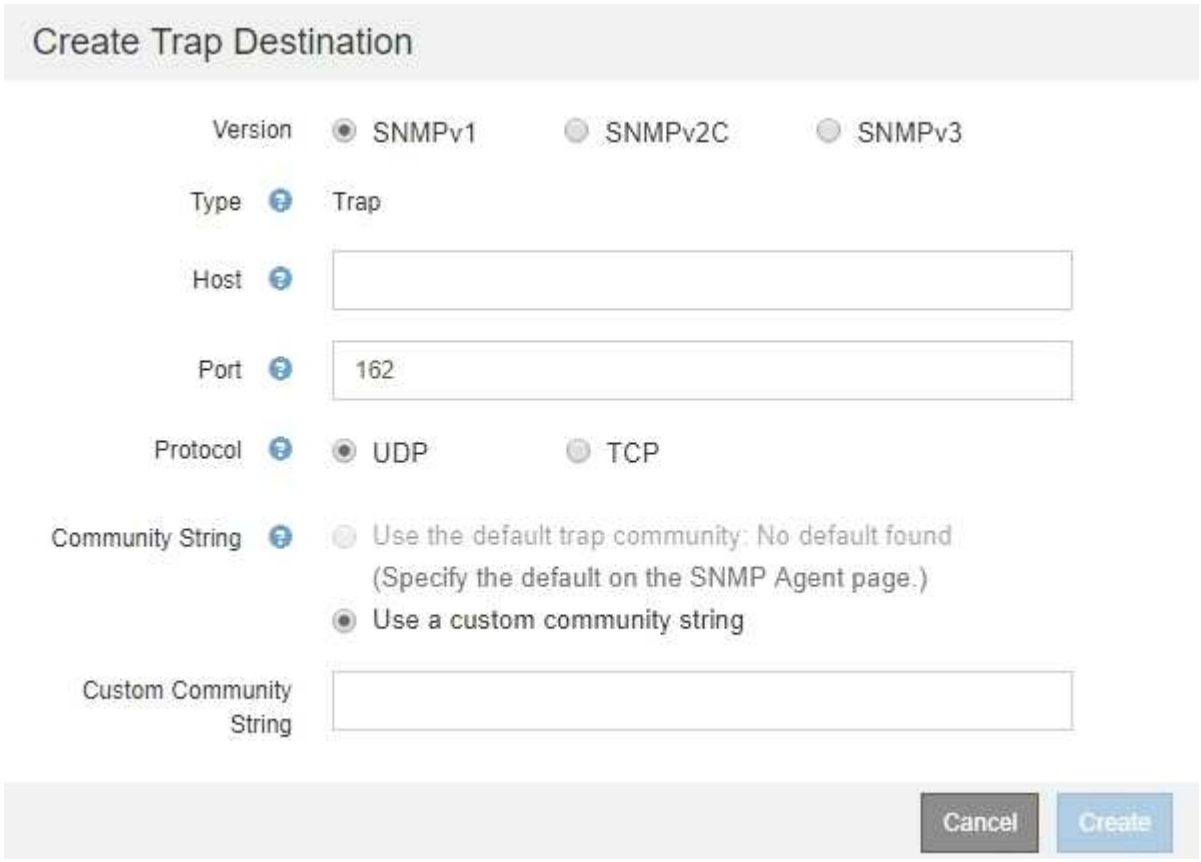



10. [その他の設定]セクションで、[トラップ送信先]タブを選択します。

トラップ送信先タブでは、 StorageGRID トラップまたは通知の送信先を 1 つ以上定義できます。SNMP エージェントを有効にして * Save * をクリックすると、 StorageGRID は定義された各宛先への通知の送信を開始します。通知は、アラートとアラームがトリガーされたときに送信されます。標準通知は、サポートされている MIB-II エンティティ（ ifdown や coldStart など）についても送信されます。

a. [ 作成（ Create ） ] をクリックします。

トラップ送信先の作成ダイアログボックスが表示されます。




b. [* Version] フィールドで、この通知に使用する SNMP バージョンを選択します。

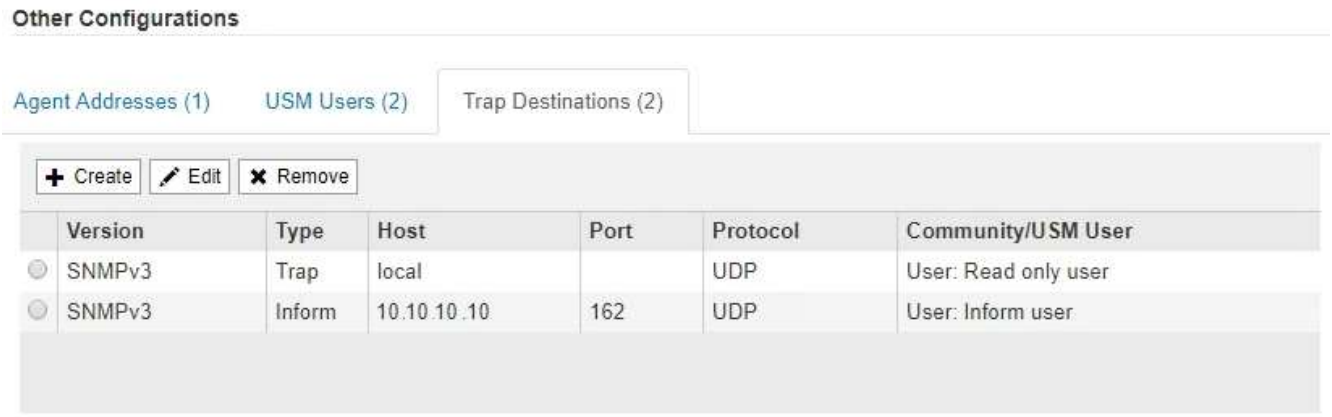
c. 選択したバージョンに応じて、フォームに入力します

| バージョン | この情報を指定します |
| --- | --- |
| SNMPv1 | • 注： SNMPv1 の場合、 SNMP エージェントはトラップのみを送信できます。インフォームはサポートされません。<br>i. [* Host*] フィールドに、トラップを受信する IPv4 または IPv6 アドレス（または FQDN ）を入力します。<br>ii. * Port * には、別の値を使用する必要がある場合を除き、デフォルト（ 162 ）を使用してください。（ 162 は SNMP トラップの標準ポートです）。<br>iii. **Protocol** には、デフォルト（ UDP ）を使用します。TCP もサポートされています。（ UDP は標準の SNMP トラッププロトコルです）。<br>iv. SNMP Agent ページでトラップコミュニティが指定されている場合は、デフォルトのトラップコミュニティを使用するか、このトラップ送信先のカスタムコミュニティストリングを入力します。<br>カスタムコミュニティストリングの最大文字数は 32 文字で、空白を含めることはできません。 |

| バージョン | この情報を指定します |
| --- | --- |
| SNMPv2c の場合 | i. トラップまたはインフォームに宛先を使用するかどうかを選択します。<br>ii. [* Host*] フィールドに、トラップを受信する IPv4 または IPv6 アドレス（または FQDN ）を入力します。<br>iii. * Port * には、別の値を使用する必要がある場合を除き、デフォルト（ 162 ）を使用してください。（ 162 は SNMP トラップの標準ポートです）。<br>iv. **Protocol** には、デフォルト（ UDP ）を使用します。TCP もサポートされています。（ UDP は標準の SNMP トラッププロトコルです）。<br>v. SNMP Agent ページでトラップコミュニティが指定されている場合は、デフォルトのトラップコミュニティを使用するか、このトラップ送信先のカスタムコミュニティストリングを入力します。<br><br>カスタムコミュニティストリングの最大文字数は 32 文字で、空白を含めることはできません。 |
| SNMPv3 | i. トラップまたはインフォームに宛先を使用するかどうかを選択します。<br>ii. [* Host*] フィールドに、トラップを受信する IPv4 または IPv6 アドレス（または FQDN ）を入力します。<br>iii. * Port * には、別の値を使用する必要がある場合を除き、デフォルト（ 162 ）を使用してください。（ 162 は SNMP トラップの標準ポートです）。<br>iv. **Protocol** には、デフォルト（ UDP ）を使用します。TCP もサポートされています。（ UDP は標準の SNMP トラッププロトコルです）。<br>v. 認証に使用する USM ユーザを選択します。<br>◦ [*Trap] を選択した場合は、権限のあるエンジン ID を持たない USM ユーザだけが表示されます。<br>◦ *INFORM を選択した場合は、権限のあるエンジン ID を持つ USM ユーザのみが表示されます。 |

d. [ 作成（ Create ） ] をクリックします。

トラップの送信先が作成され、テーブルに追加されます。




11. SNMP エージェントの設定が完了したら、 * Save * をクリックします

新しい SNMP エージェント設定がアクティブになります。

関連情報

"アラート通知のサイレント化"

**SNMP**エージェントを更新しています

## SNMP 通知の無効化、コミュニティストリングの更新、エージェントアドレス、 USM ユーザ、トラップの送信先の追加や削除を行うことができます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限が必要です。

このタスクについて

SNMPエージェント設定を更新する場合は、[SNMP Agent]ページの下部にある[*Save]をクリックして、各タブで行った変更をコミットする必要があります。

手順

1. * Configuration > Monitoring > SNMP Agent *を選択します。

SNMP Agent ページが表示されます。

2. すべてのグリッドノードで SNMP エージェントを無効にする場合は、 * SNMP を有効にする * チェックボックスをオフにして、 * 保存 * をクリックします。

SNMP エージェントはすべてのグリッドノードで無効になっています。あとでエージェントを再度有効にした場合、以前の SNMP 設定は保持されます。

3. 必要に応じて、入力した値を * System Contact * および * System Location * で更新します。

4. StorageGRID SNMP エージェントがトラップおよびインフォーム通知を送信しないようにするには、必要に応じて、 [SNMP エージェント通知を有効にする *] チェックボックスをオフにします。

   このチェックボックスをオフにすると、 SNMP エージェントは読み取り専用 MIB アクセスをサポートしますが、 SNMP 通知は送信しません。

5. 認証されていないプロトコルメッセージを StorageGRID SNMP エージェントが受信したときに認証トラップを送信しないようにするには、必要に応じて、 [ 認証トラップを有効にする *] チェックボックスをオフにします。

6. SNMPv1 または SNMPv2c を使用する場合は、必要に応じてコミュニティストリングセクションを更新します。

   このセクションのフィールドは、 SNMPv1 または SNMPv2c でのコミュニティベースの認証に使用されます。これらのフィールドは SNMPv3 には適用されません。

   デフォルトのコミュニティストリングを削除する場合は、最初にすべてのトラップ送信先でカスタムのコミュニティストリングを使用する必要があります。

7. エージェントアドレスを更新する場合は、 [ その他の設定 ] セクションの [ エージェントアドレス ] タブを選択します。

   このタブを使用して '1 つまたは複数の " リスニング・アドレス " を指定します これらは、 SNMP エージェントがクエリを受信できる StorageGRID アドレスです。各エージェントアドレスには、インターネットプロトコル、転送プロトコル、 StorageGRID ネットワーク、ポートが含まれます。

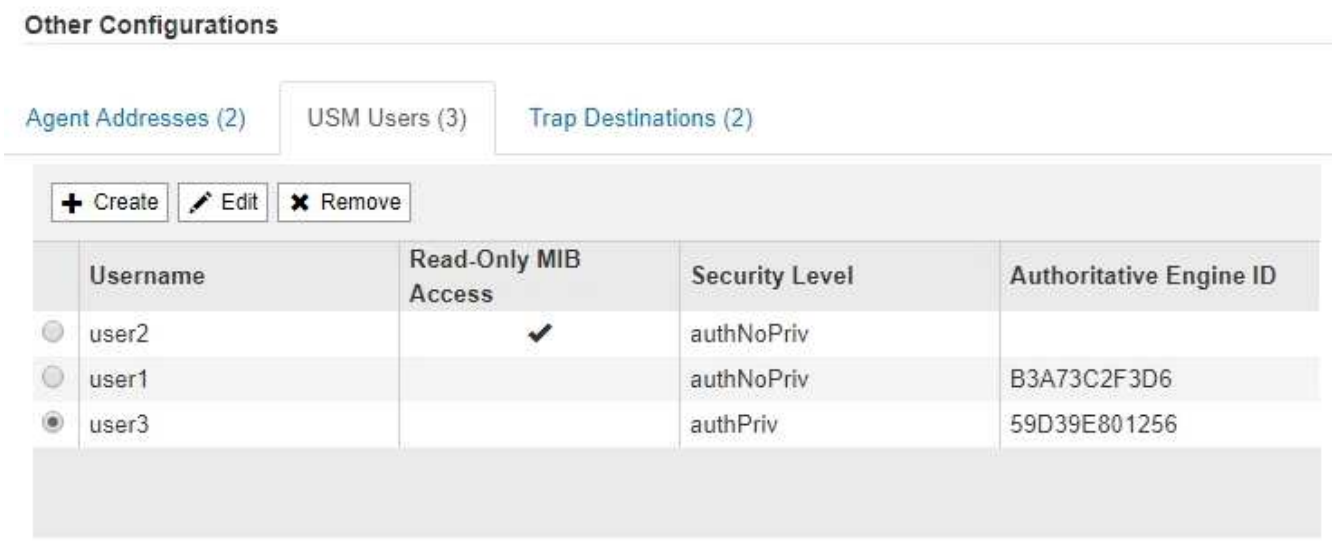
   a. エージェントアドレスを追加するには、 * 作成 * をクリックします。次に、 SNMP エージェントの設定手順に記載されているエージェントアドレスの手順を参照してください。

   b. エージェントアドレスを編集するには、アドレスのラジオボタンを選択し、 * Edit * をクリックします。次に、 SNMP エージェントの設定手順に記載されているエージェントアドレスの手順を参照してください。

   c. エージェントアドレスを削除するには、アドレスのラジオボタンを選択し、 * 削除 * をクリックします。次に、 [OK] をクリックして、このアドレスを削除することを確認します。

   d. 変更をコミットするには、 SNMP Agent ページの下部にある **Save** をクリックします。

8. USM ユーザを更新するには、 Other Configurations セクションで USM Users タブを選択します。




このタブを使用して、 MIB の照会またはトラップおよびインフォームの受信を許可されている USM ユーザを定義します。

a. USM ユーザを追加するには、 * Create * をクリックします。次に、 SNMP エージェントの設定手順の USM ユーザ向けの手順を参照してください。

b. USM ユーザを編集するには、ユーザのオプションボタンを選択し、 * Edit * をクリックします。次に、 SNMP エージェントの設定手順の USM ユーザ向けの手順を参照してください。

   既存の USM ユーザのユーザ名は変更できません。ユーザ名を変更する必要がある場合は、ユーザを削除して新しいユーザを作成する必要があります。

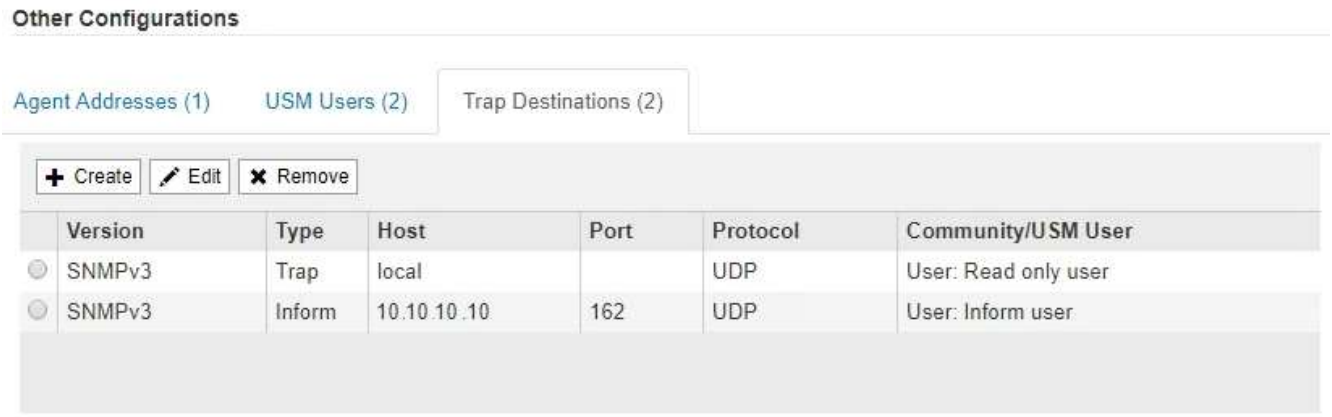
   ユーザの権限のあるエンジン ID を追加または削除した場合、そのユーザが現在デスティネーションに対して選択されているときは、手順の説明に従って、デスティネーションを編集または削除する必要があります SNMP トラップの送信先。そうしないと、 SNMP エージェント設定を保存したときに検証エラーが発生します。

c. USM ユーザを削除するには、ユーザのオプションボタンを選択し、 * Remove * をクリックします。次に、 [OK] をクリックして、このユーザーを削除することを確認します。

   削除したユーザがトラップの送信先として選択されている場合は、手順の説明に従って、送信先を編集または削除する必要があります SNMP トラップの送信先。そうしないと、 SNMP エージェント設定を保存したときに検証エラーが発生します。

a. 変更をコミットするには、 SNMP Agent ページの下部にある **Save** をクリックします。

1. トラップ送信先を更新する場合は、[その他の設定]セクションの[トラップ送信先]タブを選択します。




トラップ送信先タブでは、 StorageGRID トラップまたは通知の送信先を 1 つ以上定義できます。SNMP エージェントを有効にして * Save * をクリックすると、 StorageGRID は定義された各宛先への通知の送信を開始します。通知は、アラートとアラームがトリガーされたときに送信されます。標準通知は、サポートされている MIB-II エンティティ（ ifdown や coldStart など）についても送信されます。

a. トラップ送信先を追加するには、 * 作成 * をクリックします。次に、 SNMP エージェントの設定手順のトラップ送信先の手順を参照してください。

b. トラップ送信先を編集するには、ユーザのオプションボタンを選択し、 * Edit * をクリックします。次に、 SNMP エージェントの設定手順のトラップ送信先の手順を参照してください。

c. トラップ送信先を削除するには、送信先のオプションボタンを選択し、 * Remove * （削除）をクリックします。次に、 [OK] をクリックして、この宛先を削除することを確認します。

d. 変更をコミットするには、 SNMP Agent ページの下部にある **Save** をクリックします。

2. SNMP エージェント設定を更新したら、 * Save * をクリックします。

関連情報

"SNMPエージェントの設定"

## 追加の**StorageGRID** データを収集しています

データを収集および分析する方法はほかにもいくつかあり、StorageGRID システムの状態を調査する場合や、テクニカルサポートと協力して問題を解決する場合に役立ちます。

- "グラフとレポートを使用する"
- "PUTおよびGETパフォーマンスの監視"
- "オブジェクト検証処理を監視します"
- "イベントの監視"
- "監査メッセージの確認"
- "ログファイルとシステムデータを収集しています"

- "手動でのAutoSupport メッセージのトリガー"
- "グリッドトポロジツリーの表示"
- "サポート指標の確認"
- "診断の実行"
- "カスタムの監視アプリケーションを作成する"

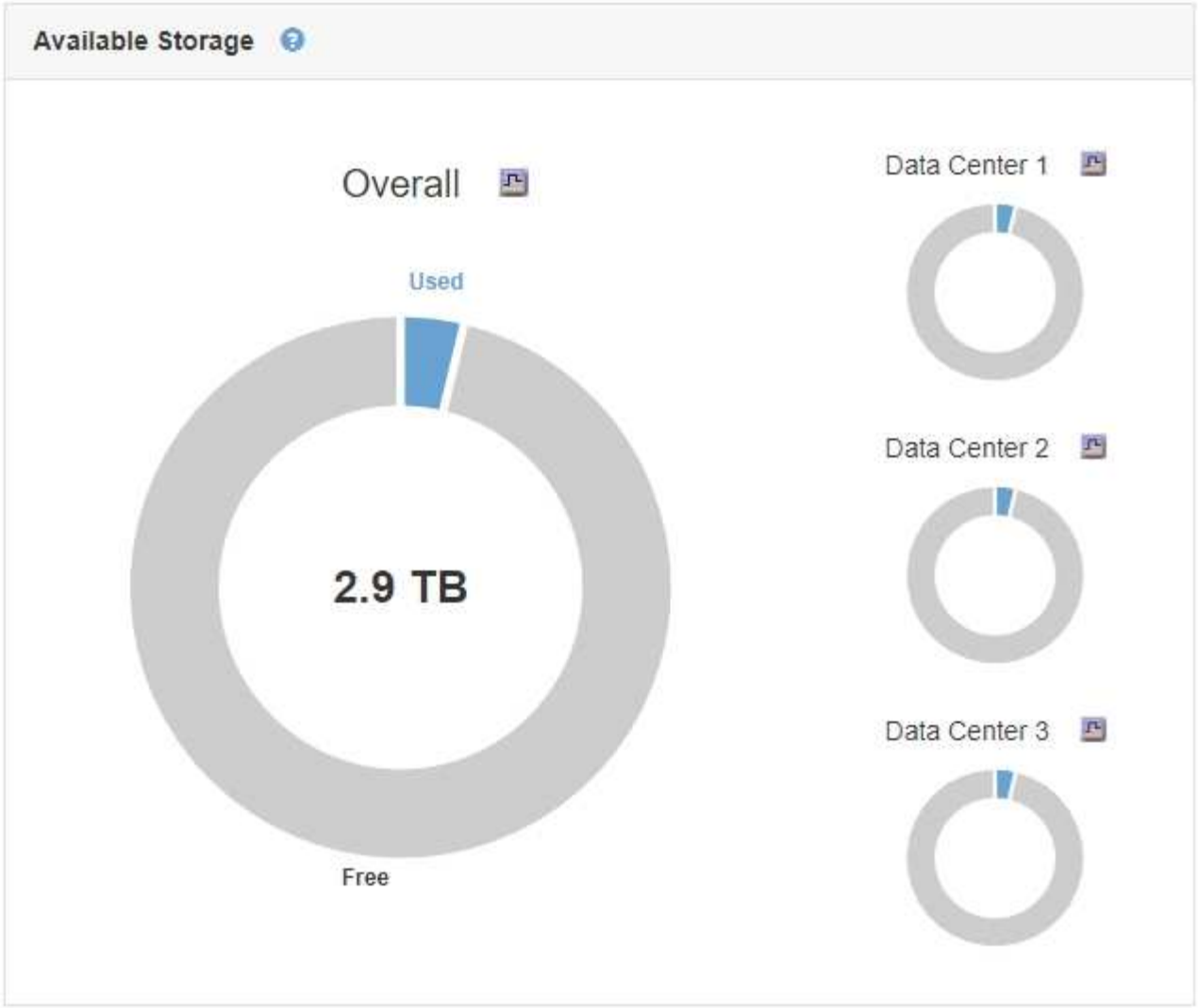
グラフとレポートを使用する

# グラフやレポートを使用して、 StorageGRID システムの状態を監視し、問題のトラブルシューティングを行うことができます。Grid Managerで使用できるグラフとレポートのタイプには、円グラフ（ダッシュボードのみ）、グラフ、テキストレポートがあります。

グラフとグラフの種類

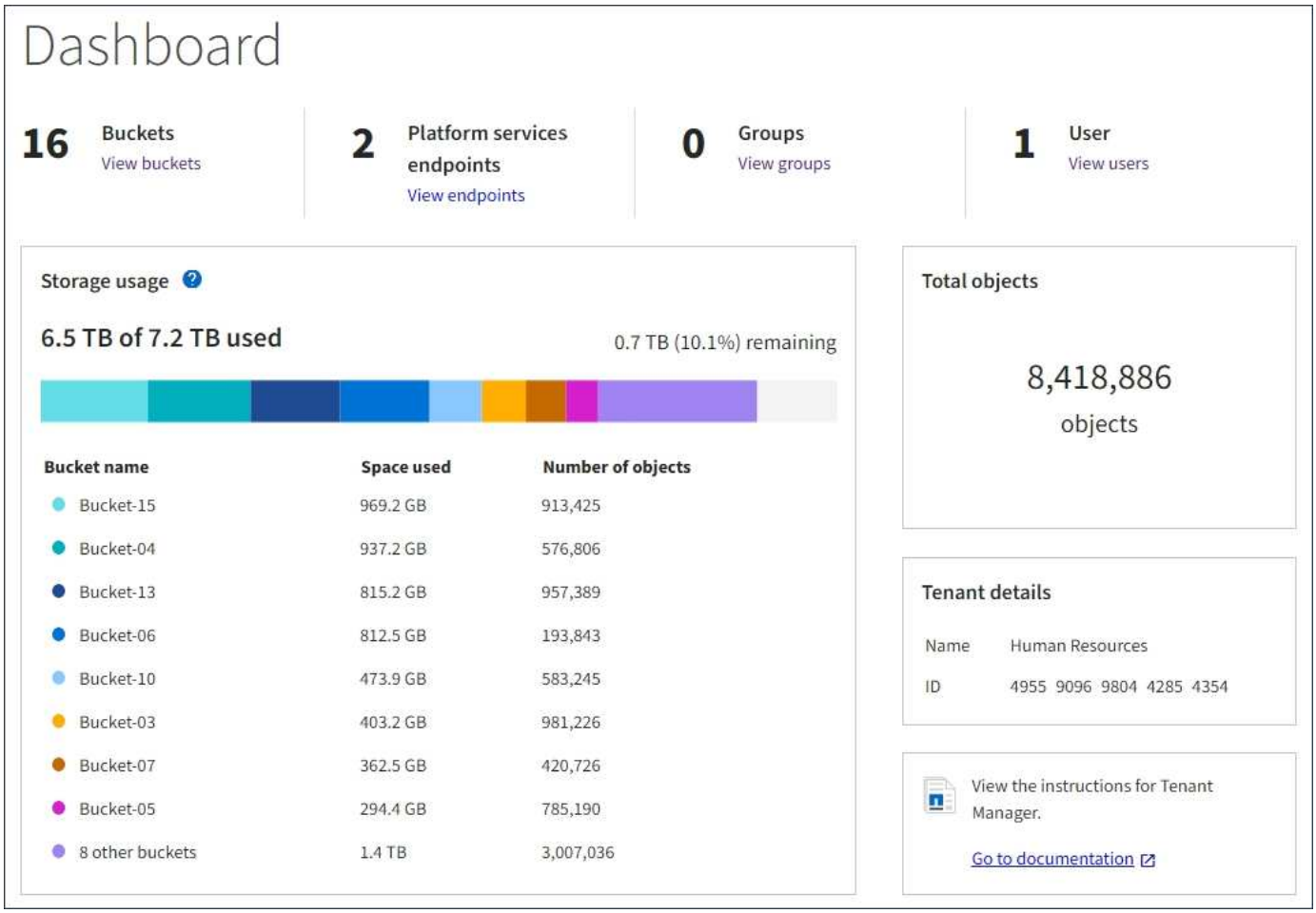
## グラフには、特定の StorageGRID 指標や属性の値がまとめて表示されます。

Grid Managerのダッシュボードには、グリッドと各サイトで利用可能なストレージをまとめた円グラフ（ドーナツグラフ）が表示されます。




Tenant Manager のダッシュボードの Storage usage パネルには、次の情報が表示されます。

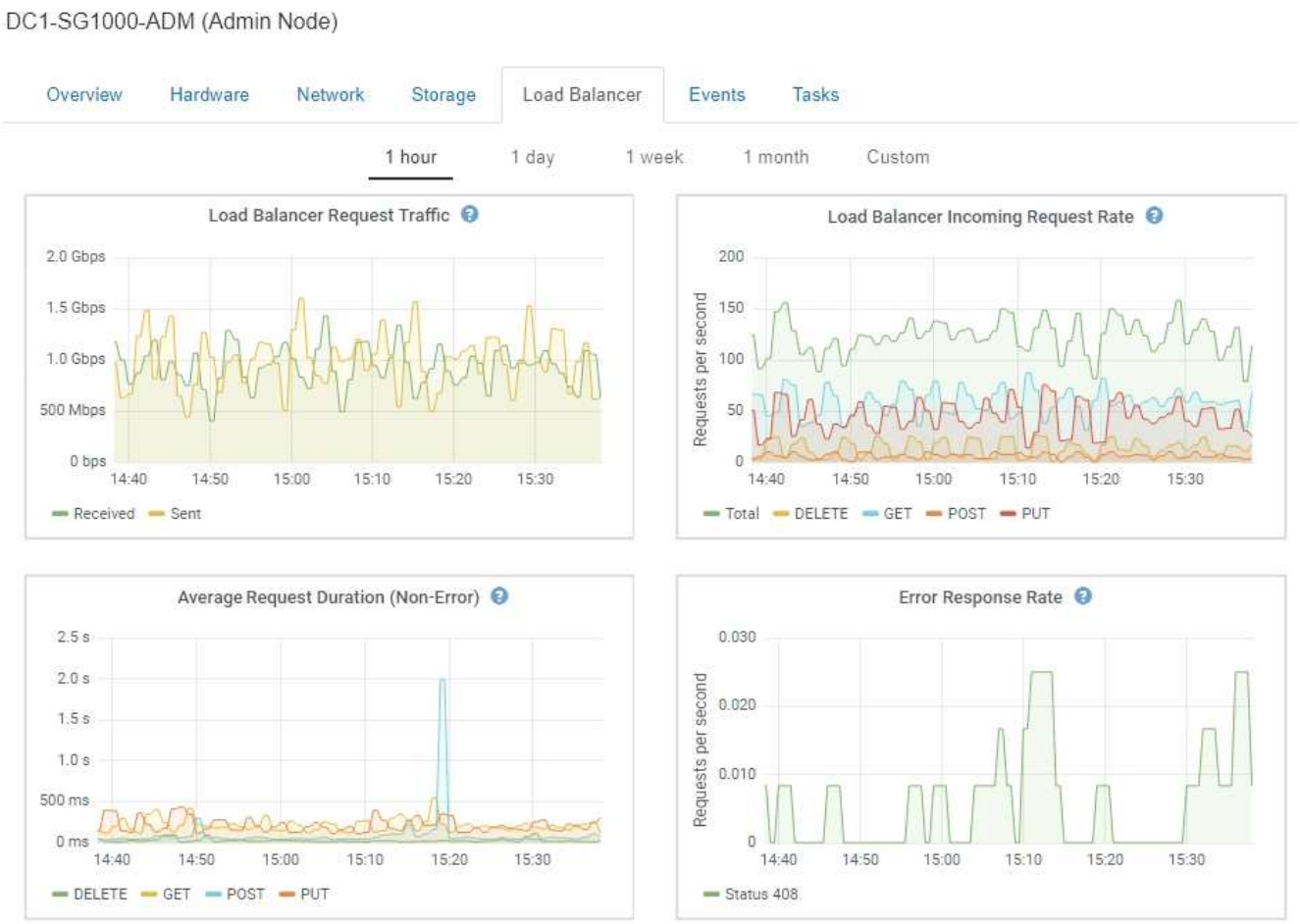
- テナントの最大バケット（ S3 ）またはコンテナ（ Swift ）のリスト
- 最大のバケットまたはコンテナの相対サイズを表す棒グラフ
- 使用済みスペースの合計。クォータが設定されている場合は、残りのスペースの量と割合




また、StorageGRID の指標や属性の変化を示すグラフは、Nodesページと* Support > Tools > Grid Topology *ページからも参照できます。

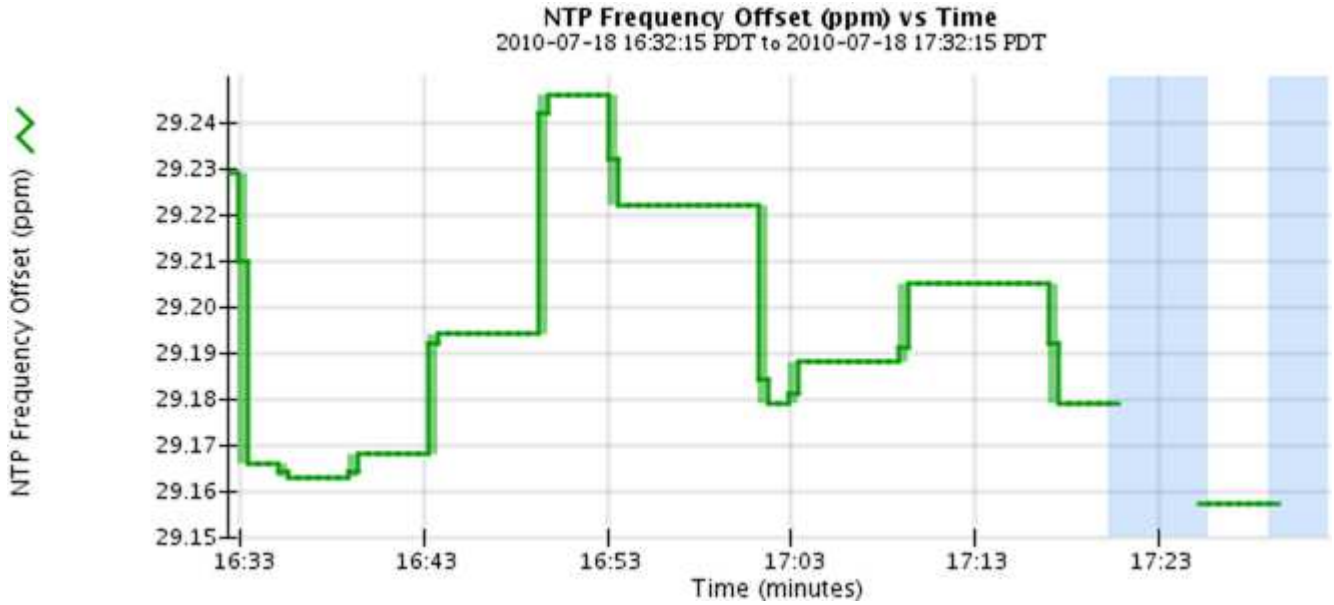
グラフには次の 4 種類があります。

- * Grafana チャート * ：ノードページで表示される、 Grafana チャートは、時間の経過に伴う Prometheus 指標の値のプロットに使用されます。たとえば、管理ノードの* Nodes > Load Balancer *タブには、4つのGrafanaチャートが含まれています。

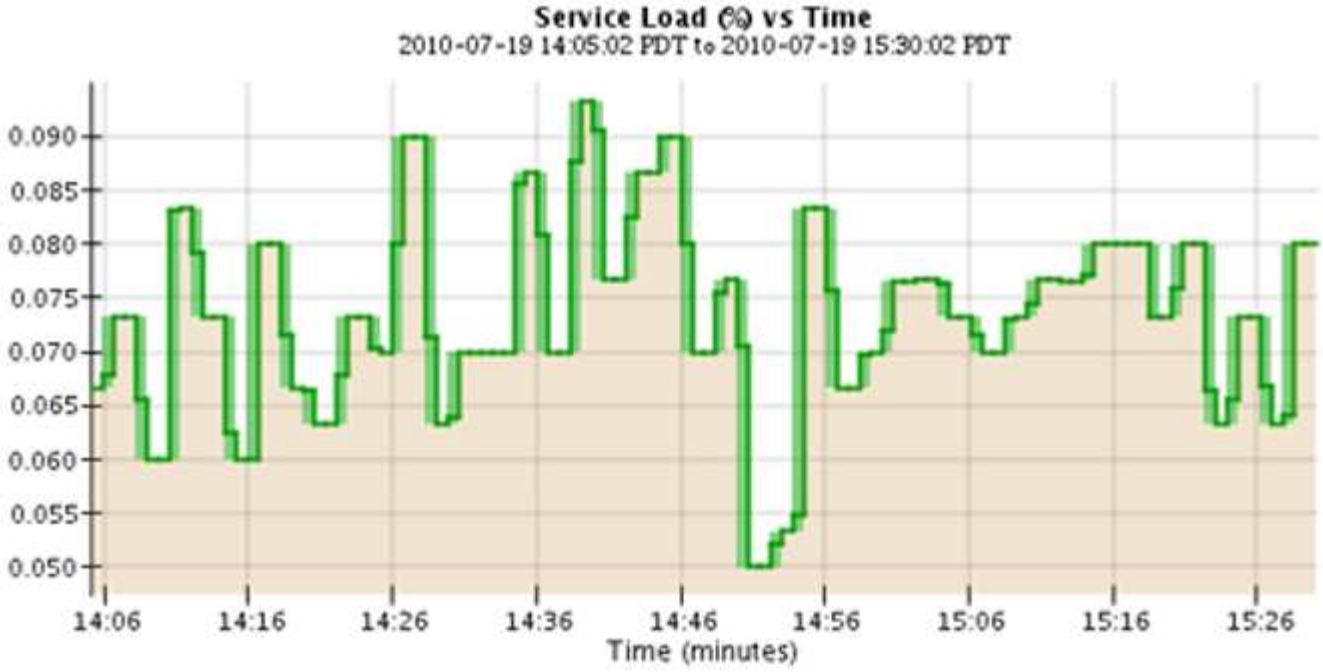



Grafanaチャートは、* Support > Tools > Metrics *ページで使用可能な事前構築済みのダッシュボードにも含まれています。

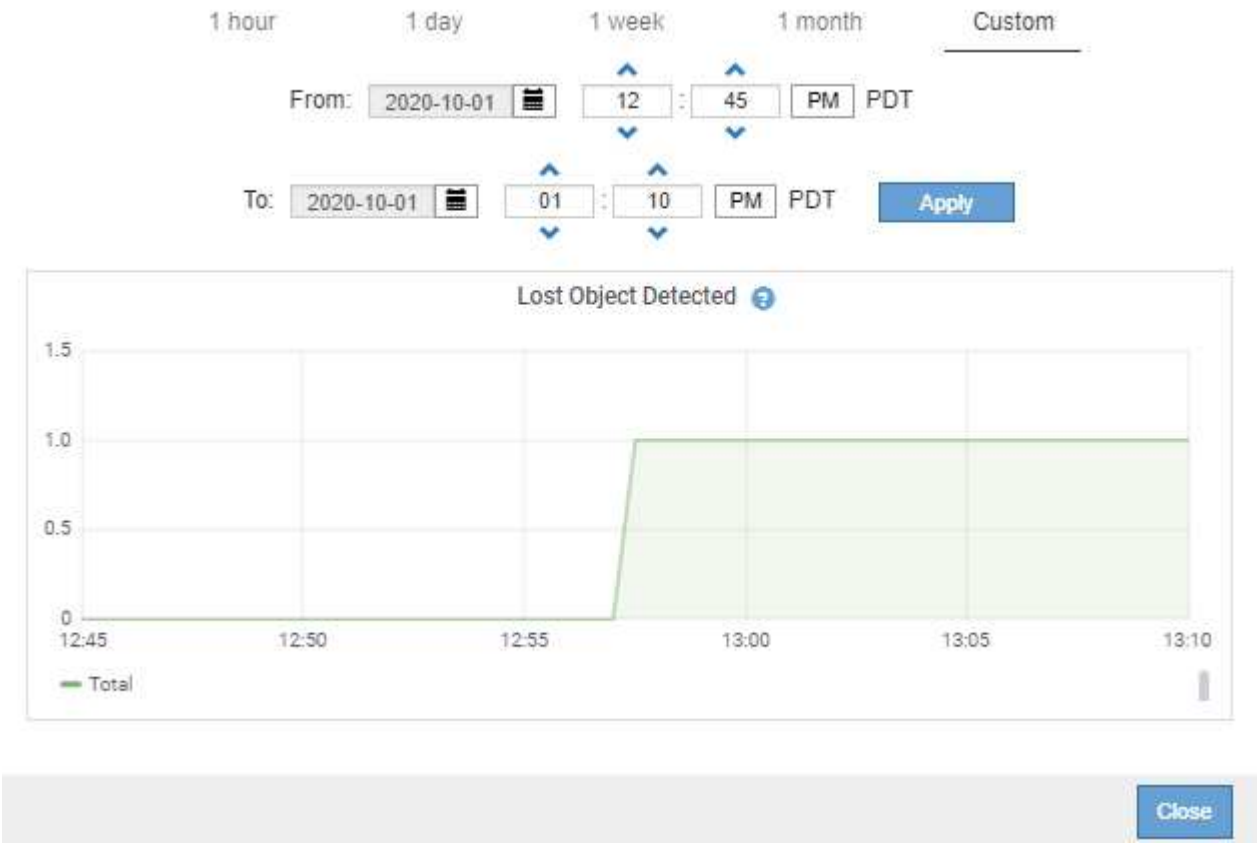
- 折れ線グラフ：ノードページおよび* Support > Tools > Grid Topology *ページ（グラフアイコンをクリック）で使用できます データ値のあとに線グラフを使用して、単位値（ NTP 周波数オフセットの ppm など）を含む StorageGRID 属性の値がプロットされます。値の変化が時間の経過に合わせて一定の間隔でプロットされます。



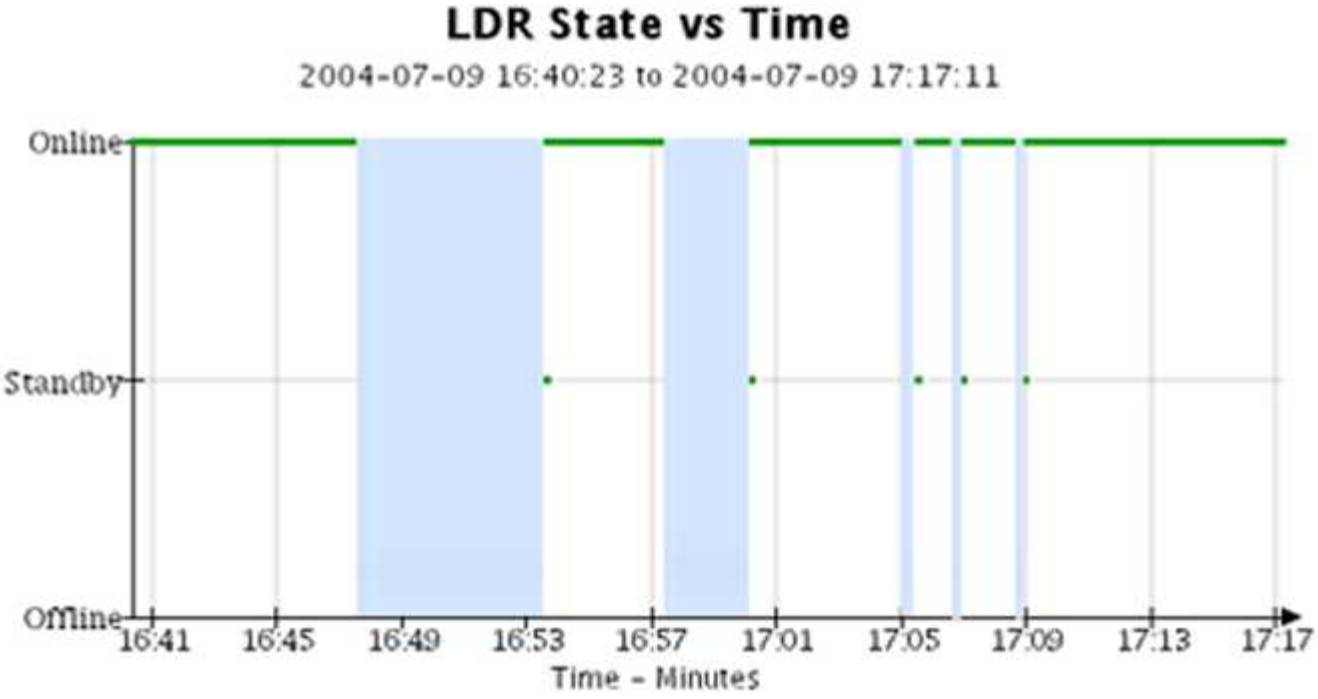
- 面グラフ：ノードページまたは*サポート*>*ツール*>*グリッドトポロジ*ページ（グラフアイコンをクリック）で確認できます データ値のあとに）オブジェクト数やサービスの負荷の値など、容量の属性値のプロットには面グラフが使用されます。面グラフは折れ線グラフに似ていますが、線の下の部分の背景が薄い茶色になります。値の変化が時間の経過に合わせて一定の間隔でプロットされます。




- グラフの中には、別の種類のグラフアイコンで示されるものもあります また、形式が異なります。



- 状態グラフ：サポート*>*ツール*>*グリッドトポロジ*ページで使用できます（グラフアイコンをクリックします） データ値のあとに）状態グラフを使用して、オンライン、スタンバイ、オフラインのいずれかの状態を表す属性値がプロットされます。状態グラフは折れ線グラフに似ていますが、値が連続しておらず、別の状態に切り替わると値が飛んで表示されます。




関連情報

"Nodesページを表示します"

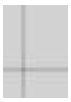
"グリッドトポロジツリーの表示"

"サポート指標の確認"

グラフの凡例

## グラフの描画に使用される線と色には特定の意味があります。

| サンプル | 意味 |
| --- | --- |
|  | レポートされる属性値は濃い緑の線でプロットされます。 |
| | 濃い緑の線の背景の薄い緑は、その時間範囲の実際の値が異なることを示します。また、描画を高速化するために「ビンニング」されています。濃い線は加重平均を表し、薄い緑は最大値から最小値までの範囲を示します。薄い茶色の背景は面グラフで累計データを示すために使用されます。 |

| サンプル | 意味 |
| --- | --- |
|  | データがプロットされていない空白の部分は、属性値が使用できなかったことを示します。背景色は、属性をレポートするサービスの状態に応じて、青、グレー、またはグレーと青の中間色になります。 |
|  | 薄い青の背景は、サービスの状態が不明なため属性値がレポートされず、一部またはすべての属性値を特定できなかった時間範囲を示します。 |
|  | グレーの背景は、属性をレポートするサービスが管理上の理由で停止しているために、一部またはすべての属性値を取得できなかった時間範囲を示します。 |
| | グレーと青の中間色の背景は、サービスの状態が不明なために属性値を特定できなかったか、属性をレポートするサービスが管理上の理由で停止しているために属性値を取得できなかった時間範囲を示します。 |

グラフやグラフの表示

# ノードページには、ストレージ容量やスループットなどの属性を監視するために定期的にアクセスする必要があるグラフやグラフが表示されます。一部のケース、特にテクニカルサポートと一緒に作業しているときに、* Support > Tools > Grid Topology *ページを使用して追加のチャートにアクセスできます。

必要なもの

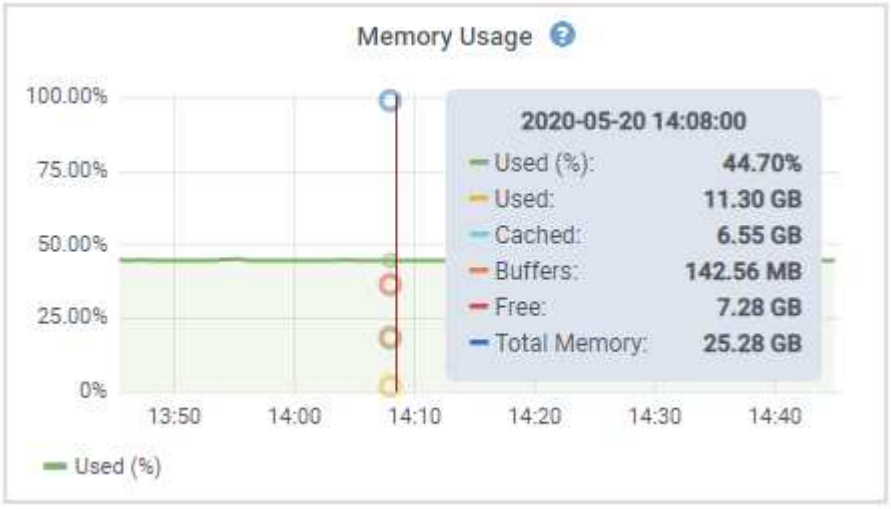
Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

手順

1. [ノード（ Nodes）]を選択し次に、ノード、サイト、またはグリッド全体を選択します。
2. 情報を表示するタブを選択します。

   一部のタブには、 Prometheus 指標の値の経時的プロットに使用される 1 つ以上の Grafana チャートがあります。たとえば、ノードの* Nodes > Hardware *タブには、2つのGrafanaチャートがあります。

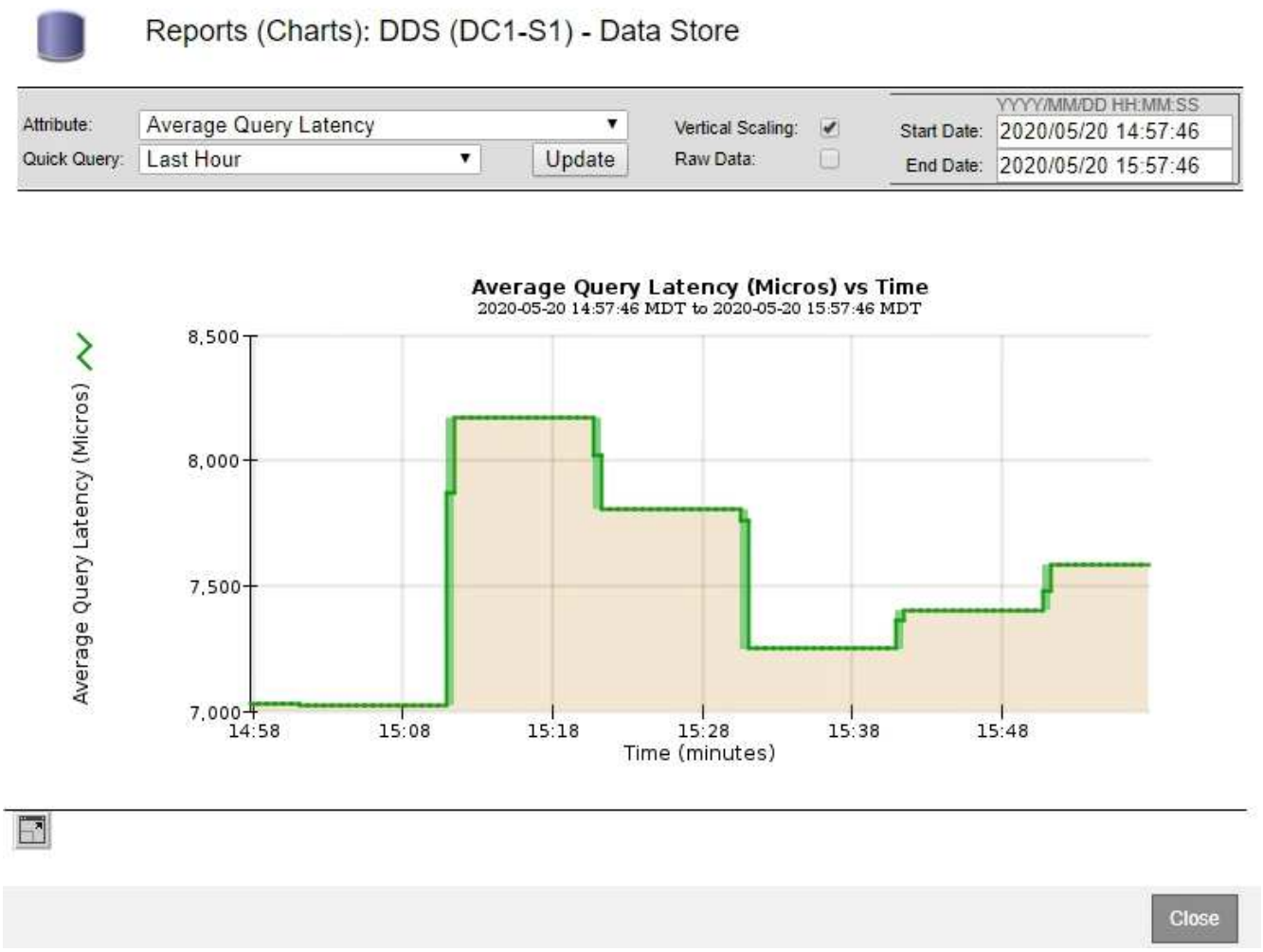
3. 必要に応じて、グラフにカーソルを合わせると特定の時点における詳細な値が表示されます。



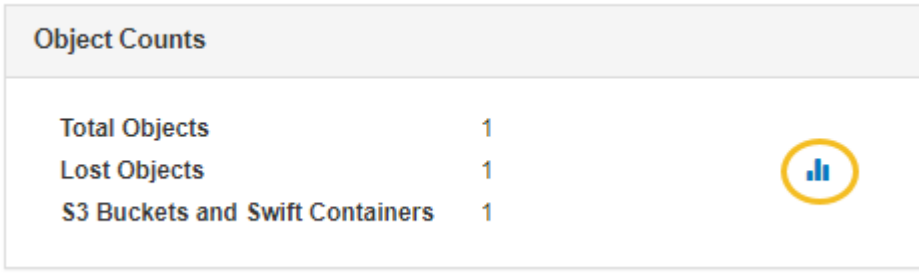

4. 必要に応じて、特定の属性や指標のグラフを表示することもできます。ノードページのテーブルで、グラフアイコンをクリックします または をクリックします。

> 一部の指標および属性に対してチャートを使用することはできません。

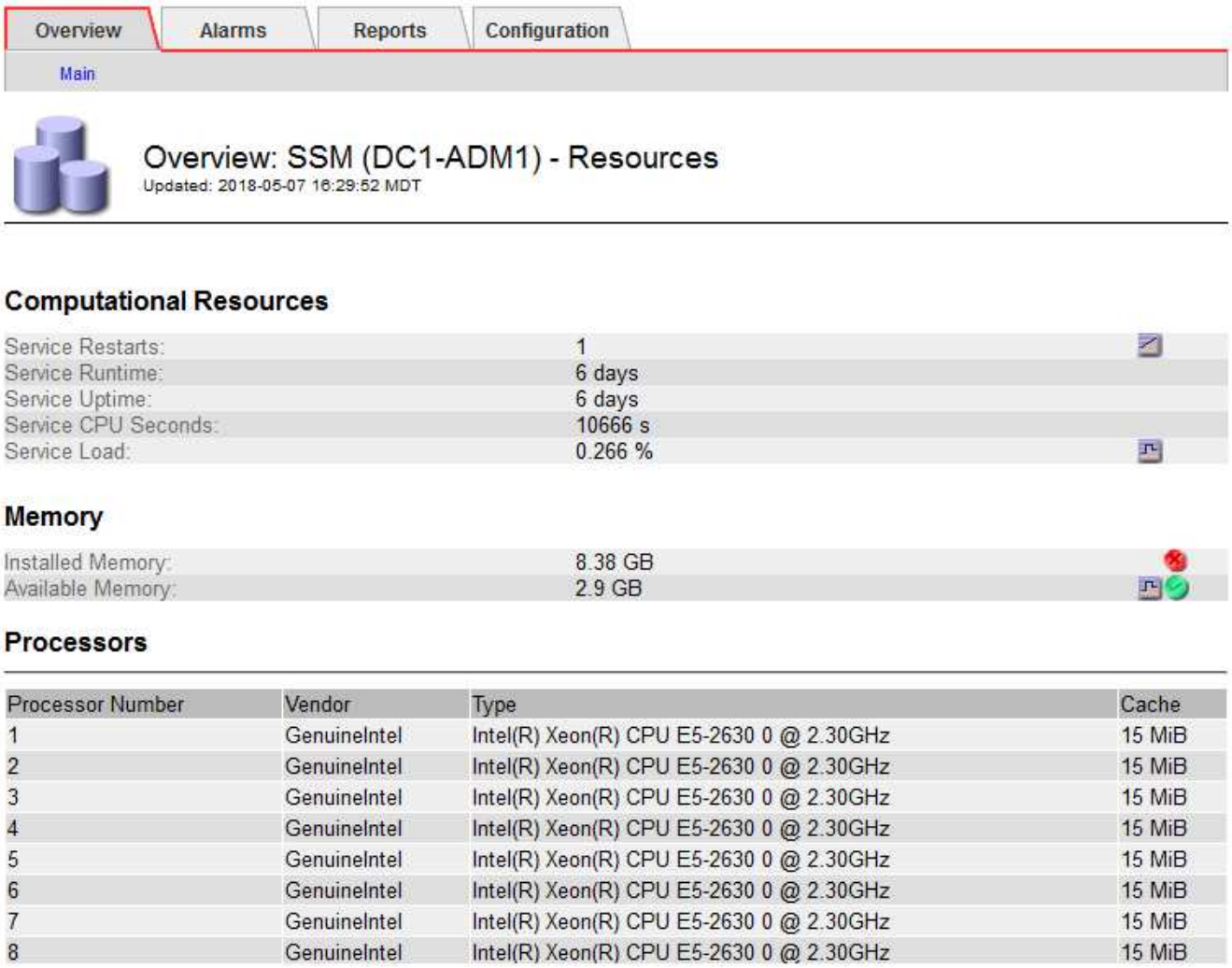
*例1 *：ストレージノードの[オブジェクト]タブで、グラフアイコンをクリックします をクリックすると、ある期間におけるメタデータクエリの平均レイテンシが表示されます。




*例2 *：ストレージノードの[オブジェクト]タブで、グラフアイコンをクリックします 一定の期間に検出された損失オブジェクトの数の Grafana グラフを確認する場合。



5. ノードページに表示されない属性のグラフを表示するには、* Support **>** Tools **>** Grid Topology *を選択します。
6. ***grid node***>**component* または *SERVICE*>* Overview **>** Main * を選択します。




7. グラフアイコンをクリックします をクリックします。

   表示は自動的に * Reports * > * Charts * ページに変わります。このグラフには、過去 1 日間の属性のデータが表示されます。

グラフの生成

# グラフには、属性データ値がグラフィカルな形式で表示されます。データセンターサイト、グリッドノード、コンポーネント、またはサービスについてのレポートを作成できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

手順

1. Support **>** Tools **>** Grid Topology *を選択します。
2. ***grid node***>**component* または *SERVICE*>* Reports **>** Charts * を選択します。
3. [* 属性 * （ * Attribute * ） ] ドロップダウンリストからレポートする属性を選択します。

4. Y 軸をゼロから開始するには、 [ 垂直スケーリング * （ Vertical Scaling * ） ] チェックボックスの選択を解除します。
5. 完全精度で値を表示するには、 * 生データ * チェックボックスをオンにするか、小数点以下の桁数を最大 3 桁まで（パーセント値としてレポートされた属性など）丸めを行うには、 * 生データ * チェックボックスの選択を解除します。
6. [*Quick Query] ドロップダウン・リストから、レポートする期間を選択します。

   カスタムクエリオプションを選択して、特定の期間を選択します。

   グラフが表示されるまでに少し時間がかかります。期間が長い場合は集計に数分かかることもあります。
7. [ カスタムクエリ ] を選択した場合は、 [ 開始日 ] と [ 終了日 ] を入力してグラフの期間をカスタマイズします。

   の形式を使用します *YYYY/MM/DDHH:MM:SS* 現地時間。この形式に一致するには、先頭にゼロを補う必要があります。たとえば、「 2017/4/6 7 ： 30 ： 00 」と入力すると検証に失敗します。正しい形式は「 2017/04/06 07 ： 30 ： 00 」です。
8. [ 更新（ Update ） ] をクリックします。

   グラフが生成されるまでに少し時間がかかります。期間が長い場合は集計に数分かかることもあります。クエリで設定した時間の長さに応じて、フルレポートか要約レポートのいずれかが表示されます。
9. チャートを印刷する場合は、右クリックして[*Print]を選択し、必要なプリンタ設定を変更して[*Print]をクリックします。

テキストレポートのタイプ

テキストレポートには、 NMS サービスで処理された属性データの値がテキスト形式で表示されます。レポート対象の期間に応じて、フルレポートと要約レポートの 2 種類が生成されます。期間が 1 週間未満の場合はフルレポート、期間が 1 週間を超える場合は要約レポートです。

フルレポート

フルレポートには、選択した属性に関する詳細が表示されます。

- Time Received ：属性のデータのサンプル値が NMS サービスで処理された日付と時刻。
- Sample Time ：ソースで属性値がサンプリングまたは変更された現地の日時。
- Value ：サンプル時の属性値です。

**Text Results for Services: Load - System Logging**

2010-07-18 15:58:39 PDT To 2010-07-19 15:58:39 PDT

| Time Received | Sample Time | Value |
|---|---|---|
| 2010-07-19 15:58:09 | 2010-07-19 15:58:09 | 0.016 % |
| 2010-07-19 15:56:06 | 2010-07-19 15:56:06 | 0.024 % |
| 2010-07-19 15:54:02 | 2010-07-19 15:54:02 | 0.033 % |
| 2010-07-19 15:52:00 | 2010-07-19 15:52:00 | 0.016 % |
| 2010-07-19 15:49:57 | 2010-07-19 15:49:57 | 0.008 % |
| 2010-07-19 15:47:54 | 2010-07-19 15:47:54 | 0.024 % |
| 2010-07-19 15:45:50 | 2010-07-19 15:45:50 | 0.016 % |
| 2010-07-19 15:43:47 | 2010-07-19 15:43:47 | 0.024 % |
| 2010-07-19 15:41:43 | 2010-07-19 15:41:43 | 0.032 % |
| 2010-07-19 15:39:40 | 2010-07-19 15:39:40 | 0.024 % |
| 2010-07-19 15:37:37 | 2010-07-19 15:37:37 | 0.008 % |
| 2010-07-19 15:35:34 | 2010-07-19 15:35:34 | 0.016 % |
| 2010-07-19 15:33:31 | 2010-07-19 15:33:31 | 0.024 % |
| 2010-07-19 15:31:27 | 2010-07-19 15:31:27 | 0.032 % |
| 2010-07-19 15:29:24 | 2010-07-19 15:29:24 | 0.032 % |
| 2010-07-19 15:27:21 | 2010-07-19 15:27:21 | 0.049 % |
| 2010-07-19 15:25:18 | 2010-07-19 15:25:18 | 0.024 % |
| 2010-07-19 15:21:12 | 2010-07-19 15:21:12 | 0.016 % |
| 2010-07-19 15:19:09 | 2010-07-19 15:19:09 | 0.008 % |
| 2010-07-19 15:17:07 | 2010-07-19 15:17:07 | 0.016 % |

要約レポート

要約レポートには、フルレポートよりも長い期間（通常は 1 週間）のデータが表示されます。一定の期間の複数の属性値が NMS サービスによって集計され、その結果から計算された平均値、最大値、および最小値が 1 つのエントリとして表示されます。

各エントリには、次の情報が表示されます。

- Aggregate Time ：変更された一連の属性値が NMS サービスで最後に集計（収集）された日時（現地時間）です。
- Average Value ：集計期間における属性の平均値です。
- Minimum Value ：集計期間における最小値です。
- Maximum Value ：集計期間における最大値です。

## Text Results for Attribute Send to Relay Rate

2010-07-11 16:02:46 PDT To 2010-07-19 16:02:46 PDT

| Aggregate Time | Average Value | Minimum Value | Maximum Value |
|---|---|---|---|
| 2010-07-19 15:59:52 | 0.271072196 Messages/s | 0.266649743 Messages/s | 0.274983464 Messages/s |
| 2010-07-19 15:53:52 | 0.275585378 Messages/s | 0.266562352 Messages/s | 0.283302736 Messages/s |
| 2010-07-19 15:49:52 | 0.279315709 Messages/s | 0.233318712 Messages/s | 0.333313579 Messages/s |
| 2010-07-19 15:43:52 | 0.28181323 Messages/s | 0.241651024 Messages/s | 0.374976601 Messages/s |
| 2010-07-19 15:39:52 | 0.284233141 Messages/s | 0.249982001 Messages/s | 0.324971987 Messages/s |
| 2010-07-19 15:33:52 | 0.325752083 Messages/s | 0.266641993 Messages/s | 0.358306197 Messages/s |
| 2010-07-19 15:29:52 | 0.278531507 Messages/s | 0.274984766 Messages/s | 0.283320999 Messages/s |
| 2010-07-19 15:23:52 | 0.281437642 Messages/s | 0.274981961 Messages/s | 0.291577735 Messages/s |
| 2010-07-19 15:17:52 | 0.261563307 Messages/s | 0.258318006 Messages/s | 0.266655787 Messages/s |
| 2010-07-19 15:13:52 | 0.265159147 Messages/s | 0.258318557 Messages/s | 0.26663986 Messages/s |

テキストレポートの生成

# テキストレポートには、 NMS サービスで処理された属性データの値がテキスト形式で表示されます。データセンターサイト、グリッドノード、コンポーネント、またはサービスについてのレポートを作成できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

継続的に変化することが想定される属性データについては、 NMS サービス（ソース側）によって一定の間隔でデータがサンプリングされます。変化の少ない属性データ（状態やステータスが変わったときに変化するデータなど）については、属性の値が変わったときに NMS サービスに送信されます。

表示されるレポートの種類は、設定されている期間によって異なります。デフォルトでは、期間が 1 週間を超える場合は要約レポートが生成されます。

グレーのテキストは、サンプリング中にサービスが管理上の理由で停止していた期間を示します。青のテキストは、サービスの状態が不明であることを示します。

手順

1. Support **>** Tools **>** Grid Topology *を選択します。
2. ***grid node***>**component* または *SERVICE*>* Reports **>** Text * を選択します。
3. [* 属性 * （ * Attribute * ） ] ドロップダウンリストからレポートする属性を選択します。
4. 1 ページあたりの結果数を [ * 1 ページあたりの結果数 * （ * Results per Page * ） ] ドロップダウンリストから選択します。
5. 最大 3 桁までの値を丸めるには（パーセント値としてレポートされた属性など）、 * 生データ * チェックボックスの選択を解除します。
6. [*Quick Query] ドロップダウン・リストから、レポートする期間を選択します。

カスタムクエリオプションを選択して、特定の期間を選択します。

レポートが表示されるまでに少し時間がかかります。期間が長い場合は集計に数分かかることもあります。

7. [ カスタムクエリ ] を選択した場合は、 [ 開始日 ] と [ 終了日 ] を入力してレポートする期間をカスタマイズする必要があります。

   の形式を使用します `YYYY/MM/DDHH:MM:SS` 現地時間。この形式に一致するには、先頭にゼロを補う必要があります。たとえば、「 2017/4/6 7 ： 30 ： 00 」と入力すると検証に失敗します。正しい形式は「 2017/04/06 07 ： 30 ： 00 」です。

8. [ 更新（ Update ） ] をクリックします。

   テキストレポートが生成されるまでに少し時間がかかります。期間が長い場合は集計に数分かかることもあります。クエリで設定した時間の長さに応じて、フルレポートか要約レポートのいずれかが表示されます。

9. レポートを印刷する場合は、右クリックして[*Print]を選択し、必要なプリンタ設定を変更して[*Print]をクリックします。

テキストレポートのエクスポート

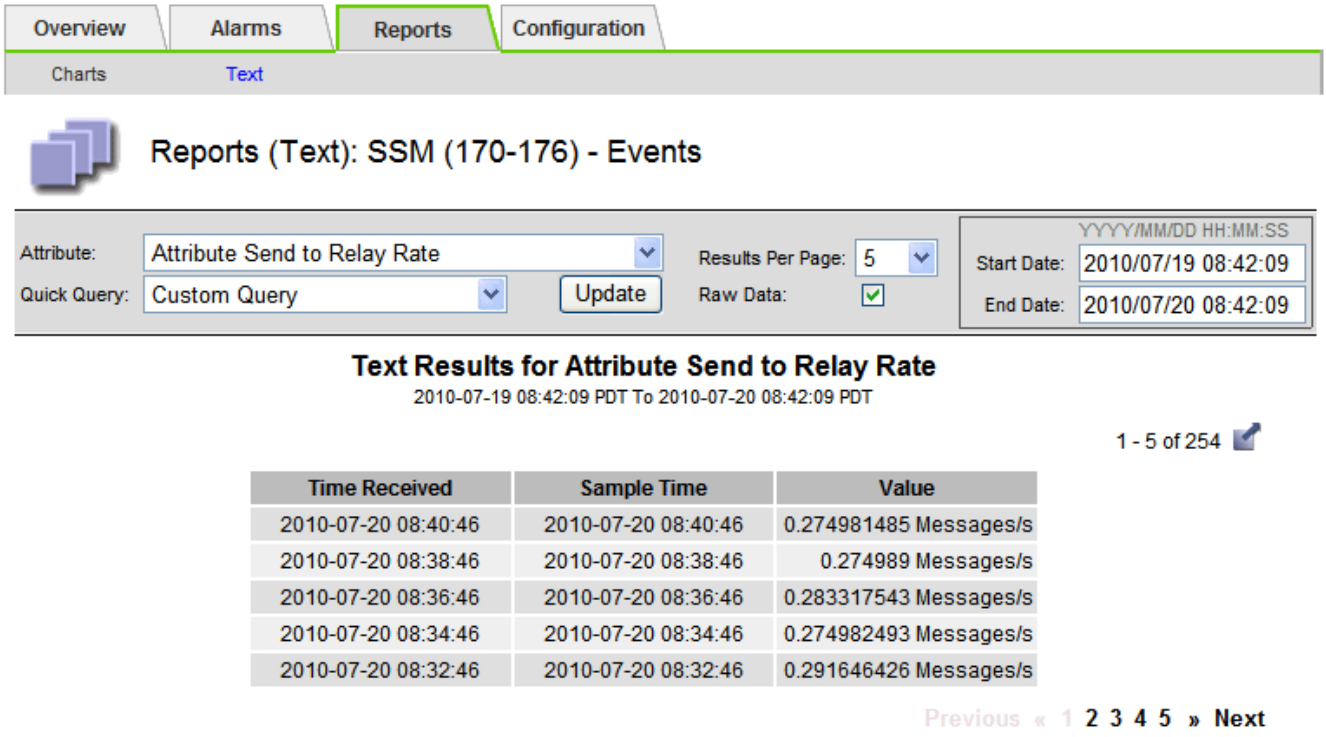
## テキストレポートをエクスポートすると、ブラウザの新しいタブが開き、データを選択してコピーできます。

このタスクについて

コピーしたデータを新しいドキュメント（スプレッドシートなど）に保存して、 StorageGRID システムのパフォーマンスの分析に使用できます。

手順

1. Support **>** Tools **>** Grid Topology *を選択します。
2. テキストレポートを作成します。
3. [ * エクスポート（ Export ） ] をクリックします。




Export Text Report ウィンドウが開き、レポートが表示されます。

```
Grid ID: 000 000
OID: 2.16.124.113590.2.1.400019.1.1.1.1.16996732.200
Node Path: Site/170-176/SSM/Events
Attribute: Attribute Send to Relay Rate (ABSR)
Query Start Date: 2010-07-19 08:42:09 PDT
Query End Date: 2010-07-20 08:42:09 PDT
Time Received,Time Received (Epoch),Sample Time,Sample Time (Epoch),Value,Type
2010-07-20 08:40:46,1279640446559000,2010-07-20 08:40:46,1279640446537209,0.274981485 Messages/s,U
2010-07-20 08:38:46,1279640326561000,2010-07-20 08:38:46,1279640326529124,0.274989 Messages/s,U
2010-07-20 08:36:46,1279640206556000,2010-07-20 08:36:46,1279640206524330,0.283317543 Messages/s,U
2010-07-20 08:34:46,1279640086540000,2010-07-20 08:34:46,1279640086517645,0.274982493 Messages/s,U
2010-07-20 08:32:46,1279639966543000,2010-07-20 08:32:46,1279639966510022,0.291646426 Messages/s,U
2010-07-20 08:30:46,1279639846561000,2010-07-20 08:30:46,1279639846501672,0.308315369 Messages/s,U
2010-07-20 08:28:46,1279639726527000,2010-07-20 08:28:46,1279639726494673,0.291657509 Messages/s,U
2010-07-20 08:26:46,1279639606526000,2010-07-20 08:26:46,1279639606490890,0.266627739 Messages/s,U
2010-07-20 08:24:46,1279639486495000,2010-07-20 08:24:46,1279639486473368,0.258318523 Messages/s,U
2010-07-20 08:22:46,1279639366480000,2010-07-20 08:22:46,1279639366466497,0.274985902 Messages/s,U
2010-07-20 08:20:46,1279639246469000,2010-07-20 08:20:46,1279639246460346,0.283253871 Messages/s,U
2010-07-20 08:18:46,1279639126469000,2010-07-20 08:18:46,1279639126426669,0.274982804 Messages/s,U
2010-07-20 08:16:46,1279639006437000,2010-07-20 08:16:46,1279639006419168,0.283315503 Messages/s,U
```

4. テキストレポートのエクスポートウィンドウの内容を選択してコピーします。

   このデータをスプレッドシートなどのサードパーティのドキュメントに貼り付けることができるようになりました。

## オブジェクトストアや読み出しなどの特定の処理のパフォーマンスを監視して、詳しい調査が必要な変更を特定することができます。

このタスクについて

PUT および GET パフォーマンスを監視するには、ワークステーションから直接、またはオープンソースの S3tester アプリケーションを使用して、 S3 および Swift コマンドを実行します。これらの方法を使用すると、クライアントアプリケーションの問題や外部ネットワークの問題など、 StorageGRID の外部にある要因とは関係なくパフォーマンスを評価できます。

PUT 処理と GET 処理のテストを実行するときは、次のガイドラインに従ってください。

- グリッドに通常取り込むオブジェクトと同等のサイズのオブジェクトを使用します。
- ローカルサイトとリモートサイトの両方に対して処理を実行します。

監査ログのメッセージには、特定の処理の実行に必要な合計時間が記載されています。たとえば、 S3 GET 要求に対する合計処理時間を確認するには、 SGET 監査メッセージの TIME 属性の値を確認します。次の処理の監査メッセージで TIME 属性を確認することもできます。

- * S3 * ： DELETE 、 GET 、 HEAD 、 Metadata Updated 、 POST 、 PUT
- * Swift * ： DELETE 、 GET 、 HEAD 、 PUT

結果を分析する際には、要求を満たすために必要な平均時間と、達成可能な全体的なスループットを確認します。同じテストを定期的に繰り返し、調査が必要な傾向を特定できるように結果を記録します。

- S3testerはgithub：https://github.com/s3testerからダウンロードできます

関連情報

"監査ログを確認します"

オブジェクト検証処理を監視します

## StorageGRID システムは、ストレージノード上のオブジェクトデータの整合性を検証して、オブジェクトの破損や欠落の有無を確認します。

必要なもの

Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

このタスクについて

データの整合性を確保するために、2つの検証プロセスが連携して機能します。

- * バックグラウンド検証 * は、オブジェクトデータの正確性を継続的にチェックするために自動的に実行されます。

  バックグラウンド検証では、すべてのストレージノードが自動的かつ継続的にチェックされて、レプリケートオブジェクトデータとイレイジャーコーディングオブジェクトデータのコピーが破損していないかどうかが確認されます。問題が見つかった場合、 StorageGRID システムは、システム内の別の場所に格納されているコピーから、破損したオブジェクトデータを自動的に置き換えます。バックグラウンド検証は、アーカイブノードやクラウドストレージプール内のオブジェクトに対しては実行されません。

自動的に修正できない破損オブジェクトが検出されると、「 * 未確認 Corrupt object detected * 」アラートがトリガーされます。

- *フォアグラウンド検証*は、オブジェクトデータの有無（正確性ではなく）をより迅速に確認するためにユーザによってトリガーされます。

  フォアグラウンド検証では、特定のストレージノードでレプリケートオブジェクトデータとイレイジャーコーディングオブジェクトデータの有無が確認され、その場所にあるべきオブジェクトがチェックされます。ストレージノードのすべてのオブジェクトストアまたは一部のオブジェクトストアでフォアグラウンド検証を実行して、ストレージデバイスとの整合性に問題がないかどうかを確認できます。多数のオブジェクトが欠落している場合は、ストレージを備えた問題 が存在する可能性があります。

オブジェクトの破損や欠落などのバックグラウンド検証とフォアグラウンド検証の結果を確認するには、ストレージノードのNodesページを参照します。オブジェクトデータの破損や欠落が見つかった場合は、すぐに調査してルート原因 を特定する必要があります。

手順

1. [ノード（ Nodes）]を選択し
2. [***Storage Node***>* Objects*] を選択します。
3. 検証結果を確認するには：

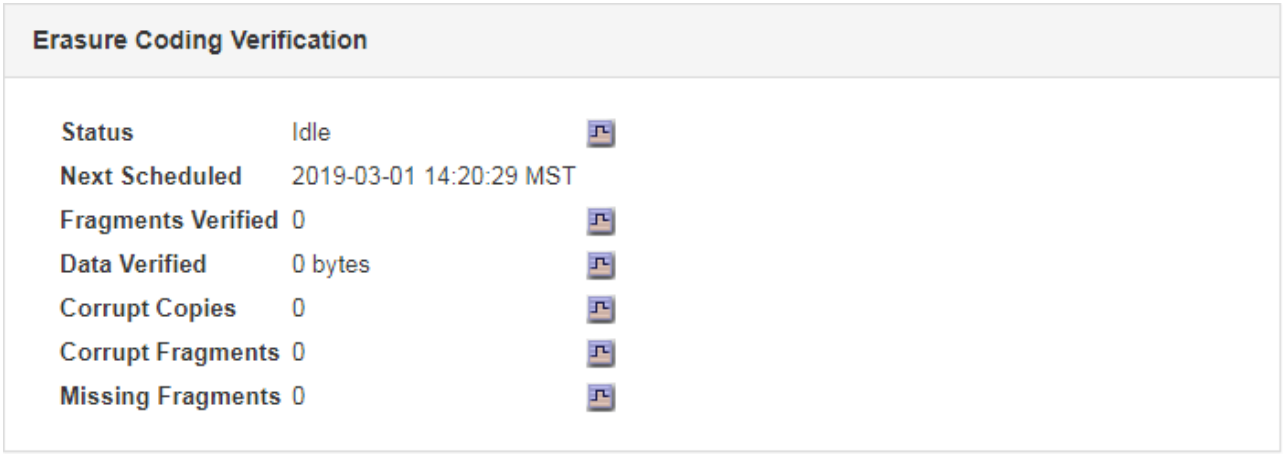
   - レプリケートされたオブジェクトデータの検証を確認するには、 Verification セクションの属性を確認します。

     **Verification**

     | | | |
     |---|---|---|
     | Status | No Errors | |
     | Rate Setting | Adaptive | |
     | Percent Complete | 0.00% | |
     | Average Stat Time | 0.00 microseconds | |
     | Objects Verified | 0 | |
     | Object Verification Rate | 0.00 objects / second | |
     | Data Verified | 0 bytes | |
     | Data Verification Rate | 0.00 bytes / second | |
     | Missing Objects | 0 | |
     | Corrupt Objects | 0 | |
     | Corrupt Objects Unidentified | 0 | |
     | Quarantined Objects | 0 | |

     テーブル内の属性名をクリックすると、ヘルプテキストが表示されます。

   - イレイジャーコーディングフラグメントの検証を確認するには、「ストレージノード>* ILM *」を選択し、イレイジャーコーディング検証テーブルの属性を確認します。




テーブル内の属性名をクリックすると、ヘルプテキストが表示されます。

関連情報

"オブジェクトの整合性を検証してい"

イベントの監視

グリッドノードによって検出されたイベントを監視できます。これには、 syslog サーバに記録されたイベントを追跡するために作成したカスタムイベントも含まれます。グリッドマネージャに表示される Last Event メッセージには、最新のイベントに関する詳細が表示されます。

イベントメッセージは、にも表示されます `/var/local/log/bycast-err.log` ログファイル：

SMTT （ Total events ）アラームは、ネットワークの問題、電源の停止、アップグレードなどの問題によって繰り返しトリガーされることがあります。このセクションでは、イベントを調査する方法について説明します。これにより、これらのアラームが発生した理由をより詳しく理解できます。既知の問題 が原因でイベントが発生した場合、イベントカウンタをリセットしても安全です。

**Nodes**ページでイベントを確認します

ノードページには、各グリッドノードのシステムイベントがリストされます。

1. [ノード（ Nodes）]を選択し
2. ***grid node***>* Eventsを選択します。
3. ページの上部で、グリッドノードで検出された最後のイベントを示す「* Last Event *」のイベントが表示されるかどうかを確認します。

   イベントはグリッドノードからそのままリレーされ、重大度レベルが「ERROR」または「CRITICAL」のログメッセージがすべて含まれます。
4. テーブルを参照して、イベントまたはエラーの数がゼロでないことを確認します。
5. 問題を解決したら、[イベントカウントのリセット*]をクリックしてカウントをゼロに戻します。

グリッドトポロジページでイベントを確認する

また、グリッドトポロジページには、グリッドノードごとのシステムイベントも表示されます。

1. Support > Tools > Grid Topology *を選択します。
2. [*site *>] > [*_grid node*>] > * ssm * > * Events * > * Overview * > * Main * の順に選択します。

関連情報

"イベント数のリセット"

"ログファイル参照"

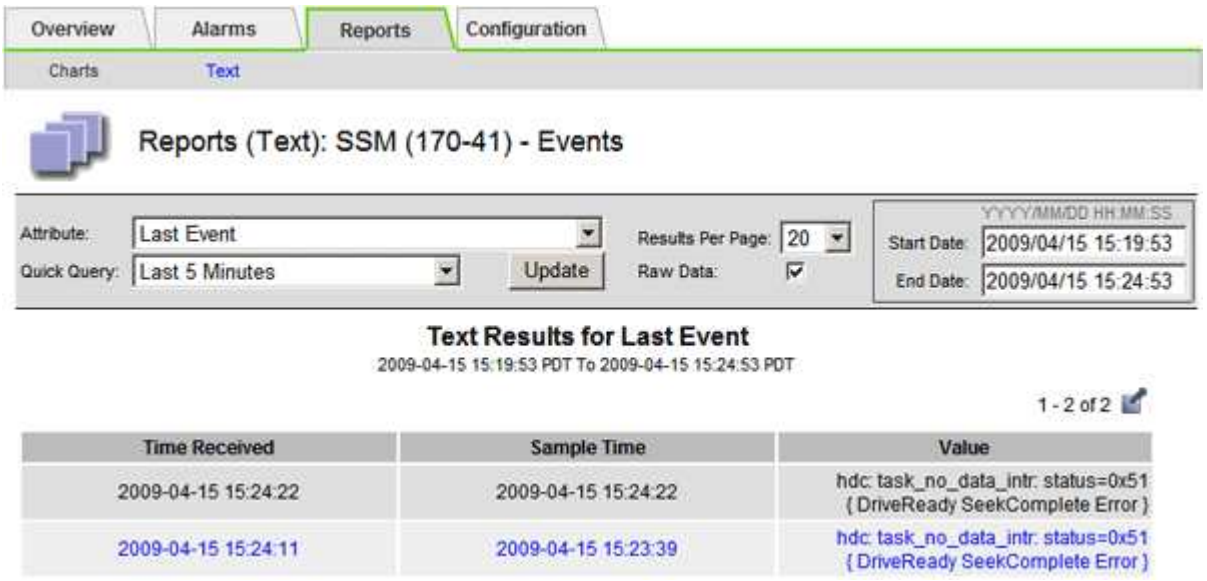
以前のイベントを確認しています

## 以前のイベントメッセージのリストを生成して、過去に発生した問題を特定することができます。

1. Support > Tools > Grid Topology *を選択します。
2. [*site *>] > [*_grid node*] > * ssm * > * Events * > * Reports * ] を選択します。
3. 「 * テキスト * 」を選択します。

   「* Last Event *」属性は「Charts（チャート）」ビューには表示されません。

4. 属性 * を * 最後のイベント * に変更します。
5. 必要に応じて、 * クイッククエリ * の期間を選択します。
6. [ 更新（ Update ） ] をクリックします。




関連情報

"グラフとレポートを使用する"

# システムイベントを解決したら、イベント数を0にリセットできます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Grid Topology Page Configuration権限が必要です。

手順

1. ノード*>*グリッドノード*>*イベント*を選択します。
2. カウントが0より大きいイベントがすべて解決されたことを確認します。
3. [イベントカウントのリセット]をクリックします。

## Events

**Last Event** No Events

| Description | Count |
|---|---|
| Abnormal Software Events | 0 |
| Account Service Events | 0 |
| Cassandra Heap Out Of Memory Errors | 0 |
| Cassandra unhandled exceptions | 0 |
| Chunk Service Events | 0 |
| Custom Events | 0 |
| Data-Mover Service Events | 0 |
| File System Errors | 0 |
| Forced Termination Events | 0 |
| Hotfix Installation Failure Events | 0 |
| I/O Errors | 0 |
| IDE Errors | 0 |
| Identity Service Events | 0 |
| Kernel Errors | 0 |
| Kernel Memory Allocation Failure | 0 |
| Keystone Service Events | 0 |
| Network Receive Errors | 0 |
| Network Transmit Errors | 0 |
| Node Errors | 0 |
| Out Of Memory Errors | 0 |
| Replicated State Machine Service Events | 0 |
| SCSI Errors | 0 |
| Stat Service Events | 0 |
| Storage Hardware Events | 0 |
| System Time Events | 0 |

Reset event counts

# カスタムイベントでは、カーネル、デーモン、エラーとクリティカルのレベルのユーザイベントなど、 syslog サーバに記録されるすべてのイベントを追跡できます。カスタムイベントは、システムログメッセージ（ネットワークセキュリティイベントやハードウェア障害）の発生を監視するのに役立ちます。

このタスクについて

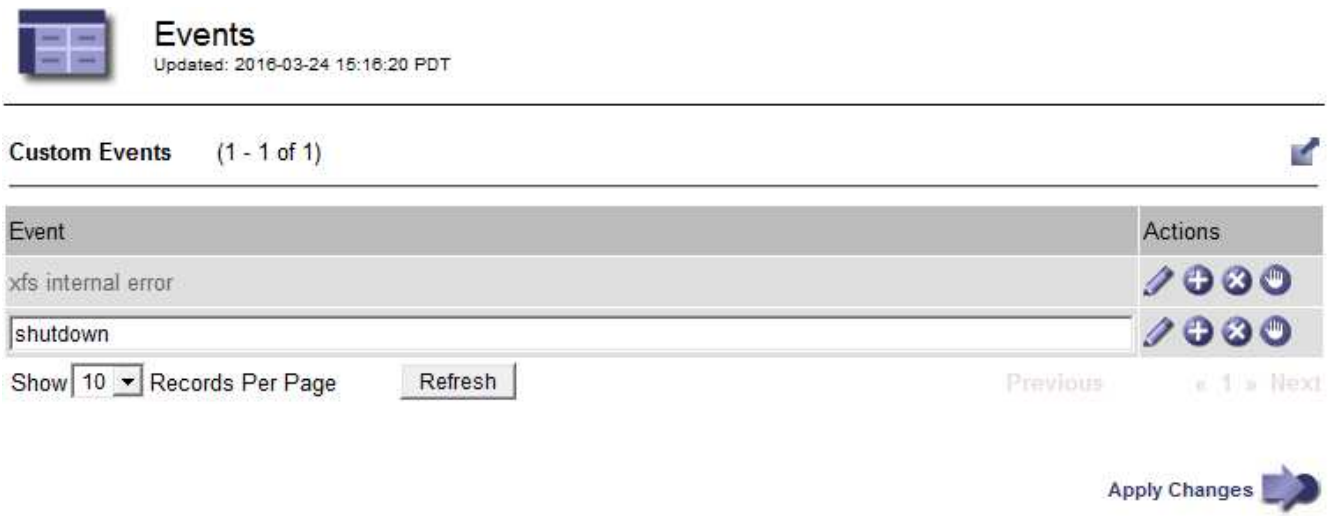
繰り返し発生する問題については、カスタムイベントの作成を検討してください。カスタムイベントを使用する際は、次の点を考慮する必要があり

- カスタムイベントが作成されると、該当するイベントが発生するたびに監視されます。すべてのカスタムイベントの累積数の値は、* Nodes **>*_grid node_name >** Events *ページで確認できます。
- でキーワードに基づいてカスタムイベントを作成します `/var/log/messages` または `/var/log/syslog` ファイル。これらのファイルのログは次のようにする必要があります。
  - カーネルによって生成されます
  - デーモンまたはユーザプログラムによってエラーまたはクリティカルのレベルで生成されます

*注：*内のすべてのエントリが含まれているわけではありません `/var/log/messages` または `/var/log/syslog` 上記の要件を満たしていないファイルは照合されます。

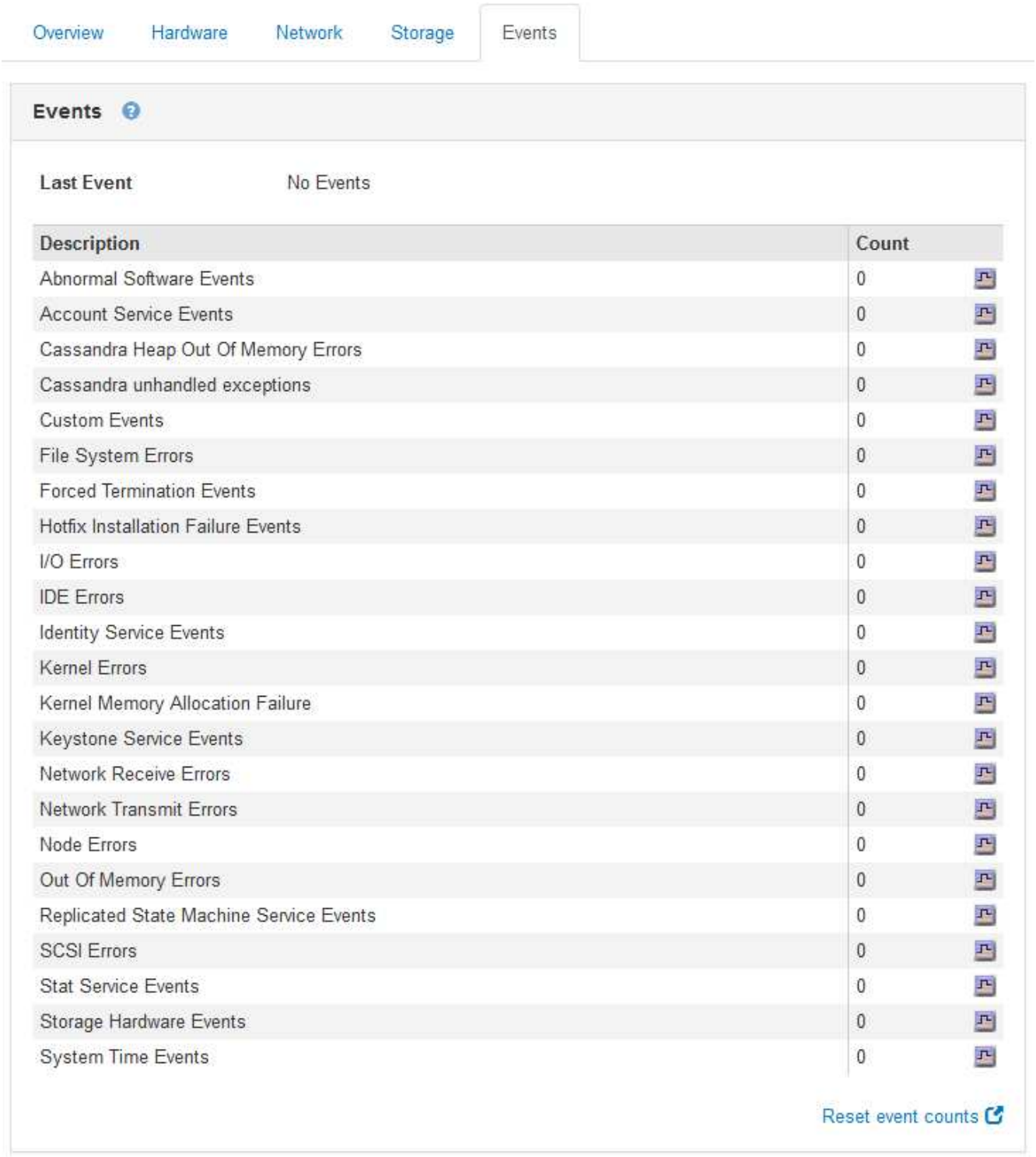
手順

1. * Configuration **>** Monitoring **>** Events *を選択します。
2. [ 編集（ Edit ） ] をクリックします。 （または * Insert * ） 最初のイベントではない場合）をクリックします。
3. shutdown などのカスタムイベント文字列を入力します




4. [ 変更の適用 *] をクリックします。
5. [ノード（ Nodes）]を選択し次に、**_ grid node_**>* Events *を選択します。
6. Events テーブルで Custom Events のエントリを探し、 * Count * の値を監視します。

   カウントが増えていれば、そのグリッドノードで監視しているカスタムイベントがトリガーされています。



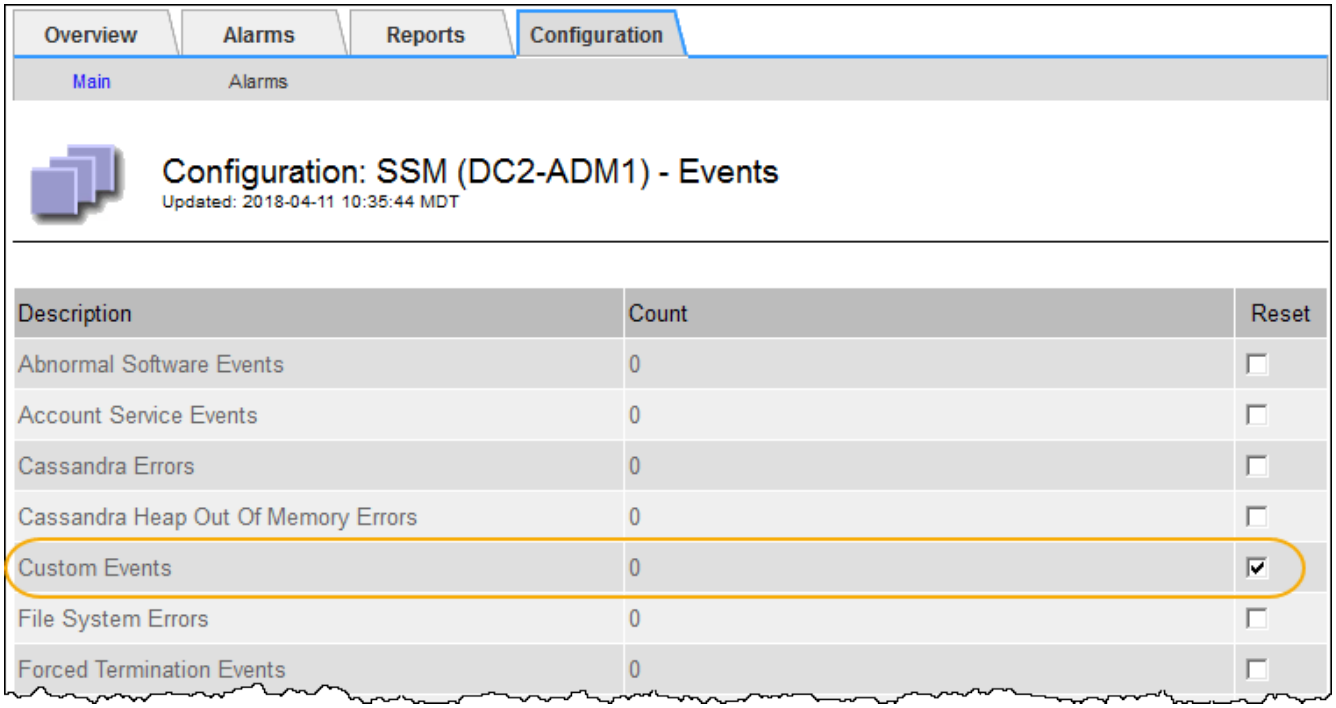

カスタムイベントのカウントを**0**にリセットします

## カスタムイベントのカウンタのみをリセットする場合は、のサポートメニューのグリッドトポロジページを使用する必要があります。

このタスクについて

カウンタをリセットすると、次のイベントによってアラームがトリガーされます。一方、アラームを確認した場合は、次のしきい値レベルに達したときにのみアラームが再度トリガーされます。

1. Support > Tools > Grid Topology *を選択します。
2. * *grid node** > * ssm * > * Events * > * Configuration * > * Main * を選択します。
3. カスタムイベントの * リセット * チェックボックスをオンにします。




4. [ 変更の適用 *] をクリックします。

監査メッセージの確認

## 監査メッセージは、 StorageGRID システムの詳細な運用状況を的確に把握するために役立ちます。監査ログを使用して、問題のトラブルシューティングやパフォーマンスの評価を行うことができます。

通常のシステム運用中、すべての StorageGRID サービスは次の監査メッセージを生成します。

- システム監査メッセージは、監査システム自体、グリッドノードの状態、システム全体のタスクアクティビティ、およびサービスバックアップ処理に関連します。
- オブジェクトストレージの監査メッセージは、オブジェクトの格納と読み出し、グリッドノードからグリッドノードへの転送、検証など、 StorageGRID 内のオブジェクトの格納と管理に関連します。
- クライアント読み取り / 書き込み監査メッセージは、 S3 または Swift クライアントアプリケーションがオブジェクトの作成、変更、または読み出しの要求を行うときに記録されます。
- 管理監査メッセージには、管理 API に対するユーザ要求が記録されます。

各管理ノードで、監査メッセージがテキストファイルに保存されます。監査共有には、アクティブファイル（ audit.log ）と、圧縮された過去の監査ログが含まれています。

監査ログへのアクセスを簡単にするためには、NFSとCIFSの両方についてクライアントから監査共有へのアクセスを設定します（現在CIFSは廃止）。管理ノードのコマンドラインから直接監査ログファイルにアクセスすることもできます。

監査ログファイル、監査メッセージの形式、監査メッセージの種類、および監査メッセージを分析するためのツールの詳細については、監査メッセージに関する手順を参照してください。監査クライアントアクセスの設定方法については、 StorageGRID の管理手順を参照してください。

関連情報

"監査ログを確認します"

"StorageGRID の管理"

ログファイルとシステムデータを収集しています

# Grid Manager を使用して、 StorageGRID システムのログファイルとシステムデータ（設定データを含む）を取得できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- プロビジョニングパスフレーズが必要です。

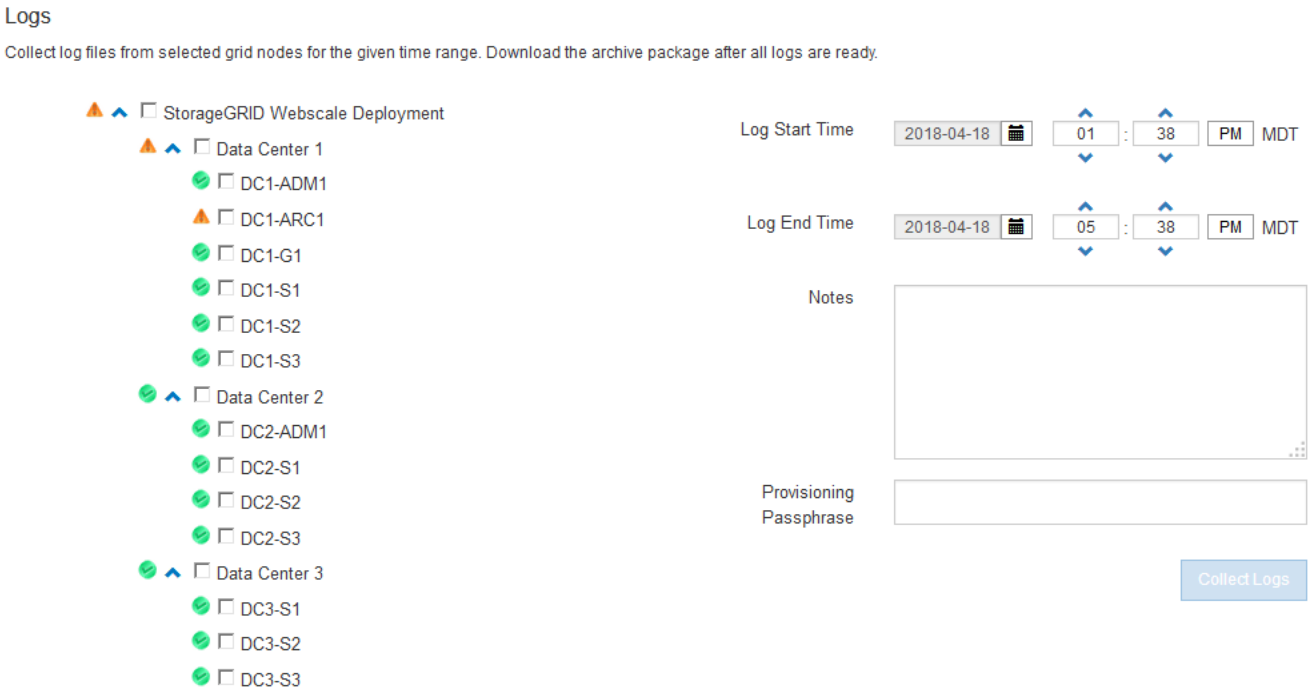
このタックについて

Grid Managerを使用して、選択した期間について任意のグリッドノードからログファイル、システムデータ、および設定データを収集できます。収集されたデータは .tar.gz ファイルにアーカイブされ、ローカルコンピュータにダウンロードできます。

アプリケーションログファイルは非常に大きくなる可能性があるため、アーカイブされたログファイルのダウンロード先ディレクトリには1GB以上の空きスペースが必要です。

手順

1. [サポート（Support ）]>[*ツール（* Tools ）]>[*ログ（* Logs *）]



2. ログファイルを収集するグリッドノードを選択します。

   必要に応じて、グリッド全体またはデータセンターサイト全体のログファイルを収集できます。

3. ログファイルに含めるデータの時間範囲を設定するには、 * Start Time * および * End Time * を選択します。

   非常に長い期間を選択したり、大規模なグリッド内のすべてのノードからログを収集したりすると、ログアーカイブが大きくなりすぎてノードに格納できなくなったり、ダウンロード用にプライマリ管理ノードに保存できなくなったりすることがあります。その場合は、より小さなデータセットを使用してログ収集を再開する必要があります。

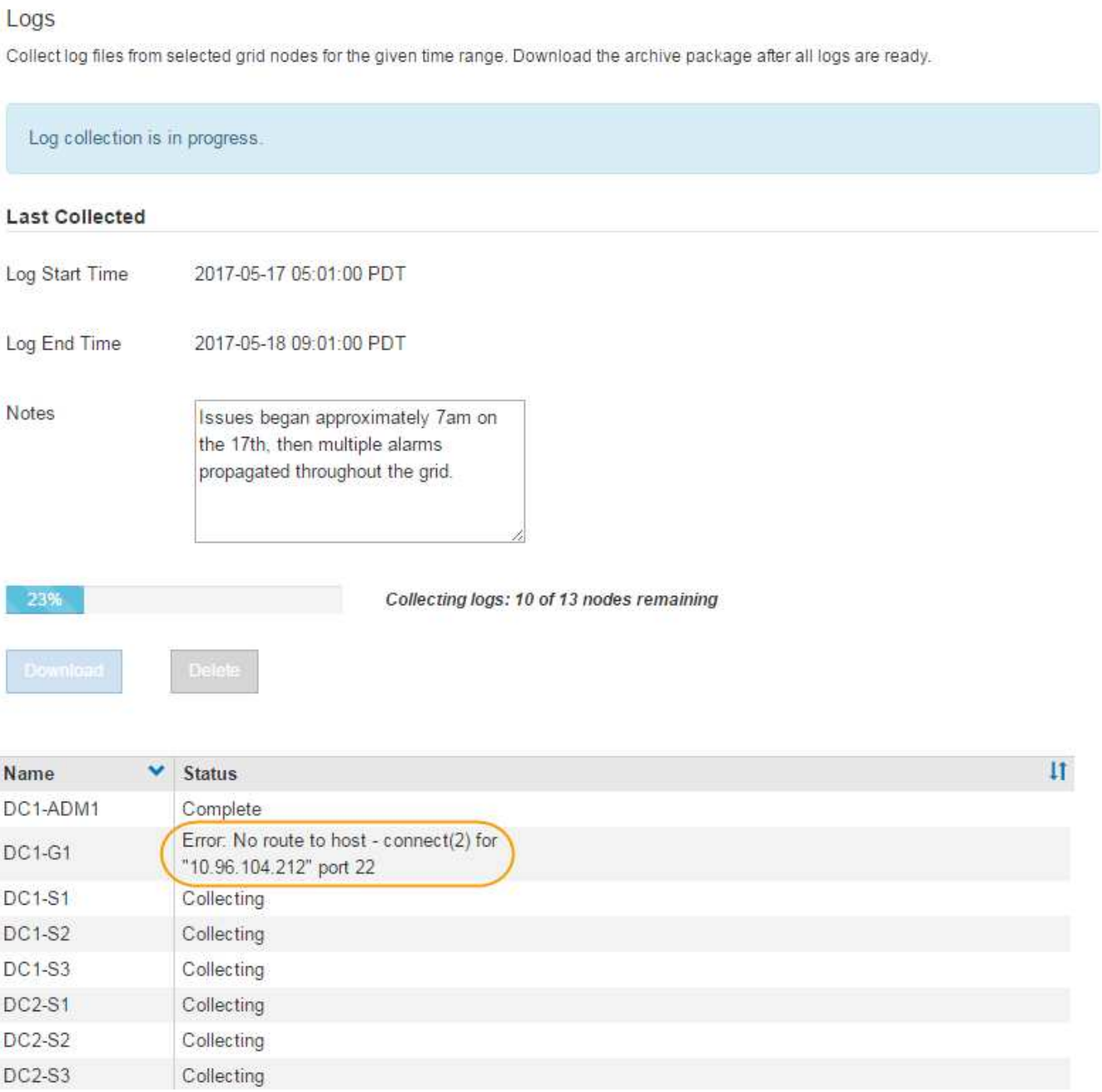
4. 必要に応じて、収集するログファイルに関するメモを* Notes *テキストボックスに入力します。

   このメモを使用して、ログファイルを収集する原因となった問題に関するテクニカルサポート情報を入力できます。メモはというファイルに追加されます `info.txt`と、ログファイルの収集に関するその他の情報。。 `info.txt` ファイルはログファイルのアーカイブパッケージに保存されます。

5. StorageGRID システムのプロビジョニングパスフレーズを * プロビジョニングパスフレーズ * テキストボックスに入力します。

6. [**Collect Logs**](ログの収集)をクリック

   新しい要求を送信すると、以前に収集されたログファイルは削除されます。




ログページを使用して、各グリッドノードのログファイル収集の進捗状況を監視できます。

ログサイズに関するエラーメッセージが表示された場合は、ログを収集する期間を短縮するか、またはノードの数を減らしてください。

7. ログファイルの収集が完了したら、* Download *をクリックします。

完了後

必要に応じて、ログファイルのアーカイブパッケージはあとから再度ダウンロードできます。

必要に応じて、* Delete *をクリックしてログファイルアーカイブパッケージを削除し、ディスクスペースを解放できます。ログファイルの現在のアーカイブパッケージは、次回ログファイルを収集すると自動的に削除されます。

関連情報

"ログファイル参照"

手動での**AutoSupport** メッセージのトリガー

テクニカルサポートによる StorageGRID システムの問題のトラブルシューティングを支援するために、 AutoSupport メッセージの送信を手動でトリガーできます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限または Other Grid Configuration 権限が必要です。

手順

1. [サポート（Support ）**]>[***ツール（* Tools ）**]>[** AutoSupport （*）]

   AutoSupport ページが表示され、 * 設定 * タブが選択されます。

2. [ ユーザー起動 AutoSupport 送信 ] を選択します。

   StorageGRID は、テクニカルサポートに AutoSupport メッセージを送信しようとします。試行に成功した場合は、 [ 結果（ Results ） ] タブの [ 最新結果（ Recent Result ） ] * 値と [ 前回成功した時間（ Last Successful Time ） ] * 値が更新されます。問題がある場合、「最新の結果 * 」の値が「失敗」に更新され、 StorageGRID は AutoSupport メッセージの送信を再試行しません。

   ユーザトリガー型 AutoSupport メッセージを送信したあと、 1 分後にブラウザの AutoSupport ページを更新して最新の結果にアクセスします。

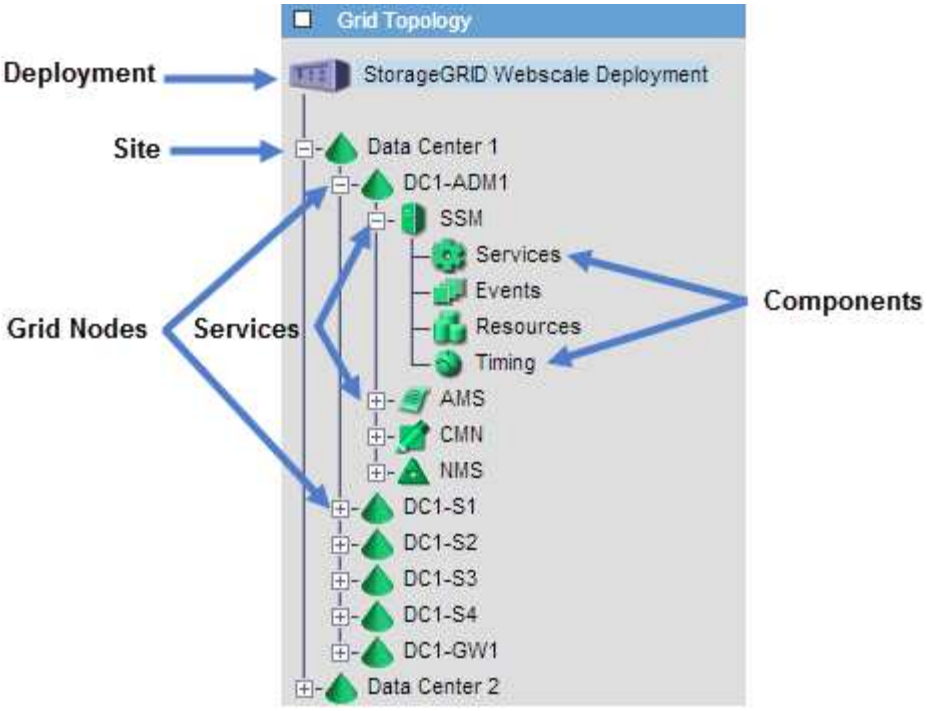
関連情報

"アラーム用Eメールサーバの設定（従来のシステム）"

グリッドトポロジツリーの表示

グリッドトポロジツリーを使用すると、サイト、グリッドノード、サービス、コンポーネントなど、 StorageGRID のシステム要素に関する詳細情報にアクセスできます。ほとんどの場合、グリッドトポロジツリーへのアクセスが必要になるのは、ドキュメントで指示されているとき、またはテクニカルサポートとともに作業するときに限られます。

グリッドトポロジツリーにアクセスするには、* Support **>** Tools **>** Grid Topology *を選択します。




グリッドトポロジツリーを展開または折りたたむには、をクリックします ⊞ または ⊟ をクリックします。サイト全体または各ノードのすべての項目を展開または折りたたむには、 * <Ctrl>* キーを押しながらクリックします。

サポート指標の確認

## 問題 のトラブルシューティングでは、テクニカルサポートと協力して StorageGRID システムの詳細な指標とグラフを確認することができます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

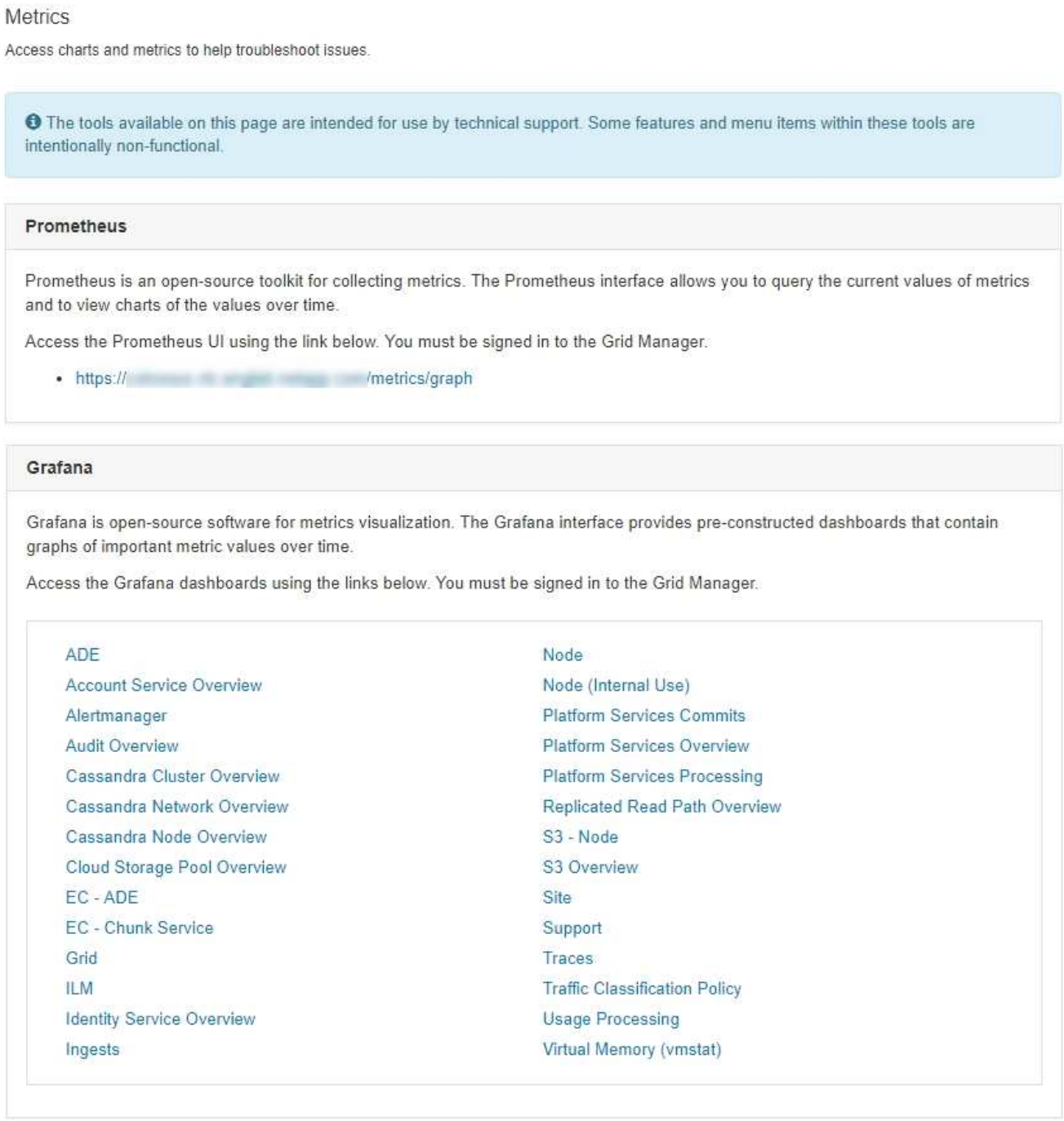
Metrics ページでは、 Prometheus と Grafana のユーザインターフェイスにアクセスできます。Prometheus は指標を収集するオープンソースソフトウェアです。Grafana は指標を視覚化するオープンソースソフトウェアです。

> ⓘ Metrics ページで使用可能なツールは、テクニカルサポートが使用することを目的としています。これらのツールの一部の機能およびメニュー項目は意図的に機能しないため、変更される場合があります。

手順

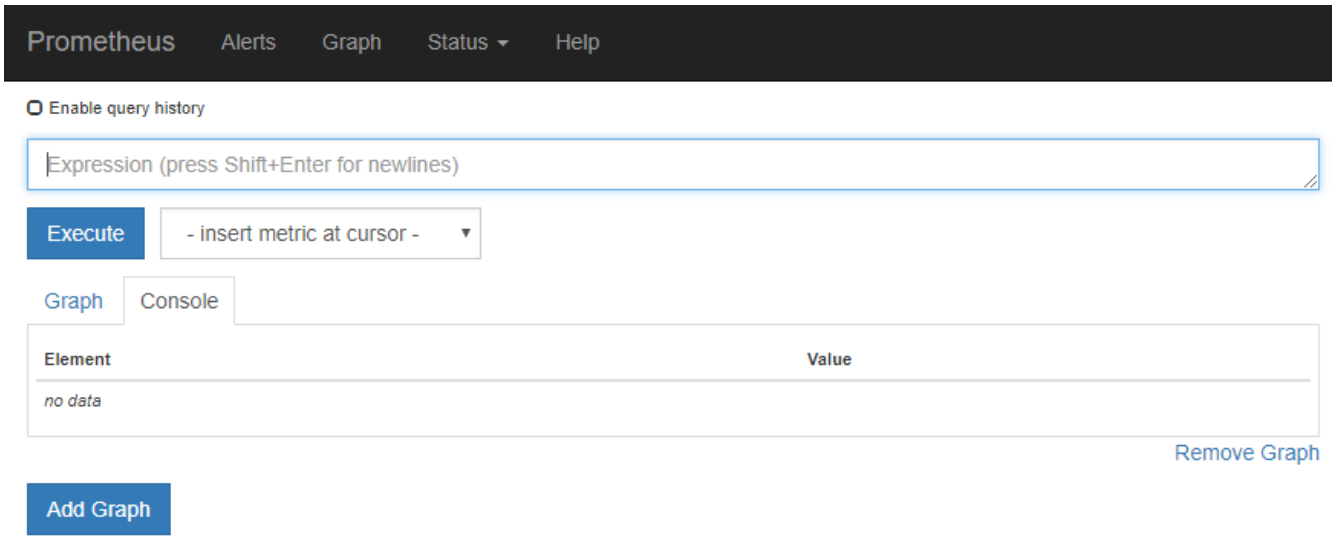
1. テクニカルサポートの指示に従って、* Support > Tools > Metrics *を選択します。

   [Metrics]ページが表示されます。




2. StorageGRID 指標の現在の値を照会し、一定期間の値のグラフを表示するには、 Prometheus セクション内のリンクをクリックします。

   Prometheus インターフェイスが表示されます。このインターフェイスでは、使用可能な StorageGRID 指標に対してクエリを実行したり、 StorageGRID 指標の推移をグラフ化したりできます。




名前に *private* が含まれる指標は内部専用です。 StorageGRID のリリースごとに予告なく変更されることがあります。

3. 時間の経過に伴う StorageGRID 指標のグラフを含む構築済みのダッシュボードにアクセスするには、Grafana セクションのリンクをクリックします。

   選択したリンクに対応した Grafana インターフェイスが表示されます。

関連情報

"よく使用される Prometheus 指標"

診断の実行

## 問題 のトラブルシューティングを行う場合、テクニカルサポートと協力して StorageGRID システムの診断を実行し、結果を確認します。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

Diagnostics （診断）ページでは、グリッドの現在の状態に対して一連の診断チェックが実行されます。各診断点検には、次の 3 つのいずれかのステータスがあります。

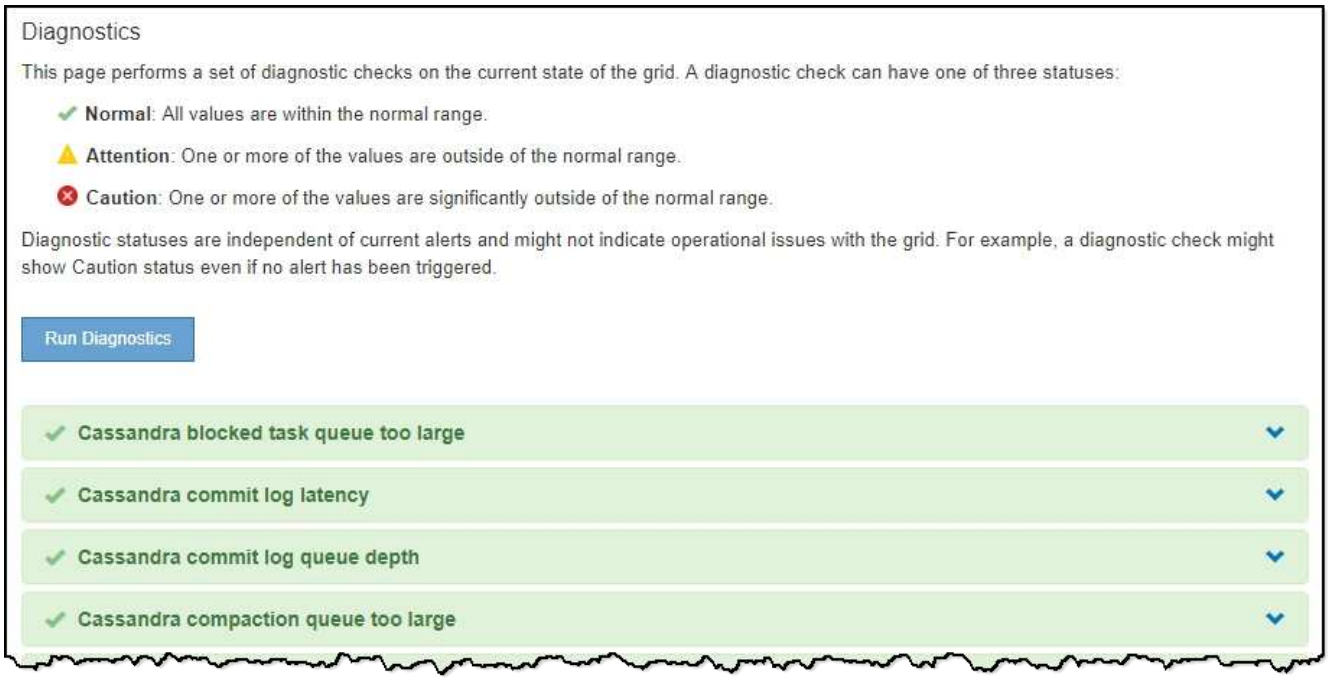
- * 標準 * ：すべての値が標準範囲内です。
- * 注意 * ： 1 つ以上の値が正常範囲外です。
- * 注意 * ： 1 つ以上の値が通常の範囲外です。

診断ステータスは現在のアラートとは関係なく、グリッドで発生している処理の問題を示しているとは限りません。たとえば、アラートがトリガーされていない場合でも、診断チェックで警告ステータスが表示されることがあります。

手順

1. [サポート（Support ）]>[*ツール（* Tools ）]>[*診断（Diagnostics

   Diagnostics （診断）ページが表示され、診断チェックごとの結果がリストされます。この例では、すべての診断のステータスは Normal です。



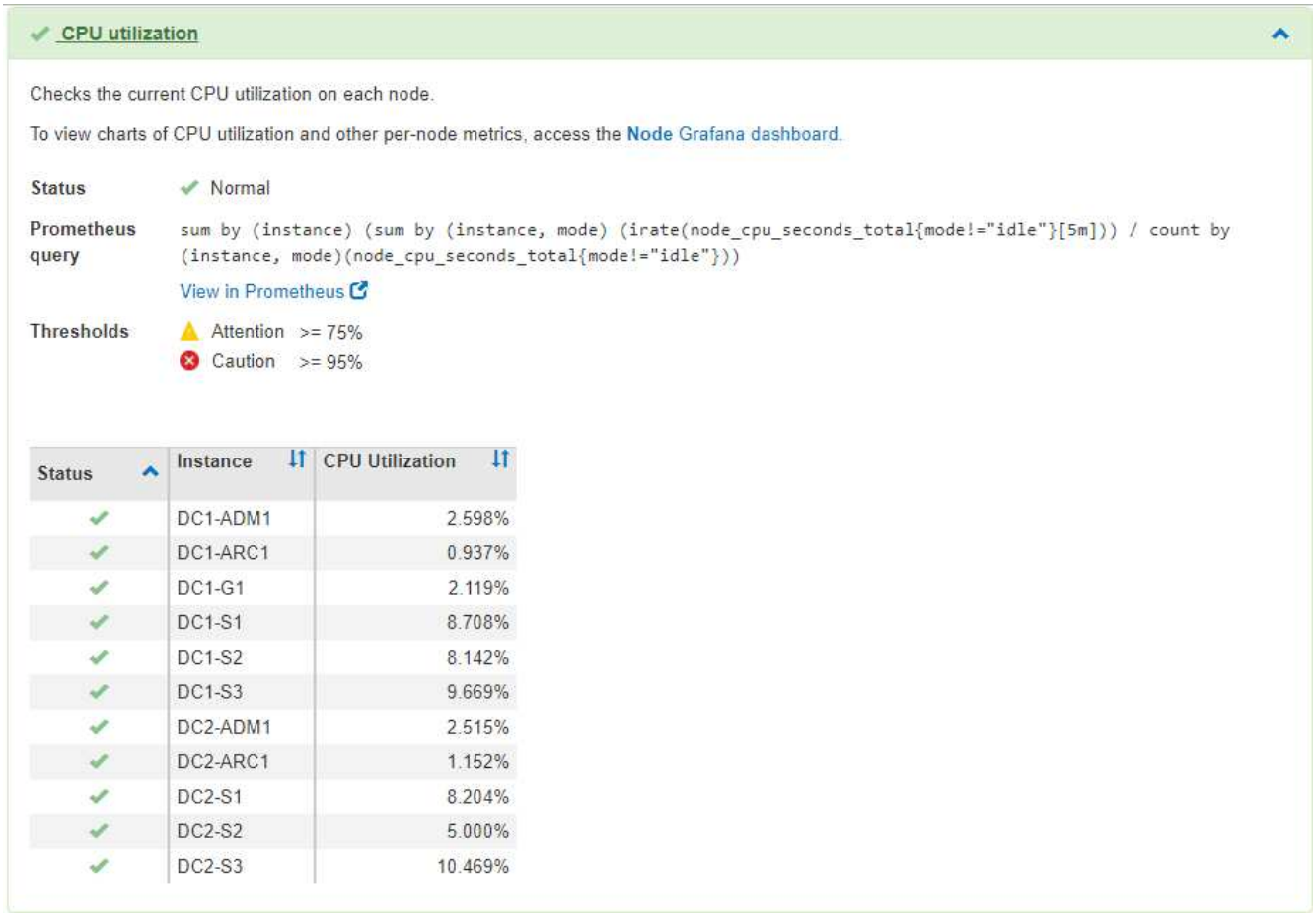

2. 特定の診断の詳細については、行の任意の場所をクリックしてください。

   診断とその現在の結果の詳細が表示されます。以下の詳細が表示されます。

   - * ステータス * ：この診断の現在のステータス。正常、注意、または注意。
   - * Prometheus クエリ * ：診断に使用した場合、ステータス値の生成に使用した Prometheus 式。（ Prometheus 式は一部の診断には使用されません）。
   - * しきい値 * ：診断に使用できる場合は、異常な診断ステータスごとにシステム定義のしきい値。（しきい値はすべての診断に使用されるわけではありません）。

     これらのしきい値は変更できません。

   - * ステータス値 * ： StorageGRID システム全体の診断ステータスと値を示すテーブル。この例では、StorageGRID システム内のすべてのノードの現在の CPU 利用率が表示されています。すべてのノードの値が警告と警告のしきい値を下回っているため、診断の全体的なステータスは「正常」です。




3. * オプション * ：この診断に関連した Grafana チャートを表示するには、 * Grafana dashboard dashboard * リンクをクリックします。

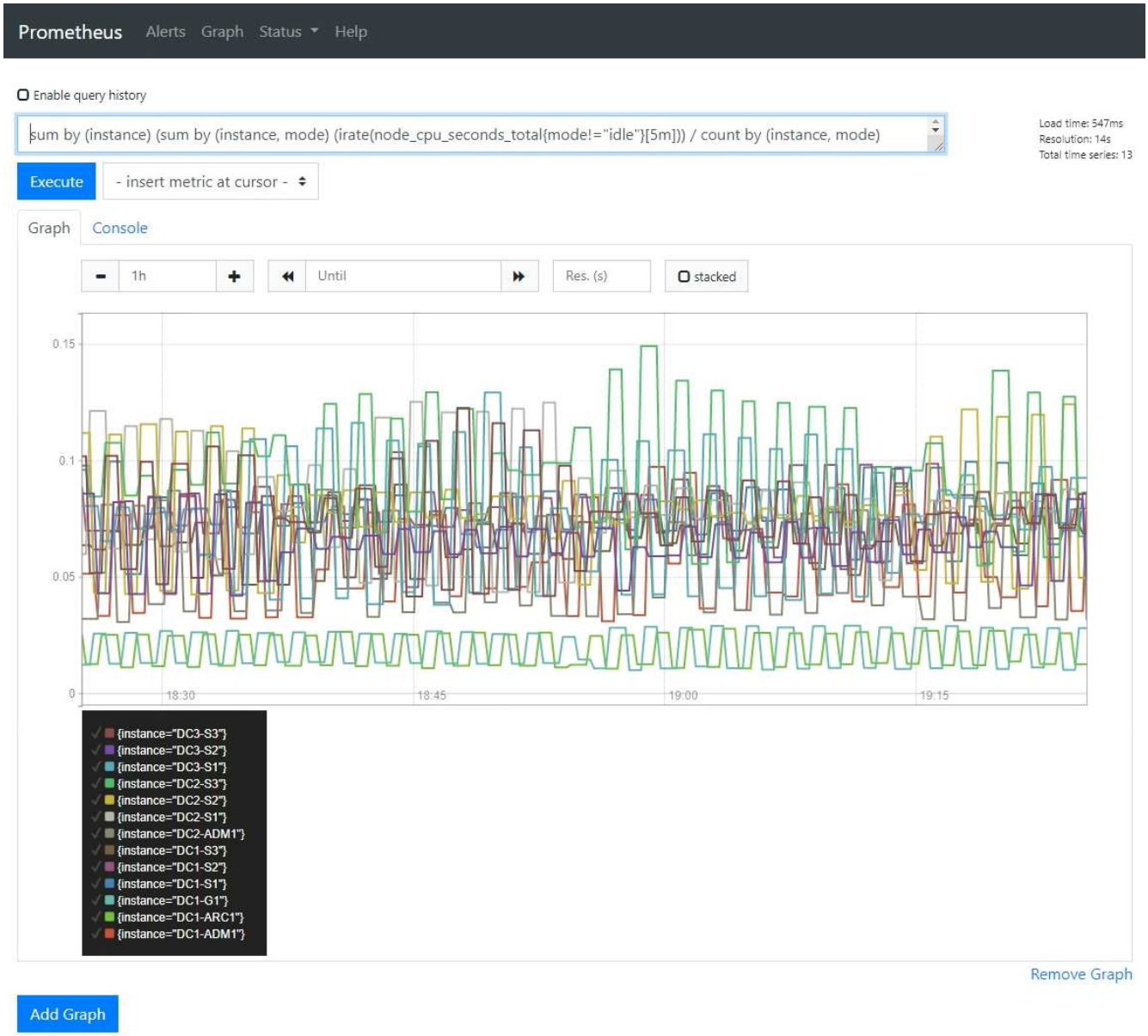
   このリンクは、すべての診断で表示されるわけではありません。

   関連する Grafana ダッシュボードが表示されます。この例では、このノードの CPU 利用率とノードの他の Grafana チャートを示すノードダッシュボードが表示されます。

   また、構築済みのGrafanaダッシュボードには、* Support > Tools > Metrics *ページのGrafanaセクションからアクセスできます。

4. * オプション * ：一定の期間にわたる Prometheus 式のチャートを表示するには、 * Prometheus で表示 * をクリックします。

   診断に使用された式の Prometheus グラフが表示されます。




関連情報

"サポート指標の確認"

"よく使用される Prometheus 指標"

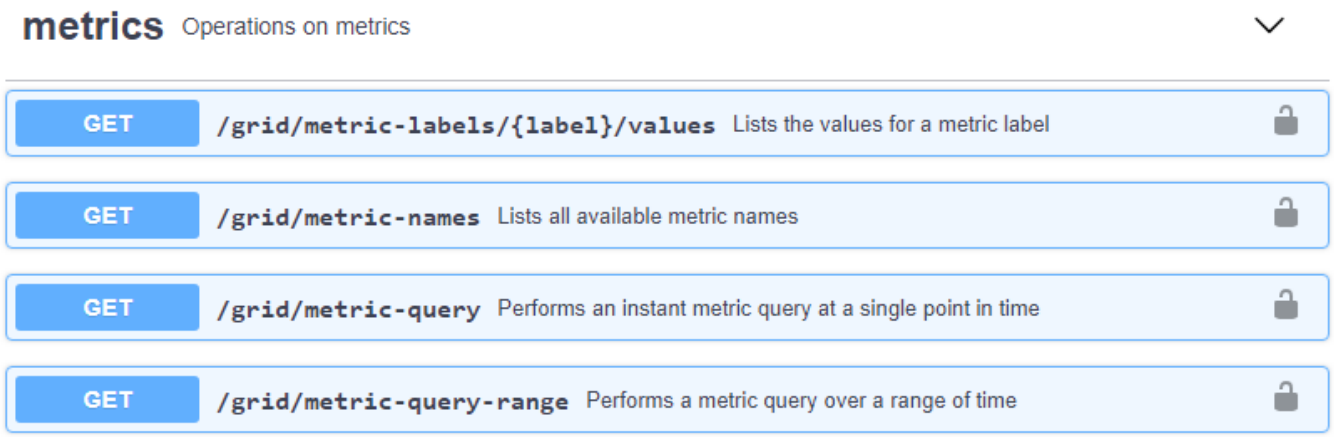
カスタムの監視アプリケーションを作成する

## グリッド管理 API から取得される StorageGRID 指標を使用して、カスタムの監視アプリケーションやダッシュボードを構築できます。

グリッドマネージャの既存のページに表示されない指標を監視する場合や、 StorageGRID 用のカスタムダッシュボードを作成する場合は、グリッド管理 API を使用して StorageGRID 指標を照会できます。

また、 Grafana などの外部監視ツールを使用して、 Prometheus 指標に直接アクセスすることもできます。外部ツールを使用するには、管理用クライアント証明書をアップロードまたは生成して、 StorageGRID でセキュリティを確保するためにツールを認証する必要があります。StorageGRID の管理手順を参照してください。

使用可能なすべての指標を含む指標APIの処理を表示するには、Grid Managerで* Help > API Documentation > metrics *を選択します。




カスタム監視アプリケーションの実装方法の詳細については、このガイドでは説明していません。

関連情報

"StorageGRID の管理"

## アラート一覧

次の表に、デフォルトの StorageGRID アラートをすべて示します。必要に応じて、システムの管理方法に合わせてカスタムのアラートルールを作成できます。

一部のアラートで使用される指標については、よく使用されるPrometheus指標に関する情報を参照してください。

| アラート名 | 概要 および推奨される対処方法 |
| --- | --- |
| アプライアンスのバッテリの有効期間が終了し | アプライアンスのストレージコントローラのバッテリの有効期間が終了しました。<br><br>1. バッテリを交換します。バッテリの取り外しと交換の手順は、アプライアンスの設置とメンテナンスの手順のストレージコントローラを交換するための手順 に含まれています。<br>◦ "SG6000 ストレージアプライアンス"<br>◦ "SG5700 ストレージアプライアンス"<br>◦ "SG5600 ストレージアプライアンス"<br>2. このアラートが解決しない場合は、テクニカルサポートにお問い合わせください。 |

| アラート名 | 概要 および推奨される対処方法 |
| --- | --- |
| アプライアンスのバッテリに問題があります | アプライアンスのストレージコントローラのバッテリに障害が発生しました。<br><br>1. バッテリを交換します。バッテリの取り外しと交換の手順は、アプライアンスの設置とメンテナンスの手順のストレージコントローラを交換するための手順 に含まれています。<br>◦ "SG6000 ストレージアプライアンス"<br>◦ "SG5700 ストレージアプライアンス"<br>◦ "SG5600 ストレージアプライアンス"<br>2. このアラートが解決しない場合は、テクニカルサポートにお問い合わせください。 |
| アプライアンスバッテリの学習容量が不足しています | アプライアンスのストレージコントローラのバッテリで学習容量が不足しています。<br><br>1. バッテリを交換します。バッテリの取り外しと交換の手順は、アプライアンスの設置とメンテナンスの手順のストレージコントローラを交換するための手順 に含まれています。<br>◦ "SG6000 ストレージアプライアンス"<br>◦ "SG5700 ストレージアプライアンス"<br>◦ "SG5600 ストレージアプライアンス"<br>2. このアラートが解決しない場合は、テクニカルサポートにお問い合わせください。 |
| アプライアンスバッテリの有効期限が近づいています | アプライアンスのストレージコントローラのバッテリの有効期限が近づいています。<br><br>1. すぐにバッテリを交換してください。バッテリの取り外しと交換の手順は、アプライアンスの設置とメンテナンスの手順のストレージコントローラを交換するための手順 に含まれています。<br>◦ "SG6000 ストレージアプライアンス"<br>◦ "SG5700 ストレージアプライアンス"<br>◦ "SG5600 ストレージアプライアンス"<br>2. このアラートが解決しない場合は、テクニカルサポートにお問い合わせください。 |

| アラート名 | 概要 および推奨される対処方法 |
| --- | --- |
| アプライアンスのバッテリが取り外されました | アプライアンスのストレージコントローラのバッテリがありません。<br><br>1. バッテリを取り付けます。バッテリの取り外しと交換の手順は、アプライアンスの設置とメンテナンスの手順のストレージコントローラを交換するための手順 に含まれています。<br>◦ "SG6000 ストレージアプライアンス"<br>◦ "SG5700 ストレージアプライアンス"<br>◦ "SG5600 ストレージアプライアンス"<br>2. このアラートが解決しない場合は、テクニカルサポートにお問い合わせください。 |
| アプライアンスのバッテリが高温になっています | アプライアンスのストレージコントローラのバッテリが過熱しています。<br><br>1. このノードに影響している別のアラートがないかを確認します。他のアラートを解決することで、このアラートが解決する可能性があります。<br>2. ファンや HVAC の故障など、温度上昇の考えられる原因を調査する。<br>3. このアラートが解決しない場合は、テクニカルサポートにお問い合わせください。 |
| アプライアンスの BMC 通信エラー | ベースボード管理コントローラ（ BMC ）との通信が失われました。<br><br>1. BMC が正常に動作していることを確認します。ノード*を選択し、アプライアンスノードのハードウェア*タブを選択します。Compute Controller BMC IP フィールドを探し、その IP を参照します。<br>2. ノードをメンテナンスモードにしてから、アプライアンスの電源をオフにしてオンにし、 BMC の通信をリストアします。使用しているアプライアンスのインストールとメンテナンスの手順を参照してください。<br>◦ "SG6000 ストレージアプライアンス"<br>◦ "SG100 SG1000サービスアプライアンス"<br>3. このアラートが解決しない場合は、テクニカルサポートにお問い合わせください。 |

| アラート名 | 概要 および推奨される対処方法 |
| --- | --- |
| アプライアンスキャッシュバックアップデバイスに障害が発生しました | 永続的キャッシュバックアップデバイスで障害が発生しました。<br><br>1. このノードに影響している別のアラートがないかを確認します。他のアラートを解決することで、このアラートが解決する可能性があります。<br>2. テクニカルサポートにお問い合わせください。 |
| アプライアンスキャッシュバックアップデバイスに十分な容量がありません | キャッシュバックアップデバイスの容量が不足しています。テクニカルサポートにお問い合わせください。 |
| アプライアンスのキャッシュ・バックアップ・デバイスの書き込み保護 | キャッシュバックアップデバイスは書き込み保護されています。テクニカルサポートにお問い合わせください。 |
| アプライアンスのキャッシュメモリサイズが一致しません | アプライアンスの2台のコントローラのキャッシュサイズが異なります。テクニカルサポートにお問い合わせください。 |
| アプライアンスコンピューティングコントローラシャーシの温度が高すぎます | StorageGRID アプライアンスのコンピューティングコントローラの温度が公称のしきい値を超えました。<br><br>1. ハードウェアコンポーネントの過熱状態を確認し、推奨される対処方法に従います。<br>◦ SG100 、 SG1000 、または SG6000 を使用している場合は、 BMC を使用します。<br>◦ SG5600 または SG5700 を使用している場合は、 SANtricity System Manager を使用します。<br>2. 必要に応じて、コンポーネントを交換します。使用しているアプライアンスハードウェアの設置とメンテナンスの手順を参照してください。<br>◦ "SG6000 ストレージアプライアンス"<br>◦ "SG5700 ストレージアプライアンス"<br>◦ "SG5600 ストレージアプライアンス"<br>◦ "SG100 SG1000サービスアプライアンス" |

| アラート名 | 概要 および推奨される対処方法 |
| --- | --- |
| アプライアンスのコンピューティングコントローラの CPU 温度が高すぎます | StorageGRID アプライアンスのコンピューティングコントローラの CPU 温度が公称のしきい値を超えました。<br><br>1. ハードウェアコンポーネントの過熱状態を確認し、推奨される対処方法に従います。<br>◦ SG100 、 SG1000 、または SG6000 を使用している場合は、 BMC を使用します。<br>◦ SG5600 または SG5700 を使用している場合は、 SANtricity System Manager を使用します。<br>2. 必要に応じて、コンポーネントを交換します。使用しているアプライアンスハードウェアの設置とメンテナンスの手順を参照してください。<br>◦ "SG6000 ストレージアプライアンス"<br>◦ "SG5700 ストレージアプライアンス"<br>◦ "SG5600 ストレージアプライアンス"<br>◦ "SG100 SG1000サービスアプライアンス" |
| アプライアンスのコンピューティングコントローラを確認する必要があります | StorageGRID アプライアンスのコンピューティングコントローラでハードウェア障害が検出されました。<br><br>1. ハードウェアコンポーネントにエラーがないかどうかを確認し、推奨される対処方法に従います。<br>◦ SG100 、 SG1000 、または SG6000 を使用している場合は、 BMC を使用します。<br>◦ SG5600 または SG5700 を使用している場合は、 SANtricity System Manager を使用します。<br>2. 必要に応じて、コンポーネントを交換します。使用しているアプライアンスハードウェアの設置とメンテナンスの手順を参照してください。<br>◦ "SG6000 ストレージアプライアンス"<br>◦ "SG5700 ストレージアプライアンス"<br>◦ "SG5600 ストレージアプライアンス"<br>◦ "SG100 SG1000サービスアプライアンス" |

| アラート名 | 概要 および推奨される対処方法 |
| --- | --- |
| アプライアンスコンピューティングコントローラの電源装置 A に問題があります | コンピューティングコントローラの電源装置 A に問題があります。このアラートは、電源装置に障害が発生したか、電源の供給に問題があることを示している可能性があります。<br><br>1. ハードウェアコンポーネントにエラーがないかどうかを確認し、推奨される対処方法に従います。<br>◦ SG100 、 SG1000 、または SG6000 を使用している場合は、 BMC を使用します。<br>◦ SG5600 または SG5700 を使用している場合は、 SANtricity System Manager を使用します。<br>2. 必要に応じて、コンポーネントを交換します。使用しているアプライアンスハードウェアの設置とメンテナンスの手順を参照してください。<br>◦ "SG6000 ストレージアプライアンス"<br>◦ "SG5700 ストレージアプライアンス"<br>◦ "SG5600 ストレージアプライアンス"<br>◦ "SG100 SG1000サービスアプライアンス" |
| アプライアンスコンピューティングコントローラの電源装置 B に問題があります | コンピューティングコントローラの電源装置Bに問題があります。このアラートは、電源装置に障害が発生したか、電源の供給に問題があることを示している可能性があります。<br><br>1. ハードウェアコンポーネントにエラーがないかどうかを確認し、推奨される対処方法に従います。<br>◦ SG100 、 SG1000 、または SG6000 を使用している場合は、 BMC を使用します。<br>◦ SG5600 または SG5700 を使用している場合は、 SANtricity System Manager を使用します。<br>2. 必要に応じて、コンポーネントを交換します。使用しているアプライアンスハードウェアの設置とメンテナンスの手順を参照してください。<br>◦ "SG6000 ストレージアプライアンス"<br>◦ "SG5700 ストレージアプライアンス"<br>◦ "SG5600 ストレージアプライアンス"<br>◦ "SG100 SG1000サービスアプライアンス" |

| アラート名 | 概要 および推奨される対処方法 |
| --- | --- |
| アプライアンスコンピューティングハードウェアモニタのサービスが停止する | ストレージハードウェアのステータスを監視するサービスによってデータのレポートが停止されました。<br>1. ベース OS の EOS-system-status サービスのステータスを確認する。<br>2. サービスが停止またはエラー状態の場合は、サービスを再起動します。<br>3. このアラートが解決しない場合は、テクニカルサポートにお問い合わせください。 |
| アプライアンスのファイバ・チャネル障害が検出されました | アプライアンスのストレージコントローラとコンピューティングコントローラの間のFibre Channel接続に問題があります。<br>1. ハードウェアコンポーネントにエラーがないかどうかを確認します（* Nodes **>*_appliance node_name >** Hardware *）。いずれかのコンポーネントのステータスが「公称」でない場合は、次のアクションを実行します。<br>a. コントローラ間の Fibre Channel ケーブルが完全に接続されていることを確認します。<br>b. ファイバチャネルケーブルが過度に曲がっていないことを確認します。<br>c. SFP+ モジュールが正しく装着されていることを確認します。<br>▪ 注：* この問題が解決しない場合、StorageGRID システムは問題のある接続を自動的にオフラインにすることがあります。<br>2. 必要に応じて、コンポーネントを交換します。使用しているアプライアンスのインストールとメンテナンスの手順を参照してください。 |
| アプライアンスのファイバ・チャネル HBA ポート障害 | ファイバチャネルHBAポートで障害が発生しているか、障害が発生しています。テクニカルサポートにお問い合わせください。 |

| アラート名 | 概要 および推奨される対処方法 |
| --- | --- |
| アプライアンスのフラッシュキャッシュドライブが最適な状態でありません | SSD キャッシュに使用されているドライブが最適な状態でありません。<br><br>1. SSD キャッシュドライブを交換します。アプライアンスの設置とメンテナンスの手順を参照してください。<br>◦ "SG6000 ストレージアプライアンス"<br>◦ "SG5700 ストレージアプライアンス"<br>◦ "SG5600 ストレージアプライアンス"<br>2. このアラートが解決しない場合は、テクニカルサポートにお問い合わせください。 |
| アプライアンスインターコネクト / バッテリキャニスターが取り外されました | インターコネクト / バッテリキャニスターがありません。<br><br>1. バッテリを交換します。バッテリの取り外しと交換の手順は、アプライアンスの設置とメンテナンスの手順のストレージコントローラを交換するための手順 に含まれています。<br>◦ "SG6000 ストレージアプライアンス"<br>◦ "SG5700 ストレージアプライアンス"<br>◦ "SG5600 ストレージアプライアンス"<br>2. このアラートが解決しない場合は、テクニカルサポートにお問い合わせください。 |
| アプライアンスの LACP ポートがありません | StorageGRID アプライアンスのポートが LACP ボンドに参加していません。<br><br>1. スイッチの設定を確認します。インターフェイスが正しいリンクアグリゲーショングループに設定されていることを確認してください。<br>2. このアラートが解決しない場合は、テクニカルサポートにお問い合わせください。 |

| アラート名 | 概要 および推奨される対処方法 |
| --- | --- |
| アプライアンス全体の電源装置がデグレード状態になりました | StorageGRID アプライアンスの電源が、推奨される動作電圧から逸脱しています。<br><br>1. 電源装置 A と B のステータスを調べ、どちらの電源装置に異常があるかを確認し、推奨される対処方法に従います。<br>◦ SG100 、 SG1000 、または SG6000 を使用している場合は、 BMC を使用します。<br>◦ SG5600 または SG5700 を使用している場合は、 SANtricity System Manager を使用します。<br>2. 必要に応じて、コンポーネントを交換します。使用しているアプライアンスハードウェアの設置とメンテナンスの手順を参照してください。<br>◦ "SG6000 ストレージアプライアンス"<br>◦ "SG5700 ストレージアプライアンス"<br>◦ "SG5600 ストレージアプライアンス"<br>◦ "SG100 SG1000サービスアプライアンス" |
| アプライアンスストレージコントローラ A の障害 | StorageGRID アプライアンスのストレージコントローラ A で障害が発生した。<br><br>1. SANtricity System Manager を使用してハードウェアコンポーネントを確認し、推奨される対処方法に従います。<br>2. 必要に応じて、コンポーネントを交換します。使用しているアプライアンスハードウェアの設置とメンテナンスの手順を参照してください。<br>◦ "SG6000 ストレージアプライアンス"<br>◦ "SG5700 ストレージアプライアンス"<br>◦ "SG5600 ストレージアプライアンス" |

| アラート名 | 概要 および推奨される対処方法 |
| --- | --- |
| アプライアンスストレージコントローラ B の障害 | StorageGRID アプライアンスのストレージコントローラ B で障害が発生した。<br><br>1. SANtricity System Manager を使用してハードウェアコンポーネントを確認し、推奨される対処方法に従います。<br>2. 必要に応じて、コンポーネントを交換します。使用しているアプライアンスハードウェアの設置とメンテナンスの手順を参照してください。<br>◦ "SG6000 ストレージアプライアンス"<br>◦ "SG5700 ストレージアプライアンス"<br>◦ "SG5600 ストレージアプライアンス" |
| アプライアンスストレージコントローラのドライブ障害 | StorageGRID アプライアンスの 1 つ以上のドライブで障害が発生しているか、または最適な状態でありません。<br><br>1. SANtricity System Manager を使用してハードウェアコンポーネントを確認し、推奨される対処方法に従います。<br>2. 必要に応じて、コンポーネントを交換します。使用しているアプライアンスハードウェアの設置とメンテナンスの手順を参照してください。<br>◦ "SG6000 ストレージアプライアンス"<br>◦ "SG5700 ストレージアプライアンス"<br>◦ "SG5600 ストレージアプライアンス" |
| アプライアンスストレージコントローラハードウェア問題 | SANtricity ソフトウェアから、 StorageGRID アプライアンスのコンポーネントについて「 Needs Attention 」が報告されます。<br><br>1. SANtricity System Manager を使用してハードウェアコンポーネントを確認し、推奨される対処方法に従います。<br>2. 必要に応じて、コンポーネントを交換します。使用しているアプライアンスハードウェアの設置とメンテナンスの手順を参照してください。<br>◦ "SG6000 ストレージアプライアンス"<br>◦ "SG5700 ストレージアプライアンス"<br>◦ "SG5600 ストレージアプライアンス" |

| アラート名 | 概要 および推奨される対処方法 |
| --- | --- |
| アプライアンスストレージコントローラの電源装置 A に障害が発生しました | StorageGRID アプライアンスの電源装置 A が、推奨される動作電圧から逸脱しています。<br><br>1. SANtricity System Manager を使用してハードウェアコンポーネントを確認し、推奨される対処方法に従います。<br>2. 必要に応じて、コンポーネントを交換します。使用しているアプライアンスハードウェアの設置とメンテナンスの手順を参照してください。<br>◦ "SG6000 ストレージアプライアンス"<br>◦ "SG5700 ストレージアプライアンス"<br>◦ "SG5600 ストレージアプライアンス" |
| アプライアンスストレージコントローラの電源装置 B に障害が発生しました | StorageGRID アプライアンスの電源装置 B が、推奨される動作電圧から逸脱しています。<br><br>1. SANtricity System Manager を使用してハードウェアコンポーネントを確認し、推奨される対処方法に従います。<br>2. 必要に応じて、コンポーネントを交換します。使用しているアプライアンスハードウェアの設置とメンテナンスの手順を参照してください。<br>◦ "SG6000 ストレージアプライアンス"<br>◦ "SG5700 ストレージアプライアンス"<br>◦ "SG5600 ストレージアプライアンス" |
| アプライアンスストレージハードウェアモニタのサービスが停止する | ストレージハードウェアのステータスを監視するサービスによってデータのレポートが停止されました。<br><br>1. ベース OS の EOS-system-status サービスのステータスを確認する。<br>2. サービスが停止またはエラー状態の場合は、サービスを再起動します。<br>3. このアラートが解決しない場合は、テクニカルサポートにお問い合わせください。 |

| アラート名 | 概要 および推奨される対処方法 |
| --- | --- |
| アプライアンスストレージシェルフがデグレード状態になります | ストレージアプライアンスのストレージシェルフのいずれかのコンポーネントのステータスがデグレードになっています。<br><br>1. SANtricity System Manager を使用してハードウェアコンポーネントを確認し、推奨される対処方法に従います。<br>2. 必要に応じて、コンポーネントを交換します。使用しているアプライアンスハードウェアの設置とメンテナンスの手順を参照してください。<br>◦ "SG6000 ストレージアプライアンス"<br>◦ "SG5700 ストレージアプライアンス"<br>◦ "SG5600 ストレージアプライアンス" |
| アプライアンスの温度が超過しました | アプライアンスのストレージコントローラの公称温度または最大温度を超えました。<br><br>1. このノードに影響している別のアラートがないかを確認します。他のアラートを解決することで、このアラートが解決する可能性があります。<br>2. ファンや HVAC の故障など、温度上昇の考えられる原因を調査する。<br>3. このアラートが解決しない場合は、テクニカルサポートにお問い合わせください。 |
| アプライアンスの温度センサーが取り外されました | 温度センサーが取り外されました。テクニカルサポートにお問い合わせください。 |
| Cassandra 自動コンパクターエラーです | Cassandraの自動compactorでエラーが発生しました。Cassandraの自動compactorはすべてのストレージノードに存在し、オーバーライトおよび大量のワークロードを削除するためにCassandraデータベースのサイズを管理します。この状態が解消されない間は、特定のワークロードでメタデータの消費量が予期せずに増加します。<br><br>1. このノードに影響している別のアラートがないかを確認します。他のアラートを解決することで、このアラートが解決する可能性があります。<br>2. テクニカルサポートにお問い合わせください。 |

| アラート名 | 概要 および推奨される対処方法 |
| --- | --- |
| Cassandra 自動コンパクターメトリックが古くなっています | Cassandra の自動圧縮機能を説明する指標が最新ではありません。Cassandra の自動圧縮機能はすべてのストレージノードに存在し、オーバーライトや大量のワークロードの削除用に Cassandra データベースのサイズを管理します。このアラートが解決しない間、特定のワークロードでメタデータの使用量が予期せずに増加します。<br><br>1. このノードに影響している別のアラートがないかを確認します。他のアラートを解決することで、このアラートが解決する可能性があります。<br>2. テクニカルサポートにお問い合わせください。 |
| Cassandra 通信エラー | Cassandraサービスを実行するノード間の通信で問題が発生しています。このアラートは、ノード間の通信に干渉していることを示しています。1 つ以上のストレージノードでネットワーク問題 または Cassandra サービスが停止している可能性があります。<br><br>1. 1 つ以上のストレージノードに影響している別のアラートがないかを確認します。他のアラートを解決することで、このアラートが解決する可能性があります。<br>2. 1 つ以上のストレージノードに影響している可能性のあるネットワーク問題 がないかどうかを確認します。<br>3. Support **>** Tools **>** Grid Topology *を選択します。<br>4. システム内のストレージノードごとに、 * SSM * > * Services * を選択します。Cassandraサービスのステータスが「running」であることを確認します。<br>5. Cassandraが実行されていない場合は、リカバリとメンテナンスの手順のサービスを開始または再開する手順に従います。<br>6. Cassandra サービスのすべてのインスタンスが実行中でアラートが解決されない場合は、テクニカルサポートに連絡してください。<br><br>"" |

| アラート名 | 概要 および推奨される対処方法 |
| --- | --- |
| Cassandra の圧縮処理が過負荷です | Cassandraのコンパクションプロセスが過負荷状態です。コンパクションプロセスが過負荷の場合、読み取りパフォーマンスが低下し、RAMが使用される可能性があります。Cassandra サービスが応答しなくなったり、クラッシュしたりする可能性もあります。<br><br>1. リカバリとメンテナンスの手順のサービスを再起動する手順に従って、Cassandraサービスを再起動します。<br>2. このアラートが解決しない場合は、テクニカルサポートにお問い合わせください。<br><br>"" |
| Cassandra 修復指標が最新ではありません | Cassandra 修復ジョブを説明する指標が最新ではありません。この状況が 48 時間以上続く場合は、バケットのリストなどのクライアントクエリで削除されたデータが表示されることがあります。<br><br>1. ノードをリブートします。Grid Managerから* Nodes *に移動し、ノードを選択してTasksタブを選択します。<br>2. このアラートが解決しない場合は、テクニカルサポートにお問い合わせください。 |
| Cassandra の修復の進捗が遅い | Cassandraデータベースの修復の進捗状況が低速化しています。データベースの修復が低速化すると、Cassandraのデータ整合性処理が中断されます。この状況が 48 時間以上続く場合は、バケットのリストなどのクライアントクエリで削除されたデータが表示されることがあります。<br><br>1. すべてのストレージノードがオンラインで、ネットワーク関連のアラートがないことを確認します。<br>2. このアラートを最大 2 日間監視して、問題 が自動的に解決するかどうかを確認します。<br>3. データベースの修復に時間がかかる場合は、テクニカルサポートに連絡してください。 |

| アラート名 | 概要 および推奨される対処方法 |
| --- | --- |
| Cassandra 修復サービスを使用できません | Cassandra修復サービスは使用できません。Cassandra修復サービスはすべてのストレージノードに存在し、Cassandraデータベースに重要な修復機能を提供します。この状況が 48 時間以上続く場合は、バケットのリストなどのクライアントクエリで削除されたデータが表示されることがあります。<br><br>1. Support > Tools > Grid Topology *を選択します。<br>2. システム内のストレージノードごとに、 * SSM * > * Services * を選択します。Cassandra Reaper サービスのステータスが「 Running 」であることを確認します。<br>3. Cassandra Reaperが実行されていない場合は、リカバリとメンテナンスの手順のサービスを開始または再起動する手順に従います。<br>4. Cassandra Reaper サービスのすべてのインスタンスが実行中で、アラートが解決されない場合は、テクニカルサポートにお問い合わせください。<br><br>"" |
| クラウドストレージプールの接続エラー | クラウドストレージプールの健全性チェックで、新たなエラーが 1 つ以上検出されました。<br><br>1. ストレージプールページのクラウドストレージプールセクションに移動します。<br>2. Last Error 列を確認して、エラーが発生しているクラウドストレージプールを特定します。<br>3. 情報ライフサイクル管理を使用してオブジェクトを管理する手順を参照してください。<br><br>"ILM を使用してオブジェクトを管理する" |

| アラート名 | 概要 および推奨される対処方法 |
| --- | --- |
| DHCP リースの期限が切れました | ネットワークインターフェイスのDHCPリースが期限切れです。DHCPリースの期限が切れている場合は、推奨される対処方法に従います。<br><br>1. このノードと該当するインターフェイス上の DHCP サーバが接続されていることを確認してください。<br>2. DHCP サーバの影響を受けるサブネットで割り当てることができる IP アドレスがあることを確認します。<br>3. DHCP サーバで設定されている IP アドレスが永続的に予約されていることを確認します。または、 StorageGRID IP 変更ツールを使用して、 DHCP アドレスプールの外部に静的 IP アドレスを割り当てます。リカバリとメンテナンスの手順を参照してください。<br><br>"" |
| DHCP リースがまもなく期限切れになります | ネットワークインターフェイスのDHCPリースがまもなく期限切れになります。DHCPリースが期限切れにならないようにするには、推奨される対処方法に従います。<br><br>1. このノードと該当するインターフェイス上の DHCP サーバが接続されていることを確認してください。<br>2. DHCP サーバの影響を受けるサブネットで割り当てることができる IP アドレスがあることを確認します。<br>3. DHCP サーバで設定されている IP アドレスが永続的に予約されていることを確認します。または、 StorageGRID IP 変更ツールを使用して、 DHCP アドレスプールの外部に静的 IP アドレスを割り当てます。リカバリとメンテナンスの手順を参照してください。<br><br>"" |

| アラート名 | 概要 および推奨される対処方法 |
| --- | --- |
| DHCP サーバが使用できません | DHCPサーバが使用できません。StorageGRID ノードがDHCPサーバに接続できません。ノードの IP アドレスの DHCP リースを検証できません。<br><br>1. このノードと該当するインターフェイス上の DHCP サーバが接続されていることを確認してください。<br>2. DHCP サーバの影響を受けるサブネットで割り当てることができる IP アドレスがあることを確認します。<br>3. DHCP サーバで設定されている IP アドレスが永続的に予約されていることを確認します。または、 StorageGRID IP 変更ツールを使用して、DHCP アドレスプールの外部に静的 IP アドレスを割り当てます。リカバリとメンテナンスの手順を参照してください。<br><br>"" |
| ディスク I/O が非常に遅い | ディスク I/O が非常に遅いと、 StorageGRID のパフォーマンスに影響している可能性があります。<br><br>1. 問題 がストレージアプライアンスノードに関連している場合は、 SANtricity システムマネージャを使用して、障害が発生しているドライブ、予測される障害が発生しているドライブ、または進行中のドライブの修復を確認します。また、アプライアンスのコンピューティングコントローラとストレージコントローラ間のファイバチャネルまたは SAS リンクのステータスを調べて、リンクが停止しているか、エラー率が高いリンクが表示されていないかを確認します。<br>2. このノードのボリュームをホストしているストレージシステムを調べて、低速な I/O のルート原因を特定して修正します<br>3. このアラートが解決しない場合は、テクニカルサポートにお問い合わせください。<br><br>影響を受けるノードでは、グリッドの全体的なパフォーマンスへの影響を回避するために、サービスが無効になって、ノード自体原因となった状態が解消されて通常の I/O パフォーマンスが検出された場合は、フルサービスに自動的に戻ります。 |

| アラート名 | 概要 および推奨される対処方法 |
| --- | --- |
| E メール通知のエラーです | アラートのEメール通知を送信できませんでした。このアラートは、アラートEメール通知が失敗した場合、またはテストEメール（* Alerts > Email Setup * ページから送信）を配信できない場合にトリガーされます。<br><br>1. アラートの「 * Site/Node * 」列に表示されている管理ノードから Grid Manager にサインインします。<br>2. [アラート>*電子メール設定*]ページに移動し、設定を確認して、必要に応じて変更します。<br>3. [ テストメールの送信 ] をクリックし、テスト受信者の電子メールの受信ボックスを確認します。テスト用 E メールを送信できない場合は、このアラートの新しいインスタンスがトリガーされることがあります。<br>4. テスト用 E メールを送信できなかった場合は、 E メールサーバがオンラインであることを確認します。<br>5. サーバが動作している場合は、* Support > Tools > Logs *を選択し、管理ノードのログを収集します。アラートの前後 15 分の期間を指定します。<br>6. ダウンロードしたアーカイブを展開し、の内容を確認します `prometheus.log` (`_/GID<gid><time_stamp>/<site_node>/<time_stamp>/metrics/prometheus.log`)。<br>7. 問題を解決できない場合は、テクニカルサポートにお問い合わせください。 |
| クライアント証明書ページで設定された証明書の有効期限 | [クライアント証明書]ページで設定されている1つ以上の証明書の有効期限が近づいています。<br><br>1. [* Configuration > Access Control > Client Certificates *]を選択します。<br>2. 有効期限が近い証明書を選択してください。<br>3. 「* Edit *」を選択して、新しい証明書をアップロードまたは生成します。<br>4. 有効期限が近い証明書ごとに、上記の手順を繰り返します。<br><br>"StorageGRID の管理" |

| アラート名 | 概要 および推奨される対処方法 |
| --- | --- |
| ロードバランサエンドポイント証明書の有効期限 | 1 つ以上のロードバランサエンドポイント証明書の有効期限が近づいています。<br><br>1. [* Configuration > Network Settings > Load Balancer Endpoints *]を選択します。<br>2. まもなく期限切れになる証明書を含むエンドポイントを選択してください。<br>3. 「 * エンドポイントの編集」を選択して、新しい証明書をアップロードまたは生成します。<br>4. 証明書の有効期限が切れているエンドポイントまたはまもなく期限切れになるエンドポイントごとに、上記の手順を繰り返します。<br><br>ロードバランサエンドポイントの管理の詳細については、StorageGRID の管理手順を参照してください。<br><br>"StorageGRID の管理" |
| 管理インターフェイス用のサーバ証明書の有効期限 | 管理インターフェイスで使用されるサーバ証明書の有効期限が近づいています。<br><br>1. [* Configuration ]>[ Network Settings ]>[ Server Certificates*]を選択します。<br>2. 管理インターフェイスのサーバ証明書セクションで、新しい証明書をアップロードします。<br><br>"StorageGRID の管理" |
| ストレージAPIエンドポイント用のサーバ証明書の有効期限 | ストレージ API エンドポイントへのアクセスに使用されるサーバ証明書の有効期限が近づいています。<br><br>1. [* Configuration ]>[ Network Settings ]>[ Server Certificates*]を選択します。<br>2. Object Storage API Service EndpointsのServer Certificateセクションで、新しい証明書をアップロードします。<br><br>"StorageGRID の管理" |

| アラート名 | 概要 および推奨される対処方法 |
| --- | --- |
| Grid ネットワーク MTU が一致しません | グリッドネットワークインターフェイス（eth0）の最大伝送ユニット（MTU）設定は、グリッド内のノード間で大きく異なります。MTU設定の違いによって、eth0ネットワークの一部がジャンボフレーム用に設定されていることがわかります。MTU サイズが 1000 を超えると、原因 のネットワークパフォーマンスの問題が発生する可能性があります。<br><br>"Grid Network MTU mismatchアラートのトラブルシューティング" |
| Java ヒープの使用率が高い | Javaヒープスペースの使用率が高くなっています。Javaヒープがいっぱいになると、メタデータサービスが使用できなくなり、クライアント要求が失敗することがあります。<br><br>1. ダッシュボードで ILM アクティビティを確認します。このアラートは、 ILM ワークロードが減少すると自動的に解決する場合があります。<br>2. このノードに影響している別のアラートがないかを確認します。他のアラートを解決することで、このアラートが解決する可能性があります。<br>3. このアラートが解決しない場合は、テクニカルサポートにお問い合わせください。 |
| メタデータクエリのレイテンシが高くなっています | Cassandraメタデータクエリの平均時間が長すぎます。ディスクの交換などのハードウェアの変更や、取り込みの急増などのワークロードの変化が原因で、クエリのレイテンシが増加する可能性があります。<br><br>1. クエリのレイテンシが増大した時間帯にハードウェアやワークロードの変化がなかったかを確認します。<br>2. 問題を解決できない場合は、テクニカルサポートにお問い合わせください。 |

| アラート名 | 概要 および推奨される対処方法 |
| --- | --- |
| アイデンティティフェデレーションの同期に失敗する | アイデンティティソースからフェデレーテッドグループとフェデレーテッドユーザを同期できません。<br><br>1. 設定した LDAP サーバがオンラインで使用可能であることを確認します。<br>2. アイデンティティフェデレーションページの設定を確認します。すべての値が最新であることを確認します。StorageGRID の管理手順の「フェデレーテッドアイデンティティソースの設定」を参照してください。<br>3. ［ * 接続のテスト * ］ をクリックして、 LDAP サーバーの設定を確認します。<br>4. 問題 を解決できない場合は、テクニカルサポートにお問い合わせください。<br><br>"StorageGRID の管理" |

| アラート名 | 概要 および推奨される対処方法 |
| --- | --- |
| ILM 配置を実現できません | 特定のオブジェクトに対するILMルールの配置手順を実行できません。このアラートは、配置手順に必要なノードが使用できないか、ILMルールの設定が正しくないことを示しています。たとえば、レプリケートコピーをストレージノードよりも多く指定するルールがあるとします。<br><br>1. すべてのノードがオンラインであることを確認してください。<br>2. すべてのノードがオンラインの場合は、アクティブな ILM ポリシーを使用しているすべての ILM ルールの配置手順を確認します。すべてのオブジェクトに対して有効な手順があることを確認します。情報ライフサイクル管理を使用してオブジェクトを管理する手順を参照してください。<br>3. 必要に応じて、ルールの設定を更新し、新しいポリシーをアクティブ化します。<br><br>アラートがクリアされるまでに1日程度かかる場合があります。<br><br>4. 問題が解決しない場合は、テクニカルサポートにお問い合わせください。<br><br>このアラートはアップグレード中に表示され、アップグレードが正常に完了してから1日間は存続する場合があります。アップグレードによってこのアラートがトリガーされると、アラートは自動的にクリアされます。<br><br>"ILM を使用してオブジェクトを管理する" |

| アラート名 | 概要 および推奨される対処方法 |
| --- | --- |
| ILM のスキャン期間が長すぎます | オブジェクトのスキャン、評価、およびILMの適用に必要な時間が長すぎます。ILMによるすべてのオブジェクトのフルスキャンが完了するまでの推定時間が長すぎると（ダッシュボードの* Scan Period - Estimated *を参照）、アクティブなILMポリシーが新たに取り込まれたオブジェクトに適用されない可能性があります。ILM ポリシーへの変更が既存のオブジェクトに適用されない場合があります。<br><br>1. このノードに影響している別のアラートがないかを確認します。他のアラートを解決することで、このアラートが解決する可能性があります。<br>2. すべてのストレージノードがオンラインであることを確認します。<br>3. クライアントトラフィックの量を一時的に減らします。たとえば、グリッドマネージャから、**Configuration**>*Network Settings*>*Traffic Classification*を選択し、帯域幅または要求数を制限するポリシーを作成します。<br>4. ディスク I/O または CPU が過負荷状態の場合は、負荷を減らすか、リソースを増やしてください。<br>5. 必要に応じて、同期配置を使用するように ILM ルールを更新します（ StorageGRID 11.3 以降に作成されたルールのデフォルト）。<br>6. このアラートが解決しない場合は、テクニカルサポートにお問い合わせください。<br><br>"StorageGRID の管理" |

| アラート名 | 概要 および推奨される対処方法 |
| --- | --- |
| ILM のスキャン速度が低下しています | ILMのスキャン速度が100オブジェクト/秒未満に設定されています。このアラートは、システムのILMスキャン速度が1秒あたり100オブジェクト未満に変更されたことを示しています（デフォルト：400オブジェクト/秒）。新しく取り込まれたオブジェクトにはアクティブな ILM ポリシーが適用されない場合があります。以降に ILM ポリシーに対して行われた変更は、既存のオブジェクトには適用されません。<br><br>1. 継続的なサポート調査の一環として ILM スキャン率に一時的に変更が加えられたかどうかを確認します。<br>2. テクニカルサポートにお問い合わせください。<br><br>テクニカルサポートに連絡しなくても ILM のスキャン速度を変更しないでください。 |
| KMS CA 証明書の有効期限 | キー管理サーバ（ KMS ）証明書への署名に使用する CA 証明書の有効期限が近づいています。<br><br>1. KMS ソフトウェアを使用して、キー管理サーバの CA 証明書を更新します。<br>2. Grid Managerから、* Configuration > System Settings > Key Management Server *の順に選択します。<br>3. 証明書ステータスの警告がある KMS を選択します。<br>4. 「 * 編集 * 」を選択します。<br>5. 「 * 次へ * 」を選択して、手順 2 （サーバー証明書のアップロード）に進みます。<br>6. 新しい証明書をアップロードするには、 * Browse * を選択します。<br>7. [ 保存（ Save ） ] を選択します。<br><br>"StorageGRID の管理" |

| アラート名 | 概要 および推奨される対処方法 |
| --- | --- |
| KMS クライアント証明書の有効期限 | キー管理サーバのクライアント証明書の有効期限が近づいています。<br><br>1. Grid Managerから、* Configuration > System Settings > Key Management Server *の順に選択します。<br>2. 証明書ステータスの警告がある KMS を選択します。<br>3. 「 * 編集 * 」を選択します。<br>4. 「 * 次へ * 」を選択して、手順 3 （クライアント証明書のアップロード）に進みます。<br>5. 新しい証明書をアップロードするには、 * Browse * を選択します。<br>6. 新しい秘密鍵をアップロードするには、 * Browse * を選択します。<br>7. [ 保存（ Save ） ] を選択します。<br><br>"StorageGRID の管理" |
| KMS の設定をロードできませんでした | キー管理サーバの設定は存在しますが、ロードできませんでした。<br><br>1. このノードに影響している別のアラートがないかを確認します。他のアラートを解決することで、このアラートが解決する可能性があります。<br>2. このアラートが解決しない場合は、テクニカルサポートにお問い合わせください。 |

| アラート名 | 概要 および推奨される対処方法 |
| --- | --- |
| KMS 接続エラー | アプライアンスノードがサイトのキー管理サーバに接続できませんでした。<br><br>1. Grid Managerから、* Configuration > System Settings > Key Management Server *の順に選択します。<br>2. ポートおよびホスト名のエントリが正しいことを確認します。<br>3. サーバ証明書、クライアント証明書、およびクライアント証明書の秘密鍵が正しいかどうか、および有効期限が切れていないかどうかを確認します。<br>4. ファイアウォールの設定により、アプライアンスノードが指定された KMS と通信できることを確認してください。<br>5. ネットワークまたは DNS の問題を修正します。<br>6. サポートが必要な場合やアラートが解決しない場合は、テクニカルサポートにお問い合わせください。 |
| KMS 暗号化キー名が見つかりません | 設定されているキー管理サーバに、指定した名前と一致する暗号化キーがありません。<br><br>1. サイトに割り当てられている KMS が、暗号化キーと以前のバージョンに対応する正しい名前を使用していることを確認します。<br>2. サポートが必要な場合やアラートが解決しない場合は、テクニカルサポートにお問い合わせください。 |
| KMS 暗号化キーのローテーションに失敗しました | アプライアンスのすべてのボリュームが復号化されましたが、 1 つ以上のボリュームを最新のキーにローテーションできませんでした。テクニカルサポートにお問い合わせください。 |
| KMS は設定されていません | このサイトにはキー管理サーバがありません。<br><br>1. Grid Managerから、* Configuration > System Settings > Key Management Server *の順に選択します。<br>2. このサイトに KMS を追加するか、デフォルトの KMS を追加します。<br><br>"StorageGRID の管理" |

| アラート名 | 概要 および推奨される対処方法 |
| --- | --- |
| KMS キーでアプライアンスボリュームを復号化できませんでした | ノード暗号化が有効になっているアプライアンス上の 1 つ以上のボリュームを、現在の KMS キーで復号化できませんでした。<br><br>1. このノードに影響している別のアラートがないかを確認します。他のアラートを解決することで、このアラートが解決する可能性があります。<br>2. キー管理サーバ（ KMS ）に設定されている暗号化キーと以前のバージョンのキーがあることを確認します。<br>3. サポートが必要な場合やアラートが解決しない場合は、テクニカルサポートにお問い合わせください。 |
| KMS サーバ証明書の有効期限 | キー管理サーバ（ KMS ）で使用されるサーバ証明書の有効期限が近づいています。<br><br>1. KMS ソフトウェアを使用して、キー管理サーバのサーバ証明書を更新します。<br>2. サポートが必要な場合やアラートが解決しない場合は、テクニカルサポートにお問い合わせください。<br><br>"StorageGRID の管理" |
| 大規模な監査キュー | 監査メッセージのディスクキューがいっぱいです。<br><br>1. システムの負荷を確認します — 大量のトランザクションが発生した場合は ' 時間が経過するとアラートは自動的に解決され ' このアラートは無視してかまいません<br>2. アラートが解除されず重大度が上がった場合は、キューサイズのグラフを確認します。数時間から数日にわたって数値が増え続けている場合は、監査の負荷がシステムの監査キャパシティを超えている可能性があります。<br>3. クライアントの書き込みとクライアントの読み取りの監査レベルをErrorまたはOff（* Configuration > Monitoring > Audit *）に変更することで、クライアントの処理速度を下げるか、ログに記録される監査メッセージの数を減らします。<br><br>"監査ログを確認します" |

| アラート名 | 概要 および推奨される対処方法 |
| --- | --- |
| 監査ログのディスク容量が不足しています | 監査ログに使用できるスペースが少なくなっています。<br><br>1. このアラートを監視して、問題 が自動的に解決し、ディスクスペースが再び使用可能になるかどうかを確認します。<br>2. 使用可能なスペースが減少し続ける場合は、テクニカルサポートにお問い合わせください。 |
| 利用可能なノードメモリが少なくなっています | ノードの使用可能なRAMの容量が少なくなっています。使用可能なRAMが少ない場合は、ワークロードに変化があるか、1つ以上のノードでメモリリークが発生している可能性があります。<br><br>1. このアラートを監視して、問題 が自動的に解決するかどうかを確認します。<br>2. 使用可能なメモリが Major アラートのしきい値を下回った場合は、テクニカルサポートに連絡してください。 |
| ストレージプールの空き容量が不足しています | オブジェクトデータをストレージプールに格納できるスペースが少なくなっています。<br><br>1. ILM **>** Storage Pools *を選択します。<br>2. アラートに表示されたストレージプールを選択し、 * 詳細の表示 * を選択します。<br>3. 追加のストレージ容量が必要かどうかを判断ストレージプール内の各サイトにストレージノードを追加するか、 1 つ以上の既存のストレージノードにストレージボリューム（ LUN ）を追加できます。<br>4. 拡張手順 を実行してストレージ容量を増やします。<br><br>"グリッドを展開します" |

| アラート名 | 概要 および推奨される対処方法 |
| --- | --- |
| ノードメモリが不足しています | ノードに搭載されているメモリの量が少なくなっています。仮想マシンまたはLinuxホストで使用できるRAMの容量を増やしてください。Major アラートのしきい値を確認して、 StorageGRID ノードのデフォルトの最小要件を決定します。使用しているプラットフォームに対応したインストール手順を参照してください。<br><br>• "Red Hat Enterprise Linux または CentOS をインストールします"<br>• "Ubuntu または Debian をインストールします"<br>• "VMware をインストールする" |
| メタデータストレージが不足しています | オブジェクトメタデータを格納できるスペースが少なくなっています。* Criticalアラート*<br><br>1. オブジェクトの取り込みを停止します。<br>2. 拡張手順 にただちにストレージノードを追加します。<br>◦ 主要アラート *<br><br>拡張手順 にただちにストレージノードを追加します。<br><br>• Minor アラート *<br>1. オブジェクトメタデータスペースの使用率を監視します。ノード*>*ストレージノード*>*ストレージ*を選択し、使用済みストレージオブジェクトメタデータのグラフを表示します。<br>2. 拡張手順 にできるだけ早くストレージノードを追加します。<br><br>新しいストレージノードが追加されると、すべてのストレージノード間でオブジェクトメタデータが自動的にリバランシングされ、アラームが解除されます。<br><br>"Low metadata storageアラートのトラブルシューティング"<br><br>"グリッドを展開します" |

| アラート名 | 概要 および推奨される対処方法 |
| --- | --- |
| ディスク容量不足です | 指標データベースに使用できるスペースが少なくなっています。<br><br>1. このアラートを監視して、問題 が自動的に解決し、ディスクスペースが再び使用可能になるかどうかを確認します。<br>2. 使用可能なスペースが減少し続ける場合は、テクニカルサポートにお問い合わせください。 |
| オブジェクトデータのストレージが少ない | オブジェクトデータを格納できるスペースが少なくなっています。拡張手順 を実行してください。既存のストレージノードにストレージボリューム（ LUN ）を追加するか、または新しいストレージノードを追加することができます。<br><br>"Low object data storageアラートのトラブルシューティング"<br><br>"グリッドを展開します" |
| ルートディスク容量が不足しています | ルートディスクに使用できるスペースが少なくなっています。<br><br>1. このアラートを監視して、問題 が自動的に解決し、ディスクスペースが再び使用可能になるかどうかを確認します。<br>2. 使用可能なスペースが減少し続ける場合は、テクニカルサポートにお問い合わせください。 |
| システムのデータ容量が不足しています | ローカルファイルシステム/var/local上のStorageGRID システムデータに使用できるスペースが少なくなっています。<br><br>1. このアラートを監視して、問題 が自動的に解決し、ディスクスペースが再び使用可能になるかどうかを確認します。<br>2. 使用可能なスペースが減少し続ける場合は、テクニカルサポートにお問い合わせください。 |
| ノードのネットワーク接続エラー | nodes.Network間でのデータ転送中にエラーが発生した場合、手動操作なしに接続エラーがクリアされることがあります。エラーが解消されない場合は、テクニカルサポートにお問い合わせください。<br><br>"Network Receive Error（NRER）アラームのトラブルシューティングを行います" |

| アラート名 | 概要 および推奨される対処方法 |
| --- | --- |
| ノードネットワーク受信フレームエラー | ノードで受信したネットワークフレームの割合が高いとエラーが発生しました。このアラートは、ケーブル不良やイーサネット接続のいずれかの端のトランシーバ不良など、ハードウェア問題 であることを示している可能性があります。<br><br>1. アプライアンスを使用している場合は、 SFP+ または SFP28 トランシーバとケーブルを 1 本ずつ交換し、アラートが解除されるかどうかを確認します。<br>2. このアラートが解決しない場合は、テクニカルサポートにお問い合わせください。 |
| ノードが NTP サーバと同期されていません | ノードの時刻がネットワークタイムプロトコル（ NTP ）サーバと同期されていません。<br><br>1. Stratum 3 以上の外部 NTP サーバが 4 つ以上指定されていることを確認します。<br>2. すべての NTP サーバが正常に動作していることを確認します。<br>3. NTP サーバへの接続を確認します。ファイアウォールによってブロックされていないことを確認してください。 |
| NTP サーバでノードがロックされていません | ノードがネットワークタイムプロトコル（ NTP ）サーバにロックされていません。<br><br>1. Stratum 3 以上の外部 NTP サーバが 4 つ以上指定されていることを確認します。<br>2. すべての NTP サーバが正常に動作していることを確認します。<br>3. NTP サーバへの接続を確認します。ファイアウォールによってブロックされていないことを確認してください。 |
| 非アプライアンスノードネットワークが停止しています | 1 つ以上のネットワークデバイスが停止しているか切断されています。仮想マシンまたは Linux ホストにインストールされているノードのネットワークインターフェイス（ eth ）にアクセスできないことを示すアラートが表示されます。<br><br>テクニカルサポートにお問い合わせください。 |

| アラート名 | 概要 および推奨される対処方法 |
| --- | --- |
| オブジェクトが失われた | グリッドから1つ以上のオブジェクトが失われています。このアラートは、データが永続的に失われて読み出しできなくなったことを示している可能性があります。<br><br>1. このアラートはすぐに調査してください。これ以上のデータ損失を防ぐための対処が必要になる場合があります。迅速に対処すれば、損失オブジェクトをリストアできる場合もあります。<br><br>"オブジェクトデータの損失と欠落が発生した場合のトラブルシューティング"<br><br>2. 原因となっている問題を解決したら、カウンタをリセットします。<br><br>a. Support **>** Tools **>** Grid Topology *を選択します。<br><br>b. アラートを生成したストレージノードに対して、 * _site _ * > * _grid node_name * > * LDR * > * Data Store * > * Configuration * > * Main * の順に選択します。<br><br>c. [ * Lost Objects Count * ] を選択し、 [ * Apply Changes * ] をクリックします。 |
| プラットフォームサービスを利用できません | RSMサービスを搭載したストレージノードが少なすぎて、サイトで稼働中または使用可能です。該当するサイトでRSMサービスを搭載したストレージノードの大部分がエラーのない状態で稼働していることを確認してください。<br><br>StorageGRID の管理手順の「プラットフォームサービスのトラブルシューティング」を参照してください。<br><br>"StorageGRID の管理" |

| アラート名 | 概要 および推奨される対処方法 |
| --- | --- |
| 管理ネットワークポート 1 のサービスアプライアンスリンクが停止しています | アプライアンスの管理ネットワークポート 1 が停止しているか切断されています。<br><br>1. 管理ネットワークポート 1 に接続されているケーブルと物理的な接続を確認します。<br>2. 接続の問題に対処します。使用しているアプライアンスハードウェアの設置とメンテナンスの手順を参照してください。<br>3. このポートが目的で切断されている場合は、このルールを無効にします。Grid Managerから* Alerts > Alert Rules を選択し、ルールを選択して Edit rule をクリックします。次に、 **[*enabled]** チェックボックスをオフにします。<br>◦ "SG100 SG1000サービスアプライアンス"<br>◦ "アラートルールを無効にします" |
| 管理ネットワーク（またはクライアントネットワーク）上のサービスアプライアンスのリンクがダウン | 管理ネットワーク（ eth1 ）またはクライアントネットワーク（ eth2 ）へのアプライアンスインターフェイスが停止しているか切断されている。<br><br>1. StorageGRID ネットワークへのケーブル、 SFP 、および物理接続を確認します。<br>2. 接続の問題に対処します。使用しているアプライアンスハードウェアの設置とメンテナンスの手順を参照してください。<br>3. このポートが目的で切断されている場合は、このルールを無効にします。Grid Managerから* Alerts > Alert Rules を選択し、ルールを選択して Edit rule をクリックします。次に、 **[*enabled]** チェックボックスをオフにします。<br>◦ "SG100 SG1000サービスアプライアンス"<br>◦ "アラートルールを無効にします" |

| アラート名 | 概要 および推奨される対処方法 |
| --- | --- |
| サービスアプライアンスは、ネットワークポート 1 、 2 、 3 、または 4 でリンクダウンします | アプライアンスのネットワークポート 1 、 2 、 3 、または 4 が停止しているか、切断されています。<br><br>1. StorageGRID ネットワークへのケーブル、 SFP 、および物理接続を確認します。<br>2. 接続の問題に対処します。使用しているアプライアンスハードウェアの設置とメンテナンスの手順を参照してください。<br>3. このポートが目的で切断されている場合は、このルールを無効にします。Grid Managerから* Alerts > Alert Rules を選択し、ルールを選択して Edit rule をクリックします。次に、 **[*enabled]** チェックボックスをオフにします。<br>◦ "SG100 SG1000サービスアプライアンス"<br>◦ "アラートルールを無効にします" |
| サービスアプライアンスストレージの接続がデグレードされました | サービスアプライアンス内の2つのSSDのうちの1つで障害が発生したか、もう一方と同期が外れています。アプライアンスの機能には影響はありませんが、問題 にはすぐに対処する必要があります。両方のドライブに障害が発生すると、アプライアンスは動作しなくなります。<br><br>1. Grid Managerから、* Nodes *>***_services applie__**を選択し、 Hardware *タブを選択します。<br>2. Storage RAID Mode * フィールドでメッセージを確認します。<br>3. メッセージに再同期処理の進捗が表示された場合は、処理が完了するのを待ってから、アラートが解決したことを確認します。再同期メッセージは、 SSD が最近交換されたこと、または別の理由で再同期中であることを示します。<br>4. いずれかの SSD で障害が発生したことを示すメッセージが表示された場合は、障害が発生したドライブをできるだけ早く交換します。<br><br>サービスアプライアンスのドライブを交換する方法については、 SG100 および SG1000 アプライアンスのインストールおよびメンテナンスガイドを参照してください。<br><br>"SG100 SG1000サービスアプライアンス" |

| アラート名 | 概要 および推奨される対処方法 |
| --- | --- |
| 管理ネットワークポート 1 のストレージアプライアンスのリンクが停止しています | アプライアンスの管理ネットワークポート 1 が停止しているか切断されています。<br><br>1. 管理ネットワークポート 1 に接続されているケーブルと物理的な接続を確認します。<br>2. 接続の問題に対処します。使用しているアプライアンスハードウェアの設置とメンテナンスの手順を参照してください。<br>3. このポートが目的で切断されている場合は、このルールを無効にします。Grid Managerから* Alerts > Alert Rules を選択し、ルールを選択して Edit rule をクリックします。次に、 **[*enabled]** チェックボックスをオフにします。<br>◦ "SG6000 ストレージアプライアンス"<br>◦ "SG5700 ストレージアプライアンス"<br>◦ "SG5600 ストレージアプライアンス"<br>◦ "アラートルールを無効にします" |
| 管理ネットワーク（またはクライアントネットワーク）でのストレージアプライアンスのリンクが停止 | 管理ネットワーク（ eth1 ）またはクライアントネットワーク（ eth2 ）へのアプライアンスインターフェイスが停止しているか切断されている。<br><br>1. StorageGRID ネットワークへのケーブル、 SFP 、および物理接続を確認します。<br>2. 接続の問題に対処します。使用しているアプライアンスハードウェアの設置とメンテナンスの手順を参照してください。<br>3. このポートが目的で切断されている場合は、このルールを無効にします。Grid Managerから* Alerts > Alert Rules を選択し、ルールを選択して Edit rule をクリックします。次に、 **[*enabled]** チェックボックスをオフにします。<br>◦ "SG6000 ストレージアプライアンス"<br>◦ "SG5700 ストレージアプライアンス"<br>◦ "SG5600 ストレージアプライアンス"<br>◦ "アラートルールを無効にします" |

| アラート名 | 概要 および推奨される対処方法 |
| --- | --- |
| ネットワークポート 1 、 2 、 3 、または 4 でストレージアプライアンスのリンクが停止しています | アプライアンスのネットワークポート 1 、 2 、 3 、または 4 が停止しているか、切断されています。<br><br>1. StorageGRID ネットワークへのケーブル、 SFP 、および物理接続を確認します。<br>2. 接続の問題に対処します。使用しているアプライアンスハードウェアの設置とメンテナンスの手順を参照してください。<br>3. このポートが目的で切断されている場合は、このルールを無効にします。Grid Managerから* Alerts > Alert Rules を選択し、ルールを選択して Edit rule をクリックします。次に、 **[*enabled]** チェックボックスをオフにします。<br>◦ "SG6000 ストレージアプライアンス"<br>◦ "SG5700 ストレージアプライアンス"<br>◦ "SG5600 ストレージアプライアンス"<br>◦ "アラートルールを無効にします" |
| ストレージアプライアンスストレージの接続がデグレードされました | コンピューティングコントローラとストレージコントローラの間の接続に問題があります。<br><br>1. アプライアンスに移動して、ポートのインジケータライトを確認します。<br>2. ポートの LED が消灯している場合は、ケーブルが正しく接続されていることを確認します。必要に応じて、ケーブルを交換します。<br>3. 最大 5 分待ちます。<br><br>2本目のケーブルを交換する必要がある場合は、5分以上プラグを取り外さないでください。そうしないと、ルートボリュームが読み取り専用になり、ハードウェアの再起動が必要になることがあります。<br><br>4. Grid Managerから* Nodes *を選択します。次に、問題があるノードの Hardware タブを選択します。アラート状態が解決したことを確認します。 |

| アラート名 | 概要 および推奨される対処方法 |
| --- | --- |
| ストレージデバイスにアクセスできません | ストレージデバイスにアクセスできません。このアラートは、基盤となるストレージデバイスの問題が原因でボリュームをマウントまたはアクセスできないことを示します。<br><br>1. ノードに使用されているすべてのストレージデバイスのステータスを確認します。<br>◦ ノードが仮想マシンまたは Linux ホストにインストールされている場合は、オペレーティングシステムに応じた手順に従って、ハードウェアの診断を実行するか、ファイルシステムのチェックを実行します。<br>▪ "Red Hat Enterprise Linux または CentOS をインストールします"<br>▪ "Ubuntu または Debian をインストールします"<br>▪ "VMware をインストールする"<br>◦ ノードが SG100 、 SG1000 、または SG6000 アプライアンスに設置されている場合は、 BMC を使用します。<br>◦ ノードが SG5600 アプライアンスまたは SG5700 アプライアンスにインストールされている場合は、 SANtricity System Manager を使用します。<br>2. 必要に応じて、コンポーネントを交換します。使用しているアプライアンスハードウェアの設置とメンテナンスの手順を参照してください。<br>◦ "SG6000 ストレージアプライアンス"<br>◦ "SG5700 ストレージアプライアンス"<br>◦ "SG5600 ストレージアプライアンス" |

| アラート名 | 概要 および推奨される対処方法 |
| --- | --- |
| テナントクォータの使用率が高い | テナントクォータスペースの使用率が高くなっています。テナントのクォータを超えると、新しい取り込みは拒否されます。<br><br>多数の通知が生成される可能性があるため、このアラートルールはデフォルトで無効になっています。<br><br>1. Grid Managerから* tenants *を選択します。<br>2. テーブルを * クォータ使用率 * でソートします。<br>3. クォータ使用率が 100% に近いテナントを選択します。<br>4. 次のいずれか、または両方を実行します。<br>◦ 「 * Edit * 」を選択して、テナントのストレージ・クォータを増やします。<br>◦ クォータ使用率が高いことをテナントに通知します。 |

| アラート名 | 概要 および推奨される対処方法 |
| --- | --- |
| ノードと通信できません | 1つ以上のサービスが応答していないか、ノードに到達できません。このアラートは、ノードが不明な理由で切断されたことを示しています。たとえば、ノードのサービスが停止したり、電源障害や予期しない停止によってノードのネットワーク接続が失われたりする場合があります。<br><br>このアラートを監視して、問題 が自動的に解決するかどうかを確認します。問題 が維持される場合は、次の手順<br><br>1. このノードに影響している別のアラートがないかを確認します。他のアラートを解決することで、このアラートが解決する可能性があります。<br>2. このノードですべてのサービスが実行されていることを確認します。サービスが停止している場合は、開始してみてください。リカバリとメンテナンスの手順を参照してください。<br>3. ノードのホストの電源がオンになっていることを確認します。表示されない場合は、ホストを起動します。<br><br>ⓘ 複数のホストの電源がオフになっている場合は、リカバリとメンテナンスの手順を参照してください。<br><br>4. このノードと管理ノードの間にネットワーク接続問題 があるかどうかを確認します。<br>5. このアラートを解決できない場合は、テクニカルサポートにお問い合わせください。<br><br>"" |
| 予期しないノードのリブートです | 過去 24 時間以内にノードが予期せずリブートされました。<br><br>1. このアラートを監視します。このアラートは 24 時間後にクリアされます。ただし、ノードが予期せずにリブートされた場合、このアラートは再度トリガーされます。<br>2. アラートを解決できない場合は、ハードウェア障害が発生している可能性があります。テクニカルサポートにお問い合わせください。 |

| アラート名 | 概要 および推奨される対処方法 |
| --- | --- |
| 未識別の破損オブジェクトが検出されました | レプリケートオブジェクトストレージにファイルが見つかりましたが、レプリケートオブジェクトとして識別できませんでした。<br><br>1. ストレージノード上の基盤となるストレージに問題がないかどうかを確認します。たとえば、ハードウェア診断を実行するか、ファイルシステムチェックを実行します。<br>2. ストレージの問題を解決したら、フォアグラウンド検証を実行してオブジェクトが欠落しているかどうかを確認し、可能であれば置き換えます。<br>3. このアラートを監視します。このアラートは 24 時間後にクリアされますが、問題 が修正されていない場合は再度トリガーされます。<br>4. このアラートを解決できない場合は、テクニカルサポートにお問い合わせください。<br><br>"フォアグラウンド検証を実行しています" |

