はじめに
StorageGRID

NetApp
October 03, 2025

This PDF was generated from https://docs.netapp.com/ja-jp/storagegrid-116/primer/index.html on October 03, 2025. Always check docs.netapp.com for the latest.

目次

はじめに 1
グリッド入門 1
グリッド入門：概要 1
StorageGRID を使用したハイブリッドクラウド 3
StorageGRID のアーキテクチャとネットワークトポロジ 4
オブジェクト管理 15
StorageGRID の使用方法 26
ネットワークのガイドライン 70
ネットワークガイドライン：概要 70
StorageGRID のネットワークタイプ 71
ネットワークトポロジの例 75
ネットワーク要件 82
ネットワーク固有の要件 83
環境固有のネットワークに関する考慮事項 85
ネットワークのインストールとプロビジョニング 88
インストール後のガイドライン 89
ネットワークポートのリファレンス 89

はじめに

グリッド入門

グリッド入門：概要

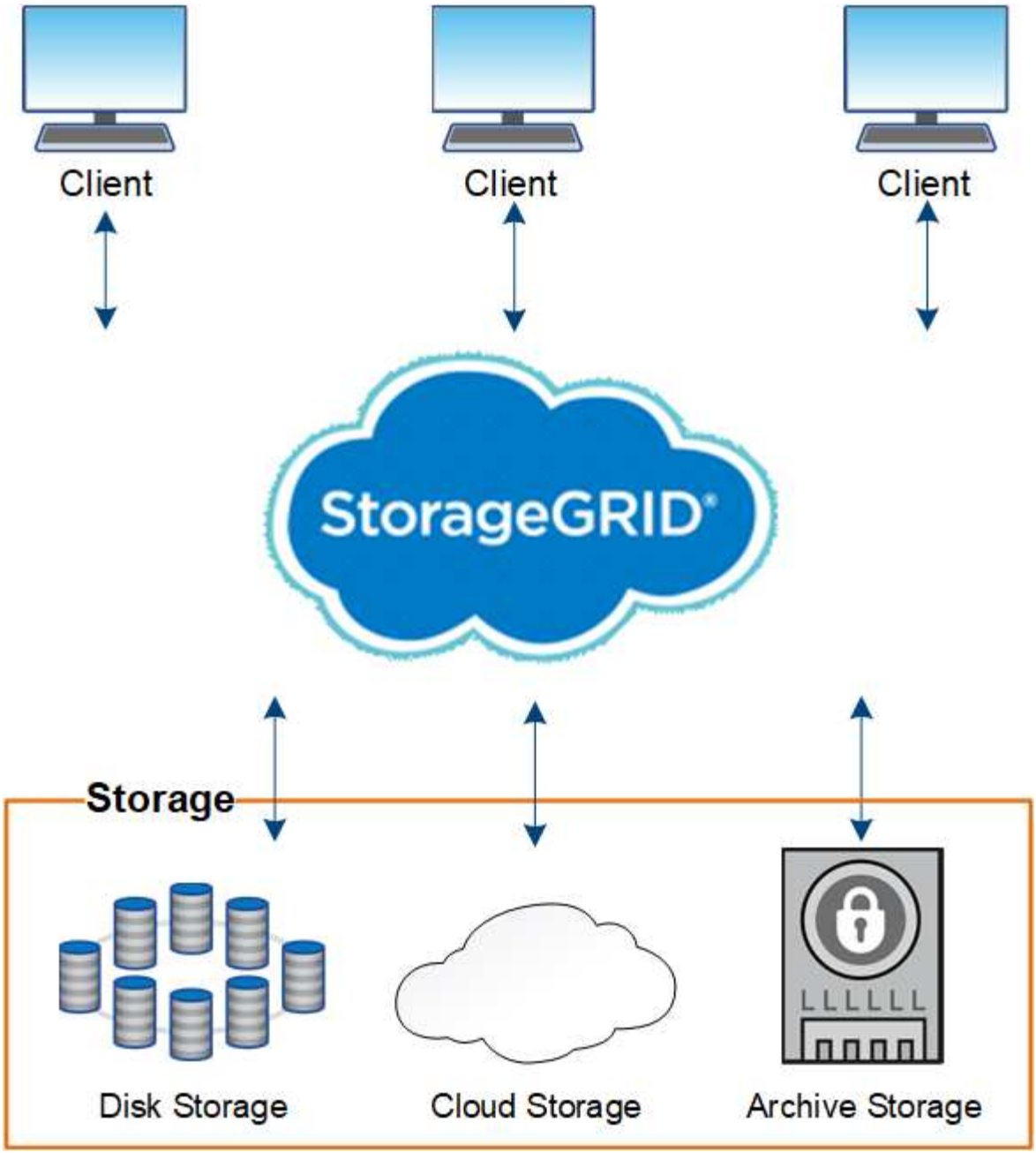
これらの概要を使用して、 StorageGRID システムの概要、および StorageGRID アーキテクチャとネットワークトポロジ、データ管理機能、ユーザインターフェイスについて説明します。

StorageGRID とは

NetApp®StorageGRID ®は、ソフトウェアで定義されるオブジェクトストレージスイートで、パブリック、プライベート、ハイブリッドのマルチクラウド環境での幅広いユースケースに対応します。StorageGRID はAmazon S3 APIをネイティブでサポートし、自動化されたライフサイクル管理などの業界をリードする革新的なテクノロジを提供して、非構造化データを長期にわたってコスト効率よく格納、保護、保持します。

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

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



StorageGRID システムには次の利点があります。

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

します。

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

StorageGRID を使用したハイブリッドクラウド

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

クラウドストレージプール

クラウドストレージプールを使用すると、 StorageGRID システムの外部にオブジェクトを格納できます。たとえば、 Amazon S3 Glacier 、 S3 Glacier Deep Archive 、 Microsoft Azure Blob Storage のアーカイブアクセス階層など、アクセス頻度の低いオブジェクトを低コストのクラウドストレージに移動できます。また、

StorageGRID オブジェクトのクラウドバックアップを保持しておくことで、ストレージボリュームやストレージノードの障害によって失われたデータをリカバリすることができます。

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

S3 プラットフォームサービス

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

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

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

StorageGRID による **ONTAP** データの階層化

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

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

関連情報

- StorageGRID の管理
- テナントアカウントを使用する
- ILM を使用してオブジェクトを管理する
- StorageGRID for FabricPool を設定します

StorageGRID のアーキテクチャとネットワークトポロジ

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

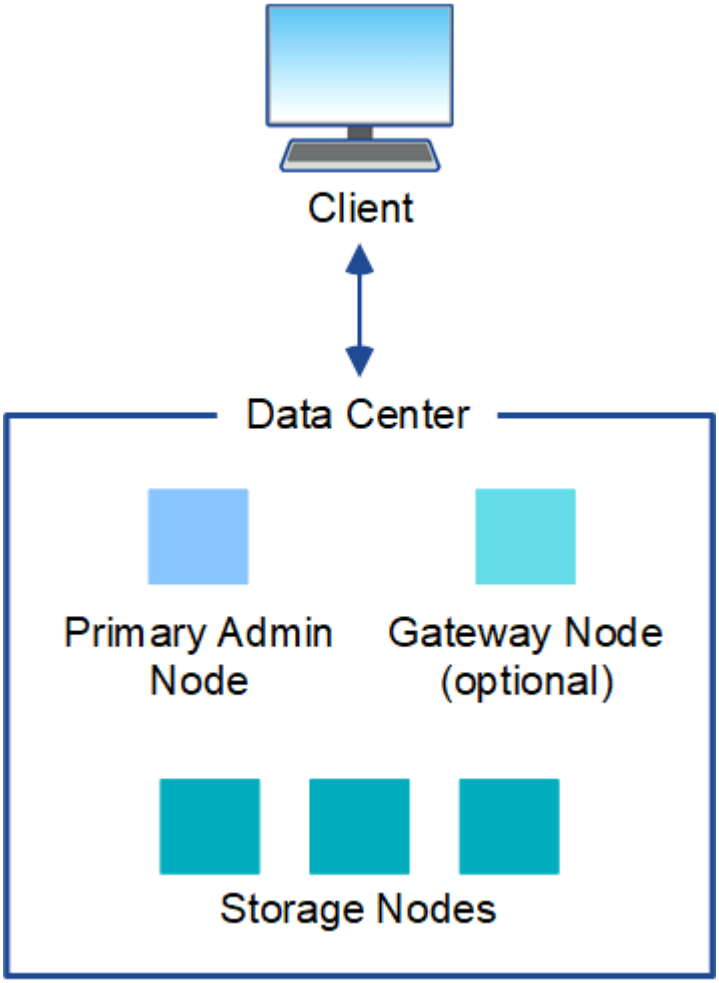
追加情報 の StorageGRID ネットワークトポロジ、要件、およびグリッド通信については、を参照してください ネットワークのガイドライン。

導入トポロジ

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

単一サイト

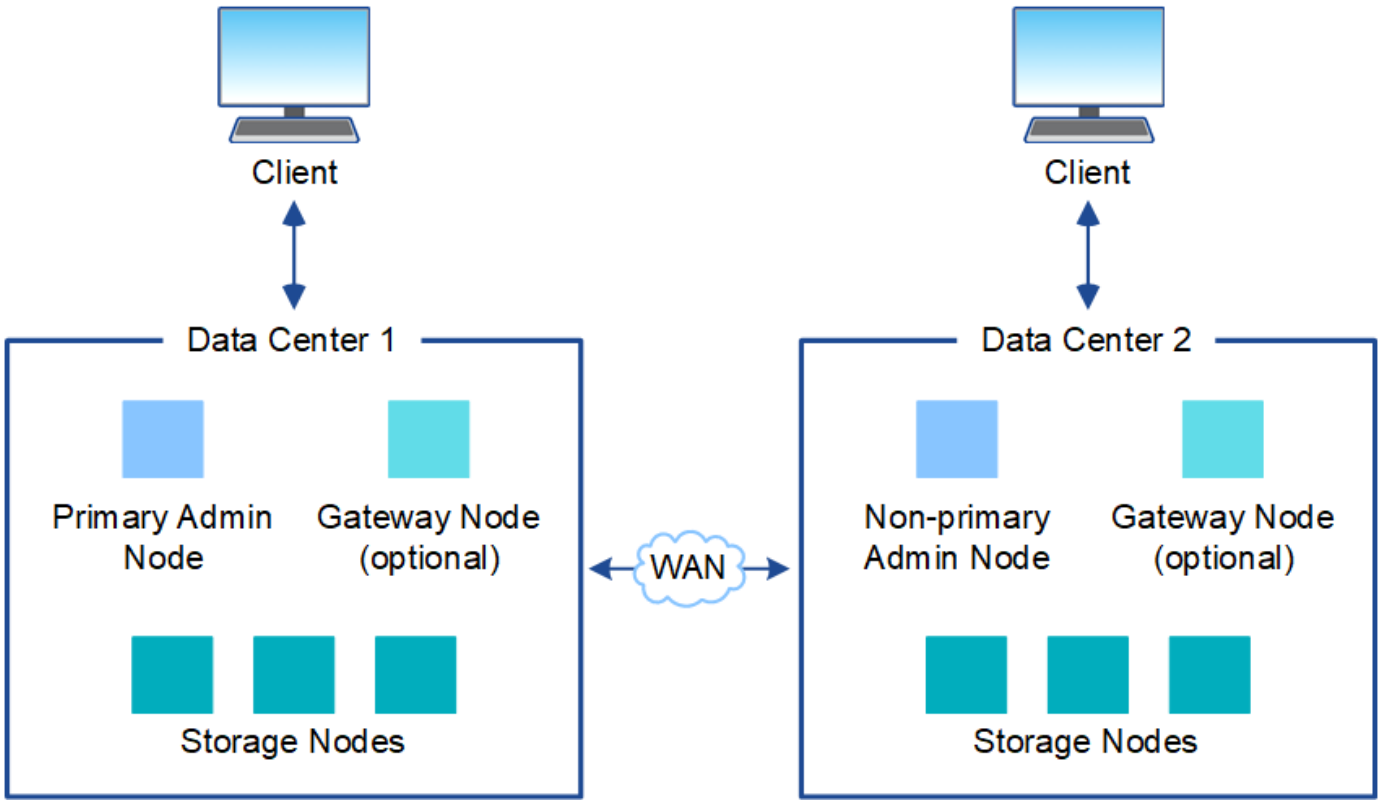
単一サイトに導入する場合は、 StorageGRID システムのインフラと運用が一元化されます。