- 関連情報 *

"よく使用される Prometheus 指標"

よく使用される **Prometheus** 指標

管理ノードの Prometheus サービスは、すべてのノード上のサービスから時系列の指標を収集します。Prometheus は 1 、 000 件以上の指標を収集しますが、 StorageGRID の最も重要な処理を監視するために必要な指標は比較的少数です。

次の表に、最もよく使用されるPrometheus指標と、各指標に対応する属性（アラームシステムで使用）を示します。

このリストを参照して、デフォルトのアラートルールの条件を把握したり、カスタムのアラートルールの条件を作成したりできます。すべての指標の一覧を表示するには、* Help > API Documentation *を選択します。

名前に *private* が含まれる指標は内部専用です。 StorageGRID のリリースごとに予告なく変更されることがあります。

Prometheus指標の保存期間は31日です。

| **Prometheus** 指標 | 説明 |
| --- | --- |
| alertmanager_notifications_failed_total | 失敗したアラート通知の総数。 |

| **Prometheus** 指標 | 説明 |
| --- | --- |
| Node_filesystem_avail_bytes です | root 以外のユーザが使用できるファイルシステムスペースのバイト数。 |
| node_memory_MemAvailable_bytes | Memory information （メモリ情報）フィールド MemAvailable_bytes 。 |
| Node_network_carrier | /sys/class/net/<iface> のキャリア値。 |
| Node_network_receate_errs_total | ネットワークデバイスの統計受信エラー。 |
| Node_network_transmit_errs_total | ネットワークデバイス統計 transmit_errs 。 |
| storagegrid_administrative_down | 想定内の理由でノードがグリッドに接続されていません。たとえば、ノードまたはノード上のサービスが正常にシャットダウンされた、ノードがリブート中である、ソフトウェアのアップグレード中であるなどの原因が考えられます。 |
| storagegrid_apply_compute_controller_hardware_status | アプライアンスのコンピューティングコントローラハードウェアのステータス。 |
| storagegrid_apply_failed_disks を指定します | アプライアンス内のストレージコントローラの、最適な状態でないドライブの数。 |
| storagegrid_apply_storage_controller_hardware_status | アプライアンス内のストレージコントローラハードウェアの全体的なステータス。 |
| storagegrid_content_bbuckets_or_containers | このストレージノードによって認識されている S3 バケットと Swift コンテナの総数。 |
| storagegrid_content_objects を参照してください | このストレージノードによって認識されている S3 および Swift データオブジェクトの総数。S3 または Swift 経由でシステムとやり取りするクライアントアプリケーションで作成されたデータオブジェクトのみが対象です。 |
| storagegrid_content_objects_lost | StorageGRID システムに存在しないことが検出されたオブジェクトの合計数。損失の原因 を特定し、リカバリが可能かどうかを確認する必要があります。<br><br>"オブジェクトデータの損失と欠落が発生した場合のトラブルシューティング" |
| storagegrid_http_session_ining_attempted 」というメッセージが表示されます | ストレージノードに対して試行された HTTP セッションの総数。 |

| **Prometheus** 指標 | 説明 |
| --- | --- |
| storagegrid_http_session_ining_currently established | ストレージノード上で現在アクティブな（開いている） HTTP セッションの数。 |
| storagegrid_http_session_ining_failed | 不正な形式の HTTP 要求または処理中のエラーが原因で、正常に完了しなかった HTTP セッションの総数。 |
| storagegrid_http_session_ining_successful | 正常に完了した HTTP セッションの総数。 |
| storagegrid_ilm_Awaiting _background_objects | スキャンによる ILM に評価を待機しているこのノード上のオブジェクトの合計数です。 |
| storagegrid_ilm_Awaiting _client_evaluation_objects_per_second | このノードで ILM ポリシーに照らしてオブジェクトが評価されている現在の速度です。 |
| storagegrid_ilm_Awaiting _client_objects | クライアント処理（取り込みなど）の ILM に評価を待機しているこのノード上のオブジェクトの合計数です。 |
| storagegrid_ilm_Awaiting _total_objects | ILM 評価を待っているオブジェクトの合計数です。 |
| storagegrid_ilm_scan_objects_per_second | このノードが所有するオブジェクトが ILM 用にスキャンされてキューに登録される速度です。 |
| storagegrid_ilm_scan_periodEstimated _ minutes （ StorageGRID _ ILM _ スキャン期間 _ 推定 _ 分） | このノードで ILM のフルスキャンが完了するまでの推定時間です。<br>• 注： * フルスキャンは、このノードが所有するすべてのオブジェクトに ILM が適用されたことを保証するものではありません。 |
| storagegrid_load-balancer _endpoint_cert_expiry_time | エポックからのロードバランサエンドポイント証明書の有効期限（秒数）。 |
| storagegrid_meta_query_average _latency _milliseconds | このサービスを使用してメタデータストアに対してクエリを実行するのに必要な平均時間。 |
| storagegrid_network_received_bytes | インストール後に受信したデータの総容量。 |
| storagegrid_network_transmitted _bytes | インストール後に送信されたデータの総容量。 |

| **Prometheus** 指標 | 説明 |
| --- | --- |
| storagegrid_ntp_Chosen_time_source_offset_milliseconds | 選択した時間ソースによって提供される体系的な時間オフセット。オフセットは、時間ソースに到達するまでの遅延が、時間ソースが NTP クライアントに到達するために必要な時間と等しくない場合に適用されます。 |
| storagegrid_ntp_locked | ノードがネットワークタイムプロトコル（ NTP ）サーバにロックされていません。 |
| storagegrid_s3_data_transfers _bytes_取り込み 済み | 属性の前回リセット後に S3 クライアントからこのストレージノードに取り込まれたデータの総容量。 |
| storagegrid_s3_data_transfers *bytes* Retrieved 」のように表示されます | 属性の前回リセット後に S3 クライアントがこのストレージノードから読み出したデータの総容量。 |
| storagegrid_s3_operations_failed 」というエラーが表示されます | 失敗した S3 処理（ HTTP ステータスコード 4xx と 5xx ）の総数。 S3 の認証エラーが原因のものは除きます。 |
| storagegrid_s3_operations_successful | 成功した S3 処理（ HTTP ステータスコード 2xx ）の総数。 |
| storagegrid_s3_operations_unauthorized | 認証エラーが原因で失敗した S3 処理の総数。 |
| storagegrid_servercertificate_management_interface_cert_expiry_days のように指定します | 管理インターフェイス証明書が期限切れになるまでの日数。 |
| storagegrid_servercertificate_storage_api_endpoints_cert_expiry_days のように指定します | オブジェクトストレージ API 証明書が期限切れになるまでの日数。 |
| storagegrid_service_cpu_seconds で指定します | インストール後にこのサービスが CPU を使用した時間の累計。 |
| storagegrid_service_load | 使用可能な CPU 時間のうち、このサービスが現在使用している割合。サービスのビジー状態を示します。使用可能な CPU 時間は、サーバの CPU 数によって異なります。 |
| storagegrid_service_memory_usage_bytes | このサービスが現在使用しているメモリ（ RAM ）の容量。この値は、 Linux の top ユーティリティで RES として表示される値と同じです。 |
| storagegrid_service_network_received_bytes | インストール後にこのサービスが受信したデータの総容量。 |

| **Prometheus** 指標 | 説明 |
| --- | --- |
| storagegrid_service_network_transmitted バイト数 | このサービスから送信されたデータの総容量。 |
| storagegrid_service_restarts | サービスが再起動された回数。 |
| storagegrid_service_runtime_seconds | インストール後にサービスが実行されていた合計時間。 |
| storagegrid_service_uptime</1> を指定します | 前回のサービス再起動以降にサービスが実行されていた時間の合計。 |
| storagegrid_storage_state_current | ストレージサービスの現在の状態。属性値は次のとおりです。<br>• 10 = オフライン<br>• 15 = メンテナンス<br>• 20 = 読み取り専用<br>• 30 = オンライン |
| storagegrid_storage_status のように指定します | ストレージサービスの現在のステータス。属性値は次のとおりです。<br>• 0 = エラーなし<br>• 10 = 移行中<br>• 20 = 空きスペースが不足しています<br>• 30 = ボリュームを使用できません<br>• 40= エラー |
| storagegrid_storage_utilization_metadata_bytes | ストレージノード上のレプリケートオブジェクトデータとイレイジャーコーディングオブジェクトデータの推定合計サイズ。 |
| storagegrid_storage_utilization_meta_allowed_bytes | オブジェクトメタデータに使用できる各ストレージノードのボリューム 0 上の合計スペース。この値は、ノードでメタデータ用にリザーブされている実際のスペースよりも常に小さくなります。これは、重要なデータベース処理（コンパクションや修復など）や将来のハードウェアおよびソフトウェアのアップグレードに必要なリザーブスペースの一部が必要なためです。オブジェクトメタデータ用の許可スペースは、オブジェクトの全体的な容量を制御します。 |

| Prometheus 指標 | 説明 |
| --- | --- |
| storagegrid_storage_utilization_metadata_bytes | ストレージボリューム 0 上のオブジェクトメタデータのバイト数。 |
| storagegrid_storage_utilization_meta_reserved_bytes | 各ストレージノードのボリューム0上の、オブジェクトメタデータ用に実際にリザーブされている合計スペース。ある特定のストレージノードについて、メタデータ用に実際にリザーブされるスペースは、ノードのボリューム0のサイズとシステム全体のMetadata Reserved Space設定によって異なります。 |
| storagegrid_storage_utilization_total_space_bytes | すべてのオブジェクトストアに割り当てられているストレージスペースの総容量。 |
| storagegrid_storage_utilization_usable_space_bytes | オブジェクトストレージスペースの残り容量。ストレージノード上のすべてのオブジェクトストアの使用可能スペースを合計して算出されます。 |
| storagegrid_swify_data_transfers _bytes_取り込み 済み | 属性の前回リセット以降にこのストレージノードに取り込まれたデータの総容量。 |
| storagegrid_wift_data_transfers _byts_retrieved | 属性の前回リセット後に Swift クライアントがこのストレージノードから読み出したデータの総容量。 |
| storagegrid_swift_operations_failed 」というエラーが発生しました | 失敗した Swift 処理（ HTTP ステータスコード 4xx と 5xx ）の総数。 Swift の認証エラーが原因のものは除きます。 |
| storagegrid_swift_operations_successful | 成功した Swift 処理（ HTTP ステータスコード 2xx ）の総数。 |
| storagegrid_swift_operations_unauthorized | 認証エラーが原因で失敗した Swift 処理（ HTTP ステータスコード 401 、 403 、 405 ）の総数。 |
| storagegrid_stenantUsagedata_bytes | テナントのすべてのオブジェクトの論理サイズ。 |
| storagegrid_stenantUsageobject_count | テナントのオブジェクトの数。 |
| storagegrid_tenant_dusation_QUOTA_bytes | テナントのオブジェクトに使用できる論理スペースの最大容量。クォータ指標を指定しない場合、使用可能なスペースは無制限です。 |

## アラーム一覧（従来のシステム）

次の表に、これらの従来のデフォルトアラームをすべて示します。アラームがトリガー

された場合は、この表のアラームコードを参照して、推奨される対処方法を確認できます。

従来のアラームシステムは引き続きサポートされますが、アラートシステムには大きなメリットがあり、使いやすくなっています。

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| ABRL | 使用可能な属性リレー | BADC 、 BAMS 、 BARC 、 BCLB 、 BCMN 、 BCMN 、 BLDR 、 BNMS 、 BSSM 、 BDDS | Attribute Relay Service を実行しているサービス（ ADC サービス）への接続をできるだけ早くリストアします。属性リレーが接続されていないと、グリッドノードから NMS サービスに属性の値をレポートできません。そのため、 NMS サービスでサービスのステータスの監視やサービスの属性の更新を行うことができなくなります。<br><br>問題が解決しない場合は、テクニカルサポートにお問い合わせください。 |
| ACMS | 使用可能なメタデータサービス | BARC 、 BLDR 、 BCMN | LDR サービスまたは ARC サービスからの DDS サービスへの接続が失われた場合にアラームがトリガーされます。この場合、取り込みや読み出しのトランザクションを処理できません。DDS サービスを使用できない状態が短時間の一時問題 のみである場合は、トランザクションが遅延する可能性があります。<br><br>このアラームを解除し、サービスのすべての機能を復旧するには、 DDS サービスへの接続を確認してリストアします。 |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| ACTS | クラウドの階層化サービスのステータス | 円弧（ Arc ） | ターゲットタイプが「 Cloud Tiering - Simple Storage Service （ S3 ）」のアーカイブノードにのみ適用されます。<br><br>アーカイブノードの ACTS 属性が「 Read-Only Enabled 」または「 Read-Write Disabled 」に設定されている場合、「 Read-Write Enabled 」に設定する必要があります。<br><br>認証エラーによって Major アラームがトリガーされた場合は、デスティネーションバケットに関連付けられているクレデンシャルを確認し、必要に応じて値を更新します。<br><br>それ以外の理由で Major アラームがトリガーされた場合は、テクニカルサポートに連絡してください。 |
| ADCA | ADC ステータス | ADC | アラームがトリガーされた場合は、* Support **>** Tools **>** Grid Topology を選択します。次に、 ***site _ * > * _ grid node*** > * ADC * > * Overview * > * Main * and * ADC * > * Alarms * > * Main * を選択して、アラームの原因 を確認します。<br><br>問題が解決しない場合は、テクニカルサポートにお問い合わせください。 |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| ADCE | ADC State のことです | ADC | 「ADC State 」の値が「Standby 」の場合は、しばらくサービスを監視し、問題が解決しなければテクニカルサポートに連絡します。<br><br>「ADC State 」の値が「Offline 」の場合は、サービスを再起動します。問題が解決しない場合は、テクニカルサポートにお問い合わせください。 |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| AITE | 読み出し状態 | BARC | ターゲットタイプが「 Tivoli Storage Manager （ TSM ）」のアーカイブノードにのみ適用されます。<br><br>「 Retrieve State 」の値が「 Waiting for Target 」の場合は、 TSM ミドルウェアサーバを調べ、正常に動作していることを確認します。アーカイブノードを StorageGRID システムに追加したばかりの場合は、アーカイブノードから対象の外部アーカイブストレージシステムへの接続が正しく設定されていることを確認します。<br><br>「 Archive Retrieve State 」の値が「 Offline 」の場合は、状態を「 Online 」に更新できるか試します。 Support **>** Tools **>** Grid Topology を選択します。次に、 ***site*** **_ * > * _** ***grid node*** > * ARC * > * Retrieve * > * Configuration * > * Main * を選択し、 * Archive Retrieve State * > * Online * を選択して、 * Apply Changes * をクリックします。<br><br>問題が解決しない場合は、テクニカルサポートにお問い合わせください。 |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| AITU | ステータスを取得します | BARC | 「 Retrieve Status 」の値が「 Target Error 」の場合は、対象の外部アーカイブストレージシステムにエラーがないかを確認します。<br><br>「 Archive Retrieve Status 」の値が「 Session Lost 」の場合は、対象の外部アーカイブストレージシステムがオンラインで正常に動作していることを確認します。ターゲットとのネットワーク接続を確認します。<br><br>「 Archive Retrieve Status 」の値が「 Unknown Error 」の場合は、テクニカルサポートに連絡してください。 |
| ALIS | インバウンド属性セッション | ADC | 属性リレーのインバウンド属性セッション数が大幅に増加している場合、StorageGRID システムのバランスが悪くなっている可能性があります。通常の状態であれば、属性セッションは ADC サービスに均等に分散されます。バランスが悪い状態が続くと、パフォーマンスの問題につながる可能性があり<br><br>問題が解決しない場合は、テクニカルサポートにお問い合わせください。 |
| ALOS | アウトバウンド属性セッション | ADC | ADC サービスの属性セッションが多く、過負荷状態になっています。このアラームがトリガーされた場合は、テクニカルサポートに連絡してください。 |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| ALUR | 到達不能な属性リポジトリ | ADC | NMS サービスとのネットワーク接続を調べ、属性リポジトリに接続できることを確認します。<br><br>このアラームがトリガーされ、ネットワーク接続に問題がない場合は、テクニカルサポートに連絡してください。 |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| AMQS （ AMQS ） | キューに登録された監査メッセージ | BADC 、 BAMS 、 BARC 、 BCLB 、 BCMN 、 BCMN 、 BLDR 、 BNMS 、 BDDS | 監査メッセージは、監査リレーまたは監査リポジトリにすぐに転送できない場合、ディスクキューに格納されます。ディスクキューがいっぱいになると、システムが停止する可能性があります。<br><br>時間内に対応して停止を回避できるように、ディスクキュー内のメッセージ数が次のしきい値に達すると AMQS アラームがトリガーされます。<br><br>• Notice ： 10 万件を超えるメッセージ<br>• Minor ： 50 万件以上のメッセージ<br>• Major ： 200 万件以上のメッセージ<br>• Critical ： 500 万件以上のメッセージ<br><br>AMQS アラームがトリガーされた場合は、システムの負荷を確認します。大量のトランザクションが発生していた場合は、時間が経つとアラームは自然に解消されます。この場合、このアラームは無視してかまいません。<br><br>アラームが解除されず重大度が上がった場合は、キューサイズのグラフを確認します。数時間から数日にわたって数値が増え続けている場合は、監査の負荷がシステムの監査キャパシティを超えている可能性があります。クライアントの処理率を下げるか、監査レベルを「 Error 」または「 Off 」に変更して、ログに記録される監査メッセージの数を減らしてください。監査メッセージについて_の「監査メッセージレベルの変更」を参照してください。 |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| AOTE | ストアの状態 | BARC | ターゲットタイプが「 Tivoli Storage Manager （ TSM ）」のアーカイブノードにのみ適用されます。<br><br>「 Store State 」の値が「 Waiting for Target 」の場合は、外部アーカイブストレージシステムを調べ、正常に動作していることを確認します。アーカイブノードを StorageGRID システムに追加したばかりの場合は、アーカイブノードから対象の外部アーカイブストレージシステムへの接続が正しく設定されていることを確認します。<br><br>「 Store State 」の値が「 Offline 」の場合は、「 Store Status 」の値を確認します。問題がある場合は解決してから、「 Store State 」を「 Online 」に戻します。 |
| AOTU | ストアのステータス | BARC | 「 Store Status 」の値が「 Session Lost 」の場合は、外部アーカイブストレージシステムが接続されてオンラインになっていることを確認します。<br><br>「 Target Error 」の値を入力して、外部アーカイブストレージシステムにエラーがないかを確認します。<br><br>「 Store Status 」の値が「 Unknown Error 」の場合は、テクニカルサポートに連絡してください。 |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| APMS | ストレージマルチパス接続 | SSM のことです | マルチパス状態アラームが「Degraded」と表示される場合（* Support **>** Tools **>** Grid Topology を選択し、***_site _**>*_grid node_name **>** SSM **>** Events *）、次の手順を実行します。<br><br>1. インジケータライトが表示されていないケーブルを接続するか交換します。<br>2. 1~5 分ほど待ちます。<br><br>最初のケーブルを接続してから少なくとも 5 分経過するまでは、他のケーブルを取り外さないでください。それよりも早くケーブルを取り外すと原因 、ルートボリュームが読み取り専用になり、ハードウェアの再起動が必要になります。<br><br>3. SSM*>*Resources* ページに戻り ' ストレージ・ハードウェアのセクションで ' Degraded マルチパス・ステータスが Nominal に変更されていることを確認します |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| ARCE | アークの状態 | 円弧（ Arc ） | ARC サービスの状態は、 ARC のすべてのコンポーネント（ Replication 、 Store 、 Retrieve 、 Target ）が起動されるまでは「 Standby 」となり、その後、 Online に移行します。<br><br>「 ARC State 」の値が「 Standby 」から「 Online 」に切り替わらない場合は、 ARC のコンポーネントのステータスを確認します。<br><br>「 ARC State 」の値が「 Offline 」の場合は、サービスを再起動します。問題が解決しない場合は、テクニカルサポートにお問い合わせください。 |
| AROQ | Objects Queued （オブジェクトのキュー | 円弧（ Arc ） | このアラームは、対象の外部アーカイブストレージシステムの問題が原因でリムーバブルストレージデバイスが低速になっている場合や、複数の読み取りエラーが発生している場合にトリガーされることがあります。外部アーカイブストレージシステムにエラーがないかどうかを確認し、正常に動作していることを確認します。<br><br>このエラーは、データ要求の割合が高いことが原因で発生することがあります。この場合は、システムアクティビティが少なくなるとキューに登録されたオブジェクトの数も少なくなります |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| ARRF | 要求の失敗 | 円弧（ Arc ） | 対象の外部アーカイブストレージシステムからの読み出しに失敗した場合、一時的な問題 が原因である可能性があるため、アーカイブノードで読み出しが再試行されます。ただし、オブジェクトデータが破損している場合や完全に使用できないものとしてマークされている場合は、読み出しが失敗することはありません。この場合、アーカイブノードで読み出しの再試行が繰り返され、「 Request Failures 」の値が増え続けることになります。<br><br>このアラームは、要求されたデータを格納するストレージメディアが破損していることを示している可能性があります。外部アーカイブストレージシステムを調べて問題を詳しく診断します。<br><br>オブジェクトデータがアーカイブにないことが判明した場合は、オブジェクトを StorageGRID システムから削除する必要があります。詳細については、テクニカルサポートにお問い合わせください。<br><br>このアラームをトリガーした問題が解消されたら、障害数をリセットします。Support **>** Tools **>** Grid Topology を選択します。次に、 **** site _ * > * _ grid node*** > * ARC * > * Retrieve * > * Configuration * > * Main * を選択し、 * Reset Request Failure Count * を選択して、 * Apply Changes * をクリックします。 |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| ARRV | 検証エラー | 円弧（ Arc ） | この問題の診断と修正については、テクニカルサポートにお問い合わせください。<br><br>このアラームをトリガーした問題が解消されたら、障害数をリセットします。Support **>** Tools **>** Grid Topology を選択します。次に、 ***site*** **_ * > * _** ***grid node*** > * ARC * > * Retrieve * > * Configuration * > * Main * を選択し、 * Reset Verification Failure Count * を選択して * Apply Changes * をクリックします。 |
| ARVF | Store Failures （ストア障害） | 円弧（ Arc ） | このアラームは、対象の外部アーカイブストレージシステムのエラーが原因で発生することがあります。外部アーカイブストレージシステムにエラーがないかどうかを確認し、正常に動作していることを確認します。<br><br>このアラームをトリガーした問題が解消されたら、障害数をリセットします。Support **>** Tools **>** Grid Topology を選択します。次に、 ***site*** **_ * > * _** ***grid node*** > * ARC * > * Retrieve * > * Configuration * > * Main * を選択し、 * Reset Store Failure Count * を選択して、 * Apply Changes * をクリックします。 |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| ASXP | 監査共有 | AMS | 「 Audit Shares 」の値が「 Unknown 」の場合にアラームがトリガーされます。このアラームは、管理ノードのインストールまたは設定に問題があることを示している可能性があります。<br><br>問題が解決しない場合は、テクニカルサポートにお問い合わせください。 |
| AUMA | AMS ステータス | AMS | 「 AMS Status 」の値が「 DB Connectivity Error 」の場合は、グリッドノードを再起動します。<br><br>問題が解決しない場合は、テクニカルサポートにお問い合わせください。 |
| AUME | AMS の状態 | AMS | 「 AMS State 」の値が「 Standby 」の場合は、しばらく StorageGRID システムを監視し、問題が解決しない場合は、テクニカルサポートにお問い合わせください。<br><br>「 AMS State 」の値が「 Offline 」の場合は、サービスを再起動します。問題が解決しない場合は、テクニカルサポートにお問い合わせください。 |
| 補助 | 監査エクスポートのステータス | AMS | アラームがトリガーされた場合は、原因となっている問題を修正し、 AMS サービスを再起動します。<br><br>問題が解決しない場合は、テクニカルサポートにお問い合わせください。 |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| BADD | ストレージコントローラ障害ドライブ数 | SSM のことです | このアラームは、StorageGRID アプライアンスの 1 つ以上のドライブが故障したか、または最適な状態でない場合にトリガーされます。必要に応じてドライブを交換します。 |
| BASF | 使用可能なオブジェクト ID | CMN | StorageGRID システムのプロビジョニング時、CMN サービスに決まった数のオブジェクト ID が割り当てられます。このアラームは、 StorageGRID システムでオブジェクト ID が不足し始めるとトリガーされます。<br><br>ID の割り当てを増やすには、テクニカルサポートにお問い合わせください。 |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| 低音 | ID ブロック割り当てステータス | CMN | デフォルトでは、 ADC のクォーラムに達しないためにオブジェクト ID を割り当てることができない場合にアラームがトリガーされます。<br><br>CMN サービスでの ID ブロックの割り当てには、オンラインで接続されている ADC サービスがクォーラム（過半数）に達している必要があります。クォーラムに満たない場合、 ADC のクォーラムが再確立されるまで CMN サービスは新しい ID ブロックを割り当てることができません。ADC のクォーラムが失われても、グリッドのどこかに約 1 カ月分の ID がキャッシュされているため、通常は StorageGRID システムにすぐに影響が及ぶことはありません（クライアントによるコンテンツの取り込みと読み出しは引き続き可能です）。 ただし、この状態が続くと、StorageGRID システムは新しいコンテンツを取り込むことができなくなります。<br><br>アラームがトリガーされた場合は、 ADC のクォーラムが失われた理由（ネットワークやストレージノードの障害など）を調べて適切に対処します。<br><br>問題が解決しない場合は、テクニカルサポートにお問い合わせください。 |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| BRDT | コンピューティングコントローラシャーシの温度 | SSM のことです | StorageGRID アプライアンスのコンピューティングコントローラの温度が公称のしきい値を超えるとアラームがトリガーされます。<br><br>過熱の原因となっているハードウェアコンポーネントや環境の問題を確認します。必要に応じて、コンポーネントを交換します。 |
| BTOF | オフセット（ Offset ） | BADC 、 BLDR 、 BNMS 、 BAMS 、 BCLB 、 BCMN 、 BARC | サービスの時間（秒）とオペレーティングシステムの時間が大きく異なる場合にアラームがトリガーされます。通常の状態であれば、サービスは自動的に再同期されます。サービスの時間とオペレーティングシステムの時間のずれが大きくなると、システムの運用に影響を及ぼすことがあります。StorageGRID システムの時間ソースが正しいことを確認します。<br><br>問題が解決しない場合は、テクニカルサポートにお問い合わせください。 |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| BTSE | クロックの状態 | BADC 、 BLDR 、 BNMS 、 BAMS 、 BCLB 、 BCMN 、 BARC | サービスの時間がオペレーティングシステムで追跡された時間と同期されていない場合にアラームがトリガーされます。通常の状態であれば、サービスは自動的に再同期されます。オペレーティングシステムの時間とのずれが大きくなると、システムの運用に影響を及ぼすことがあります。StorageGRID システムの時間ソースが正しいことを確認します。<br><br>問題が解決しない場合は、テクニカルサポートにお問い合わせください。 |
| CAHP | Java ヒープ使用率 | DDS | Java のガベージコレクションが追いつかず、システムの正常な動作に必要なヒープスペースを確保できなくなった場合にアラームがトリガーされます。アラームは、 DDS のメタデータストアに対するユーザのワークロードがシステム全体で利用できるリソースを超えていることを示している可能性があります。ダッシュボードでILMアクティビティを確認するか、* Support **>** Tools **>** Grid Topology を選択し、***_site _**>*_grid node_name >* DDS **>** Resources **>** Overview **>** Main *を選択します。<br><br>問題が解決しない場合は、テクニカルサポートにお問い合わせください。 |
| CAIH | 使用可能な取り込み先の数 | CLB の機能です | このアラームは廃止されました。 |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| CAQH | 使用可能な宛先の数 | CLB の機能です | このアラームは、使用可能な LDR サービスの根本的な問題が修正されると解除されます。LDR サービスの HTTP コンポーネントがオンラインで正常に実行されていることを確認します。<br><br>問題が解決しない場合は、テクニカルサポートにお問い合わせください。 |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| カーサ | データストアのステータス | DDS | Cassandra のメタデータストアが使用できなくなるとアラームが生成されます。<br><br>Cassandra のステータスを確認します。<br><br>1. ストレージノードで、adminおよびとしてログインします `su` Passwords.txtファイルに記載されているパスワードを使用してrootに変更します。<br>2. 入力するコマンド `service cassandra status`<br>3. Cassandraが実行されていない場合は再起動します。 `service cassandra restart`<br><br>このアラームは、ストレージノードに対するメタデータストア（Cassandra データベース）のリビルドが必要なことを示している可能性もあります。<br><br>"サービスのトラブルシューティング：Status - Cassandra（SVST）アラーム"<br><br>問題が解決しない場合は、テクニカルサポートにお問い合わせください。 |
| ケース | データストアの状態 | DDS | このアラームは、インストール時または拡張時にトリガーされ、新しいデータストアがグリッドに追加されていることを示します。 |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| CCES | Incoming Sessions - Established | CLB の機能です | このアラームは、ゲートウェイノード上の現在アクティブな（開いている） HTTP セッションの数が 20 、 000 以上になるとトリガーされます。クライアントの接続数が多すぎると、接続エラーが発生することがあります。ワークロードを減らす必要があります。 |
| CCNA | コンピューティングハードウェア | SSM のことです | このアラームは、StorageGRID アプライアンスのコンピューティングコントローラハードウェアのステータスが「 Needs Attention 」になるとトリガーされます。 |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| CDLP | Metadata Used Space （ Percent ） | DDS | このアラームは、「 Metadata Effective Space （ CEMS ）」が 70% 使用済み（ Minor アラーム）、 90% 使用済み（ Major アラーム）、 100% 使用済み（ Critical アラーム）に達した場合に、それぞれトリガーされます。<br><br>このアラームが 90% のしきい値に達すると、 Grid Manager のダッシュボードに警告が表示されます。できるだけ早く拡張手順 を実行して新しいストレージノードを追加する必要があります。StorageGRID グリッドの拡張手順を参照してください。<br><br>このアラームが 100% のしきい値に達した場合は、オブジェクトの取り込みを停止し、すぐにストレージノードを追加する必要があります。Cassandra は、コンパクションや修復などの必須処理を実行するために一定量のスペースを必要とします。オブジェクトメタデータの使用スペースが使用可能なスペースの 100% を超えると、これらの処理に影響します。望ましくない結果が生じる可能性があります。<br><br>• 注：ストレージノードを追加できない場合は、テクニカルサポートにお問い合わせください。<br><br>新しいストレージノードが追加されると、すべてのストレージノード間でオブジェクトメタデータが自動的にリバランシングされ、アラームが解除されます。 |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| CLBA | CLB のステータス | CLB の機能です | アラームがトリガーされた場合は、* Support > Tools > Grid Topology を選択し、***site _>*** grid node_name > CLB > Overview > Main および CLB > Alarms > Main *を選択して、アラームの原因 を確認し、問題のトラブルシューティングを行います。<br><br>問題が解決しない場合は、テクニカルサポートにお問い合わせください。 |
| CLBE | CLB の状態 | CLB の機能です | 「 CLB State 」の値が「 Standby 」の場合は、しばらく状況を監視し、問題が解決しなければテクニカルサポートに連絡します。<br><br>「 Offline 」の場合は、サーバハードウェアの既知の問題（サーバが接続されていないなど）や計画的停止がないことを確認し、サービスを再起動します。問題が解決しない場合は、テクニカルサポートにお問い合わせください。 |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| CMNA | CMN のステータス | CMN | CMN Statusの値がErrorの場合は、* Support **>** Tools **>** Grid Topology を選択し、***site _>*** grid node_name **>** CMN **>** Overview **>** Main および CMN **>** Alarms **>** Main *を選択してエラーの原因 を確認し、問題のトラブルシューティングを行います。<br><br>プライマリ管理ノードのハードウェアの更新時に CMN の状態が切り替わると（「 CMN State 」の値が「 Standby 」から「 Online 」に変わると）、アラームがトリガーされ、「 CMN Status 」の値が「 No Online CMN 」になります。<br><br>問題が解決しない場合は、テクニカルサポートにお問い合わせください。 |
| CPRC | 残り容量 | NMS | 残り容量（ NMS データベースに対して確立できる接続の数）が設定されたアラームの重大度を下回るとアラームがトリガーされます。<br><br>アラームがトリガーされた場合は、テクニカルサポートに連絡してください。 |
| cPSA | コンピューティングコントローラの電源装置 A | SSM のことです | StorageGRID アプライアンスのコンピューティングコントローラに電源装置 A を搭載した問題 がある場合にアラームがトリガーされます。<br><br>必要に応じて、コンポーネントを交換します。 |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| cPSB | コンピューティングコントローラの電源装置 B | SSM のことです | StorageGRID アプライアンスのコンピューティングコントローラに電源装置 B を搭載した問題 があると、アラームがトリガーされます。<br><br>必要に応じて、コンポーネントを交換します。 |
| CPUT | コンピューティングコントローラの CPU 温度 | SSM のことです | StorageGRID アプライアンスのコンピューティングコントローラの CPU の温度が公称のしきい値を超えるとアラームがトリガーされます。<br><br>ストレージノードが StorageGRID アプライアンスである場合は、StorageGRID システムのコントローラを調査する必要があります。<br><br>過熱の原因となっているハードウェアコンポーネントや環境の問題を確認します。必要に応じて、コンポーネントを交換します。 |
| DNST | DNS ステータス | SSM のことです | インストールが完了すると、 SSM サービスで DNST アラームがトリガーされます。DNS の設定が完了し、新しいサーバの情報がすべてのグリッドノードに送られると、アラームはキャンセルされます。 |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| ECCD | 破損フラグメントが検出されました | LDR | バックグラウンド検証プロセスでイレイジャーコーディングされたフラグメントの破損が検出されるとアラームがトリガーされます。破損したフラグメントが検出された場合、フラグメントの再構築が試行されます。「 Corrupt Fragments Detected 」属性と「 Copies Lost 」属性を 0 にリセットし、それらのカウントが再び増えるかどうかを確認します。カウントが増える場合は、ストレージノードの基盤となるストレージに問題がある可能性があります。イレイジャーコーディングされたオブジェクトデータのコピーは、損失または破損したフラグメントの数がイレイジャーコーディングのフォールトトレランスを超えないかぎり欠落とはみなされません。したがって、破損したフラグメントがあっても、オブジェクトの読み出しは引き続き可能な場合もあります。<br><br>問題が解決しない場合は、テクニカルサポートにお問い合わせください。 |
| ECST | 検証ステータス | LDR | このアラームは、このストレージノードのイレイジャーコーディングオブジェクトデータに対するバックグラウンド検証プロセスの現在のステータスを示します。<br><br>バックグラウンド検証プロセスでエラーが発生すると、 Major アラームがトリガーされます。 |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| FOPN | オープンファイル記述子 | BADC 、 BAMS 、 BARC 、 BCLB 、 BCMN 、 BCMN 、 BLDR 、 BNMS 、 BSSM 、 BDDS | アクティビティのピーク時に FOPN が大きくなることがあります。アクティビティが少ない時間帯も低下しない場合は、テクニカルサポートにお問い合わせください。 |
| HSTE | HTTP State のことです | BLDR | HSTU の推奨処置を参照してください。 |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| ステュディオ | HTTP ステータス | BLDR | HSTE と HSTU は、 S3 、 Swift 、およびその他の内部 StorageGRID トラフィックを含むすべての LDR トラフィックの HTTP プロトコルに関連したアラームです。アラームは、次のいずれかの状況が発生したことを示します。<br><br>• HTTP プロトコルが手動でオフラインにされた。<br>• Auto-Start HTTP 属性が無効になりました。<br>• LDR サービスがシャットダウン中である。<br><br>Auto-Start HTTP 属性はデフォルトで有効になっています。この設定を変更すると、再起動後も HTTP がオフラインのままになる可能性があります。<br><br>必要に応じて、 LDR サービスが再起動するまで待ちます。<br><br>Support **>** Tools **>** Grid Topology *を選択します。次に、「 * _ ストレージ・ノード _ * > * LDR * > * Configuration * 」を選択します。HTTP プロトコルがオフラインの場合は、オンラインにします。Auto-Start HTTP 属性が有効になっていることを確認します。<br><br>HTTP プロトコルがオフラインのままになる場合は、テクニカルサポートにお問い合わせください。 |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| HTAS | HTTP を自動起動します | LDR | 起動時に HTTP サービスを自動的に開始するかどうかを指定します。これはユーザ指定の設定オプションです。 |
| IRSU | インバウンドレプリケーションステータス | BLDR 、 BARC | インバウンドレプリケーションが無効になっていることを示します。構成設定を確認します。* Support **>** Tools **>** Grid Topology *を選択します。次に、 * _site _ * > * _ grid node_name > * LDR * > * Replication * > * Configuration * > * Main * を選択します。 |
| LATA （ LATA | 平均レイテンシ | NMS | 接続に問題がないかを確認します。<br><br>システムアクティビティを調べ、システムアクティビティが増えていることを確認します。システムアクティビティが増えれば、属性データアクティビティも増えます。このアクティビティが増加すると、属性データの処理に遅延が生じます。これは正常なシステムアクティビティであり、自然に解消されます。<br><br>複数のアラームがないか確認します。トリガーされたアラームの数が多すぎると、平均レイテンシが高くなることがあります。<br><br>問題が解決しない場合は、テクニカルサポートにお問い合わせください。 |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| LDRE | LDR の状態 | LDR | 「 LDR State 」の値が「 Standby 」の場合は、しばらく状況を監視し、問題が解決しなければテクニカルサポートに連絡します。<br><br>「 LDR State 」の値が「 Offline 」の場合は、サービスを再起動します。問題が解決しない場合は、テクニカルサポートにお問い合わせください。 |
| 失われました | Lost Objects | DDS 、 LDR | 要求されたオブジェクトのコピーを StorageGRID システム内のいずれの場所からも読み出せない場合にトリガーされます。LOST （ Lost Objects ）アラームがトリガーされる前に、欠落オブジェクトをシステム内の他の場所から読み出して置き換えることができます。<br><br>損失オブジェクトとは、データが失われたことを表します。Lost Objects 属性の値は、 ILM ポリシーを満たすためにコンテンツが DDS サービスで意図的にパージされた場合を除き、オブジェクトの場所の数が 0 になるたびに増えていきます。<br><br>LOST （ Lost Object ）アラームはすぐに調査する必要があります。問題が解決しない場合は、テクニカルサポートにお問い合わせください。<br><br>"オブジェクトデータの損失と欠落が発生した場合のトラブルシューティング" |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| MCEP | 管理インターフェイス証明書の有効期限 | CMN | 管理インターフェイスへのアクセスに使用される証明書の有効期限が近づくとトリガーされます。<br><br>1. 「* Configuration > Server Certificates *」に移動します。<br>2. 管理インターフェイスのサーバ証明書セクションで、新しい証明書をアップロードします。<br><br>"StorageGRID の管理" |
| MINQ | キューに登録された電子メール通知 | NMS | NMS サービスをホストするサーバと外部のメールサーバのネットワーク接続を確認します。また、E メールサーバの設定が正しいことを確認します。<br><br>"アラーム用Eメールサーバの設定（従来のシステム）" |
| 分 | 電子メール通知のステータス | BNMS | NMS サービスでメールサーバに接続できない場合に Minor アラームがトリガーされます。NMS サービスをホストするサーバと外部のメールサーバのネットワーク接続を確認します。また、 E メールサーバの設定が正しいことを確認します。<br><br>"アラーム用Eメールサーバの設定（従来のシステム）" |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| お見逃しなく | NMS インターフェイスエンジンステータス | BNMS | インターフェイスコンテンツを収集および生成する管理ノードの NMS インターフェイスエンジンがシステムから切断されている場合にアラームがトリガーされます。Server Manager で、サーバの個々のアプリケーションが停止しているかどうかを確認します。 |
| ナン | ネットワーク自動ネゴシエーション設定 | SSM のことです | ネットワークアダプタの設定を確認します。設定は、ネットワークのルータとスイッチの設定と一致する必要があります。<br><br>設定が正しくないと、システムのパフォーマンスに重大な影響を及ぼす可能性があります。 |
| NDUP （ NDUP ） | ネットワークのデュプレックス設定 | SSM のことです | ネットワークアダプタの設定を確認します。設定は、ネットワークのルータとスイッチの設定と一致する必要があります。<br><br>設定が正しくないと、システムのパフォーマンスに重大な影響を及ぼす可能性があります。 |
| NLNK | ネットワークリンク検出 | SSM のことです | ポートとスイッチのネットワークケーブル接続を確認します。<br><br>ネットワークルータ、スイッチ、およびアダプタの設定を確認します。<br><br>サーバを再起動します。<br><br>問題が解決しない場合は、テクニカルサポートにお問い合わせください。 |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| NRER | 受信エラー | SSM のことです | NRER アラームの原因としては、次のようなものが考えられます。<br><br>• Forward Error Correction （ FEC; 前方誤り訂正）の不一致<br>• スイッチポートと NIC の MTU が一致しません<br>• リンクエラー率が高くなっています<br>• NIC リングバッファオーバーラン<br><br>"Network Receive Error （NRER）アラームのトラブルシューティングを行います" |
| NRLY の場合 | 使用可能な監査リレー | BADC 、 BARC 、 BCLB 、 BCMN 、 BLDR 、 BNMS 、 BDDS | ADC サービスに監査リレーが接続されていないと、監査イベントを報告できません。接続がリストアされるまではキューに登録され、ユーザには提供されません。<br><br>できるだけ早く ADC サービスへの接続をリストアします。<br><br>問題が解決しない場合は、テクニカルサポートにお問い合わせください。 |
| NSCA | NMS ステータス | NMS | 「 NMS Status 」の値が「 DB Connectivity Error 」の場合は、サービスを再起動します。問題が解決しない場合は、テクニカルサポートにお問い合わせください。 |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| NSCE | NMS State （ NMS 状態 ） | NMS | 「 NMS State 」の値が「 Standby 」の場合は、しばらく状況を監視し、問題が解決しなければテクニカルサポートに連絡します。<br><br>「 NMS State 」の値が「 Offline 」の場合は、サービスを再起動します。問題が解決しない場合は、テクニカルサポートにお問い合わせください。 |
| NSPD | スピード | SSM のことです | ネットワーク接続またはドライバの互換性の問題が原因である可能性があります。問題が解決しない場合は、テクニカルサポートにお問い合わせください。 |
| NTBR | 空きテーブルスペース | NMS | アラームがトリガーされた場合は、データベースの使用量がどのくらいのペースで変化しているかを確認します。時間とともに徐々に変化するのではなく、急激に低下した場合は、エラー状態を示します。問題が解決しない場合は、テクニカルサポートにお問い合わせください。<br><br>アラームのしきい値を調整することで、追加のストレージの割り当てが必要になったときにプロアクティブに管理できます。<br><br>使用可能なスペースがしきい値の下限（アラームのしきい値を参照）に達した場合は、テクニカルサポートに連絡してデータベースの割り当てを変更します。 |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| 入力します | 送信エラー | SSM のことです | これらのエラーは、手動でリセットしなくても解消されます。解消されない場合は、ネットワークハードウェアを確認します。アダプタのハードウェアとドライバが正しくインストールされ、ネットワークのルータやスイッチと連携するように設定されていることを確認します。<br><br>原因となっている問題を解決したら、カウンタをリセットします。Support **>** Tools **>** Grid Topology を選択します。次に、 ***site _ * > * _ grid node*** > * SSM * > * Resources * > * Configuration * > * Main * を選択し、 * Reset Transmit Error Count * を選択して、 * Apply Changes * をクリックします。 |
| NTFQ | NTP 周波数オフセット | SSM のことです | 周波数オフセットが設定されたしきい値を超えている場合は、ハードウェアのローカルクロックに問題がある可能性があります。問題が解決しない場合は、テクニカルサポートに連絡して交換を手配してください。 |
| NTLK | NTP ロック | SSM のことです | NTP デーモンが外部の時間ソースにロックされていない場合は、指定された外部時間ソースへのネットワーク接続とそれらの可用性および安定性を確認します。 |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| NTOF | NTP 時間オフセット | SSM のことです | 時間オフセットが設定されたしきい値を超えている場合は、ハードウェアのローカルクロックのオシレーターに問題がある可能性があります。問題が解決しない場合は、テクニカルサポートに連絡して交換を手配してください。 |
| NTSJ | 選択された時間ソースジッタ | SSM のことです | この値は、ローカルサーバ上の NTP が参照として使用している時間ソースの信頼性と安定性を示します。<br><br>アラームがトリガーされた場合は、時間ソースのオシレーターが故障しているか、時間ソースへの WAN リンクに問題がある可能性があります。 |
| NTSU | NTP ステータス | SSM のことです | 「 NTP Status 」の値が「 Not Running 」の場合は、テクニカルサポートに連絡してください。 |
| OPST の場合 | 全体的な電源ステータス | SSM のことです | StorageGRID アプライアンスの電源が推奨される動作電圧と大きく異なる場合にアラームがトリガーされます。<br><br>電源装置 A と B のステータスを調べ、どちらの電源装置に異常があるかを確認します。<br><br>必要に応じて、電源装置を交換します。 |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| OQRT の場合 | 隔離されたオブジェクト | LDR | StorageGRID システムでオブジェクトが自動的にリストアされたあと、隔離されたオブジェクトを隔離ディレクトリから削除できます。<br><br>1. Support **>** Tools **>** Grid Topology *を選択します。<br>2. サイト * > * ストレージノード * > * LDR * > * Verification * > * Configuration * > * Main * の順に選択します。<br>3. ［ * 隔離オブジェクトの削除 * ］ を選択します。<br>4. [ 変更の適用 *] をクリックします。<br><br>隔離されたオブジェクトが削除され、数がゼロにリセットされます。 |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| ORSU | アウトバウンドレプリケーションステータス | BLDR 、 BARC | アウトバウンドレプリケーションを実行できず、ストレージからオブジェクトを読み出せない状態になっていることを示します。アウトバウンドレプリケーションが手動で無効になった場合にアラームがトリガーされます。Support **>** Tools **>** Grid Topology *を選択します。次に、 * _site _ * > * _ grid node_name > * LDR * > * Replication * > * Configuration * を選択します。<br><br>LDR サービスでレプリケーションを実行できない場合にもアラームがトリガーされます。Support **>** Tools **>** Grid Topology *を選択します。次に、 * _site _ * > * _grid node_name * > * ldr * > * Storage * を選択します。 |
| OSLF | シェルフステータス | SSM のことです | ストレージアプライアンスのストレージシェルフのいずれかのコンポーネントのステータスがデグレードになると、アラームがトリガーされます。ストレージシェルフコンポーネントには、 IOM 、ファン、電源装置、ドライブドロワーが含まれます。このアラームがトリガーされた場合は、アプライアンスのメンテナンス手順を参照してください。 |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| PMEM | サービスメモリ使用率（パーセント） | BADC 、 BAMS 、 BARC 、 BCLB 、 BCMN 、 BCMN 、 BLDR 、 BNMS 、 BSSM 、 BDDS | には、 Over Y% RAM の値を指定できます。 Y は、サーバで使用されているメモリの割合を表します。<br><br>80% 未満であれば問題ありません。90% を超える場合は問題があると考えられます。<br><br>1 つのサービスのメモリ使用率が高い場合は、状況を監視して調査します。<br><br>問題が解決しない場合は、テクニカルサポートにお問い合わせください。 |
| PSAS | Power Supply A Status の順に選択します | SSM のことです | StorageGRID アプライアンスの電源装置 A が推奨される動作電圧と大きく異なる場合にアラームがトリガーされます。<br><br>必要に応じて、電源装置 A を交換します |
| PSBS | 電源装置 B のステータス | SSM のことです | StorageGRID アプライアンスの電源装置 B が推奨される動作電圧と大きく異なる場合にアラームがトリガーされます。<br><br>必要に応じて、電源装置 B を交換します |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| RDTE | Tivoli Storage Manager の状態 | BARC | ターゲットタイプが「 Tivoli Storage Manager （ TSM ）」のアーカイブノードにのみ適用されます。<br><br>「 Tivoli Storage Manager State 」の値が「 Offline 」の場合は、「 Tivoli Storage Manager Status 」を確認して問題を解決します。<br><br>コンポーネントをオンラインに戻します。Support **>** Tools **>** Grid Topology を選択します。次に、 ***site _ * > * _ grid node*** > * ARC * > * Target * > * Configuration * > * Main * を選択し、 * Tivoli Storage Manager State * > * Online * を選択して、 * Apply Changes * をクリックします。 |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| RDTU | Tivoli Storage Manager のステータス | BARC | ターゲットタイプが「 Tivoli Storage Manager （ TSM ）」のアーカイブノードにのみ適用されます。<br><br>「 Tivoli Storage Manager Status 」の値が「 Configuration Error 」で、アーカイブノードを StorageGRID システムに追加したばかりの場合は、 TSM ミドルウェアサーバが正しく設定されていることを確認します。<br><br>「 Tivoli Storage Manager Status 」の値が「 Connection Failure 」または「 Connection Failure 、 Retrying 」の場合は、 TSM ミドルウェアサーバのネットワーク設定、および TSM ミドルウェアサーバと StorageGRID システムの間のネットワーク接続を確認します。<br><br>「 Tivoli Storage Manager Status 」の値が「 Authentication Failure 」または「 Authentication Failure 、 Reconnecting 」の場合は、 StorageGRID システムから TSM ミドルウェアサーバに接続は可能ですが、接続を認証できません。TSM ミドルウェアサーバでユーザ、パスワード、および権限が正しく設定されていることを確認し、サービスを再起動します。<br><br>「 Tivoli Storage Manager Status 」の値が「 Session Failure 」の場合は、確立されたセッションが予期せずに切断されています。TSM ミドルウェアサーバと StorageGRID システムの間のネットワーク接続を確認します。ミドルウェアサーバにエラーがない |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| RIRF | インバウンドレプリケーション — 失敗 | BLDR 、 BARC | このアラームは、負荷が高いときやネットワークが一時的に停止しているときに発生する可能性があります。このアラームは、システムアクティビティが減ると解除されます。レプリケーションの失敗回数が増え続ける場合は、ネットワークに問題がないかを調べ、ソースとデスティネーションの LDR サービスおよび ARC サービスがオンラインで使用可能な状態になっていることを確認します。<br><br>カウントをリセットするには、* Support **>** Tools **>** Grid Topology を選択し、***_site _**>*_grid node_name >* LDR **>** Replication **>** Configuration **>** Main *を選択します。「 * インバウンド複製エラー数のリセット * 」を選択し、「 * 変更を適用 * 」をクリックします。 |
| RIRQ | Inbound Replications — Queued （インバウンドレプリケーション — キューイング済み | BLDR 、 BARC | 負荷が高いときやネットワークが一時的に停止しているときにアラームが発生することがあります。このアラームは、システムアクティビティが減ると解除されます。レプリケーションのキューが増え続ける場合は、ネットワークに問題がないかを調べ、ソースとデスティネーションの LDR サービスおよび ARC サービスがオンラインで使用可能な状態になっていることを確認します。 |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| RORQ | Outbound Replications - Queued （アウトバウンドレプリケーション - キューイング済み | BLDR 、 BARC | アウトバウンドレプリケーションのキューには、 ILM ルールを満たすためにコピーされるオブジェクトデータと、クライアントから要求されたオブジェクトが含まれます。<br><br>システムが過負荷になると、アラームが発生することがあります。このアラームはシステムアクティビティが減ると解除されるため、しばらく状況を監視します。アラームが繰り返し発生する場合は、ストレージノードを追加して容量を増やします。 |
| SAVP の | 使用可能な合計スペース（割合） | LDR | 使用可能なスペースがしきい値の下限に達した場合は、 StorageGRID システムを拡張するか、オブジェクトデータをアーカイブノード経由でアーカイブに移動します。 |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| SCAS | ステータス | CMN | アクティブなグリッドタスクの「 Status 」の値が「 Error 」の場合は、グリッドタスクのメッセージを検索します。Support **>** Tools **>** Grid Topology *を選択します。次に、 * _site _ * > * _ grid node_name * > * CMN * > * Grid Tasks * > * Overview * > * Main * の順に選択します。グリッドタスクのメッセージには、エラーに関する情報が表示されます（例：「 check failed on node 12130011` 」）。<br><br>問題の調査と修正が完了したら、グリッドタスクを再起動します。Support **>** Tools **>** Grid Topology * を選択します。次に、 * _site _ * > * _ grid node_name * > * CMN * > * Grid Tasks * > * Configuration * > * Main * を選択し、 * Actions * > * Run * を選択します。<br><br>中止しているグリッドタスクの「 Status 」の値が「 Error 」の場合は、グリッドタスクの中止を再試行します。<br><br>問題が解決しない場合は、テクニカルサポートにお問い合わせください。 |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| SCEP （ SCEP ） | ストレージ API サービスエンドポイントの証明書有効期限 | CMN | ストレージ API エンドポイントへのアクセスに使用される証明書の有効期限が近づくとトリガーされます。<br><br>1. 「* Configuration > Server Certificates *」に移動します。<br>2. Object Storage API Service Endpoints のServer Certificateセクションで、新しい証明書をアップロードします。<br><br>"StorageGRID の管理" |
| SCHR | ステータス | CMN | 過去のグリッドタスクの「 Status 」の値が「 Aborted 」の場合は、原因を調べ、必要に応じてもう一度タスクを実行します。<br><br>問題が解決しない場合は、テクニカルサポートにお問い合わせください。 |
| SCSA | ストレージコントローラ A | SSM のことです | StorageGRID アプライアンスにストレージコントローラ A を搭載した問題があると、アラームがトリガーされます。<br><br>必要に応じて、コンポーネントを交換します。 |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| SCSB | ストレージコントローラ B | SSM のことです | StorageGRID アプライアンスにストレージコントローラ B を搭載した問題がある場合にアラームがトリガーされます。<br><br>必要に応じて、コンポーネントを交換します。<br><br>一部のアプライアンスモデルには、ストレージコントローラ B がありません |
| SHLH | 健常性 | LDR | オブジェクトストアの「 Health 」の値が「 Error 」の場合は、以下を確認して修正します。<br><br>• マウントされているボリュームの問題<br>• ファイルシステムエラー |
| slsa | CPU Load Average （ CPU 負荷平均） | SSM のことです | この値が大きいほど、システムはビジーになります。<br><br>「 CPU Load Average 」の値が高いまま推移している場合は、システムのトランザクション数を調べ、一時的な負荷の増加によるものかどうかを確認する必要があります。CPU負荷の平均値のグラフを表示します。* Support **>** Tools **>** Grid Topology *を選択します。次に、 * _site _ * > * _ grid node_name > * SSM * > * Resources * > * Reports * > * Charts * を選択します。<br><br>システムの負荷が高くない状況でも問題が解決しない場合は、テクニカルサポートにお問い合わせください。 |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| SMST | Log Monitor State の略 | SSM のことです | 「 Log Monitor State 」の値が「 Connected 」にならない状態が続く場合は、テクニカルサポートに連絡してください。 |
| SMTT | 合計イベント数 | SSM のことです | 「 Total Events 」の値が 0 より大きい場合は、原因 となる既知のイベント（ネットワーク障害など）がないかを確認します。これらのエラーが解消されていない（カウントが 0 にリセットされていない）と、 Total Events アラームがトリガーされることがあります。<br><br>問題 が解決したら、カウンタをリセットしてアラームを解除します。ノード*>*_site **>*_grid node_name >** Events **>** Reset event counts *を選択します。<br><br>イベント数をリセットするには、 Grid Topology Page Configuration 権限が必要です。<br><br>「 Total Events 」の値が 0 の場合や数が増えて問題が解決しない場合は、テクニカルサポートに連絡してください。 |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| SNST | ステータス | CMN | グリッドタスクバンドルの格納に問題があることを示します。「 Status 」の値が「 Checkpoint Error 」または「 Quorum Not Reached 」の場合は、半数を超える ADC サービスが StorageGRID システムに接続されていることを確認し、そのまま数分待ちます。<br><br>問題が解決しない場合は、テクニカルサポートにお問い合わせください。 |
| SOSS | ストレージオペレーティングシステムのステータス | SSM のことです | SANtricity ソフトウェアが、 StorageGRID アプライアンス内のコンポーネントに「 Needs attention 」の問題 が存在することを示す場合に、アラームがトリガーされます。<br><br>[ノード（ Nodes）]を選択し次に、 * アプライアンス・ストレージ・ノード * > * ハードウェア * を選択します。下にスクロールして各コンポーネントのステータスを確認します。SANtricity ソフトウェアで、他のアプライアンスコンポーネントを調べて問題 を特定します。 |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| SSMA | SSM のステータス | SSM のことです | 「SSM Status」の値が「Error」の場合は、「* Support **>** Tools **>** Grid Topology 」を選択し、「***site* _>*** grid node_*>* SSM **>** Main * and * SSM **>** Overview **>** Alarms *」を選択して、アラームの原因 を判断します。<br><br>問題が解決しない場合は、テクニカルサポートにお問い合わせください。 |
| SSME | SSM の状態 | SSM のことです | 「 SSM State 」の値が「 Standby 」の場合は、しばらく状況を監視し、問題が解決しなければテクニカルサポートに連絡します。<br><br>「 SSM State 」の値が「 Offline 」の場合は、サービスを再起動します。問題が解決しない場合は、テクニカルサポートにお問い合わせください。 |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| SSTS のコマンドです | ストレージステータス | BLDR | 「 Storage Status 」の値が「 Insufficient Usable Space 」の場合は、ストレージノードの使用可能なストレージがなくなり、データの取り込みが他の使用可能なストレージノードにリダイレクトされています。このグリッドノードからの読み出し要求は引き続き可能です。<br><br>ストレージを追加する必要があります。エンドユーザの作業には影響しませんが、ストレージを追加しないかぎりアラームは解除されません。<br><br>「 Storage Status 」の値が「 Volume （ s ） Unavailable 」の場合は、ストレージの一部が使用できない状態になっています。これらのボリュームでは格納も読み出しも実行できません。ボリュームの健全性を確認して詳細を確認します。* Support **>** Tools **>** Grid Topology を選択します。次に、 **** site _ * > * _ grid node*** > * LDR * > * Storage * > * Overview * > * Main * を選択します。ボリュームの健全性がオブジェクトストアのリストに表示されます。<br><br>「 Storage Status 」の値が「 Error 」の場合は、テクニカルサポートに連絡してください。<br><br>"Storage Status（SSTS）アラームのトラブルシューティングを行います" |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| SVST | ステータス | SSM のことです | このアラームは、サービスの実行の問題に関する他のアラームが解決されると解除されます。ソース側のサービスのアラームを追跡してリストアします。<br><br>Support **>** Tools **>** Grid Topology を選択します。次に、 **** site _ * > * _ grid node*** > * SSM * > * Services * > * Overview * > * Main * の順に選択します。サービスのステータスが「 Not Running 」と表示される場合は、状態が「 Administratively Down 」です。サービスのステータスが「 Not Running 」と表示される状況は次のとおりです。<br><br>• サービスが手動で停止されました（`/etc/init.d/<service\> stop`）。<br>• MySQL データベースを持つ問題 があり 'Server Manager によって MI サービスがシャットダウンされます<br>• グリッドノードが追加されたが開始されていない。<br>• インストール時にグリッドノードが管理ノードに接続されていない。<br><br>サービスが「Not Running」と表示される場合は、サービスを再起動します（`/etc/init.d/<service\> restart`）。<br><br>このアラームは、ストレージノードに対するメタデータストア（ Cassandra データベース）のリビルドが必要なことを示している可能性も |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| TMEM | メモリを取り付けた | SSM のことです | ノードの搭載メモリが 24GiB 未満の場合、パフォーマンスの問題が発生し、システムが不安定になることがあります。システムの搭載メモリを 24GiB 以上に増やす必要があります。 |
| TPOP | 保留中の処理です | ADC | メッセージのキューが形成されている場合、 ADC サービスが過負荷状態になっている可能性があります。StorageGRID システムに接続されている ADC サービスの数が少なすぎることが考えられます。大規模な環境では、 ADC サービスのコンピューティングリソースを増やすか、システムに ADC サービスを追加することが必要になる可能性があります。 |
| UMEM | 使用可能なメモリ | SSM のことです | 使用可能な RAM が少なくなった場合は、ハードウェア問題 とソフトウェア RAM のどちらであるかを確認します。ハードウェア問題 以外の場合、または使用可能なメモリが 50MB （デフォルトのアラームのしきい値）を下回った場合は、テクニカルサポートに連絡してください。 |
| VMFI | エントリが使用可能です | SSM のことです | 追加のストレージが必要なことを示しています。テクニカルサポートにお問い合わせください。 |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| VMFR | 使用可能なスペース | SSM のことです | 「 Space Available 」の値が低すぎる（アラームのしきい値を参照）場合は、大きくなりすぎているログファイルや大量のディスクスペースを消費しているオブジェクト（アラームのしきい値を参照）がないかどうかを調べ、必要に応じてそれらを減らすか削除します。<br><br>問題が解決しない場合は、テクニカルサポートにお問い合わせください。 |
| VMST | ステータス | SSM のことです | マウントされたボリュームの「 Status 」の値が「 Unknown 」の場合にアラームがトリガーされます。値が「 Unknown 」または「 Offline 」の場合、基盤となるストレージデバイスの問題が原因でボリュームをマウントまたはアクセスできないことを示している可能性があります。 |
| VPRI （ VPRI ） | 検証の優先順位 | BLDR 、 BARC | 「 Verification Priority 」のデフォルトの値は「 Adaptive 」です。「 Verification Priority 」が「 High 」に設定されている場合、ストレージの検証が優先されてサービスの通常の運用に影響する可能性があるため、アラームがトリガーされます。 |

| コード | 名前 | サービス | 推奨される対処方法 |
| --- | --- | --- | --- |
| VSTU | オブジェクトの検証ステータス | BLDR | Support **>** Tools **>** Grid Topology を選択します。次に、 **** site _ * > * _ grid node*** > * LDR * > * Storage * > * Overview * > * Main * を選択します。<br><br>オペレーティングシステムで、ブロックデバイスやファイルシステムのエラーの兆候がないかどうかを確認します。<br><br>「 Object Verification Status 」の値が「 Unknown Error 」の場合は、通常、下位レベルのファイルシステムやハードウェアの問題（ I/O エラー）が原因で、ストレージ検証タスクが格納されたコンテンツにアクセスできないことを示します。テクニカルサポートにお問い合わせください。 |
| XAMS の場合 | 到達不能な監査リポジトリ | BADC 、 BARC 、 BCLB 、 BCMN 、 BLDR 、 BNMS | 管理ノードをホストするサーバへのネットワーク接続を確認します。<br><br>問題が解決しない場合は、テクニカルサポートにお問い合わせください。 |

**SNMP** 通知を生成するアラーム（従来のシステム）

次の表に、 SNMP 通知を生成するレガシーアラームを示します。アラートとは異なり、すべてのアラームが SNMP 通知を生成するわけではありません。リストされたアラームだけが SNMP 通知を生成し、指定された重大度以上の重大度のみが生成されます。

従来のアラームシステムは引き続きサポートされますが、アラートシステムには大きなメリットがあり、使いやすくなっています。

| コード | 名前 | 重大度 |
| --- | --- | --- |
| ACMS | 使用可能なメタデータサービス | 重要 |

| コード | 名前 | 重大度 |
| --- | --- | --- |
| AITE | 読み出し状態 | マイナー |
| AITU | ステータスを取得します | メジャー（ Major ） |
| AMQS （ AMQS ） | キューに登録された監査メッセージ | 注意 |
| AOTE | ストアの状態 | マイナー |
| AOTU | ストアのステータス | メジャー（ Major ） |
| AROQ | Objects Queued （オブジェクトのキュー | マイナー |
| ARRF | 要求の失敗 | メジャー（ Major ） |
| ARRV | 検証エラー | メジャー（ Major ） |
| ARVF | Store Failures （ストア障害） | メジャー（ Major ） |
| ASXP | 監査共有 | マイナー |
| AUMA | AMS ステータス | マイナー |
| 補助 | 監査エクスポートのステータス | マイナー |
| BTOF | オフセット（ Offset ） | 注意 |
| CAHP | Java ヒープ使用率 | メジャー（ Major ） |
| CAQH | 使用可能な宛先の数 | 注意 |
| カーサ | データストアのステータス | メジャー（ Major ） |
| CDLP | Metadata Used Space （ Percent ） | メジャー（ Major ） |
| CLBE | CLB の状態 | 重要 |
| DNST | DNS ステータス | 重要 |
| ECST | 検証ステータス | メジャー（ Major ） |

| コード | 名前 | 重大度 |
| --- | --- | --- |
| HSTE | HTTP State のことです | メジャー（ Major ） |
| HTAS | HTTP を自動起動します | 注意 |
| 失われました | Lost Objects | メジャー（ Major ） |
| MINQ | キューに登録された電子メール通知 | 注意 |
| 分 | 電子メール通知のステータス | マイナー |
| ナン | ネットワーク自動ネゴシエーション設定 | 注意 |
| NDUP （ NDUP ） | ネットワークのデュプレックス設定 | マイナー |
| NLNK | ネットワークリンク検出 | マイナー |
| NRER | 受信エラー | 注意 |
| NSPD | スピード | 注意 |
| 入力します | 送信エラー | 注意 |
| NTFQ | NTP 周波数オフセット | マイナー |
| NTLK | NTP ロック | マイナー |
| NTOF | NTP 時間オフセット | マイナー |
| NTSJ | 選択された時間ソースジッタ | マイナー |
| NTSU | NTP ステータス | メジャー（ Major ） |
| OPST の場合 | 全体的な電源ステータス | メジャー（ Major ） |
| ORSU | アウトバウンドレプリケーションステータス | 注意 |
| PSAS | Power Supply A Status の順に選択します | メジャー（ Major ） |

| コード | 名前 | 重大度 |
| --- | --- | --- |
| PSBS | 電源装置 B のステータス | メジャー（ Major ） |
| RDTE | Tivoli Storage Manager の状態 | 注意 |
| RDTU | Tivoli Storage Manager のステータス | メジャー（ Major ） |
| SAVP の | 使用可能な合計スペース（割合） | 注意 |
| SHLH | 健常性 | 注意 |
| slsa | CPU Load Average （ CPU 負荷平均） | 注意 |
| SMTT | 合計イベント数 | 注意 |
| SNST | ステータス | |
| SOSS | ストレージオペレーティングシステムのステータス | 注意 |
| SSTS のコマンドです | ストレージステータス | 注意 |
| SVST | ステータス | 注意 |
| TMEM | メモリを取り付けた | マイナー |
| UMEM | 使用可能なメモリ | マイナー |
| VMST | ステータス | マイナー |
| VPRI （ VPRI ） | 検証の優先順位 | 注意 |
| VSTU | オブジェクトの検証ステータス | 注意 |

## ログファイル参照

以降のセクションでは、イベント、診断メッセージ、およびエラー状態のキャプチャに使用するログについて説明します。テクニカルサポートにトラブルシューティングを依頼すると、ログファイルを収集して転送するように求められることがあります。

- "StorageGRID ソフトウェアのログ"

- "導入とメンテナンスのログ"
- "サードパーティソフトウェアのログ"
- "bycast.log について"

> このセクションの表は参考用です。これらのログは、テクニカルサポートが高度なトラブルシューティングに使用することを目的としています。監査ログやアプリケーションログファイルを使用して問題の履歴を再構築する高度な手法については、このガイドでは説明していません。

これらのログにアクセスするには、ログファイルとシステムデータを収集します（* Support > Tools > Logs * ）。プライマリ管理ノードを使用できない場合や特定のノードに到達できない場合は、次の手順で各グリッドノードのログにアクセスできます。

1. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
2. に記載されているパスワードを入力します `Passwords.txt` ファイル。
3. 次のコマンドを入力してrootに切り替えます。 `su -`
4. に記載されているパスワードを入力します `Passwords.txt` ファイル。

関連情報

"ログファイルとシステムデータを収集しています"

**StorageGRID** ソフトウェアのログ

## StorageGRID のログを問題のトラブルシューティングに使用できます。

一般的な **StorageGRID** ログです

| ファイル名 | 注： | にあります |
| --- | --- | --- |
| `/var/local/log/bycast.log` | ファイル `bycast.log` は、StorageGRID のトラブルシューティングに使用する主要なファイルです。ファイル `bycast-err.log` のサブセットを含みます `bycast.log` （ERROR とCRITICALの重大度のメッセージ）。クリティカルなメッセージはシステムにも表示されます。Support > Tools > Grid Topology を選択します。次に、[*_Site_*>*_Node_*>*SSM*>*Events] を選択します。 | すべてのノード |

| ファイル名 | 注： | にあります |
| --- | --- | --- |
| `/var/local/log/bycast-err.log` | ファイル `bycast.log` は、StorageGRID のトラブルシューティングに使用する主要なファイルです。ファイル `bycast-err.log` のサブセットを含みます `bycast.log` （ERROR とCRITICALの重大度のメッセージ）。クリティカルなメッセージはシステムにも表示されます。Support **>** Tools **>** Grid Topology を選択します。次に、[*_Site_*>*_Node_*>*SSM*>*Events] を選択します。 | すべてのノード |
| `/var/local/core/` | プログラムが異常終了した場合に作成されるコアダンプファイルが格納されます。原因としては、アサーションエラー、違反、スレッドのタイムアウトなどが考えられます。<br><br>*注：*ファイル `/var/local/core/kexec_cmd` 通常はアプライアンスノードに存在し、エラーを示しているわけではありません。 | すべてのノード |

**Server Manager** のログです

| ファイル名 | 注： | にあります |
| --- | --- | --- |
| `/var/local/log/servermanager.log` | サーバで実行されている Server Manager アプリケーションのログファイルです。 | すべてのノード |
| `/var/local/log/GridstatBackend.errlog` | Server Manager GUI バックエンドアプリケーションのログファイルです。 | すべてのノード |
| `/var/local/log/gridstat.errlog` | Server Manager GUI のログファイルです。 | すべてのノード |

**StorageGRID** サービスのログ

| ファイル名 | 注： | にあります |
| --- | --- | --- |
| /var/local/log/acct.errlog | | ADC サービスを実行しているストレージノード |
| /var/local/log/adc.errlog | 対応するサービスの標準エラー（ stderr ）ストリームが格納されます。サービスごとに 1 つのログファイルがあります。これらのファイルは、サービスに問題がなければ通常は空になります。 | ADC サービスを実行しているストレージノード |
| /var/local/log/ams.errlog | | 管理ノード |
| /var/local/log/arc.errlog | | アーカイブノード |
| /var/local/log/cassandra/system.log | メタデータストア（ Cassandra データベース）の情報。新しいストレージノードの追加時に問題が発生した場合、または nodetool repair タスクが停止した場合に使用できます。 | ストレージノード |
| /var/local/log/cassandra-reaper.log | Cassandra Reaper サービスの情報。 Cassandra データベース内のデータの修復を実行します。 | ストレージノード |
| /var/local/log/cassandra-reaper.errlog | Cassandra Reaper サービスのエラー情報。 | ストレージノード |
| /var/local/log/chunk.errlog | | ストレージノード |
| /var/local/log/clb.errlog | CLB サービスのエラー情報。<br>• 注： * CLB サービスは廃止されました。 | ゲートウェイノード |
| /var/local/log/cmn.errlog | | 管理ノード |
| /var/local/log/cms.errlog | このログファイルは、古いバージョンの StorageGRID からアップグレードされたシステムに存在する場合があります。古い情報が含まれています。 | ストレージノード |

| ファイル名 | 注： | にあります |
| --- | --- | --- |
| /var/local/log/cts.errlog | このログファイルは、ターゲットタイプが * Cloud Tiering - Simple Storage Service （ S3 ） . * の場合にのみ作成されます | アーカイブノード |
| /var/local/log/dds.errlog | | ストレージノード |
| /var/local/log/dmv.errlog | | ストレージノード |
| /var/local/log/dynip* | グリッドで IP の動的な変更を監視してローカル設定を更新する dynip サービスに関連するログが記録されます。 | すべてのノード |
| /var/local/log/grafana.log | Grid Manager で指標を視覚化するために使用される Grafana サービスに関連付けられたログ。 | 管理ノード |
| /var/local/log/hagroups.log | ハイアベイラビリティグループに関連付けられているログ。 | 管理ノードとゲートウェイノード |
| /var/local/log/hagroups_events.log | バックアップからマスターまたは障害への移行など、状態の変化を追跡します。 | 管理ノードとゲートウェイノード |
| /var/local/log/idnt.errlog | | ADC サービスを実行しているストレージノード |
| /var/local/log/jaeger.log | Jaeger サービスに関連付けられたログ。これは、トレース収集に使用されます。 | すべてのノード |
| /var/local/log/kstn.errlog | | ADC サービスを実行しているストレージノード |
| /var/local/log/ldr.errlog | | ストレージノード |

| ファイル名 | 注： | にあります |
| --- | --- | --- |
| `/var/local/log/miscd/*.log` | MISCd （ Information Service Control Daemon ）サービスのログが記録されます。このサービスは、他のノード上のサービスの照会と管理、およびノードの環境設定の管理（他のノードで実行されているサービスの状態の照会など）を行うためのインターフェイスを提供します。 | すべてのノード |
| `/var/local/log/nginx/*.log` | nginx サービスのログが記録されます。このサービスは、各種のグリッドサービス（ Prometheus や dynip など）が HTTPS API を介して他のノード上のサービスと通信できるようにするための、認証とセキュアな通信のメカニズムとして機能します。 | すべてのノード |
| `/var/local/log/nginx-gw/*.log` | 管理ノード上の制限された管理ポートのログ、およびクライアントからストレージノードへの S3 と Swift のトラフィックのロードバランシングを実現するロードバランササービスのログが記録されます。 | 管理ノードとゲートウェイノード |
| `/var/local/log/persistence*` | Persistence サービスのログが記録されます。このサービスは、リブート後も維持する必要があるルートディスク上のファイルを管理します。 | すべてのノード |
| `/var/local/log/prometheus.log` | すべてのノードを対象に、 node exporter サービスのログと ade-exporter サービスのログが記録されます。<br><br>管理ノードについては、 Prometheus サービスと Alert Manager サービスのログも記録されます。 | すべてのノード |
| `/var/local/log/raft.log` | RSM サービスで Rraft プロトコルに使用されるライブラリの出力が含まれます。 | RSM サービスを搭載しているストレージノードです |

| ファイル名 | 注： | にあります |
| --- | --- | --- |
| /var/local/log/rms.errlog | S3 プラットフォームサービスで使用される Replicated State Machine （ RSM ）サービスのログが記録されます。 | RSM サービスを搭載しているストレージノードです |
| /var/local/log/ssm.errlog | | すべてのノード |
| /var/local/log/update-s3vs-domains.log | S3 仮想ホストドメイン名設定の更新の処理に関連するログが記録されます。 S3 クライアントアプリケーションを実装する手順を参照してください。 | 管理ノードとゲートウェイノード |
| /var/local/log/update-snmp-firewall.* | SNMP 用に管理されているファイアウォールポートに関連するログが記録されます。 | すべてのノード |
| /var/local/log/update-sysl.log | システムの syslog 設定に対する変更に関連するログが記録されます。 | すべてのノード |
| /var/local/log/update-traffic-classes.log | トラフィック分類子設定の変更に関連するログが含まれます。 | 管理ノードとゲートウェイノード |
| /var/local/log/update-utcn.log | このノードでの「信頼されていないクライアントネットワーク」モードに関連するログが記録されます。 | すべてのノード |

**NMS** ログ

| ファイル名 | 注： | にあります |
| --- | --- | --- |
| /var/local/log/nms.log | • Grid Manager と Tenant Manager からの通知が記録されます。<br>• アラーム処理、 E メール通知、設定の変更など、 NMS サービスの処理に関連するイベントが記録されます。<br>• システムで行われた設定の変更に伴う XML バンドルの更新が格納されます。<br>• 1 日に 1 回実行される属性のダウンサンプリングに関連するエラーメッセージが格納されます。<br>• ページ生成エラーや HTTP ステータス 500 エラーなど、 Java Web サーバのエラーメッセージが格納されます。 | 管理ノード |
| /var/local/log/nms.errlog | MySQL データベースのアップグレードに関連するエラーメッセージが格納されます。<br><br>対応するサービスの標準エラー（ stderr ）ストリームが格納されます。サービスごとに 1 つのログファイルがあります。これらのファイルは、サービスに問題がなければ通常は空になります。 | 管理ノード |
| /var/local/log/nms.requestlog | 管理 API から内部 StorageGRID サービスへの発信接続に関する情報が含まれます。 | 管理ノード |

関連情報

"bycast.log について"

"S3 を使用する"

導入とメンテナンスのログ

導入とメンテナンスのログを問題のトラブルシューティングに使用できます。

| ファイル名 | 注： | にあります |
| --- | --- | --- |
| /var/local/log/install.log | ソフトウェアのインストール時に作成されます。インストールイベントが記録されます。 | すべてのノード |
| /var/local/log/expansion-progress.log | 拡張処理中に作成されます。拡張イベントが記録されます。 | ストレージノード |
| /var/local/log/gdu-server.log | GDU サービスによって作成されます。プライマリ管理ノードによって管理されるプロビジョニングとメンテナンスの手順に関連するイベントが記録されます。 | プライマリ管理ノード |
| /var/local/log/send_admin_hw.log | インストール時に作成されます。プライマリ管理ノードとの通信に関連するデバッグ情報が記録されます。 | すべてのノード |
| /var/local/log/upgrade.log | ソフトウェアのアップグレード中に作成されます。ソフトウェア更新イベントが記録されます。 | すべてのノード |

サードパーティソフトウェアのログ

## サードパーティソフトウェアのログを問題のトラブルシューティングに使用できます。

| カテゴリ | ファイル名 | 注： | にあります |
| --- | --- | --- | --- |
| apache2のログです | /var/local/log/apache2/access.log<br>/var/local/log/apache2/error.log<br><br>/var/local/log/apache2/other_vhosts_access.log | apache2のログファイルです。 | 管理ノード |
| アーカイブ | /var/local/log/dsierror.log | TSM クライアント API のエラー情報。 | アーカイブノード |

| カテゴリ | ファイル名 | 注： | にあります |
| --- | --- | --- | --- |
| MySQL | /var/local/log/mysql.err<br><br>`/var/local/log/mysql.err`<br>`/var/local/log/mysql-slow.log` | MySQL によって生成されるログファイルです。<br><br>mysql.errファイルには、データベースのエラーと起動やシャットダウンなどのイベントが記録されます。<br><br>mysql-slow.logファイル（スロークエリログ）には、実行に10秒以上かかったSQLステートメントが記録されます。 | 管理ノード |
| オペレーティングシステム | `/var/local/log/messages` | このディレクトリには、オペレーティングシステムのログファイルが格納されます。これらのログに記録されたエラーは、Grid Manager にも表示されます。Support **>** Tools **>** Grid Topology を選択します。次に、 ***Topology* > *Site*** > *Node** > * SSM * > * Events * を選択します。 | すべてのノード |
| NTP | `/var/local/log/ntp.log`<br><br>`/var/lib/ntp/var/log/ntpstats/` | 。`/var/local/log/ntp.log` NTPのエラーメッセージのログファイルが格納されます。<br><br>。`/var/lib/ntp/var/log/ntpstats/` Directory には、NTPタイミング統計情報が格納されます<br><br>`loopstats` ループフィルタの統計情報を記録します。<br><br>`peerstats` には、ピア統計情報が記録されます | すべてのノード |

| カテゴリ | ファイル名 | 注： | にあります |
| --- | --- | --- | --- |
| サンバ | `/var/local/log/samba/` | Samba のログディレクトリには、各 Samba プロセス（ smb 、 nmb 、および winbind ）とすべてのクライアントのホスト名 / IP を記録したログファイルが格納されます。 | CIFS 経由で監査共有をエクスポートするように設定された管理ノード |

#### bycast.log について

ファイル `/var/local/log/bycast.log` は、StorageGRID ソフトウェアのトラブルシューティングに使用する主要なファイルです。があります `bycast.log` ファイルを選択します。ファイルに、そのグリッドノードに固有のメッセージが含まれています。

ファイル `/var/local/log/bycast-err.log` はのサブセットです `bycast.log`。ERROR と CRITICAL の重大度のメッセージが含まれています。

#### bycast.log ファイルのローテーション

をクリックします `bycast.log` ファイルが1GBに達し、既存のファイルが保存され、新しいログファイルが開始されます。

保存されたファイルの名前が変更されます `bycast.log.1`をクリックすると、新しいファイルの名前がになります `bycast.log`。新しいとき `bycast.log` 1GBに達しました。 `bycast.log.1` が圧縮されて名前がに変更されます `bycast.log.2.gz`および `bycast.log` の名前がに変更され `bycast.log.1`。

の回転制限です `bycast.log` は21ファイルです。の22番目のバージョン `bycast.log` ファイルが作成され、最も古いファイルが削除されます。

の回転制限です `bycast-err.log` は7つのファイルです。

> 圧縮されたログファイルは、ファイルが圧縮された同じ場所に解凍しないでください。ファイルを同じ場所で解凍すると、ログローテーションスクリプトの妨げになることがあります。

関連情報

"ログファイルとシステムデータを収集しています"

#### bycast.log のメッセージです

のメッセージ `bycast.log` ADE（Asynchronous Distributed Environment）によって記述されます。ADE は、グリッドノードの各サービスで使用されるランタイム環境です。

ADEのメッセージの例を次に示します。

```
May 15 14:07:11 um-sec-rg1-agn3 ADE: |12455685    0357819531
SVMR EVHR 2019-05-05T27T17:10:29.784677| ERROR 0906 SVMR: Health
check on volume 3 has failed with reason 'TOUT'
```

ADE のメッセージには次の情報が含まれています。

| メッセージセグメント | 例の値 |
| --- | --- |
| ノード ID | 12455685 |
| ADE プロセス ID | 0357819531 |
| モジュール名 | SVMR |
| メッセージ ID | EVHR |
| UTC システム時間 | 2019-05-05T27T17 ： 10 ： 29.784677 （ YYYY-MM-DDTHH ： MM ： SS.uuuuuuuuuu ） |
| 重大度レベル | エラー |
| 内部追跡番号 | 0906. |
| メッセージ | SVMR ：ボリューム 3 のヘルスチェックが失敗しました。理由：「 TOUT 」 |

**bycast.log** のメッセージの重大度

## のメッセージ `bycast.log` 重大度レベルが割り当てられている。

例：

- *notice *-- 記録すべきイベントが発生しました。ほとんどのログメッセージはこのレベルです。
- * warning * — 予期しない状態が発生しました。
- * error * — 操作に影響を与える大きなエラーが発生しました。
- * critical * — 異常な状態が発生し、通常の動作が停止しました。原因となった状態にすぐに対処する必要があります。クリティカルなメッセージは Grid Manager にも表示されます。Support **>** Tools **>** Grid Topology *を選択します。次に、 [ * Site * ] > [ * Node * ] > * SSM * > * Events * を選択します。

**bycast.log** のエラーコード

## のほとんどのエラーメッセージです `bycast.log` エラーコードを含む。

次の表に、の代表的な非数値コードを示します `bycast.log`。非数値コードの正確な意味は、レポートされるコンテキストによって異なります。

| エラーコード | 意味 |
| --- | --- |
| SUCS | エラーはありません |
| GERR | 不明です |
| CANC | キャンセルされました |
| ABRT | 中止しました |
| TOUT | タイムアウト |
| INVL | 無効です |
| NFND | が見つかりません |
| vers | バージョン |
| 会議 | 設定 |
| 失敗 | 失敗しました |
| ICPL | 不完全です |
| 完了しました | 完了しました |
| SUNV | サービスを利用できません |

次の表に、の数値エラーコードを示します `bycast.log`。

| エラー番号 | エラーコード | 意味 |
| --- | --- | --- |
| 001 | EPERM | 操作は許可されていません |
| 002 | ENOENT | 指定したファイルまたはディレクトリは存在しません |
| 003 | ESRCH | そのようなプロセスはありません |
| 004.00 | EINTR | システムコールが中断されました |
| 005 | EIO | I/O エラー |

| エラー番号 | エラーコード | 意味 |
| --- | --- | --- |
| 6 、 6 | ENXIO | 該当するデバイスまたはアドレスはありません |
| 007 | E2BIG | 引数リストが長すぎます |
| 008 | ENOEXEC | EXEC フォーマットエラー |
| 009 | EBADF | ファイル番号が正しくありません |
| 010 | ECHILD | 子プロセスはありません |
| 011 | EAGAIN | 再試行してください |
| 012. | ENOMEM | メモリ不足です |
| 013 | EACCES | 権限が拒否されました |
| 014 | デフォルト | アドレスが無効です |
| 015 | ENOTBLK | ブロックデバイスが必要です |
| 016 | EBUSY | デバイスまたはリソースがビジー |
| 017 | EEXIST | ファイルが存在します |
| 018 | EXDEV の場合 | クロスデバイスリンク |
| 019 | ENODEV | 該当するデバイスはありません |
| 020 | ENOTDIR | ディレクトリではありません |
| 021 | EISDIR | はディレクトリです |
| 022 | EINVAL | 引数が無効です |
| 023 | ENFILE | ファイルテーブルオーバーフローです |
| 024 | EMFILE | 開いているファイルが多すぎます |
| 025 | ENOTTY | タイプライターではありません |

| エラー番号 | エラーコード | 意味 |
| --- | --- | --- |
| 026 | ETXTBSY | テキストファイルがビジーです |
| 027 | EFBIG | ファイルが大きすぎます |
| 028 | ENOSPC | デバイスにスペースが残っていません |
| 029 | ESPIPE | 不正なシークです |
| 030 | EROFS | 読み取り専用ファイルシステム |
| 031 | EMLINK | リンクが多すぎます |
| 032 | EPIPE | パイプ破損 |
| 033 | エドム | 関数のドメイン外の数学引数 |
| 034 | エスランゲ | 数学結果は表現できません |
| 035 | EDEADLK | リソースのデッドロックが発生する |
| 036 | ENAMETOOLONG | ファイル名が長すぎます |
| 037 | ENOLCK | 使用可能なレコードロックがありません |
| 038 | ENOSYS | 関数が実装されていません |
| 039 | ENOTEMPTY | ディレクトリが空ではありません |
| 040 | ELOOP | シンボリックリンクが多すぎます |
| 041 | | |
| 042 | ENOMSG | 必要なタイプのメッセージがありません |
| 043 | EIDRM | 識別子が削除されました |
| 044 | ECHRNG | チャネル番号が範囲外です |

| エラー番号 | エラーコード | 意味 |
| --- | --- | --- |
| 045 | EL2NSYNC | レベル 2 が同期されていません |
| 046 | EL3HLT | レベル 3 が停止しました |
| 047 | EL3RST | レベル 3 リセット |
| 048 | ELNRNG | リンク番号が範囲外です |
| 049 | EUNATCH | プロトコルドライバが接続されていません |
| 050 | ENOCSI | CSI 構造がありません |
| 051 | EL2HLT | レベル 2 が停止しました |
| 052 | EBADE の実行 | 無効な交換です |
| 053. | EBADR | 無効な要求記述子です |
| 054 | EXFULL （完全） | Exchange がいっぱいです |
| 055 | ENOANO | アノードなし |
| 056 | EBADRQC | 無効な要求コードです |
| 057. | EBADSLT | 無効なスロットです |
| 058 | | |
| 059. | EBFONT | フォントファイルの形式が正しくありません |
| 060 | ENOSTR | デバイスはストリームではありません |
| 061 | ENODATA | 使用できるデータがありません |
| 062 | イータイム | タイマーが切れました |
| 063 | ENOSR | Out of Streams のリソース |

| エラー番号 | エラーコード | 意味 |
| --- | --- | --- |
| 064 | ENONET | マシンがネットワーク上にありません |
| 065 | ENOPKG | パッケージがインストールされていません |
| 066 | EREMOTE | オブジェクトがリモートです |
| 067 | ENOLINK | リンクが切断されました |
| 068 | EADV | アドバタイズエラー |
| 069 | ESRMNT | Srmount エラー |
| 070 | エコム | 送信時の通信エラーです |
| 071 | EPROTO | プロトコルエラー |
| 072 | EMULTIHOP | マルチホップが試行されました |
| 073 | EDOTDOT | RFS 固有のエラー |
| 074 | EBADMSG と入力します | データメッセージではありません |
| 075 | EOVERFLOW | 定義されたデータ型の値が大きすぎます |
| 076 | ENOTUNIQ | 名前がネットワーク上で一意ではありません |
| 077 | EBADFD | ファイル記述子が無効な状態です |
| 078 | エルム変更 | リモートアドレスが変更されました |
| 079 | ELIBACC | 必要な共有ライブラリにアクセスできません |
| 080 | ELIBBAD 社 | 破損した共有ライブラリにアクセスしています |
| 081. | ELIBSCN | |

| エラー番号 | エラーコード | 意味 |
| --- | --- | --- |
| 082 | ELIBMAX | リンクしようとしている共有ライブラリが多すぎます |
| 083 | ELIBEXEC | 共有ライブラリを直接実行することはできません |
| 084 | EILSEQ | 不正なバイトシーケンスです |
| 085 | ERESTART | 中断されたシステムコールを再開する必要があります |
| 086 | ESTRPIPE | ストリームパイプエラー |
| 087 | EUSERS | ユーザが多すぎます |
| 088 | ENOTSOCK | ソケット以外でのソケット操作 |
| 089 | EDESTADDRREQ | 送信先アドレスは必須です |
| 090 | エMSGSIZE | メッセージが長すぎます |
| 091. | EPROTOTYPE | ソケットのプロトコルタイプが正しくありません |
| 092. | ENOPROTOOPT | プロトコルを使用できません |
| 093. | EPROTONOSUPPORT | サポートされていないプロトコルです |
| 094 | ESOCKTNOSUPPORT の略 | ソケットタイプはサポートされていません |
| 095 | EOPNOZ TSUPP | この処理は転送エンドポイントではサポートされません |
| 096 | EPFNOSUPPORT | サポートされていないプロトコルファミリーです |
| 097. | EAFNOSUPPORT | アドレスファミリーはプロトコルでサポートされていません |
| 098 | EADDRINUSE | アドレスはすでに使用されています |

| エラー番号 | エラーコード | 意味 |
| --- | --- | --- |
| 099 | EADDRNOTAVAIL | 要求アドレスを割り当てることができません |
| 100 | ENETDOWN | ネットワークが停止しています |
| 101 | ENETUNREACH | ネットワークに到達できません |
| 102 | ENETRESET | リセットのためネットワークが接続を切断しました |
| 103 | ECONNABORTED | ソフトウェアが接続を中止しました |
| 104 | ECONNRESET | ピアによって接続がリセットされました |
| 105 | ENOBUFS | 使用可能なバッファスペースがありません |
| 106. | EISCONN | トランスポートエンドポイントはすでに接続されています |
| 107 | ENOTCONN | トランスポートエンドポイントが接続されていません |
| 108 | ESH ダウンタウン | 転送エンドポイントのシャットダウン後に送信できません |
| 109 | ETOOMANYREFS | 参照が多すぎます：スプライスできません |
| 110 | ETIMEDOUT | 接続がタイムアウトしました |
| 111 | ECONNREFUSED | 接続が拒否されました |
| 112 | EHOSTDOWN | ホストが停止しています |
| 113. | EHOSTUNREACH | ホストへのルートがありません |
| 114 | エアルレーダド | 処理をすでに実行中です |
| 115 | 実行中 | 処理を実行中です |

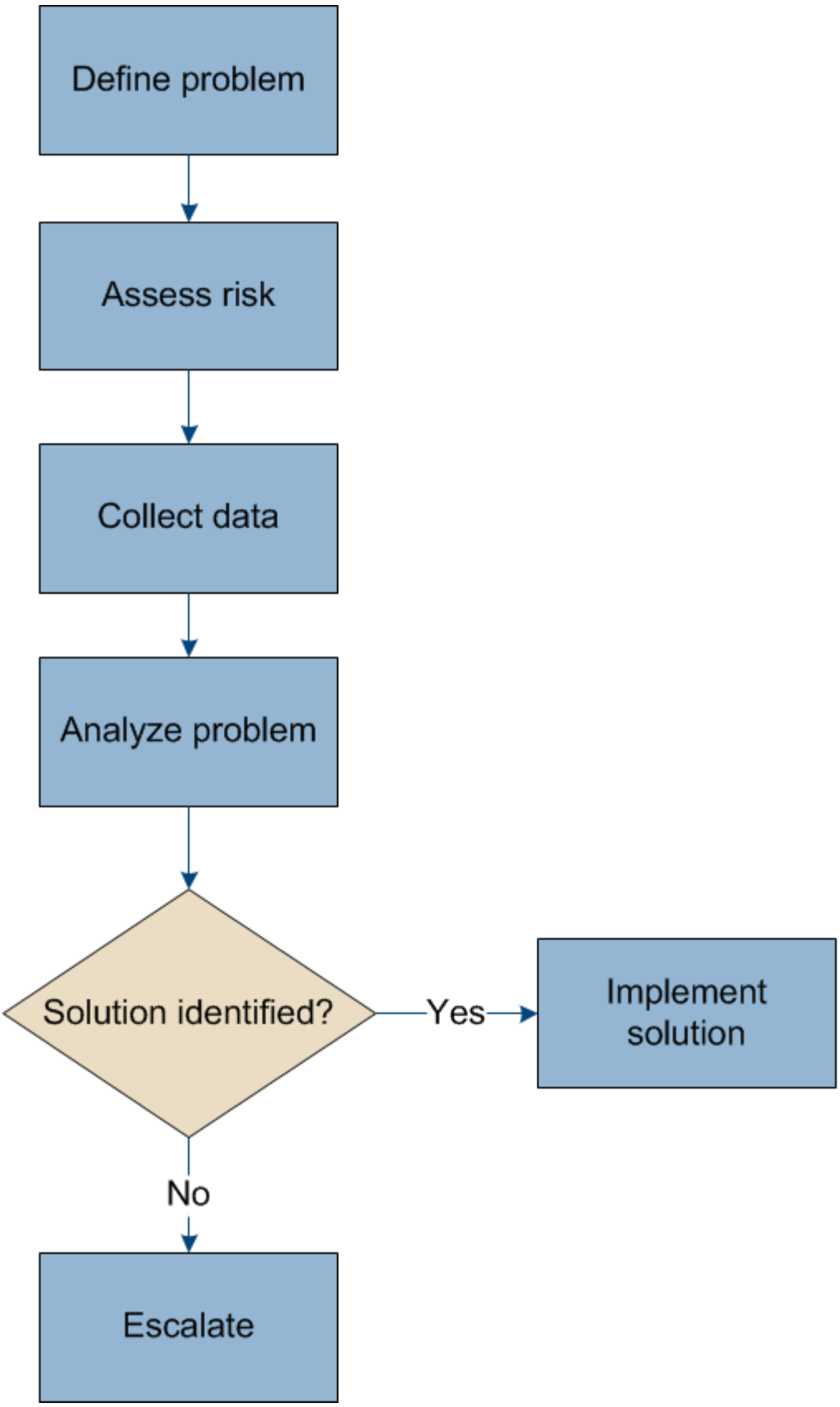
| エラー番号 | エラーコード | 意味 |
| --- | --- | --- |
| 116 | | |
| 117. | EUCLEAN | 構造はクリーニングが必要です |
| 118 | ENOTNAM | XENIX という名前のファイルではありません |
| 119 番 | ENAVAIL | XENIX セマフォーがありません |
| 120 | EISNAM | は、名前付きタイプファイルです |
| 121. | EREMOTEIO | リモート I/O エラーです |
| 122 | EDQUOT | クォータを超過しました |
| 123 | ENOMEDIUM | メディアが見つかりません |
| 124 | EMEDIUMTYPE | メディアタイプが正しくありません |
| 125 | ECANCELED | 処理がキャンセルされました |
| 126 | ENOKEY | 必要なキーがありません |
| 127 | エクイメピ RED も含まれています | キーの有効期限が切れました |
| 128 | エーケヨヴォエド | キーが取り消されました |
| 129 | EKEYREJECTED | キーがサービスによって拒否されました |
| 130 | EOWNERDEAD の場合 | 堅牢な mutex のため : 所有者は死んだ |
| 131 | ENOTRECOVERABLE | 堅牢な mutex の場合：状態は回復できません |

# StorageGRID システムのトラブルシューティングを行う

StorageGRID システムの使用中に問題が発生した場合は、このセクションのヒントとガイドラインを参考に、問題 を特定し、解決してください。

# 問題の特定の概要

StorageGRID システムの管理で問題が発生した場合は、次の図に示すプロセスを使用して、問題 を特定し、分析できます。多くの場合、問題は自力で解決できますが、一部の問題についてはテクニカルサポートへのエスカレーションが必要になることがあります。




問題を定義する

問題を解決するための最初のステップは、問題を明確に定義することです。

次の表に、問題を定義するために収集する情報の種類の例を示します。

| 質問 | 回答例 |
| --- | --- |
| StorageGRID システムはどのような状況にあり、どのような症状があるか？ | StorageGRID にオブジェクトを取り込めないことをクライアントアプリケーションが報告している。 |
| 問題はいつ発生しましたか？ | 2020 年 1 月 8 日 14 ： 50 頃にオブジェクトの取り込みが最初に拒否された。 |
| 最初にどのようにして問題に気付いたか。 | クライアントアプリケーションから通知される。アラートの E メール通知も受け取った。 |
| 問題は一貫して発生しますか、または時々発生しますか？ | 問題は現在も続いています。 |
| 問題が定期的に発生する場合は、原因 を実行する手順を確認してください | 問題は、クライアントがオブジェクトの取り込みを試みるたびに発生します。 |
| 問題が断続的に発生する場合は、いつ発生しますか？各インシデントの発生時刻を記録します。 | 問題は間欠的ではありません。 |
| この問題を以前に見たことがありますか？過去にこの問題が発生した頻度はどのくらいですか？ | この問題 を初めて見たときです。 |

システムに対するリスクと影響の評価

問題を定義したら、 StorageGRID システムに対するリスクと影響を評価します。たとえば、クリティカルなアラートがあるからといって、システムがコアサービスを提供していないわけではありません。

次の表は、前述の問題の例について、システムの運用に対する影響をまとめたものです。

| 質問 | 回答例 |
| --- | --- |
| StorageGRID システムでコンテンツを取り込むことはできますか。 | いいえ |
| クライアントアプリケーションでコンテンツを読み出せるかどうか | オブジェクトによっては読み出し可能なものと読み出せないものがあります。 |
| データがリスクにさらされているかどうか | いいえ |
| 業務を遂行する能力に重大な影響はありますか。 | はい。クライアントアプリケーションから StorageGRID システムにオブジェクトを格納できず、データを読み出す際の整合性が確保されない。 |

データの収集中です

問題を定義し、リスクと影響を評価したら、分析のためにデータを収集します。収集に最も役立つデータの種類は、問題の内容によって異なります。

| 収集するデータのタイプ | データを収集する理由 | 手順 |
| --- | --- | --- |
| 最近の変更のタイムラインを作成します | StorageGRID システム、その設定、または環境を変更すると、原因 の新しい動作を開始できます。 | • 最近の変更のタイムラインを作成する |
| アラートとアラームを確認します | アラートとアラームを使用すると、原因となっている問題に関する重要な手がかりを提供して、問題のルート原因 をすばやく特定することができます。<br><br>現在のアラートとアラームのリストを確認して、StorageGRID が問題のルート原因 を特定したかどうかを確認します。<br><br>過去にトリガーされたアラートやアラームを確認して、詳細な分析情報を入手できます。 | • "現在のアラートの表示"<br>• "古いアラームの表示"<br>• "解決済みのアラートの表示"<br>• "アラーム履歴とアラーム頻度の確認（従来のシステム）" |
| イベントを監視する | イベントには、ノードのシステムエラーまたは障害イベント、ネットワークエラーなどのエラーが含まれます。イベントを監視して、問題の詳細やトラブルシューティングに役立てることができます。 | • "[イベントタブを表示します"]<br>• "イベントの監視" |
| グラフレポートとテキストレポートを使用して傾向を特定します | 傾向は、問題が発生したときに役立つヒントを提供し、変化の速さを把握するのに役立ちます。 | • "グラフとレポートを使用する" |
| ベースラインを設定する | さまざまな運用値の通常レベルに関する情報を収集します。これらのベースライン値とこれらのベースラインからの偏差は、貴重な手がかりとなります。 | • ベースラインを設定する |
| 取り込みと読み出しのテストを実行する | 取り込みと読み出しに関するパフォーマンスの問題のトラブルシューティングを行うには、ワークステーションを使用してオブジェクトの格納と読み出しを行います。クライアントアプリケーションを使用して確認した結果と比較します。 | • "PUTおよびGETパフォーマンスの監視" |
| 監査メッセージを確認します | StorageGRID の処理の詳細については、監査メッセージを確認してください。監査メッセージの詳細は、パフォーマンスの問題など、さまざまな種類の問題のトラブルシューティングに役立ちます。 | • "監査メッセージの確認" |
| オブジェクトの場所とストレージの整合性をチェックする | ストレージに問題がある場合は、オブジェクトが想定どおりに配置されていることを確認します。ストレージノード上のオブジェクトデータの整合性をチェックします。 | "オブジェクト検証処理を監視します"。 |

| 収集するデータのタイプ | データを収集する理由 | 手順 |
| --- | --- | --- |
| テクニカルサポートに使用するデータを収集します | テクニカルサポートに問い合わせた際に、問題のトラブルシューティングに役立つデータの収集や特定の情報の確認を求められることがあります。 | • "ログファイルとシステムデータを収集しています"<br>• "手動でのAutoSupportメッセージのトリガー"<br>• "サポート指標の確認" |

最近の変更のタイムラインを作成する

問題が発生した場合は、最近の変更内容と、その変更がいつ行われたかを検討する必要があります。

- StorageGRID システム、その設定、または環境を変更すると、原因 の新しい動作を開始できます。
- 変更のスケジュールを確認することで、問題 の担当となる変更を特定し、各変更がその開発にどのような影響を及ぼすかを特定できます。

システムに最近行われた変更の表を作成します。この表には、各変更がいつ行われたかに関する情報と、変更の進行中に他に何が行われたかに関する関連情報が含まれます。

| 変更時刻 | 変更のタイプ | 詳細 |
| --- | --- | --- |
| 例：<br>• ノードのリカバリを開始したのはいつですか？<br>• ソフトウェアのアップグレードはいつ完了しましたか？<br>• プロセスを中断しましたか？ | どうしましたか？何をしましたか？ | 変更に関連する詳細を文書化します。例：<br>• ネットワークの詳細が変更されました。<br>• インストールされたホットフィックス。<br>• クライアントのワークロードの変化<br>同時に複数の変更が発生した場合は注意してください。たとえば、アップグレードの実行中にこの変更が行われたかどうかを確認します。 |

最近の重要な変更の例

重要な変更の例をいくつか示します。

- StorageGRID システムのインストール、拡張、リカバリを最近行ったかどうか
- システムは最近アップグレードされましたか？ホットフィックスが適用されましたか？
- ハードウェアの修理や交換を最近行ったかどうか
- ILM ポリシーは更新されているか。
- クライアントのワークロードは変化しましたか。
- クライアントアプリケーションまたはその動作に変化はありますか。

- ロードバランサを変更したか、管理ノードまたはゲートウェイノードのハイアベイラビリティグループを追加または削除したか。
- 開始されたタスクのうち、完了までに時間がかかるものはありますか？たとえば、次のようなもの
  - 障害が発生したストレージノードのリカバリ
  - ストレージノードの運用停止
- テナントの追加や LDAP 設定の変更など、ユーザ認証に変更がないかどうか
- データ移行を実行中かどうか
- プラットフォームサービスが最近有効化または変更されましたか？
- 最近、コンプライアンスを有効にしましたか？
- クラウドストレージプールは追加または削除されていますか？
- ストレージの圧縮や暗号化に変更がないかどうか
- ネットワークインフラに変更はありますか。たとえば、 VLAN 、ルータ、 DNS などです。
- NTP ソースに変更がないかどうか
- グリッド、管理、クライアントの各ネットワークインターフェイスに変更がないかどうか
- アーカイブノードの設定に変更がないかどうか
- StorageGRID システムや環境にその他の変更がないかどうか

ベースラインを設定する

さまざまな運用値の通常レベルを記録することで、システムのベースラインを設定できます。将来的には、現在の値をこれらのベースラインと比較して、異常な値を検出して解決することができます。

| プロパティ（ **Property** ） | 価値 | 取得方法 |
| --- | --- | --- |
| ストレージの平均消費量 | 1 日あたりの GB 消費量<br><br>1 日あたりの消費率 | Grid Manager に移動します。ノードページで、グリッド全体またはサイトを選択し、ストレージタブに移動します。<br><br>Storage Used - Object Data チャートで、この線がかなり安定している期間を探します。グラフにカーソルを合わせると、 1 日に消費されるストレージの量が推定されます<br><br>この情報は、システム全体または特定のデータセンターについて収集できます。 |
| メタデータの平均消費量 | 1 日あたりの GB 消費量<br><br>1 日あたりの消費率 | Grid Manager に移動します。ノードページで、グリッド全体またはサイトを選択し、ストレージタブに移動します。<br><br>Storage Used - Object Metadata チャートで、この線がかなり安定している期間を探します。グラフにカーソルを合わせて、 1 日に消費されるメタデータストレージの量を見積もります<br><br>この情報は、システム全体または特定のデータセンターについて収集できます。 |

| プロパティ（ **Property** ） | 価値 | 取得方法 |
| --- | --- | --- |
| S3 / Swift 処理のレート | 処理数 / 秒 | Grid Manager のダッシュボードに移動します。プロトコル処理セクションで、 S3 速度と Swift 速度の値を表示します。<br><br>特定のサイトまたはノードの取り込み速度と読み出し速度、および数を表示するには、* Nodes ***>*site***または***Storage Node***>* Objects *を選択します。S3 または Swift の取り込みと読み出しのグラフにカーソルを合わせます。 |
| 失敗した S3 / Swift 処理 | 処理 | Support **>** Tools **>** Grid Topology *を選択します。API Operations セクションの Overview タブで、 S3 Operations - Failed または Swift Operations - Failed の値を確認します。 |
| ILM 評価の速度 | オブジェクト数 / 秒 | ノードページで、 * *GRID_NETWORK** > * ILM * を選択します。<br><br>ILM キューグラフで、この線がかなり安定している期間を探します。グラフにカーソルを合わせて、システムの * 評価率 * のベースライン値を見積もります。 |
| ILM のスキャン速度 | オブジェクト数 / 秒 | ノード*>**GRID_NETWORK*>* ILM *を選択します。<br><br>ILM キューグラフで、この線がかなり安定している期間を探します。グラフにカーソルを合わせると、システムの * スキャンレート * のベースライン値が推定されます。 |
| クライアント処理からキューに登録されたオブジェクト | オブジェクト数 / 秒 | ノード*>**GRID_NETWORK*>* ILM *を選択します。<br><br>ILM キューグラフで、この線がかなり安定している期間を探します。グラフにカーソルを合わせて、システムの「 * Objects queued （ from client operations ） * 」のベースライン値を見積もります。 |
| クエリの平均レイテンシ | 表示されます | ノード*>*ストレージノード*>*オブジェクト*を選択します。クエリテーブルで、平均レイテンシの値を確認します。 |

データを分析中です

収集した情報を使用して、問題の原因 と潜在的な解決策を特定します。

分析方法は問題の内容によって異なりますが、一般的には次の手順に従ってください。

- アラームを使用して、障害が発生したポイントやボトルネックを特定します。
- アラーム履歴とチャートを使用して、問題の履歴を再構築します。
- チャートを使用して異常を特定し、問題の状況を通常の動作と比較します。

エスカレーション情報のチェックリスト

自分で問題を解決できない場合は、テクニカルサポートにお問い合わせください。テクニカルサポートに連絡する前に、次の表に記載された問題解決に必要な情報を収集してください。

| ✔ | 項目 | 注： |
|---|---|---|
| | 問題点 | 問題の症状は何ですか？問題はいつ発生しましたか？一貫して、または断続的に発生しますか？断続的に発生した場合、何回起きましたか？<br><br>"問題を定義する" |
| | 影響の評価 | 問題の重大度はどの程度ですか。クライアントアプリケーションにはどのような影響がありますか？<br><br>• クライアントは以前に正常に接続されていますか？<br>• クライアントはデータの取り込み、読み出し、削除を実行できますか。 |
| | StorageGRID システム ID | [* Maintenance （メンテナンス）**]>[** System （*システム）]>[* License *（*ライセンスStorageGRID システム ID は現在のライセンスの一部として表示されます。 |
| | ソフトウェアのバージョン | StorageGRID のバージョンを確認するには、* Help **>** About * をクリックします。 |
| | カスタマイズ | StorageGRID システムの構成をまとめます。たとえば、次のように指定します。<br><br>• グリッドでストレージ圧縮、ストレージ暗号化、コンプライアンスを使用していますか？<br>• ILM によってレプリケートオブジェクトまたはイレイジャーコーディングオブジェクトが作成されるか、ILM によってサイトの冗長性が確保されるか、ILM ルールの取り込み動作は Strict 、 Balanced 、 Dual Commit のいずれか）ですか。 |

| ✔ | 項目 | 注： |
| --- | --- | --- |
| | ログファイルとシステムデータ | システムのログファイルとシステムデータを収集します。[サポート（Support ）]>[*ツール（* Tools ）]>[*ログ（* Logs * ）] <br><br> ログは、グリッド全体または選択したノードについて収集できます。 <br><br> 選択したノードのログのみを収集する場合は、 ADC サービスがあるストレージノードを 1 つ以上含めるようにしてください。（サイトの最初の 3 つのストレージノードに ADC サービスが含まれています）。 <br><br> "ログファイルとシステムデータを収集しています" |
| | ベースライン情報 | 取り込み処理、読み出し処理、およびストレージ消費量に関するベースライン情報を収集します。 <br><br> "ベースラインを設定する" |
| | 最近の変更のタイムライン | システムや環境に対する最近の変更をまとめたタイムラインを作成 <br><br> "最近の変更のタイムラインを作成する" |
| | 問題 を診断するための取り組みの歴史 | 問題 の診断またはトラブルシューティングの手順を自分で実行した場合は、実行した手順と結果を記録しておいてください。 |

関連情報

"StorageGRID の管理"

# オブジェクトとストレージの問題のトラブルシューティング

ここでは、オブジェクトとストレージの問題の原因を特定するのに役立ついくつかのタスクを紹介します。

## オブジェクトデータの場所を確認する

問題の内容によっては、オブジェクトデータの格納場所の確認が必要になることがあります。たとえば、 ILM ポリシーが想定どおりに機能し、オブジェクトデータが意図した場所に格納されていることを確認できます。

必要なもの

- 次のいずれかのオブジェクト ID が必要です。
  - **UUID** ：オブジェクトの Universally Unique Identifier です。UUID はすべて大文字で入力します。
  - * CBID * ： StorageGRID 内のオブジェクトの一意の識別子。監査ログからオブジェクトの CBID を取得できます。CBID はすべて大文字で入力します。

- * S3 のバケットとオブジェクトキー * ：オブジェクトが S3 インターフェイスから取り込まれた場合、クライアントアプリケーションはバケットとオブジェクトキーの組み合わせを使用してオブジェクトを格納および識別します。
- * Swift のコンテナとオブジェクト名 * ：オブジェクトが Swift インターフェイスから取り込まれた場合、クライアントアプリケーションはコンテナとオブジェクト名の組み合わせを使用してオブジェクトを格納および識別します。

手順

1. 「* ILM > Object Metadata Lookup *」を選択します。
2. [ * 識別子 * （ * Identifier * ） ] フィールドにオブジェクトの識別子を入力します。

   UUID 、 CBID 、 S3 バケット / オブジェクトキー、または Swift コンテナ / オブジェクト名を入力できます。

3. [*検索（Look Up）]をクリックします。

   オブジェクトメタデータの検索結果が表示されます。このページには、次の種類の情報が表示されます。

   - システムメタデータ（オブジェクト ID （ UUID ）、オブジェクト名、コンテナの名前、テナントアカウントの名前または ID 、オブジェクトの論理サイズ、オブジェクトの作成日時、オブジェクトの最終変更日時など）。
   - オブジェクトに関連付けられているカスタムユーザメタデータのキーと値のペア。
   - S3 オブジェクトの場合、オブジェクトに関連付けられているオブジェクトタグのキーと値のペア。
   - レプリケートオブジェクトコピーの場合、各コピーの現在の格納場所。
   - イレイジャーコーディングオブジェクトコピーの場合、各フラグメントの現在の格納場所。
   - クラウドストレージプール内のオブジェクトコピーの場合、外部バケットの名前とオブジェクトの一意の識別子を含むオブジェクトの場所。
   - セグメント化されたオブジェクトとマルチパートオブジェクトの場合、セグメント ID とデータサイズを含むオブジェクトセグメントのリスト。100 個を超えるセグメントを持つオブジェクトの場合は、最初の 100 個のセグメントだけが表示されます。
   - 未処理の内部ストレージ形式のすべてのオブジェクトメタデータ。この未加工のメタデータには、リリース間で維持されるとはかぎらない内部のシステムメタデータが含まれます。

     次の例では、 2 つのレプリケートコピーとして格納された S3 テストオブジェクトのオブジェクトメタデータの検索結果が表示されています。

**System Metadata**

| | |
|---|---|
| Object ID | A12E96FF-B13F-4905-9E9E-45373F6E7DA8 |
| Name | testobject |
| Container | source |
| Account | t-1582139188 |
| Size | 5.24 MB |
| Creation Time | 2020-02-19 12:15:59 PST |
| Modified Time | 2020-02-19 12:15:59 PST |

**Replicated Copies**

| Node | Disk Path |
|---|---|
| 99-97 | /var/local/rangedb/2/p/06/0B/00nM8H$|TFbnQQ}|CV2E |
| 99-99 | /var/local/rangedb/1/p/12/0A/00nM8H$|TFboW28|CXG% |

**Raw Metadata**


```
{
    "TYPE": "CTNT",
    "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
    "NAME": "testobject",
    "CBID": "0x8823DE7EC7C10416",
    "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
    "PPTH": "source",
    "META": {
        "BASE": {
            "PAWS": "2",
```


関連情報

"ILM を使用してオブジェクトを管理する"

"S3 を使用する"

"Swift を使用します"

オブジェクトストア（ストレージボリューム）の障害

ストレージノードの基盤となるストレージは、複数のオブジェクトストアに分割されます。これらのオブジェクトストアは物理的なパーティションであり、StorageGRID システムのストレージのマウントポイントとして機能します。オブジェクトストアはストレージボリュームとも呼ばれます。

各ストレージノードのオブジェクトストアの情報を表示できます。オブジェクトストアは、ノード*>*ストレージノード*>*ストレージ*ページの下部に表示されます。

**Disk Devices**

| Name | World Wide Name | I/O Load | Read Rate | Write Rate |
|---|---|---|---|---|
| croot(8:1,sda1) | N/A | 1.62% | 0 bytes/s | 177 KB/s |
| cvloc(8:2,sda2) | N/A | 17.28% | 0 bytes/s | 2 MB/s |
| sdc(8:16,sdb) | N/A | 0.00% | 0 bytes/s | 11 KB/s |
| sdd(8:32,sdc) | N/A | 0.00% | 0 bytes/s | 0 bytes/s |
| sds(8:48,sdd) | N/A | 0.00% | 0 bytes/s | 0 bytes/s |

**Volumes**

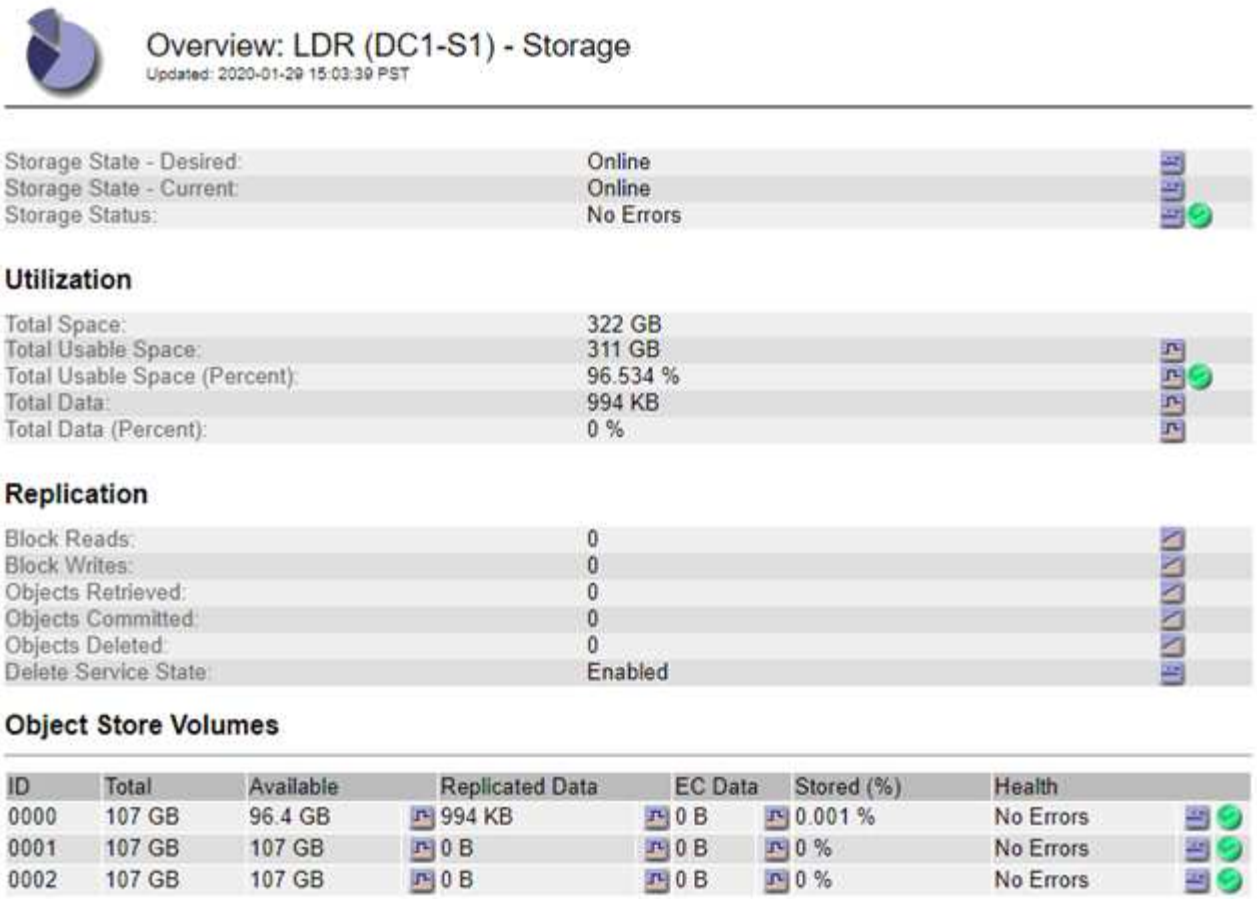
| Mount Point | Device | Status | Size | Available | Write Cache Status |
|---|---|---|---|---|---|
| / | croot | Online | 21.00 GB | 14.25 GB | Unknown |
| /var/local | cvloc | Online | 85.86 GB | 84.39 GB | Unknown |
| /var/local/rangedb/0 | sdc | Online | 107.32 GB | 107.18 GB | Enabled |
| /var/local/rangedb/1 | sdd | Online | 107.32 GB | 107.18 GB | Enabled |
| /var/local/rangedb/2 | sds | Online | 107.32 GB | 107.18 GB | Enabled |

**Object Stores**

| ID | Size | Available | Replicated Data | EC Data | Object Data (%) | Health |
|---|---|---|---|---|---|---|
| 0000 | 107.32 GB | 96.45 GB | 994.37 KB | 0 bytes | 0.00% | No Errors |
| 0001 | 107.32 GB | 107.18 GB | 0 bytes | 0 bytes | 0.00% | No Errors |
| 0002 | 107.32 GB | 107.18 GB | 0 bytes | 0 bytes | 0.00% | No Errors |

各ストレージノードの詳細を確認するには、次の手順を実行します。

1. Support **>** Tools **>** Grid Topology *を選択します。
2. [***site *>] > [*_Storage Node***] > [* ldr **] > [** Storage*] > [* Overview*] > [* Main*] を選択します。




ストレージボリュームの障害は、障害の性質に応じて、ストレージのステータスまたはオブジェクトストアの健常性のアラームに反映されます。ストレージボリュームに障害が発生した場合は、ストレージノードのすべての機能を復旧するために、障害が発生したストレージボリュームをできるだけ早く修復する必要があります。必要に応じて、「 * Configuration * 」タブに移動し、サーバを完全にリカバリするまでの間、StorageGRID システムがデータの読み出しに使用できるようにストレージノードを読み取り専用状態にすることができます。

関連情報

""

オブジェクトの整合性を検証してい

## StorageGRID システムは、ストレージノード上のオブジェクトデータの整合性を検証し、オブジェクトの破損や欠落の有無を確認します。

検証プロセスには、バックグラウンド検証とフォアグラウンド検証の2つがあります。データの整合性を確保するために連携して機能します。バックグラウンド検証は、オブジェクトデータの正確性を継続的にチェックするために自動的に実行されます。フォアグラウンド検証は、オブジェクトの有無（正確性ではなく）をより迅速に確認するためにユーザによってトリガーされます。

### バックグラウンド検証とは

バックグラウンド検証プロセスは、ストレージノードにオブジェクトデータの破損したコピーがないかどうかを自動的かつ継続的にチェックし、問題が見つかった場合は自動的に修復を試みます。

バックグラウンド検証は、レプリケートオブジェクトとイレイジャーコーディングオブジェクトの整合性を次

の方法でチェックします。

- * レプリケートオブジェクト * ：バックグラウンド検証プロセスで破損したレプリケートオブジェクトが検出された場合、破損したコピーはその場所から削除され、ストレージノード上の他の場所に隔離されます。その後、アクティブな ILM ポリシーに従って新しいコピーが生成され、配置されます。新しいコピーは、元のコピーに使用されていたストレージノードに配置されるとはかぎりません。

> 破損したオブジェクトデータは、引き続きアクセスできるように、システムから削除されるのではなく隔離されます。隔離されたオブジェクトデータへのアクセス方法については、テクニカルサポートにお問い合わせください。

- * イレイジャーコーディングオブジェクト * ：バックグラウンド検証プロセスでイレイジャーコーディングオブジェクトのフラグメントの破損が検出された場合、 StorageGRID は自動的に残りのデータとパリティフラグメントを使用して同じストレージノード上に欠落フラグメントの再構築を試みます。破損したフラグメントを再構築できなかった場合は、「Corrupt Copies Detected（ECOR）」属性の値が1つ増え、オブジェクトの別のコピーを読み出そうとします。読み出しに成功すると、 ILM 評価が実行されて、イレイジャーコーディングオブジェクトの置き換え用のコピーが作成されます。

  バックグラウンド検証プロセスでは、ストレージノード上のオブジェクトのみチェックされます。アーカイブノード上またはクラウドストレージプール内のオブジェクトはチェックされません。バックグラウンド検証を実行するには、 4 日以上経過したオブジェクトが必要です。

バックグラウンド検証は、通常のシステムアクティビティを妨げないように設定された間隔で継続的に実行されます。バックグラウンド検証を停止することはできません。ただし、問題があると疑われる場合は、バックグラウンド検証の回数を増やして、ストレージノードの内容をより迅速に検証することができます。

### バックグラウンド検証に関連するアラートとアラーム（レガシー）

破損したオブジェクトが自動的に修正できないことがシステムによって検出された場合（破損によってオブジェクトが特定されないため）、「識別されていない破損オブジェクトが検出されました * 」アラートがトリガーされます。

別のコピーが見つからないため、バックグラウンド検証が破損したオブジェクトを置き換えることができない場合は、* Objects lost *アラートとLOST（Lost Objects）レガシーアラームがトリガーされます。

### バックグラウンド検証レートを変更しています

データ整合性に関する懸念事項がある場合は、バックグラウンド検証によってストレージノード上のレプリケートオブジェクトデータをチェックする速度を変更できます。

#### 必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

#### このタスクについて

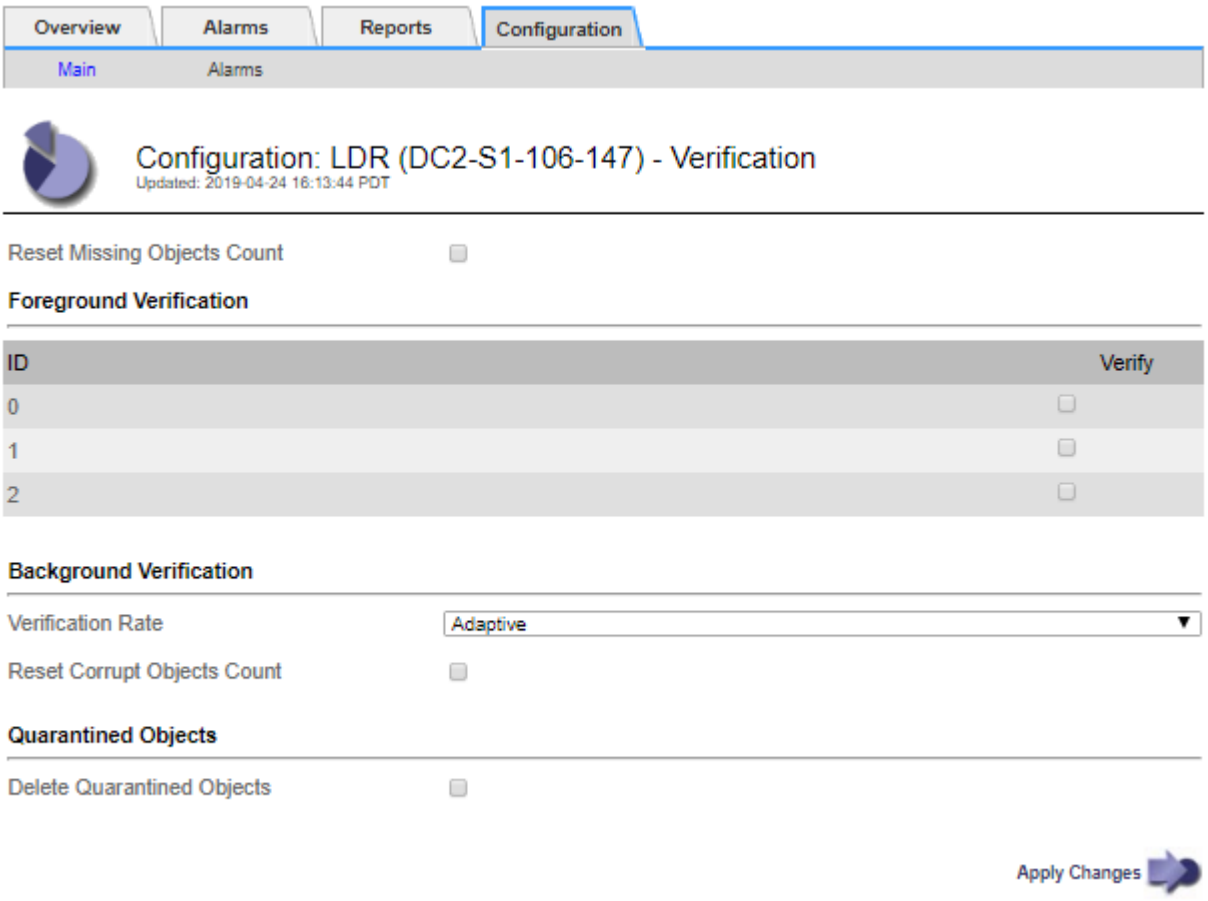
ストレージノードに対するバックグラウンド検証の検証レートを変更できます。

- Adaptive ：デフォルト設定です。最大 4MB/ 秒または 10 オブジェクト / 秒（先に超過した方）で検証するようにタスクが設計されます。
- High ：ストレージ検証は高速で実行され、通常のシステムアクティビティの処理速度が低下する可能性があります。

この設定は、ハードウェアまたはソフトウェアの障害により、オブジェクトデータが破損している可能性がある場合にのみ使用します。優先度の高いバックグラウンド検証が完了すると、検証レートは自動的に適応にリセットされます。

手順

1. Support **>** Tools **>** Grid Topology *を選択します。
2. [**_Storage Node]>[ldr]>[Verification**]を選択します。
3. * Configuration * > * Main * を選択します。
4. 「 * LDR * > * Verification * > * Configuration * > * Main * 」に移動します。
5. バックグラウンド検証で、 * 検証レート * > * 高 * または * 検証レート * > * 適応 * を選択します。




Verification Rate を High に設定すると、 Notice レベルで VPRI （ Verification Rate ） レガシーアラームがトリガーされます。

1. [ 変更の適用 *] をクリックします。
2. レプリケートオブジェクトのバックグラウンド検証の結果を監視します。
   a. ノード*>*ストレージノード*>*オブジェクト*に移動します。
   b. 「検証」セクションで、「破損したオブジェクト」および「破損したオブジェクトの特定なし」の値を監視します。

バックグラウンド検証で破損したレプリケートオブジェクトデータが見つかった場合は、「破損したオブジェクト * 」指標が増分され、 StorageGRID は次のようにデータからオブジェクト ID の抽出を試みます。

- オブジェクト ID を抽出できる場合は、 StorageGRID によってオブジェクトデータの新しいコピーが自動的に作成されます。新しいコピーは、アクティブな ILM ポリシーを満たしていれば、StorageGRID システム内のどこにでも作成できます。
- オブジェクト ID を抽出できない場合（破損しているため）は、「 Corrupt Objects Unidentified * 」指標が増分され、「 Unidentified Corrupt Objects Detected * 」アラートがトリガーされます。

c. 破損したレプリケートオブジェクトデータが見つかった場合は、テクニカルサポートに連絡して破損のルート原因 を確認します。

3. イレイジャーコーディングオブジェクトのバックグラウンド検証の結果を監視します。

バックグラウンド検証でイレイジャーコーディングオブジェクトデータの破損したフラグメントが検出された場合は、 Corrupt Fragments Detected 属性がその分だけ増分します。StorageGRID は、破損したフラグメントを同じストレージノード上に再構築して、この状況からリカバリします。

a. Support **>** Tools **>** Grid Topology *を選択します。

b. [*_Storage Node]>[ldr]>[Erasure Coding]を選択します。

c. Verification Results テーブルで、 Corrupt Fragments Detected （ ECCD ）属性を監視します。

4. 破損したオブジェクトが StorageGRID システムによって自動的にリストアされたら、破損したオブジェクトの数をリセットします。

a. Support **>** Tools **>** Grid Topology *を選択します。

b. [**_Storage Node]>[ldr]>[Verification]>[Configuration**]を選択します。

c. 「破損オブジェクト数をリセット」を選択します。

d. [ 変更の適用 *] をクリックします。

5. 隔離されたオブジェクトが不要であることが確実な場合は、オブジェクトを削除できます。

> Objects Lost * アラートまたは LOST （ Lost Objects ）レガシーアラームがトリガーされた場合、テクニカルサポートは、隔離されたオブジェクトにアクセスして、基になる問題 のデバッグやデータリカバリを試みることができます。

1. Support **>** Tools **>** Grid Topology *を選択します。
2. 「 * _ ストレージノード _ * > * LDR * > * Verification * > * Configuration * 」を選択します。
3. ［ * 隔離オブジェクトの削除 * ］ を選択します。
4. [ 変更の適用 *] をクリックします。

フォアグラウンド検証とは

フォアグラウンド検証はユーザが開始するプロセスで、想定されるすべてのオブジェクトデータがストレージノード上に存在するかどうかをチェックします。フォアグラウンド検証は、ストレージデバイスの整合性を検証するために使用します。

フォアグラウンド検証は、ストレージノード上のオブジェクトデータの存在はチェックしても整合性はチェックしないため、バックグラウンド検証よりも実行時間が短くて済みます。フォアグラウンド検証で多くの項目

が欠落していることが見つかった場合、ストレージノードに関連付けられているストレージデバイスのすべてまたは一部を含む問題 が存在する可能性があります。

フォアグラウンド検証は、レプリケートオブジェクトデータとイレイジャーコーディングオブジェクトデータの両方を次のようにチェックします。

- レプリケートオブジェクト：レプリケートされたオブジェクトデータのコピーが欠落していることがわかった場合、StorageGRID はシステム内の別の場所に格納されているコピーでコピーを自動的に置き換えます。ストレージノードは既存のコピーに対してILMを評価します。欠落したコピーはすでに想定される場所に存在しないため、このオブジェクトに関して現在のILMポリシーは満たされていないという結果となります。その結果、システムのアクティブなILMポリシーに沿って新しいコピーが生成されて配置されます。この新しいコピーは、欠落したコピーが格納されていた場所に配置されるとはかぎりません。
- イレイジャーコーディングオブジェクト：イレイジャーコーディングオブジェクトのフラグメントが欠落していることがわかった場合、StorageGRID は自動的に残りのフラグメントを使用して同じストレージノード上に欠落フラグメントの再構築を試みます。欠落フラグメントを再構築できなかった場合（失われたフラグメントの数が多すぎるため）は、「Corrupt Copies Detected（ECOR）」属性の値が1つ増えます。次にILMは、新しいイレイジャーコーディングコピーを生成するために使用できる、オブジェクトの別のコピーを探します。

  フォアグラウンド検証でストレージボリューム上のイレイジャーコーディングを含む問題 が特定されると、フォアグラウンド検証タスクは一時停止し、影響を受けたボリュームを示すエラーメッセージが表示されます。該当するストレージボリュームに対してリカバリ手順 を実行する必要があります。

欠落しているレプリケートオブジェクトまたは破損したイレイジャーコーディングオブジェクトの他のコピーがグリッド内に見つからなかった場合は、* Objects Lost *アラートとLOST（Lost Objects）レガシーアラームがトリガーされます。

### フォアグラウンド検証を実行しています

フォアグラウンド検証では、ストレージノードにデータが存在するかどうかを確認できます。オブジェクトデータが欠落している場合、基盤となるストレージデバイスに問題 が存在している可能性があります。

#### 必要なもの

- 次のグリッドタスクが実行されていないことを確認します。
  - Gridの拡張：ストレージノードを追加する際にサーバを追加（GEXP
  - Storage Node Decommissioning（LDCM）。グリッドタスクが実行中の場合は、それらが完了するまで待つか、ロックを解除します。
- ストレージがオンラインであることを確認します（* Support **>** Tools **>** Grid Topology を選択します。次に、「*ストレージ・ノード>* LDR **>** Storage **>** Overview **>** Main 」を選択します。 Storage State-Current *がOnlineであることを確認します）。
- 次のリカバリ手順が同じストレージノード上で実行されていないことを確認します。
  - 障害ストレージボリュームのリカバリ
  - システムドライブのフォアグラウンド検証でエラーが発生したストレージノードをリカバリすると、リカバリ手順の実行中に役立つ情報が得られません。

#### このタスクについて

フォアグラウンド検証は、欠落しているレプリケートオブジェクトデータとイレイジャーコーディングオブジェクトデータの両方をチェックします。

- フォアグラウンド検証で大量の欠落オブジェクトデータが見つかった場合は、調査および対処が必要なストレージノードのストレージを備えた問題 が存在する可能性があります。
- イレイジャーコーディングデータに関連する重大なストレージエラーがフォアグラウンド検証で見つかった場合は、通知が送信されます。ストレージボリュームのリカバリを実行してエラーを修復する必要があります。

フォアグラウンド検証では、ストレージノードのすべてのオブジェクトストアをチェックすることも、特定のオブジェクトストアのみをチェックすることもできます。

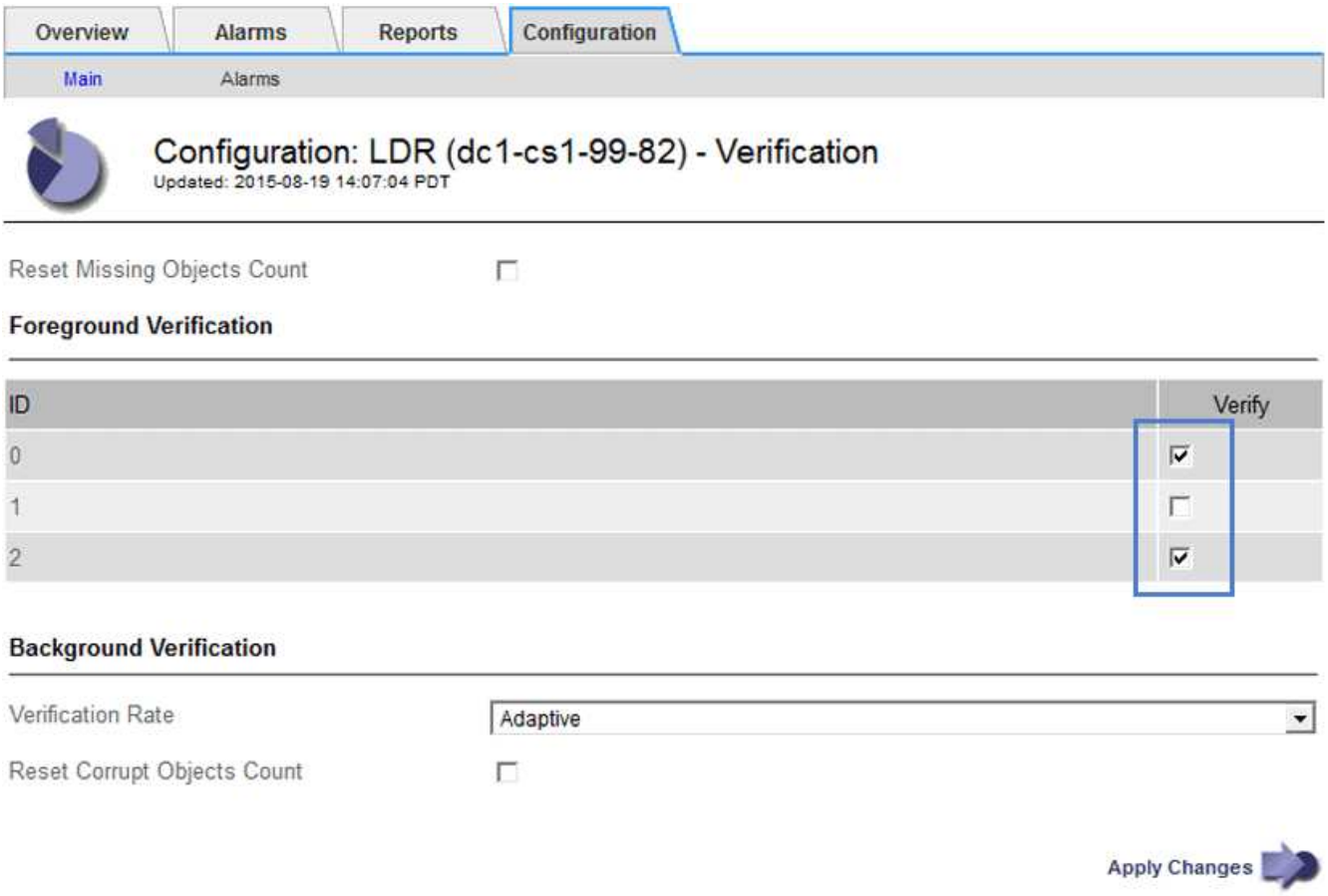
フォアグラウンド検証で欠落オブジェクトデータが見つかった場合、StorageGRID システムはデータの置き換えを試みます。置き換え用のコピーを作成できない場合、LOST（Lost Objects）アラームがトリガーされることがあります。

フォアグラウンド検証を実行すると、LDRフォアグラウンド検証グリッドタスクが生成されます。このタスクの所要時間はストレージノードに格納されているオブジェクトの数によって異なり、完了までに数日から数週間かかることがあります。同時に複数のストレージノードを選択できますが、これらのグリッドタスクが同時に実行されることはありません。代わりに、キューに登録され、1つずつ順番に実行されます。あるストレージノードでフォアグラウンド検証が実行中のときは、そのストレージノードで他のボリュームを検証するオプションを選択できたとしても、同じストレージノードで別のフォアグラウンド検証タスクを開始することはできません。

フォアグラウンド検証の実行中でないストレージノードがオフラインになった場合は、**% complete *属性が**99.99%**に達するまでグリッドタスクが続行されます。この場合、「%complete」属性は50%にフォールバックされ、ストレージノードがオンラインステータスに戻るまで待機します。ストレージノードがオンライン状態に戻ると、LDRフォアグラウンド検証グリッドタスクが再開されて完了するまで実行されます。

手順

1. 「* _ ストレージノード _ * > * LDR * > * Verification * 」を選択します。
2. * Configuration * > * Main * を選択します。
3. [* Foreground Verification]で、確認する各ストレージボリュームIDのチェックボックスを選択します。




4. [ 変更の適用 *] をクリックします。

   ページが自動的に更新されてリロードされるまで待ってから、ページを終了します。ページが更新されると、そのストレージノードのオブジェクトストアは選択できなくなります。

   LDRフォアグラウンド検証グリッドタスクが生成され、完了または一時停止するか、または中止されるまで実行されます。

5. 欠落オブジェクトまたは欠落フラグメントを監視します。

   a. 「 * _ ストレージノード _ * > * LDR * > * Verification * 」を選択します。

   b. [Overview（概要）]タブの[* Verification Results（検証結果）**]**の下にある**[** Missing Objects Detected（不足オブジェクトが検出されました）]の値を

      注：Nodesページで、「* Lost Objects 」と同じ値が報告されます。ノード>*ストレージノード*に移動し、*オブジェクト*タブを選択します。

      「Missing Objects Detected」の数が多い場合（欠落オブジェクトが数百ある場合）は、ストレージノードのストレージを含む問題 が存在する可能性があります。テクニカルサポートにお問い合わせください。

   c. 「 * _ ストレージノード _ * > * LDR * > * イレイジャーコーディング * 」を選択します。

   d. [Overview（概要）]タブの[* Verification Results]（検証結果）で、[**Missing Fragments Detected**（欠落フラグメントが検出されました）]の値を確認

      「Missing Fragments Detected」の数が多い場合（欠落フラグメントが数百個ある場合）は、ストレ

ージノードのストレージを含む問題 が存在する可能性があります。テクニカルサポートにお問い合わせください。

レプリケートオブジェクトコピーまたはフラグメントの欠落がフォアグラウンド検証で大量に見つからなければ、ストレージは正常に動作しています。

6. フォアグラウンド検証グリッドタスクが完了するまで監視します。
   a. Support **>** Tools **>** Grid Topology を選択します。次に、 site ***>Admin Node***>* cmn **>** Grid Task **>** Overview **>** Main *の順に選択します。
   b. フォアグラウンド検証グリッドタスクがエラーなく実行されていることを確認します。

      *注：フォアグラウンド検証グリッドタスクが一時停止すると、グリッドタスクステータス（SCAS）に対してNoticeレベルのアラームがトリガーされます。

   c. を使用してグリッドタスクが一時停止した場合 `critical storage error`をクリックし、影響を受けたボリュームをリカバリしてから、残りのボリュームでフォアグラウンド検証を実行してさらにエラーが発生していないかを確認します。

      注意：フォアグラウンド検証グリッドタスクがメッセージとともに一時停止した場合 `Encountered a critical storage error in volume *volID*`では、障害ストレージボリュームをリカバリするために手順 を実行する必要があります。リカバリとメンテナンスの手順を参照してください。

完了後

データの整合性についてまだ懸念がある場合は、「* LDR **>** Verification **>** Configuration **>** Main *」に移動し、バックグラウンド検証レートを増やしてください。バックグラウンド検証は、格納されているすべてのオブジェクトデータの正確性を確認し、見つかった問題を修復します。潜在的な問題をできるだけ早く検出して修復することで、データ損失のリスクが軽減されます。

関連情報

""

オブジェクトデータの損失と欠落が発生した場合のトラブルシューティング

## オブジェクトはさまざまな理由で読み出されます。たとえば、クライアントアプリケーションからの読み取り要求、レプリケートされたオブジェクトデータのバックグラウンド検証、 ILM ルールによる再評価、ストレージノードのリカバリ時のオブジェクトデータのリストアなどの目的で行われます。

StorageGRID システムは、オブジェクトのメタデータに記載された場所の情報を使用して、オブジェクトの読み出し元の場所を特定します。想定される場所でオブジェクトのコピーが見つからない場合、システムは ILM ポリシーにオブジェクトのコピーを複数保持するルールが含まれているものとして、システム内の他の場所から別のコピーを読み出そうとします。

この読み出しに成功すると、欠落しているオブジェクトのコピーが StorageGRID システムによって置き換えられます。そうしないと、* Objects lost *アラートとレガシーLOST（Lost Objects）アラームが次のようにトリガーされます。

- レプリケートコピーについては、別のコピーを読み出せない場合、オブジェクトが失われたとみなされ、アラートとアラームがトリガーされます。
- イレイジャーコーディングされたコピーについては、想定される場所からコピーを読み出せない場合、他

の場所からの読み出しが試行される前に「 Corrupt Copies Detected （ ECOR ）」属性の値が 1 つ増分されます。他のコピーが見つからないと、アラートとアラームがトリガーされます。

すべての * Objects Lost * アラートをすぐに調査して損失のルート原因 を特定し、オフラインなどの何らかの理由で現在使用できないストレージノードやアーカイブノードにオブジェクトが残っていないかどうかを確認する必要があります。

コピーがないオブジェクトデータが失われた場合、リカバリ解決策 はありません。ただし、既知の損失オブジェクトが新しい損失オブジェクトをマスキングしないように、Lost Objectカウンタをリセットする必要があります。

関連情報

"損失オブジェクトを調査しています"

"損失オブジェクトと欠落オブジェクトのカウントのリセット"

損失オブジェクトを調査しています

## Objects lost *アラートとレガシーLOST（Lost Objects）アラームがトリガーされた場合は、すぐに調査する必要があります。影響を受けるオブジェクトに関する情報を収集し、テクニカルサポートに連絡してください。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- を用意しておく必要があります `Passwords.txt` ファイル。

このタスクについて

Objects lost *アラートとLOSTアラームは、StorageGRID がグリッド内にオブジェクトのコピーがないと判断したことを示しています。データが完全に失われた可能性があります。

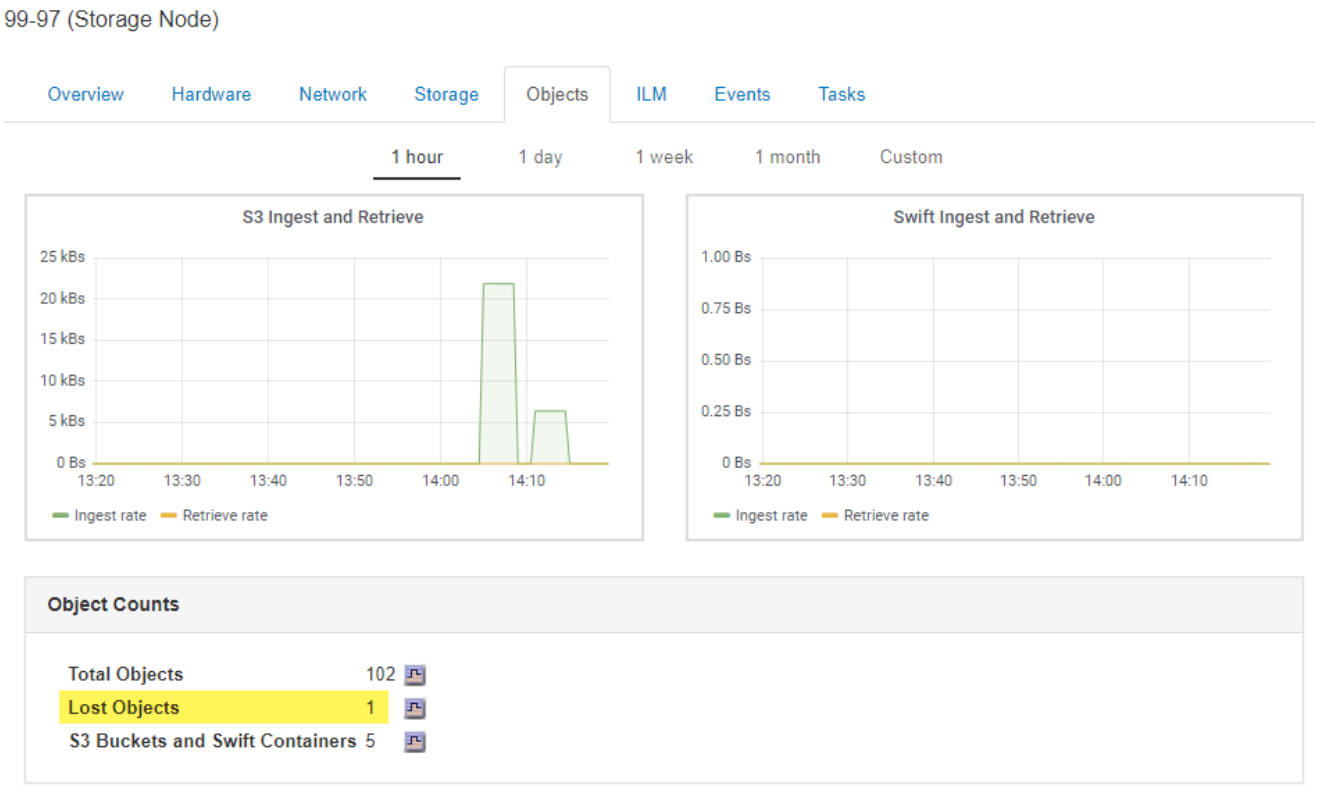
LOSTオブジェクトのアラームやアラートをすぐに調査する必要があります。これ以上のデータ損失を防ぐための対処が必要になる場合があります。迅速に対処すれば、損失オブジェクトをリストアできる場合があります。

Lost Objectsの数がGrid Managerに表示されます。

手順

1. [ノード（ Nodes）]を選択し
2. [***Storage Node***>* Objects*] を選択します。
3. Object Countsテーブルに表示されているLost Objectsの数を確認します。

   この数値は、 StorageGRID システム全体で欠落していることがグリッドノードで検出されたオブジェクトの合計数を示します。この値は、LDRサービスとDDSサービスに含まれるData Storeコンポーネントのlost Objectsカウンタの合計です。




4. 管理ノードから監査ログにアクセスして、* Objects Lost *アラートとLOSTアラームをトリガーしたオブジェクトの一意の識別子（UUID）を確認します。
   a. グリッドノードにログインします。
      i. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
      ii. に記載されているパスワードを入力します `Passwords.txt` ファイル。
      iii. 次のコマンドを入力してrootに切り替えます。 `su -`
      iv. に記載されているパスワードを入力します `Passwords.txt` ファイル。rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。
   b. 監査ログが格納されているディレクトリに移動します。入力するコマンド `cd /var/local/audit/export/`
   c. grep を使用して Object Lost （ OLST ）監査メッセージを抽出します。入力するコマンド `grep OLST audit_file_name`
   d. メッセージに含まれている UUID の値をメモします。

```
>Admin: # grep OLST audit.log
2020-02-12T19:18:54.780426
[AUDT:[CBID(UI64):0x38186FE53E3C49A5][UUID(CSTR):926026C4-00A4-449B-
AC72-BCCA72DD1311]
[PATH(CSTR):"source/cats"][NOID(UI32):12288733][VOLI(UI64):3222345986
][RSLT(FC32):NONE][AVER(UI32):10]
[ATIM(UI64):1581535134780426][ATYP(FC32):OLST][ANID(UI32):12448208][A
MID(FC32):ILMX][ATID(UI64):7729403978647354233]]
```

5. を使用します `ObjectByUUID` コマンドを使用して識別子（UUID）でオブジェクトを検索し、データにリスクがあるかどうかを確認できます。

   a. Telnet で localhost 1402 に接続して、 LDR コンソールにアクセスします。

   b. 入力するコマンド `/proc/OBRP/ObjectByUUID UUID_value`

      この最初の例では、を持つオブジェクトです `UUID 926026C4-00A4-449B-AC72-BCCA72DD1311` には2つの場所が表示されて

```
ade 12448208: /proc/OBRP > ObjectByUUID 926026C4-00A4-449B-AC72-
BCCA72DD1311

{
    "TYPE(Object Type)": "Data object",
    "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
    "NAME": "cats",
    "CBID": "0x38186FE53E3C49A5",
    "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-
ACBB00BB82DD",
    "PPTH(Parent path)": "source",
    "META": {
        "BASE(Protocol metadata)": {
            "PAWS(S3 protocol version)": "2",
            "ACCT(S3 account ID)": "44084621669730638018",
            "*ctp(HTTP content MIME type)": "binary/octet-stream"
        },
        "BYCB(System metadata)": {
            "CSIZ(Plaintext object size)": "5242880",
            "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
            "BSIZ(Content block size)": "5252084",
            "CVER(Content block version)": "196612",
            "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
            "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
            "ITME": "1581534970983000"
        },
        "CMSM": {
            "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
        },
        "AWS3": {
            "LOCC": "us-east-1"
        }
    },
```

```
    "CLCO\(Locations\)": \[
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12448208",
            "VOLI\(Volume ID\)": "3222345473",
            "Object File Path":
"/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila\#3udu",
            "LTIM\(Location timestamp\)": "2020-02-
12T19:36:17.880569"
        \},
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12288733",
            "VOLI\(Volume ID\)": "3222345984",
            "Object File Path":
"/var/local/rangedb/0/p/19/11/00rH0%DkRt78Rrb\#3s;L",
            "LTIM\(Location timestamp\)": "2020-02-
12T19:36:17.934425"
        }
    ]
}
```

2番目の例では、を指定したオブジェクトです `UUID 926026C4-00A4-449B-AC72-BCCA72DD1311` 場所が表示されていません。

```
ade 12448208: / > /proc/OBRP/ObjectByUUID 926026C4-00A4-449B-AC72-
BCCA72DD1311

{
    "TYPE(Object Type)": "Data object",
    "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
    "NAME": "cats",
    "CBID": "0x38186FE53E3C49A5",
    "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-ACBB00BB82DD",
    "PPTH(Parent path)": "source",
    "META": {
        "BASE(Protocol metadata)": {
            "PAWS(S3 protocol version)": "2",
            "ACCT(S3 account ID)": "44084621669730638018",
            "*ctp(HTTP content MIME type)": "binary/octet-stream"
        },
        "BYCB(System metadata)": {
            "CSIZ(Plaintext object size)": "5242880",
            "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
            "BSIZ(Content block size)": "5252084",
            "CVER(Content block version)": "196612",
            "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
            "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
            "ITME": "1581534970983000"
        },
        "CMSM": {
            "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
        },
        "AWS3": {
            "LOCC": "us-east-1"
        }
    }
}
```

a. /proc/OBRP/ObjectByUUID の出力を確認し、適切な処理を実行します。

| メタデータ | まとめ |
| --- | --- |
| オブジェクトが見つかりません（ "ERROR" ： "" ） | オブジェクトが見つからない場合は「 ERROR 」：というメッセージが返されます。<br><br>オブジェクトが見つからない場合は、このアラームを無視してかまいません。オブジェクトがない場合は、意図的に削除されたオブジェクトであることを示しています。 |
| 場所が 0 より大きい | 出力に場所が表示される場合は、Lost Objectsアラームが誤検知されることがあります。<br><br>オブジェクトが存在することを確認します。出力に表示されたノード ID とファイルパスを使用して、オブジェクトファイルがリストされた場所にあることを確認します。<br><br>（失われた可能性があるオブジェクトを検索するための手順 では、ノードIDを使用して正しいストレージノードを検索する方法について説明しています）。<br><br>"失われた可能性があるオブジェクトの検索とリストア"<br><br>オブジェクトが存在する場合は、Lost Objectsの数をリセットして、アラームとアラートをクリアできます。 |
| 場所 = 0 | 出力に場所が表示されない場合は、オブジェクトが欠落している可能性があります。オブジェクトを手動で検索してリストアするか、テクニカルサポートにお問い合わせください。<br><br>"失われた可能性があるオブジェクトの検索とリストア"<br><br>テクニカルサポートに問い合わせた際に、実行中のストレージリカバリ手順 がないかどうかを確認するように求められることがあります。つまり、いずれかのストレージノードで _repair-data_command が実行されたあとにリカバリを実行中でないかを確認します。リカバリとメンテナンスの手順のストレージボリュームへのオブジェクトデータのリストアに関する情報を参照してください。 |

関連情報

""

"監査ログを確認します"

失われた可能性があるオブジェクトの検索とリストア

## Lost Objects （ LOST ）アラームと * Object lost * アラートをトリガーした（失われた可能性があると特定した）オブジェクトを検索してリストアできる場合があります。

必要なもの

- 「損失オブジェクトの調査」で特定した損失オブジェクトの UUID が必要です。
- を用意しておく必要があります `Passwords.txt` ファイル。

このタスクについて

この手順 を使用して、グリッド内の他の場所で損失オブジェクトのレプリケートコピーを検索できます。ほとんどの場合、損失オブジェクトは見つかりません。ただし、迅速に対処すれば、損失レプリケートオブジェクトを検索してリストアできる場合があります。

この手順 のサポートについては、テクニカルサポートにお問い合わせください。

手順

1. 管理ノードの監査ログで、オブジェクトが存在する可能性のある場所を検索します。
   a. グリッドノードにログインします。
      i. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
      ii. に記載されているパスワードを入力します `Passwords.txt` ファイル。
      iii. 次のコマンドを入力してrootに切り替えます。 `su -`
      iv. に記載されているパスワードを入力します `Passwords.txt` ファイル。rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。
   b. 監査ログが格納されているディレクトリに移動します。 `cd /var/local/audit/export/`
   c. grep を使用して、失われた可能性があるオブジェクトに関連付けられている監査メッセージを抽出し、出力ファイルに送信します。入力するコマンド `grep uuid-valueaudit_file_name > output_file_name`