複数のサイト

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

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



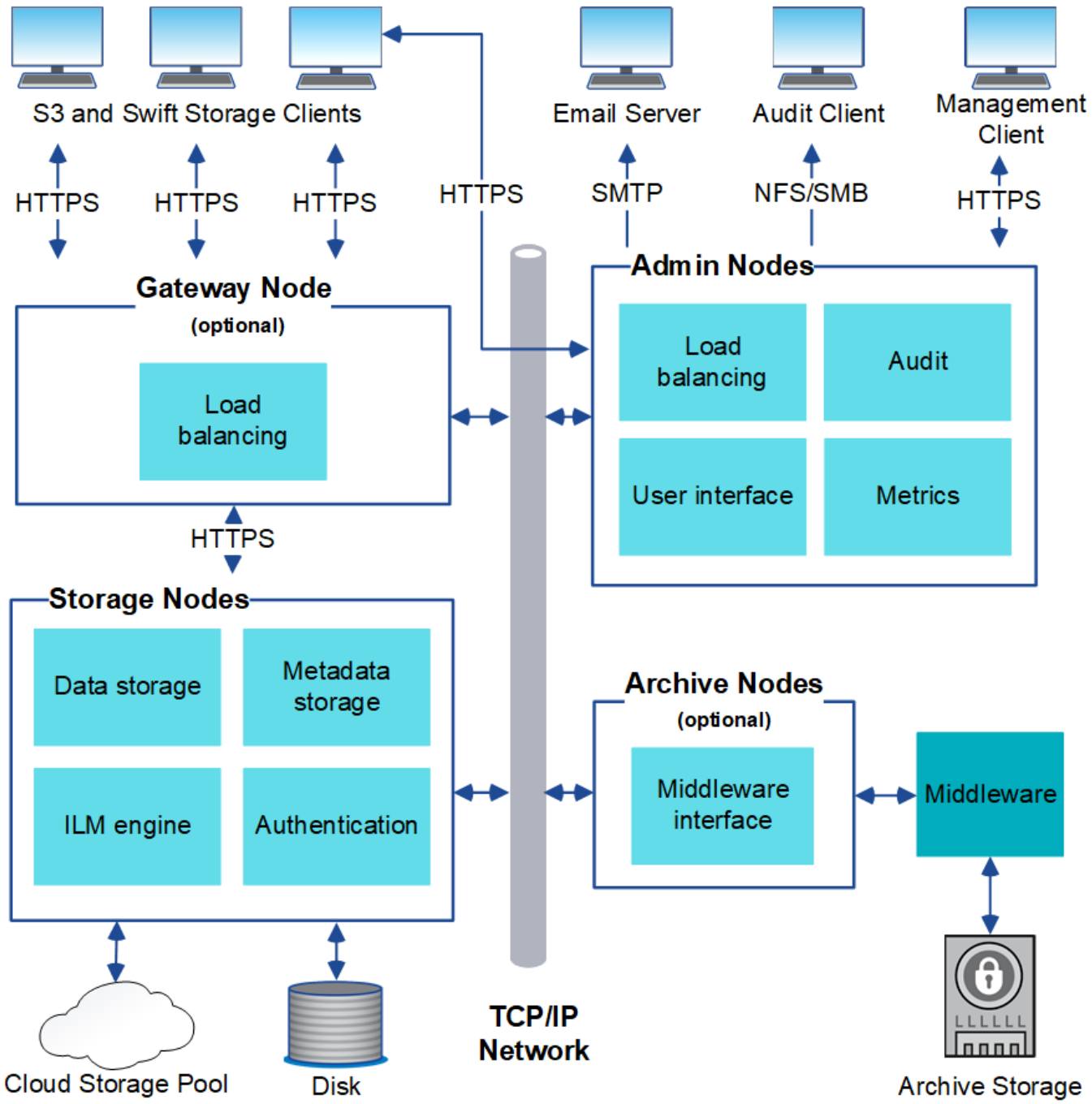
単一のデータセンター内に複数の論理サイトを配置して、分散レプリケーションとイレイジャーコーディングによって可用性と耐障害性を向上させることもできます。

グリッドノードの冗長性

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

システムアーキテクチャ

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



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

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

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

グリッドノードおよびサービス

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

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

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

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

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

詳細については、を参照してください StorageGRID の管理。

ソフトウェアベースのノード

ソフトウェアベースのグリッドノードは、次の方法で導入できます。

- VMware vSphere で仮想マシン（ VM ）として導入
- Linux ホストのコンテナエンジン内。次のオペレーティングシステムがサポートされています。
  - Red Hat Enterprise Linux の場合
  - CentOS の場合
  - Ubuntu
  - Debian

詳細については、次を参照してください。

- VMware をインストールする
- Red Hat Enterprise Linux または CentOS をインストールします
- Ubuntu または Debian をインストールします

を使用します "NetApp Interoperability Matrix Tool で確認できます" をクリックすると、サポートされるバージョンのリストが表示されます。

StorageGRID アプライアンスノード

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

StorageGRID アプライアンスには、次の 4 種類があります。

- SG100 および SG1000 サービスアプライアンス * は、それぞれプライマリ管理ノード、非プライマリ管理ノード、またはゲートウェイノードとして機能する 1 ラックユニット（ 1U ）サーバです。両方のアプライアンスをゲートウェイノードと管理ノード（プライマリノードと非プライマリノード）として同時に動作させることができます。
- SG6000 ストレージアプライアンス * は、 1U SG6000-CN コンピューティングコントローラと 2U または 4U ストレージコントローラシェルフを組み合わせたストレージノードとして機能します。SG6000には次の3つのモデルがあります。
  - * SGF6024 * ： SG6000-CN コンピューティングコントローラと、 24 本のソリッドステートドライブ（ SSD ）と冗長ストレージコントローラを搭載した 2U ストレージコントローラシェルフを組み合わせたものです。
  - * SG6060とSG6060X *：SG6000-CNのコンピューティングコントローラと、58本のNL-SASドライブ、2本のSSD、冗長ストレージコントローラを搭載した4Uエンクロージャを組み合わせたものです。SG6060とSG6060Xはそれぞれ1台または2台の60ドライブ拡張シェルフをサポートし、オブジェクトストレージ専用のドライブを最大で178本提供します。
- SG5700 ストレージアプライアンス * は、ストレージとコンピューティングを統合したプラットフォームであり、ストレージノードとして機能します。SG5700には次の4つのモデルがあります。
  - **SG5712**および**SG5712 12X**：12本のNL-SASドライブと統合ストレージ/コンピューティングコントローラを搭載した2Uエンクロージャ。
  - * SG5760およびSG5712 60X *：60本のNL-SASドライブと統合ストレージ/コンピューティングコントローラを搭載した4Uエンクロージャ。
- SG5600 ストレージアプライアンス * は、ストレージノードとして機能する、ストレージとコンピューティングを統合したプラットフォームです。SG5600 には、次の 2 つのモデルがあります。
  - * SG5612 * ： 12 本の NL-SAS ドライブと統合されたストレージ / コンピューティングコントローラを搭載した 2U エンクロージャ。
  - * SG5660 * ： 60 本の NL-SAS ドライブと統合されたストレージおよびコンピューティングコントローラを搭載した 4U エンクロージャ。

詳細については、次を参照してください。

- "NetApp Hardware Universe の略"
- SG100 および SG1000 サービスアプライアンス
- SG6000 ストレージアプライアンス
- SG5700 ストレージアプライアンス
- SG5600 ストレージアプライアンス

管理ノードのプライマリサービス

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

サービス	キー機能
Audit Management System （AMS）	システムアクティビティを追跡します。
Configuration Management Node （CMN）	システム全体の設定を管理します。プライマリ管理ノードのみ
管理アプリケーションプログラミングインターフェイス（mgmt-api）	グリッド管理 API とテナント管理 API からの要求を処理します。
高可用性	管理ノードとゲートウェイノードのグループのハイアベイラビリティ仮想 IP アドレスを管理します。 • 注：* このサービスはゲートウェイノードにも搭載されています。
ロードバランサ	クライアントからストレージノードへの S3 および Swift トラフィックのロードバランシングを実現します。 • 注：* このサービスはゲートウェイノードにも搭載されています。
ネットワーク管理システム（NMS）	Grid Manager の機能を提供します。
Prometheus	指標を収集して格納します。
SSM （サーバステータスモニタ）	オペレーティングシステムと基盤のハードウェアを監視します。

ストレージノードのプライマリサービス

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

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

サービス	キー機能
アカウント（acct）	テナントアカウントを管理します。

サービス	キー機能
Administrative Domain Controller （ADC ；管理ドメインコントローラ）	トポロジとグリッド全体の構成を管理します。
Cassandra	オブジェクトメタデータを格納し、保護します。
Cassandra Reaper	オブジェクトメタデータの自動修復を実行します。
チャンク	イレイジャーコーディングされたデータフラグメントとパリティフラグメントを管理します。
Data Mover （DMV）	クラウドストレージプールにデータを移動します。
Distributed Data Store （DDS）	オブジェクトメタデータストレージを監視します。
ID （idnt）	LDAP および Active Directory から取得したユーザ ID を統合する
Local Distribution Router （LDR）（ローカル分散ルータ（LDR）	オブジェクトストレージプロトコル要求を処理し、ディスク上のオブジェクトデータを管理します。
Replicated State Machine （RSM）	S3 プラットフォームサービス要求がそれぞれのエンドポイントに送信されるようにします。
SSM （サーバステータスモニタ）	オペレーティングシステムと基盤のハードウェアを監視します。