      例：

      ```
      Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
      messages_about_lost_object.txt
      ```

   d. grep を使用して、この出力ファイルから Location Lost （ LLST ）監査メッセージを抽出します。入力するコマンド `grep LLST output_file_name`

      例：

      ```
      Admin: # grep LLST messages_about_lost_objects.txt
      ```

      LLST 監査メッセージは次のサンプルメッセージのようになります。

```
[AUDT:\[NOID\(UI32\):12448208\][CBIL(UI64):0x38186FE53E3C49A5]
[UUID(CSTR):"926026C4-00A4-449B-AC72-BCCA72DD1311"][LTYP(FC32):CLDI]
[PCLD\(CSTR\):"/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%\#3tN6"\]
[TSRC(FC32):SYST][RSLT(FC32):NONE][AVER(UI32):10][ATIM(UI64):
1581535134379225][ATYP(FC32):LLST][ANID(UI32):12448208][AMID(FC32):CL
SM]
[ATID(UI64):7086871083190743409]]
```

e. LLST メッセージで PCLD フィールドと NOID フィールドを検索します。

PCLD の値は、欠落しているレプリケートオブジェクトコピーへのディスク上の完全なパスです。NOID の値は、オブジェクトのコピーが存在する可能性のある LDR のノード ID です。

オブジェクトの場所が見つかった場合は、オブジェクトをリストアできる場合があります。

f. この LDR ノード ID のストレージノードを探します。

ノード ID を使用してストレージノードを特定する方法は 2 つあります。

- Grid Managerで、* Support > Tools > Grid Topology *を選択します。次に、「 * _ データセンター _ * > * _ ストレージノード _ * > * LDR * 」を選択します。LDR ノード ID は Node Information テーブルに含まれています。この LDR をホストしているストレージノードが見つかるまで、各ストレージノードの情報を確認します。
- グリッドのリカバリパッケージをダウンロードして解凍します。SAID パッケージには _\docs_directory があります。index.html ファイルを開くと、 Servers Summary には、すべてのグリッドノードのすべてのノード ID が表示されます。

2. 監査メッセージで指定されているストレージノードにオブジェクトが存在するかどうかを確認します。

a. グリッドノードにログインします。

i. 次のコマンドを入力します。 `ssh admin@grid_node_IP`

ii. に記載されているパスワードを入力します `Passwords.txt` ファイル。

iii. 次のコマンドを入力してrootに切り替えます。 `su -`

iv. に記載されているパスワードを入力します `Passwords.txt` ファイル。

rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

b. オブジェクトのファイルパスが存在するかどうかを確認します。

オブジェクトのファイルパスには、 LLST 監査メッセージの PCLD の値を使用します。

たとえば、次のように入力します。

```
ls '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'
```

- 注 * ：オブジェクトファイルのパスは、特殊文字をエスケープするために、必ず一重引用符で囲んでください。

- オブジェクトパスが見つからない場合はオブジェクトが失われるため、この手順 を使用してリストアすることはできません。テクニカルサポートにお問い合わせください。
- オブジェクトパスが見つかった場合は、手順に進みます オブジェクトを StorageGRID にリストアします。見つかったオブジェクトを StorageGRID にリストアできます。

1. オブジェクトパスが見つかった場合は、オブジェクトをStorageGRID にリストアします。
   a. 同じストレージノードから、オブジェクトファイルの所有権を変更して StorageGRID で管理できるようにします。入力するコマンド `chown ldr-user:bycast 'file_path_of_object'`
   b. Telnet で localhost 1402 に接続して、 LDR コンソールにアクセスします。入力するコマンド `telnet 0 1402`
   c. 入力するコマンド `cd /proc/STOR`
   d. 入力するコマンド `Object_Found 'file_path_of_object'`

      たとえば、次のように入力します。

      ```
      Object_Found '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'
      ```

      を発行します `Object\_Found` コマンドは、グリッドにオブジェクトの場所を通知します。また、アクティブな ILM ポリシーがトリガーされ、ポリシーの指定に従って追加のコピーが作成されます。

      - 注：オブジェクトが見つかったストレージノードがオフラインの場合は、オンラインの任意のストレージノードにオブジェクトをコピーできます。オンラインのストレージノードの /var/local/rangedb ディレクトリにオブジェクトを配置します。次に、問題 を実行します `Object\_Found` コマンドを使用し、オブジェクトへのファイルパスを指定します。
        - オブジェクトをリストアできない場合は、を参照してください `Object\_Found` コマンドが失敗します。テクニカルサポートにお問い合わせください。
        - オブジェクトが StorageGRID に正常にリストアされた場合は、成功を伝えるメッセージが表示されます。例：

          ```
          ade 12448208: /proc/STOR > Object_Found
          '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'

          ade 12448208: /proc/STOR > Object found succeeded.
          First packet of file was valid. Extracted key: 38186FE53E3C49A5
          Renamed '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6' to
          '/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila#3udu'
          ```

          手順に進みます 新しい場所が作成されたことを確認します

1. オブジェクトがStorageGRID に正常にリストアされた場合は、新しい場所が作成されていることを確認します。
   a. 入力するコマンド `cd /proc/OBRP`

b. 入力するコマンド `ObjectByUUID UUID_value`

次の例は、 UUID 926026C4-00A4-449B-AC72-BCCA72DD1311 のオブジェクトに 2 つの場所があることを示しています。

```
ade 12448208: /proc/OBRP > ObjectByUUID 926026C4-00A4-449B-AC72-
BCCA72DD1311

{
    "TYPE(Object Type)": "Data object",
    "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
    "NAME": "cats",
    "CBID": "0x38186FE53E3C49A5",
    "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-ACBB00BB82DD",
    "PPTH(Parent path)": "source",
    "META": {
        "BASE(Protocol metadata)": {
            "PAWS(S3 protocol version)": "2",
            "ACCT(S3 account ID)": "44084621669730638018",
            "*ctp(HTTP content MIME type)": "binary/octet-stream"
        },
        "BYCB(System metadata)": {
            "CSIZ(Plaintext object size)": "5242880",
            "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
            "BSIZ(Content block size)": "5252084",
            "CVER(Content block version)": "196612",
            "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
            "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
            "ITME": "1581534970983000"
        },
        "CMSM": {
            "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
        },
        "AWS3": {
            "LOCC": "us-east-1"
        }
    },
    "CLCO\(Locations\)": \[
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12448208",
            "VOLI\(Volume ID\)": "3222345473",
```

```
            "Object File Path":
"/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila\#3udu",
            "LTIM\(Location timestamp\)": "2020-02-12T19:36:17.880569"
        \},
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12288733",
            "VOLI\(Volume ID\)": "3222345984",
            "Object File Path":
"/var/local/rangedb/0/p/19/11/00rH0%DkRt78Rrb\#3s;L",
            "LTIM\(Location timestamp\)": "2020-02-12T19:36:17.934425"
        }
    ]
}
```

a. LDR コンソールからサインアウトします。入力するコマンド `exit`

2. 管理ノードから、監査ログを検索してこのオブジェクトを ORLM 監査メッセージで探し、必要に応じて情報ライフサイクル管理（ ILM ）によってコピーが配置されていることを確認します。

a. グリッドノードにログインします。

i. 次のコマンドを入力します。 `ssh admin@grid_node_IP`

ii. に記載されているパスワードを入力します `Passwords.txt` ファイル。

iii. 次のコマンドを入力してrootに切り替えます。 `su -`

iv. に記載されているパスワードを入力します `Passwords.txt` ファイル。rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

b. 監査ログが格納されているディレクトリに移動します。 `cd /var/local/audit/export/`

c. grep を使用して、オブジェクトに関連付けられている監査メッセージを出力ファイルに抽出します。入力するコマンド `grep uuid-valueaudit_file_name > output_file_name`

例：

```
Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
messages_about_restored_object.txt
```

d. grep を使用して、この出力ファイルから Object Rules Met （ ORLM ）監査メッセージを抽出します。入力するコマンド `grep ORLM output_file_name`

例：

```
Admin: # grep ORLM messages_about_restored_object.txt
```

以下は、 ORLM 監査メッセージの例です。

```
[AUDT:[CBID(UI64):0x38186FE53E3C49A5][RULE(CSTR):"Make 2 Copies"]
[STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"926026C4-00A4-449B-AC72-
BCCA72DD1311"]
[LOCS(CSTR):"**CLDI 12828634 2148730112**, CLDI 12745543 2147552014"]
[RSLT(FC32):SUCS][AVER(UI32):10][ATYP(FC32):ORLM][ATIM(UI64):15633982306
69]
[ATID(UI64):15494889725796157557][ANID(UI32):13100453][AMID(FC32):BCMS]]
```

a. 監査メッセージで LOCS フィールドを検索します。

   このフィールドの CLDI の値は、オブジェクトコピーが作成されたノード ID とボリューム ID です。このメッセージは、 ILM が適用され、 2 つのオブジェクトコピーがグリッド内の 2 つの場所に作成されたことを示しています。

b. Grid Manager で損失オブジェクトの数をリセットします。

関連情報

"損失オブジェクトを調査しています"

"オブジェクトデータの場所を確認する"

"損失オブジェクトと欠落オブジェクトのカウントのリセット"

"監査ログを確認します"

損失オブジェクトと欠落オブジェクトのカウントのリセット

## StorageGRID システムを調査し、記録されたすべての損失オブジェクトが完全に失われていること、または誤ったアラームであることを確認できたら、 Lost Objects 属性の値を 0 にリセットできます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

Lost Objects カウンタは次のどちらかのページからリセットできます。

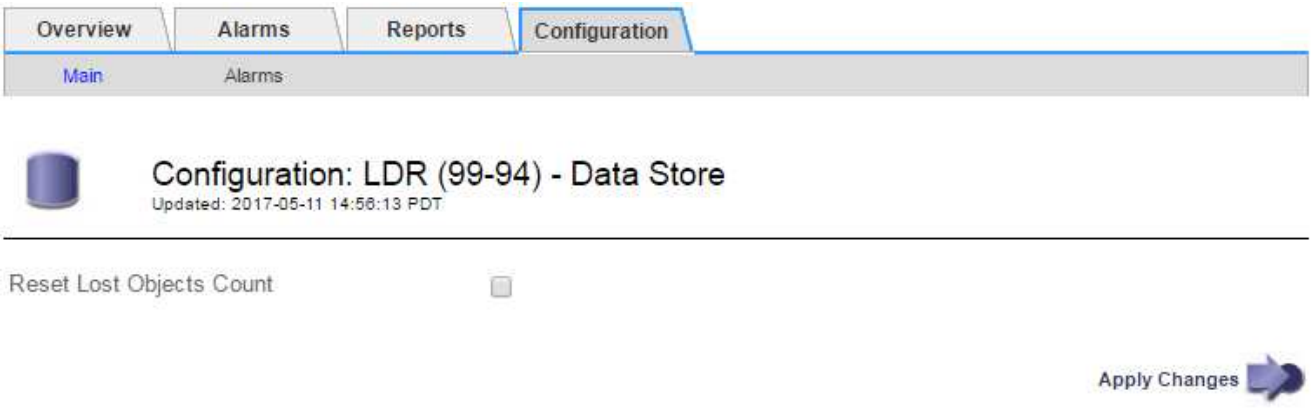
- サポート>*ツール*>*グリッドトポロジ*>**site* >ストレージ・ノード*>* LDR **>***データ・ストア>*概要*>* Main *
- サポート>*ツール*>*グリッド・トポロジ*>**site* >ストレージ・ノード*>* DDS **>***データ・ストア>*概要*>* Main *

これらの手順は、 **ldr**>*Data Store* ページからカウンタをリセットする方法を示しています。

手順

1. Support **>** Tools **>** Grid Topology *を選択します。

2. 警告またはLOSTアラームが発生しているストレージノードについて、「**_ Site > Storage Node_**>* LDR **>** Data Store **>** Configuration *」を選択します。
3. 「 * Lost Objects Count * をリセット」を選択します。




4. [ 変更の適用 *] をクリックします。

   Lost Objects 属性が 0 にリセットされ、 * Objects lost * アラートと LOST アラームが解除されます。これには数分かかることがあります。

5. 必要に応じて、損失オブジェクトを特定するプロセスで増分された可能性がある、その他の関連属性の値をリセットできます。

   a. [***Site]>[Storage Node***]>[* ldr*]>[イレイジャーコーディング]>[設定]を選択します。
   b. 「 Reset Reads Failure Count 」と「 Reset Corrupt Copies Detected Count 」を選択します。
   c. [ 変更の適用 *] をクリックします。
   d. [***site]>[Storage Node***]>[* ldr*]>[* Verification]**>[** Configuration]*を選択します。
   e. 「 Reset Missing Objects Count 」（不足オブジェクト数のリセット）および「 Reset Corrupt Objects Count 」（破損オブジェクト数のリセット）を選択します
   f. 隔離されたオブジェクトが不要であることが確実な場合は、 [ * 隔離されたオブジェクトの削除 * ] を選択します。

      隔離されたオブジェクトは、バックグラウンド検証で破損したレプリケートオブジェクトコピーが確認されると作成されます。ほとんどの場合、 StorageGRID は破損したオブジェクトを自動的に置き換え、隔離されたオブジェクトを削除しても安全です。ただし、 * Objects lost * アラートがトリガーされた場合や、 LOST アラームがトリガーされた場合は、テクニカルサポートが隔離されたオブジェクトにアクセスすることを推奨します。

   g. [ 変更の適用 *] をクリックします。

   [ 変更の適用（ Apply Changes ） ] をクリックした後、属性がリセットされるまでに少し時間がかかる場合があります。

関連情報

"StorageGRID の管理"

# Low object data storage * アラートは、オブジェクトデータを格納可能な各ストレージノードのスペースを監視します。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

Low object data storage *は、ストレージノード上のレプリケートオブジェクトデータおよびイレイジャーコーディングオブジェクトデータの合計容量が、アラートルールで設定されている条件のいずれかを満たした場合にトリガーされます。

デフォルトでは、次の条件が true と評価されると、 Major アラートがトリガーされます。

```
(storagegrid_storage_utilization_data_bytes/
(storagegrid_storage_utilization_data_bytes +
storagegrid_storage_utilization_usable_space_bytes)) >=0.90
```

この条件では、次のように

- `storagegrid_storage_utilization_data_bytes` は、ストレージノードのレプリケートオブジェクトデータとイレイジャーコーディングオブジェクトデータの推定合計サイズです。
- `storagegrid_storage_utilization_usable_space_bytes` は、ストレージノードに残っているオブジェクトストレージスペースの総容量です。

Major または Minor * Low object data storage * アラートがトリガーされた場合は、できるだけ早く拡張手順を実行する必要があります。

手順

1. [* Alerts*>*current*]を選択します。

   [Alerts] ページが表示されます。

2. アラートの表で、必要に応じて「 * Low object data storage * 」アラートグループを展開し、表示するアラートを選択します。

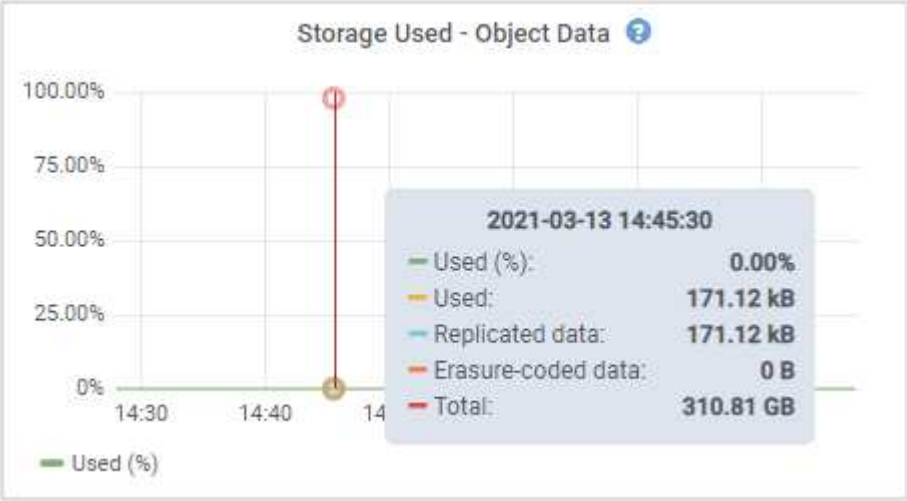
   アラートグループの見出しではなく、アラートを選択します。

3. ダイアログボックスで詳細を確認し、次の点に注意してください。
   - トリガーされた時刻
   - サイトとノードの名前
   - このアラートに関する指標の現在の値
4. ノード*>*ストレージノードまたはサイト*>*ストレージ*を選択します。

5. Storage Used - Object Data グラフにカーソルを合わせます。

   次の値が表示されます。

   - * Used （ % ） * ：オブジェクトデータに使用されている合計使用可能スペースの割合。
   - * Used * ：オブジェクトデータに使用されている合計使用可能スペースの量。
   - * Replicated data * ：このノード、サイト、またはグリッド上のレプリケートオブジェクトデータの推定量。
   - * イレイジャーコーディングデータ * ：このノード、サイト、またはグリッドにあるイレイジャーコーディングオブジェクトデータの推定量。
   - * Total * ：このノード、サイト、またはグリッドで使用可能なスペースの総容量。使用済みの値はです `storagegrid_storage_utilization_data_bytes` メートル法。




6. グラフ上部の時間コントロールを選択して、期間を変えながらストレージの使用状況を確認します。

   ストレージの使用状況の推移を確認することで、アラートがトリガーされた前後のストレージの使用量がわかり、ノードの残りのスペースがいっぱいになるまでの時間を予測できます。

7. できるだけ早く拡張手順 を実行してストレージ容量を追加します。

   既存のストレージノードにストレージボリューム（ LUN ）を追加するか、または新しいストレージノードを追加することができます。

   ストレージノードがいっぱいになったときの対応については、 StorageGRID の管理手順を参照してください。

関連情報

"Storage Status（SSTS）アラームのトラブルシューティングを行います"

"グリッドを展開します"

"StorageGRID の管理"

**Storage Status（SSTS）アラームのトラブルシューティングを行います**

# Storage Status （ SSTS ）アラームは、ストレージノードにオブジェクトストレージ用の十分な空きスペースが残っていない場合にトリガーされます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

ストレージノード内のすべてのボリュームの空きスペース量がStorage Volume Soft Read Only Watermark（* Configuration **>** Storage Options **>** Overview *）の値を下回ると、SSTS（Storage Status）アラームがNoticeレベルでトリガーされます。

Storage Options Overview

Updated: 2019-10-09 13:09:30 MDT

**Object Segmentation**

| Description | Settings |
|---|---|
| Segmentation | Enabled |
| Maximum Segment Size | 1 GB |

**Storage Watermarks**

| Description | Settings |
|---|---|
| Storage Volume Read-Write Watermark | 30 GB |
| Storage Volume Soft Read-Only Watermark | 10 GB |
| Storage Volume Hard Read-Only Watermark | 5 GB |
| Metadata Reserved Space | 3,000 GB |

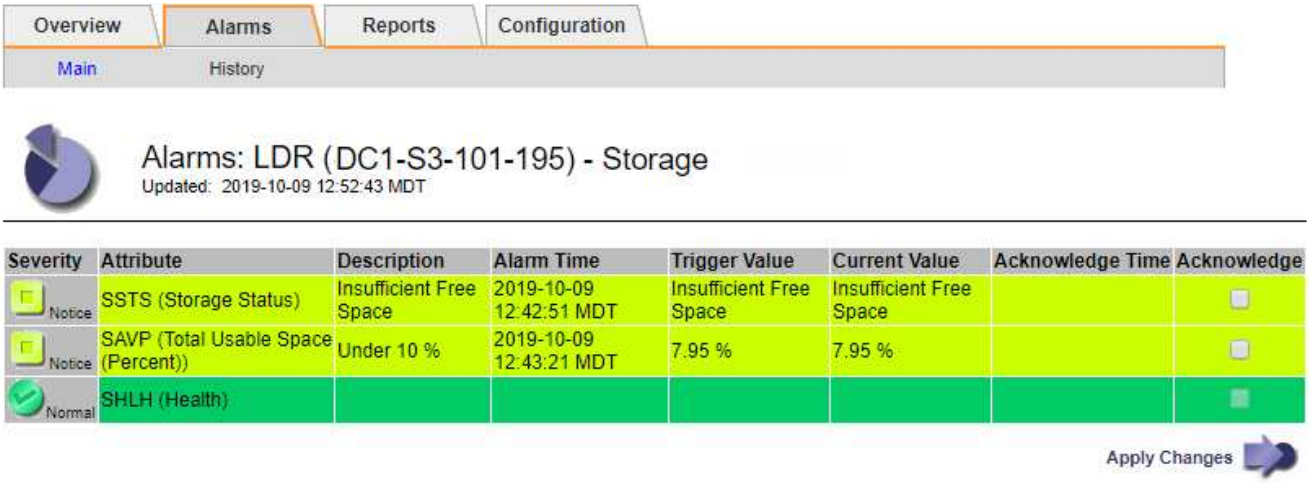
たとえば、 Storage Volume Soft Read-Only Watermark がデフォルト値の 10GB に設定されているとします。ストレージノード内の各ストレージボリュームに残っている使用可能スペースが 10GB 未満になると、 SSTS アラームがトリガーされます。いずれかのボリュームに 10GB 以上の空き容量があれば、アラームはトリガーされません。

SSTS アラームがトリガーされた場合は、次の手順を実行して問題 を詳しく把握する必要があります。

手順

1. [**Support**>]>[* Alarms (legac)**>]>[** Current Alarms]を選択します。
2. Service 列で、 SSTS アラームに関連付けられているデータセンター、ノード、およびサービスを選択します。

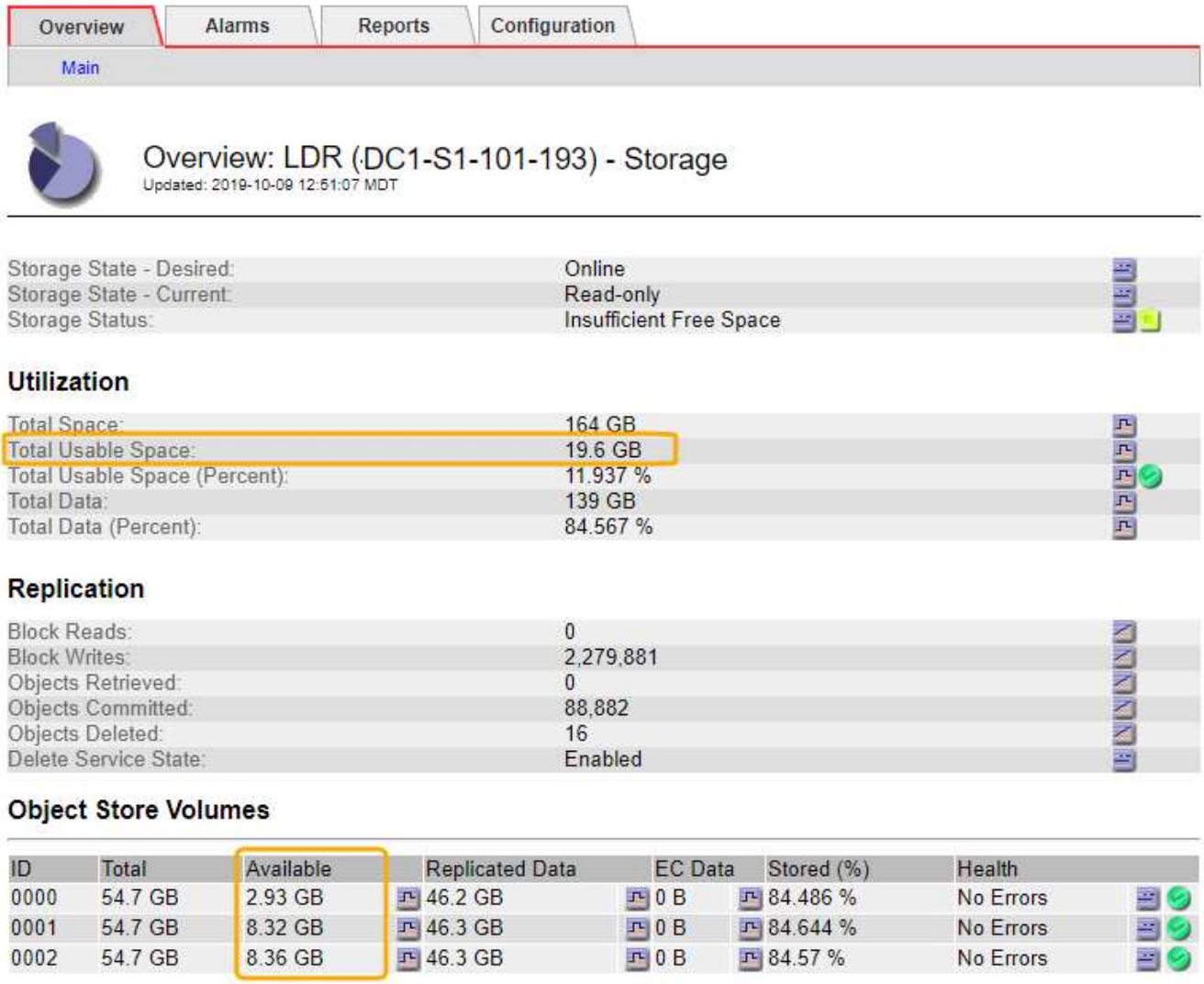
   Grid Topology ページが表示されます。Alarms タブには、選択したノードおよびサービスのアクティブなアラームが表示されます。




この例では、 SSTS （ Storage Status ）アラームと SAVP （ Total Usable Space （ Percent ））アラームの両方が Notice レベルでトリガーされています。

> 通常は、 SSTS アラームと SAVP アラームの両方がほぼ同時にトリガーされます。ただし、両方のアラームがどちらトリガーされるかはウォーターマークの設定（ GB ）と SAVP アラームの設定で決まります。

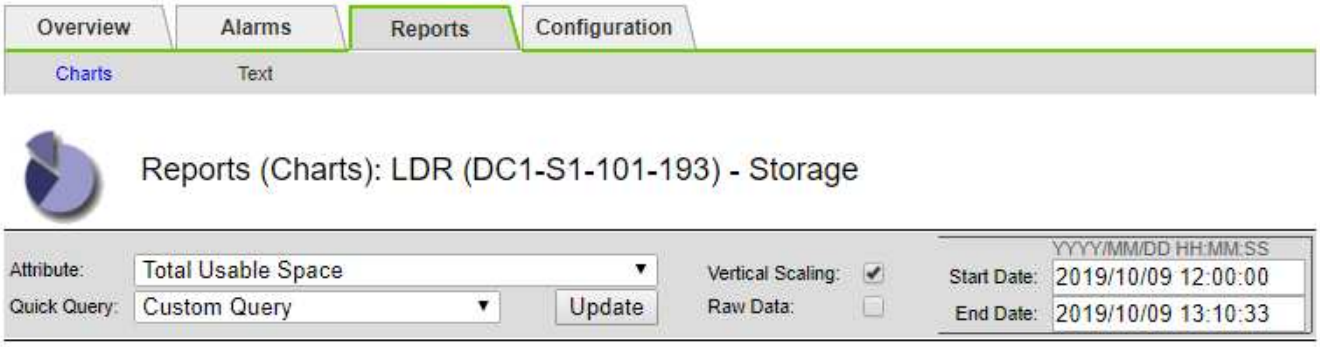
3. 実際に使用可能なスペース量を確認するには、 **ldr**>*Storage*>*Overview* を選択し、 Total Usable Space （ STAS ）属性を検索します。

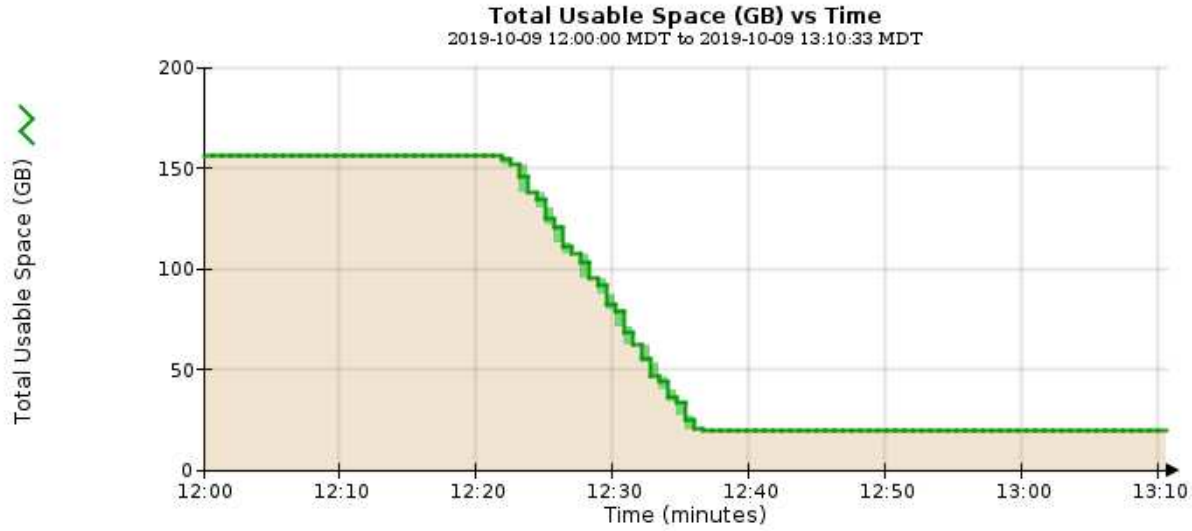



この例のストレージノードでは、 164GB 中 19.6GB しか使用可能なスペースが残っていません。合計は 3 つのオブジェクトストアボリュームの「使用可能な」 * 値の合計です。3 つのストレージボリュームのそれぞれに 10GB 未満の空きスペースがあったため、 SSTS アラームがトリガーされました。

4. 一定期間にわたるストレージの使用状況を確認するには、 * Reports * タブを選択し、過去数時間の Total Usable Space のプロットを使用します。

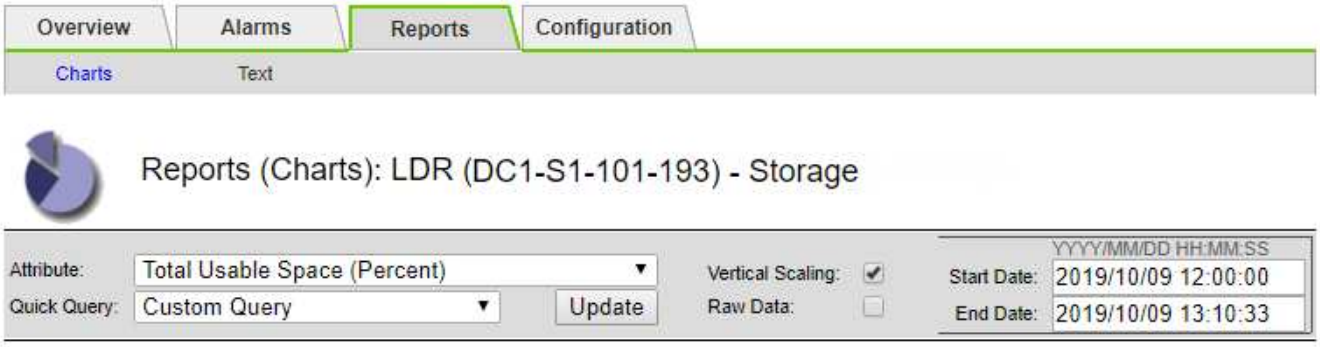
   この例では、 12 ： 00 の時点の使用可能な合計スペースは約 155 GB でしたが、 12 ： 35 には 20 GB まで減り、その時点で SSTS アラームがトリガーされています。

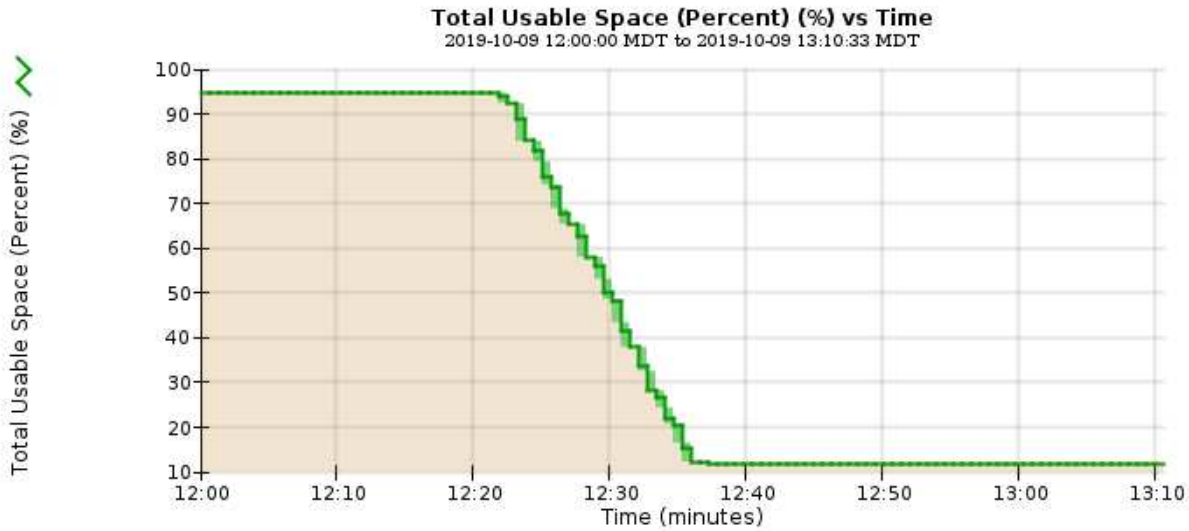



5. 合計容量の割合としてストレージがどのように使用されているかを確認するには、過去数時間の合計使用可能スペース（割合）をプロットします。

   この例では、ほぼ同じタイミングで使用可能な合計スペースが 95% から 10% 強に減少しています。




6. 必要に応じて、StorageGRID システムを拡張してストレージ容量を追加します。

   ストレージノードがいっぱいになったときの管理手順については、StorageGRID の管理手順を参照してください。

関連情報

"グリッドを展開します"

"StorageGRID の管理"

プラットフォームサービスメッセージの配信のトラブルシューティング（**SMTT**アラーム）

## データを受信できないデスティネーションにプラットフォームサービスメッセージが配信された場合、 Grid Manager で Total Events （ SMTT ）アラームがトリガーされます。

このタスクについて

たとえば S3 マルチパートアップロードは、関連するレプリケーションまたは通知メッセージを設定済みのエンドポイントに配信できなくても成功します。または、 CloudMirror レプリケーションのメッセージはメタデータが長すぎると配信できません。

SMTTアラームには、 `Failed to publish notifications for bucket-name object key` 通知が失敗した最後のオブジェクト

追加情報 プラットフォームサービスのトラブルシューティングについては、 StorageGRID の管理手順を参照してください。プラットフォームサービスエラーをデバッグするために、Tenant Managerからテナントへのアクセスが必要になる場合があります。

手順

1. アラームを表示するには、* Nodes **>*site *>* grid node_name *>** Events *を選択します。
2. 表の一番上に Last Event が表示されます。

   イベントメッセージは、にも表示されます `/var/local/log/bycast-err.log`。

3. SMTT アラームに記載されている指示に従って問題 を修正します。
4. [イベントカウントのリセット]をクリックします。
5. プラットフォームサービスメッセージが配信されていないオブジェクトについてテナントに通知します。
6. テナントで、オブジェクトのメタデータまたはタグを更新することで、失敗したレプリケーションまたは通知をトリガーするよう指定します。

関連情報

"StorageGRID の管理"

"テナントアカウントを使用する"

"ログファイル参照"

"イベント数のリセット"

# メタデータに関する問題のトラブルシューティング

メタデータの問題の原因を特定するのに役立ついくつかのタスクを実行できます。

## **Low metadata storage**アラートのトラブルシューティング

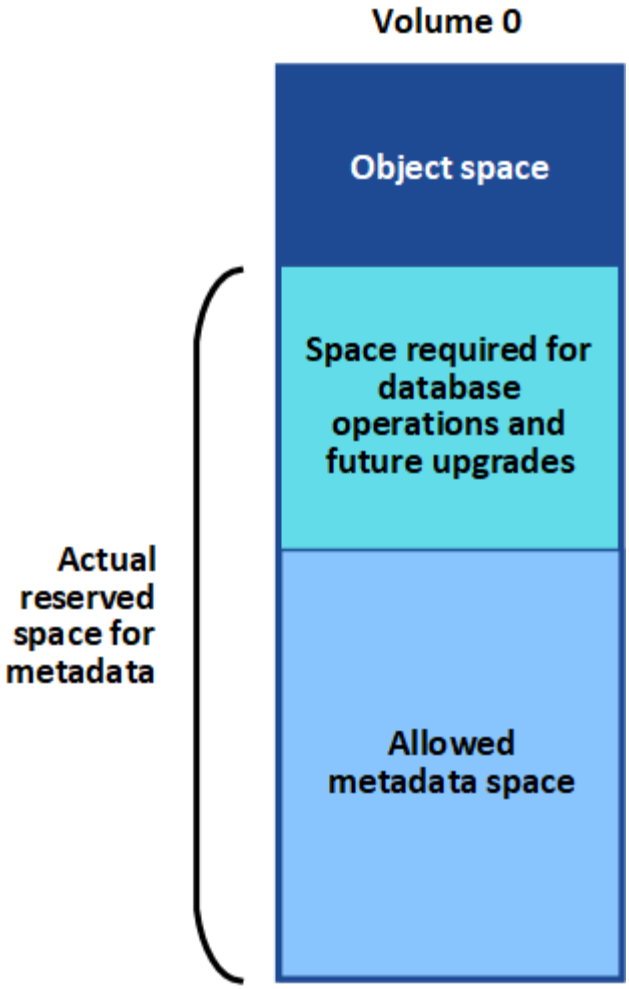
Low metadata storage * アラートがトリガーされた場合は、新しいストレージノードを追加する必要があります。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

このタスクについて

StorageGRID は、各ストレージノードのボリューム 0 上にオブジェクトメタデータ用に一定量のスペースをリザーブします。このスペースは、実際のリザーブスペースと呼ばれ、オブジェクトメタデータに使用できるスペース（許容されるメタデータスペース）と、コンパクションや修復などの重要なデータベース処理に必要なスペースに分割されます。許可されるメタデータスペースは、オブジェクトの全体的な容量を決定します。




オブジェクトメタデータがメタデータに使用できるスペースの使用量の 100% を超えると、データベース処理を効率的に実行できず、エラーが発生します。

StorageGRID は、次の Prometheus 指標を使用して、許可されているメタデータスペースの使用状況を測定します。

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utiliza
tion_metadata_allowed_bytes
```

この Prometheus 式が特定のしきい値に達すると、 * Low metadata storage * アラートがトリガーされます。

- * Minor * ：オブジェクトメタデータが、許可されているメタデータスペースの 70% 以上を使用しています。できるだけ早く新しいストレージノードを追加する必要があります。
- * Major * ：オブジェクトメタデータが使用しているメタデータスペースが 90% 以上あります。すぐに新しいストレージノードを追加する必要があります。

> オブジェクトメタデータが使用可能なメタデータスペースの 90% 以上を使用している場合、ダッシュボードに警告が表示されます。この警告が表示された場合は、すぐに新しいストレージノードを追加する必要があります。オブジェクトメタデータの使用量は、使用できるスペースの 100% を超えないようにする必要があります。

- * クリティカル * ：オブジェクトメタデータが使用可能なメタデータスペースの 100% 以上を使用しており、重要なデータベース処理に必要なスペースを使い始めています。新しいオブジェクトの取り込みを停止し、すぐに新しいストレージノードを追加する必要があります。

次の例では、オブジェクトメタデータが使用しているメタデータスペースが 100% を超えています。これは重大な状況であり、データベース処理の効率低下とエラーの発生につながります。

The following Storage Nodes are using more than 90% of the space allowed for object metadata:

| Node | % Used | Used | Allowed |
|---|---|---|---|
| DC1-S2-227 | 104.51% | 6.73 GB | 6.44 GB |
| DC1-S3-228 | 104.36% | 6.72 GB | 6.44 GB |
| DC2-S2-233 | 104.20% | 6.71 GB | 6.44 GB |
| DC1-S1-226 | 104.20% | 6.71 GB | 6.44 GB |
| DC2-S3-234 | 103.43% | 6.66 GB | 6.44 GB |

Undesirable results can occur if object metadata uses more than 100% of the allowed space. You must add new Storage Nodes immediately or contact support.

ボリューム 0 のサイズが Metadata Reserved Space ストレージオプションより小さい場合（非本番環境など）は、「 Low metadata storage * 」アラートが正確に計算されないことがあります。

手順

1. [* Alerts*>*current*]を選択します。
2. アラートの表で、必要に応じて「 * Low metadata storage * 」アラートグループを展開し、表示する特定のアラートを選択します。
3. アラートダイアログボックスで詳細を確認します。
4. Major または Critical の * Low metadata storage * アラートがトリガーされた場合は、すぐに拡張を実行してストレージノードを追加します。

   StorageGRID は各サイトですべてのオブジェクトメタデータの完全なコピーを保持するため、グリッド全体のメタデータ容量は最も小規模なサイトのメタデータ容量によって制限されます。一方のサイトにメタデータ容量を追加する必要がある場合は、同じ数のストレージノードで他のサイトも拡張してください。

   拡張の実行後、 StorageGRID によって既存のオブジェクトメタデータが新しいノードに再配分され、グリッドの全体的なメタデータ容量が増加します。ユーザによる操作は必要ありません。Low metadata storage * アラートがクリアされます。

関連情報

"各ストレージノードのオブジェクトメタデータ容量を監視します"

"グリッドを展開します"

サービスのトラブルシューティング：**Status - Cassandra（SVST）**アラーム

Services ： Status - Cassandra （ SVST ）アラームは、ストレージノードに対する Cassandra データベースのリビルドが必要となる可能性があることを示します。Cassandra は StorageGRID 用のメタデータストアとして使用されます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- を用意しておく必要があります `Passwords.txt` ファイル。

このタスクについて

Cassandra が停止している（ストレージノードの電源がオフになっているなど）期間が 15 日を超える場合、ノードがオンライン状態に戻っても Cassandra は起動されません。この場合、該当する DDS サービスの Cassandra データベースをリビルドする必要があります。

診断ページを使用すると、グリッドの現在の状態の追加情報 を取得できます。

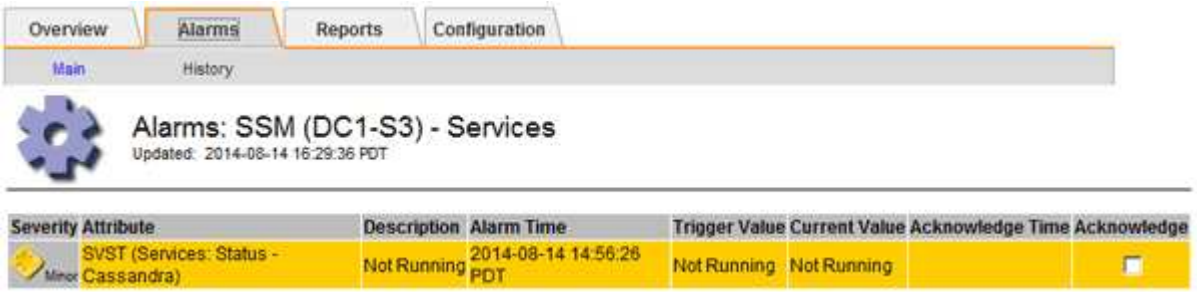
"診断の実行"

停止期間が 15 日を超える Cassandra データベースのサービスが複数ある場合は、この手順は実行せずにテクニカルサポートに連絡してください。

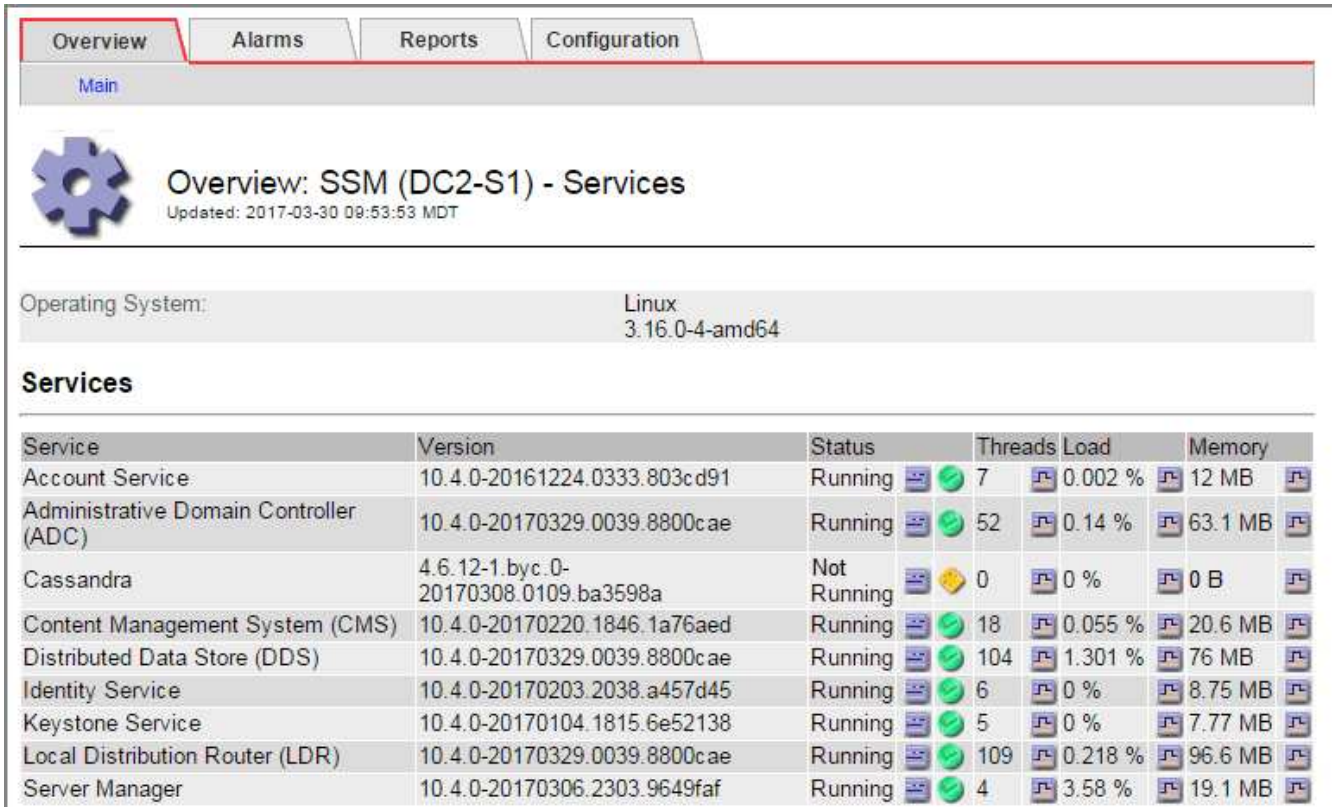
手順

1. Support **>** Tools **>** Grid Topology *を選択します。
2. アラームを表示するには、***site** **>** **Storage Node***>* SSM **>** Services **>** Alarms **>** Main *を選択します。

   この例は、 SVST アラームがトリガーされたことを示しています。




   SSM Services のメインページには、 Cassandra が実行されていないことも表示されます。




1. ストレージノードからCassandraを再起動できるか試します。
   a. グリッドノードにログインします。
      i. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
      ii. に記載されているパスワードを入力します `Passwords.txt` ファイル。
      iii. 次のコマンドを入力してrootに切り替えます。 `su -`
      iv. に記載されているパスワードを入力します `Passwords.txt` ファイル。rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。
   b. 入力するコマンド `/etc/init.d/cassandra status`
   c. Cassandraが実行されていない場合は再起動します。 `/etc/init.d/cassandra restart`
2. Cassandra が再起動されない場合は、 Cassandra が停止していた期間を調べます。Cassandra の停止期間が 15 日を超えている場合、 Cassandra データベースをリビルドする必要があります。

   Cassandra データベースのサービスが複数停止している場合は、この手順は実行せずにテクニカルサポートに連絡してください。

   グラフを作成するか、 servermanager.log ファイルを確認することで、 Cassandra が停止していた期間を調べることができます。

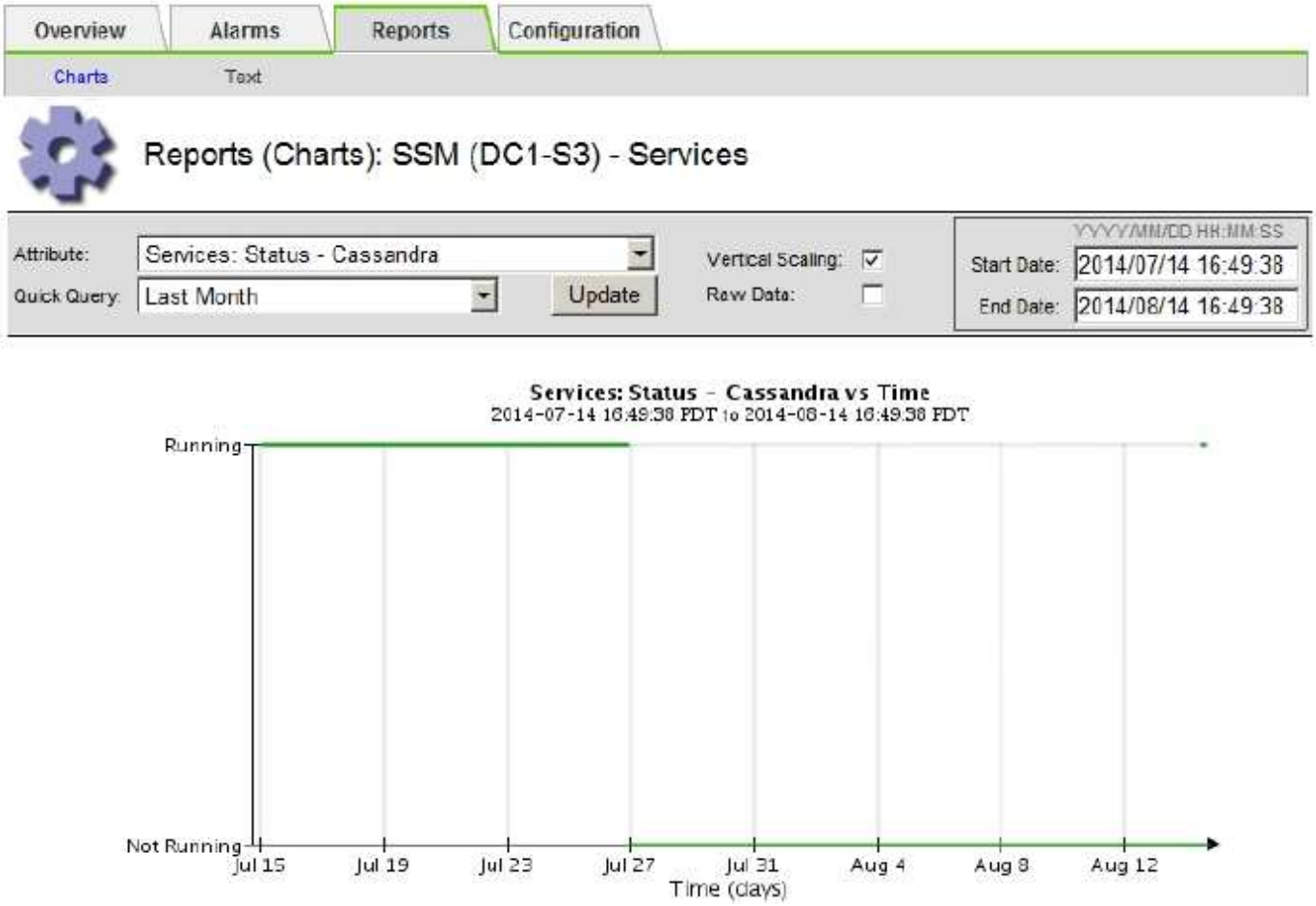
3. Cassandra のグラフを確認する手順は次
   a. Support **>** Tools **>** Grid Topology を選択します。次に、**[*site* > *Storage Node*>*** SSM **>** Services **>** Reports **>** Charts *]を選択します。
   b. 「 * Attribute * > * Service ： Status - Cassandra * 」を選択します。

c. [ 開始日 ] には、現在の日付よりも **16** 日前の日付を入力します。[ 終了日 *] には、現在の日付を入力します。

d. [ 更新（ Update ） ] をクリックします。

e. グラフから Cassandra の停止期間が 15 日を超えていることがわかった場合は、 Cassandra データベースをリビルドします。

次のグラフの例では、 Cassandra が少なくとも 17 日間は停止していることがわかります。




1. ストレージノードで servermanager.log ファイルを確認するには、次の手順を実行します。

a. グリッドノードにログインします。

i. 次のコマンドを入力します。 `ssh admin@grid_node_IP`

ii. に記載されているパスワードを入力します `Passwords.txt` ファイル。

iii. 次のコマンドを入力してrootに切り替えます。 `su -`

iv. に記載されているパスワードを入力します `Passwords.txt` ファイル。rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

b. 入力するコマンド `cat /var/local/log/servermanager.log`

servermanager.log ファイルの内容が表示されます。

Cassandra の停止期間が 15 日を超えている場合、 servermanager.log ファイルに次のメッセージが表

示されます。

```
"2014-08-14 21:01:35 +0000 | cassandra | cassandra not
started because it has been offline for longer than
its 15 day grace period - rebuild cassandra
```

a. このメッセージのタイムスタンプが手順に従って Cassandra の再起動を試行した時間になっていることを確認してください ストレージノードから Cassandra を再起動します。

   Cassandra のエントリは 1 つとは限らないため、最新のエントリを確認する必要があります。

b. Cassandra の停止期間が 15 日を超えている場合、 Cassandra データベースをリビルドする必要があります。

   手順については'リカバリとメンテナンスの手順の15日以上停止している単一のストレージ・ノードからのリカバリを参照してください

c. Cassandra をリビルドしたあともアラームがクリアされない場合は、テクニカルサポートに連絡してください。

関連情報

""

**Cassandra**のメモリ不足エラーのトラブルシューティング（**SMTT**アラーム）

Total Events （ SMTT ）アラームは、 Cassandra データベースでメモリ不足エラーが発生するとトリガーされます。このエラーが発生した場合は、テクニカルサポートに連絡して問題 の処理を依頼してください。

このタスクについて

Cassandra データベースにメモリ不足エラーが発生すると、ヒープダンプが作成され、 Total Events （ SMTT ）アラームがトリガーされて、 Cassandra Heap Out Of Memory Errors のカウントが 1 つ増えます。

手順

1. イベントを表示するには、* Nodes **>*_grid node_name >** Events *を選択します。
2. Cassandra Heap Out Of Memory Errors のカウントが 1 以上であることを確認します。

   診断ページを使用すると、グリッドの現在の状態の追加情報 を取得できます。

   "診断の実行"

3. に進みます `/var/local/core/`を圧縮します `Cassandra.hprof` ファイルを保存してテクニカルサポートに送信します。
4. のバックアップを作成します `Cassandra.hprof` ファイルを選択し、から削除します `/var/local/core/ directory`。

   このファイルは 24GB もの大きさになることがあるため、削除してスペースを解放してください。

5. 問題 が解決したら、*イベントカウントのリセット*をクリックします。

イベント数をリセットするには、 Grid Topology Page Configuration 権限が必要です。

関連情報

"イベント数のリセット"

# 証明書エラーのトラブルシューティング

## Web ブラウザ、 S3 または Swift クライアント、または外部の監視ツールを使用して StorageGRID に接続しようとしたときに、セキュリティまたは証明書の問題 が表示される場合は、証明書を確認してください。

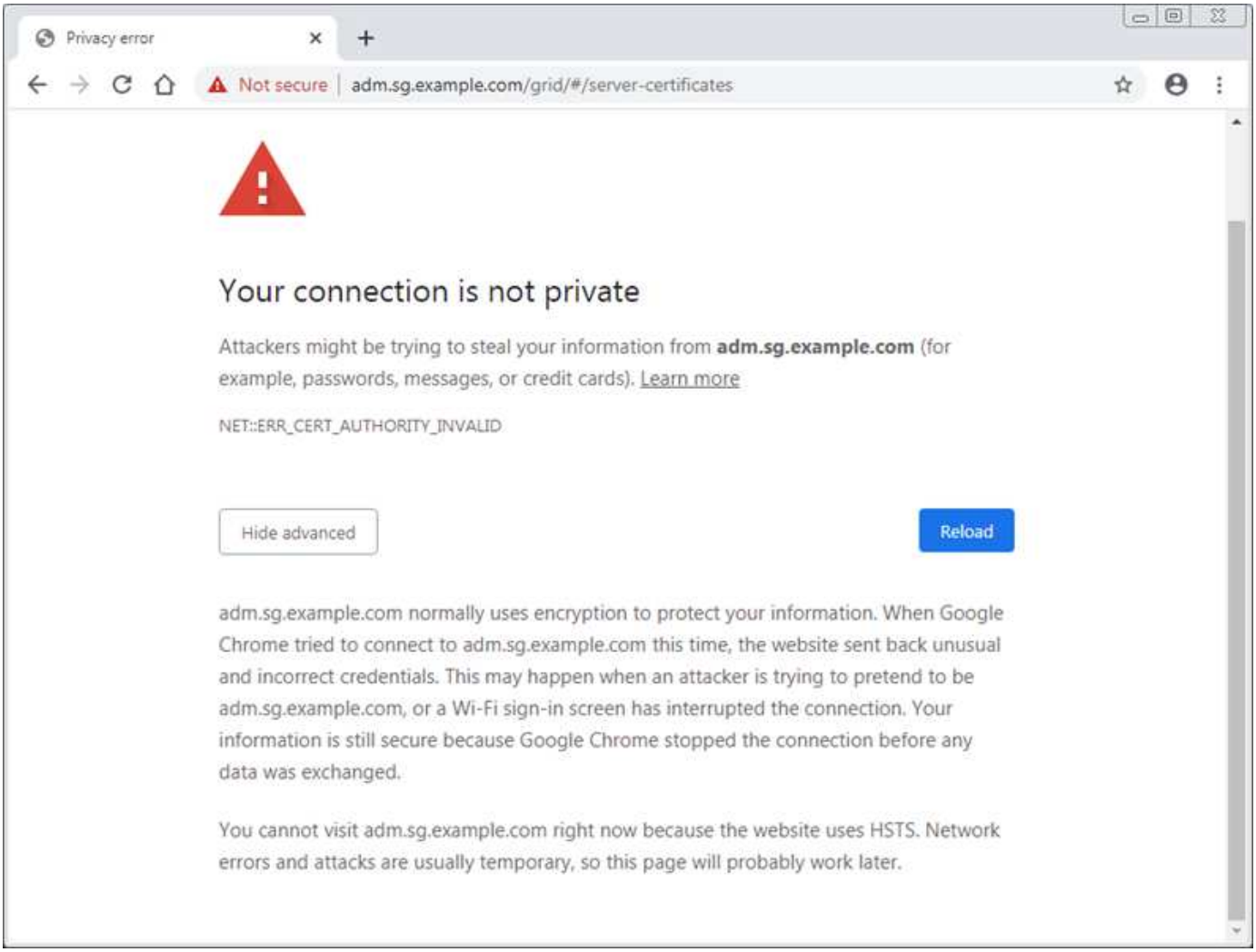
このタスクについて

証明書エラーは、グリッドマネージャ、グリッド管理 API 、テナントマネージャ、またはテナント管理 API を使用して StorageGRID に接続しようとしたときに、原因 で発生する可能性があります。証明書のエラーは、 S3 / Swift クライアントまたは外部の監視ツールを使用して接続しようとした場合にも発生します。

IP アドレスではなくドメイン名を使用して Grid Manager または Tenant Manager にアクセスする場合は、次のいずれかの場合に証明書のエラーが表示され、バイパスするオプションはありません。

- カスタム管理インターフェイスサーバ証明書の有効期限が切れます。
- カスタムの管理インターフェイスサーバ証明書をデフォルトのサーバ証明書に戻した場合。

次の例は、カスタム管理インターフェイスサーバ証明書の期限が切れたときの証明書エラーを示しています。




サーバ証明書の問題によって処理が中断されないようにするために、サーバ証明書の有効期限が近づくと、「Expiration of server certificate for Management Interface * 」アラートがトリガーされます。

外部Prometheus統合にクライアント証明書を使用している場合、証明書のエラーは、StorageGRID 管理インターフェイスのサーバ証明書またはクライアント証明書が原因で発生することがあります。クライアント証明書の有効期限が近づくと、クライアント証明書ページで設定された証明書の有効期限*アラートがトリガーされます。

手順

1. 期限切れの証明書に関するアラート通知を受け取った場合は、証明書の詳細にアクセスします。
   - サーバ証明書の場合は、* Configuration > Network Settings > Server Certificates *を選択します。
   - クライアント証明書の場合は、* Configuration > Access Control > Client Certificates *を選択します。
2. 証明書の有効期間を確認します。

   一部のWebブラウザおよびS3 / Swiftクライアントでは、有効期間が398日を超える証明書は受け入れられません。

3. 証明書の有効期限が切れているか、まもなく期限切れになる場合は、新しい証明書をアップロードまたは生成します。
   - サーバ証明書については、StorageGRID の管理手順のグリッドマネージャとテナントマネージャのカ

スタムサーバ証明書を設定する手順を参照してください。

- クライアント証明書については、StorageGRID の管理手順のクライアント証明書の設定手順を参照してください。

4. サーバ証明書エラーの場合は、次のいずれかまたは両方を実行してください。
   - 証明書の Subject Alternative Name （ SAN ）が設定されていること、および SAN が接続先のノードの IP アドレスまたはホスト名と一致していることを確認してください。
   - ドメイン名を使用して StorageGRID に接続しようとしている場合は、次の手順を実行します。
     i. 接続エラーをバイパスして Grid Manager にアクセスするために、ドメイン名ではなく管理ノードの IP アドレスを入力します。
     ii. Grid Managerから* Configuration > Network Settings > Server Certificates *を選択して新しいカスタム証明書をインストールするか、デフォルトのまま続行します。
     iii. StorageGRID の管理手順で、Grid Managerおよびテナントマネージャ用のカスタムサーバ証明書を設定する手順を参照してください。

関連情報

"StorageGRID の管理"

# 管理ノードとユーザインターフェイスの問題のトラブルシューティング

## ここでは、管理ノードと StorageGRID ユーザインターフェイスに関連する問題の原因を特定するのに役立ついくつかのタスクを紹介します。

### サインオンエラーのトラブルシューティング

StorageGRID 管理ノードへのサインインでエラーが発生した場合は、システムの問題 にアイデンティティフェデレーションの設定、ネットワークまたはハードウェア、管理ノードサービスを含む問題 、接続されているストレージノード上の Cassandra データベースを含む問題 がある可能性があります。

必要なもの

- を用意しておく必要があります `Passwords.txt` ファイル。
- 特定のアクセス権限が必要です。

このタスクについて

管理ノードにサインインしようとしたときに次のいずれかのエラーメッセージが表示された場合は、以下のトラブルシューティングのガイドラインに従ってください。

- `Your credentials for this account were invalid. Please try again.`
- `Waiting for services to start…`
- `Internal server error. The server encountered an error and could not complete your request. Please try again. If the problem persists, contact Technical Support.`
- `Unable to communicate with server. Reloading page…`

手順

1. 10 分待ってから、もう一度サインインしてください。

エラーが自動的に解決されない場合は、次の手順に進みます。

2. StorageGRID システムに複数の管理ノードがある場合は、別の管理ノードからグリッドマネージャにサインインしてみます。
   - サインインできる場合は、* Dashboard 、 Nodes 、 Alerts 、 Support *の各オプションを使用して、エラーの原因 を特定できます。
   - 管理ノードが 1 つしかない場合またはサインインできない場合は、次の手順に進みます。
3. ノードのハードウェアがオフラインかどうかを確認します。
4. StorageGRID システムでシングルサインオン（ SSO ）が有効になっている場合は、 StorageGRID の管理手順のシングルサインオンの設定を参照してください。

   問題を解決するには、 1 つの管理ノードの SSO を一時的に無効にしてから再度有効にする必要があります。

   > SSO が有効になっている場合は、制限されたポートを使用してサインオンできません。ポート 443 を使用する必要があります。

5. 使用しているアカウントがフェデレーテッドユーザに属しているかどうかを確認します。

   フェデレーテッドユーザアカウントが機能していない場合は、 root などのローカルユーザとして Grid Manager にサインインしてみてください。

   - ローカルユーザがサインインできる場合は、次の手順を実行します。
     i. 表示されているアラームを確認します。
     ii. [設定>*アイデンティティフェデレーション*]を選択します。
     iii. [ 接続のテスト * ] をクリックして、 LDAP サーバーの接続設定を確認します。
     iv. テストに失敗した場合は、設定エラーを解決します。
   - ローカルユーザがサインインできず、クレデンシャルが正しい場合は、次の手順に進みます。
6. Secure Shell （ SSH ）を使用して管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@Admin_Node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

   rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

7. グリッドノード上で実行されているすべてのサービスのステータスを表示します。 `storagegrid-status`

   NMS 、 mi 、 nginx 、 mgmt の各 API サービスがすべて実行されていることを確認します。

   出力は、サービスのステータスが変わるとすぐに更新されます。

```
$ storagegrid-status
Host Name                      99-211
IP Address                     10.96.99.211
Operating System Kernel        4.19.0          Verified
Operating System Environment   Debian 10.1     Verified
StorageGRID Webscale Release   11.4.0          Verified
Networking                                     Verified
Storage Subsystem                              Verified
Database Engine                5.5.9999+default Running
Network Monitoring             11.4.0          Running
Time Synchronization           1:4.2.8p10+dfsg Running
ams                            11.4.0          Running
cmn                            11.4.0          Running
nms                            11.4.0          Running
ssm                            11.4.0          Running
mi                             11.4.0          Running
dynip                          11.4.0          Running
nginx                          1.10.3          Running
tomcat                         9.0.27          Running
grafana                        6.4.3           Running
mgmt api                       11.4.0          Running
prometheus                     11.4.0          Running
persistence                    11.4.0          Running
ade exporter                   11.4.0          Running
alertmanager                   11.4.0          Running
attrDownPurge                  11.4.0          Running
attrDownSamp1                  11.4.0          Running
attrDownSamp2                  11.4.0          Running
node exporter                  0.17.0+ds       Running
sg snmp agent                  11.4.0          Running
```

8. Apache Webサーバが実行されていることを確認します。 `# service apache2 status`

1. Lumberjackを使用してログを収集します。 `# /usr/local/sbin/lumberjack.rb`

   過去に認証に失敗したことがある場合は、 --start および --end Lumberjack スクリプトオプションを使用して適切な期間を指定します。これらのオプションの詳細については、 lumberjack -h を使用してください。

   ログアーカイブがコピーされた場所がターミナル画面に出力されます。

1. 次のログを確認します。

   - `/var/local/log/bycast.log`
   - `/var/local/log/bycast-err.log`
   - `/var/local/log/nms.log`

◦ `**/*commands.txt`

2. 管理ノードで問題を特定できなかった場合は、次のいずれかのコマンドを問題 で実行し、サイトで ADC サービスを実行する 3 つのストレージノードの IP アドレスを確認します。通常はサイトにインストールされた最初の 3 つのストレージノードです。

```
# cat /etc/hosts
```

```
# vi /var/local/gpt-data/specs/grid.xml
```

管理ノードは認証プロセスで ADC サービスを使用します。

3. 特定した IP アドレスを使用して、管理ノードから各 ADC ストレージノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

   rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

4. グリッドノード上で実行されているすべてのサービスのステータスを表示します。 `storagegrid-status`

   idnt 、 acct 、 nginx 、および Cassandra のサービスがすべて実行されていることを確認します。

5. 手順を繰り返します Lumberjack を使用してログを収集します および ログを確認します をクリックしてストレージノード上のログを確認します。
6. 問題を解決できない場合は、テクニカルサポートにお問い合わせください。

   収集したログをテクニカルサポートに送信します。

関連情報

"StorageGRID の管理"

"ログファイル参照"

ユーザインターフェイスの問題のトラブルシューティング

StorageGRID ソフトウェアを新しいバージョンにアップグレードしたあとに、 Grid Manager またはテナントマネージャで問題が発生することがある。

**Web** インターフェイスが想定どおりに応答しません

StorageGRID ソフトウェアのアップグレード後に Grid Manager またはテナントマネージャが想定どおりに応答しない場合がある。

Web インターフェイスで問題が発生した場合：

- サポートされているブラウザを使用していることを確認します。

  StorageGRID 11.5 でサポートされるブラウザが変更になりました。サポート対象のバージョンを使用していることを確認してください。

- Web ブラウザのキャッシュをクリアします。

  キャッシュをクリアすると、以前のバージョンの StorageGRID ソフトウェアで使用されていた古いリソースが削除され、ユーザインターフェイスが再び正しく動作するようになります。手順については、 Web ブラウザのドキュメントを参照してください。

関連情報

"Web ブラウザの要件"

"StorageGRID の管理"

使用できない管理ノードのステータスの確認

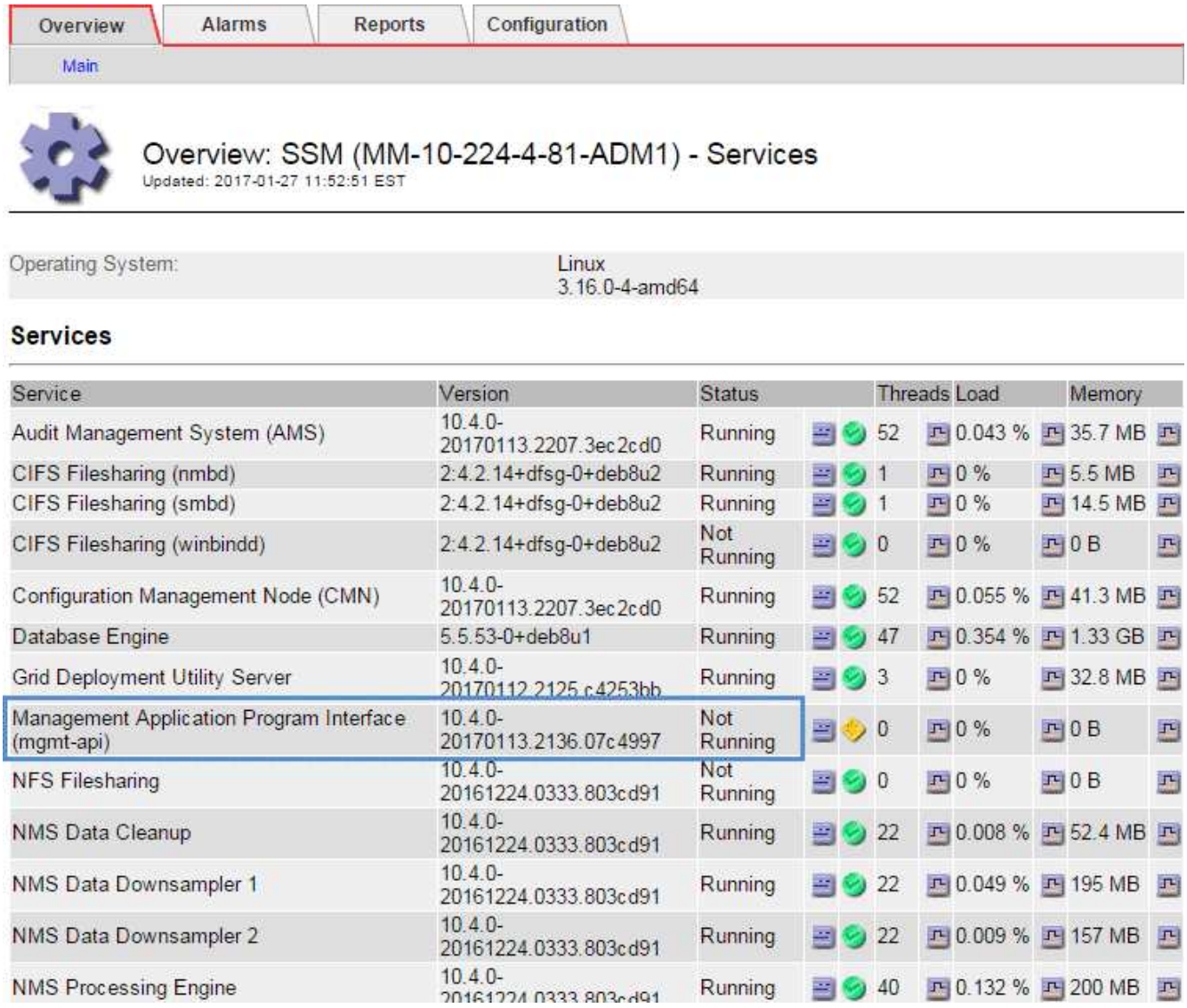
StorageGRID システムに複数の管理ノードが含まれている場合、使用できない管理ノードのステータスを別の管理ノードから確認できます。

必要なもの

特定のアクセス権限が必要です。

手順

1. 使用可能な管理ノードから、サポートされているブラウザを使用してGrid Managerにサインインします。
2. Support **>** Tools **>** Grid Topology *を選択します。
3. [***site*>] > [Unavailable Admin Node**] > [* SSM*] > [* Services] * [* Overview*] > [* Main*] を選択します。
4. ステータスが「 Not Running 」で、青で表示されているサービスがないかどうかを確認します。




5. アラームがトリガーされているかどうかを確認します。
6. 適切な方法で問題 を解決します。

関連情報

"StorageGRID の管理"

# ネットワーク、ハードウェア、およびプラットフォームの問題のトラブルシューティング

ここでは、 StorageGRID ネットワーク、ハードウェア、およびプラットフォームの問題に関連する問題の原因を特定するのに役立ついくつかのタスクを紹介します。

## 「**422**：**Unprocessable Entity**」エラーのトラブルシューティング

422 ： Unprocessable Entity というエラーは、多くの場合に発生することがあります。エラーメッセージを調べて、問題 の原因を特定します。

表示されたいずれかのエラーメッセージが表示された場合は、推奨される対処方法を実行してください。

| エラーメッセージです | ルート原因 および対処方法 |
| --- | --- |
| `422: Unprocessable Entity`<br><br>`Validation failed. Please check the values you entered for errors. Test connection failed. Please verify your configuration. Unable to authenticate, please verify your username and password: LDAP Result Code 8 "Strong Auth Required": 00002028: LdapErr: DSID-0C090256, comment: The server requires binds to turn on integrity checking if SSL\TLS are not already active on the connection, data 0, v3839` | このメッセージは、 Windows Active Directory （ AD ）を使用してアイデンティティフェデレーションを設定するときに、 Transport Layer Security （ TLS ）で「 TLS を使用しない」オプションを選択した場合に表示されることがあります。<br><br>LDAP 署名を強制する AD サーバでは、「 TLS を使用しない」オプションの使用はサポートされていません。STARTTLS を使用する * オプションまたは TLS に LDAPS * を使用するオプションのいずれかを選択する必要があります。 |
| `422: Unprocessable Entity`<br><br>`Validation failed. Please check the values you entered for errors. Test connection failed. Please verify your configuration.Unable to begin TLS, verify your certificate and TLS configuration: LDAP Result Code 200 "Network Error": TLS handshake failed (EOF)` | このメッセージは、サポートされない暗号を使用して、 StorageGRID からフェデレーションまたはクラウドストレージプールの識別に使用する外部システムへの Transport Layer Security （ TLS ）接続を試みた場合に表示されます。<br><br>外部システムで提供されている暗号を確認します。システムは、 StorageGRID の管理手順に示すように、発信 TLS 接続で StorageGRID でサポートされているいずれかの暗号を使用する必要があります。 |

関連情報

"StorageGRID の管理"

**Grid Network MTU mismatch**アラートのトラブルシューティング

グリッドネットワークインターフェイス（ eth0 ）の最大伝送ユニット（ MTU ）設定がグリッド内のノード間で大きく異なる場合に、 * Grid Network MTU mismatch * アラートがトリガーされます。

このタスクについて

MTU 設定の違いから、 eth0 ネットワークの一部がジャンボフレーム用に設定されているが、すべてではないことがわかります。MTU サイズが 1000 を超えると、原因 のネットワークパフォーマンスの問題が発生する可能性があります。

手順

1. すべてのノードの eth0 についての MTU 設定を表示します。
   - Grid Manager に用意されているクエリを使用する。
   - に移動します *primary Admin Node IP address*/metrics/graph をクリックし、次のクエリを入力します。 `node_network_mtu_bytes{interface='eth0'}`
2. 必要に応じて MTU 設定を変更し、すべてのノードのグリッドネットワークインターフェイス（ eth0 ）で同じになるようにします。
   - アプライアンスノードの場合は、使用しているアプライアンスのインストールとメンテナンスの手順を参照してください。
   - LinuxベースおよびVMwareベースのノードの場合は、次のコマンドを使用します。
     `/usr/sbin/change-mtu.py [-h] [-n node] mtu network [network...]`
     - 例 * ： `change-mtu.py -n node 1500 grid admin`

       *注：Linuxベースのノードでは、コンテナのネットワークに必要なMTU値がホストインターフェイスですでに設定されている値を超える場合、まずホストインターフェイスを設定して必要なMTU値を設定し、を使用する必要があります `change-mtu.py` コンテナ内のネットワークのMTU値を変更するスクリプト。

     Linux または VMware ベースのノードで MTU を変更するには、次の引数を使用します。

| 位置指定引数 | 説明 |
| --- | --- |
| `mtu` | 設定する MTU 。1280 ～ 9216 の範囲内にある必要があります。 |
| `network` | MTU を適用するネットワーク。次のネットワークタイプを 1 つ以上指定します。<br>• グリッド（ Grid ）<br>• 管理<br>• クライアント |

+

| オプションの引数 | 説明 |
| --- | --- |
| `-h, - help` | ヘルプメッセージを表示して終了します。 |
| `-n node, --node node` | ノード。デフォルトはローカルノードです。 |

関連情報

"SG100 SG1000サービスアプライアンス"

"SG6000 ストレージアプライアンス"

"SG5700 ストレージアプライアンス"

"SG5600 ストレージアプライアンス"

## **Network Receive Error**（**NRER**）アラームのトラブルシューティングを行います

ネットワーク受信エラー（ NRER ）アラームは、 StorageGRID とネットワークハードウェア間の接続の問題が原因で発生することがあります。場合によっては、 NRER エラーが手動操作なしでクリアされることがあります。エラーが解消されない場合は、推奨される対処方法を実行します。

このタスクについて

NRER アラームは、 StorageGRID に接続するネットワークハードウェアに関する次の問題が原因で発生する可能性があります。

- Forward Error Correction （ FEC; 前方誤り訂正）が必要で、使用されていません
- スイッチポートと NIC の MTU が一致しません
- リンクエラー率が高くなっています
- NIC リングバッファオーバーラン

手順

1. ネットワーク設定によっては、 NRER アラームの潜在的な原因に対処するためのトラブルシューティング手順を実行してください。
    - FEC の不一致が原因でエラーが発生した場合は、次の手順を実行します。
        - 注：これらの手順は、 StorageGRID アプライアンスの FEC 不一致によって発生した NRER エラーにのみ適用できます。
            i. StorageGRID アプライアンスに接続されているスイッチのポートの FEC ステータスを確認します。
            ii. アプライアンスからスイッチへのケーブルの物理的な整合性をチェックしてください。
            iii. NRER アラームを解決するために FEC 設定を変更する場合は、まず、 StorageGRID アプライアンスインストーラの [Link Configuration] ページでアプライアンスが **Auto** モードに設定されていることを確認します（アプライアンスのインストールおよびメンテナンスの手順を参照）。次に、スイッチポートの FEC 設定を変更します。StorageGRID アプライアンスのポートは、可能であれば、 FEC 設定を調整して一致させます。

            （ StorageGRID アプライアンスでは FEC 設定はできません。アプライアンスは、接続先のスイッチポートで FEC 設定を検出し、ミラーリングしようとします。リンクが 25GbE または 100GbE のネットワーク速度に強制的に設定されている場合、スイッチと NIC が共通の FEC 設定をネゴシエートできない可能性があります。共通の FEC 設定がない場合、ネットワークは「 no-fec 」モードに戻ります。FEC がイネーブルになっていない場合、接続は電気的ノイズによるエラーの影響を受けやすくなります）。
        - 注 * ： StorageGRID アプライアンスは、 FEC なしに加えて、 Firecode （ FC ）および Reed

Solomon （ RS ） FEC をサポートしています。

- エラーの原因がスイッチポートと NIC MTU の不一致である場合は、ノードに設定されている MTU サイズがスイッチポートの MTU 設定と同じであることを確認してください。

  ノードに設定されている MTU サイズは、そのノードが接続されているスイッチポートの設定よりも小さい場合があります。StorageGRID ノードが MTU より大きいイーサネットフレームを受信すると、この設定では NRER アラームが報告される場合があります。このような状況が発生していると思われる場合は、スイッチポートの MTU を StorageGRID ネットワークインターフェイスの MTU に一致するように変更するか、 StorageGRID ネットワークインターフェイスの MTU をスイッチポートに合わせて変更します。 MTU の目的または要件に応じて変更します。

  > ネットワークのパフォーマンスを最大限に高めるには、すべてのノードのグリッドネットワークインターフェイスで MTU 値がほぼ同じになるように設定する必要があります。個々のノードのグリッドネットワークの MTU 設定に大きな違いがある場合は、 * Grid Network MTU mismatch * アラートがトリガーされます。MTU 値はすべてのネットワークタイプで同じである必要はありません。

  > MTU の設定を変更するには、使用しているアプライアンスのインストールおよびメンテナンスガイドを参照してください。

- エラーの原因が高リンクエラーの場合は、次の手順に従います。

  i. まだイネーブルになっていない場合は、 FEC をイネーブル

  ii. ネットワークケーブルの品質が良好で、損傷や不適切な接続がないことを確認します。

  iii. 問題が解決しないケーブルがある場合は、テクニカルサポートにお問い合わせください。

  > 電気的ノイズが大きい環境では、エラー率が高くなることがあります。

- エラーが NIC リングのバッファオーバーランである場合は、テクニカルサポートに連絡してください。

  StorageGRID システムが過負荷になっていて、ネットワークイベントをタイムリーに処理できない場合、リングバッファがオーバーランする可能性があります。

2. 原因となっている問題を解決したら、エラーカウンタをリセットします。
   a. Support **>** Tools **>** Grid Topology *を選択します。
   b. _site * > * _grid node_name > * SSM * > * Resources * > * Configuration * > * Main * を選択します。
   c. [* 受信エラーカウントをリセットする * ] を選択し、 [ * 変更を適用する * ] をクリックします。

関連情報

"Grid Network MTU mismatchアラートのトラブルシューティング"

"アラーム一覧（従来のシステム）"

"SG6000 ストレージアプライアンス"

"SG5700 ストレージアプライアンス"

"SG5600 ストレージアプライアンス"

"SG100 SG1000サービスアプライアンス"

時刻同期エラーのトラブルシューティング

グリッドで時刻の同期に関する問題が発生する可能性があります。

時刻の同期の問題が発生する場合は、少なくとも 4 つの外部 NTP ソースが指定されており、それぞれ Stratum 3 以上であることを確認します。それらのすべての外部 NTP ソースが正常に動作しており、StorageGRID のノードからアクセスできることを確認する必要があります。

本番レベルの StorageGRID インストール環境で外部 NTP ソースを指定する場合は、 Windows Server 2016 より前のバージョンの Windows で Windows Time （ W32Time ）サービスを使用しないでください。以前のバージョンの Windows のタイムサービスは精度が十分でないため、StorageGRID などの高精度環境での使用は Microsoft でサポートされていません。

関連情報

""

**Linux** ：ネットワーク接続の問題

Linux ホストでホストされている StorageGRID グリッドノードのネットワーク接続に問題が発生することがあります。

**MAC** アドレスのクローニング

ネットワークの問題は、 MAC アドレスのクローニングを使用して解決できる場合があります。仮想ホストを使用している場合は、各ネットワークの MAC アドレスクローニングキーの値をノード構成ファイルで「 true 」に設定します。この設定により、 StorageGRID コンテナの MAC アドレスがホストの MAC アドレスを使用するようになります。ノード構成ファイルを作成するには、使用するプラットフォームに対応したインストールガイドの手順を参照してください。

Linux ホスト OS で使用する個別の仮想ネットワークインターフェイスを作成します。Linux ホスト OS 原因 と StorageGRID コンテナに同じネットワークインターフェイスを使用すると、ハイパーバイザーでプロミスキャスモードが有効になっていない場合、ホスト OS が到達不能になることがあります。

MAC クローニングの有効化の詳細については、ご使用のプラットフォームのインストールガイドに記載されている手順を参照してください。

プロミスキャスモードです

MAC アドレスのクローニングを使用せずに、ハイパーバイザーによって割り当てられた MAC アドレス以外の MAC アドレスのデータをすべてのインターフェイスが送受信できるようにする場合は、次の手順を実行します。 仮想スイッチおよびポートグループレベルのセキュリティプロパティが、無差別モード、 MAC アドレスの変更、および Forged Transmits の **Accept** に設定されていることを確認します。仮想スイッチに設定された値は、ポートグループレベルの値によって上書きできるため、両方のレベルで設定が同じであることを確認してください。

関連情報

"Red Hat Enterprise Linux または CentOS をインストールします"

"Ubuntu または Debian をインストールします"

**Linux**：ノードのステータスは「**orphaned**」です。

orphaned 状態の Linux ノードは、通常、 StorageGRID サービスまたはノードのコンテナを制御している StorageGRID ノードデーモンが予期せず停止したことを示しています。

このタスクについて

Linux ノードが orphaned 状態になった場合は、次のように対応策を実行してください。

- ログでエラーとメッセージを確認します。
- ノードを再起動してみます。
- 必要に応じて、Dockerコマンドを使用して既存のノードコンテナを停止します。
- ノードを再起動します。

手順

1. サービスデーモンと orphaned 状態のノードの両方のログを調べ、明らかなエラーや予期しない終了に関するメッセージがないか確認します。
2. ホストに root としてログインするか、 sudo 権限を持つアカウントを使ってログインします。
3. 次のコマンドを実行して、ノードの再起動を試行します。 `$ sudo storagegrid node start node-name`

   ```
   $ sudo storagegrid node start DC1-S1-172-16-1-172
   ```

   ノードが孤立している場合、応答はになります

   ```
   Not starting ORPHANED node DC1-S1-172-16-1-172
   ```

4. Linuxから、Dockerコンテナ、およびStorageGRIDノードを制御しているすべてのプロセスを停止します。`sudo docker stop --time secondscontainer-name`

   の場合 `seconds`で、コンテナの停止を待機する秒数を入力します（通常は15分以下）。

   ```
   sudo docker stop --time 900 storagegrid-DC1-S1-172-16-1-172
   ```

5. ノードを再起動します。 `storagegrid node start node-name`

   ```
   storagegrid node start DC1-S1-172-16-1-172
   ```

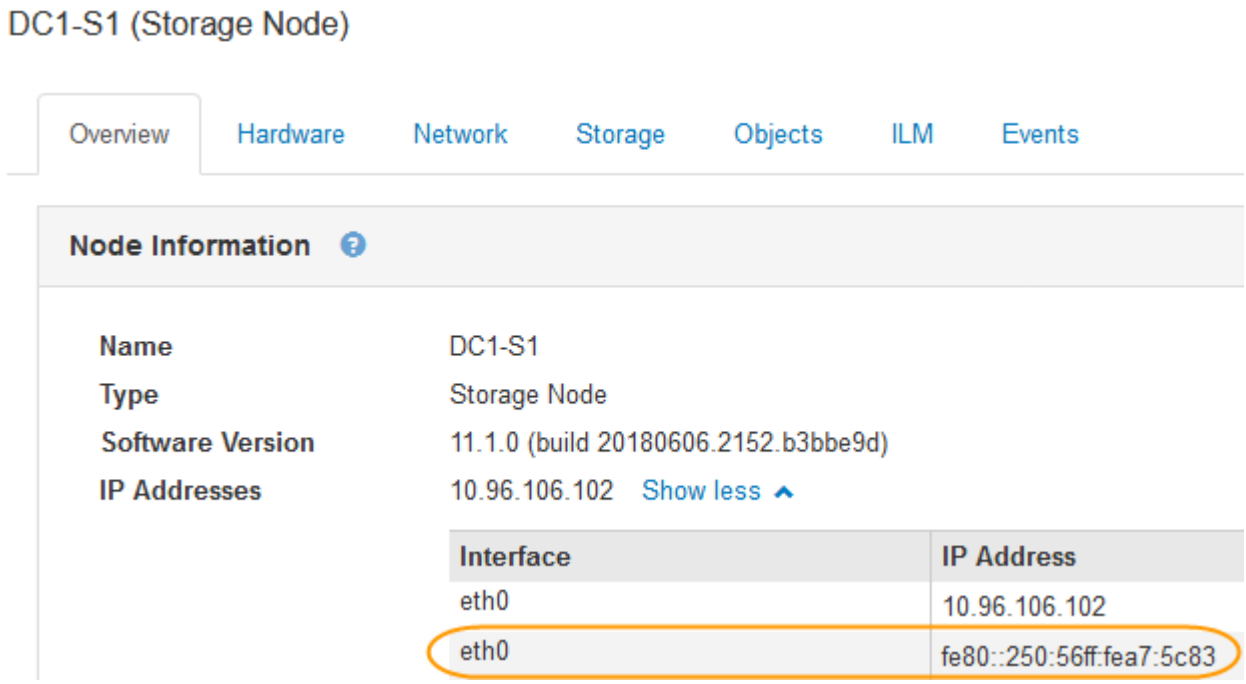
## Linux：IPv6サポートのトラブルシューティング

Linux ホストに StorageGRID ノードをインストールしていて、 IPv6 アドレスが想定どおりにノードコンテナに割り当てられていない場合は、カーネルでの IPv6 サポートの有効化が必要となることがあります。

このタスクについて

Grid Manager の次の場所で、グリッドノードに割り当てられている IPv6 アドレスを確認できます。

- ノード*を選択し、ノードを選択します。次に、Overview（概要）タブの* IP Addresses の横にある Show More *（詳細を表示）をクリックします。




- Support > Tools > Grid Topology を選択します。次に、 * ***Node*** > * SSM * > * Resources * を選択します。IPv6 アドレスが割り当てられている場合は、「 * ネットワークアドレス * 」セクションの IPv4 アドレスの下に表示されます。

IPv6 アドレスが表示されず、ノードが Linux ホストにインストールされている場合は、次の手順に従ってカーネルで IPv6 サポートを有効にします。

手順

1. ホストに root としてログインするか、 sudo 権限を持つアカウントを使ってログインします。
2. 次のコマンドを実行します。 `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@SG:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

結果は 0 になります。

```
net.ipv6.conf.all.disable_ipv6 = 0
```

結果が0でない場合は、オペレーティングシステムのドキュメントで変更方法を確認してください `sysctl` 設定：次に進む前に、値を 0 に変更します。

3. StorageGRID ノードコンテナを入力します。 `storagegrid node enter node-name`
4. 次のコマンドを実行します。 `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@DC1-S1:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

結果は 1 になります。

```
net.ipv6.conf.all.disable_ipv6 = 1
```

結果が 1 でない場合、この手順 は適用されません。テクニカルサポートにお問い合わせください。

5. コンテナを終了します。 `exit`

```
root@DC1-S1:~ # exit
```

6. rootとして次のファイルを編集します。 `/var/lib/storagegrid/settings/sysctl.d/net.conf`。

```
sudo vi /var/lib/storagegrid/settings/sysctl.d/net.conf
```

7. 次の 2 行を探して、コメントタグを削除します。次に、ファイルを保存して閉じます。

```
net.ipv6.conf.all.disable_ipv6 = 0
```

```
net.ipv6.conf.default.disable_ipv6 = 0
```

8. 次のコマンドを実行して、 StorageGRID コンテナを再起動します。

```
storagegrid node stop node-name
```

```
storagegrid node start node-name
```

# 監査ログを確認します

StorageGRID システムの監査ログについて説明し、すべての監査メッセージの一覧を確認します。

- "監査メッセージの概要"
- "監査ログファイルおよびメッセージの形式"
- "監査メッセージとオブジェクトライフサイクル"
- "監査メッセージ"

## 監査メッセージの概要

ここでは、 StorageGRID 監査メッセージおよび監査ログの構造と内容について説明します。この情報を使用して、システムアクティビティの監査証跡を判読し、分析できます。

ここに記載する手順は、システムのアクティビティおよび使用状況のレポート生成を担当する管理者を対象としています。このようなレポートの生成には、 StorageGRID システムの監査メッセージの分析が必要となります。

StorageGRID システム内の監査対象アクティビティの性質を十分に理解していることを前提としています。テキストログファイルを使用するには、管理ノード上に設定されている監査共有へのアクセスが必要です。

関連情報

"StorageGRID の管理"

### 監査メッセージのフローと保持

すべての StorageGRID サービスは通常のシステム運用中に監査メッセージを生成します。これらの監査メッセージがStorageGRID システムからにどのように転送されるかを理解しておく必要があります `audit.log` ファイル。

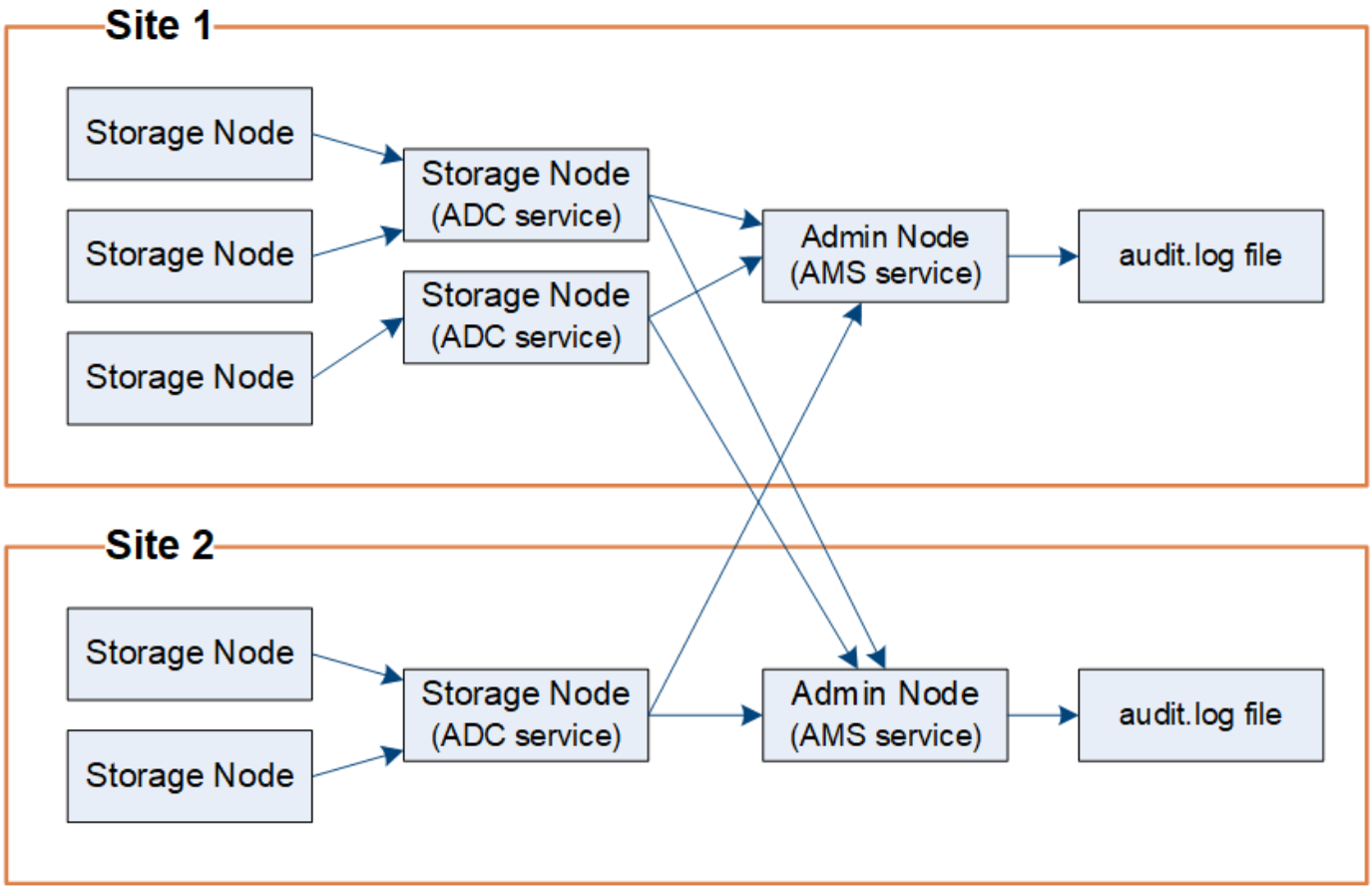
#### 監査メッセージのフロー

監査メッセージは、管理ノードおよび Administrative Domain Controller （ ADC ）サービスが用意されているストレージノードによって処理されます。

監査メッセージのフロー図に示すように、各 StorageGRID ノードは監査メッセージをデータセンターサイトにあるいずれかの ADC サービスに送信します。ADC サービスは、各サイトに設置されている最初の 3 つのストレージノードで自動的に有効になります。

次に、各 ADC サービスはリレーとして機能し、監査メッセージの集合を StorageGRID システム内のすべての管理ノードに送信します。これにより、システムアクティビティの完全な記録が各管理ノードに提供されます。

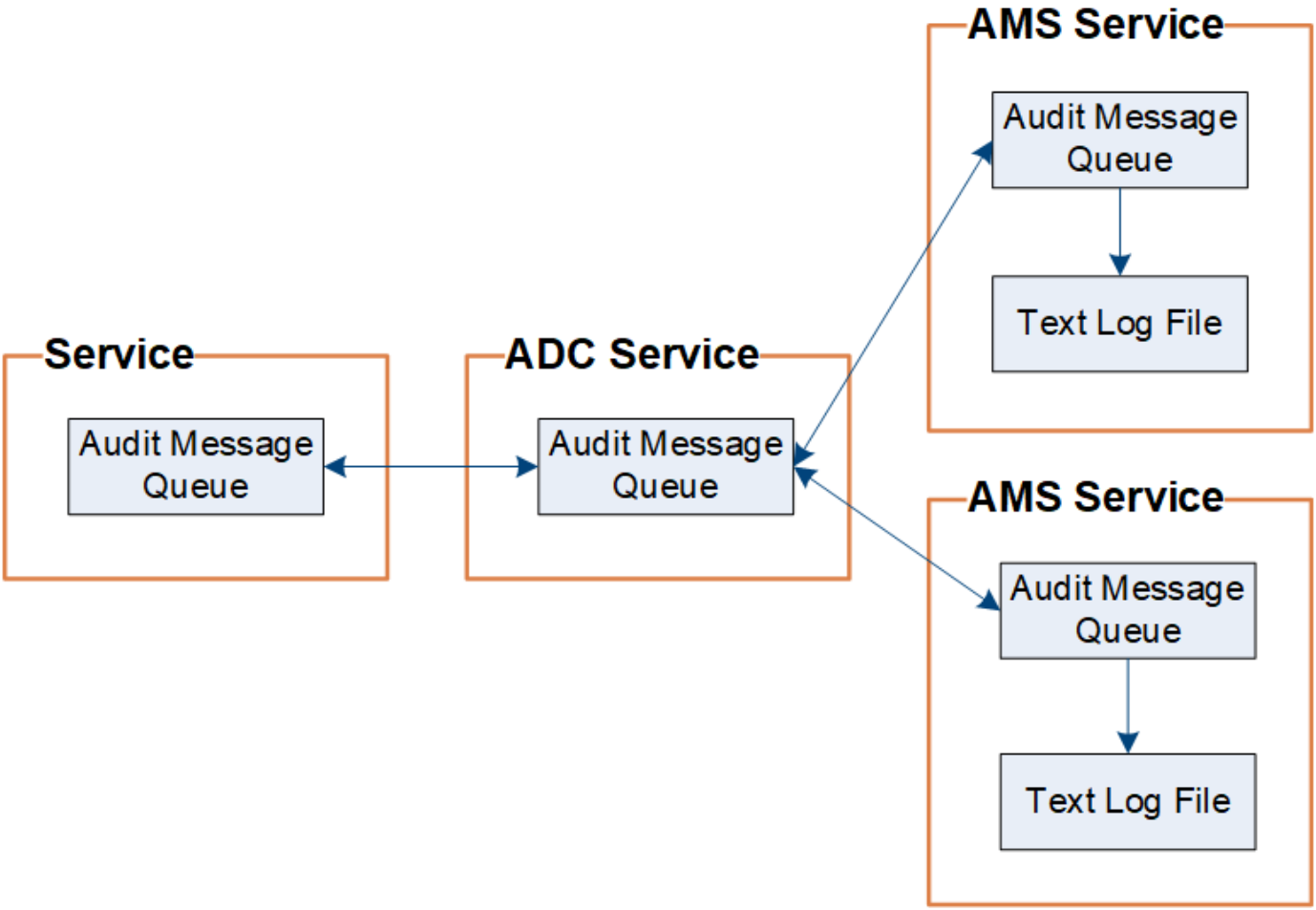
各管理ノードでは、監査メッセージがテキストログファイルに保存されます。アクティブなログファイルの名前はです `audit.log`。




監査メッセージの保持

StorageGRID では、コピー / 削除プロセスを使用して、監査ログに書き込まれる前に監査メッセージが失われないようにします。

ノードが生成またはリレーした監査メッセージは、グリッドノードのシステムディスク上の監査メッセージキューに格納されます。メッセージが管理ノード内の監査ログファイルに書き込まれるまで、メッセージのコピーは常に監査メッセージキューに保持されます `/var/local/audit/export` ディレクトリ。これにより、監査メッセージが転送中に失われることはありません。




ネットワーク接続の問題または監査容量の不足が原因で、監査メッセージキューが一時的に増加する可能性があります。キューが増加すると、各ノードの使用可能スペースがキューによってさらに消費されます `/var/local/` ディレクトリ。問題 が解除されず、ノードの監査メッセージディレクトリがいっぱいになると、個々のノードがバックログの処理の優先順位を設定し、一時的に新しいメッセージに使用できなくなります。

具体的には、次のような動作が発生することがあります。

- 状況に応じて `/var/local/audit/export` 管理ノードで使用されるディレクトリがいっぱいになると、ディレクトリに空きが出るまでその管理ノードを新しい監査メッセージに使用できないことを示すフラグが設定されます。S3 および Swift クライアント要求には影響しません。監査リポジトリにアクセスできない場合に XAMS （ Unreachable Audit Repositories ）アラームがトリガーされます。
- 状況に応じて `/var/local/` ADCサービスを採用するストレージノードで使用されるディレクトリが92%フルになると、ディレクトリが87%フルになるまでそのノードを監査メッセージに使用できないことを示すフラグが設定されます。他のノードに対する S3 および Swift クライアント要求には影響しません。監査リレーにアクセスできない場合に NRLY （ Available Audit Relays ）アラームがトリガーされます。

  ADCサービスを採用するストレージノードがない場合は、ストレージノードが監査メッセージをローカルに格納します。

- 状況に応じて `/var/local/` ストレージノードで使用されるディレクトリが85%フルになると、ノードはS3およびSwiftクライアントの要求を拒否し始めます `503 Service Unavailable`。

原因 監査メッセージキューが大幅に増加すると、次のような問題が発生する可能性があります。

- 管理ノードまたは ADC サービスを採用するストレージノードの停止。システムのいずれかのノードが停止すると、残りのノードはバックログ状態になる可能性があります。
- システムの監査キャパシティを超えるアクティビティ率の継続。
- 。 `/var/local/` 監査メッセージには関連のない理由でADCストレージノード上ののスペースがいっぱいになる。この場合、ノードは新しい監査メッセージの受け入れを停止し、現在のバックログの優先順位を設定します。これにより、他のノードで原因 バックログが発生する可能性があります。

**Large audit queue** アラートと **Audit Messages Queued** （ **AMQS** ）アラーム

時間の経過に伴う監査メッセージキューのサイズを監視できるように、ストレージノードキューまたは管理ノードキュー内のメッセージの数が特定のしきい値に達すると、 * Large audit queue * アラートと従来の AMQS アラームがトリガーされます。

「 Large audit queue * 」アラートまたは従来の AMQS アラームがトリガーされた場合は、最初にシステムの負荷を確認します。最近のトランザクションの数が膨大であった場合は、アラートとアラームは時間が経過すると解決するため、無視してかまいません。

アラートまたはアラームが解決せず重大度が上がった場合は、キューサイズのグラフを確認します。数時間から数日にわたって数値が増え続けている場合は、監査の負荷がシステムの監査キャパシティを超えている可能性があります。クライアントの書き込みとクライアントの読み取りでエラーまたはオフの監査レベルを変更して、クライアントの処理速度を下げるか、ログに記録される監査メッセージの数を減らしてください。「」を参照"監査メッセージレベルの変更". 」

重複メッセージです

StorageGRID システムは、ネットワークまたはノードの障害が発生した場合に保守的なアプローチを採用します。そのため、監査ログでメッセージが重複する可能性があります。

監査メッセージレベルの変更

## 監査レベルを調整して、監査ログに記録する監査メッセージの数を監査メッセージカテゴリごとに増減できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

監査ログに記録された監査メッセージは、* Configuration > Monitoring > Audit *ページの設定に基づいてフィルタリングされます。

次のメッセージカテゴリごとに異なる監査レベルを設定できます。

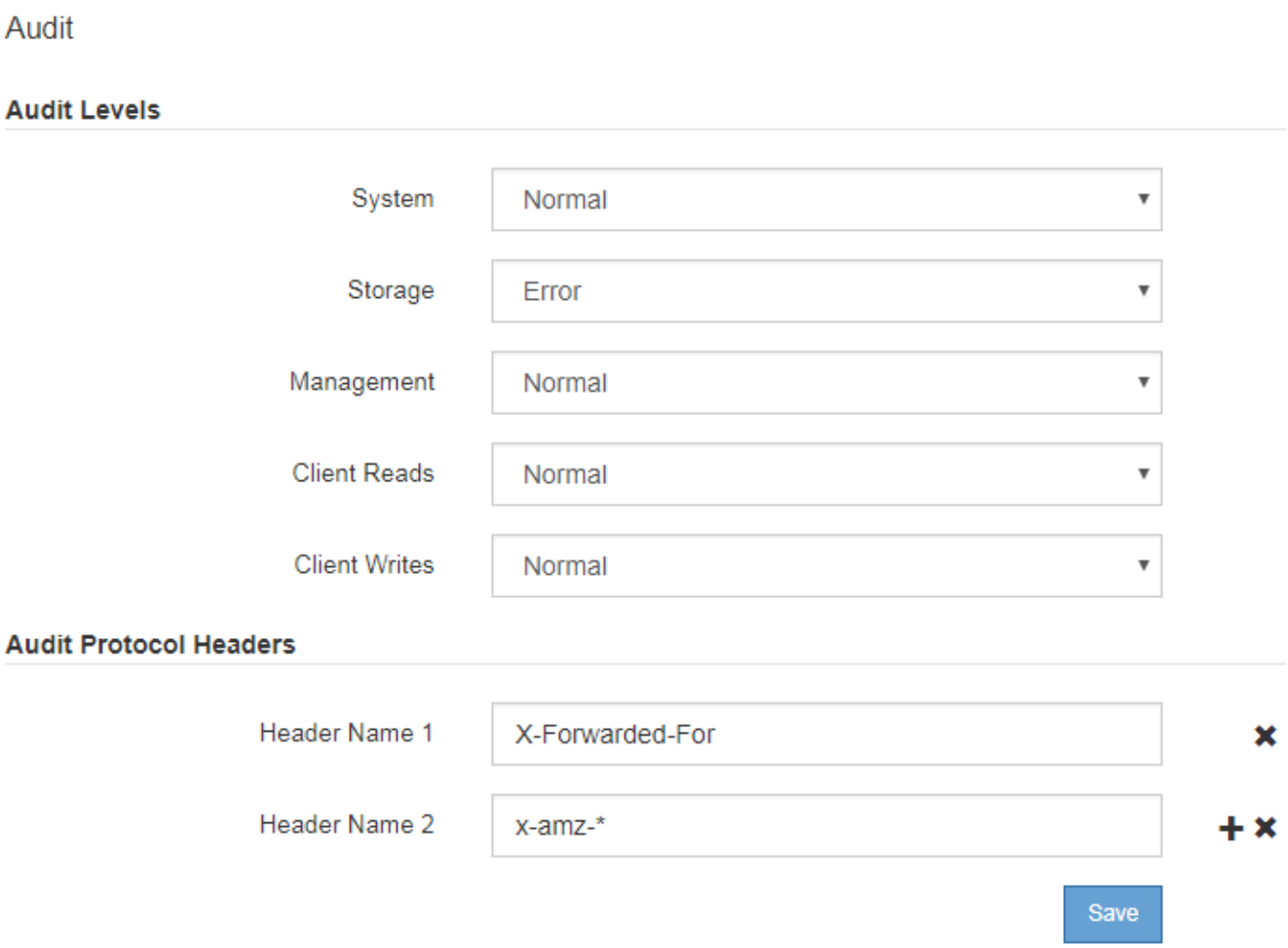
- システム：デフォルトでは、このレベルは[標準]に設定されています。
- * Storage *：デフォルトでは、このレベルはErrorに設定されています。
- 管理：デフォルトでは、このレベルは[標準]に設定されています。
- クライアント読み取り:デフォルトでは、このレベルはNormalに設定されています。
- クライアント書き込み：デフォルトでは、このレベルはNormalに設定されます。

これらのデフォルト値は、 StorageGRID 10.3 以降を最初にインストールした場合に適用されます。以前のバージョンの StorageGRID からアップグレードした場合、すべてのカテゴリのデフォルトは Normal に設定されます。

アップグレード中は、監査レベルの設定はすぐには有効になりません。

手順

1. * Configuration > Monitoring > Audit *を選択します。




2. 監査メッセージのカテゴリごとに、ドロップダウンリストから監査レベルを選択します。

| 監査レベル | 説明 |
| --- | --- |
| オフ | このカテゴリの監査メッセージはログに記録されません。 |
| エラー | エラーメッセージのみがログに記録されます — 結果コードが「成功」（ SUCS ）以外の監査メッセージ。 |
| 正常 | 標準のトランザクション・メッセージはログに記録されますこのメッセージは ' カテゴリに関する次の手順に記載されています |

| 監査レベル | 説明 |
| --- | --- |
| デバッグ | 非推奨。このレベルの動作は Normal 監査レベルと同じです。 |

特定のレベルに含まれるメッセージには、上位レベルでロギングされるメッセージも含まれます。たとえば、 Normal レベルには Error レベルのメッセージがすべて含まれます。

3. 監査プロトコルヘッダー*で、クライアント読み取りおよびクライアント書き込み監査メッセージに含めるHTTP要求ヘッダーの名前を入力します。ワイルドカードとしてアスタリスク（*）を使用するか、リテラルアスタリスクとしてエスケープシーケンス（*）を使用します。プラス記号をクリックして、ヘッダー名フィールドのリストを作成します。

   監査プロトコルヘッダーは、 S3 要求と Swift 要求にのみ適用されます。

   このようなHTTPヘッダーが要求に含まれている場合、HTTPヘッダーはHTRHフィールドの下の監査メッセージに含まれます。

   監査プロトコル要求ヘッダーは、 * クライアント読み取り * または * クライアント書き込み * の監査レベルが * オフ * でない場合にのみ記録されます。

4. [ 保存（ Save ） ] をクリックします。

関連情報

"システム監査メッセージ"

"オブジェクトストレージ監査メッセージ"

"管理監査メッセージ"

"クライアント読み取り監査メッセージ"

"StorageGRID の管理"

監査ログファイルへのアクセス

監査共有にはアクティブなが含まれています `audit.log` ファイルおよび圧縮された監査ログファイル。監査ログへのアクセスを簡単にするためには、NFSとCIFSの両方についてクライアントから監査共有へのアクセスを設定します（現在CIFSは廃止）。管理ノードのコマンドラインから直接監査ログファイルにアクセスすることもできます。

必要なもの

- 特定のアクセス権限が必要です。
- を用意しておく必要があります `Passwords.txt` ファイル。
- 管理ノードの IP アドレスを確認しておく必要があります。

手順

1. 管理ノードにログインします。

a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`

b. に記載されているパスワードを入力します `Passwords.txt` ファイル。

2. 監査ログファイルが保存されているディレクトリに移動します。

```
cd /var/local/audit/export
```

3. 必要に応じて、現在の監査ログファイルまたは保存された監査ログファイルを表示します。

関連情報

"StorageGRID の管理"

監査ログファイルのローテーション

## 監査ログファイルは管理ノードに保存されます `/var/local/audit/export` ディレクトリ。アクティブな監査ログファイルの名前はです `audit.log`。

1日に1回、アクティブです `audit.log` ファイルが保存され、新しいファイルが作成されます `audit.log` ファイルが開始されました。保存されたファイルの名前は、保存された日時をの形式で示しています *`yyyy-mm-dd.txt`*。1日に複数の監査ログが作成される場合、ファイル名には、ファイルが保存された日付と番号が付加された日付が使用されます *`yyyy-mm-dd.txt.n`*。例： `2018-04-15.txt` および `2018-04-15.txt.1` 2018年4月15日に作成および保存された1つ目のログファイルおよび2つ目のログファイルです。

1日後、保存されたファイルは圧縮され、という形式で名前が変更されます *`yyyy-mm-dd.txt.gz`*`元の日付を保持します。そのため、時間の経過とともに、管理ノード上の監査ログ用に割り当てられたストレージが消費されます。スクリプトによって監査ログのスペース消費が監視され、のスペースを解放するために、必要に応じてログファイルが削除されます `/var/local/audit/export` ディレクトリ。監査ログは、作成日に基づいて、古い順に削除されます。スクリプトの処理は、次のファイルで監視できます。 `/var/local/log/manage-audit.log`。

この例は、アクティブを示しています `audit.log` ファイル。前日のファイルです (`2018-04-15.txt`）、および前日の圧縮ファイルです (`2018-04-14.txt.gz`）。

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

## 監査ログファイルおよびメッセージの形式

監査ログを使用して、システムに関する情報を収集し、問題のトラブルシューティングを行うことができます。監査ログファイルの形式と、監査メッセージに使用される一般的な形式を理解しておく必要があります。

監査ログファイルの形式

## 監査ログファイルはすべての管理ノードに存在し、一連の監査メッセージが格納されています。

各監査メッセージには次の情報が含まれます。

- 監査メッセージ（ ATIM ）をトリガーしたイベントの協定世界時（ UTC ）を ISO 8601 形式で表した値と、末尾のスペース。

  *YYYY-MM-DDTHH:MM:SS.UUUUUU*、ここで *UUUUUU* はマイクロ秒です。

- 監査メッセージ。全体が角かっこで囲まれ、で始まる `AUDT`。

次の例は、監査ログファイル内の 3 つの監査メッセージを示しています（読みやすくするために改行しています）。これらのメッセージは、テナントが S3 バケットを作成し、オブジェクトを 2 つバケットに追加したときに生成されました。

```
2019-08-07T18:43:30.247711
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991681][TIME(UI64):73520][SAI
P(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][AVER(UI32):10][ATIM(UI64):1565203410247711]
[ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):7074142
142472611085]]

2019-08-07T18:43:30.783597
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991696][TIME(UI64):120713][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-0"]
[CBID(UI64):0x779557A069B2C037][UUID(CSTR):"94BA6949-38E1-4B0C-BC80-
EB44FB4FCC7F"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410783597][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):8439606722108456022]]

2019-08-07T18:43:30.784558
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991693][TIME(UI64):121666][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-2000"]
[CBID(UI64):0x180CBD8E678EED17][UUID(CSTR):"19CE06D0-D2CF-4B03-9C38-
E578D66F7ADD"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410784558][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):13489590586043706682]]
```

デフォルトの形式のままでは、監査ログファイル内の監査メッセージを読んで解釈するのは簡単ではありません。を使用できます `audit-explain` 監査ログ内の監査メッセージの概要を取得するためのツール。を使用できます `audit-sum` ログに記録された書き込み、読み取り、削除の処理数と、それらの処理に要した時間を表示するツールです。

関連情報

"audit-explainツールの使用"

"audit-sumツールを使用する"

# を使用できます audit-explain 監査ログ内の監査メッセージをわかりやすい形式に変換するツール。

必要なもの

- 特定のアクセス権限が必要です。
- を用意しておく必要があります Passwords.txt ファイル。
- プライマリ管理ノードの IP アドレスを確認しておく必要があります。

このタスクについて

。 audit-explain ツールはプライマリ管理ノードで使用でき、監査ログ内の監査メッセージの簡単な概要を取得できます。

> 。 audit-explain ツールは、主にトラブルシューティング処理の際にテクニカルサポートが使用することを目的としています。処理中です audit-explain クエリは大量のCPUパワーを消費する可能性があるため、StorageGRID の処理に影響を及ぼす場合があります。

次の例は、からの一般的な出力を示しています audit-explain ツール。4 つの SPUT 監査メッセージが、アカウント ID が 92484777680322627870 の S3 テナントが S3 PUT 要求を使用して「 bucket1 」という名前のバケットを作成し、バケットにオブジェクトを 3 つ追加したときに生成されました。

```
SPUT S3 PUT bucket bucket1 account:92484777680322627870 usec:124673
SPUT S3 PUT object bucket1/part1.txt tenant:92484777680322627870
cbid:9DCB157394F99FE5 usec:101485
SPUT S3 PUT object bucket1/part2.txt tenant:92484777680322627870
cbid:3CFBB07AB3D32CA9 usec:102804
SPUT S3 PUT object bucket1/part3.txt tenant:92484777680322627870
cbid:5373D73831ECC743 usec:93874
```

。 audit-explain ツールは、プレーン形式または圧縮形式の監査ログを処理できます。例：

```
audit-explain audit.log
```

```
audit-explain 2019-08-12.txt.gz
```

。 audit-explain ツールは、複数のファイルを一度に処理することもできます。例：

```
audit-explain audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-explain /var/local/audit/export/*
```

最後に、 audit-explain ツールは、パイプからの入力を受け入れます。これにより、を使用して入力をフィルタ処理および前処理できます grep コマンドまたはその他の手段。例：

```
grep SPUT audit.log | audit-explain
```

```
grep bucket-name audit.log | audit-explain
```

監査ログは非常に大きくなり、解析に時間がかかることがあるため、調べる部分や実行する部分をフィルタリングすることで時間を節約できます audit-explain ファイル全体ではなく、部分的に。

。 audit-explain ツールは圧縮ファイルをパイプ付き入力として受け入れません。圧縮ファイルを処理するには、ファイル名をコマンドライン引数として指定するか、を使用します zcat 最初にファイルを解凍するツール。例：

```
zcat audit.log.gz | audit-explain
```

を使用します help （-h）使用可能なオプションを表示するためのオプション。例：

```
$ audit-explain -h
```

手順

1. プライマリ管理ノードにログインします。
   a. 次のコマンドを入力します。 ssh admin@*primary_Admin_Node_IP*
   b. に記載されているパスワードを入力します Passwords.txt ファイル。
2. 次のコマンドを入力します /var/local/audit/export/audit.log 分析するファイルの名前と場所を表します。

   ```
   $ audit-explain /var/local/audit/export/audit.log
   ```

   。 audit-explain ツールは、指定されたファイル内のすべてのメッセージを、判読可能な形式に変換して出力します。

   各行を短く読みやすくするために、デフォルトではタイムスタンプは表示されません。タイムスタンプを表示するには、タイムスタンプを使用します (-t）をクリックします。

関連情報

"SPUT ： S3 PUT"

**audit-sum**ツールを使用する

を使用できます audit-sum 書き込み、読み取り、HEAD、削除の各監査メッセージを

カウントし、それぞれの処理タイプの最小、最大、平均時間（またはサイズ）を表示するツールです。

必要なもの

- 特定のアクセス権限が必要です。
- を用意しておく必要があります `Passwords.txt` ファイル。
- プライマリ管理ノードの IP アドレスを確認しておく必要があります。

このタスクについて

。 `audit-sum` ツールはプライマリ管理ノードで使用でき、ログに記録された書き込み、読み取り、削除の処理数と、それらの処理に要した時間を取得できます。

> 。 `audit-sum` ツールは、主にトラブルシューティング処理の際にテクニカルサポートが使用することを目的としています。処理中です `audit-sum` クエリは大量のCPUパワーを消費する可能性があるため、StorageGRID の処理に影響を及ぼす場合があります。

次の例は、からの一般的な出力を示しています `audit-sum` ツール。この例は、プロトコル処理に要した時間を示しています。

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  IDEL                      274
  SDEL                   213371        0.004          20.934
0.352
  SGET                   201906        0.010        1740.290
1.132
  SHEA                    22716        0.005           2.349
0.272
  SPUT                 1771398        0.011        1770.563
0.487
```

。 `audit-sum` ツールは、監査ログ内の次のS3、Swift、およびILM監査メッセージの数と時間を取得します。

| コード | 説明 | を参照してください |
|---|---|---|
| ARCT | アーカイブをクラウド階層から取得します | "ARCT ：クラウド階層からアーカイブを取得します" |
| ▽ SCT 。△ | アーカイブストア - クラウド階層 | "ASCT ：アーカイブストアのクラウド階層" |
| IDEL | ILM Initiated Delete ： ILM がオブジェクトを削除する処理を開始すると記録されます。 | "IDEL ： ILM Initiated Delete" |

| コード | 説明 | を参照してください |
| --- | --- | --- |
| SDEL | S3 DELETE ：オブジェクトまたはバケットを削除するトランザクションの成功をログに記録します。 | "SDEL ： S3 DELETE" |
| SGET | S3 GET ：バケット内のオブジェクトを読み出しまたはリストアップするトランザクションの成功をログに記録します。 | "SGET ： S3 GET" |
| Shea | S3 HEAD ：オブジェクトまたはバケットの存在を確認するトランザクションの成功をログに記録します。 | "Shea ： S3 ヘッド" |
| SPUT | S3 PUT ：オブジェクトまたはバケットを新規に作成するトランザクションの成功をログに記録します。 | "SPUT ： S3 PUT" |
| WDEL | Swift DELETE ：オブジェクトまたはコンテナを削除するトランザクションの成功をログに記録します。 | "WDEL ： Swift の削除" |
| wget | Swift GET ：コンテナ内のオブジェクトを読み出しまたはリストアップするトランザクションの成功をログに記録します。 | "wget ： Swift GET" |
| WHEA | Swift HEAD ：オブジェクトまたはコンテナの存在を確認するトランザクションの成功をログに記録します。 | "WHEA ： Swift ヘッド" |
| WPUT | Swift PUT ：オブジェクトまたはコンテナを新規に作成するトランザクションの成功をログに記録します。 | "WPUT ： Swift PUT" |

。 `audit-sum` ツールは、プレーン形式または圧縮形式の監査ログを処理できます。例：

```
audit-sum audit.log
```

```
audit-sum 2019-08-12.txt.gz
```

。 `audit-sum` ツールは、複数のファイルを一度に処理することもできます。例：

```
audit-sum audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-sum /var/local/audit/export/*
```

最後に、 `audit-sum` ツールは、パイプからの入力を受け入れることもできます。これにより、を使用して、入力をフィルタ処理および前処理できます `grep` コマンドまたはその他の手段。例：

```
grep WGET audit.log | audit-sum
```

```
grep bucket1 audit.log | audit-sum
```

```
grep SPUT audit.log | grep bucket1 | audit-sum
```

このツールは、圧縮ファイルをパイプ付き入力として受け入れません。圧縮ファイルを処理するには、ファイル名をコマンドライン引数として指定するか、を使用します `zcat` 最初にファイルを解凍するツール。例：

```
audit-sum audit.log.gz
```

```
zcat audit.log.gz | audit-sum
```

コマンドラインオプションを使用して、バケットに対する処理をオブジェクトに対する処理とは別にまとめたり、メッセージの概要をバケット名、期間、ターゲットタイプ別にグループ化したりできます。デフォルトでは、概要には最小、最大、平均の処理時間が表示されますが、を使用することもできます `size (-s)` オブジェクトサイズを表示するオプションです。

を使用します `help (-h)` 使用可能なオプションを表示するためのオプション。例：

```
$ audit-sum -h
```

手順

1. プライマリ管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
2. 書き込み、読み取り、 HEAD 、削除の処理に関連するすべてのメッセージを分析するには、次の手順を実行します。
   a. 次のコマンドを入力します `/var/local/audit/export/audit.log` 分析するファイルの名前と場所を表します。

```
$ audit-sum /var/local/audit/export/audit.log
```

次の例は、からの一般的な出力を示しています `audit-sum` ツール。この例は、プロトコル処理に要した時間を示しています。

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  IDEL                      274
  SDEL                   213371        0.004          20.934
0.352
  SGET                   201906        0.010        1740.290
1.132
  SHEA                    22716        0.005           2.349
0.272
  SPUT                 1771398        0.011        1770.563
0.487
```

この例では、平均処理時間では SGET （ S3 GET ）処理が 1.13 秒と最も長い一方で、最大処理時間では SGET 処理と SPUT （ S3 PUT ）処理がどちらも約 1 、 770 秒と一番長くなっています。

b. 最も時間がかかった読み出し処理を10件表示するには、grepコマンドを使用してSGETメッセージのみを選択し、long出力オプションを追加します (`-l`）オブジェクトパスを含めるには： `grep SGET audit.log | audit-sum -l`

結果にはタイプ（オブジェクトまたはバケット）とパスが含まれます。この情報を使用して、監査ログを grep してこれらのオブジェクトに関連する他のメッセージを出力できます。

```
Total:          201906 operations
    Slowest:      1740.290 sec
    Average:         1.132 sec
    Fastest:         0.010 sec
    Slowest operations:
        time(usec)       source ip         type      size(B) path
        ========== ============== ============ ============ ====
        1740289662   10.96.101.125       object   5663711385
backup/r9O1OaQ8JB-1566861764-4519.iso
        1624414429   10.96.101.125       object   5375001556
backup/r9O1OaQ8JB-1566861764-6618.iso
        1533143793   10.96.101.125       object   5183661466
backup/r9O1OaQ8JB-1566861764-4518.iso
             70839   10.96.101.125       object        28338
bucket3/dat.1566861764-6619
             68487   10.96.101.125       object        27890
bucket3/dat.1566861764-6615
             67798   10.96.101.125       object        27671
bucket5/dat.1566861764-6617
             67027   10.96.101.125       object        27230
bucket5/dat.1566861764-4517
             60922   10.96.101.125       object        26118
bucket3/dat.1566861764-4520
             35588   10.96.101.125       object        11311
bucket3/dat.1566861764-6616
             23897   10.96.101.125       object        10692
bucket3/dat.1566861764-4516
```

+
この出力例からは、最も時間がかかった 3 個の S3 GET 要求が、他のオブジェクトよりもはるかに大きい約 5GB のオブジェクトに対して実行されたことがわかります。サイズが大きいと、最悪の場合の読み出し時間が長くなります。

3. グリッドに取り込まれているオブジェクトとグリッドから読み出されているオブジェクトのサイズを特定するには、sizeオプションを使用します (`-s`）：

```
audit-sum -s audit.log
```

```
  message group            count       min(MB)          max(MB)
average(MB)
  =============            =====     ========        ========
============
  IDEL                       274        0.004        5000.000
1654.502
  SDEL                    213371        0.000          10.504
1.695
  SGET                    201906        0.000        5000.000
14.920
  SHEA                     22716        0.001          10.504
2.967
  SPUT                   1771398        0.000        5000.000
2.495
```

この例では、 SPUT の平均オブジェクトサイズは 2.5MB 未満ですが、 SGET の平均サイズははるかに大きいことがわかります。SPUT メッセージの数は SGET メッセージの数よりもはるかに多く、ほとんどのオブジェクトが読み出されていないことを示しています。

4. 昨日の読み出しに時間がかかっていないかどうかを確認するには、次の手順を実行

   a. 該当する監査ログに対してコマンドを問題 処理し、group-by-timeオプションを使用します (`-gt`）に続けて期間（例：15M、1H、10S）を指定します。

      ```
      grep SGET audit.log | audit-sum -gt 1H
      ```

```
  message group           count    min(sec)       max(sec)
average(sec)
  =============           =====     ========        ========
============
  2019-09-05T00            7591        0.010        1481.867
1.254
  2019-09-05T01            4173        0.011        1740.290
1.115
  2019-09-05T02           20142        0.011        1274.961
1.562
  2019-09-05T03           57591        0.010        1383.867
1.254
  2019-09-05T04          124171        0.013        1740.290
1.405
  2019-09-05T05          420182        0.021        1274.511
1.562
  2019-09-05T06         1220371        0.015        6274.961
5.562
  2019-09-05T07          527142        0.011        1974.228
2.002
  2019-09-05T08          384173        0.012        1740.290
1.105
  2019-09-05T09           27591        0.010        1481.867
1.354
```

上記の結果は、 06 ： 00 と 07 ： 00 の間に S3 GET トラフィックが急増したことを示しています。この時間帯は最大時間と平均時間も大幅に長くなっており、データの増加に伴って徐々に長くなっているわけではありません。このことから、ネットワークまたはグリッドによる要求の処理能力のどこかでキャパシティを超えた可能性があります。

b. どのサイズのオブジェクトが前日に読み出されていたかを1時間単位で確認するには、sizeオプションを追加します (`-s`）をコマンドに追加します。

```
grep SGET audit.log | audit-sum -gt 1H -s
```

```
  message group           count       min(B)          max(B)
average(B)
  =============           =====     ========        ========
============
  2019-09-05T00            7591        0.040        1481.867
1.976
  2019-09-05T01            4173        0.043        1740.290
2.062
  2019-09-05T02           20142        0.083        1274.961
2.303
  2019-09-05T03           57591        0.912        1383.867
1.182
  2019-09-05T04          124171        0.730        1740.290
1.528
  2019-09-05T05          420182        0.875        4274.511
2.398
  2019-09-05T06         1220371        0.691  5663711385.961
51.328
  2019-09-05T07          527142        0.130        1974.228
2.147
  2019-09-05T08          384173        0.625        1740.290
1.878
  2019-09-05T09           27591        0.689        1481.867
1.354
```

この結果から、読み出しトラフィックの量が最大に達したときに、非常に大容量の読み出しが発生したことがわかります。

c. 詳細を確認するには、を使用します `audit-explain` その時間にすべてのSGET処理を確認するためのツール：

```
grep 2019-09-05T06 audit.log | grep SGET | audit-explain | less
```

grepコマンドの出力が多くの行になると予想される場合は、を追加します `less` 監査ログファイルの内容を一度に1ページ（1画面）表示するコマンド。

5. バケットに対する SPUT 処理にオブジェクトに対する SPUT 処理よりも時間がかかっているかどうかを確認するには、次の手順を実行します。

a. 最初にを使用します `-go` オプション。オブジェクト処理とバケット処理でメッセージをグループ化します。

```
grep SPUT sample.log | audit-sum -go
```

```
  message group            count     min(sec)        max(sec)
average(sec)
  =============            =====     ========        ========
============
  SPUT.bucket                  1        0.125           0.125
0.125
  SPUT.object                 12        0.025           1.019
0.236
```

上記の結果から、バケットに対する SPUT 処理とオブジェクトに対する SPUT 処理でパフォーマンス特性が異なることがわかります。

b. SPUT処理に最も時間がかかっているバケットを特定するには、を使用します `-gb` オプション。バケットごとにメッセージをグループ化します。

```
grep SPUT audit.log | audit-sum -gb
```

```
  message group                  count     min(sec)        max(sec)
average(sec)
  =============                  =====     ========        ========
============
  SPUT.cho-non-versioning        71943        0.046        1770.563
1.571
  SPUT.cho-versioning            54277        0.047        1736.633
1.415
  SPUT.cho-west-region           80615        0.040          55.557
1.329
  SPUT.ldt002                  1564563        0.011          51.569
0.361
```

c. SPUTオブジェクトのサイズが最も大きいバケットを特定するには、両方を使用します `-gb` および `-s` オプション：

```
grep SPUT audit.log | audit-sum -gb -s
```

```
  message group                    count       min(B)          max(B)
average(B)
  =============                    =====     ========        ========
============
  SPUT.cho-non-versioning          71943        2.097        5000.000
21.672
  SPUT.cho-versioning              54277        2.097        5000.000
21.120
  SPUT.cho-west-region             80615        2.097         800.000
14.433
  SPUT.ldt002                    1564563        0.000         999.972
0.352
```

関連情報

"audit-explainツールの使用"

監査メッセージの形式

## StorageGRID システム内でやり取りされる監査メッセージには、すべてのメッセージに共通の標準情報と、報告対象のイベントまたはアクティビティを説明する固有のコンテンツが含まれます。

によって提供された概要情報の場合 `audit-explain` および `audit-sum` ツールで十分ではありません。すべての監査メッセージの一般的な形式を把握するには、このセクションを参照してください。

以下は、監査ログファイルに記録されている監査メッセージの例です。

```
2014-07-17T03:50:47.484627
[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP(F
C32):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265006
03516]]
```

各監査メッセージには、一連の属性要素で構成されます。文字列全体が角かっこで囲まれます（`[ ]`）、および文字列内の各属性要素には、次の特性があります。

- 角かっこで囲まれています `[ ]`
- 文字列で導入されます `AUDT`を指定します
- 前後に区切り記号（カンマやスペース）がない
- 改行文字で終了します `\n`

各要素には、次の形式で報告される属性コード、データ型、および値が含まれます。

```
[ATTR(type):value][ATTR(type):value]...
[ATTR(type):value]\n
```

メッセージ内の属性要素の数は、メッセージのイベントタイプによって異なります。属性要素は特定の順序でリストされません。

次に、属性要素について説明します。

- `ATTR` は、報告される属性の4文字のコードです。すべての監査メッセージに共通する属性とイベント固有の属性があります。
- `type` は、UI64、FC32など、値のプログラミングデータ型の4文字の識別子です。タイプはかっこで囲まれます `( )`。
- `value` は属性の内容で、通常は数値またはテキスト値です。値の前には常にコロンが付きます (`:`）。データタイプCSTRの値は二重引用符で囲まれます `" "`。

関連情報

"audit-explainツールの使用"

"audit-sumツールを使用する"

"監査メッセージ"

"監査メッセージの共通要素"

"データ型"

"監査メッセージの例"

データ型

## 監査メッセージ内の情報の格納にはさまざまなデータタイプが使用されます。

| を入力します | 説明 |
|---|---|
| UI32 | 符号なし長整数（ 32 ビット）。 0~4 、 294 、 967 、 295 の数値を格納できます。 |
| UI64 | 符号なし倍精度長整数（ 64 ビット）。 0~18 、 446 、 744 、 073 、 709 、 551 、 615 の数値を格納できます。 |
| FC32 | 4 文字の定数。 "ABCD" などの 4 つの ASCII 文字で表される 32 ビットの符号なし整数値です。 |
| iPad | IP アドレスに使用されます。 |

| を入力します | 説明 |
| --- | --- |
| CSTR | UTF-8 文字の可変長アレイです。文字は次の方法でエスケープできます。<br>• バックスラッシュは \\ 。<br>• 復帰文字は \r です<br>• 二重引用符は \" 。<br>• 改行（新しい行）は \n です<br>• 文字は、それぞれに相当する 16 進数に置き換えることができます（ \xHH の形式、 HH は該当する文字を表す 16 進値）。 |

イベント固有のデータ

## 監査ログ内の各監査メッセージはシステムイベントに固有のデータを記録します。

開口部に続いて `[AUDT:` メッセージ自体を識別するコンテナ。次の一連の属性は、監査メッセージによって記述されるイベントまたはアクションに関する情報を提供します。以下の例では、これらの属性を強調表示しています。

```
2018-12-05T08:24:45.921845 [AUDT:[RSLT(FC32):SUCS] [] `*[TIME(UI64):11454]
[SAIP(IPAD):"10.224.0.100"] [S3AI(CSTR):"60025621595611246499"]*` `[*SACC(CSTR):"account"]
[S3AK(CSTR):"SGKH4_Nc8SO1H6w3w0nCOFCGgk__E6dYzKlumRsKJA=="]*`
`*[SUSR(CSTR):"urn:sgws:identity::60025621595611246499:root"]*` []
[SBAI(CSTR):"60025621595611246499"] [SBAC(CSTR):"account"] [S3BK(CSTR):"bucket"] []
`*[S3KY(CSTR):"object"] [CBID(UI64):0xCC128B9B9E428347]*` []
[UUID(CSTR):"B975D2CE-E4DA-4D14-8A23-1CB4B83F2CD8"] [CSIZ(UI64):30720]
[AVER(UI32):10]
[ATIM(UI64):1543998285921845] [ATYP(FC32):SHEA] [ANID(UI32):12281045]
[AMID(FC32):S3RQ]
[ATID(UI64):15552417629170647261]]
```

。 `ATYP` 要素（この例では下線付き）は、メッセージを生成したイベントを識別します。この例のメッセージには、 SHEA メッセージコード（ [ATYP （ FC32 ） ： SHEA] ）が含まれています。これは、成功した S3 HEAD 要求によってメッセージが生成されたことを示します。

関連情報

"監査メッセージの共通要素"

"監査メッセージ"

監査メッセージの共通要素

## すべての監査メッセージには、共通の要素が含まれています。

| コード | を入力します | 説明 |
| --- | --- | --- |
| AMid | FC32 | Module ID ：メッセージを生成したモジュールの 4 文字の識別子。これは、監査メッセージが生成されたコードセグメントを示します。 |
| ANID | UI32 | Node ID ：メッセージを生成したサービスに割り当てられたグリッドノード ID 。各サービスには、 StorageGRID システムの設定およびインストール時に一意の識別子が割り当てられます。この ID は変更できません。 |
| ASES | UI64 | Audit Session Identifier ：以前のリリースでは、この要素はサービスの開始後に監査システムが初期化された時間を示していました。この時間値は、オペレーティングシステムのエポック（ 1970 年 1 月 1 日 00 ： 00 ： 00 UTC ）からのマイクロ秒数で計測されていました。<br><br>• 注： * この要素は廃止され、監査メッセージには表示されなくなりました。 |
| ASQN | UI64 | Sequence Count ：以前のリリースでは、このカウンタはグリッドノード（ ANID ）上で監査メッセージが生成されるたびに増分し、サービスの再起動時にゼロにリセットされていました。<br><br>• 注： * この要素は廃止され、監査メッセージには表示されなくなりました。 |
| ATID | UI64 | Trace ID ： 1 つのイベントによってトリガーされた一連のメッセージで共有される識別子。 |
| ATIM | UI64 | Timestamp ：監査メッセージをトリガーしたイベントが生成された時刻。オペレーティングシステムのエポック（ 1970 年 1 月 1 日 00 ： 00 ： 00 UTC ）からのマイクロ秒数で計測されます。タイムスタンプをローカルの日時に変換するためのツールは、ほとんどがミリ秒に基づいています。<br><br>ログに記録されたタイムスタンプの丸めや切り捨てが必要な場合があります。の監査メッセージの先頭に表示される、人間が判読できる時間 `audit.log` file は、ISO 8601形式のATIM属性です。日付と時刻はの形式で表示されます *`YYYY-MMDDTHH:MM:SS.UUUUUU`* を参照してください `T` は、日付の時間セグメントの先頭を示すリテラル文字です。 *`UUUUUU`* はマイクロ秒です。 |
| ATYP | FC32 | Event Type ：ログに記録されるイベントの 4 文字の識別子。これは、メッセージの「ペイロード」コンテンツ、つまり含まれる属性を管理します。 |
| ビーバー | UI32 | Version ：監査メッセージのバージョン。StorageGRID ソフトウェアのバージョンアップに伴い、新しいバージョンのサービスによって新しい機能が監査レポートに組み込まれる可能性があります。このフィールドは、旧バージョンのサービスのメッセージを処理できるよう、 AMS サービスにおける下位互換性を可能にします。 |
| RSLT | FC32 | Result ：イベント、プロセス、またはトランザクションの結果。該当しないメッセージの場合は、誤ってフィルタリングされないように SUCS ではなく NONE が使用されます。 |

# 各監査メッセージには詳細な情報が含まれています。監査メッセージはすべて同じ形式です。

に表示される監査メッセージの例を次に示します `audit.log` ファイル：

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPUT
][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224144
102530435]]
```

監査メッセージには、記録されたイベントに関する情報と、監査メッセージ自体に関する情報が含まれています。

監査メッセージによって記録されているイベントは、 ATYP 属性（以下で強調表示されている部分）で識別します。

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224
144102530435]]
```

ATYP 属性の値は SPUT です。SPUT は S3 PUT トランザクションを表し、バケットへのオブジェクトの取り込みをログに記録します。

次の監査メッセージは、オブジェクトが関連付けられているバケットも示しています。

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3
KY(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):
0][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPU
T][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):157922414
4102530435]]
```

PUT イベントがいつ発生したかを調べるには、監査メッセージの先頭の世界標準時（ UTC ）のタイムスタンプを確認します。この値は、監査メッセージ自体の ATIM 属性を判読可能な形式で表したものです。

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):15792241
44102530435]]
```

ATIM は、 UNIX エポックの開始時点からの時間をマイクロ秒数で記録します。この例では、の値を指定します `1405631878959669` 2014年7月17日（木）21：17：59 UTCに変換されます。

関連情報

"SPUT ： S3 PUT"

"監査メッセージの共通要素"

## 監査メッセージとオブジェクトライフサイクル

監査メッセージは、オブジェクトの取り込み、読み出し、または削除が行われるたびに生成されます。監査ログでこれらのトランザクションを特定するには、 API 固有の（ S3 または Swift ）監査メッセージを検索します。

監査メッセージは各プロトコルに固有な識別子によってリンクされます。

| プロトコル | コード |
| --- | --- |
| S3 処理をリンクしています | S3BK （ S3 バケット）および / または S3KY （ S3 キー） |
| Swift 処理をリンクしています | WCON （ Swift コンテナ）および / または WOBJ （ Swift オブジェクト） |
| 内部処理をリンクしています | CBID （オブジェクトの内部識別子） |

監査メッセージのタイミング

グリッドノード間のタイミングの違い、オブジェクトサイズ、ネットワーク遅延などの要因により、各サービスによって生成される監査メッセージの順序はこのセクションに記載する例とは異なる場合があります。

情報ライフサイクル管理ポリシーの設定

デフォルトの ILM ポリシー（ Baseline 2 Copy ）では、オブジェクトデータは 1 回コピーされ、コピーは合計 2 つになります。3 つ以上のコピーが必要な ILM ポリシーの場合は、追加コピーごとに CBRE 、 CBSE 、

SCMT メッセージのセットが生成されます。ILM ポリシーの詳細については、情報ライフサイクル管理によるオブジェクトの管理に関する情報を参照してください。

アーカイブノード

アーカイブノードから外部アーカイブストレージシステムにオブジェクトデータを送信するときに生成される一連の監査メッセージは、 SCMT （ Store Object Commit ）メッセージがないことを除き、ストレージノードの場合と似ています。 さらに、オブジェクトデータのアーカイブコピーごとに ATCE （ Archive Object Store Begin ）メッセージと ASCE （ Archive Object Store End ）メッセージが生成されます。

アーカイブノードが外部のアーカイブストレージシステムからオブジェクトデータを読み出すときに生成される一連の監査メッセージは、ストレージノードの場合と似ていますが、オブジェクトデータのアーカイブコピーごとに ARCB （ Archive Object Retrieve Begin ）メッセージと ARCE （ Archive Object Retrieve End ）メッセージが生成される点が異なります。

アーカイブノードが外部のアーカイブストレージシステムからオブジェクトデータを削除するときに生成される一連の監査メッセージは、ストレージノードのメッセージと似ています。ただし、 SREM （ Object Store Remove ）メッセージがなく、削除要求ごとに AREM （ Archive Object Remove ）メッセージが生成される点が異なります。

関連情報

"ILM を使用してオブジェクトを管理する"

オブジェクトの取り込みトランザクション

## 監査ログでクライアントの取り込みトランザクションを特定するには、 API 固有の（ S3 または Swift ）監査メッセージを検索します。

以下の表には、取り込みトランザクション中に生成されたすべての監査メッセージが含まれているわけではなく、取り込みトランザクションをトレースするために必要なメッセージのみが含まれています。

**S3** の取り込み監査メッセージ

| コード | 名前 | 説明 | トレース | を参照してください |
|---|---|---|---|---|
| SPUT | S3 PUT トランザクション | S3 PUT 取り込みトランザクションが正常に完了しました。 | CBID 、 S3BK 、 S3KY | "SPUT ： S3 PUT" |
| ORLM の場合 | オブジェクトルールを満たしました | このオブジェクトが ILM ポリシーを満たしました。 | CBID | "ORLM ：オブジェクトルールが満たされています" |

**Swift** の取り込み監査メッセージ

| コード | 名前 | 説明 | トレース | を参照してください |
| --- | --- | --- | --- | --- |
| WPUT | Swift PUT トランザクション | Swift PUT 取り込みトランザクションが正常に完了しました。 | CBID 、 WCON 、 WOBJ | "WPUT ： Swift PUT" |
| ORLM の場合 | オブジェクトルールを満たしました | このオブジェクトが ILM ポリシーを満たしました。 | CBID | "ORLM ：オブジェクトルールが満たされています" |

例： **S3** オブジェクトの取り込み

## 以下の一連の監査メッセージは、 S3 クライアントがストレージノード（ LDR サービス）にオブジェクトを取り込んだときに生成され、監査ログに保存された監査メッセージの例です。

この例では、アクティブな ILM ポリシーに、組み込みの ILM ルール「 Make 2 Copies 」が含まれています。

> 以下の例には、トランザクション中に生成されたすべての監査メッセージが含まれているわけではなく、S3 取り込みトランザクション（ SPUT ）に関連するメッセージだけが示されています。

この例では、 S3 バケットは以前に作成済みであることを前提としています。

**SPUT ： S3 PUT**

SPUT メッセージは、特定のバケットにオブジェクトを作成する S3 PUT トランザクションが実行されたことを示します。

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):25771][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"][S3BK(CSTR):"example"]<strong
class="S3KY(CSTR):"testobject-0-
3"">[CBID(UI64):0x8EF52DF8025E63A8]</strong>[CSIZ(UI64):30720][AVER(UI32):
10]<strong
class="ATIM(UI64):150032627859669">[ATYP(FC32):SPUT]</strong>[ANID(UI32):1
2086324][AMID(FC32):S3RQ][ATID(UI64):14399932238768197038]]
```

**ORLM** ：オブジェクトルールが満たされています

ORLM メッセージは、このオブジェクトが ILM ポリシーに準拠していることを示します。メッセージには、オブジェクトの CBID と適用された ILM ルールの名前が含まれています。

レプリケートオブジェクトの場合、 LOCS フィールドにはオブジェクトの場所の LDR ノード ID とボリューム ID が記録されます。

```
2019-07-17T21:18:31.230669[AUDT:
<strong>[CBID(UI64):0x50C4F7AC2BC8EDF7]</strong> [RULE(CSTR):"Make 2
Copies"][STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"0B344E18-98ED-4F22-
A6C8-A93ED68F8D3F"]<strong class="LOCS(CSTR): *"CLDI 12828634
2148730112">[RSLT(FC32):SUCS][AVER(UI32):10] [ATYP(FC32):ORLM]</strong>
[ATIM(UI64):1563398230669][ATID(UI64):15494889725796157557][ANID(UI32):131
00453][AMID(FC32):BCMS]]
```

イレイジャーコーディングオブジェクトの場合、 LOCS フィールドには、イレイジャーコーディングのプロファイル ID とグループ ID が記録されます

```
2019-02-23T01:52:54.647537
[AUDT:[CBID(UI64):0xFA8ABE5B5001F7E2][RULE(CSTR):"EC_2_plus_1"][STAT(FC32)
:DONE][CSIZ(UI64):10000][UUID(CSTR):"E291E456-D11A-4701-8F51-
D2F7CC9AFECA"][LOCS(CSTR): "CLEC 1 A471E45D-A400-47C7-86AC-12E77F229831"]
[RSLT(FC32):SUCS][AVER(UI32):10][ATYP(FC32):ORLM][ANID(UI32):12355278][AMI
D(FC32):ILMX][ATID(UI64):4168559046473725560]]
```

Path フィールドには、使用される API に応じて、 S3 バケットとキーの情報または Swift コンテナとオブジェクトの情報が記録されます。

```
2019-09-15.txt:2018-01-24T13:52:54.131559
[AUDT:[CBID(UI64):0x82704DFA4C9674F4][RULE(CSTR):"Make 2
Copies"][STAT(FC32):DONE][CSIZ(UI64):3145729][UUID(CSTR):"8C1C9CAC-22BB-
4880-9115-
CE604F8CE687"][PATH(CSTR):"frisbee_Bucket1/GridDataTests151683676324774_1_
1vf9d"][LOCS(CSTR):"CLDI 12525468, CLDI
12222978"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1568555574559][ATYP(
FC32):ORLM][ANID(UI32):12525468][AMID(FC32):OBDI][ATID(UI64):3448338865383
69336]]
```

オブジェクトの削除トランザクション

## 監査ログでオブジェクトの削除トランザクションを特定するには、 API 固有の（ S3 および Swift ）監査メッセージを検索します。

以下の表には、削除トランザクション中に生成されたすべての監査メッセージが含まれているわけではなく、削除トランザクションをトレースするために必要なメッセージのみが含まれています。

**S3** の削除監査メッセージ

| コード | 名前 | 説明 | トレース | を参照してください |
|---|---|---|---|---|
| SDEL | S3 削除 | バケットからのオブジェクトの削除が要求されました。 | CBID 、 S3KY | "SDEL ： S3 DELETE" |

**Swift** の削除監査メッセージ

| コード | 名前 | 説明 | トレース | を参照してください |
|---|---|---|---|---|
| WDEL | Swift の削除 | コンテナまたはコンテナからのオブジェクトの削除が要求されました。 | CBID 、 WOBJ | "WDEL ： Swift の削除" |

例： **S3** オブジェクトの削除

## S3 クライアントがストレージノード（ LDR サービス）からオブジェクトを削除すると、監査メッセージが生成されて監査ログに保存されます。

以下の例には、削除トランザクション中に生成されたすべての監査メッセージが含まれているわけではなく、S3 の削除トランザクション（ SDEL ）に関連するメッセージだけが示されています。

**SDEL ： S3** 削除

オブジェクトの削除は、クライアントが LDR サービスに DELETE Object 要求を送信した時点で始まります。メッセージには、オブジェクトの削除元のバケットと、オブジェクトの識別に使用される S3 キーが含まれています。

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):14316][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"] <strong>[S3BK(CSTR):"example"][S3KY(CSTR):"testobject-0-
7"][CBID(UI64):0x339F21C5A6964D89]</strong>
[CSIZ(UI64):30720][AVER(UI32):10][ATIM(UI64):150032627859669]
<strong>[ATYP(FC32):SDEL]</strong>[ANID(UI32):12086324][AMID(FC32):S3RQ][A
TID(UI64):4727861330952970593]]
```

オブジェクトの読み出しトランザクション

## 監査ログでオブジェクトの読み出しトランザクションを特定するには、 API 固有の（ S3 および Swift ）監査メッセージを検索します。

以下の表には、読み出しトランザクション中に生成されたすべての監査メッセージが含まれているわけではなく、読み出しトランザクションをトレースするために必要なメッセージのみが含まれています。

**S3** の読み出し監査メッセージ

| コード | 名前 | 説明 | トレース | を参照してください |
|---|---|---|---|---|
| SGET | S3 GET | バケットからのオブジェクトの読み出しが要求されました。 | CBID 、 S3BK 、 S3KY | "SGET ： S3 GET" |

**Swift** の読み出し監査メッセージ

| コード | 名前 | 説明 | トレース | を参照してください |
|---|---|---|---|---|
| wget | Swift GET | コンテナからのオブジェクトの読み出しが要求されました。 | CBID 、 WCON 、 WOBJ | "wget ： Swift GET" |

例： **S3** オブジェクトの読み出し

## S3 クライアントがストレージノード（ LDR サービス）からオブジェクトを読み出すと、監査メッセージが生成されて監査ログに保存されます。

以下の例には、トランザクション中に生成されたすべての監査メッセージが含まれているわけではなく、S3 読み出しトランザクション（ SGET ）に関連するメッセージだけが示されています。

### SGET ： S3 GET

オブジェクトの読み出しは、クライアントが LDR サービスに GET Object 要求を送信した時点で開始されます。メッセージには、オブジェクトの読み出し元のバケットと、オブジェクトの識別に使用される S3 キーが含まれています。

```
2017-09-20T22:53:08.782605
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):47807][SAIP(IPAD):"10.96.112.26"][S3AI(
CSTR):"43979298178977966408"][SACC(CSTR):"s3-account-
a"][S3AK(CSTR):"SGKHt7GzEcu0yXhFhT_rL5mep4nJt1w75GBh-
O_FEw=="][SUSR(CSTR):"urn:sgws:identity::43979298178977966408:root"][SBAI(
CSTR):"43979298178977966408"][SBAC(CSTR):"s3-account-a"]
[S3BK(CSTR):"bucket-
anonymous"][S3KY(CSTR):"Hello.txt"][CBID(UI64):0x83D70C6F1F662B02][CSIZ(UI
64):12][AVER(UI32):10][ATIM(UI64):1505947988782605][ATYP(FC32):SGET][ANID(
UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):17742374343649889669]]
```

バケットポリシーで許可されている場合、クライアントはオブジェクトを匿名で読み出したり、別のテナントアカウントが所有しているバケットからオブジェクトを読み出すことができます。監査メッセージには、このような匿名要求およびクロスアカウント要求を追跡できるように、バケット所有者のテナントアカウントに関する情報が含まれています。

次のメッセージ例では、クライアントは、自身が所有していないバケットに格納されているオブジェクトに対する GET Object 要求を送信します。SBAI と SBAC の値にはバケット所有者のテナントアカウント ID と名前が記録されますが、これは S3AI および SACC に記録されているクライアントのテナントアカウント ID および名前とは異なります。

```
2017-09-20T22:53:15.876415
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):53244][SAIP(IPAD):"10.96.112.26"]
<strong>[S3AI(CSTR):"17915054115450519830"][SACC(CSTR):"s3-account-
b"]</strong>[S3AK(CSTR):"SGKHpoblWlP_kBkqSCbTi754Ls8lBUog67I2LlSiUg=="]<st
rong
class="SUSR(CSTR):"urn:sgws:identity::17915054115450519830:root"">[SBAI(CS
TR):"43979298178977966408"][SBAC(CSTR):"s3-account-
a"]</strong>[S3BK(CSTR):"bucket-
anonymous"][S3KY(CSTR):"Hello.txt"][CBID(UI64):0x83D70C6F1F662B02][CSIZ(UI
64):12][AVER(UI32):10][ATIM(UI64):1505947995876415][ATYP(FC32):SGET][ANID(
UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):68887802475156249O2]]
```

メタデータの更新メッセージです

## S3 クライアントがオブジェクトのメタデータを更新すると、監査メッセージが生成されます。

**S3** メタデータの更新監査メッセージ

| コード | 名前 | 説明 | トレース | を参照してください |
|---|---|---|---|---|
| SUPD | S3 メタデータが更新されました | S3 クライアントが取り込まれたオブジェクトのメタデータを更新すると生成されます。 | CBID 、 S3KY 、 HTRH | "SUPD ： S3 メタデータが更新されました" |

例： **S3** メタデータの更新

## 次の例は、既存の S3 オブジェクトのメタデータを更新するトランザクションの成功を示しています。

**SUPD ： S3** メタデータの更新

S3クライアントが、指定されたメタデータを更新する要求（SUPD）を実行します (`x-amz-meta-*`）をクリックします。この例では、要求ヘッダーは監査プロトコルヘッダー(**Configuration> Monitoring> Audit**)として設定されているため、HTRHフィールドに含まれています。

```
2017-07-11T21:54:03.157462
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):17631][SAIP(IPAD):"10.96.100.254"]
[HTRH(CSTR):"{\"accept-encoding\":\"identity\",\"authorization\":\"AWS
LIUF17FGJARQHPY2E761:jul/hnZs/uNY+aVvV0lTSYhEGts=\",
\"content-length\":\"0\",\"date\":\"Tue, 11 Jul 2017 21:54:03
GMT\",\"host\":\"10.96.99.163:18082\",
\"user-agent\":\"aws-cli/1.9.20 Python/2.7.6 Linux/3.13.0-119-generic
botocore/1.3.20\",
\"x-amz-copy-source\":\"/testbkt1/testobj1\",\"x-amz-metadata-
directive\":\"REPLACE\",\"x-amz-meta-city\":\"Vancouver\"}"]
[S3AI(CSTR):"20956855414285633225"][SACC(CSTR):"acct1"][S3AK(CSTR):"SGKHyy
v9ZQqWRbJSQc5vI7mgioJwrdplShE02AUaww=="]
[SUSR(CSTR):"urn:sgws:identity::20956855414285633225:root"]
[SBAI(CSTR):"20956855414285633225"][SBAC(CSTR):"acct1"][S3BK(CSTR):"testbk
t1"]
[S3KY(CSTR):"testobj1"][CBID(UI64):0xCB1D5C213434DD48][CSIZ(UI64):10][AVER
(UI32):10]
[ATIM(UI64):1499810043157462][ATYP(FC32):SUPD][ANID(UI32):12258396][AMID(F
C32):S3RQ]
[ATID(UI64):8987436599021955788]]
```

関連情報

"監査メッセージレベルの変更"

## 監査メッセージ

システムから返される監査メッセージの詳細について、次のセクションで説明します。各監査メッセージをメッセージが表すアクティビティのクラスでグループ化して、表に記載します。これらの分類は、監査対象のアクティビティのタイプを理解し、必要な監査メッセージフィルタリングのタイプを選択する場合に役立ちます。

監査メッセージは、 4 文字のコードでアルファベット順に一覧表示されます。アルファベット順に記載されているため、特定のメッセージに関する情報を簡単に見つけることができます。

この章で使用されている 4 文字のコードは、次のサンプルメッセージに示すように、監査メッセージ内にある ATYP 値です。