ゲートウェイノードのプライマリサービス

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

サービス	キー機能
Connection Load Balancer （CLB ；接続ロードバランサ）	クライアントからストレージノードへの S3 および Swift トラフィックのレイヤ 3 とレイヤ 4 のロードバランシングを実現します。従来のロードバランシングメカニズムです。 • 注： * CLB サービスは廃止されました。
高可用性	管理ノードとゲートウェイノードのグループのハイアベイラビリティ仮想 IP アドレスを管理します。 • 注： * このサービスは管理ノードにも搭載されています。

サービス	キー機能
ロードバランサ	クライアントからストレージノードへの S3 および Swift トラフィックのレイヤ 7 のロードバランシングを実現します。これは推奨されるロードバランシングメカニズムです。 • 注：* このサービスは管理ノードにも搭載されています。
SSM （サーバステータスモニタ）	オペレーティングシステムと基盤のハードウェアを監視します。

アーカイブノードのプライマリサービス

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

サービス	キー機能
アーカイブ（ ARC ）	Tivoli Storage Manager （ TSM ）外部テープストレージシステムと通信します。
SSM （サーバステータスモニタ）	オペレーティングシステムと基盤のハードウェアを監視します。

StorageGRID サービス

StorageGRID サービスの一覧を以下に示します。

- * アカウントサービスフォワーダ *

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

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

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

- * AMS サービス (監査管理システム)*

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

- * ARC サービス（アーカイブ） *

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

- * Cassandra Reaper サービス *

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

- * チャンクサービス *

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

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

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

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

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

- * DDS サービス (分散データストア)*

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

- * DMV サービス（ Data Mover ） *

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

- * ダイナミック IP サービス *

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

- * Grafana サービス *

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

- * 高可用性サービス *

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

- * アイデンティティ (idnt) サービス *

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

- * Lambda 仲裁人サービス *

  S3 Select SelectObjectContent 要求を管理します。

- * ロードバランササービス *

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

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

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

- *MISCd Information Service Control Daemon サービス *

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

- * nginx サービス *

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

- * nginx-gw サービス *

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

- * NMS サービス（ネットワーク管理システム） *

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

- * 持続性サービス *

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

- * Prometheus サービス *

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

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

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

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

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

- * トレースコレクタサービス *

  トレース収集を実行し、テクニカルサポートが使用する情報を収集します。TRACE コレクタサービスは

オープンソースの Jaeger ソフトウェアを使用し、管理ノードに存在します。

オブジェクト管理

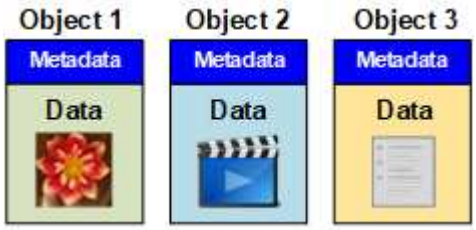
StorageGRID によるデータの管理方法

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

オブジェクトとは

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

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



オブジェクトデータ

写真、映画、診療記録など、あらゆるものが含まれます。

オブジェクトメタデータ

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

オブジェクトメタデータには、次のような情報が含まれます。

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

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

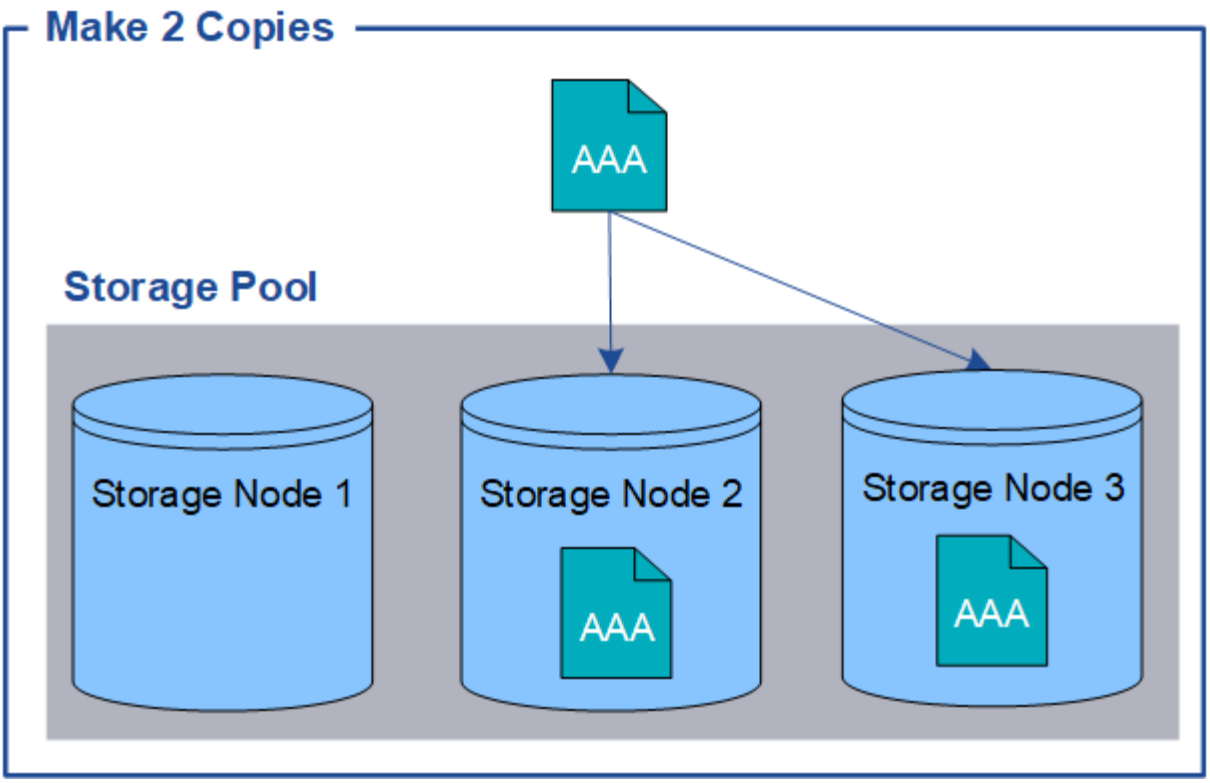
StorageGRID がオブジェクトメタデータを格納する方法と場所の詳細については、を参照してください オブジェクトメタデータストレージを管理する。

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

レプリケーション

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

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

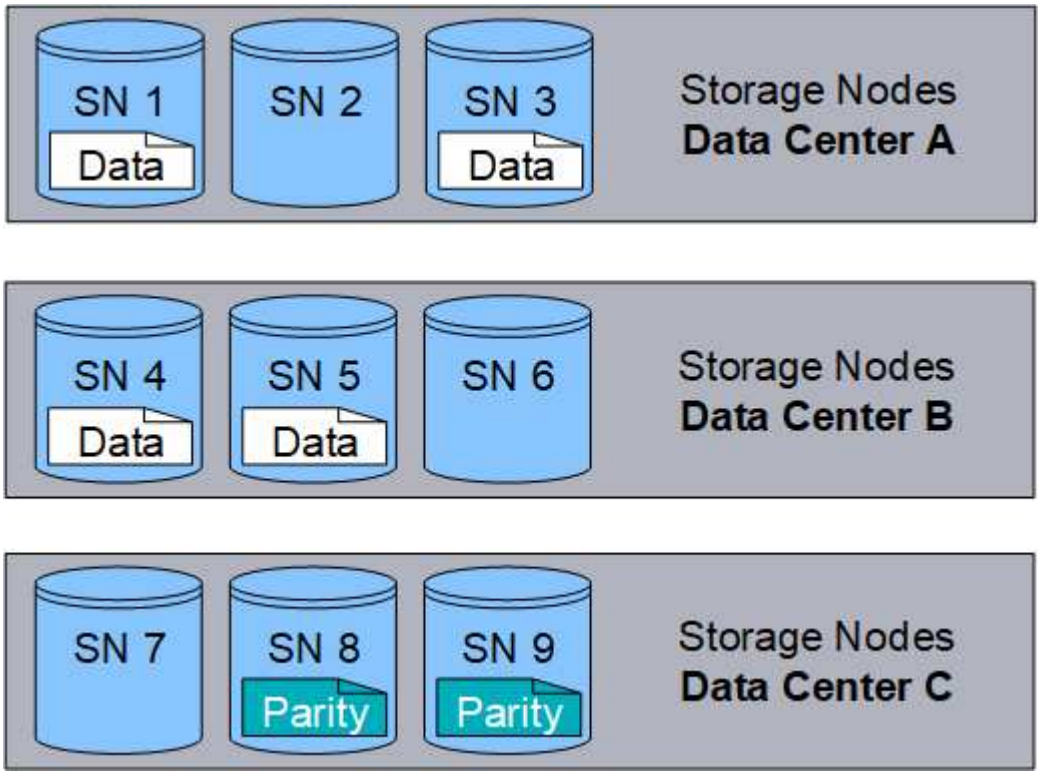


イレイジャーコーディング

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

次の例は、オブジェクトのデータにイレイジャーコーディングを使用する方法を示しています。この例の ILM ルールでは 4+2 のイレイジャーコーディングスキームを使用します。各オブジェクトは 4 つのデータフラグメントに等分され、オブジェクトデータから 2 つのパリティフラグメントが計算されます。ノードやサイト