```
2014-07-17T03:50:47.484627
\[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][<stro
ng>ATYP\(FC32\):SYSU</strong>][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(
UI64):9445736326500603516]]
```

関連情報

"監査メッセージ"

"監査メッセージレベルの変更"

監査メッセージのカテゴリ

監査メッセージの各カテゴリについて理解しておく必要があります。これらのグループは、メッセージが表すアクティビティのクラスに基づいて分類されます。

システム監査メッセージ

システム監査カテゴリに属する監査メッセージについて十分に理解しておく必要があります。潜在的な問題に対処できるよう、監査システム自体、グリッドノードの状態、システム全体のタスクアクティビティ（グリッドタスク）、およびサービスバックアップ処理に関連するイベントについて生成されます。

| コード | メッセージのタイトルと概要 | を参照してください |
|---|---|---|
| ECOC | Corrupt Erasure Coded Data Fragment ：イレイジャーコーディングされたデータフラグメントの破損が検出されたことを示します。 | "ECOC ：イレイジャーコーディングされたデータフラグメントが破損しています" |
| ETAF | Security Authentication Failed ： Transport Layer Security （ TLS ）を使用した接続試行が失敗しました。 | "ETAF ：セキュリティ認証に失敗しました" |
| GNRG | GNDS Registration ：サービスが StorageGRID システムに自身に関する情報を更新または登録しました。 | "GNRG ： GNDS 登録" |
| GNUR | GNDS Unregistration ：サービスが StorageGRID システムから自身の登録を解除しました。 | "GNUR ： GNDS 登録解除" |
| GTED | Grid Task Ended ： CMN サービスがグリッドタスクの処理を完了しました。 | "GTED ： Grid タスクが終了しました" |
| GTSt | Grid Task Started ： CMN サービスがグリッドタスクの処理を開始しました。 | "GTSt ： Grid タスクが開始されました" |
| GTSU | Grid Task Submitted ：グリッドタスクが CMN サービスに送信されました。 | "GTSU ： Grid タスクが送信されました" |

| コード | メッセージのタイトルと概要 | を参照してください |
| --- | --- | --- |
| IDEL | ILM Initiated Delete ：この監査メッセージは、 ILM がオブジェクトを削除する処理を開始すると生成されます。 | "IDEL ： ILM Initiated Delete" |
| LCU | 上書きされたオブジェクトのクリーンアップ。この監査メッセージは、ストレージスペースを解放するために上書きされたオブジェクトが自動的に削除されたときに生成されます。 | "LKCU: 上書きされたオブジェクトのクリーンアップ" |
| LLST | Location Lost ：この監査メッセージは、場所が失われたときに生成されます。 | "LLST ：ロケーションが失われました" |
| OLST | Object Lost ：要求されたオブジェクトが StorageGRID システム内に見つかりません。 | "OLST: システムが損失オブジェクトを検出しました" |
| ORLM の場合 | Object Rules Met ：オブジェクトデータが ILM ルールに沿って格納されました。 | "ORLM ：オブジェクトルールが満たされています" |
| サッド | Security Audit Disable ：監査メッセージのロギングがオフになりました。 | "SADD ：セキュリティ監査無効" |
| Sade 社 | Security Audit Enable ：監査メッセージのロギングが再開されました。 | "Sade ：セキュリティ監査を有効にします" |
| SVRF | Object Store Verify Fail ：コンテンツブロックが検証チェックに失敗しました。 | "SVRF ：オブジェクトストアの検証に失敗しました" |
| SVRU の場合 | Object Store Verify Unknown ：オブジェクトストアで想定外のオブジェクトデータが検出されました。 | "SVRU ：オブジェクトストア検証が不明です" |
| SYSD | Node Stop ：シャットダウンが要求されました。 | "SYSD ：ノード停止" |
| SYST | Node Stopping ：サービスが正常な停止を開始しました。 | "SYST ：ノードを停止しています" |

| コード | メッセージのタイトルと概要 | を参照してください |
| --- | --- | --- |
| SYSU | Node Start ：サービスが開始されました。前回のシャットダウンのタイプがメッセージに示されます。 | "SYSU ：ノードが開始されました" |
| VLST | User Initiated Volume Lost `/proc/CMSI/Volume_Lost` コマンドが実行されました。 | "VLST ：ユーザーが開始したボリュームが失われました" |

関連情報

"LKCU: 上書きされたオブジェクトのクリーンアップ"

オブジェクトストレージ監査メッセージ

オブジェクトストレージ監査カテゴリに属する監査メッセージについて十分に理解しておく必要があります。StorageGRID システム内のオブジェクトのストレージと管理に関連するイベントを示します。オブジェクトの格納と読み出し、グリッドノードからグリッドノードへの転送、および検証が含まれます。

| コード | 説明 | を参照してください |
| --- | --- | --- |
| APCT | Archive Purge from Cloud-Tier ：S3 API を使用して StorageGRID に接続する外部アーカイブストレージシステムから、アーカイブされたオブジェクトデータが削除されました。 | "APCT ：クラウド階層からのアーカイブの削除" |
| ARCB | Archive Object Retrieve Begin ：ARC サービスが、外部アーカイブストレージシステムからオブジェクトデータの読み出しを開始しました。 | "ARCB ：アーカイブオブジェクトの読み出しが開始されました" |
| ARCE | Archive Object Retrieve End ：オブジェクトデータが外部アーカイブストレージシステムから読み出され、 ARC サービスが読み出し処理のステータスをレポートします。 | "ARCE ：アーカイブオブジェクトの読み出しが終了しました" |
| ARCT | Archive Retrieve from Cloud-Tier ：S3 API を使用して StorageGRID に接続する外部アーカイブストレージシステムから、アーカイブされたオブジェクトデータが読み出されました。 | "ARCT ：クラウド階層からアーカイブを取得します" |

| コード | 説明 | を参照してください |
| --- | --- | --- |
| AREM | Archive Object Remove ：外部アーカイブストレージシステムからのコンテンツブロックの削除が成功または失敗しました。 | "AREM ：アーカイブオブジェクトの削除" |
| ASCE | Archive Object Store End ：コンテンツブロックが外部アーカイブストレージシステムに書き込まれ、ARC サービスが書き込み処理のステータスをレポートします。 | "ASCE ：アーカイブオブジェクトストアの終了" |
| ▽ SCT 。△ | Archive Store Cloud-Tier ： S3 API を使用して StorageGRID に接続する外部アーカイブストレージシステムに、オブジェクトデータが格納されました。 | "ASCT ：アーカイブストアのクラウド階層" |
| ATCE | Archive Object Store Begin ：外部アーカイブストレージへのコンテンツブロックの書き込みが開始されました。 | "ATCE ：アーカイブオブジェクトストアが開始されました" |
| AVCC の場合 | Archive Validate Cloud-Tier Configuration ：指定されたアカウントおよびバケットの設定の検証に成功または失敗しました。 | "AVCC ：アーカイブによってクラウド階層の構成を検証" |
| CBSE | Object Send End ：ソースエンティティが、グリッドノードからグリッドノードへのデータ転送処理を完了しました。 | "CBSE ：オブジェクト送信終了" |
| CBRE | Object Receive End ：デスティネーションエンティティが、グリッドノードからグリッドノードへのデータ転送処理を完了しました。 | "CBRE ：オブジェクト受信終了" |
| SCMT | Object Store Commit ：コンテンツブロックの格納と検証がすべて完了し、要求可能な状態になりました。 | "SCMT ：オブジェクトストアのコミット" |
| SREM | Object Store Remove ：コンテンツブロックがグリッドノードから削除され、直接要求できなくなりました。 | "SREM ：オブジェクトストアの削除" |

## クライアント読み取り監査メッセージは、 S3 または Swift クライアントアプリケーションがオブジェクトを読み出す要求を行うときに記録されます。

| コード | 説明 | によって使用されます | を参照してください |
|---|---|---|---|
| SGET | S3 GET ：バケット内のオブジェクトを読み出しまたはリストアップするトランザクションの成功をログに記録します。<br><br>• 注：トランザクションがサブリソースで動作している場合、監査メッセージには S3SR フィールドが含まれます。 | S3 クライアント | "SGET ： S3 GET" |
| Shea | S3 HEAD ：オブジェクトまたはバケットの存在を確認するトランザクションの成功をログに記録します。 | S3 クライアント | "Shea ： S3 ヘッド" |
| wget | Swift GET ：コンテナ内のオブジェクトを読み出しまたはリストアップするトランザクションの成功をログに記録します。 | Swift クライアント | "wget ： Swift GET" |
| WHEA | Swift HEAD ：オブジェクトまたはコンテナの存在を確認するトランザクションの成功をログに記録します。 | Swift クライアント | "WHEA ： Swift ヘッド" |



## クライアント書き込み監査メッセージは、 S3 または Swift クライアントアプリケーションがオブジェクトを作成または変更する要求を行うときに記録されます。

| コード | 説明 | によって使用されます | を参照してください |
|---|---|---|---|
| OWR | Object Overwrite ：あるオブジェクトを別のオブジェクトで上書きするトランザクションをログに記録します。 | S3 クライアント<br><br>Swift クライアント | "OVWR ：オブジェクトを上書き" |

| コード | 説明 | によって使用されます | を参照してください |
| --- | --- | --- | --- |
| SDEL | S3 DELETE ：オブジェクトまたはバケットを削除するトランザクションの成功をログに記録します。<br><br>• 注：トランザクションがサブリソースで動作している場合、監査メッセージには S3SR フィールドが含まれます。 | S3 クライアント | "SDEL ： S3 DELETE" |
| SPO | S3 POST ：オブジェクトを AWS Glacier ストレージからクラウドストレージプールにリストアするトランザクションの成功をログに記録します。 | S3 クライアント | "SPO ： S3 POST" |
| SPUT | S3 PUT ：オブジェクトまたはバケットを新規に作成するトランザクションの成功をログに記録します。<br><br>• 注：トランザクションがサブリソースで動作している場合、監査メッセージには S3SR フィールドが含まれます。 | S3 クライアント | "SPUT ： S3 PUT" |
| SUPD | S3 Metadata Updated ：既存のオブジェクトまたはバケットのメタデータを更新するトランザクションの成功をログに記録します。 | S3 クライアント | "SUPD ： S3 メタデータが更新されました" |
| WDEL | Swift DELETE ：オブジェクトまたはコンテナを削除するトランザクションの成功をログに記録します。 | Swift クライアント | "WDEL ： Swift の削除" |

| コード | 説明 | によって使用されます | を参照してください |
| --- | --- | --- | --- |
| WPUT | Swift PUT ：オブジェクトまたはコンテナを新規に作成するトランザクションの成功をログに記録します。 | Swift クライアント | "WPUT ： Swift PUT" |

管理監査メッセージ

## 管理カテゴリでは、管理 API に対するユーザ要求がログに記録されます。

| コード | メッセージのタイトルと概要 | を参照してください |
| --- | --- | --- |
| MGAU | 管理 API 監査メッセージ：ユーザ要求のログ。 | "MGAU ：管理監査メッセージ" |

監査メッセージ

## システムイベントが発生すると、StorageGRID システムは監査メッセージを生成して監査ログに記録します。

**APCT** ：クラウド階層からのアーカイブの削除

## このメッセージは、 S3 API を使用して StorageGRID に接続する外部アーカイブストレージシステムから、アーカイブされたオブジェクトデータが削除されたときに生成されます。

| コード | フィールド | 説明 |
| --- | --- | --- |
| CBID | コンテンツブロック ID | 削除されたコンテンツブロックの一意の識別子。 |
| CSIZ | コンテンツサイズ（ Content Size ） | オブジェクトのサイズ（バイト単位）。常に 0 を返します。 |
| RSLT | 結果コード | 成功（ SUCS ）、またはバックエンドによって報告されたエラーが返されます。 |
| SUID | Storage Unique Identifier の略 | オブジェクトが削除されたクラウド階層の一意の識別子（ UUID ）。 |

**ARCB** ：アーカイブオブジェクトの読み出しが開始されました

## このメッセージは、アーカイブされたオブジェクトデータの読み出し要求が送信されて

読み出しプロセスが開始されたときに生成されます。読み出し要求はすぐに処理されますが、順序を変更してテープなどのリニアなメディアからの読み出し効率を高めることができます。

| コード | フィールド | 説明 |
| --- | --- | --- |
| CBID | コンテンツブロック ID | 外部アーカイブストレージシステムから読み出すコンテンツブロックの一意の識別子。 |
| RSLT | 結果 | アーカイブ読み出しプロセスを開始した結果を示します。現在定義されている値： SUCS ：コンテンツ要求が受信され、読み出しのためにキューに登録されました。 |

この監査メッセージにはアーカイブ読み出しの時間が記録されます。メッセージを対応する ARCE 終了メッセージと照合することで、アーカイブ読み出しの所要時間および処理が成功したかどうかを判断できます。

**ARCE** ：アーカイブオブジェクトの読み出しが終了しました

このメッセージは、アーカイブノードが外部アーカイブストレージシステムからオブジェクトデータを読み出す試行が完了したときに生成されます。成功した場合、メッセージには、要求されたオブジェクトデータがアーカイブ先から完全に読み取られ、検証に成功したことが示されます。読み出しと検証が完了すると、オブジェクトデータは要求元のサービスに配信されます。

| コード | フィールド | 説明 |
| --- | --- | --- |
| CBID | コンテンツブロック ID | 外部アーカイブストレージシステムから読み出すコンテンツブロックの一意の識別子。 |
| VLID | ボリューム識別子 | データがアーカイブされたボリュームの識別子。コンテンツのアーカイブの場所が見つからない場合は、ボリューム ID 0 が返されます。 |

| コード | フィールド | 説明 |
| --- | --- | --- |
| RSLT | 取得結果 | アーカイブ読み出しプロセスの完了ステータス：<br>• SUCS ：成功しました<br>• VRFL ：失敗（オブジェクトの検証に失敗）<br>• ARUN ：失敗（外部アーカイブストレージシステムを使用できない）<br>• CANC ：失敗（読み出し処理がキャンセルされた）<br>• GERR ：失敗（一般的なエラー） |

このメッセージと対応する ARCB メッセージを組み合わせることで、アーカイブ読み出しの所要時間を特定できます。このメッセージは読み出しが成功したかどうかを示し、失敗した場合には原因 がコンテンツブロックの読み出しに失敗したことを示します。

**ARCT** ：クラウド階層からアーカイブを取得します

このメッセージは、 S3 API を使用して StorageGRID に接続する外部アーカイブストレージシステムから、アーカイブされたオブジェクトデータが読み出されたときに生成されます。

| コード | フィールド | 説明 |
| --- | --- | --- |
| CBID | コンテンツブロック ID | 読み出されたコンテンツブロックの一意の識別子。 |
| CSIZ | コンテンツサイズ（ Content Size ） | オブジェクトのサイズ（バイト単位）。読み出しが成功した場合にのみ正確な値が表示されます。 |
| RSLT | 結果コード | 成功（ SUCS ）、またはバックエンドによって報告されたエラーが返されます。 |
| SUID | Storage Unique Identifier の略 | 外部アーカイブストレージシステムの一意の識別子（ UUID ）。 |
| 時間 | 時間 | 要求の合計処理時間（マイクロ秒）。 |

**AREM** ：アーカイブオブジェクトの削除

Archive Object Remove 監査メッセージは、アーカイブノードからのコンテンツブロックの削除が成功または失敗したことを示します。アーカイブノードが StorageGRID がオブジェクトの場所を解放したことを外部アーカイブストレージシステムに通知した場合、結果は成功です。オブジェクトが外部アーカイブストレージシステムから削除されるかどうかは、システムのタイプと構成によって異なります。

| コード | フィールド | 説明 |
| --- | --- | --- |
| CBID | コンテンツブロック ID | 外部アーカイブメディアシステムから読み出すコンテンツブロックの一意の識別子。 |
| VLID | ボリューム識別子 | オブジェクトデータがアーカイブされていたボリュームの識別子。 |
| RSLT | 結果 | アーカイブ削除プロセスの完了ステータス：<br>• SUCS ：成功しました<br>• ARUN ：失敗（外部アーカイブストレージシステムを使用できない）<br>• GERR ：失敗（一般的なエラー） |

**ASCE** ：アーカイブオブジェクトストアの終了

このメッセージは、外部アーカイブストレージシステムへのコンテンツブロックの書き込みが終了したことを示します。

| コード | フィールド | 説明 |
| --- | --- | --- |
| CBID | Content Block Identifier の略 | 外部アーカイブストレージシステムに格納されているコンテンツブロックの識別子。 |
| VLID | ボリューム識別子 | オブジェクトデータの書き込み先のアーカイブボリュームの一意の識別子。 |

| コード | フィールド | 説明 |
| --- | --- | --- |
| VREN | 検証が有効です | コンテンツブロックに対して検証が実行されるかどうかを示します。現在定義されている値は次のとおり<br>• VENA ：検証が有効になっています<br>• VDSA ：検証は無効です |
| MCLS | 管理クラス | コンテンツブロックが割り当てられている TSM 管理クラスを識別する文字列（該当する場合）。 |
| RSLT | 結果 | アーカイブプロセスの結果を示します。現在定義されている値は次のとおり<br>• SUCS ：成功（アーカイブプロセスが成功）<br>• OFFL ：失敗（アーカイブがオフライン）<br>• VRFL ：失敗（オブジェクトの検証に失敗）<br>• ARUN ：失敗（外部アーカイブストレージシステムを使用できない）<br>• GERR ：失敗（一般的なエラー） |

この監査メッセージは、指定されたコンテンツブロックが外部アーカイブストレージシステムに書き込まれたことを意味します。書き込みが失敗した場合は、どこで失敗したかを示す基本的なトラブルシューティング情報が結果として記録されます。より詳細な失敗原因については、 StorageGRID システムでアーカイブノードの属性を調べてください。

**ASCT** ：アーカイブストアのクラウド階層

## このメッセージは、 S3 API を使用して StorageGRID に接続する外部アーカイブストレージシステムに、アーカイブされたオブジェクトデータが格納されたときに生成されます。

| コード | フィールド | 説明 |
| --- | --- | --- |
| CBID | コンテンツブロック ID | 読み出されたコンテンツブロックの一意の識別子。 |

| コード | フィールド | 説明 |
| --- | --- | --- |
| CSIZ | コンテンツサイズ（ Content Size ） | オブジェクトのサイズ（バイト単位）。 |
| RSLT | 結果コード | 成功（ SUCS ）、またはバックエンドによって報告されたエラーが返されます。 |
| SUID | Storage Unique Identifier の略 | コンテンツ格納先クラウド階層の一意の識別子（ UUID ）。 |
| 時間 | 時間 | 要求の合計処理時間（マイクロ秒）。 |

**ATCE** ：アーカイブオブジェクトストアが開始されました

このメッセージは、外部アーカイブストレージへのコンテンツブロックの書き込みが開始されたことを示します。

| コード | フィールド | 説明 |
| --- | --- | --- |
| CBID | コンテンツブロック ID | アーカイブされるコンテンツブロックの一意の識別子。 |
| VLID | ボリューム識別子 | コンテンツブロックの書き込み先のボリュームの一意の識別子。処理に失敗した場合は 0 が返されます。 |
| RSLT | 結果 | コンテンツブロックの転送結果を示します。現在定義されている値は次のとおり<br>• SUCS ：成功（コンテンツブロックは正常に格納されました）<br>• EXIS ：無視（コンテンツブロックはすでに格納されています）<br>• ISFD ：失敗（ディスクスペースが足りません）<br>• STER ：失敗（ CBID の格納エラー）<br>• OFFL ：失敗（アーカイブがオフライン）<br>• GERR ：失敗（一般的なエラー） |

**AVCC** ：アーカイブによってクラウド階層の構成を検証

このメッセージは、クラウド階層 - Simple Storage Service （ S3 ）ターゲットタイプの構成設定が検証されたときに生成されます。

| コード | フィールド | 説明 |
| --- | --- | --- |
| RSLT | 結果コード | 成功（ SUCS ）、またはバックエンドによって報告されたエラーが返されます。 |
| SUID | Storage Unique Identifier の略 | 検証対象の外部アーカイブストレージシステムに関連付けられている UUID 。 |

**CBRB** ：オブジェクト受信が開始されました

通常のシステム運用中は、データへのアクセスおよびデータのレプリケートと保持が行われる際に、異なるノード間でコンテンツブロックが継続的に転送されます。このメッセージは、あるノードから別のノードへのコンテンツブロックの転送が開始したときに転送先のエンティティによって生成されます。

| コード | フィールド | 説明 |
| --- | --- | --- |
| CNID | 接続識別子 | ノード間のセッション / 接続の一意の識別子。 |
| CBID | Content Block Identifier の略 | 転送されるコンテンツブロックの一意の識別子。 |
| CTDR | 転送方向（ Transfer Direction ） | CBID 転送がプッシュで開始されたかプルで開始されたかを示します。<br><br>PUSH ：転送処理は送信側エンティティによって要求されました。<br><br>PULL ：転送処理は受信側エンティティによって要求されました。 |
| CTSR | ソースエンティティ | CBID 転送のソース（送信側）のノード ID 。 |
| CTD | デスティネーションエンティティ | CBID 転送のデスティネーション（受信側）のノード ID 。 |

| コード | フィールド | 説明 |
| --- | --- | --- |
| CTSS | 開始シーケンスカウント（ Start Sequence Count ） | 最初のシーケンスカウントが要求されたことを示します。成功すると、このシーケンスカウントから転送が開始されます。 |
| CTES | 想定される終了シーケンス数 | 最後に要求されたシーケンスカウントを示します。成功すると、このシーケンスカウントを受信したときに転送が完了したとみなされます。 |
| RSLT | 転送開始ステータス | 転送が開始された時点のステータス：<br><br>SUCS ：転送が開始されました。 |

この監査メッセージは、 Content Block Identifier で識別されたとおりに単一のコンテンツでノード間のデータ転送処理が開始されたことを意味します。この処理では、「 Start Sequence Count 」から「 Expected End Sequence Count 」までのデータが要求されます。送信側と受信側のノードは、ノード ID によって識別されます。この情報を使用すると、システムのデータフローを追跡できます。ストレージ監査メッセージと組み合わせて使用すると、レプリカ数を検証できます。

**CBRE** ：オブジェクト受信終了

このメッセージは、あるノードから別のノードへのコンテンツブロックの転送が完了したときに転送先のエンティティによって生成されます。

| コード | フィールド | 説明 |
| --- | --- | --- |
| CNID | 接続識別子 | ノード間のセッション / 接続の一意の識別子。 |
| CBID | Content Block Identifier の略 | 転送されるコンテンツブロックの一意の識別子。 |
| CTDR | 転送方向（ Transfer Direction ） | CBID 転送がプッシュで開始されたかプルで開始されたかを示します。<br><br>PUSH ：転送処理は送信側エンティティによって要求されました。<br><br>PULL ：転送処理は受信側エンティティによって要求されました。 |
| CTSR | ソースエンティティ | CBID 転送のソース（送信側）のノード ID 。 |

| コード | フィールド | 説明 |
| --- | --- | --- |
| CTD | デスティネーションエンティティ | CBID 転送のデスティネーション（受信側）のノード ID 。 |
| CTSS | 開始シーケンスカウント（ Start Sequence Count ） | 転送が開始されたシーケンスカウントを示します。 |
| CTA | 実際の終了シーケンス数 | 転送に成功した最後のシーケンスカウントを示します。実際の終了シーケンスカウントが開始シーケンスカウントと同じで、転送結果が成功しなかった場合、データは交換されませんでした。 |
| RSLT | 転送結果 | （送信側エンティティから見た）転送処理の結果：<br><br>SUCS ：転送が正常に完了しました。要求されたすべてのシーケンスカウントが送信されました。<br><br>CONL ：転送中に接続が失われました<br><br>CTMO ：接続の確立中または転送中に接続がタイムアウトしました<br><br>UNRE ：デスティネーションノード ID に到達できません<br><br>CRPT ：破損または無効なデータを受信したため、転送が終了しました（改ざんの可能性があります）。 |

この監査メッセージは、ノード間のデータ転送処理が完了したことを意味します。転送結果が成功した場合は、「 Start Sequence Count 」から「 Actual End Sequence Count 」にデータが転送されます。送信側と受信側のノードは、ノード ID によって識別されます。この情報を使用すると、システムのデータフローを追跡し、エラーを検出、集計、分析できます。ストレージ監査メッセージと組み合わせれば、レプリカ数の検証にも使用できます。

**CBSB** ：オブジェクト送信の開始

通常のシステム運用中は、データへのアクセスおよびデータのレプリケートと保持が行われる際に、異なるノード間でコンテンツブロックが継続的に転送されます。このメッセージは、あるノードから別のノードへのコンテンツブロックの転送が開始したときにソースエンティティによって生成されます。

| コード | フィールド | 説明 |
| --- | --- | --- |
| CNID | 接続識別子 | ノード間のセッション / 接続の一意の識別子。 |
| CBID | Content Block Identifier の略 | 転送されるコンテンツブロックの一意の識別子。 |
| CTDR | 転送方向（ Transfer Direction ） | CBID 転送がプッシュで開始されたかプルで開始されたかを示します。<br><br>PUSH ：転送処理は送信側エンティティによって要求されました。<br><br>PULL ：転送処理は受信側エンティティによって要求されました。 |
| CTSR | ソースエンティティ | CBID 転送のソース（送信側）のノード ID 。 |
| CTD | デスティネーションエンティティ | CBID 転送のデスティネーション（受信側）のノード ID 。 |
| CTSS | 開始シーケンスカウント（ Start Sequence Count ） | 最初のシーケンスカウントが要求されたことを示します。成功すると、このシーケンスカウントから転送が開始されます。 |
| CTES | 想定される終了シーケンス数 | 最後に要求されたシーケンスカウントを示します。成功すると、このシーケンスカウントを受信したときに転送が完了したとみなされます。 |
| RSLT | 転送開始ステータス | 転送が開始された時点のステータス：<br><br>SUCS ：転送が開始されました。 |

この監査メッセージは、 Content Block Identifier で識別されたとおりに単一のコンテンツでノード間のデータ転送処理が開始されたことを意味します。この処理では、「 Start Sequence Count 」から「 Expected End Sequence Count 」までのデータが要求されます。送信側と受信側のノードは、ノード ID によって識別されます。この情報を使用すると、システムのデータフローを追跡できます。ストレージ監査メッセージと組み合わせて使用すると、レプリカ数を検証できます。

**CBSE** ：オブジェクト送信終了

このメッセージは、あるノードから別のノードへのコンテンツブロックの転送が完了し

たときに転送元のエンティティによって生成されます。

| コード | フィールド | 説明 |
| --- | --- | --- |
| CNID | 接続識別子 | ノード間のセッション / 接続の一意の識別子。 |
| CBID | Content Block Identifier の略 | 転送されるコンテンツブロックの一意の識別子。 |
| CTDR | 転送方向（ Transfer Direction ） | CBID 転送がプッシュで開始されたかプルで開始されたかを示します。<br><br>PUSH ：転送処理は送信側エンティティによって要求されました。<br><br>PULL ：転送処理は受信側エンティティによって要求されました。 |
| CTSR | ソースエンティティ | CBID 転送のソース（送信側）のノード ID 。 |
| CTD | デスティネーションエンティティ | CBID 転送のデスティネーション（受信側）のノード ID 。 |
| CTSS | 開始シーケンスカウント（ Start Sequence Count ） | 転送が開始されたシーケンスカウントを示します。 |
| CTA | 実際の終了シーケンス数 | 転送に成功した最後のシーケンスカウントを示します。実際の終了シーケンスカウントが開始シーケンスカウントと同じで、転送結果が成功しなかった場合、データは交換されませんでした。 |

| コード | フィールド | 説明 |
| --- | --- | --- |
| RSLT | 転送結果 | （送信側エンティティから見た）転送処理の結果：<br><br>SUCS ：転送が正常に完了しました。要求されたすべてのシーケンスカウントが送信されました。<br><br>CONL ：転送中に接続が失われました<br><br>CTMO ：接続の確立中または転送中に接続がタイムアウトしました<br><br>UNRE ：デスティネーションノード ID に到達できません<br><br>CRPT ：破損または無効なデータを受信したため、転送が終了しました（改ざんの可能性があります）。 |

この監査メッセージは、ノード間のデータ転送処理が完了したことを意味します。転送結果が成功した場合は、「 Start Sequence Count 」から「 Actual End Sequence Count 」にデータが転送されます。送信側と受信側のノードは、ノード ID によって識別されます。この情報を使用すると、システムのデータフローを追跡し、エラーを検出、集計、分析できます。ストレージ監査メッセージと組み合わせれば、レプリカ数の検証にも使用できます。

**ECOC** ：イレイジャーコーディングされたデータフラグメントが破損しています

## この監査メッセージは、イレイジャーコーディングされたデータフラグメントの破損がシステムで検出されたことを示します。

| コード | フィールド | 説明 |
| --- | --- | --- |
| Vcco | VCS ID を入力します | 破損したチャンクが含まれている VCS の名前。 |
| VLID | ボリューム ID | 破損したイレイジャーコーディングフラグメントが含まれている RangeDB ボリューム。 |
| CCID | チャンク ID | 破損したイレイジャーコーディングフラグメントの識別子。 |

| コード | フィールド | 説明 |
| --- | --- | --- |
| RSLT | 結果 | このフィールドの値は「 NONE 」です。RSLT は必須のメッセージフィールドですが、このメッセージには該当しません。このメッセージがフィルタリングされないように、「 UCS 」ではなく「 none 」が使用されます。 |

**ETAF** ：セキュリティ認証に失敗しました

このメッセージは、 Transport Layer Security （ TLS ）を使用した接続試行が失敗した場合に生成されます。

| コード | フィールド | 説明 |
| --- | --- | --- |
| CNID | 接続識別子 | 認証が失敗した TCP / IP 接続の一意のシステム識別子。 |
| RUID | ユーザ ID | リモートユーザの ID を表すサービスに依存する識別子。 |

| コード | フィールド | 説明 |
| --- | --- | --- |
| RSLT | 理由コード | 失敗の理由：<br><br>SCNI ：セキュアな接続を確立できませんでした。<br><br>CERM ：証明書がありません。<br><br>CERT ：証明書が無効です。<br><br>CERE ：証明書が期限切れです。<br><br>CERR ：証明書が取り消されています。<br><br>CSGN ：証明書の署名が無効です。<br><br>CSGU ：証明書の署名者が不明です。<br><br>UCRM ：ユーザクレデンシャルがありません。<br><br>UCRI ：ユーザクレデンシャルが無効です。<br><br>UCRU ：ユーザのクレデンシャルが拒否されました。<br><br>TOUT ：認証がタイムアウトしました。 |

TLS を使用するセキュアなサービスへの接続が確立されると、サービスに組み込まれている TLS プロファイルおよびその他のロジックを使用してリモートエンティティのクレデンシャルが検証されます。無効、想定外、許可されていない証明書またはクレデンシャルが原因でこの認証が失敗すると、監査メッセージがログに記録されます。これにより、不正アクセスやその他のセキュリティ関連の接続問題を照会できます。

このメッセージは、リモートエンティティの設定が正しくない場合や、無効または許可されていないクレデンシャルをシステムに提示しようとした場合に生成されることがあります。この監査メッセージを監視して、システムへの不正なアクセス試行を検出する必要があります。

**GNRG** ： **GNDS** 登録

CMN サービスは、 StorageGRID システムで CMN サービスに関する情報を更新または登録したときにこの監査メッセージを生成します。

| コード | フィールド | 説明 |
| --- | --- | --- |
| RSLT | 結果 | 更新リクエストの結果：<br>• SUCS ：成功しました<br>• SUNV ：サービスを使用できません<br>• GERR ：その他の失敗 |
| GNID | ノード ID | 更新要求を開始したサービスのノード ID 。 |
| GNTP | デバイスタイプ | グリッドノードのデバイスタイプ（ LDR サービスの場合は BLDR など）。 |
| GNDV | デバイスモデルのバージョン | DMDL バンドル内のグリッドノードのデバイスモデルバージョンを識別する文字列。 |
| GNGP | グループ | グリッドノードが属するグループ（リンクコストとサービス - クエリランキングのコンテキストで）。 |
| GNIA | IP アドレス | グリッドノードの IP アドレス。 |

このメッセージは、グリッドノードがグリッドノードバンドル内の自身のエントリを更新するたびに生成されます。

**GNUR** ： **GNDS** 登録解除

CMN サービスは、 StorageGRID システムから CMN サービスに関する情報の登録を解除したときにこの監査メッセージを生成します。

| コード | フィールド | 説明 |
| --- | --- | --- |
| RSLT | 結果 | 更新リクエストの結果：<br>• SUCS ：成功しました<br>• SUNV ：サービスを使用できません<br>• GERR ：その他の失敗 |
| GNID | ノード ID | 更新要求を開始したサービスのノード ID 。 |

**GTED ： Grid** タスクが終了しました

この監査メッセージは、 CMN サービスが指定されたグリッドタスクの処理を完了し、タスクを Historical テーブルに移動したことを示します。結果が SUCS 、 ABRT 、 ROLF のいずれかである場合は、対応する Grid Task Started 監査メッセージも生成されます。それ以外の結果は、このグリッドタスクの処理が開始されなかったことを示します。

| コード | フィールド | 説明 |
| --- | --- | --- |
| TSID | タスク ID | このフィールドは、生成されたグリッドタスクを一意に識別します。また、グリッドタスクをライフサイクル全体にわたって管理できます。<br><br>• 注： * タスク ID は、グリッドタスクが送信された時点ではなく、生成された時点で割り当てられます。特定のグリッドタスクを複数回送信することができます。この場合、送信済み、開始、および終了の監査メッセージを一意にリンクするためのタスク ID フィールドでは不十分です。 |

| コード | フィールド | 説明 |
| --- | --- | --- |
| RSLT | 結果 | グリッドタスクの最終ステータス：<br>• SUCS ：グリッドタスクが正常に完了しました。<br>• ABRT ：グリッドタスクがロールバックエラーなしで中止されました。<br>• ROLF ：グリッドタスクが中止され、ロールバックプロセスを完了できませんでした。<br>• CANC ：グリッドタスクは開始前にユーザによってキャンセルされました。<br>• EXPR ：グリッドタスクは開始前に期限切れとなりました。<br>• IVLD ：グリッドタスクは無効でした。<br>• AUTH ：グリッドタスクは許可されていませんでした。<br>• DUPL ：グリッドタスクは重複として拒否されました。 |

**GTSt** ： **Grid** タスクが開始されました

この監査メッセージは、 CMN サービスが指定されたグリッドタスクの処理を開始したことを示します。この監査メッセージは、内部の Grid Task Submission サービスによって開始されて自動アクティブ化用に選択されているグリッドタスクの Grid Task Submitted メッセージの直後に生成されます。Pending テーブルに送信されるグリッドタスクの場合、このメッセージはユーザがグリッドタスクを開始するときに生成されます。

| コード | フィールド | 説明 |
| --- | --- | --- |
| TSID | タスク ID | このフィールドは、生成されたグリッドタスクを一意に識別します。また、タスクをライフサイクル全体にわたって管理できます。<br><br>• 注：* タスク ID は、グリッドタスクが送信された時点ではなく、生成された時点で割り当てられます。特定のグリッドタスクを複数回送信することができます。この場合、送信済み、開始、および終了の監査メッセージを一意にリンクするためのタスク ID フィールドでは不十分です。 |
| RSLT | 結果 | 結果。このフィールドの値は 1 つだけです。<br><br>• SUCS ：グリッドタスクが正常に開始されました。 |

**GTSU** ： **Grid** タスクが送信されました

この監査メッセージは、グリッドタスクが CMN サービスに送信されたことを示します。

| コード | フィールド | 説明 |
| --- | --- | --- |
| TSID | タスク ID | 生成されたグリッドタスクを一意に識別し、タスクをライフサイクル全体にわたって管理できるようにします。<br><br>• 注：* タスク ID は、グリッドタスクが送信された時点ではなく、生成された時点で割り当てられます。特定のグリッドタスクを複数回送信することができます。この場合、送信済み、開始、および終了の監査メッセージを一意にリンクするためのタスク ID フィールドでは不十分です。 |
| ttyp | タスクタイプ（ Task Type ） | グリッドタスクのタイプ。 |

| コード | フィールド | 説明 |
| --- | --- | --- |
| Tver | タスクバージョン | グリッドタスクのバージョンを示す番号。 |
| TDSC | Task 概要 の略 | グリッドタスクの判読可能な概要。 |
| 付加価値を提供します | タイムスタンプ後の有効な値 | グリッドタスクの有効期間の開始時間（ UNIX 時間 1970 年 1 月 1 日からの UINT64 マイクロ秒数）。 |
| VBTS | タイムスタンプの前に有効です | グリッドタスクの有効期間の終了時間（ UNIX 時間 1970 年 1 月 1 日からの UINT64 マイクロ秒数）。 |
| TsRC | ソース | タスクのソース：<br>• TXTB ：グリッドタスクは、 StorageGRID システム経由で署名付きテキストブロックとして送信されました。<br>• GRID ：グリッドタスクは、内部の Grid Task Submission サービス経由で送信されました。 |
| ACTV | アクティベーションタイプ | アクティブ化のタイプ：<br>• Auto ：グリッドタスクは自動でアクティブ化されます。<br>• PEND ：グリッドタスクは Pending テーブルに追加されました。TXTB ソースの場合はこのタイプのみです。 |
| RSLT | 結果 | 送信結果：<br>• SUCS ：グリッドタスクは正常に送信されました。<br>• FAIL ：タスクは Historical テーブルに直接移動されました。 |

**IDEL ： ILM Initiated Delete**

このメッセージは、 ILM によってオブジェクトを削除する処理が開始された場合に生成されます。

IDEL メッセージは、次のいずれかの状況で生成されます。

- * 準拠 S3 バケット内のオブジェクト * ：このメッセージは、保持期間が経過したために ILM によってオブジェクトの自動削除処理が開始された場合に生成されます（自動削除設定が有効になっていて、リーガルホールドがオフの場合）。
- * 非準拠 S3 バケットまたは Swift コンテナ内のオブジェクト * 。このメッセージは、現在オブジェクトに適用される配置手順がアクティブな ILM ポリシーにないために、オブジェクトを削除する処理が ILM によって開始された場合に生成されます。

| コード | フィールド | 説明 |
| --- | --- | --- |
| CBID | Content Block Identifier の略 | オブジェクトの CBID 。 |
| CMPA | 準拠：自動削除 | 準拠 S3 バケット内のオブジェクトのみが対象。0 （ false ）または 1 （ true ）。バケットがリーガルホールドの対象である場合を除き、保持期間の終了時に準拠オブジェクトを自動的に削除するかどうかを示します。 |
| テンプレート | コンプライアンス：リーガルホールド | 準拠 S3 バケット内のオブジェクトのみが対象。0 （ false ）または 1 （ true ）。バケットが現在リーガルホールドの対象であるかどうかを示します。 |
| CMPR | 準拠：保持期間 | 準拠 S3 バケット内のオブジェクトのみが対象。オブジェクトの保持期間の長さ（分）。 |
| CTME | 準拠：取り込み時間 | 準拠 S3 バケット内のオブジェクトのみが対象。オブジェクトの取り込み時間。この値に保持期間を分単位で追加することで、オブジェクトをバケットから削除できるタイミングを判断できます。 |
| dmrk | マーカーバージョン ID を削除します | バージョン管理されたバケットからオブジェクトを削除するときに作成された削除マーカーのバージョン ID 。バケットに対する処理ではこのフィールドは記録されません。 |
| CSIZ | コンテンツのサイズ | オブジェクトのサイズ（バイト単位）。 |

| コード | フィールド | 説明 |
| --- | --- | --- |
| LOCS | ロケーション | StorageGRID システム内のオブジェクトデータの格納場所。オブジェクトに場所がない場合（削除されている場合など）、 LOCS の値は "" です。<br><br>CLEC ：イレイジャーコーディングされたオブジェクトの場合、オブジェクトのデータに適用されているイレイジャーコーディングプロファイル ID とイレイジャーコーディンググループ ID 。<br><br>CLDI ：レプリケートされたオブジェクトの場合、オブジェクトの場所の LDR ノード ID とボリューム ID 。<br><br>CLNL ：オブジェクトデータがアーカイブされている場合は、オブジェクトの場所の ARC ノード ID 。 |
| パス | S3 バケット / キーまたは Swift コンテナ / オブジェクト ID | S3 バケット名と S3 キー名、または Swift コンテナ名と Swift オブジェクト識別子。 |
| RSLT | 結果 | ILM 処理の結果。<br><br>SUCS ： ILM 処理が成功しました。 |
| ルール | ルールラベル（ Rules Label ） | • 保持期間が経過したために準拠 S3 バケット内のオブジェクトが自動的に削除されている場合、このフィールドは空白になります。<br>• 現在オブジェクトに適用される配置手順がないためにオブジェクトが削除されている場合、このフィールドには、オブジェクトに適用された最後の ILM ルールの判読可能なラベルが表示されます。 |
| UUID | Universally Unique Identifier の略 | StorageGRID システム内でのオブジェクトの識別子。 |

| コード | フィールド | 説明 |
| --- | --- | --- |
| VSID | バージョン ID | 削除されたオブジェクトの特定のバージョンのバージョン ID 。バージョン管理されていないバケット内のバケットやオブジェクトに対する処理には、このフィールドは含まれません。 |

**LKCU:** 上書きされたオブジェクトのクリーンアップ

このメッセージは、ストレージスペースを解放するためにクリーンアップが必要な上書きされたオブジェクトを StorageGRID が削除した場合に生成されます。オブジェクトがすでに含まれているパスに S3 または Swift クライアントがオブジェクトを書き込むと、オブジェクトが上書きされます。削除処理は自動的にバックグラウンドで実行されます。

| コード | フィールド | 説明 |
| --- | --- | --- |
| CSIZ | コンテンツのサイズ | オブジェクトのサイズ（バイト単位）。 |
| LTYP | クリーンアップのタイプ | _ 内部使用のみ。 _ |
| LUID （ LUID ） | オブジェクト UUID が削除されました | 削除されたオブジェクトの識別子。 |
| パス | S3 バケット / キーまたは Swift コンテナ / オブジェクト ID | S3 バケット名と S3 キー名、または Swift コンテナ名と Swift オブジェクト識別子。 |
| SEGC | コンテナ UUID | セグメント化されたオブジェクトのコンテナの UUID 。この値は、オブジェクトがセグメント化されている場合にのみ使用できます。 |
| UUID | Universally Unique Identifier の略 | まだ存在するオブジェクトの ID 。この値は、オブジェクトが削除されていない場合にのみ使用できます。 |

**LLST** ：ロケーションが失われました

このメッセージは、オブジェクトをコピー（レプリケートまたはイレイジャーコーディング）する場所が見つからない場合に生成されます。

| コード | フィールド | 説明 |
| --- | --- | --- |
| CBIL | CBID | 影響を受ける CBID 。 |
| NOID | ソースノード ID | 場所が失われたノード ID 。 |
| UUID | Universally Unique ID の略 | StorageGRID システムでの該当オブジェクトの識別子。 |
| ECPR | イレイジャーコーディングプロファイル | イレイジャーコーディングされたオブジェクトデータ用。使用されているイレイジャーコーディングプロファイルの ID です。 |
| LTYP | 保管場所タイプ | CLDI （ Online ）：レプリケートされたオブジェクトデータ用<br><br>CLEC （ Online ）：イレイジャーコーディングされたオブジェクトデータ用<br><br>CLNL （ Nearline ）：アーカイブされたレプリケートオブジェクトデータ用 |
| PCLD | レプリケートオブジェクトへのパス | 損失オブジェクトデータのディスクの場所への完全なパス。LTYP の値が CLDI （つまりレプリケートオブジェクトの場合）の場合にのみ返されます。<br><br>フォームを使用します `/var/local/rangedb/2/p/13/13/00oJs6X%{h{U)SeUFxE@` |
| RSLT | 結果 | 常に NONE 。RSLT は必須のメッセージフィールドですが、このメッセージには該当しません。このメッセージがフィルタリングされないように、 SUCS ではなく NONE が使用されます。 |
| TsRC | トリガ元 | USER ：ユーザがトリガーしました<br><br>SYST ：システムがトリガーされました |

管理カテゴリでは、管理 API に対するユーザ要求がログに記録されます。API に対する GET または HEAD 以外のすべての要求は、応答に加えて要求のユーザ名、 IP 、およびタイプをログに記録します。

| コード | フィールド | 説明 |
| --- | --- | --- |
| MDIP | 宛先 IP アドレス | サーバ（デスティネーション）の IP アドレス。 |
| MDNA | ドメイン名 | ホストのドメイン名。 |
| MPAT | 要求のパス | 要求のパス。 |
| MPQP | 要求クエリパラメータ | 要求のクエリパラメータ。 |
| MRBD の略 | 本文を要求します | 要求の本文の内容。応答の本文はデフォルトでログに記録されますが、要求の本文は応答の本文が空の特定のケースでログに記録されます。応答の本文には次の情報が含まれていないため、それぞれの POST メソッドの要求本文から取り込まれます。<br>• ユーザ名とアカウント ID ： * POST authorize *<br>• 新しいサブネット設定： * POST /grid/grid-networks/update *<br>• 新しい NTP サーバ： * POST /grid/ntp-servers /update * に含まれています<br>• 運用停止されたサーバ ID は、 * POST /grid/servers/decommission * に記載されています<br>• 注： * 機密情報は、削除（ S3 アクセスキーなど）またはアスタリスクでマスク（パスワードなど）されます。 |

| コード | フィールド | 説明 |
| --- | --- | --- |
| 検査 | 要求メソッド | HTTP 要求メソッド：<br>• 投稿（ Post ）<br>• PUT<br>• 削除<br>• パッチ |
| MRSC | 応答コード | 応答コード。 |
| MRSP | 応答の本文 | デフォルトでは、応答の内容（応答の本文）がログに記録されます。<br>• 注： * 機密情報は、削除（ S3 アクセスキーなど）またはアスタリスクでマスク（パスワードなど）されます。 |
| MSIP | 送信元 IP アドレス | クライアント（送信元）の IP アドレス。 |
| MUUN | ユーザの URN | 要求を送信したユーザの URN （ Uniform Resource Name ）。 |
| RSLT | 結果 | 成功（ SUCS ）、またはバックエンドによって報告されたエラーが返されます。 |

**OLST:** システムが損失オブジェクトを検出しました

このメッセージは、 DDS サービスが StorageGRID システム内にオブジェクトのコピーを 1 つも見つけることができない場合に生成されます。

| コード | フィールド | 説明 |
| --- | --- | --- |
| CBID | Content Block Identifier の略 | 損失オブジェクトの CBID 。 |
| NOID | ノード ID | 損失オブジェクトが最後に確認されたダイレクトまたはニアラインの場所がある場合。ボリューム情報がない場合は、ノード ID だけでボリューム ID がないケースもあります。 |

| コード | フィールド | 説明 |
| --- | --- | --- |
| パス | S3 バケット / キーまたは Swift コンテナ / オブジェクト ID | 該当する場合は、 S3 バケット名と S3 キー名、または Swift コンテナ名と Swift オブジェクト識別子。 |
| RSLT | 結果 | このフィールドの値は NONE です。RSLT は必須のメッセージフィールドですが、このメッセージには該当しません。このメッセージがフィルタリングされないように、 SUCS ではなく NONE が使用されます。 |
| UUID | Universally Unique ID の略 | StorageGRID システム内の損失オブジェクトの識別子。 |
| ヴォル | ボリューム ID | 使用可能な場合は、損失オブジェクトが最後に確認された場所のストレージノードまたはアーカイブノードのボリューム ID 。 |

**ORLM** ：オブジェクトルールが満たされています

このメッセージは、 ILM ルールで指定されたとおりにオブジェクトが格納およびコピーされた場合に生成されます。

ORLM メッセージは、ポリシー内の別のルールで高度なフィルタ「オブジェクトサイズ」が使用されている場合に、オブジェクトがデフォルトの Make 2 Copies ルールによって格納されたときには生成されません。

| コード | フィールド | 説明 |
| --- | --- | --- |
| CBID | Content Block Identifier の略 | オブジェクトの CBID 。 |
| CSIZ | コンテンツのサイズ | オブジェクトのサイズ（バイト単位）。 |

| コード | フィールド | 説明 |
| --- | --- | --- |
| LOCS | ロケーション | StorageGRID システム内のオブジェクトデータの格納場所。オブジェクトに場所がない場合（削除されている場合など）、 LOCS の値は "" です。<br><br>CLEC ：イレイジャーコーディングされたオブジェクトの場合、オブジェクトのデータに適用されているイレイジャーコーディングプロファイル ID とイレイジャーコーディンググループ ID 。<br><br>CLDI ：レプリケートされたオブジェクトの場合、オブジェクトの場所の LDR ノード ID とボリューム ID 。<br><br>CLNL ：オブジェクトデータがアーカイブされている場合は、オブジェクトの場所の ARC ノード ID 。 |
| パス | S3 バケット / キーまたは Swift コンテナ / オブジェクト ID | S3 バケット名と S3 キー名、または Swift コンテナ名と Swift オブジェクト識別子。 |
| RSLT | 結果 | ILM 処理の結果。<br><br>SUCS ： ILM 処理が成功しました。 |
| ルール | ルールラベル（ Rules Label ） | このオブジェクトに適用されている ILM ルールの判読可能なラベル。 |
| SEGC | コンテナ UUID | セグメント化されたオブジェクトのコンテナの UUID 。この値は、オブジェクトがセグメント化されている場合にのみ使用できます。 |
| SGCB | コンテナの CBID | セグメント化されたオブジェクトのコンテナの CBID 。この値は、オブジェクトがセグメント化されている場合にのみ使用できます。 |

| コード | フィールド | 説明 |
| --- | --- | --- |
| 統計 | ステータス | ILM 処理のステータス。<br><br>DONE ：オブジェクトに対する ILM 処理が完了しました。<br><br>DFER ： ILM によって再評価されるようオブジェクトがマークされました。<br><br>PRGD ：オブジェクトが StorageGRID システムから削除されました。<br><br>NLOC ：オブジェクトデータを StorageGRID システムで検出できなくなります。このステータスは、オブジェクトデータのすべてのコピーが欠落または破損していることを示している可能性があります。 |
| UUID | Universally Unique Identifier の略 | StorageGRID システム内でのオブジェクトの識別子。 |

ORLM 監査メッセージは、 1 つのオブジェクトに対して複数回生成でき、たとえば、次のいずれかのイベントが発生するたびに発行されます。

- オブジェクトが対応する ILM ルールを無期限に満たしたとき。
- オブジェクトが対応する ILM ルールを一時的に満たしたとき。
- オブジェクトが ILM ルールによって削除されたとき。
- バックグラウンド検証プロセスにより、レプリケートされたオブジェクトデータのコピーが破損していることが検出されたとき。StorageGRID システムは、破損したオブジェクトを交換するために ILM 評価を実行します。

関連情報

"オブジェクトの取り込みトランザクション"

"オブジェクトの削除トランザクション"

**OVWR** ：オブジェクトを上書き

このメッセージは、外部（クライアントが要求した）処理によって、あるオブジェクトが別のオブジェクトで上書きされた場合に生成されます。

| コード | フィールド | 説明 |
| --- | --- | --- |
| CBID | Content Block Identifier （新規） | 新しいオブジェクトの CBID 。 |

| コード | フィールド | 説明 |
| --- | --- | --- |
| CSIZ | 前のオブジェクトサイズ | 上書きされるオブジェクトのサイズ（バイト単位）。 |
| OCBD | コンテンツブロック識別子（前のもの） | 既存のオブジェクトの CBID 。 |
| UUID | Universally Unique ID （新規） | StorageGRID システム内での新しいオブジェクトの識別子。 |
| OUID | Universally Unique ID （旧） | StorageGRID システム内での以前のオブジェクトの識別子。 |
| パス | S3 または Swift オブジェクトのパス | 既存のオブジェクトと新しいオブジェクトの両方に使用する S3 または Swift オブジェクトのパス |
| RSLT | 結果コード | Object Overwrite トランザクションの結果。常に次の結果になります。<br><br>SUCS ：成功しました |

**SADD** ：セキュリティ監査無効

このメッセージは、元のサービス（ノード ID ）が監査メッセージのロギングをオフにしたことを示します。監査メッセージの収集や配信は停止しています。

| コード | フィールド | 説明 |
| --- | --- | --- |
| AETM | enable メソッド | 監査を無効にするために使用されたメソッド。 |
| EUN | ユーザ名 | 監査ログを無効にするコマンドを実行したユーザ名。 |
| RSLT | 結果 | このフィールドの値は NONE です。RSLT は必須のメッセージフィールドですが、このメッセージには該当しません。このメッセージがフィルタリングされないように、 SUCS ではなく NONE が使用されます。 |

このメッセージは、以前は有効だったロギングが現在は無効になっていることを示します。一般には、システムのパフォーマンスを向上させるために一括取り込み時にのみ実行される処理です。一括アクティビティ後に監査がリストアされ（ SADE ）、監査を無効にする機能は永続的にブロックされます。

**Sade** ：セキュリティ監査を有効にします

このメッセージは、元のサービス（ノード ID ）が監査メッセージのロギングをリストアしたことを示します。監査メッセージの収集や配信は再開されています。

| コード | フィールド | 説明 |
| --- | --- | --- |
| AETM | enable メソッド | 監査を有効にするために使用されたメソッド。 |
| EUN | ユーザ名 | 監査ログを有効にするコマンドを実行したユーザ名。 |
| RSLT | 結果 | このフィールドの値は NONE です。RSLT は必須のメッセージフィールドですが、このメッセージには該当しません。このメッセージがフィルタリングされないように、 SUCS ではなく NONE が使用されます。 |

このメッセージは、以前は無効（ SADD ）だったロギングが現在は有効になっていることを示します。一般には、システムのパフォーマンスを向上させるために一括取り込み時にのみ実行される処理です。一括アクティビティ後に監査がリストアされ、監査を無効にする機能は永続的にブロックされます。

**SCMT** ：オブジェクトストアのコミット

グリッドコンテンツは、コミット（永続的に格納）されるまでは、使用可能にならず、格納済みとして認識されません。永続的に格納されたコンテンツは、ディスクに完全に書き込まれ、関連する整合性チェックに合格したコンテンツです。このメッセージは、コンテンツブロックがストレージにコミットされたときに生成されます。

| コード | フィールド | 説明 |
| --- | --- | --- |
| CBID | Content Block Identifier の略 | 永続的ストレージにコミットされたコンテンツブロックの一意の識別子。 |
| RSLT | 結果コード | オブジェクトがディスクに格納された時点のステータス：<br><br>SUCS ：オブジェクトが正常に格納されました。 |

このメッセージは、コンテンツブロックの格納と検証がすべて完了し、要求可能な状態になったことを意味します。この機能を使用すると、システム内のデータフローを追跡できます。

**SDEL ： S3 DELETE**

S3 クライアントが DELETE トランザクションを実行すると、指定したオブジェクトまたはバケットを削除する要求が送信されます。このメッセージは、トランザクションが成功した場合にサーバによって出力されます。

| コード | フィールド | 説明 |
| --- | --- | --- |
| CBID | Content Block Identifier の略 | 要求されたコンテンツブロックの一意の識別子。CBID が不明な場合、このフィールドは 0 に設定されます。バケットに対する処理ではこのフィールドは記録されません。 |
| CNCH | 整合性制御ヘッダー | 要求に Consistency-Control HTTP 要求ヘッダーが存在する場合は、その値。 |
| CNID | 接続識別子 | TCP / IP 接続の一意のシステム識別子。 |
| CSIZ | コンテンツサイズ（ Content Size ） | 削除されたオブジェクトのサイズ（バイト単位）。バケットに対する処理ではこのフィールドは記録されません。 |
| dmrk | マーカーバージョン ID を削除します | バージョン管理されたバケットからオブジェクトを削除するときに作成された削除マーカーのバージョン ID 。バケットに対する処理ではこのフィールドは記録されません。 |
| HTRH | HTTP 要求ヘッダー | 設定時に選択した、ログに記録される HTTP 要求ヘッダーの名前と値のリスト。<br><br>• 注： * `X-Forwarded-For` は、要求に存在する場合、およびに存在する場合は自動的に含まれます `X-Forwarded-For` 値が要求送信者のIPアドレス（SAIP監査フィールド）と異なります。 |
| MTME | 最終変更時刻 | オブジェクトが最後に変更された日時を示す Unix タイムスタンプ（マイクロ秒）。 |

| コード | フィールド | 説明 |
| --- | --- | --- |
| RSLT | 結果コード | DELETE トランザクションの結果。常に次の結果になります。<br><br>SUCS ：成功しました |
| S3AI | S3 テナントアカウント ID （要求の送信者） | 要求を送信したユーザのテナントアカウント ID 。空の値は匿名アクセスであることを示します。 |
| S3AK | S3 アクセスキー ID （要求の送信者） | 要求を送信したユーザのハッシュ済み S3 アクセスキー ID 。空の値は匿名アクセスであることを示します。 |
| S3BK | S3 バケット | S3 バケット名。 |
| S3KY | S3 キー | バケット名を除く S3 キーの名前。バケットに対する処理ではこのフィールドは記録されません。 |
| S3SR | S3 サブリソース | 必要に応じて、処理対象のバケットまたはオブジェクトサブリソース。 |
| SACC | S3 テナントアカウント名（要求の送信者） | 要求を送信したユーザのテナントアカウントの名前。匿名の要求の場合は空です。 |
| saip | IP アドレス（要求送信者） | 要求を送信したクライアントアプリケーションの IP アドレス。 |
| SBAC | S3 テナントアカウント名（バケット所有者） | バケット所有者のテナントアカウント名。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。 |
| SBAI | S3 テナントアカウント ID （バケット所有者） | ターゲットバケットの所有者のテナントアカウント ID 。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。 |

| コード | フィールド | 説明 |
| --- | --- | --- |
| サスペンション | S3 ユーザの URN （要求の送信者） | 要求を送信しているユーザのテナントアカウント ID とユーザ名。ローカルユーザまたは LDAP ユーザです。例：<br>`urn:sgws:identity::03393893651506583485:root`<br><br>匿名の要求の場合は空です。 |
| 時間 | 時間 | 要求の合計処理時間（マイクロ秒）。 |
| TLIP | 信頼できるロードバランサの IP アドレス | 要求が信頼できるレイヤ 7 ロードバランサによってルーティングされた場合は、ロードバランサの IP アドレス。 |
| UUID | Universally Unique Identifier の略 | StorageGRID システム内でのオブジェクトの識別子。 |
| VSID | バージョン ID | 削除されたオブジェクトの特定のバージョンのバージョン ID 。バージョン管理されていないバケット内のバケットやオブジェクトに対する処理には、このフィールドは含まれません。 |

**SGET ： S3 GET**

S3 クライアントが GET トランザクションを実行すると、オブジェクトを読み出しまたはバケット内のオブジェクトを一覧表示する要求が送信されます。このメッセージは、トランザクションが成功した場合にサーバによって出力されます。

| コード | フィールド | 説明 |
| --- | --- | --- |
| CBID | Content Block Identifier の略 | 要求されたコンテンツブロックの一意の識別子。CBID が不明な場合、このフィールドは 0 に設定されます。バケットに対する処理ではこのフィールドは記録されません。 |
| CNCH | 整合性制御ヘッダー | 要求に Consistency-Control HTTP 要求ヘッダーが存在する場合は、その値。 |

| コード | フィールド | 説明 |
| --- | --- | --- |
| CNID | 接続識別子 | TCP / IP 接続の一意のシステム識別子。 |
| CSIZ | コンテンツサイズ（ Content Size ） | 読み出されたオブジェクトのサイズ（バイト単位）。バケットに対する処理ではこのフィールドは記録されません。 |
| HTRH | HTTP 要求ヘッダー | 設定時に選択した、ログに記録される HTTP 要求ヘッダーの名前と値のリスト。<br><br>• 注： * `X-Forwarded-For` は、要求に存在する場合、および存在する場合は自動的に含まれます `X-Forwarded-For` 値が要求送信者のIPアドレス（SAIP監査フィールド）と異なります。 |
| rang | 範囲の読み取り | 範囲読み取り処理の場合のみ。この要求によって読み取られたバイトの範囲を示します。スラッシュ（ / ）の後の値は、オブジェクト全体のサイズを示します。 |
| RSLT | 結果コード | GET トランザクションの結果。常に次の結果になります。<br><br>SUCS ：成功しました |
| S3AI | S3 テナントアカウント ID （要求の送信者） | 要求を送信したユーザのテナントアカウント ID 。空の値は匿名アクセスであることを示します。 |
| S3AK | S3 アクセスキー ID （要求の送信者） | 要求を送信したユーザのハッシュ済み S3 アクセスキー ID 。空の値は匿名アクセスであることを示します。 |
| S3BK | S3 バケット | S3 バケット名。 |
| S3KY | S3 キー | バケット名を除く S3 キーの名前。バケットに対する処理ではこのフィールドは記録されません。 |

| コード | フィールド | 説明 |
| --- | --- | --- |
| S3SR | S3 サブリソース | 必要に応じて、処理対象のバケットまたはオブジェクトサブリソース。 |
| SACC | S3 テナントアカウント名（要求の送信者） | 要求を送信したユーザのテナントアカウントの名前。匿名の要求の場合は空です。 |
| saip | IP アドレス（要求送信者） | 要求を送信したクライアントアプリケーションの IP アドレス。 |
| SBAC | S3 テナントアカウント名（バケット所有者） | バケット所有者のテナントアカウント名。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。 |
| SBAI | S3 テナントアカウント ID （バケット所有者） | ターゲットバケットの所有者のテナントアカウント ID 。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。 |
| サスペンション | S3 ユーザの URN （要求の送信者） | 要求を送信しているユーザのテナントアカウント ID とユーザ名。ローカルユーザまたは LDAP ユーザです。例： `urn:sgws:identity::03393893651506583485:root`<br><br>匿名の要求の場合は空です。 |
| 時間 | 時間 | 要求の合計処理時間（マイクロ秒）。 |
| TLIP | 信頼できるロードバランサの IP アドレス | 要求が信頼できるレイヤ 7 ロードバランサによってルーティングされた場合は、ロードバランサの IP アドレス。 |
| UUID | Universally Unique Identifier の略 | StorageGRID システム内でのオブジェクトの識別子。 |
| VSID | バージョン ID | 要求されたオブジェクトの特定のバージョンのバージョン ID 。バージョン管理されていないバケット内のバケットやオブジェクトに対する処理には、このフィールドは含まれません。 |

S3 クライアントが HEAD トランザクションを実行すると、オブジェクトまたはバケットの存在をチェックし、オブジェクトに関するメタデータを読み出す要求が送信されます。このメッセージは、トランザクションが成功した場合にサーバによって出力されます。

| コード | フィールド | 説明 |
| --- | --- | --- |
| CBID | Content Block Identifier の略 | 要求されたコンテンツブロックの一意の識別子。CBID が不明な場合、このフィールドは 0 に設定されます。バケットに対する処理ではこのフィールドは記録されません。 |
| CNID | 接続識別子 | TCP / IP 接続の一意のシステム識別子。 |
| CSIZ | コンテンツサイズ（ Content Size ） | チェックしたオブジェクトのサイズ（バイト単位）。バケットに対する処理ではこのフィールドは記録されません。 |
| HTRH | HTTP 要求ヘッダー | 設定時に選択した、ログに記録される HTTP 要求ヘッダーの名前と値のリスト。<br><br>• 注： * `X-Forwarded-For` は、要求に存在する場合、および存在する場合は自動的に含まれます `X-Forwarded-For` 値が要求送信者のIPアドレス（SAIP監査フィールド）と異なります。 |
| RSLT | 結果コード | GET トランザクションの結果。常に次の結果になります。<br><br>SUCS ：成功しました |
| S3AI | S3 テナントアカウント ID （要求の送信者） | 要求を送信したユーザのテナントアカウント ID 。空の値は匿名アクセスであることを示します。 |
| S3AK | S3 アクセスキー ID （要求の送信者） | 要求を送信したユーザのハッシュ済み S3 アクセスキー ID 。空の値は匿名アクセスであることを示します。 |

| コード | フィールド | 説明 |
| --- | --- | --- |
| S3BK | S3 バケット | S3 バケット名。 |
| S3KY | S3 キー | バケット名を除く S3 キーの名前。バケットに対する処理ではこのフィールドは記録されません。 |
| SACC | S3 テナントアカウント名（要求の送信者） | 要求を送信したユーザのテナントアカウントの名前。匿名の要求の場合は空です。 |
| saip | IP アドレス（要求送信者） | 要求を送信したクライアントアプリケーションの IP アドレス。 |
| SBAC | S3 テナントアカウント名（バケット所有者） | バケット所有者のテナントアカウント名。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。 |
| SBAI | S3 テナントアカウント ID （バケット所有者） | ターゲットバケットの所有者のテナントアカウント ID 。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。 |
| サスペンション | S3 ユーザの URN （要求の送信者） | 要求を送信しているユーザのテナントアカウント ID とユーザ名。ローカルユーザまたは LDAP ユーザです。例：<br>`urn:sgws:identity::03393893651506583485:root`<br><br>匿名の要求の場合は空です。 |
| 時間 | 時間 | 要求の合計処理時間（マイクロ秒）。 |
| TLIP | 信頼できるロードバランサの IP アドレス | 要求が信頼できるレイヤ 7 ロードバランサによってルーティングされた場合は、ロードバランサの IP アドレス。 |
| UUID | Universally Unique Identifier の略 | StorageGRID システム内でのオブジェクトの識別子。 |

| コード | フィールド | 説明 |
| --- | --- | --- |
| VSID | バージョン ID | 要求されたオブジェクトの特定のバージョンのバージョン ID 。バージョン管理されていないバケット内のバケットやオブジェクトに対する処理には、このフィールドは含まれません。 |

**SPO ： S3 POST**

S3クライアントがPOST Object restore要求を実行すると、オブジェクトをAWS Glacierストレージからクラウドストレージプールにリストアする要求が送信されます。このメッセージは、トランザクションが成功した場合にサーバによって出力されます。

| コード | フィールド | 説明 |
| --- | --- | --- |
| CBID | Content Block Identifier の略 | 要求されたコンテンツブロックの一意の識別子。CBID が不明な場合、このフィールドは 0 に設定されます。 |
| CNCH | 整合性制御ヘッダー | 要求に Consistency-Control HTTP 要求ヘッダーが存在する場合は、その値。 |
| CNID | 接続識別子 | TCP / IP 接続の一意のシステム識別子。 |
| CSIZ | コンテンツサイズ（ Content Size ） | 読み出されたオブジェクトのサイズ（バイト単位）。 |
| HTRH | HTTP 要求ヘッダー | 設定時に選択した、ログに記録される HTTP 要求ヘッダーの名前と値のリスト。<br><br>• 注： * `X-Forwarded-For` は、要求に存在する場合、および存在する場合は自動的に含まれます `X-Forwarded-For` 値が要求送信者のIPアドレス（SAIP監査フィールド）と異なります。 |
| RSLT | 結果コード | POST Object restore 要求の結果。常に次の結果になります。<br><br>SUCS ：成功しました |

| コード | フィールド | 説明 |
| --- | --- | --- |
| S3AI | S3 テナントアカウント ID （要求の送信者） | 要求を送信したユーザのテナントアカウント ID 。空の値は匿名アクセスであることを示します。 |
| S3AK | S3 アクセスキー ID （要求の送信者） | 要求を送信したユーザのハッシュ済み S3 アクセスキー ID 。空の値は匿名アクセスであることを示します。 |
| S3BK | S3 バケット | S3 バケット名。 |
| S3KY | S3 キー | バケット名を除く S3 キーの名前。バケットに対する処理ではこのフィールドは記録されません。 |
| S3SR | S3 サブリソース | 必要に応じて、処理対象のバケットまたはオブジェクトサブリソース。 |
| SACC | S3 テナントアカウント名（要求の送信者） | 要求を送信したユーザのテナントアカウントの名前。匿名の要求の場合は空です。 |
| saip | IP アドレス（要求送信者） | 要求を送信したクライアントアプリケーションの IP アドレス。 |
| SBAC | S3 テナントアカウント名（バケット所有者） | バケット所有者のテナントアカウント名。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。 |
| SBAI | S3 テナントアカウント ID （バケット所有者） | ターゲットバケットの所有者のテナントアカウント ID 。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。 |
| SRCF | サブリソースの設定 | リストア情報。 |
| サスペンション | S3 ユーザの URN （要求の送信者） | 要求を送信しているユーザのテナントアカウント ID とユーザ名。ローカルユーザまたは LDAP ユーザです。例： `urn:sgws:identity::03393893651506583485:root` 匿名の要求の場合は空です。 |

| コード | フィールド | 説明 |
| --- | --- | --- |
| 時間 | 時間 | 要求の合計処理時間（マイクロ秒）。 |
| TLIP | 信頼できるロードバランサの IP アドレス | 要求が信頼できるレイヤ 7 ロードバランサによってルーティングされた場合は、ロードバランサの IP アドレス。 |
| UUID | Universally Unique Identifier の略 | StorageGRID システム内でのオブジェクトの識別子。 |
| VSID | バージョン ID | 要求されたオブジェクトの特定のバージョンのバージョン ID 。バージョン管理されていないバケット内のバケットやオブジェクトに対する処理には、このフィールドは含まれません。 |

**SPUT ： S3 PUT**

S3 クライアントが PUT トランザクションを実行すると、新しいオブジェクトまたはバケットを作成する要求が送信されます。このメッセージは、トランザクションが成功した場合にサーバによって出力されます。

| コード | フィールド | 説明 |
| --- | --- | --- |
| CBID | Content Block Identifier の略 | 要求されたコンテンツブロックの一意の識別子。CBID が不明な場合、このフィールドは 0 に設定されます。バケットに対する処理ではこのフィールドは記録されません。 |
| CMP | コンプライアンス設定 | バケットを作成する際に使用された準拠設定（ PUT Bucket 要求にこの設定がある場合、最初の 1024 文字に切り詰められます）。 |
| CNCH | 整合性制御ヘッダー | 要求に Consistency-Control HTTP 要求ヘッダーが存在する場合は、その値。 |
| CNID | 接続識別子 | TCP / IP 接続の一意のシステム識別子。 |

| コード | フィールド | 説明 |
| --- | --- | --- |
| CSIZ | コンテンツサイズ（ Content Size ） | 読み出されたオブジェクトのサイズ（バイト単位）。バケットに対する処理ではこのフィールドは記録されません。 |
| HTRH | HTTP 要求ヘッダー | 設定時に選択した、ログに記録される HTTP 要求ヘッダーの名前と値のリスト。<br><br>• 注： * `X-Forwarded-For` は、要求に存在する場合、および存在する場合は自動的に含まれます `X-Forwarded-For` 値が要求送信者のIPアドレス（SAIP監査フィールド）と異なります。 |
| LKEN | オブジェクトロックが有効になりました | 要求ヘッダーの値 `x-amz-bucket-object-lock-enabled`に設定されている場合は、PUT Bucket要求に。 |
| LKLH | オブジェクトロックリーガルホールド | 要求ヘッダーの値 `x-amz-object-lock-legal-hold`に設定されている場合は、PUT Object要求に。 |
| LKMD | オブジェクトロック保持モード | 要求ヘッダーの値 `x-amz-object-lock-mode`に設定されている場合は、PUT Object要求に。 |
| LKRU | オブジェクトロック終了日まで保持 | 要求ヘッダーの値 `x-amz-object-lock-retain-until-date`に設定されている場合は、PUT Object要求に。 |
| MTME | 最終変更時刻 | オブジェクトが最後に変更された日時を示す Unix タイムスタンプ（マイクロ秒）。 |
| RSLT | 結果コード | PUT トランザクションの結果。常に次の結果になります。<br><br>SUCS ：成功しました |
| S3AI | S3 テナントアカウント ID （要求の送信者） | 要求を送信したユーザのテナントアカウント ID 。空の値は匿名アクセスであることを示します。 |

| コード | フィールド | 説明 |
| --- | --- | --- |
| S3AK | S3 アクセスキー ID （要求の送信者） | 要求を送信したユーザのハッシュ済み S3 アクセスキー ID 。空の値は匿名アクセスであることを示します。 |
| S3BK | S3 バケット | S3 バケット名。 |
| S3KY | S3KY | バケット名を除く S3 キーの名前。バケットに対する処理ではこのフィールドは記録されません。 |
| S3SR | S3 サブリソース | 必要に応じて、処理対象のバケットまたはオブジェクトサブリソース。 |
| SACC | S3 テナントアカウント名（要求の送信者） | 要求を送信したユーザのテナントアカウントの名前。匿名の要求の場合は空です。 |
| saip | IP アドレス（要求送信者） | 要求を送信したクライアントアプリケーションの IP アドレス。 |
| SBAC | S3 テナントアカウント名（バケット所有者） | バケット所有者のテナントアカウント名。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。 |
| SBAI | S3 テナントアカウント ID （バケット所有者） | ターゲットバケットの所有者のテナントアカウント ID 。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。 |
| SRCF | サブリソースの設定 | 新しいサブリソース設定（最初の 1024 文字に切り詰められます）。 |
| サスペンション | S3 ユーザの URN （要求の送信者） | 要求を送信しているユーザのテナントアカウント ID とユーザ名。ローカルユーザまたは LDAP ユーザです。例：<br>`urn:sgws:identity::03393893651506583485:root`<br><br>匿名の要求の場合は空です。 |
| 時間 | 時間 | 要求の合計処理時間（マイクロ秒）。 |

| コード | フィールド | 説明 |
| --- | --- | --- |
| TLIP | 信頼できるロードバランサの IP アドレス | 要求が信頼できるレイヤ 7 ロードバランサによってルーティングされた場合は、ロードバランサの IP アドレス。 |
| ULID | ID をアップロードします | Complete Multipart Upload 処理の SPUT メッセージのみに含まれます。すべてのパーツがアップロードされ、アセンブルされたことを示します。 |
| UUID | Universally Unique Identifier の略 | StorageGRID システム内でのオブジェクトの識別子。 |
| VSID | バージョン ID | バージョン管理されたバケットで作成された新しいオブジェクトのバージョン ID 。バージョン管理されていないバケット内のバケットやオブジェクトに対する処理には、このフィールドは含まれません。 |
| VSST | バージョン管理の状態 | バケットの新しいバージョン管理状態。「 enabled 」または「 suspended 」のどちらかです。 オブジェクトに関する処理ではこのフィールドは記録されません。 |

**SREM** ：オブジェクトストアの削除

このメッセージは、コンテンツが永続的ストレージから削除され、通常の API でアクセスできなくなった場合に表示されます。

| コード | フィールド | 説明 |
| --- | --- | --- |
| CBID | Content Block Identifier の略 | 永続的ストレージから削除されたコンテンツブロックの一意の識別子。 |
| RSLT | 結果コード | コンテンツ削除処理の結果を示します。次の値のみが定義されています。<br><br>SUCS ：コンテンツが永続的ストレージから削除されました |

この監査メッセージは、指定されたコンテンツブロックがノードから削除され、直接要求できなくなったこと

を意味します。このメッセージを使用して、システム内の削除されたコンテンツのフローを追跡できます。

**SUPD** ： **S3** メタデータが更新されました

このメッセージは、 S3 クライアントが取り込まれたオブジェクトのメタデータを更新したときに S3 API によって生成されます。このメッセージは、メタデータの更新が成功した場合にサーバによって出力されます。

| コード | フィールド | 説明 |
| --- | --- | --- |
| CBID | Content Block Identifier の略 | 要求されたコンテンツブロックの一意の識別子。CBID が不明な場合、このフィールドは 0 に設定されます。バケットに対する処理ではこのフィールドは記録されません。 |
| CNCH | 整合性制御ヘッダー | バケットの準拠設定の更新時に要求に Consistency-Control HTTP 要求ヘッダーが存在する場合は、その値。 |
| CNID | 接続識別子 | TCP / IP 接続の一意のシステム識別子。 |
| CSIZ | コンテンツサイズ（ Content Size ） | 読み出されたオブジェクトのサイズ（バイト単位）。バケットに対する処理ではこのフィールドは記録されません。 |
| HTRH | HTTP 要求ヘッダー | 設定時に選択した、ログに記録される HTTP 要求ヘッダーの名前と値のリスト。<br><br>• 注： * `X-Forwarded-For` は、要求に存在する場合、および存在する場合は自動的に含まれます `X-Forwarded-For` 値が要求送信者のIPアドレス（SAIP監査フィールド）と異なります。 |
| RSLT | 結果コード | GET トランザクションの結果。常に次の結果になります。<br><br>SUCS ：成功しました |
| S3AI | S3 テナントアカウント ID （要求の送信者） | 要求を送信したユーザのテナントアカウント ID 。空の値は匿名アクセスであることを示します。 |

| コード | フィールド | 説明 |
| --- | --- | --- |
| S3AK | S3 アクセスキー ID （要求の送信者） | 要求を送信したユーザのハッシュ済み S3 アクセスキー ID 。空の値は匿名アクセスであることを示します。 |
| S3BK | S3 バケット | S3 バケット名。 |
| S3KY | S3 キー | バケット名を除く S3 キーの名前。バケットに対する処理ではこのフィールドは記録されません。 |
| SACC | S3 テナントアカウント名（要求の送信者） | 要求を送信したユーザのテナントアカウントの名前。匿名の要求の場合は空です。 |
| saip | IP アドレス（要求送信者） | 要求を送信したクライアントアプリケーションの IP アドレス。 |
| SBAC | S3 テナントアカウント名（バケット所有者） | バケット所有者のテナントアカウント名。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。 |
| SBAI | S3 テナントアカウント ID （バケット所有者） | ターゲットバケットの所有者のテナントアカウント ID 。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。 |
| サスペンション | S3 ユーザの URN （要求の送信者） | 要求を送信しているユーザのテナントアカウント ID とユーザ名。ローカルユーザまたは LDAP ユーザです。例： `urn:sgws:identity::03393893651506583485:root`<br><br>匿名の要求の場合は空です。 |
| 時間 | 時間 | 要求の合計処理時間（マイクロ秒）。 |
| TLIP | 信頼できるロードバランサの IP アドレス | 要求が信頼できるレイヤ 7 ロードバランサによってルーティングされた場合は、ロードバランサの IP アドレス。 |

| コード | フィールド | 説明 |
| --- | --- | --- |
| UUID | Universally Unique Identifier の略 | StorageGRID システム内でのオブジェクトの識別子。 |
| VSID | バージョン ID | メタデータが更新されたオブジェクトの特定のバージョンのバージョン ID 。バージョン管理されていないバケット内のバケットやオブジェクトに対する処理には、このフィールドは含まれません。 |

**SVRF** ：オブジェクトストアの検証に失敗しました

このメッセージは、コンテンツブロックが検証プロセスに失敗したときに生成されます。レプリケートされたオブジェクトデータがディスクに対して読み書きされるたびに、要求元ユーザに送信されるデータがシステムにもともと取り込まれたデータと同一であることを確認するために複数の検証チェックと整合性チェックが実行されます。これらのチェックのいずれかが失敗した場合、破損したレプリケートオブジェクトデータは再び読み出されないように自動的に隔離されます。

| コード | フィールド | 説明 |
| --- | --- | --- |
| CBID | Content Block Identifier の略 | 検証に失敗したコンテンツブロックの一意の識別子。 |

| コード | フィールド | 説明 |
| --- | --- | --- |
| RSLT | 結果コード | 検証失敗のタイプ：<br><br>CRCF ：巡回冗長検査（ CRC ）が失敗しました。<br><br>HMAC ：ハッシュベースのメッセージ認証コード（ HMAC ）チェックが失敗しました。<br><br>EHSH ：暗号化されたコンテンツハッシュが想定外です。<br><br>PHSH ：元のコンテンツハッシュが想定外です。<br><br>SEQC ：ディスク上のデータシーケンスが正しくありません。<br><br>PERR ：ディスクファイルの構造が無効です。<br><br>DERR ：ディスクエラーです。<br><br>FNAM ：ファイル名が無効です。 |

- 注： * このメッセージは注意深く監視する必要があります。コンテンツ検証が失敗する場合、コンテンツが改ざんされようとしている可能性や、ハードウェア障害が近いうちに発生する可能性があり

メッセージをトリガーした処理を確認するには、 AMID （ Module ID ）フィールドの値を参照してください。たとえば、 SVFY はバックグラウンド検証である Storage Verifier モジュールによってメッセージが生成されたことを示し、 STOR はコンテンツの読み出しによってメッセージがトリガーされたことを示します。

**SVRU** ：オブジェクトストア検証が不明です

LDR サービスのストレージコンポーネントは、オブジェクトストア内のレプリケートされたオブジェクトデータのすべてのコピーを継続的にスキャンします。このメッセージは、レプリケートされたオブジェクトデータの不明または想定外のコピーがオブジェクトストアで検出されて隔離ディレクトリに移動されたときに生成されます。

| コード | フィールド | 説明 |
| --- | --- | --- |
| FPTH | ファイルパス | 想定外のオブジェクトコピーのファイルパス。 |

| コード | フィールド | 説明 |
| --- | --- | --- |
| RSLT | 結果 | このフィールドの値は「 NONE 」です。RSLT は必須のメッセージフィールドですが、このメッセージには該当しません。このメッセージがフィルタリングされないように、「 UCS 」ではなく「 none 」が使用されます。 |

- 注： * SVRU ： Object Store Verify Unknown 監査メッセージは注意深く監視する必要があります。オブジェクトストアでオブジェクトデータの想定外のコピーが検出されたことを意味します。コンテンツが改ざんされようとしている可能性や、ハードウェア障害が近いうちに発生する可能性があるため、ただちに状況を調査してこれらのコピーが作成された経緯を特定する必要があります。

**SYSD** ：ノード停止

サービスが正常に停止されると、シャットダウンが要求されたことを示すためにこのメッセージが生成されます。監査メッセージキューはシャットダウン前にクリアされないため、通常このメッセージはその後の再起動後に送信されます。サービスが再起動していない場合は、シャットダウンシーケンスの最初に送信された SYST メッセージを確認します。

| コード | フィールド | 説明 |
| --- | --- | --- |
| RSLT | シャットダウンをクリーニングします | シャットダウンのタイプ：<br><br>SUCS ：システムはクリーンシャットダウンされました。 |

このメッセージが示すのはレポート元のサービスの停止のみで、ホストサーバの停止については示されません。SYSD メッセージはクリーンシャットダウンによってのみ生成されるため、 RSLT がダーティーシャットダウンを示すことはありません。

**SYST** ：ノードを停止しています

サービスが正常に停止されると、シャットダウンが要求されてサービスがシャットダウンシーケンスを開始したことを示すためにこのメッセージが生成されます。SYST を使用すると、シャットダウンが要求されたかどうかをサービスが再起動される前に特定できます（ SYSD は通常、サービスの再起動後に送信されます）。

| コード | フィールド | 説明 |
| --- | --- | --- |
| RSLT | シャットダウンをクリーニングします | シャットダウンのタイプ：<br><br>SUCS ：システムはクリーンシャットダウンされました。 |

このメッセージが示すのはレポート元のサービスの停止のみで、ホストサーバの停止については示されませ

ん。SYST メッセージはクリーンシャットダウンによってのみ生成されるため、メッセージの RSLT がダーティーシャットダウンを示すことはありません。

**SYSU** ：ノードが開始されました

サービスが再起動されると、前回のシャットダウンがクリーン（コマンドによるもの）か不規則（想定外）かを示すためにこのメッセージが生成されます。

| コード | フィールド | 説明 |
| --- | --- | --- |
| RSLT | シャットダウンをクリーニングします | シャットダウンのタイプ：<br><br>SUCS ：システムはクリーンシャットダウンされました。<br><br>DSDN ：システムはクリーンシャットダウンされませんでした。<br><br>VRGN ：サーバインストール（または再インストール）後の初めての起動です。 |

このメッセージが示すのはレポート元のサービスの起動のみで、ホストサーバの起動については示されません。このメッセージは、次の場合に使用できます。

- 監査証跡における不連続を検出します。
- サービスが処理中に失敗していないかどうかを確認します（ StorageGRID システムの分散によってこれらのエラーが隠されることがあります）。失敗したサービスは、 Server Manager によって自動的に再開されます。

**VLST** ：ユーザーが開始したボリュームが失われました

このメッセージは、が発行するたびに発行されます `/proc/CMSI/Volume_Lost` コマンドが実行されます。

| コード | フィールド | 説明 |
| --- | --- | --- |
| VOLL | Volume Identifier （ボリューム識別子）下限 | 影響を受けるボリューム範囲の下端、または単一ボリューム。 |
| volu | ボリューム識別子上限 | 影響を受けるボリューム範囲の終了 ID 。単一ボリュームの場合は VOLL と同じです。 |
| NOID | ソースノード ID | 場所が失われたノード ID 。 |

| コード | フィールド | 説明 |
| --- | --- | --- |
| LTYP | 保管場所タイプ | 「 CLDI 」（オンライン）または「 CLNL 」（ニアライン）。指定しない場合、デフォルトは「 CLDI 」です。 |
| RSLT | 結果 | 常に「 NONE 」。RSLT は必須のメッセージフィールドですが、このメッセージには該当しません。このメッセージがフィルタリングされないように、「 UCS 」ではなく「 none 」が使用されます。 |

**WDEL** ： **Swift** の削除

Swift クライアントが DELETE トランザクションを実行すると、指定したオブジェクトまたはコンテナを削除する要求が送信されます。このメッセージは、トランザクションが成功した場合にサーバによって出力されます。

| コード | フィールド | 説明 |
| --- | --- | --- |
| CBID | Content Block Identifier の略 | 要求されたコンテンツブロックの一意の識別子。CBID が不明な場合、このフィールドは 0 に設定されます。コンテナに関する処理ではこのフィールドは記録されません。 |
| CSIZ | コンテンツサイズ（ Content Size ） | 削除されたオブジェクトのサイズ（バイト単位）。コンテナに関する処理ではこのフィールドは記録されません。 |
| HTRH | HTTP 要求ヘッダー | 設定時に選択した、ログに記録される HTTP 要求ヘッダーの名前と値のリスト。<br><br>• 注： * `X-Forwarded-For` は、要求に存在する場合、および に存在する場合は自動的に含まれます `X-Forwarded-For` 値が要求送信者のIPアドレス（SAIP監査フィールド）と異なります。 |
| MTME | 最終変更時刻 | オブジェクトが最後に変更された日時を示す Unix タイムスタンプ（マイクロ秒）。 |

| コード | フィールド | 説明 |
| --- | --- | --- |
| RSLT | 結果コード | DELETE トランザクションの結果。常に次の結果になります。<br><br>SUCS ：成功しました |
| saip | 要求元クライアントの IP アドレス | 要求を送信したクライアントアプリケーションの IP アドレス。 |
| 時間 | 時間 | 要求の合計処理時間（マイクロ秒）。 |
| TLIP | 信頼できるロードバランサの IP アドレス | 要求が信頼できるレイヤ 7 ロードバランサによってルーティングされた場合は、ロードバランサの IP アドレス。 |
| UUID | Universally Unique Identifier の略 | StorageGRID システム内でのオブジェクトの識別子。 |
| WACC | Swift アカウント ID | StorageGRID システムによって指定された一意のアカウント ID 。 |
| WCON | Swift コンテナ | Swift コンテナ名。 |
| WOBJ | Swift オブジェクト | Swift オブジェクトの識別子。コンテナに関する処理ではこのフィールドは記録されません。 |
| WUSR | Swift アカウントユーザ | トランザクションを実行するクライアントを一意に識別する Swift アカウントのユーザ名。 |

**wget ： Swift GET**

Swift クライアントが GET トランザクションを実行すると、オブジェクトを読み出す、コンテナ内のオブジェクトを一覧表示する、またはアカウント内のコンテナを一覧表示する要求が送信されます。このメッセージは、トランザクションが成功した場合にサーバによって出力されます。

| コード | フィールド | 説明 |
| --- | --- | --- |
| CBID | Content Block Identifier の略 | 要求されたコンテンツブロックの一意の識別子。CBID が不明な場合、このフィールドは 0 に設定されます。アカウントおよびコンテナに関する処理ではこのフィールドは記録されません。 |
| CSIZ | コンテンツサイズ（ Content Size ） | 読み出されたオブジェクトのサイズ（バイト単位）。アカウントおよびコンテナに関する処理ではこのフィールドは記録されません。 |
| HTRH | HTTP 要求ヘッダー | 設定時に選択した、ログに記録される HTTP 要求ヘッダーの名前と値のリスト。<br><br>• 注：* `X-Forwarded-For` は、要求に存在する場合、およびに存在する場合は自動的に含まれます `X-Forwarded-For` 値が要求送信者のIPアドレス（SAIP監査フィールド）と異なります。 |
| RSLT | 結果コード | GET トランザクションの結果。結果は常にです<br><br>SUCS ：成功しました |
| saip | 要求元クライアントの IP アドレス | 要求を送信したクライアントアプリケーションの IP アドレス。 |
| 時間 | 時間 | 要求の合計処理時間（マイクロ秒）。 |
| TLIP | 信頼できるロードバランサの IP アドレス | 要求が信頼できるレイヤ 7 ロードバランサによってルーティングされた場合は、ロードバランサの IP アドレス。 |
| UUID | Universally Unique Identifier の略 | StorageGRID システム内でのオブジェクトの識別子。 |
| WACC | Swift アカウント ID | StorageGRID システムによって指定された一意のアカウント ID 。 |

| コード | フィールド | 説明 |
| --- | --- | --- |
| WCON | Swift コンテナ | Swift コンテナ名。アカウントに関する処理ではこのフィールドは記録されません。 |
| WOBJ | Swift オブジェクト | Swift オブジェクトの識別子。アカウントおよびコンテナに関する処理ではこのフィールドは記録されません。 |
| WUSR | Swift アカウントユーザ | トランザクションを実行するクライアントを一意に識別する Swift アカウントのユーザ名。 |

**WHEA** ： **Swift** ヘッド

Swift クライアントが HEAD トランザクションを実行すると、アカウント、コンテナ、またはオブジェクトの存在をチェックし、関連するメタデータを読み出す要求が送信されます。このメッセージは、トランザクションが成功した場合にサーバによって出力されます。

| コード | フィールド | 説明 |
| --- | --- | --- |
| CBID | Content Block Identifier の略 | 要求されたコンテンツブロックの一意の識別子。CBID が不明な場合、このフィールドは 0 に設定されます。アカウントおよびコンテナに関する処理ではこのフィールドは記録されません。 |
| CSIZ | コンテンツサイズ（ Content Size ） | 読み出されたオブジェクトのサイズ（バイト単位）。アカウントおよびコンテナに関する処理ではこのフィールドは記録されません。 |
| HTRH | HTTP 要求ヘッダー | 設定時に選択した、ログに記録される HTTP 要求ヘッダーの名前と値のリスト。<br><br>• 注： `* X-Forwarded-For` は、要求に存在する場合、およびに存在する場合は自動的に含まれます `X-Forwarded-For` 値が要求送信者のIPアドレス（SAIP監査フィールド）と異なります。 |

| コード | フィールド | 説明 |
| --- | --- | --- |
| RSLT | 結果コード | HEAD トランザクションの結果。常に次の結果になります。<br><br>SUCS ：成功しました |
| saip | 要求元クライアントの IP アドレス | 要求を送信したクライアントアプリケーションの IP アドレス。 |
| 時間 | 時間 | 要求の合計処理時間（マイクロ秒）。 |
| TLIP | 信頼できるロードバランサの IP アドレス | 要求が信頼できるレイヤ 7 ロードバランサによってルーティングされた場合は、ロードバランサの IP アドレス。 |
| UUID | Universally Unique Identifier の略 | StorageGRID システム内でのオブジェクトの識別子。 |
| WACC | Swift アカウント ID | StorageGRID システムによって指定された一意のアカウント ID 。 |
| WCON | Swift コンテナ | Swift コンテナ名。アカウントに関する処理ではこのフィールドは記録されません。 |
| WOBJ | Swift オブジェクト | Swift オブジェクトの識別子。アカウントおよびコンテナに関する処理ではこのフィールドは記録されません。 |
| WUSR | Swift アカウントユーザ | トランザクションを実行するクライアントを一意に識別する Swift アカウントのユーザ名。 |

**WPUT ： Swift PUT**

Swift クライアントが PUT トランザクションを実行すると、新しいオブジェクトまたはコンテナを作成する要求が送信されます。このメッセージは、トランザクションが成功した場合にサーバによって出力されます。

| コード | フィールド | 説明 |
| --- | --- | --- |
| CBID | Content Block Identifier の略 | 要求されたコンテンツブロックの一意の識別子。CBID が不明な場合、このフィールドは 0 に設定されます。コンテナに関する処理ではこのフィールドは記録されません。 |
| CSIZ | コンテンツサイズ（ Content Size ） | 読み出されたオブジェクトのサイズ（バイト単位）。コンテナに関する処理ではこのフィールドは記録されません。 |
| HTRH | HTTP 要求ヘッダー | 設定時に選択した、ログに記録される HTTP 要求ヘッダーの名前と値のリスト。<br><br>• 注： `*X-Forwarded-For` は、要求に存在する場合、および `X-Forwarded-For` 値が要求送信者のIPアドレス（SAIP監査フィールド）と異なります。 |
| MTME | 最終変更時刻 | オブジェクトが最後に変更された日時を示す Unix タイムスタンプ（マイクロ秒）。 |
| RSLT | 結果コード | PUT トランザクションの結果。常に次の結果になります。<br><br>SUCS ：成功しました |
| saip | 要求元クライアントの IP アドレス | 要求を送信したクライアントアプリケーションの IP アドレス。 |
| 時間 | 時間 | 要求の合計処理時間（マイクロ秒）。 |
| TLIP | 信頼できるロードバランサの IP アドレス | 要求が信頼できるレイヤ 7 ロードバランサによってルーティングされた場合は、ロードバランサの IP アドレス。 |
| UUID | Universally Unique Identifier の略 | StorageGRID システム内でのオブジェクトの識別子。 |

| コード | フィールド | 説明 |
| --- | --- | --- |
| WACC | Swift アカウント ID | StorageGRID システムによって指定された一意のアカウント ID 。 |
| WCON | Swift コンテナ | Swift コンテナ名。 |
| WOBJ | Swift オブジェクト | Swift オブジェクトの識別子。コンテナに関する処理ではこのフィールドは記録されません。 |
| WUSR | Swift アカウントユーザ | トランザクションを実行するクライアントを一意に識別する Swift アカウントのユーザ名。 |

# メンテナンス

## グリッドを展開します

システムの運用を中断することなくStorageGRID システムを拡張する方法をご紹介します。

- "StorageGRID 拡張の計画"
- "拡張の準備"
- "拡張手順 の概要"
- "ストレージノードへのストレージボリュームの追加"
- "既存のサイトへのグリッドノードの追加と新しいサイトの追加"
- "拡張後のStorageGRID システムの設定"
- "テクニカルサポートにお問い合わせください"

### StorageGRID 拡張の計画

StorageGRID を拡張して、ストレージ容量の拡張、メタデータ容量の追加、冗長性や新機能の追加、新しいサイトの追加を行うことができます。追加する必要があるノードの数、タイプ、場所は、拡張の理由によって異なります。

- "ストレージ容量を追加しています"
- "メタデータ容量の追加"
- "システムの機能を追加するためのグリッドノードの追加"
- "新しいサイトを追加しています"

ストレージ容量を追加しています

既存のストレージノードがいっぱいになったら、StorageGRID システムのストレージ容量を増やす必要があります。

ストレージ容量を増やすには、まずデータの格納場所を把握し、必要なすべての場所に容量を追加する必要があります。たとえば、オブジェクトデータのコピーを複数のサイトに格納している場合は、各サイトのストレージ容量の拡張が必要になることがあります。

- "オブジェクト容量を追加する場合のガイドラインを次に示します"
- "レプリケートオブジェクトにストレージ容量を追加しています"
- "イレイジャーコーディングオブジェクトのストレージ容量の追加"
- "イレイジャーコーディングデータのリバランシングに関する考慮事項"

# StorageGRID システムのオブジェクトストレージ容量を拡張するには、既存のストレージノードにストレージボリュームを追加するか、または既存のサイトに新しいストレージノードを追加します。情報ライフサイクル管理（ ILM ）ポリシーの要件を満たす方法でストレージ容量を追加する必要があります。

## ストレージボリュームの追加に関するガイドラインを次に示します

既存のストレージノードにストレージボリュームを追加する前に、次のガイドラインと制限事項を確認してください。

- 現在の ILM ルールを調べて、ストレージボリュームを追加してレプリケートオブジェクトまたはイレイジャーコーディングオブジェクトに使用できるストレージを増やす場所とタイミングを決定する必要があります。情報ライフサイクル管理を使用してオブジェクトを管理する手順を参照してください。
- オブジェクトメタデータはボリューム 0 にしか格納されないため、ストレージボリュームを追加してシステムのメタデータ容量を増やすことはできません。
- 各ソフトウェアベースのストレージノードでサポートされるストレージボリュームは最大 16 個です。それよりも多くの容量が必要な場合は、新しいストレージノードを追加する必要があります。
- 各 SG6060 アプライアンスには、 1 台または 2 台の拡張シェルフを追加できます。各拡張シェルフには、 16 個のストレージボリュームが追加されます。両方の拡張シェルフを設置した場合、 SG6060 では合計 48 個のストレージボリュームをサポートできます。
- ストレージボリュームを他のストレージアプライアンスに追加することはできません。
- 既存のストレージボリュームのサイズを拡張することはできません。
- ストレージノードへのストレージボリュームの追加は、システムのアップグレードやリカバリの処理や他の拡張と同時に実行することはできません。

ストレージボリュームを追加することにし、 ILM ポリシーを満たすために拡張する必要があるストレージノードを決めたら、該当するタイプのストレージノードの手順に従います。

- 拡張シェルフをSG6060ストレージアプライアンスに追加するには、SG6000アプライアンスの設置およびメンテナンス手順を参照してください。

  "SG6000 ストレージアプライアンス"

- ソフトウェアベースのノードの場合は、ストレージノードにストレージボリュームを追加する手順に従います。

  "ストレージノードへのストレージボリュームの追加"

## ストレージノードの追加に関するガイドラインを次に示します

既存のサイトにストレージノードを追加する前に、次のガイドラインと制限事項を確認してください。

- 現在の ILM ルールを調べて、ストレージノードを追加してレプリケートオブジェクトまたはイレイジャーコーディングオブジェクトに使用できるストレージを増やす場所とタイミングを決定する必要があります。
- 1 つの拡張手順 に追加できるストレージノードは 10 個までです。

- 単一の拡張手順 で複数のサイトにストレージノードを追加することができます。
- 1 つの拡張手順 で、ストレージノードとその他のタイプのノードを追加できます。
- 拡張手順 を開始する前に、リカバリの一環として実行されるデータ修復処理がすべて完了したことを確認する必要があります。リカバリとメンテナンスの手順のデータ修復ジョブを確認する手順を参照してください。
- 拡張の実行前または実行後にストレージノードを削除する必要がある場合は、 1 つの運用停止ノード手順の 10 個を超えるストレージノードの運用を停止しないでください。

ストレージノード上の**ADC**サービスについてのガイドラインを参照してください

拡張を設定する場合は、新しい各ストレージノードに Administrative Domain Controller （ ADC ）サービスを含めるかどうかを選択する必要があります。ADC サービスは、グリッドサービスの場所と可用性を追跡します。

- StorageGRID システムでは、各サイトで ADC サービスのクォーラムが常に利用可能である必要があります。

  リカバリとメンテナンスの手順のADCクォーラムに関する情報を参照してください。

- 各サイトで少なくとも 3 つのストレージノードに ADC サービスが含まれている必要があります。
- すべてのストレージノードに ADC サービスを追加することは推奨されません。ノード間の通信量が増加しているため、 ADC サービスが多すぎると原因 の速度が低下する可能性があります。
- 1 つのグリッドに ADC サービスがあるストレージノードが 48 個を超えないようにします。各サイトに ADC サービスが 3 つある 16 のサイトに相当します。
- 一般に、新しいノードの * ADC Service * 設定を選択する場合は、 * Automatic * を選択してください。ADC サービスを含む別のストレージノードを新しいノードで置き換える場合にのみ、「 * Yes 」を選択します。残りの ADC サービスの数が少なすぎるとストレージノードの運用を停止できないため、古いサービスが削除される前に新しい ADC サービスが利用可能になります。
- 導入後のノードに ADC サービスを追加することはできません。
- 関連情報 *

"ILM を使用してオブジェクトを管理する"

"SG6000 ストレージアプライアンス"

"ストレージノードへのストレージボリュームの追加"

""

"拡張の実施"

レプリケートオブジェクトにストレージ容量を追加しています

## 環境の情報ライフサイクル管理（ ILM ）ポリシーに、オブジェクトのレプリケートコピーを作成するルールが含まれている場合は、追加するストレージの量と、新しいストレージボリュームまたはストレージノードの追加先を検討する必要があります。

ストレージを追加する場所については、レプリケートコピーを作成する ILM ルールを確認してください。ILM

ルールで複数のオブジェクトコピーが作成される場合は、オブジェクトコピーが作成されるそれぞれの場所にストレージを追加することを検討してください。単純な例として、 2 サイトグリッドがあり、各サイトにオブジェクトコピーを 1 つ作成する ILM ルールがある場合は、グリッドの全体的なオブジェクト容量を増やすために各サイトにストレージを追加する必要があります。

パフォーマンス上の理由から、サイト間でストレージ容量と処理能力のバランスを維持することをお勧めします。そのため、この例では、各サイトに同じ数のストレージノードを追加するか、各サイトにストレージボリュームを追加する必要があります。

より複雑な ILM ポリシーで、バケット名などの条件に基づいてオブジェクトを別々の場所に配置するルールや、オブジェクトの場所を一定期間変更するルールが含まれている場合は、拡張に必要なストレージについての分析も似ていますが、より複雑です。

全体的なストレージ容量がどれだけ早く消費されるかを記録しておくと、拡張に必要なストレージ容量や、追加のストレージ容量が必要になる時期を把握するのに役立ちます。グリッドマネージャを使用して、StorageGRID の監視とトラブルシューティングの手順に従って、ストレージ容量を監視し、グラフ化することができます。

拡張をいつ実施するかを計画するときは、追加のストレージを調達して設置するのにどれくらいの時間がかかるかを考慮する必要があります。

- 関連情報 *

"ILM を使用してオブジェクトを管理する"

"トラブルシューティングを監視します"

イレイジャーコーディングオブジェクトのストレージ容量の追加

## イレイジャーコーディングコピーを作成するルールが ILM ポリシーに含まれている場合は、新しいストレージの追加場所と新しいストレージを追加するタイミングを計画する必要があります。追加するストレージの量や追加のタイミングによって、グリッドの使用可能なストレージ容量が左右される場合があります。

ストレージ拡張を計画するための最初の手順は、イレイジャーコーディングオブジェクトを作成する ILM ポリシーのルールを調べることです。StorageGRID はイレイジャーコーディングされた各オブジェクト用に _k+m_fragments を作成して各フラグメントを別のストレージノードに格納するため、拡張後にイレイジャーコーディングされた新しいデータ用のスペースを少なくとも -k +m_Storage ノードに確保する必要があります。イレイジャーコーディングプロファイルでサイト障害から保護されている場合は、各サイトにストレージを追加する必要があります。

追加する必要があるノードの数は、拡張を実施する時点での既存のノードの使用状況によっても異なります。

イレイジャーコーディングオブジェクト用のストレージ容量の追加に関する一般的な推奨事項

詳細な計算を行わない場合は、既存のストレージノードの容量が 70% に達した時点で各サイトに 2 つのストレージノードを追加できます。

この一般的な推奨事項は、単一サイトのグリッドとイレイジャーコーディングによってサイト障害から保護されるグリッドの両方で、広範なイレイジャーコーディングスキームに渡って合理的な結果を提供します。

この推奨事項につながる要因を理解したり、サイトのより正確な計画を作成したりするには、次のセクション

を参照してください。状況に応じて最適化されたカスタムの推奨事項については、ネットアップの営業担当者にお問い合わせください。

### イレイジャーコーディングオブジェクト用に追加する拡張ストレージノードの数を計算します

イレイジャーコーディングオブジェクトを格納する環境の拡張方法を最適化するには、次の多くの要素を考慮する必要があります。

- イレイジャーコーディングスキームを使用中です
- イレイジャーコーディングに使用されるストレージプールの特徴。各サイトのノードの数と各ノードの空きスペースの量など
- グリッドが以前に拡張されたかどうか（ストレージノードあたりの空きスペースがすべてのノードでほぼ同じでない場合があるため）
- ILM ポリシーの正確な内容。 ILM ルールがレプリケートオブジェクトとイレイジャーコーディングオブジェクトの両方を作成するかどうかなど

次の例は、イレイジャーコーディングスキームによる影響、ストレージプール内のノードの数、各ノードの空きスペースの量を把握するのに役立ちます。

同様の考慮事項は、レプリケートデータとイレイジャーコーディングデータの両方を格納する ILM ポリシーの計算、および以前に拡張されたグリッドの計算に影響します。

> ここでは、 StorageGRID システムにストレージ容量を追加する場合のベストプラクティスを紹介します。推奨さ手順 れる数のノードを追加できない場合は、 EC のリバランシングを実行して、イレイジャーコーディングオブジェクトを追加で格納できるようにする必要があります。
>
> "イレイジャーコーディングデータのリバランシングに関する考慮事項"

#### 例**1**：**2+1**イレイジャーコーディングを使用する**1**サイトグリッドを拡張する

この例は、ストレージノードが 3 つだけのシンプルなグリッドを拡張する方法を示しています。

> この例では、簡易化のためにストレージノードを 3 つだけ使用していますただし、使用するストレージノードは 3 つだけにすることは推奨されません。実際の本番環境のグリッドでは、冗長性を確保するために最低でも *k*+*m*+1 のストレージノードを使用する必要があります。この例では 4 つのストレージノード（ 2+1 ）に相当します。

以下を想定しています。

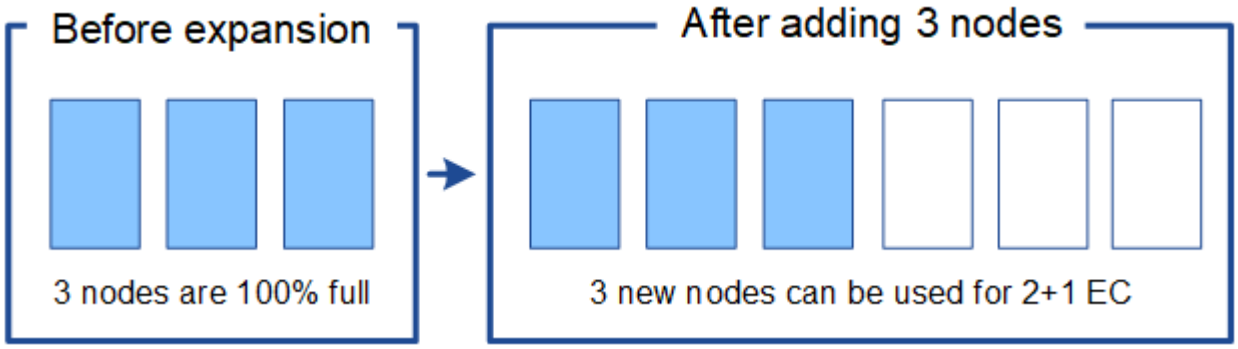
- すべてのデータは 2+1 イレイジャーコーディングスキームを使用して格納されます。2+1 イレイジャーコーディングスキームでは、すべてのオブジェクトが 3 つのフラグメントとして格納され、各フラグメントが別々のストレージノードに保存されます。
- 1 つのサイトに 3 つのストレージノードがあります。各ストレージノードの総容量は 100TB です。
- 新しい 100TB のストレージノードを追加して拡張します。
- 最終的には、イレイジャーコーディングされたデータを古いノードと新しいノードに分散したい。

拡張を実施する際のストレージノードの使用状況に応じて、いくつかのオプションがあります。

- * 既存のノードが 100% 使用されている場合は、 100TB のストレージノードを 3 つ追加します *

  この例では、既存のノードが 100% フルであることを示します。空き容量がないため、すぐに 3 つのノードを追加して 2+1 イレイジャーコーディングを続行する必要があります。

  拡張の完了後、オブジェクトがイレイジャーコーディングされると、すべてのフラグメントが新しいノードに配置されます。

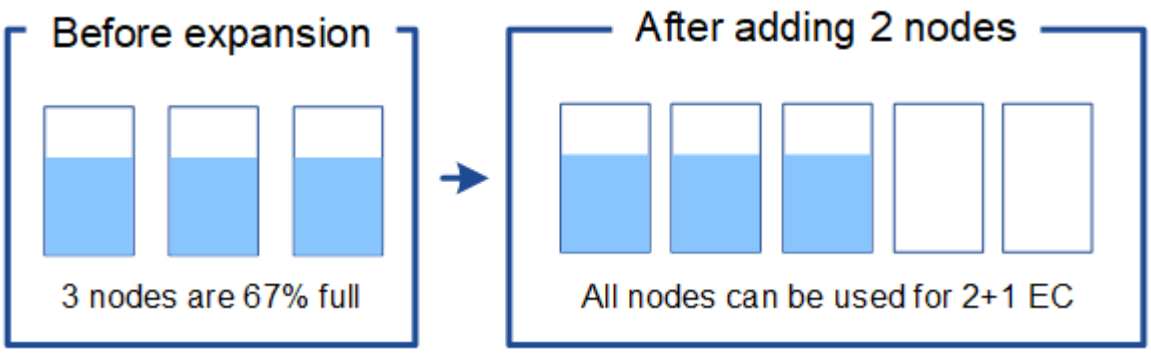



> この拡張により、 -k + m_nodes が追加されます。冗長性を確保するために、ノードを 4 つ追加することを推奨既存のノードが100%フルのときに追加するストレージノードが_k + m_expansionである場合、すべての新しいオブジェクトを拡張ノードに格納する必要があります。一時的にでも使用できなくなった新しいノードがあると、 StorageGRID は ILM 要件を満たすことができません。

- * 既存のストレージノードの使用率が 67% になったら、 2 つの 100TB のストレージノードを追加します *

  この例では、既存のノードの使用率は 67% です。既存のノードに 100TB の空き容量がある（ノードあたり 33TB ）ため、拡張を実施する場合は、ノードを 2 つ追加するだけで済みます。

  200TB の容量を追加することで、 2+1 のイレイジャーコーディングを継続し、最終的にはすべてのノード間でイレイジャーコーディングデータのバランスを取ることができます。

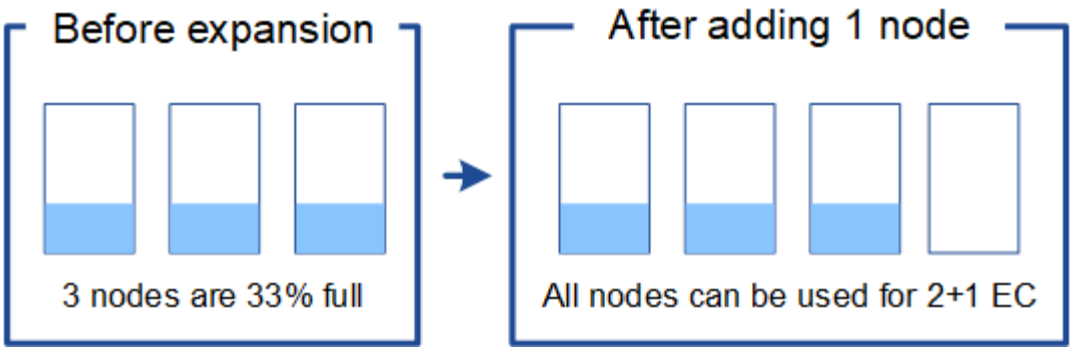



- * 既存のストレージノードの使用率が 33% に達した場合は、 100TB のストレージノードを 1 つ追加してください *

  この例では、既存のノードの使用率は 33% です。既存のノードに 200TB の空き容量（各ノードに 67TB ）があるため、拡張を実施する場合、ノードを 1 つ追加するだけで済みます。

  100TB の容量を追加することで、 2+1 のイレイジャーコーディングを続行し、最終的にはイレイジャー

コーディングされたデータをすべてのノードに分散させることができます。




例**2**：**6+3**のイレイジャーコーディングを使用する**3**サイトグリッドを拡張する

この例は、フラグメント数が多いイレイジャーコーディングスキームを含むマルチサイトグリッドの拡張計画を作成する方法を示しています。これらの例の違いにもかかわらず、推奨される拡張計画は非常に似ています。

以下を想定しています。

- すべてのデータは 6+3 イレイジャーコーディングスキームを使用して格納されます。6+3 イレイジャーコーディングスキームでは、すべてのオブジェクトが 9 個のフラグメントとして格納され、各フラグメントが別々のストレージノードに保存されます。
- サイトが 3 つあり、各サイトにストレージノードが 4 つ（合計 12 ノード）ある。各ノードの合計容量は 100TB です。
- 新しい 100TB のストレージノードを追加して拡張します。
- 最終的には、イレイジャーコーディングされたデータを古いノードと新しいノードに分散したい。

拡張を実施する際のストレージノードの使用状況に応じて、いくつかのオプションがあります。

- * 既存のノードが 100% フルの場合は、 100TB のストレージノードを 9 つ（サイトごとに 3 つ）追加します *

  この例では、 12 個の既存ノードが 100% フルであることを確認します。空き容量がないため、 6 + 3 のイレイジャーコーディングを続行するには、すぐに 9 つのノード（追加の容量 900 TB ）を追加する必要があります。

  拡張の完了後、オブジェクトがイレイジャーコーディングされると、すべてのフラグメントが新しいノードに配置されます。

  > この拡張により、 -k + m_nodes が追加されます。冗長性を確保するために、ノードを 12 個（サイトごとに 4 個）追加することを推奨します。既存のノードが100%フルのときに追加するストレージノードが_k + m_expansionである場合、すべての新しいオブジェクトを拡張ノードに格納する必要があります。一時的にでも使用できなくなった新しいノードがあると、 StorageGRID は ILM 要件を満たすことができません。

- * 既存のノードが 75% フルの場合、 6 つの 100TB のストレージノード（サイトごとに 2 つ）を追加します *

この例では、 12 個の既存ノードが 75% 使用されています。300TB の空き容量（ノードあたり 25TB ）があるため、拡張を実施する場合は、 6 つのノードを追加するだけで済みます。3 つのサイトにそれぞれ 2 つのノードを追加します。

600TB のストレージ容量を追加することで、 6+3 のイレイジャーコーディングを続行して、最終的にイレイジャーコーディングされたデータをすべてのノードに分散させることができます。

- * 既存のノードが 50% 使用されている場合は、 100TB のストレージノードを 3 つ（サイトごとに 1 つ）追加します *

  この例では、 12 個の既存ノードが 50% 使用されています。600TB の空き容量（ノードあたり 50TB ）があるため、拡張を実施する場合は、ノードを 3 つ追加するだけで済みます。3 つのサイトのそれぞれに 1 つのノードを追加します。

  300TB のストレージ容量を追加することで、 6+3 のイレイジャーコーディングを続行して、イレイジャーコーディングされたデータをすべてのノードに分散できるようになります。

- 関連情報 *

"ILM を使用してオブジェクトを管理する"

"トラブルシューティングを監視します"

"イレイジャーコーディングデータのリバランシングに関する考慮事項"



## ストレージノードを追加するために拡張を実行する際に、 ILM ポリシーにデータをイレイジャーコーディングするための ILM ルールが 1 つ以上含まれている場合は、拡張完了後に EC のリバランシング手順 の実行が必要になることがあります。

たとえば、推奨数のストレージノードを追加できない場合は、ECのリバランシング手順 を実行して、イレイジャーコーディングオブジェクトを追加して格納しなければならないことがあります。

### **EC** のリバランシングとは何ですか？

EC のリバランシングは、ストレージノードの拡張後に必要になる可能性がある StorageGRID 手順 です。手順 は、プライマリ管理ノードからコマンドラインスクリプトとして実行されます。EC Rebalance 手順 を実行すると、 StorageGRID は、サイト内の既存および新しく拡張されたストレージノード間でイレイジャーコーディングフラグメントを再配分します。

EC Rebalance手順 が実行されるタイミング：

- イレイジャーコーディングされたオブジェクトデータのみを移動します。レプリケートされたオブジェクトデータは移動されません。
- サイト内のデータを再配布します。サイト間でデータを移動することはありません。
- この機能は、サイト内のすべてのストレージノードにデータを再配分します。ストレージボリューム内でデータが再配置されることはありません。

EC Rebalance 手順 が完了すると、次のようになります。

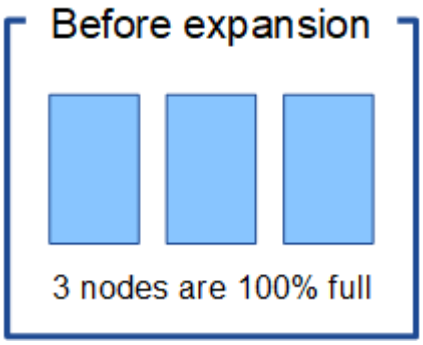
- イレイジャーコーディングされたデータは、使用可能なスペースが少ないストレージノードから、使用可能なスペースが多いストレージノードに移動されます。
- EC のリバランシング手順 によってレプリケートされたオブジェクトコピーが移動されないため、ストレージノード間で使用済み（ % ）値が異なるままになることがあります。
- イレイジャーコーディングオブジェクトのデータ保護は変更されません。

EC のリバランシング手順 が実行されている場合、 ILM 処理と S3 および Swift クライアント処理のパフォーマンスに影響する可能性があります。そのため、この手順 は限られた場合にのみ実行してください。

**EC**のリバランシングを実行しない場合

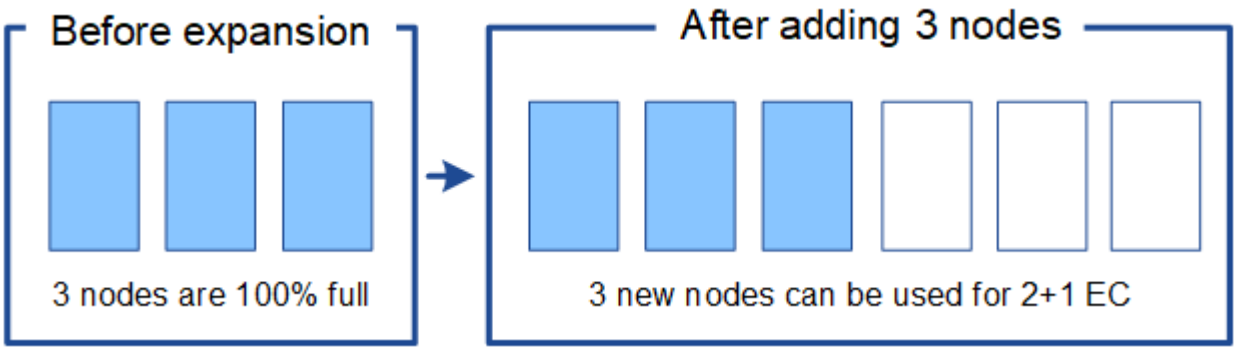
EC のリバランシングを実行する必要がない状況の例としては、次の点を考慮してください。

- StorageGRID は、 3 つのストレージノードで構成される単一サイトで実行されています。
- ILMポリシーでは、0.2MBを超えるすべてのオブジェクトに2+1のイレイジャーコーディングルールを使用し、サイズの小さいオブジェクトには2-copyレプリケーションルールを使用します。
- すべてのストレージノードがいっぱいになり、 Major 重大度レベルで * Low Object Storage * アラートがトリガーされています。推奨される方法は、拡張手順 を実行してストレージノードを追加することです。



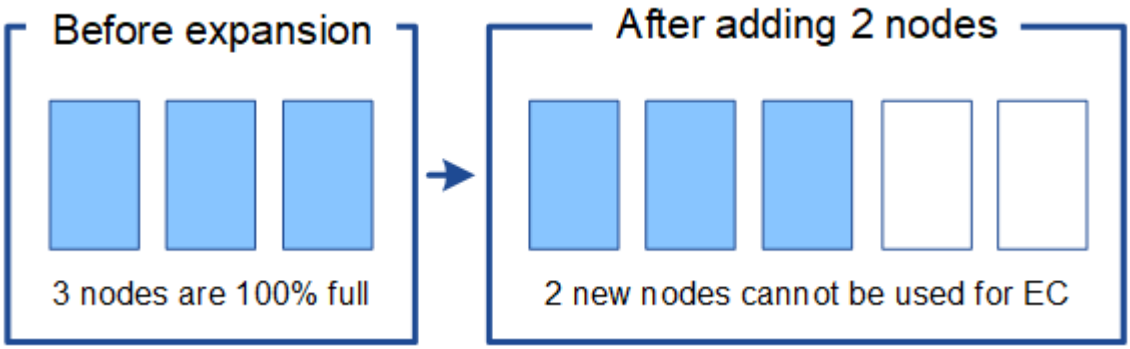

この例でサイトを拡張するには、新しいストレージノードを 3 つ以上追加することを推奨します。StorageGRID では、 2 つのデータフラグメントと 1 つのパリティフラグメントを別々のノードに配置できるように、 2+1 イレイジャーコーディング用に 3 つのストレージノードが必要です。

3 つのストレージノードを追加したあとも、元のストレージノードはいっぱいになりますが、オブジェクトは引き続き新しいノード上の 2+1 イレイジャーコーディングスキームに取り込むことができます。この場合、EC Rebalance 手順 を実行することは推奨されません。手順 を実行すると、パフォーマンスが一時的に低下し、クライアントの処理に影響する可能性があります。

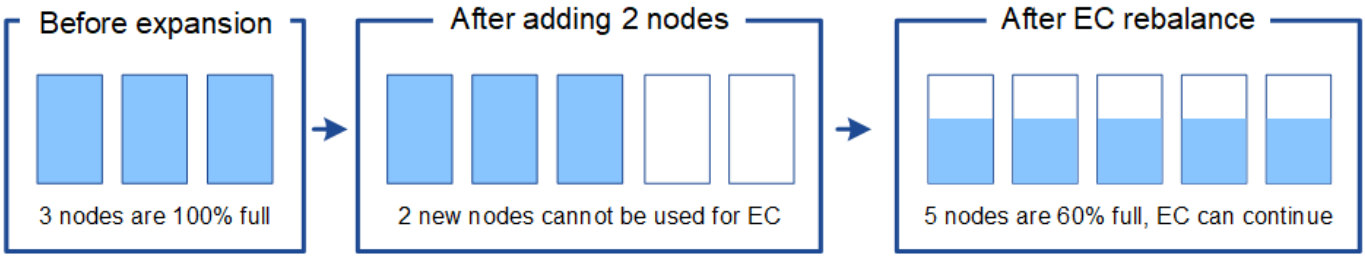


### ECのリバランシングを実行するタイミング

EC のリバランシングを行う手順 の例としては、同じ例を考えてみてください。ただし、ストレージノードを 2 つしか追加できないとします。2+1 イレイジャーコーディングには少なくとも 3 つのストレージノードが必要であるため、新しいノードをイレイジャーコーディングデータに使用することはできません。




この問題 を解決して新しいストレージノードを利用するには、 EC Rebalance 手順 を実行します。この手順を実行すると、 StorageGRID によって、イレイジャーコーディングされたデータフラグメントとパリティフラグメントがサイト内のすべてのストレージノードに再配分されます。この例では、 EC Rebalance 手順 が完了すると、 5 つのノードすべてが 60% フルになり、すべてのストレージノード上の 2+1 イレイジャーコーディングスキームにオブジェクトを引き続き取り込むことができます。




### ECのリバランシングに関する考慮事項

一般に、 EC Rebalance 手順 は限られた場合にのみ実行してください。具体的には、次の条件がすべて当てはまる場合にのみ EC のリバランシングを実行する必要があります。

- オブジェクトデータにイレイジャーコーディングを使用します。
- Low Object Storage * アラートがトリガーされました。このアラートは、ノードが 80% 以上フルであることを示します。
- 使用中のイレイジャーコーディングスキームに推奨される数の新しいストレージノードを追加することはできません。

  "イレイジャーコーディングオブジェクトのストレージ容量の追加"

- S3 / Swift クライアントは、 EC のリバランシング手順 が実行されている間の書き込み処理と読み取り処理のパフォーマンスの低下を許容できます。

### ECのリバランシング手順 が他のメンテナンスタスクと連携する仕組み

特定のメンテナンス手順を、 EC Rebalance 手順 の実行中に同時に実行することはできません。

| 手順 | **EC** のリバランシングで許可される手順 ？ |
| --- | --- |
| 追加の EC リバランシング手順 | いいえ<br><br>一度に実行できる EC のリバランシング手順 は 1 つだけです。 |
| 手順 の運用を停止<br><br>EC データの修復ジョブ | いいえ<br><br>• EC Rebalance 手順 が実行されている間は、手順 または EC データの修復の運用を停止することはできません。<br>• ストレージノードが手順 を運用停止したり、 EC データの修復が実行されている間は、 EC のリバランシング手順 を開始できません。 |
| Expansion 手順 の略 | いいえ<br><br>拡張時に新しいストレージノードを追加する必要がある場合は、すべての新しいノードを追加するまで、 EC Rebalance 手順 を実行します。新しいストレージノードの追加時に EC Rebalance 手順 が進行中の場合、それらのノードにデータは移動されません。 |
| 手順 をアップグレードします | いいえ<br><br>StorageGRID ソフトウェアをアップグレードする必要がある場合は、 EC Rebalance 手順 を実行する前または実行したあとにアップグレード手順 を実行する必要があります。必要に応じて、ソフトウェアアップグレードを実行するために EC Rebalance 手順 を終了できます。 |
| アプライアンスノードのクローン手順 | いいえ<br><br>アプライアンスストレージノードをクローニングする必要がある場合は、新しいノードを追加してから EC 手順 のリバランシングを実行する必要があります。新しいストレージノードの追加時に EC Rebalance 手順 が進行中の場合、それらのノードにデータは移動されません。 |
| Hotfix 手順 の略 | はい。<br><br>StorageGRID ホットフィックスは、 EC Rebalance 手順 の実行中に適用できます。 |
| その他のメンテナンス手順 | いいえ<br><br>他のメンテナンス手順を実行する前に、 EC Rebalance 手順 を終了する必要があります。 |

**EC**のリバランシングが行われる手順 と**ILM**の相互作用

EC のリバランシング手順 を実行している間は、 ILM を変更して既存のイレイジャーコーディングオブジェクトの場所が変更されないようにしてください。たとえば、別のイレイジャーコーディングプロファイルを持つ ILM ルールは使用しないでください。このよう手順 な ILM の変更が必要になった場合は、 EC のリバラン

シングを中止します。

関連情報

"ストレージノードの追加後におけるイレイジャーコーディングデータのリバランシング"

メタデータ容量の追加

## オブジェクトメタデータ用のスペースを十分に確保するために、各サイトに新しいストレージノードを追加する拡張手順 の実行が必要になる場合があります。

StorageGRID は、各ストレージノードのボリューム 0 にオブジェクトメタデータ用のスペースをリザーブします。すべてのオブジェクトメタデータのコピーが各サイトに 3 つ保持され、すべてのストレージノードに均等に分散されます。

Grid Manager を使用してストレージノードのメタデータ容量を監視し、メタデータ容量がどれくらいの速さで消費されているかを見積もることができます。また、使用済みメタデータスペースが特定のしきい値に達すると、ストレージノードに対して * Low metadata storage * アラートがトリガーされます。詳細については、StorageGRID の監視とトラブルシューティングの手順を参照してください。

グリッドの使用方法によっては、グリッドのオブジェクトメタデータ容量がオブジェクトのストレージ容量よりも早く消費される場合があります。たとえば、一般に大量の小さいオブジェクトを取り込みたり、大量のユーザメタデータやタグをオブジェクトに追加したりする場合、オブジェクトストレージの容量が十分に残っていても、メタデータ容量を増やすためにストレージノードの追加が必要になることがあります。

### メタデータ容量を増やす場合のガイドライン

ストレージノードを追加してメタデータ容量を増やす前に、次のガイドラインと制限事項を確認してください。

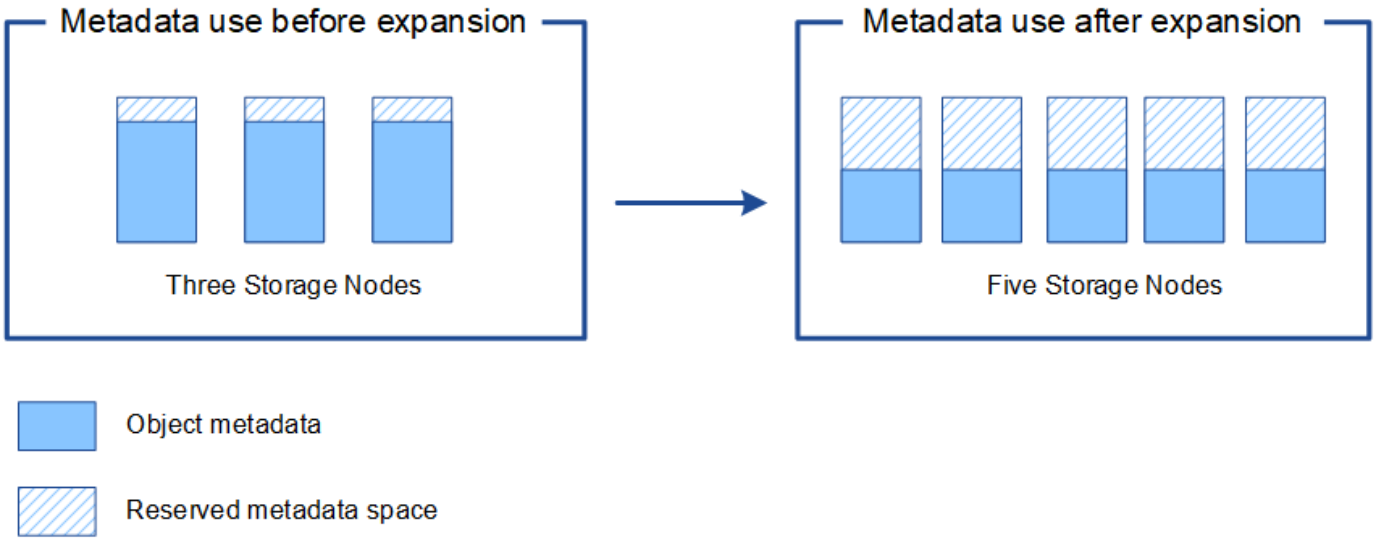
- 十分なオブジェクトストレージ容量がある場合は、オブジェクトメタデータ用の使用可能なスペースが増えると、 StorageGRID システムに格納できるオブジェクトの数も増えます。
- 各サイトにストレージノードを 1 つ以上追加して、グリッドのメタデータ容量を増やすことができます。
- 特定のストレージノードでオブジェクトメタデータ用にリザーブされている実際のスペースは、Metadata Reserved Space ストレージオプション（システム全体の設定）、ノードに割り当てられている RAM の容量、ノードのボリューム 0 のサイズによって異なります。詳細については、 StorageGRID の管理手順を参照してください。
- メタデータはボリューム 0 にのみ格納されるため、既存のストレージノードにストレージボリュームを追加してメタデータ容量を増やすことはできません。
- 新しいサイトを追加してメタデータ容量を増やすことはできません。
- StorageGRID は、すべてのオブジェクトメタデータのコピーを各サイトで 3 つ保持します。このため、システムのメタデータ容量は最小のサイトのメタデータ容量によって制限されます。
- メタデータ容量を追加するときは、各サイトに同じ数のストレージノードを追加する必要があります。

### ストレージノードを追加したときにメタデータが再配分される仕組み

拡張時にストレージノードを追加すると、 StorageGRID によって、既存のオブジェクトメタデータが各サイトの新しいノードに再配分され、グリッドの全体的なメタデータ容量が増加します。ユーザによる操作は必要ありません。

次の図は、拡張でストレージノードを追加した場合に StorageGRID によってオブジェクトメタデータがどのように再配分されるかを示しています。図の左側は、拡張前の 3 つのストレージノードのボリューム 0 を表しています。メタデータが各ノードの使用可能なメタデータスペースの大部分を消費しており、「 Low metadata storage * 」アラートがトリガーされています。

図の右側は、サイトへの 2 つのストレージノードの追加後に既存のメタデータがどのように再配置されるかを示しています。各ノードのメタデータの量が減少し、「 Low metadata storage * 」アラートがトリガーされなくなり、メタデータに使用できるスペースが増えました。




- 関連情報 *

"StorageGRID の管理"

"トラブルシューティングを監視します"

システムの機能を追加するためのグリッドノードの追加

## 既存のサイトに新しいグリッドノードを追加することで、 StorageGRID システムに冗長性を追加したり機能を追加したりできます。

たとえば、ゲートウェイノードのハイアベイラビリティグループの作成をサポートするゲートウェイノードを追加したり、ローカルノードを使用した監視を許可する管理ノードをリモートサイトに追加したりできます。

次のタイプの 1 つ以上のノードを、 1 回の拡張処理で 1 つ以上の既存のサイトに追加することができます。

- 非プライマリ管理ノード
- ストレージノード
- ゲートウェイノード
- アーカイブノード

グリッドノードを追加する場合は、次の制限事項に注意してください。

- プライマリ管理ノードは最初のインストール時に導入されます。プライマリ管理ノードを拡張時に追加することはできません。

- 同じ拡張内でストレージノードとその他のタイプのノードを追加できます。
- ストレージノードを追加するときは、新しいノードの数と場所を慎重に計画する必要があります。

  "ストレージ容量を追加しています"

- アーカイブノードを追加する場合は、 Tivoli Storage Manager （ TSM ）ミドルウェア経由のテープのみが各アーカイブノードでサポートされます。
- [信頼されていないクライアントネットワーク]ページで[新しいノードクライアントネットワークのデフォルト*]オプションが[信頼されていない*]に設定されている場合、クライアントネットワークを使用して拡張ノードに接続するクライアントアプリケーションは、ロードバランサエンドポイントポート（* Configuration > Network Settings > Untrusted Client Network *）を使用して接続する必要があります。新しいノードの設定を変更してロードバランサエンドポイントを設定するには、StorageGRID の管理手順を参照してください。
- 関連情報 *

"StorageGRID の管理"

新しいサイトを追加しています

## 新しいサイトを追加して StorageGRID システムを拡張することができます。

サイトの追加に関するガイドライン

サイトを追加する前に、次の要件および制限事項を確認してください。

- 拡張処理で追加できるサイトは 1 つだけです。
- 同じ拡張の一環として既存のサイトにグリッドノードを追加することはできません。
- すべてのサイトに少なくとも 3 つのストレージノードが含まれている必要があります。
- 新しいサイトを追加しても、格納できるオブジェクトの数は自動的に増えません。グリッドの合計オブジェクト容量は、使用可能なストレージの量、 ILM ポリシー、および各サイトのメタデータ容量によって異なります。
- 新しいサイトのサイジングを行うときは、十分なメタデータ容量が確保されている必要があります。

  StorageGRID は、すべてのオブジェクトメタデータのコピーをすべてのサイトで保持します。新しいサイトを追加するときは、既存のオブジェクトメタデータ用の十分なメタデータ容量と、拡張に対応できる十分なメタデータ容量が追加されている必要があります。

  オブジェクトメタデータ容量の監視については、StorageGRID の監視とトラブルシューティングの手順を参照してください。

- サイト間の使用可能なネットワーク帯域幅およびネットワークレイテンシのレベルを考慮する必要があります。すべてのオブジェクトが取り込まれたサイトにのみ格納されている場合でも、メタデータの更新はサイト間で継続的にレプリケートされます。
- StorageGRID システムは拡張時も動作し続けるため、拡張手順 を開始する前に ILM ルールを確認し、拡張手順 が完了するまではオブジェクトコピーが新しいサイトに格納されないようにする必要があります。

  たとえば、拡張を開始する前に、デフォルトのストレージプール（すべてのストレージノード）を使用するルールがないかを確認します。その場合は、既存のストレージノードを含む新しいストレージプールを

作成し、新しいストレージプールを使用するように ILM ルールを更新する必要があります。そうしないと、そのサイトの最初のノードがアクティブになるとすぐに新しいサイトにオブジェクトがコピーされます。

新しいサイトを追加する際のILMの変更の詳細については、情報ライフサイクル管理を使用してオブジェクトを管理する手順のILMポリシーの変更例を参照してください。

- 関連情報 *

"ILM を使用してオブジェクトを管理する"

## 拡張の準備

### StorageGRID 拡張の準備として、必要な情報やデータ、機器を揃え、新しいハードウェアやネットワークを設置および設定する必要があります。

前提要件

拡張処理を実行する前に、次の表に記載された情報やデータ、機器を揃えておく必要があります。

| 項目 | 注： |
| --- | --- |
| StorageGRID インストールアーカイブ | 新しいグリッドノードや新しいサイトを追加する場合は、StorageGRID インストールアーカイブをダウンロードして展開する必要があります。グリッドで現在実行されているバージョンと同じバージョンを使用する必要があります。<br><br>詳細については、StorageGRID インストールファイルのダウンロードと展開の手順を参照してください。<br><br>• 注：既存のストレージノードに新しいストレージボリュームを追加する場合や新しい StorageGRID アプライアンスをインストールする場合、ファイルをダウンロードする必要はありません。 |
| サービスラップトップ | サービスラップトップは、次の要件を満たしている必要があります。<br><br>• ネットワークポート<br>• SSH クライアント（ PuTTY など）<br>• サポートされているブラウザ |
| プロビジョニングパスフレーズ | このパスフレーズは、 StorageGRID システムが最初にインストールされるときに作成されて文書化されます。プロビジョニングパスフレーズはに含まれていません `Passwords.txt` ファイル。 |
| StorageGRID のドキュメント | • StorageGRID の管理_<br>• StorageGRID リリースノート_<br>• 使用しているプラットフォームに対応したインストール手順 |

| 項目 | 注： |
| --- | --- |
| ご使用のプラットフォームの最新ドキュメント | サポートされるバージョンについては、 Interoperability Matrix を参照してください。 |

関連情報

"StorageGRID の管理"

"リリースノート"

"VMware をインストールする"

"Red Hat Enterprise Linux または CentOS をインストールします"

"Ubuntu または Debian をインストールします"

"NetApp Interoperability Matrix Tool で確認できます"

#### Web ブラウザの要件

サポートされている Web ブラウザを使用する必要があります。

| Web ブラウザ | サポートされる最小バージョン |
| --- | --- |
| Google Chrome | 87 |
| Microsoft Edge の場合 | 87 |
| Mozilla Firefox | 84 |

ブラウザウィンドウの幅を推奨される値に設定してください。

| ブラウザの幅 | ピクセル |
| --- | --- |
| 最小（ Minimum ） | 1024 |
| 最適 | 1280 |

### StorageGRID インストールファイルのダウンロードと展開

新しいグリッドノードや新しいサイトを追加する前に、適切な StorageGRID インストールアーカイブをダウンロードし、ファイルを展開する必要があります。

このタスクについて

拡張処理は、グリッドで現在実行されているバージョンの StorageGRID を使用して実行する必要があります。

手順

1. ネットアップの StorageGRID ダウンロードページにアクセスします。

   "ネットアップのダウンロード： StorageGRID"

2. グリッドで現在実行されている StorageGRID のバージョンを選択します。
3. ネットアップアカウントのユーザ名とパスワードを使用してサインインします。
4. エンドユーザライセンス契約を読み、チェックボックスをオンにして、「 * 同意して続行 * 」を選択します。
5. ダウンロードページの「* Install StorageGRID *」列で、を選択します `.tgz` または `.zip` ご使用のプラットフォームに対応するファイルです。

   インストールアーカイブファイルに表示されるバージョンは、現在インストールされているソフトウェアのバージョンと一致している必要があります。

   を使用します `.zip` ファイルサービスラップトップでWindowsを実行している場合。

| プラットフォーム | インストールアーカイブ |
| --- | --- |
| VMware | StorageGRID-Webscale-*version*-VMware-*uniqueID*.zip StorageGRIDWebscale—vmware-uniqueID_tgz |
| Red Hat Enterprise Linux または CentOS | StorageGRID-Webscale-*version*-RPM-*uniqueID*.zip StorageGRIDWebscale--*version*-rpm_uniqueID_tgz |
| UbuntuまたはDebianおよびアプライアンス | StorageGRID-Webscale-*version*-DEB-*uniqueID*.zip StorageGRIDWebscale--*version*-bDEB --_uniqueID_tgz |
| OpenStack / その他のハイパーバイザー | OpenStack の既存の環境を拡張する場合は、上記のサポートされている Linux ディストリビューションのいずれかを実行する仮想マシンを導入し、 Linux に関する適切な手順に従う必要があります。 |

6. アーカイブファイルをダウンロードして展開します。
7. プラットフォームに応じた手順に従って、プラットフォーム、計画したグリッドトポロジ、および StorageGRID システムの拡張方法に基づいて、必要なファイルを選択します。

   各プラットフォームの手順に記載されているパスは、アーカイブファイルによってインストールされた最上位ディレクトリに対する相対パスです。

8. VMware システムを拡張する場合は、適切なファイルを選択します。

| パスとファイル名 | 説明 |
| --- | --- |
|  | StorageGRID ダウンロードファイルに含まれているすべてのファイルについて説明するテキストファイル。 |

| パスとファイル名 | 説明 |
| --- | --- |
| | 製品サポートのない無償ライセンス。 |
| | グリッドノード仮想マシンを作成するためのテンプレートとして使用される仮想マシンディスクファイル。 |
| | Open Virtualization Formatテンプレートファイル (`.ovf`)とマニフェストファイル (`.mf`）を使用してください。 |
| | テンプレートファイル (`.ovf`)とマニフェストファイル (`.mf`）。非プライマリ管理ノードを導入する場合に使用します。 |
| | テンプレートファイル (`.ovf`)とマニフェストファイル (`.mf`）を使用してアーカイブノードを導入します。 |
| | テンプレートファイル (`.ovf`)とマニフェストファイル (`.mf`）を選択します。 |
| | テンプレートファイル (`.ovf`)とマニフェストファイル (`.mf`）を選択します。 |
| 導入スクリプトツール | 説明 |
| | 仮想グリッドノードの導入を自動化するための Bash シェルスクリプト。 |
| | で使用するサンプル構成ファイル `deploy-vsphere-ovftool.sh` スクリプト： |
| | StorageGRID システムの設定を自動化するための Python スクリプト。 |
| | StorageGRID アプライアンスの設定を自動化するための Python スクリプト。 |
| | シングルサインオンが有効な場合にグリッド管理 API にサインインするために使用できる Python スクリプトの例。 |
| | で使用するサンプル構成ファイル `configure-storagegrid.py` スクリプト： |

| パスとファイル名 | 説明 |
| --- | --- |
| | で使用する空の構成ファイル `configure-storagegrid.py` スクリプト： |

9. Red Hat Enterprise Linux または CentOS のシステムを拡張する場合は、該当するファイルを選択します。

| パスとファイル名 | 説明 |
| --- | --- |
| | StorageGRID ダウンロードファイルに含まれているすべてのファイルについて説明するテキストファイル。 |
| | 製品サポートのない無償ライセンス。 |
| | RHEL ホストまたは CentOS ホストに StorageGRID ノードイメージをインストールするための RPM パッケージ。 |
| | RHEL ホストまたは CentOS ホストに StorageGRID ホストサービスをインストールするための RPM パッケージ。 |
| 導入スクリプトツール | 説明 |
| | StorageGRID システムの設定を自動化するための Python スクリプト。 |
| | StorageGRID アプライアンスの設定を自動化するための Python スクリプト。 |
| | で使用するサンプル構成ファイル `configure-storagegrid.py` スクリプト： |
| | シングルサインオンが有効な場合にグリッド管理 API にサインインするために使用できる Python スクリプトの例。 |
| | で使用する空の構成ファイル `configure-storagegrid.py` スクリプト： |
| | StorageGRID コンテナ導入用の RHEL ホストまたは CentOS ホストを設定するためのサンプルの Ansible のロールとプレイブック。必要に応じて、ロールまたはプレイブックをカスタマイズできます。 |

10. Ubuntu または Debian システムを拡張する場合は、適切なファイルを選択します。

| パスとファイル名 | 説明 |
| --- | --- |
| | StorageGRID ダウンロードファイルに含まれているすべてのファイルについて説明するテキストファイル。 |
| | テスト環境およびコンセプトの実証環境に使用できる、非本番環境のネットアップライセンスファイル。 |
| | Ubuntu ホストまたは Debian ホストに StorageGRID ノードイメージをインストールするための DEB パッケージ。 |
| | ファイルのMD5チェックサム `/debs/storagegrid-webscale-images-version-SHA.deb`。 |
| | Ubuntu ホストまたは Debian ホストに StorageGRID ホストサービスをインストールするための DEB パッケージ。 |
| 導入スクリプトツール | 説明 |
| | StorageGRID システムの設定を自動化するための Python スクリプト。 |
| | StorageGRID アプライアンスの設定を自動化するための Python スクリプト。 |
| | シングルサインオンが有効な場合にグリッド管理 API にサインインするために使用できる Python スクリプトの例。 |
| | で使用するサンプル構成ファイル `configure-storagegrid.py` スクリプト： |
| | で使用する空の構成ファイル `configure-storagegrid.py` スクリプト： |
| | StorageGRID コンテナ導入用の Ubuntu ホストまたは Debian ホストを設定するためのサンプルの Ansible のロールとプレイブック。必要に応じて、ロールまたはプレイブックをカスタマイズできます。 |

11. StorageGRID アプライアンスベースのシステムを拡張する場合は、該当するファイルを選択してください。

| パスとファイル名 | 説明 |
| --- | --- |
| | アプライアンスに StorageGRID ノードイメージをインストールするための DEB パッケージ。 |
| | DEB インストールパッケージのチェックサム。アップロード後にパッケージに変更が加えられていないことを確認するために StorageGRID アプライアンスインストーラで使用されます。 |

アプライアンスのインストールの場合、これらのファイルが必要になるのは、ネットワークトラフィックを回避する必要がある場合だけです。アプライアンスは、プライマリ管理ノードから必要なファイルをダウンロードできます。

ハードウェアとネットワークの確認

StorageGRID システムの拡張を開始する前に、新しいグリッドノードまたは新しいサイトをサポートするために必要なハードウェアを設置して設定しておく必要があります。

サポートされるバージョンについては、Interoperability Matrixを参照してください。

また、サイトのサーバ間のネットワーク接続を確認し、プライマリ管理ノードがStorageGRID システムをホストするすべての拡張サーバと通信できることを確認する必要があります。

新しいサブネットの追加を含む拡張アクティビティを実行する場合は、拡張手順 を開始する前に新しいグリッドサブネットを追加する必要があります。

グリッドノード間または StorageGRID サイト間のグリッドネットワークでは、ネットワークアドレス変換（ NAT ）を使用しないでください。グリッドネットワークにプライベート IPv4 アドレスを使用する場合は、使用するアドレスに各サイトのすべてのグリッドノードから直接ルーティングできる必要があります。ただし、必要に応じて、ゲートウェイノードにパブリック IP アドレスを指定するなど、外部クライアントとグリッドノードの間で NAT を使用できます。NAT を使用してパブリックネットワークセグメントをブリッジする方法は、グリッド内のすべてのノードに対して透過的なトンネリングアプリケーションを採用する場合、つまりグリッドノードがパブリック IP アドレスを認識する必要がない場合にのみサポートされます。

- 関連情報 *

"NetApp Interoperability Matrix Tool で確認できます"

"グリッドネットワークのサブネットを更新しています"

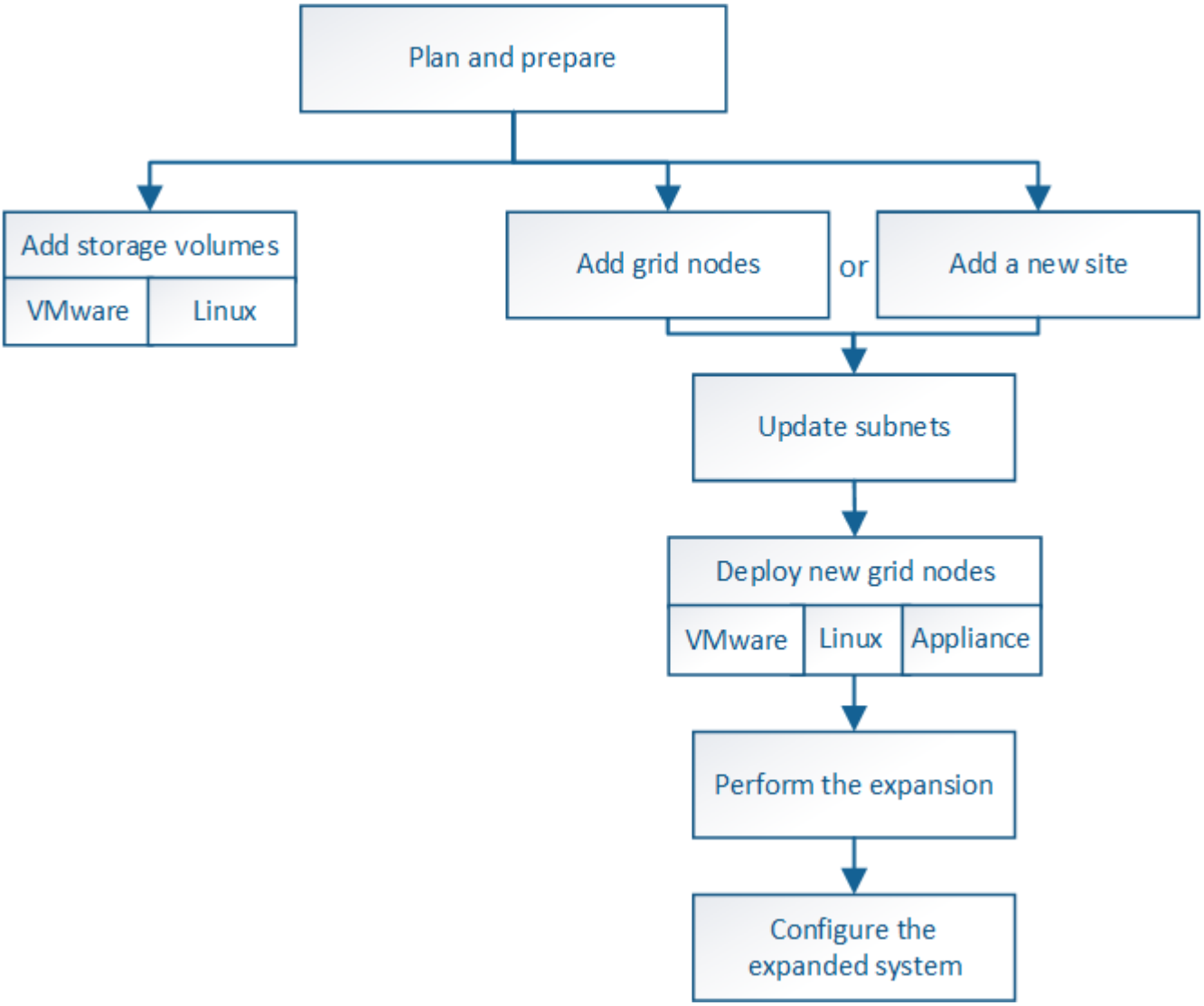
## 拡張手順 の概要

StorageGRID 拡張を実行するための基本的な手順は、拡張のタイプによって異なります。ストレージノードへのストレージボリュームの追加、既存のサイトへの新しいノードの追加、または新しいサイトの追加です。いずれの場合も、拡張は現在のシステムの処理を中断せずに実行できます。

グリッドに追加するノードのタイプやノードを追加する理由は、基本的な拡張手順 には影響しません。次のワークフロー図に示すように、ノードを追加する手順は、StorageGRID アプライアンスと、VMwareまたはLinuxを実行しているホストのどちらを追加するかによって多少異なります。

ネットアップでは、OpenStackでのStorageGRID の新規インストールまたは拡張を対象とした仮想マシンディスクファイルおよびスクリプトの提供は現在は行っていません。OpenStackの既存の環境を拡張する場合は、Linuxディストリビューション向けの手順に従ってください。

「 Linux 」とは、 Red Hat ® Enterprise Linux ® 、 Ubuntu ® 、 CentOS 、または Debian ® の環境を指します。サポートされているバージョンの一覧については、 NetApp Interoperability Matrix Tool を参照してください。




- 関連情報 *

"NetApp Interoperability Matrix Tool で確認できます"

"StorageGRID 拡張の計画"

"拡張の準備"

"ストレージノードへのストレージボリュームの追加"

"既存のサイトへのグリッドノードの追加と新しいサイトの追加"

# ストレージノードへのストレージボリュームの追加

ストレージボリュームを 16 個以下にすることでストレージノードのストレージ容量を拡張できます。ILM のレプリケートコピーまたはイレイジャーコーディングコピーの要件を満たすために、複数のストレージノードへのストレージボリュームの追加が必要になる場合があります。

必要なもの

ストレージボリュームを追加する前に、ストレージ容量を追加する際のガイドラインを確認し、ILMポリシーの要件を満たすボリュームの追加先を確認してください。

"ストレージ容量を追加しています"

> この手順はソフトウェアベースのストレージノードにのみ該当します。拡張シェルフを設置してSG6060にストレージボリュームを追加する方法については、SG6060アプライアンスの設置とメンテナンスの手順を参照してください。それ以外のアプライアンスストレージノードは拡張できません。
>
> "SG6000 ストレージアプライアンス"

このタスクについて

ストレージノードの基盤となるストレージは、複数のストレージボリュームに分割されます。ストレージボリュームは、 StorageGRID システムでフォーマットされてオブジェクトの格納用にマウントされたブロックベースのストレージデバイスです。各ストレージノードでサポートされるストレージボリュームは、 Grid Manager では _ オブジェクトストア _ と呼ばれ、最大 16 個です。

> オブジェクトメタデータは常にオブジェクトストア 0 に格納されます。

各オブジェクトストアは、 ID に対応するボリュームにマウントされます。つまり、IDが0000のオブジェクトストアはに対応しています `/var/local/rangedb/0` マウントポイント：

新しいストレージボリュームを追加する前に、 Grid Manager を使用して、各ストレージノードの現在のオブジェクトストアと対応するマウントポイントを表示します。この情報は、ストレージボリュームを追加するときに役立ちます。

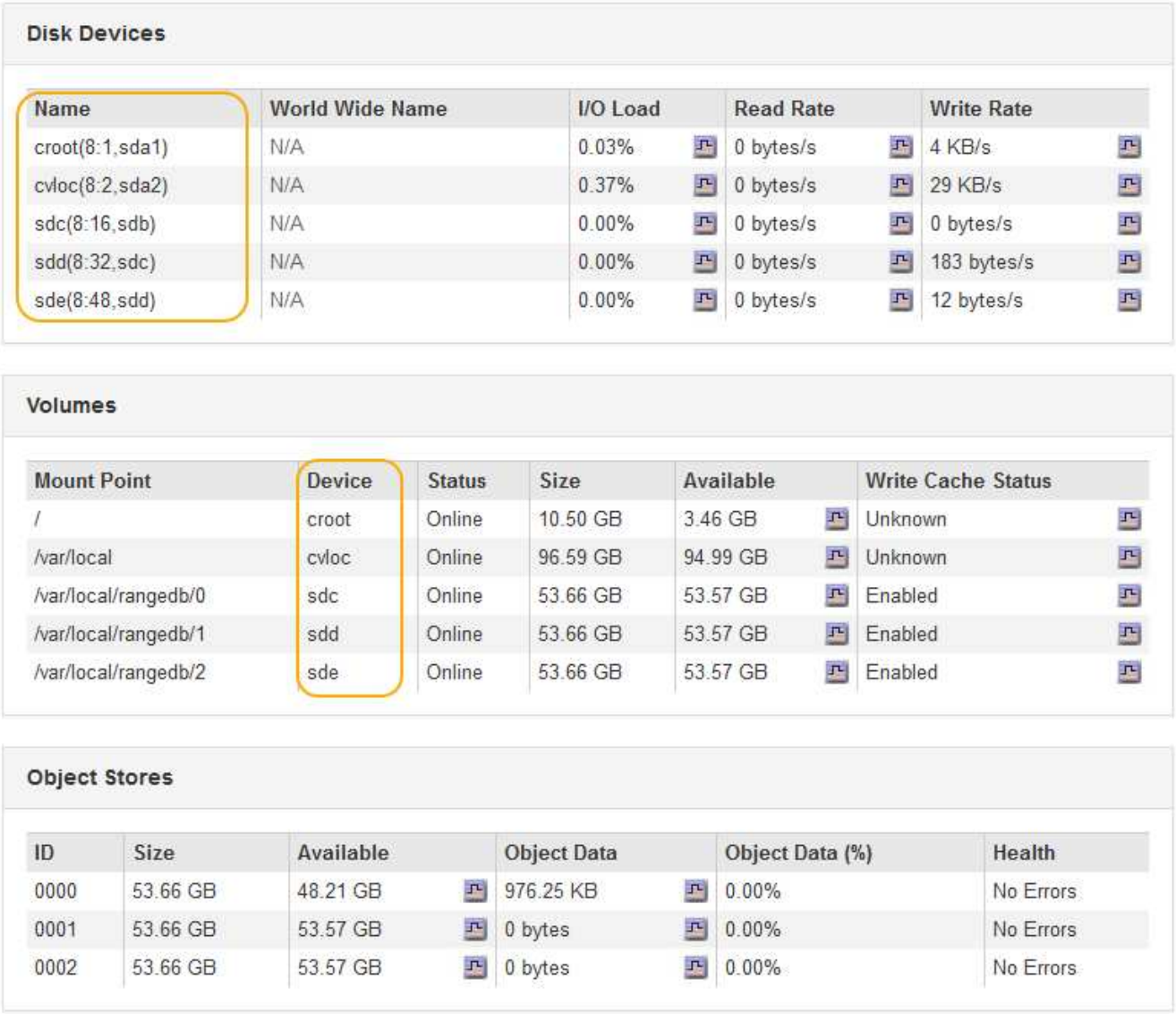
手順

1. ノード*>**site* >*_ストレージノード>*ストレージ*を選択します。
2. 下にスクロールして、各ボリュームとオブジェクトストアに使用可能なストレージ容量を表示します。

   アプライアンスストレージノードの場合、各ディスクの Worldwide Name は、 SANtricity ソフトウェア（アプライアンスのストレージコントローラに接続される管理ソフトウェア）で標準のボリュームプロパティとして表示される、ボリュームの World-Wide Identifier （ WWID ）と同じです。

   ボリュームマウントポイントに関連するディスクの読み取りと書き込みの統計情報を解釈できるように、 Disk Devices テーブルの * Name * 列に表示される名前の最初の部分（つまり、 *sdc*_*sd*,*sde* ）が Volumes

テーブルの * Device * 列に表示される値と一致していることを確認します。



**Disk Devices**

| Name | World Wide Name | I/O Load | Read Rate | Write Rate |
|---|---|---|---|---|
| croot(8:1,sda1) | N/A | 0.03% | 0 bytes/s | 4 KB/s |
| cvloc(8:2,sda2) | N/A | 0.37% | 0 bytes/s | 29 KB/s |
| sdc(8:16,sdb) | N/A | 0.00% | 0 bytes/s | 0 bytes/s |
| sdd(8:32,sdc) | N/A | 0.00% | 0 bytes/s | 183 bytes/s |
| sde(8:48,sdd) | N/A | 0.00% | 0 bytes/s | 12 bytes/s |

**Volumes**

| Mount Point | Device | Status | Size | Available | Write Cache Status |
|---|---|---|---|---|---|
| / | croot | Online | 10.50 GB | 3.46 GB | Unknown |
| /var/local | cvloc | Online | 96.59 GB | 94.99 GB | Unknown |
| /var/local/rangedb/0 | sdc | Online | 53.66 GB | 53.57 GB | Enabled |
| /var/local/rangedb/1 | sdd | Online | 53.66 GB | 53.57 GB | Enabled |
| /var/local/rangedb/2 | sde | Online | 53.66 GB | 53.57 GB | Enabled |

**Object Stores**

| ID | Size | Available | Object Data | Object Data (%) | Health |
|---|---|---|---|---|---|
| 0000 | 53.66 GB | 48.21 GB | 976.25 KB | 0.00% | No Errors |
| 0001 | 53.66 GB | 53.57 GB | 0 bytes | 0.00% | No Errors |
| 0002 | 53.66 GB | 53.57 GB | 0 bytes | 0.00% | No Errors |

3. プラットフォームに応じた手順に従って、ストレージノードに新しいストレージボリュームを追加します。
   - "VMware：ストレージノードへのストレージボリュームの追加"
   - "Linux：ストレージノードへの直接接続型ボリュームまたはSANボリュームの追加"

**VMware**：ストレージノードへのストレージボリュームの追加

ストレージノードのストレージボリュームが 16 個より少ない場合は、 VMware vSphere を使用してボリュームを追加することで容量を増やすことができます。

必要なもの

- StorageGRID for VMware環境のインストール手順を参照できる必要があります。
- を用意しておく必要があります `Passwords.txt` ファイル。
- 特定のアクセス権限が必要です。

ソフトウェアのアップグレード、リカバリ用手順 、または別の拡張手順 がアクティブな状態でストレージノードにストレージボリュームを追加しないでください。

このタスクについて

ストレージボリュームを追加するときは、ストレージノードが一時的に使用できない状態になっています。クライアント向けのグリッドサービスへの影響を回避するために、この手順 は一度に 1 つのストレージノードでのみ実行してください。

手順

1. 必要に応じて、新しいストレージハードウェアを設置し、新しい VMware データストアを作成します。
2. ストレージとして使用する仮想マシン（オブジェクトストア）に 1 つ以上のハードディスクを追加します。

   a. VMware vSphere Client を開きます。

   b. 仮想マシンの設定を編集して、 1 つ以上のハードディスクを追加します。

   通常、ハードディスクは仮想マシンディスク（ VMDK ）として設定されます。一般に使用され、管理も容易であるのは VMDK ですが、大きなオブジェクトサイズ（たとえば 100MB 超）を使用するワークロードのパフォーマンスは RDM の方が高くなります。仮想マシンへのハードディスクの追加の詳細については、 VMware vSphere のドキュメントを参照してください。

3. VMware vSphere Clientの* Restart Guest OS *オプションを使用するか、または仮想マシンへのsshセッションで次のコマンドを入力して、仮想マシンを再起動します。`sudo reboot`

   仮想マシンの再起動には、 * 電源オフ * または * リセット * を使用しないでください。

4. ストレージノードで使用する新しいストレージを設定します。

   a. グリッドノードにログインします。

      i. 次のコマンドを入力します。 `ssh admin@grid_node_IP`

      ii. に記載されているパスワードを入力します `Passwords.txt` ファイル。

      iii. 次のコマンドを入力してrootに切り替えます。 `su -`

      iv. に記載されているパスワードを入力します `Passwords.txt` ファイル。rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

   b. 新しいストレージボリュームを設定します。

   ```
   sudo add_rangedbs.rb
   ```

   新しいストレージボリュームがすべて検出され、それらをフォーマットするように求められます。

   a. 「 * y * 」と入力して、フォーマットを確定します。

   b. 以前にフォーマットされたボリュームがある場合は、それらを再フォーマットするかどうかを決めます。

      - 再フォーマットするには「 * y * 」と入力します。
      - 再フォーマットをスキップするには「 * n * 」と入力します。ストレージボリュームがフォーマットされます。

c. プロンプトが表示されたら、「 * y 」と入力してストレージサービスを停止します。

ストレージサービスが停止され、が停止されます `setup_rangedbs.sh` スクリプトは自動的に実行されます。ボリュームが rangedb として使用できるようになると、サービスが再び開始されます。

5. サービスが正しく開始されることを確認します。

a. サーバ上のすべてのサービスのステータスのリストを表示します。

```
sudo storagegrid-status
```

ステータスは自動的に更新されます。

a. すべてのサービスが「 Running 」または「 Verified 」になるまで待ちます。

b. ステータス画面を終了します。

```
Ctrl+C
```

6. ストレージノードがオンラインであることを確認します。

a. サポートされているブラウザを使用してGrid Managerにサインインします。

b. Support **>** Tools **>** Grid Topology *を選択します。

c. 「 * *site* * > * _ *Storage Node** > * LDR * > * Storage * 」を選択します。

d. [* 構成 **]** タブを選択し、次に **[** メイン *] タブを選択します。

e. [* Storage State-Desired * （ストレージ状態 - 目的 * ） ] ドロップダウンリストが [ 読み取り専用 ] または [ オフライン ] に設定されている場合は、 [* オンライン * ] を選択します。

f. [ 変更の適用 *] をクリックします。

7. 新しいオブジェクトストアを確認するには、次の手順を実行し

a. ノード*>**site* **>*_**ストレージノード>*ストレージ*を選択します。

b. 詳細は、 * Object Stores * テーブルを参照してください。

結果

拡張したストレージノードの容量をオブジェクトデータの保存に使用できるようになりました。

関連情報

"VMware をインストールする"

**Linux**：ストレージノードへの直接接続型ボリュームまたは**SAN**ボリュームの追加

## ストレージノードのストレージボリュームが 16 個より少ない場合は、新しいブロックストレージデバイスを追加して Linux ホストから認識されるようにし、ストレージノードで使用される StorageGRID 構成ファイルに新しいブロックデバイスマッピングを追加することで、ストレージノードの容量を増やすことができます。

必要なもの

- Linuxプラットフォーム用のStorageGRID のインストール手順を参照できる必要があります。

- を用意しておく必要があります `Passwords.txt` ファイル。
- 特定のアクセス権限が必要です。

> ソフトウェアのアップグレード、リカバリ用手順 、または別の拡張手順 がアクティブな状態でストレージノードにストレージボリュームを追加しないでください。

このタスクについて

ストレージボリュームを追加するときは、ストレージノードが一時的に使用できない状態になっています。クライアント向けのグリッドサービスへの影響を回避するために、この手順 は一度に 1 つのストレージノードでのみ実行してください。

手順

1. 新しいストレージハードウェアを設置します。

   詳細については、ハードウェアベンダーが提供しているドキュメントを参照してください。

2. 必要なサイズの新しいブロックストレージボリュームを作成します。
   - 新しいディスクドライブを接続して RAID コントローラ構成を必要に応じて更新するか、共有ストレージアレイに新しい SAN LUN を割り当てて Linux ホストにアクセスを許可します。
   - 既存のストレージノード上のストレージボリュームと同じ永続的な命名規則を使用します。
   - StorageGRID のノード移行機能を使用する場合は、このストレージノードの移行のターゲットとなる他の Linux ホストから新しいボリュームが認識されるようにします。詳細については、使用している Linux プラットフォーム用の StorageGRID のインストール手順を参照してください。
3. ストレージノードをサポートする Linux ホストに、 root アカウントまたは sudo 権限を持つアカウントでログインします。
4. 新しいストレージボリュームが Linux ホストで認識されていることを確認します。

   デバイスを再スキャンしなければならない場合があります。

5. 次のコマンドを実行して、ストレージノードを一時的に無効にします。

   ```
   sudo storagegrid node stop <node-name>
   ```

6. vimやpicoなどのテキストエディタを使用して、ストレージノードのノード構成ファイルを編集します `/etc/storagegrid/nodes/<node-name>.conf`。
7. ノード構成ファイルで、既存のオブジェクトストレージのブロックデバイスマッピングが含まれているセクションを探します。

   この例では、 `BLOCK_DEVICE_RANGEDB_00` 終了： `BLOCK_DEVICE_RANGEDB_03` は、既存のオブジェクトストレージのブロックデバイスマッピングです。

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/sgws-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/sgws-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/sgws-sn1-rangedb-3
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

8. このストレージノード用に追加したブロックストレージボリュームに対応する新しいオブジェクトストレージのブロックデバイスマッピングを追加します。

   次のから始めてください `BLOCK_DEVICE_RANGEDB_nn`。間を空けずに続けて指定してください。

   - 上記の例に基づいて、から開始します `BLOCK_DEVICE_RANGEDB_04`。
   - 次の例では、4つのブロックストレージボリュームが新しいノードに追加されています。 `BLOCK_DEVICE_RANGEDB_04` 終了： `BLOCK_DEVICE_RANGEDB_07`。

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/sgws-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/sgws-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/sgws-sn1-rangedb-3
<strong>BLOCK_DEVICE_RANGEDB_04 = /dev/mapper/sgws-sn1-rangedb-
4</strong>
<strong>BLOCK_DEVICE_RANGEDB_05 = /dev/mapper/sgws-sn1-rangedb-
5</strong>
<strong>BLOCK_DEVICE_RANGEDB_06 = /dev/mapper/sgws-sn1-rangedb-
6</strong>
<strong>BLOCK_DEVICE_RANGEDB_07 = /dev/mapper/sgws-sn1-rangedb-
7</strong>
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

9. 次のコマンドを実行して、ストレージノードのノード構成ファイルに対する変更を検証します。

   ```
   sudo storagegrid node validate <node-name>
   ```

   エラーや警告がある場合は、次の手順に進む前に対処してください。

   次のようなエラーが表示される場合は、で使用されるブロックデバイスのマッピングがノード構成ファイルで試行されていることを示しています `<node-name>` の場合 `<PURPOSE>` を指定したに移動します `<path-name>` Linuxファイルシステムに、有効なブロックデバイススペシャルファイル（またはブロックデバイススペシャルファイルへのソフトリンク）がない。

   ```
   Checking configuration file for node <node-name>…
   ERROR: BLOCK_DEVICE_<PURPOSE> = <path-name>
   <path-name> is not a valid block device
   ```

   正しいが入力されていることを確認してください `<path-name>`。

10. 次のコマンドを実行して、新しいブロックデバイスマッピングを設定したノードを再起動します。

    ```
    sudo storagegrid node start <node-name>
    ```

11. に記載されているパスワードを使用して、ストレージノードにadminとしてログインします `Passwords.txt` ファイル。
12. サービスが正しく開始されることを確認します。
    a. サーバ上のすべてのサービスのステータスのリストを表示します:+
       `sudo storagegrid-status`

       ステータスは自動的に更新されます。

    b. すべてのサービスが「 Running 」または「 Verified 」になるまで待ちます。
    c. ステータス画面を終了します。

       `Ctrl+C`

13. ストレージノードで使用する新しいストレージを設定します。
    a. 新しいストレージボリュームを設定します。

       `sudo add_rangedbs.rb`

    新しいストレージボリュームがすべて検出され、それらをフォーマットするように求められます。

    a. 「 * y * 」と入力して、ストレージボリュームをフォーマットします。
    b. 以前にフォーマットされたボリュームがある場合は、それらを再フォーマットするかどうかを決めます。
       - 再フォーマットするには「 * y * 」と入力します。

- 再フォーマットをスキップするには「 * n * 」と入力します。ストレージボリュームがフォーマットされます。

c. プロンプトが表示されたら、「 * y 」と入力してストレージサービスを停止します。

ストレージサービスが停止され、が停止されます `setup_rangedbs.sh` スクリプトは自動的に実行されます。ボリュームが rangedb として使用できるようになると、サービスが再び開始されます。

14. サービスが正しく開始されることを確認します。

a. サーバ上のすべてのサービスのステータスのリストを表示します。

```
sudo storagegrid-status
```

ステータスは自動的に更新されます。

a. すべてのサービスが「 Running 」または「 Verified 」になるまで待ちます。

b. ステータス画面を終了します。