の障害時にもデータが保護されるよう、 6 つの各フラグメントは 3 つのデータセンターの別々のストレージノードに格納されます。



関連情報

- ILM を使用してオブジェクトを管理する
- 情報ライフサイクル管理を使用

オブジェクトライフサイクル

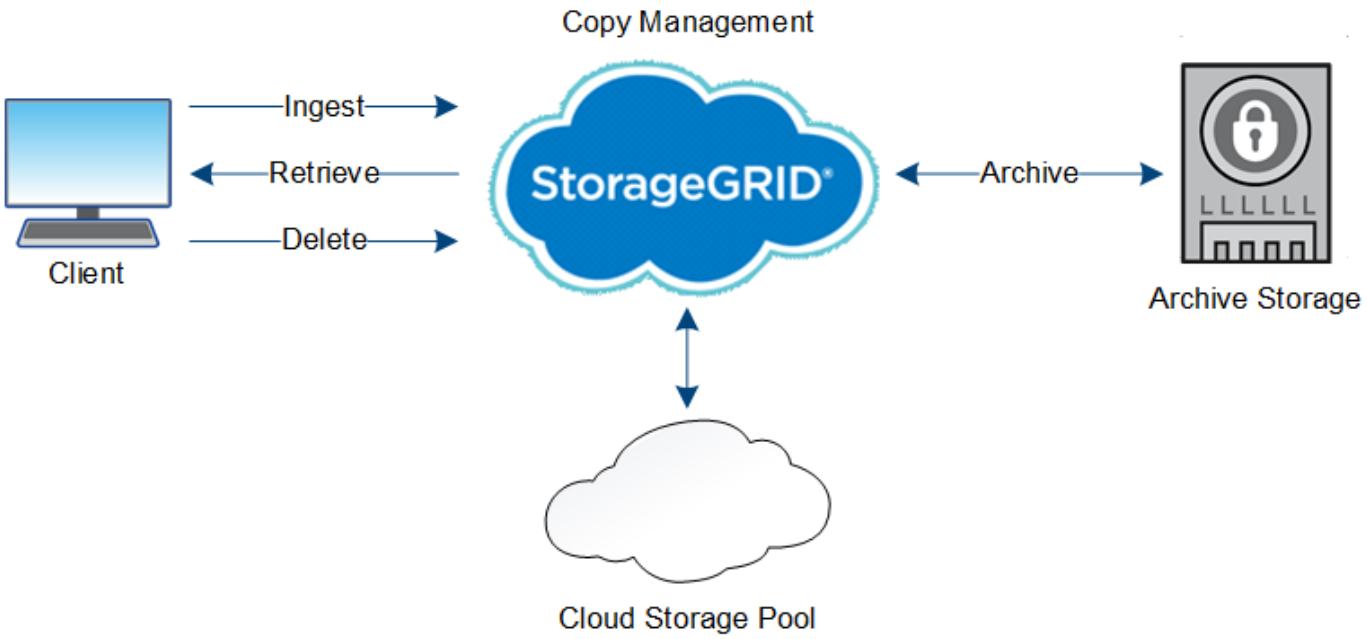
オブジェクトのライフサイクル

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

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

- * 取り込み： S3 または Swift クライアントアプリケーションから、 HTTP 経由で StorageGRID システムにオブジェクトを保存するプロセスです。このステージでは、 StorageGRID システムがオブジェクトの管理を開始します。
- * コピー管理 * ：アクティブな ILM ポリシーの ILM ルールで説明されているように、 StorageGRID でレプリケートコピーとイレイジャーコーディングコピーを管理するプロセス。コピー管理ステージでは、 StorageGRID が指定された数とタイプのオブジェクトコピーをストレージノード、クラウドストレージプール、またはアーカイブノードに作成して保持することで、オブジェクトデータを損失から保護します。
- * Retrieve * ： StorageGRID システムに格納されたオブジェクトにクライアントアプリケーションがアクセスするプロセス。クライアントがオブジェクトを読み取ると、オブジェクトがストレージノード、クラウドストレージプール、またはアーカイブノードから読み出されます。
- * 削除 * ：グリッドからすべてのオブジェクトコピーを削除するプロセス。オブジェクトは、クライアントアプリケーションが StorageGRID システムに削除要求を送信することで削除されるか、オブジェクト

の有効期間が終了したときに StorageGRID が実行する自動プロセスによって削除されます。



関連情報

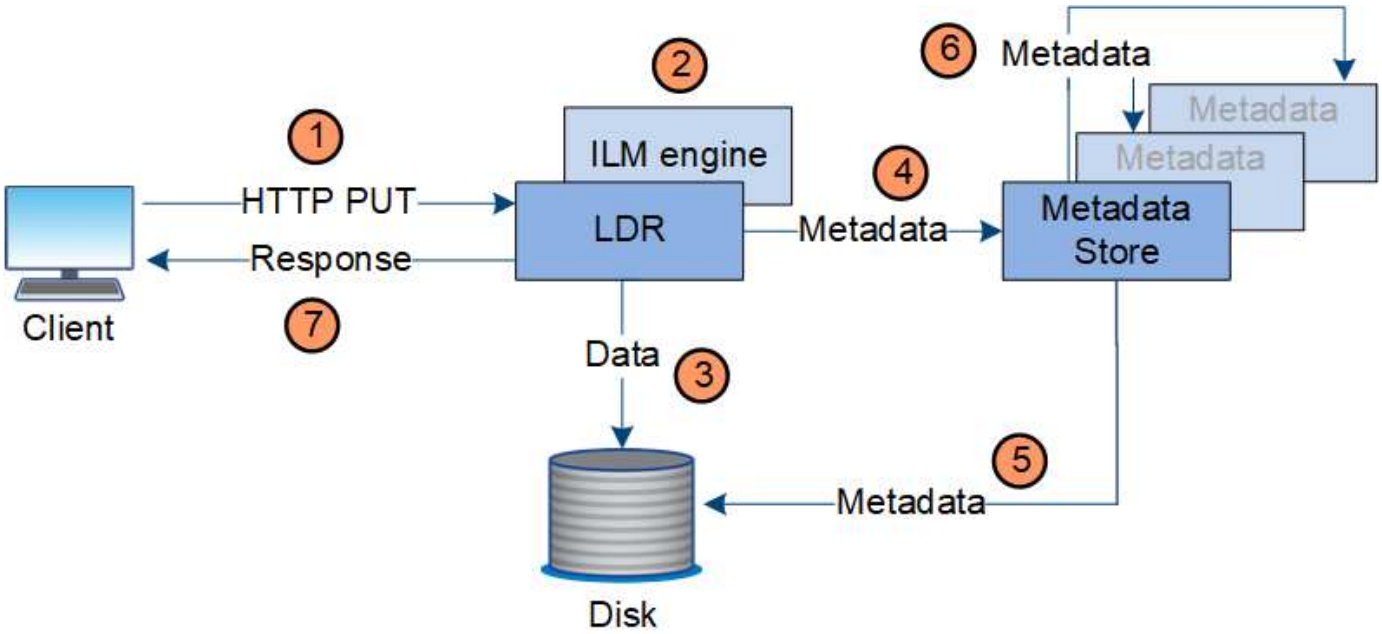
- ILM を使用してオブジェクトを管理する
- 情報ライフサイクル管理を使用

取り込みのデータフロー

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

データフロー

クライアントが StorageGRID システムにオブジェクトを取り込んだ場合、ストレージノード上の LDR サービスが要求を処理し、メタデータとデータをディスクに格納します。



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

コピー管理

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

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

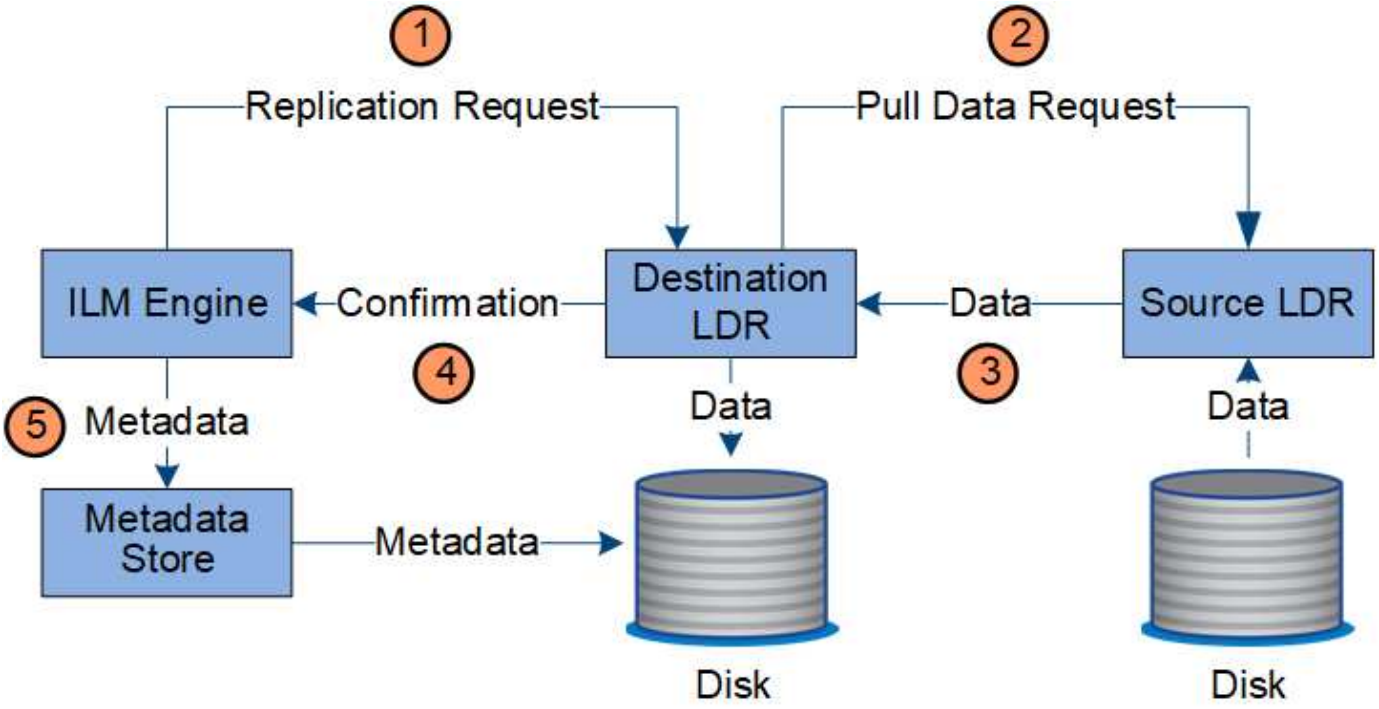
オブジェクトデータは LDR サービスで管理されます。

コンテンツの保護：レプリケーション

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

データフロー

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



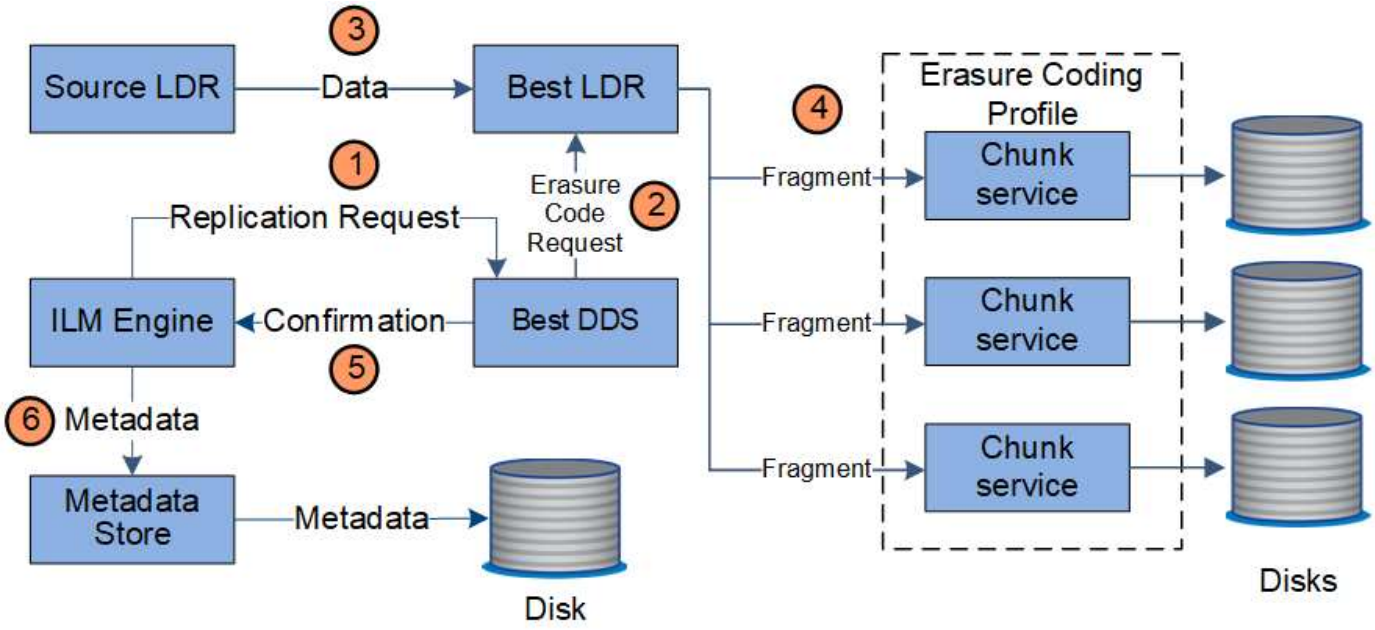
1. ILM エンジンが、 ILM ルールで指定されたストレージプール内で最適なデスティネーション LDR サービスを ADC サービスに照会します。その後、レプリケーションを開始するコマンドをその LDR サービスに送信します。
2. デスティネーション LDR サービスから、 ADC サービスを照会することで最適なソースの場所が特定されます。その後、レプリケーション要求をソース LDR サービスに送信します。
3. ソース LDR サービスからデスティネーション LDR サービスにコピーが送信されます。
4. デスティネーション LDR サービスから ILM エンジンに、オブジェクトデータ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

コンテンツの保護：イレイジャーコーディング

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

データフロー

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



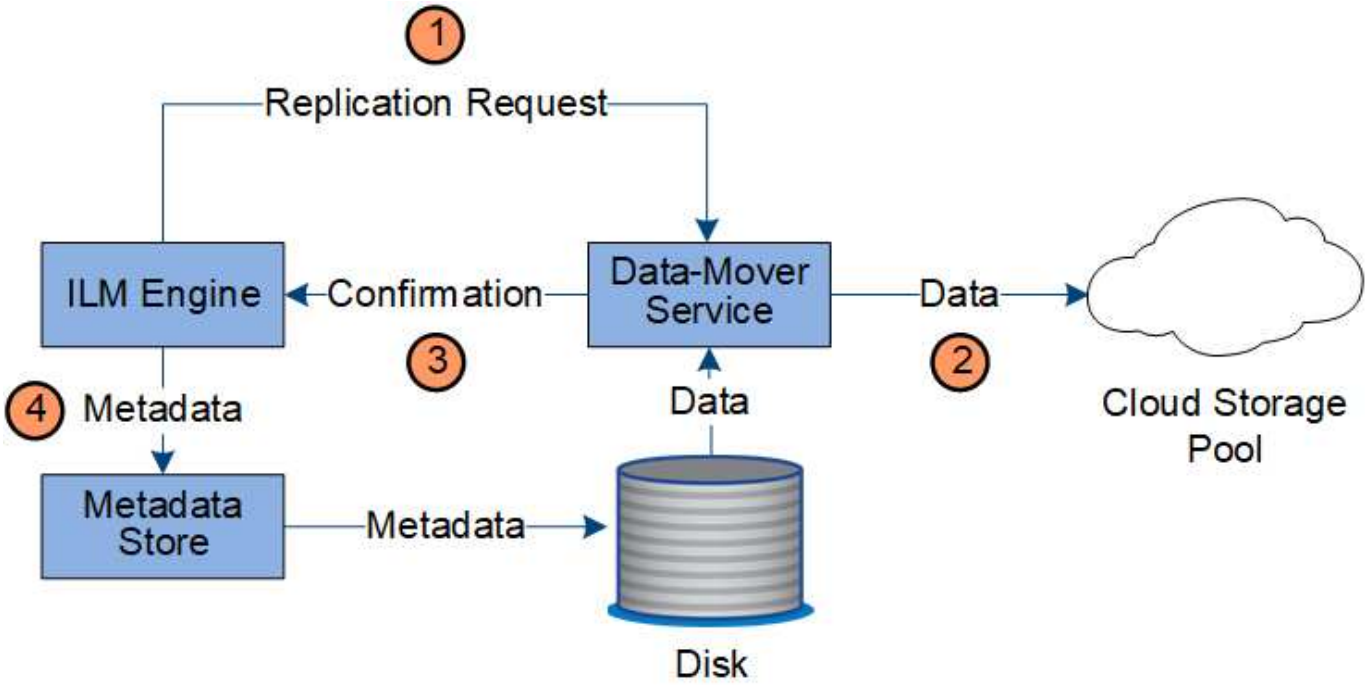
1. ILM エンジンから、 ADC サービスを照会することでイレイジャーコーディング処理の実行に最も適した DDS サービスが特定され、そのサービスに「開始」要求を送信します。
2. DDS サービスが、オブジェクトデータのイレイジャーコーディングを実行するように LDR に指示します。
3. ソース LDR サービスから、イレイジャーコーディングの対象として選択された LDR サービスにコピーが送信されます。
4. LDR サービスにより、オブジェクトデータが適切な数のパリティとデータのフラグメントに分割され、それらのフラグメントがイレイジャーコーディングプロファイルのストレージプールを構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

コンテンツの保護：クラウドストレージプール

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

データフロー

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

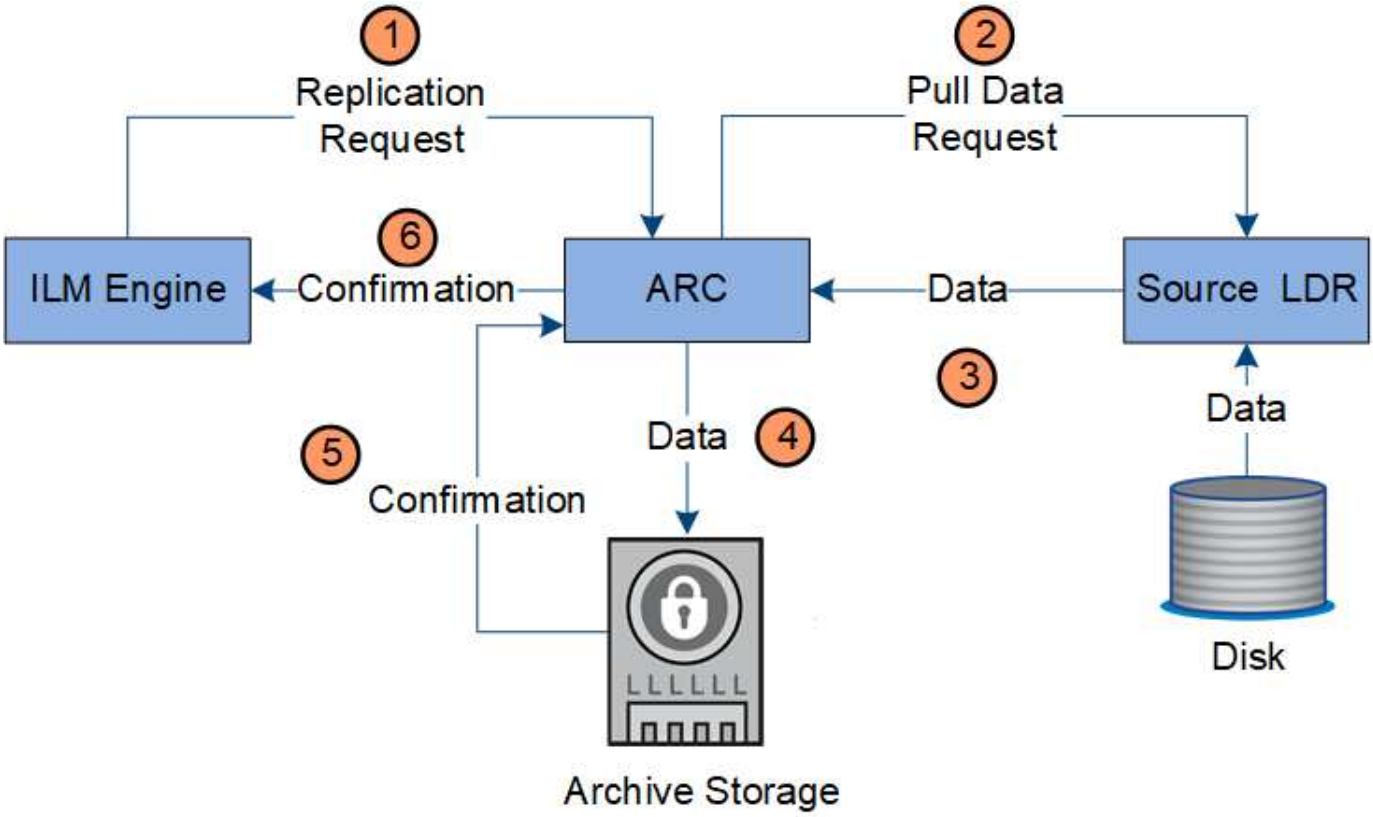


1. ILM エンジンが、クラウドストレージプールにレプリケートするための Data Mover サービスを選択します。
2. Data Mover サービスが、オブジェクトデータをクラウドストレージプールに送信します。
3. Data Mover サービスが、オブジェクトデータが格納されたことを ILM エンジンに通知します。
4. ILM エンジンが、メタデータストアのオブジェクトの場所を示すメタデータを更新します。