```
Ctrl+C
```

15. ストレージノードがオンラインであることを確認します。

a. サポートされているブラウザを使用してGrid Managerにサインインします。

b. Support **>** Tools **>** Grid Topology *を選択します。

c. 「 * *site* * > * _ *Storage Node** > * LDR * > * Storage * 」を選択します。

d. [* 構成 **]** タブを選択し、次に **[** メイン *] タブを選択します。

e. [* Storage State-Desired * （ストレージ状態 - 目的 * ） ] ドロップダウンリストが [ 読み取り専用 ] または [ オフライン ] に設定されている場合は、 [* オンライン * ] を選択します。

f. [ 変更の適用 *] をクリックします。

16. 新しいオブジェクトストアを確認するには、次の手順を実行し

a. ノード*>**site* **>*_**ストレージノード>*ストレージ*を選択します。

b. 詳細は、 * Object Stores * テーブルを参照してください。

結果

拡張したストレージノードの容量をオブジェクトデータの保存に使用できるようになりました。

関連情報

"Red Hat Enterprise Linux または CentOS をインストールします"

"Ubuntu または Debian をインストールします"

## 既存のサイトへのグリッドノードの追加と新しいサイトの追加

この手順 を使用して、既存のサイトにグリッドノードを追加したり、新しいサイトを追加したりできますが、両方のタイプの拡張を同時に実行することはできません。

必要なもの

- root権限またはmaintenance権限が必要です。詳細については、管理者ユーザアカウントおよびグループを使用したシステムアクセスの制御に関する情報を参照してください。
- グリッド内のすべての既存ノードがすべてのサイトで動作している必要があります。
- 前の拡張、アップグレード、運用停止、またはリカバリの手順が完了している必要があります。

> 拡張は、別の拡張、アップグレード、リカバリ、またはアクティブな運用停止の手順 を実行中のときは開始できません。ただし、必要に応じて、運用停止手順 を一時停止して拡張を開始できます。

手順

1. "グリッドネットワークのサブネットを更新しています"
2. "新しいグリッドノードの導入"
3. "拡張の実施"

グリッドネットワークのサブネットを更新しています

## グリッドノードまたは新しいサイトを追加した場合は、サブネットの更新、またはグリッドネットワークへのサブネットの追加が必要になることがあります。

StorageGRID は、グリッドネットワーク（ eth0 ）上のグリッドノード間の通信に使用されるネットワークサブネットのリストを管理します。このエントリには、 StorageGRID システムの各サイトでグリッドネットワークに使用されているサブネット、およびグリッドネットワークゲートウェイ経由でアクセスされる NTP 、 DNS 、 LDAP 、またはその他の外部サーバに使用されるサブネットが含まれます。

必要なもの

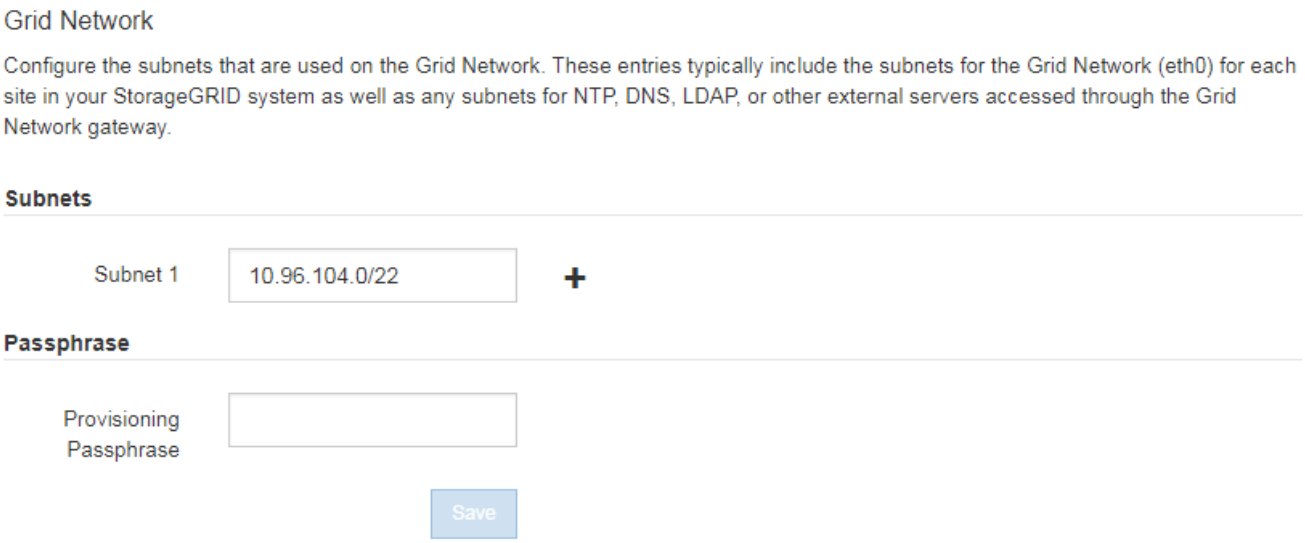
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Maintenance または Root Access 権限が必要です。
- プロビジョニングパスフレーズが必要です。
- 設定するサブネットのネットワークアドレスを CIDR 表記で指定する必要があります。

このタスクについて

新しいサブネットの追加を含む拡張アクティビティを実行する場合は、拡張手順 を開始する前に新しいグリッドサブネットを追加する必要があります。

手順

1. [* Maintenance （メンテナンス）**]>[** Network （*ネットワーク）]>[* Grid Network（*グリッドネットワーク）




2. サブネットのリストで、プラス記号をクリックして、 CIDR 表記の新しいサブネットを追加します。

   たとえば、「 10.96.104.0/22 」と入力します。

3. プロビジョニングパスフレーズを入力し、 * Save * をクリックします。

   指定したサブネットが、 StorageGRID システムに対して自動的に設定されます。

新しいグリッドノードの導入

## 拡張時に新しいグリッドノードを導入する手順は、グリッドを最初にインストールしたときに使用した手順と同じです。拡張を実行する前に、すべての新しいグリッドノードの導入が完了している必要があります。

グリッドを拡張する際に、追加するノードが既存のノードと同じタイプである必要はありません。VMware ノード、 Linux コンテナベースのノード、またはアプライアンスノードを追加できます。

**VMware**：グリッドノードの導入

拡張で追加する VMware ノードごとに、 VMware vSphere で仮想マシンを導入する必要があります。

手順

1. 新しいグリッドノードを仮想マシンとして導入し、1つ以上のStorageGRID ネットワークに接続します。

   ノードを導入する際には、必要に応じてノードポートを再マッピングしたり、 CPU やメモリの設定を増やしたりできます。

   "仮想マシンとしてのStorageGRID ノードの導入"

2. すべての新しいVMwareノードを導入したら、次の手順に戻って拡張手順 を実行します。

   "拡張の実施"

**Linux**：グリッドノードの導入

グリッドノードは、新規の Linux ホストにも既存の Linux ホストにも導入できます。グリッドに追加する StorageGRID ノードの CPU 、 RAM 、およびストレージの要件に対応するために追加の Linux ホストが必要な場合は、最初にインストールしたときと同じ方法で準備します。その後、インストール時のグリッドノードと同じ方法で拡張ノードを導入します。

必要なもの

- 使用している Linux のバージョンに対応した StorageGRID のインストール手順が必要です。また、ハードウェアとストレージの要件を確認しておく必要があります。
- 既存のホストに新しいグリッドノードを導入する場合は、既存のホストが追加のノードに対応する十分な CPU 、 RAM 、ストレージ容量を備えていることを確認しておきます。
- 障害ドメインを最小限に抑えるための計画が必要です。たとえば、すべてのゲートウェイノードを 1 つの物理ホストに導入することは避けてください。

> ⓘ 本番環境では、 1 つの物理ホストまたは仮想ホストで複数のストレージノードを実行しないでください。各ストレージノードに専用のホストを使用すると、分離された障害ドメインが提供されます。

- StorageGRID ノードが NetApp AFF システムから割り当てられたストレージを使用している場合は、ボリュームで FabricPool 階層化ポリシーが有効になっていないことを確認してください。StorageGRID ノードで使用するボリュームで FabricPool による階層化を無効にすることで、トラブルシューティングとストレージの処理がシンプルになります。

> ⓘ StorageGRID を使用して StorageGRID に関連するデータを FabricPool 自体に階層化しないでください。StorageGRID データを StorageGRID に階層化すると、トラブルシューティングと運用がより複雑になります。

手順

1. ホストを新規に追加する場合は、 StorageGRID ノードの導入に関するインストール手順を参照します。
2. 新しいホストを導入するには、ホストの準備手順に従います。
3. ノード構成ファイルを作成し、 StorageGRID の設定を検証するには、グリッドノードの導入手順に従います。
4. 新しい Linux ホストにノードを追加する場合は、 StorageGRID ホストサービスを開始します。
5. 既存のLinuxホストにノードを追加する場合は、StorageGRID ホストサービスCLIを使用して新しいノードを開始します。`sudo storagegrid node start [<node name\>]`

完了後

すべての新しいグリッドノードの導入が完了したら、拡張を実施できます。

- 関連情報 *

"Red Hat Enterprise Linux または CentOS をインストールします"

"Ubuntu または Debian をインストールします"

"拡張の実施"

アプライアンスノードに StorageGRID ソフトウェアをインストールするには、アプライアンスに含まれている StorageGRID アプライアンスインストーラを使用します。拡張時、各ストレージアプライアンスは単一のストレージノードとして機能し、各サービスアプライアンスは単一のゲートウェイノードまたは非プライマリ管理ノードとして機能します。すべてのアプライアンスは、グリッドネットワーク、管理ネットワーク、およびクライアントネットワークに接続できます。

必要なもの

- アプライアンスをラックまたはキャビネットに設置し、ネットワークに接続し、電源を投入しておきます。
- StorageGRID アプライアンス・インストーラを使用して'アプライアンスのインストールおよびメンテナンス手順のすべてのハードウェアの構成手順を完了しました

  アプライアンスハードウェアの設定には、 StorageGRID 接続（ネットワークリンクおよび IP アドレス）の設定に必要な手順、およびノードの暗号化を有効にする手順、 RAID モードの変更、ネットワークポートの再マッピングを行うオプションの手順が含まれます。

- StorageGRID アプライアンスインストーラの IP 設定ページに表示されるすべてのグリッドネットワークサブネットが、プライマリ管理ノードのグリッドネットワークサブネットリストで定義されている。
- 交換用アプライアンスのStorageGRID アプライアンスインストーラのバージョンがStorageGRID システムのソフトウェアバージョンと同じであることを確認します。（バージョンが一致しない場合は、StorageGRID アプライアンスインストーラファームウェアをアップグレードする必要があります）。

  手順については、アプライアンスのインストールとメンテナンスの手順を参照してください。

  - "SG100 SG1000サービスアプライアンス"
  - "SG5600 ストレージアプライアンス"
  - "SG5700 ストレージアプライアンス"
  - "SG6000 ストレージアプライアンス"
- サポートされている Web ブラウザがインストールされたサービスラップトップを用意しておきます。
- アプライアンスのコンピューティングコントローラに割り当てられている IP アドレスのいずれかを確認しておきます。接続されているどの StorageGRID ネットワークの IP アドレスでも使用できます。

このタスクについて

アプライアンスノードに StorageGRID をインストールするプロセスには、次のフェーズがあります。

- プライマリ管理ノードの IP アドレスおよびアプライアンスノードの名前を指定または確認します。
- インストールを開始し、ボリュームの設定とソフトウェアのインストールが行われている間待機します。

  アプライアンスインストールタスクの途中で、インストールが一時停止します。インストールを再開するには、 Grid Manager にサインインし、グリッドノードをすべて承認し、 StorageGRID のインストールプロセスを完了します。

> 一度に複数のアプライアンスノードを導入する必要がある場合は、を使用してインストールプロセスを自動化できます `configure-sga.py` アプライアンスインストールスクリプト。

手順

1. ブラウザを開き、アプライアンスのコンピューティングコントローラの IP アドレスのいずれかを入力します。

   `https://Controller_IP:8443`

   StorageGRID アプライアンスインストーラのホームページが表示されます。

2. 「 * プライマリ管理ノード * 接続」セクションで、プライマリ管理ノードの IP アドレスを指定する必要があるかどうかを確認します。

   このデータセンターに他のノードがすでにインストールされている場合は、プライマリ管理ノードまたは ADMIN_IP が設定された少なくとも 1 つのグリッドノードが同じサブネットにあるという想定で、StorageGRID アプライアンスインストーラがこの IP アドレスを自動的に検出します。

3. この IP アドレスが表示されない場合や変更する必要がある場合は、アドレスを指定します。

| オプション | 説明 |
| --- | --- |
| IP を手動で入力します | a. Enable Admin Node discovery * チェックボックスの選択を解除します。<br>b. IP アドレスを手動で入力します。<br>c. [ 保存（ Save ） ] をクリックします。<br>d. 新しい IP アドレスの接続状態が READY になるまで待ちます。 |
| 接続されたすべてのプライマリ管理ノードの自動検出 | a. Enable Admin Node discovery * チェックボックスを選択します。<br>b. 検出された IP アドレスのリストが表示されるまで待ちます。<br>c. このアプライアンスストレージノードを導入するグリッドのプライマリ管理ノードを選択します。<br>d. [ 保存（ Save ） ] をクリックします。<br>e. 新しい IP アドレスの接続状態が READY になるまで待ちます。 |

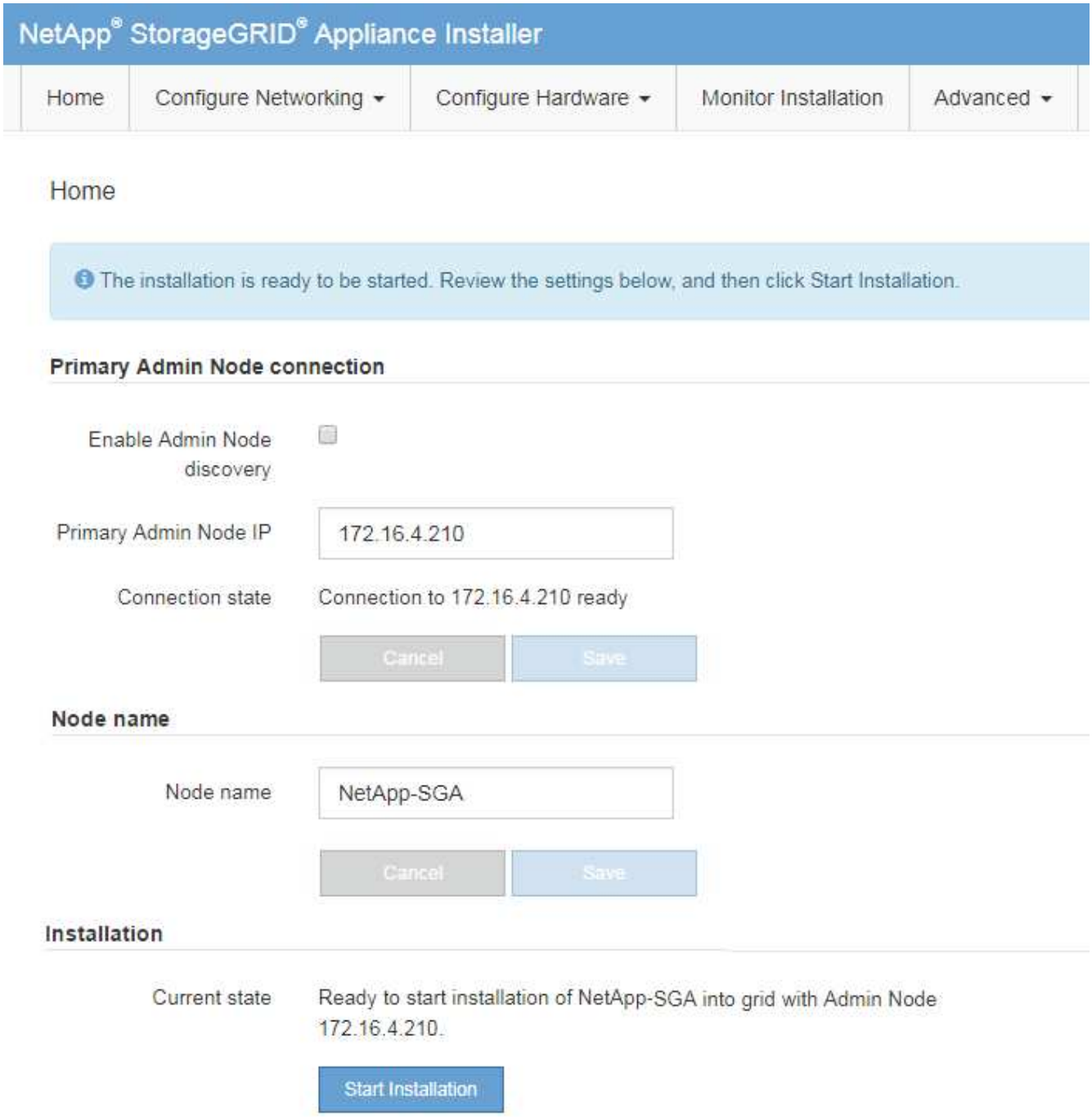
4. [* Node name* （ノード名 * ） ] フィールドに、このアプライアンスノードに使用する名前を入力し、 [ * Save * （保存） ] をクリックします。

   このノード名は、 StorageGRID システムでこのアプライアンスノードに割り当てられ、このタブは、Grid Manager のノードページ（概要タブ）に表示されます。ノードを承認するときに、必要に応じて、この名前を変更できます。

5. 「 * インストール * 」セクションで、現在の状態が「プライマリ管理ノード *admin_ip*` を使用した _ ノード name_into グリッドのインストールを開始する準備ができている」であり、「インストールの開始 * 」ボタンが有効になっていることを確認します。

   [Start Installation* （インストールの開始） ] ボタンが有効になっていない場合は、ネットワーク設定またはポート設定の変更が必要になることがあります。手順については、使用しているアプライアンスのインストールとメンテナンスの手順を参照してください。

6. StorageGRID アプライアンスインストーラのホームページで、 * インストールの開始 * をクリックします。




現在の状態が「 Installation is in progress 」に変わり、「 Monitor Installation 」ページが表示されます。

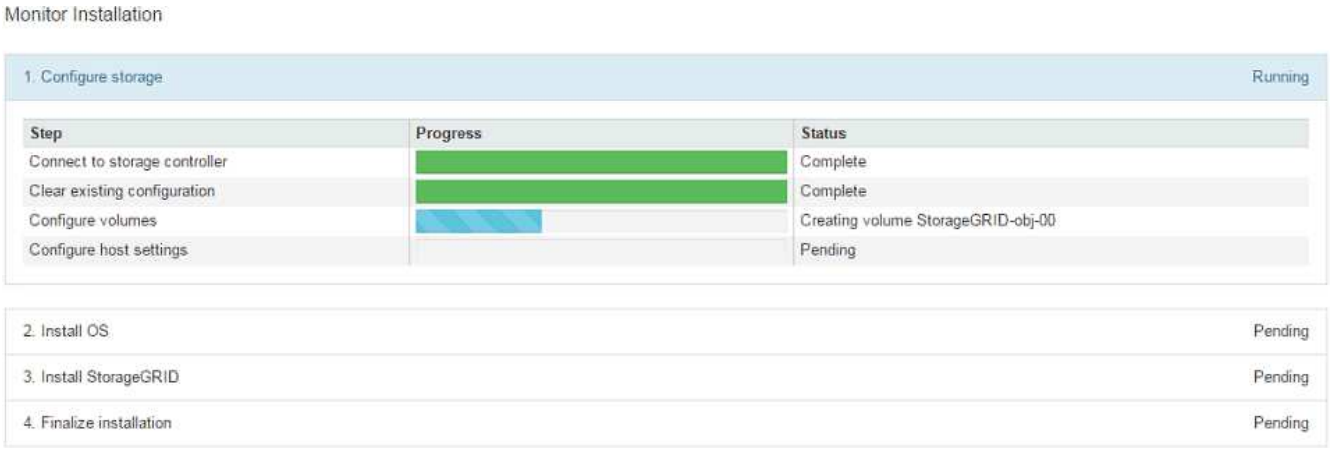
7. 拡張に複数のアプライアンスノードが含まれている場合は、アプライアンスごとに上記の手順を繰り返します。

> 一度に複数のアプライアンスストレージノードを導入する必要がある場合は、 configure-sga.py アプライアンスインストールスクリプトを使用してインストールプロセスを自動化できます。

8. モニタのインストールページに手動でアクセスする必要がある場合は、メニューバーから*モニタのイン

ストール*をクリックします。

Monitor Installation ページにインストールの進行状況が表示されます。




青色のステータスバーは、現在進行中のタスクを示します。緑のステータスバーは、正常に完了したタスクを示します。

インストーラは、以前のインストールで完了したタスクが再実行されないようにします。インストールを再実行している場合 ' 再実行する必要のないタスクは ' 緑色のステータスバーとステータスが [ スキップ済み ] と表示されます

9. インストールの最初の 2 つのステージの進行状況を確認します。

◦ 1 。アプライアンスを設定 *

この段階では、次のいずれかのプロセスが実行されます。

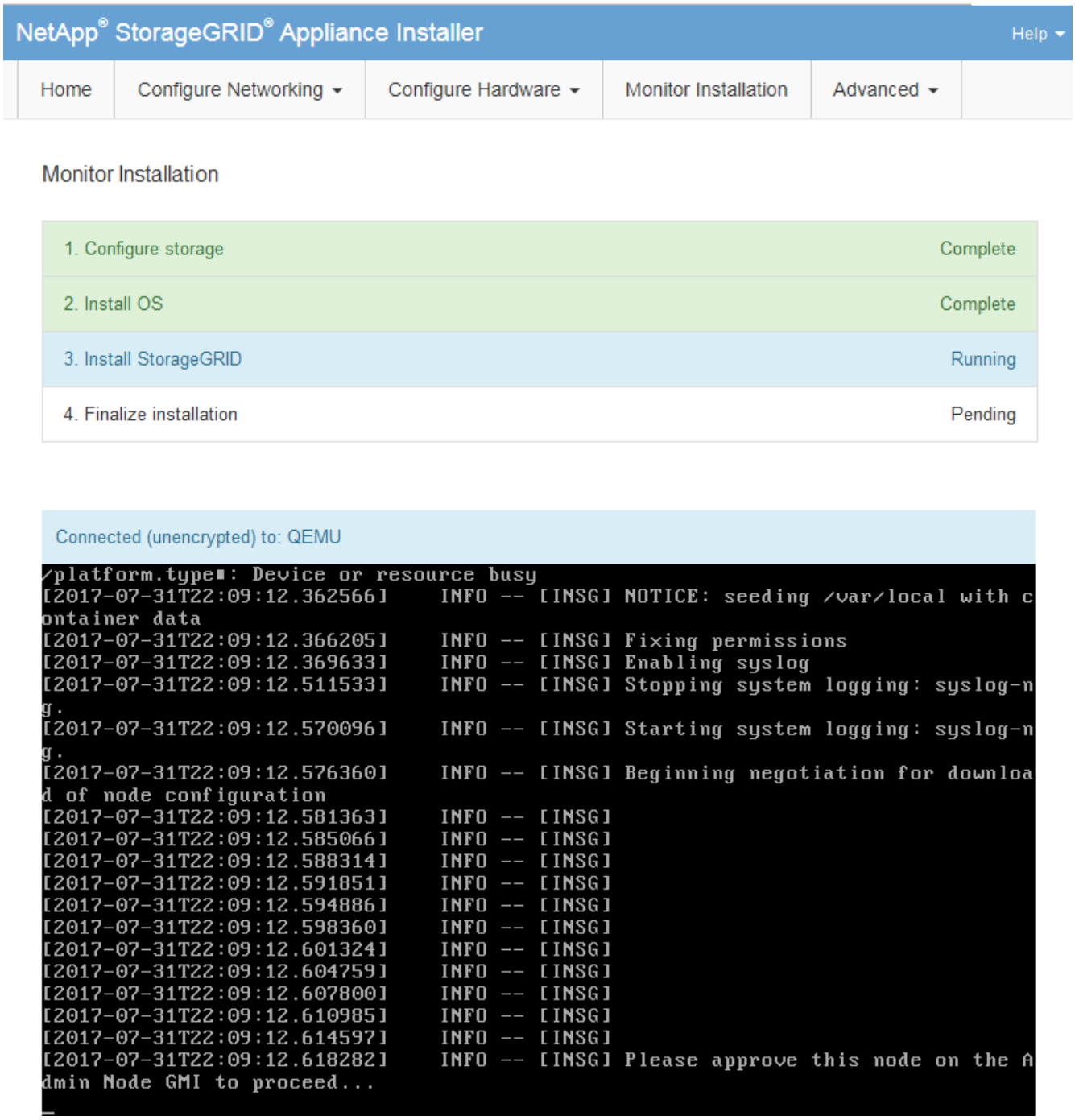
- ストレージアプライアンスの場合、インストーラがストレージコントローラに接続し、既存の設定があれば消去し、 SANtricity ソフトウェアと通信してボリュームを設定し、ホストを設定します。
- サービスアプライアンスの場合、既存の設定があればインストーラがコンピューティングコントローラのドライブから消去し、ホストを設定します。

※ 2OS * をインストールします

インストーラが StorageGRID のベースとなるオペレーティングシステムイメージをアプライアンスにコピーします。

10. コンソールウィンドウにメッセージが表示され、 Grid Manager を使用してノードを承認するように求めるメッセージが表示されるまで、インストールの進行状況の監視を続けます。

この拡張で追加したすべてのノードが承認できる状態になるまでは、 Grid Manager でノードを承認しないでください。




◦ 関連情報 *

"SG5700 ストレージアプライアンス"

"SG5600 ストレージアプライアンス"

"SG6000 ストレージアプライアンス"

"SG100 SG1000サービスアプライアンス"

# 拡張を行うと、新しいグリッドノードが既存の StorageGRID 環境に追加されます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Maintenance または Root Access 権限が必要です。
- プロビジョニングパスフレーズが必要です。
- この拡張で追加するすべてのグリッドノードの導入が完了している必要があります。
- ストレージノードを追加する場合は、リカバリの一環として実行されるデータ修復処理がすべて完了したことを確認しておく必要があります。リカバリとメンテナンスの手順のデータ修復ジョブを確認する手順を参照してください。
- 新しいサイトを追加する場合は、拡張手順 を開始する前に ILM ルールを確認して更新し、拡張が完了するまでオブジェクトコピーが新しいサイトに格納されないようにする必要があります。たとえば、デフォルトのストレージプール（すべてのストレージノード）を使用するルールの場合は、既存のストレージノードのみを含む新しいストレージプールを作成し、その新しいストレージプールを使用するように ILM ルールを更新する必要があります。そうしないと、そのサイトの最初のノードがアクティブになるとすぐに新しいサイトにオブジェクトがコピーされます。情報ライフサイクル管理を使用してオブジェクトを管理する手順を参照してください。

このタスクについて

拡張は次のフェーズで行います。

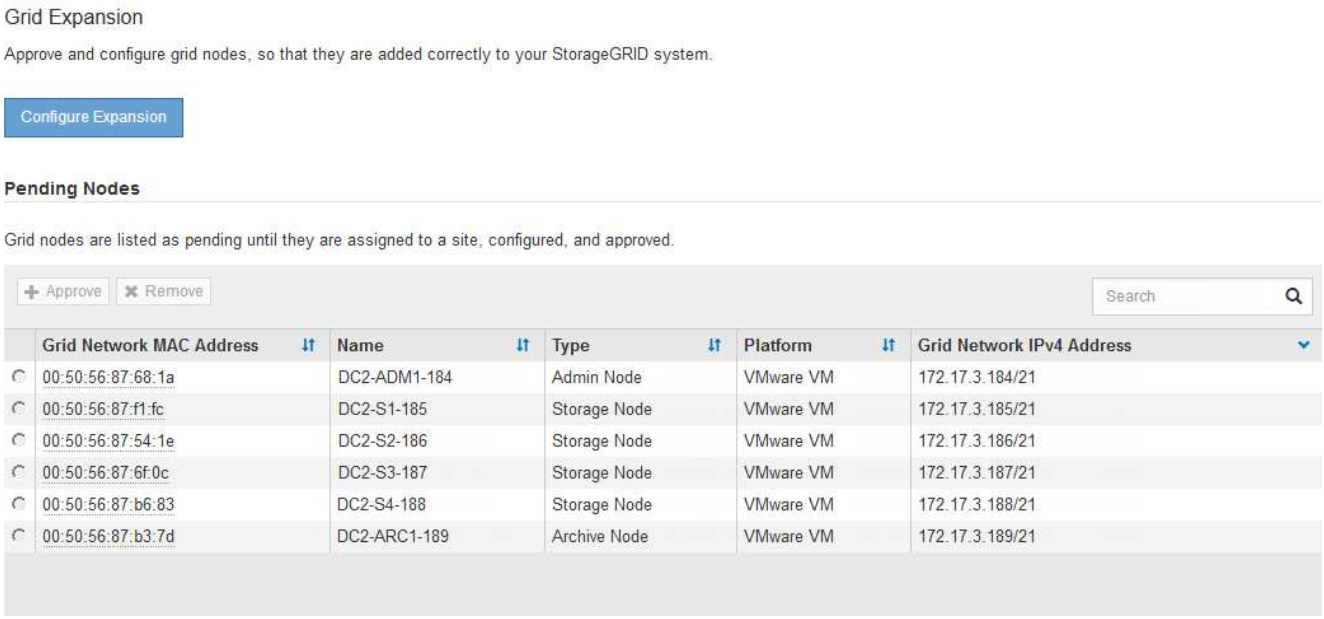
1. 拡張を設定するには、新しいグリッドノードと新しいサイトのどちらを追加するかを指定し、追加するグリッドノードを承認します。
2. 拡張を開始します。
3. 拡張プロセスの実行中に、新しいリカバリパッケージファイルをダウンロードします。
4. グリッド設定タスクのステータスを監視します。このタスクは自動的に実行されます。タスクのセットは、追加するグリッドノードのタイプおよび新しいサイトが追加されるかどうかによって異なります。

> 大規模なグリッドにおいては、一部のタスクの実行にかなりの時間がかかることがあります。たとえば、新しいストレージノードへのCassandraのストリーミングは、Cassandraデータベースが空に近い状態であれば数分程度で完了します。ただし、 Cassandra データベースに大量のオブジェクトメタデータが含まれている場合は、数時間以上かかることがあります。「Starting Cassandra and streaming data」ステージで表示される「streamed」の割合を見ると、Cassandraストリーミング処理の完了状況を判断できます。

手順

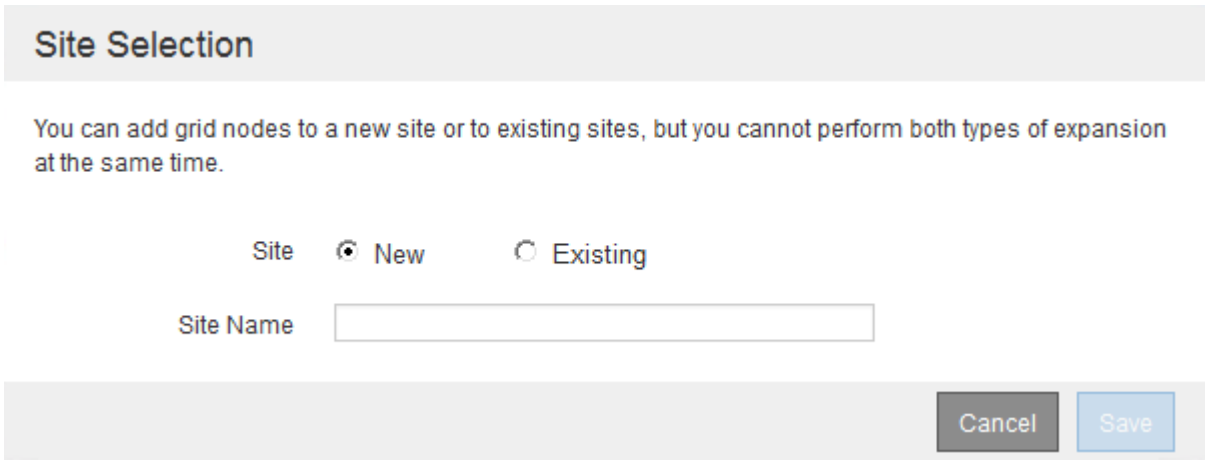
1. [* Maintenance（メンテナンス）> Maintenance Tasks（メンテナンスタスク）> Expansion（拡張）*]を選択します。

   Grid Expansion ページが表示されます。Pending Nodes セクションには、追加する準備ができているすべてのノードが表示されます。



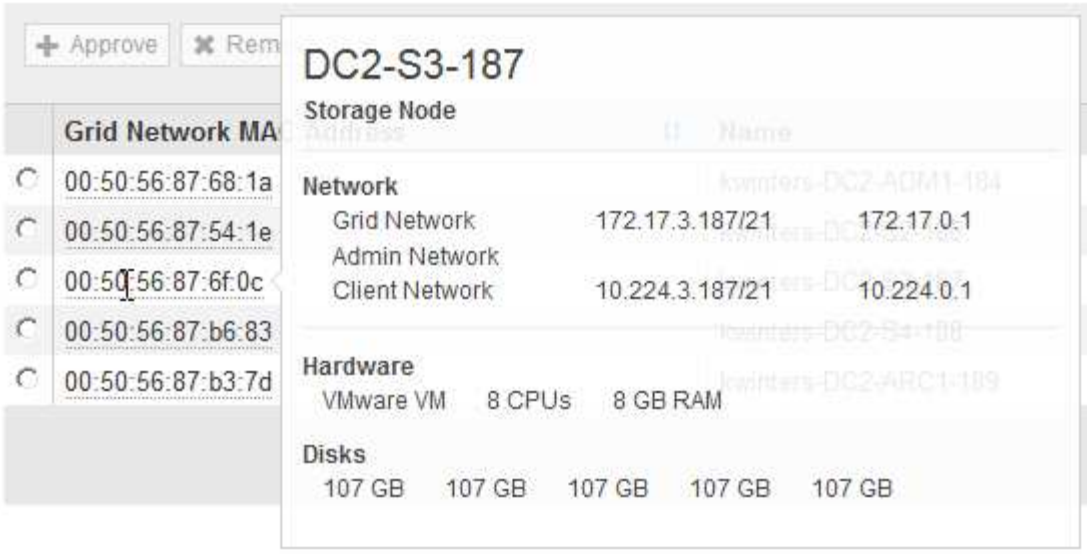

2. [拡張の構成*]をクリックします。

   [ サイトの選択 ] ダイアログボックスが表示されます。




3. 開始する拡張のタイプを選択します。
   - 新しいサイトを追加する場合は、「 * 新規」を選択し、新しいサイトの名前を入力します。
   - 既存のサイトにグリッドノードを追加する場合は、「 * existing * 」を選択します。
4. [ 保存（ Save ） ] をクリックします。
5. 「 * Pending Nodes * 」のリストを確認し、導入したすべてのグリッドノードが表示されていることを確認します。

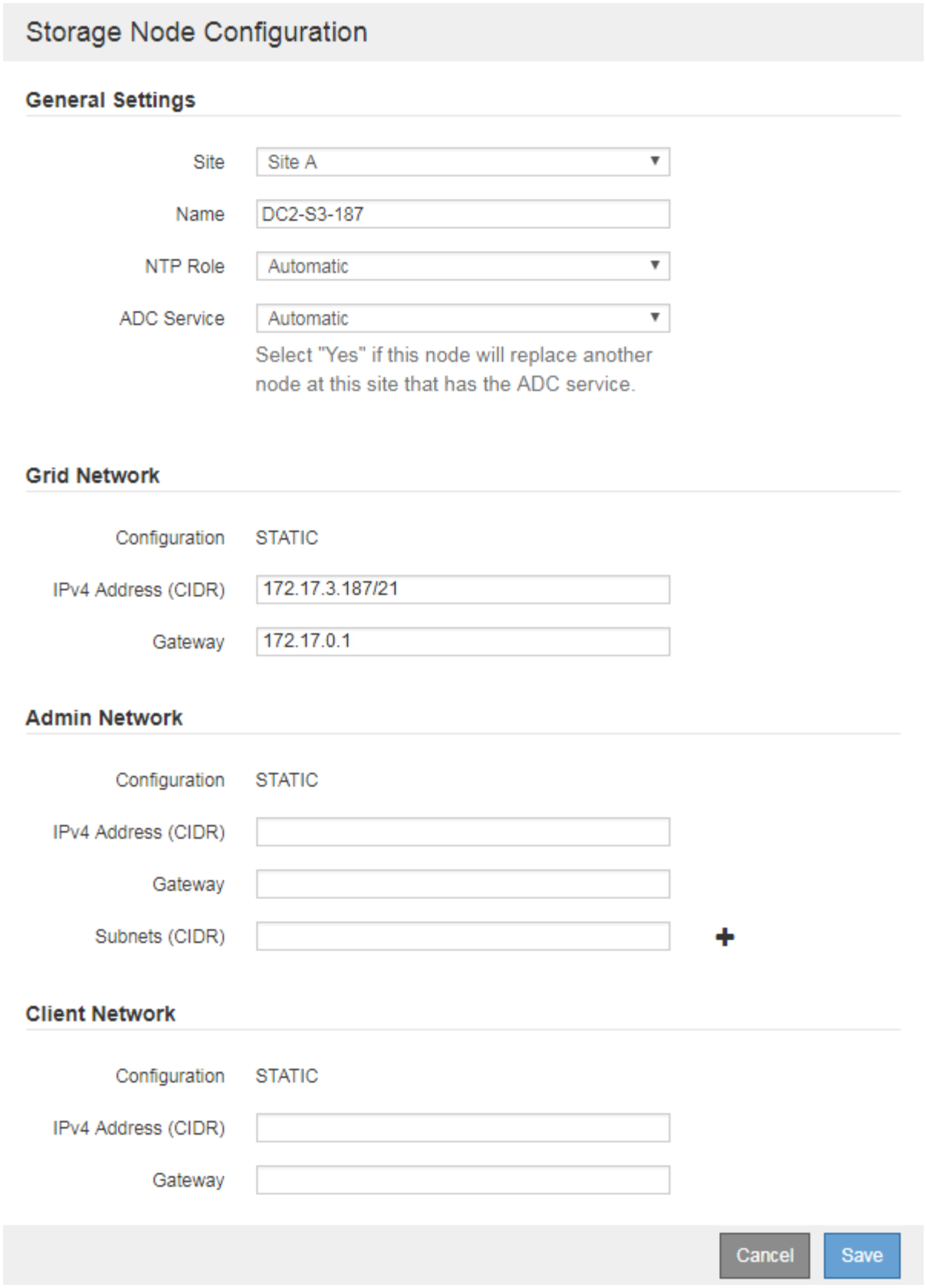
   必要に応じて、ノードの * グリッドネットワークの MAC アドレス * にカーソルを合わせると、そのノードに関する詳細を確認できます。




見つからないグリッドノードがある場合は、正常に導入されたことを確認します。

6. 保留中のノードのリストで、この拡張用のグリッドノードを承認します。
   a. 承認する最初の保留中のグリッドノードの横にあるラジオボタンを選択します。
   b. [ 承認（ Approve ） ] をクリックします

      グリッドノードの設定フォームが表示されます。




c. 必要に応じて、一般設定を変更します。

- * サイト * ：グリッドノードが関連付けられるサイトの名前。複数のノードを追加する場合は、各ノードに適したサイトを選択してください。新しいサイトを追加する場合は、すべてのノードが新しいサイトに追加されます。

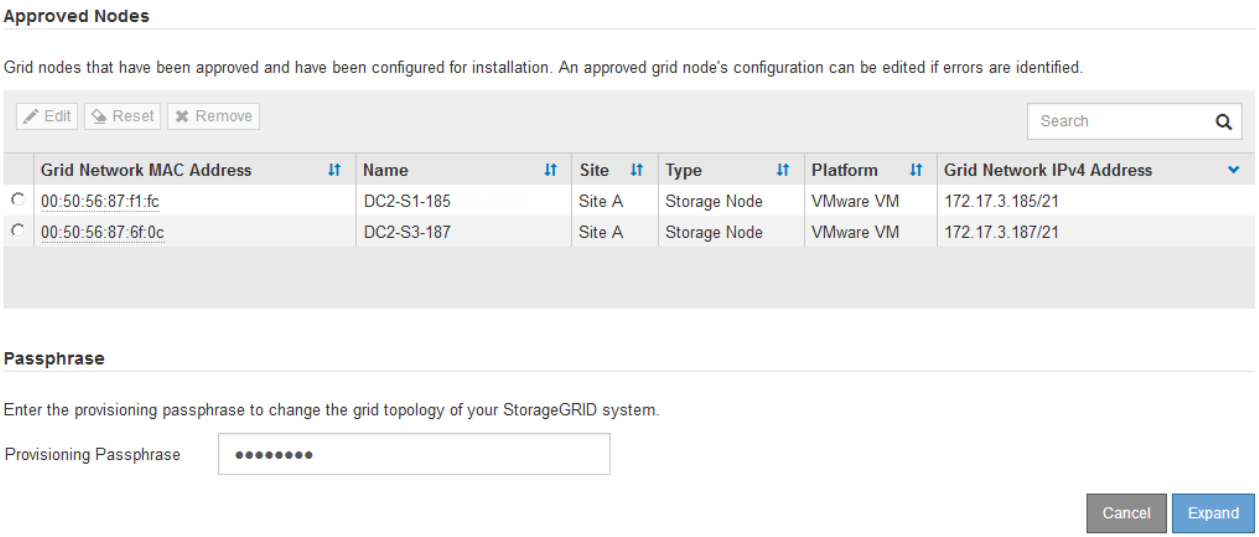
- * 名前 * ：ノードに割り当てられるホスト名と Grid Manager に表示される名前。
- * NTP Role * ：グリッドノードのネットワークタイムプロトコル（ NTP ）ロール。オプションは * Automatic * 、 * Primary * 、 * Client * です。「 * 自動」を選択すると、管理ノード、 ADC サービスを採用するストレージノード、ゲートウェイノード、および静的な IP アドレスでないグリッドノードにプライマリロールが割り当てられます。他のすべてのグリッドノードにはクライアントロールが割り当てられます。

  Primary NTP ロールは、各サイトで少なくとも 2 つのノードに割り当ててください。これにより、外部タイミングソースへのシステムアクセスが冗長化されます。

- * ADC Service * （ストレージノードのみ）：このストレージノードで Administrative Domain Controller （ ADC ）サービスを実行するかどうかを指定します。 ADC サービスは、グリッドサービスの場所と可用性を追跡します。各サイトで少なくとも 3 つのストレージノードに ADC サービスが含まれている必要があります。導入後のノードに ADC サービスを追加することはできません。
  - このノードを追加してストレージノードを交換する場合は、交換するノードに ADC サービスが含まれている場合は「 * Yes 」を選択します。残りの ADC サービスの数が少なすぎるとストレージノードの運用を停止できないため、古いサービスが削除される前に新しい ADC サービスが利用可能になります。
  - それ以外の場合は、 * Automatic * を選択して、このノードに ADC サービスが必要かどうかをシステムに確認させます。リカバリとメンテナンスの手順のADCクォーラムに関する情報を参照してください。

d. 必要に応じて、グリッドネットワーク、管理ネットワーク、およびクライアントネットワークの設定を変更します。
   - * IPv4 Address （ CIDR ） * ：ネットワークインターフェイスの CIDR ネットワークアドレス。たとえば、 172.16.10.100/24 のようになります
   - * Gateway * ：グリッドノードのデフォルトゲートウェイ。たとえば、 172.16.10.1 と入力します
   - * Subnets （ CIDR ） * ：管理ネットワーク用の 1 つ以上のサブネットワーク。
e. [ 保存（ Save ） ] をクリックします。

   承認済みグリッドノードが [ 承認済みノード ] リストに移動します。



- 承認済みグリッドノードのプロパティを変更するには、そのラジオボタンを選択し、*編集*をクリックします。
- 承認済みのグリッドノードを保留中のノードのリストに戻すには、該当するオプションボタンを選択し、*リセット*をクリックします。
- 承認済みのグリッドノードを完全に削除するには、ノードの電源をオフにします。次に、そのラジオボタンを選択し、*削除*をクリックします。

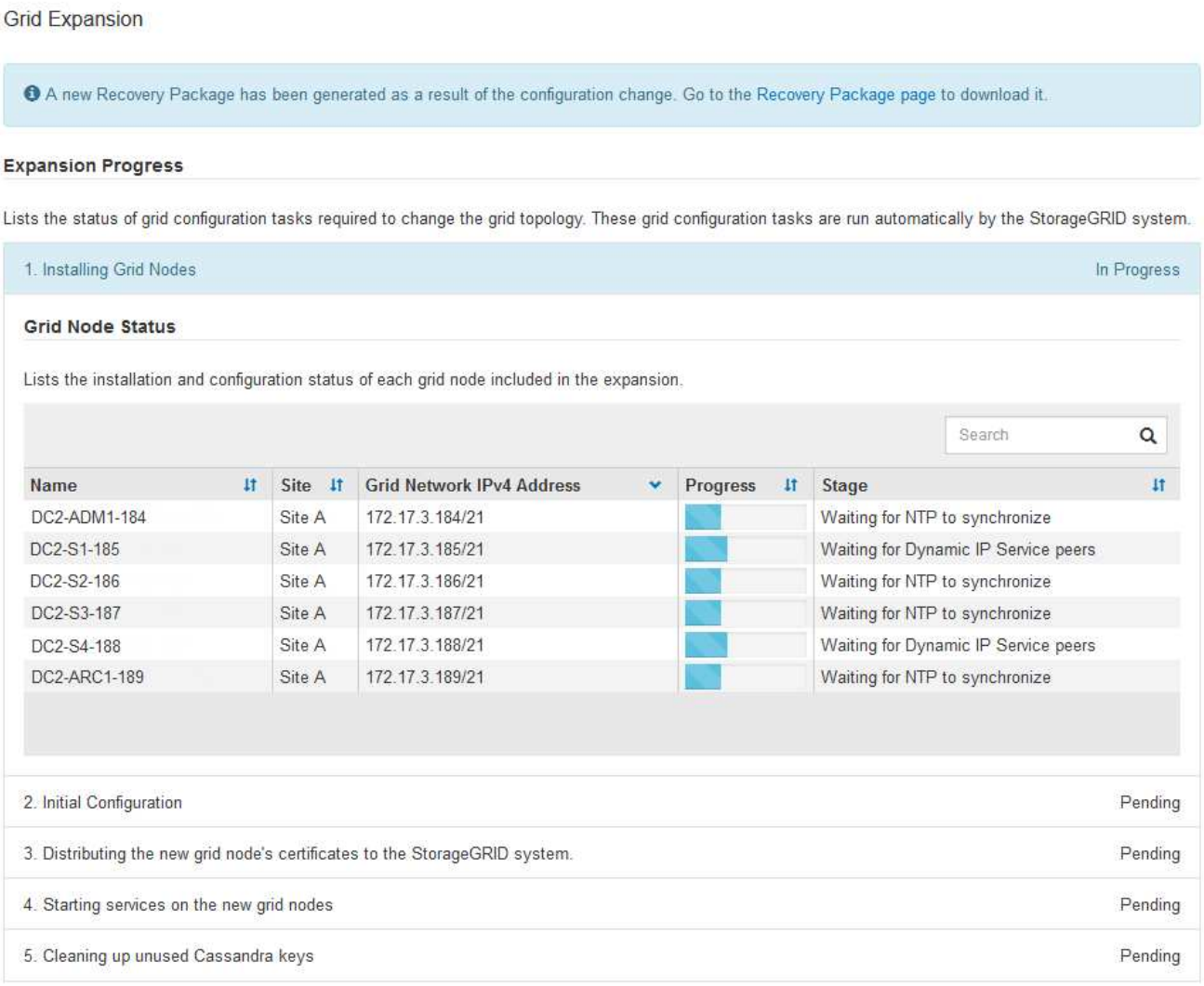
f. 承認する保留中のグリッドノードごとに、上記の手順を繰り返します。

> 可能であれば、保留中のグリッドノードをすべて承認し、 1 回の拡張を実施してください。小規模な拡張を複数回実施すると、さらに時間がかかります。

7. すべてのグリッドノードを承認したら、「*プロビジョニングパスフレーズ」と入力し、「*拡張」をクリックします。

   数分後にページが更新され、拡張手順 のステータスが表示されます。個々のグリッドノードに影響するタスクが実行中の場合は、グリッドノードのステータスセクションに各グリッドノードの現在のステータスが表示されます。

> アプライアンスの場合、インストールがステージ 3 からステージ 4 、 Finalize Installation に移行していることを示す StorageGRID アプライアンスインストーラの処理が実行されます。ステージ 4 が完了すると、コントローラがリブートします。




サイトの拡張には、新しいサイト用の Cassandra を設定するための追加タスクが含まれます。

8. [Download Recovery Package* ] リンクが表示されたら、すぐにリカバリパッケージファイルをダウンロードします。

StorageGRID システムでグリッドトポロジを変更した場合は、できるだけ早くリカバリパッケージファイルの最新コピーをダウンロードする必要があります。リカバリパッケージファイルは、障害が発生した場合にシステムをリストアするために使用します。

a. ダウンロードリンクをクリックします。

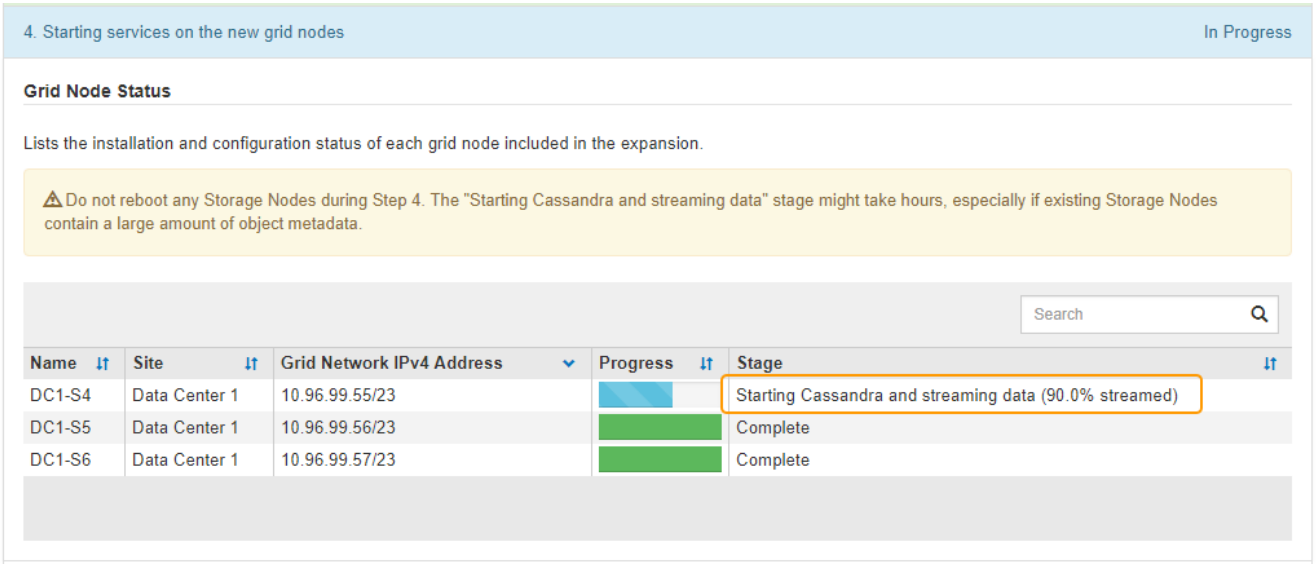
b. プロビジョニングパスフレーズを入力し、*ダウンロードの開始*をクリックします。

c. ダウンロードが完了したら、を開きます `.zip` をファイルし、が含まれていることを確認します `gpt-backup` ディレクトリと `_SAID.zip` ファイル。次に、を展開します `_SAID.zip` ファイルで、に移動します `/GID*_REV*` を開き、確認します `passwords.txt` ファイル。

d. ダウンロードしたリカバリパッケージファイル（ .zip ）を、 2 箇所の安全な場所にコピーします。

リカバリパッケージファイルには StorageGRID システムからデータを取得するための暗号キーとパスワードが含まれているため、安全に保管する必要があります。

9. 1つ以上のストレージノードを追加する場合は、ステータスメッセージに表示される割合を確認して、「Starting Cassandra and streaming data」ステージの進行状況を監視します。




この割合は、使用可能な Cassandra データの合計量と、新しいノードに書き込み済みの量に基づいて、Cassandra のストリーミング処理の進捗状況から概算したものです。

> 手順4（新しいグリッドノードでサービスを開始する）の実行中は、ストレージノードをリブートしないでください。特に、既存のストレージノードに大量のオブジェクトメタデータが含まれている場合は、「Starting Cassandra and streaming data」ステージが新しいストレージノードごとに完了するまでに数時間かかることがあります。

10. すべてのタスクが完了し、 * 拡張の設定 * ボタンが再表示されるまで、拡張の監視を続けます。

完了後

追加したグリッドノードのタイプに応じて、統合と設定のための追加の手順を実行する必要があります。

関連情報

"ILM を使用してオブジェクトを管理する"

""

"拡張後のStorageGRID システムの設定"

## 拡張後のStorageGRID システムの設定

拡張が完了したら、統合と設定のための追加の手順を実行する必要があります。

このタスクについて

拡張で追加するグリッドノードに応じて、次の表の設定タスクを実行する必要があります。システムのインストールや管理の作業で選択したオプションのほか、拡張で追加したグリッドノードの設定方法によっては、省略可能なタスクもあります。

手順

1. ストレージノードを追加した場合は、次の設定タスクを実行します。

| ストレージノードの設定タスク | を参照してください |
| --- | --- |
| ILM ルールで使用されているストレージプールを確認して、新しいストレージが使用されるようにします。<br><br>• サイトを追加した場合は、そのサイトのストレージプールを作成し、新しいストレージプールを使用する ILM ルールを更新します。<br>• 既存のサイトにストレージノードを追加した場合は、新しいノードが正しいストレージグレードを使用していることを確認します。<br><br>注：デフォルトでは、新しいストレージノードが**All Storage Nodes**ストレージグレードに割り当てられ、そのグレードを使用するストレージプールに追加されます。新しいノードでカスタムのストレージグレードを使用する場合は、カスタムグレードに手動で割り当てる必要があります（ ILM **>***ストレージグレード）。 | "ILM を使用してオブジェクトを管理する" |
| ストレージノードがオブジェクトを取り込んでいることを確認する。 | "ストレージノードがアクティブであることを確認しています" |
| イレイジャーコーディングデータのリバランシングを行います（推奨数のストレージノードを追加できなかった場合のみ）。 | "ストレージノードの追加後におけるイレイジャーコーディングデータのリバランシング" |

2. ゲートウェイノードを追加した場合は、次の設定タスクを実行します。

| ゲートウェイノードの設定作業 | を参照してください |
| --- | --- |
| クライアント接続にハイアベイラビリティグループが使用される場合は、HAグループにゲートウェイノードを追加します。既存のHAグループのリストを確認して新しいノードを追加するには、* Configuration **>** Network Settings **>** High Availability Groups *を選択します。 | "StorageGRID の管理" |

3. 管理ノードを追加した場合は、次の設定タスクを実行します。

| 管理ノードの設定タスク | を参照してください |
| --- | --- |
| StorageGRID システムでシングルサインオンが有効になっている場合は、Active Directory Federation Services（AD FS；Active Directoryフェデレーションサービス）で新しい管理ノードの証明書利用者信頼を作成する必要があります。この証明書利用者信頼を作成するまで、ノードにサインインすることはできません。 | "シングルサインオンを設定しています" |

| 管理ノードの設定タスク | を参照してください |
| --- | --- |
| 管理ノードでロードバランササービスを使用する場合は、ハイアベイラビリティグループに管理ノードを追加しなければならないことがあります。既存のHAグループのリストを確認して新しいノードを追加するには、* Configuration > Network Settings > High Availability Groups *を選択します。 | "StorageGRID の管理" |
| 必要に応じて、管理ノードデータベースをプライマリ管理ノードから拡張管理ノードにコピーします。これは、各管理ノードで属性と監査の情報の整合性を維持する場合に行います。 | "管理ノードデータベースをコピーしています" |
| 必要に応じて、 Prometheus データベースをプライマリ管理ノードから拡張管理ノードにコピーします。これは、各管理ノードで指標の履歴の整合性を維持する場合に行います。 | "Prometheus指標のコピー" |
| 必要に応じて、既存の監査ログをプライマリ管理ノードから拡張管理ノードにコピーします。これは、各管理ノードでログの履歴情報の整合性を維持する場合に行います。 | "監査ログをコピーしています" |
| 必要に応じて、 NFS または CIFS ファイル共有を通じて、監査を目的としたシステムへのアクセスを設定します。<br><br>*注意：CIFS / Sambaによる監査エクスポートは廃止されており、今後のStorageGRID リリースで削除される予定です。 | "StorageGRID の管理" |
| 必要に応じて、通知の優先送信者を変更します。拡張管理ノードを優先送信者にすることができます。設定を更新しない場合は、優先送信者として設定された既存の管理ノードから引き続き、 AutoSupport メッセージ、 SNMP 通知、アラート E メール、アラーム E メール（従来のシステム）などの通知が送信されます。 | "StorageGRID の管理" |

4. アーカイブノードを追加した場合は、次の設定タスクを実行します。

| アーカイブノードの設定タスク | を参照してください |
| --- | --- |
| アーカイブノードからターゲットの外部アーカイブストレージシステムへの接続を設定します。拡張が完了すると、 * ARC * > * Target * コンポーネントを通じて接続情報を設定するまで、アーカイブノードはアラーム状態になります。 | "StorageGRID の管理" |
| 新しいアーカイブノードを介してオブジェクトデータをアーカイブするように ILM ポリシーを更新します。 | "ILM を使用してオブジェクトを管理する" |
| アーカイブノードからオブジェクトデータを読み出す速度と効率を監視する属性に対してカスタムアラームを設定します。 | "StorageGRID の管理" |

5. 拡張ノードが信頼されていないクライアントネットワークで追加されたかどうかを確認する方法、またはノードのクライアントネットワークが信頼されていないかどうかを変更する方法については、*

Configuration > Network Settings > Untrusted Client Network *を参照してください。

拡張ノードのクライアントネットワークが信頼されていない場合は、ロードバランサエンドポイントを使用してクライアントネットワークのノードへの接続を確立する必要があります。詳細については、StorageGRID の管理手順を参照してください。

6. Domain Name System （ DNS ；ドメインネームシステム）を設定します。

   DNS 設定をグリッドノードごとに個別に指定していた場合は、新しいノード用のノード単位のカスタム DNS 設定を追加する必要があります。リカバリおよびメンテナンスの手順で、単一グリッドノードのDNS設定の変更に関する情報を参照してください。

   各サイトからローカルでアクセスできる DNS サーバをグリッド全体の DNS サーバリストにいくつか含めることを推奨します。新しいサイトを追加した場合は、そのサイト用の新しい DNS サーバをグリッド全体の DNS 設定に追加します。

   > DNS サーバの IPv4 アドレスは 2~6 個指定します。ネットワーク分離が発生した場合に各サイトがローカルにアクセスできる DNS サーバを選択する必要があります。これにより、分離されたサイトは引き続き DNS サービスにアクセスできます。グリッド全体の DNS サーバリストを設定したあとに、ノードごとに DNS サーバリストをカスタマイズできます。詳細については、リカバリおよびメンテナンスの手順にある DNS 設定の変更に関する情報を参照してください。

7. 新しいサイトを追加した場合は、そのサイトから Network Time Protocol （ NTP ；ネットワークタイムプロトコル）サーバにアクセスできることを確認します。

   > 各サイトの少なくとも 2 つのノードが、少なくとも 4 つの外部 NTP ソースにアクセスできることを確認します。NTP ソースにアクセスできるノードがサイトに 1 つしかないと、そのノードがダウンした場合にタイミングの問題が生じます。また、各サイトで 2 つのノードをプライマリ NTP ソースとして指定することにより、サイトがグリッドの他の部分から分離されても、正確なタイミングが保証されます。

   詳細については、リカバリとメンテナンスの手順を参照してください。

関連情報

"ILM を使用してオブジェクトを管理する"

"ストレージノードがアクティブであることを確認しています"

"管理ノードデータベースをコピーしています"

"Prometheus指標のコピー"

"監査ログをコピーしています"

"ソフトウェアをアップグレードする"

""

ストレージノードがアクティブであることを確認しています

## 新しいストレージノードを追加する拡張処理が完了すると、 StorageGRID システムは新しいストレージノードの使用を自動的に開始します。StorageGRID システムを使用して、新しいストレージノードがアクティブになっていることを確認する必要があります。

手順

1. サポートされているブラウザを使用してGrid Managerにサインインします。
2. ノード*>*拡張ストレージノード*>*ストレージ*を選択します。
3. グラフの「 Storage Used - Object Data 」にカーソルを合わせて、オブジェクトデータに使用されている合計使用可能スペースの量である「 Used * 」の値を表示します。
4. グラフ上でカーソルを右に移動して、「使用済み」の値が増加していることを確認します。

管理ノードデータベースをコピーしています

## 拡張手順 を使用して管理ノードを追加する場合は、必要に応じてプライマリ管理ノードから新しい管理ノードにデータベースをコピーできます。データベースをコピーすると、属性、アラート、およびアラートに関する履歴情報を保持できます。

必要なもの

- 管理ノードを追加する拡張手順が完了している必要があります。
- を用意しておく必要があります `Passwords.txt` ファイル。
- プロビジョニングパスフレーズが必要です。

このタスクについて

拡張管理ノードには、 StorageGRID ソフトウェアのアクティブ化プロセスによって NMS サービス用の空のデータベースが作成されます。拡張管理ノードで NMS サービスが開始されると、システムに現在追加されているか以降に追加されたサーバとサービスに関する情報が記録されます。この管理ノードデータベースには次の情報が含まれています。

- アラートの履歴
- アラームの履歴
- ヒストリカル属性データ。* Support **>** Tools **>** Grid Topology *ページで利用可能なチャートおよびテキストレポートで使用されます

ノード間で管理ノードデータベースの整合性を確保するには、プライマリ管理ノードから拡張管理ノードにデータベースをコピーします。

> プライマリ管理ノード（ ソース管理ノード ）から拡張管理ノードへのデータベースのコピーは、完了までに数時間かかる場合があります。この間は Grid Manager にアクセスできません。

次の手順に従って、プライマリ管理ノードと拡張管理ノードの両方で MI サービスと管理 API サービスを停止してからデータベースをコピーします。

手順

1. プライマリ管理ノードで次の手順を実行します。
   a. 管理ノードにログインします。
      i. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
      ii. に記載されているパスワードを入力します `Passwords.txt` ファイル。
      iii. 次のコマンドを入力してrootに切り替えます。 `su -`
      iv. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   b. 次のコマンドを実行します。 `recover-access-points`
   c. プロビジョニングパスフレーズを入力します。
   d. MIサービスを停止します。 `service mi stop`
   e. 管理アプリケーションプログラミングインターフェイス（mgmt-api）サービスを停止します。 `service mgmt-api stop`
2. 拡張管理ノードで次の手順を実行します。
   a. 拡張管理ノードにログインします。
      i. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
      ii. に記載されているパスワードを入力します `Passwords.txt` ファイル。
      iii. 次のコマンドを入力してrootに切り替えます。 `su -`
      iv. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   b. MIサービスを停止します。 `service mi stop`
   c. mgmt-apiサービスを停止します。 `service mgmt-api stop`
   d. SSH エージェントに SSH 秘密鍵を追加します。入力するコマンド`ssh-add`
   e. に記載されているSSHアクセスパスワードを入力します `Passwords.txt` ファイル。
   f. ソース管理ノードのデータベースを拡張管理ノードにコピーします。 `/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`
   g. プロンプトが表示されたら、拡張管理ノードで MI データベースを上書きすることを確定します。

      データベースとその履歴データが拡張管理ノードにコピーされます。コピー処理が完了すると、拡張管理ノードがスクリプトによって起動されます。

   h. 他のサーバにパスワードなしでアクセスする必要がなくなった場合は、 SSH エージェントから秘密鍵を削除します。入力するコマンド`ssh-add -D`
3. プライマリ管理ノードでサービスを再起動します。 `service servermanager start`

**Prometheus**指標のコピー

新しい管理ノードを追加したら、 Prometheus で管理されている指標の履歴を必要に応じてプライマリ管理ノードから新しい管理ノードにコピーできます。指標をコピーすると、管理ノード間で指標の履歴の整合性が確保されます。

必要なもの

- 新しい管理ノードがインストールされて実行されている必要があります。
- を用意しておく必要があります `Passwords.txt` ファイル。
- プロビジョニングパスフレーズが必要です。

このタスクについて

管理ノードを追加すると、ソフトウェアのインストールプロセスによって新しい Prometheus データベースが作成されます。Prometheus データベースをプライマリ管理ノード（ *source Admin Node*） から新しい管理ノードにコピーすることで、ノード間で指標の履歴の整合性を維持できます。

> Prometheus データベースのコピーには 1 時間以上かかる場合があります。ソース管理ノードでサービスが停止している間は、グリッドマネージャの一部の機能が使用できなくなります。

手順

1. ソース管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。
2. ソース管理ノードからPrometheusサービスを停止します。 `service prometheus stop`
3. 新しい管理ノードで次の手順を実行します。
   a. 新しい管理ノードにログインします。
      i. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
      ii. に記載されているパスワードを入力します `Passwords.txt` ファイル。
      iii. 次のコマンドを入力してrootに切り替えます。 `su -`
      iv. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   b. Prometheusサービスを停止します。 `service prometheus stop`
   c. SSH エージェントに SSH 秘密鍵を追加します。入力するコマンド`ssh-add`
   d. に記載されているSSHアクセスパスワードを入力します `Passwords.txt` ファイル。
   e. ソース管理ノードのPrometheusデータベースを新しい管理ノードにコピーします。
      `/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`
   f. プロンプトが表示されたら、 * Enter * を押して、新しい管理ノード上の新しい Prometheus データベースを破棄することを確認します。

      元の Prometheus データベースとその履歴データが新しい管理ノードにコピーされます。コピー処理が完了すると、新しい管理ノードがスクリプトによって起動されます。次のステータスが表示されます。

```
Database cloned, starting services
```

a. 他のサーバにパスワードなしでアクセスする必要がなくなった場合は、 SSH エージェントから秘密鍵を削除します。入力するコマンド

```
ssh-add -D
```

4. ソース管理ノードで Prometheus サービスを再起動します。

```
service prometheus start
```

監査ログをコピーしています

## 拡張手順 を使用して新しい管理ノードを追加した場合、その AMS サービスでログに記録されるのは、システムへの追加後に発生したイベントと処理のみになります。以前にインストールされていた管理ノードから新しい拡張管理ノードに監査ログをコピーして、残りのStorageGRID システムと同期されるようにすることができます。

必要なもの

- 管理ノードを追加する拡張手順が完了している必要があります。
- を用意しておく必要があります `Passwords.txt` ファイル。

このタスクについて

他の管理ノードの監査メッセージの履歴を拡張管理ノードで使用できるようにするには、プライマリ管理ノードまたは別の既存の管理ノードから拡張管理ノードに手動で監査ログファイルをコピーする必要があります。

手順

1. プライマリ管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@_primary_Admin_Node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

      rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

2. AMSサービスを停止して新しいファイルが作成されないようにします。 `service ams stop`
3. の名前を変更します `audit.log` fileを指定します。これにより、拡張管理ノードにコピーしたファイルが上書きされません。

```
cd /var/local/audit/export [] `ls -l` []
mv audit.log new_name.txt
```

4. すべての監査ログファイルを拡張管理ノードにコピーします。

```
scp -p * IP_address:/var/local/audit/export
```

5. プロンプトが表示されたら、のパスフレーズを入力します `/root/.ssh/id_rsa`で、に表示されているプライマリ管理ノードのSSHアクセスパスワードを入力します `Passwords.txt` ファイル。

6. 元のを復元します `audit.log` ファイル：

   ```
   mv new_name.txt audit.log
   ```

7. AMS サービスを開始します。

   ```
   service ams start
   ```

8. サーバからログアウトします。

   ```
   exit
   ```

9. 拡張管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@expansion_Admin_Node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

   rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

10. 監査ログファイルのユーザとグループの設定を更新します。

    ```
    cd /var/local/audit/export [+]
    chown ams-user:bycast *
    ```

11. サーバからログアウトします。

    ```
    exit
    ```

ストレージノードの追加後におけるイレイジャーコーディングデータのリバランシング

## 場合によっては、新しいストレージノードを追加したあとにイレイジャーコーディングデータのリバランシングが必要になることがあります。

必要なもの

- 新しいストレージノードを追加する拡張手順が完了している必要があります。
- イレイジャーコーディングデータのリバランシングに関する考慮事項を確認しておく必要があります。

  "イレイジャーコーディングデータのリバランシングに関する考慮事項"

  この手順 は、サイトの 1 つ以上のストレージノードに対して * Low Object Storage * アラートがトリガーされ、推奨数の新しいストレージノードを追加できなかった場合にのみ実行してください。

- を用意しておく必要があります `Passwords.txt` ファイル。

このタスクについて

EC のリバランシング手順 が実行されている場合、 ILM 処理と S3 および Swift クライアント処理のパフォーマンスに影響する可能性があります。そのため、この手順 は限られた場合にのみ実行してください。

EC のリバランシングによって、手順 が一時的に大量のストレージをリザーブします。ストレージアラートがトリガーされる場合がありますが、リバランシングが完了すると解決します。予約に十分なストレージがない場合、 EC のリバランシング手順 は失敗します。ストレージ予約は、手順 が失敗したか成功したかに関係なく、 EC のリバランシング手順 が完了したときに解放されます。

オブジェクト（またはオブジェクトパーツ）をアップロードするために S3 および Swift API 処理を実行すると、 EC のリバランシング中に 24 時間以上かかる場合に手順 のリバランシングが失敗することがあります。該当する ILM ルールの取り込みに Strict または Balanced 配置が使用されている場合、長時間の PUT 処理は失敗します。次のエラーが報告されます。

```
500 Internal Server Error
```

手順

1. [[review_object_storage] ] リバランシングするサイトの現在のオブジェクトストレージの詳細を確認します。
   a. [ノード（ Nodes）]を選択し
   b. サイトで最初のストレージノードを選択します。
   c. [ * ストレージ * ] タブを選択します。
   d. Storage Used - Object Data チャートにカーソルを合わせて、ストレージノード上のレプリケートデータとイレイジャーコーディングデータの現在の量を表示します。
   e. 同じ手順を繰り返して、サイトの他のストレージノードを表示します。
2. プライマリ管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

      rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。
3. 次のコマンドを入力します。

   ```
   rebalance-data start --site "site-name"
   ```

   の場合 "`site-name`"`をクリックし、新しいストレージノードを追加した最初のサイトを指定します。囲みます `site-name` 引用符で囲みます。

   EC Rebalance 手順 が開始され、ジョブ ID が返されます。
4. ジョブ ID をコピーします。
5. EC Rebalance 手順 のステータスを監視します。

- 単一の EC Rebalance 手順 のステータスを表示するには、次の手順を実行します

  ```
  rebalance-data status --job-id job-id
  ```

  の場合 `_job-id_` で、手順 の起動時に返されたIDを指定します。

- 現在の EC Rebalance 手順 と、以前に完了した手順のステータスを表示するには、次の手順を実行します。

  ```
  rebalance-data status
  ```

> rebalance -dataコマンド のヘルプを表示するには、次の手順を実行します。
>
> ```
> rebalance-data --help
> ```

6. 返されたステータスに基づいて、追加の手順を実行します。
   - ステータスがの場合 `In progress`を実行している場合、ECのリバランシング処理はまだ実行中です。手順 は、完了するまで定期的に監視する必要があります。
   - ステータスがの場合 `Failure`をクリックし、を実行します 失敗の手順。
   - ステータスがの場合 `Success`をクリックし、を実行します 成功のステップ。
7. EC Rebalance 手順 によって大量の負荷が生成されている（取り込み処理に影響があるなど）場合は、手順 を一時停止します。

   ```
   rebalance-data pause --job-id job-id
   ```

8. EC のリバランシング手順 を終了する必要がある場合（ StorageGRID ソフトウェアのアップグレードを実行できるようにする場合など）は、次のように入力します。

   ```
   rebalance-data abort --job-id job-id
   ```

> EC のリバランシング手順 を終了すると、移動済みのデータフラグメントは新しい場所に残ります。データは元の場所に戻されません。

9. [[rebalance _fail]] EC rebalance手順 のステータスがの場合 `Failure`、次の手順を実行します。
   a. サイトのすべてのストレージノードがグリッドに接続されていることを確認します。
   b. これらのストレージノードに影響している可能性があるアラートがないかどうかを確認し、解決してください。

      特定のアラートの詳細については、監視とトラブルシューティングの手順を参照してください。

   c. EC Rebalance手順 ：+を再起動します
      ```
      rebalance-data start --job-id job-id
      ```
   d. ECのリバランシング手順 のステータスがまだの場合 `Failure`、テクニカルサポートにお問い合わせください。
10. [rebalance _succeed ]] EC Rebalance手順 のステータスがの場合 `Success`必要に応じて オブジェクトストレージを確認する をクリックすると、サイトの最新の詳細が表示されます。

イレイジャーコーディングされたデータをサイトのストレージノード間でより均等に配置します。

> レプリケートされたオブジェクトデータは、EC Rebalance手順 によって移動されません。

11. 複数のサイトでイレイジャーコーディングを使用している場合は、影響を受ける他のすべてのサイトに対してこの手順 を実行します。

関連情報

"イレイジャーコーディングデータのリバランシングに関する考慮事項"

"トラブルシューティングを監視します"

## テクニカルサポートにお問い合わせください

## グリッド拡張プロセスで解決できないエラーが発生した場合やグリッドタスクに失敗した場合は、テクニカルサポートにお問い合わせください。

このタスクについて

テクニカルサポートにお問い合わせいただく際は、発生したエラーのトラブルシューティングに必要なログファイルをお送りください。

手順

1. 障害が発生した拡張ノードに接続します。

   a. 次のコマンドを入力します。`ssh -p 8022 admin@grid_node_IP`

   > ポート8022はベースOSのSSHポートで、ポート22はStorageGRID を実行しているDockerコンテナのSSHポートです。

   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。

   c. 次のコマンドを入力してrootに切り替えます。 `su -`

   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

   rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

2. インストールの段階に応じて、グリッドノードから次のいずれかのログを取得します。

| プラットフォーム | ログ |
| --- | --- |
| VMware | • `/var/log/daemon.log`<br>• `/var/log/storagegrid/daemon.log`<br>• `/var/log/storagegrid/nodes/<node-name>.log` |

| プラットフォーム | ログ |
| --- | --- |
| Linux の場合 | • `/var/log/storagegrid/daemon.log`<br>• `/etc/storagegrid/nodes/<node-name>.conf` （障害が発生した各ノード）<br>• `/var/log/storagegrid/nodes/<node-name>.log` （障害が発生した各ノード、ない場合もある） |

# リカバリを維持します

ホットフィックスを適用する方法、障害が発生したグリッドノードをリカバリする方法、グリッドノードとサイトの運用を停止する方法、システム障害が発生した場合にオブジェクトをリカバリする方法について説明します。

- "StorageGRID のリカバリとメンテナンスの概要"
- "StorageGRID ホットフィックス手順"
- "グリッドノードのリカバリ手順"
- "テクニカルサポートによるサイトリカバリの実行方法"
- "手順 の運用を停止"
- "ネットワークのメンテナンス手順"
- "ホストレベルおよびミドルウェアの手順"
- "グリッドノードの手順"
- "アプライアンスノードのクローニング"

## StorageGRID のリカバリとメンテナンスの概要

StorageGRID のリカバリとメンテナンスの手順には、ソフトウェアホットフィックスの適用、グリッドノードのリカバリ、障害が発生したサイトのリカバリ、グリッドノードまたはサイト全体の運用停止、ネットワークメンテナンスの実行、ホストレベルおよびミドルウェアのメンテナンス手順の実行、グリッドノードの手順の実行が含まれます。

リカバリとメンテナンスのすべての作業には、StorageGRID システムに関する幅広い知識が必要です。StorageGRID システムのトポロジを確認して、グリッドの設定を把握しておく必要があります。

すべての指示に厳密に従い、すべての警告に注意する必要があります。

ここで説明していないメンテナンス手順は、サポートされていない手順であるか、またはサービス契約が必要

ハードウェアの手順については、使用している StorageGRID アプライアンスのインストールとメンテナンスの手順を参照してください。

「 Linux 」とは、 Red Hat ® Enterprise Linux ® 、 Ubuntu ® 、 CentOS 、または Debian ® の環境を指します。サポートされているバージョンの一覧については、 NetApp Interoperability Matrix Tool を参照してください。

関連情報

"グリッド入門"

"ネットワークガイドライン"

"StorageGRID の管理"

"SG100 SG1000サービスアプライアンス"

"SG6000 ストレージアプライアンス"

"SG5700 ストレージアプライアンス"

"SG5600 ストレージアプライアンス"

"NetApp Interoperability Matrix Tool で確認できます"

**Web** ブラウザの要件

## サポートされている Web ブラウザを使用する必要があります。

| **Web** ブラウザ | サポートされる最小バージョン |
|---|---|
| Google Chrome | 87 |
| Microsoft Edge の場合 | 87 |
| Mozilla Firefox | 84 |

ブラウザウィンドウの幅を推奨される値に設定してください。

| ブラウザの幅 | ピクセル |
|---|---|
| 最小（ Minimum ） | 1024 |
| 最適 | 1280 |

リカバリパッケージをダウンロードしています

## リカバリパッケージファイルを使用すると、障害発生時に StorageGRID システムをリストアできます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

- プロビジョニングパスフレーズが必要です。
- 特定のアクセス権限が必要です。

StorageGRID システムでグリッドトポロジの変更を行う前、またはソフトウェアをアップグレードする前に、現在のリカバリパッケージファイルをダウンロードしてください。グリッドトポロジを変更するかソフトウェアをアップグレードしたあとに、リカバリパッケージの新しいコピーをダウンロードします。

手順

1. [* Maintenance * （メンテナンス） ] > [* System * （システム * ） ] > [* Recovery Package] （リカバリパッケージ * ）
2. プロビジョニングパスフレーズを入力し、 * ダウンロードの開始 * を選択します。

   ダウンロードがすぐに開始されます。

3. ダウンロードが完了したら、次の手順を実行
   a. を開きます `.zip` ファイル。
   b. これには、gpt-backupディレクトリと内部が含まれていることを確認します `.zip` ファイル。
   c. 内側を引き出します `.zip` ファイル。
   d. を開くことができることを確認します `Passwords.txt` ファイル。
4. ダウンロードしたリカバリパッケージファイルをコピーします (`.zip`)を2箇所に安全に、安全に、そして別 々 の場所に移動します。

> リカバリパッケージファイルには StorageGRID システムからデータを取得するための暗号キーとパスワードが含まれているため、安全に保管する必要があります。

関連情報

"StorageGRID の管理"

## StorageGRID ホットフィックス手順

### ソフトウェアの問題が検出され、次の機能リリースの前に解決された場合は、StorageGRID システムへのホットフィックスの適用が必要になる場合があります。

StorageGRID のホットフィックスには、フィーチャーパックまたはフィーチャーパックに含まれないソフトウェアの変更が含まれます。今後のリリースにも同じ変更が含まれます。さらに、各ホットフィックスリリースには、その機能またはパッチリリースに含まれる以前のすべてのホットフィックスがまとめて含まれています。

- "ホットフィックスの適用に関する考慮事項"
- "ホットフィックス適用時のシステムへの影響"
- "ホットフィックスに必要な項目の確認"
- "ホットフィックスファイルをダウンロードしています"
- "ホットフィックス適用前のシステムの状態の確認"
- "ホットフィックスの適用"

# ホットフィックスを適用すると、 StorageGRID システム内のノードにソフトウェア更新が累積的に適用されます。

別のメンテナンス手順 の実行中は、 StorageGRID ホットフィックスを適用できません。たとえば、運用停止、拡張、またはリカバリ用の手順 の実行中は、ホットフィックスを適用できません。

> ノードまたはサイトの運用停止手順 が一時停止されている場合、ホットフィックスを安全に適用できます。また、 StorageGRID アップグレード手順 の最終段階でホットフィックスを適用できる場合があります。詳細については、 StorageGRID ソフトウェアのアップグレード手順を参照してください。

Grid Manager でホットフィックスをアップロードすると、ホットフィックスはプライマリ管理ノードに自動的に適用されます。その後、 StorageGRID システム内の残りのノードへのホットフィックスの適用を承認できます。

1 つ以上のノードへのホットフィックスの適用に失敗した場合は、ホットフィックスの進捗状況テーブルの Details 列に障害の理由が表示されます。エラーの原因となった問題を解決してから、プロセス全体を再試行する必要があります。ホットフィックスの適用に成功していたノードは、以降のアプリケーションではスキップされます。必要に応じて、すべてのノードが更新されるまで、ホットフィックスの適用を何度でも安全に再試行できます。アプリケーションを完了するには、すべてのグリッドノードにホットフィックスが正常にインストールされている必要があります。

新しいバージョンのホットフィックスによってグリッドノードが更新されますが、ホットフィックスの実際の変更内容が、特定のタイプのノードの特定のサービスにしか影響しない場合があります。たとえば、あるホットフィックスが、ストレージノード上の LDR サービスにしか影響しない場合があります。

## リカバリと拡張のためのホットフィックスの適用方法

ホットフィックスがグリッドに適用されると、プライマリ管理ノードは、リカバリ処理でリストアされたすべてのノード、または拡張時に追加されたすべてのノードに、同じバージョンのホットフィックスを自動的にインストールします。

ただし、プライマリ管理ノードのリカバリが必要な場合は、適切な StorageGRID リリースを手動でインストールしてからホットフィックスを適用する必要があります。プライマリ管理ノードの最終 StorageGRID バージョンがグリッド内の他のノードと同じである必要があります。

次の例は、プライマリ管理ノードをリカバリする際にホットフィックスを適用する方法を示しています。

1. グリッドで StorageGRID 11.*A.B_VERSION* が実行されており、最新のホットフィックスが適用されているとします。「 *Grid* バージョン」は *11._A.B.C.* です。
2. プライマリ管理ノードに障害が発生した場合。
3. プライマリ管理ノードを StorageGRID 11.*A.B_* を使用して再導入し、リカバリ手順 を実行します。

   > グリッドのバージョンに応じて、ノードの導入時にマイナーリリースを使用できます。メジャーリリースを最初に導入する必要はありません。

4. 次に、プライマリ管理ノードにホットフィックス 11.*A.B.C.* を適用します。

## 関連情報

"交換用プライマリ管理ノードの設定"

ホットフィックス適用時のシステムへの影響

# ホットフィックスを適用したときに、 StorageGRID システムにどのような影響が生じるのかを理解しておく必要があります。

クライアントアプリケーションが短時間中断される可能性があります

StorageGRID システムは、ホットフィックス適用プロセス中もクライアントアプリケーションからデータを取り込み、読み出すことができますが、ホットフィックスが個々のゲートウェイノードまたはストレージノードのサービスを再開する必要がある場合は、それらのノードへのクライアント接続が一時的に中断されることがあります。接続はホットフィックスの適用終了後に再開され、個々のノードのサービスも再開されます。

接続の中断が短時間でも許容されない場合は、ホットフィックス適用時のダウンタイムをスケジュールする必要があります。特定のノードが更新されるタイミングをスケジュールするには、選択的な承認を使用できます。

> 複数のゲートウェイとハイアベイラビリティ（ HA ）グループを使用すると、ホットフィックス適用プロセス中に自動フェイルオーバーを実行できます。ハイアベイラビリティグループを設定するには、StorageGRID の管理手順を参照してください。

アラートおよび **SNMP** 通知がトリガーされる可能性があります

サービスが再起動されたとき、および StorageGRID システムを複数バージョンが混在した環境で使用している場合（一部のグリッドノードで以前のバージョンを実行し、その他のノードはより新しいバージョンにアップグレードしている場合）には、アラートと SNMP 通知がトリガーされることがあります。通常、これらのアラートと通知はホットフィックスが完了するとクリアされます。

設定の変更は制限されています

StorageGRID にホットフィックスを適用する際は、次の点に注意

- ホットフィックスがすべてのノードに適用されるまでは、グリッドの設定を変更しないでください（グリッドネットワークのサブネットの指定や保留中のグリッドノードの承認など）。
- ホットフィックスがすべてのノードに適用されるまで、 ILM 設定は更新しないでください。

ホットフィックスに必要な項目の確認

# ホットフィックスを適用する前に、必要な項目をすべて用意する必要があります。

| 項目 | 注： |
| --- | --- |
| StorageGRID ホットフィックスファイル | StorageGRID ホットフィックスファイルをダウンロードする必要があります。 |

| 項目 | 注： |
| --- | --- |
| • ネットワークポート<br>• サポートされている Web ブラウザ<br>• SSH クライアント（ PuTTY など） | 「Webブラウザの要件」を参照してください。 |
| リカバリパッケージ (.zip)ファイル | ホットフィックスを適用する前に、ホットフィックスの適用中に問題が発生した場合に最新のリカバリパッケージファイルをダウンロードします。その後、ホットフィックスの適用後に、リカバリパッケージファイルの新しいコピーをダウンロードして安全な場所に保存します。更新されたリカバリパッケージファイルは、障害発生時のシステムのリストアに使用できます。 |
| Passwords.txt ファイル | 任意。 SSH クライアントを使用してホットフィックスを手動で適用する場合にのみ使用します。。 `Passwords.txt` ファイルは、リカバリパッケージに含まれるSAIDパッケージに含まれています `.zip` ファイル。 |
| プロビジョニングパスフレーズ | このパスフレーズは、 StorageGRID システムが最初にインストールされるときに作成されて文書化されます。プロビジョニングパスフレーズは、に表示されません `Passwords.txt` ファイル。 |
| 関連ドキュメント | `readme.txt` ホットフィックスのファイル。このファイルは、ホットフィックスのダウンロードページにあります。必ずを確認してください `readme` ホットフィックスを適用する前にファイルを慎重に作成してください |

関連情報

"ホットフィックスファイルをダウンロードしています"

"リカバリパッケージをダウンロードしています"

ホットフィックスファイルをダウンロードしています

## ホットフィックスを適用する前に、ホットフィックスファイルをダウンロードする必要があります。

手順

1. ネットアップの StorageGRID ダウンロードページにアクセスします。

   "ネットアップのダウンロード： StorageGRID"

2. [ 利用可能なソフトウェア ] の下にある下矢印をクリックすると、ダウンロード可能なホットフィックスのリストが表示されます。

ホットフィックスファイルのバージョンの形式は 11.4_.x.y__ です。

3. 更新に含まれている変更を確認します。

プライマリ管理ノードをリカバリした直後でホットフィックスを適用する必要がある場合は、他のグリッドノードにインストールされているものと同じバージョンのホットフィックスを選択します。

a. ダウンロードするホットフィックスのバージョンを選択し、 * Go * を選択します。
b. ネットアップアカウントのユーザ名とパスワードを使用してサインインします。
c. エンドユーザライセンス契約を読んで同意します。

選択したバージョンのダウンロードページが表示されます。

d. ホットフィックスをダウンロードします `readme.txt` ファイルをクリックして、ホットフィックスに含まれる変更の概要を確認します。

4. ホットフィックスのダウンロードボタンを選択してファイルを保存します。

このファイルの名前は変更しないでください。

macOSデバイスを使用している場合、ホットフィックスファイルは自動的にとして保存されます `.txt` ファイル。その場合は、を使用せずにファイルの名前を変更する必要があります `.txt` 内線番号。

5. ダウンロードする場所を選択し、「 * 保存 * 」を選択します。

関連情報

"交換用プライマリ管理ノードの設定"

ホットフィックスを適用する前に、システムの状態を確認します

## システムにホットフィックスを適用する準備ができていることを確認する必要があります。

1. サポートされているブラウザを使用してGrid Managerにサインインします。
2. 可能であれば、システムが正常に稼働し、すべてのグリッドノードがグリッドに接続されていることを確認します。

接続されているノードには緑のチェックマークが付いて をクリックします。

3. 可能であれば、現在のアラートがないかを確認し、ある場合は解決します。

特定のアラートの詳細については、 StorageGRID の監視とトラブルシューティングの手順を参照してください。

4. 手順 のアップグレード、リカバリ、拡張、運用停止など、他のメンテナンス手順が実行中でないことを確認します。

アクティブなメンテナンス手順が完了してからホットフィックスを適用してください。

別のメンテナンス手順 の実行中は、 StorageGRID ホットフィックスを適用できません。たとえば、運用停止、拡張、またはリカバリ用の手順 の実行中は、ホットフィックスを適用できません。

ノードまたはサイトの運用停止手順 が一時停止されている場合、ホットフィックスを安全に適用できます。また、 StorageGRID アップグレード手順 の最終段階でホットフィックスを適用できる場合があります。詳細については、 StorageGRID ソフトウェアのアップグレード手順を参照してください。

関連情報

"トラブルシューティングを監視します"

"ストレージノードの運用停止プロセスの一時停止と再開"

ホットフィックスの適用

ホットフィックスは、最初にプライマリ管理ノードに自動的に適用されます。その後、すべてのノードが同じバージョンのソフトウェアを実行するまでの間、他のグリッドノードへのホットフィックスの適用を承認する必要があります。個々のグリッドノード、グリッドノードのグループ、またはすべてのグリッドノードを選択して、承認順序をカスタマイズできます。

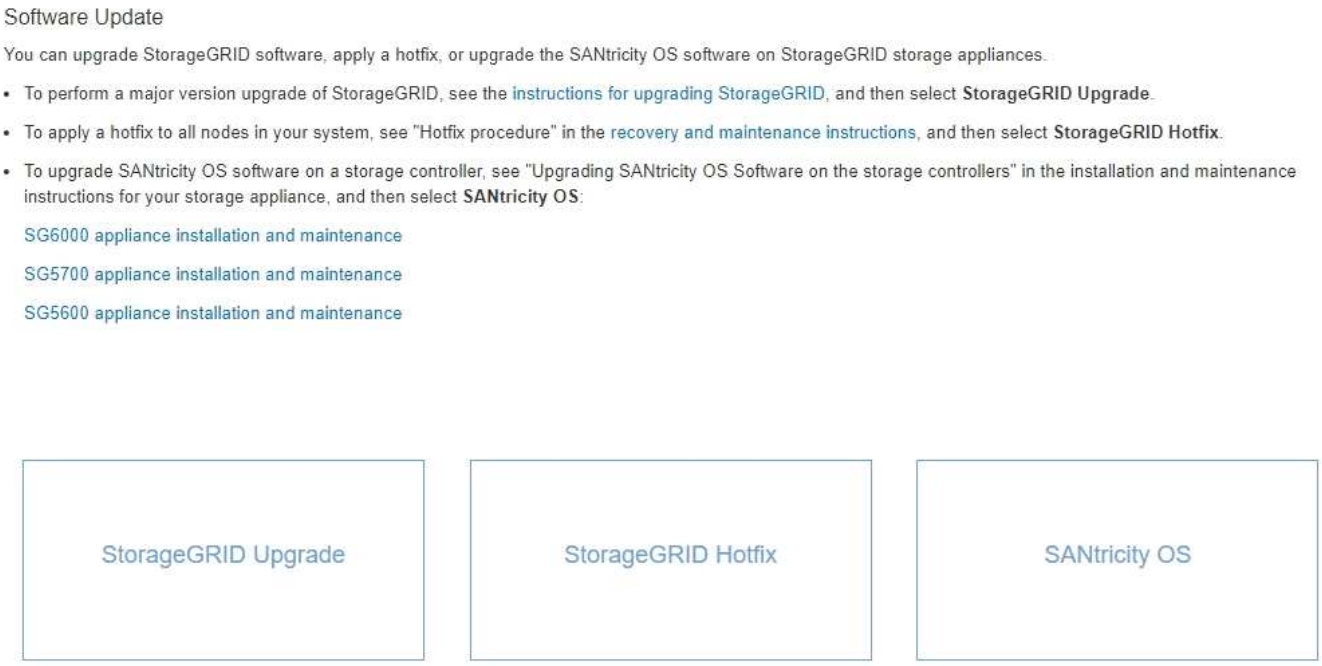
必要なもの

- 「ホットフィックスの計画と準備」のすべての考慮事項を確認し、すべての手順を完了しました。
- プロビジョニングパスフレーズが必要です。
- Root Access権限またはMaintenance権限が必要です。
- ホットフィックスのノードへの適用は遅延できますが、ホットフィックスの適用はすべてのノードにホットフィックスを適用するまで完了しません。
- ホットフィックスのプロセスが完了するまでは、 StorageGRID ソフトウェアのアップグレードまたは SANtricity OS のアップグレードを実行できません。

手順

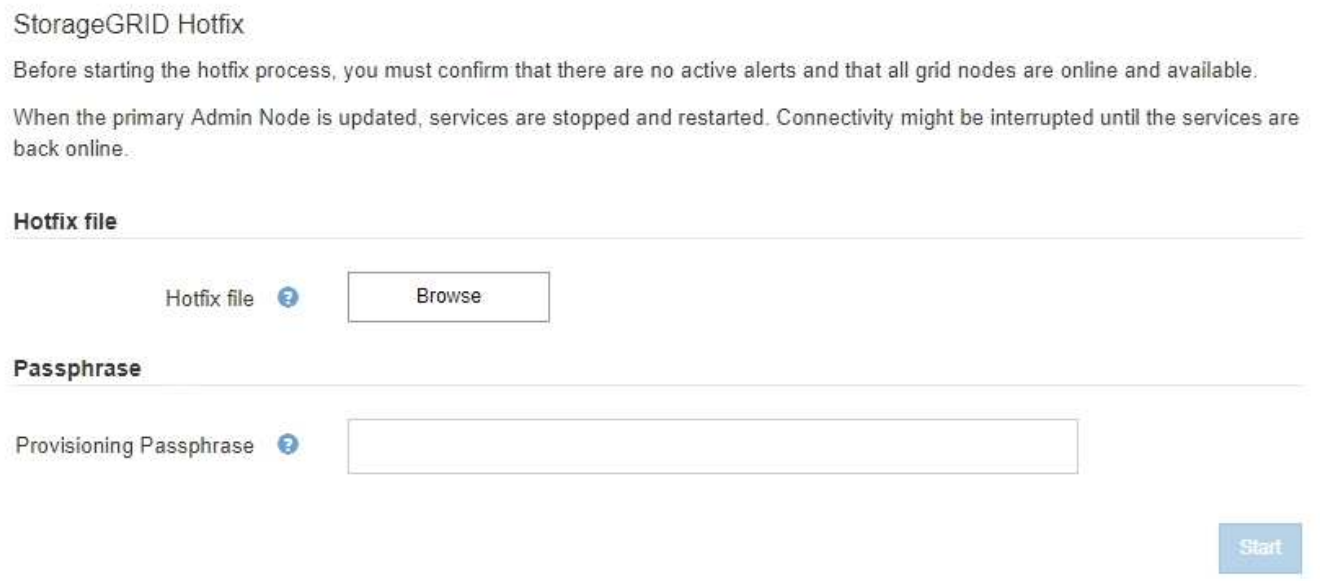
1. サポートされているブラウザを使用してGrid Managerにサインインします。
2. [* Maintenance * （メンテナンス） ] > [* System * （ * システム * ） ] > [* Software Update * （ソフトウェア・アップデート

   Software Update ページが表示されます。




3. StorageGRID Hotfix *を選択します。

   StorageGRID Hotfix ページが表示されます。




4. NetApp Support Siteからダウンロードしたホットフィックスファイルを選択します。

   a. [ * 参照 * ] を選択します。
   b. ファイルを探して選択します。

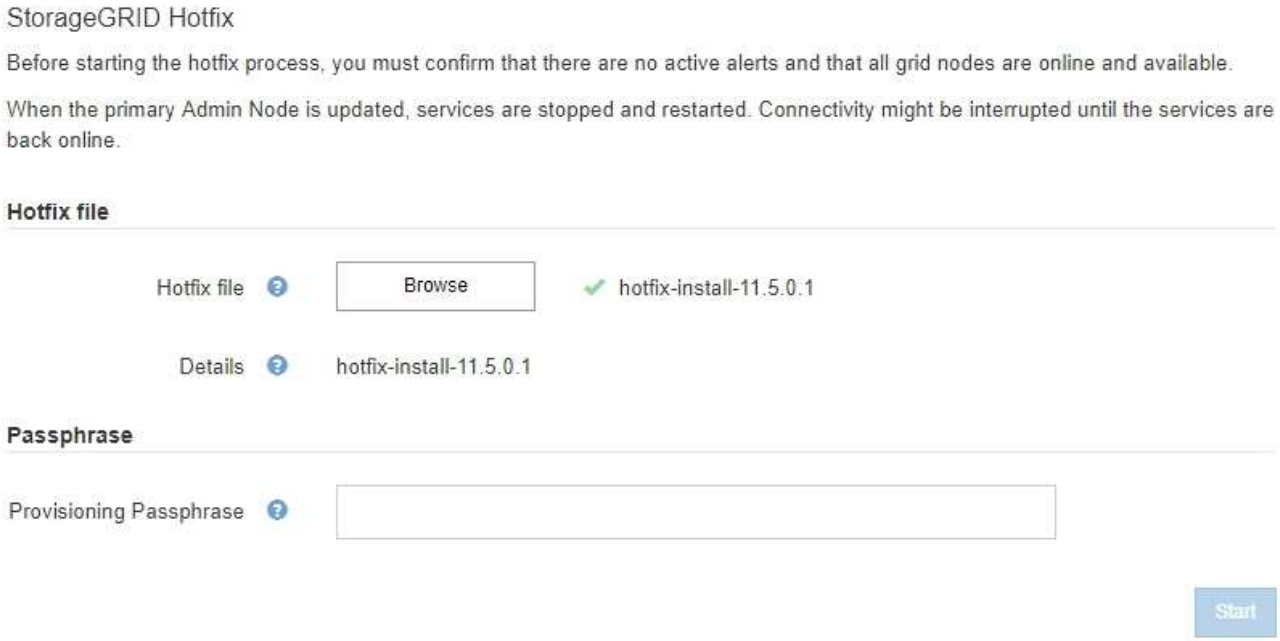
      `hotfix-install-version`

   c. 「 * 開く * 」を選択します。

      ファイルがアップロードされます。アップロードが完了すると、ファイル名が [ 詳細 ] フィールドに表

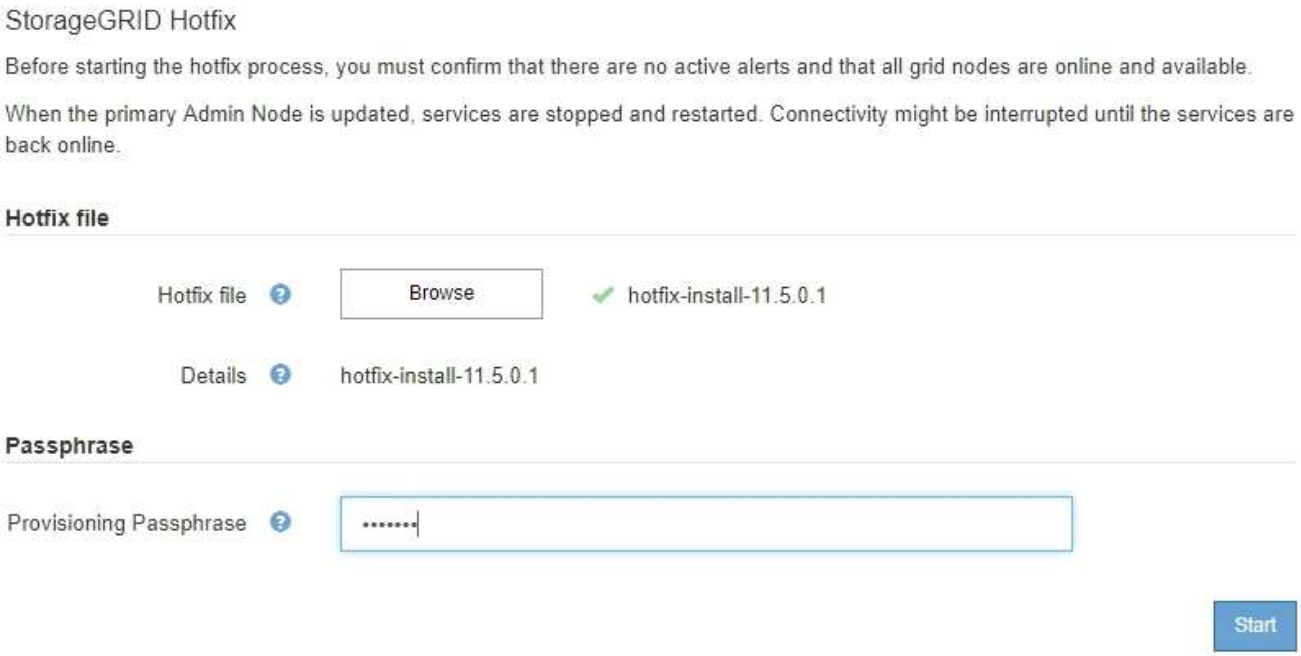
示されます。

ファイル名は検証プロセスで指定されるため変更しないでください。



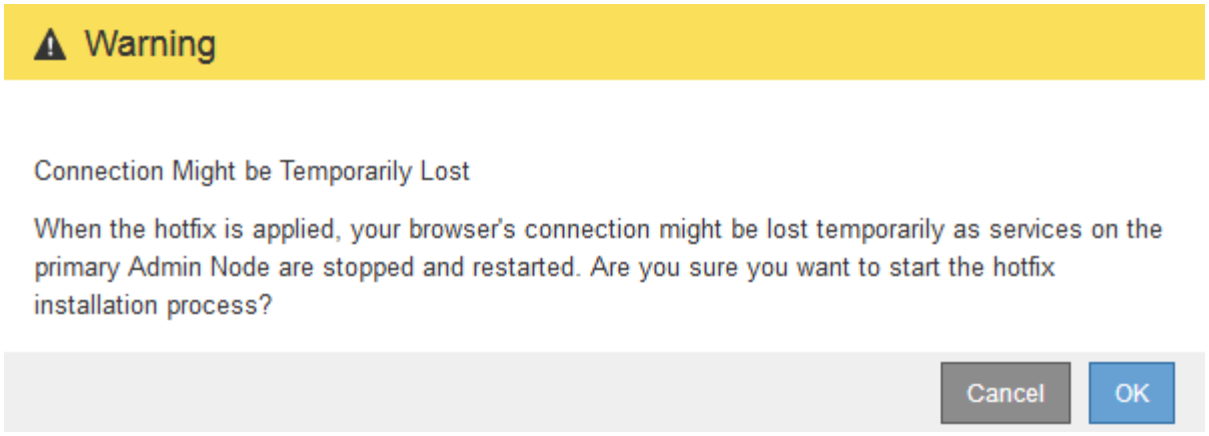

5. プロビジョニングパスフレーズをテキストボックスに入力します。

「 * Start * （スタート * ）」ボタンが有効になります。




6. 「 * Start （開始）」を選択します

プライマリ管理ノードのサービスを再起動する際にブラウザの接続が一時的に失われる可能性があることを示す警告が表示されます。




7. [OK] を選択して、プライマリ管理ノードへのホットフィックスの適用を開始します。

   ホットフィックスの適用が開始されると、次

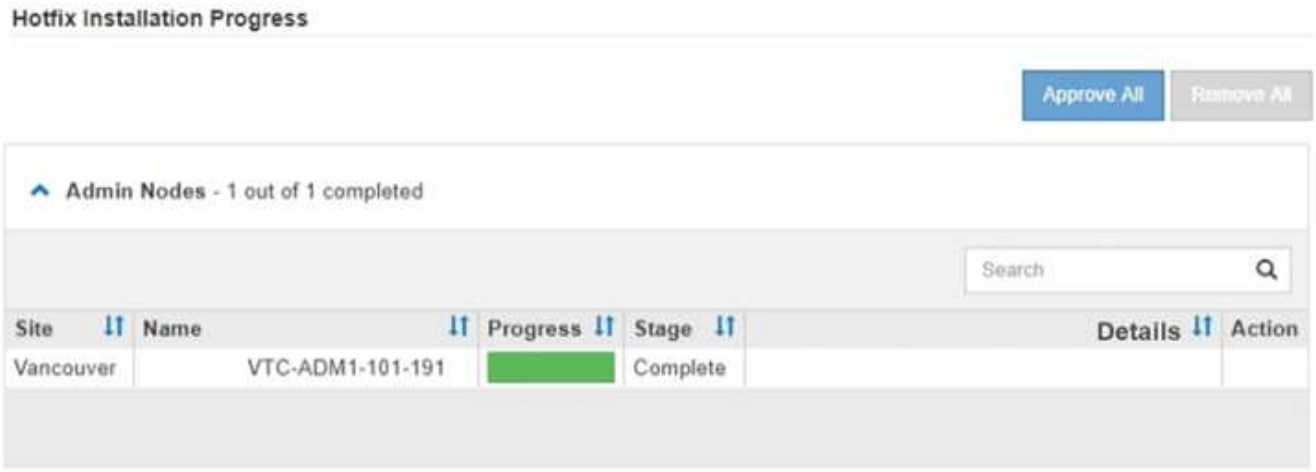
   a. ホットフィックスの検証が実行されます。

      エラーが報告された場合は解決し、ホットフィックスファイルを再アップロードして、 * Start * を再度選択します。

   b. ホットフィックスのインストールの進行状況の表が表示されます。この表には、グリッド内のすべてのノードと、ホットフィックスのインストールの現在のステージがノードごとに表示されます。テーブル内のノードはタイプ別にグループ化されています。

      - 管理ノード
      - ゲートウェイノード
      - ストレージノード
      - アーカイブノード

      進捗バーが完了すると ' プライマリ管理ノードが最初に表示され ' ステージが「 complete 」になります




8. 必要に応じて、各グループ内のノードのリストを * Site * 、 * Name * 、 * Progress * 、 * Stage * 、また

は * Details * で昇順または降順にソートします。または、 * 検索 * ボックスに用語を入力して特定のノードを検索します。

9. 更新する準備ができたグリッドノードを承認します。同じタイプの承認済みノードが一度に 1 つずつアップグレードされます。

   ノードのホットフィックスは、更新の準備ができていることを確認しないかぎり、承認しないでください。ホットフィックスがグリッドノードに適用されると、そのノード上の一部のサービスが再起動される場合があります。このような処理を実行すると、ノードと通信しているクライアントで原因 サービスが中断する可能性があります。

   - 1 つまたは複数の * 承認 * ボタンを選択して、 1 つまたは複数のノードをホットフィックスキューに追加します。
   - 各グループ内の * すべて承認 * ボタンを選択して、同じタイプのすべてのノードをホットフィックスキューに追加します。[ * 検索 * （ * Search * ） ] ボックスに検索条件を入力した場合は、 [ すべて承認（ Approve All * ） ] ボタンをクリックすると、検索条件で選択したすべてのノードが環境 されます。

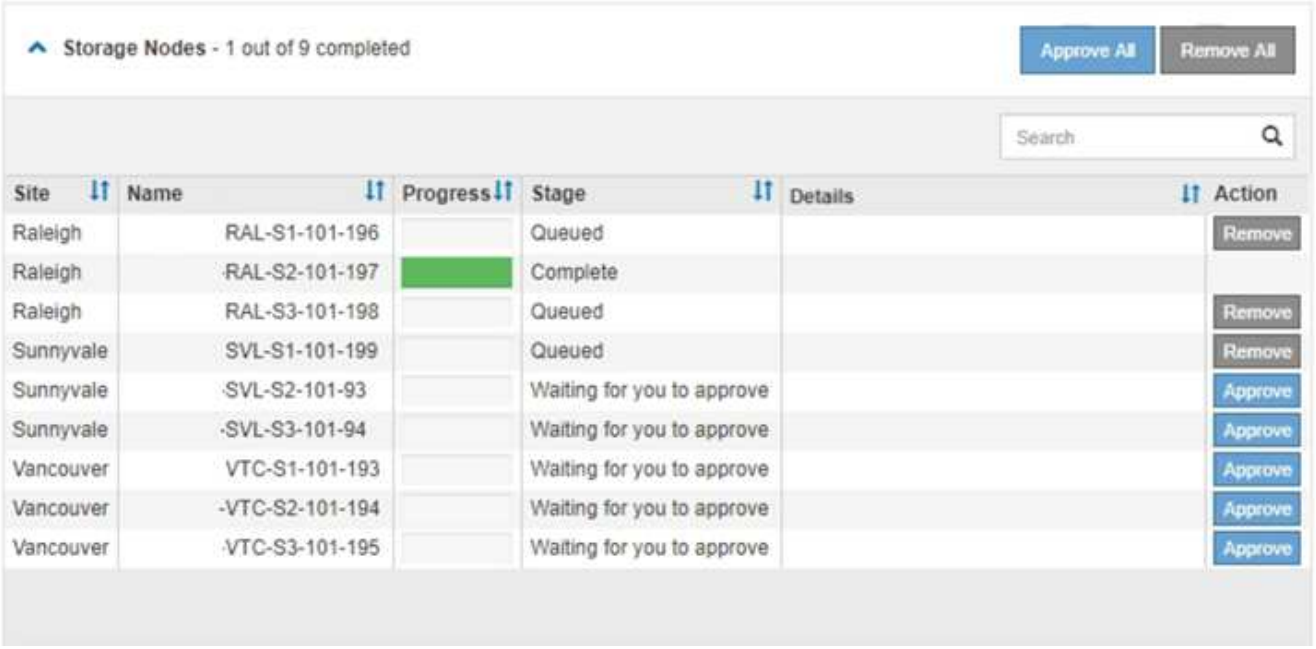
     ページ上部の * すべて承認 * ボタンをクリックすると、ページにリストされているすべてのノードが承認されます。一方、テーブルグループの上部にある * すべて承認 * ボタンをクリックすると、そのグループ内のすべてのノードのみが承認されます。ノードのアップグレード順序が重要な場合は、ノードまたはノードグループを 1 つずつ承認し、各ノードでアップグレードが完了するまで待ってから、次のノードを承認します。

   - ページ上部の最上位レベルの * すべて承認 * ボタンを選択して、グリッド内のすべてのノードをホットフィックスキューに追加します。

     別のソフトウェア更新を開始する前に、 StorageGRID ホットフィックスを完了する必要があります。ホットフィックスを完了できない場合は、テクニカルサポートにお問い合わせください。

10. ホットフィックスキューからノードまたはすべてのノードを削除する必要がある場合は、「* Remove 」または「 Remove All *」を選択します。

    例に示すように、ステージが「Queued」より先に進むと、「* Remove *」ボタンが非表示になり、ホットフィックスの処理からノードを削除できなくなります。




11. 承認された各グリッドノードにホットフィックスが適用されるまで待ちます。

    ホットフィックスがすべてのノードに正常にインストールされると、ホットフィックスのインストールの進捗状況の表が閉じます。緑のバナーは、ホットフィックスが完了した日時を示します。

12. ホットフィックスをどのノードにも適用できなかった場合は、各ノードのエラーを確認し、問題 を解決してから、上記の手順を繰り返します。

    手順 は、ホットフィックスがすべてのノードに正常に適用されるまで完了しません。必要に応じて、完了するまでホットフィックスの適用を何度でも安全に再試行できます。

関連情報

"ホットフィックス適用の計画と準備"

"StorageGRID の管理"

"トラブルシューティングを監視します"

## グリッドノードのリカバリ手順

### グリッドノードで障害が発生した場合は、障害が発生した物理または仮想サーバを交換し、 StorageGRID ソフトウェアを再インストールし、リカバリ可能なデータをリストアすることでリカバリできます。

グリッドノードの障害は、ハードウェア、仮想化、オペレーティングシステム、またはソフトウェアの障害によってそのノードが動作しなくなったり、信頼性が低下した場合に発生することがあります。グリッドノードのリカバリが必要になる障害には、さまざまな種類があります。

グリッドノードのリカバリ手順は、グリッドノードがホストされているプラットフォームと、そのグリッドノードのタイプによって異なります。グリッドノードのタイプごとに、厳密に従う必要があるリカバリ手順 があります。

通常は、障害グリッドノードのデータをできるだけ保持し、障害ノードを修理または交換し、 Grid Manager を使用して交換用ノードを設定し、ノードのデータをリストアします。

> StorageGRID サイト全体で障害が発生した場合は、テクニカルサポートにお問い合わせください。テクニカル・サポートは ' お客様と協力して ' リカバリされるデータ量を最大化し ' ビジネス目標を達成するためのサイト・リカバリ・プランを作成し ' 実行します

関連情報

"テクニカルサポートによるサイトリカバリの実行方法"

### グリッドノードのリカバリに関する警告と考慮事項

## グリッドノードに障害が発生した場合は、できるだけ早くリカバリする必要があります。ノードのリカバリを開始する前に、ノードのリカバリに関する警告と考慮事項をすべて確認しておく必要があります。

> StorageGRID は、複数のノードが相互に連携する分散システムです。グリッドノードのリストアにディスクの Snapshot を使用しないでください。各タイプのノードのリカバリとメンテナンスの手順を参照してください。

障害グリッドノードをできるだけ早くリカバリする理由には、次のものがあります。

- グリッドノードで障害が発生すると、システムデータとオブジェクトデータの冗長性が低下して、別のノードで障害が発生した場合にデータが永続的に失われるリスクが高まります。
- グリッドノードに障害が発生すると、日常処理の効率が低下する可能性があります。
- グリッドノードで障害が発生すると、システム処理の監視を減らすことができます。
- 厳格な ILM ルールが適用されている場合、障害が発生したグリッドノードで原因 500 Internal Server エラーが発生する可能性があります。
- グリッドノードがすぐにリカバリされないと、リカバリ時間が長くなる可能性があります。たとえば、リカバリが完了する前にキューをクリアする必要が生じる場合があります。

リカバリするグリッドノードのタイプに応じて、必ずリカバリ手順 に従ってください。リカバリ手順は、プライマリまたは非プライマリ管理ノード、ゲートウェイノード、アーカイブノード、アプライアンスノード、ストレージノードのそれぞれで異なります。

### グリッドノードをリカバリするための前提条件

グリッドノードをリカバリする際の前提条件は次のとおりです。

- 障害が発生した物理または仮想ハードウェアの交換と設定が完了している。
- 交換用アプライアンスの StorageGRID アプライアンスインストーラのバージョンは、ハードウェアの設置とメンテナンスで説明している StorageGRID アプライアンスインストーラのバージョンを確認およびアップグレードするための StorageGRID システムのソフトウェアのバージョンと一致します。
  - "SG100 SG1000サービスアプライアンス"
  - "SG5600 ストレージアプライアンス"
  - "SG5700 ストレージアプライアンス"

- "SG6000 ストレージアプライアンス"

- プライマリ管理ノード以外のグリッドノードをリカバリする場合は、リカバリするグリッドノードとプライマリ管理ノードが接続されています。

複数のグリッドノードをホストしているサーバで障害が発生した場合のノードリカバリの順序

複数のグリッドノードをホストしているサーバで障害が発生した場合、ノードは任意の順序でリカバリできます。ただし、障害サーバがプライマリ管理ノードをホストしている場合は、最初にそのノードをリカバリする必要があります。プライマリ管理ノードを最初にリカバリすると、プライマリ管理ノードへの接続を待機するために他のノードのリカバリが停止するのを防ぐことができます。

リカバリしたノードの **IP** アドレス

現在ほかのノードに割り当てられている IP アドレスを使用してノードをリカバリしないでください。新しいノードを導入するときは、障害が発生したノードの現在の IP アドレスまたは未使用の IP アドレスを使用します。

グリッドノードリカバリに必要な項目の収集

メンテナンス手順を実行する前に、障害グリッドノードのリカバリに必要な情報、ファイル、機器などが揃っていることを確認する必要があります。

| 項目 | 注： |
| --- | --- |
| StorageGRID インストールアーカイブ | グリッドノードをリカバリする必要がある場合は、使用しているプラットフォーム用のStorageGRID インストールアーカイブが必要です。<br><br>• 注： * ストレージノード上の障害ストレージボリュームをリカバリする場合、ファイルをダウンロードする必要はありません。 |
| リカバリパッケージ `.zip` ファイル。 | 最新のリカバリパッケージのコピーを取得します `.zip` ファイル： `sgws-recovery-package-id-revision.zip`<br><br>の内容 `.zip` ファイルは、システムが変更されるたびに更新されます。そのような変更を行うと、最新バージョンのリカバリパッケージを安全な場所に保管するよう求められます。グリッド障害からリカバリするには、最新のコピーを使用します。<br><br>プライマリ管理ノードが正常に動作している場合は、 Grid Manager からリカバリパッケージをダウンロードできます。[Maintenance * System * Recovery Package]を選択します。<br><br>Grid Manager にアクセスできない場合は、 ADC サービスが含まれる一部のストレージノードにリカバリパッケージの暗号化コピーがあります。各ストレージノードで、リカバリパッケージが格納された場所を確認します。 `/var/local/install/sgws-recovery-package-grid-id-revision.zip.gpg` リビジョン番号が最も大きいリカバリパッケージを使用してください。 |

| 項目 | 注： |
| --- | --- |
| `Passwords.txt` ファイル。 | コマンドラインでグリッドノードにアクセスするために必要なパスワードが含まれています。リカバリパッケージに含まれています。 |
| プロビジョニングパスフレーズ | このパスフレーズは、 StorageGRID システムが最初にインストールされるときに作成されて文書化されます。プロビジョニングパスフレーズはに含まれていません `Passwords.txt` ファイル。 |
| ご使用のプラットフォームの最新ドキュメント | 現在サポートされているプラットフォームのバージョンについては、Interoperability Matrix Toolを参照してください。<br><br>"NetApp Interoperability Matrix Tool で確認できます"<br><br>ドキュメントについては、プラットフォームのベンダーの Web サイトを参照してください。 |

関連情報

"StorageGRID インストールファイルのダウンロードと展開"

"Web ブラウザの要件"

**StorageGRID** インストールファイルのダウンロードと展開

## StorageGRID グリッドノードをリカバリする前に、ソフトウェアをダウンロードしてファイルを展開する必要があります。

グリッドで現在実行されているバージョンの StorageGRID を使用する必要があります。

手順

1. 現在インストールされているソフトウェアのバージョンを確認します。Grid Managerから*ヘルプ*バージョン情報*へ進んでください。
2. ネットアップの StorageGRID ダウンロードページにアクセスします。

   "ネットアップのダウンロード： StorageGRID"

3. グリッドで現在実行されている StorageGRID のバージョンを選択します。

   StorageGRID ソフトウェアのバージョンの形式は、 11.x.y です

4. ネットアップアカウントのユーザ名とパスワードを使用してサインインします。
5. エンドユーザライセンス契約を読み、チェックボックスをオンにして、「 * 同意して続行 * 」を選択します。
6. ダウンロードページの「* Install StorageGRID *」列で、を選択します `.tgz` または `.zip` ご使用のプラットフォームに対応するファイルです。

   インストールアーカイブファイルに表示されるバージョンは、現在インストールされているソフトウェアのバージョンと一致している必要があります。

を使用します `.zip` ファイル（File）Windowsを実行している場合。

| プラットフォーム | インストールアーカイブ |
| --- | --- |
| VMware | StorageGRID-Webscale-*version*-VMware-*uniqueID*.zip<br>StorageGRIDWebscale—vmware-uniqueID_tgz |
| Red Hat Enterprise Linux または CentOS | StorageGRID-Webscale-*version*-RPM-*uniqueID*.zip<br>StorageGRIDWebscale--*version*-rpm_uniqueID_tgz |
| Ubuntu または Debian<br><br>またはアプライアンス | StorageGRID-Webscale-*version*-DEB-*uniqueID*.zip<br>StorageGRIDWebscale--*version*-bDEB --_uniqueID_tgz |
| OpenStackまたはその他のハイパーバイザー | リカバリ処理を対象とした OpenStack 用の仮想マシンディスクファイルおよびスクリプトは、現在は提供されていません。OpenStack 環境で実行されているノードのリカバリが必要な場合は、使用している Linux オペレーティングシステム用のファイルをダウンロードしてください。その後、手順 に従って Linux ノードを交換します。 |

7. アーカイブファイルをダウンロードして展開します。
8. プラットフォームに応じた手順に従って、プラットフォームとリカバリが必要なグリッドノードに基づいて必要なファイルを選択します。

   各プラットフォームの手順に記載されているパスは、アーカイブファイルによってインストールされた最上位ディレクトリに対する相対パスです。

9. VMwareシステムをリカバリする場合は、適切なファイルを選択します。

| パスとファイル名 | 説明 |
| --- | --- |
| | StorageGRID ダウンロードファイルに含まれているすべてのファイルについて説明するテキストファイル。 |
| | 製品サポートのない無償ライセンス。 |
| | グリッドノード仮想マシンを作成するためのテンプレートとして使用される仮想マシンディスクファイル。 |
| | Open Virtualization Formatテンプレートファイル (`.ovf`)とマニフェストファイル (`.mf`）を使用してください。 |
| | テンプレートファイル (`.ovf`)とマニフェストファイル (`.mf`）。非プライマリ管理ノードを導入する場合に使用します。 |

| パスとファイル名 | 説明 |
| --- | --- |
| /vsphere/vsphere-archive.ovf ./vsphere-archive.mf | テンプレートファイル (.ovf)とマニフェストファイル (.mf）を使用してアーカイブノードを導入します。 |
|  | テンプレートファイル (.ovf)とマニフェストファイル (.mf）を選択します。 |
|  | テンプレートファイル (.ovf)とマニフェストファイル (.mf）を選択します。 |
| 導入スクリプトツール | 説明 |
|  | 仮想グリッドノードの導入を自動化するための Bash シェルスクリプト。 |
|  | で使用するサンプル構成ファイル `deploy-vsphere-ovftool.sh` スクリプト： |
|  | StorageGRID システムの設定を自動化するための Python スクリプト。 |
|  | StorageGRID アプライアンスの設定を自動化するための Python スクリプト。 |
|  | シングルサインオンが有効な場合にグリッド管理 API にサインインするために使用できる Python スクリプトの例。 |
|  | で使用するサンプル構成ファイル `configure-storagegrid.py` スクリプト： |
|  | で使用する空の構成ファイル `configure-storagegrid.py` スクリプト： |

10. Red Hat Enterprise LinuxまたはCentOSのシステムをリカバリする場合は、該当するファイルを選択します。

| パスとファイル名 | 説明 |
| --- | --- |
|  | StorageGRID ダウンロードファイルに含まれているすべてのファイルについて説明するテキストファイル。 |
|  | 製品サポートのない無償ライセンス。 |

| パスとファイル名 | 説明 |
| --- | --- |
| | RHEL ホストまたは CentOS ホストに StorageGRID ノードイメージをインストールするための RPM パッケージ。 |
| | RHEL ホストまたは CentOS ホストに StorageGRID ホストサービスをインストールするための RPM パッケージ。 |
| 導入スクリプトツール | 説明 |
| | StorageGRID システムの設定を自動化するための Python スクリプト。 |
| | StorageGRID アプライアンスの設定を自動化するための Python スクリプト。 |
| | で使用するサンプル構成ファイル `configure-storagegrid.py` スクリプト： |
| | シングルサインオンが有効な場合にグリッド管理 API にサインインするために使用できる Python スクリプトの例。 |
| | で使用する空の構成ファイル `configure-storagegrid.py` スクリプト： |
| | StorageGRID コンテナ導入用の RHEL ホストまたは CentOS ホストを設定するためのサンプルの Ansible のロールとプレイブック。必要に応じて、ロールまたはプレイブックをカスタマイズできます。 |

11. UbuntuまたはDebianシステムをリカバリする場合は、適切なファイルを選択します。

| パスとファイル名 | 説明 |
| --- | --- |
| | StorageGRID ダウンロードファイルに含まれているすべてのファイルについて説明するテキストファイル。 |
| | テスト環境およびコンセプトの実証環境に使用できる、非本番環境のネットアップライセンスファイル。 |

| パスとファイル名 | 説明 |
| --- | --- |
| | Ubuntu ホストまたは Debian ホストに StorageGRID ノードイメージをインストールするための DEB パッケージ。 |
| | ファイルのMD5チェックサム `/debs/storagegrid-webscale-images-version-SHA.deb` |
| | Ubuntu ホストまたは Debian ホストに StorageGRID ホストサービスをインストールするための DEB パッケージ。 |
| 導入スクリプトツール | 説明 |
| | StorageGRID システムの設定を自動化するための Python スクリプト。 |
| | StorageGRID アプライアンスの設定を自動化するための Python スクリプト。 |
| | シングルサインオンが有効な場合にグリッド管理 API にサインインするために使用できる Python スクリプトの例。 |
| | で使用するサンプル構成ファイル `configure-storagegrid.py` スクリプト： |
| | で使用する空の構成ファイル `configure-storagegrid.py` スクリプト： |
| | StorageGRID コンテナ導入用の Ubuntu ホストまたは Debian ホストを設定するためのサンプルの Ansible のロールとプレイブック。必要に応じて、ロールまたはプレイブックをカスタマイズできます。 |

12. StorageGRID アプライアンスベースのシステムをリカバリする場合は、該当するファイルを選択してください。

| パスとファイル名 | 説明 |
| --- | --- |
| | アプライアンスに StorageGRID ノードイメージをインストールするための DEB パッケージ。 |

| パスとファイル名 | 説明 |
| --- | --- |
| | DEB インストールパッケージのチェックサム。アップロード後にパッケージに変更が加えられていないことを確認するために StorageGRID アプライアンスインストーラで使用されます。 |

*注：*アプライアンスのインストールでは、これらのファイルはネットワーク・トラフィックを回避する必要がある場合にのみ必要です。アプライアンスは、プライマリ管理ノードから必要なファイルをダウンロードできます。

関連情報

"VMware をインストールする"

"Red Hat Enterprise Linux または CentOS をインストールします"

"Ubuntu または Debian をインストールします"

ノードリカバリ手順 を選択しています

## 障害が発生したノードのタイプに適したリカバリ手順 を選択する必要があります。

| **Grid** ノード | **Recovery** 手順 の略 |
| --- | --- |
| 複数のストレージノード | テクニカルサポートにお問い合わせください。複数のストレージノードで障害が発生した場合は、データ損失につながる可能性のあるデータベースの不整合を防ぐために、テクニカルサポートがリカバリを支援する必要があります。サイトリカバリ手順 が必要な場合があります。<br><br>"テクニカルサポートによるサイトリカバリの実行方法" |
| 単一のストレージノード | ストレージノードのリカバリ手順 は、障害のタイプと期間によって異なります。<br><br>"ストレージノードの障害からのリカバリ" |
| 管理ノード | 管理ノードの手順 は、プライマリ管理ノードと非プライマリ管理ノードのどちらをリカバリする必要があるかによって異なります。<br><br>"管理ノードの障害からのリカバリ" |
| ゲートウェイノード | "ゲートウェイノードの障害からのリカバリ"。 |
| アーカイブノード | "アーカイブノードの障害からのリカバリ"。 |

複数のグリッドノードをホストしているサーバで障害が発生した場合、ノードは任意の順序でリカバリできます。ただし、障害サーバがプライマリ管理ノードをホストしている場合は、最初にそのノードをリカバリする必要があります。プライマリ管理ノードを最初にリカバリすると、プライマリ管理ノードへの接続を待機するために他のノードのリカバリが停止するのを防ぐことができます。

ストレージノードの障害からのリカバリ

# 障害ストレージノードをリカバリする手順 は、障害のタイプおよび障害が発生したストレージノードのタイプによって異なります。

次の表を参照して、障害が発生したストレージノードのリカバリ手順 を選択してください。

| 問題 | アクション | 注： |
| --- | --- | --- |
| • 複数のストレージノードで障害が発生した。<br>• ストレージノードの障害またはリカバリ後 15 日たたたないうちに 2 つ目のストレージノードで障害が発生した<br><br>これには、別のストレージノードのリカバリ中にストレージノードで障害が発生した場合が含まれます。 | テクニカルサポートに連絡する必要があります。 | 障害が発生したすべてのストレージノードが同じサイトにある場合は、サイトリカバリ手順 の実行が必要になる可能性があります。<br><br>テクニカルサポートは、お客様の状況を評価し、リカバリプランを作成します。<br><br>"テクニカルサポートによるサイトリカバリの実行方法"<br><br>複数のストレージノード（または 15 日以内に複数のストレージノード）をリカバリすると、Cassandra データベースの整合性に影響し、原因 のデータが失われる可能性があります。<br><br>2 つ目のストレージノードのリカバリを安全に開始できるタイミングはテクニカルサポートが判断します。<br><br>• 注： 1 つのサイトで ADC サービスを含む複数のストレージノードに障害が発生すると、そのサイトに対する保留中のプラットフォームサービス要求はすべて失われます。 |
| ストレージノードが 15 日以上オフラインになっている。 | "15日以上停止しているストレージノードのリカバリ" | この手順 は、 Cassandra データベースの整合性を確保するために必要です。 |

| 問題 | アクション | 注： |
| --- | --- | --- |
| アプライアンスストレージノードで障害が発生した。 | "StorageGRID アプライアンスストレージノードのリカバリ" | アプライアンスストレージノードのリカバリ手順 は、すべての障害で同じです。 |
| ストレージボリュームで障害が発生したが、システムドライブには損傷がない | "システムドライブに損傷がない場合のストレージボリューム障害からのリカバリ" | この手順 はソフトウェアベースのストレージノードに使用されます。 |
| システムドライブで障害が発生した。 | "システムドライブ障害からのリカバリ" | ノード交換用手順 は、導入プラットフォーム、およびストレージボリュームに障害が発生しているかどうかによって異なります。 |

一部の StorageGRID リカバリ手順では、 Reaper を使用して Cassandra の修復を処理します。関連サービスまたは必要なサービスが開始されるとすぐに修理が自動的に行われます。スクリプトの出力には、「 reaper 」または「 Cassandra repair 」が含まれていることがあります。 修復が失敗したことを示すエラーメッセージが表示された場合は、エラーメッセージに示されたコマンドを実行します。

**15**日以上停止しているストレージノードのリカバリ

# 単一のストレージノードがオフラインになって他のストレージノードに接続されなくなってから 15 日以上が経過した場合は、そのノードで Cassandra を再構築する必要があります。

必要なもの

- ストレージノードの運用停止処理が進行中でないこと、またはノードの手順 の運用停止処理が一時停止されていることを確認しておきます（Grid Managerで、* Maintenance * Maintenance Tasks * Decommission *を選択します）。
- 拡張が進行中でないことを確認しておきます（Grid Managerで、* Maintenance * Maintenance Tasks * Expansion *を選択します。）

このタスクについて

ストレージノードには、オブジェクトメタデータを含む Cassandra データベースがあります。他のストレージノードと 15 日以上通信できていないストレージノードの Cassandra データベースは、 StorageGRID によって古いとみなされます。他のストレージノードからの情報を使用して Cassandra が再構築されるまで、そのストレージノードはグリッドに再参加できません。

この手順 は、 1 つのストレージノードが停止している場合にのみ Cassandra を再構築するために使用します。追加のストレージノードがオフラインの場合や、 15 日以内に別のストレージノードで Cassandra が再構築されている場合は、テクニカルサポートにお問い合わせください。たとえば、障害ストレージボリュームのリカバリ手順または障害ストレージノードのリカバリ手順の一環として Cassandra が再構築されている可能性があります。

複数のストレージノードで障害が発生した場合（またはオフラインの場合）は、テクニカルサポートにお問い合わせください。次のリカバリ手順 は実行しないでください。データが失われる可能性があります。

ストレージノードの障害またはリカバリ後 15 日以内に 2 つ目のストレージノードの障害が発生した場合は、テクニカルサポートにお問い合わせください。次のリカバリ手順 は実行しないでください。データが失われる可能性があります。

サイトの複数のストレージノードで障害が発生した場合は、サイトリカバリ手順 が必要になる可能性があります。テクニカルサポートにお問い合わせください。

"テクニカルサポートによるサイトリカバリの実行方法"

手順

1. 必要に応じて、リカバリが必要なストレージノードの電源をオンにします。
2. グリッドノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

   rootとしてログインすると、プロンプトがから変わります `$` 終了： `#.+`

グリッドノードにログインできない場合は、システムディスクが破損している可能性があります。手順 にアクセスして、システムドライブ障害からのリカバリを実行します。 "システムドライブ障害からのリカバリ"

1. ストレージノードで次のチェックを実行します。
   a. 問題コマンド： `nodetool status`

      出力がになっている必要があります `Connection refused`
   b. Grid Managerで、* Support ** Tools * Grid Topology *を選択します。
   c. _site ストレージノード SSM *サービス*を選択します。Cassandraサービスが表示されていることを確認します `Not Running`。
   d. Storage Node * SSM * Resources *を選択します。ボリュームセクションにエラーステータスがないことを確認します。
   e. 問題コマンド： `grep -i Cassandra /var/local/log/servermanager.log`

      出力に次のメッセージが表示されます。

```
Cassandra not started because it has been offline for more than 15 day
grace period - rebuild Cassandra
```

2. 問題 ：このコマンドを使用して、スクリプトの出力を監視します。 `check-cassandra-rebuild`
   ◦ ストレージサービスが実行されている場合は、それらを停止するように求められます。「 * y * 」と入

力します

- スクリプト内の警告を確認します。いずれの状況も該当しない場合は、 Cassandra の再構築を確定します。「 * y * 」と入力します

> 一部の StorageGRID リカバリ手順では、 Reaper を使用して Cassandra の修復を処理します。関連サービスまたは必要なサービスが開始されるとすぐに修理が自動的に行われます。スクリプトの出力には、「 reaper 」または「 Cassandra repair 」が含まれていることがあります。 修復が失敗したことを示すエラーメッセージが表示された場合は、エラーメッセージに示されたコマンドを実行します。

3. リビルドが完了したら、次のチェックを実行します。
   a. Grid Managerで、* Support ** Tools * Grid Topology *を選択します。
   b. _site _*リカバリ済みストレージノード* SSM *サービス*を選択します。
   c. すべてのサービスが実行されていることを確認します。
   d. DDS *データストア*を選択します。
   e. * データ・ストアのステータス * が「アップ」であり、 * データ・ストアの状態 * が「通常」であることを確認します。

関連情報

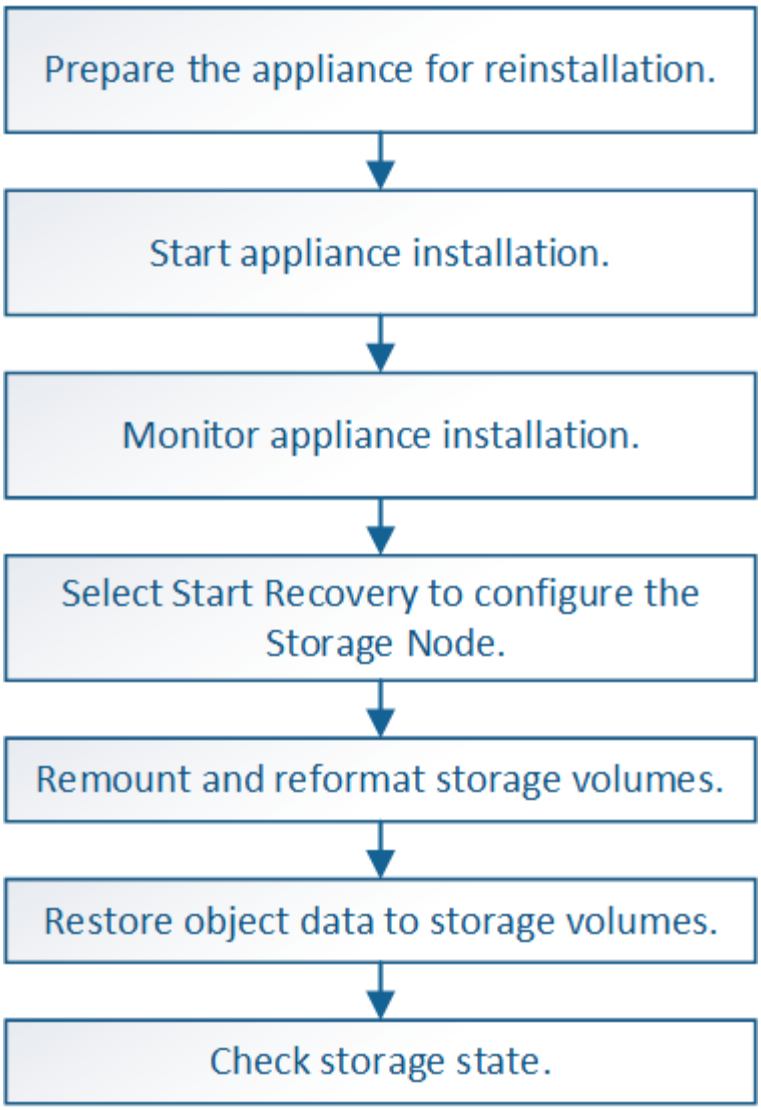
"システムドライブ障害からのリカバリ"

**StorageGRID** アプライアンスストレージノードのリカバリ

## 障害が発生した StorageGRID アプライアンスストレージノードのリカバリ用手順 は、システムドライブの損失からリカバリする場合も、ストレージボリュームのみの損失からリカバリする場合も同じです。

このタスクについて

アプライアンスを準備してソフトウェアを再インストールし、ノードがグリッドに再参加するように設定し、ストレージを再フォーマットし、オブジェクトデータをリストアする必要があります。




複数のストレージノードで障害が発生した場合（またはオフラインの場合）は、テクニカルサポートにお問い合わせください。次のリカバリ手順 は実行しないでください。データが失われる可能性があります。

ストレージノードの障害またはリカバリ後 15 日以内に 2 つ目のストレージノードの障害が発生した場合は、テクニカルサポートにお問い合わせください。15 日以内に複数のストレージノードで Cassandra を再構築すると、データが失われることがあります。

サイトの複数のストレージノードで障害が発生した場合は、サイトリカバリ手順 が必要になる可能性があります。テクニカルサポートにお問い合わせください。

"テクニカルサポートによるサイトリカバリの実行方法"

レプリケートコピーを 1 つだけ保存するように ILM ルールを設定している場合に、そのコピーがあるストレージボリュームで障害が発生すると、オブジェクトをリカバリできません。

リカバリ中に Services ： Status - Cassandra （ SVST ）アラームが発生した場合は、監視とトラブルシューティングの手順を参照して、 Cassandra を再構築してアラームからリカバリしてください。Cassandra を再構築すると、アラームは解除されます。アラームが解除されない場合は、テクニカルサポートに連絡してください。

コントローラの交換や SANtricity OS の再インストールの手順など、ハードウェアのメンテナンス手順については、ご使用のストレージアプライアンスの設置とメンテナンスの手順を参照してください。

関連情報

"トラブルシューティングを監視します"

"SG6000 ストレージアプライアンス"

"SG5700 ストレージアプライアンス"

"SG5600 ストレージアプライアンス"

手順

- "再インストールのためのアプライアンスストレージノードの準備"
- "StorageGRID アプライアンスのインストールを開始しています"
- "StorageGRID アプライアンスのインストールの監視"
- "Start Recoveryを選択して、アプライアンスストレージノードを設定します"
- "アプライアンス・ストレージ・ボリュームの再マウントと再フォーマット（手動手順）"
- "アプライアンスのストレージボリュームへのオブジェクトデータのリストア"
- "アプライアンスストレージノードのリカバリ後のストレージの状態の確認"

再インストールのためのアプライアンスストレージノードの準備

## アプライアンスストレージノードをリカバリする場合は、最初に StorageGRID ソフトウェアを再インストールするアプライアンスを準備する必要があります。

1. 障害が発生したストレージノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

   rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。
2. StorageGRID ソフトウェアをインストールできるようにアプライアンスストレージノードを準備します。 `sgareinstall`
3. 続行するかどうかを尋ねられたら、と入力します。 `y`

アプライアンスがリブートされ、 SSH セッションが終了します。通常は 5 分程度で StorageGRID アプライアンスインストーラが使用可能になりますが、場合によっては最大で 30 分待つ必要があります。

StorageGRID アプライアンスストレージノードがリセットされ、ストレージノード上のデータにアクセスできなくなります。元のインストールプロセスで設定した IP アドレスはそのまま使用する必要がありますが、手順 の完了時に確認しておくことを推奨します。

を実行したあとに `sgareinstall` コマンドを実行すると、StorageGRIDでプロビジョニングされたすべてのアカウント、パスワード、およびSSHキーが削除され、新しいホストキーが生成されます。

**StorageGRID** アプライアンスのインストールを開始しています

## StorageGRID をアプライアンスストレージノードにインストールするには、アプライアンスに含まれている StorageGRID アプライアンスインストーラを使用します。

必要なもの

- アプライアンスをラックに設置し、ネットワークに接続し、電源を投入しておきます。
- StorageGRID アプライアンスインストーラを使用してアプライアンスのネットワークリンクと IP アドレスを設定しておきます。
- StorageGRID グリッドのプライマリ管理ノードの IP アドレスを確認しておきます。
- StorageGRID アプライアンスインストーラの IP 設定ページに表示されるすべてのグリッドネットワークサブネットが、プライマリ管理ノードのグリッドネットワークサブネットリストで定義されている。
- ストレージアプライアンスの設置とメンテナンスの手順に従って、必要な準備作業を完了しておきます。
  - "SG5600 ストレージアプライアンス"
  - "SG5700 ストレージアプライアンス"
  - "SG6000 ストレージアプライアンス"
- サポートされているWebブラウザを使用します。
- アプライアンスのコンピューティングコントローラに割り当てられている IP アドレスのいずれかを確認しておきます。管理ネットワーク（コントローラの管理ポート 1 ）、グリッドネットワーク、またはクライアントネットワークの IP アドレスを使用できます。

このタスクについて

StorageGRID をアプライアンスストレージノードにインストールするには、次の手順を実行します。

- プライマリ管理ノードの IP アドレスおよびノードの名前を指定または確認します。
- インストールを開始し、ボリュームの設定とソフトウェアのインストールが行われている間待機します。
- プロセスの途中でインストールが一時停止します。インストールを再開するには、 Grid Manager にサインインして、保留状態のストレージノードを障害ノードの代わりとして設定する必要があります。
- ノードを設定すると、アプライアンスのインストールプロセスが完了してアプライアンスがリブートされます。

手順

1. ブラウザを開き、コンピューティングコントローラの IP アドレスのいずれかを入力します。

```
https://Controller_IP:8443
```

StorageGRID アプライアンスインストーラのホームページが表示されます。

2. プライマリ管理ノードの接続セクションで、プライマリ管理ノードの IP アドレスを指定する必要があるかどうかを確認します。

   プライマリ管理ノードまたは ADMIN_IP が設定された少なくとも 1 つのグリッドノードが同じサブネットにある場合は、 StorageGRID アプライアンスインストーラがこの IP アドレスを自動的に検出します。

3. この IP アドレスが表示されない場合や変更する必要がある場合は、アドレスを指定します。

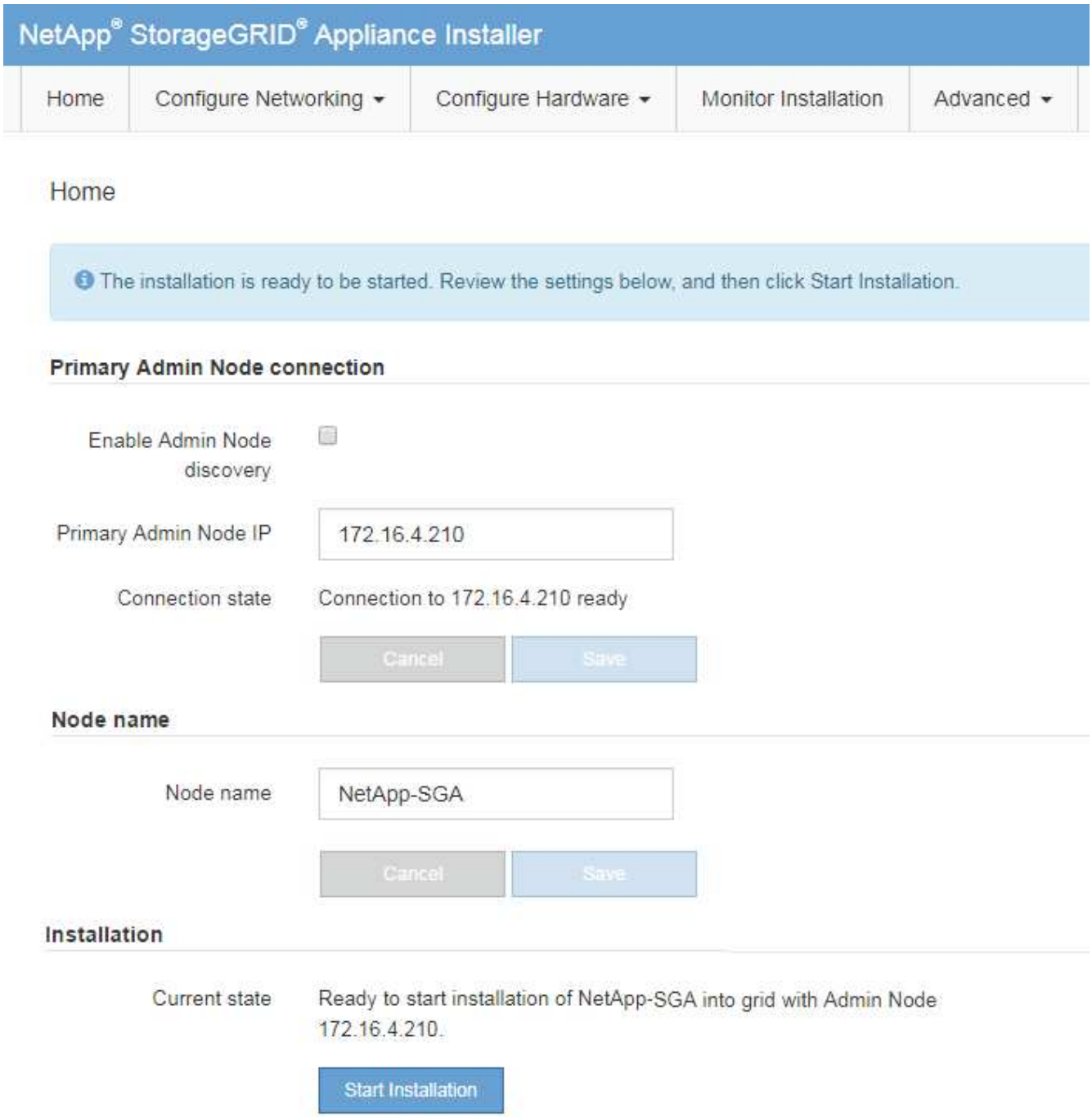
| オプション | 手順 |
| --- | --- |
| IP を手動で入力します | a. Enable Admin Node discovery * チェックボックスの選択を解除します。<br>b. IP アドレスを手動で入力します。<br>c. [ 保存（ Save ） ] をクリックします。<br>d. 新しい IP アドレスの接続状態が「 ready 」になるまで待機します。 |
| 接続されたすべてのプライマリ管理ノードの自動検出 | a. Enable Admin Node discovery * チェックボックスを選択します。<br>b. 検出された IP アドレスのリストから、このアプライアンスストレージノードを導入するグリッドのプライマリ管理ノードを選択します。<br>c. [ 保存（ Save ） ] をクリックします。<br>d. 新しい IP アドレスの接続状態が「 ready 」になるまで待機します。 |

4. [ ノード名 *] フィールドに ' リカバリするノードに使用されていた名前を入力し '[ 保存 *] をクリックします

5. Installation （インストール）セクションで、現在の状態が「 Ready to start installation of node name into grid with Primary Admin Node admin_IP 」（プライマリ管理ノード admin_ip によるノード名のグリッドへのインストールを開始する準備ができました）であり、 * Start Installation * （インストールの開始）ボタンが有効になっていることを

   [Start Installation* （インストールの開始） ] ボタンが有効になっていない場合は、ネットワーク設定またはポート設定の変更が必要になることがあります。手順については、使用しているアプライアンスのインストールとメンテナンスの手順を参照してください。

6. StorageGRID アプライアンスインストーラのホームページで、 * インストールの開始 * をクリックします。




現在の状態が「 Installation is in progress 」に変わり、「 Monitor Installation 」ページが表示されます。

モニタのインストールページに手動でアクセスする必要がある場合は、メニューバーから * モニタのインストール * をクリックします。

関連情報

"SG100 SG1000サービスアプライアンス"

"SG6000 ストレージアプライアンス"

"SG5700 ストレージアプライアンス"

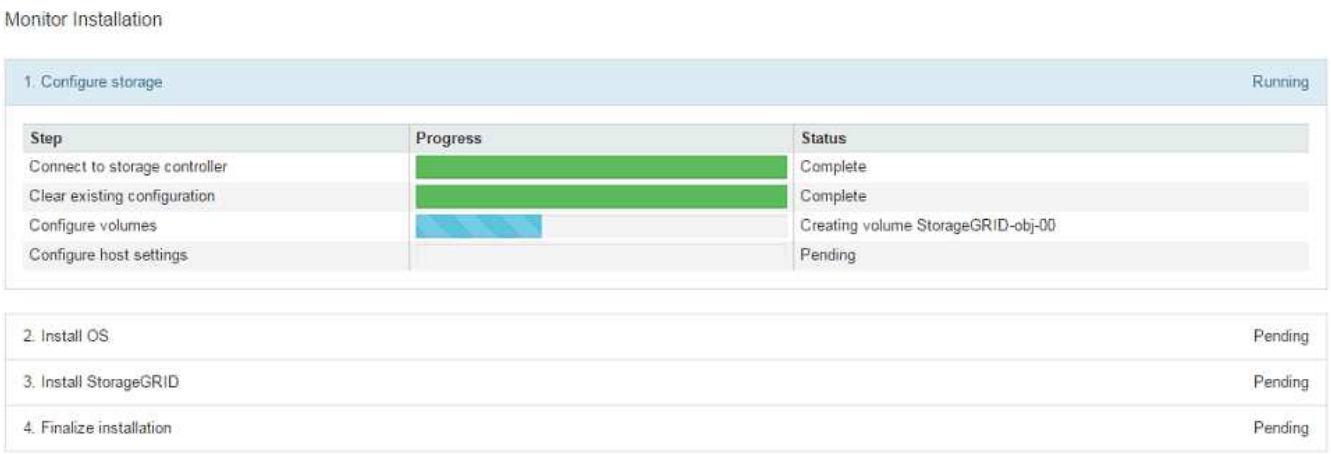
"SG5600 ストレージアプライアンス"

**StorageGRID** アプライアンスのインストールの監視

StorageGRID アプライアンスインストーラでは、インストールが完了するまでステータスが提供されます。ソフトウェアのインストールが完了すると、アプライアンスがリブートされます。

1. インストールの進行状況を監視するには、メニューバーの * インストールの監視 * をクリックします。

   Monitor Installation ページにインストールの進行状況が表示されます。




   青色のステータスバーは、現在進行中のタスクを示します。緑のステータスバーは、正常に完了したタスクを示します。

   インストーラは、以前のインストールで完了したタスクが再実行されないようにします。インストールを再実行している場合 ' 再実行する必要のないタスクは ' 緑色のステータスバーとステータスが [ スキップ済み ] と表示されます

2. インストールの最初の 2 つのステージの進行状況を確認します。

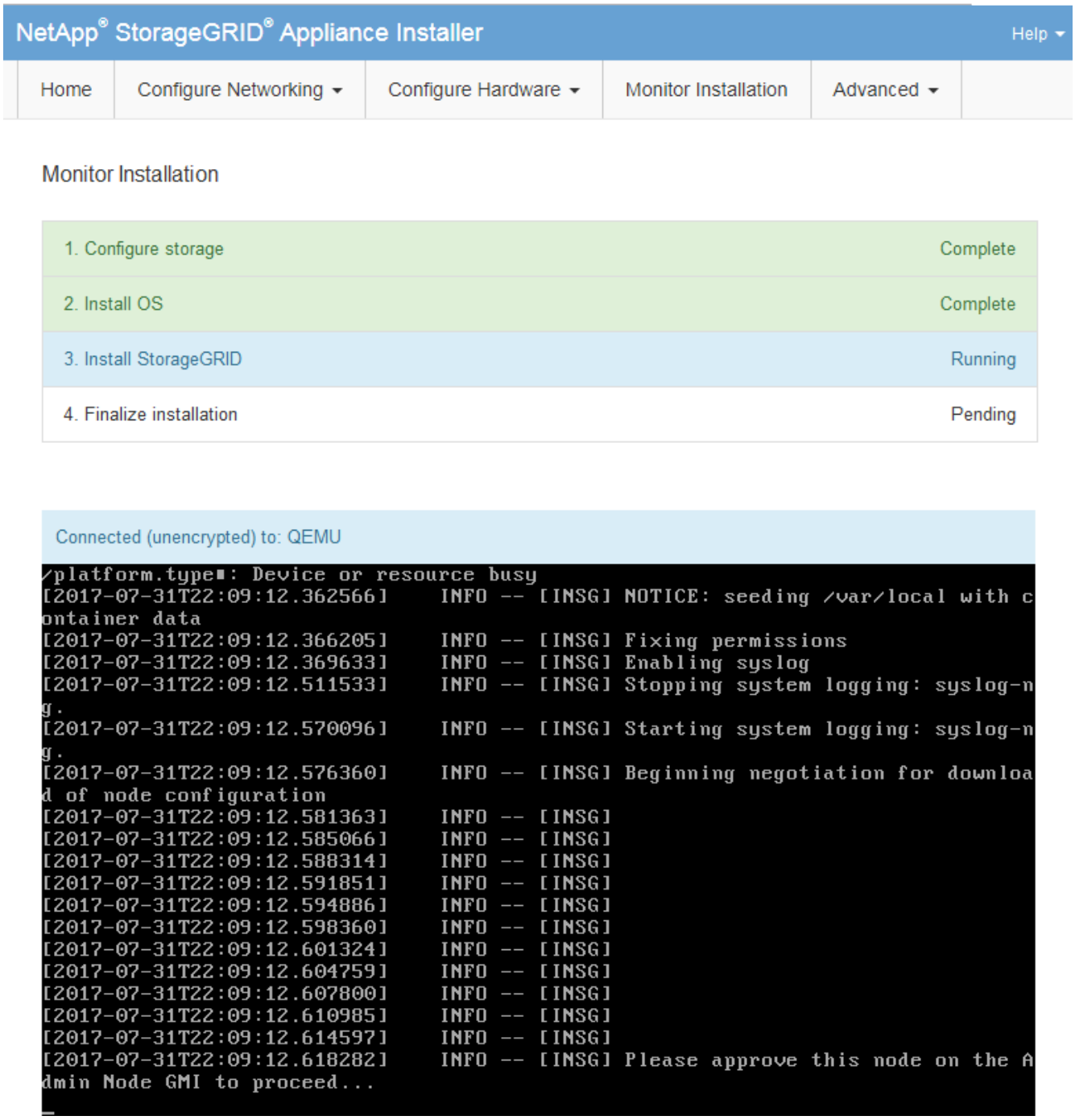
   - * 1 。ストレージの構成 *

     インストーラがストレージコントローラに接続し、既存の設定があれば消去し、 SANtricity ソフトウェアと通信してボリュームを設定し、ホストを設定します。

   - ※ 2OS * をインストールします

     インストーラが StorageGRID のベースとなるオペレーティングシステムイメージをアプライアンスにコピーします。

3. インストールの進行状況の監視を続けて、組み込みのコンソールに「 Install StorageGRID * 」ステージが一時停止し、グリッドマネージャを使用して管理ノード上でこのノードを承認するように求めるメッセージが表示されるまで待ちます。




4. 手順 にアクセスしてアプライアンスストレージノードを設定します。

**Start Recovery**を選択して、アプライアンスストレージノードを設定します

## 障害が発生したノードの代わりとしてアプライアンスストレージノードを設定するには、 Grid Manager で [Start Recovery] を選択する必要があります。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Maintenance または Root Access 権限が必要です。
- プロビジョニングパスフレーズが必要です。

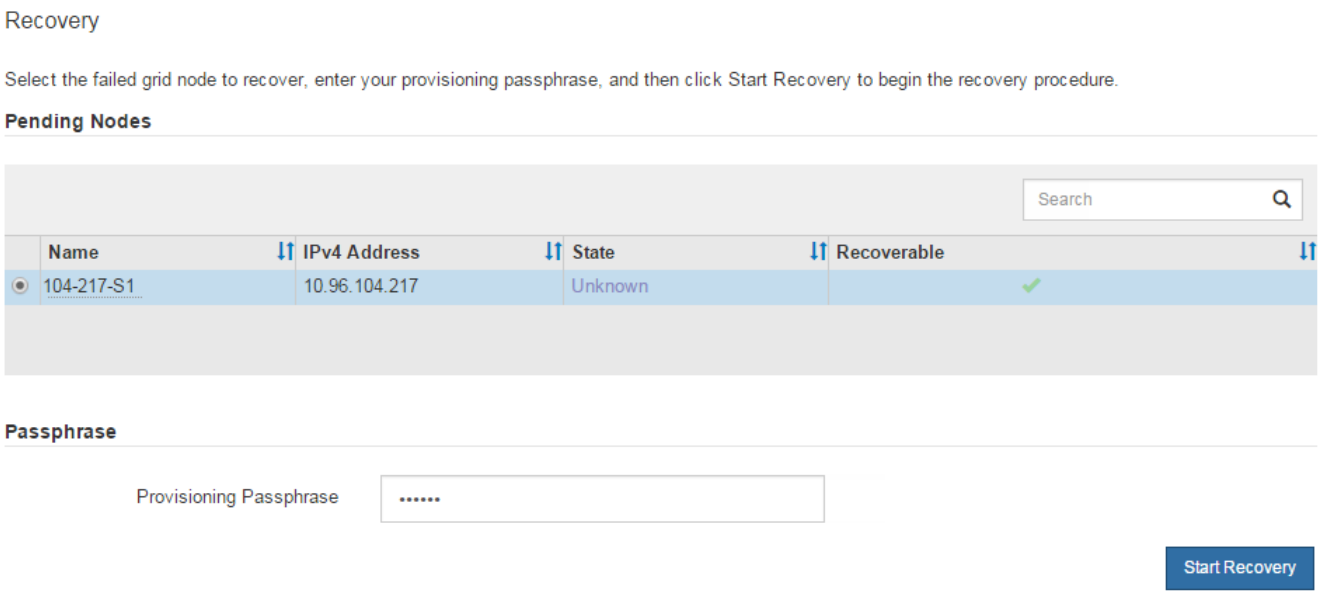
- リカバリ用アプライアンスストレージノードを導入しておく必要があります。
- イレイジャーコーディングデータの修復ジョブの開始日を把握しておく必要があります。
- ストレージノードが過去 15 日以内に再構築されていないことを確認しておく必要があります。

手順

1. Grid Managerから、* Maintenance * Maintenance Tasks * Recovery *（メンテナンス*メンテナンスタスク*リカバリ）を選択します。
2. リカバリするグリッドノードを Pending Nodes リストで選択します。

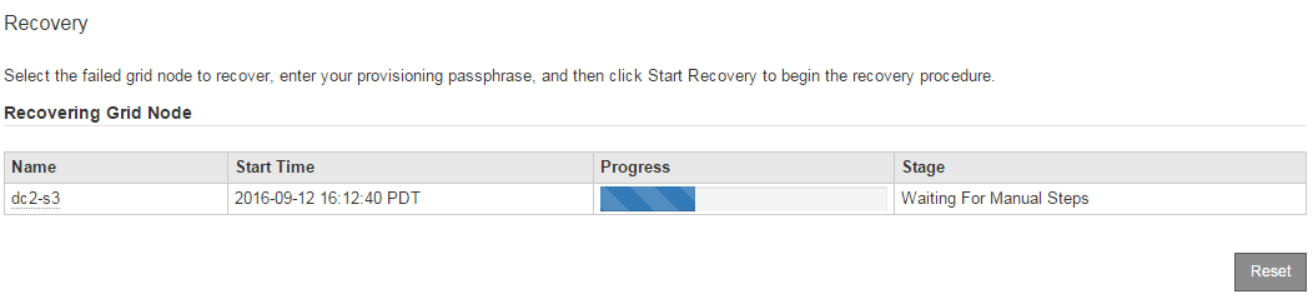
   ノードは障害が発生するとリストに追加されますが、再インストールされてリカバリの準備ができるまでは選択できません。

3. プロビジョニングパスフレーズ * を入力します。
4. [ リカバリの開始 ] をクリックします。

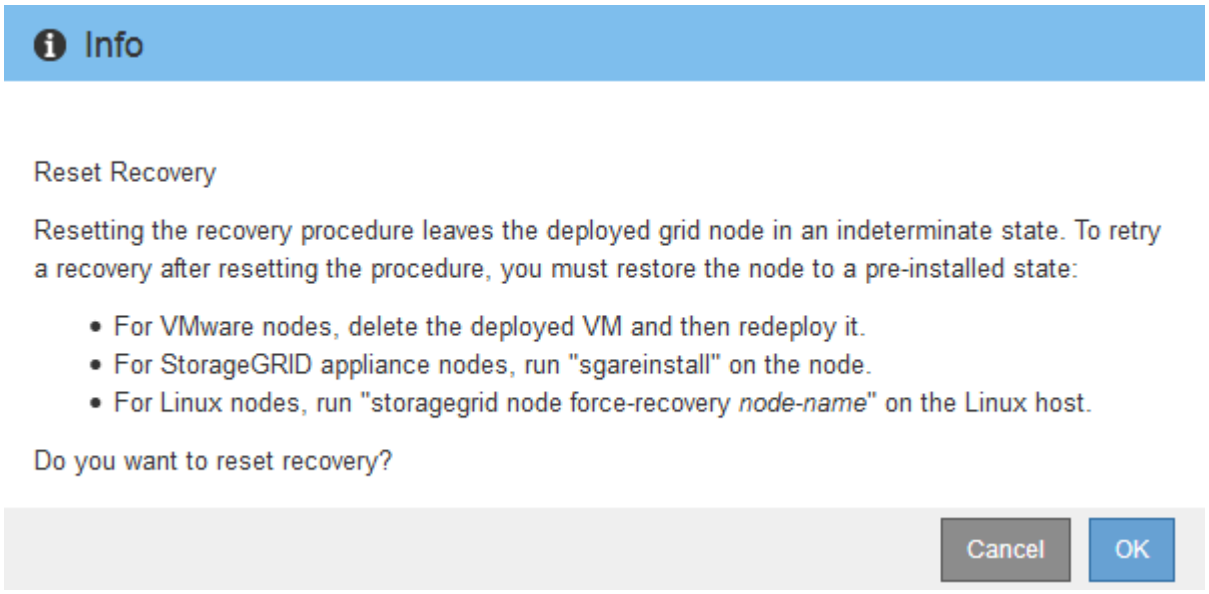



5. リカバリ中のグリッドノードテーブルで、リカバリの進行状況を監視します。

   グリッドノードが「 Waiting for Manual Steps 」ステージに進んだら、次のトピックの手順に従って、アプライアンスのストレージボリュームを手動で再マウントし、再フォーマットします。



リカバリ中の任意の時点で、 [* リセット ] をクリックして新しいリカバリを開始できます。情報ダイアログボックスが表示され、手順 をリセットするとノードが不確定な状態のままになることが示されます。




手順 をリセットしたあとにリカバリを再試行する場合は、を実行してアプライアンスノードをインストール前の状態にリストアする必要があります `sgareinstall` をクリックします。

アプライアンスストレージボリュームの再マウントと再フォーマット（「手動手順」）

2 つのスクリプトを手動で実行して、保持されているストレージボリュームを再マウントし、障害ストレージボリュームを再フォーマットする必要があります。最初のスクリプトは、 StorageGRID ストレージボリュームとして適切にフォーマットされているボリュームを再マウントします。2 番目のスクリプトは、マウントされていないボリュームを再フォーマットし、必要に応じて Cassandra データベースを再構築して、サービスを開始します。

必要なもの

- 障害が発生したストレージボリュームのうち、必要と判断した場合はハードウェアを交換しておく必要があります。

  を実行します `sn-remount-volumes` スクリプトを使用すると、障害ストレージボリュームを追加で特定できる場合があります。

- ストレージノードの運用停止処理が進行中でないこと、またはノードの手順 の運用停止処理が一時停止されていることを確認しておきます（Grid Managerで、* Maintenance * Maintenance Tasks * Decommission *を選択します）。
- 拡張が進行中でないことを確認しておきます（Grid Managerで、* Maintenance * Maintenance Tasks * Expansion *を選択します。）

複数のストレージノードがオフラインの場合、またはこのグリッド内のストレージノードが過去 15 日以内に再構築されている場合は、テクニカルサポートにお問い合わせください。を実行しないでください `sn-recovery-postinstall.sh` スクリプト：15 日以内に複数のストレージノードで Cassandra を再構築すると、データが失われることがあります。

このタスクについて

この手順 を完了するには、次の作業を行います。

- リカバリされたストレージノードにログインします。
- を実行します `sn-remount-volumes` 適切にフォーマットされたストレージボリュームを再マウントするスクリプト。このスクリプトを実行すると、次の処理が行われます。
  - 各ストレージボリュームをマウントしてアンマウントし、 XFS ジャーナルをリプレイします。
  - XFS ファイルの整合性チェックを実行します。
  - ファイルシステムに整合性がある場合は、ストレージボリュームが適切にフォーマットされた StorageGRID ストレージボリュームであるかどうかを確認します。
  - ストレージボリュームが適切にフォーマットされている場合は、ストレージボリュームを再マウントします。ボリューム上の既存のデータはそのまま維持されます。
- スクリプトの出力を確認し、問題を解決します。
- を実行します `sn-recovery-postinstall.sh` スクリプト：このスクリプトを実行すると、次の処理が実行されます。

  リカバリの実行中はストレージノードをリブートしないでください `sn-recovery-postinstall.sh` （手順4）障害ストレージボリュームの再フォーマットとオブジェクトメタデータのリストア実行前にストレージノードをリブートしています `sn-recovery-postinstall.sh` completesを指定すると、サービスが開始しようとするとエラーが発生し、StorageGRID アプライアンスノードが保守モードを終了します。

  - で指定したストレージボリュームを再フォーマットします `sn-remount-volumes` スクリプトをマウントできなかったか、またはスクリプトの形式が正しくありませんでした。

    ストレージボリュームを再フォーマットすると、そのボリューム上のデータはすべて失われます。複数のオブジェクトコピーを格納するように ILM ルールが設定されている場合は、グリッド内の他の場所からオブジェクトデータをリストアするために追加の手順 を実行する必要があります。

  - 必要に応じて、ノードの Cassandra データベースを再構築します。
  - ストレージノードのサービスを開始します。

手順

1. リカバリしたストレージノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`

d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

2. 最初のスクリプトを実行し、適切にフォーマットされたストレージボリュームを再マウントします。

> すべてのストレージボリュームが新規でフォーマットが必要な場合、またはすべてのストレージボリュームで障害が発生した場合は、この手順を省略して 2 つ目のスクリプトを実行し、マウントされていないストレージボリュームをすべて再フォーマットします。

a. スクリプトを実行します。 `sn-remount-volumes`

データが格納されたストレージボリュームでこのスクリプトを実行すると、数時間かかることがあります。

b. スクリプトの実行時に、出力と回答 のプロンプトを確認します。

> 必要に応じて、を使用できます `tail -f` スクリプトのログファイルの内容を監視するコマンド (`/var/local/log/sn-remount-volumes.log`) 。ログファイルには、コマンドラインの出力よりも詳細な情報が含まれています。

```
root@SG:~ # sn-remount-volumes
The configured LDR noid is 12632740

====== Device /dev/sdb ======
Mount and unmount device /dev/sdb and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sdb:
Mount device /dev/sdb to /tmp/sdb-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12632740, volume number 0 in the volID file
Attempting to remount /dev/sdb
Device /dev/sdb remounted successfully

====== Device /dev/sdc ======
Mount and unmount device /dev/sdc and checking file system
consistency:
Error: File system consistency check retry failed on device /dev/sdc.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh, this volume and any data on this volume will be
deleted. If you only had two copies of object data, you will
temporarily have only a single copy.
StorageGRID Webscale will attempt to restore data redundancy by
```

```
making additional replicated copies or EC fragments, according to the
rules in the active ILM policy.

Do not continue to the next step if you believe that the data
remaining on this volume cannot be rebuilt from elsewhere in the grid
(for example, if your ILM policy uses a rule that makes only one copy
or if volumes have failed on multiple nodes). Instead, contact
support to determine how to recover your data.

====== Device /dev/sdd ======
Mount and unmount device /dev/sdd and checking file system
consistency:
Failed to mount device /dev/sdd
This device could be an uninitialized disk or has corrupted
superblock.
File system check might take a long time. Do you want to continue? (y
or n) [y/N]? y

Error: File system consistency check retry failed on device /dev/sdd.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh, this volume and any data on this volume will be
deleted. If you only had two copies of object data, you will
temporarily have only a single copy.
StorageGRID Webscale will attempt to restore data redundancy by
making additional replicated copies or EC fragments, according to the
rules in the active ILM policy.

Do not continue to the next step if you believe that the data
remaining on this volume cannot be rebuilt from elsewhere in the grid
(for example, if your ILM policy uses a rule that makes only one copy
or if volumes have failed on multiple nodes). Instead, contact
support to determine how to recover your data.

====== Device /dev/sde ======
Mount and unmount device /dev/sde and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sde:
Mount device /dev/sde to /tmp/sde-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12000078, volume number 9 in the volID file
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

この出力例では、 1 つのストレージボリュームが正常に再マウントされ、 3 つのストレージボリュームでエラーが発生しています。

- `/dev/sdb` は、XFSファイルシステムの整合性チェックに合格し、ボリューム構造が有効なため、正常に再マウントされました。スクリプトによって再マウントされたデバイスのデータは保持されています。
- `/dev/sdc` は、ストレージボリュームが新規または破損していたため、XFSファイルシステムの整合性チェックに合格できませんでした。
- `/dev/sdd` ディスクが初期化されていないか、ディスクのスーパーブロックが破損していたため、をマウントできませんでした。スクリプトは、ストレージボリュームをマウントできない場合、ファイルシステムの整合性チェックを実行するかどうかを確認するメッセージを表示します。
  - ストレージ・ボリュームが新しいディスクに接続されている場合は、回答 * N * をプロンプトに表示します。新しいディスクのファイルシステムをチェックする必要はありません。
  - ストレージ・ボリュームが既存のディスクに接続されている場合は、回答 * Y * がプロンプトに表示されます。ファイルシステムのチェックの結果を使用して、破損の原因を特定できます。結果がに保存されます `/var/local/log/sn-remount-volumes.log` ログファイル：
- `/dev/sde` は、XFSファイルシステムの整合性チェックに合格し、ボリューム構造が有効でした。ただし、のLDRノードIDです `volID` ファイルがこのストレージノードのIDと一致しませんでした（ `configured LDR noid` 上部に表示）。このメッセージは、このボリュームが別のストレージノードに属していることを示しています。

3. スクリプトの出力を確認し、問題を解決します。

> ストレージボリュームが XFS ファイルシステムの整合性チェックに合格できなかった場合、またはストレージボリュームをマウントできなかった場合は、出力のエラーメッセージをよく確認してください。を実行した場合の影響を理解しておく必要があります `sn-recovery-postinstall.sh` これらのボリュームにスクリプトを設定します。

a. 想定しているすべてのボリュームのエントリが結果に含まれていることを確認します。表示されていないボリュームがある場合は、スクリプトを再実行します。

b. マウントされたすべてのデバイスのメッセージを確認します。ストレージボリュームがこのストレージノードに属していないことを示すエラーがないことを確認します。

この例では、 /dev/sde の出力に、次のエラーメッセージが含まれています。

```
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

> あるストレージボリュームが別のストレージノードに属していると報告される場合は、テクニカルサポートにお問い合わせください。を実行する場合は、を実行します `sn-recovery-postinstall.sh` スクリプトでは、ストレージボリュームが再フォーマットされますが、原因 のデータが失われることがあります。

c. マウントできなかったストレージデバイスがある場合は、デバイス名をメモし、デバイスを修理または交換します。

マウントできなかったストレージデバイスはすべて修理または交換する必要があります。

デバイス名を使用してボリュームIDを検索します。このIDは、を実行する際に必要な入力情報です `repair-data` オブジェクトデータをボリューム（次の手順）にリストアするスクリプト。

d. マウントできないデバイスをすべて修復または交換したら、を実行します `sn-remount-volumes` もう一度スクリプトを実行して、再マウントできるすべてのストレージボリュームが再マウントされたことを確認します。

ストレージボリュームをマウントできない場合、またはストレージボリュームが適切にフォーマットされなかった場合に次の手順に進むと、ボリュームとそのボリューム上のデータが削除されます。オブジェクトデータのコピーが 2 つあった場合、次の手順（オブジェクトデータのリストア）が完了するまでコピーは 1 つだけになります。

を実行しないでください `sn-recovery-postinstall.sh` スクリプト：障害ストレージボリュームに残っているデータをグリッド内の他の場所から再構築することができないと考えられる場合（ILMポリシーでコピーを1つだけ作成するルールが使用されている場合や、複数のノードでボリュームに障害が発生した場合など）。代わりに、テクニカルサポートに問い合わせてデータのリカバリ方法を確認してください。

4. を実行します `sn-recovery-postinstall.sh` スクリプト： `sn-recovery-postinstall.sh`

このスクリプトは、マウントできなかったストレージボリューム、または適切にフォーマットされていないストレージボリュームを再フォーマットし、必要に応じてノードの Cassandra データベースを再構築して、ストレージノードのサービスを開始します。

次の点に注意してください。

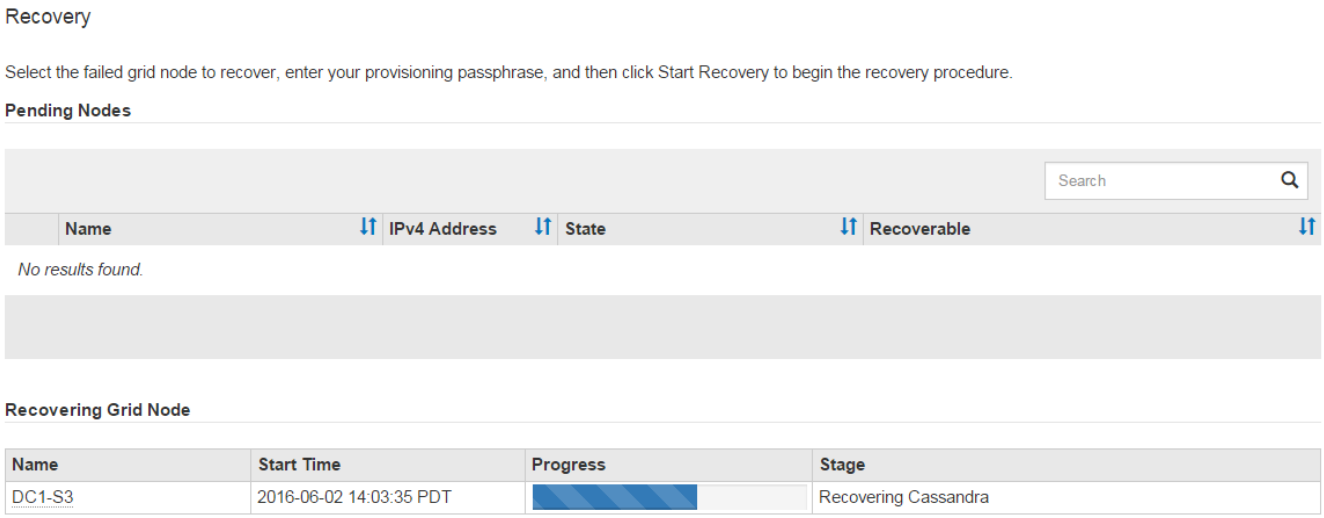
- スクリプトの実行には数時間かかることがあります。
- 一般に、スクリプトの実行中は、 SSH セッションは単独で行う必要があります。
- SSH セッションがアクティブになっている間は、 * Ctrl+C キーを押さないでください。
- このスクリプトは、ネットワークの中断が発生して SSH セッションが終了した場合にバックグラウンドで実行されますが、進行状況はリカバリページで確認できます。
- ストレージノードで RSM サービスを使用している場合は、ノードサービスの再起動時にスクリプトが 5 分間停止しているように見えることがあります。この 5 分間の遅延は、 RSM サービスが初めて起動するときに発生します。

RSM サービスは、 ADC サービスが含まれるストレージノードにあります。

一部の StorageGRID リカバリ手順では、 Reaper を使用して Cassandra の修復を処理します。関連サービスまたは必要なサービスが開始されるとすぐに修理が自動的に行われます。スクリプトの出力には、「 reaper 」または「 Cassandra repair 」が含まれていることがあります。 修復が失敗したことを示すエラーメッセージが表示された場合は、エラーメッセージに示されたコマンドを実行します。

5. として `sn-recovery-postinstall.sh` スクリプトが実行され、Grid Managerのリカバリページが監視されます。

のステータスの概要は、リカバリページの進捗状況バーとステージ列で確認できます `sn-recovery-postinstall.sh` スクリプト：




6. と入力して、StorageGRID アプライアンスインストーラのMonitor Installページに戻ります `\http://Controller_IP:8080`コンピューティングコントローラのIPアドレスを使用して割り当てます。

   Monitor Install ページには、スクリプトの実行中のインストールの進行状況が表示されます。

のあとに入力します `sn-recovery-postinstall.sh` スクリプトによってノードでサービスが開始されました。次の手順 で説明するように、スクリプトでフォーマットされた任意のストレージボリュームにオブジェクトデータをリストアできます。

関連情報

"ストレージノードのシステムドライブのリカバリに関する警告の確認"

"アプライアンスのストレージボリュームへのオブジェクトデータのリストア"

アプライアンスのストレージボリュームへのオブジェクトデータのリストア

## アプライアンスストレージノードのストレージボリュームをリカバリしたら、ストレージノードの障害で失われたオブジェクトデータをリストアできます。

必要なもの

- リカバリされたストレージノードの接続状態が * connected * であることを確認しておく必要があります✔ Grid Managerの* Nodes > Overview *タブ。

このタスクについて

グリッドの ILM ルールがオブジェクトコピーを作成するように設定されていた場合、他のストレージノード、アーカイブノード、またはクラウドストレージプールからオブジェクトデータをリストアできます。

> ⓘ レプリケートされたコピーを 1 つだけ保存するように ILM ルールが設定されていて、そのコピーがストレージボリュームに障害が発生した場合、オブジェクトをリカバリすることはできません。

オブジェクトのコピーがクラウドストレージプールにしか残っていない場合、 StorageGRID は、オブジェクトデータをリストアするために複数の要求をクラウドストレージプールエンドポイントに問題 する必要があります。この手順 を実行する前に、テクニカルサポートに問い合わせて、リカバリ期間と関連コストの見積もりを依頼してください。

オブジェクトのコピーがアーカイブノードにしか残っていない場合は、アーカイブノードからオブジェクトデータが読み出されます。外部アーカイブストレージシステムからの読み出しには遅延が伴うため、アーカイブノードからストレージノードへのオブジェクトデータのリストアには、他のストレージノードからコピーをリストアする場合に比べて時間がかかります。

オブジェクトデータをリストアするには、を実行します `repair-data` スクリプト：このスクリプトは、オブジェクトデータのリストアプロセスを開始し、 ILM スキャンと連動して ILM ルールを適用します。では、さまざまなオプションを使用します `repair-data` 次の方法で、レプリケートデータとイレイジャーコーディングデータのどちらをリストアするかに基づくスクリプトです。

- レプリケートデータ：レプリケートデータをリストアするコマンドは、ノード全体を修復するのか、ノード上の一部のボリュームのみを修復するのかに応じて2つあります。

```
repair-data start-replicated-node-repair
```

```
repair-data start-replicated-volume-repair
```

- イレイジャーコーディング（**EC**）データ：イレイジャーコーディングデータをリストアするコマンドは、ノード全体を修復するのか、ノード上の一部のボリュームのみを修復するのかに応じて2つあります。

```
repair-data start-ec-node-repair
```

```
repair-data start-ec-volume-repair
```

イレイジャーコーディングデータの修復は、一部のストレージノードがオフライン状態で開始できます。修復はすべてのノードが使用可能になったあとに完了します。次のコマンドを使用して、イレイジャーコーディングデータの修復を追跡できます。

```
repair-data show-ec-repair-status
```

EC 修復ジョブによって、大量のストレージが一時的にリザーブされます。ストレージアラートがトリガーされることもありますが、修復が完了すると解決します。予約に必要なストレージが不足していると、 EC の修復ジョブが失敗します。ストレージリザベーションは、ジョブが失敗したか成功したかに関係なく、 EC 修復ジョブが完了すると解放されます。

を使用する方法の詳細については、を参照してください `repair-data` スクリプトを入力します `repair-`

`data --help` プライマリ管理ノードのコマンドラインを使用します。

手順

1. プライマリ管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

   rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。
2. を使用します `/etc/hosts` リストアされたストレージボリュームのストレージノードのホスト名を特定するファイル。グリッド内のすべてのノードのリストを表示するには、次のように入力します。 `cat /etc/hosts`
3. すべてのストレージボリュームで障害が発生した場合は、ノード全体を修復します。（一部のボリュームだけで障害が発生した場合は、次の手順に進みます）。

   を実行できません `repair-data` 複数のノードに対して同時に処理を実行すること。複数のノードをリカバリする場合は、テクニカルサポートにお問い合わせください。

   - グリッドにレプリケートデータがある場合は、を使用します `repair-data start-replicated-node-repair` コマンドにを指定します `--nodes` ストレージノード全体を修復するオプションです。

     次のコマンドは、 SG-DC-SN3 というストレージノードにあるレプリケートデータを修復します。

     ```
     repair-data start-replicated-node-repair --nodes SG-DC-SN3
     ```

     オブジェクトデータのリストア時、 StorageGRID システムがレプリケートされたオブジェクトデータを見つけられない場合は、 * Objects lost * アラートがトリガーされます。システム全体のストレージノードでアラートがトリガーされることがあります。損失の原因 と、リカバリが可能かどうかを確認する必要があります。StorageGRID の監視とトラブルシューティングの手順を参照してください。

   - グリッドにイレイジャーコーディングデータがある場合は、を使用します `repair-data start-ec-node-repair` コマンドにを指定します `--nodes` ストレージノード全体を修復するオプションです。

     次のコマンドは、SG-DC-SN3というストレージノードにあるイレイジャーコーディングデータを修復します。

     ```
     repair-data start-ec-node-repair --nodes SG-DC-SN3
     ```

     一意のが返されます `repair ID` これを識別します `repair_data` 操作。これを使用します `repair ID` をクリックして、の進捗状況と結果を追跡します `repair_data` 操作。リカバリプロセスが完了しても、それ以外のフィードバックは返されません。

イレイジャーコーディングデータの修復は、一部のストレージノードがオフライン状態で開始できます。修復はすべてのノードが使用可能になったあとに完了します。

- グリッドにレプリケートデータとイレイジャーコーディングデータの両方がある場合は、両方のコマンドを実行します。

4. 一部のボリュームだけで障害が発生した場合は、影響を受けたボリュームを修復します。

ボリューム ID を 16 進数で入力します。例： `0000` は、最初のボリュームとです `000F` 16番目のボリュームです。1 つのボリューム、一連のボリューム、または連続していない複数のボリュームを指定できます。

すべてのボリュームが同じストレージノードにある必要があります。複数のストレージノードのボリュームをリストアする必要がある場合は、テクニカルサポートにお問い合わせください。

- グリッドにレプリケートデータがある場合は、を使用します `start-replicated-volume-repair` コマンドにを指定します `--nodes` ノードを識別するオプション。次に、を追加します `--volumes` または `--volume-range` 次の例に示すように、オプションを指定します。

  単一ボリューム：レプリケートされたデータをボリュームにリストアします `0002` SG-DC-SN3という名前のストレージノードで次のように設定します。

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3
--volumes 0002
```

  ボリューム範囲：レプリケートされたデータを範囲内のすべてのボリュームにリストアします `0003` 終了： `0009` SG-DC-SN3という名前のストレージノードで次のように設定します。

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume
-range 0003-0009
```

  複数のボリュームが連続していません：このコマンドは、複製されたデータをボリュームにリストアします `0001`、 `0005`および `0008` SG-DC-SN3という名前のストレージノードで次のように設定します。

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3
--volumes 0001,0005,0008
```

  オブジェクトデータのリストア時、 StorageGRID システムがレプリケートされたオブジェクトデータを見つけられない場合は、 * Objects lost * アラートがトリガーされます。システム全体のストレージノードでアラートがトリガーされることがあります。損失の原因 と、リカバリが可能かどうかを確認する必要があります。StorageGRID の監視とトラブルシューティングの手順を参照してください。

- グリッドにイレイジャーコーディングデータがある場合は、を使用します `start-ec-volume-repair` コマンドにを指定します `--nodes` ノードを識別するオプション。次に、を追加します `--volumes` または `--volume-range` 次の例に示すように、オプションを指定します。

単一ボリューム：イレイジャーコーディングされたデータをボリュームにリストアします `0007` SG-DC-SN3という名前のストレージノードで次のように設定します。

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 0007
```

ボリューム範囲：イレイジャーコーディングされたデータを範囲内のすべてのボリュームにリストアします `0004` 終了： `0006` SG-DC-SN3という名前のストレージノードで次のように設定します。

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range
0004-0006
```

複数のボリュームが連続していません：このコマンドはイレイジャーコーディングされたデータをボリュームにリストアします `000A`、 `000C`および `000E` SG-DC-SN3という名前のストレージノードで次のように設定します。

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes
000A,000C,000E
```

。 `repair-data` 一意のが返されます `repair ID` これを識別します `repair_data` 操作。これを使用します `repair ID` をクリックして、の進捗状況と結果を追跡します `repair_data` 操作。リカバリプロセスが完了しても、それ以外のフィードバックは返されません。

> イレイジャーコーディングデータの修復は、一部のストレージノードがオフライン状態で開始できます。修復はすべてのノードが使用可能になったあとに完了します。

- グリッドにレプリケートデータとイレイジャーコーディングデータの両方がある場合は、両方のコマンドを実行します。

5. レプリケートデータの修復を監視します。
   a. 「* Nodes > Storage Node being repaired > ILM *」を選択します。
   b. 「評価」セクションの属性を使用して、修理が完了したかどうかを判断します。

      修復が完了すると、Awaiting - All属性は0個のオブジェクトを示します。

   c. 修復の詳細を監視するには、* Support > Tools > Grid Topology *を選択します。
   d. 「* grid > Storage Node being repaired > LDR > Data Store *」を選択します。
   e. 次の属性を組み合わせて、レプリケートデータの修復が完了したかどうかを可能なかぎり判別します。

      > Cassandra に不整合が生じている可能性があり、また、失敗した修復は追跡されません。

      - * Repairs Attempted （ XRPA ） * ：レプリケートデータの修復の進行状況を追跡します。この属性は、ストレージノードがハイリスクオブジェクトの修復を試みるたびに値が増分します。この属性の値が現在のスキャン期間（ * Scan Period - - Estimated * 属性で指定）よりも長い期間にわ

たって上昇しない場合、 ILM スキャンはすべてのノードで修復が必要なハイリスクオブジェクトを検出していません。

> ハイリスクオブジェクトとは、完全に失われる危険があるオブジェクトです。ILM 設定を満たしていないオブジェクトは含まれません。

- * スキャン期間 - 推定（ XSCM ） * ：この属性を使用して、以前に取り込まれたオブジェクトにポリシー変更が適用されるタイミングを見積もります。「 * Repairs Attempted * 」属性が現在のスキャン期間よりも長くなっていない場合は、複製修復が実行されている可能性があります。スキャン期間は変わる可能性があるので注意してください。* Scan Period - - Estimated （ XSCM ） * 属性は、グリッド全体の環境 を示します。これは、すべてのノードのスキャン期間の最大値です。グリッドの * Scan Period - - Estimated * 属性履歴を照会して、適切な期間を判断できます。

6. イレイジャーコーディングデータの修復を監視し、失敗した可能性のある要求を再試行します。

   a. イレイジャーコーディングデータの修復ステータスを確認します。

      - 特定ののののステータスを表示するには、このコマンドを使用します `repair-data` 操作：

      ```
      repair-data show-ec-repair-status --repair-id repair ID
      ```

      - すべての修復処理を表示するには、次のコマンドを使用します

      ```
      repair-data show-ec-repair-status
      ```

      出力には、などの情報が表示されます `repair ID`以前に、現在実行中のすべての修復。

```
root@DC1-ADM1:~ # repair-data show-ec-repair-status

Repair ID Scope Start Time  End Time  State  Est Bytes
Affected/Repaired Retry Repair
================================================================================
================
 949283 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:27:06.9 Success 17359
17359 No
 949292 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:37:06.9 Failure 17359
0     Yes
 949294 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:47:06.9 Failure 17359
0     Yes
 949299 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:57:06.9 Failure 17359
0     Yes
```

   b. 失敗した修復処理が出力された場合は、を使用します `--repair-id` 修復を再試行するオプションです。

      このコマンドは、修復IDを使用して、障害が発生したノードの修復を再試行します

83930030303133434：

```
repair-data start-ec-node-repair --repair-id 83930030303133434
```

このコマンドは、修復IDを使用して、障害が発生したボリュームの修復を再試行します 83930030303133434：

```
repair-data start-ec-volume-repair --repair-id 83930030303133434
```

関連情報

"トラブルシューティングを監視します"

アプライアンスストレージノードのリカバリ後のストレージの状態の確認

## アプライアンスストレージノードをリカバリしたら、アプライアンスストレージノードに必要とされる状態が「 Online 」に設定されていることを確認し、ストレージノードサーバが再起動するたびにオンライン状態になるようにする必要があります。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- ストレージノードがリカバリされ、データリカバリが完了している必要があります。

手順

1. Support **>** Tools **>** Grid Topology *を選択します。
2. リカバリされたストレージノード* LDR * Storage * **Storage State - Desired** *および Storage State - Current *の値を確認します。

   両方の属性の値が Online である必要があります。

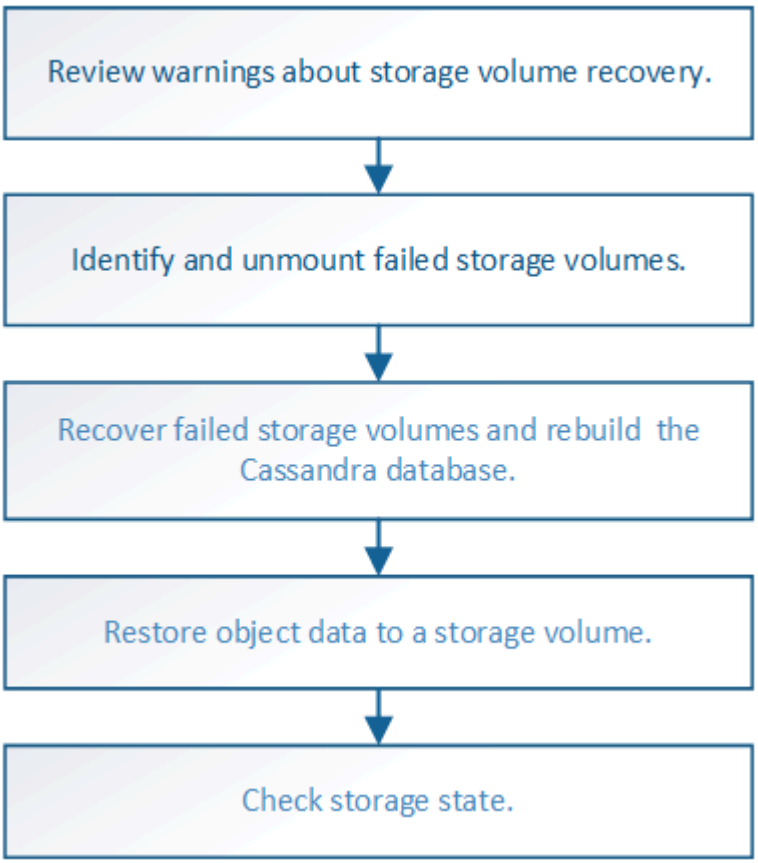
3. Storage State --Desired が Read-Only に設定されている場合は、次の手順を実行します。
   a. [* 構成 *] タブをクリックします。
   b. [* Storage State] — [Desired *] ( 保存状態 — 希望する *)] ドロップダウンリストから [*Online] ( オンライン ) を選択します。
   c. [ 変更の適用 *] をクリックします。
   d. [* 概要 **]** タブをクリックし、 **[** ストレージ状態 **--Desired** * および * ストレージ状態 **--current** ] の値が [ オンライン ] に更新されていることを確認します。

システムドライブに損傷がない場合のストレージボリューム障害からのリカバリ

## ストレージノードで 1 個以上のストレージボリュームに障害が発生したものの、システムドライブに損傷がない場合は、一連のタスクを実行してソフトウェアベースのストレージノードをリカバリする必要があります。ストレージボリュームだけで障害が発生した場合は、ストレージノードを引き続き StorageGRID システムで使用できます。

このタスクについて

このリカバリ用 手順 環境 ソフトウェアベースのストレージノードのみ。アプライアンス・ストレージ・ノードでストレージ・ボリュームに障害が発生した場合は、手順 を使用して「StorageGRID アプライアンス・ストレージ・ノードのリカバリ」を実行してください。




関連情報

"StorageGRID アプライアンスストレージノードのリカバリ"

手順

- "ストレージボリュームのリカバリに関する警告を確認しています"
- "障害ストレージボリュームを特定し、アンマウントします"
- "障害ストレージボリュームのリカバリとCassandraデータベースの再構築"
- "システムドライブに損傷がない場合のストレージボリュームへのオブジェクトデータのリストア"
- "ストレージボリュームのリカバリ後のストレージの状態の確認"

ストレージボリュームのリカバリに関する警告を確認しています

## ストレージノードの障害ストレージボリュームをリカバリする前に、次の警告を確認する必要があります。

ストレージノード内のストレージボリューム（ rangedb ）は、ボリューム ID と呼ばれる 16 進数で識別されます。たとえば、 0000 は最初のボリューム、 000F は 16 番目のボリュームです。各ストレージノードの最初のオブジェクトストア（ボリューム 0 ）は、オブジェクトメタデータと Cassandra データベースの処理に最大 4TB のスペースを使用します。このボリュームの残りのスペースはオブジェクトデータに使用されま

す。他のすべてのストレージボリュームは、オブジェクトデータ専用のボリュームです。

ボリューム 0 で障害が発生してリカバリが必要な場合は、ボリュームリカバリ手順 の一部として Cassandra データベースの再構築が必要になることがあります。次の状況でも、 Cassandra が再構築されることがあります。

- ストレージノードが 15 日以上オフラインになったあと、オンラインに戻ります。
- システムドライブと 1 つ以上のストレージボリュームで障害が発生し、リカバリされた。

Cassandra の再構築時、システムは他のストレージノードからの情報を使用します。オフラインのストレージノードが多すぎると、一部の Cassandra データを使用できない可能性があります。最近 Cassandra が再構築された場合は、 Cassandra データの一貫性がまだグリッド全体で確保されていないことがあります。オフラインのストレージノードが多すぎる場合や複数のストレージノードが 15 日以内に再構築されている場合は、データ損失が発生する可能性があります。

> 複数のストレージノードで障害が発生した場合（またはオフラインの場合）は、テクニカルサポートにお問い合わせください。次のリカバリ手順 は実行しないでください。データが失われる可能性があります。

> ストレージノードの障害またはリカバリ後 15 日以内に 2 つ目のストレージノードの障害が発生した場合は、テクニカルサポートにお問い合わせください。15 日以内に複数のストレージノードで Cassandra を再構築すると、データが失われることがあります。

> サイトの複数のストレージノードで障害が発生した場合は、サイトリカバリ手順 が必要になる可能性があります。テクニカルサポートにお問い合わせください。

"テクニカルサポートによるサイトリカバリの実行方法"

> レプリケートコピーを 1 つだけ保存するように ILM ルールを設定している場合に、そのコピーがあるストレージボリュームで障害が発生すると、オブジェクトをリカバリできません。

> リカバリ中に Services ： Status - Cassandra （ SVST ）アラームが発生した場合は、監視とトラブルシューティングの手順を参照して、 Cassandra を再構築してアラームからリカバリしてください。Cassandra を再構築すると、アラームは解除されます。アラームが解除されない場合は、テクニカルサポートに連絡してください。

関連情報

"トラブルシューティングを監視します"

"グリッドノードのリカバリに関する警告と考慮事項"

障害ストレージボリュームを特定し、アンマウントします

ストレージボリュームに障害が発生したストレージノードをリカバリする場合は、障害ボリュームを特定し、アンマウントする必要があります。障害ストレージボリュームのみがリカバリ手順 で再フォーマットされることを確認する必要があります。

必要なもの

Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

このタスクについて

障害が発生したストレージボリュームはできるだけ早くリカバリする必要があります。

まず最初に、接続解除されたボリューム、アンマウントが必要なボリューム、または I/O エラーが発生しているボリュームを検出します。障害ボリュームがランダムに破損したファイルシステムを含んでいる状態で接続されている場合は、ディスクの未使用部分または未割り当て部分の破損をシステムが検出できないことがあります。

ディスクの追加や再接続、ノードの停止、ノードの開始、リブートなど、ボリュームをリカバリするための手動手順を実行する前に、この手順 を完了しておく必要があります。それ以外の場合は、を実行したときに `reformat_storage_block_devices.rb` スクリプトでファイルシステムエラーが発生し、スクリプトがハングしたり失敗したりする場合があります。

を実行する前に、ハードウェアを修理し、ディスクを適切に接続します `reboot` コマンドを実行します

障害ストレージボリュームは慎重に特定してください。この情報を使用して、再フォーマットが必要なボリュームを確認します。ボリュームを再フォーマットすると、そのボリュームのデータはリカバリできません。

障害ストレージボリュームを正しくリカバリするには、障害ストレージボリュームのデバイス名とそのボリューム ID の両方を把握しておく必要があります。

インストール時に、各ストレージデバイスにはファイルシステムの Universal Unique Identifier （ UUID ）が割り当てられ、その UUID を使用してストレージノードの rangedb ディレクトリにマウントされます。ファイルシステムのUUIDとrangedbディレクトリは、に記載されています `/etc/fstab` ファイル。デバイス名、rangedb ディレクトリ、およびマウントされたボリュームのサイズは、 Grid Manager に表示されます。

次の例では、deviceです `/dev/sdc` には4TBのボリュームがマウントされています `/var/local/rangedb/0`デバイス名を使用します `/dev/disk/by-uuid/822b0547-3b2b-472e-ad5e-e1cf1809faba` を参照してください `/etc/fstab` ファイル：

手順

1. 次の手順を実行して、障害ストレージボリュームとそのデバイス名を記録します。

   a. Support **>** Tools **>** Grid Topology *を選択します。

   b. 「* site * failed Storage Node **LDR * Storage** Overview ** Main *」を選択し、アラームが発生しているオブジェクトストアを探します。

**Object Stores**

| ID | Total | Available | Stored Data | Stored (%) | Health |
|---|---|---|---|---|---|
| 0000 | 96.6 GB | 96.6 GB | 823 KB | 0.001 % | Error |
| 0001 | 107 GB | 107 GB | 0 B | 0 % | No Errors |
| 0002 | 107 GB | 107 GB | 0 B | 0 % | No Errors |

   c. 「* site * failed Storage Node **SSM * Resources * Overview** Main *」を選択します。前の手順で特定した各障害ストレージボリュームのマウントポイントとボリュームサイズを確認します。

   オブジェクトストアには、 16 進表記の番号が付けられています。たとえば、 0000 は最初のボリューム、 000F は 16 番目のボリュームです。この例では、IDが0000のオブジェクトストアはに対応しています `/var/local/rangedb/0` デバイス名がsdcで、サイズが107GBの場合。

**Volumes**

| Mount Point | Device | Status | Size | Space Available | Total Entries | Entries Available | Write Cache |
|---|---|---|---|---|---|---|---|
| / | croot | Online | 10.4 GB | 4.17 GB | 655,360 | 554,806 | Unknown |
| /var/local | cvloc | Online | 96.6 GB | 96.1 GB | 94,369,792 | 94,369,423 | Unknown |
| /var/local/rangedb/0 | sdc | Online | 107 GB | 107 GB | 104,857,600 | 104,856,202 | Enabled |
| /var/local/rangedb/1 | sdd | Online | 107 GB | 107 GB | 104,857,600 | 104,856,536 | Enabled |
| /var/local/rangedb/2 | sde | Online | 107 GB | 107 GB | 104,857,600 | 104,856,536 | Enabled |

2. 障害が発生したストレージノードにログインします。

   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`

   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。

   c. 次のコマンドを入力してrootに切り替えます。 `su -`

   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

   rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

3. 次のスクリプトを実行してストレージサービスを停止し、障害ストレージボリュームをアンマウントします。

```
sn-unmount-volume object_store_ID
```

   。 `object_store_ID` は、障害ストレージボリュームのIDです。たとえば、と指定します `0` IDが0000のオブジェクトストアのコマンド。

4. プロンプトが表示されたら、 * y * を押してストレージノード上のストレージサービスを停止します。

ストレージサービスがすでに停止している場合は、プロンプトは表示されません。Cassandra サービスは、ボリューム 0 に対してのみ停止します。

```
root@Storage-180:~ # sn-unmount-volume 0
Storage services (ldr, chunk, dds, cassandra) are not down.
Storage services must be stopped before running this script.
Stop storage services [y/N]? y
Shutting down storage services.
Storage services stopped.
Unmounting /var/local/rangedb/0
/var/local/rangedb/0 is unmounted.
```

数秒後にストレージサービスが停止し、ボリュームがアンマウントされます。プロセスの各ステップを示すメッセージが表示されます。最後のメッセージは、ボリュームがアンマウントされたことを示しています。

障害ストレージボリュームのリカバリと**Cassandra**データベースの再構築

## 障害が発生したストレージボリュームでストレージを再フォーマットして再マウントするスクリプトを実行し、システムが必要であると判断した場合にはストレージノードの Cassandra データベースを再構築する必要があります。

- を用意しておく必要があります `Passwords.txt` ファイル。
- サーバ上のシステムドライブに損傷がないことが必要です。
- 障害の原因 を特定し、必要に応じて交換用ストレージハードウェアを入手しておく必要があります。
- 交換用ストレージの合計サイズは、元のストレージと同じである必要があります。
- ストレージノードの運用停止処理が進行中でないこと、またはノードの手順 の運用停止処理が一時停止されていることを確認しておきます（Grid Managerで、* Maintenance * Maintenance Tasks * Decommission *を選択します）。
- 拡張が進行中でないことを確認しておきます（Grid Managerで、* Maintenance * Maintenance Tasks * Expansion *を選択します。）
- ストレージボリュームのリカバリに関する警告を確認しておく必要があります。

  "ストレージボリュームのリカバリに関する警告を確認しています"

  a. 必要に応じて、前述の手順で特定してアンマウントした障害ストレージボリュームに関連付けられた、障害が発生した物理または仮想ストレージを交換します。

     ストレージを交換したら、オペレーティングシステムによって認識されるようにストレージを再スキャンまたはリブートします。ただし、ボリュームは再マウントしないでください。ストレージが再マウントされてに追加されます `/etc/fstab` 後の手順で実行します。

  b. 障害が発生したストレージノードにログインします。

i. 次のコマンドを入力します。 `ssh admin@grid_node_IP`

ii. に記載されているパスワードを入力します `Passwords.txt` ファイル。

iii. 次のコマンドを入力してrootに切り替えます。 `su -`

iv. に記載されているパスワードを入力します `Passwords.txt` ファイル。

rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

c. テキストエディタ（viまたはvim）を使用して、から障害ボリュームを削除します `/etc/fstab` ファイルを選択し、ファイルを保存します。

で障害ボリュームをコメントアウトします `/etc/fstab` ファイルが不十分です。ボリュームをから削除する必要があります `fstab` を使用してリカバリ処理を実行すると、のすべての行が検証されます `fstab` マウントされたファイルシステムとファイルが一致している。

d. 障害ストレージボリュームを再フォーマットし、必要に応じて Cassandra データベースを再構築します。入力するコマンド `reformat_storage_block_devices.rb`

- ストレージサービスが実行されている場合は、それらを停止するように求められます。「 * y * 」と入力します
- 必要に応じて Cassandra データベースを再構築するよう求められます。
  - 警告を確認します。いずれの状況も該当しない場合は、 Cassandra データベースを再構築します。「 * y * 」と入力します
  - 複数のストレージノードがオフラインの場合、または別のストレージノードが 15 日以内に再構築されている場合は、「 * n * 」と入力します

    スクリプトは Cassandra を再構築せずに終了します。テクニカルサポートにお問い合わせください。
- ストレージノード上の各rangedbドライブについて尋ねられたときは、次のようになります。 `Reformat the rangedb drive <name> (device <major number>:<minor number>)? [y/n]?`で、次のいずれかの応答を入力します。
  - * y * ：エラーが発生したドライブを再フォーマットします。ストレージボリュームが再フォーマットされ、にストレージボリュームが追加されます `/etc/fstab` ファイル。
  - *n * ドライブにエラーがなく、ドライブを再フォーマットしない場合。

*n * を選択すると、スクリプトが終了します。ドライブをマウントするか（ドライブ上のデータを保持する必要があり、ドライブが誤ってアンマウントされた場合）、ドライブを取り外します。次に、を実行します `reformat_storage_block_devices.rb` コマンドをもう一度実行します。

一部の StorageGRID リカバリ手順では、 Reaper を使用して Cassandra の修復を処理します。関連サービスまたは必要なサービスが開始されるとすぐに修理が自動的に行われます。スクリプトの出力には、「 reaper 」または「 Cassandra repair 」が含まれていることがあります。 修復が失敗したことを示すエラーメッセージが表示された場合は、エラーメッセージに示されたコマンドを実行します。

次の出力例では、ドライブが表示されています `/dev/sdf` 再フォーマットが必要で、Cassandraを再構築する必要はありませんでした。

```
root@DC1-S1:~ # reformat_storage_block_devices.rb
Storage services must be stopped before running this script.
Stop storage services [y/N]? **y**
Shutting down storage services.
Storage services stopped.
Formatting devices that are not in use...
Skipping in use device /dev/sdc
Skipping in use device /dev/sdd
Skipping in use device /dev/sde
Reformat the rangedb drive /dev/sdf (device 8:64)? [Y/n]? **y**
Successfully formatted /dev/sdf with UUID c817f87f-f989-4a21-8f03-
b6f42180063f
Skipping in use device /dev/sdg
All devices processed
Running: /usr/local/ldr/setup_rangedb.sh 12075630
Cassandra does not need rebuilding.
Starting services.

Reformatting done.  Now do manual steps to
restore copies of data.
```

関連情報

"ストレージボリュームのリカバリに関する警告を確認しています"

システムドライブに損傷がない場合のストレージボリュームへのオブジェクトデータのリストア

## システムドライブに損傷がないストレージノードでストレージボリュームをリカバリしたら、ストレージボリュームの障害で失われたオブジェクトデータをリストアできます。

必要なもの

- リカバリされたストレージノードの接続状態が * connected * であることを確認しておく必要があります✔ Grid Managerの* Nodes > Overview *タブ。

このタスクについて

グリッドの ILM ルールがオブジェクトコピーを作成するように設定されていた場合、他のストレージノード、アーカイブノード、またはクラウドストレージプールからオブジェクトデータをリストアできます。

> ⓘ レプリケートされたコピーを 1 つだけ保存するように ILM ルールが設定されていて、そのコピーがストレージボリュームに障害が発生した場合、オブジェクトをリカバリすることはできません。

オブジェクトのコピーがクラウドストレージプールにしか残っていない場合、 StorageGRID は、オブジェクトデータをリストアするために複数の要求をクラウドストレージプールエンドポイントに問題 する必要があります。この手順 を実行する前に、テクニカルサポートに問い合わせて、リカバリ期間と関連コストの見積もりを依頼してください。

オブジェクトのコピーがアーカイブノードにしか残っていない場合は、アーカイブノードからオブジェクトデータが読み出されます。外部アーカイブストレージシステムからの読み出しには遅延が伴うため、アーカイブノードからストレージノードへのオブジェクトデータのリストアには、他のストレージノードからコピーをリストアする場合に比べて時間がかかります。

オブジェクトデータをリストアするには、を実行します `repair-data` スクリプト：このスクリプトは、オブジェクトデータのリストアプロセスを開始し、 ILM スキャンと連動して ILM ルールを適用します。では、さまざまなオプションを使用します `repair-data` 次の方法で、レプリケートデータとイレイジャーコーディングデータのどちらをリストアするかに基づくスクリプトです。

- レプリケートデータ：レプリケートデータをリストアするコマンドは、ノード全体を修復するのか、ノード上の一部のボリュームのみを修復するのかに応じて2つあります。

```
repair-data start-replicated-node-repair
```

```
repair-data start-replicated-volume-repair
```

- イレイジャーコーディング（**EC**）データ：イレイジャーコーディングデータをリストアするコマンドは、ノード全体を修復するのか、ノード上の一部のボリュームのみを修復するのかに応じて2つあります。

```
repair-data start-ec-node-repair
```

```
repair-data start-ec-volume-repair
```

イレイジャーコーディングデータの修復は、一部のストレージノードがオフライン状態で開始できます。修復はすべてのノードが使用可能になったあとに完了します。次のコマンドを使用して、イレイジャーコーディングデータの修復を追跡できます。

```
repair-data show-ec-repair-status
```

EC 修復ジョブによって、大量のストレージが一時的にリザーブされます。ストレージアラートがトリガーされることもありますが、修復が完了すると解決します。予約に必要なストレージが不足していると、 EC の修復ジョブが失敗します。ストレージリザベーションは、ジョブが失敗したか成功したかに関係なく、 EC 修復ジョブが完了すると解放されます。

を使用する方法の詳細については、を参照してください `repair-data` スクリプトを入力します `repair-`

`data --help` プライマリ管理ノードのコマンドラインを使用します。

手順

1. プライマリ管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

   rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。
2. を使用します `/etc/hosts` リストアされたストレージボリュームのストレージノードのホスト名を特定するファイル。グリッド内のすべてのノードのリストを表示するには、次のように入力します。 `cat /etc/hosts`
3. すべてのストレージボリュームで障害が発生した場合は、ノード全体を修復します。（一部のボリュームだけで障害が発生した場合は、次の手順に進みます）。

   を実行できません `repair-data` 複数のノードに対して同時に処理を実行すること。複数のノードをリカバリする場合は、テクニカルサポートにお問い合わせください。

   - グリッドにレプリケートデータがある場合は、を使用します `repair-data start-replicated-node-repair` コマンドにを指定します `--nodes` ストレージノード全体を修復するオプションです。

     次のコマンドは、 SG-DC-SN3 というストレージノードにあるレプリケートデータを修復します。

     ```
     repair-data start-replicated-node-repair --nodes SG-DC-SN3
     ```

     オブジェクトデータのリストア時、 StorageGRID システムがレプリケートされたオブジェクトデータを見つけられない場合は、 * Objects lost * アラートがトリガーされます。システム全体のストレージノードでアラートがトリガーされることがあります。損失の原因 と、リカバリが可能かどうかを確認する必要があります。StorageGRID の監視とトラブルシューティングの手順を参照してください。

   - グリッドにイレイジャーコーディングデータがある場合は、を使用します `repair-data start-ec-node-repair` コマンドにを指定します `--nodes` ストレージノード全体を修復するオプションです。

     次のコマンドは、SG-DC-SN3というストレージノードにあるイレイジャーコーディングデータを修復します。

     ```
     repair-data start-ec-node-repair --nodes SG-DC-SN3
     ```

     一意のが返されます `repair ID` これを識別します `repair_data` 操作。これを使用します `repair ID` をクリックして、の進捗状況と結果を追跡します `repair_data` 操作。リカバリプロセスが完了しても、それ以外のフィードバックは返されません。

イレイジャーコーディングデータの修復は、一部のストレージノードがオフライン状態で開始できます。修復はすべてのノードが使用可能になったあとに完了します。

- グリッドにレプリケートデータとイレイジャーコーディングデータの両方がある場合は、両方のコマンドを実行します。

4. 一部のボリュームだけで障害が発生した場合は、影響を受けたボリュームを修復します。

ボリューム ID を 16 進数で入力します。例： `0000` は、最初のボリュームとです `000F` 16番目のボリュームです。1 つのボリューム、一連のボリューム、または連続していない複数のボリュームを指定できます。

すべてのボリュームが同じストレージノードにある必要があります。複数のストレージノードのボリュームをリストアする必要がある場合は、テクニカルサポートにお問い合わせください。

- グリッドにレプリケートデータがある場合は、を使用します `start-replicated-volume-repair` コマンドにを指定します `--nodes` ノードを識別するオプション。次に、を追加します `--volumes` または `--volume-range` 次の例に示すように、オプションを指定します。

  単一ボリューム：レプリケートされたデータをボリュームにリストアします `0002` SG-DC-SN3という名前のストレージノードで次のように設定します。

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3
--volumes 0002
```

  ボリューム範囲：レプリケートされたデータを範囲内のすべてのボリュームにリストアします `0003` 終了： `0009` SG-DC-SN3という名前のストレージノードで次のように設定します。

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume
-range 0003-0009
```

  複数のボリュームが連続していません：このコマンドは、複製されたデータをボリュームにリストアします `0001`、 `0005`および `0008` SG-DC-SN3という名前のストレージノードで次のように設定します。

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3
--volumes 0001,0005,0008
```

  オブジェクトデータのリストア時、 StorageGRID システムがレプリケートされたオブジェクトデータを見つけられない場合は、 * Objects lost * アラートがトリガーされます。システム全体のストレージノードでアラートがトリガーされることがあります。損失の原因 と、リカバリが可能かどうかを確認する必要があります。StorageGRID の監視とトラブルシューティングの手順を参照してください。

- グリッドにイレイジャーコーディングデータがある場合は、を使用します `start-ec-volume-repair` コマンドにを指定します `--nodes` ノードを識別するオプション。次に、を追加します `--volumes` または `--volume-range` 次の例に示すように、オプションを指定します。

単一ボリューム：イレイジャーコーディングされたデータをボリュームにリストアします `0007` SG-DC-SN3という名前のストレージノードで次のように設定します。

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 0007
```

ボリューム範囲：イレイジャーコーディングされたデータを範囲内のすべてのボリュームにリストアします `0004` 終了： `0006` SG-DC-SN3という名前のストレージノードで次のように設定します。

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range
0004-0006
```

複数のボリュームが連続していません：このコマンドはイレイジャーコーディングされたデータをボリュームにリストアします `000A`、 `000C`および `000E` SG-DC-SN3という名前のストレージノードで次のように設定します。

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes
000A,000C,000E
```

。 `repair-data` 一意のが返されます `repair ID` これを識別します `repair_data` 操作。これを使用します `repair ID` をクリックして、の進捗状況と結果を追跡します `repair_data` 操作。リカバリプロセスが完了しても、それ以外のフィードバックは返されません。

> イレイジャーコーディングデータの修復は、一部のストレージノードがオフライン状態で開始できます。修復はすべてのノードが使用可能になったあとに完了します。

- グリッドにレプリケートデータとイレイジャーコーディングデータの両方がある場合は、両方のコマンドを実行します。

5. レプリケートデータの修復を監視します。
   a. 「* Nodes > Storage Node being repaired > ILM *」を選択します。
   b. 「評価」セクションの属性を使用して、修理が完了したかどうかを判断します。

      修復が完了すると、Awaiting - All属性は0個のオブジェクトを示します。

   c. 修復の詳細を監視するには、* Support > Tools > Grid Topology *を選択します。
   d. 「* grid > Storage Node being repaired > LDR > Data Store *」を選択します。
   e. 次の属性を組み合わせて、レプリケートデータの修復が完了したかどうかを可能なかぎり判別します。

      > Cassandra に不整合が生じている可能性があり、また、失敗した修復は追跡されません。

      - * Repairs Attempted （ XRPA ） * ：レプリケートデータの修復の進行状況を追跡します。この属性は、ストレージノードがハイリスクオブジェクトの修復を試みるたびに値が増分します。この属性の値が現在のスキャン期間（ * Scan Period - - Estimated * 属性で指定）よりも長い期間にわ

たって上昇しない場合、 ILM スキャンはすべてのノードで修復が必要なハイリスクオブジェクトを検出していません。

> ハイリスクオブジェクトとは、完全に失われる危険があるオブジェクトです。ILM 設定を満たしていないオブジェクトは含まれません。

- * スキャン期間 - 推定（ XSCM ） * ：この属性を使用して、以前に取り込まれたオブジェクトにポリシー変更が適用されるタイミングを見積もります。「 * Repairs Attempted * 」属性が現在のスキャン期間よりも長くなっていない場合は、複製修復が実行されている可能性があります。スキャン期間は変わる可能性があるので注意してください。* Scan Period - - Estimated （ XSCM ） * 属性は、グリッド全体の環境 を示します。これは、すべてのノードのスキャン期間の最大値です。グリッドの * Scan Period - - Estimated * 属性履歴を照会して、適切な期間を判断できます。

6. イレイジャーコーディングデータの修復を監視し、失敗した可能性のある要求を再試行します。

   a. イレイジャーコーディングデータの修復ステータスを確認します。

      - 特定ののののステータスを表示するには、このコマンドを使用します `repair-data` 操作：

      ```
      repair-data show-ec-repair-status --repair-id repair ID
      ```

      - すべての修復処理を表示するには、次のコマンドを使用します

      ```
      repair-data show-ec-repair-status
      ```

      出力には、などの情報が表示されます `repair ID`以前に、現在実行中のすべての修復。

```
root@DC1-ADM1:~ # repair-data show-ec-repair-status

 Repair ID Scope  Start Time  End Time  State  Est Bytes
Affected/Repaired Retry Repair
=============================================================================
==================
 949283 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:27:06.9 Success 17359
17359 No
 949292 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:37:06.9 Failure 17359
0     Yes
 949294 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:47:06.9 Failure 17359
0     Yes
 949299 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:57:06.9 Failure 17359
0     Yes
```

   b. 失敗した修復処理が出力された場合は、を使用します `--repair-id` 修復を再試行するオプションです。

      次のコマンドは、修復ID 83930030303133434を使用して、障害が発生したノードの修復を再試行し

ます。

```
repair-data start-ec-node-repair --repair-id 83930030303133434
```

次のコマンドは、修復ID 83930030303133434を使用して、障害が発生したボリュームの修復を再試行します。

```
repair-data start-ec-volume-repair --repair-id 83930030303133434
```

関連情報

"StorageGRID の管理"

"トラブルシューティングを監視します"

ストレージボリュームのリカバリ後のストレージの状態の確認

## ストレージボリュームをリカバリしたら、ストレージノードに必要とされる状態が「 Online 」に設定されていることを確認し、ストレージノードサーバが再起動するたびにオンライン状態になるようにする必要があります。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- ストレージノードがリカバリされ、データリカバリが完了している必要があります。

手順

1. Support **>** Tools **>** Grid Topology *を選択します。
2. リカバリされたストレージノード* LDR * Storage * **Storage State - Desired** *および Storage State - Current *の値を確認します。

   両方の属性の値が Online である必要があります。

3. Storage State --Desired が Read-Only に設定されている場合は、次の手順を実行します。
   a. [* 構成 *] タブをクリックします。
   b. [* Storage State] — [Desired *] ( 保存状態 — 希望する *)] ドロップダウンリストから [*Online] ( オンライン ) を選択します。
   c. [ 変更の適用 *] をクリックします。
   d. [* 概要 **]** タブをクリックし、 **[** ストレージ状態 **--Desired** * および * ストレージ状態 **--current** ] の値が [ オンライン ] に更新されていることを確認します。

システムドライブ障害からのリカバリ

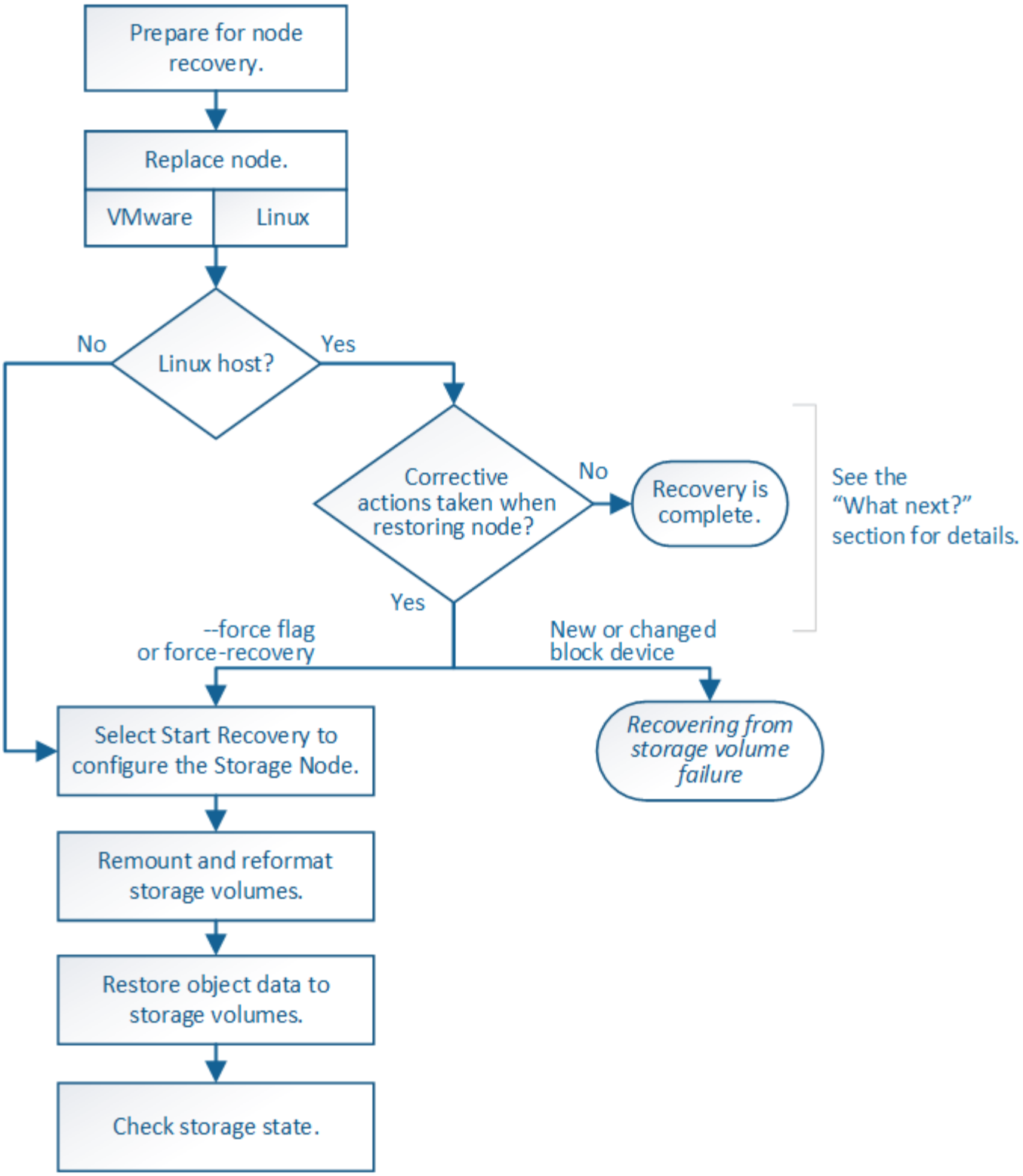
## ソフトウェアベースのストレージノードのシステムドライブで障害が発生すると、そのストレージノードは StorageGRID システムで使用できなくなります。システムドライブの障害からリカバリするには、特定のタスクを実行する必要があります。

このタスクについて

この手順 を使用して、ソフトウェアベースのストレージノードでシステムドライブ障害が発生した場合にリカバリします。この手順 には、障害が発生したストレージボリュームや再マウントできないストレージボリュームがある場合の手順も含まれています。

> この 手順 環境 ソフトウェアベースのストレージノードのみ。アプライアンスストレージノードをリカバリするには、別の手順 に従う必要があります。

"StorageGRID アプライアンスストレージノードのリカバリ"




手順

- "ストレージノードのシステムドライブのリカバリに関する警告の確認"
- "ストレージノードの交換"
- "Start Recoveryを選択して、ストレージノードを設定します"
- "ストレージ・ボリュームの再マウントと再フォーマット（手動手順）"

- "必要に応じたストレージボリュームへのオブジェクトデータのリストア"
- "ストレージノードシステムドライブのリカバリ後のストレージの状態の確認"

ストレージノードのシステムドライブのリカバリに関する警告の確認

## ストレージノードの障害システムドライブをリカバリする前に、次の警告を確認する必要があります。

ストレージノードには、オブジェクトメタデータを含む Cassandra データベースがあります。次の状況では、 Cassandra データベースが再構築されることがあります。

- ストレージノードが 15 日以上オフラインになったあと、オンラインに戻ります。
- ストレージボリュームで障害が発生し、リカバリされた。
- システムドライブと 1 つ以上のストレージボリュームで障害が発生し、リカバリされた。

Cassandra の再構築時、システムは他のストレージノードからの情報を使用します。オフラインのストレージノードが多すぎると、一部の Cassandra データを使用できない可能性があります。最近 Cassandra が再構築された場合は、 Cassandra データの一貫性がまだグリッド全体で確保されていないことがあります。オフラインのストレージノードが多すぎる場合や複数のストレージノードが 15 日以内に再構築されている場合は、データ損失が発生する可能性があります。

複数のストレージノードで障害が発生した場合（またはオフラインの場合）は、テクニカルサポートにお問い合わせください。次のリカバリ手順 は実行しないでください。データが失われる可能性があります。

ストレージノードの障害またはリカバリ後 15 日以内に 2 つ目のストレージノードの障害が発生した場合は、テクニカルサポートにお問い合わせください。15 日以内に複数のストレージノードで Cassandra を再構築すると、データが失われることがあります。

サイトの複数のストレージノードで障害が発生した場合は、サイトリカバリ手順 が必要になる可能性があります。テクニカルサポートにお問い合わせください。

"テクニカルサポートによるサイトリカバリの実行方法"

このストレージノードが、障害ストレージボリュームがある別のストレージノードにオブジェクトを読み出せるように読み取り専用メンテナンスモードになっている場合は、障害ストレージボリュームがあるそのストレージノードでボリュームをリカバリしてから、この障害ストレージノードをリカバリします。システムドライブに損傷がない場合のストレージボリューム損失からのリカバリ手順を参照してください。

レプリケートコピーを 1 つだけ保存するように ILM ルールを設定している場合に、そのコピーがあるストレージボリュームで障害が発生すると、オブジェクトをリカバリできません。

リカバリ中に Services ： Status - Cassandra （ SVST ）アラームが発生した場合は、監視とトラブルシューティングの手順を参照して、 Cassandra を再構築してアラームからリカバリしてください。Cassandra を再構築すると、アラームは解除されます。アラームが解除されない場合は、テクニカルサポートに連絡してください。

関連情報

"トラブルシューティングを監視します"

"グリッドノードのリカバリに関する警告と考慮事項"

"システムドライブに損傷がない場合のストレージボリューム障害からのリカバリ"

ストレージノードの交換

## システムドライブで障害が発生した場合は、最初にストレージノードを交換する必要があります。

使用しているプラットフォームに対応するノード交換用手順 を選択する必要があります。ノードの交換手順は、すべてのタイプのグリッドノードで同じです。

この 手順 環境 ソフトウェアベースのストレージノードのみ。アプライアンスストレージノードをリカバリするには、別の手順 に従う必要があります。

"StorageGRID アプライアンスストレージノードのリカバリ"

- Linux ： * システムドライブで障害が発生したかどうかが不明な場合は、ノードの交換手順に従って、必要なリカバリ手順を確認してください。

| プラットフォーム | 手順 |
| --- | --- |
| VMware | "VMwareノードの交換" |
| Linux の場合 | "Linuxノードの交換" |
| OpenStack の機能を使用 | リカバリ処理を対象とした OpenStack 用の仮想マシンディスクファイルおよびスクリプトは、現在は提供されていません。OpenStack 環境で実行されているノードのリカバリが必要な場合は、使用している Linux オペレーティングシステム用のファイルをダウンロードしてください。その後、手順 に従って Linux ノードを交換します。 |

**Start Recovery**を選択して、ストレージノードを設定します

## ストレージノードを交換したら、 Grid Manager で Start Recovery を選択して、障害が発生したノードの代わりとして新しいノードを設定する必要があります。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Maintenance または Root Access 権限が必要です。
- プロビジョニングパスフレーズが必要です。
- 交換用ノードの導入と設定が完了している必要があります。
- イレイジャーコーディングデータの修復ジョブの開始日を把握しておく必要があります。

- ストレージノードが過去 15 日以内に再構築されていないことを確認しておく必要があります。

このタスクについて

ストレージノードが Linux ホストにコンテナとしてインストールされている場合は、次のいずれかに該当する場合にのみこの手順を実行する必要があります。

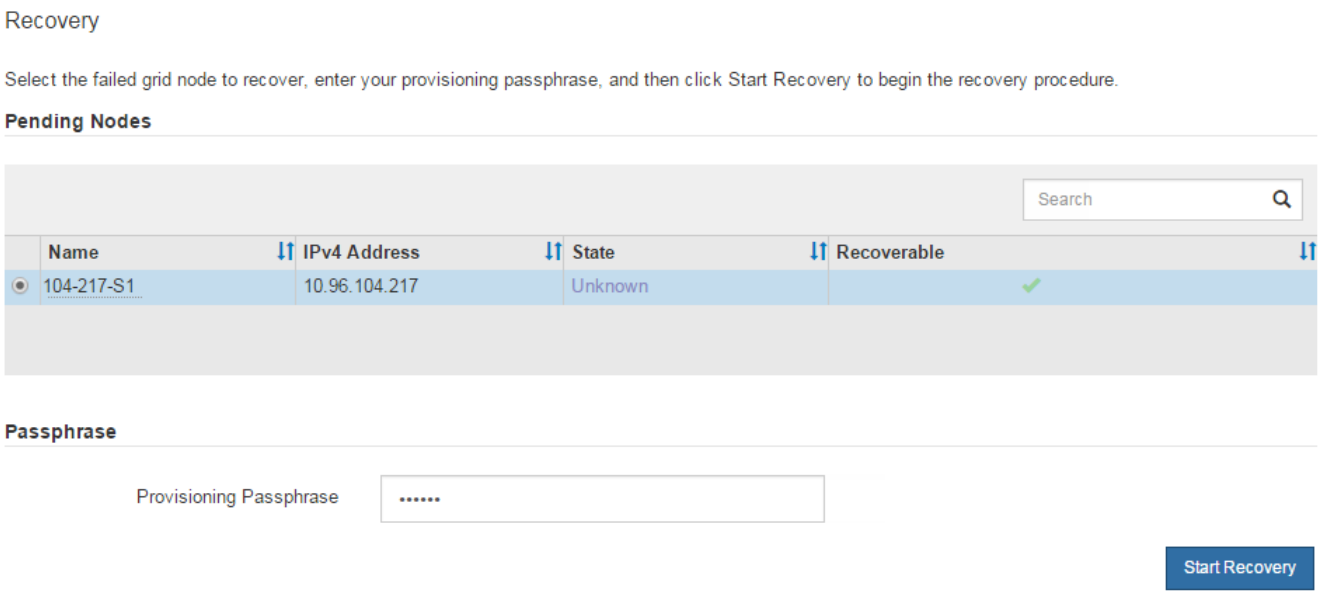
- を使用する必要がありました `--force` ノードをインポートするためのフラグ、またはを実行した `storagegrid node force-recovery node-name`
- ノードの完全な再インストールを実行するか、 /var/local をリストアする必要がありました。

手順

1. Grid Managerから、* Maintenance * Maintenance Tasks * Recovery *（メンテナンス*メンテナンスタスク*リカバリ）を選択します。
2. リカバリするグリッドノードを Pending Nodes リストで選択します。

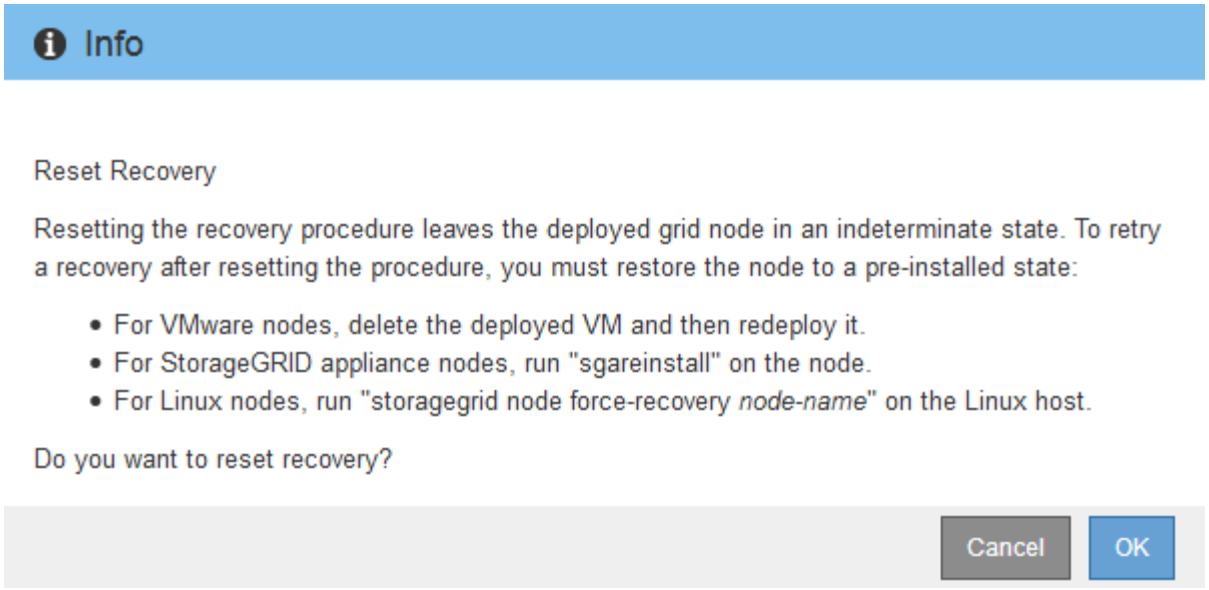
   ノードは障害が発生するとリストに追加されますが、再インストールされてリカバリの準備ができるまでは選択できません。

3. プロビジョニングパスフレーズ * を入力します。
4. [ リカバリの開始 ] をクリックします。




5. リカバリ中のグリッドノードテーブルで、リカバリの進行状況を監視します。

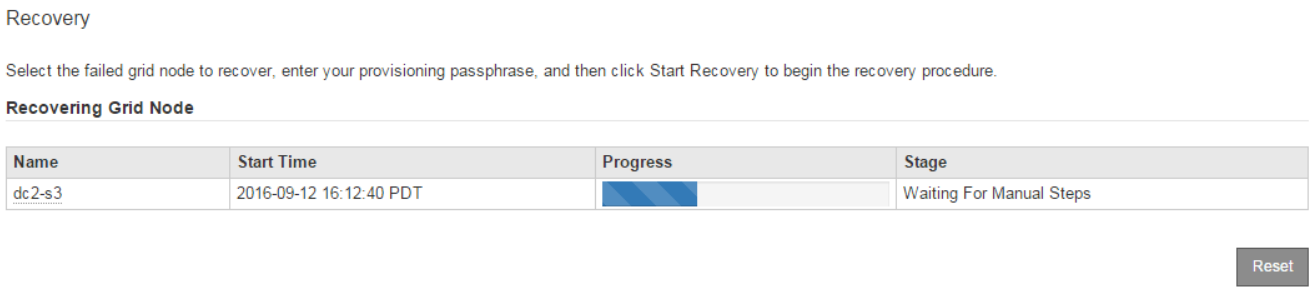
> リカバリ手順 の実行中に [* リセット ] をクリックすると、新しいリカバリを開始できます。情報ダイアログボックスが表示され、手順 をリセットするとノードが不確定な状態のままになることが示されます。




手順 をリセットしたあとにリカバリを再試行する場合は、次の手順でノードをインストール前の状態にリストアする必要があります。

- * vmware * ：導入した仮想グリッドノードを削除します。その後、リカバリを再開する準備ができたら、ノードを再導入します。
- * Linux *：Linuxホストで次のコマンドを実行して、ノードを再起動します。 `storagegrid node force-recovery node-name`

6. ストレージ・ノードが Waiting for Manual Steps ステージに進んだら ' リカバリ手順 の次のタスクに進み ' ストレージ・ボリュームを再マウントして再フォーマットします




関連情報

"再インストールのためのアプライアンスの準備（プラットフォームの交換のみ）"

ストレージボリュームの再マウントと再フォーマット（「手動手順」）

2 つのスクリプトを手動で実行して、保持されているストレージボリュームを再マウントし、障害ストレージボリュームを再フォーマットする必要があります。最初のスクリプトは、 StorageGRID ストレージボリュームとして適切にフォーマットされているボリュームを再マウントします。2 番目のスクリプトは、マウントされていないボリュームを再フォーマットし、必要に応じて Cassandra を再構築してサービスを開始します。

必要なもの

- 障害が発生したストレージボリュームのうち、必要と判断した場合はハードウェアを交換しておく必要があります。

  を実行します `sn-remount-volumes` スクリプトを使用すると、障害ストレージボリュームを追加で特定できる場合があります。

- ストレージノードの運用停止処理が進行中でないこと、またはノードの手順 の運用停止処理が一時停止されていることを確認しておきます（Grid Managerで、* Maintenance * Maintenance Tasks * Decommission *を選択します）。
- 拡張が進行中でないことを確認しておきます（Grid Managerで、* Maintenance * Maintenance Tasks * Expansion *を選択します。）
- ストレージノードのシステムドライブのリカバリに関する警告を確認しておく必要があります。

  "ストレージノードのシステムドライブのリカバリに関する警告の確認"

> 複数のストレージノードがオフラインの場合、またはこのグリッド内のストレージノードが過去 15 日以内に再構築されている場合は、テクニカルサポートにお問い合わせください。を実行しないでください `sn-recovery-postinstall.sh` スクリプト：15 日以内に複数のストレージノードで Cassandra を再構築すると、データが失われることがあります。

このタスクについて

この手順 を完了するには、次の作業を行います。

- リカバリされたストレージノードにログインします。
- を実行します `sn-remount-volumes` 適切にフォーマットされたストレージボリュームを再マウントするスクリプト。このスクリプトを実行すると、次の処理が行われます。
  - 各ストレージボリュームをマウントしてアンマウントし、 XFS ジャーナルをリプレイします。
  - XFS ファイルの整合性チェックを実行します。
  - ファイルシステムに整合性がある場合は、ストレージボリュームが適切にフォーマットされた StorageGRID ストレージボリュームであるかどうかを確認します。
  - ストレージボリュームが適切にフォーマットされている場合は、ストレージボリュームを再マウントします。ボリューム上の既存のデータはそのまま維持されます。
- スクリプトの出力を確認し、問題を解決します。
- を実行します `sn-recovery-postinstall.sh` スクリプト：このスクリプトを実行すると、次の処理が実行されます。

> リカバリの実行中はストレージノードをリブートしないでください `sn-recovery-postinstall.sh` （の手順を参照してください インストール後のスクリプト）障害ストレージボリュームの再フォーマットとオブジェクトメタデータのリストアを行います。実行前にストレージノードをリブートしています `sn-recovery-postinstall.sh` completesを指定すると、サービスが開始しようとするとエラーが発生し、StorageGRID アプライアンスノードが保守モードを終了します。

  - で指定したストレージボリュームを再フォーマットします `sn-remount-volumes` スクリプトをマウントできなかったか、またはスクリプトの形式が正しくありませんでした。

ストレージボリュームを再フォーマットすると、そのボリューム上のデータはすべて失われます。複数のオブジェクトコピーを格納するように ILM ルールが設定されている場合は、グリッド内の他の場所からオブジェクトデータをリストアするために追加の手順 を実行する必要があります。

- 必要に応じて、ノードの Cassandra データベースを再構築します。
- ストレージノードのサービスを開始します。

手順

1. リカバリしたストレージノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

   rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

2. 最初のスクリプトを実行し、適切にフォーマットされたストレージボリュームを再マウントします。

   すべてのストレージボリュームが新規でフォーマットが必要な場合、またはすべてのストレージボリュームで障害が発生した場合は、この手順を省略して 2 つ目のスクリプトを実行し、マウントされていないストレージボリュームをすべて再フォーマットします。

   a. スクリプトを実行します。 `sn-remount-volumes`

      データが格納されたストレージボリュームでこのスクリプトを実行すると、数時間かかることがあります。

   b. スクリプトの実行時に、出力と回答 のプロンプトを確認します。

      必要に応じて、を使用できます `tail -f` スクリプトのログファイルの内容を監視するコマンド (`/var/local/log/sn-remount-volumes.log`) 。ログファイルには、コマンドラインの出力よりも詳細な情報が含まれています。

```
root@SG:~ # sn-remount-volumes
The configured LDR noid is 12632740

====== Device /dev/sdb ======
Mount and unmount device /dev/sdb and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sdb:
Mount device /dev/sdb to /tmp/sdb-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12632740, volume number 0 in the volID file
```

```
Attempting to remount /dev/sdb
Device /dev/sdb remounted successfully

====== Device /dev/sdc ======
Mount and unmount device /dev/sdc and checking file system
consistency:
Error: File system consistency check retry failed on device /dev/sdc.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh,
this volume and any data on this volume will be deleted. If you only
had two
copies of object data, you will temporarily have only a single copy.
StorageGRID Webscale will attempt to restore data redundancy by
making
additional replicated copies or EC fragments, according to the rules
in
the active ILM policy.

Do not continue to the next step if you believe that the data
remaining on
this volume cannot be rebuilt from elsewhere in the grid (for
example, if
your ILM policy uses a rule that makes only one copy or if volumes
have
failed on multiple nodes). Instead, contact support to determine how
to
recover your data.

====== Device /dev/sdd ======
Mount and unmount device /dev/sdd and checking file system
consistency:
Failed to mount device /dev/sdd
This device could be an uninitialized disk or has corrupted
superblock.
File system check might take a long time. Do you want to continue? (y
or n) [y/N]? y

Error: File system consistency check retry failed on device /dev/sdd.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh,
```

```
this volume and any data on this volume will be deleted. If you only
had two
copies of object data, you will temporarily have only a single copy.
StorageGRID Webscale will attempt to restore data redundancy by
making
additional replicated copies or EC fragments, according to the rules
in
the active ILM policy.

Do not continue to the next step if you believe that the data
remaining on
this volume cannot be rebuilt from elsewhere in the grid (for
example, if
your ILM policy uses a rule that makes only one copy or if volumes
have
failed on multiple nodes). Instead, contact support to determine how
to
recover your data.

====== Device /dev/sde ======
Mount and unmount device /dev/sde and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sde:
Mount device /dev/sde to /tmp/sde-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12000078, volume number 9 in the volID file
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

この出力例では、 1 つのストレージボリュームが正常に再マウントされ、 3 つのストレージボリュームでエラーが発生しています。

- `/dev/sdb` は、XFSファイルシステムの整合性チェックに合格し、ボリューム構造が有効なため、正常に再マウントされました。スクリプトによって再マウントされたデバイスのデータは保持されています。
- `/dev/sdc` は、ストレージボリュームが新規または破損していたため、XFSファイルシステムの整合性チェックに合格できませんでした。
- `/dev/sdd` ディスクが初期化されていないか、ディスクのスーパーブロックが破損していたため、をマウントできませんでした。スクリプトは、ストレージボリュームをマウントできない場合、ファイルシステムの整合性チェックを実行するかどうかを確認するメッセージを表示します。
  - ストレージ・ボリュームが新しいディスクに接続されている場合は、回答 * N * をプロンプトに表示します。新しいディスクのファイルシステムをチェックする必要はありません。
  - ストレージ・ボリュームが既存のディスクに接続されている場合は、回答 * Y * がプロンプトに表示されます。ファイルシステムのチェックの結果を使用して、破損の原因を特定できま

す。結果がに保存されます `/var/local/log/sn-remount-volumes.log` ログファイル：

- `/dev/sde` は、XFSファイルシステムの整合性チェックに合格し、ボリューム構造が有効でした。ただし、volIDファイルのLDRノードIDがこのストレージノードのID（）と一致していません `configured LDR noid` 上部に表示）。このメッセージは、このボリュームが別のストレージノードに属していることを示しています。

3. スクリプトの出力を確認し、問題を解決します。

> ストレージボリュームが XFS ファイルシステムの整合性チェックに合格できなかった場合、またはストレージボリュームをマウントできなかった場合は、出力のエラーメッセージをよく確認してください。を実行した場合の影響を理解しておく必要があります `sn-recovery-postinstall.sh` これらのボリュームにスクリプトを設定します。

a. 想定しているすべてのボリュームのエントリが結果に含まれていることを確認します。表示されていないボリュームがある場合は、スクリプトを再実行します。

b. マウントされたすべてのデバイスのメッセージを確認します。ストレージボリュームがこのストレージノードに属していないことを示すエラーがないことを確認します。

この例では、の出力を示します `/dev/sde` には、次のエラーメッセージが含まれます。

```
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

> あるストレージボリュームが別のストレージノードに属していると報告される場合は、テクニカルサポートにお問い合わせください。を実行する場合は、を実行します `sn-recovery-postinstall.sh` スクリプトでは、ストレージボリュームが再フォーマットされますが、原因 のデータが失われることがあります。

c. マウントできなかったストレージデバイスがある場合は、デバイス名をメモし、デバイスを修理または交換します。

> マウントできなかったストレージデバイスはすべて修理または交換する必要があります。

デバイス名を使用してボリュームIDを検索します。このIDは、を実行する際に必要な入力情報です `repair-data` オブジェクトデータをボリューム（次の手順 ）にリストアするスクリプト。

d. マウントできないデバイスをすべて修復または交換したら、を実行します `sn-remount-volumes` もう一度スクリプトを実行して、再マウントできるすべてのストレージボリュームが再マウントされたことを確認します。

> ストレージボリュームをマウントできない場合、またはストレージボリュームが適切にフォーマットされなかった場合に次の手順に進むと、ボリュームとそのボリューム上のデータが削除されます。オブジェクトデータのコピーが 2 つあった場合、次の手順 （オブジェクトデータのリストア）が完了するまでコピーは 1 つだけになります。

を実行しないでください `sn-recovery-postinstall.sh` スクリプト：障害ストレージボリュームに残っているデータをグリッド内の他の場所から再構築することができないと考えられる場合（ILMポリシーでコピーを1つだけ作成するルールが使用されている場合や、複数のノードでボリュームに障害が発生した場合など）。代わりに、テクニカルサポートに問い合わせてデータのリカバリ方法を確認してください。

4. を実行します `sn-recovery-postinstall.sh` スクリプト： `sn-recovery-postinstall.sh`

   このスクリプトは、マウントできなかったストレージボリューム、または適切にフォーマットされていないストレージボリュームを再フォーマットし、必要に応じてノードの Cassandra データベースを再構築して、ストレージノードのサービスを開始します。

   次の点に注意してください。

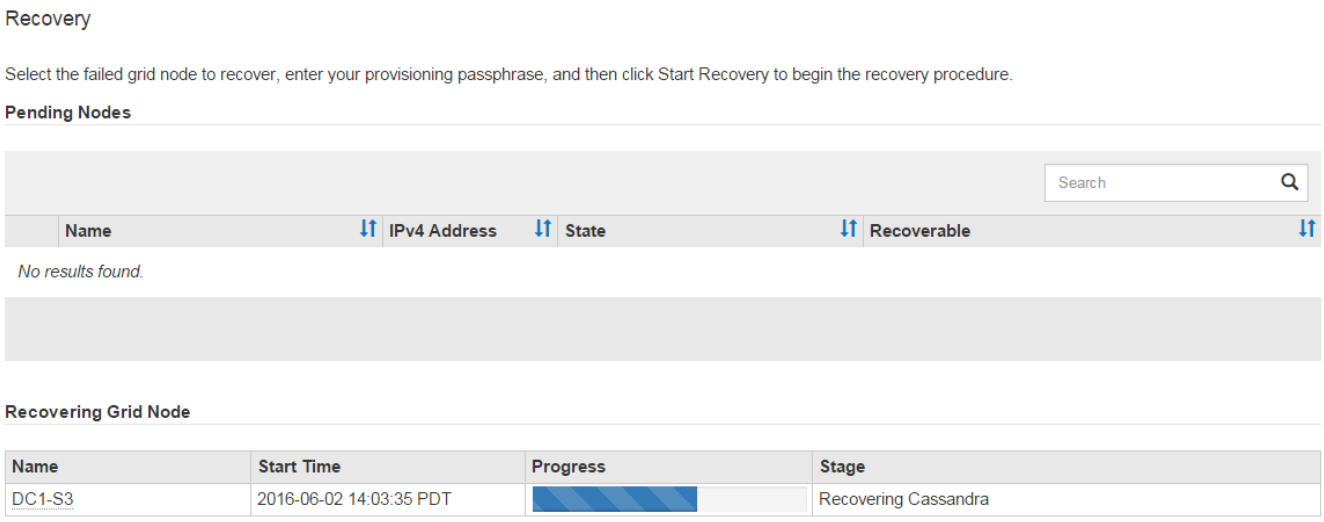
   - スクリプトの実行には数時間かかることがあります。
   - 一般に、スクリプトの実行中は、 SSH セッションは単独で行う必要があります。
   - SSH セッションがアクティブになっている間は、 * Ctrl+C キーを押さないでください。
   - このスクリプトは、ネットワークの中断が発生して SSH セッションが終了した場合にバックグラウンドで実行されますが、進行状況はリカバリページで確認できます。
   - ストレージノードで RSM サービスを使用している場合は、ノードサービスの再起動時にスクリプトが 5 分間停止しているように見えることがあります。この 5 分間の遅延は、 RSM サービスが初めて起動するときに発生します。

     RSM サービスは、 ADC サービスが含まれるストレージノードにあります。

   一部の StorageGRID リカバリ手順では、 Reaper を使用して Cassandra の修復を処理します。関連サービスまたは必要なサービスが開始されるとすぐに修理が自動的に行われます。スクリプトの出力には、「 reaper 」または「 Cassandra repair 」が含まれていることがあります。 修復が失敗したことを示すエラーメッセージが表示された場合は、エラーメッセージに示されたコマンドを実行します。

5. をとして使用します `sn-recovery-postinstall.sh` スクリプトが実行され、Grid Managerのリカバリページが監視されます。

   のステータスの概要は、リカバリページの進捗状況バーとステージ列で確認できます `sn-recovery-postinstall.sh` スクリプト：




のあとに入力します `sn-recovery-postinstall.sh` スクリプトによってノードでサービスが開始されました。スクリプトでフォーマットされた任意のストレージボリュームにオブジェクトデータをリストアできます。詳細については、その手順 を参照してください。

関連情報

"ストレージノードのシステムドライブのリカバリに関する警告の確認"

"必要に応じたストレージボリュームへのオブジェクトデータのリストア"

必要に応じたストレージボリュームへのオブジェクトデータのリストア

状況に応じて `sn-recovery-postinstall.sh` スクリプトは、障害ストレージボリュームの1つ以上を再フォーマットするために必要です。他のストレージノードとアーカイブノードから再フォーマットされたストレージボリュームにオブジェクトデータをリストアする必要があります。これらの手順は、 1 つ以上のストレージボリュームを再フォーマットしないかぎり必要ありません。

必要なもの

- リカバリされたストレージノードの接続状態が * connected * であることを確認しておく必要があります✔ Grid Managerの* Nodes > Overview *タブ。

このタスクについて

グリッドの ILM ルールがオブジェクトコピーを作成するように設定されていた場合、他のストレージノード、アーカイブノード、またはクラウドストレージプールからオブジェクトデータをリストアできます。

レプリケートされたコピーを 1 つだけ保存するように ILM ルールが設定されていて、そのコピーがストレージボリュームに障害が発生した場合、オブジェクトをリカバリすることはできません。

オブジェクトのコピーがクラウドストレージプールにしか残っていない場合、 StorageGRID は、オブジェクトデータをリストアするために複数の要求をクラウドストレージプールエンドポイントに問題 する必要があります。この手順 を実行する前に、テクニカルサポートに問い合わせて、リカバリ期間と関連コストの見積もりを依頼してください。

オブジェクトのコピーがアーカイブノードにしか残っていない場合は、アーカイブノードからオブジェクトデータが読み出されます。外部アーカイブストレージシステムからの読み出しには遅延が伴うため、アーカイブノードからストレージノードへのオブジェクトデータのリストアには、他のストレージノードからコピーをリストアする場合に比べて時間がかかります。

オブジェクトデータをリストアするには、を実行します `repair-data` スクリプト：このスクリプトは、オブジェクトデータのリストアプロセスを開始し、 ILM スキャンと連動して ILM ルールを適用します。では、さまざまなオプションを使用します `repair-data` 次の方法で、レプリケートデータとイレイジャーコーディングデータのどちらをリストアするかに基づくスクリプトです。

- レプリケートデータ：レプリケートデータをリストアするコマンドは、ノード全体を修復するのか、ノード上の一部のボリュームのみを修復するのかに応じて2つあります。

```
repair-data start-replicated-node-repair
```

```
repair-data start-replicated-volume-repair
```

- イレイジャーコーディング（**EC**）データ：イレイジャーコーディングデータをリストアするコマンドは、ノード全体を修復するのか、ノード上の一部のボリュームのみを修復するのかに応じて2つあります。

```
repair-data start-ec-node-repair
```

```
repair-data start-ec-volume-repair
```

イレイジャーコーディングデータの修復は、一部のストレージノードがオフライン状態で開始できます。修復はすべてのノードが使用可能になったあとに完了します。次のコマンドを使用して、イレイジャーコーディングデータの修復を追跡できます。

```
repair-data show-ec-repair-status
```

EC 修復ジョブによって、大量のストレージが一時的にリザーブされます。ストレージアラートがトリガーされることもありますが、修復が完了すると解決します。予約に必要なストレージが不足していると、 EC の修復ジョブが失敗します。ストレージリザベーションは、ジョブが失敗したか成功したかに関係なく、 EC 修復ジョブが完了すると解放されます。

を使用する方法の詳細については、を参照してください `repair-data` スクリプトを入力します `repair-data --help` プライマリ管理ノードのコマンドラインを使用します。

手順

1. プライマリ管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`

b. に記載されているパスワードを入力します `Passwords.txt` ファイル。

c. 次のコマンドを入力してrootに切り替えます。 `su -`

d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

2. を使用します `/etc/hosts` リストアされたストレージボリュームのストレージノードのホスト名を特定するファイル。グリッド内のすべてのノードのリストを表示するには、次のように入力します。 `cat /etc/hosts`

3. すべてのストレージボリュームで障害が発生した場合は、ノード全体を修復します。（一部のボリュームだけで障害が発生した場合は、次の手順に進みます）。

> を実行できません `repair-data` 複数のノードに対して同時に処理を実行すること。複数のノードをリカバリする場合は、テクニカルサポートにお問い合わせください。

◦ グリッドにレプリケートデータがある場合は、を使用します `repair-data start-replicated-node-repair` コマンドにを指定します `--nodes` ストレージノード全体を修復するオプションです。

次のコマンドは、 SG-DC-SN3 というストレージノードにあるレプリケートデータを修復します。

```
repair-data start-replicated-node-repair --nodes SG-DC-SN3
```

> オブジェクトデータのリストア時、 StorageGRID システムがレプリケートされたオブジェクトデータを見つけられない場合は、 * Objects lost * アラートがトリガーされます。システム全体のストレージノードでアラートがトリガーされることがあります。損失の原因 と、リカバリが可能かどうかを確認する必要があります。StorageGRID の監視とトラブルシューティングの手順を参照してください。

◦ グリッドにイレイジャーコーディングデータがある場合は、を使用します `repair-data start-ec-node-repair` コマンドにを指定します `--nodes` ストレージノード全体を修復するオプションです。

次のコマンドは、SG-DC-SN3というストレージノードにあるイレイジャーコーディングデータを修復します。

```
repair-data start-ec-node-repair --nodes SG-DC-SN3
```

一意のが返されます `repair ID` これを識別します `repair_data` 操作。これを使用します `repair ID` をクリックして、の進捗状況と結果を追跡します `repair_data` 操作。リカバリプロセスが完了しても、それ以外のフィードバックは返されません。

> イレイジャーコーディングデータの修復は、一部のストレージノードがオフライン状態で開始できます。修復はすべてのノードが使用可能になったあとに完了します。

◦ グリッドにレプリケートデータとイレイジャーコーディングデータの両方がある場合は、両方のコマンドを実行します。

4. 一部のボリュームだけで障害が発生した場合は、影響を受けたボリュームを修復します。

   ボリューム ID を 16 進数で入力します。例： `0000` は、最初のボリュームとです `000F` 16番目のボリュームです。1 つのボリューム、一連のボリューム、または連続していない複数のボリュームを指定できます。

   すべてのボリュームが同じストレージノードにある必要があります。複数のストレージノードのボリュームをリストアする必要がある場合は、テクニカルサポートにお問い合わせください。

   - グリッドにレプリケートデータがある場合は、を使用します `start-replicated-volume-repair` コマンドにを指定します `--nodes` ノードを識別するオプション。次に、を追加します `--volumes` または `--volume-range` 次の例に示すように、オプションを指定します。

     単一ボリューム：レプリケートされたデータをボリュームにリストアします `0002` SG-DC-SN3という名前のストレージノードで次のように設定します。

     ```
     repair-data start-replicated-volume-repair --nodes SG-DC-SN3
     --volumes 0002
     ```

     ボリューム範囲：レプリケートされたデータを範囲内のすべてのボリュームにリストアします `0003` 終了： `0009` SG-DC-SN3という名前のストレージノードで次のように設定します。

     ```
     repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume
     -range 0003-0009
     ```

     複数のボリュームが連続していません：このコマンドは、複製されたデータをボリュームにリストアします `0001`、 `0005`および `0008` SG-DC-SN3という名前のストレージノードで次のように設定します。

     ```
     repair-data start-replicated-volume-repair --nodes SG-DC-SN3
     --volumes 0001,0005,0008
     ```

     > オブジェクトデータのリストア時、 StorageGRID システムがレプリケートされたオブジェクトデータを見つけられない場合は、 * Objects lost * アラートがトリガーされます。システム全体のストレージノードでアラートがトリガーされることがあります。損失の原因 と、リカバリが可能かどうかを確認する必要があります。StorageGRID の監視とトラブルシューティングの手順を参照してください。

   - グリッドにイレイジャーコーディングデータがある場合は、を使用します `start-ec-volume-repair` コマンドにを指定します `--nodes` ノードを識別するオプション。次に、を追加します `--volumes` または `--volume-range` 次の例に示すように、オプションを指定します。

     単一ボリューム：イレイジャーコーディングされたデータをボリュームにリストアします `0007` SG-DC-SN3という名前のストレージノードで次のように設定します。

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 0007
```

ボリューム範囲：イレイジャーコーディングされたデータを範囲内のすべてのボリュームにリストアします `0004` 終了： `0006` SG-DC-SN3という名前のストレージノードで次のように設定します。

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range
0004-0006
```

複数のボリュームが連続していません：このコマンドはイレイジャーコーディングされたデータをボリュームにリストアします `000A`、 `000C`および `000E` SG-DC-SN3という名前のストレージノードで次のように設定します。

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes
000A,000C,000E
```

。 `repair-data` 一意のが返されます `repair ID` これを識別します `repair_data` 操作。これを使用します `repair ID` をクリックして、の進捗状況と結果を追跡します `repair_data` 操作。リカバリプロセスが完了しても、それ以外のフィードバックは返されません。

> イレイジャーコーディングデータの修復は、一部のストレージノードがオフライン状態で開始できます。修復はすべてのノードが使用可能になったあとに完了します。

- グリッドにレプリケートデータとイレイジャーコーディングデータの両方がある場合は、両方のコマンドを実行します。

5. レプリケートデータの修復を監視します。
   a. 「* Nodes > Storage Node being repaired > ILM *」を選択します。
   b. 「評価」セクションの属性を使用して、修理が完了したかどうかを判断します。

      修復が完了すると、Awaiting - All属性は0個のオブジェクトを示します。

   c. 修復の詳細を監視するには、* Support > Tools > Grid Topology *を選択します。
   d. 「* grid > Storage Node being repaired > LDR > Data Store *」を選択します。
   e. 次の属性を組み合わせて、レプリケートデータの修復が完了したかどうかを可能なかぎり判別します。

      > Cassandra に不整合が生じている可能性があり、また、失敗した修復は追跡されません。

      - * Repairs Attempted （ XRPA ） * ：レプリケートデータの修復の進行状況を追跡します。この属性は、ストレージノードがハイリスクオブジェクトの修復を試みるたびに値が増分します。この属性の値が現在のスキャン期間（ * Scan Period - - Estimated * 属性で指定）よりも長い期間にわたって上昇しない場合、 ILM スキャンはすべてのノードで修復が必要なハイリスクオブジェクトを検出していません。

ハイリスクオブジェクトとは、完全に失われる危険があるオブジェクトです。ILM設定を満たしていないオブジェクトは含まれません。

- * スキャン期間 - 推定（ XSCM ） * ：この属性を使用して、以前に取り込まれたオブジェクトにポリシー変更が適用されるタイミングを見積もります。「 * Repairs Attempted * 」属性が現在のスキャン期間よりも長くなっていない場合は、複製修復が実行されている可能性があります。スキャン期間は変わる可能性があるので注意してください。* Scan Period - - Estimated （ XSCM ） * 属性は、グリッド全体の環境 を示します。これは、すべてのノードのスキャン期間の最大値です。グリッドの * Scan Period - - Estimated * 属性履歴を照会して、適切な期間を判断できます。

6. イレイジャーコーディングデータの修復を監視し、失敗した可能性のある要求を再試行します。

   a. イレイジャーコーディングデータの修復ステータスを確認します。

      - 特定ののののステータスを表示するには、このコマンドを使用します `repair-data` 操作：

      ```
      repair-data show-ec-repair-status --repair-id repair ID
      ```

      - すべての修復処理を表示するには、次のコマンドを使用します

      ```
      repair-data show-ec-repair-status
      ```

      出力には、などの情報が表示されます `repair ID`以前に、現在実行中のすべての修復。

```
root@DC1-ADM1:~ # repair-data show-ec-repair-status

Repair ID Scope Start Time End Time State Est Bytes Affected/Repaired
Retry Repair
================================================================================
=============
949283 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:27:06.9 Success 17359
17359 No
949292 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:37:06.9 Failure 17359
0 Yes
949294 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:47:06.9 Failure 17359
0 Yes
949299 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:57:06.9 Failure 17359
0 Yes
```

   b. 失敗した修復処理が出力された場合は、を使用します `--repair-id` 修復を再試行するオプションです。

      次のコマンドは、修復ID 83930030303133434を使用して、障害が発生したノードの修復を再試行します。

```
repair-data start-ec-node-repair --repair-id 83930030303133434
```

次のコマンドは、修復ID 83930030303133434を使用して、障害が発生したボリュームの修復を再試行します。

```
repair-data start-ec-volume-repair --repair-id 83930030303133434
```

関連情報

"StorageGRID の管理"

"トラブルシューティングを監視します"

ストレージノードシステムドライブのリカバリ後のストレージの状態の確認

## ストレージノードのシステムドライブをリカバリしたら、ストレージノードに必要とされる状態が「 Online 」に設定されていることを確認し、ストレージノードサーバが再起動するたびにオンライン状態になるようにする必要があります。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- ストレージノードがリカバリされ、データリカバリが完了している必要があります。

手順

1. Support **>** Tools **>** Grid Topology *を選択します。
2. リカバリされたストレージノード* LDR * Storage * **Storage State - Desired** *および Storage State - Current *の値を確認します。

   両方の属性の値が Online である必要があります。

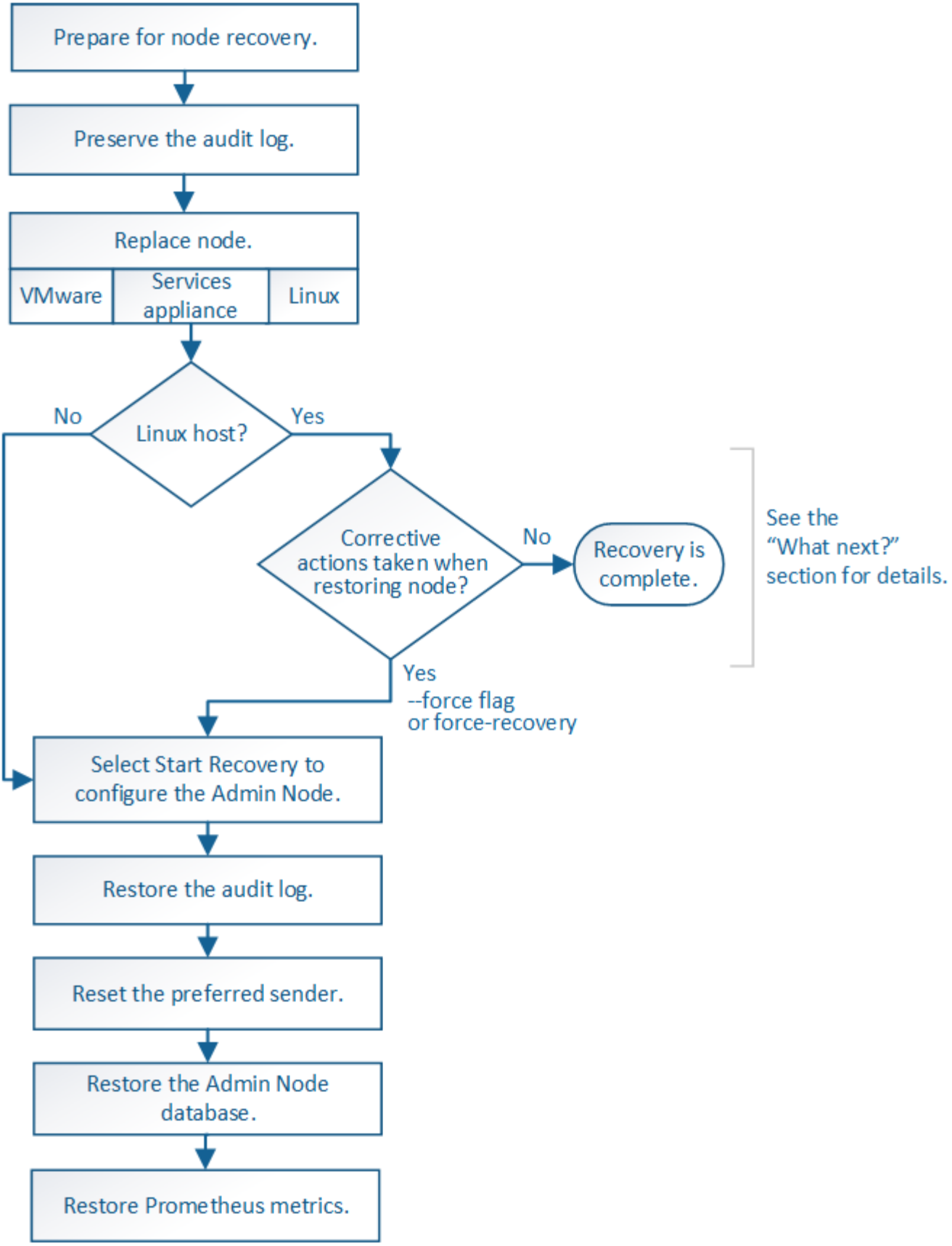
3. Storage State --Desired が Read-Only に設定されている場合は、次の手順を実行します。
   a. [* 構成 *] タブをクリックします。
   b. [* Storage State] — [Desired *] ( 保存状態 — 希望する *)] ドロップダウンリストから [*Online] ( オンライン ) を選択します。
   c. [ 変更の適用 *] をクリックします。
   d. [* 概要 **]** タブをクリックし、 **[** ストレージ状態 **--Desired** * および * ストレージ状態 **--current** ] の値が [ オンライン ] に更新されていることを確認します。

管理ノードの障害からのリカバリ

## 管理ノードのリカバリプロセスは、プライマリ管理ノードと非プライマリ管理ノードで異なります。

このタスクについて

プライマリまたは非プライマリ管理ノードのおおまかなリカバリ手順は同じですが、詳細は異なります。




リカバリ対象の管理ノードの正しいリカバリ手順 に必ず従ってください。手順の概要は同じように見えますが、詳細な手順は異なります。

関連情報

"SG100 SG1000サービスアプライアンス"

選択肢

- "プライマリ管理ノードの障害からのリカバリ"
- "非プライマリ管理ノードの障害からのリカバリ"

プライマリ管理ノードの障害からのリカバリ

# プライマリ管理ノードの障害からリカバリするには、特定のタスクを実行する必要があります。プライマリ管理ノードは、グリッドの Configuration Management Node （ CMN ）サービスをホストします。

このタスクについて

障害が発生したプライマリ管理ノードはすぐに交換する必要があります。プライマリ管理ノード上の Configuration Management Node （ CMN ）サービスは、グリッドに対してオブジェクト ID のブロックを発行します。これらの ID は、オブジェクトの取り込み時にオブジェクトに割り当てられます。使用可能な ID がないと、新しいオブジェクトを取り込むことはできません。グリッドには約 1 カ月分の ID がキャッシュされているため、 CMN を使用できない場合でもオブジェクトの取り込みを続行できます。ただし、キャッシュされた識別子を使い切ると、新しいオブジェクトを追加できなくなります。

> グリッドでのオブジェクトの取り込みに影響が生じないように、障害が発生したプライマリ管理ノードはおよそ 1 カ月以内に修復または交換する必要があります。正確な期間はオブジェクトの取り込み頻度によって異なります。お使いのグリッドでの正確な期間が必要な場合は、テクニカルサポートにお問い合わせください。

手順

- "障害が発生したプライマリ管理ノードから監査ログをコピーする"
- "プライマリ管理ノードの交換"
- "交換用プライマリ管理ノードの設定"
- "リカバリされたプライマリ管理ノードでの監査ログのリストア"
- "リカバリ済みプライマリ管理ノードで優先送信者をリセットしています"
- "プライマリ管理ノードをリカバリする際の管理ノードデータベースのリストア"
- "プライマリ管理ノードをリカバリする際のPrometheus指標のリストア"

障害が発生したプライマリ管理ノードから監査ログをコピーする

# 障害が発生したプライマリ管理ノードから監査ログをコピーできる場合は、グリッドのシステムアクティビティと使用状況のレコードを維持するために監査ログを保存します。リカバリしたプライマリ管理ノードが起動したら、保存しておいた監査ログをそのノードにリストアします。

この手順 は、障害が発生した管理ノードの監査ログファイルを別のグリッドノードの一時的な場所にコピーします。保存した監査ログは、交換用管理ノードにコピーできます。新しい管理ノードには監査ログが自動的にコピーされません。

障害の種類によっては、障害が発生した管理ノードから監査ログをコピーできない場合があります。管理ノードが 1 つしかない環境の場合、リカバリした管理ノードで新しい空のファイルの監査ログへのイベントの記録が開始され、以前に記録されたデータは失われます。管理ノードが複数ある環境の場合は、別の管理ノードから監査ログをリカバリできます。

ここで障害管理ノード上の監査ログにアクセスできない場合は、ホストのリカバリ後など、あとから監査ログにアクセスできる可能性があります。

1. 可能であれば、障害管理ノードにログインします。できない場合は、プライマリ管理ノードまたは別の管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

      rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。
2. AMSサービスを停止して新しいログファイルが作成されないようにします。`service ams stop`
3. audit.log ファイルの名前を変更して、リカバリした管理ノードへのコピー時に既存のファイルが上書きされないようにします。

   audit.log の名前を、 yyyy-mm-dd.txt.1 などの一意の番号の付いたファイル名に変更します。たとえば、audit.logファイルの名前を2015-10-25.txt.1に変更しますcd /var/local/audit/export/
4. AMSサービスを再起動します。 `service ams start`
5. すべての監査ログファイルを別のグリッドノードの一時的な場所にコピーするためのディレクトリを作成します。 `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

   プロンプトが表示されたら、 admin のパスワードを入力します。
6. すべての監査ログファイルをコピーします。 `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

   プロンプトが表示されたら、 admin のパスワードを入力します。
7. rootとしてログアウトします。 `exit`

プライマリ管理ノードの交換

## プライマリ管理ノードをリカバリするには、まず物理または仮想ハードウェアの交換が必要です。

障害が発生したプライマリ管理ノードを同じプラットフォームで実行されているプライマリ管理ノードと交換することも、 VMware または Linux ホストで実行されているプライマリ管理ノードをサービスアプライアンスでホストされているプライマリ管理ノードと交換することもできます。

ノードに対して選択した交換用プラットフォームに一致する手順 を使用します。（すべてのノードタイプに適した）ノード交換手順 を完了すると、プライマリ管理ノードのリカバリに関する次のステップが手順 から

表示されます。

| 交換用プラットフォーム | 手順 |
| --- | --- |
| VMware | "VMwareノードの交換" |
| Linux の場合 | "Linuxノードの交換" |
| SG100 および SG1000 サービスアプライアンス | "サービスアプライアンスの交換" |
| OpenStack の機能を使用 | リカバリ処理を対象とした OpenStack 用の仮想マシンディスクファイルおよびスクリプトは、現在は提供されていません。OpenStack 環境で実行されているノードのリカバリが必要な場合は、使用している Linux オペレーティングシステム用のファイルをダウンロードしてください。その後、手順 に従って Linux ノードを交換します。 |

交換用プライマリ管理ノードの設定

## 交換用ノードは、 StorageGRID システムのプライマリ管理ノードとして設定する必要があります。

必要なもの

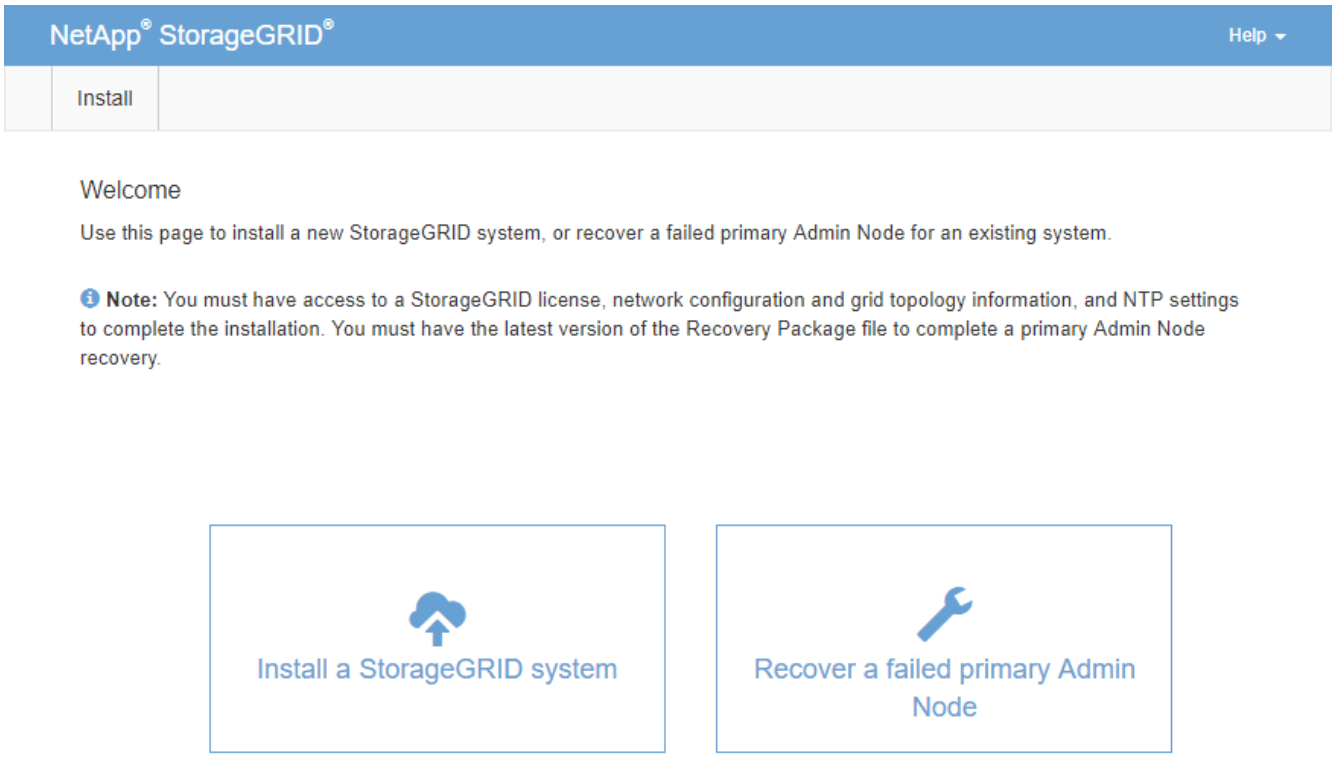
- 仮想マシンでホストされるプライマリ管理ノードの場合は、仮想マシンを導入し、電源をオンにして初期化する必要があります。
- サービスアプライアンスでホストされるプライマリ管理ノードの場合は、アプライアンスを交換し、ソフトウェアをインストールしておく必要があります。使用するアプライアンスのインストールガイドを参照してください。

  "SG100 SG1000サービスアプライアンス"

- リカバリパッケージファイルの最新のバックアップが必要です (`sgws-recovery-package-id-revision.zip`) 。
- プロビジョニングパスフレーズが必要です。

手順

1. Webブラウザを開き、に移動します `https://primary_admin_node_ip`。




2. [*Recover a failed primary Admin Node] をクリックします。
3. リカバリパッケージの最新のバックアップをアップロードします。
   a. [* 参照 ] をクリックします。
   b. StorageGRID システムに対応した最新のリカバリパッケージファイルを探し、 * Open * をクリックします。
4. プロビジョニングパスフレーズを入力します。
5. [ リカバリの開始 ] をクリックします。

   リカバリプロセスが開始されます。必要なサービスが開始されるまでの数分間、 Grid Manager を使用できなくなることがあります。リカバリが完了すると、サインインページが表示されます。

6. StorageGRID システムでシングルサインオン（SSO）が有効になっており、リカバリした管理ノードの証明書利用者信頼がデフォルトの管理インターフェイスサーバ証明書を使用するように設定されている場合は、ノードの証明書利用者信頼をActive Directoryフェデレーションサービス（AD FS）で更新（削除および再作成）します。管理ノードのリカバリプロセス中に生成された新しいデフォルトサーバ証明書を使用します。

   証明書利用者信頼を設定するには、 StorageGRID の管理手順を参照してください。デフォルトのサーバ証明書にアクセスするには、管理ノードのコマンドシェルにログインします。にアクセスします `/var/local/mgmt-api` ディレクトリに移動し、を選択します `server.crt` ファイル。

7. ホットフィックスの適用が必要かどうかを判断します。
   a. サポートされているブラウザを使用してGrid Managerにサインインします。
   b. [ノード（ Nodes）]を選択し

c. 左側のリストで、プライマリ管理ノードを選択します。

d. [ 概要 ] タブの [ ソフトウェアバージョン ] フィールドに表示されているバージョンを確認します。

e. 他のグリッドノードを選択します。

f. [ 概要 ] タブの [ ソフトウェアバージョン ] フィールドに表示されているバージョンを確認します。

- [ ソフトウェアバージョン * ] フィールドに表示されるバージョンが同じ場合、修正プログラムを適用する必要はありません。
- [ ソフトウェアバージョン * ] フィールドに表示されるバージョンが異なる場合は、ホットフィックスを適用して、リカバリされたプライマリ管理ノードを同じバージョンに更新する必要があります。

関連情報

"StorageGRID の管理"

"StorageGRID ホットフィックス手順"

リカバリされたプライマリ管理ノードでの監査ログのリストア

## 障害が発生したプライマリ管理ノードから監査ログを保存できた場合は、リカバリするプライマリ管理ノードにそのログをコピーできます。

- リカバリした管理ノードをインストールして実行する必要があります。
- 元の管理ノードで障害が発生したあとに、監査ログを別の場所にコピーしておく必要があります。

管理ノードで障害が発生すると、その管理ノードに保存された監査ログが失われる可能性があります。障害が発生した管理ノードから監査ログをコピーし、リカバリされた管理ノードにリストアすることで、データを損失から守ることができる場合があります。障害によっては、障害が発生した管理ノードから監査ログをコピーできない場合があります。その場合、管理ノードが複数ある環境ではすべての管理ノードに監査ログがレプリケートされるため、別の管理ノードから監査ログをリカバリできます。

管理ノードが 1 つしかない環境で障害ノードから監査ログをコピーできない場合は、リカバリされた管理ノードで、新規インストールの場合と同じように監査ログへのイベントの記録が開始されます。

ロギング機能を復旧させるために、管理ノードはできるだけ早くリカバリする必要があります。

1. リカバリした管理ノードにログインします。

   a. 次のコマンドを入力します。 `ssh admin@recovery_Admin_Node_IP`

   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。

   c. 次のコマンドを入力してrootに切り替えます。 `su -`

   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

   rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

2. 保持されている監査ファイルを確認します。 `cd /var/local/audit/export`

3. 保持されている監査ログファイルをリカバリされた管理ノードにコピーします。 `scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY* .`

プロンプトが表示されたら、 admin のパスワードを入力します。

4. セキュリティ上の理由により、監査ログがリカバリされた管理ノードにコピーされたことを確認したら、監査ログを障害グリッドノードから削除します。
5. リカバリされた管理ノードで、監査ログファイルのユーザとグループの設定を更新します。 `chown ams-user:bycast *`
6. rootとしてログアウトします。 `exit`

監査共有への既存のクライアントアクセスもリストアする必要があります。詳細については、 StorageGRID の管理手順を参照してください。

関連情報

"StorageGRID の管理"

リカバリ済みプライマリ管理ノードで優先送信者をリセットしています

## リカバリするプライマリ管理ノードが、アラート通知、アラーム通知、および AutoSupport メッセージの優先送信者として設定されている場合は、この設定を変更する必要があります。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- リカバリした管理ノードをインストールして実行する必要があります。

手順

1. * Configuration > System Settings > Display Options *を選択します。
2. [*Preferred Sender] ドロップダウン・リストからリカバリされた管理ノードを選択します
3. [ 変更の適用 *] をクリックします。

関連情報

"StorageGRID の管理"

プライマリ管理ノードをリカバリする際の管理ノードデータベースのリストア

## 障害が発生したプライマリ管理ノードの属性、アラーム、およびアラートの履歴情報を維持したい場合は、管理ノードデータベースをリストアします。このデータベースをリストアできるのは、 StorageGRID システムに別の管理ノードがある場合のみです。

- リカバリした管理ノードをインストールして実行する必要があります。
- StorageGRID システムには管理ノードが少なくとも 2 つ必要です。
- を用意しておく必要があります `Passwords.txt` ファイル。
- プロビジョニングパスフレーズが必要です。

管理ノードで障害が発生すると、その管理ノードデータベースに格納されていた履歴情報が失われます。この

データベースには次の情報が含まれています。

- アラートの履歴
- アラームの履歴
- 履歴属性データ。サポート**ツール*グリッドトポロジ*ページで確認できるチャートおよびテキストレポートで使用されます。

管理ノードをリカバリする際に、ソフトウェアのインストールプロセスによって、リカバリしたノードに空の管理ノードデータベースが作成されます。ただし、新しいデータベースには、現在システムに含まれているサーバとサービス、またはあとで追加されたサーバの情報だけが含まれます。

プライマリ管理ノードをリストアした StorageGRID システムに別の管理ノードがある場合は、プライマリでない管理ノード（ *source Admin Nod* ）の管理ノードデータベースをリカバリしたプライマリ管理ノードにコピーすることで、履歴情報をリストアできます。システムにプライマリ管理ノードしかない場合は、管理ノードデータベースをリストアできません。

> 管理ノードデータベースのコピーには数時間かかることがあります。ソース管理ノードでサービスが停止している間は、グリッドマネージャの一部の機能が使用できなくなります。

1. ソース管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。
2. ソース管理ノードからMIサービスを停止します。 `service mi stop`
3. ソース管理ノードから、管理アプリケーションプログラミングインターフェイス（mgmt-api）サービスを停止します。 `service mgmt-api stop`
4. リカバリした管理ノードで次の手順を実行します。
   a. リカバリした管理ノードにログインします。
      i. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
      ii. に記載されているパスワードを入力します `Passwords.txt` ファイル。
      iii. 次のコマンドを入力してrootに切り替えます。 `su -`
      iv. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   b. MIサービスを停止します。 `service mi stop`
   c. mgmt-apiサービスを停止します。 `service mgmt-api stop`
   d. SSH エージェントに SSH 秘密鍵を追加します。入力するコマンド`ssh-add`
   e. に記載されているSSHアクセスパスワードを入力します `Passwords.txt` ファイル。
   f. ソース管理ノードのデータベースをリカバリした管理ノードにコピーします。
   `/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`
   g. プロンプトが表示されたら、リカバリした管理ノードで MI データベースを上書きすることを確定します。

データベースとその履歴データが、リカバリした管理ノードにコピーされます。コピー処理が完了すると、リカバリした管理ノードがスクリプトによって起動されます。

h. 他のサーバにパスワードなしでアクセスする必要がなくなった場合は、 SSH エージェントから秘密鍵を削除します。入力するコマンド`ssh-add -D`

5. ソース管理ノードでサービスを再起動します。 `service servermanager start`

プライマリ管理ノードをリカバリする際の**Prometheus**指標のリストア

プライマリ管理ノードで障害が発生した場合、そのノード上の Prometheus で管理されていた過去の指標を必要に応じてリストアすることができます。Prometheus 指標をリストアできるのは、 StorageGRID システムに別の管理ノードがある場合のみです。

- リカバリした管理ノードをインストールして実行する必要があります。
- StorageGRID システムには管理ノードが少なくとも 2 つ必要です。
- を用意しておく必要があります `Passwords.txt` ファイル。
- プロビジョニングパスフレーズが必要です。

管理ノードで障害が発生すると、 Prometheus データベースで管理されていた管理ノード上の指標は失われます。管理ノードをリカバリする際に、ソフトウェアのインストールプロセスによって新しい Prometheus データベースが作成されます。リカバリした管理ノードを起動すると、 StorageGRID システムを新規にインストールした場合と同様に指標が記録されます。

プライマリ管理ノードをリストアした StorageGRID システムに別の管理ノードがある場合は、プライマリでない管理ノード（ _SOURCE 管理ノード）の Prometheus データベースをリカバリしたプライマリ管理ノードにコピーすることで、過去の指標をリストアできます。システムにプライマリ管理ノードしかない場合は、Prometheus データベースをリストアできません。

Prometheus データベースのコピーには 1 時間以上かかる場合があります。ソース管理ノードでサービスが停止している間は、グリッドマネージャの一部の機能が使用できなくなります。

1. ソース管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。
2. ソース管理ノードからPrometheusサービスを停止します。 `service prometheus stop`
3. リカバリした管理ノードで次の手順を実行します。
   a. リカバリした管理ノードにログインします。
      i. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
      ii. に記載されているパスワードを入力します `Passwords.txt` ファイル。
      iii. 次のコマンドを入力してrootに切り替えます。 `su -`

iv. に記載されているパスワードを入力します `Passwords.txt` ファイル。

b. Prometheusサービスを停止します。 `service prometheus stop`

c. SSH エージェントに SSH 秘密鍵を追加します。入力するコマンド`ssh-add`

d. に記載されているSSHアクセスパスワードを入力します `Passwords.txt` ファイル。

e. ソース管理ノードのPrometheusデータベースをリカバリした管理ノードにコピーします。
`/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`

f. プロンプトが表示されたら、 * Enter * を押して、リカバリした管理ノード上の新しい Prometheus データベースを破棄することを確認します。

元の Prometheus データベースとその履歴データが、リカバリした管理ノードにコピーされます。コピー処理が完了すると、リカバリした管理ノードがスクリプトによって起動されます。次のステータスが表示されます。

データベースのクローニング、サービスの開始

a. 他のサーバにパスワードなしでアクセスする必要がなくなった場合は、 SSH エージェントから秘密鍵を削除します。入力するコマンド`ssh-add -D`

4. ソース管理ノードでPrometheusサービスを再起動します.`service prometheus start`

非プライマリ管理ノードの障害からのリカバリ

非プライマリ管理ノードの障害からリカバリするには、次のタスクを実行する必要があります。1 つの管理ノードが Configuration Management Node （ CMN ）サービスをホストしており、これをプライマリ管理ノードと呼びます。管理ノードを複数使用することはできますが、 StorageGRID システムごとに配置できるプライマリ管理ノードは 1 つだけです。それ以外の管理ノードはすべて非プライマリ管理ノードです。

関連情報

"SG100 SG1000サービスアプライアンス"

手順

- "障害が発生した非プライマリ管理ノードから監査ログをコピーする"
- "非プライマリ管理ノードの交換"
- "リカバリの開始を選択して非プライマリ管理ノードを設定します"
- "リカバリ済み非プライマリ管理ノードでの監査ログのリストア"
- "リカバリ済み非プライマリ管理ノードで優先送信者をリセットしています"
- "非プライマリ管理ノードをリカバリする際の管理ノードデータベースのリストア"
- "非プライマリ管理ノードをリカバリする際のPrometheus指標のリストア"

障害が発生した非プライマリ管理ノードから監査ログをコピーする

障害が発生した管理ノードから監査ログをコピーできる場合は、グリッドのシステムアクティビティと使用状況のレコードを維持するために監査ログを保存します。リカバリ

## した非プライマリ管理ノードが起動したら、保存しておいた監査ログをそのノードにリストアします。

この手順 は、障害が発生した管理ノードの監査ログファイルを別のグリッドノードの一時的な場所にコピーします。保存した監査ログは、交換用管理ノードにコピーできます。新しい管理ノードには監査ログが自動的にコピーされません。

障害の種類によっては、障害が発生した管理ノードから監査ログをコピーできない場合があります。管理ノードが 1 つしかない環境の場合、リカバリした管理ノードで新しい空のファイルの監査ログへのイベントの記録が開始され、以前に記録されたデータは失われます。管理ノードが複数ある環境の場合は、別の管理ノードから監査ログをリカバリできます。

ここで障害管理ノード上の監査ログにアクセスできない場合は、ホストのリカバリ後など、あとから監査ログにアクセスできる可能性があります。

1. 可能であれば、障害管理ノードにログインします。できない場合は、プライマリ管理ノードまたは別の管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

      rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。
2. AMSサービスを停止して新しいログファイルが作成されないようにします。`service ams stop`
3. audit.log ファイルの名前を変更して、リカバリした管理ノードへのコピー時に既存のファイルが上書きされないようにします。

   audit.log の名前を、 yyyy-mm-dd.txt.1 などの一意の番号の付いたファイル名に変更します。たとえば、audit.logファイルの名前を2015-10-25.txt.1に変更します`cd /var/local/audit/export/`
4. AMSサービスを再起動します。 `service ams start`
5. すべての監査ログファイルを別のグリッドノードの一時的な場所にコピーするためのディレクトリを作成します。 `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

   プロンプトが表示されたら、 admin のパスワードを入力します。
6. すべての監査ログファイルをコピーします。 `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

   プロンプトが表示されたら、 admin のパスワードを入力します。
7. rootとしてログアウトします。 `exit`

非プライマリ管理ノードの交換

## 非プライマリ管理ノードをリカバリするには、まず物理または仮想ハードウェアの交換が必要です。

障害が発生した非プライマリ管理ノードを同じプラットフォームで実行されている非プライマリ管理ノードと交換することも、 VMware または Linux ホストで実行されている非プライマリ管理ノードをサービスアプライアンスでホストされている非プライマリ管理ノードと交換することもできます。

ノードに対して選択した交換用プラットフォームに一致する手順 を使用します。（すべてのノードタイプに適した）ノード交換手順 を完了すると、非プライマリ管理ノードのリカバリに関する次の手順がその手順 から指示されます。

| 交換用プラットフォーム | 手順 |
| --- | --- |
| VMware | "VMwareノードの交換" |
| Linux の場合 | "Linuxノードの交換" |
| SG100 および SG1000 サービスアプライアンス | "サービスアプライアンスの交換" |
| OpenStack の機能を使用 | リカバリ処理を対象とした OpenStack 用の仮想マシンディスクファイルおよびスクリプトは、現在は提供されていません。OpenStack 環境で実行されているノードのリカバリが必要な場合は、使用している Linux オペレーティングシステム用のファイルをダウンロードしてください。その後、手順 に従って Linux ノードを交換します。 |

リカバリの開始を選択して非プライマリ管理ノードを設定します

## 非プライマリ管理ノードを交換したら、 Grid Manager で Start Recovery を選択して、新しいノードを障害ノードの代わりとして設定する必要があります。

必要なもの

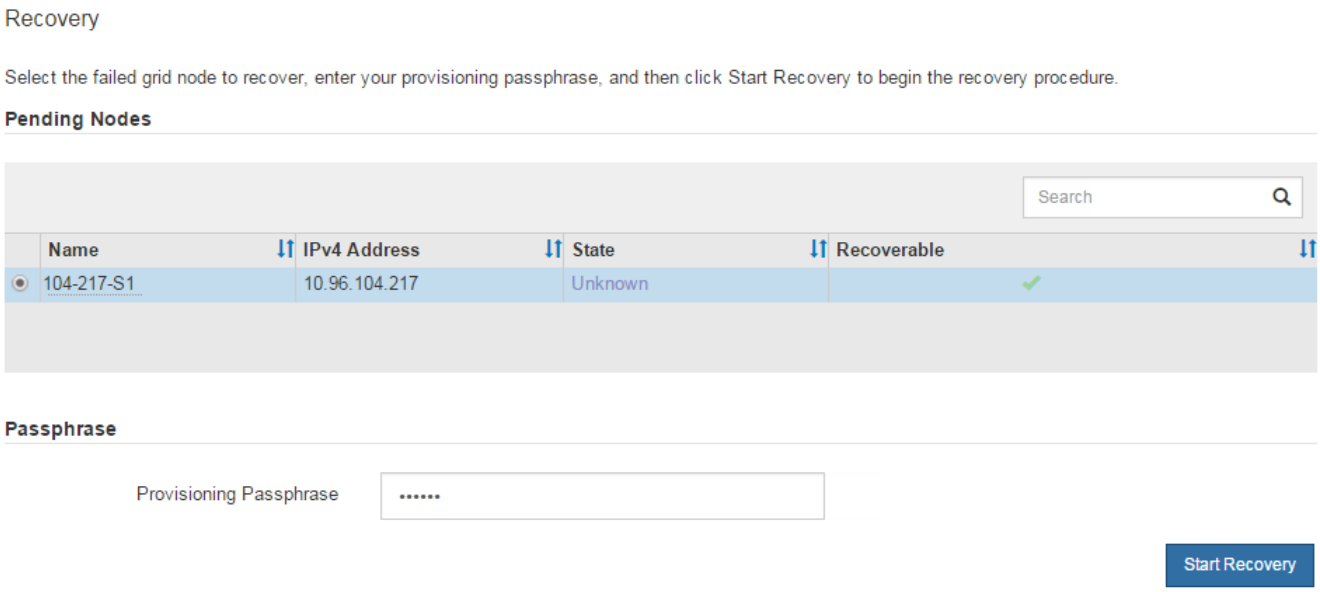
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Maintenance または Root Access 権限が必要です。
- プロビジョニングパスフレーズが必要です。
- 交換用ノードの導入と設定が完了している必要があります。

手順

1. Grid Managerから、* Maintenance * Maintenance Tasks * Recovery *（メンテナンス*メンテナンスタスク*リカバリ）を選択します。
2. リカバリするグリッドノードを Pending Nodes リストで選択します。

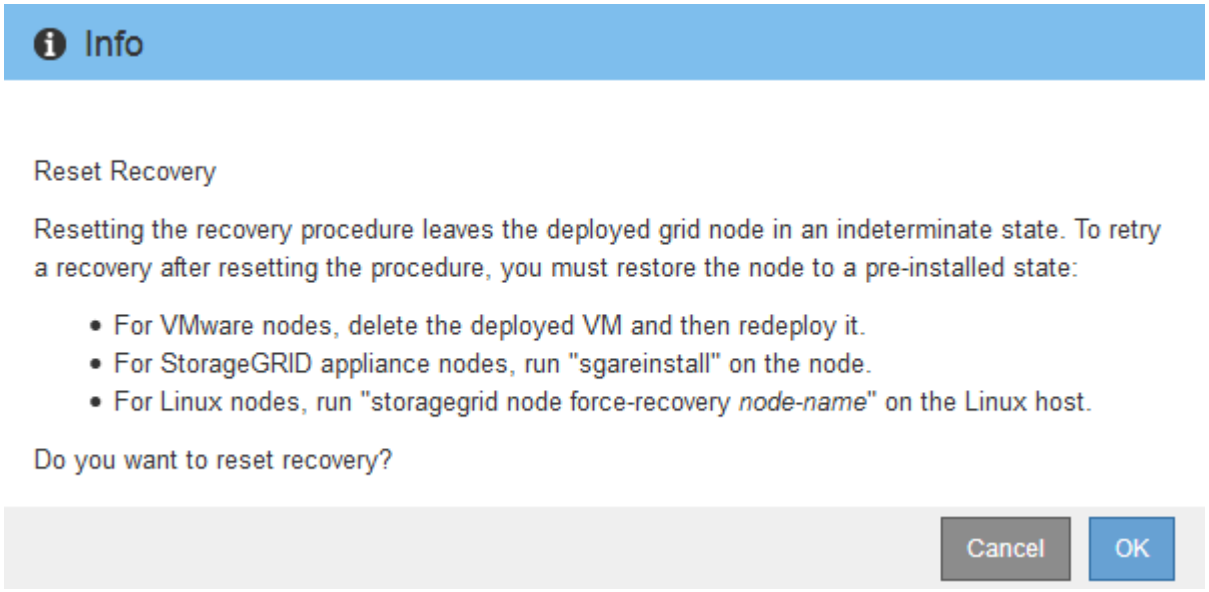
   ノードは障害が発生するとリストに追加されますが、再インストールされてリカバリの準備ができるまでは選択できません。

3. プロビジョニングパスフレーズ * を入力します。
4. [ リカバリの開始 ] をクリックします。




5. リカバリ中のグリッドノードテーブルで、リカバリの進行状況を監視します。

リカバリ手順 の実行中に [* リセット ] をクリックすると、新しいリカバリを開始できます。情報ダイアログボックスが表示され、手順 をリセットするとノードが不確定な状態のままになることが示されます。




手順 をリセットしたあとにリカバリを再試行する場合は、次の手順でノードをインストール前の状態にリストアする必要があります。

- * vmware * ：導入した仮想グリッドノードを削除します。その後、リカバリを再開する準備ができたら、ノードを再導入します。
- * Linux *：Linuxホストで次のコマンドを実行して、ノードを再起動します。 `storagegrid node force-recovery node-name`
- アプライアンス：手順 をリセットしたあとにリカバリを再試行する場合は、を実行してアプライアンスノードをインストール前の状態にリストアする必要があります `sgareinstall` をクリックします。

6. StorageGRID システムでシングルサインオン（SSO）が有効になっており、リカバリした管理ノードの証明書利用者信頼がデフォルトの管理インターフェイスサーバ証明書を使用するように設定されている場合は、ノードの証明書利用者信頼をActive Directoryフェデレーションサービス（AD FS）で更新（削除および再作成）します。管理ノードのリカバリプロセス中に生成された新しいデフォルトサーバ証明書を使用します。

> 証明書利用者信頼を設定するには、 StorageGRID の管理手順を参照してください。デフォルトのサーバ証明書にアクセスするには、管理ノードのコマンドシェルにログインします。にアクセスします `/var/local/mgmt-api` ディレクトリに移動し、を選択します `server.crt` ファイル。

関連情報

"StorageGRID の管理"

"再インストールのためのアプライアンスの準備（プラットフォームの交換のみ）"

リカバリ済み非プライマリ管理ノードでの監査ログのリストア

## 障害が発生した非プライマリ管理ノードから監査ログを保存できたために監査ログの履歴情報が保持されている場合は、リカバリする非プライマリ管理ノードにその情報をコピーできます。

- リカバリした管理ノードをインストールして実行する必要があります。
- 元の管理ノードで障害が発生したあとに、監査ログを別の場所にコピーしておく必要があります。

管理ノードで障害が発生すると、その管理ノードに保存された監査ログが失われる可能性があります。障害が発生した管理ノードから監査ログをコピーし、リカバリされた管理ノードにリストアすることで、データを損失から守ることができる場合があります。障害によっては、障害が発生した管理ノードから監査ログをコピーできない場合があります。その場合、管理ノードが複数ある環境ではすべての管理ノードに監査ログがレプリケートされるため、別の管理ノードから監査ログをリカバリできます。

管理ノードが 1 つしかない環境で障害ノードから監査ログをコピーできない場合は、リカバリされた管理ノードで、新規インストールの場合と同じように監査ログへのイベントの記録が開始されます。

ロギング機能を復旧させるために、管理ノードはできるだけ早くリカバリする必要があります。

1. リカバリした管理ノードにログインします。

   a. 次のコマンドを入力します。+
   `ssh admin@recovery_Admin_Node_IP`

   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。

   c. 次のコマンドを入力してrootに切り替えます。 `su -`

   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

   rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

2. 保持されている監査ファイルを確認します。

   ```
   cd /var/local/audit/export
   ```

3. 保持されている監査ログファイルをリカバリされた管理ノードにコピーします。

   ```
   scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY*
   ```

   プロンプトが表示されたら、 admin のパスワードを入力します。

4. セキュリティ上の理由により、監査ログがリカバリされた管理ノードにコピーされたことを確認したら、監査ログを障害グリッドノードから削除します。
5. リカバリされた管理ノードで、監査ログファイルのユーザとグループの設定を更新します。

   ```
   chown ams-user:bycast *
   ```

6. rootとしてログアウトします。 `exit`

監査共有への既存のクライアントアクセスもリストアする必要があります。詳細については、 StorageGRID の管理手順を参照してください。

関連情報

"StorageGRID の管理"

リカバリ済み非プライマリ管理ノードで優先送信者をリセットしています

## リカバリする非プライマリ管理ノードが、アラート通知、アラーム通知、および AutoSupport メッセージの優先送信者として設定されている場合は、 StorageGRID システムでこの設定を変更する必要があります。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- リカバリした管理ノードをインストールして実行する必要があります。

手順

1. * Configuration > System Settings > Display Options *を選択します。
2. [*Preferred Sender] ドロップダウン・リストからリカバリされた管理ノードを選択します
3. [ 変更の適用 *] をクリックします。

関連情報

"StorageGRID の管理"

非プライマリ管理ノードをリカバリする際の管理ノードデータベースのリストア

## 障害が発生した非プライマリ管理ノードの属性、アラーム、およびアラートの履歴情報を維持したい場合は、プライマリ管理ノードから管理ノードデータベースをリストアします。

- リカバリした管理ノードをインストールして実行する必要があります。

- StorageGRID システムには管理ノードが少なくとも 2 つ必要です。
- を用意しておく必要があります `Passwords.txt` ファイル。
- プロビジョニングパスフレーズが必要です。

管理ノードで障害が発生すると、その管理ノードデータベースに格納されていた履歴情報が失われます。このデータベースには次の情報が含まれています。

- アラートの履歴
- アラームの履歴
- 履歴属性データ。サポート**ツール*グリッドトポロジ*ページで確認できるチャートおよびテキストレポートで使用されます。

管理ノードをリカバリする際に、ソフトウェアのインストールプロセスによって、リカバリしたノードに空の管理ノードデータベースが作成されます。ただし、新しいデータベースには、現在システムに含まれているサーバとサービス、またはあとで追加されたサーバの情報だけが含まれます。

非プライマリ管理ノードをリストアした場合は、プライマリ管理ノード（ *source Admin Node*） の管理ノードデータベースをリカバリしたノードにコピーすることで、履歴情報をリストアできます。

> 管理ノードデータベースのコピーには数時間かかることがあります。ソースノードでサービスが停止している間は、 Grid Manager の一部の機能が使用できなくなります。

1. ソース管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。
2. ソース管理ノードから次のコマンドを実行します。プロンプトが表示されたら、プロビジョニングパスフレーズを入力します。 `recover-access-points`
3. ソース管理ノードからMIサービスを停止します。 `service mi stop`
4. ソース管理ノードから、管理アプリケーションプログラミングインターフェイス（mgmt-api）サービスを停止します。 `service mgmt-api stop`
5. リカバリした管理ノードで次の手順を実行します。
   a. リカバリした管理ノードにログインします。
      i. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
      ii. に記載されているパスワードを入力します `Passwords.txt` ファイル。
      iii. 次のコマンドを入力してrootに切り替えます。 `su -`
      iv. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   b. MIサービスを停止します。 `service mi stop`
   c. mgmt-apiサービスを停止します。 `service mgmt-api stop`

d. SSH エージェントに SSH 秘密鍵を追加します。入力するコマンド`ssh-add`

e. に記載されているSSHアクセスパスワードを入力します `Passwords.txt` ファイル。

f. ソース管理ノードのデータベースをリカバリした管理ノードにコピーします。
`/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`

g. プロンプトが表示されたら、リカバリした管理ノードで MI データベースを上書きすることを確定します。

データベースとその履歴データが、リカバリした管理ノードにコピーされます。コピー処理が完了すると、リカバリした管理ノードがスクリプトによって起動されます。

h. 他のサーバにパスワードなしでアクセスする必要がなくなった場合は、 SSH エージェントから秘密鍵を削除します。入力するコマンド`ssh-add -D`

6. ソース管理ノードでサービスを再起動します。 `service servermanager start`

非プライマリ管理ノードをリカバリする際の**Prometheus**指標のリストア

## 非プライマリ管理ノードで障害が発生した場合、そのノード上の Prometheus で管理されていた過去の指標を必要に応じてリストアすることができます。

- リカバリした管理ノードをインストールして実行する必要があります。
- StorageGRID システムには管理ノードが少なくとも 2 つ必要です。
- を用意しておく必要があります `Passwords.txt` ファイル。
- プロビジョニングパスフレーズが必要です。

管理ノードで障害が発生すると、 Prometheus データベースで管理されていた管理ノード上の指標は失われます。管理ノードをリカバリする際に、ソフトウェアのインストールプロセスによって新しい Prometheus データベースが作成されます。リカバリした管理ノードを起動すると、 StorageGRID システムを新規にインストールした場合と同様に指標が記録されます。

非プライマリ管理ノードをリストアした場合は、プライマリ管理ノード（ *source Admin Node* ） の Prometheus データベースをリカバリした管理ノードにコピーすることで、過去の指標をリストアできます。

Prometheus データベースのコピーには 1 時間以上かかる場合があります。ソース管理ノードでサービスが停止している間は、グリッドマネージャの一部の機能が使用できなくなります。

1. ソース管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。
2. ソース管理ノードからPrometheusサービスを停止します。 `service prometheus stop`
3. リカバリした管理ノードで次の手順を実行します。
   a. リカバリした管理ノードにログインします。

i. 次のコマンドを入力します。 `ssh admin@grid_node_IP`

ii. に記載されているパスワードを入力します `Passwords.txt` ファイル。

iii. 次のコマンドを入力してrootに切り替えます。 `su -`

iv. に記載されているパスワードを入力します `Passwords.txt` ファイル。

b. Prometheusサービスを停止します。 `service prometheus stop`

c. SSH エージェントに SSH 秘密鍵を追加します。入力するコマンド`ssh-add`

d. に記載されているSSHアクセスパスワードを入力します `Passwords.txt` ファイル。

e. ソース管理ノードのPrometheusデータベースをリカバリした管理ノードにコピーします。
`/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`

f. プロンプトが表示されたら、 * Enter * を押して、リカバリした管理ノード上の新しい Prometheus データベースを破棄することを確認します。

元の Prometheus データベースとその履歴データが、リカバリした管理ノードにコピーされます。コピー処理が完了すると、リカバリした管理ノードがスクリプトによって起動されます。次のステータスが表示されます。

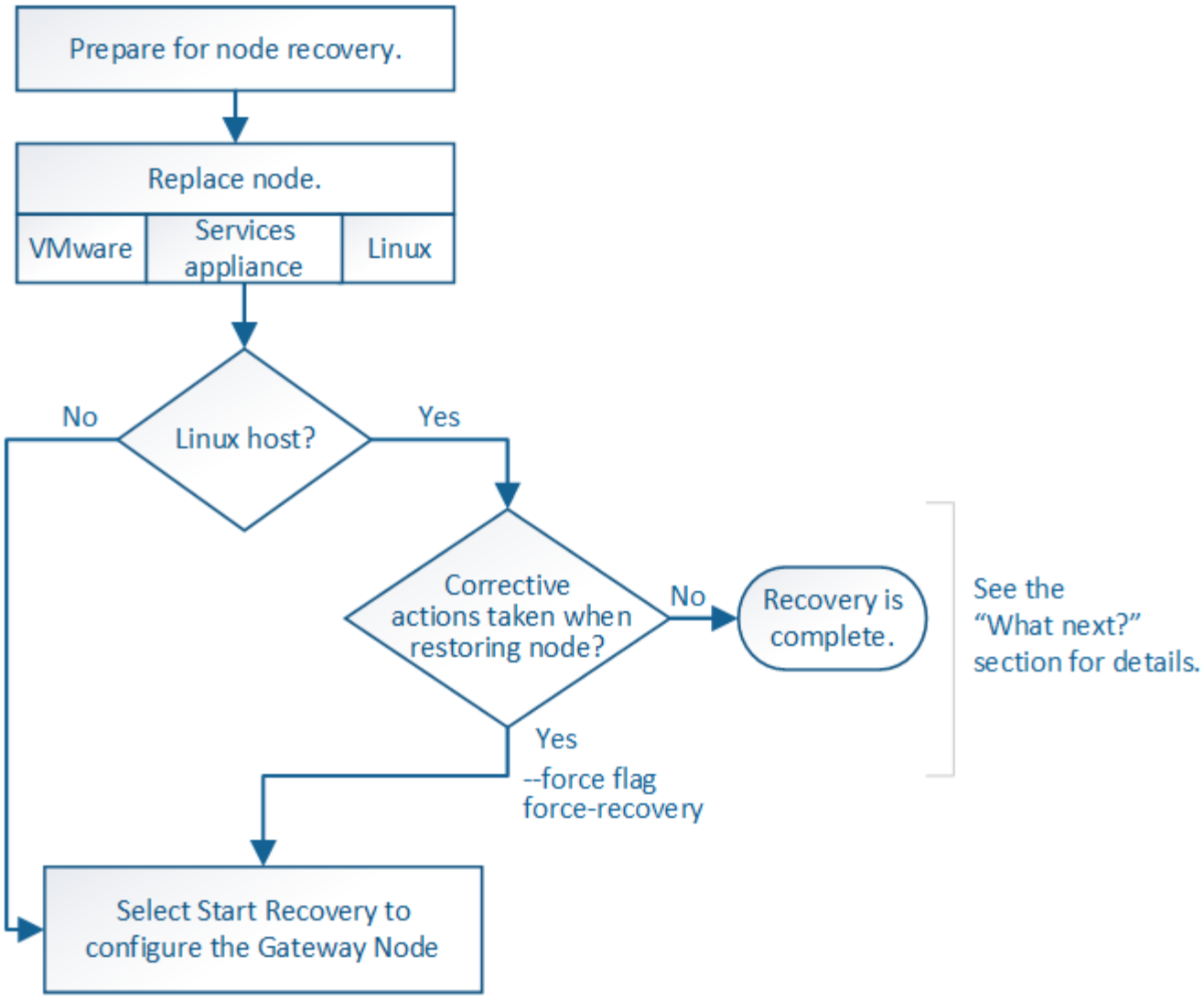
データベースのクローニング、サービスの開始

a. 他のサーバにパスワードなしでアクセスする必要がなくなった場合は、 SSH エージェントから秘密鍵を削除します。入力するコマンド`ssh-add -D`

4. ソース管理ノードでPrometheusサービスを再起動します.`service prometheus start`

ゲートウェイノードの障害からのリカバリ

## ゲートウェイノードの障害からリカバリするには、一連のタスクを正しい順序で実行する必要があります。




関連情報

"SG100 SG1000サービスアプライアンス"

手順

- "ゲートウェイノードの交換"
- "Start Recovery（リカバリの開始）を選択してゲートウェイノードを設定します"

ゲートウェイノードの交換

障害が発生したゲートウェイノードを同じ物理または仮想ハードウェアで実行されているゲートウェイノードと交換することも、 VMware または Linux ホストで実行されているゲートウェイノードをサービスアプライアンスでホストされているゲートウェイノードと交換することもできます。

ノードの交換用手順 を確認する必要があるのは、交換用ノードで使用するプラットフォームによって異なります。（すべてのノードタイプに適した）ノードの交換手順 が完了すると、手順 からゲートウェイノードのリカバリに関する次の手順が表示されます。

| 交換用プラットフォーム | 手順 |
| --- | --- |
| VMware | "VMwareノードの交換" |
| Linux の場合 | "Linuxノードの交換" |
| SG100 および SG1000 サービスアプライアンス | "サービスアプライアンスの交換" |
| OpenStack の機能を使用 | リカバリ処理を対象とした OpenStack 用の仮想マシンディスクファイルおよびスクリプトは、現在は提供されていません。OpenStack 環境で実行されているノードのリカバリが必要な場合は、使用している Linux オペレーティングシステム用のファイルをダウンロードしてください。その後、手順 に従って Linux ノードを交換します。 |

**Start Recovery**（リカバリの開始）を選択してゲートウェイノードを設定します

## ゲートウェイノードを交換したら、 Grid Manager で Start Recovery を選択して、障害が発生したノードの代わりとして新しいノードを設定する必要があります。

必要なもの

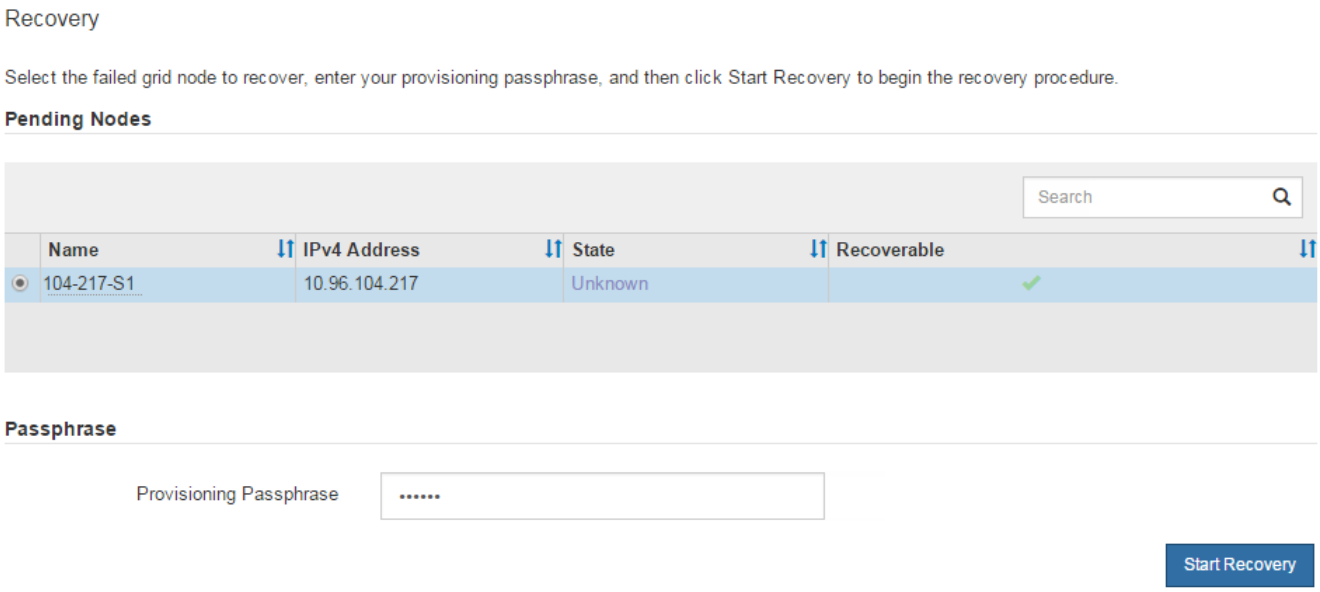
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Maintenance または Root Access 権限が必要です。
- プロビジョニングパスフレーズが必要です。
- 交換用ノードの導入と設定が完了している必要があります。

手順

1. Grid Managerから、* Maintenance * Maintenance Tasks * Recovery *（メンテナンス*メンテナンスタスク*リカバリ）を選択します。
2. リカバリするグリッドノードを Pending Nodes リストで選択します。

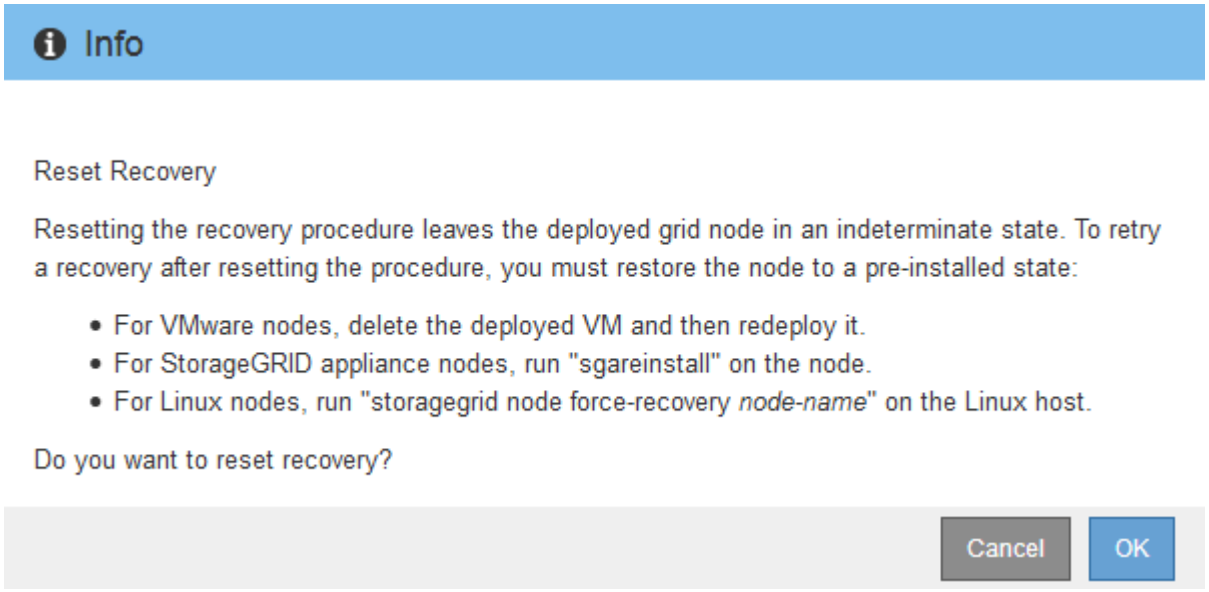
   ノードは障害が発生するとリストに追加されますが、再インストールされてリカバリの準備ができるまでは選択できません。

3. プロビジョニングパスフレーズ * を入力します。
4. [ リカバリの開始 ] をクリックします。




5. リカバリ中のグリッドノードテーブルで、リカバリの進行状況を監視します。

リカバリ手順 の実行中に [* リセット ] をクリックすると、新しいリカバリを開始できます。情報ダイアログボックスが表示され、手順 をリセットするとノードが不確定な状態のままになることが示されます。




手順 をリセットしたあとにリカバリを再試行する場合は、次の手順でノードをインストール前の状態にリストアする必要があります。

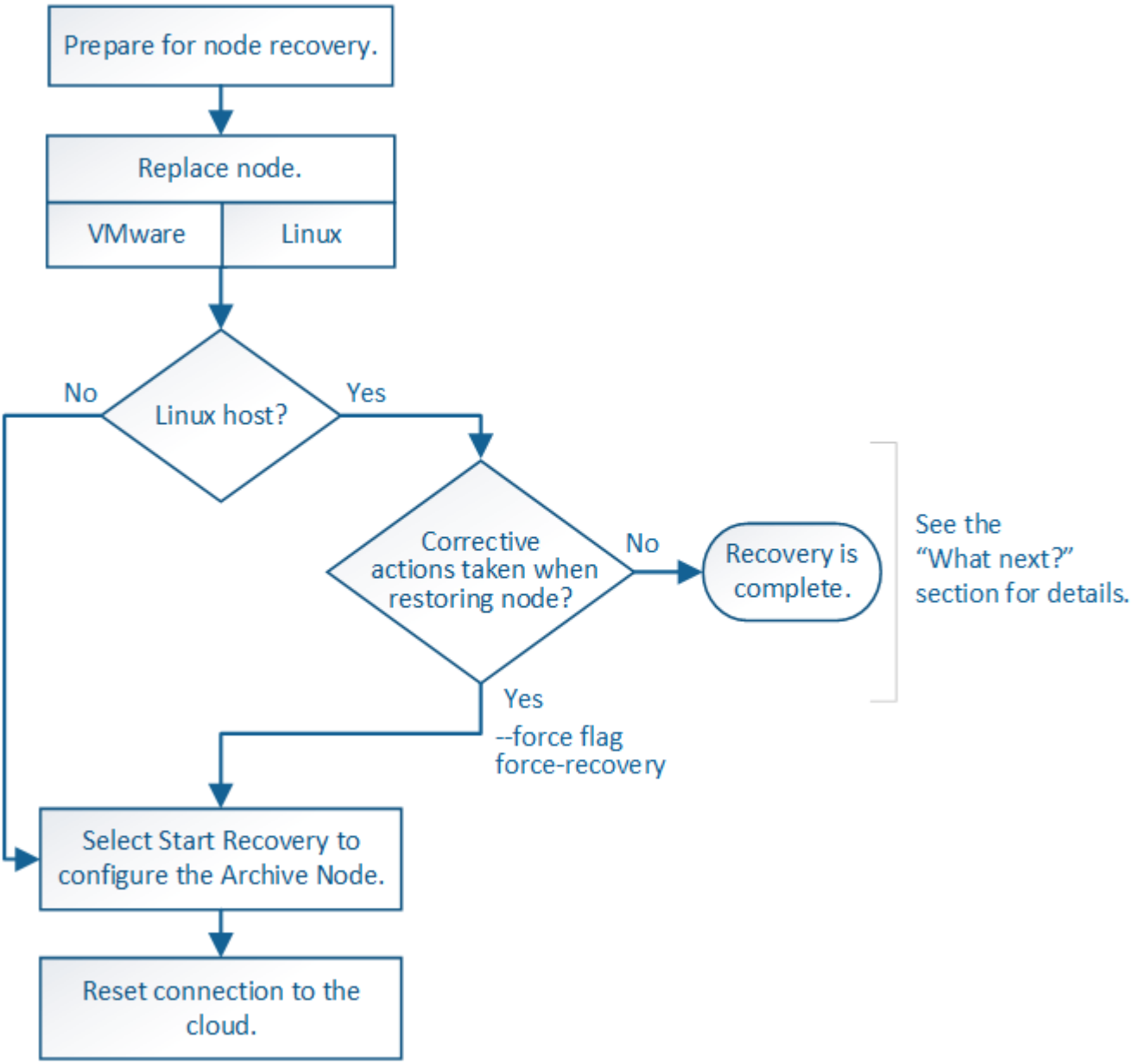
- * vmware * ：導入した仮想グリッドノードを削除します。その後、リカバリを再開する準備ができたら、ノードを再導入します。
- * Linux *：Linuxホストで次のコマンドを実行して、ノードを再起動します。 `storagegrid node force-recovery node-name`
- アプライアンス：手順 をリセットしたあとにリカバリを再試行する場合は、を実行してアプライアンスノードをインストール前の状態にリストアする必要があります `sgareinstall` をクリックします。

関連情報

"再インストールのためのアプライアンスの準備（プラットフォームの交換のみ）"

アーカイブノードの障害からのリカバリ

# アーカイブノードの障害からリカバリするには、一連のタスクを正しい順序で実行する必要があります。




このタスクについて

アーカイブノードのリカバリには、次の問題が影響します。

- 単一のコピーをレプリケートするように ILM ポリシーが設定されている場合。

  オブジェクトの単一のコピーを作成するように設定されている StorageGRID システムでは、アーカイブノードの障害によってデータが失われて回復できなくなる可能性があります。障害が発生すると ' これらのオブジェクトはすべて失われますが ' リカバリ手順を実行して StorageGRID システムをクリーンアップ

し ' 失われたオブジェクト情報をデータベースからパージする必要があります

- ストレージノードのリカバリ中にアーカイブノードで障害が発生した場合。

  ストレージノードのリカバリの一環として一括読み出しを処理中にアーカイブノードで障害が発生した場合は、 アーカイブノードから読み出したすべてのオブジェクトデータがストレージノードにリストアされるようにするには、手順 を繰り返してオブジェクトデータのコピーをストレージノードにリカバリする必要があります。

手順

- "アーカイブノードの交換"
- "Start Recoveryを選択して、アーカイブノードを設定します"
- "アーカイブノードからクラウドへの接続のリセット"

アーカイブノードの交換

## アーカイブノードをリカバリするには、まずノードの交換が必要です。

使用しているプラットフォームに対応するノード交換用手順 を選択する必要があります。ノードの交換手順は、すべてのタイプのグリッドノードで同じです。

| プラットフォーム | 手順 |
| --- | --- |
| VMware | "VMwareノードの交換" |
| Linux の場合 | "Linuxノードの交換" |
| OpenStack の機能を使用 | リカバリ処理を対象とした OpenStack 用の仮想マシンディスクファイルおよびスクリプトは、現在は提供されていません。OpenStack 環境で実行されているノードのリカバリが必要な場合は、使用している Linux オペレーティングシステム用のファイルをダウンロードしてください。その後、手順 に従って Linux ノードを交換します。 |

**Start Recovery**を選択して、アーカイブノードを設定します

## アーカイブノードを交換したら、 Grid Manager で Start Recovery を選択して、障害ノードの代わりとして新しいノードを設定する必要があります。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Maintenance または Root Access 権限が必要です。
- プロビジョニングパスフレーズが必要です。
- 交換用ノードの導入と設定が完了している必要があります。

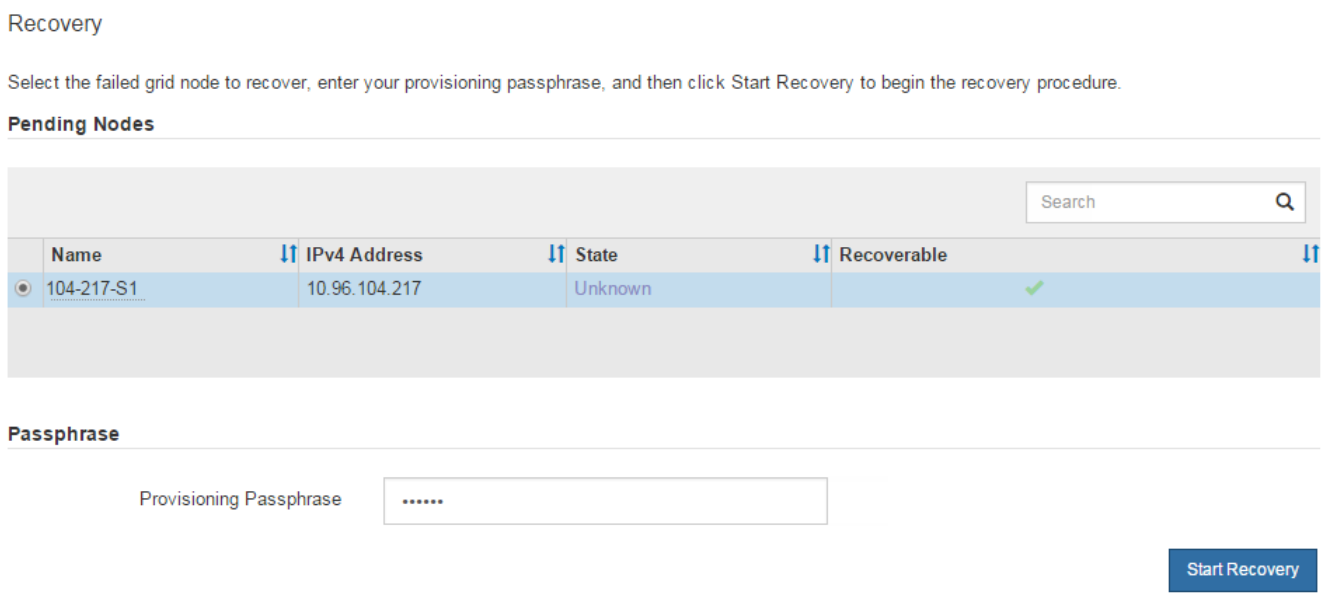
手順

1. Grid Managerから、* Maintenance * Maintenance Tasks * Recovery *（メンテナンス*メンテナンスタスク*リカバリ）を選択します。

2. リカバリするグリッドノードを Pending Nodes リストで選択します。

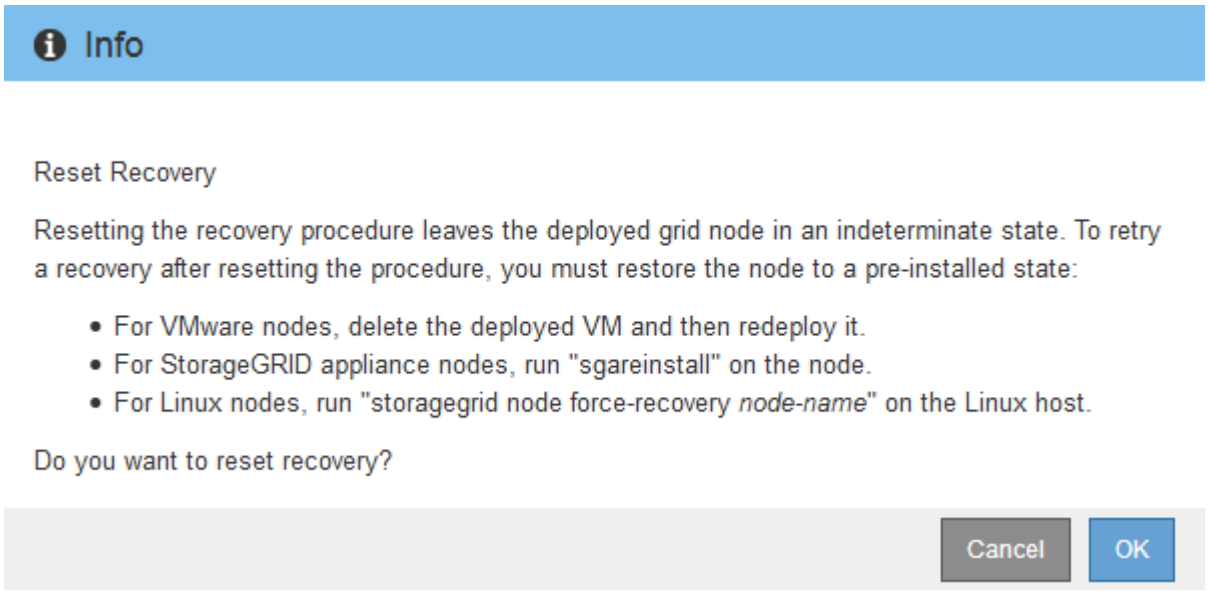
   ノードは障害が発生するとリストに追加されますが、再インストールされてリカバリの準備ができるまでは選択できません。

3. プロビジョニングパスフレーズ * を入力します。
4. [ リカバリの開始 ] をクリックします。




5. リカバリ中のグリッドノードテーブルで、リカバリの進行状況を監視します。

   リカバリ手順 の実行中に [* リセット ] をクリックすると、新しいリカバリを開始できます。情報ダイアログボックスが表示され、手順 をリセットするとノードが不確定な状態のままになることが示されます。




手順 をリセットしたあとにリカバリを再試行する場合は、次の手順でノードをインストール前の状態にリストアする必要があります。

- * vmware * ：導入した仮想グリッドノードを削除します。その後、リカバリを再開する準備ができたら、ノードを再導入します。
- * Linux *：Linuxホストで次のコマンドを実行して、ノードを再起動します。 `storagegrid node force-recovery node-name`

アーカイブノードからクラウドへの接続のリセット

## S3 API 経由でクラウドをターゲットとして使用するアーカイブノードをリカバリしたら、設定を変更して接続をリセットする必要があります。アーカイブノードがオブジェクトデータを読み出せない場合、 Outbound Replication Status （ ORSU ）アラームがトリガーされます。

アーカイブノードが TSM ミドルウェア経由で外部ストレージに接続されている場合は、ノードが自動的にリセットされるので再設定は不要です。

必要なもの

Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

手順

1. Support **>** Tools **>** Grid Topology *を選択します。
2. アーカイブノード* ARC *ターゲット*を選択します。
3. 誤った値を入力し、 * 変更の適用 * をクリックして、 * アクセスキー * フィールドを編集します。
4. 正しい値を入力し、 * 変更の適用 * をクリックして、 * アクセスキー * フィールドを編集します。

すべてのグリッドノードタイプ：**VMware**ノードの交換

## VMware でホストされていた障害 StorageGRID ノードをリカバリする場合は、障害ノードを削除してリカバリノードを導入する必要があります。

必要なもの

仮想マシンをリストアできず、交換しなければならないことを確認しておく必要があります。

このタスクについて

VMware vSphere Web Client を使用して、最初に障害グリッドノードに関連付けられた仮想マシンを削除します。その後、新しい仮想マシンを導入できます。

この手順 は、グリッドノードのリカバリプロセスの一部です。ノードの削除と導入の手順 は、管理ノード、ストレージノード、ゲートウェイノード、アーカイブノードを含むすべての VMware ノードで同じです。

手順

1. VMware vSphere Web Client にログインします。
2. 障害が発生したグリッドノード仮想マシンに移動します。
3. リカバリノードを導入するために必要なすべての情報をメモしておきます。
   a. 仮想マシンを右クリックし、 * 設定の編集 * タブを選択して、使用中の設定を確認します。
   b. [* vApp Options* ] タブを選択して、グリッドノードのネットワーク設定を表示し、記録します。

4. 障害グリッドノードがストレージノードである場合は、データストレージに使用されている仮想ハードディスクが破損していないかどうかを確認し、リカバリされたグリッドノードへの再接続に備えて保持しておきます。
5. 仮想マシンの電源をオフにします。
6. 仮想マシンを削除するには、* Actions **All vCenter Actions** Delete from Disk *を選択します。
7. 新しい仮想マシンを交換用ノードとして導入し、 1 つ以上の StorageGRID ネットワークに接続します。

   ノードを導入する際には、必要に応じてノードポートを再マッピングしたり、 CPU やメモリの設定を増やしたりできます。

   > 新しいノードを導入したら、ストレージ要件に従って新しい仮想ディスクを追加し、以前に削除した障害グリッドノードから保存した仮想ハードディスクを再接続するか、またはその両方を実行します。

   手順：

   "VMware をインストールする" 仮想マシンとしてのStorageGRID ノードの導入

8. リカバリするノードのタイプに応じて、ノードのリカバリ手順 を実行します。

| ノードのタイプ | に進みます |
| --- | --- |
| プライマリ管理ノード | "交換用プライマリ管理ノードの設定" |
| 非プライマリ管理ノード | "リカバリの開始を選択して非プライマリ管理ノードを設定します" |
| ゲートウェイノード | "Start Recovery（リカバリの開始）を選択してゲートウェイノードを設定します" |
| ストレージノード | "Start Recoveryを選択して、ストレージノードを設定します" |
| アーカイブノード | "Start Recoveryを選択して、アーカイブノードを設定します" |

すべてのグリッドノードタイプ：**Linux**ノードの交換

## 障害に対処するために 1 つ以上の新しい物理ホストまたは仮想ホストを導入するか、または既存のホストに Linux を再インストールする必要がある場合は、グリッドノードをリカバリする前に交換ホストを導入して設定する必要があります。この手順 は、すべてのタイプのグリッドノードのリカバリプロセスの 1 つのステップです。

「 Linux 」とは、 Red Hat ® Enterprise Linux ® 、 Ubuntu ® 、 CentOS 、または Debian ® の環境を指します。サポートされているバージョンの一覧については、 NetApp Interoperability Matrix Tool を参照してください。

この手順 は、ソフトウェアベースのストレージノード、プライマリまたは非プライマリ管理ノード、ゲートウェイノード、またはアーカイブノードのリカバリプロセスの一部としてのみ実行されます。リカバリするグリッドノードのタイプに関係なく、手順は同じです。

物理 / 仮想 Linux ホストで複数のグリッドノードがホストされている場合は、任意の順序でグリッドノードをリカバリできます。ただし、プライマリ管理ノードがある場合は最初にリカバリします。リカバリのためにプライマリ管理ノードに接続しようとするときに、他のグリッドノードのリカバリが停止することはありません。

1. "新しいLinuxホストの導入"
2. "ホストへのグリッドノードのリストア"
3. "次の手順：必要に応じて追加のリカバリ手順を実行します"

関連情報

"NetApp Interoperability Matrix Tool で確認できます"

新しい**Linux**ホストの導入

## いくつかの例外を除き、最初のインストールプロセス時と同じ方法で新しいホストを準備します。

新規または再インストールされた物理 / 仮想 Linux ホストを導入するには、お使いの Linux オペレーティングシステム用の StorageGRID のインストール手順に記載されているホストの準備について、手順 で説明しています。

この手順 には、次のタスクが含まれています。

1. Linux をインストールします。
2. ホストネットワークを設定する。
3. ホストストレージを設定する。
4. Dockerをインストールする。
5. StorageGRID ホストサービスをインストールする。

> インストール手順の「 Install StorageGRID host service 」タスクを完了した後で停止します。「グリッドノードの配置」タスクは開始しないでください。

これらの手順を実行する際は、次の重要なガイドラインに注意してください。

- 元のホストと同じホストインターフェイス名を使用してください。
- 共有ストレージを使用して StorageGRID ノードをサポートする場合や、障害ノードから一部またはすべてのディスクドライブ / SSD を交換ノードに移動した場合は、元のホストと同じストレージマッピングを再確立する必要があります。たとえば、でWWIDとエイリアスを使用していた場合などです `/etc/multipath.conf` インストール手順で推奨されるように、で同じエイリアス/ WWIDのペアを使用してください `/etc/multipath.conf` 交換用ホスト。
- StorageGRID ノードが NetApp AFF システムから割り当てられたストレージを使用している場合は、ボリュームで FabricPool 階層化ポリシーが有効になっていないことを確認してください。StorageGRID ノードで使用するボリュームで FabricPool による階層化を無効にすることで、トラブルシューティングとストレージの処理がシンプルになります。

StorageGRID を使用して StorageGRID に関連するデータを FabricPool 自体に階層化しないでください。StorageGRID データを StorageGRID に階層化すると、トラブルシューティングと運用がより複雑になります。

関連情報

"Red Hat Enterprise Linux または CentOS をインストールします"

"Ubuntu または Debian をインストールします"

ホストへのグリッドノードのリストア

# 障害グリッドノードを新しい Linux ホストにリストアするには、適切なコマンドを使用してノード構成ファイルをリストアします。

新規インストールを実行するときは、ホストにインストールするグリッドノードごとにノード構成ファイルを作成します。交換ホストにグリッドノードをリストアするときは、障害グリッドノードのノード構成ファイルをリストアまたは交換します。

以前のホストのブロックストレージボリュームが保持されている場合は、追加のリカバリ手順の実行が必要になることがあります。このセクションのコマンドを使用して、必要な追加手順を特定できます。

手順

- "グリッドノードのリストアと検証"
- "StorageGRID ホストサービスを開始しています"
- "正常に開始しないノードのリカバリ"

グリッドノードのリストアと検証

# 障害グリッドノードのグリッド構成ファイルをリストアして検証し、エラーをすべて解決する必要があります。

このタスクについて

ホストに必要なグリッドノードは、すべてインポートできます `/var/local` 前のホストで障害が発生したためにボリュームが失われませんでした。たとえば、などです `/var/local` 使用しているLinuxオペレーティングシステムでのStorageGRID のインストール手順に従って、StorageGRID システムのデータボリュームに共有ストレージを使用していた場合は、ボリュームが残っている可能性があります。ノードをインポートすると、ノード構成ファイルがホストにリストアされます。

ノードをインポートできない場合は、グリッド構成ファイルを再作成する必要があります。

次に、 StorageGRID の再起動に進む前に、グリッド構成ファイルを検証し、予想されるネットワークまたはストレージの問題を解決する必要があります。ノードの構成ファイルを再作成する場合は、リカバリするノードに使用されていたのと同じ名前を交換用ノードに使用する必要があります。

の場所の詳細については、インストール手順を参照してください `/var/local` ノードのボリューム。

手順

1. リカバリしたホストのコマンドラインで、現在設定されているすべてのStorageGRID グリッドノードを表

示します。`sudo storagegrid node list`

グリッドノードが設定されていない場合、出力は表示されません。グリッドノードが設定されている場合は、次の形式で出力が表示されます。

```
Name                Metadata-Volume
=====================================================================
dc1-adm1            /dev/mapper/sgws-adm1-var-local
dc1-gw1             /dev/mapper/sgws-gw1-var-local
dc1-sn1             /dev/mapper/sgws-sn1-var-local
dc1-arc1            /dev/mapper/sgws-arc1-var-local
```

ホストで設定する必要のある一部またはすべてのグリッドノードが表示されない場合は、そのグリッドノードをリストアする必要があります。

2. を含むグリッドノードをインポートします `/var/local` ボリューム：

   a. インポートする各ノードに対して次のコマンドを実行します。`sudo storagegrid node import node-var-local-volume-path`

   。 `storagegrid node import` コマンドが成功するのは、対象のノードが最後に実行されたホストでクリーンシャットダウンされている場合のみです。そうでない場合は、次のようなエラーが表示されます。

   `This node (node-name) appears to be owned by another host (UUID host-uuid).`

`Use the --force flag if you are sure import is safe.`

   a. 別のホストが所有しているノードに関するエラーが表示された場合は、を指定してもう一度コマンドを実行します `--force` インポートを完了するためのフラグ：`sudo storagegrid --force node import node-var-local-volume-path`

> を使用してインポートされたノード `--force` フラグは、「必要に応じた追加のリカバリ手順の実行」の説明に従って、グリッドに再参加する前に追加のリカバリ手順を必要とします。

3. がないグリッドノード `/var/local` ボリュームで、ノードの構成ファイルを再作成してホストにリストアします。

   インストール手順の「ノード構成ファイルの作成」のガイドラインに従ってください。

> ノードの構成ファイルを再作成する場合は、リカバリするノードに使用されていたのと同じ名前を交換用ノードに使用する必要があります。Linux 環境の場合は、構成ファイルの名前にノード名が含まれていることを確認します。可能な場合は、同じネットワークインターフェイス、ブロックデバイスマッピング、および IP アドレスを使用してください。これにより、リカバリ時にノードにコピーしなければならないデータ量を最小限に抑えることができるため、リカバリにかかる時間を大幅に（場合によっては、数週間から数分に）短縮できます。

新しいブロックデバイス（StorageGRID ノードで以前に使用していなかったデバイス）を、で始まる設定変数の値として使用する場合 `BLOCK_DEVICE_` ノードの構成ファイルを再作成するときは、「ブロックデバイスが見つからないエラーの修正」のすべてのガイドラインに従ってください。

4. リカバリしたホストで次のコマンドを実行して、すべての StorageGRID ノードを一覧表示します。

   ```
   sudo storagegrid node list
   ```

5. StorageGRID のノードリストの出力に表示されている各グリッドノードのノード構成ファイルを検証します。

   ```
   sudo storagegrid node validate node-name
   ```

   StorageGRID ホストサービスを開始する前に、すべてのエラーまたは警告に対処する必要があります。以下のセクションでは、リカバリ時に特に問題となるエラーについて詳しく説明します。

関連情報

"Red Hat Enterprise Linux または CentOS をインストールします"

"Ubuntu または Debian をインストールします"

"ネットワークインターフェイスが見つからないエラーの修正"

"ブロックデバイスが見つからないエラーの修正"

"次の手順：必要に応じて追加のリカバリ手順を実行します"

ネットワークインターフェイスが見つからないエラーの修正

## ホストネットワークが正しく設定されていない場合や名前のスペルが間違っている場合、StorageGRID がで指定されたマッピングを確認する際にエラーが発生します `/etc/storagegrid/nodes/node-name.conf` ファイル。

次のエラーまたは警告が表示されることがあります。

`Checking configuration file `/etc/storagegrid/nodes/node-name.conf` <ノード名>の場合> `ERROR: *node-name*: GRID_NETWORK_TARGET = *host-interface-name*``*node-name*:インターフェイス'_host-interface-name'は存在しません

エラーは、グリッドネットワーク、管理ネットワーク、またはクライアントネットワークについて報告される場合があります。このエラーは、を意味します `/etc/storagegrid/nodes/node-name.conf` ファイルは、指定されたStorageGRID ネットワークをというホストインターフェイスにマッピングします `*host-interface-name*`とはいえ、現在のホストには、この名前のインターフェイスがありません。

このエラーが表示された場合は、「新しいLinuxホストの導入」の手順を完了していることを確認してください。すべてのホストインターフェイスに、元のホストで使用されていた名前と同じ名前を使用します。

ノード構成ファイルに指定されている名前をホストインターフェイスに付けることができない場合は、ノード構成ファイルを編集して、 GRID_NETWORK_TARGET 、 ADMIN_NETWORK_TARGET 、または CLIENT_network_target の値を既存のホストインターフェイスに一致するように変更できます。

ホストインターフェイスが適切な物理ネットワークポートまたは VLAN へのアクセスを提供し、インターフェイスがボンドデバイスまたはブリッジデバイスを直接参照していないことを確認してください。ホストのボンドデバイスの上に VLAN （または他の仮想インターフェイス）を設定するか、ブリッジと仮想イーサネット（ veth ）のペアを使用する必要があります。

関連情報

"新しいLinuxホストの導入"

ブロックデバイスが見つからないエラーの修正

システムは、リカバリされた各ノードが有効なブロックデバイススペシャルファイル、またはブロックデバイススペシャルファイルへの有効なソフトリンクにマッピングされていることを確認します。StorageGRID がで無効なマッピングを検出した場合 `/etc/storagegrid/nodes/node-name.conf` ファイル。ブロックデバイスが見つからないことを示すエラーが表示されます。

次のエラーが発生することがあります。

```
Checking configuration file /etc/storagegrid/nodes/node-name.conf for node node-name…
ERROR: node-name: BLOCK_DEVICE_PURPOSE = path-name``node-name:_path-name_does not exist
```

これはそのことを意味します `/etc/storagegrid/nodes/node-name.conf` Linuxファイルシステムで特定のパス名に目的として_node-name_forで使用されているブロックデバイスをマッピングしますが、有効なブロックデバイススペシャルファイル、またはブロックデバイススペシャルファイルへのソフトリンクがこの場所にありません。

「新しいLinuxホストの導入」の手順を完了したことを確認します。すべてのブロックデバイスに、元のホストで使用されていたのと同じ永続的なデバイス名を使用します。

見つからないブロックデバイスのスペシャルファイルをリストアまたは再作成できない場合は、適切なサイズとストレージカテゴリの新しいブロックデバイスを割り当て、ノード構成ファイルを編集して新しいブロックデバイスのスペシャルファイルを参照するように block_device_purpose の値を変更します。

Linux オペレーティングシステムのインストール手順の「ストレージ要件」の表から適切なサイズとストレージカテゴリを決定します。ブロック・デバイスの交換に進む前に ' ホスト・ストレージの構成に記載されている推奨事項を確認してください

で始まる構成ファイル変数に新しいブロックストレージデバイスを指定する必要がある場合 `BLOCK_DEVICE_` 元のブロックデバイスは障害ホストとともに失われたため、リカバリ手順を進める前に新しいブロックデバイスがフォーマットされていないことを確認してください。共有ストレージを使用していて新しいボリュームを作成済みの場合、新しいブロックデバイスはアンフォーマットされます。状況がわからない場合は、新しいブロックストレージデバイスのスペシャルファイルに対して次のコマンドを実行します。

次のコマンドは、新しいブロックストレージデバイスに対してのみ実行してください。デバイス上のデータがすべて失われるため、リカバリされているノードの有効なデータがブロックストレージに格納されている可能性がある場合は、このコマンドを実行しないでください。

```
sudo dd if=/dev/zero of=/dev/mapper/my-block-device-name bs=1G count=1
```

関連情報

"新しいLinuxホストの導入"

"Red Hat Enterprise Linux または CentOS をインストールします"

"Ubuntu または Debian をインストールします"

**StorageGRID** ホストサービスを開始しています

## StorageGRID ノードを起動し、ホストのリブート後もノードが再起動されるようにするには、 StorageGRID ホストサービスを有効にして開始する必要があります。

1. 各ホストで次のコマンドを実行します。

   ```
   sudo systemctl enable storagegrid
   sudo systemctl start storagegrid
   ```

2. 次のコマンドを実行して、導入の進行状況を確認します。

   ```
   sudo storagegrid node status node-name
   ```

   ステータスが Not-Running または Stopped に対して、次のコマンドを実行します。

   ```
   sudo storagegrid node start node-name
   ```

3. StorageGRID ホストサービスを以前に有効にして開始している場合（またはサービスを有効にして開始したかどうかがわからない場合）は、次のコマンドも実行します。

   ```
   sudo systemctl reload-or-restart storagegrid
   ```

正常に開始しないノードのリカバリ

## グリッドに正常に再参加できずリカバリ可能と表示されない StorageGRID ノードは破損している可能性があります。ノードを強制的にリカバリモードに設定することができます。

ノードを強制的にリカバリモードにするには、次の手順を実行

```
sudo storagegrid node force-recovery node-name
```

このコマンドを実行する前に、ノードのネットワーク設定が正しいことを確認してください。ネットワークインターフェイスのマッピングまたはグリッドネットワークの IP アドレスまたはゲートウェイが正しくないために、ノードがグリッドに再参加できなかった可能性があります。

を発行した後 `storagegrid node force-recovery node-name` コマンドを使用して、_node-name _についての追加のリカバリ手順を実行する必要があります。

関連情報

"次の手順：必要に応じて追加のリカバリ手順を実行します"

次の手順：必要に応じて追加のリカバリ手順を実行します

## 交換ホストで実行されている StorageGRID ノードをリカバリした方法によっては、ノードごとに追加のリカバリ手順を実行する必要があります。

Linux ホストを交換、または障害グリッドノードを新しいホストにリストアした際に対応処置が不要であった場合は、ノードのリカバリはこれで完了です。

対処方法と次の手順

ノードの交換時に次のいずれかの対応処置を実施した可能性があります。

- を使用する必要がありました `--force` ノードをインポートするためのフラグ。
- を使用できます `<PURPOSE>`、の値 `BLOCK_DEVICE_<PURPOSE>` 構成ファイル変数とは、ホスト障害前と同じデータを含んでいないブロックデバイスを指します。
- あなたは発行しました `storagegrid node force-recovery node-name` をクリックします。
- 新しいブロックデバイスを追加した。

これらの対処方法のいずれかを実行した場合は、追加のリカバリ手順を実行する必要があります。

| リカバリのタイプ | 次の手順に進みます |
| --- | --- |
| プライマリ管理ノード | "交換用プライマリ管理ノードの設定" |
| 非プライマリ管理ノード | "リカバリの開始を選択して非プライマリ管理ノードを設定します" |
| ゲートウェイノード | "Start Recovery（リカバリの開始）を選択してゲートウェイノードを設定します" |
| アーカイブノード | "Start Recoveryを選択して、アーカイブノードを設定します" |

| リカバリのタイプ | 次の手順に進みます |
| --- | --- |
| ストレージノード（ソフトウェアベース）：<br>• を使用しなければならなかった場合 `--force` ノードをインポートするためのフラグ、またはを実行した `storagegrid node force-recovery node-name`<br>• ノードの完全な再インストールを実行する必要があった場合や、 /var/local をリストアする必要があった場合 | "Start Recoveryを選択して、ストレージノードを設定します" |
| ストレージノード（ソフトウェアベース）：<br>• 新しいブロックデバイスを追加した場合。<br>• 該当する場合 `<PURPOSE>`、の値 `BLOCK_DEVICE_<PURPOSE>` 構成ファイル変数とは、ホスト障害前と同じデータを含んでいないブロックデバイスを指します。 | "システムドライブに損傷がない場合のストレージボリューム障害からのリカバリ" |

障害が発生したノードをサービスアプライアンスと交換する

SG100 または SG1000 サービスアプライアンスを使用して、障害が発生したゲートウェイノード、障害が発生した非プライマリ管理ノード、または VMware 、 Linux ホスト、サービスアプライアンスでホストされていた障害が発生したプライマリ管理ノードをリカバリできます。この手順 は、グリッドノードのリカバリ手順 の 1 つのステップです。

必要なもの

- 次のいずれかの状況に該当することを確認しておく必要があります。
  - ノードをホストしている仮想マシンをリストアできない。
  - グリッドノードの物理 / 仮想 Linux ホストに障害が発生したため、交換する必要がある。
  - グリッドノードをホストしているサービスアプライアンスを交換する必要があります。
- StorageGRID アプライアンスインストーラのバージョンを確認およびアップグレードするためのハードウェアの設置とメンテナンスの説明に従って、サービスアプライアンス上の StorageGRID アプライアンスインストーラのバージョンが StorageGRID システムのソフトウェアバージョンと一致していることを確認する必要があります。

  "SG100 SG1000サービスアプライアンス"

> SG100 と SG1000 サービスアプライアンスの両方を同じサイトに導入しないでください。パフォーマンスが予測不能になる可能性があります

このタスクについて

次の場合は、 SG100 または SG1000 サービスアプライアンスを使用して、障害が発生したグリッドノードをリカバリできます。

- 障害ノードが VMware または Linux でホストされていた（プラットフォームの変更）
- 障害ノードがサービスアプライアンスでホストされていた（プラットフォームの交換）

手順

- "サービスアプライアンスの設置（プラットフォーム変更のみ）"
- "再インストールのためのアプライアンスの準備（プラットフォームの交換のみ）"
- "サービスアプライアンスでソフトウェアのインストールを開始します"
- "サービスアプライアンスのインストールの監視"

サービスアプライアンスの設置（プラットフォーム変更のみ）

## 交換用ノードに SG100 または SG1000 サービスアプライアンスを使用していた、VMware または Linux ホストでホストされていた障害グリッドノードをリカバリする場合は、最初に障害ノードと同じノード名を使用して新しいアプライアンスハードウェアを設置する必要があります。

障害ノードに関する次の情報が必要です。

- * ノード名 * ：障害が発生したノードと同じノード名を使用してサービスアプライアンスをインストールする必要があります。
- * IP アドレス * ：障害が発生したノードと同じ IP アドレスをサービスアプライアンスに割り当てることができます。これは推奨されるオプションであり、各ネットワークで新しい未使用の IP アドレスを選択することもできます。

この手順 は、 VMware または Linux でホストされていた障害ノードをサービスアプライアンスでホストされているノードと交換してリカバリする場合にのみ実行してください。

1. 新しい SG100 または SG1000 サービスアプライアンスの設置手順に従ってください。
2. ノード名の入力を求められたら、障害ノードのノード名を使用します。

関連情報

"SG100 SG1000サービスアプライアンス"

再インストールのためのアプライアンスの準備（プラットフォームの交換のみ）

## サービスアプライアンスでホストされていたグリッドノードをリカバリする場合は、最初に StorageGRID ソフトウェアを再インストールするアプライアンスを準備する必要があります。

この手順 は、サービスアプライアンスでホストされていた障害ノードを交換する場合にのみ実行してください。障害ノードが VMware または Linux ホストでホストされていた場合は実行しないでください。

1. 障害が発生したグリッドノードにログインします。
    a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
    b. に記載されているパスワードを入力します `Passwords.txt` ファイル。

c. 次のコマンドを入力してrootに切り替えます。 `su -`

d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

2. StorageGRID ソフトウェアをアプライアンスにインストールする準備をします。入力するコマンド `sgareinstall`

3. 続行するかどうかを尋ねられたら、と入力します。 `y`

アプライアンスがリブートされ、 SSH セッションが終了します。通常は 5 分程度で StorageGRID アプライアンスインストーラが使用可能になりますが、場合によっては最大で 30 分待つ必要があります。

サービスアプライアンスがリセットされ、グリッドノード上のデータにアクセスできなくなります。元のインストールプロセスで設定した IP アドレスはそのまま使用する必要がありますが、手順 の完了時に確認しておくことを推奨します。

を実行したあとに `sgareinstall` コマンドを実行すると、StorageGRIDでプロビジョニングされたすべてのアカウント、パスワード、およびSSHキーが削除され、新しいホストキーが生成されます。

サービスアプライアンスでソフトウェアのインストールを開始します

## ゲートウェイノードまたは管理ノードを SG100 または SG1000 サービスアプライアンスにインストールするには、アプライアンスに含まれている StorageGRID アプライアンスインストーラを使用します。

必要なもの

- アプライアンスをラックに設置し、ネットワークに接続し、電源を投入しておく必要があります。
- StorageGRID アプライアンスインストーラを使用してアプライアンスのネットワークリンクと IP アドレスを設定する必要があります。
- ゲートウェイノードまたは非プライマリ管理ノードをインストールする場合は、 StorageGRID グリッドのプライマリ管理ノードの IP アドレスを確認しておきます。
- StorageGRID アプライアンスインストーラの IP 設定ページに表示されるすべてのグリッドネットワークサブネットを、プライマリ管理ノードのグリッドネットワークサブネットリストで定義する必要があります。

これらの必要な準備作業の実行手順については、 SG100 または SG1000 サービスアプライアンスのインストールとメンテナンスの手順を参照してください。

- サポートされているWebブラウザを使用する必要があります。
- アプライアンスに割り当てられている IP アドレスのいずれかを確認しておく必要があります。管理ネットワーク、グリッドネットワーク、またはクライアントネットワークの IP アドレスを使用できます。
- プライマリ管理ノードをインストールする場合は、このバージョンの StorageGRID 用の Ubuntu または Debian のインストールファイルが必要です。

> 最新バージョンの StorageGRID ソフトウェアは、製造時にサービスアプライアンスにプリロードされています。プリロードバージョンのソフトウェアが StorageGRID 環境で使用されているバージョンと同じ場合、インストールファイルは必要ありません。

このタスクについて

SG100 または SG1000 サービスアプライアンスに StorageGRID ソフトウェアをインストールするには、次の手順を実行します。

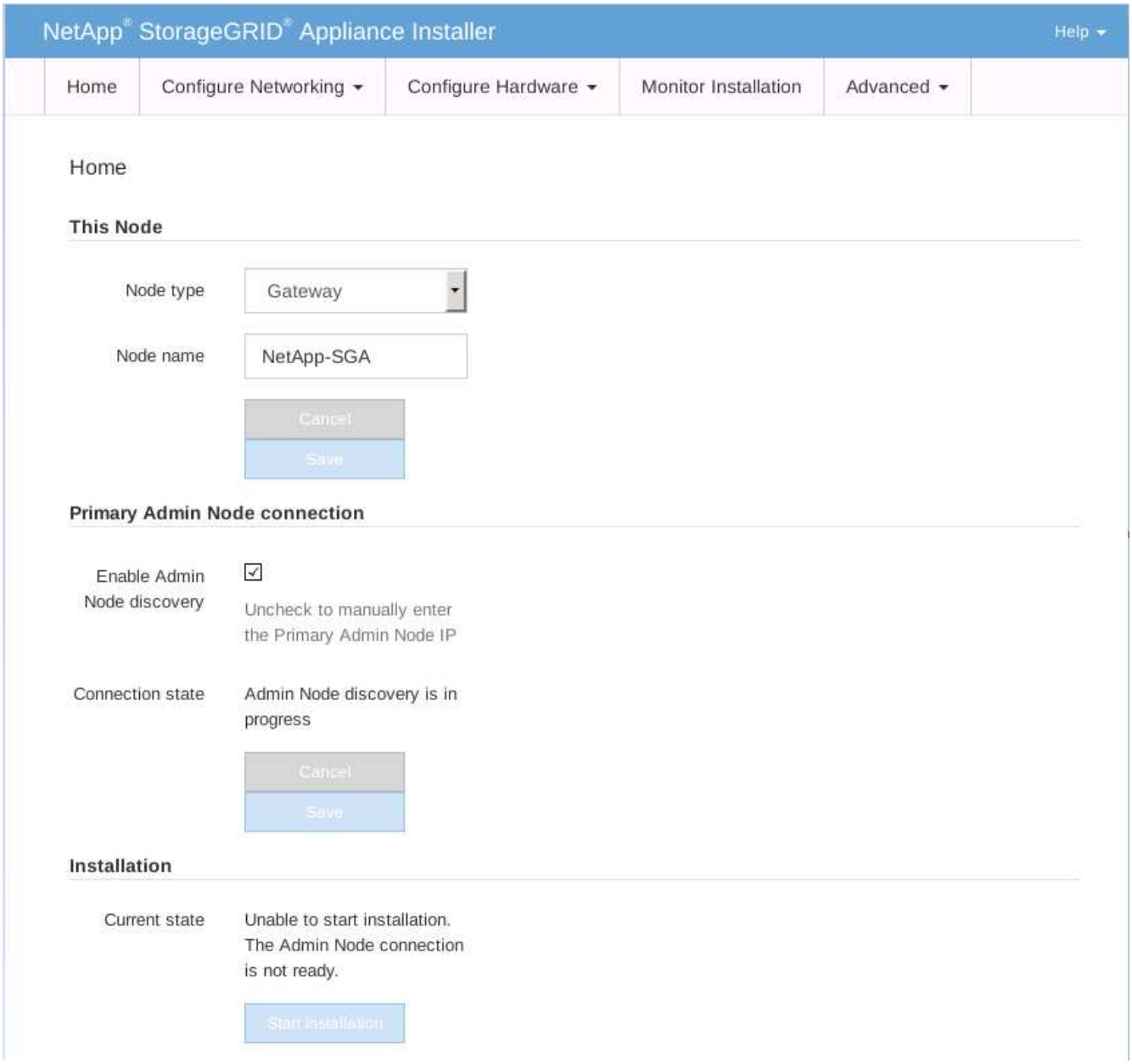
- プライマリ管理ノードの場合は、ノードの名前を指定し、必要に応じて適切なソフトウェアパッケージをアップロードします。
- 非プライマリ管理ノードまたはゲートウェイノードの場合は、プライマリ管理ノードの IP アドレスとノードの名前を指定または確認します。
- インストールを開始し、ボリュームの設定とソフトウェアのインストールが行われている間待機します。
- プロセスの途中でインストールが一時停止します。インストールを再開するには、 Grid Manager にサインインして、保留状態のノードを障害ノードの代わりとして設定する必要があります。
- ノードを設定すると、アプライアンスのインストールプロセスが完了してアプライアンスがリブートされます。

手順

1. ブラウザを開き、 SG100 または SG1000 サービスアプライアンスの IP アドレスのいずれかを入力します。

   ```
   https://Controller_IP:8443
   ```

   StorageGRID アプライアンスインストーラのホームページが表示されます。




2. プライマリ管理ノードをインストールするには、次の手順に従います。

   a. このノードセクションで、 * ノードタイプ * に * プライマリ管理者 * を選択します。

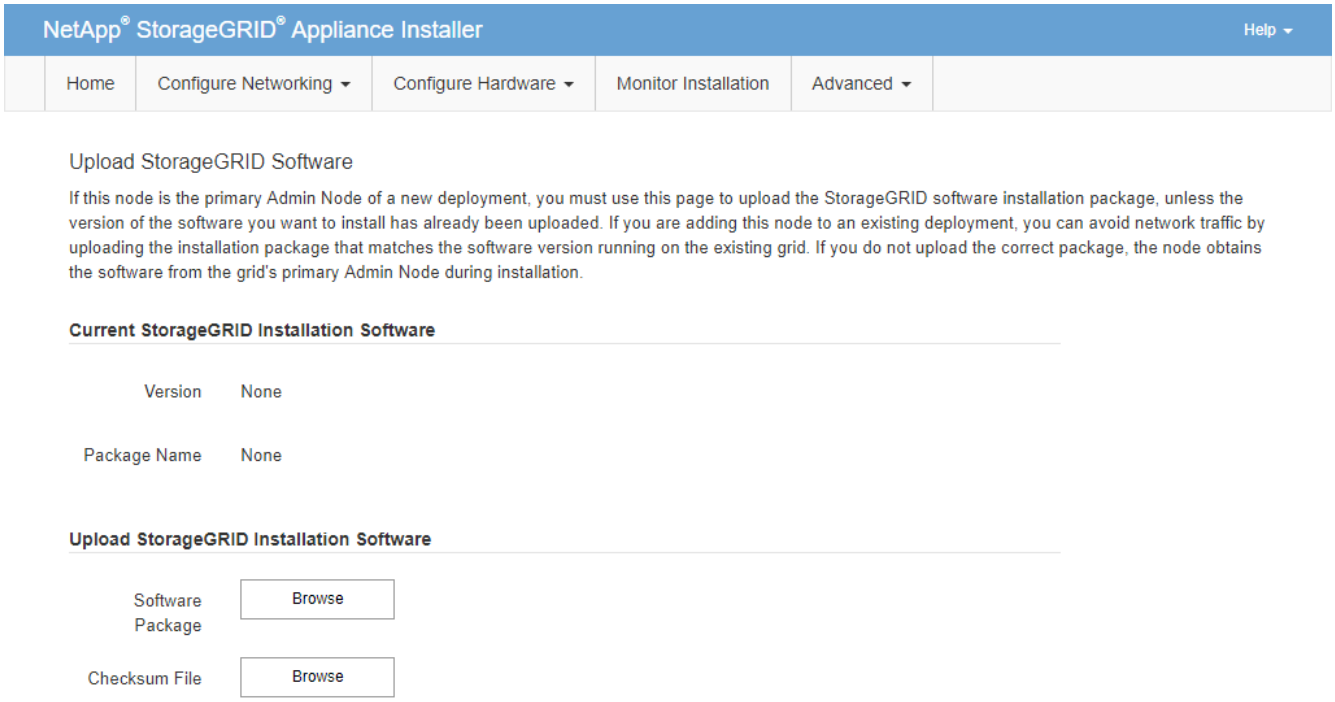
   b. [ ノード名 *] フィールドに ' リカバリするノードに使用されていた名前を入力し '[ 保存 *] をクリックします

   c. [ インストール ] セクションで、 [ 現在の状態 ] の下に表示されているソフトウェアバージョンを確認します

      インストールできるソフトウェアのバージョンが正しい場合は、に進みます インストール手順。

   d. 別のバージョンのソフトウェアをアップロードする必要がある場合は、 * 詳細設定 * メニューで * StorageGRID ソフトウェアのアップロード * を選択します。

      [Upload StorageGRID Software] ページが表示されます。




a. [* 参照 ] をクリックして、 StorageGRID ソフトウェア用の * ソフトウェア・パッケージ * および * チェックサム・ファイル * をアップロードします。

   選択したファイルが自動的にアップロードされます。

b. StorageGRID アプライアンス・インストーラのホームページに戻るには、 * ホーム * をクリックします。

3. ゲートウェイノードまたは非プライマリ管理ノードをインストールするには、次の手順を実行します。

a. このノードセクションで、 * ノードタイプ * には、リストアするノードのタイプに応じて * ゲートウェイ * または * 非プライマリ管理 * を選択します。

b. [ ノード名 *] フィールドに ' リカバリするノードに使用されていた名前を入力し '[ 保存 *] をクリックします

c. プライマリ管理ノードの接続セクションで、プライマリ管理ノードの IP アドレスを指定する必要があるかどうかを確認します。

   プライマリ管理ノードまたは ADMIN_IP が設定された少なくとも 1 つのグリッドノードが同じサブネットにある場合は、 StorageGRID アプライアンスインストーラがこの IP アドレスを自動的に検出します。

d. この IP アドレスが表示されない場合や変更する必要がある場合は、アドレスを指定します。

| オプション | 説明 |
| --- | --- |
| IP を手動で入力します | a. Enable Admin Node discovery * チェックボックスの選択を解除します。<br>b. IP アドレスを手動で入力します。<br>c. [ 保存（ Save ） ] をクリックします。<br>d. 新しい IP アドレスの接続状態が「 ready 」になるまで待機します。 |
| 接続されたすべてのプライマリ管理ノードの自動検出 | a. Enable Admin Node discovery * チェックボックスを選択します。<br>b. 検出された IP アドレスのリストから、このサービスアプライアンスを導入するグリッドのプライマリ管理ノードを選択します。<br>c. [ 保存（ Save ） ] をクリックします。<br>d. 新しい IP アドレスの接続状態が「 ready 」になるまで待機します。 |

4. インストールセクションで、現在の状態がノード名のインストールを開始する準備ができていること、および * インストールの開始 * ボタンが有効になっていることを確認します。

   [Start Installation*（インストールの開始） ] ボタンが有効になっていない場合は、ネットワーク設定またはポート設定の変更が必要になることがあります。手順については、使用しているアプライアンスのインストールとメンテナンスの手順を参照してください。

5. StorageGRID アプライアンスインストーラのホームページで、 * インストールの開始 * をクリックします。

   現在の状態が「 Installation is in progress 」に変わり、「 Monitor Installation 」ページが表示されます。

   モニタのインストールページに手動でアクセスする必要がある場合は、メニューバーから * モニタのインストール * をクリックします。

関連情報

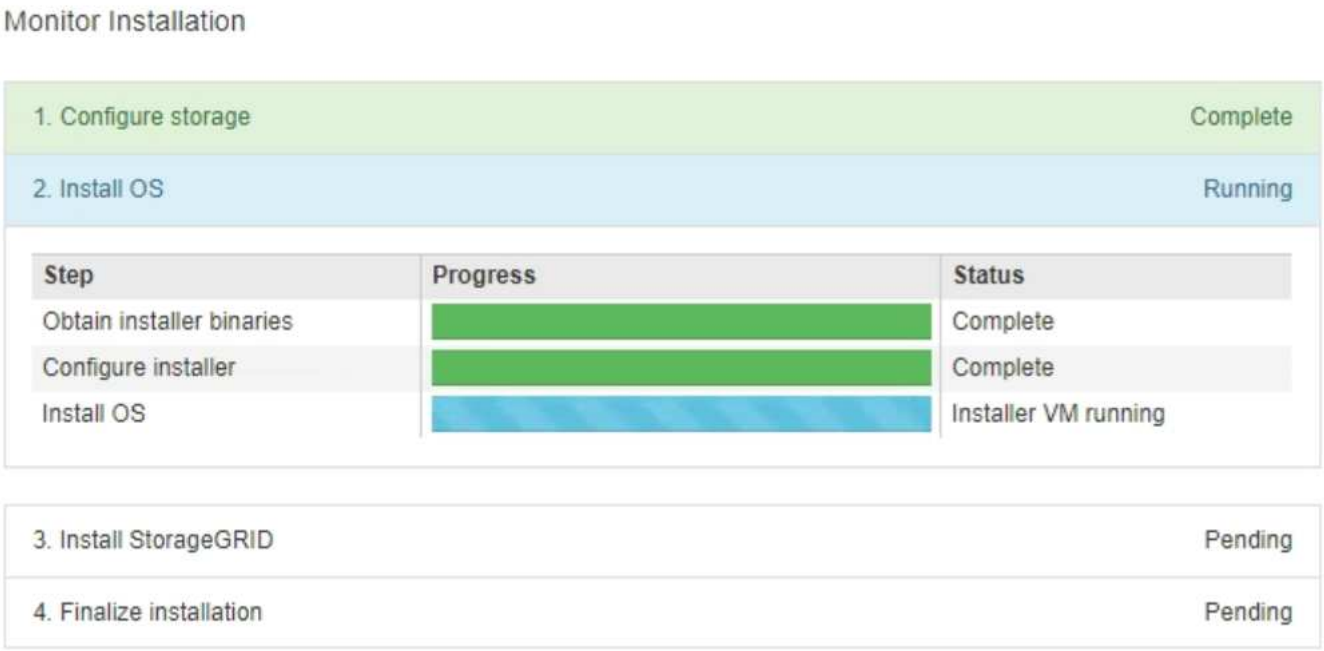
"SG100 SG1000サービスアプライアンス"

サービスアプライアンスのインストールの監視

## StorageGRID アプライアンスインストーラでは、インストールが完了するまでステータスが提供されます。ソフトウェアのインストールが完了すると、アプライアンスがリブートされます。

1. インストールの進行状況を監視するには、メニューバーの * インストールの監視 * をクリックします。

   Monitor Installation ページにインストールの進行状況が表示されます。




青色のステータスバーは、現在進行中のタスクを示します。緑のステータスバーは、正常に完了したタスクを示します。

> インストーラは、以前のインストールで完了したタスクが再実行されないようにします。インストールを再実行している場合 ' 再実行する必要のないタスクは ' 緑色のステータスバーとステータスが [ スキップ済み ] と表示されます