コンテンツの保護：アーカイブ

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

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



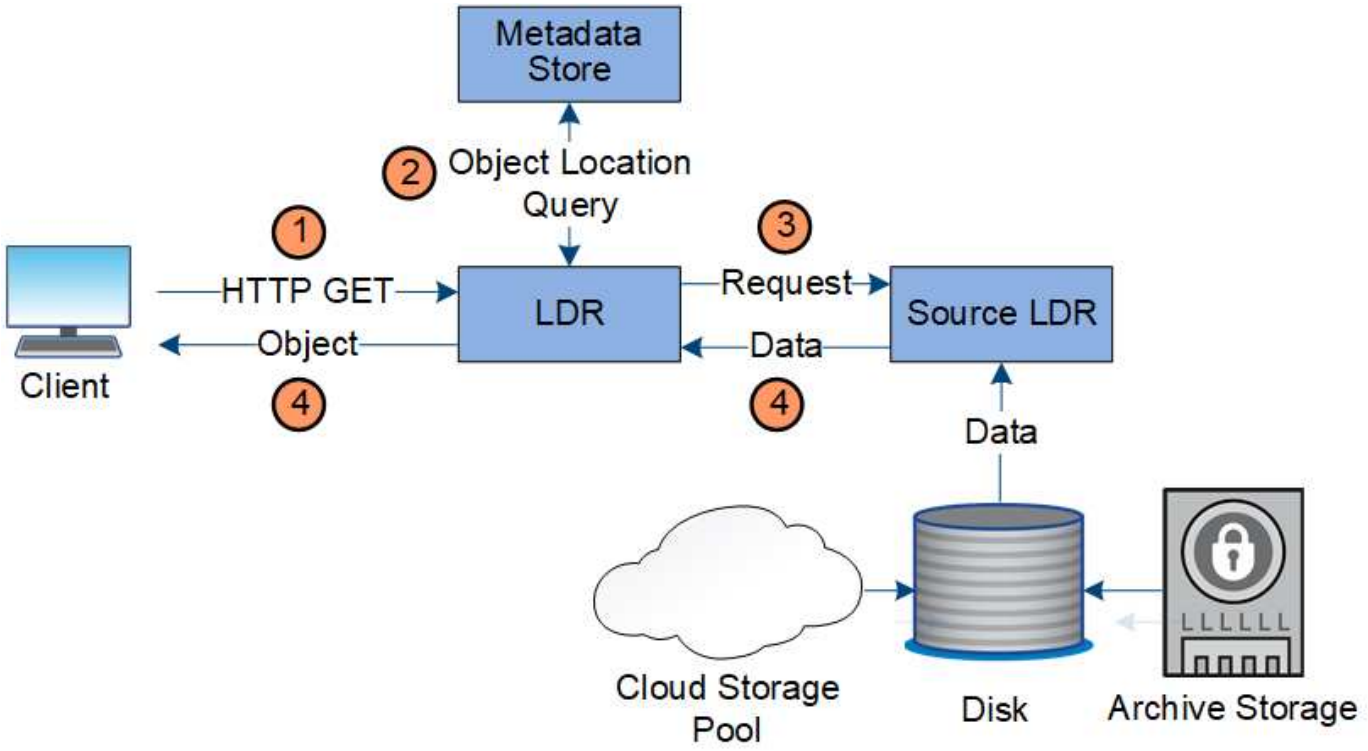
1. ILM エンジンが ARC サービスに要求を送信し、アーカイブメディアにコピーを格納するように指示します。
2. ARC サービスから、 ADC サービスを照会することで最適なソースの場所が特定され、ソース LDR サービスに要求が送信されます。
3. ARC サービスが、 LDR サービスからオブジェクトデータを読み出します。
4. ARC サービスが、対象のアーカイブメディアにオブジェクトデータを送信します。
5. アーカイブメディアから ARC サービスに、オブジェクトデータが格納されたことが通知されます。
6. ARC サービスから ILM エンジンに、オブジェクトデータが格納さ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

読み出しのデータフロー

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

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

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



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

データフローを削除します

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

削除階層

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

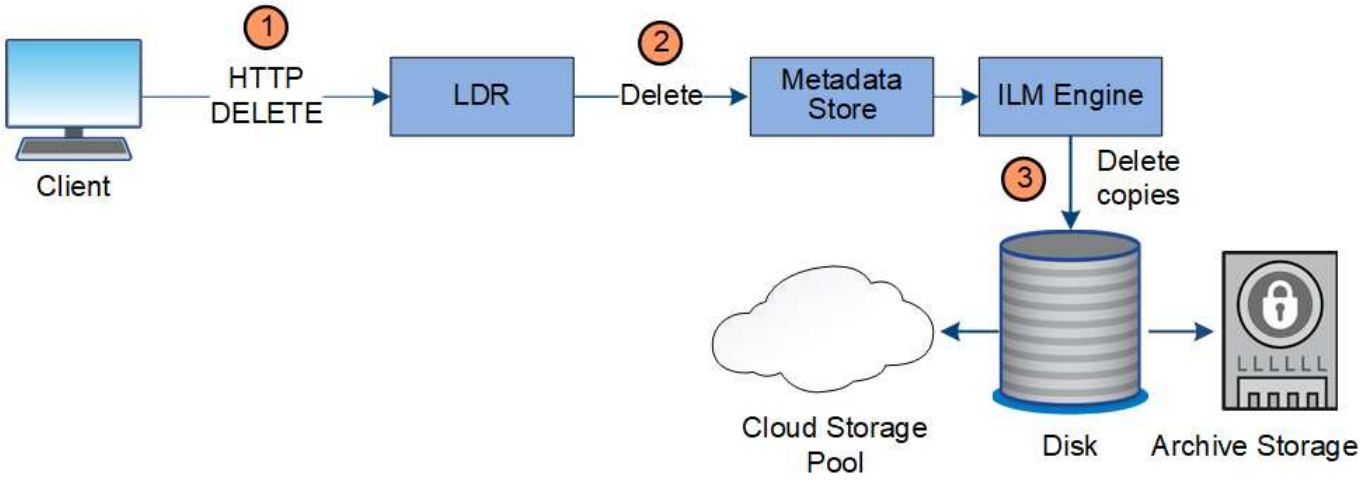
- * S3 オブジェクトのロック * ：グリッドでグローバルな S3 オブジェクトのロック設定が有効になっている場合、 S3 クライアントは S3 オブジェクトのロックを有効にしたバケットを作成し、 S3 REST API を使用して、そのバケットに追加された各オブジェクトバージョンの最新の保持設定とリーガルホールド設定を指定できます。
  - リーガルホールドの対象になっているオブジェクトバージョンは、どの方法でも削除できません。
  - オブジェクトバージョンの retain-until - date に到達するまでは、どのメソッドでもそのバージョンを削除することはできません。

- S3 オブジェクトロックが有効になっているバケット内のオブジェクトは、 ILM によって「無期限」に保持されます。ただし、それまでの保持期間が終了したあとは、クライアント要求やバケットライフサイクルの終了によってオブジェクトバージョンを削除できます。
- S3 クライアントがバケットにデフォルトの retain-date を適用する場合、オブジェクトごとに retain-date を指定する必要はありません。

- * クライアントの削除要求 * ： S3 または Swift クライアントは、オブジェクトの削除要求を問題 できます。クライアントがオブジェクトを削除すると、そのオブジェクトのすべてのコピーが StorageGRID システムから削除されます。
- * S3 バケットライフサイクル * ： S3 クライアントは、 Expiration アクションを指定するライフサイクル設定をバケットに追加できます。バケットライフサイクルが設定されている場合、クライアントが先にオブジェクトを削除しないかぎり、 Expiration アクションで指定された日付または日数が経過した時点で、 StorageGRID はオブジェクトのすべてのコピーを自動的に削除します。
- * ILM の配置手順 * ：バケットで S3 オブジェクトロックが有効になっておらず、バケットライフサイクルがない場合、 StorageGRID は ILM ルールの最後の期間が終了してオブジェクトにそれ以降の配置が指定されていないときにオブジェクトを自動的に削除します。

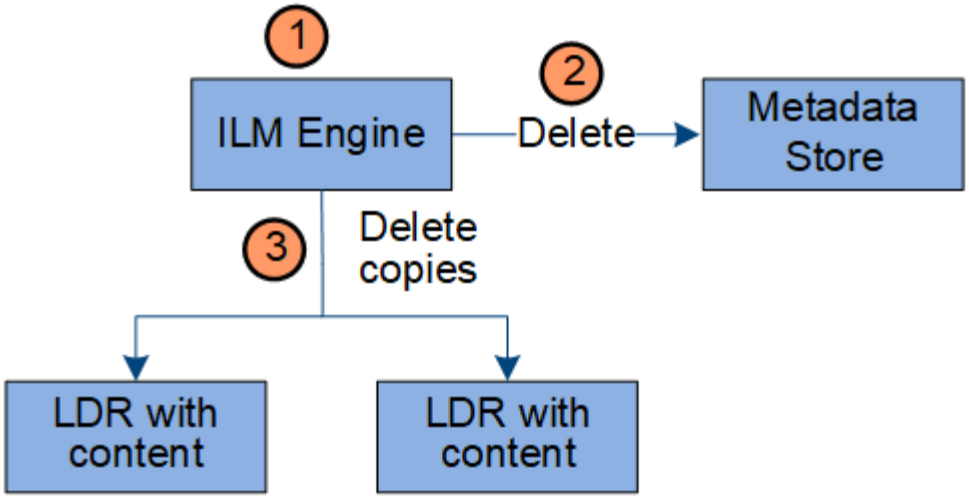
> S3 バケットライフサイクルの Expiration アクションは、常に ILM 設定よりも優先されます。その結果、 ILM のオブジェクト配置手順がすべて終了したあとも、オブジェクトがグリッドに保持されることがあります。

クライアント削除のデータフロー



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

ILM による削除のデータフローを示します



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

StorageGRID の使用方法

Grid Manager の詳細を見る

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

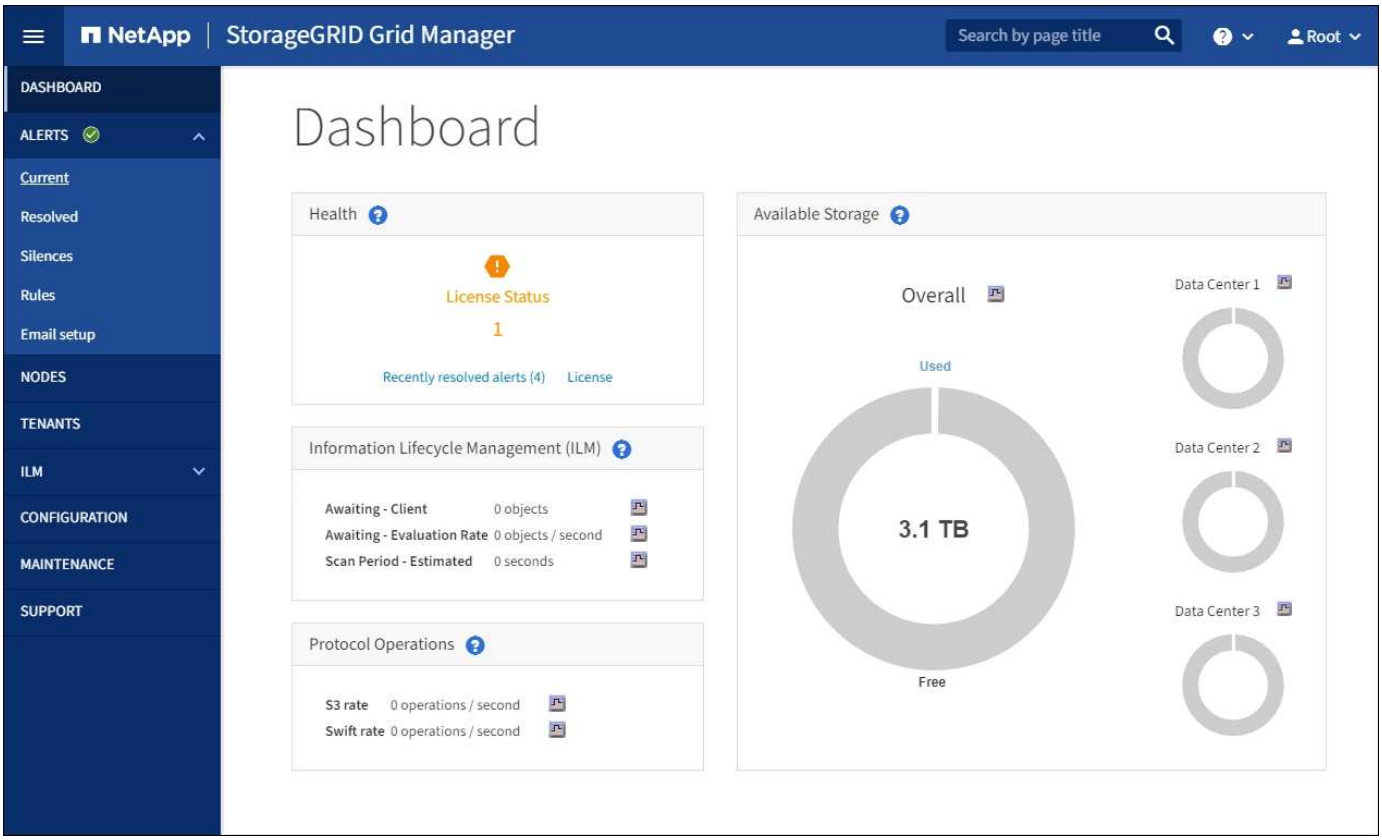
Grid Manager にサインインすると、管理ノードに接続されます。各 StorageGRID システムには、 1 つのプライマリ管理ノードと、任意の数のプライマリ以外の管理ノードが含まれています。どの管理ノードにも接続が可能で、各管理ノードに表示される StorageGRID システムのビューもほぼ同じです。