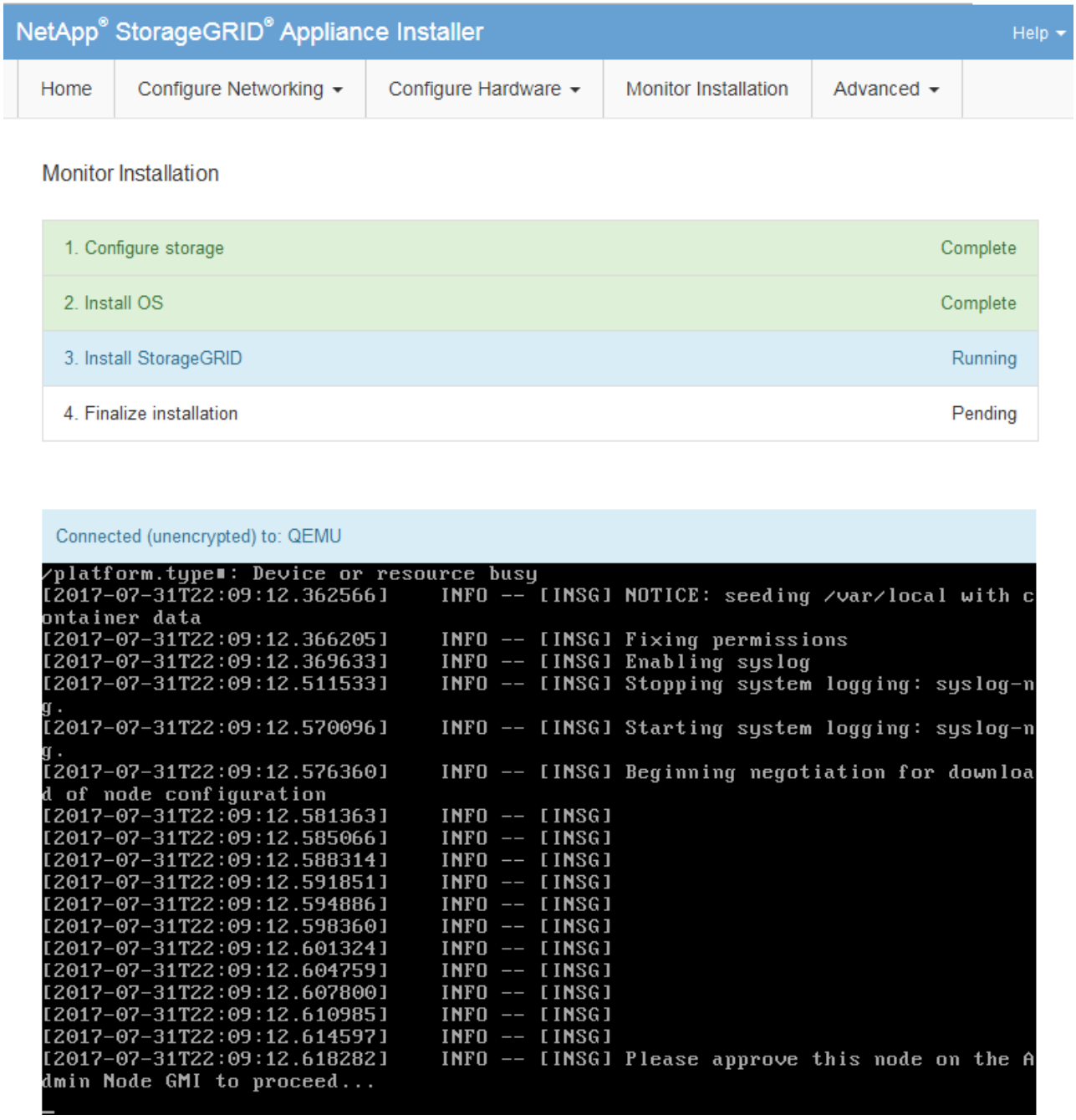
2. インストールの最初の 2 つのステージの進行状況を確認します。
   - * 1 。ストレージの構成 *

     インストーラが既存の設定をすべてドライブから消去し、ホストを設定します。

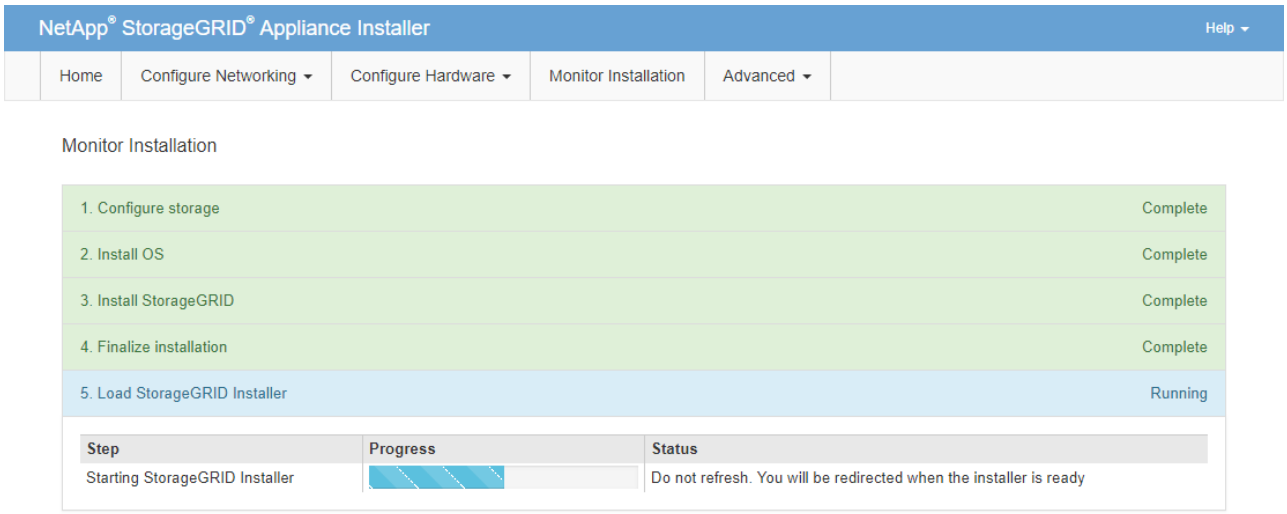
   - ※ 2OS * をインストールします

     インストーラが StorageGRID のベースとなるオペレーティングシステムイメージをプライマリ管理ノードからアプライアンスにコピーするか、ベースとなるオペレーティングシステムイメージをプライマリ管理ノードのインストールパッケージからインストールします。

3. 次のいずれかが実行されるまで、インストールの進行状況を監視します。
   - アプライアンスゲートウェイノードまたは非プライマリアプライアンス管理ノードの場合、 * Install StorageGRID * ステージが一時停止し、組み込みのコンソールにメッセージが表示されて、グリッドマネージャを使用して管理ノードでこのノードを承認するように求められます。




◦ アプライアンスプライマリ管理ノードの場合、第 5 フェーズ（ Load StorageGRID Installer ）が表示されます。5 つ目のフェーズが 10 分以上たっても完了しない場合は、ページを手動で更新してください。




4. リカバリするアプライアンスグリッドノードのタイプに応じて、次のリカバリプロセスステップに進みます。

| リカバリのタイプ | 参照 |
| --- | --- |
| ゲートウェイノード | "Start Recovery（リカバリの開始）を選択してゲートウェイノードを設定します" |
| 非プライマリ管理ノード | "リカバリの開始を選択して非プライマリ管理ノードを設定します" |
| プライマリ管理ノード | "交換用プライマリ管理ノードの設定" |

## テクニカルサポートによるサイトリカバリの実行方法

StorageGRID サイト全体に障害が発生した場合、または複数のストレージノードで障害が発生した場合は、テクニカルサポートにお問い合わせください。テクニカルサポートは、お客様の状況を評価し、リカバリプランを作成してから、障害が発生したノードまたはサイトをビジネス目標に沿った方法でリカバリし、リカバリ時間を最適化して、不要なデータ損失を防ぎます。

サイトリカバリは、テクニカルサポートのみが実行できます。

StorageGRID システムは、さまざまな障害に対する耐障害性を備えており、多くのリカバリ手順やメンテナンス手順を自分で実行できます。ただし、一般化された単純なサイトリカバリ手順 は作成が困難です。詳細な手順は、状況に固有の要因によって異なるためです。例：

- * あなたのビジネス目標 *: StorageGRID の場所の完全な損失の後、あなたのビジネス目的を満たす最もよい方法を評価するべきである。たとえば、失われたサイトをインプレースで再構築しますか？失われた StorageGRID サイトを新しい場所に交換しますか？お客様の状況はそれぞれ異なり、優先事項に対応するようにリカバリプランを設計する必要があります。
- * 障害の正確な性質 * ：サイトのリカバリを開始する前に、障害が発生したサイトのいずれかのノードに損傷がないか、またはリカバリ可能なオブジェクトが含まれているストレージノードがないかを確認することが重要です。有効なデータが含まれているノードまたはストレージボリュームを再構築すると、不要

なデータ損失が発生する可能性があります。

- * アクティブな ILM ポリシー * ：グリッド内のオブジェクトコピーの数、タイプ、および場所は、アクティブな ILM ポリシーによって制御されます。ILM ポリシーの詳細は、リカバリ可能なデータの量、およびリカバリに必要な特定の手法に影響する可能性があります。

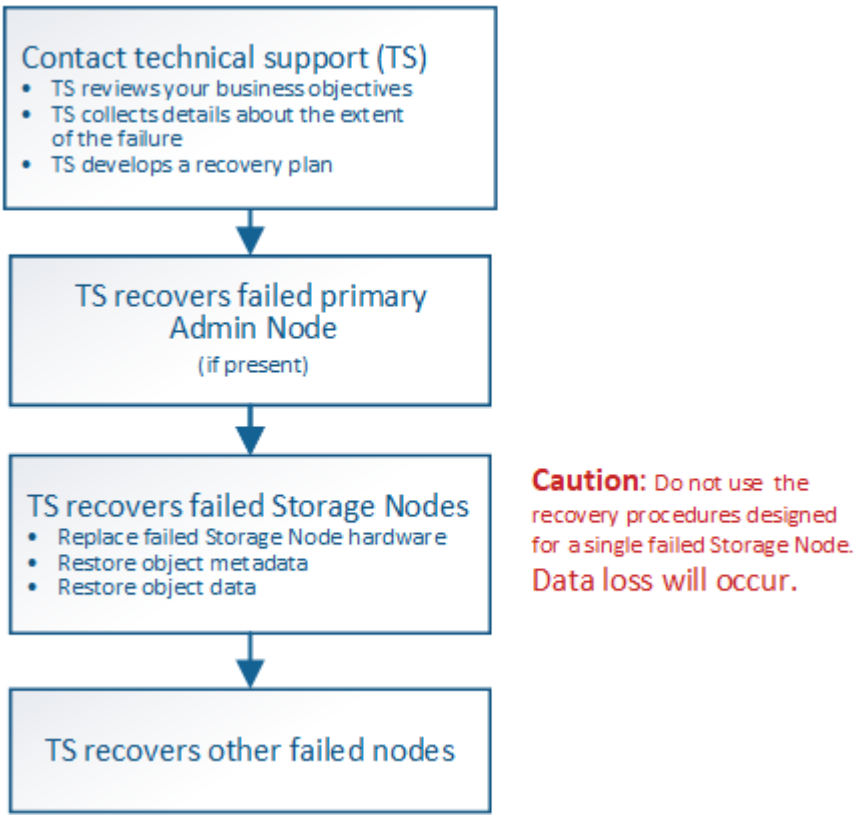
  サイトにオブジェクトの唯一のコピーが含まれていてサイトが失われると、そのオブジェクトは失われます。

- * バケット（またはコンテナ）の整合性 * ：バケット（またはコンテナ）に適用される整合性レベルは、StorageGRID がオブジェクトの取り込みが成功したことをクライアントに通知する前に、すべてのノードとサイトにオブジェクトメタデータを完全にレプリケートするかどうかに影響します。整合性レベルで結果整合性を確保できる場合は、サイト障害時に一部のオブジェクトメタデータが失われている可能性があります。リカバリ可能なデータの量や、リカバリ手順 の詳細に影響する可能性があります。
- * 最新の変更履歴 * ：リカバリ手順 の詳細は、障害発生時のメンテナンス手順の進行状況や、 ILM ポリシーに最近変更が加えられたかどうかによって影響を受ける可能性があります。テクニカルサポートは、サイトのリカバリを開始する前に、グリッドの最新の履歴と現在の状況を評価する必要があります。

サイトリカバリの概要

これは、障害が発生したサイトのリカバリでテクニカルサポートが使用するプロセスの概要です。

サイトリカバリは、テクニカルサポートのみが実行できます。




1. テクニカルサポートにお問い合わせください。

   テクニカルサポートは、障害に関する詳細な評価を行い、パートナー様と協力してビジネス目標を確認します。この情報に基づいて、テクニカルサポートはお客様の状況に合わせたリカバリプランを作成しま

す。

2. テクニカルサポートは、障害が発生したプライマリ管理ノードをリカバリします。
3. テクニカルサポートは、以下の概要に従って、すべてのストレージノードをリカバリします。

   a. 必要に応じて、ストレージノードのハードウェアまたは仮想マシンを交換します。

   b. 障害が発生したサイトにオブジェクトメタデータをリストアする。

   c. リカバリしたストレージノードにオブジェクトデータをリストアします。

   単一の障害ストレージノードのリカバリ手順を使用すると、データが失われます。

   サイト全体で障害が発生した場合、オブジェクトとオブジェクトメタデータを正常にリストアするには特別なコマンドが必要になります。

4. テクニカルサポートは障害が発生した他のノードをリカバリします

   オブジェクトメタデータとデータのリカバリが完了したら、障害が発生したゲートウェイノード、非プライマリ管理ノード、またはアーカイブノードを標準の手順でリカバリできます。

関連情報

"サイトの運用停止"

## 手順 の運用を停止

## 手順 の運用停止を実行して、グリッドノードまたはサイト全体を StorageGRID システムから完全に削除できます。

グリッドノードまたはサイトを削除するには、次のいずれかの運用停止手順を実行します。

- ノードの運用停止 * を実行し、 1 つ以上のサイトにある 1 つ以上のノードを削除します。削除するノードは、オンラインで StorageGRID システムに接続されている場合とオフラインで切断されている場合があります。
- 接続されているサイトの運用停止 * を実行し、すべてのノードが StorageGRID に接続されているサイトを削除します。
- 「切断されたサイトの運用停止」を実行し、すべてのノードが StorageGRID から切断されているサイトを削除します。

  切断されたサイトの運用停止を実行する前に、ネットアップのアカウント担当者にお問い合わせください。運用停止サイトのウィザードですべての手順を有効にする前に、要件を確認してください。切断されているサイトの運用停止は、サイトをリカバリしたり、サイトからオブジェクトデータをリカバリしたりできる可能性がある場合は、試行しないでください。

サイトに接続された（✔）および切断されているノード（ または ）の場合は、すべてのオフラインノードをオンラインに戻す必要があります。

関連情報

"グリッドノードの運用停止"

"サイトの運用停止"

グリッドノードの運用停止

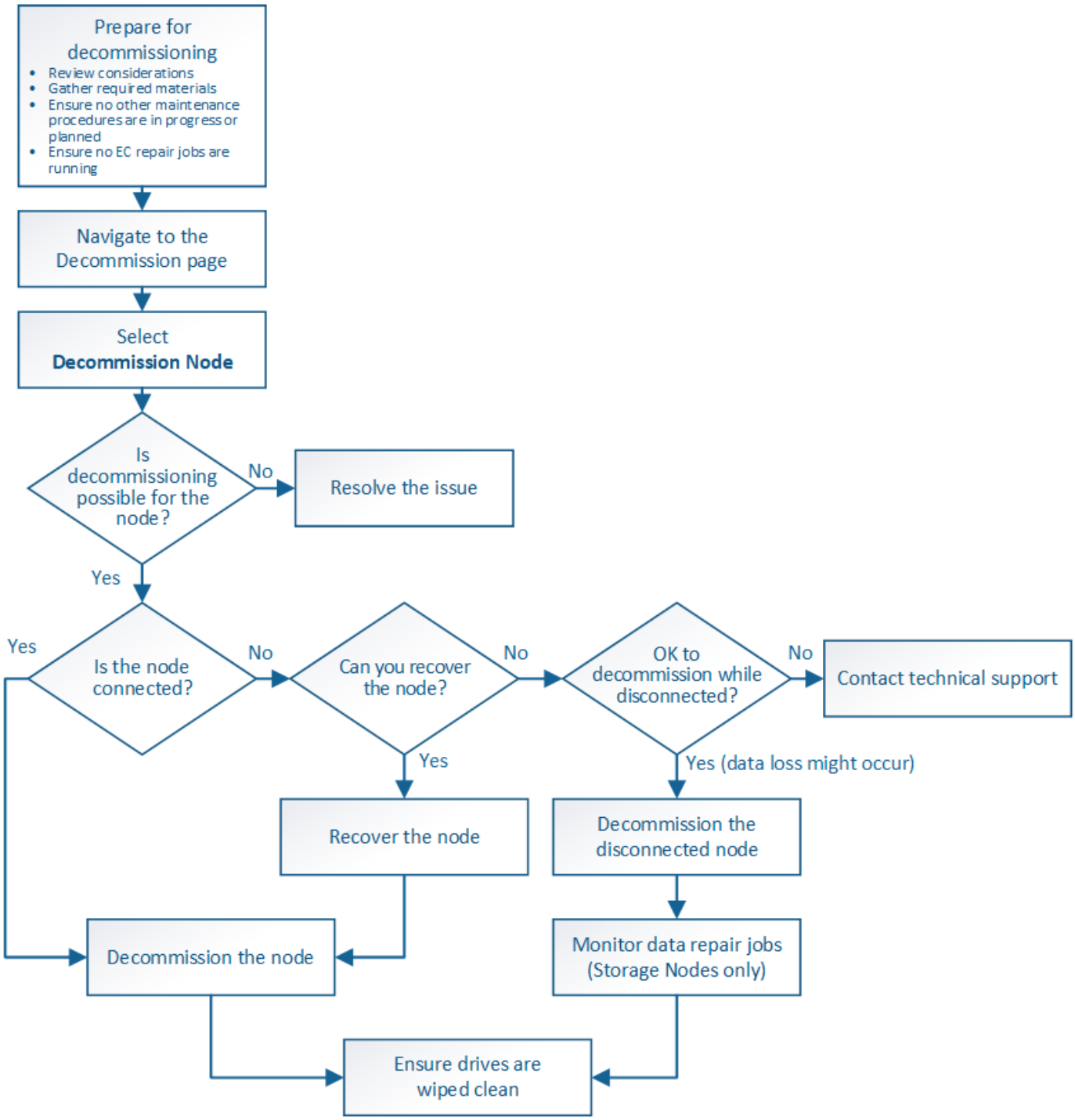
## ノードの運用停止手順 を使用して、 1 つ以上のサイトの 1 つ以上のストレージノード、ゲートウェイノード、または非プライマリ管理ノードを削除できます。プライマリ管理ノードとアーカイブノードの運用を停止することはできません。

一般に、グリッドノードの運用を停止するのは、グリッドノードがStorageGRID システムに接続されていて、すべてのノードが正常な状態であるときにしてください（* Nodes ページおよび Decommission Nodes * ページに緑色のアイコンが表示されています）。ただし、必要に応じて、切断されているグリッドノードの運用を停止できます。切断されているノードを削除する前に、そのプロセスの影響と制限を理解しておいてください。

次のいずれかに該当する場合は、ノードの運用停止手順 を使用します。

- システムに大きなストレージノードを追加したあとに、オブジェクトを保持したまま小さなストレージノードを 1 つ以上削除する場合。
- 総ストレージ容量を減らす必要がある場合。
- ゲートウェイノードが不要になった場合。
- 非プライマリ管理ノードが不要になった場合。
- 切断されていて、リカバリしたりオンラインに戻したりすることができないノードがグリッドに含まれている場合。

次のフローチャートは、グリッドノードの運用停止手順の概要を示しています。




手順

- "グリッドノードの運用を停止する準備をしています"
- "前提要件"
- "Decommission Nodesページにアクセスします"
- "切断されているグリッドノードの運用停止"
- "接続されているグリッドノードの運用停止"
- "ストレージノードの運用停止プロセスの一時停止と再開"
- "ノードの運用停止のトラブルシューティング"

# グリッドノードの削除に関する考慮事項を確認し、イレイジャーコーディングデータのアクティブな修復ジョブがないことを確認する必要があります。

手順

- "ストレージノードの運用停止に関する考慮事項"
- "データ修復ジョブを確認しています"

グリッドノードの運用停止に関する考慮事項

## この手順 を開始して 1 つ以上のノードの運用を停止する前に、各タイプのノードが削除された場合の影響を理解しておく必要があります。ノードの運用が正常に停止されると、ノードのサービスが無効になり、ノードが自動的にシャットダウンされます。

StorageGRID が無効な状態になる場合は、ノードの運用を停止できません。次のルールが適用されます。

- プライマリ管理ノードは運用停止できません。
- アーカイブノードは運用停止できません。
- ネットワークインターフェイスの 1 つが High Availability （ HA ；高可用性）グループに属している場合は、管理ノードまたはゲートウェイノードの運用を停止できません。
- 削除することで ADC クォーラムに影響を与えるストレージノードは、運用停止できません。
- アクティブな ILM ポリシーに必要なストレージノードは運用停止できません。
- 1 つのノードの運用停止手順 では、 10 個を超えるストレージノードの運用を停止しないでください。
- 切断されているノード（健全性が「 Unknown 」または「 Administratively Down 」のノード）がグリッドに含まれている場合は、接続されているノードの運用を停止できません。切断されているノードは、運用停止するかリカバリしておく必要があります。
- グリッド内に切断されているノードが複数ある場合は、それらのノードの運用をすべて同時に停止する必要があるため、予期しない結果になる可能性があります。
- 切断されているノードを削除できない場合（ ADC クォーラムに必要なストレージノードなど）は、切断されている他のノードを削除できません。
- 古いアプライアンスを新しいアプライアンスに交換する場合は、古いノードの運用を停止して新しいノードを拡張に追加するのではなく、アプライアンスノードのクローニング手順 を使用することを検討してください。

  "アプライアンスノードのクローニング"

> 運用停止手順での指示があるまでは、グリッドノードの仮想マシンやその他のリソースを削除しないでください。

管理ノードまたはゲートウェイノードの運用停止に関する考慮事項

## 管理ノードまたはゲートウェイノードの運用を停止する前に、次の考慮事項を確認してください。

- 運用停止手順 では、一部のシステムリソースに排他的にアクセスする必要があるため、他のメンテナンス手順が実行されていないことを確認する必要があります。
- プライマリ管理ノードは運用停止できません。
- ネットワークインターフェイスの 1 つが High Availability （ HA ；高可用性）グループに属している場合は、管理ノードまたはゲートウェイノードの運用を停止できません。最初に、 HA グループからネットワークインターフェイスを削除する必要があります。StorageGRID の管理手順を参照してください。
- 必要に応じて、ゲートウェイノードまたは管理ノードの運用停止中に、安全に ILM ポリシーを変更できます。
- シングルサインオン（ SSO ）が有効な StorageGRID システムで管理ノードの運用を停止した場合は、ノードの証明書利用者信頼を Active Directory フェデレーションサービス（ AD FS ）から削除する必要があります。

関連情報

"StorageGRID の管理"

ストレージノードの運用停止に関する考慮事項

## ストレージノードの運用を停止する際には、 StorageGRID がそのノードのオブジェクトデータとメタデータをどのように管理しているかを理解しておく必要があります。

ストレージノードの運用停止には、次の考慮事項と制限事項が適用されます。

- ADC クォーラムやアクティブな ILM ポリシーなどの運用要件を満たす十分な数のストレージノードが常にシステムに存在している必要があります。この要件を満たすために、拡張処理で新しいストレージノードを追加してから既存のストレージノードの運用を停止することが必要になる場合があります。
- 運用を停止する際に対象のストレージノードが切断されていると、システムは接続されているストレージノードのデータを使用してデータを再構築する必要があり、その結果、データが失われる可能性があります。
- ストレージノードを削除する場合、大量のオブジェクトデータをネットワーク経由で転送する必要があります。この転送が通常のシステム処理に影響することはありませんが、 StorageGRID システムが消費するネットワーク帯域幅の総量に影響する可能性があります。
- ストレージノードの運用停止に関連するタスクは、通常のシステム処理に関連するタスクよりも優先度が低くなっています。つまり、運用停止処理が StorageGRID の通常のシステム処理を妨げることはなく、システムがアクティブでない期間に運用停止処理をスケジュールする必要もありません。運用停止処理はバックグラウンドで実行されるため、プロセスの所要時間を見積もることは困難です。一般に、システムがビジー状態でないとき、または一度に 1 つのストレージノードのみを削除するときは、運用停止処理が迅速に終了します。
- ストレージノードの運用停止には、数日から数週間かかることがあります。それに応じてこの手順 を計画してください運用停止プロセスはシステム処理に影響しないように設計されていますが、他の手順が制限される可能性があります。一般に、システムのアップグレードや拡張を計画している場合は、グリッドノードを削除する前に実行する必要があります。
- 必要に応じて、ストレージノードが関係する運用停止手順を特定の段階で一時停止して他のメンテナンス手順を実行し、その完了後に運用停止手順を再開できます。
- 運用停止タスクが実行されている間は、どのグリッドノードでもデータ修復処理を実行できません。
- ストレージノードの運用停止中は、 ILM ポリシーに変更を加えないでください。
- ストレージノードを削除すると、そのノードのデータは他のグリッドノードに移行されます。ただし、こ

のデータは運用停止されたグリッドノードから完全には削除されません。完全かつ安全にデータを削除するには、運用停止手順 の完了後に、運用停止したグリッドノードのドライブを消去する必要があります。

- ストレージノードの運用を停止すると、次のアラートとアラームが生成され、関連する E メール通知および SNMP 通知が送信される可能性があります。
  - * ノードと通信できません * アラート。このアラートは、 ADC サービスが含まれるストレージノードの運用を停止した場合にトリガーされます。このアラートは、運用停止処理が完了すると解決します。
  - VSTU （ Object Verification Status ）アラーム。このアラームは Notice レベルで、運用停止プロセスでストレージノードがメンテナンスモードに移行していることを示しています。
  - Casa （ Data Store Status ）アラーム。このアラームは Major レベルで、サービスが停止したために Cassandra データベースが停止することを示しています。

関連情報

"必要に応じたストレージボリュームへのオブジェクトデータのリストア"

"ADCクォーラムを理解していること"

"ILMポリシーとストレージ構成を確認します"

"切断されているストレージノードの運用停止"

"ストレージノードの統合"

"複数のストレージノードの運用停止"

**ADC**クォーラムを理解していること

運用停止後に残る Administrative Domain Controller （ ADC ）サービスが少なすぎる場合は、データセンターサイトの一部のストレージノードの運用を停止できないことがあります。一部のストレージノードで使用されるこのサービスは、グリッドトポロジ情報を保持し、設定サービスをグリッドに提供します。StorageGRID システムでは、各サイトで ADC サービスのクォーラムが常に利用可能である必要があります。

ストレージノードを削除すること原因 で ADC クォーラムが満たされなくなる場合は、そのノードの運用を停止することはできません。運用停止時に ADC クォーラムを満たすには、各データセンターサイトで少なくとも 3 つのストレージノードに ADC サービスが必要です。ADCサービスがあるストレージノードが1つのデータセンターサイトに3つ以上ある場合は、運用停止後も過半数のノードが利用可能な状態のままである必要があります（（0.5x） `Storage Nodes with ADC`）+ 1）。

たとえば、 ADC サービスがあるストレージノードが 1 つのデータセンターサイトに 6 つあり、そのうちの 3 つの運用を停止するとします。ADC クォーラムの要件により、次の 2 つの運用停止手順を実行する必要があります。

- 手順 の最初の運用停止では、 ADC サービスがある 4 つのストレージノードが利用可能な状態で残るようにする必要があります（（ 0.5x6 ） +1 ）。そのため、最初に運用停止できるのは、 2 つのストレージノードのみです。
- 2 回目の手順 運用停止では、 3 つ目のストレージノードを削除できます。 ADC クォーラムの要件により、利用可能な状態で残す必要のある ADC サービスが 3 つになったためです（（ 0.5x4 ） +1 ）。

ストレージノードの運用を停止する必要があるものの、 ADC クォーラムの要件が原因で運用停止できない場合は、拡張の際に新しいストレージノードを追加し、そのノードに ADC サービスを配置するよう指定する必要があります。そのあと、既存のストレージノードの運用を停止できます。

関連情報

"グリッドを展開します"

**ILM**ポリシーとストレージ構成を確認します

## ストレージノードの運用を停止する場合は、運用停止プロセスを開始する前に StorageGRID システムの ILM ポリシーを確認してください。

運用停止時に、運用停止されたストレージノードのすべてのオブジェクトデータが他のストレージノードに移行されます。

運用停止中の ILM ポリシーは、運用停止後のポリシーとして使用されます。運用停止を開始する前と運用停止の完了後に、このポリシーがデータの要件を満たしていることを確認する必要があります。

StorageGRID システムがストレージノードの運用停止に対応するために適切な場所に適切なタイプの容量を引き続き十分に確保できるように、アクティブな ILM ポリシーのルールを確認する必要があります。

次の点を考慮してください。

- ILM 評価サービスで ILM ルールを満たすようにオブジェクトデータをコピーすることは可能か。
- 運用停止処理の進行中にサイトが一時的に使用不能になった場合は、どうなりますか？追加のコピーを別の場所に作成できるか。
- 運用停止プロセスは、コンテンツの最終的な配信にどのように影響しますか。「ストレージノードの統合」で説明したように、古いストレージノードの運用を停止する前に新しいストレージノードを追加する必要があります。小さいストレージノードの運用を停止してから、交換用に大きいストレージノードを追加すると、以前からあるストレージノードが容量の限界に近づき、新しいストレージノードにはほとんどコンテンツが存在しない状態になる可能性があります。新しいオブジェクトデータの書き込み処理のほとんどは新しいストレージノードに送信されるため、システム処理の全体的な効率が低下します。
- アクティブな ILM ポリシーを満たす十分な数のストレージノードが常にシステムに存在しているか。

ILM ポリシーを満たすことができないと、バックログやアラームが発生し、 StorageGRID システムの運用が停止する可能性があります。

次の表に示す要素を評価して、運用停止プロセスによって実現する推奨トポロジが ILM ポリシーを満たすことを確認します。

| 評価する領域 | 注： |
| --- | --- |
| 使用可能容量 | StorageGRID システムに格納されているすべてのオブジェクトデータに対応できるだけの十分なストレージ容量があるか。 運用停止が必要なストレージノードに現在格納されているオブジェクトデータの永続的なコピーを含めるかどうか。運用停止処理が完了してから妥当な期間、格納されるオブジェクトデータについて予測される増加に対応できるだけの十分な容量があるか。 |
| ストレージの場所 | StorageGRID システム全体に十分な容量が残っている場合、StorageGRID システムのビジネスルールを満たす適切な場所に容量が配置されているか。 |
| ストレージタイプ | 運用停止処理が完了したあとに、適切なタイプのストレージを十分に確保できるか。たとえば、コンテンツをその保管期間に応じて特定のタイプのストレージから別のタイプのストレージに移動するように ILM ルールで指示される場合があります。その場合は、 StorageGRID システムの最終的な構成に、適切なタイプのストレージが十分に確保されていることを確認する必要があります。 |

関連情報

"ストレージノードの統合"

"ILM を使用してオブジェクトを管理する"

"グリッドを展開します"

切断されているストレージノードの運用停止

## 切断されているストレージノードの運用を停止した場合（ヘルスが「 Unknown 」または「 Administratively Down 」）は、どうなるかを理解しておく必要があります。

グリッドから切断されているストレージノードの運用を停止すると、 StorageGRID は他のストレージノードのデータを使用して、切断されているノード上にあったオブジェクトデータとメタデータを再構築します。この処理は、運用停止手順の最後にデータ修復ジョブを自動的に開始することで行われます。

切断されているストレージノードの運用を停止する前に、次の点を確認してください。

- 切断されているノードは、オンラインに戻したりリカバリしたりできないことが確実な場合以外は、運用停止しないでください。

> ノードからオブジェクトデータをリカバリできる可能性がある場合は、この手順 を実行しないでください。代わりに、テクニカルサポートに問い合わせて、ノードのリカバリが可能かどうかを確認してください。

- 切断されているストレージノードに特定のオブジェクトの唯一のコピーが含まれている場合、ノードの運用を停止するとそのオブジェクトは失われます。データ修復ジョブは、現在接続されているストレージノードに、 1 つ以上のレプリケートコピーまたは十分なイレイジャーコーディングフラグメントが含まれている場合のみ、オブジェクトを再構築してリカバリできます。

- 切断されているストレージノードの運用を停止する場合、手順 の運用停止は比較的短時間で完了します。ただし、データ修復ジョブは実行に数日から数週間かかることがあり、運用停止手順 によって監視されません。これらのジョブは手動で監視し、必要に応じて再開してください。データ修復の監視手順を参照してください。

  "データ修復ジョブを確認しています"

- 切断されている複数のストレージノードを一度に運用停止すると、データが失われる可能性があります。利用可能な状態で残るオブジェクトデータ、メタデータ、またはイレイジャーコーディングフラグメントのコピーが少なすぎると、システムがデータを再構築できない場合があります。

  切断されていてリカバリできない複数のストレージノードがある場合は、テクニカルサポートに問い合わせて、最適な対処方法を確認してください。

ストレージノードの統合

## ストレージノードを統合すると、サイトや環境のストレージノード数を減らしながら、ストレージ容量を増やすことができます。

ストレージノードを統合するときは、 StorageGRID システムを拡張して容量の大きなストレージノードを新たに追加したあとに、容量の小さい古いストレージノードの運用を停止します。手順 の運用を停止すると、オブジェクトが古いストレージノードから新しいストレージノードに移行されます。

たとえば、 3 つの古いストレージノードを 2 つの新しい大容量のストレージノードで置き換えます。最初に拡張手順 を使用して 2 つの新しい大容量のストレージノードを追加し、そのあとに運用停止手順 を使用して 3 つの古い小容量のストレージノードを削除します。

既存のストレージノードを削除する前に新たな容量を追加することで、 StorageGRID システム全体でバランスよくデータを分散できます。また、既存のストレージノードがストレージのウォーターマークレベルを超える可能性が低くなります。

関連情報

"グリッドを展開します"

複数のストレージノードの運用停止

## 複数のストレージノードを削除する必要がある場合は、運用停止処理を順次実行することも並列に実行することもできます。

- 複数のストレージノードの運用を順次停止する場合は、最初のストレージノードの運用停止が完了するのを待ってから、次のストレージノードの運用停止を開始する必要があります。
- 複数のストレージノードの運用を並列に停止する場合は、対象となるすべてのストレージノードで同時に運用停止タスクが処理されます。その結果、ファイルの永続的なコピーがすべて「読み取り専用」としてマークされ、この機能が有効になっているグリッドでの削除が一時的に無効になることがあります。

データ修復ジョブを確認しています

## グリッドノードの運用を停止する前に、アクティブなデータ修復ジョブがないことを確認する必要があります。修復に失敗した場合は、手順 の運用を停止する前に、修復を再

開し、完了させておく必要があります。

切断されているストレージノードの運用を停止する必要がある場合は、手順 の運用停止が完了したあとに、データ修復ジョブが正常に完了するように、この手順も実行します。削除したノードにイレイジャーコーディングフラグメントがあった場合は、適切にリストアされたことを確認してください。

以下の手順は、イレイジャーコーディングオブジェクトがあるシステムにのみ適用されます。

1. プライマリ管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`

      rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。
2. 実行中の修復の有無を確認します。 `repair-data show-ec-repair-status`
   - データ修復ジョブを実行したことがない場合、出力はになります `No job found`。修復ジョブを再開する必要はありません。
   - データ修復ジョブを以前に実行したか、現在実行している場合は、出力には修復に関する情報が表示されます。各修復には、一意の修復 ID が割り当てられます。次の手順に進みます。

```
root@DC1-ADM1:~ # repair-data show-ec-repair-status

Repair ID Scope Start Time End Time State Est/Affected Bytes Repaired
Retry Repair
================================================================================
===========
949283 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:27:06.9 Success 17359
17359 No
949292 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:37:06.9 Failure 17359 0
Yes
949294 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:47:06.9 Failure 17359 0
Yes
949299 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:57:06.9 Failure 17359 0
Yes
```

3. すべての修理のStateがの場合 `Success`修復ジョブを再開する必要はありません。
4. いずれかの修理のStateがの場合 `Failure`、その修復を再開する必要があります。
   a. 出力から、障害が発生した修復の修復 ID を取得します。
   b. を実行します `repair-data start-ec-node-repair` コマンドを実行します

      を使用します `--repair-id` 修復IDを指定するオプション。たとえば、修復IDが949292の修復を再試行する場合、実行するコマンドはです。 `repair-data start-ec-node-repair --repair-id`

```
949292
```

c. すべての修復のStateがになるまで、引き続きECデータの修復のステータスを追跡します `Success`。

前提要件

## グリッドノードの運用停止を実行する前に、次の情報を取得する必要があります。

| 項目 | 注： |
| --- | --- |
| リカバリパッケージ `.zip` ファイル。 | 最新のリカバリパッケージをダウンロードする必要があります `.zip` ファイル。（`sgws-recovery-package-id-revision.zip`）。リカバリパッケージファイルは、障害発生時のシステムのリストアに使用できます。 |
| `Passwords.txt` ファイル。 | このファイルには、コマンドラインでグリッドノードにアクセスするために必要なパスワードが格納されます。このファイルはリカバリパッケージに含まれています。 |
| プロビジョニングパスフレーズ | このパスフレーズは、 StorageGRID システムが最初にインストールされるときに作成されて文書化されます。プロビジョニングパスフレーズはに含まれていません `Passwords.txt` ファイル。 |
| 運用停止前の StorageGRID システムのトポロジの概要 | システムの現在のトポロジを記載したドキュメントがあれば、すべて入手します。 |

関連情報

"Web ブラウザの要件"

"リカバリパッケージをダウンロードしています"

**Decommission Nodes**ページにアクセスします

## Grid Manager の Decommission Nodes ページにアクセスすると、運用停止できるノードが一目でわかります。

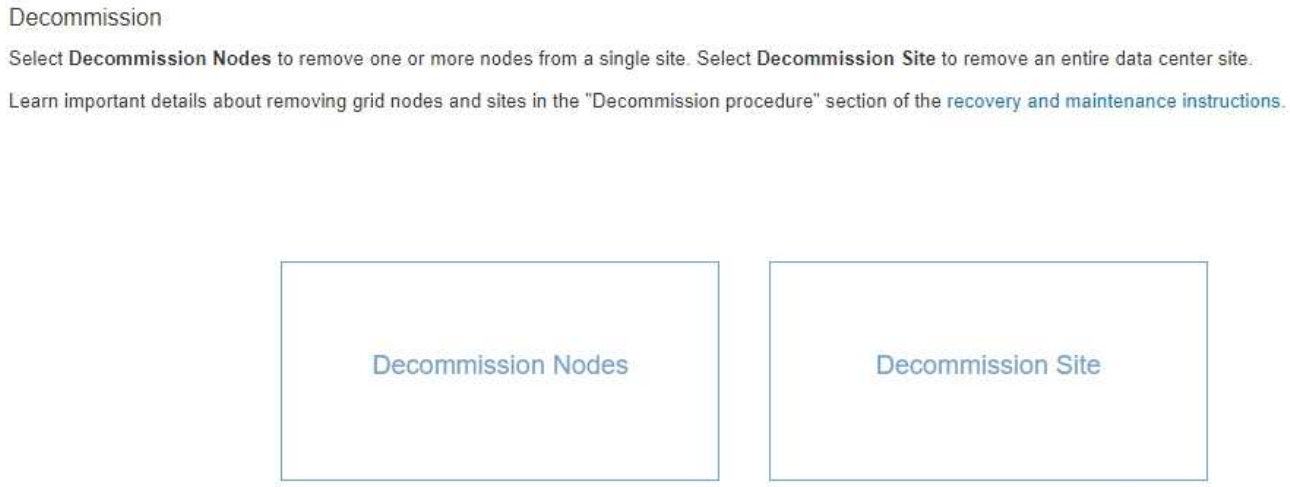
必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Maintenance または Root Access 権限が必要です。

手順

1. [* Maintenance （メンテナンス）**]>[** Maintenance Tasks（メンテナンスタスク）]**>[** Decommission]*を選択します

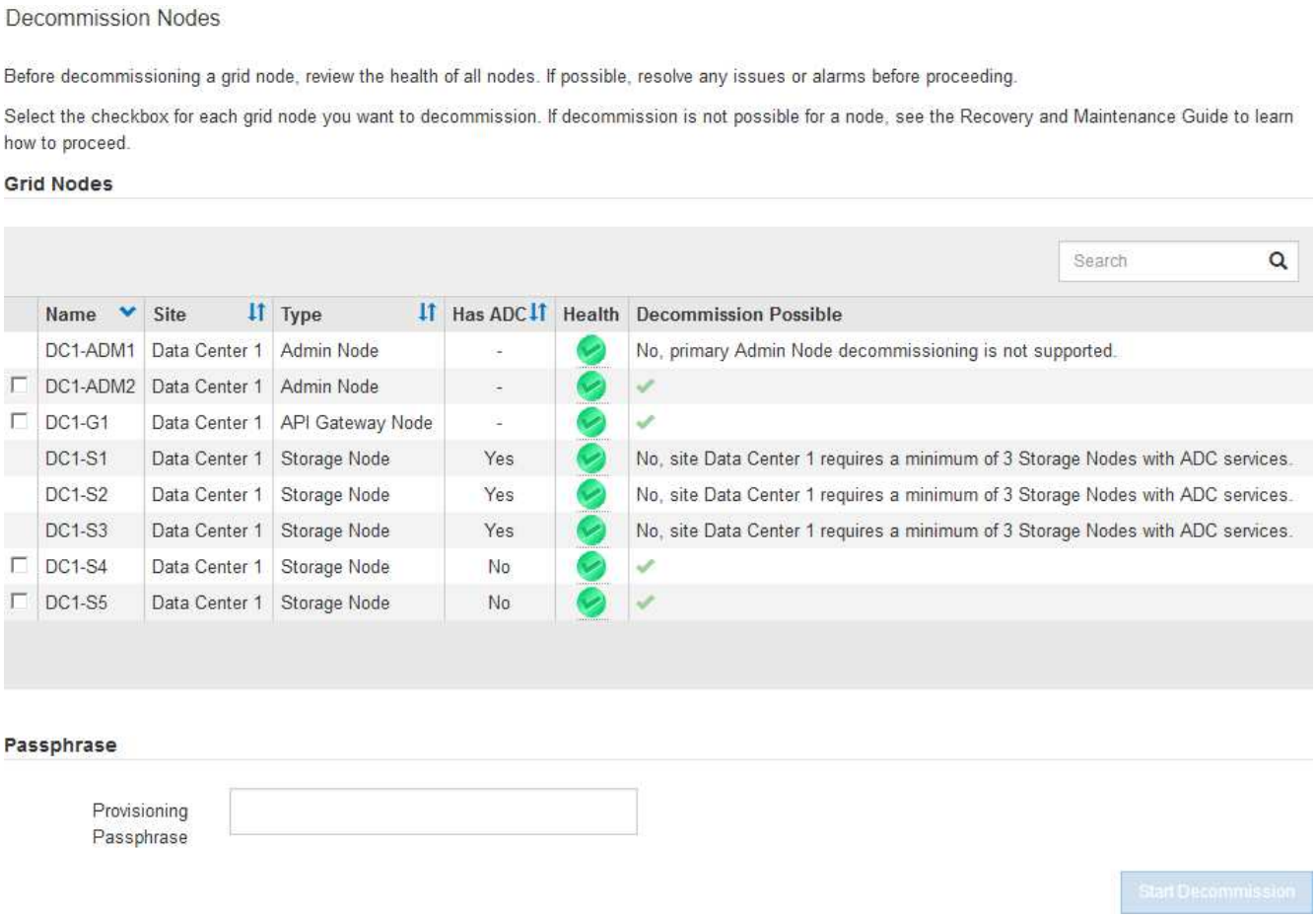
   Decommission ページが表示されます。




2. [Decommission Nodes]ボタンをクリックします。

   Decommission Nodes ページが表示されます。このページでは、次の操作を実行できます。

   - 現時点で運用停止できるグリッドノードを確認できます。
   - すべてのグリッドノードの健全性を確認できます
   - リストを * Name * 、 * Site * 、 * Type * 、または * has ADC* で昇順または降順にソートします。
   - 検索キーワードを入力すると、特定のノードをすばやく検索できます。たとえば、このページには、単一のデータセンター内のすべてのグリッドノードが表示されます。Decommission列には、非プライマリ管理ノード、ゲートウェイノード、および5つのストレージノードのうちの2つの運用を停止できます。




3. 運用停止するノードごとに「 * Decommission possible * 」列を確認します。

運用停止できるグリッドノードの場合は、この列に緑のチェックマークが表示され、左端の列にチェックボックスが表示されます。運用を停止できないノードの場合は、この列に問題 の説明が表示されます。ノードの運用を停止できない理由が複数ある場合は、最も重大な理由が表示されます。

| 運用停止の可能性がある理由 | 説明 | 解決する手順 |
| --- | --- | --- |
| いいえ。ノードタイプの運用停止はサポートされていません。 | プライマリ管理ノードとアーカイブノードの運用を停止することはできません。 | なし |

| 運用停止の可能性がある理由 | 説明 | 解決する手順 |
| --- | --- | --- |
| いいえ。少なくとも 1 つのグリッドノードが切断されています。<br>• 注：* このメッセージは、接続されているグリッドノードにのみ表示されます。 | 切断されているグリッドノードがある場合、接続されているグリッドノードの運用を停止することはできません。<br>• Health * 列には、切断されているグリッドノード用の次のアイコンが表示されます。<br>◦ （グレー）：Administratively Down<br>◦ （青）：Unknown | にアクセスします 運用停止の手順 選択肢を表示する手順。 |
| いいえ。必要なノードが現在切断されており、リカバリが必要です。<br>• 注：* このメッセージは、切断されたグリッドノードについてのみ表示されます。 | 切断されているグリッドノード（ ADC クォーラムに必要なストレージノードなど）も切断されている場合は、運用を停止できません。 | a. 切断されているすべてのノードについて、運用停止の可能性があるメッセージを確認します。<br>b. 運用停止が必要なノードを特定します。<br>◦ 必要なノードのヘルスが「 Administratively Down 」の場合は、ノードをオンラインに戻します。<br>◦ 必要なノードの健全性が「 Unknown 」の場合は、ノードリカバリ手順 を実行して必要なノードをリカバリします。 |
| いいえ、 HA グループのメンバー： *x* 。このノードの運用を停止するには、すべての HA グループからノードを削除する必要があります。 | ノードインターフェイスがハイアベイラビリティ（ HA ）グループに属している場合は、管理ノードまたはゲートウェイノードの運用を停止することはできません。 | HA グループを編集して、ノードのインターフェイスを削除するか、 HA グループ全体を削除します。StorageGRID の管理手順を参照してください。 |
| いいえ、 site_B では、 ADC サービスを使用するストレージノードが必要です。 | • ストレージノードのみ。 * ADC クォーラムの要件を満たす十分なノードがサイトに残らない場合は、ストレージノードの運用を停止できません。 | 拡張を実行します。サイトに新しいストレージノードを追加し、 ADC サービスを配置するよう指定します。ADC クォーラムに関する情報を参照してください。 |

| 運用停止の可能性がある理由 | 説明 | 解決する手順 |
| --- | --- | --- |
| いいえ。 1 つ以上のイレイジャーコーディングプロファイルには少なくとも _n_Storage ノードが必要です。プロファイルが ILM ルールで使用されていない場合は、非アクティブ化できます。 | • ストレージノードのみ。 * 既存のイレイジャーコーディングプロファイルに十分なノードが残っていないと、ストレージノードの運用を停止することはできません。<br><br>たとえば、 4+2 のイレイジャーコーディングのイレイジャーコーディングプロファイルがある場合は、少なくとも 6 つのストレージノードが残っている必要があります。 | 影響を受ける各イレイジャーコーディングプロファイルについて、プロファイルの使用方法に基づいて次のいずれかの手順を実行します。<br><br>• * アクティブな ILM ポリシーで使用される * ：拡張を実行します。イレイジャーコーディングを続行できるように十分な数の新しいストレージノードを追加してください。StorageGRID の拡張手順を参照してください。<br>• * ILM ルールで使用されているものの、アクティブな ILM ポリシーには使用されていない場合 * ：ルールを編集または削除してから、イレイジャーコーディングプロファイルを非アクティブ化します。<br>• * いずれの ILM ルールでも使用されていない * ：イレイジャーコーディングプロファイルを非アクティブ化します。<br>◦ 注： * イレイジャーコーディングプロファイルを非アクティブ化しようとしたときに、オブジェクトデータがまだプロファイルに関連付けられていると、エラーメッセージが表示されます。無効化プロセスを再度実行する前に、数週間待つ必要がある場合があります。<br><br>情報ライフサイクル管理を使用してオブジェクトを管理する手順で、イレイジャーコーディングプロファイルを非アクティブ化する方法について説明します。 |

4. [[decomsor_procedure ]] ノードで運用停止が可能な場合は、実行する必要がある手順 を特定します。

| グリッドに含まれるノード | 手順 |
| --- | --- |
| 切断されているグリッドノードがある場合 | "切断されているグリッドノードの運用停止" |
| 接続されているグリッドノードのみ | "接続されているグリッドノードの運用停止" |

関連情報

"データ修復ジョブを確認しています"

"ADCクォーラムを理解していること"

"ILM を使用してオブジェクトを管理する"

"グリッドを展開します"

"StorageGRID の管理"

切断されているグリッドノードの運用停止

# グリッドに現在接続されていないノード（「 Health 」が「 Unknown 」または「 Administratively Down 」のノード）の運用を停止することが必要になる場合があります。

必要なもの

- グリッドノードの運用停止に関する要件と考慮事項を理解しておく必要があります。

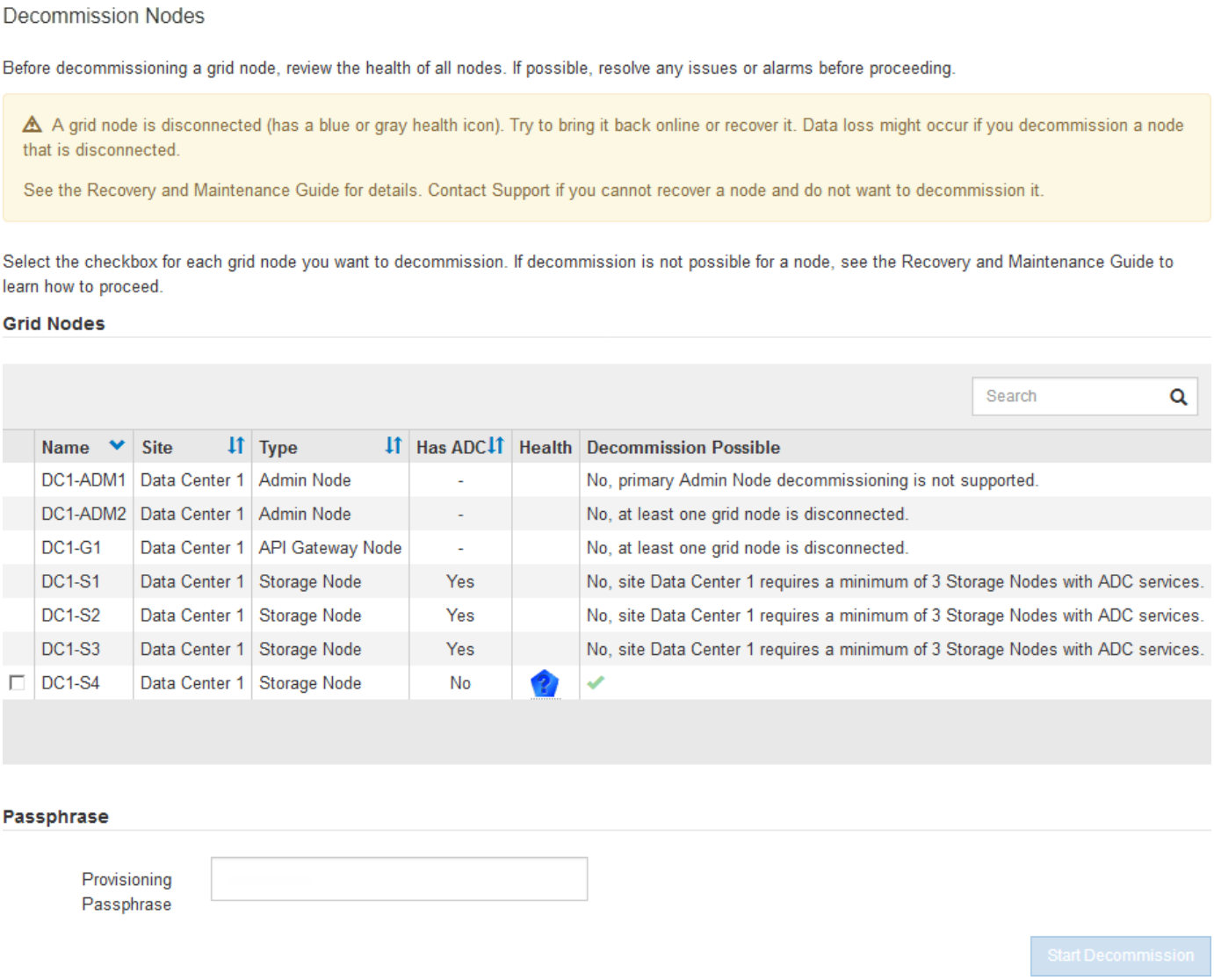
  "グリッドノードの運用停止に関する考慮事項"

- 前提条件となる項目をすべて用意しておきます。
- アクティブなデータ修復ジョブがないことを確認しておきます。

  "データ修復ジョブを確認しています"

- グリッド内でストレージノードのリカバリが実行中でないことを確認します。実行中の場合は、リカバリの一環として実行される Cassandra の再構築が完了するまで待機する必要があります。そのあとで運用停止を続行できます。
- ノード運用停止手順 が一時停止されていないかぎり、ノード手順 の運用停止中に他のメンテナンス手順が実行されないようにしておきます。
- 運用停止するノードの * 運用停止可能な * 列には、緑のチェックマークが表示されます。
- プロビジョニングパスフレーズが必要です。

切断されているノードは、「 * Health * 」列で「 Unknown 」（青）または「 Administratively Down 」（グレー）のアイコンで特定できます。この例では、 DC1-S4 という名前のストレージノードが接続解除されており、他のすべてのノードが接続されています。




切断されているノードの運用を停止する前に、次の点に注意して

- この手順 は、主に切断されている 1 つのノードを削除することを目的としています。グリッド内に切断されているノードが複数ある場合は、それらのノードの運用をすべて同時に停止する必要があるため、予期しない結果になる可能性があります。

> 切断されている複数のグリッドノードを一度に運用停止する場合は、特に複数の切断されているストレージノードを選択する場合は注意が必要です。

- 切断されているノードを削除できない場合（ADC クォーラムに必要なストレージノードなど）は、切断されている他のノードを削除できません。

切断されている * ストレージノード * の運用を停止する前に、次の点に注意してください

- 切断されているストレージノードの運用を停止するのは、オンラインに戻したりリカバリしたりすることができないことが確実な場合だけにしてください。

> この場合もオブジェクトデータをノードからリカバリできると考えられる場合は、この手順 を実行しないでください。代わりに、テクニカルサポートに問い合わせて、ノードのリカバリが可能かどうかを確認してください。

- 切断されている複数のストレージノードの運用を停止すると、データが失われる可能性があります。十分な数のオブジェクトコピー、イレイジャーコーディングフラグメント、またはオブジェクトメタデータが残っていると、システムがデータを再構築できない場合があります。

  > 切断されていてリカバリできない複数のストレージノードがある場合は、テクニカルサポートに問い合わせて、最適な対処方法を確認してください。

- 切断されているストレージノードの運用を停止すると、 StorageGRID は運用停止手順の終了時にデータ修復ジョブを開始します。これらのジョブは、切断されているノードに格納されていたオブジェクトデータとメタデータの再構築を試みます。
- 切断されているストレージノードの運用を停止する場合、手順 の運用停止は比較的短時間で完了します。ただし、データ修復ジョブは実行に数日から数週間かかることがあり、運用停止手順 によって監視されません。これらのジョブは手動で監視し、必要に応じて再開してください。データ修復の監視手順を参照してください。

  "データ修復ジョブを確認しています"

- オブジェクトの唯一のコピーを含む切断されているストレージノードの運用を停止すると、そのオブジェクトは失われます。データ修復ジョブは、現在接続されているストレージノードに、 1 つ以上のレプリケートコピーまたは十分なイレイジャーコーディングフラグメントが含まれている場合のみ、オブジェクトを再構築してリカバリできます。

切断されている * 管理ノード * または * ゲートウェイノード * の運用を停止する前に、次の点に注意してください。

- 切断されている管理ノードの運用を停止すると、そのノードの監査ログが失われますが、これらのログはプライマリ管理ノードにも存在している必要があります。
- 切断されているゲートウェイノードは安全に運用停止できます。

手順

1. 切断されているグリッドノードのオンラインへの復帰またはリカバリを試行します。

   手順については、リカバリ手順を参照してください。

2. 切断されているグリッドノードをリカバリできず、そのノードを切断状態のまま運用を停止する場合は、そのノードのチェックボックスを選択します。

   > グリッド内に切断されているノードが複数ある場合は、それらのノードの運用をすべて同時に停止する必要があるため、予期しない結果になる可能性があります。

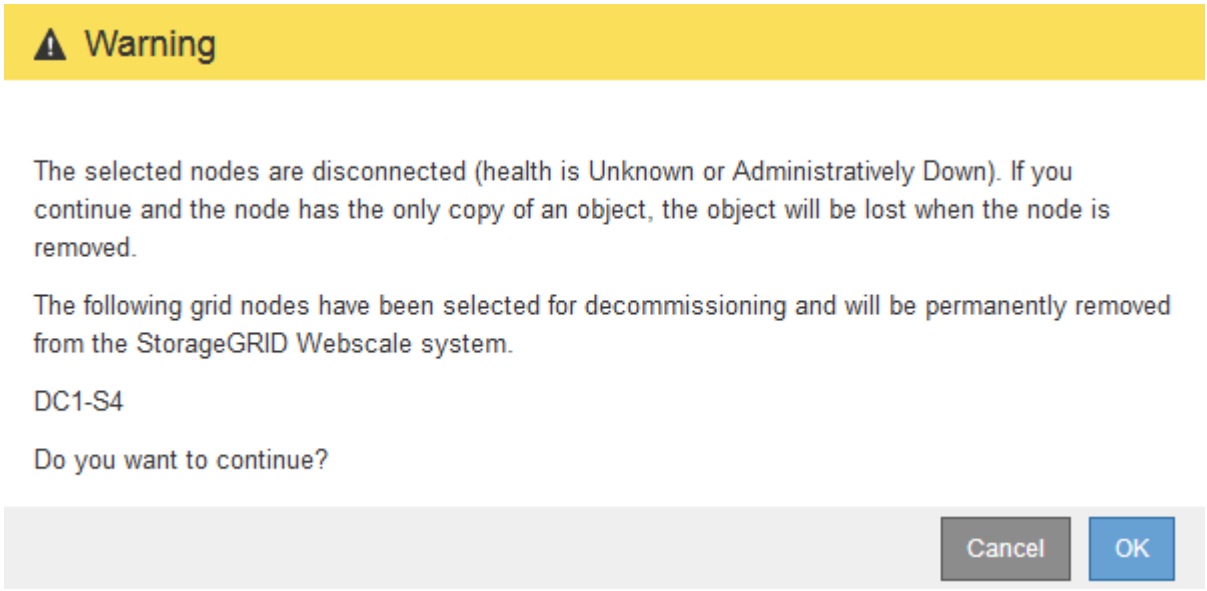
   > 切断されている複数のグリッドノード、特に複数のストレージノードの運用を停止する場合は、特に注意が必要です。切断されていてリカバリできない複数のストレージノードがある場合は、テクニカルサポートに問い合わせて、最適な対処方法を確認してください。

3. プロビジョニングパスフレーズを入力します。

   [ * 分解を開始 * （ Start Decommission * ） ] ボタンが有効になります。

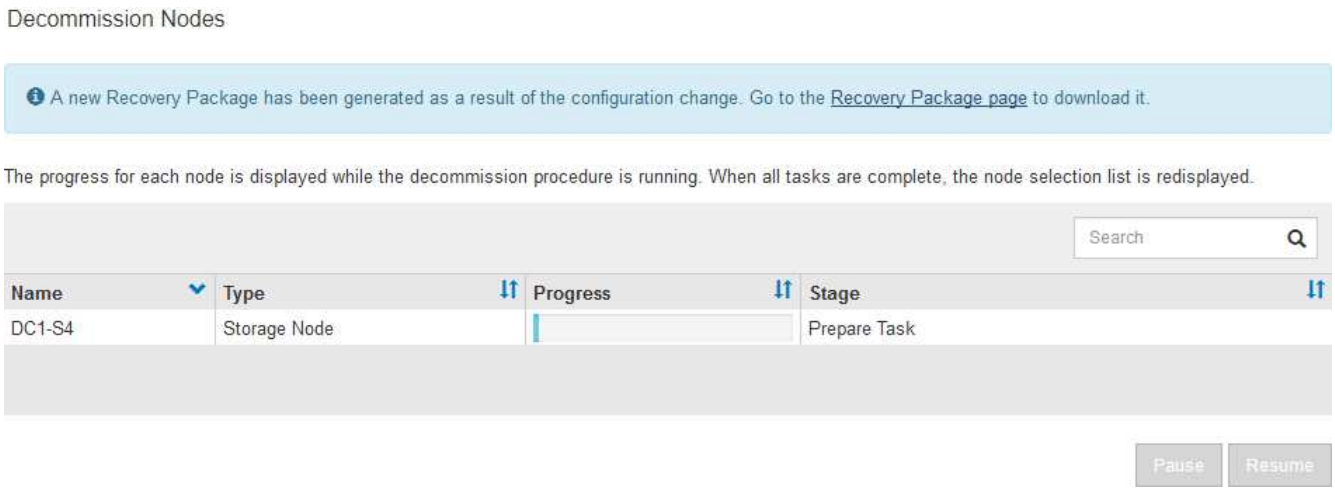
4. * 分解を開始 * をクリックします。

切断されているノードが選択されていることと、そのノードにオブジェクトの唯一のコピーが含まれている場合はオブジェクトデータが失われることを示す警告が表示されます。




5. ノードのリストを確認し、 * OK * をクリックします。

運用停止手順 が開始され、ノードごとの進行状況が表示されます。手順 の実行中に、グリッド設定の変更を含む新しいリカバリパッケージが生成されます。




6. 新しいリカバリパッケージが利用可能になったら、リンクをクリックするか、* Maintenance ** System * Recovery Package *を選択して、Recovery Packageページにアクセスします。次に、をダウンロードします `.zip` ファイル。

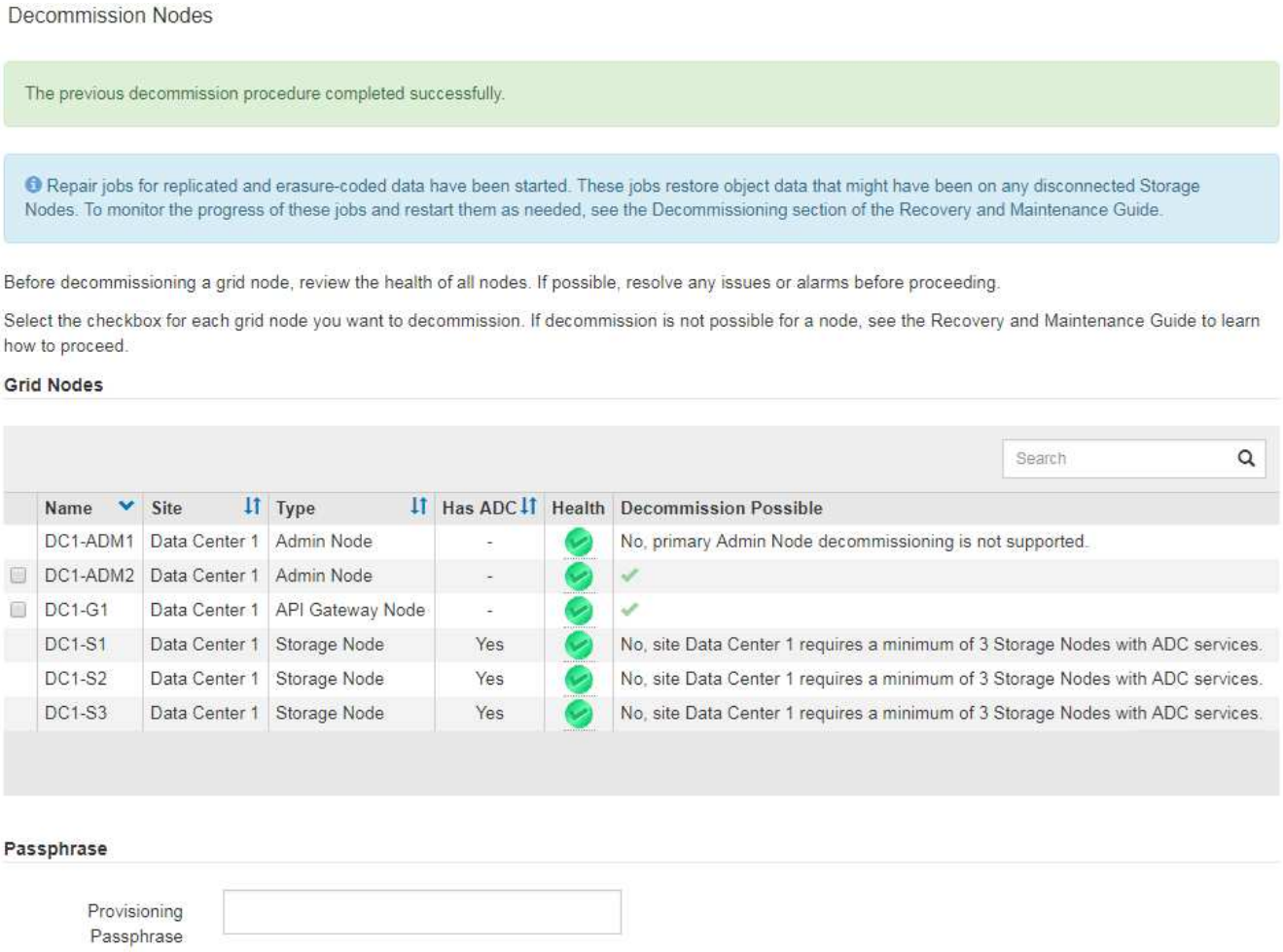
リカバリパッケージのダウンロード手順を参照してください。

手順 の運用停止中に問題が発生した場合にグリッドをリカバリできるよう、できるだけ早くリカバリパッケージをダウンロードしてください。

リカバリパッケージファイルには StorageGRID システムからデータを取得するための暗号キーとパスワードが含まれているため、安全に保管する必要があります。

7. 運用停止ページを定期的に監視して、選択したすべてのノードの運用が正常に停止されることを確認してください。

   ストレージノードの運用停止には、数日から数週間かかることがあります。すべてのタスクが完了すると、成功メッセージとともにノード選択リストが再表示されます。切断されているストレージノードの運用を停止した場合は、修復ジョブが開始されたことを示す情報メッセージが表示されます。




8. 運用停止手順 の一環としてノードが自動的にシャットダウンされたら、運用停止したノードに関連付けられている残りの仮想マシンやその他のリソースをすべて削除します。

   この手順は、ノードが自動的にシャットダウンするまでは実行しないでください。

9. ストレージノードの運用を停止している場合は、運用停止プロセス中に自動的に開始されるデータ修復ジョブのステータスを監視します。

   a. Support > Tools > Grid Topology *を選択します。

   b. グリッドトポロジツリーの上部にある「* StorageGRID deployment」を選択します。

   c. 概要タブで、ILMアクティビティセクションを探します。

   d. 次の属性を組み合わせて、レプリケートデータの修復が完了したかどうかを可能なかぎり判別します。

Cassandra に不整合が生じている可能性があり、また、失敗した修復は追跡されません。

- * Repairs Attempted （ XRPA ） * ：レプリケートデータの修復の進行状況を追跡します。この属性は、ストレージノードがハイリスクオブジェクトの修復を試みるたびに値が増分します。この属性の値が現在のスキャン期間（ * Scan Period - - Estimated * 属性で指定）よりも長い期間にわたって上昇しない場合、 ILM スキャンはすべてのノードで修復が必要なハイリスクオブジェクトを検出していません。

  ハイリスクオブジェクトとは、完全に失われる危険があるオブジェクトです。ILM 設定を満たしていないオブジェクトは含まれません。

- * スキャン期間 - 推定（ XSCM ） * ：この属性を使用して、以前に取り込まれたオブジェクトにポリシー変更が適用されるタイミングを見積もります。「 * Repairs Attempted * 」属性が現在のスキャン期間よりも長くなっていない場合は、複製修復が実行されている可能性があります。スキャン期間は変わる可能性があるので注意してください。* Scan Period - - Estimated （ XSCM ） * 属性は、グリッド全体の環境 を示します。これは、すべてのノードのスキャン期間の最大値です。グリッドの * Scan Period - - Estimated * 属性履歴を照会して、適切な期間を判断できます。

e. 修復を追跡または再開するには、次のコマンドを使用します。

   - を使用します `repair-data show-ec-repair-status` イレイジャーコーディングデータの修復を追跡するコマンド。
   - を使用します `repair-data start-ec-node-repair` コマンドにを指定します `--repair-id` 失敗した修復を再開するオプションです。データ修復ジョブの確認手順を参照してください。

10. 修復ジョブがすべて正常に完了するまで、引き続きECデータの修復のステータスを追跡します。

    切断されているノードが運用停止され、すべてのデータ修復ジョブが完了したら、必要に応じて、接続されているグリッドノードの運用を停止できます。

手順 の運用停止が完了したら、次の手順を実行します。

- 運用停止したグリッドノードのドライブを確実に消去します。市販のデータ消去ツールまたはデータ消去サービスを使用して、ドライブからデータを完全かつ安全に削除します。
- アプライアンスノードの運用を停止し、ノード暗号化を使用してアプライアンスのデータが保護されていた場合は、 StorageGRID アプライアンスインストーラを使用してキー管理サーバ設定（ Clear KMS ）をクリアします。アプライアンスを別のグリッドに追加する場合は、 KMS の設定をクリアする必要があります。

  "SG100 SG1000サービスアプライアンス"

  "SG5600 ストレージアプライアンス"

  "SG5700 ストレージアプライアンス"

  "SG6000 ストレージアプライアンス"

関連情報

"グリッドノードのリカバリ手順"

"リカバリパッケージをダウンロードしています"

"データ修復ジョブを確認しています"

接続されているグリッドノードの運用停止

# グリッドに接続されているノードは、運用停止して完全に削除できます。

必要なもの

- グリッドノードの運用停止に関する要件と考慮事項を理解しておく必要があります。

  "グリッドノードの運用停止に関する考慮事項"

- 必要な情報やデータ、機器をすべて揃えておきます。
- アクティブなデータ修復ジョブがないことを確認しておきます。
- グリッド内でストレージノードのリカバリが実行中でないことを確認します。実行中の場合は、リカバリの一環として実行される Cassandra の再構築が完了するまで待機する必要があります。そのあとで運用停止を続行できます。
- ノード運用停止手順 が一時停止されていないかぎり、ノード手順 の運用停止中に他のメンテナンス手順が実行されないようにしておきます。
- プロビジョニングパスフレーズを用意します。
- Grid ノードが接続されています。
- 運用停止するノードの*運用停止の候補*列に、緑のチェックマークが表示されます。
- すべてのグリッドノードが正常（緑）な状態です。* Health * 列に次のいずれかのアイコンが表示された場合は、問題 を解決する必要があります。

| をクリックします。 | 色（ Color ） | 重大度 |
| --- | --- | --- |
| | 黄色 | 注意 |
| | 薄いオレンジ | マイナー |
| | 濃いオレンジ | メジャー（ Major ） |
| | 赤 | 重要 |

- 以前に切断されているストレージノードの運用を停止した場合は、データ修復ジョブがすべて正常に完了している。データ修復ジョブの確認手順を参照してください。

この手順 で指示されるまでは、グリッドノードの仮想マシンやその他のリソースを削除しないでください。

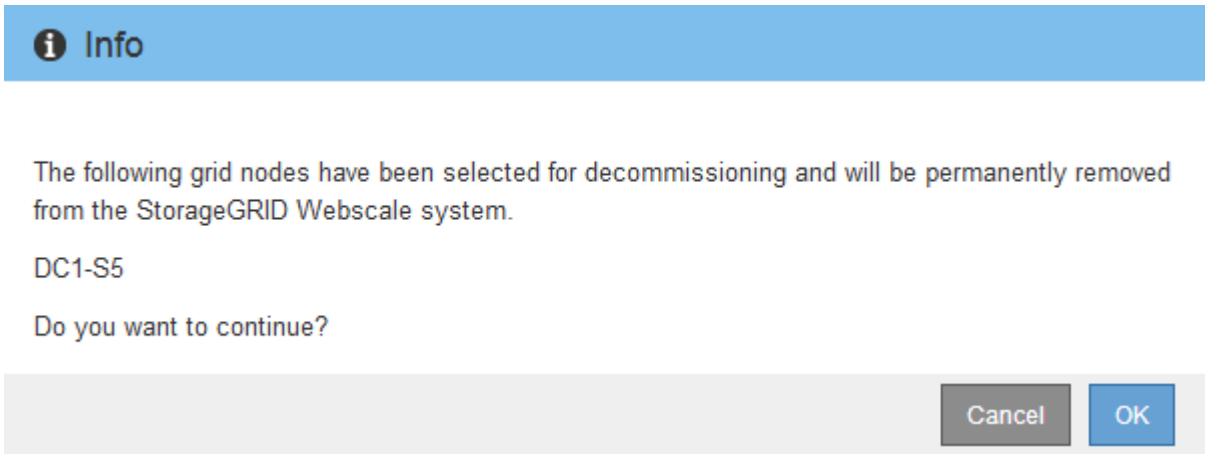
手順

1. Decommission Nodes ページで、運用を停止するグリッドノードのチェックボックスを選択します。
2. プロビジョニングパスフレーズを入力します。

   [ * 分解を開始 * （ Start Decommission * ） ] ボタンが有効になります。

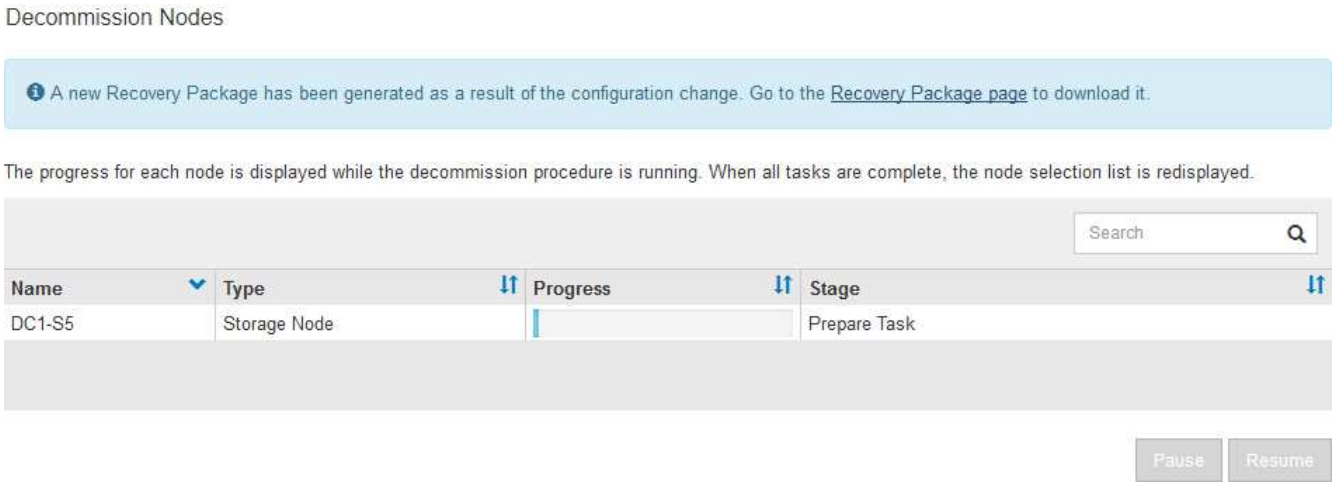
3. * 分解を開始 * をクリックします。

   確認のダイアログボックスが表示されます。




4. 選択したノードのリストを確認し、 * OK * をクリックします。

   ノードの運用停止手順 が開始され、各ノードの進捗状況が表示されます。手順 の実行中、グリッド設定の変更を反映するために新しいリカバリパッケージが生成されます。




> 運用停止手順 の開始後は、ストレージノードをオフラインにしないでください。状態を変更すると、一部のコンテンツが他の場所にコピーされなくなる可能性があります。

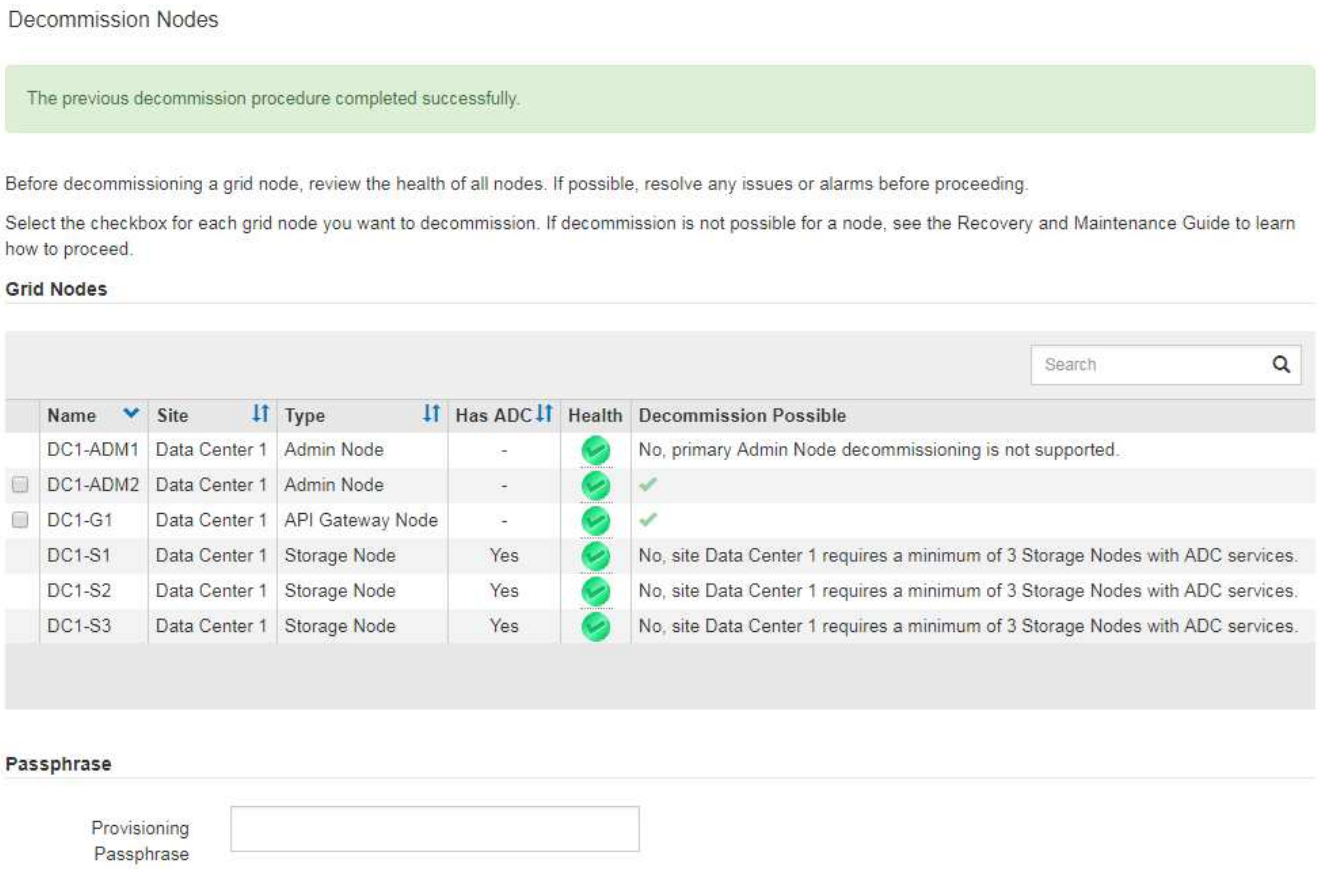
5. 新しいリカバリパッケージが利用可能になったら、リンクをクリックするか、* Maintenance ** System * Recovery Package *を選択して、Recovery Packageページにアクセスします。次に、をダウンロードします `.zip` ファイル。

   リカバリパッケージのダウンロード手順を参照してください。

手順 の運用停止中に問題が発生した場合にグリッドをリカバリできるよう、できるだけ早くリカバリパッケージをダウンロードしてください。

6. Decommission Nodes ページを定期的に監視して、選択したすべてのノードの運用が正常に停止されることを確認します。

   ストレージノードの運用停止には、数日から数週間かかることがあります。すべてのタスクが完了すると、成功メッセージとともにノード選択リストが再表示されます。




7. プラットフォームに応じた手順に従います。例：

   - * Linux * ：インストール中に作成したノード構成ファイルを削除してボリュームの接続を解除できます。
   - **vmware**: vCenter の「 Delete from Disk 」オプションを使用して、仮想マシンを削除できます。また、仮想マシンに依存しないデータディスクを削除しなければならない場合もあります。
   - * StorageGRID アプライアンス * ：アプライアンスノードは自動的に導入されていない状態に戻り、StorageGRID アプライアンスインストーラにアクセスできます。アプライアンスの電源をオフにするか、別の StorageGRID システムに追加できます。

ノードの運用停止手順 が完了したら、次の手順を実行します。

- 運用停止したグリッドノードのドライブを確実に消去します。市販のデータ消去ツールまたはデータ消去サービスを使用して、ドライブからデータを完全かつ安全に削除します。
- アプライアンスノードの運用を停止し、ノード暗号化を使用してアプライアンスのデータが保護されていた場合は、 StorageGRID アプライアンスインストーラを使用してキー管理サーバ設定（ Clear KMS ）をクリアします。アプライアンスを別のグリッドで使用する場合は、 KMS の設定をクリアする必要があり

ます。

"SG100 SG1000サービスアプライアンス"

"SG5600 ストレージアプライアンス"

"SG5700 ストレージアプライアンス"

"SG6000 ストレージアプライアンス"

関連情報

"データ修復ジョブを確認しています"

"リカバリパッケージをダウンロードしています"

"Red Hat Enterprise Linux または CentOS をインストールします"

ストレージノードの運用停止プロセスの一時停止と再開

必要に応じて、ストレージノードの運用停止手順 を特定の段階で一時停止できます。別のメンテナンス手順 を開始するには、ストレージノードで運用停止手順を一時停止する必要があります。もう一方の手順 の運用停止が完了したら、運用停止手順を再開できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Maintenance または Root Access 権限が必要です。

手順

1. [* Maintenance （メンテナンス）**]>[** Maintenance Tasks（メンテナンスタスク）]**>[** Decommission]*を選択します

   Decommission ページが表示されます。

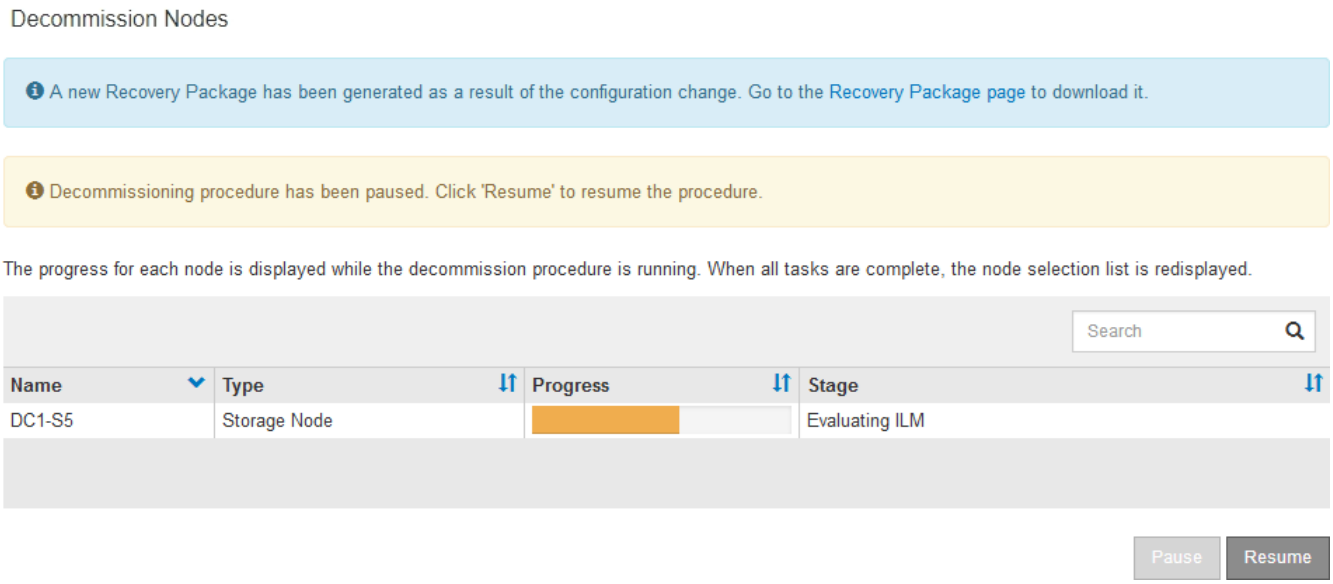
2. [* Decommission Nodes]をクリックします。

   Decommission Nodes ページが表示されます。手順 の運用停止が次のいずれかの段階に達すると、 * 一時停止 * ボタンが有効になります。

   - ILM を評価中です
   - イレイジャーコーディングデータの運用停止

3. 手順 を一時停止するには、*一時停止*をクリックします。

   現在のステージが一時停止され、 * Resume * （続行）ボタンが有効になります。




4. もう1つのメンテナンス手順 が終了したら、[* Resume（続行）]をクリックして運用停止を続行します。

ノードの運用停止のトラブルシューティング

# エラーが原因でノードの手順 の運用が停止した場合は、特定の手順に従って問題のトラブルシューティングを実施できます。

必要なもの

Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

このタスクについて

運用停止処理中のグリッドノードをシャットダウンすると、グリッドノードが再起動されるまでタスクが停止します。グリッドノードはオンラインである必要があります。

手順

1. Support > Tools > Grid Topology *を選択します。
2. グリッドトポロジツリーで各ストレージノードエントリを展開し、 DDS サービスと LDR サービスがオンラインになっていることを確認します。

   ストレージノードの運用を停止するには、StorageGRID システムのDDSサービス（ストレージノードでホストされるサービス）がオンラインになっている必要があります。これはILMルールによる再評価の要件です。

3. アクティブなグリッドタスクを表示するには、「* primary Admin Node * CMN * Grid Tasks * Overview *」を選択します。
4. グリッドタスクの運用停止のステータスを確認します。

   a. グリッドタスクの運用停止ステータスがグリッドタスクバンドルの保存の問題を示している場合は、「* primary Admin Node ** CMN * Events * Overview *」を選択します

   b. 使用可能な監査リレーの数を確認します。

      Available Audit Relay 属性が 1 つ以上の場合、 CMN サービスは少なくとも 1 つの ADC サービスに接続されています。ADC サービスは監査リレーとして機能します。

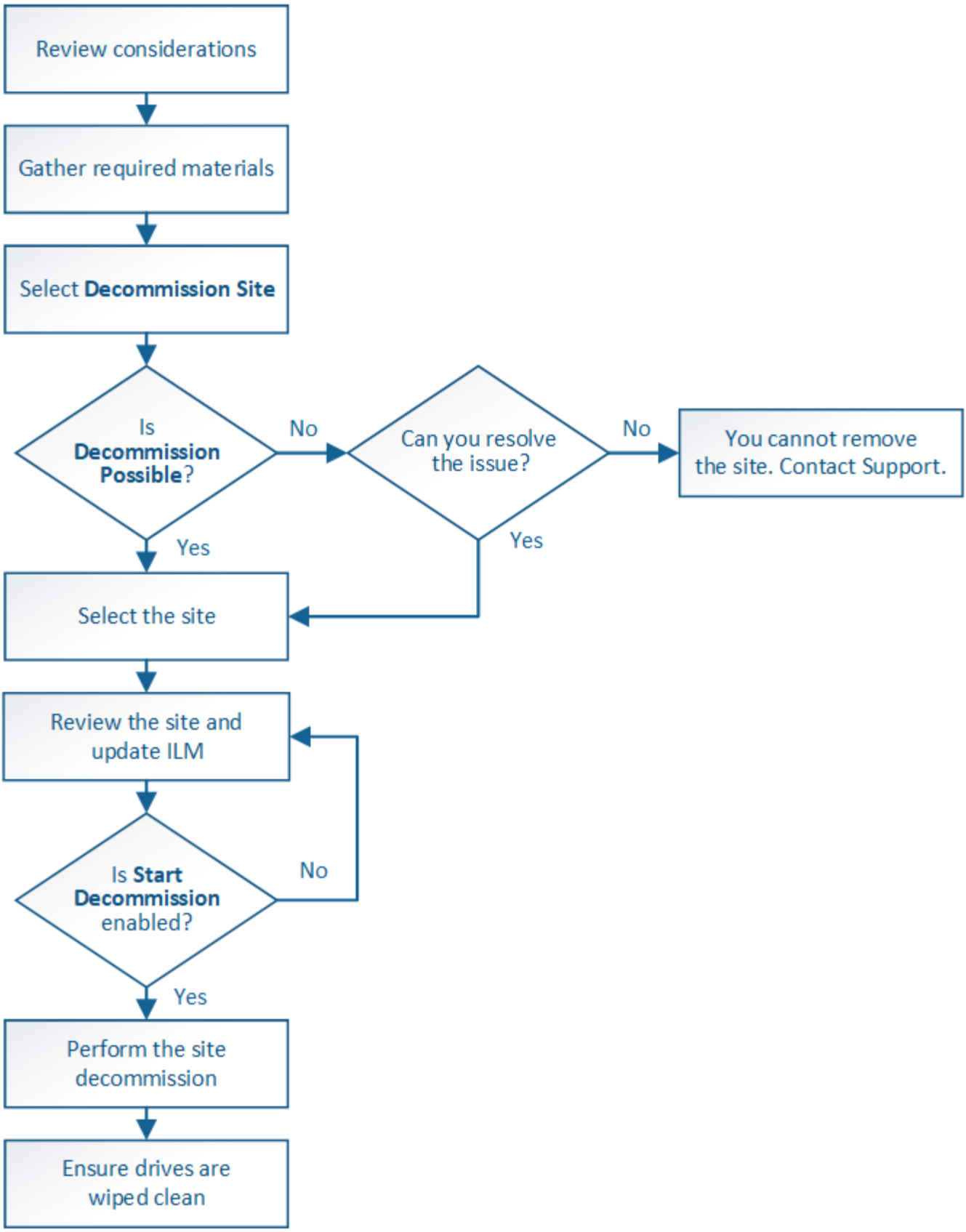
グリッドタスクで運用停止処理をあるステージから別のステージに進めて終了させるには、 CMN サービスが少なくとも 1 つの ADC サービスに接続され、かつ StorageGRID システムの ADC サービスの過半数（ 50%+1 ）が使用可能である必要があります。

a. CMN サービスが十分な数の ADC サービスに接続されていない場合は、ストレージノードがオンラインであることを確認し、プライマリ管理ノードとストレージノードの間のネットワーク接続を確認します。

サイトの運用停止

## データセンターサイトの StorageGRID システムからの削除が必要になる場合があります。サイトを削除するには、サイトの運用を停止する必要があります。

次のフローチャートは、サイトの運用停止手順の概要を示しています。




手順

- "サイトの削除に関する考慮事項"
- "前提要件"

- "手順 1 ： [ サイト ] を選択します"]
- "手順 2 ：詳細を表示する"
- "手順 3 ： ILM ポリシーを改訂する"
- "手順 4 ： ILM 参照を削除する"
- "手順 5 ：ノードの競合を解決する（運用停止を開始する）"
- "ステップ 6 ：運用停止を監視する"

サイトの削除に関する考慮事項

# サイトの運用停止手順 を使用してサイトを削除する前に、考慮事項を確認しておく必要があります。

## サイトの運用を停止した場合の動作

サイトの運用を停止すると、 StorageGRID はサイトのすべてのノードとサイト自体を StorageGRID システムから完全に削除します。

## サイトの運用停止手順 が完了したら、次の手順を実行します

- StorageGRID を使用してサイトやサイトの任意のノードを表示したり、アクセスしたりすることはできなくなります。
- サイトを参照するストレージプールやイレイジャーコーディングプロファイルは使用できなくなります。サイトを StorageGRID が運用停止すると、これらのストレージプールが自動的に削除され、イレイジャーコーディングプロファイルが非アクティブ化されます。

## 接続されているサイトと切断されているサイトの運用停止手順の違い

サイト運用停止手順 を使用すると、すべてのノードが StorageGRID に接続されているサイト（接続されていないサイトの運用停止と呼ばれる）を削除したり、すべてのノードが StorageGRID から切断されているサイト（切断されたサイトの運用停止と呼ばれる）を削除したりできます。作業を開始する前に、これらの手順の違いを理解しておく必要があります。

> サイトに接続された（✔）および切断されているノード（⬟ または ⬟）の場合は、すべてのオフラインノードをオンラインに戻す必要があります。

- 接続されたサイトの運用停止機能を使用すると、 StorageGRID システムから運用サイトを削除できます。たとえば、接続されたサイトの運用停止を実行して、機能しているが不要になったサイトを削除できます。
- StorageGRID は、接続されているサイトを削除する際、 ILM を使用してサイトのオブジェクトデータを管理します。接続されたサイトの運用停止を開始するには、すべての ILM ルールからサイトを削除し、新しい ILM ポリシーをアクティブ化する必要があります。オブジェクトデータを移行するための ILM プロセスとサイトを削除するための内部プロセスは同時に発生する可能性がありますが、実際の運用停止手順を開始する前に ILM の手順を完了しておくことを推奨します。
- 切断されたサイトの運用停止機能を使用すると、障害が発生したサイトを StorageGRID システムから削除できます。たとえば、切断されたサイトの運用停止を実行して、火災や洪水によって破壊されたサイトを削除できます。

切断されているサイトを削除すると、 StorageGRID はすべてのノードをリカバリ不能とみなし、データの保持を試みません。ただし、切断されたサイトの運用停止を開始する前に、サイトをすべての ILM ルールから削除して、新しい ILM ポリシーをアクティブ化する必要があります。

> ⓘ 切断されたサイトの運用停止手順 を実行する前に、ネットアップのアカウント担当者にお問い合わせください。運用停止サイトのウィザードですべての手順を有効にする前に、要件を確認してください。切断されているサイトの運用停止は、サイトをリカバリしたり、サイトからオブジェクトデータをリカバリしたりできる可能性がある場合は、試行しないでください。

接続されているサイトまたは切断されているサイトを削除するための一般的な要件

接続されているサイトや切断されているサイトを削除する前に、次の要件について確認しておく必要があります。

- プライマリ管理ノードを含むサイトの運用を停止することはできません。
- アーカイブノードが含まれているサイトは運用停止できません。
- ハイアベイラビリティ（ HA ）グループに属するインターフェイスがあるノードがある場合は、サイトの運用を停止できません。HA グループを編集してノードのインターフェイスを削除するか、 HA グループ全体を削除する必要があります。
- 接続されているサイト（ ）および切断（ または ）をクリックします。
- 他のサイトのいずれかのノードが切断されている（の場合）は、サイトの運用を停止できません または ）。
- EC ノードの修復処理が進行中の場合、サイトの運用停止手順 を開始することはできません。イレイジャーコーディングデータの修復を追跡するには、次のトピックを参照してください。

  "データ修復ジョブを確認しています"

- サイトの運用停止中は、手順 は次の処理を実行します。
  - 運用停止するサイトを参照する ILM ルールは作成できません。サイトを参照する既存の ILM ルールを編集することもできません。
  - 拡張やアップグレードなどの他のメンテナンス手順は実行できません。

    > ⓘ 接続されているサイトの運用停止中に別のメンテナンス手順 を実行する必要がある場合は、ストレージノードを削除している間に手順 を一時停止できます。[Pause （一時停止） ] ボタンは、「デコミッション・レプリケート・データとイレイジャーコーディング・データ」ステージの間に有効になります。

  - サイトの運用停止手順 の開始後にノードをリカバリする必要がある場合は、サポートにお問い合わせください。
- 一度に複数のサイトの運用を停止することはできません。
- サイトに 1 つ以上の管理ノードが含まれており、 StorageGRID システムでシングルサインオン（ SSO ）が有効になっている場合は、そのサイトに対する証明書利用者信頼をすべて Active Directory フェデレーションサービス（ AD FS ）から削除する必要があります。

### 情報ライフサイクル管理（ **ILM** ）の要件

サイトを削除する場合は、 ILM 設定を更新する必要があります。Decommission Site ウィザードでは、次のことを確認するために、いくつかの前提条件となる手順を実行できます。

- アクティブな ILM ポリシーではサイトが参照されません。その場合は、新しい ILM ルールを使用して新しい ILM ポリシーを作成してアクティブ化する必要があります。
- ドラフトの ILM ポリシーが存在しません。ドラフトポリシーがある場合は削除する必要があります。
- アクティブポリシーまたはドラフトポリシーで使用されていない ILM ルールはサイトを参照していません。サイトを参照するすべてのルールを削除または編集する必要があります。

サイトを StorageGRID が運用停止すると、そのサイトを参照している未使用のイレイジャーコーディングプロファイルは自動的に非アクティブ化され、サイトを参照している未使用のストレージプールが自動的に削除されます。システムデフォルトの All Storage Nodes ストレージプールは、すべてのサイトを使用するため削除されます。

> サイトを削除する前に、新しい ILM ルールを作成して新しい ILM ポリシーをアクティブ化する必要がある場合があります。この手順を実行するには、 ILM の仕組みと、ストレージプール、イレイジャーコーディングプロファイル、 ILM ルール、 ILM ポリシーのシミュレートとアクティブ化について十分に理解している必要があります。情報ライフサイクル管理を使用してオブジェクトを管理する手順を参照してください。

"ILM を使用してオブジェクトを管理する"

### 接続されているサイトでのオブジェクトデータに関する考慮事項

接続されたサイトの運用停止を実行する場合は、新しい ILM ルールと新しい ILM ポリシーを作成するときに、サイトの既存のオブジェクトデータで実行する処理を決定する必要があります。次のいずれか、または両方を実行できます。

- 選択したサイトからグリッド内の 1 つ以上の他のサイトにオブジェクトデータを移動します。
- データ移動の例 * ：サニーベールで新しいサイトを追加したために、ローリーでサイトの運用を停止するとします。この例では、すべてのオブジェクトデータを古いサイトから新しいサイトに移動します。ILM ルールと ILM ポリシーを更新する前に、両方のサイトで容量を確認する必要があります。サニーベールサイトにローリーサイトのオブジェクトデータを保存できるだけの十分な容量があり、将来の成長に備えてサニーベールに十分な容量が残っていることを確認する必要があります。

  > 十分な容量を使用できるようにするために、この手順 を実行する前に既存のサイトにストレージボリュームまたはストレージノードを追加したり、新しいサイトを追加したりしなければならない場合があります。StorageGRID システムの拡張手順を参照してください。

- 選択したサイトからオブジェクトコピーを削除します。
- データの削除の例 * ：現在、 3 コピーの ILM ルールを使用して 3 つのサイト間でオブジェクトデータをレプリケートしているとします。サイトの運用を停止する前に、同等の 2-copy ILM ルールを作成して、 2 つのサイトにのみデータを格納することができます。2-copy ルールを使用する新しい ILM ポリシーをアクティブ化すると、 ILM 要件を満たさなくなるため、 StorageGRID は 3 番目のサイトからコピーを削除します。ただし、オブジェクトデータは引き続き保護され、残りの 2 つのサイトの容量は同じになります。

サイトの削除に対応するためにシングルコピーの ILM ルールを作成しないでください。ある期間にレプリケートコピーを 1 つしか作成しない ILM ルールには、データが永続的に失われるリスクがあります。オブジェクトのレプリケートコピーが 1 つしかない場合、ストレージノードに障害が発生したり、重大なエラーが発生すると、そのオブジェクトは失われます。また、アップグレードなどのメンテナンス作業中は、オブジェクトへのアクセスが一時的に失われます。

### 接続されたサイトの運用停止に関する追加要件

StorageGRID で接続されているサイトを削除する前に、次の点を確認してください。

- StorageGRID システムのすべてのノードの接続状態が * connected * （）です。ただし、ノードにはアクティブなアラートを含めることができます。

1 つ以上のノードが切断されている場合は、 Decommission Site ウィザードの手順 1~4 を完了できます。ただし、すべてのノードが接続されていないと、ウィザードの手順 5 を実行して運用停止プロセスを開始することはできません。

- 削除するサイトにゲートウェイノードまたは負荷分散に使用される管理ノードが含まれている場合は、拡張手順 を実行して同等の新しいノードを別のサイトに追加しなければならないことがあります。サイトの運用停止手順 を開始する前に、クライアントが交換用ノードに接続できることを確認してください。
- 削除するサイトにハイアベイラビリティ（ HA ）グループ内のゲートウェイノードまたは管理ノードがある場合は、運用停止サイトウィザードの手順 1~4 を完了できます。ただし、ウィザードの手順 5 を実行して運用停止プロセスを開始する場合は、これらのノードをすべての HA グループから削除する必要があります。既存のクライアントがサイトのノードを含む HA グループに接続している場合は、サイトの削除後も引き続き StorageGRID に接続できることを確認する必要があります。
- 削除するサイトのストレージノードにクライアントが直接接続している場合は、サイトの運用停止手順 を開始する前に、それらのクライアントが他のサイトのストレージノードに接続できることを確認する必要があります。
- アクティブな ILM ポリシーの変更に伴い移動されるオブジェクトデータに対応できる十分なスペースを残りのサイトに確保する必要があります。接続されているサイトの運用停止を完了する前に、ストレージノード、ストレージボリューム、または新しいサイトを追加して StorageGRID システムの拡張が必要になる場合があります。
- 手順 の運用停止が完了するまでに、十分な時間を確保する必要があります。StorageGRID の ILM プロセスの運用が停止されるまでに、サイトからオブジェクトデータを移動または削除するのに数日、数週間、場合によっては数カ月かかることがあります。

サイトからオブジェクトデータを移動または削除するには、サイトのデータ量、システムの負荷、ネットワークのレイテンシ、および ILM に求められる変更の性質に応じて、数日、数週間、場合によっては数カ月かかることがあります。

- Decommission Site ウィザードの手順 1~4 をできるだけ早く完了する必要があります。実際の運用停止手順 を開始する前にサイトからデータを移動できるようにすると（ウィザードの手順 5 で「運用停止 * を開始」を選択して）、運用停止手順 の処理がより迅速になり、システム停止やパフォーマンスへの影響も少なくなります。

### 切断されたサイトの運用停止に関する追加要件

StorageGRID で切断されているサイトを削除する前に、次の点を確認してください。

- ネットアップのアカウント担当者に連絡しておきます。運用停止サイトのウィザードですべての手順を有効にする前に、要件を確認してください。

> 切断されているサイトの運用停止は、サイトをリカバリしたり、サイトからオブジェクトデータをリカバリしたりできる可能性がある場合は、試行しないでください。

- サイトのすべてのノードの接続状態が次のいずれかである必要があります。
  - * 不明 * （）：不明な理由でノードがグリッドに接続されていません。たとえば、ノード間のネットワーク接続が失われた、電源が切れたなどの原因が考えられます。
  - * 管理上のダウン * （）：想定される理由でノードがグリッドに接続されていません。たとえば、ノード上のノードまたはサービスが正常にシャットダウンされたとします。
- 他のすべてのサイトのすべてのノードの接続状態が * connected * （のようになっている必要があります ただし、これらの他のノードにはアクティブなアラートを含めることができます。
- StorageGRID を使用してサイトに格納されているオブジェクトデータを表示したり読み出したりすることができなくなることを理解しておく必要があります。StorageGRID はこの手順 を実行する際、切断されているサイトのデータを一切保持しません。

> ILM ルールとポリシーが単一サイトの損失を防ぐように設計されている場合は、オブジェクトのコピーが残りのサイトに存在します。

- サイトにオブジェクトの唯一のコピーが含まれていた場合は、オブジェクトが失われて読み出しできないことを理解しておく必要があります。

サイトを削除するときの整合性制御に関する考慮事項

S3 バケットまたは Swift コンテナの整合性レベルにより、オブジェクトの取り込みが成功したことをクライアントに通知する前に、 StorageGRID がすべてのノードおよびサイトにオブジェクトメタデータを完全にレプリケートするかどうかが決まります。整合性レベルを設定する場合は、オブジェクトの可用性と、異なるストレージノードおよびサイト間におけるオブジェクトの整合性のどちらかを犠牲にしなければなりません。

StorageGRID でサイトを削除するときは、削除するサイトにデータが書き込まれていないことを確認する必要があります。その結果、各バケットまたはコンテナの整合性レベルが一時的に上書きされます。サイトの運用停止プロセスの開始後、 StorageGRID は一時的に strong-site 整合性を使用し、オブジェクトのメタデータがサイトに書き込まれないようにします。

この一時的な上書きの結果、残りのサイトで複数のノードが使用できなくなった場合、サイトの運用停止中に発生するクライアントの書き込み、更新、および削除の処理が失敗する可能性があることに注意してください。

関連情報

"テクニカルサポートによるサイトリカバリの実行方法"

"ILM を使用してオブジェクトを管理する"

"グリッドを展開します"

前提要件

## サイトの運用を停止する前に、以下を準備しておく必要があります。

| 項目 | 注： |
| --- | --- |
| リカバリパッケージ .zip ファイル。 | 最新のリカバリパッケージをダウンロードする必要があります .zip ファイル。（sgws-recovery-package-id-revision.zip）。リカバリパッケージファイルは、障害発生時のシステムのリストアに使用できます。 |
| Passwords.txt ファイル。 | このファイルには、コマンドラインでグリッドノードにアクセスするために必要なパスワードが格納されます。このファイルはリカバリパッケージに含まれています。 |
| プロビジョニングパスフレーズ | このパスフレーズは、 StorageGRID システムが最初にインストールされるときに作成されて文書化されます。プロビジョニングパスフレーズはに含まれていません Passwords.txt ファイル。 |
| 運用停止前の StorageGRID システムのトポロジの概要 | システムの現在のトポロジを記載したドキュメントがあれば、すべて入手します。 |

関連情報

"Web ブラウザの要件"

"リカバリパッケージをダウンロードしています"

手順 **1** ： **[** サイト **]** を選択します

## サイトの運用を停止できるかどうかを判断するには、まず Decommission Site ウィザードにアクセスします。

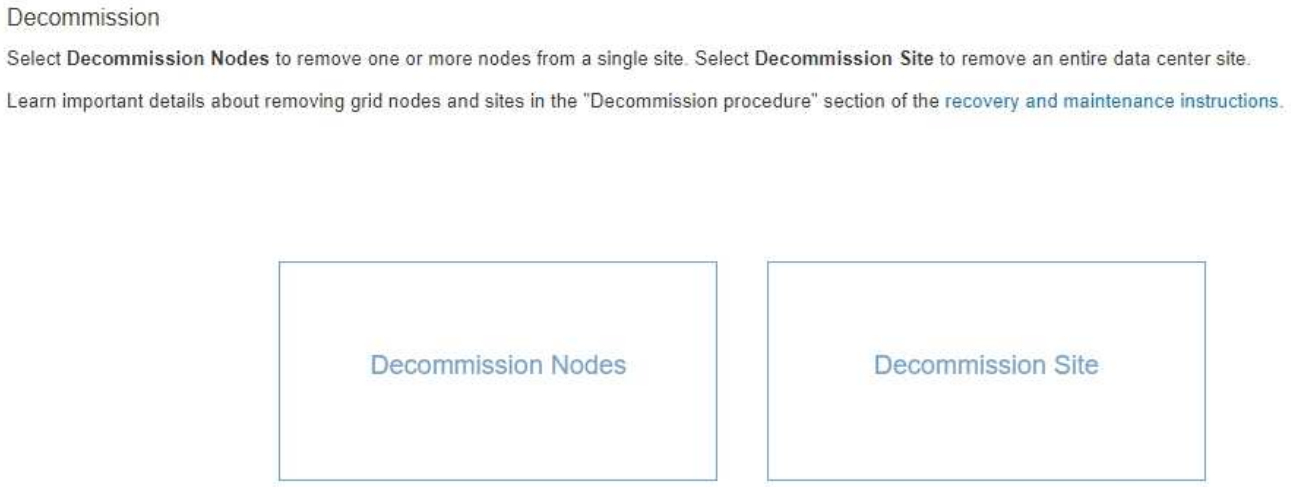
必要なもの

- 必要な情報やデータ、機器をすべて揃えておく必要があります。
- サイトの削除に関する考慮事項を確認しておく必要があります。
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限または Maintenance と ILM 権限が必要です。

手順

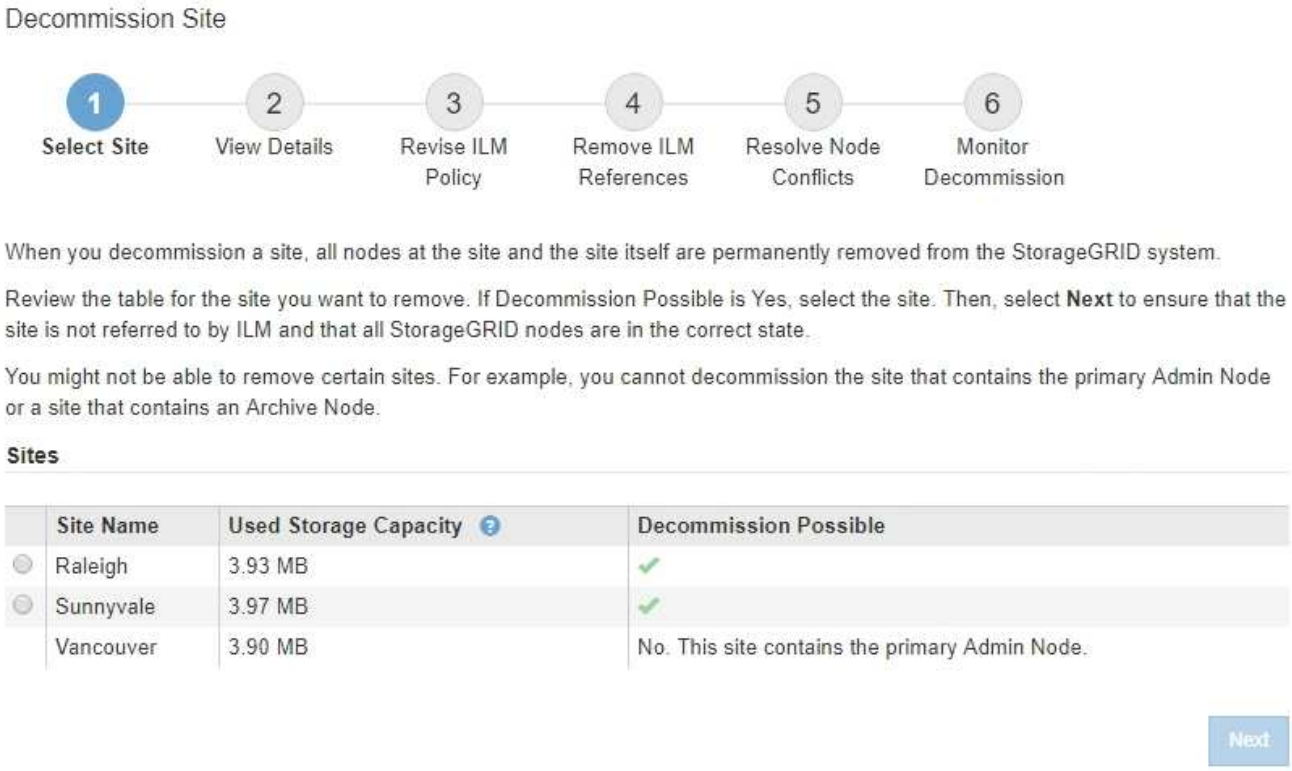
1. [* Maintenance （メンテナンス）**]>[** Maintenance Tasks（メンテナンスタスク）**]>[** Decommission]*を選択します

   Decommission ページが表示されます。




2. [Decommission Site]ボタンを選択します。

   Decommission Site ウィザードの Step 1 （ Select Site ）が表示されます。この手順には、 StorageGRID システムのサイトのアルファベット順に記載されています。




3. 「使用済みストレージ容量」列の値を確認し、各サイトのオブジェクトデータに現在使用されているストレージの容量を特定します。

   使用済みストレージ容量は概算値です。ノードがオフラインの場合は、ストレージの使用容量が最後に確認されたサイトの値になります。

   - 接続されたサイトの運用停止の場合、この値は、このサイトを安全に運用停止するために、他のサイトに移動したり、 ILM によって削除したりする必要があるオブジェクトデータの量を表します。

◦ 切断されているサイトの運用停止の場合、この値は、このサイトの運用を停止するとシステムのデータストレージにアクセスできなくなる容量を表します。

> 単一サイトの損失を防ぐように ILM ポリシーを設定した場合、オブジェクトデータのコピーが残りのサイトに残っている必要があります。

4. 「 * Decommission possible * 」列の理由を確認して、現在運用停止できるサイトを特定します。

> サイトの運用を停止できない理由が複数ある場合は、最も重大な理由が表示されます。

| 運用停止の可能性がある理由 | 説明 | 次の手順に進みます |
| --- | --- | --- |
| 緑のチェックマーク（✔) | このサイトは運用停止できます。 | に進みます 次の手順に進みます。 |
| いいえこのサイトにはプライマリ管理ノードが含まれています。 | プライマリ管理ノードを含むサイトの運用を停止することはできません。 | なしこの手順 は実行できません。 |
| いいえこのサイトにはアーカイブノードが 1 つ以上含まれています。 | アーカイブノードを含むサイトの運用を停止することはできません。 | なしこの手順 は実行できません。 |
| いいえこのサイトのすべてのノードが切断されています。ネットアップの担当者にお問い合わせください。 | サイト内のすべてのノードが接続されていないかぎり、接続されたサイトの運用停止を実行することはできません（✔）。 | 切断されたサイトの運用停止を実行する場合は、ネットアップのアカウント担当者にお問い合わせください。この担当者が要件を確認し、残りの運用停止サイトウィザードを有効にします。<br>• 重要 * ：サイトを削除できるように、オンラインノードをオフラインにしないでください。データが失われます。 |

この例は、 3 つのサイトからなる StorageGRID システムを示しています。緑のチェックマーク（✔）をローリーとサニーベールのサイトで運用停止できることを示しています。ただし、プライマリ管理ノードが含まれているため、バンクーバーサイトの運用を停止することはできません。

1. 運用停止が可能な場合は、サイトのオプションボタンを選択します。

   「 * 次へ * 」ボタンが有効になっています。

2. 「 * 次へ * 」を選択します。

   手順 2 （詳細を表示）が表示されます。

手順 **2** ：詳細を表示する

運用停止サイトウィザードの手順 2 （詳細を表示）では、サイトに含まれているノー

ド、各ストレージノードで使用されているスペースの量、およびグリッド内の他のサイトで利用可能な空きスペースの量を確認できます。

必要なもの

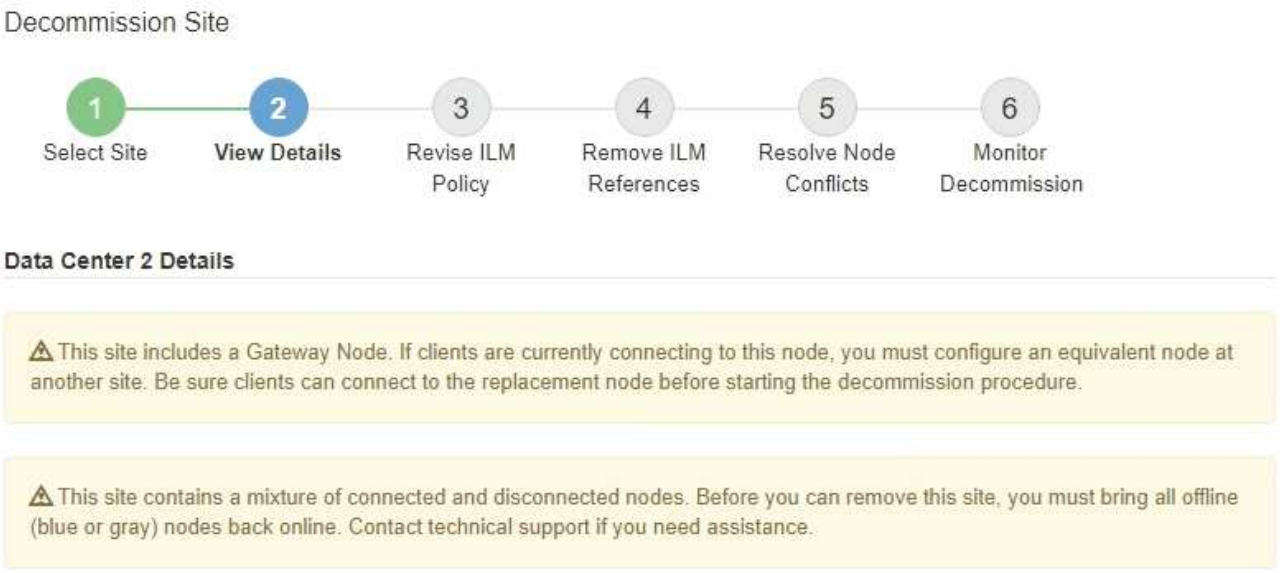
サイトの運用を停止する前に、サイトに格納されているオブジェクトデータの量を確認する必要があります。

- 接続されたサイトの運用停止処理を実行する場合は、 ILM を更新する前にサイトに現在存在しているオブジェクトデータの量を把握しておく必要があります。サイトの容量とデータ保護のニーズに基づいて、新しい ILM ルールを作成して、データを他のサイトに移動したり、サイトからオブジェクトデータを削除したりできます。
- 可能であれば、運用停止手順 を開始する前にストレージノードを拡張する必要があります。
- 切断されたサイトの運用停止処理を実行する場合は、サイトを削除した時点で永続的にアクセスできなくなるオブジェクトデータの量を把握しておく必要があります。

> ⓘ 切断されたサイトの運用停止を実行する場合、 ILM はオブジェクトデータを移動または削除できません。サイトに残っているデータはすべて失われます。ただし、単一サイトの損失を防ぐように ILM ポリシーが設計されている場合、オブジェクトデータのコピーは残りのサイトに残ります。

手順

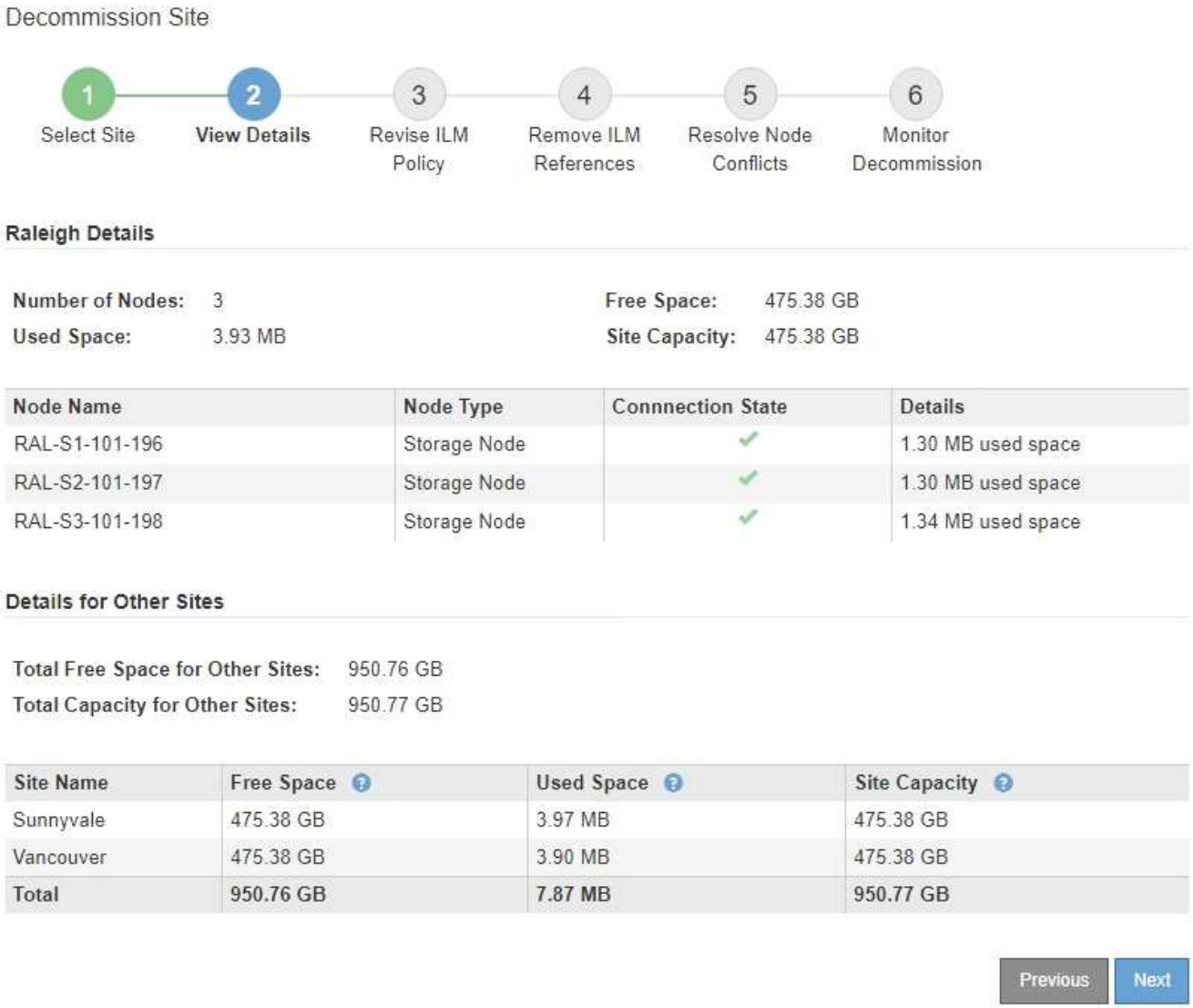
1. 手順 2 （詳細の表示）で、削除するように選択したサイトに関連する警告を確認します。




次の場合は警告が表示されます。

- サイトにゲートウェイノードが含まれている。S3 および Swift クライアントがこのノードに接続中の場合は、別のサイトに同じノードを設定する必要があります。手順 の運用停止を続行する前に、クライアントが交換用ノードに接続できることを確認してください。
- サイトには、接続された（✔）および切断されているノード（● または ?）。このサイトを削除する前に、すべてのオフラインノードをオンラインに戻す必要があります。

2. 削除するように選択したサイトの詳細を確認します。




選択したサイトについては、次の情報が表示されます。

- ノードの数
- サイト内のすべてのストレージノードの使用済みスペース、空きスペース、および容量の合計。
  - 接続されているサイトの運用停止の場合、「使用済みスペース」の値は、 ILM を使用して他のサイトに移動または削除する必要があるオブジェクトデータの量を表します。
  - 切断されたサイトの運用停止処理の場合、サイトを削除したときにアクセスできなくなるオブジェクトデータの量は「 * Used Space * 」の値で示されます。
- ノード名、タイプ、および接続状態：
  - （接続済み）
  - （意図的な停止）
  - （不明）
- 各ノードの詳細：
  - 各ストレージノードについて、オブジェクトデータに使用されているスペースの量。
  - 管理ノードとゲートウェイノードの場合、ノードが現在ハイアベイラビリティ（ HA ）グループで

使用されているかどうか。HA グループで使用されている管理ノードまたはゲートウェイノードの運用を停止することはできません。運用停止を開始する前に、 HA グループを編集して、サイトのすべてのノードを削除する必要があります。または、このサイトのノードだけが含まれている HA グループを削除することもできます。

"StorageGRID の管理"

3. ページの詳細セクションで、グリッド内の他のサイトで利用可能なスペースを評価します。

**Details for Other Sites**

| | |
|---|---|
| Total Free Space for Other Sites: | 950.76 GB |
| Total Capacity for Other Sites: | 950.77 GB |

| Site Name | Free Space | Used Space | Site Capacity |
|---|---|---|---|
| Sunnyvale | 475.38 GB | 3.97 MB | 475.38 GB |
| Vancouver | 475.38 GB | 3.90 MB | 475.38 GB |
| Total | 950.76 GB | 7.87 MB | 950.77 GB |

接続されたサイトの運用停止処理を実行していて、 ILM を使用して（削除するだけでなく）選択したサイトからオブジェクトデータを移動する場合は、移動されたデータに対応できる十分な容量を他のサイトに確保し、将来の拡張に備えて十分な容量を確保する必要があります。

削除するサイトの * 使用済みスペース * が、他のサイトの * 合計空きスペース * より大きい場合、警告が表示されます。サイトの削除後に十分なストレージ容量が確保されるようにするために、この手順 を実行する前に拡張の実行が必要になる場合があります。

4. 「 * 次へ * 」を選択します。

手順 3 （ ILM ポリシーの改訂）が表示されます。

関連情報

"ILM を使用してオブジェクトを管理する"

手順 **3** ： **ILM** ポリシーを改訂する

## 運用停止サイトウィザードの手順 3 （ ILM ポリシーを改訂）から、サイトがアクティブな ILM ポリシーで参照されているかどうかを確認できます。

必要なもの

ILM の仕組みを理解し、ストレージプール、イレイジャーコーディングプロファイル、 ILM ルールの作成、 ILM ポリシーのシミュレートとアクティブ化に精通していることを確認しておく必要があります。

"ILM を使用してオブジェクトを管理する"

このタスクについて

アクティブな ILM ポリシーのいずれかの ILM ルールでそのサイトが参照されている場合、 StorageGRID はサイトの運用を停止できません。

現在の ILM ポリシーが削除するサイトを参照している場合は、特定の要件を満たす新しい ILM ポリシーをアクティブ化する必要があります。具体的には、新しい ILM ポリシー：

- サイトを参照するストレージプールは使用できません。
- サイトを参照するイレイジャーコーディングプロファイルは使用できません。
- デフォルトの * All Storage Nodes * ストレージプール、またはデフォルトの * All Sites * サイトを使用することはできません。
- 組み込みの * Make 2 Copies * ルールを使用できません。
- すべてのオブジェクトデータを完全に保護するように設計する必要があります。

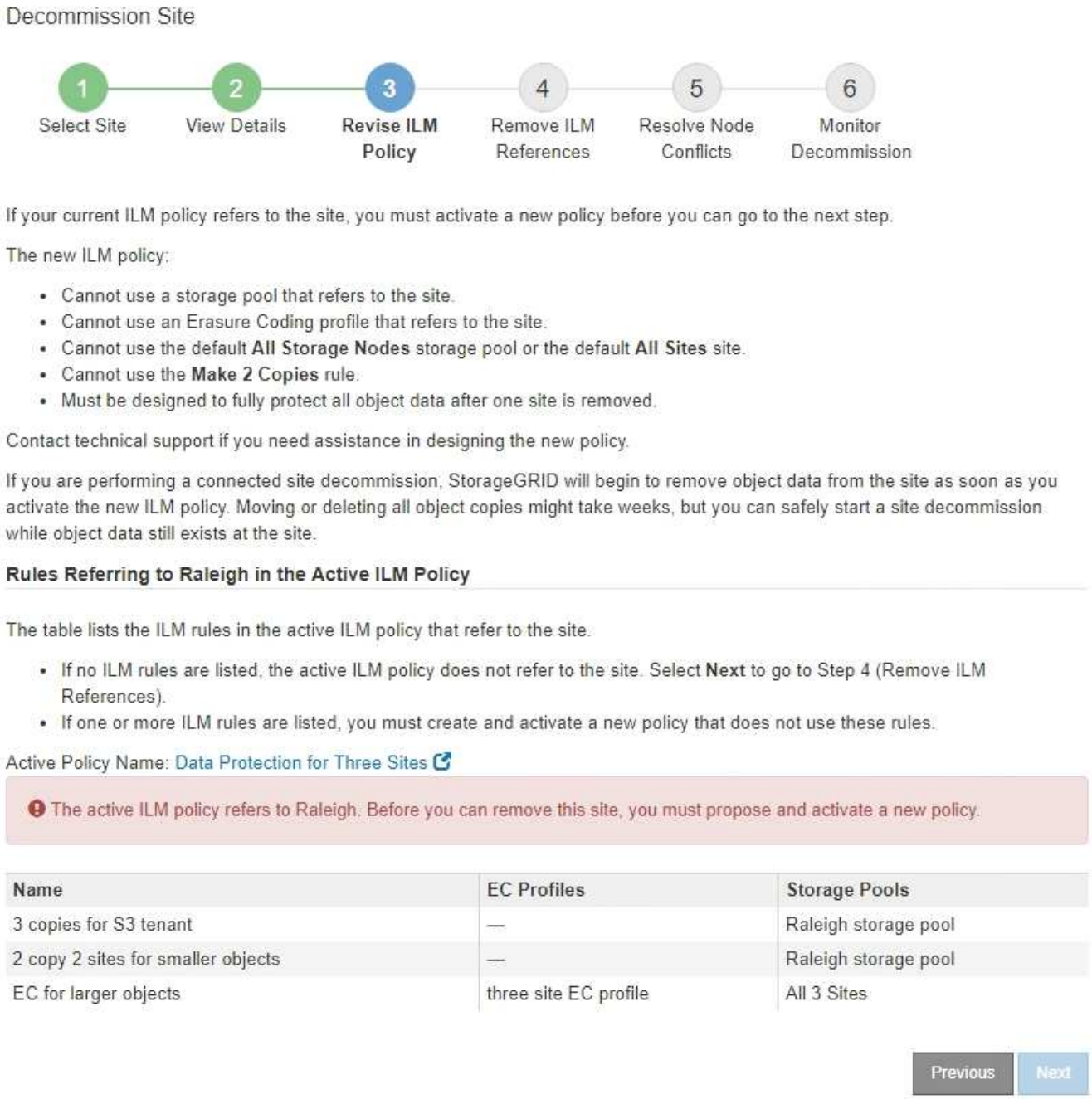
> サイトの削除に対応するためにシングルコピーの ILM ルールを作成しないでください。ある期間にレプリケートコピーを 1 つしか作成しない ILM ルールには、データが永続的に失われるリスクがあります。オブジェクトのレプリケートコピーが 1 つしかない場合、ストレージノードに障害が発生したり、重大なエラーが発生すると、そのオブジェクトは失われます。また、アップグレードなどのメンテナンス作業中は、オブジェクトへのアクセスが一時的に失われます。

_connected サイトの運用停止 _ を実行する場合は、削除するサイトに現在あるオブジェクトデータを StorageGRID でどのように管理するかを検討する必要があります。データ保護要件に応じて、新しいルールによって既存のオブジェクトデータを別のサイトに移動したり、不要になったオブジェクトコピーを削除したりできます。

新しいポリシーの設計でサポートが必要な場合は、テクニカルサポートにお問い合わせください。

手順

1. 手順 3 （ ILM ポリシーの改訂）で、アクティブな ILM ポリシー内の ILM ルールが削除対象として選択したサイトを参照しているかどうかを確認します。




2. ルールが表示されない場合は、「 * Next * 」を選択して手順 4 （ ILM 参照の削除）に進みます。

   "手順 4 ： ILM 参照を削除する"

3. テーブルに ILM ルールが 1 つ以上表示されている場合は、アクティブポリシー名 * の横のリンクを選択します。

   ブラウザの新しいタブに ILM ポリシーページが表示されます。このタブを使用して ILM を更新します。[Decommission Site] ページは、 [other] タブに表示されたままになります。

   a. 必要に応じて、* ILM **ストレージ・プール*を選択して、サイトを参照しない1つ以上のストレージ・プールを作成します。

詳細については、情報ライフサイクル管理を使用してオブジェクトを管理する手順を参照してください。

b. イレイジャーコーディングを使用する場合は、「* ILM イレイジャーコーディング」を選択して1つ以上のイレイジャーコーディングプロファイルを作成します。

サイトを参照していないストレージプールを選択する必要があります。

イレイジャーコーディングプロファイルでは、「 * All Storage Nodes * 」ストレージプールを使用しないでください。

4. 「* ILM ルール」を選択し、手順3（ILMポリシーの改訂）の表に記載された各ルールをクローニングします。

詳細については、情報ライフサイクル管理を使用してオブジェクトを管理する手順を参照してください。

a. 新しいポリシーでこれらのルールを簡単に選択できるように、名前を使用します。

b. 配置手順を更新します。

サイトを参照するストレージプールまたはイレイジャーコーディングプロファイルをすべて削除して、新しいストレージプールまたはイレイジャーコーディングプロファイルに置き換えます。

新しいルールでは、「 * All Storage Nodes * 」ストレージプールを使用しないでください。

5. 「* ILM ポリシー」を選択し、新しいルールを使用する新しいポリシーを作成します。

詳細については、情報ライフサイクル管理を使用してオブジェクトを管理する手順を参照してください。

a. アクティブなポリシーを選択し、 * Clone * を選択します。

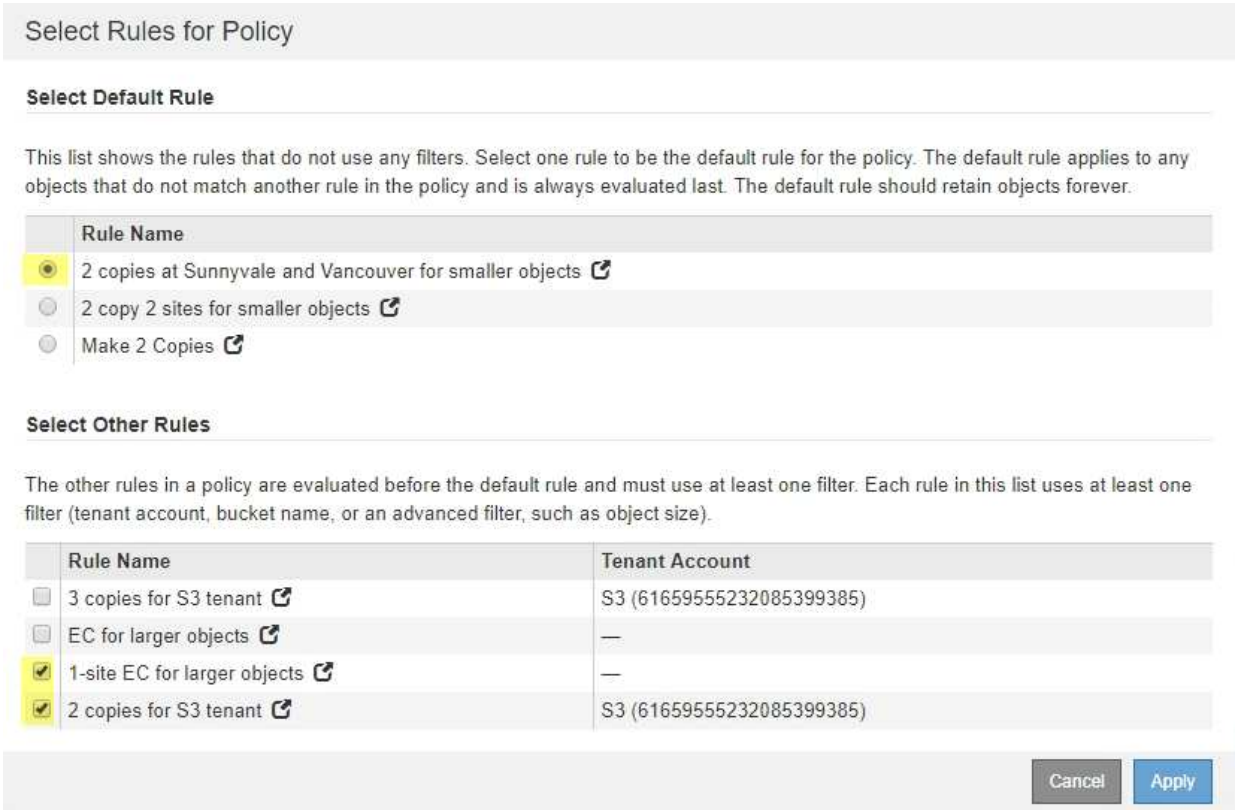
b. ポリシー名と変更理由を指定してください。

c. クローニングしたポリシーのルールを選択します。

- Decommission Site ページの Step 3 （ Revise ILM Policy ）にリストされているすべてのルールの選択を解除します。
- サイトを参照しないデフォルトのルールを選択します。

「 * Make 2 Copies * 」ルールは選択しないでください。このルールは、「 * All Storage Nodes * 」ストレージプールを使用し、これは許可されません。

- 作成した他の置換ルールを選択します。これらのルールはサイトを指していない必要があります。




d. * 適用 * を選択します。

e. 行をドラッグアンドドロップしてポリシー内のルールの順序を変更します。

デフォルトのルールは移動できません。

ILM ルールの順序が正しいことを確認してください。ポリシーをアクティブ化すると、新規および既存のオブジェクトがリスト内の順にルールによって評価されます。

a. ドラフトポリシーを保存します。

6. オブジェクトを取り込み、ドラフトポリシーをシミュレートして正しいルールが適用されることを確認します。

原因 ポリシーにエラーがあると、回復不能なデータ損失が発生する可能性があります。ポリシーをアクティブ化する前によく確認およびシミュレートし、想定どおりに機能することを確認してください。

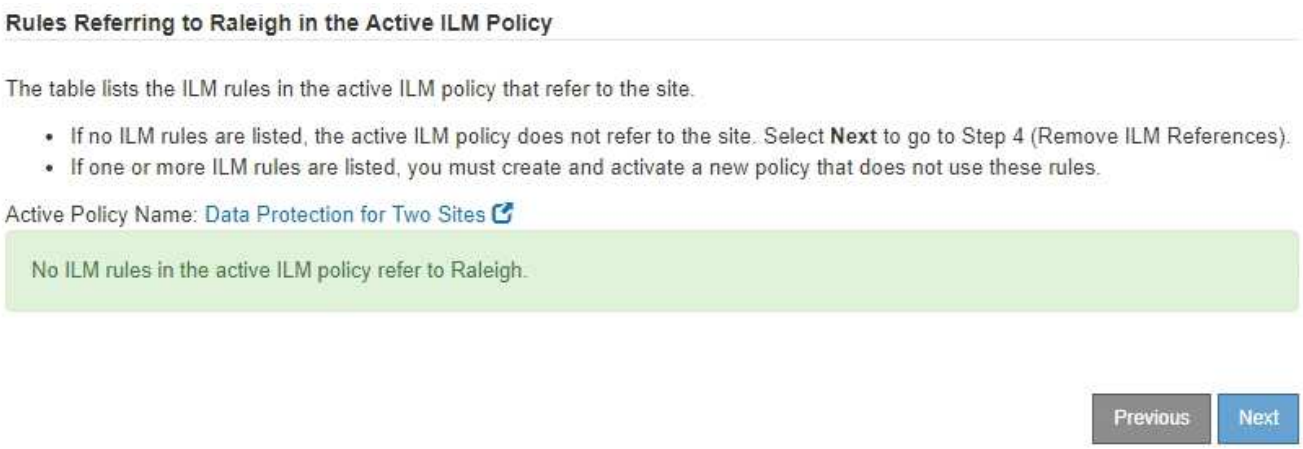
新しい ILM ポリシーをアクティブ化すると、 StorageGRID は、そのポリシーを使用して、既存のオブジェクトと新たに取り込まれたオブジェクトを含むすべてのオブジェクトを管理します。新しい ILM ポリシーをアクティブ化する前に、既存のレプリケートオブジェクトとイレイジャーコーディングオブジェクトの配置に対する変更を確認してください。既存のオブジェクトの場所を変更すると、新しい配置が評価されて実装される際に一時的なリソースの問題が発生する可能性があります。

7. 新しいポリシーをアクティブ化します。

接続さ StorageGRID れたサイトの運用停止手順を実行すると、新しい ILM ポリシーをアクティブ化した時点で、選択したサイトからオブジェクトデータの削除が開始されます。すべてのオブジェクトコピーの

移動または削除には数週間かかることがあります。サイトにオブジェクトデータが残っている間もサイトの運用停止を安全に開始できますが、実際の運用停止手順 を開始する前にデータをサイトから移動することが許可されている場合は、運用停止手順 の処理がより迅速になり、システム停止やパフォーマンスへの影響も少なくなります （ウィザードの手順 5 で「 * 分解を開始」を選択）。

8. 手順 3 （ ILM ポリシーの改訂） * に戻って、新しいアクティブポリシーに ILM ルールがサイトを参照していないこと、および * Next * ボタンが有効になっていることを確認します。




ルールが表示された場合は、続行する前に新しい ILM ポリシーを作成してアクティブ化する必要があります。

9. ルールがリストされていない場合は、「 * 次へ * 」を選択します。

   手順 4 （ Remove ILM References ）が表示されます。

手順 **4** ： **ILM** 参照を削除する

## 運用停止サイトウィザードの手順 4 （ ILM 参照を削除）から、ドラフトポリシーが存在する場合は削除し、サイトを参照している未使用の ILM ルールを削除または編集できます。

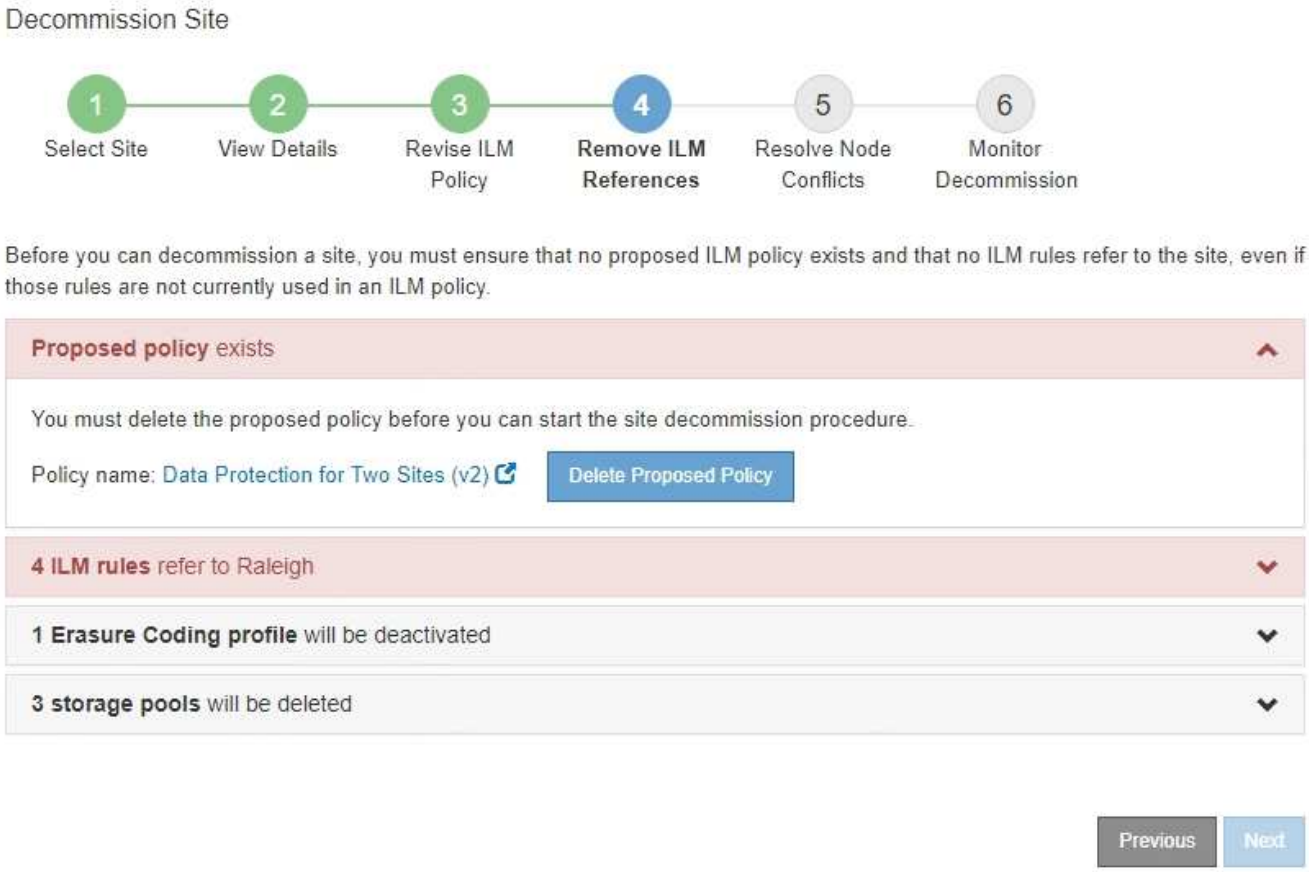
このタスクについて

次の場合は、サイト運用停止の手順 を開始することができません。

- ドラフトの ILM ポリシーが存在します。ドラフトポリシーがある場合は削除する必要があります。
- ILM ルールはサイトを参照します。これは、そのルールがどの ILM ポリシーでも使用されていない場合も同様です。サイトを参照するすべてのルールを削除または編集する必要があります。

手順

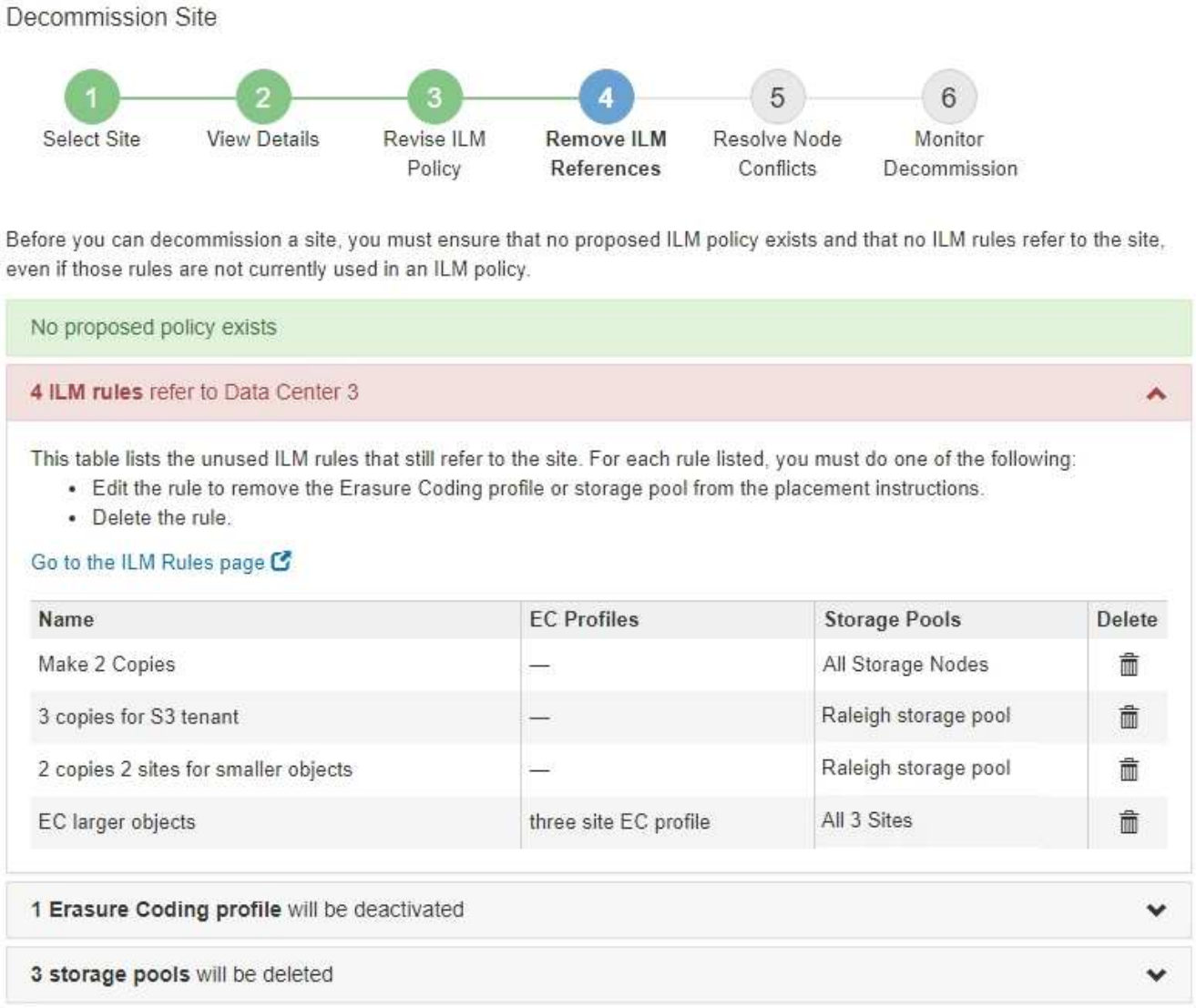
1. ドラフトポリシーが表示されている場合は削除します。




a. [ ドラフトポリシーの削除 ] を選択します。

b. 確認ダイアログボックスで「 * OK * 」を選択します。

2. 未使用の ILM ルールがサイトを参照しているかどうかを確認します。




表示される ILM ルールはサイトを参照しているものの、どのポリシーでも使用されていません。この例では、次のように

- 組み込みの * Make 2 Copies * ルールは、 All Sites サイトを使用するシステムデフォルトの * All Storage Nodes * ストレージプールを使用します。
- S3 テナント * ルールの未使用のコピーが 3 つある場合は、「ローリー * ストレージプール」と呼ばれます。
- 小容量のオブジェクト * ルール用の未使用の * 2 コピー 2 サイトは、 * ローリー * ストレージプールを表します。
- 未使用の * EC 大容量オブジェクト * ルールでは、「 3 つすべてのサイト」 * イレイジャーコーディングプロファイルのローリーサイトが使用されます。
- ILM ルールが表示されない場合は、 * Next * を選択して * Step 5 （ Resolve Node Conflicts ） * に進みます。

"手順 5 ：ノードの競合を解決する（運用停止を開始する）"

サイトを StorageGRID が運用停止すると、そのサイトを参照している未使用のイレイジャーコーディングプロファイルは自動的に非アクティブ化され、サイトを参照している未使用のストレージプールが自動的に削除されます。「すべてのサイト」サイトを使用するため、システムデフォルトの「すべてのストレージノード」ストレージプールは削除されます。

- 1 つ以上の ILM ルールが表示される場合は、次の手順に進みます。

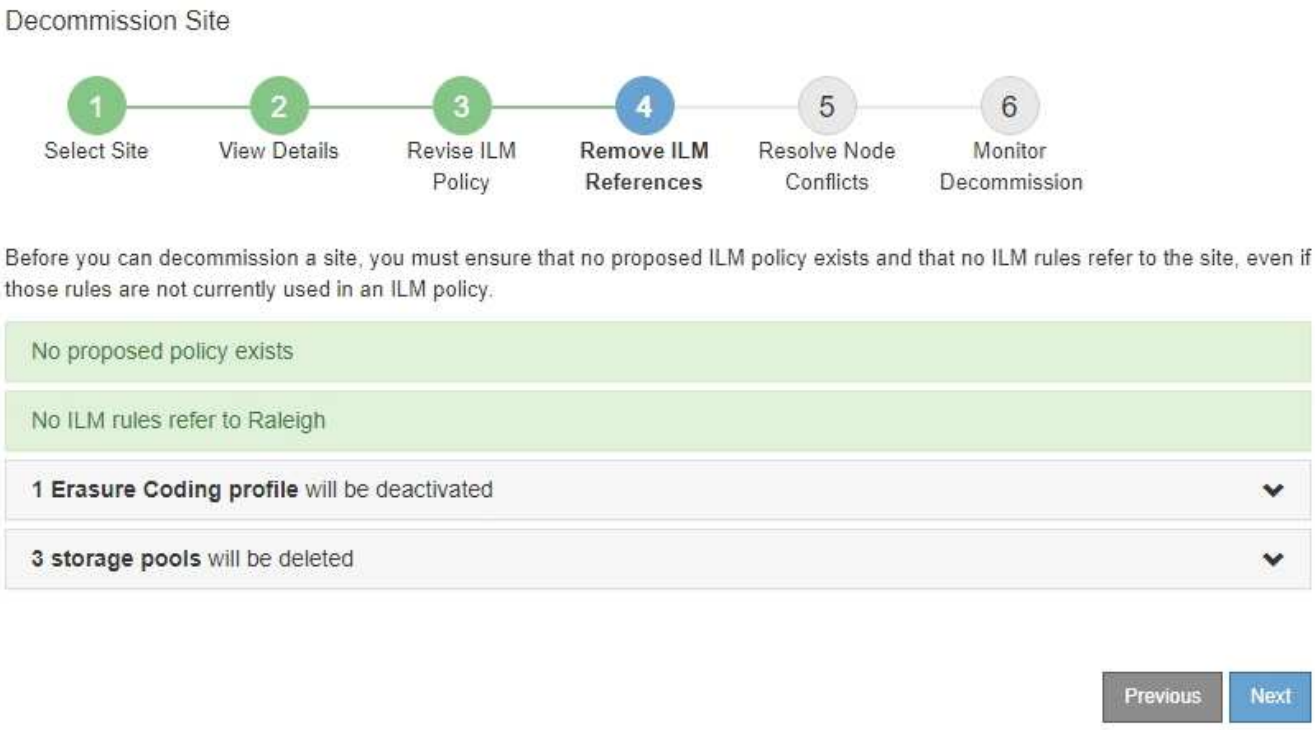
3. 使用されていない各ルールを編集または削除します。
   - ルールを編集するには、 ILM ルールページに移動し、サイトを参照するイレイジャーコーディングプロファイルまたはストレージプールを使用するすべての配置を更新します。次に、 * 手順 4 （ ILM 参照の削除） * に戻ります。

     詳細については、情報ライフサイクル管理を使用してオブジェクトを管理する手順を参照してください。

   - ルールを削除するには、ごみ箱のアイコンを選択します 「 * OK 」を選択します。

     サイトを運用停止するには、素材 * Make 2 Copies * ルールを削除する必要があります。

4. ドラフトの ILM ポリシーが存在しないこと、および未使用の ILM ルールがサイトを参照していないこと、および * Next * ボタンが有効になっていることを確認します。




5. 「 * 次へ * 」を選択します。

サイトを参照している残りのストレージプールおよびイレイジャーコーディングプロファイルは、サイトが削除されると無効になります。サイトを StorageGRID が運用停止すると、そのサイトを参照している未使用のイレイジャーコーディングプロファイルは自動的に非アクティブ化され、サイトを参照している未使用のストレージプールが自動的に削除されます。「すべてのサイト」サイトを使用するため、システムデフォルトの「すべてのストレージノード」ストレージプールは削除されます。

ステップ 5 （ノードの競合を解決）が表示されます。

手順 **5** ：ノードの競合を解決する（運用停止を開始する）

## Decommission Site ウィザードの Step 5 （ Resolve Node Conflicts ）から、StorageGRID システム内のノードが切断されているか、選択したサイトのノードが High Availability （ HA ）グループに属しているかを確認できます。いずれかのノードの競合が解決されたら、このページから運用停止手順 を開始します。

StorageGRID システムのすべてのノードが次のように正しい状態であることを確認する必要があります。

- StorageGRID システムのすべてのノードが接続されている必要があります（✔）。

切断されたサイトの運用停止を実行する場合は、削除するサイトのすべてのノードを切断し、他のすべてのサイトのすべてのノードを接続する必要があります。

- 削除するサイトにハイアベイラビリティ（ HA ）グループに属するインターフェイスを持つことはできません。

手順 5 （ノードの競合を解決）用に表示されたノードがある場合は、運用停止を開始する前に問題 を修正する必要があります。

このページからサイトの手順 の運用停止を開始する前に、次の考慮事項を確認してください。

- 手順 の運用停止が完了するまでに、十分な時間を確保する必要があります。

サイトからオブジェクトデータを移動または削除するには、サイトのデータ量、システムの負荷、ネットワークのレイテンシ、および ILM に求められる変更の性質に応じて、数日、数週間、場合によっては数カ月かかることがあります。

- サイトの運用停止中は、手順 は次の処理を実行します。
  - 運用停止するサイトを参照する ILM ルールは作成できません。サイトを参照する既存の ILM ルールを編集することもできません。
  - 拡張やアップグレードなどの他のメンテナンス手順は実行できません。

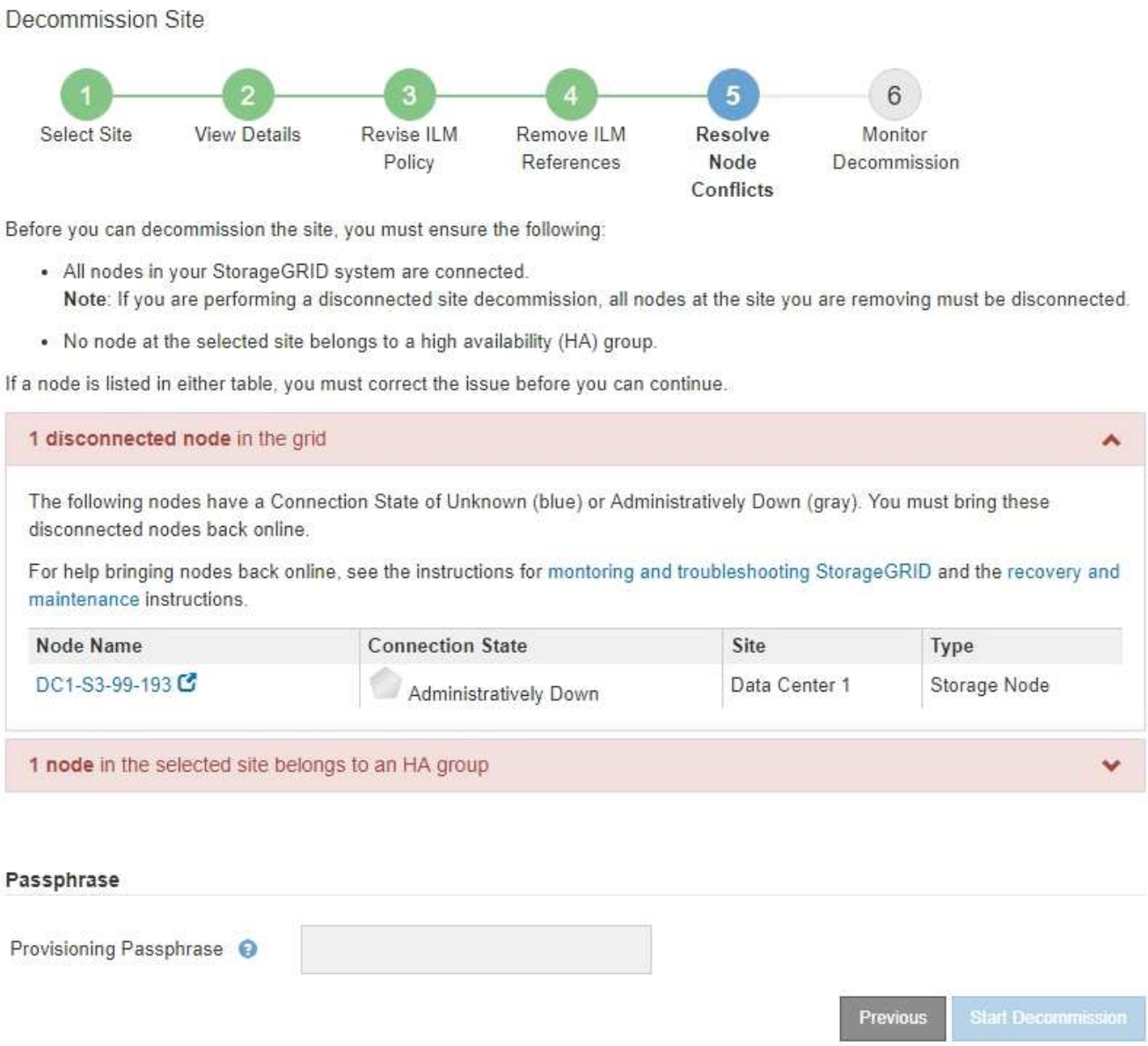
接続されているサイトの運用停止中に別のメンテナンス手順 を実行する必要がある場合は、ストレージノードを削除している間に手順 を一時停止できます。[Pause （一時停止） ] ボタンは、「デコミッション・レプリケート・データとイレイジャーコーディング・データ」ステージの間に有効になります。

  - サイトの運用停止手順 の開始後にノードをリカバリする必要がある場合は、サポートにお問い合わせ

ください。

手順

1. 手順 5 （ノードの競合を解決）の「切断されているノード」セクションで、 StorageGRID システム内のいずれかのノードの接続状態が「 Unknown 」（不明）であるかどうかを確認します）または管理上のダウン（）。

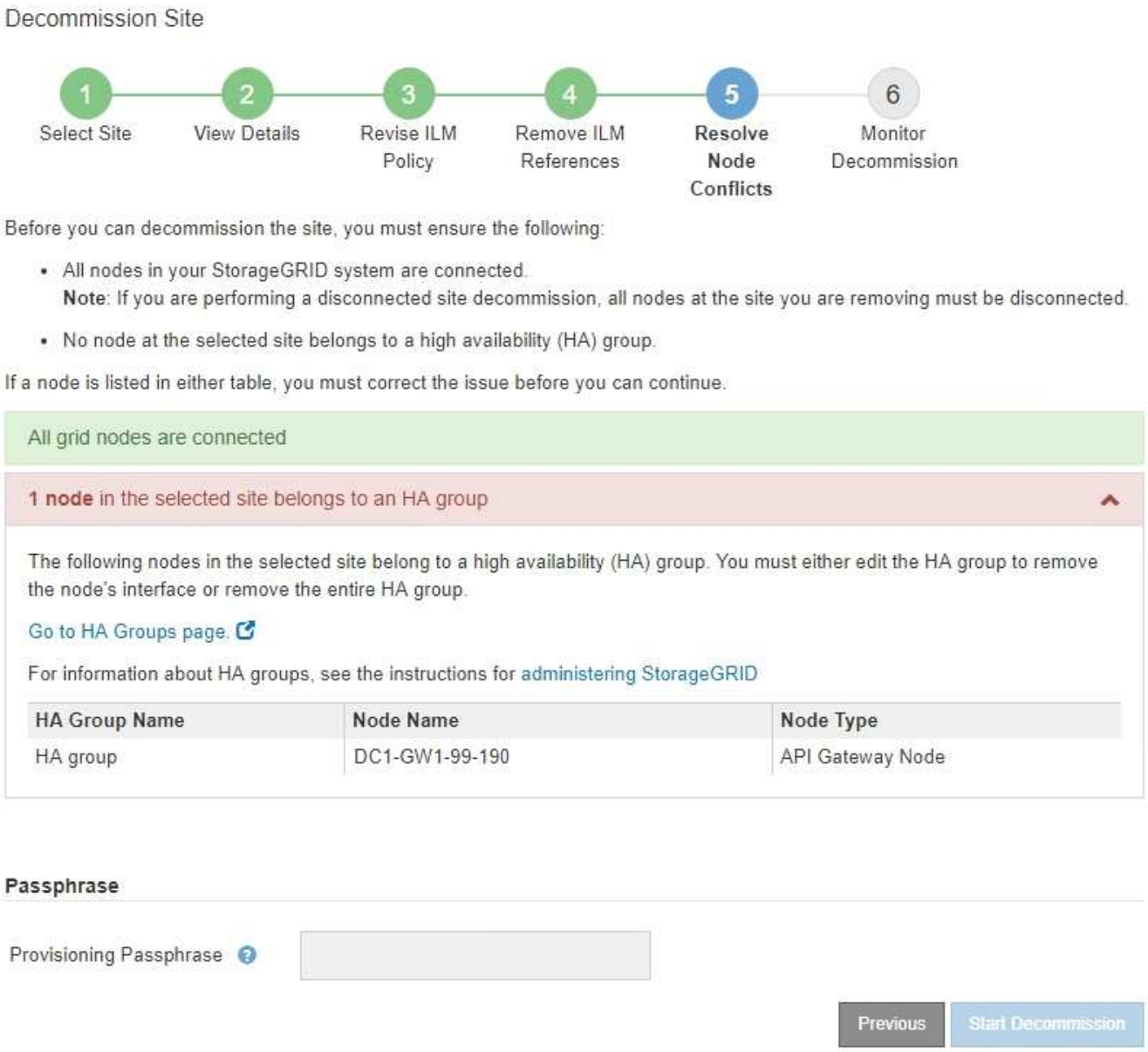



2. 切断されているノードがある場合は、オンラインに戻します。

   StorageGRID の監視とトラブルシューティングの手順およびグリッドノードの手順を参照してください。サポートが必要な場合は、テクニカルサポートにお問い合わせください。

3. 切断されているすべてのノードがオンラインに戻ったら、手順 5 （ノードの競合を解決）の HA グループに関するセクションを確認します。

   このテーブルには、選択したサイトにあるハイアベイラビリティ（ HA ）グループに属するノードがすべて表示されます。



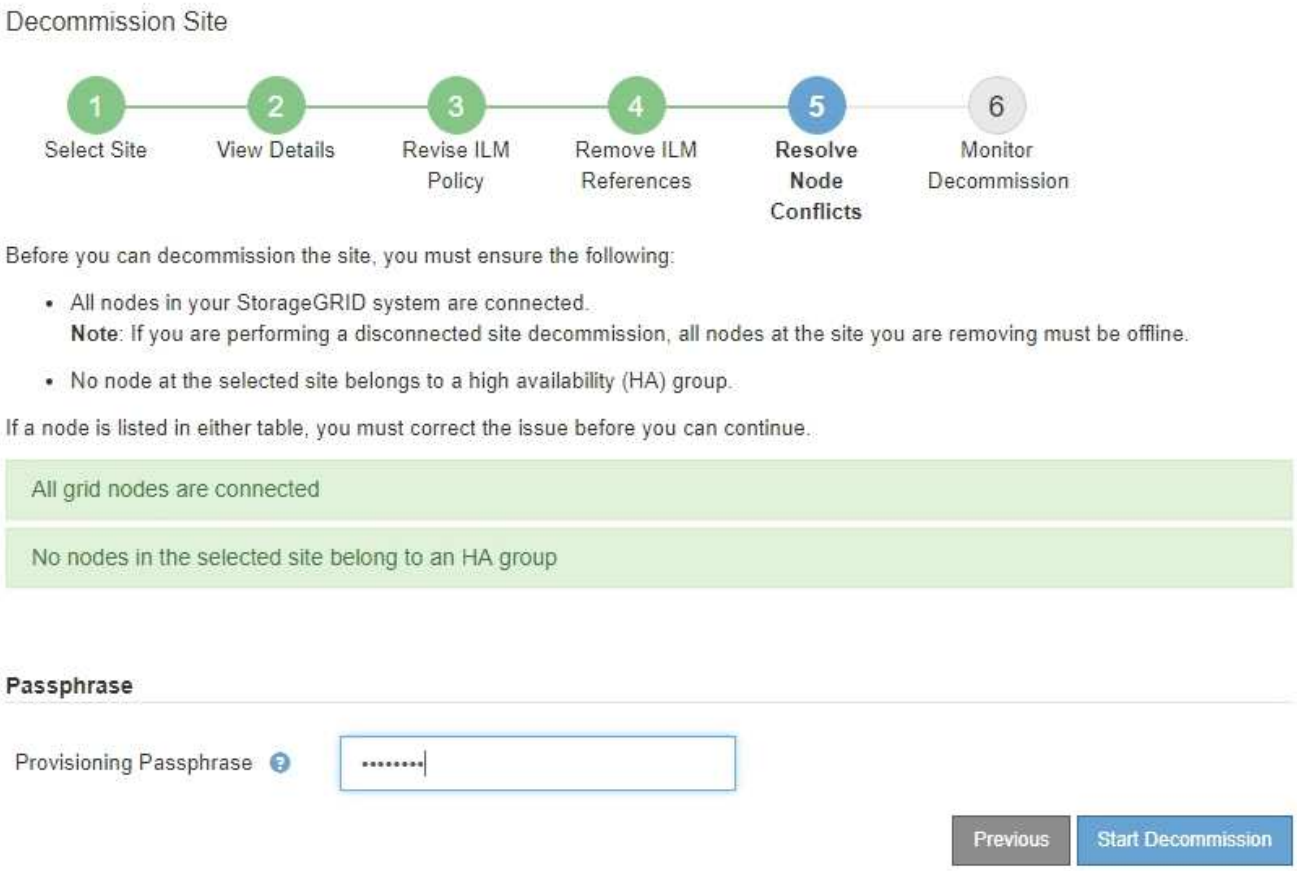

4. 表示されたノードがある場合は、次のいずれかを実行します。

   - 該当する各 HA グループを編集してノードインターフェイスを削除します。
   - このサイトからノードのみを含む HA グループを削除します。StorageGRID の管理手順を参照してください。

   すべてのノードが接続されていて、選択したサイト内のノードが HA グループで使用されていない場合は、「 * Provisioning Passphrase * 」フィールドが有効になります。

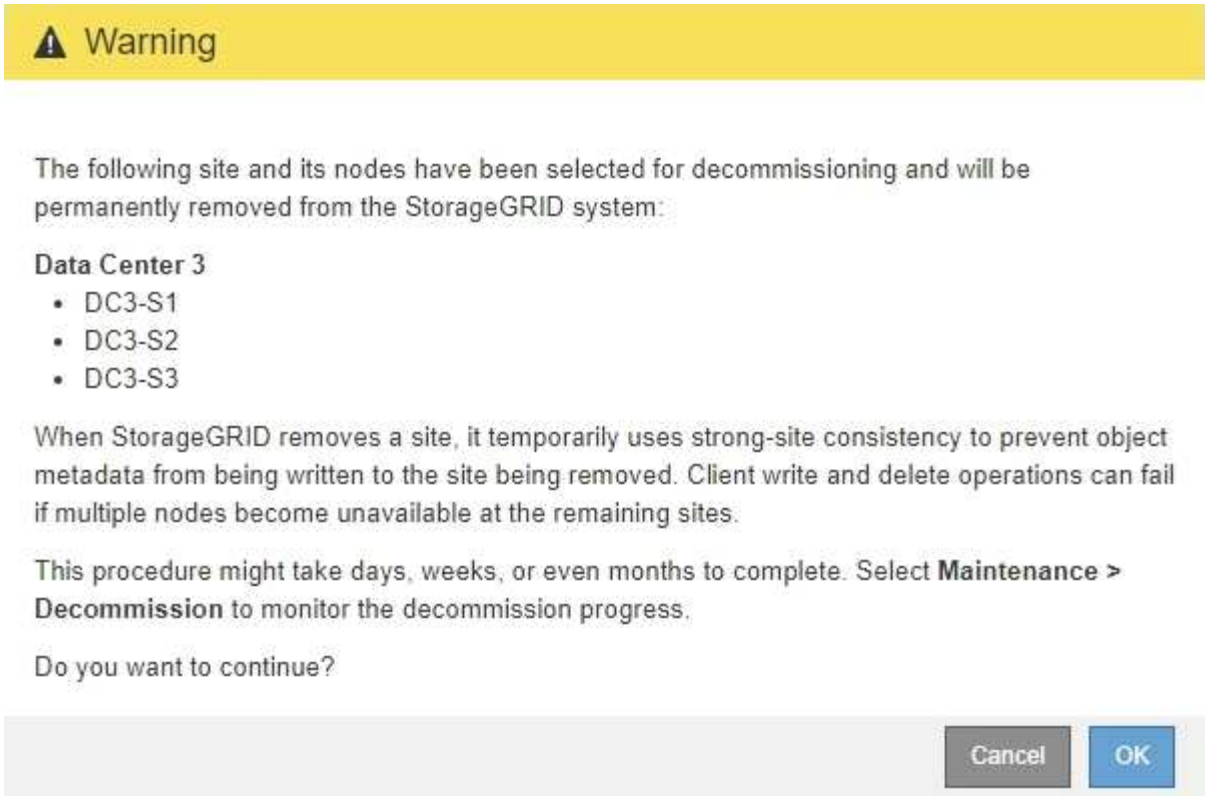
5. プロビジョニングパスフレーズを入力します。

   [ * 分解を開始 * （ Start Decommission * ） ] ボタンが有効になります。



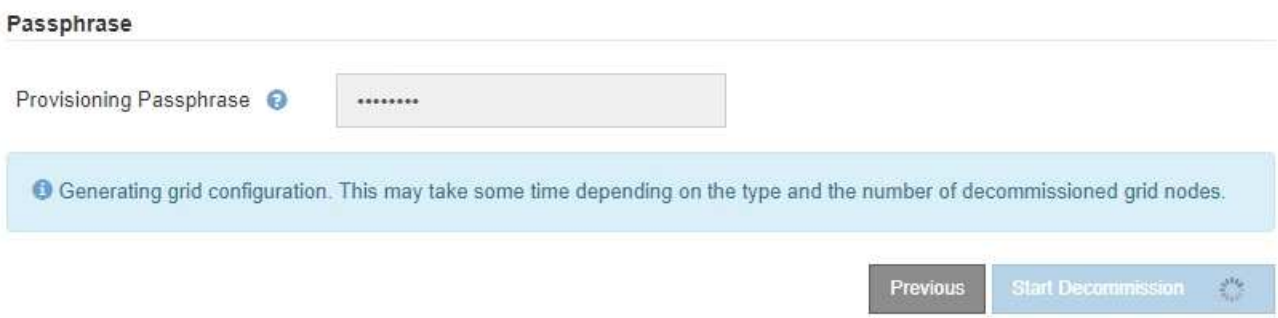

6. サイトの運用停止手順 を開始する準備ができたら、 * 運用停止を開始 * を選択します。

   削除するサイトとノードが警告として表示されます。サイトを完全に削除するには、数日、数週間、場合によっては数か月かかることがあります。




7. 警告を確認します。開始する準備ができたら、「 * OK * 」を選択します。

   新しいグリッド設定が生成されるときにメッセージが表示されます。運用停止するグリッドノードのタイプと数によっては、このプロセスには時間がかかることがあります。




   新しいグリッド設定が生成されると、ステップ 6 （ Monitor Decommission ）が表示されます。

   [ 前へ * ] ボタンは、運用停止が完了するまで無効のままです。

関連情報

"トラブルシューティングを監視します"

"グリッドノードの手順"

"StorageGRID の管理"

# Decommission Site ページウィザードの Step 6 （ Monitor Decommission ）では、サイトが削除されるまで進行状況を監視できます。

このタスクについて

StorageGRID は、接続されているサイトを削除するときに、次の順序でノードを削除します。

1. ゲートウェイノード
2. 管理ノード
3. ストレージノード

StorageGRID は切断されているサイトを削除するときに、次の順序でノードを削除します。

1. ゲートウェイノード
2. ストレージノード
3. 管理ノード

各ゲートウェイノードまたは管理ノードの削除には数分から 1 時間程度しかかかる場合がありますが、ストレージノードには数日から数週間かかる場合があります。

手順

1. 新しいリカバリパッケージが生成されたら、すぐにファイルをダウンロードします。

手順 の運用停止中に問題が発生した場合にグリッドをリカバリできるよう、できるだけ早くリカバリパッケージをダウンロードしてください。

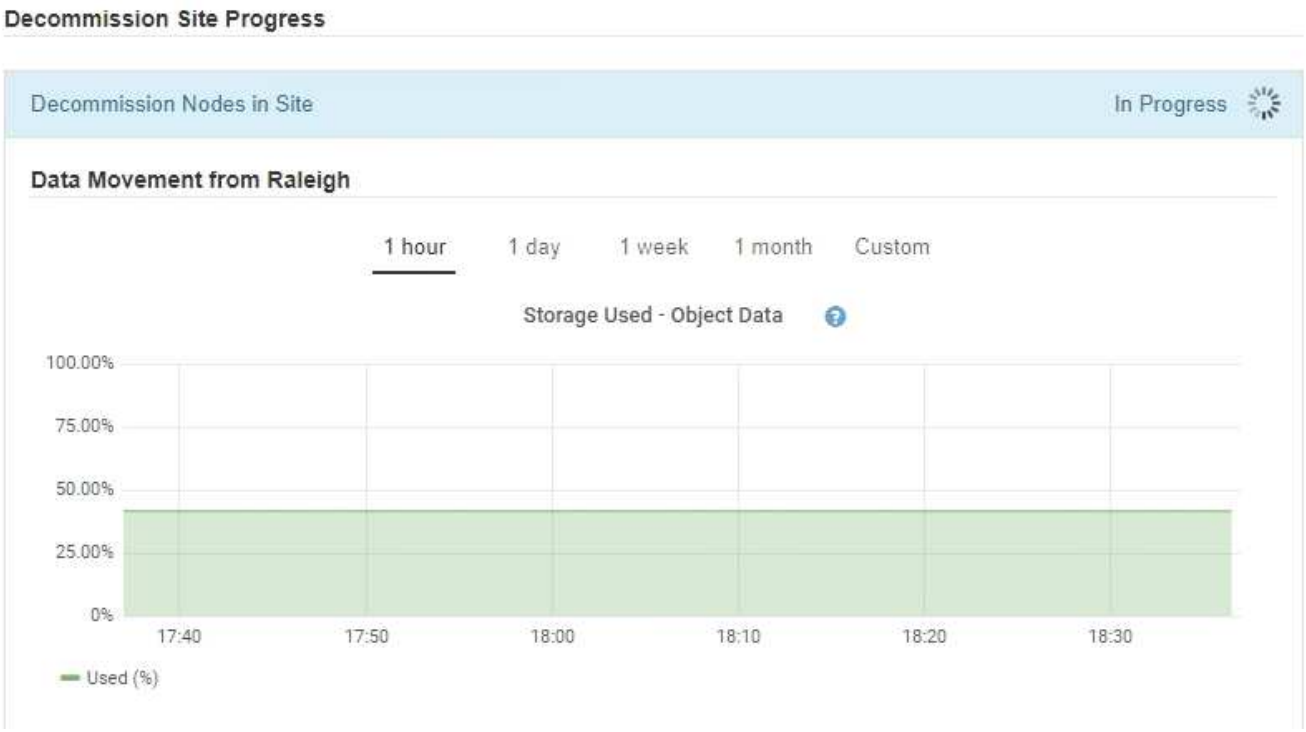
a. メッセージ内のリンクを選択するか、* Maintenance ** System * Recovery Package *を選択します。
b. をダウンロードします `.zip` ファイル。

   リカバリパッケージのダウンロード手順を参照してください。

リカバリパッケージファイルには StorageGRID システムからデータを取得するための暗号キーとパスワードが含まれているため、安全に保管する必要があります。

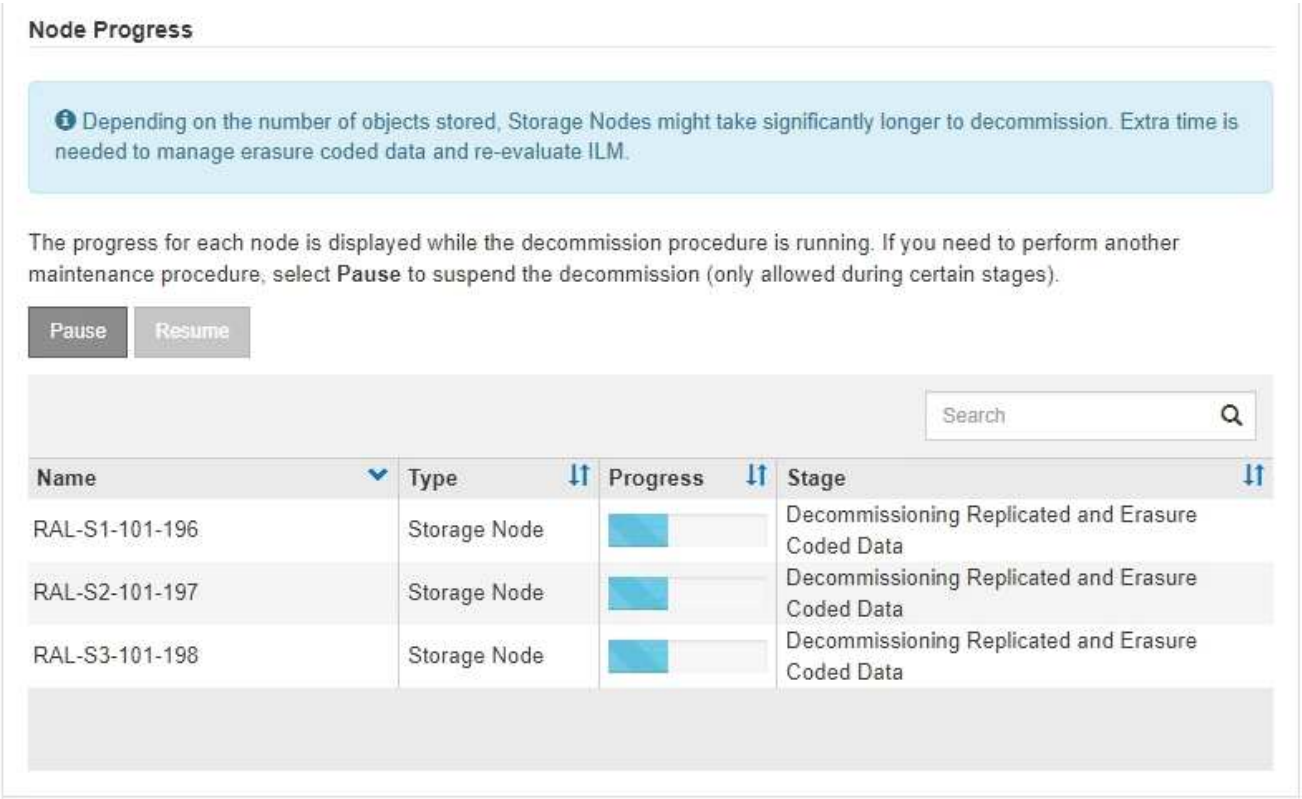
2. データ移動グラフを使用して、このサイトから他のサイトへのオブジェクトデータの移動を監視します。

データの移動は、手順 3 （ ILM ポリシーの改訂）で新しい ILM ポリシーをアクティブ化すると開始されます。データの移動は、手順 の運用停止処理の間に行われます。




3. ページの Node Progress セクションで、ノードが削除される場合の運用停止手順 の進行状況を監視します。

   ストレージノードを削除すると、各ノードで一連のステージが実行されます。これらのステージのほとんどは迅速または不透過的に行われますが、移動が必要なデータの量に応じて、他のステージが完了するまでに数日から数週間かかることがあります。イレイジャーコーディングデータを管理して ILM を再評価するために追加の時間が必要です。



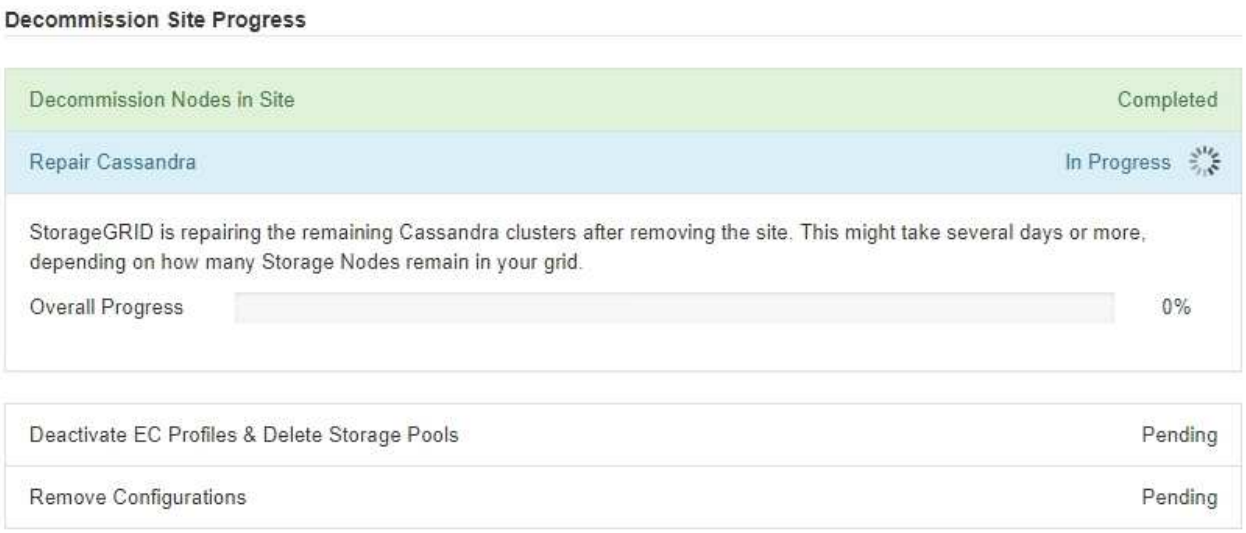

接続されているサイトの運用停止の進行状況を監視している場合は、次の表を参照して、ストレージノードの運用停止ステージを確認してください。

| 段階 | 推定時間 |
| --- | --- |
| 保留中です | 分以下 |
| ロックされるまで待ちます | 分 |
| タスクの準備 | 分以下 |
| LDR を運用停止にする | 分 |
| レプリケートデータとイレイジャーコーディングデータの運用停止 | データ量に基づく数時間、数日、または数週間<br>• 注：その他のメンテナンス作業が必要な場合は、この段階でサイトの運用停止を一時停止できます。 |
| LDR が状態を設定 | 分 |
| 監査キューをフラッシュします | メッセージ数とネットワーク遅延に基づいて、数分から数時間に短縮されます。 |
| • 完了しました | 分 |

切断されているサイトの運用停止の進行状況を監視する場合は、次の表を参照して、ストレージノードの運用停止ステージを確認してください。

| 段階 | 推定時間 |
| --- | --- |
| 保留中です | 分以下 |
| ロックされるまで待ちます | 分 |
| タスクの準備 | 分以下 |
| 外部サービスを無効にします | 分 |
| 証明書の取り消し | 分 |
| ノードの登録解除 | 分 |
| ストレージグレードの登録解除 | 分 |
| ストレージグループの削除 | 分 |
| エンティティの削除 | 分 |
| • 完了しました | 分 |

4. すべてのノードが完了ステージになったら、残りのサイトの運用停止処理が完了するまで待ちます。
   - StorageGRID は、 * Repair Cassandra * ステップ中に、グリッドに残っている Cassandra クラスタに対して必要な修復を実行します。グリッドに残っているストレージノードの数によっては、この修復に数日以上かかることがあります。




   - [ECプロファイルの非アクティブ化ストレージプールの削除*（Deactivate EC Profiles Delete Storage

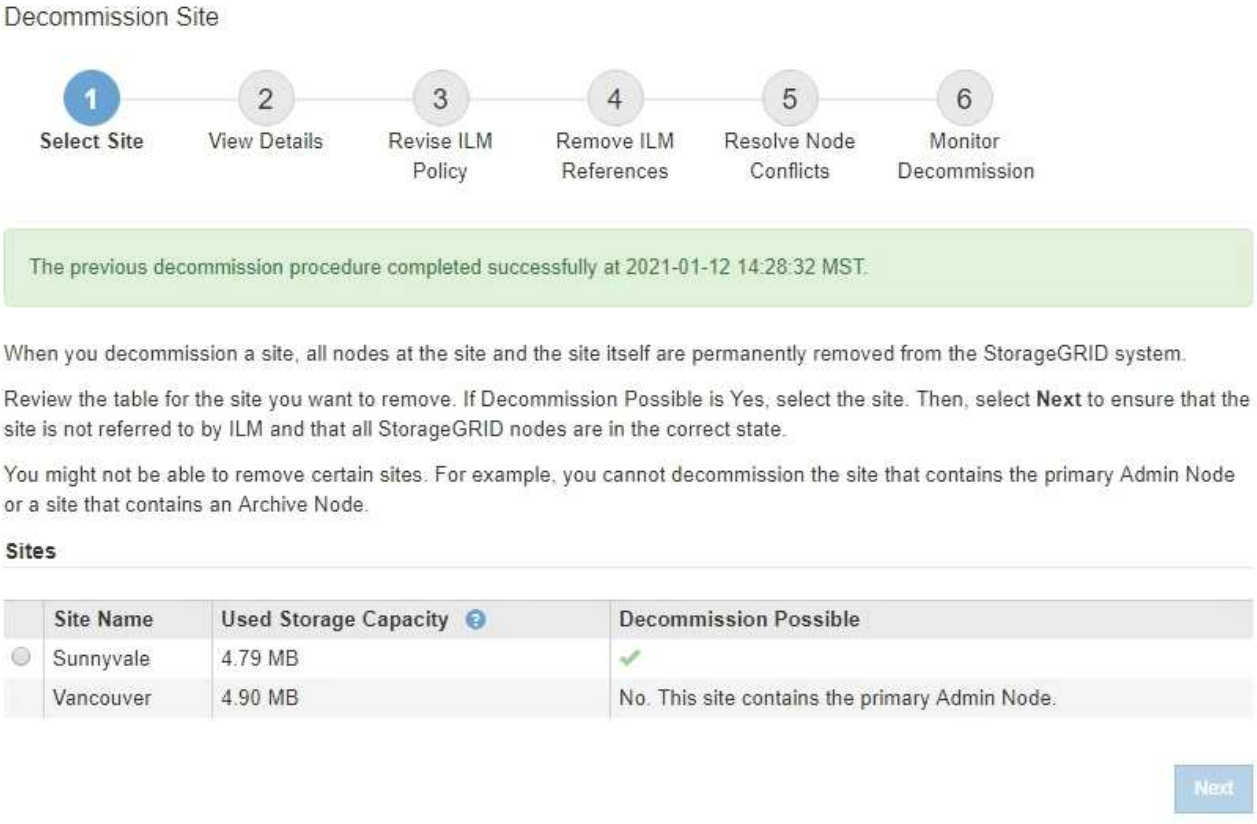
Pools *）]ステップでは、次のILMの変更が行われます。

- サイトを参照しているイレイジャーコーディングプロファイルはすべて非アクティブ化されます。
- サイトを参照していたストレージプールがすべて削除されます。

> ⓘ システムデフォルトの All Storage Nodes ストレージプールも、「すべてのサイト」サイトを使用しているため削除されます。

◦ 最後に、 * 構成の削除 * ステップで、サイトとそのノードへの残りの参照がグリッドの残りの部分から削除されます。

5. 運用停止手順 が完了すると、運用停止サイトのページに成功のメッセージが表示され、削除したサイトは表示されなくなります。



完了後

サイトの運用停止手順 が完了したら、次の作業を実行します。

- 運用停止したサイトのすべてのストレージノードのドライブを確実に消去します。市販のデータ消去ツールまたはデータ消去サービスを使用して、ドライブからデータを完全かつ安全に削除します。
- サイトに 1 つ以上の管理ノードが含まれていて、 StorageGRID システムでシングルサインオン（ SSO ）が有効になっている場合は、そのサイトに対する証明書利用者信頼をすべて Active Directory フェデレーションサービス（ AD FS ）から削除します。
- 接続されているサイトの運用停止手順 でノードの電源が自動的にオフになったら、関連する仮想マシンを削除します。

関連情報

"リカバリパッケージをダウンロードしています"

# ネットワークのメンテナンス手順

## グリッドネットワーク上のサブネットのリストを設定したり、StorageGRID システムのIPアドレス、DNSサーバ、またはNTPサーバを更新したりできます。

選択肢

- "グリッドネットワークのサブネットを更新しています"
- "IPアドレスを設定しています"
- "DNSサーバを設定しています"
- "NTPサーバを設定しています"
- "分離されているノードのネットワーク接続のリストア"

グリッドネットワークのサブネットを更新しています

## StorageGRID は、グリッドネットワーク（ eth0 ）上のグリッドノード間の通信に使用されるネットワークサブネットのリストを管理します。このエントリには、StorageGRID システムの各サイトでグリッドネットワークに使用されているサブネット、およびグリッドネットワークゲートウェイ経由でアクセスされる NTP 、 DNS 、 LDAP 、またはその他の外部サーバに使用されるサブネットが含まれます。グリッドノードまたは新しいサイトを追加した場合は、サブネットの更新、またはグリッドネットワークへのサブネットの追加が必要になることがあります。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Maintenance または Root Access 権限が必要です。
- プロビジョニングパスフレーズが必要です。
- 設定するサブネットのネットワークアドレスを CIDR 表記で指定する必要があります。

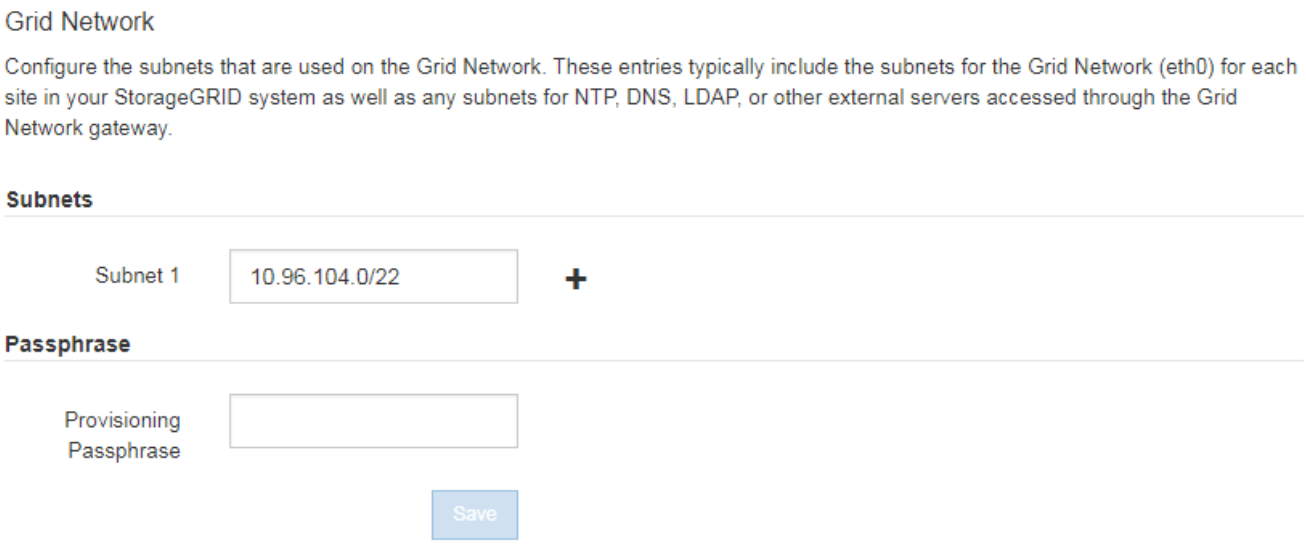
このタスクについて

新しいサブネットの追加を含む拡張アクティビティを実行する場合は、拡張手順 を開始する前に新しいグリ

ッドサブネットを追加する必要があります。

手順

1. [* Maintenance （メンテナンス）**]>[** Network （*ネットワーク）]>[* Grid Network（*グリッドネットワーク）




2. サブネットのリストで、プラス記号をクリックして、 CIDR 表記の新しいサブネットを追加します。

   たとえば、と入力します `10.96.104.0/22`。

3. プロビジョニングパスフレーズを入力し、 * Save * をクリックします。

   指定したサブネットが、 StorageGRID システムに対して自動的に設定されます。

**IP**アドレスを設定しています

## IP 変更ツールを使用してグリッドノードの IP アドレスを設定することで、ネットワーク設定を実行できます。

グリッドの導入時に設定されたネットワーク設定を変更するには、ほとんどの場合、 IP 変更ツールを使用する必要があります。標準の Linux ネットワークコマンドおよびファイルを使用して手動で変更すると、すべての StorageGRID サービスに変更が反映されなかったり、アップグレード、リブート、ノードリカバリ手順の実行後に変更が失われたりすることがあります。

グリッド内のすべてのノードのグリッドネットワークIPアドレスを変更する場合は、グリッド全体で特別な手順 を使用します。

"グリッド内のすべてのノードのIPアドレスの変更"

グリッドネットワークサブネットリストのみを変更する場合は、グリッドマネージャを使用してネットワーク設定の追加または変更を行います。グリッドネットワーク設定問題 が原因でグリッドマネージャにアクセスできない場合、またはグリッドネットワークルーティングの変更とその他のネットワーク変更を同時に実行する場合は、 IP 変更ツールを使用します。

IP 変更手順 は、停止を伴う手順 の可能性があります。グリッドの一部は、新しい設定が適用されるまで使用できない場合があります。

- イーサネット・インターフェイス *

eth0 に割り当てられる IP アドレスは、常にグリッドノードのグリッドネットワーク IP アドレスになります。eth1 に割り当てられている IP アドレスは、常にグリッドノードの管理ネットワーク IP アドレスです。eth2 に割り当てられている IP アドレスは、常にグリッドノードのクライアントネットワーク IP アドレスです。

StorageGRID アプライアンスなどの一部のプラットフォームでは、 eth0 、 eth1 、 eth2 が、下位のブリッジで構成されるアグリゲートインターフェイスや物理 / VLAN インターフェイスのボンドである場合があります。これらのプラットフォームでは、* SSM * Resources *タブに、eth0、eth1、eth2に加えて、他のインターフェイスに割り当てられているグリッドネットワーク、管理ネットワーク、およびクライアントネットワークのIPアドレスが表示されることがあります。

- DHCP *

DHCP は導入フェーズでのみ設定できます。設定時に DHCP を設定することはできません。グリッドノードの IP アドレス、サブネットマスク、およびデフォルトゲートウェイを変更する場合は、 IP アドレス変更手順を使用する必要があります。IP 変更ツールを使用すると、原因 の DHCP アドレスが静的アドレスになります。

- ハイアベイラビリティ（ HA ）グループ *
- クライアントネットワークIPアドレスは、クライアントネットワークインターフェイスで設定されたHAグループのサブネット以外に変更することはできません。
- クライアントネットワークIPアドレスを、クライアントネットワークインターフェイスで設定されたHAグループによって割り当てられた既存の仮想IPアドレスの値に変更することはできません。
- グリッドネットワークのIPアドレスは、グリッドネットワークインターフェイスで設定されているHAグループのサブネット以外に変更することはできません。
- グリッドネットワークのIPアドレスを、グリッドネットワークのインターフェイスで設定されたHAグループによって割り当てられた既存の仮想IPアドレスの値に変更することはできません。

選択肢

- "ノードのネットワーク設定を変更する"
- "管理ネットワークのサブネットリストに対する追加または変更"
- "グリッドネットワークのサブネットリストに対する追加または変更"
- "Linux：既存のノードへのインターフェイスの追加"
- "グリッド内のすべてのノードのIPアドレスの変更"

ノードのネットワーク構成を変更する

## IP 変更ツールを使用して、 1 つ以上のノードのネットワーク設定を変更できます。グリッドネットワークの設定を変更したり、管理ネットワークまたはクライアントネットワークを追加、変更、削除したりできます。

必要なもの

を用意しておく必要があります `Passwords.txt` ファイル。

このタスクについて

- Linux ： * グリッドノードを管理ネットワークまたはクライアントネットワークに初めて追加する際に、ノード構成ファイルの ADMIN_NETWORK_TARGET または CLIENT_network_target を事前に設定していない場合は、ここで設定する必要があります。

使用している Linux オペレーティングシステムでの StorageGRID のインストール手順を参照してください。

- アプライアンス： StorageGRID アプライアンスでは、初回インストール時にクライアントまたは管理ネットワークが StorageGRID アプライアンスインストーラで設定されなかった場合、 IP 変更ツールだけでネットワークを追加することはできません。先にアプライアンスをメンテナンスモードにして、リンクを設定し、アプライアンスを通常の動作モードに戻してから、IP変更ツールを使用してネットワーク設定を変更する必要があります。ネットワークリンクの設定については、使用しているアプライアンスのインストールおよびメンテナンスの手順にある手順 を参照してください。

任意のネットワーク上の 1 つ以上のノードの IP アドレス、サブネットマスク、ゲートウェイ、または MTU 値を変更できます。

クライアントネットワークまたは管理ネットワークからノードを追加または削除することもできます。

- クライアントネットワークまたは管理ネットワークにノードを追加するには、そのネットワーク上の IP アドレス / サブネットマスクをノードに追加します。
- クライアントネットワークまたは管理ネットワークからノードを削除するには、そのネットワーク上のノードの IP アドレス / サブネットマスクを削除します。

  グリッドネットワークからノードを削除することはできません。

IP アドレスの交換はできません。グリッドノード間で IP アドレスを交換する必要がある場合は、一時的な中間 IP アドレスを使用する必要があります。

StorageGRID システムでシングルサインオン（ SSO ）が有効になっている場合、管理ノードの IP アドレスを変更すると、（推奨される完全修飾ドメイン名ではなく）管理ノードの IP アドレスを使用して設定された証明書利用者信頼はすべて無効になります。ノードにサインインできなくなります。IP アドレスを変更したら、すぐに Active Directory フェデレーションサービス（ AD FS ）でそのノードの証明書利用者信頼を新しい IP アドレスで更新または再設定する必要があります。StorageGRID の管理手順を参照してください。

IP 変更ツールを使用してネットワークに加えた変更は、 StorageGRID アプライアンスのインストーラファームウェアに反映されます。そのため、アプライアンスに StorageGRID ソフトウェアを再インストールした場合や、アプライアンスをメンテナンスモードにした場合も、正しいネットワーク設定が適用されます。

手順

1. プライマリ管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`

d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

2. 次のコマンドを入力してIP変更ツールを起動します。 `change-ip`
3. プロンプトでプロビジョニングパスフレーズを入力します。

メインメニューが表示されます。

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

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

Selection:
```

4. オプションで * 1 * を選択して、更新するノードを選択します。次に、次のいずれかのオプションを選択します。
   - *1 * ：シングルノード — 名前で選択
   - * 2 * ：単一ノード — サイトで選択してから名前で選択します
   - *3: シングルノード — 現在の IP で選択
   - * 4 * ：サイト内のすべてのノード
   - * 5 * ：グリッド内のすべてのノード
     - 注： * すべてのノードを更新する場合は、「 all 」が選択されたままにしておきます。

   選択を行うと、メインメニューが表示され、 [ 選択したノード * （ Selected nodes * ） ] フィールドが更新されて選択内容が反映されます。以降のすべての操作は、表示されているノードでのみ実行されます。

5. メインメニューでオプション * 2 * を選択し、選択したノードの IP / マスク、ゲートウェイ、および MTU 情報を編集します。
   a. 変更するネットワークを選択します。
      - * 1 * ：グリッドネットワーク
      - * 2 * ：管理ネットワーク
      - *3 *: クライアントネットワーク
      - * 4 * ：すべてのネットワークを選択すると、ノード名、ネットワーク名（ Grid 、 Admin 、または Client ）、データタイプ（ IP / マスク、 ゲートウェイ（ MTU ）、および現在の値。

        DHCP によって設定されたインターフェイスの IP アドレス、プレフィックス長、ゲートウェイ、または MTU を編集すると、インターフェイスが static に変更されます。DHCP によって設定され

たインターフェイスを変更するように選択すると、インターフェイスが static に変更されることを通知する警告が表示されます。

として設定されたインターフェイス `fixed` 編集できません。

b. 新しい値を設定するには、現在の値の形式で入力します。

c. 現在の値を変更しない場合は、 **Enter** キーを押します。

d. データタイプがの場合 `IP/mask`を使用してノードから管理ネットワークまたはクライアントネットワークを削除するには、「* d 」または「 0.0.0.0/0 *」と入力します。

e. 変更するすべてのノードを編集したら、「 * q * 」と入力してメインメニューに戻ります。

変更内容は、クリアまたは適用されるまで保持されます。

6. 次のいずれかのオプションを選択して、変更内容を確認します。

◦ **5**: 変更された項目のみを表示するために分離された出力の編集を表示します。変更は、次の出力例に示すように、緑（追加）または赤（削除）で強調表示されます。

```
================================================================================
Site: RTP
================================================================================
username-x Grid    IP      [    172.16.0.239/21 ]: 172.16.0.240/21
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Admin   IP      [    10.224.0.244/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.245/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.240/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.241/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.242/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.243/21 ]: 0.0.0.0/0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   MTU     [               1400 ]: 0
username-x Admin   MTU     [               1400 ]: 0
username-x Admin   MTU     [               1400 ]: 0
username-x Admin   MTU     [               1400 ]: 0
username-x Admin   MTU     [               1400 ]: 0
username-x Admin   MTU     [               1400 ]: 0
Press Enter to continue
```

◦ **6**: 編集内容を出力に表示し、設定全体を表示します。変更は、緑（追加）または赤（削除）で強調表示されます。

> 一部のコマンドラインインターフェイスでは、追加と削除が取り消し線で示される場合があります。正しく表示されるためには、使用するターミナルクライアントが必要な VT100 エスケープシーケンスをサポートしている必要があります。

7. オプション * 7 * を選択して、すべての変更を検証します。

この検証により、重なり合うサブネットを使用していないなど、グリッドネットワーク、管理ネットワーク、クライアントネットワークのルールに違反がないことを確認します。

この例では、検証でエラーが返されています。

```
Validating new networking configuration... FAILED.

  DK-10-224-5-20-G1: The admin subnet 172.18.0.0/16 overlaps the 172.18.0.0/21 grid network.
  DK-10-224-5-22-S1: Duplicate Grid IP 172.16.5.18 (also in use by DK-10-224-5-21-ADM1)

You must correct these errors before you can apply any changes.
Checking for Grid Network IP address swaps... PASSED.

Press Enter to continue
```

この例では、検証に合格しています。

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

Press Enter to continue
```

8. 検証に合格したら、次のいずれかのオプションを選択します。
   - **8**: 適用されていない変更を保存します。

     このオプションを使用すると、適用されていない変更を失うことなく、 IP 変更ツールを終了してあとで再起動できます。

   - **10**: 新しいネットワーク設定を適用します。
9. オプション * 10 * を選択した場合は、次のいずれかのオプションを選択します。
   - * apply * ：必要に応じて、変更をただちに適用し、各ノードを自動的に再起動します。

     新しいネットワーク設定で物理的な変更が不要な場合は、 *apply * を選択して、変更をすぐに適用できます。必要に応じて、ノードが自動的に再起動されます。再起動が必要なノードが表示されます。

   - * stage * ：ノードが次回手動で再起動されるときに変更を適用します。

     新しいネットワーク構成を機能させるためにネットワーク構成を物理的または仮想的に変更する必要がある場合は、 * stage * オプションを使用して影響を受けるノードをシャットダウンし、必要な物理ネットワーク変更を行って、影響を受けるノードを再起動する必要があります。これらのネットワーク変更を行わずに [*apple] を選択すると、通常、変更は失敗します。

     > stage * オプションを使用する場合は、システムの停止を最小限に抑えるためにステージング後すぐにノードを再起動する必要があります。

   - * キャンセル * ：現時点ではネットワークに変更を加えないでください。

     提案した変更がノードの再起動を必要とするかどうかが不明である場合は、ユーザへの影響を最小限に抑えるために変更を延期できます。「 * CANCEL * 」を選択すると、メインメニューに戻り、変更内容が保持されるので、後で適用できます。

     apply * または * stage * を選択すると、新しいネットワーク構成ファイルが生成され、プロビジョニングが実行され、ノードが新しい作業情報で更新されます。

プロビジョニング中に、更新が適用されたときのステータスが出力に表示されます。

```
Generating new grid networking description file...

Running provisioning...

Updating grid network configuration on Name
```

変更を適用またはステージングすると、グリッド設定の変更を受けて新しいリカバリパッケージが生成されます。

10. 「 * stage * 」を選択した場合は、プロビジョニングが完了したあとに次の手順を実行します。

    a. ネットワークに対して必要な物理的または仮想的な変更を行います。

       - 物理ネットワークの変更 * ：必要に応じて、物理ネットワークに変更を加え、ノードを安全にシャットダウンします。

    **Linux**: ノードを初めて管理ネットワークまたはクライアントネットワークに追加する場合は、「既存のノードへのインターフェイスの追加」の説明に従って、インターフェイスが追加されていることを確認してください。

    a. 影響を受けたノードを再起動します。

11. 変更が完了したら、「 *0 」を選択して IP 変更ツールを終了します。

12. Grid Manager から新しいリカバリパッケージをダウンロードします。

    a. [* Maintenance * （メンテナンス） ] > [* System * （システム * ） ] > [* Recovery Package] （リカバリパッケージ * ）

    b. プロビジョニングパスフレーズを入力します。

関連情報

"Linux：既存のノードへのインターフェイスの追加"

"Red Hat Enterprise Linux または CentOS をインストールします"

"Ubuntu または Debian をインストールします"

"SG100 SG1000サービスアプライアンス"

"SG6000 ストレージアプライアンス"

"SG5700 ストレージアプライアンス"

"StorageGRID の管理"

"IPアドレスを設定しています"

管理ネットワークのサブネットリストに対する追加または変更

## ノードの管理ネットワークサブネットリストで、サブネットの追加、削除、または変更

を行うことができます。

必要なもの

- を用意しておく必要があります `Passwords.txt` ファイル。

管理ネットワークサブネットリストで、すべてのノードに対してサブネットの追加、削除、または変更を行うことができます。

手順

1. プライマリ管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

      rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

2. 次のコマンドを入力してIP変更ツールを起動します。 `change-ip`
3. プロンプトでプロビジョニングパスフレーズを入力します。

   メインメニューが表示されます。

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

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

Selection:
```

4. 必要に応じて、処理を実行するネットワークまたはノードを制限します。次のいずれかを選択します。
   - 操作を実行する特定のノードでフィルターを適用する場合は、 * 1 * を選択して、編集するノードを選択します。次のいずれかのオプションを選択します。
     - * 1 * ：シングルノード（名前で選択）
     - * 2 * ：シングルノード（サイトで選択したあとに名前で選択）
     - * 3 * ：シングルノード（現在の IP で選択）
     - * 4 * ：サイト内のすべてのノード
     - * 5 * ：グリッド内のすべてのノード
     - * 0 * ：戻ります

- 「 ALL 」を選択したままにします。選択が完了すると、メインメニュー画面が表示されます。[ 選択したノード ] フィールドに新しい選択内容が反映され、選択したすべての操作がこの項目に対してのみ実行されます。

5. メインメニューで、管理ネットワークのサブネットを編集するオプションを選択します（オプション * 3 * ）。
6. 次のいずれかを選択します。
   - サブネットを追加する場合は次のコマンドを入力します： `add CIDR`
   - サブネットを削除する場合は次のコマンドを入力します： `del CIDR`
   - サブネットのリストを設定する場合は、次のコマンドを入力します： `set CIDR`

   コマンドでは、次の形式で複数のアドレスを入力できます。 `add CIDR, CIDR`

   例 `add 172.14.0.0/16, 172.15.0.0/16, 172.16.0.0/16`

   「上矢印」を使用して以前に入力した値を現在の入力プロンプトに呼び出し、必要に応じて編集することで、入力の手間を省くことができます。

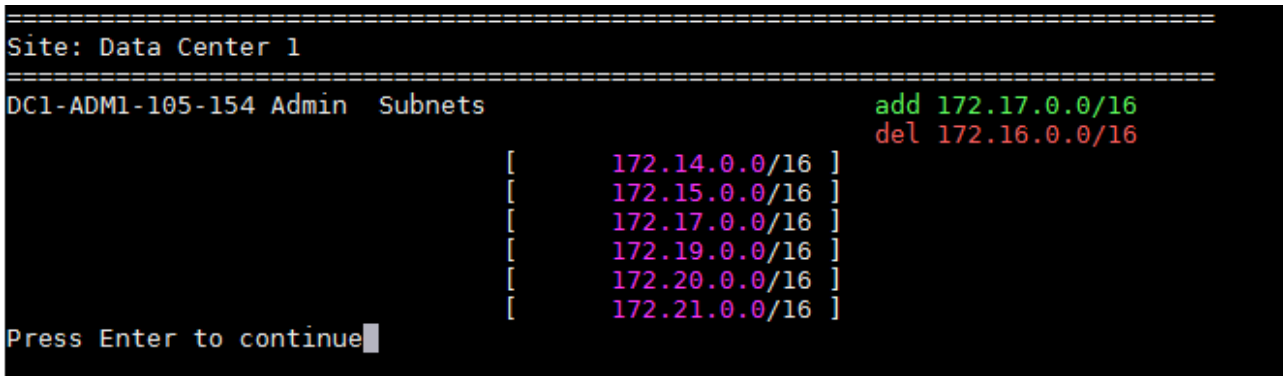
   次の入力例では、管理ネットワークサブネットリストにサブネットを追加しています。

```
Editing: Admin Network Subnet List for node DK-10-224-5-20-G1

Press <enter> to use the list as shown
Use up arrow to recall a previously typed value, which you can then edit
Use 'add <CIDR> [, <CIDR>]' to add subnets <CIDR> [, <CIDR>] to the list
Use 'del <CIDR> [, <CIDR>]' to delete subnets <CIDR> [, <CIDR>] from the list
Use 'set <CIDR> [, <CIDR>]' to set the list to the given list
Use q to complete the editing session early and return to the previous menu

DK-10-224-5-20-G1
  10.0.0.0/8
  172.19.0.0/16
  172.21.0.0/16
  172.20.0.0/16

[add/del/set/quit <CIDR>, ...]: add 172.14.0.0/16, 172.15.0.0/16
```

7. 準備ができたら、「 * q * 」と入力してメインメニュー画面に戻ります。変更内容は、クリアまたは適用されるまで保持されます。

   手順 2 で「すべて」のノード選択モードを選択した場合は、 Enter * （ * q * なし）を押して、リスト内の次のノードに移動する必要があります。

8. 次のいずれかを選択します。
   - オプション * 5 * を選択すると、変更された項目のみを表示するために分離された出力に編集内容が表示されます。次の出力例に示すように、変更は緑（追加）または赤（削除）で強調表示されます。




◦ オプション * 6 * を選択すると、設定全体を表示する出力に編集内容が表示されます。変更は、緑（追加）または赤（削除）で強調表示されます。* 注：一部のターミナルエミュレータでは、取り消し線の形式で追加と削除が表示される場合があります。

サブネットリストを変更しようとすると、次のメッセージが表示されます。

```
CAUTION: The Admin Network subnet list on the node might contain /32
subnets derived from automatically applied routes that are not
persistent. Host routes (/32 subnets) are applied automatically if
the IP addresses provided for external services such as NTP or DNS
are not reachable using default StorageGRID routing, but are
reachable using a different interface and gateway. Making and
applying changes to the subnet list will make all automatically
applied subnets persistent. If you do not want that to happen, delete
the unwanted subnets before applying changes. If you know that all
/32 subnets in the list were added intentionally, you can ignore this
caution.
```

NTP および DNS サーバのサブネットをネットワークに明確に割り当てなかった場合、 StorageGRID は接続のホストルート（ /32 ）を自動的に作成します。たとえば、 DNS サーバまたは NTP サーバへのアウトバウンド接続に /16 または /24 ルートを使用する場合は、自動的に作成された /32 ルートを削除し、必要なルートを追加する必要があります。自動的に作成されたホストルートを削除しないと、サブネットリストへの変更を適用したあともそのルートが保持されます。

> これらの自動検出されたホストルートは使用できますが、通常は、接続を確保するために DNS ルートと NTP ルートを手動で設定する必要があります。

9. オプション * 7 * を選択して、すべての段階的な変更を検証します。

この検証により、重複するサブネットを使用するなど、グリッドネットワーク、管理ネットワーク、クライアントネットワークのルールが確実に実行されます。

10. 必要に応じて、オプション * 8 を選択してステージングされたすべての変更を保存し、後で戻って変更を続行します。

このオプションを使用すると、適用されていない変更を失うことなく、 IP 変更ツールを終了してあとで再起動できます。

11. 次のいずれかを実行します。
    - 新しいネットワーク設定を保存または適用せずにすべての変更をクリアする場合は、オプション * 9 * を選択します。
    - 変更を適用し、新しいネットワーク設定をプロビジョニングする準備ができたら、オプション * 10 を選択します。プロビジョニング中に、次の出力例のように、更新が適用されている状況が出力に表示されます。

```
Generating new grid networking description file...

Running provisioning...

Updating grid network configuration on Name
```

12. Grid Manager から新しいリカバリパッケージをダウンロードします。
    a. [* Maintenance * （メンテナンス） ] > [* System * （システム * ） ] > [* Recovery Package] （リカバリパッケージ * ）
    b. プロビジョニングパスフレーズを入力します。

関連情報

"IPアドレスを設定しています"

グリッドネットワークのサブネットリストに対する追加または変更

# IP 変更ツールを使用して、グリッドネットワークのサブネットを追加または変更することができます。

必要なもの

- を使用することができます `Passwords.txt` ファイル。

このタスクについて

グリッドネットワークサブネットリストで、サブネットの追加、削除、または変更を行うことができます。変更を行うと、グリッド内のすべてのノードでのルーティングに影響します。

> グリッドネットワークサブネットリストのみを変更する場合は、グリッドマネージャを使用してネットワーク設定の追加または変更を行います。グリッドネットワーク設定問題 が原因でグリッドマネージャにアクセスできない場合、またはグリッドネットワークルーティングの変更とその他のネットワーク変更を同時に実行する場合は、 IP 変更ツールを使用します。

手順

1. プライマリ管理ノードにログインします。
    a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`
    b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
    c. 次のコマンドを入力してrootに切り替えます。 `su -`
    d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

2. 次のコマンドを入力してIP変更ツールを起動します。 `change-ip`
3. プロンプトでプロビジョニングパスフレーズを入力します。

   メインメニューが表示されます。

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

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

Selection:
```

4. メインメニューで、グリッドネットワークのサブネットを編集するオプションを選択します（オプション * 4 * ）。

   グリッドネットワークサブネットリストに対する変更は、グリッド全体に反映されます。

5. 次のいずれかを選択します。

   - サブネットを追加する場合は次のコマンドを入力します： `add CIDR`
   - サブネットを削除する場合は次のコマンドを入力します： `del CIDR`
   - サブネットのリストを設定する場合は、次のコマンドを入力します： `set CIDR`

     コマンドでは、次の形式で複数のアドレスを入力できます。 `add CIDR, CIDR`

   例 `add 172.14.0.0/16, 172.15.0.0/16, 172.16.0.0/16`

   「上矢印」を使用して以前に入力した値を現在の入力プロンプトに呼び出し、必要に応じて編集することで、入力の手間を省くことができます。

   次の入力例では、グリッドネットワークサブネットリストのサブネットを設定しています。

```
Editing: Grid Network Subnet List

Press <enter> to use the list as shown
Use up arrow to recall a previously typed value, which you can then edit
Use 'add <CIDR> [, <CIDR>]' to add subnets <CIDR> [, <CIDR>] to the list
Use 'del <CIDR> [, <CIDR>]' to delete subnets <CIDR> [, <CIDR>] from the list
Use 'set <CIDR> [, <CIDR>]' to set the list to the given list
Use q to complete the editing session early and return to the previous menu

Grid Network Subnet List
  172.16.0.0/21
  172.17.0.0/21
  172.18.0.0/21
  192.168.0.0/21

[add/del/set/quit <CIDR>, ...]: set 172.30.0.0/21, 172.31.0.0/21, 192.168.0.0/21
```

6. 準備ができたら、「 * q * 」と入力してメインメニュー画面に戻ります。変更内容は、クリアまたは適用されるまで保持されます。
7. 次のいずれかを選択します。
   - オプション * 5 * を選択すると、変更された項目のみを表示するために分離された出力に編集内容が表示されます。次の出力例に示すように、変更は緑（追加）または赤（削除）で強調表示されます。

```
Grid Network Subnet List (GNSL)

                                                    add 172.30.0.0/21
                                                    add 172.31.0.0/21
                                                    del 172.16.0.0/21
                                                    del 172.17.0.0/21
                                                    del 172.18.0.0/21
                              [      172.30.0.0/21 ]
                              [      172.31.0.0/21 ]
                              [    192.168.0.0/21 ]
Press Enter to continue
```

   - オプション * 6 * を選択すると、設定全体を表示する出力に編集内容が表示されます。変更は、緑（追加）または赤（削除）で強調表示されます。

> 一部のコマンドラインインターフェイスでは、追加と削除が取り消し線で示される場合があります。

8. オプション * 7 * を選択して、すべての段階的な変更を検証します。

   この検証により、重複するサブネットを使用するなど、グリッドネットワーク、管理ネットワーク、クライアントネットワークのルールが確実に実行されます。

9. 必要に応じて、オプション * 8 を選択してステージングされたすべての変更を保存し、後で戻って変更を続行します。

   このオプションを使用すると、適用されていない変更を失うことなく、 IP 変更ツールを終了してあとで再起動できます。

10. 次のいずれかを実行します。

- 新しいネットワーク設定を保存または適用せずにすべての変更をクリアする場合は、オプション * 9 * を選択します。
- 変更を適用し、新しいネットワーク設定をプロビジョニングする準備ができたら、オプション * 10 を選択します。プロビジョニング中に、次の出力例のように、更新が適用されている状況が出力に表示されます。

```
Generating new grid networking description file...

Running provisioning...

Updating grid network configuration on Name
```

11. グリッドネットワークの変更時にオプション * 10 を選択した場合は、次のいずれかのオプションを選択します。
    - * apply * ：必要に応じて、変更をただちに適用し、各ノードを自動的に再起動します。

      外部的な変更なしで新しいネットワーク設定が古いネットワーク設定と同時に機能する場合は、 * apply * オプションを使用して、設定の変更を完全に自動化することができます。

    - * stage * ：ノードが次回再起動されるときに変更を適用します。

      新しいネットワーク構成を機能させるためにネットワーク構成を物理的または仮想的に変更する必要がある場合は、 * stage * オプションを使用して影響を受けるノードをシャットダウンし、必要な物理ネットワーク変更を行って、影響を受けるノードを再起動する必要があります。

      > stage * オプションを使用する場合は、システムの停止を最小限に抑えるためにステージング後すぐにノードを再起動する必要があります。

    - * キャンセル * ：現時点ではネットワークに変更を加えないでください。

      提案した変更がノードの再起動を必要とするかどうかが不明である場合は、ユーザへの影響を最小限に抑えるために変更を延期できます。「 * CANCEL * 」を選択すると、メインメニューに戻り、変更内容が保持されるので、後で適用できます。

    変更を適用またはステージングすると、グリッド設定の変更を受けて新しいリカバリパッケージが生成されます。

12. エラーが原因で設定が停止した場合は、次のオプションを使用できます。
    - IP 変更手順 を中止してメインメニューに戻るには、「 * a * 」と入力します。
    - 失敗した処理を再試行するには、「 * r * 」と入力します。
    - 次の処理に進むには、 * c * と入力します。

      失敗した処理は、メインメニューからオプション * 10 * （変更の適用）を選択することで後で再試行できます。すべての処理が正常に完了するまで、 IP 変更手順 は完了しません。

    - 手動での介入（ノードのリブートなど）が必要なときに、ツールでは失敗と判断された操作が実際には正常に完了したことがわかった場合は、「 * f * 」と入力してその操作を成功とマークし、次の処理

に進みます。

13. Grid Manager から新しいリカバリパッケージをダウンロードします。

    a. [* Maintenance * （メンテナンス） ] > [* System * （システム * ） ] > [* Recovery Package] （リカバリパッケージ * ）

    b. プロビジョニングパスフレーズを入力します。

    > リカバリパッケージファイルには StorageGRID システムからデータを取得するための暗号キーとパスワードが含まれているため、安全に保管する必要があります。

関連情報

"IPアドレスを設定しています"

**Linux**：既存のノードへのインターフェイスの追加

## 最初にインストールしなかったLinuxベースのノードにインターフェイスを追加する場合は、この手順 を使用する必要があります。

インストール時に Linux ホスト上のノード構成ファイルで ADMIN_NETWORK_TARGET または ADMIN_NETWORK_TARGET を設定しなかった場合は、この手順 を使用してインターフェイスを追加します。ノード構成ファイルの詳細については、使用しているLinuxオペレーティングシステムでのStorageGRIDのインストール手順を参照してください。

"Red Hat Enterprise Linux または CentOS をインストールします"

"Ubuntu または Debian をインストールします"

この手順 は、ノード内ではなく、新しいネットワーク割り当てが必要なノードをホストしている Linux サーバ上で実行します。この手順 で追加されるのはノードだけです。他のネットワークパラメータを指定しようとすると、検証エラーが発生します。

アドレス情報を指定するには、 IP 変更ツールを使用する必要があります。ノードのネットワーク設定の変更に関する情報を参照してください。

"ノードのネットワーク設定を変更する"

手順

1. 新しいネットワーク割り当てが必要なノードをホストしているLinuxサーバにログインします。
2. ノード構成ファイルを編集します `/etc/storagegrid/nodes/node-name.conf`。

    > 他のネットワークパラメータを指定しないでください。検証エラーが発生します。

    a. 新しいネットワークターゲットを追加します。

    ```
    CLIENT_NETWORK_TARGET = bond0.3206
    ```

    b. オプション：MACアドレスを追加します。

```
CLIENT_NETWORK_MAC = aa:57:61:07:ea:5c
```

3. node validate コマンドを実行します。 `sudo storagegrid node validate node-name`
4. 検証エラーをすべて解決します。
5. node reload コマンドを実行します。 `sudo storagegrid node reload node-name`

関連情報

"Red Hat Enterprise Linux または CentOS をインストールします"

"Ubuntu または Debian をインストールします"

"ノードのネットワーク設定を変更する"

グリッド内のすべてのノードのIPアドレスの変更

## グリッド内のすべてのノードのグリッドネットワーク IP アドレスを変更する必要がある場合は、次の特別な手順 に従う必要があります。手順 を使用してグリッド全体のグリッドネットワーク IP を変更し、個々のノードを変更することはできません。

必要なもの

- を用意しておく必要があります `Passwords.txt` ファイル。

このタスクについて

グリッドが正常に起動するようにするには、すべての変更を一度に行う必要があります。

> この 手順 環境 はグリッドネットワークのみです。この手順 を使用して、管理ネットワークまたはクライアントネットワークの IP アドレスを変更することはできません。

一方のサイトのノードのIPアドレスとMTUのみを変更する場合は、ノードのネットワーク設定を変更する手順に従います。

手順

1. DNS や NTP の変更、シングルサインオン（ SSO ）設定の変更（使用している場合）など、 IP 変更ツールを使用しない変更については、事前に計画を立てる必要があります。

> 既存の NTP サーバが新しい IP アドレスでグリッドにアクセスできなくなる場合は、 IP の変更手順 を実行する前に新しい NTP サーバを追加します。

> 既存手順 の DNS サーバが新しい IP アドレスでグリッドにアクセスできなくなる場合は、 IP の変更を行う前に新しい DNS サーバを追加します。

> StorageGRID システムで SSO が有効になっており、証明書利用者信頼が（推奨される完全修飾ドメイン名ではなく）管理ノードの IP アドレスを使用して設定されている場合は、 Active Directory フェデレーションサービス（ AD FS ）でこれらの証明書利用者信頼を更新または再設定する準備をしておきます。 IP アドレスを変更した場合はすぐに反映されます。StorageGRID の管理手順を参照してください。

必要に応じて、新しい IP アドレス用の新しいサブネットを追加します。

2. プライマリ管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

   rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

3. 次のコマンドを入力してIP変更ツールを起動します。 `change-ip`
4. プロンプトでプロビジョニングパスフレーズを入力します。

   メインメニューが表示されます。デフォルトでは、が表示されます `Selected nodes` フィールドはに設定されます `all`。

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

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

Selection:
```

5. メインメニューで「 * 2 * 」を選択して、すべてのノードの IP / サブネットマスク、ゲートウェイ、 MTU 情報を編集します。
   a. 1 * を選択してグリッドネットワークを変更します。

      選択が完了すると、ノード名、グリッドネットワーク名、データタイプ（ IP / マスク、ゲートウェイ、または MTU ）がプロンプトに表示されます。 および現在の値。

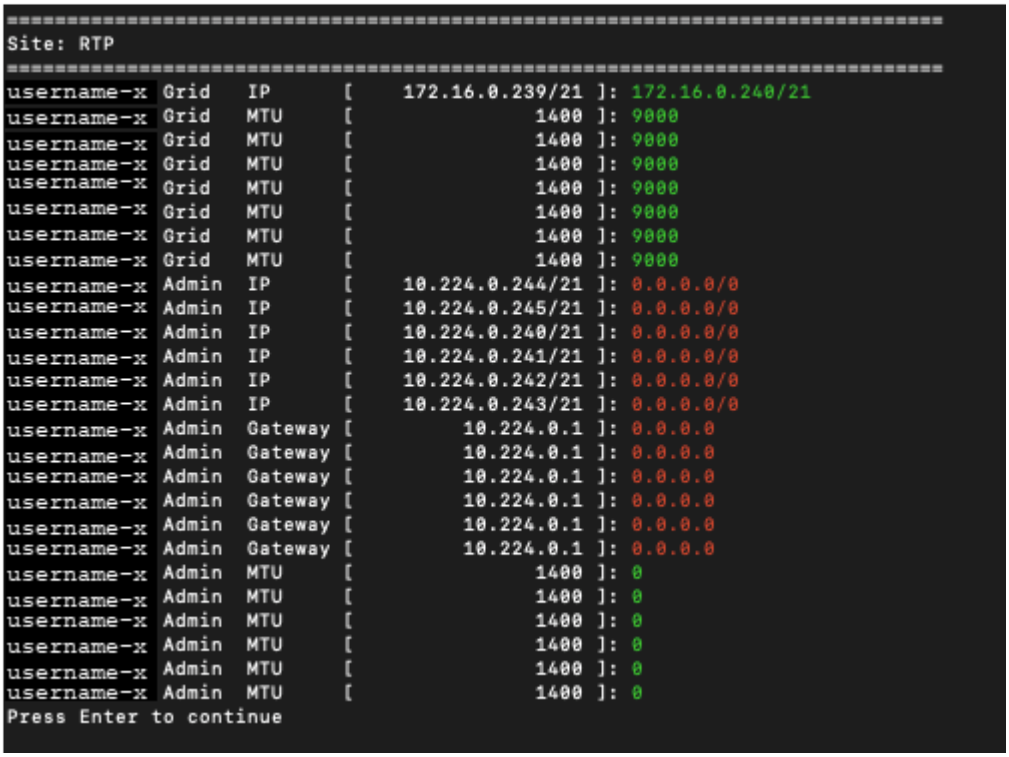
      DHCP によって設定されたインターフェイスの IP アドレス、プレフィックス長、ゲートウェイ、または MTU を編集すると、インターフェイスが static に変更されます。DHCP によって設定された各インターフェイスの前に、警告が表示されます。

   として設定されたインターフェイス `fixed` 編集できません。

   a. 新しい値を設定するには、現在の値の形式で入力します。
   b. 変更するすべてのノードを編集したら、「 * q * 」と入力してメインメニューに戻ります。

      変更内容は、クリアまたは適用されるまで保持されます。

6. 次のいずれかのオプションを選択して、変更内容を確認します。
   - **5**: 変更された項目のみを表示するために分離された出力の編集を表示します。変更は、次の出力例に示すように、緑（追加）または赤（削除）で強調表示されます。



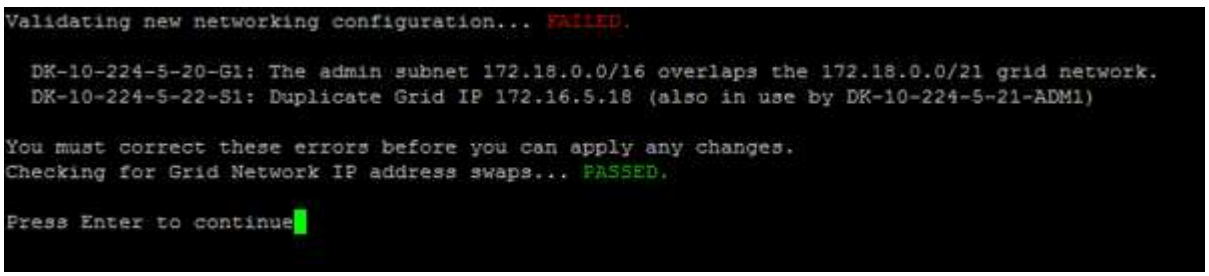

   - **6**: 編集内容を出力に表示し、設定全体を表示します。変更は、緑（追加）または赤（削除）で強調表示されます。

> 一部のコマンドラインインターフェイスでは、追加と削除が取り消し線で示される場合があります。正しく表示されるためには、使用するターミナルクライアントが必要な VT100 エスケープシーケンスをサポートしている必要があります。

7. オプション * 7 * を選択して、すべての変更を検証します。

   この検証により、重複するサブネットを使用しないようなグリッドネットワークのルールに違反しなくなります。

   この例では、検証でエラーが返されています。




   この例では、検証に合格しています。

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

Press Enter to continue
```

8. 検証に合格したら、「 * 10 」を選択して新しいネットワーク設定を適用します。
9. 次にノードを再起動したときに変更を適用するには、 * stage * を選択します。

> 「 * stage * 」を選択する必要があります。手動または * stage * の代わりに * apply * を選択してローリングリスタートを実行しないでください。グリッドが正常に起動しません。

10. 変更が完了したら、 **0** を選択して IP 変更ツールを終了します。
11. すべてのノードを同時にシャットダウンします。

> すべてのノードが同時に停止するように、グリッド全体を一度にシャットダウンする必要があります。

12. ネットワークに対して必要な物理的または仮想的な変更を行います。
13. すべてのグリッドノードが停止していることを確認します。
14. すべてのノードの電源をオンにします。
15. グリッドが正常に起動したら、次の手順を実行します
    a. 新しい NTP サーバを追加した場合は、古い NTP サーバの値を削除します。
    b. 新しい DNS サーバを追加した場合は、古い DNS サーバの値を削除します。
16. Grid Manager から新しいリカバリパッケージをダウンロードします。
    a. [* Maintenance * （メンテナンス） ] > [* System * （システム * ） ] > [* Recovery Package] （リカバリパッケージ * ）
    b. プロビジョニングパスフレーズを入力します。

関連情報

"StorageGRID の管理"

"ノードのネットワーク設定を変更する"

"グリッドネットワークのサブネットリストに対する追加または変更"

"グリッドノードをシャットダウンしています"

**DNS**サーバを設定しています

IP アドレスではなく Fully Qualified Domain Name （ FQDN ；完全修飾ドメイン名）ホスト名を使用できるよう、 Domain Name System （ DNS ；ドメインネームシステム）サーバを追加、削除、更新することができます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Maintenance または Root Access 権限が必要です。
- 設定する DNS サーバの IP アドレスを確認しておく必要があります。

このタスクについて

DNS サーバ情報を指定すると、 E メール通知や SNMP 通知、および AutoSupport に、 IP アドレスではなく完全修飾ドメイン名（ FQDN ）ホスト名を使用できるようになります。DNS サーバは少なくとも 2 つ指定することを推奨します。

> DNS サーバの IP アドレスは 2~6 つ指定します。一般に、ネットワーク分離が発生した場合に各サイトがローカルにアクセスできる DNS サーバを選択します。これにより、分離されたサイトは引き続き DNS サービスにアクセスできます。グリッド全体の DNS サーバリストを設定したあとに、ノードごとに DNS サーバリストをカスタマイズできます。

"単一グリッドノードでのDNS設定の変更"

DNS サーバ情報を省略したり誤って設定したりすると、各グリッドノードの SSM サービスで DNST アラームがトリガーされます。このアラームは、 DNS が正しく設定され、新しいサーバ情報がすべてのグリッドノードに配信された時点で解除されます。

手順

1. [* Maintenance * **Network * DNS Servers**（メンテナンス*ネットワーク DNSサーバー*）]を選択します。
2. 必要に応じて、 Servers セクションで、アップデートを追加するか、 DNS サーバエントリを削除します。

   サイトごとに少なくとも 2 つの DNS サーバを指定することを推奨します。DNS サーバは 6 つまで指定できます。

3. [ 保存（ Save ） ] をクリックします。

単一グリッドノードでの**DNS**設定の変更

## 環境全体でグローバルにドメインネームシステム（ DNS ）を設定する代わりに、スクリプトを実行してグリッドノードごとに DNS を設定することができます。

一般に、Grid Managerで* Maintenance * Network * DNS Servers *オプションを使用してDNSサーバを設定する必要があります。次のスクリプトは、グリッドノードごとに異なる DNS サーバを使用する必要がある場合にのみ使用します。

1. プライマリ管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

      rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

e. SSH エージェントに SSH 秘密鍵を追加します。入力するコマンド `ssh-add`

f. に記載されているSSHアクセスパスワードを入力します `Passwords.txt` ファイル。

2. カスタムDNS設定で更新するノードにログインします。 `ssh *node_IP_address*`

3. DNSセットアップスクリプトを実行します。 `setup_resolv.rb.`

スクリプトから、サポートされるコマンドの一覧が返されます。

```
Tool to modify external name servers

available commands:
  add search <domain>
               add a specified domain to search list
               e.g.> add search netapp.com
  remove search <domain>
               remove a specified domain from list
               e.g.> remove search netapp.com
  add nameserver <ip>
               add a specified IP address to the name server list
               e.g.> add nameserver 192.0.2.65
  remove nameserver <ip>
               remove a specified IP address from list
               e.g.> remove nameserver 192.0.2.65
  remove nameserver all
               remove all nameservers from list
  save         write configuration to disk and quit
  abort        quit without saving changes
  help         display this help message


Current list of name servers:
    192.0.2.64
Name servers inherited from global DNS configuration:
    192.0.2.126
    192.0.2.127
Current list of search entries:
    netapp.com

Enter command [`add search <domain>|remove search <domain>|add
nameserver <ip>`]
              [`remove nameserver <ip>|remove nameserver
all|save|abort|help`]
```

4. ネットワークにドメインネームサービスを提供するサーバのIPv4アドレスを追加します。 `add <nameserver IP_address>`

5. を繰り返します `add nameserver` コマンドを使用して、ネームサーバを追加します。
6. 他のコマンドについてはプロンプトが表示されたら、その指示に従います。
7. 変更を保存してアプリケーションを終了します。 `save`
8. サーバでコマンドシェルを閉じます。 `exit`
9. グリッドノードごとに、からの手順を繰り返します ノードにログインします から コマンドシェルを閉じています。
10. 他のサーバにパスワードなしでアクセスする必要がなくなった場合は、 SSH エージェントから秘密鍵を削除します。入力するコマンド `ssh-add -D`

**NTP**サーバを設定しています

## StorageGRID システムのグリッドノード間でデータが正確に同期されるようにするには、 Network Time Protocol （ NTP ；ネットワークタイムプロトコル）サーバを追加、更新、または削除します。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Maintenance または Root Access 権限が必要です。
- プロビジョニングパスフレーズが必要です。
- 設定する NTP サーバの IPv4 アドレスを確認しておく必要があります。

このタスクについて

StorageGRID システムは、 Network Time Protocol （ NTP ；ネットワークタイムプロトコル）を使用して、グリッド内のすべてのグリッドノード間で時刻を同期します。

各サイトでは、 StorageGRID システムの少なくとも 2 つのノードにプライマリ NTP ロールが割り当てられます。推奨される最低 4 つ、最大 6 つの外部時間ソース、および相互に同期します。StorageGRID システムのプライマリ NTP ノード以外のノードは、すべて NTP クライアントとして機能し、プライマリ NTP ノードと同期されます。

外部 NTP サーバは、以前にプライマリ NTP ロールを割り当てていたノードに接続されます。このため、プライマリ NTP ロールが割り当てられたノードを少なくとも 2 つ指定することを推奨します。

> 各サイトの少なくとも 2 つのノードが、少なくとも 4 つの外部 NTP ソースにアクセスできることを確認します。NTP ソースにアクセスできるノードがサイトに 1 つしかないと、そのノードがダウンした場合にタイミングの問題が生じます。また、各サイトで 2 つのノードをプライマリ NTP ソースとして指定することにより、サイトがグリッドの他の部分から分離されても、正確なタイミングが保証されます。

指定する外部 NTP サーバは、 NTP プロトコルを使用している必要があります。時間のずれに伴う問題を防ぐには、 Stratum 3 以上の NTP サーバ参照を指定する必要があります。

> 本番レベルの StorageGRID インストール環境で外部 NTP ソースを指定する場合は、 Windows Server 2016 より前のバージョンの Windows で Windows Time （ W32Time ）サービスを使用しないでください。以前のバージョンの Windows のタイムサービスは精度が十分でないため、 StorageGRID などの高精度環境での使用は Microsoft でサポートされていません。

"高精度環境用に Windows タイムサービスを構成するためのサポート境界"

インストール時に指定した最初の NTP サーバの安定性や可用性に問題が生じた場合は、サーバの追加や既存のサーバの更新や削除を行って、 StorageGRID システムが使用する外部 NTP ソースのリストを更新できます。

手順

1. [* Maintenance * **Network * NTP Servers**（メンテナンス*ネットワーク NTPサーバー*）]を選択します。
2. 必要に応じて、 Servers セクションで、アップデートを追加するか、 NTP サーバエントリを削除します。

   NTP サーバは少なくとも 4 つ指定する必要があり、最大で 6 つまで指定できます。

3. ［ * プロビジョニングパスフレーズ * ］ テキストボックスに、 StorageGRID システムのプロビジョニングパスフレーズを入力し、 ［ * 保存 * ］ をクリックします。

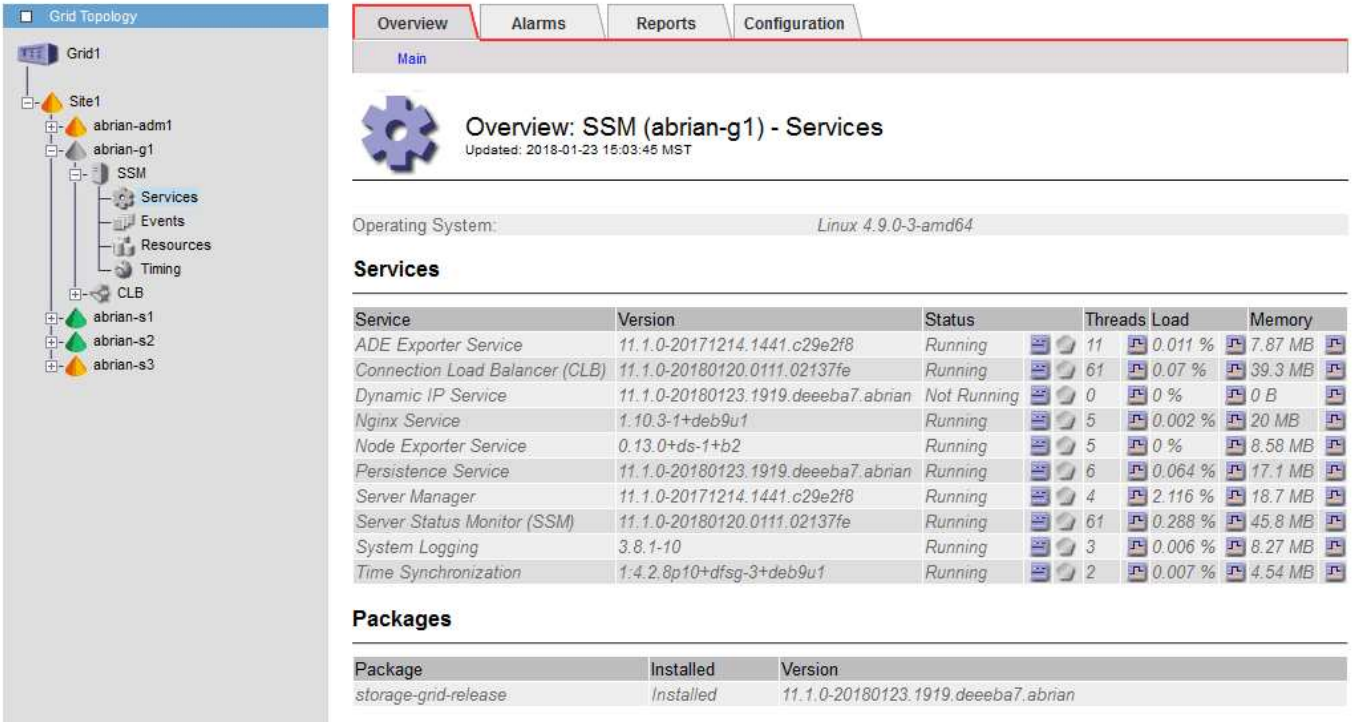
   手順 のステータスは、ページの上部に表示されます。設定の更新が完了するまで、ページは無効になります。

   新しい NTP サーバを保存したあとに、すべての NTP サーバで接続テストが失敗した場合は、次の手順に進まないでください。テクニカルサポートにお問い合わせください。

分離されているノードのネットワーク接続のリストア

## サイトまたはグリッド全体の IP アドレスの変更など、特定の状況では、ノードの 1 つ以上のグループがグリッド内の他のノードと通信できない場合があります。

グリッドマネージャ（サポート*ツール*グリッドトポロジ）で、ノードがグレー表示になっている場合、またはノードが青でそのサービスの多くがrunning以外の状態である場合は、ノードの分離を確認する必要があります。




分離されているノードがあると、次のような影響があります。

- 複数のノードが分離されていると、 Grid Manager へのサインインやアクセスができなくなる可能性があります。
- 複数のノードが分離されている場合は、ダッシュボードに表示される Tenant Manager のストレージ使用量とクォータの値が最新でない可能性があります。合計はネットワーク接続が回復すると更新されます。

分離問題 を解決するには、グリッドから分離されている各分離ノードまたはグループ内の 1 つ（プライマリ管理ノードを含まないサブネット内のすべてのノード）で、コマンドラインユーティリティを実行します。このユーティリティは、グリッド内の分離されていないノードの IP アドレスをノードに提供します。これにより、分離されているノードまたはノードのグループがグリッド全体に再びアクセスできるようになります。

マルチキャストドメインネームシステム（ mDNS ）がネットワークでディセーブルになっている場合は、独立した各ノードでコマンドラインユーティリティを実行する必要があります。

手順

1. ノードにアクセスしてチェックします `/var/local/log/dynip.log` 分離に関するメッセージの場合。

   例：

   ```
   [2018-01-09T19:11:00.545] UpdateQueue - WARNING -- Possible isolation,
   no contact with other nodes.
   If this warning persists, manual action may be required.
   ```

   VMware コンソールを使用している場合は、ノードが分離された可能性があることを示すメッセージが含まれます。

   Linux環境では、分離に関するメッセージはに表示されます

/var/log/storagegrid/node/<nodename>.log ファイル。

2. 分離に関するメッセージが繰り返し表示され、保持されている場合は、次のコマンドを実行します。

   add_node_ip.py <address\>

   ここで、 <address\> は、グリッドに接続されているリモートノードのIPアドレスです。

```
# /usr/sbin/add_node_ip.py  10.224.4.210

Retrieving local host information
Validating remote node at address 10.224.4.210
Sending node IP hint for 10.224.4.210 to local node
Local node found on remote node. Update complete.
```

3. 分離されていた各ノードについて、次の点を確認します。
   - ノードのサービスが開始されている。
   - Dynamic IP Serviceのステータスは、を実行した後に「Running」になります storagegrid-status コマンドを実行します
   - グリッドトポロジツリーで、ノードがグリッド内の他のノードから切断されていない状態になっている。

> を実行する場合 add_node_ip.py このコマンドでは問題は解決しません。解決が必要なその他のネットワーク問題が考えられます。

## ホストレベルおよびミドルウェアの手順

一部のメンテナンス手順は、 StorageGRID の Linux または VMware 環境、あるいは StorageGRID 解決策 のその他のコンポーネントに固有です。

**Linux**：新しいホストへのグリッドノードの移行

ホストのメンテナンス（ OS パッチの適用やリブートなど）を実行するために、グリッドの機能や可用性に影響を及ぼすことなく、 Linux ホスト間で StorageGRID ノードを移行できます。

1 つまたは複数のノードを 1 つの Linux ホスト（ 「ソースホスト」 ）から別の Linux ホスト（ 「ターゲットホスト」 ）に移行します。ターゲットホストで StorageGRID を使用する準備をしておく必要があります。

> この手順 は、 StorageGRID 環境で移行をサポートするように計画した場合にのみ使用できます。

グリッドノードを新しいホストに移行するには、次の両方の条件が満たされている必要があります。

- 共有ストレージは、すべてのノード単位のストレージボリュームに使用されます
- ネットワークインターフェイスの名前がホスト間で一貫している

本番環境では、 1 つのホストで複数のストレージノードを実行しないでください。各ストレージノードに専用のホストを使用すると、分離された障害ドメインが提供されます。

管理ノードやゲートウェイノードなど、他のタイプのノードは、同じホストに導入することができます。ただし、同じタイプのノードが複数ある（たとえば、 2 つのゲートウェイノード）場合は、すべてのインスタンスを同じホストにインストールしないでください。

詳細については、お使いの Linux オペレーティングシステム用の StorageGRID インストール手順の「ノード移行の要件」を参照してください。

関連情報

"新しいLinuxホストの導入"

"Red Hat Enterprise Linux または CentOS をインストールします"

"Ubuntu または Debian をインストールします"

**Linux**：ソースホストからノードをエクスポートします

## グリッドノードをシャットダウンして、ソースの Linux ホストからエクスポートします。

ソースの Linux ホストで次のコマンドを実行します。

1. ソースホストで現在実行されているすべてのノードのステータスを取得します。

```
sudo storagegrid node status all
```

```
Name Config-State Run-State

DC1-ADM1 Configured Running

DC1-ARC1 Configured Running

DC1-GW1 Configured Running

DC1-S1 Configured Running

DC1-S2 Configured Running

DC1-S3 Configured Running
```

2. 移行するノードの名前を特定し、そのRun-Stateがであれば停止します `Running`。

```
sudo storagegrid node stop DC1-S3
```

```
Stopping node DC1-S3
```

```
Waiting up to 630 seconds for node shutdown
```

3. ソースホストからノードをエクスポートします。

```
sudo storagegrid node export DC1-S3
```

```
Finished exporting node DC1-S3 to /dev/mapper/sgws-dc1-s3-var-local.

Use 'storagegrid node import /dev/mapper/sgws-dc1-s3-var-local' if you

want to import it again.
```

4. をメモします `import command suggested in the output of the `export` コマンドを実行します

次の手順で、このコマンドをターゲットホストで実行します。

**Linux**：ターゲットホストにノードをインポートします

## ソースホストからノードをエクスポートしたら、ターゲット Linux ホストにノードをインポートして検証します。検証では、ソースホストと同じブロックストレージおよびネットワークインターフェイスデバイスにノードがアクセスできるかどうかを確認します。

ターゲット Linux ホストで次のコマンドを実行します。

1. ターゲットホストにノードをインポートします。

```
sudo storagegrid node import /dev/mapper/sgws-dc1-s3-var-local
```

```
Finished importing node DC1-S3 from /dev/mapper/sgws-dc1-s3-var-local.

You should run 'storagegrid node validate DC1-S3'
```

2. 新しいホストでノード構成を検証します。

```
sudo storagegrid node validate DC1-S3
```

```
Confirming existence of node DC1-S3... PASSED

Checking configuration file /etc/storagegrid/nodes/DC1-S3.conf for node DC1-
S3... PASSED

Checking for duplication of unique values... PASSED
```

3. 検証エラーが発生した場合は、移行したノードを開始する前に対処してください。

トラブルシューティングの情報については、使用している Linux オペレーティングシステムでの StorageGRID のインストール手順を参照してください。

関連情報

"Red Hat Enterprise Linux または CentOS をインストールします"

"Ubuntu または Debian をインストールします"

**Linux**：移行済みノードの開始

## 移行済みノードの検証が完了したら、ターゲット Linux ホストでコマンドを実行して、ノードを開始します。

手順

1. 新しいホストでノードを開始します。

```
sudo storagegrid node start DC1-S3
Starting node DC1-S3
```

2. Grid Manager で、ノードのステータスが緑色であり、そのノードに対するアラームが発生していないことを確認します。

ノードのステータスが緑色の場合、移行済みノードは完全に再起動してグリッドに再参加しています。ステータスが緑色でない場合は、複数のノードがサービス停止の状態にならないようにするために、追加のノードを移行しないでください。

Grid Manager にアクセスできない場合は、 10 分待ってから次のコマンドを実行します。

```
sudo storagegrid node status node-name
```

移行済みノードのRun-Stateがであることを確認します `Running`。

**TSM** ミドルウェアでのアーカイブノードのメンテナンス

## アーカイブノードは、 TSM ミドルウェアサーバ経由でテープをターゲットとするように設定するか、 S3 API 経由でクラウドをターゲットとするように設定できます。いったん設定したアーカイブノードのターゲットは変更できません。

アーカイブノードをホストしているサーバで障害が発生した場合は、サーバを交換し、適切なリカバリ手順に従います。

アーカイブストレージデバイスの障害

アーカイブノードが Tivoli Storage Manager （ TSM ）経由でアクセスしているアーカイブストレージデバイスに障害があることがわかった場合は、アーカイブノードをオフラインにして StorageGRID システムで表示されるアラームの数を制限します。そのあとに、 TSM サーバの管理ツール、ストレージデバイスの管理ツール、またはその両方を使用して問題を詳しく診断し、解決することができます。

ターゲットコンポーネントをオフラインにしています

TSM ミドルウェアサーバのメンテナンスを行うとアーカイブノードがそのサーバを使用できなくなる場合があるため、メンテナンスの前にターゲットコンポーネントをオフライン状態にして、 TSM ミドルウェアサーバが使用できなくなった場合にトリガーされるアラームの数を制限します。

必要なもの

Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

手順

1. Support **>** Tools **>** Grid Topology *を選択します。
2. 「* Archive Node * ARC * Target * Configuration * Main *」を選択します。
3. 「 Tivoli Storage Manager State 」の値を「 * Offline * 」に変更し、「 * Apply Changes * 」をクリックします。
4. メンテナンスが完了したら、 Tivoli Storage Manager State の値を * Online * に変更し、 * Apply Changes * をクリックします。

**Tivoli Storage Manager** の管理ツール

dsmadmc ツールは、アーカイブノードにインストールされる TSM ミドルウェアサーバの管理コンソールです。ツールにアクセスするには、と入力します `dsmadmc` をクリックします。管理コンソールには、 ARC サービス用に設定された管理ユーザ名とパスワードを使用してログインします。

。 `tsmquery.rb` dsmadmcからのステータス情報を判読しやすい形式で表示するにはスクリプトを使用します。このスクリプトを実行するには、アーカイブノードのコマンドラインで次のコマンドを入力します。
`/usr/local/arc/tsmquery.rb status`

TSM 管理コンソール dsmadmc の詳細については、 _Tivoli Storage Manager for Linux ： Administrator を参照してください。

オブジェクトは永続的に使用不能です

アーカイブノードが Tivoli Storage Manager （ TSM ）サーバにオブジェクトを要求し、その読み出しが失敗すると、 10 秒後にアーカイブノードが要求を再試行します。オブジェクトが永続的に使用不能な場合（テープ上でオブジェクトが破損しているなどの原因で）、 TSM API はその状況をアーカイブノードに通知できないため、アーカイブノードは要求を再試行し続けます。

この状況が発生するとアラームがトリガーされ、値が増え続けます。このアラームを表示するには、* Support * **Tools * Grid Topology** を選択します。次に、「 **Archive Node * ARC * Retrieve** Request Failures *」を選択します。

オブジェクトが永続的に使用不能である場合は、オブジェクトを特定し、手順 の説明に従ってアーカイブノードの要求を手動でキャンセルする必要があります。 オブジェクトが永続的に使用不能かどうかを確認する。

また、オブジェクトが一時的に使用不能である場合も読み出しが失敗することがあります。この場合は、最終的に後続の読み出し要求が成功します。

単一のオブジェクトコピーを作成する ILM ルールを使用するように StorageGRID システムが設定されている場合に、そのコピーを読み出せないと、オブジェクトは失われてリカバリできません。ただし、オブジェクトが永続的に使用不能かどうかを手順 で確認し、 StorageGRID システムを「クリーンアップ」したり、アーカ

イブノードの要求をキャンセルしたり、失われたオブジェクトのメタデータをパージしたりする必要があります。

### オブジェクトが永続的に使用不能かどうかを確認する

オブジェクトが永続的に使用不能かどうかを確認するには、 TSM 管理コンソールを使用して要求を行います。

#### 必要なもの

- 特定のアクセス権限が必要です。
- を用意しておく必要があります `Passwords.txt` ファイル。
- 管理ノードの IP アドレスを確認しておく必要があります。

#### このタスクについて

ここで示す例は参考情報です。この手順 では、オブジェクトやテープボリュームが使用不能になる可能性がある障害状況をすべて特定することはできません。TSM 管理の詳細については、 TSM サーバに関するドキュメントを参照してください。

#### 手順

1. 管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@Admin_Node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
2. アーカイブノードが読み出せなかったオブジェクトを特定します。
   a. 監査ログファイルが保存されているディレクトリに移動します。 `cd /var/local/audit/export`

      アクティブな監査ログファイルの名前は audit.log です。1日に1回、アクティブです `audit.log` ファイルが保存され、新しいファイルが作成されます `audit.log` ファイルが開始されました。保存されたファイルの名前は、保存された日時をの形式で示しています `yyyy-mm-dd.txt`。1日後、保存されたファイルは圧縮され、という形式で名前が変更されます `yyyy-mm-dd.txt.gz`元の日付を保持します。

   b. 関連する監査ログファイルで、アーカイブされたオブジェクトを読み出せなかったことを示すメッセージを検索します。たとえば、次のように入力します。 `grep ARCE audit.log | less -n`

      アーカイブノードからオブジェクトを読み出せない場合は、 ARCE （ Archive Object Retrieve End ）監査メッセージの結果フィールドに、 ARUN （ Archive Middleware Unavailable ）または GERR （ General Error ）と表示されます。次に示す監査ログの例では、 CBID 498D8A1F681F05B3 に対する ARCE メッセージが ARUN という結果で終了しています。

      ```
      [AUDT:[CBID(UI64):0x498D8A1F681F05B3][VLID(UI64):□20091127][RSLT(FC32
      ):ARUN][AVER(UI32):7]
      [ATIM(UI64):1350613602969243][ATYP(FC32):ARCE][ANID(UI32):13959984][A
      MID(FC32):ARCI]
      [ATID(UI64):4560349751312520631]]
      ```

      詳細については、監査メッセージを確認する手順を参照してください。

c. 要求が失敗した各オブジェクトの CBID を記録します。

アーカイブノードで保存されるオブジェクトを識別するために、 TSM で使用される次の追加情報 を記録しておくこともできます。

- * ファイルスペース名 * ：アーカイブノード ID に相当します。アーカイブノードIDを検索するには、* Support * **Tools * Grid Topology** *を選択します。次に、「 Archive Node * ARC * Target * Overview *」を選択します。
- * 上位の名前 * ：アーカイブノードによってオブジェクトに割り当てられたボリューム ID に相当します。ボリュームIDは日付の形式で入力します（例： `20091127`）を指定し、をアーカイブ監査メッセージにオブジェクトのVLIDとして記録します。
- * Low Level Name * ： StorageGRID システムによってオブジェクトに割り当てられた CBID に相当します。

d. コマンドシェルからログアウトします。 `exit`

3. TSM サーバを調べて、手順 2 で特定したオブジェクトが永続的に使用不能かどうかを確認します。

a. TSMサーバの管理コンソールにログインします。 `dsmadmc`

ARC サービス用に設定された管理ユーザ名とパスワードを使用します。Grid Manager にユーザ名とパスワードを入力します。（ユーザ名を表示するには、* Support * Tools * Grid Topology を選択します。次に、「 Archive Node * ARC * Target * Configuration *」を選択します。）

b. オブジェクトが永続的に使用不能かどうかを確認します。

たとえば、 TSM アクティビティログでそのオブジェクトのデータ整合性エラーを検索できます。次の例は、アクティビティログでCBIDを含むオブジェクトの過去1日の検索を示しています `498D8A1F681F05B3`。

```
> query actlog begindate=-1 search=276C14E94082CC69
12/21/2008 05:39:15 ANR0548W Retrieve or restore
failed for session 9139359 for node DEV-ARC-20 (Bycast ARC)
processing file space /19130020 4 for file /20081002/
498D8A1F681F05B3 stored as Archive - data
integrity error detected. (SESSION: 9139359)
>
```

エラーの種類によっては、 TSM アクティビティログに CBID が記録されないことがあります。場合によっては、要求が失敗した時間の前後に他の TSM エラーが発生していないかをログで検索する必要があります。

c. テープ全体が永続的に使用不能である場合は、そのボリュームに格納されているすべてのオブジェクトのCBIDを特定します。 `query content TSM_Volume_Name`

ここで、 `TSM_Volume_Name` は、使用できないテープのTSM名です。このコマンドの出力例を次に示します。

```
 > query content TSM-Volume-Name
Node Name     Type Filespace  FSID Client's Name for File Name
------------- ---- ---------- ---- ----------------------------
DEV-ARC-20    Arch /19130020  216  /20081201/ C1D172940E6C7E12
DEV-ARC-20    Arch /19130020  216  /20081201/ F1D7FBC2B4B0779E
```

。 `Client's Name for File Name` は、アーカイブノードのボリュームID（またはTSMの「上位の名前」）と、オブジェクトのCBID（またはTSMの「下位の名前」）を組み合わせたものと同じです。つまり、です `Client's Name for File Name` フォームを使用します `/Archive Node volume ID /CBID`。出力例の1行目に、が表示されています `Client's Name for File Name` はです `/20081201/ C1D172940E6C7E12`。

また、を思い出してください `Filespace` はアーカイブノードのノードIDです。

読み出し要求をキャンセルするには、ボリュームに格納されている各オブジェクトの CBID 、およびアーカイブノードのノード ID が必要です。

4. 永続的に使用不能なオブジェクトごとに、読み出し要求をキャンセルし、問題 a コマンドを使用して、オブジェクトのコピーが失われたことを StorageGRID システムに通知します。

> ADE コンソールを使用する際には注意が必要です。コンソールを適切に使用しないと、システム処理が中断されてデータが破損する可能性があります。コマンドを入力する際には十分に注意し、この手順 に記載されているコマンドのみを使用してください。

   a. アーカイブノードにまだログインしていない場合は、次の手順でログインします。
      i. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
      ii. に記載されているパスワードを入力します `Passwords.txt` ファイル。
      iii. 次のコマンドを入力してrootに切り替えます。 `su -`
      iv. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   b. ARCサービスのADEコンソールにアクセスします。 `telnet localhost 1409`
   c. オブジェクトに対する要求をキャンセルします。 `/proc/BRTR/cancel -c CBID`

      ここで、 `CBID` は、TSMから読み出せないオブジェクトのIDです。

      オブジェクトのコピーがテープにしかない場合 ' 一括取得要求はキャンセルされ ' メッセージが表示されます要求はキャンセルされましたオブジェクトのコピーがシステム内の別の場所に存在する場合 ' オブジェクトの取得は別のモジュールによって処理されるため ' メッセージに対する応答は 0 要求がキャンセルされました

   d. 問題 オブジェクトのコピーが失われたこと、および追加のコピーを作成する必要があることをStorageGRID システムに通知するコマンド。 `/proc/CMSI/Object_Lost CBID node_ID`

      ここで、 `CBID` は、TSMサーバから読み出せないオブジェクトのIDです `node_ID` は、読み出しが失敗したアーカイブノードのノードIDです。

      失われたオブジェクトのコピーごとに別々のコマンドを入力する必要があります。 CBID の範囲の入

力はサポートされていません。

ほとんどの場合、 StorageGRID システムはその ILM ポリシーに従って、オブジェクトデータの追加のコピーの作成をただちに開始します。

ただし、オブジェクトの ILM ルールでコピーを 1 つだけ作成するよう指定されていて、そのコピーが失われた場合、オブジェクトをリカバリすることはできません。この場合は、を実行します `Object_Lost` コマンドは、失われたオブジェクトのメタデータをStorageGRID システムからパージします。

をクリックします `Object_Lost` コマンドが正常に完了すると、次のメッセージが返されます。

```
CLOC_LOST_ANS returned result 'SUCS'
```

+

。 `/proc/CMSI/Object_Lost` コマンドは、アーカイブノードに格納されている損失オブジェクトに対してのみ有効です。

a. ADEコンソールを終了します。 `exit`

b. アーカイブノードからログアウトします。 `exit`

5. StorageGRID システムで、要求の失敗回数の値をリセットします。

a. アーカイブノード* ARC * Retrieve * **Configuration** *に移動し、 Reset Request Failure Count *を選択します。

b. [ 変更の適用 *] をクリックします。

関連情報

"StorageGRID の管理"

"監査ログを確認します"

**VMware**：仮想マシンの自動再起動の設定

## VMware vSphere ハイパーバイザーの再起動後に仮想マシンが再起動しない場合は、仮想マシンが自動で再起動するように設定する必要があります。

グリッドノードのリカバリ中または別のメンテナンス手順 の実行中に仮想マシンが再起動しない場合は、この手順 を実行する必要があります。

手順

1. VMware vSphere Client ツリーで、起動されていない仮想マシンを選択します。
2. 仮想マシンを右クリックし、 * 電源オン * を選択します。
3. 仮想マシンが自動的に再起動されるように、 VMware vSphere ハイパーバイザーを設定します。

# グリッドノードの手順

特定のグリッドノードで作業を実行する必要がある場合があります。これらの手順の一部は Grid Manager から実行できますが、ほとんどの手順ではノードのコマンドラインから Server Manager にアクセスする必要があります。

Server Manager はすべてのグリッドノード上で実行されてサービスの開始と停止を管理し、 StorageGRID システムでサービスが正常に開始および終了するようにします。また、すべてのグリッドノードのサービスを監視し、エラーが報告された場合は自動的に再開を試みます。

> Server Manager には、テクニカルサポートから指示があった場合にのみアクセスしてください。

> Server Manager での作業が完了したら、現在のコマンドシェルセッションを閉じてログアウトする必要があります。入力するコマンド `exit`

選択肢

- "Server Managerのステータスとバージョンの表示"
- "すべてのサービスの現在のステータスを表示しています"
- "Server Managerおよびすべてのサービスを開始しています"
- "Server Managerおよびすべてのサービスを再起動しています"
- "Server Managerおよびすべてのサービスを停止しています"
- "サービスの現在のステータスを表示します"
- "サービスを停止しています"
- "アプライアンスをメンテナンスモードにします"
- "サービスを強制的に終了します"
- "サービスの開始または再開"
- "ポートの再マッピングの削除"
- "ベアメタルホストでのポートの再マッピングの削除"
- "グリッドノードのリブート"
- "グリッドノードをシャットダウンしています"
- "ホストの電源のオフ"
- "グリッド内のすべてのノードの電源のオンとオフを切り替えます"
- "DoNotStartファイルを使用する"
- "Server Managerのトラブルシューティング"

## **Server Manager**のステータスとバージョンの表示

グリッドノードごとに、そのグリッドノード上で実行されている Server Manager の現在のステータスとバージョンを表示できます。そのグリッドノード上で実行されているすべてのサービスの現在のステータスも取得できます。

必要なもの

を用意しておく必要があります `Passwords.txt` ファイル。

手順

1. グリッドノードにログインします。

   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`

   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。

   c. 次のコマンドを入力してrootに切り替えます。 `su -`

   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

   rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

2. グリッドノード上で実行されているServer Managerの現在のステータスを表示します。 **`service servermanager status`**

   グリッドノード上で実行されている Server Manager の現在のステータスが（実行中かどうかに関係なく）報告されます。Server Managerのステータスがの場合 `running`は、最後に起動されてから実行されている時刻を示しています。例：

   ```
   servermanager running for 1d, 13h, 0m, 30s
   ```

   このステータスは、ローカルコンソールディスプレイのヘッダーに表示されるステータスと同じです。

3. グリッドノード上で実行されているServer Managerの現在のバージョンを表示します。 **`service servermanager version`**

   現在のバージョンが表示されます。例：

   ```
   11.1.0-20180425.1905.39c9493
   ```

4. コマンドシェルからログアウトします。 **`exit`**

すべてのサービスの現在のステータスを表示しています

## グリッドノード上で実行されているすべてのサービスの現在のステータスはいつでも表示できます。

必要なもの

を用意しておく必要があります `Passwords.txt` ファイル。

手順

1. グリッドノードにログインします。

   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`

b. に記載されているパスワードを入力します `Passwords.txt` ファイル。

c. 次のコマンドを入力してrootに切り替えます。 `su -`

d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

2. グリッドノード上で実行されているすべてのサービスのステータスを表示します。 `storagegrid-status`

   たとえば、プライマリ管理ノードの出力には、 AMS 、 CMN 、および NMS の各サービスの現在のステータスが実行中と表示されます。この出力は、サービスのステータスが変わるとすぐに更新されます。

```
Host Name                      190-ADM1
IP Address
Operating System Kernel        4.9.0          Verified
Operating System Environment   Debian 9.4     Verified
StorageGRID Webscale Release   11.1.0         Verified
Networking                                    Verified
Storage Subsystem                             Verified
Database Engine                5.5.9999+default Running
Network Monitoring             11.1.0         Running
Time Synchronization           1:4.2.8p10+dfsg Running
ams                            11.1.0         Running
cmn                            11.1.0         Running
nms                            11.1.0         Running
ssm                            11.1.0         Running
mi                             11.1.0         Running
dynip                          11.1.0         Running
nginx                          1.10.3         Running
tomcat                         8.5.14         Running
grafana                        4.2.0          Running
mgmt api                       11.1.0         Running
prometheus                     1.5.2+ds       Running
persistence                    11.1.0         Running
ade exporter                   11.1.0         Running
attrDownPurge                  11.1.0         Running
attrDownSamp1                  11.1.0         Running
attrDownSamp2                  11.1.0         Running
node exporter                  0.13.0+ds      Running
```

3. コマンドラインに戻り、 * Ctrl * + * C * を押します。

4. 必要に応じて、グリッドノード上で実行されているすべてのサービスに関する静的レポートを表示します。 `/usr/local/servermanager/reader.rb`

   このレポートには、継続的に更新されるレポートと同じ情報が含まれますが、サービスのステータスが変わっても更新されません。

5. コマンドシェルからログアウトします。 `exit`

**Server Manager**およびすべてのサービスを開始しています

## Server Manager の起動が必要な場合があります。 Server Manager を起動すると、グリッドノード上のすべてのサービスも開始されます。

必要なもの

を用意しておく必要があります `Passwords.txt` ファイル。

このタスクについて

Server Manager がすでに実行されているグリッドノードで Server Manager を起動すると、 Server Manager が再起動し、グリッドノード上のすべてのサービスが再開されます。

手順

1. グリッドノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

   rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。
2. Server Managerを起動します。 `service servermanager start`
3. コマンドシェルからログアウトします。 `exit`

**Server Manager**およびすべてのサービスを再起動しています

## グリッドノード上で実行されている Server Manager およびすべてのサービスの再起動が必要になる場合があります。

必要なもの

を用意しておく必要があります `Passwords.txt` ファイル。

手順

1. グリッドノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

   rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。
2. グリッドノード上のServer Managerおよびすべてのサービスを再開します。 `service servermanager restart`

   グリッドノード上の Server Manager およびすべてのサービスが停止され、その後再開されます。

   > を使用する `restart` コマンドは、を使用する場合と同じです `stop` コマンドのあとにを入力します `start` コマンドを実行します
3. コマンドシェルからログアウトします。 `exit`

## Server Managerおよびすべてのサービスを停止しています

Server Manager は常時実行中であることが前提ですが、あるグリッドノードで実行されている Server Manager およびすべてのサービスの停止が必要になる場合もあります。

必要なもの

を用意しておく必要があります `Passwords.txt` ファイル。

このタスクについて

オペレーティングシステムを実行したままServer Managerを停止する必要がある唯一のシナリオは、Server Managerを他のサービスに統合する必要がある場合です。ハードウェアの保守やサーバの再設定のためにServer Managerを停止する必要がある場合は、サーバ全体を停止する必要があります。

手順

1. グリッドノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

   rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。
2. グリッドノード上で実行されているServer Managerおよびすべてのサービスを停止します。 `service servermanager stop`

   グリッドノードで実行されている Server Manager およびすべてのサービスが正常に終了します。サービスのシャットダウンには最大 15 分かかる場合があります。
3. コマンドシェルからログアウトします。 `exit`

## サービスの現在のステータスを表示します

グリッドノード上で実行されているサービスの現在のステータスはいつでも表示できます。

必要なもの

を用意しておく必要があります `Passwords.txt` ファイル。

手順

1. グリッドノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

2. グリッドノード上で実行されているサービスの現在のステータスを表示します。「 * SERVICE_SERVICE_STATUS * 」グリッドノード上で実行されている要求されたサービスの現在のステータスが報告されます（実行中かどうかは関係ありません）。例：

```
cmn running for 1d, 14h, 21m, 2s
```

3. コマンドシェルからログアウトします。 **`exit`**

サービスを停止しています

## 一部のメンテナンス手順では、グリッドノード上の他のサービスを実行したまま、単一のサービスを停止する必要があります。個々のサービスの停止は、メンテナンス手順 から指示があった場合にのみ実行してください。

必要なもの

を用意しておく必要があります `Passwords.txt` ファイル。

このタスクについて

これらの手順を使用してサービスを「管理上停止」すると、 Server Manager は自動的にサービスを再開しません。サービスを手動で開始するか、 Server Manager を再起動する必要があります。

ストレージノード上の LDR サービスを停止する必要がある場合は、アクティブな接続があると、サービスの停止に時間がかかることがあります。

手順

1. グリッドノードにログインします。

   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`

   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。

   c. 次のコマンドを入力してrootに切り替えます。 `su -`

   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

   rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

2. 個 々 のサービスを停止します。 `service servicename stop`

   例：

```
service ldr stop
```

   サービスの停止には最大 11 分かかる場合があります。

3. コマンドシェルからログアウトします。 `exit`

関連情報

"サービスを強制的に終了します"

アプライアンスをメンテナンスモードにします

# 特定のメンテナンス手順を実行する前に、アプライアンスをメンテナンスモードにする必要があります。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Maintenance または Root Access 権限が必要です。詳細については、 StorageGRID の管理手順を参照してください。

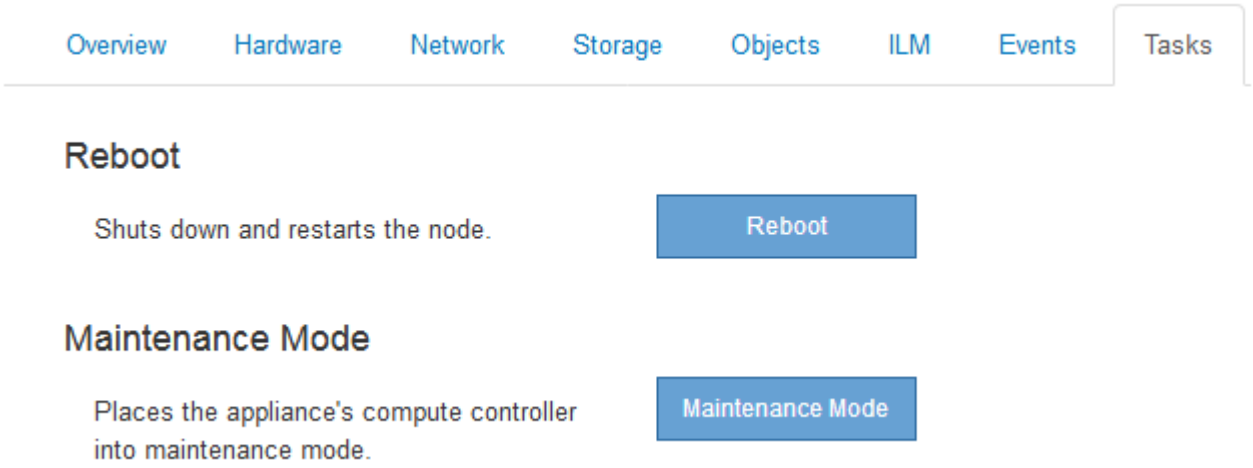
このタスクについて

StorageGRID アプライアンスをメンテナンスモードにすると、アプライアンスにリモートアクセスできなくなることがあります。

保守モードのStorageGRID アプライアンスのパスワードおよびホスト・キーは、アプライアンスが稼働していたときと同じままです。

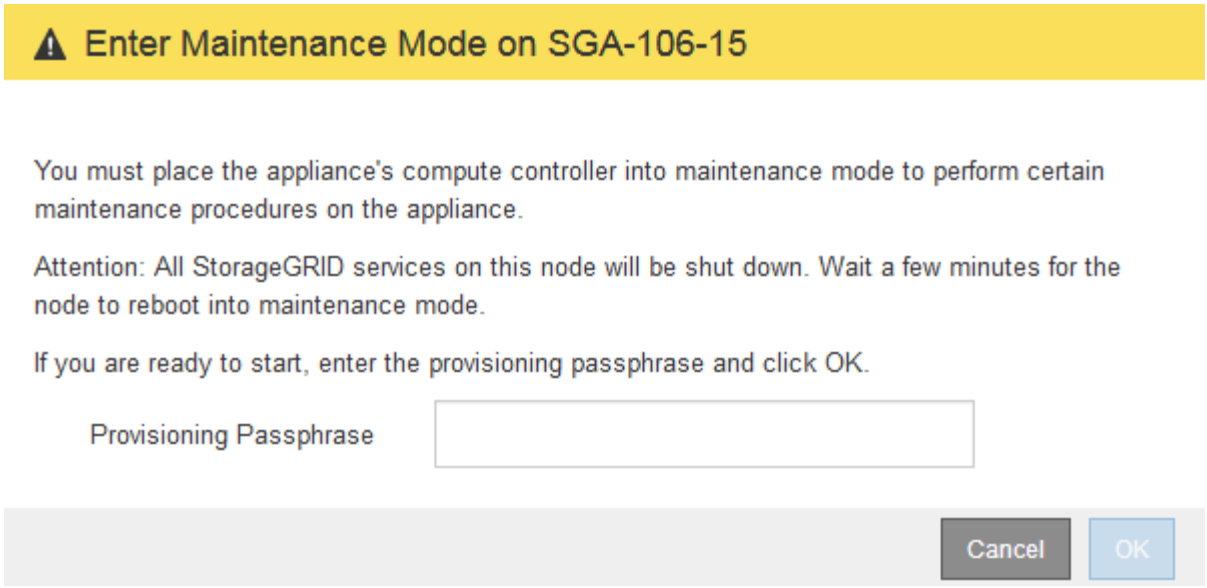
手順

1. Grid Managerから* Nodes *を選択します。
2. Nodes ページのツリービューで、アプライアンスストレージノードを選択します。
3. [ タスク ] を選択します。



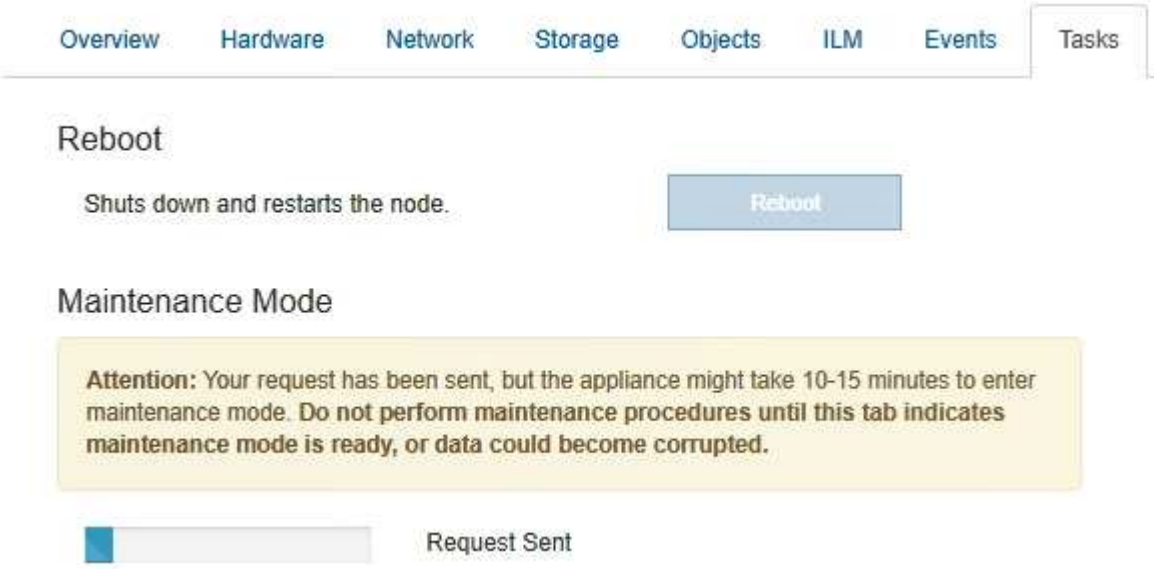

4. [* Maintenance Mode]*を選択します。

   確認のダイアログボックスが表示されます。

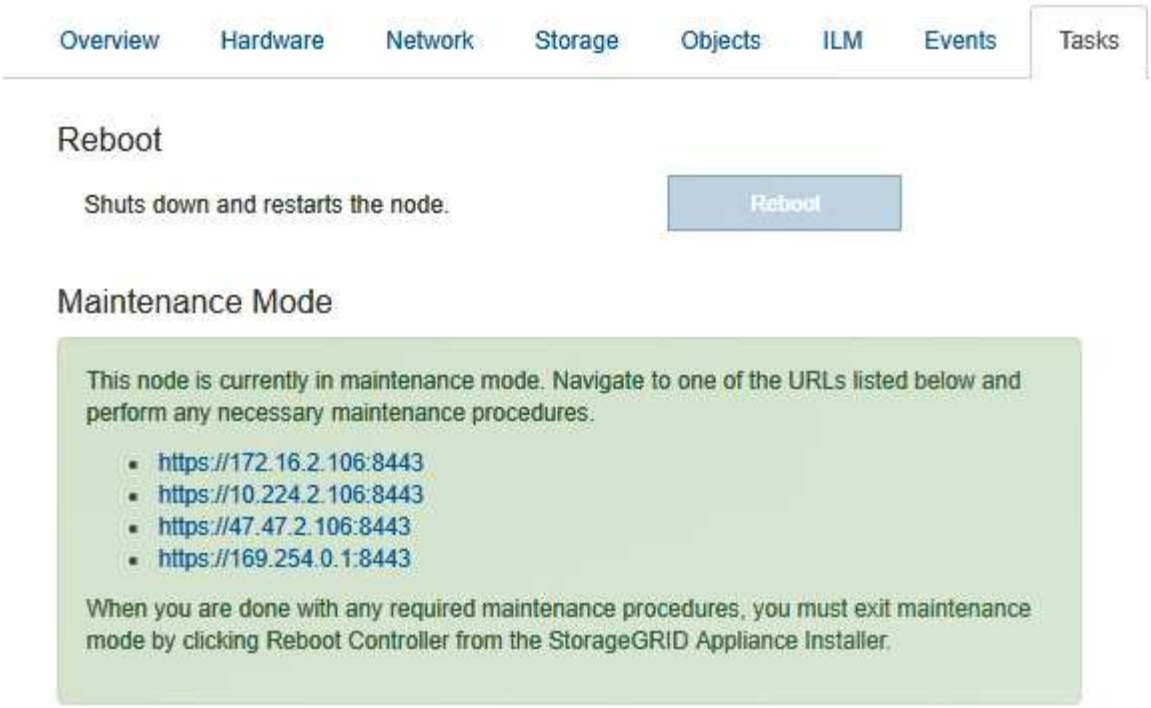



5. プロビジョニングパスフレーズを入力し、「 * OK 」を選択します。

進捗状況バーと「 Request Sent 」、「 Stopping StorageGRID 」、「 Rebaling 」などの一連のメッセージは、アプライアンスがメンテナンスモードに入るための手順を完了していることを示しています。




アプライアンスがメンテナンスモードになっている場合は、 StorageGRID アプライアンスインストーラへのアクセスに使用できる URL が確認メッセージに表示されます。



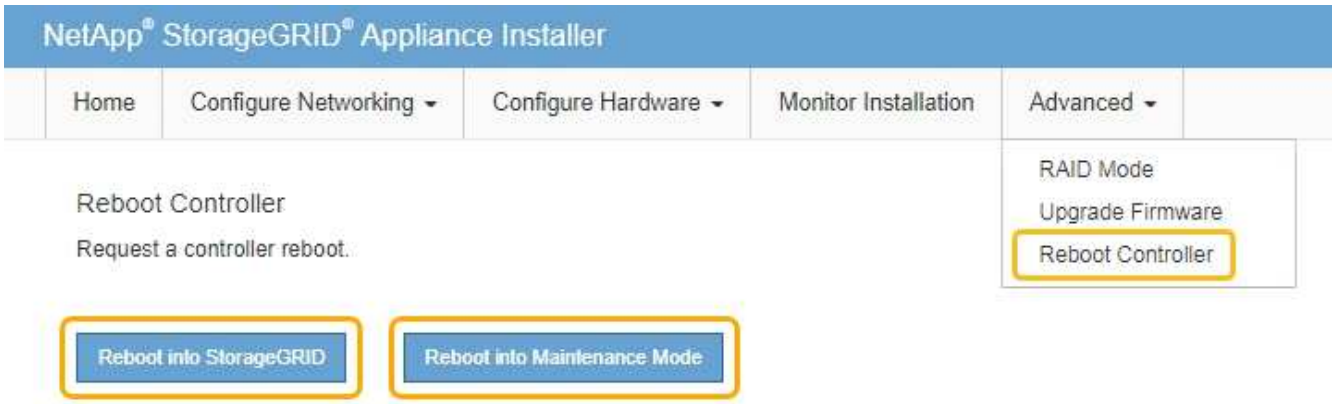

6. StorageGRID アプライアンスインストーラにアクセスするには、表示されたいずれかの URL にアクセスします。

   可能であれば、アプライアンスの管理ネットワークポートの IP アドレスを含む URL を使用します。

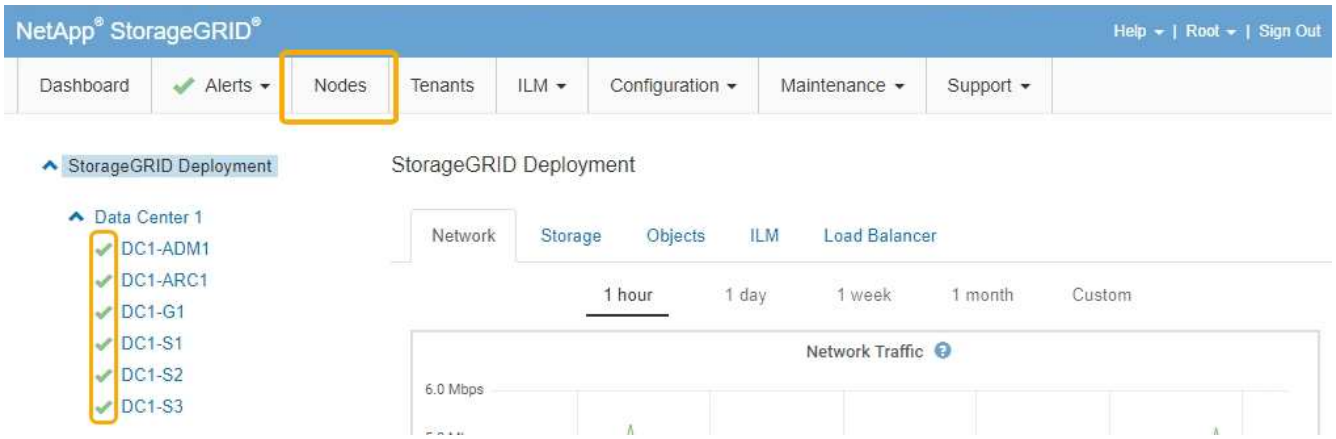
   > へのアクセス `https://169.254.0.1:8443` ローカル管理ポートに直接接続する必要があります。

7. StorageGRID アプライアンスインストーラで、アプライアンスがメンテナンスモードになっていることを確認します。

8. 必要なメンテナンスタスクを実行します。
9. メンテナンス作業が完了したら、メンテナンスモードを終了して通常のノードの運用を再開します。StorageGRID アプライアンス・インストーラから、 **Advanced**>* Reboot Controller* を選択し、 * Reboot into StorageGRID * を選択します。




アプライアンスがリブートしてグリッドに再参加するまでに最大 20 分かかることがあります。リブートが完了し、ノードが再びグリッドに参加したことを確認するには、 Grid Manager に戻ります。[ノード*（Nodes *）]タブには、通常のステータスが表示されます ✔ アクティブなアラートがなく、ノードがグリッドに接続されていることを示す、アプライアンスノードの場合。




サービスを強制的に終了します

## サービスをすぐに停止する必要がある場合は、を使用できます `force-stop` コマンドを実行します

必要なもの

を用意しておく必要があります `Passwords.txt` ファイル。

手順

1. グリッドノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

2. サービスを手動で強制終了します。 `service servicename force-stop`

   例：

   ```
   service ldr force-stop
   ```

   システムは 30 秒待機してからサービスを終了します。

3. コマンドシェルからログアウトします。 `exit`

サービスの開始または再開

## 停止されたサービスの開始や、サービスの停止と再開が必要になる場合があります。

必要なもの
を用意しておく必要があります `Passwords.txt` ファイル。

手順

1. グリッドノードにログインします。

   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

   rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

2. サービスが現在実行されているか停止されているかに基づいて、問題 に対するコマンドを決定します。

   - サービスが現在停止している場合は、を使用します `start` サービスを手動で開始するコマンド。
     `service servicename start`

     例：

     ```
     service ldr start
     ```

   - サービスが現在実行中の場合は、を使用します `restart` サービスを停止して再起動するコマンド。
     `service servicename restart`

     例：

```
service ldr restart
```

+

を使用する `restart` コマンドは、を使用する場合と同じです `stop` コマンドのあとにを入力します `start` コマンドを実行します問題 を実行できます `restart` サービスが現在停止している場合も同様です。

3. コマンドシェルからログアウトします。 `exit`

ポートの再マッピングの削除

## ロードバランササービスのエンドポイントを設定する場合、ポートの再マッピングのマッピング先ポートとしてすでに設定されているポートを使用するには、まず既存のポートの再マッピングを削除する必要があります。そうしないと、エンドポイントが有効になりません。ノードのすべてのポートの再マッピングを削除するには、再マッピングされたポートが競合している各管理ノードおよびゲートウェイノードでスクリプトを実行する必要があります。

この手順 は、ポートの再マッピングをすべて削除します。一部の再マッピングを保持する必要がある場合は、テクニカルサポートにお問い合わせください。

ロードバランサエンドポイントの設定については、 StorageGRID の管理手順を参照してください。

ポートの再マッピングでクライアントアクセスが提供される場合は、可能であればロードバランサエンドポイントとして設定した別のポートを使用するようにクライアントを再設定してください。そうしないと、ポートマッピングを削除してクライアントアクセスが失われるため、適切にスケジュールを設定する必要があります。

この手順 は、ベアメタルホスト上のコンテナとして導入した StorageGRID システムでは機能しません。ベアメタルホストでのポートの再マッピングの削除手順を参照してください。

手順

1. ノードにログインします。
   a. 次のコマンドを入力します。 `ssh -p 8022 admin@node_IP`

      ポート8022はベースOSのSSHポートで、ポート22はStorageGRID を実行しているDockerコンテナのSSHポートです。

   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

      rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

2. 次のスクリプトを実行します。 `remove-port-remap.sh`
3. ノードをリブートします。

グリッドノードのリブート手順に従ってください。

4. 再マッピングされたポートが競合している管理ノードおよびゲートウェイノードごとに上記の手順を繰り返します。

関連情報

"StorageGRID の管理"

"グリッドノードのリブート"

"ベアメタルホストでのポートの再マッピングの削除"

ベアメタルホストでのポートの再マッピングの削除

ロードバランササービスのエンドポイントを設定する場合、ポートの再マッピングのマッピング先ポートとしてすでに設定されているポートを使用するには、まず既存のポートの再マッピングを削除する必要があります。そうしないと、エンドポイントが有効になりません。ベアメタルホストで StorageGRID を実行している場合は、ポートの再マッピングを削除する一般的な手順 ではなく、この手順 に従ってください。ノードのすべてのポートの再マッピングを削除してノードを再起動するには、再マッピングされたポートが競合している各管理ノードおよびゲートウェイノードのノード構成ファイルを編集する必要があります。

この手順 は、ポートの再マッピングをすべて削除します。一部の再マッピングを保持する必要がある場合は、テクニカルサポートにお問い合わせください。

ロードバランサエンドポイントの設定については、 StorageGRID の管理手順を参照してください。

この手順 では、ノードの再起動時にサービスが一時的に失われる可能性があります。

手順

1. ノードをサポートしているホストにログインします。root として、または sudo 権限を持つアカウントでログインします。
2. 次のコマンドを実行して、ノードを一時的に無効にします。 `sudo storagegrid node stop node-name`
3. vim や pico などのテキストエディタを使用して、ノードのノード構成ファイルを編集します。

   ノード構成ファイルは、にあります `/etc/storagegrid/nodes/node-name.conf`。

4. ノード構成ファイルで、ポートの再マッピングが含まれているセクションを探します。

   次の例の最後の 2 行を参照してください。

```
ADMIN_NETWORK_CONFIG = STATIC
ADMIN_NETWORK_ESL = 10.0.0.0/8, 172.19.0.0/16, 172.21.0.0/16
ADMIN_NETWORK_GATEWAY = 10.224.0.1
ADMIN_NETWORK_IP = 10.224.5.140
ADMIN_NETWORK_MASK = 255.255.248.0
ADMIN_NETWORK_MTU = 1400
ADMIN_NETWORK_TARGET = eth1
ADMIN_NETWORK_TARGET_TYPE = Interface
BLOCK_DEVICE_VAR_LOCAL = /dev/sda2
CLIENT_NETWORK_CONFIG = STATIC
CLIENT_NETWORK_GATEWAY = 47.47.0.1
CLIENT_NETWORK_IP = 47.47.5.140
CLIENT_NETWORK_MASK = 255.255.248.0
CLIENT_NETWORK_MTU = 1400
CLIENT_NETWORK_TARGET = eth2
CLIENT_NETWORK_TARGET_TYPE = Interface
GRID_NETWORK_CONFIG = STATIC
GRID_NETWORK_GATEWAY = 192.168.0.1
GRID_NETWORK_IP = 192.168.5.140
GRID_NETWORK_MASK = 255.255.248.0
GRID_NETWORK_MTU = 1400
GRID_NETWORK_TARGET = eth0
GRID_NETWORK_TARGET_TYPE = Interface
NODE_TYPE = VM_API_Gateway
<strong>PORT_REMAP = client/tcp/8082/443</strong>
<strong>PORT_REMAP_INBOUND = client/tcp/8082/443</strong>
```

5. PORT_REMAP エントリと PORT_REMAP_INBOUND エントリを編集して、ポートの再マッピングを削除します。

```
PORT_REMAP =
PORT_REMAP_INBOUND =
```

6. 次のコマンドを実行して、ノードのノード構成ファイルに対する変更を検証します。 `sudo storagegrid node validate node-name`

   エラーや警告がある場合は、次の手順に進む前に対処してください。

7. 次のコマンドを実行して、ポートの再マッピングを使用せずにノードを再起動します。 `sudo storagegrid node start node-name`
8. に記載されているパスワードを使用して、ノードにadminとしてログインします `Passwords.txt` ファイル。
9. サービスが正しく開始されることを確認します。
   a. サーバ上のすべてのサービスのステータスのリストを表示します。`sudo storagegrid-status`

ステータスは自動的に更新されます。

b. すべてのサービスのステータスが「 Running 」または「 Verified 」になるまで待ちます。

c. ステータス画面を終了します。`Ctrl+C`

10. 再マッピングされたポートが競合している管理ノードおよびゲートウェイノードごとに上記の手順を繰り返します。

グリッドノードのリブート

# グリッドノードは、 Grid Manager またはノードのコマンドシェルからリブートできます。

このタスクについて

グリッドノードをリブートすると、ノードがシャットダウンして再起動します。すべてのサービスが自動的に再開されます。

ストレージノードをリブートする場合は、次の点に注意してください。

- ILM ルールに取り込み動作に Dual commit が指定されている場合、またはルールで Balanced が指定されていて、必要なすべてのコピーをただちに作成できない場合は、 StorageGRID は新たに取り込まれたオブジェクトをただちに同じサイトの 2 つのストレージノードにコミットしてあとから ILM を評価します。1 つのサイトで複数のストレージノードをリブートすると、リブート中はこれらのオブジェクトにアクセスできない場合があります。
- ストレージノードのリブート中もすべてのオブジェクトにアクセスできるようにするには、ノードをリブートする前に、サイトでのオブジェクトの取り込みを約 1 時間停止します。

関連情報

"StorageGRID の管理"

選択肢

- "グリッドノードのリブート- Grid Managerから"
- "グリッドノードのリブート-コマンドシェルから実行しています"

グリッドノードのリブート**- Grid Manager**から

# Grid Managerからグリッドノードをリブートすると、が実行されます `reboot` ターゲットノードでコマンドを実行します。

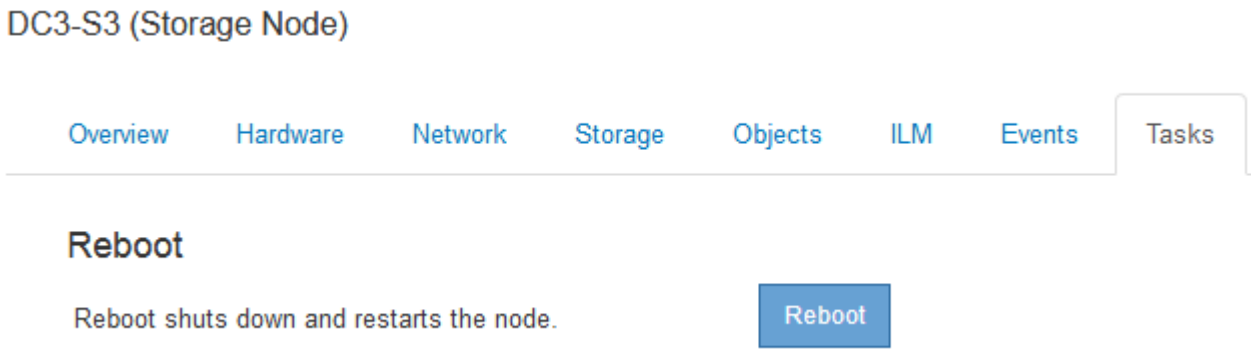
必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Maintenance または Root Access 権限が必要です。
- プロビジョニングパスフレーズが必要です。

手順

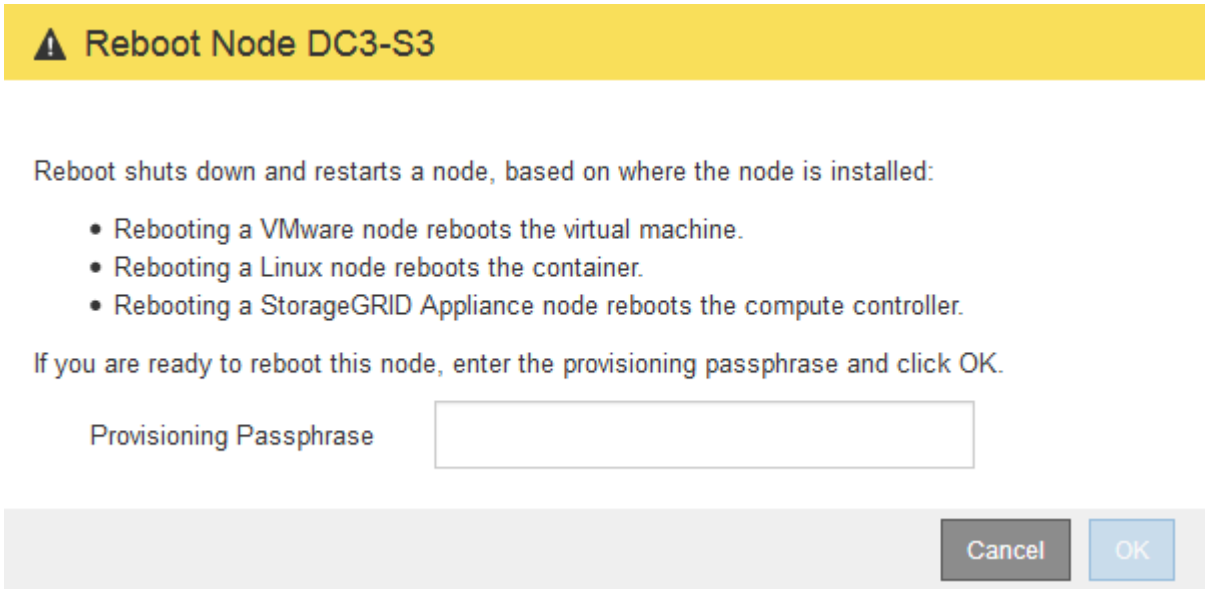
1. [ノード（ Nodes）]を選択し
2. リブートするグリッドノードを選択します。

3. [* タスク * （ Tasks * ） ] タブを選択します。




4. [Reboot]をクリックします。

確認のダイアログボックスが表示されます。




プライマリ管理ノードをリブートすると、サービスの停止中はブラウザと Grid Manager の接続が一時的に失われることを知らせる確認ダイアログボックスが表示されます。

5. プロビジョニングパスフレーズを入力し、 * OK * をクリックします。
6. ノードがリブートするまで待ちます。

サービスがシャットダウンするまでに時間がかかる場合があります。

ノードのリブート中は、Nodesページの左側にグレーのアイコン（Administratively Down）が表示されます。すべてのサービスが再び開始されると、アイコンは元の色に戻ります。

グリッドノードのリブート-コマンドシェルから実行しています

リブート処理を詳細に監視する必要がある場合や Grid Manager にアクセスできない場合は、グリッドノードにログインしてコマンドシェルから Server Manager の reboot コ

マンドを実行できます。

必要なもの

- を用意しておく必要があります `Passwords.txt` ファイル。

手順

1. グリッドノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

   rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。
2. 必要に応じて、サービスを停止します。 `service servermanager stop`

   サービスの停止は任意ですが、実行することを推奨します。サービスのシャットダウンには最大 15 分かかる場合があります。次の手順でノードをリブートする前に、リモートからシステムにログインしてシャットダウンプロセスを監視することもできます。
3. グリッドノードをリブートします。 `reboot`
4. コマンドシェルからログアウトします。 `exit`

グリッドノードをシャットダウンしています

## グリッドノードは、ノードのコマンドシェルからシャットダウンできます。

必要なもの

- を用意しておく必要があります `Passwords.txt` ファイル。

このタスクについて

この手順 を実行する前に、次の考慮事項を確認してください。

- 通常は、業務の中断を避けるために、一度に複数のノードをシャットダウンすることは避けてください。
- ドキュメントまたはテクニカルサポートから指示があった場合を除き、メンテナンス手順 の実行中にノードをシャットダウンしないでください。
- シャットダウンプロセスは、ノードがインストールされている場所によって次のように異なります。
  - VMware ノードをシャットダウンすると、仮想マシンがシャットダウンされます。
  - Linux ノードをシャットダウンすると、コンテナがシャットダウンされます。
  - StorageGRID アプライアンスノードをシャットダウンすると、コンピューティングコントローラがシャットダウンされます。
- ストレージノードをシャットダウンする場合は、次の点に注意してください。
  - ILM ルールに取り込み動作に Dual commit が指定されている場合、またはルールで Balanced が指定されていて、必要なすべてのコピーをただちに作成できない場合は、 StorageGRID は新たに取り込ま

れたオブジェクトをただちに同じサイトの 2 つのストレージノードにコミットしてあとから ILM を評価します。1 つのサイトで複数のストレージノードをシャットダウンすると、シャットダウン中はこれらのオブジェクトにアクセスできない場合があります。

- ストレージノードのシャットダウン中もすべてのオブジェクトにアクセスできるようにするには、ノードをシャットダウンする前に、サイトでのオブジェクトの取り込みを約 1 時間停止します。

手順

1. グリッドノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

   rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

2. すべてのサービスを停止します。 `service servermanager stop`

   サービスのシャットダウンには最大 15 分かかる場合があります。リモートからシステムにログインしてシャットダウンプロセスを監視することもできます。

3. コマンドシェルからログアウトします。 `exit`

シャットダウンしたら、グリッドノードの電源をオフにすることができます。

"ホストの電源のオフ"

関連情報

"StorageGRID の管理"

ホストの電源のオフ

## ホストの電源をオフにする前に、そのホスト上のすべてのグリッドノードのサービスを停止する必要があります。

手順

1. グリッドノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

   rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

2. ノードで実行中のすべてのサービスを停止します。 `service servermanager stop`

   サービスのシャットダウンには最大 15 分かかる場合があります。リモートからシステムにログインして

シャットダウンプロセスを監視することもできます。

3. ホストの各ノードについて、手順 1 と 2 を繰り返します。
4. Linux ホストの場合：
   a. ホストオペレーティングシステムにログインします。
   b. ノードを停止します。 `storagegrid node stop`
   c. ホストオペレーティングシステムをシャットダウンします。
5. VMware仮想マシンで実行さ問題 れているノード、またはアプライアンスノードの場合、shutdownコマンドを使用します。 `shutdown -h now`

   この手順は、の結果に関係なく実行します `service servermanager stop` コマンドを実行します

   > 問題 を実行した後 `shutdown -h now` アプライアンスノードでコマンドを実行するには、アプライアンスの電源を再投入してノードを再起動する必要があります。

   アプライアンスの場合、このコマンドはコントローラをシャットダウンしますが、アプライアンスの電源はオンになったままです。次の手順を実行する必要があります。

6. アプライアンスノードの電源をオフにする場合は、次の手順を実行します。
   - SG100 または SG1000 サービスアプライアンスの場合
     i. アプライアンスの電源をオフにします。
     ii. 青色の電源 LED が消灯するまで待ちます。
   - SG6000 アプライアンスの場合
     i. ストレージコントローラの背面にある緑のキャッシュアクティブ LED が消灯するまで待ちます。

     この LED は、キャッシュデータをドライブに書き込む必要があるときに点灯します。この LED が消灯するのを待ってから、電源をオフにする必要があります。

     ii. アプライアンスの電源をオフにし、青色の電源 LED が消灯するまで待ちます。
   - SG5700 アプライアンスの場合
     i. ストレージコントローラの背面にある緑のキャッシュアクティブ LED が消灯するまで待ちます。

     この LED は、キャッシュデータをドライブに書き込む必要があるときに点灯します。この LED が消灯するのを待ってから、電源をオフにする必要があります。

     ii. アプライアンスの電源をオフにし、すべての LED とデジタル表示ディスプレイの動作が停止するまで待ちます。
7. コマンドシェルからログアウトします。 `exit`

関連情報

"SG100 SG1000サービスアプライアンス"

"SG6000 ストレージアプライアンス"

"SG5700 ストレージアプライアンス"

# データセンターの移行などで、 StorageGRID システム全体のシャットダウンが必要になる場合があります。ここでは、通常の方法でシャットダウンと起動を実行する場合の推奨手順について、その概要を記載します。

サイトまたはグリッド内のすべてのノードの電源をオフにすると、ストレージノードがオフラインの間は、取り込んだオブジェクトにアクセスできなくなります。

## サービスを停止してグリッドノードをシャットダウンしています

# StorageGRID システムの電源をオフにするには、各グリッドノードの実行中のすべてのサービスを停止してから、VMware仮想マシン、Dockerコンテナ、StorageGRID アプライアンスをすべてシャットダウンする必要があります。

### このタスクについて

可能であれば、次の順序でグリッドノードのサービスを停止してください。

- 最初に、ゲートウェイノードのサービスを停止します。
- 最後に、プライマリ管理ノードのサービスを停止します。

この方法なら、プライマリ管理ノードを使用して他のグリッドノードのステータスをできるだけ長く監視できます。

> 単一のホストに複数のグリッドノードが含まれている場合は、そのホスト上のすべてのノードを停止するまで、ホストをシャットダウンしないでください。ホストにプライマリ管理ノードが含まれている場合は、そのホストを最後にシャットダウンします。

> 必要に応じて、特定のLinuxホストから別のLinuxホストにノードを移行し、グリッドの機能や可用性に影響を与えずにホストのメンテナンスを実行できます。

"Linux：新しいホストへのグリッドノードの移行"

### 手順

1. すべてのクライアントアプリケーションからグリッドへのアクセスを停止します。
2. [[log_in_on_gn] ][ 各ゲートウェイノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

      rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。
3. [[stop_all_services]ノード上で実行されているすべてのサービスを停止します。 `service servermanager stop`

サービスのシャットダウンには最大 15 分かかる場合があります。リモートからシステムにログインしてシャットダウンプロセスを監視することもできます。

4. 上記の 2 つの手順を繰り返して、すべてのストレージノード、アーカイブノード、非プライマリ管理ノードのサービスを停止します。

   これらのノードのサービスは、どの順序で停止してもかまいません。

   > 問題 を実行する場合は、を参照して `service servermanager stop` コマンド：アプライアンスストレージノードのサービスを停止するには、アプライアンスの電源を再投入してノードを再起動する必要があります。

5. プライマリ管理ノードについて、の手順を繰り返します ノードにログインします および ノードのすべてのサービスを停止しています。

6. Linux ホストで実行されているノードの場合：

   a. ホストオペレーティングシステムにログインします。

   b. ノードを停止します。 `storagegrid node stop`

   c. ホストオペレーティングシステムをシャットダウンします。

7. VMware仮想マシンで実行されているノードおよびアプライアンスストレージノードの場合問題は、shutdownコマンドを使用します。 `shutdown -h now`

   この手順は、の結果に関係なく実行します `service servermanager stop` コマンドを実行します

   アプライアンスの場合、このコマンドはコンピューティングコントローラをシャットダウンしますが、アプライアンスの電源はオンになったままです。次の手順を実行する必要があります。

8. アプライアンスノードがある場合：

   - SG100 または SG1000 サービスアプライアンスの場合
     i. アプライアンスの電源をオフにします。
     ii. 青色の電源 LED が消灯するまで待ちます。
   - SG6000 アプライアンスの場合
     i. ストレージコントローラの背面にある緑のキャッシュアクティブ LED が消灯するまで待ちます。

     この LED は、キャッシュデータをドライブに書き込む必要があるときに点灯します。この LED が消灯するのを待ってから、電源をオフにする必要があります。

     ii. アプライアンスの電源をオフにし、青色の電源 LED が消灯するまで待ちます。
   - SG5700 アプライアンスの場合
     i. ストレージコントローラの背面にある緑のキャッシュアクティブ LED が消灯するまで待ちます。

     この LED は、キャッシュデータをドライブに書き込む必要があるときに点灯します。この LED が消灯するのを待ってから、電源をオフにする必要があります。

     ii. アプライアンスの電源をオフにし、すべての LED とデジタル表示ディスプレイの動作が停止するまで待ちます。

9. 必要に応じて、コマンドシェルからログアウトします。 `exit`

   これで、 StorageGRID グリッドのシャットダウンは完了です。

関連情報

"SG100 SG1000サービスアプライアンス"

"SG6000 ストレージアプライアンス"

"SG5700 ストレージアプライアンス"

グリッドノードを起動しています

## グリッドノードを完全にシャットダウンしたあとに起動する際は、次の手順を実行してください。

> グリッド全体が 15 日以上シャットダウンされている場合は、グリッドノードを起動する前にテクニカルサポートに連絡する必要があります。Cassandra データを再構築するリカバリ手順は実行しないでください。データが失われる可能性があります。

このタスクについて

可能であれば、次の順序でグリッドノードの電源をオンにしてください。

- 最初に管理ノードの電源をオンにします。
- 最後にゲートウェイノードの電源をオンにします。

> ホストに複数のグリッドノードが含まれている場合は、ホストの電源をオンにすると各ノードが自動的にオンライン状態に戻ります。

手順

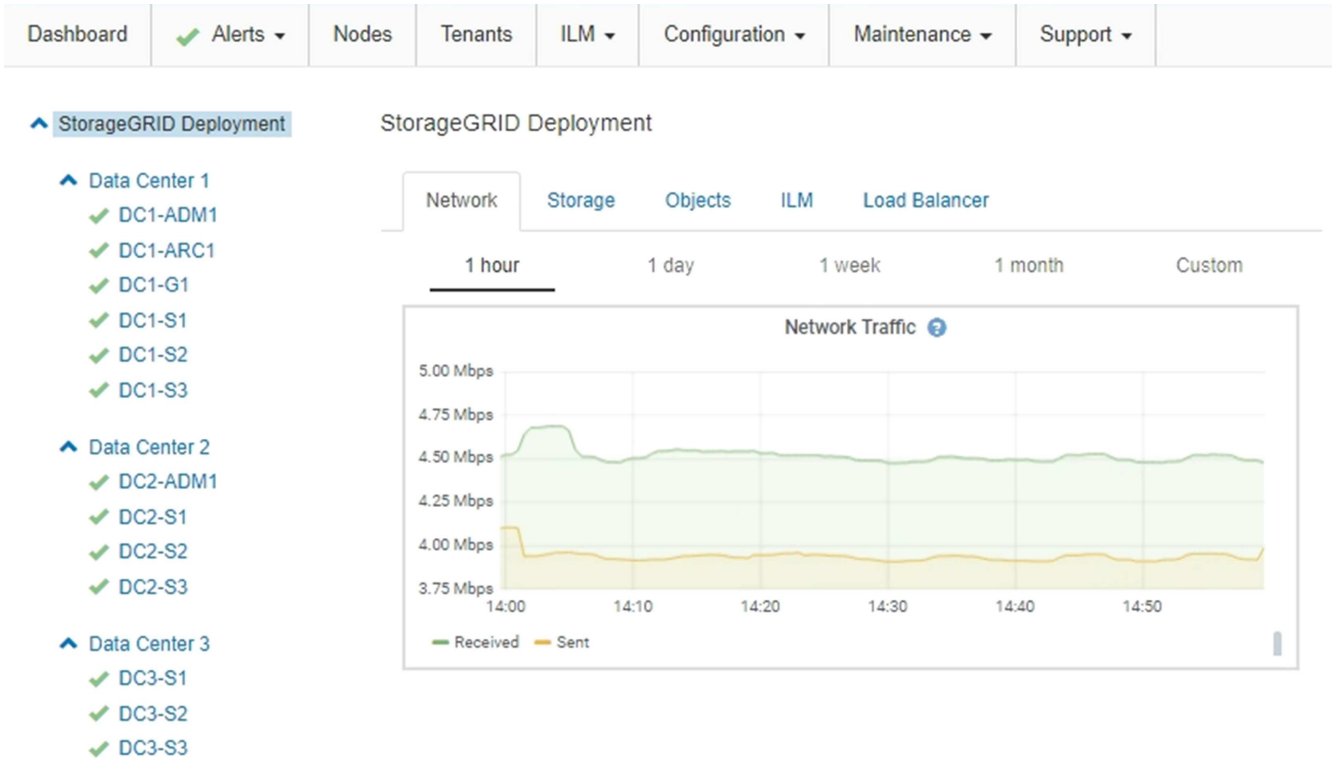
1. プライマリ管理ノードと非プライマリ管理ノードのホストの電源をオンにします。

   > ストレージノードの再起動が完了するまで、管理ノードにログインすることはできません。

2. すべてのアーカイブノードとストレージノードのホストの電源をオンにします。

   これらのノードは、どの順序で電源をオンにしてもかまいません。

3. すべてのゲートウェイノードのホストの電源をオンにします。
4. Grid Managerにサインインします。
5. ノード*をクリックして、グリッドノードのステータスを監視します。すべてのノードのステータスが「緑」に戻っていることを確認します。




**DoNotStart**ファイルを使用する

テクニカルサポートの指示の下でメンテナンスや設定の手順を実行している場合は、Server Manager の起動時または再起動時にサービスが開始されないように、DoNotStart ファイルを使用するよう求められることがあります。

DoNotStart ファイルは、テクニカルサポートから指示があった場合のみ追加または削除してください。

サービスが開始されないようにするには、そのサービスのディレクトリに DoNotStart ファイルを配置します。Server Manager は起動時に DoNotStart ファイルを検索し、ファイルが存在する場合、サービス（およびそれに依存するサービス）は開始されません。DoNotStart ファイルを削除すると、停止されていたサービスは、 Server Manager が次回起動または再起動したときに開始されます。DoNotStart ファイルを削除しても、サービスは自動的には開始されません。

すべてのサービスを再開しないようにする最も効率的な方法は、 NTP サービスを開始しないようにすることです。すべてのサービスは NTP サービスに依存しているため、 NTP サービスが実行されていない場合は実行できません。

サービスの**DoNotStart**ファイルを追加しています

個別のサービスが開始しないようにするには、グリッドノードのそのサービスのディレクトリに DoNotStart ファイルを追加します。

必要なもの

を用意しておく必要があります `Passwords.txt` ファイル。

手順

1. グリッドノードにログインします。

   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`

   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。

   c. 次のコマンドを入力してrootに切り替えます。 `su -`

   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

   rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

2. DoNotStartファイルを追加します。 `touch /etc/sv/service/DoNotStart`

   ここで、 `service` は、開始しないようにするサービスの名前です。例：

   ```
   touch /etc/sv/ldr/DoNotStart
   ```

   DoNotStart ファイルが作成されます。ファイルの内容は不要です。

   Server Manager またはグリッドノードが再起動されたときに Server Manager は再起動しますが、サービスは再開されません。

3. コマンドシェルからログアウトします。 `exit`

サービスの**DoNotStart**ファイルを削除しています

## サービスを開始できないようにする DoNotStart ファイルを削除するには、そのサービスを開始する必要があります。

必要なもの

を用意しておく必要があります `Passwords.txt` ファイル。

手順

1. グリッドノードにログインします。

   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`

   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。

   c. 次のコマンドを入力してrootに切り替えます。 `su -`

   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

   rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

2. サービスのディレクトリからDoNotStartファイルを削除します。 `rm /etc/sv/service/DoNotStart`

   ここで、 `service` は、サービスの名前です。例：

```
rm /etc/sv/ldr/DoNotStart
```

3. サービスを開始します。 `service servicename start`
4. コマンドシェルからログアウトします。 `exit`

**Server Manager**のトラブルシューティング

# テクニカルサポートから、Server Manager関連の問題の原因を突き止めるためにトラブルシューティングタスクの実行を指示される場合があります。

**Server Manager**ログファイルにアクセスします

## Server Manager の使用時に問題が発生した場合は、そのログファイルを確認します。

Server Managerに関連するエラーメッセージは、Server Managerログファイルに記録されます。このファイルは、次の場所にあります。 `/var/local/log/servermanager.log`

このファイルでエラーに関するエラーメッセージを確認してください。必要に応じて、問題 をテクニカルサポートにエスカレーションします。テクニカルサポートにログファイルを転送するよう求められる場合があります。

エラー状態のサービス

## サービスがエラー状態になったことが検出された場合は、サービスの再開を試みてください。

必要なもの

を用意しておく必要があります `Passwords.txt` ファイル。

このタスクについて

Server Manager は、サービスを監視し、予期せず停止したサービスがあれば再起動します。サービスで障害が発生すると、 Server Manager はそのサービスの再起動を試行します。5 分以内にサービスの開始が 3 回失敗すると、サービスはエラー状態になります。Server Manager は再起動を試行しません。

手順

1. グリッドノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

   rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。
2. サービスのエラー状態を確認します。 `service servicename status`

例：

```
service ldr status
```

サービスがエラー状態になっている場合は、次のメッセージが返されます。 *servicename* `in error state`。例：

```
ldr in error state
```

サービスステータスがの場合 `disabled`サービスのDoNotStartファイルの削除手順を参照してください。

3. サービスを再開して、エラー状態を解消します。 `service` *servicename* `restart`

   サービスを再開できない場合は、テクニカルサポートにお問い合わせください。

4. コマンドシェルからログアウトします。 `exit`

関連情報

"サービスのDoNotStartファイルを削除しています"

## アプライアンスノードのクローニング

StorageGRID でアプライアンスノードをクローニングして、アプライアンスの設計や機能を強化することができます。クローニングでは、既存のノード上のすべての情報が新しいアプライアンスに転送されます。ハードウェアのアップグレードプロセスを実行して簡単に実行できます。また、アプライアンスの運用停止や交換に代わる方法も提供されます。

### アプライアンスノードのクローニングの仕組み

アプライアンスノードのクローニングを使用すると、グリッド内の既存のアプライアンスノード（ソース）を、同じ論理 StorageGRID サイトに含まれる互換性のあるアプライアンス（ターゲット）に簡単に置き換えることができます。このプロセスでは、すべてのデータが新しいアプライアンスに転送され、古いアプライアンスノードを交換するためにアプライアンスが稼働中になり、古いアプライアンスは設置前の状態になります。

#### アプライアンスノードをクローニングする理由

アプライアンスノードは、次の処理が必要な場合にクローニングできます。

- 寿命が近づいているアプライアンスの交換
- 改善されたアプライアンステクノロジを活用するには、既存のノードをアップグレードしてください。
- StorageGRID システム内のストレージノードの数を変更することなく、グリッドのストレージ容量を拡張できます。

- RAID モードを DDP 8 から DDP 16 に変更する、 RAID 6 に変更するなどして、ストレージ効率を向上
- ノード暗号化を効率的に実装して、外部キー管理サーバ（ KMS ）を使用できるようにします。

どの **StorageGRID** ネットワークが使用されていますか？

クローニングでは、 3 つの StorageGRID ネットワークのいずれかで、ソースノードからターゲットアプライアンスにデータが直接転送されます。グリッドネットワークは通常は使用されますが、ソースアプライアンスがこれらのネットワークに接続されている場合は、管理ネットワークまたはクライアントネットワークも使用できます。StorageGRID ネットワークのパフォーマンスやデータの可用性を低下させることなく、最高のデータ転送パフォーマンスを提供するトラフィックのクローニングに使用するネットワークを選択してください。

交換用アプライアンスを設置するときは、 StorageGRID 接続およびデータ転送用の一時的な IP アドレスを指定する必要があります。交換用アプライアンスは交換前のアプライアンスノードと同じネットワークに含まれるため、交換用アプライアンスでこれらのネットワークごとに一時 IP アドレスを指定する必要があります。

ターゲットアプライアンスの互換性

交換用アプライアンスは、交換するソースノードと同じタイプで、両方が同じ論理 StorageGRID サイトに属している必要があります。

- 交換用サービスアプライアンスは、交換する管理ノードまたはゲートウェイノードとは異なる場合があります。
  - SG1000 サービスのターゲットアプライアンスに SG100 ソースノードアプライアンスをクローニングして、管理ノードまたはゲートウェイノードの機能を強化できます。
  - SG1000 ソースノードアプライアンスを SG100 サービスターゲットアプライアンスにクローニングして、要件の厳しいアプリケーション用に SG1000 を再導入することができます。

    たとえば、 SG1000 ソースノードアプライアンスを管理ノードとして使用していて、専用のロードバランシングノードとして使用する場合などです。

  - SG1000 ソースノードアプライアンスを SG100 サービスターゲットアプライアンスに交換すると、ネットワークポートの最大速度が 100GbE から 25GbE に減ります。
  - SG100 と SG1000 アプライアンスでは、ネットワークコネクタが異なります。アプライアンスのタイプを変更する場合は、ケーブルまたは SFP モジュールの交換が必要になることがあります。
- 交換用ストレージアプライアンスには、交換するストレージノード以上の容量が必要です。
  - ターゲットストレージアプライアンスのドライブ数がソースノードと同じ場合は、ターゲットアプライアンスのドライブの容量（ TB ）が同じかそれ以上である必要があります。
  - ターゲットストレージアプライアンスに設置されている標準ドライブ数がソースノードのドライブ数よりも少ない場合は、ソリッドステートドライブ（ SSD ）が設置されているため、ターゲットアプライアンスの標準ドライブの全体的なストレージ容量（ TB ）が表示されます。 ソースストレージノード内のすべてのドライブの機能的な合計ドライブ容量を満たしているか、超えている必要があります。

    たとえば、 60 本のドライブを搭載した SG5660 ソースストレージノードアプライアンスを 58 本の標準ドライブを搭載した SG6060 ターゲットアプライアンスにクローニングする場合は、クローニングを行ってストレージ容量を確保する前に、 SG6060 ターゲットアプライアンスに大容量のドライブを設置する必要があります。（ターゲットアプライアンス内の SSD を含む 2 つのドライブスロットは、アプライアンスのストレージ容量の合計には含まれません）。

ただし、 60 ドライブ SG5660 ソースノードアプライアンスが SANtricity Dynamic Disk Pools DDP -8 を使用して構成されている場合、 DDP 16 を使用した 58 ドライブの同じサイズのドライブ SG6060 ターゲットアプライアンスの設定によって、ストレージ効率が向上しているため、 SG6060 アプライアンスが有効なクローンターゲットになる可能性があります。

ソースアプライアンスノードの現在のRAIDモードに関する情報は、Grid Managerの* Nodes ページで確認できます。アプライアンスの **[*Storage]** タブを選択します。

#### クローニングされない情報

以下のアプライアンス設定は、クローニング中に交換用アプライアンスに転送されません。交換用アプライアンスの初期セットアップ時に設定する必要があります。

- BMC インターフェイス
- ネットワークリンク
- ノード暗号化ステータス
- SANtricity システムマネージャ（ストレージノード用）
- RAID モード（ストレージノード用）

#### クローニングの妨げとなる問題

クローニング中に次のいずれかの問題が発生すると、クローニングプロセスが停止し、エラーメッセージが生成されます。

- ネットワーク設定が正しくありません
- ソースとターゲットのアプライアンス間の接続が確立されていません
- ソースとターゲットのアプライアンスに互換性がない
- ストレージノードの場合は、容量の不十分な交換用アプライアンス

続行するには、クローニングのために各問題 を解決する必要があります。

### アプライアンスノードのクローニングに関する考慮事項と要件

アプライアンスノードをクローニングする前に、考慮事項と要件を理解しておく必要があります。

#### 交換用アプライアンスのハードウェア要件

交換用アプライアンスが次の基準を満たしていることを確認します。

- ソースノード（交換するアプライアンス）とターゲット（新しい）アプライアンスは、同じタイプのアプライアンスである必要があります。
  - クローニングできるのは、管理ノードアプライアンスまたはゲートウェイノードアプライアンスだけです。
  - クローニングできるのは、新しいストレージアプライアンスに対してのみです。
- 管理ノードまたはゲートウェイノードアプライアンスの場合、ソースノードアプライアンスとターゲット

アプライアンスで同じタイプのアプライアンスを使用する必要はありません。ただし、アプライアンスタイプを変更する場合は、ケーブルまたは SFP モジュールの交換が必要になることがあります。

たとえば、 SG1000 ノードアプライアンスを SG100 に交換したり、 SG100 アプライアンスを SG1000 アプライアンスに交換したりできます。

- ストレージノードアプライアンスの場合、ソースノードアプライアンスとターゲットアプライアンスのストレージ容量がソースアプライアンスと同じである必要はありません。ただし、ターゲットアプライアンスのストレージ容量はソースアプライアンスと同じかそれ以上である必要があります。

  たとえば、 SG5600 ノードアプライアンスを、 SG5700 アプライアンスまたは SG6000 アプライアンスと交換することができます。

StorageGRID 環境の特定のアプライアンスノードをクローニングする互換性のある交換用アプライアンスを選択する方法については、 StorageGRID の営業担当者にお問い合わせください。

### アプライアンスノードのクローンを作成する準備をしています

アプライアンスノードをクローニングするには、次の情報が必要です。

- グリッドネットワークの一時的な IP アドレスをネットワーク管理者から取得し、最初のインストール時にターゲットアプライアンスで使用します。ソースノードが管理ネットワークまたはクライアントネットワークに属している場合は、それらのネットワークの一時的な IP アドレスを取得します。

  一時的な IP アドレスは通常、クローニングするソースノードアプライアンスと同じサブネット上にあり、クローニングの完了後は必要ありません。クローニング接続を確立するには、ソースアプライアンスとターゲットアプライアンスの両方が StorageGRID のプライマリ管理ノードに接続されている必要があります。

- データ転送トラフィックのクローニングに使用するネットワークを決定し、 StorageGRID ネットワークのパフォーマンスやデータの可用性を低下させることなく、最高のデータ転送パフォーマンスを実現します。

  1GbE 管理ネットワークを使用したクローニングでデータ転送を行うと、クローニングに時間がかかります。

- ターゲットアプライアンスでキー管理サーバ（ KMS ）を使用したノード暗号化が使用されるかどうかを確認し、クローニングを実行する前に最初のターゲットアプライアンスインストール時にノードの暗号化を有効にできるようにします。アプライアンスのインストールの説明に従って、ソースアプライアンスノードでノード暗号化が有効になっているかどうかを確認できます。

  ソースノードとターゲットアプライアンスで、異なるノード暗号化設定を使用できます。データの復号化と暗号化は、データ転送中、およびターゲットノードが再起動してグリッドに参加したときに自動的に実行されます。

  - "SG100 SG1000サービスアプライアンス"
  - "SG5600 ストレージアプライアンス"
  - "SG5700 ストレージアプライアンス"
  - "SG6000 ストレージアプライアンス"

- ターゲット・アプライアンスの RAID モードをデフォルト設定から変更するかどうかを決定します。この

ため、この情報は、クローニングの前にターゲット・アプライアンスを最初にインストールするときに指定できます。ソースアプライアンスノードの現在のRAIDモードに関する情報は、Grid Managerの* Nodesページで確認できます。アプライアンスの **[*Storage]** タブを選択します。

ソースノードとターゲットアプライアンスでは、 RAID 設定が異なる場合があります。

- ノードのクローニングプロセスを完了するための十分な時間を計画します。稼働中のストレージノードからターゲットアプライアンスにデータを転送するために、数日かかる場合があります。クローニングのスケジュールを一度に設定して、ビジネスへの影響を最小限に抑えることができます。
- クローニングするアプライアンスノードは一度に 1 つだけにしてください。クローニングによって、StorageGRID の他のメンテナンス機能を同時に実行することはできません。
- アプライアンスノードのクローンを作成したら、互換性のある別のノードアプライアンスのクローンを作成するために、インストール前の状態に戻ったソースアプライアンスをターゲットとして使用できます。

アプライアンスノードの手順 クローニング

## ソースノード（交換するアプライアンス）とターゲット（新規）アプライアンスの間でデータを転送するには、クローニングプロセスに数日かかることがあります。

必要なもの

- 互換性のあるターゲットアプライアンスをキャビネットまたはラックに設置し、すべてのケーブルを接続し、電源を投入しておきます。
- 交換用アプライアンスの StorageGRID アプライアンスインストーラのバージョンが StorageGRID システムのソフトウェアバージョンと同じであることを確認し、必要に応じて StorageGRID アプライアンスインストーラファームウェアをアップグレードしておきます。
- StorageGRID 接続、 SANtricity System Manager （ストレージアプライアンスのみ）、 BMC インターフェイスの設定を含めて、ターゲットアプライアンスを設定しておきます。
  - StorageGRID 接続を設定する場合は、一時的な IP アドレスを使用します。
  - ネットワークリンクを設定する場合は、最終的なリンク設定を使用します。

> ターゲットアプライアンスの初期構成が完了したあとは、 StorageGRID アプライアンスインストーラを開いたままにしておきます。ノードのクローニングプロセスを開始したあとに、ターゲットアプライアンスのインストーラページに戻ります。

- ターゲットアプライアンスのノード暗号化を必要に応じて有効にしておきます。
- 必要に応じて、ターゲットアプライアンスの RAID モードを設定します（ストレージアプライアンスのみ）。
- "アプライアンスノードのクローニングに関する考慮事項と要件"

  "SG100 SG1000サービスアプライアンス"

  "SG5600 ストレージアプライアンス"

  "SG5700 ストレージアプライアンス"

  "SG6000 ストレージアプライアンス"

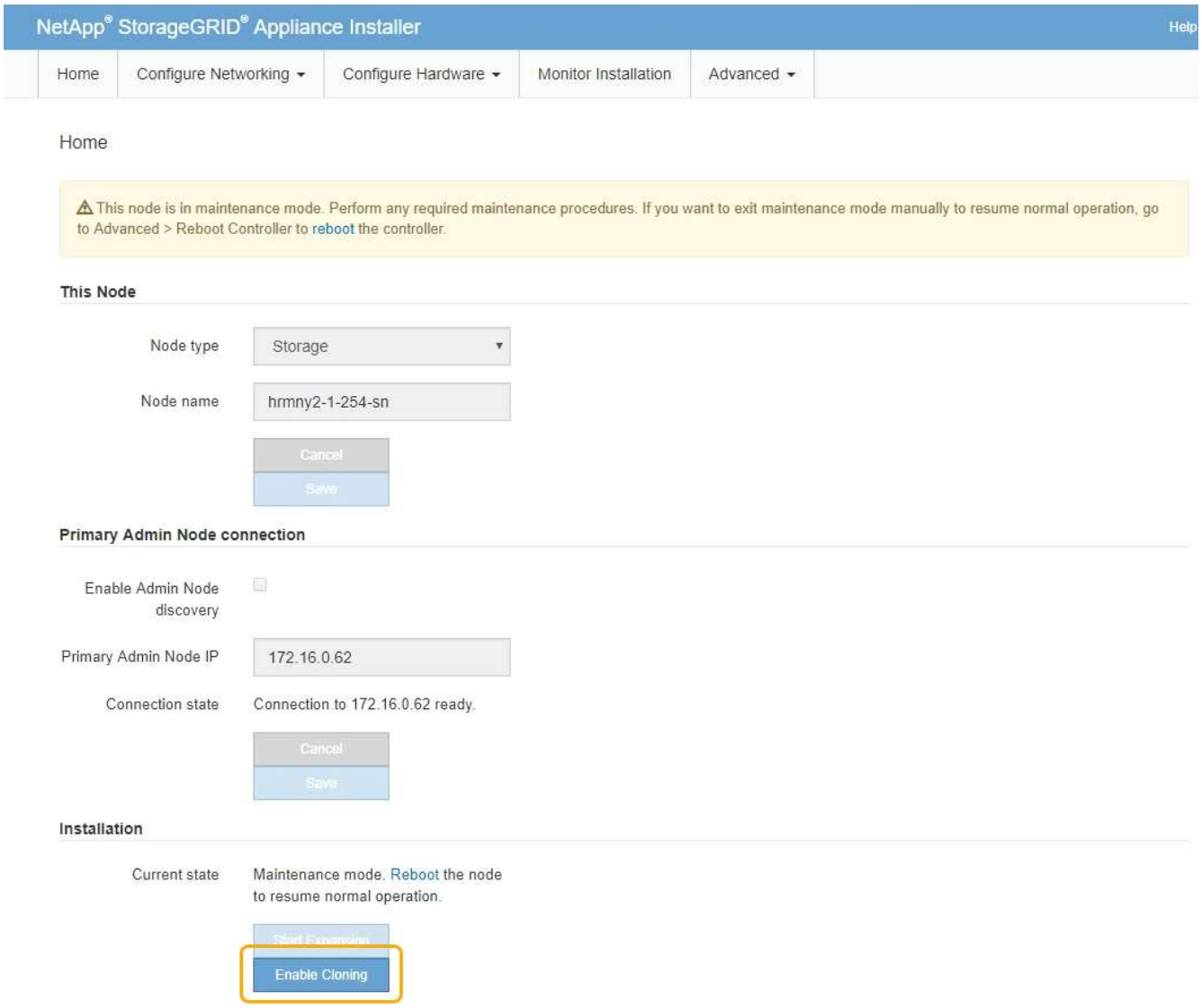
StorageGRID ネットワークのパフォーマンスとデータの可用性を維持するために、クローニングするアプライアンスノードは一度に 1 つだけにしてください。

手順

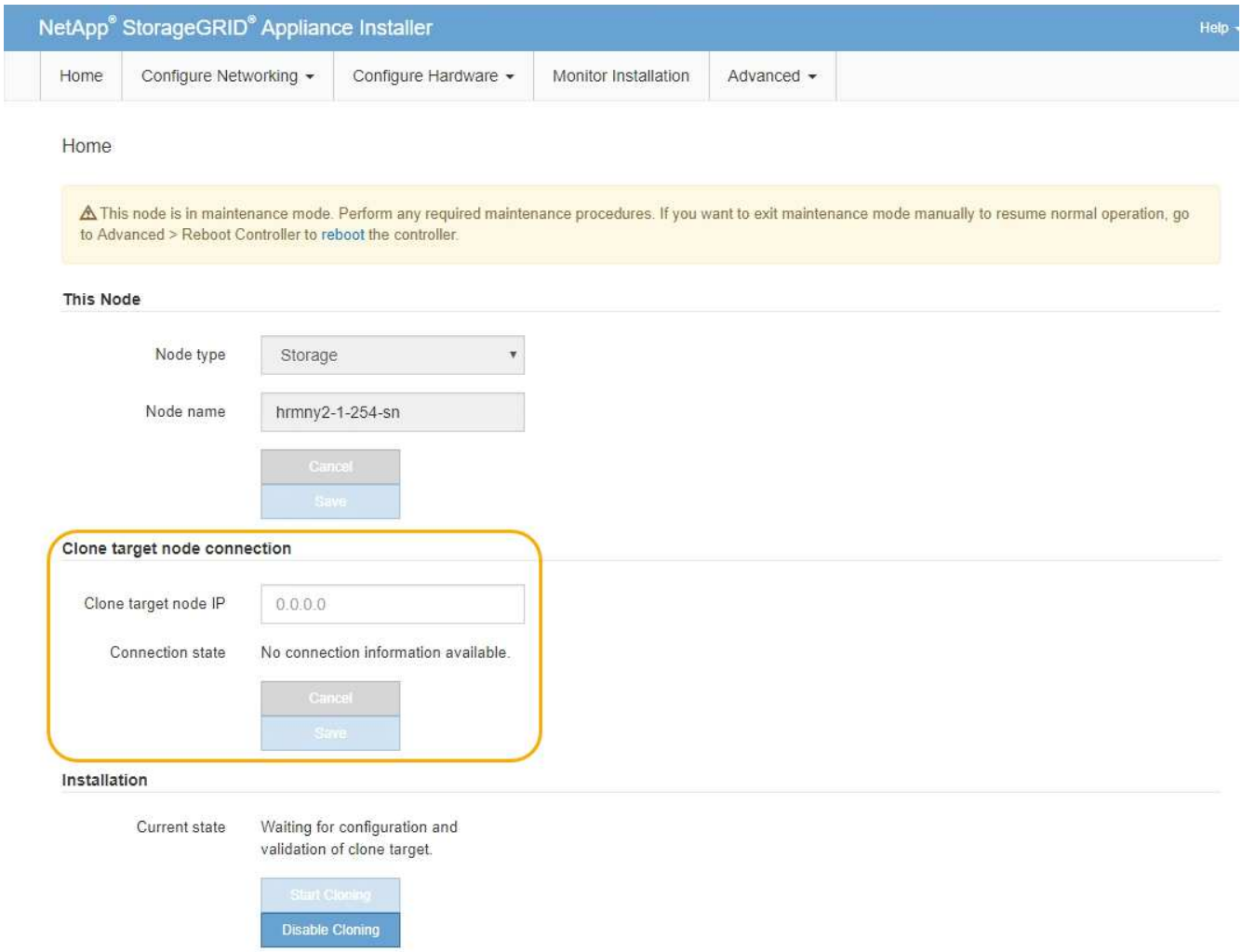
1. クローニングするソースノードをメンテナンスモードにします。

   "アプライアンスをメンテナンスモードにします"

2. ソースノードの StorageGRID アプライアンスインストーラのホームページの ［ インストール ］ セクションで、 ［ * クローン作成を有効にする * ］ を選択します。




Primary Admin Node connection セクションが Clone target node connection セクションに置き換えられました。

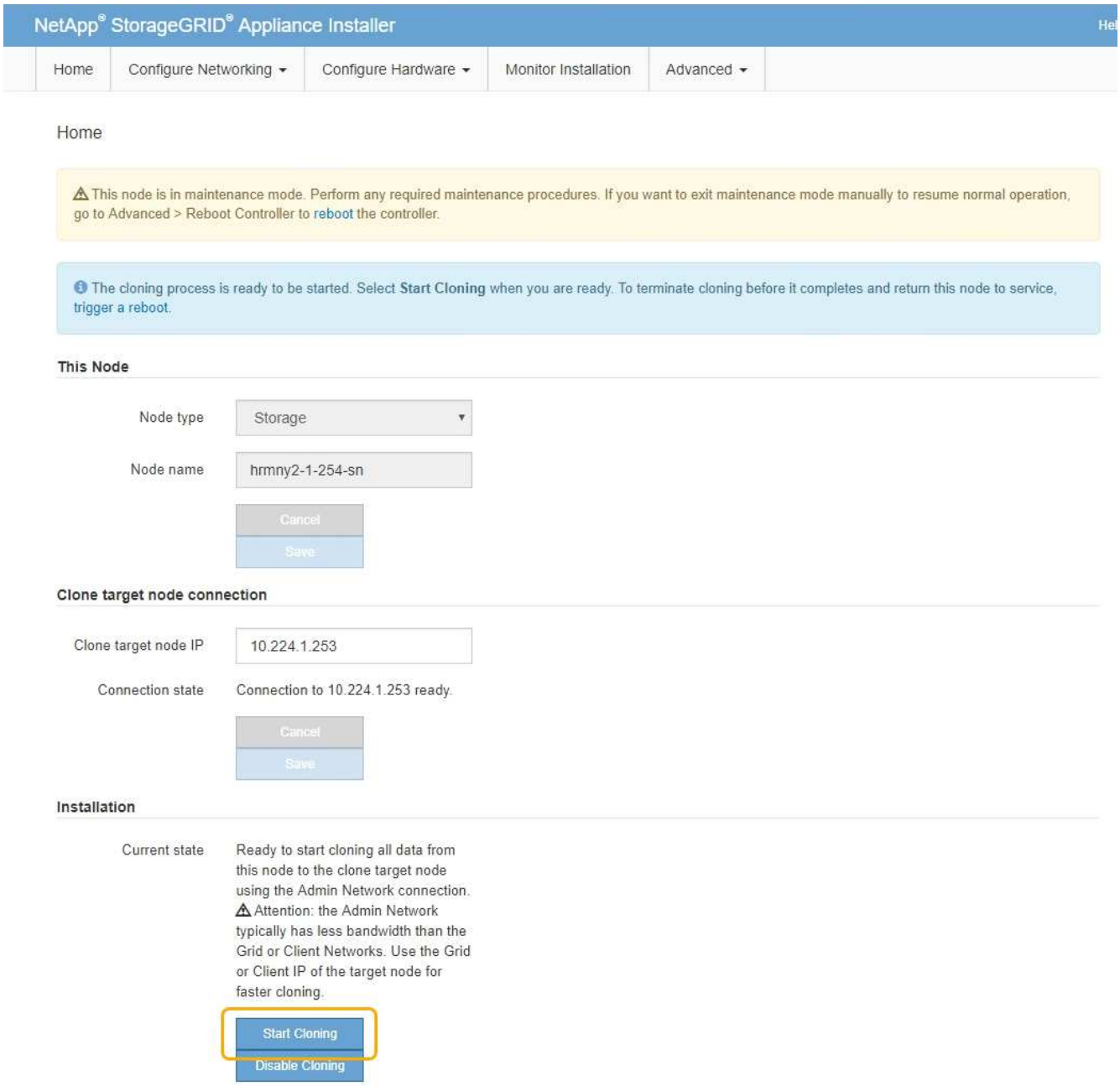



3. 「 * クローンターゲットノード IP * 」には、クローンデータ転送トラフィックに使用するネットワークのターゲットノードに割り当てられた一時的な IP アドレスを入力し、「 * 保存 * 」を選択します。

   通常はグリッドネットワークの IP アドレスを入力しますが、データ転送トラフィックのクローニングに別のネットワークを使用する必要がある場合は、そのネットワークのターゲットノードの IP アドレスを入力します。

   1GbE 管理ネットワークを使用したクローニングでデータ転送を行うと、クローニングに時間がかかります。

   ターゲットアプライアンスの設定と検証が完了すると、インストールセクションのソースノードで * クローニングの開始 * が有効になります。



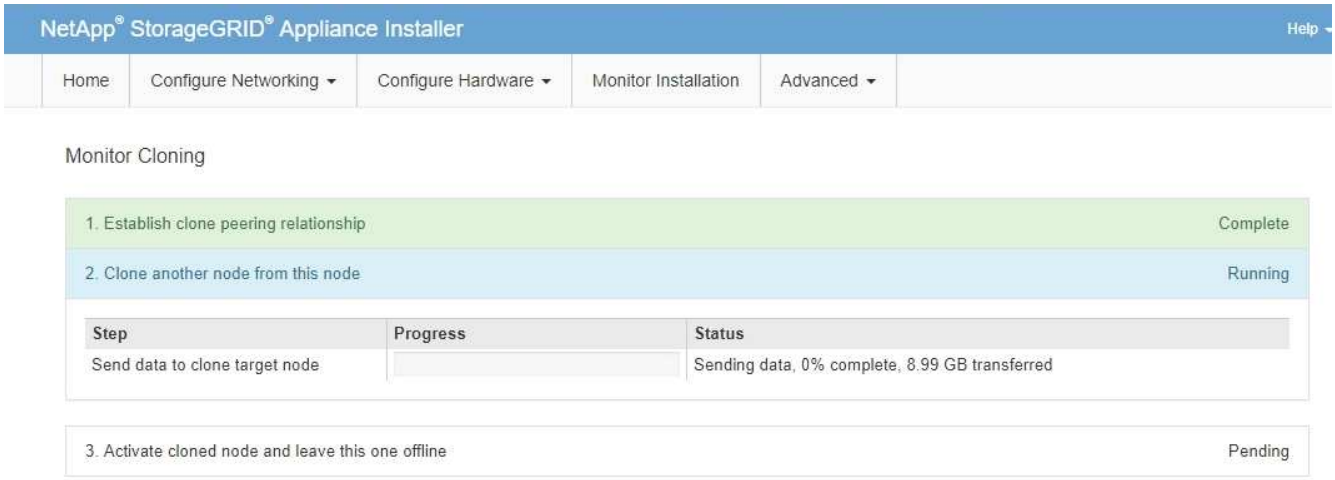

クローニングを妨げる問題が存在する場合は、 * クローニングの開始 * が有効になっておらず、解決が必要な問題が * 接続状態 * として表示されます。これらの問題は、ソースノードとターゲットアプライアンスの両方の StorageGRID アプライアンスインストーラのホームページに記載されています。一度に表示される問題 は 1 つだけで、条件の変化に応じて状態が自動的に更新されます。クローニングの開始 * を有効にするために、すべてのクローニングの問題を解決してください。

クローニングの開始 * が有効になっている場合、 * 現在の状態 * は、トラフィックのクローニングに選択された StorageGRID ネットワークと、そのネットワーク接続の使用に関する情報を示します。

"アプライアンスノードのクローニングに関する考慮事項と要件"

4. ソースノードで * クローニングを開始 * を選択します。
5. ソースノードまたはターゲットノードで StorageGRID アプライアンスインストーラを使用して、クローニングの進行状況を監視します。

ソースノードとターゲットノードの両方で StorageGRID アプライアンスインストーラのステータスが同じであることを確認します。




クローニングの監視ページでは、クローニングプロセスの各ステージについて詳細な進捗状況を確認できます。

- * クローンピア関係の確立 * に、クローニングのセットアップと設定の進捗状況が表示されます。
- * このノードから別のノードをクローニングする * と、データ転送の進捗状況が表示されます。（クローニング処理のこの処理は、完了までに数日かかることがあります）。
- * クローンノードをアクティブ化してこのノードをオフラインのままにする * は、データ転送が完了したあとに、ターゲットノードに制御を移行してインストール前の状態に移行する処理の進捗状況を示します。

6. クローニングが完了する前にクローニングプロセスを終了し、ソースノードをサービスに戻す必要がある場合は、ソースノードでStorageGRID アプライアンスインストーラのホームページに移動し、* Advanced * Reboot Controller を選択して、 Reboot into StorageGRID *を選択します。

   クローニングプロセスが終了した場合は、次の手順を実行し

   - ソースノードがメンテナンスモードを終了し、 StorageGRID に再び参加します。
   - ターゲットノードはインストール前の状態のままになります。ソースノードのクローニングを再開するには、手順 1 からクローニングプロセスを再開します。

クローニングが正常に完了した場合：

- ソースノードとターゲットノードで IP アドレスが入れ替わります。
  - これで、ターゲットノードで、グリッドネットワーク、管理ネットワーク、クライアントネットワークのソースノードに割り当てられていた IP アドレスが使用されるようになります。
  - ソースノードで、最初にターゲットノードに割り当てられた一時的な IP アドレスが使用されるようになります。
- ターゲットノードはメンテナンスモードを終了し、ソースノードに代わって StorageGRID に参加します。
- ソースアプライアンスは、再インストールの準備ができたかのように、インストール前の状態です。

  "再インストールのためのアプライアンスの準備（プラットフォームの交換のみ）"

アプライアンスがグリッドに再参加しない場合は、ソースノードのStorageGRID アプライアンスインストーラのホームページで「* Advanced * Reboot Controller 」を選択し、「 Reboot into Maintenance Mode *」を選択します。ソースノードが保守モードでリブートしたら、手順 のクローニングを繰り返します。

ターゲットノードで想定外の問題 が発生した場合、ユーザデータはリカバリオプションとしてソースアプライアンスに残ります。ターゲットノードが StorageGRID に正常に再参加すると、ソースアプライアンスのユーザデータは古くなり、不要になります。必要に応じて、 StorageGRID サポートにソースアプライアンスのクリアを依頼して、このデータを削除してください。

可能です

- 追加のクローニング処理では、ソースアプライアンスをターゲットとして使用します。追加の設定は必要ありません。このアプライアンスには、最初のクローンターゲット用に指定された一時的な IP アドレスがすでに割り当てられています。
- ソースアプライアンスを新しいアプライアンスノードとして設置し、セットアップする。
- ソースアプライアンスが StorageGRID で使用されなくなった場合は、破棄します。

# NetApp StorageGRIDのその他のバージョンのマニュアル

NetApp StorageGRID ソフトウェアの他のリリースのドキュメントは、次のURLから入手できます。

- "StorageGRID 11.9ドキュメント"
- "StorageGRID 11.8ドキュメント"
- "StorageGRID 11.7ドキュメント"
- "StorageGRID 11.6のドキュメント"
- "StorageGRID 11.4ドキュメントセンター"
- "StorageGRID 11.3ドキュメントセンター"
- "StorageGRID 11.2ドキュメントセンター"

# 法的通知

著作権に関する声明、商標、特許などにアクセスできます。

## 著作権

"https://www.netapp.com/company/legal/copyright/"

## 商標

NetApp 、 NetApp のロゴ、および NetApp の商標ページに記載されているマークは、 NetApp, Inc. の商標です。その他の会社名および製品名は、それぞれの所有者の商標である場合があります。

"https://www.netapp.com/company/legal/trademarks/"

## 特許

ネットアップが所有する特許の最新リストは、次のサイトで入手できます。

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

## プライバシーポリシー

"https://www.netapp.com/company/legal/privacy-policy/"

## オープンソース

通知ファイルには、ネットアップソフトウェアで使用されるサードパーティの著作権およびライセンスに関する情報が記載されています。

"StorageGRID 11.5に関する注意事項"

著作権に関する情報

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

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

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

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

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

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

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

商標に関する情報

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