を使用して Grid Manager にアクセスできます サポートされている Web ブラウザ。

Grid Manager ダッシュボード

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

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



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

詳細はこちら。

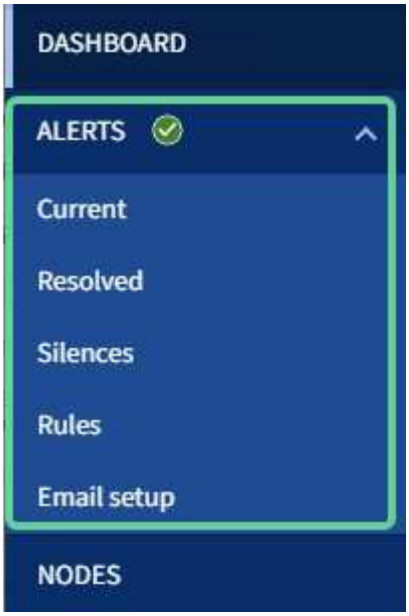
- 監視とトラブルシューティング

検索フィールド

ヘッダーバーの * Search * フィールドを使用すると、 Grid Manager 内の特定のページにすばやく移動できます。たとえば、「 * KM * 」と入力して、 Key Management Server （ KMS ）ページにアクセスできます。* Search * を使用して、 Grid Manager のサイドバーおよび設定、メンテナンス、サポートの各メニューでエントリを検索できます。

［アラート］ メニュー

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



[Alerts] メニューでは ' 次の操作を実行できます

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

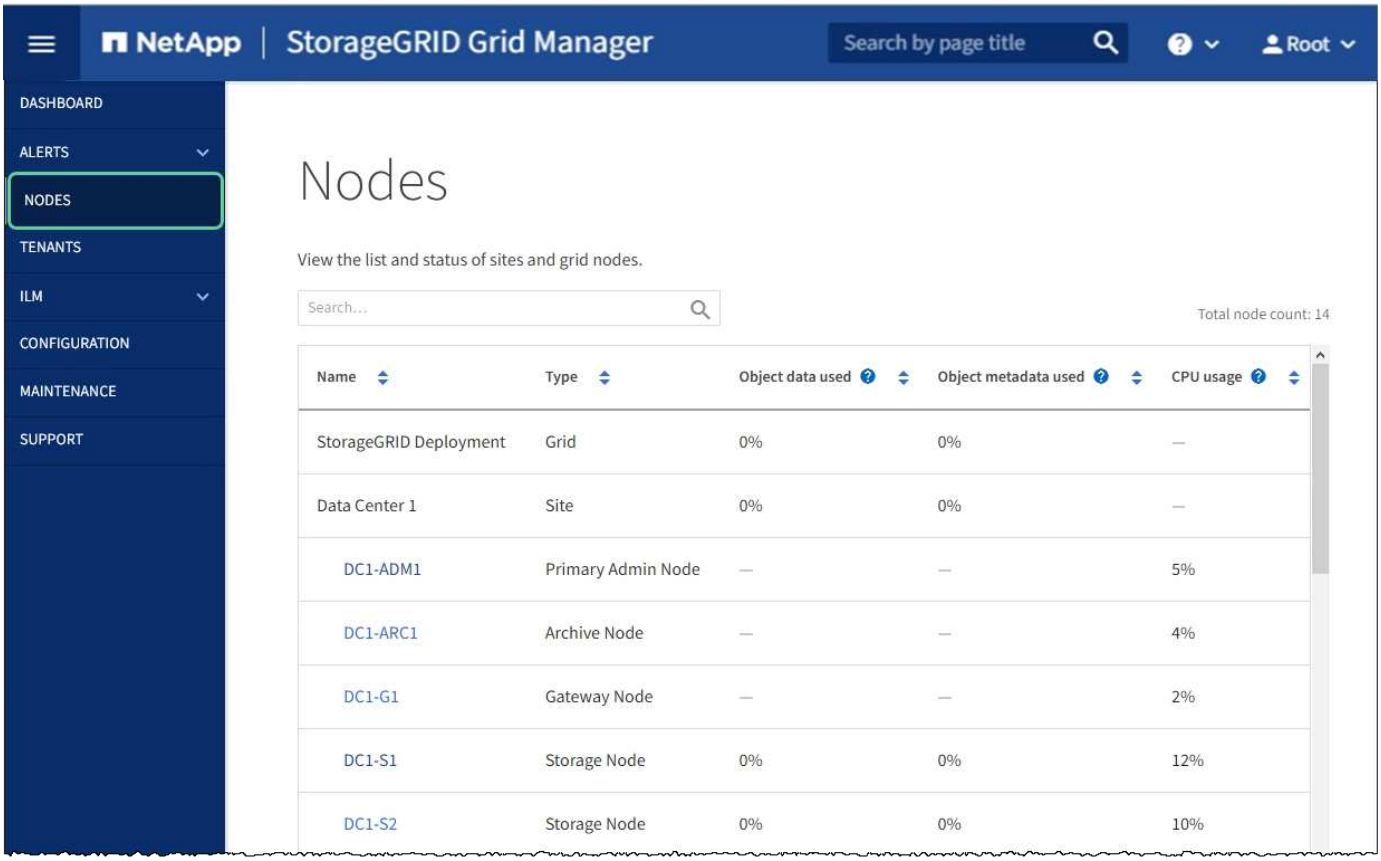
詳細はこちら。

- アラートを監視および管理する
- 監視とトラブルシューティング

Nodes ヘエシ

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

ノードのホームページには、グリッド全体の複数の指標の合計が表示されます。特定のサイトまたはノードの情報を表示するには、サイトまたはノードを選択します。



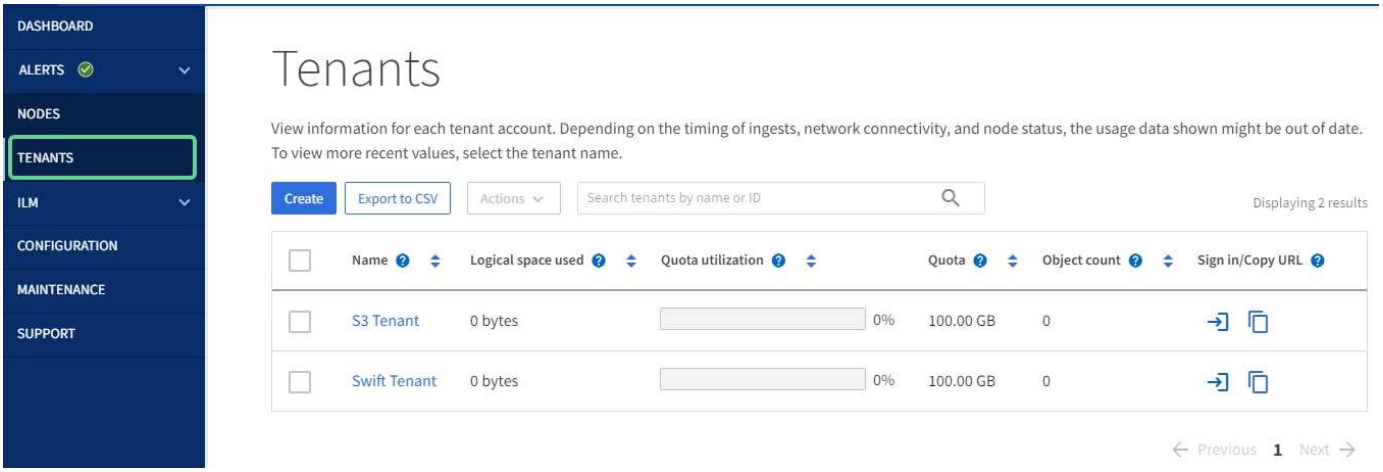
詳細はこちら。

- Nodes ページを表示します
- 監視とトラブルシューティング

テナントページ

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

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



詳細はこちら。

- テナントとクライアント接続を管理する
- StorageGRID の管理
- テナントアカウントを使用する

ILM メニュー

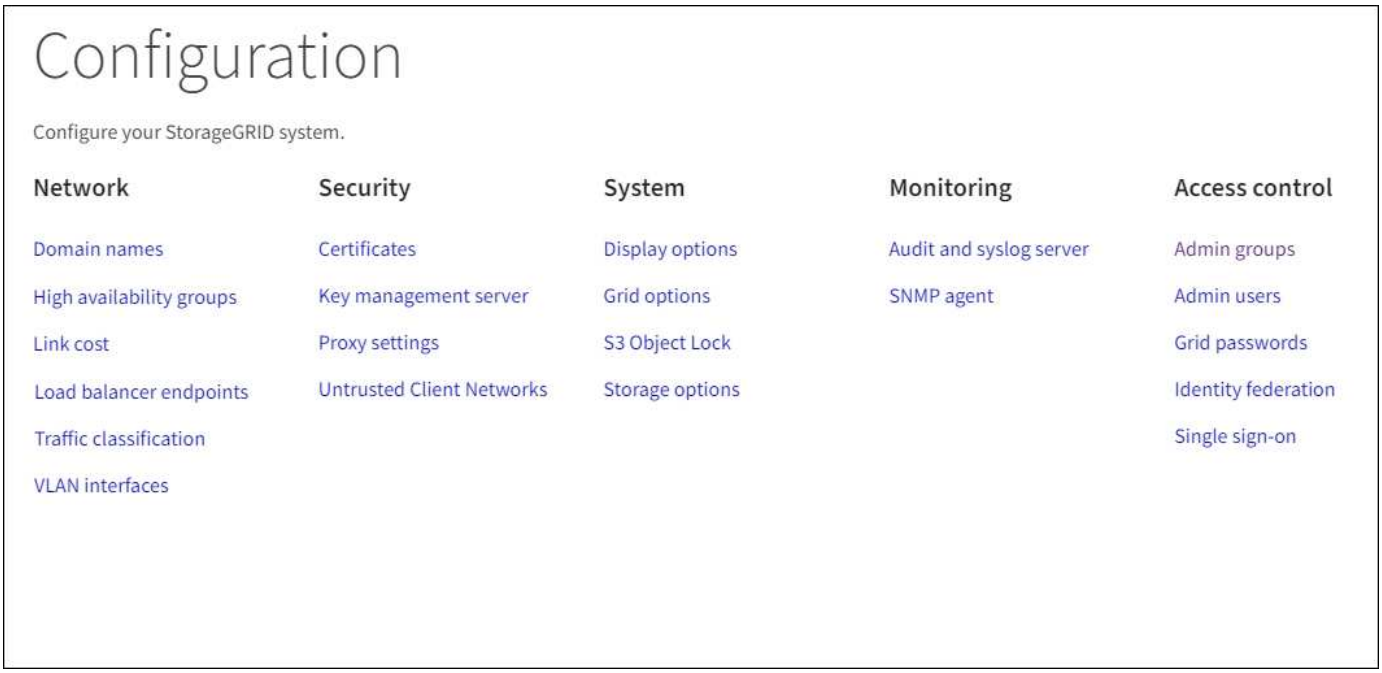
ILM メニューでは、データの保持と可用性を制御する情報ライフサイクル管理（ ILM ）のルールとポリシーを設定できます。オブジェクト ID を入力して、そのオブジェクトのメタデータを表示することもできます。

詳細はこちら。

- 情報ライフサイクル管理を使用
- ILM を使用してオブジェクトを管理する

設定メニュー

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

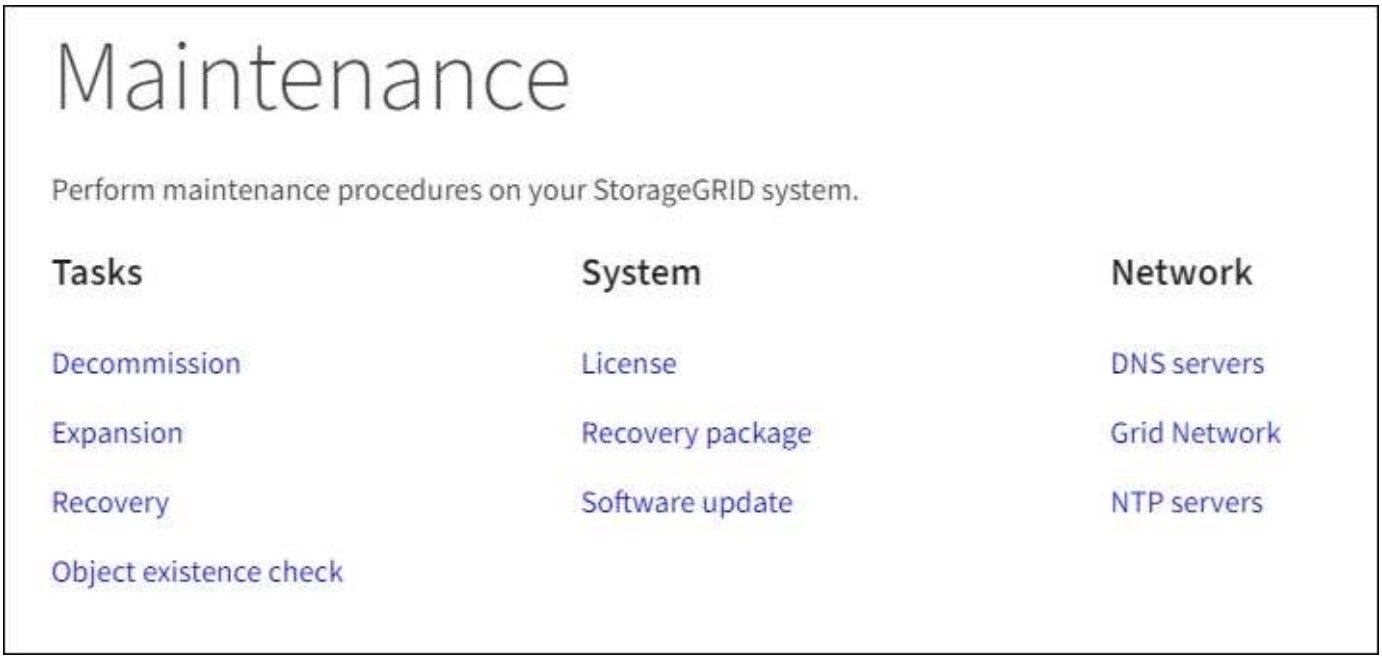


詳細はこちら。

- ネットワークの設定を行います
- テナントとクライアント接続を管理する
- 監査メッセージを確認します
- StorageGRID アクセスを制御します
- StorageGRID の管理
- 監視とトラブルシューティング
- 監査ログを確認します

メンテナンスメニュー

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



タスク

保守作業には次のものが含ま

- 運用停止処理：使用されていないグリッドノードとサイトを削除します。
- 新しいグリッドノードとサイトを追加するための拡張処理。
- 障害が発生したノードの交換とデータのリストアに使用するリカバリ処理。
- オブジェクトの有無は、オブジェクトデータの有無（正確性ではなく）を確認するためにチェックされます。

システム

実行可能なシステムメンテナンスタスクには、次のものがあります。

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

ネットワーク

実行できるネットワークメンテナンス作業には、次のものがあります。

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

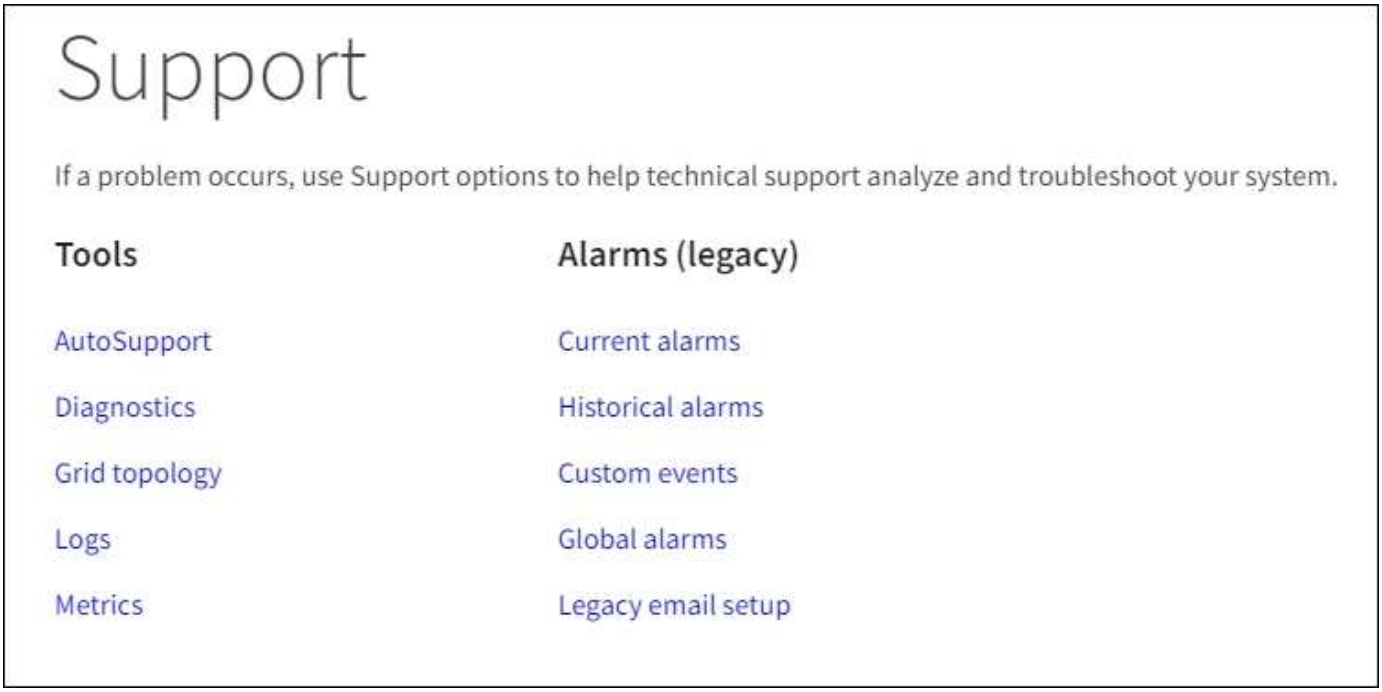
詳細はこちら。

- メンテナンスを実施します

- リカバリパッケージをダウンロードします
- グリッドを展開します
- ソフトウェアをアップグレードする
- リカバリとメンテナンス
- SG6000 ストレージアプライアンス
- SG5700 ストレージアプライアンス
- SG5600 ストレージアプライアンス

サポートメニュー

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



ツール

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

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

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

アラーム（レガシー）

サポートメニューのアラーム（レガシー）セクションでは、現在、過去、グローバルのアラームを確認したり、カスタムイベントを設定したり、従来のアラームと AutoSupport の E メール通知を設定したりできます。

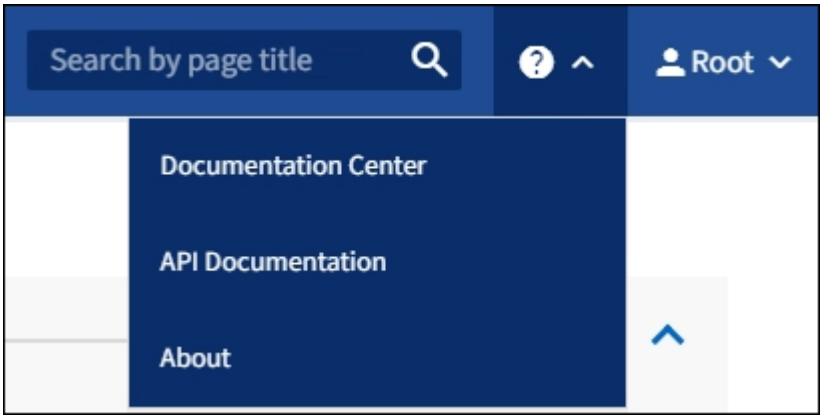
従来のアラームシステムは引き続きサポートされますが、アラートシステムには大きなメリットがあり、使いやすくなっています。

詳細はこちら。

- StorageGRID のアーキテクチャとネットワークトポロジ
- StorageGRID 属性
- StorageGRID のサポートオプションを使用する
- StorageGRID の管理
- 監視とトラブルシューティング

ヘルプメニュー

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



詳細はこちら。

- StorageGRID の管理

Tenant Manager を確認します

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

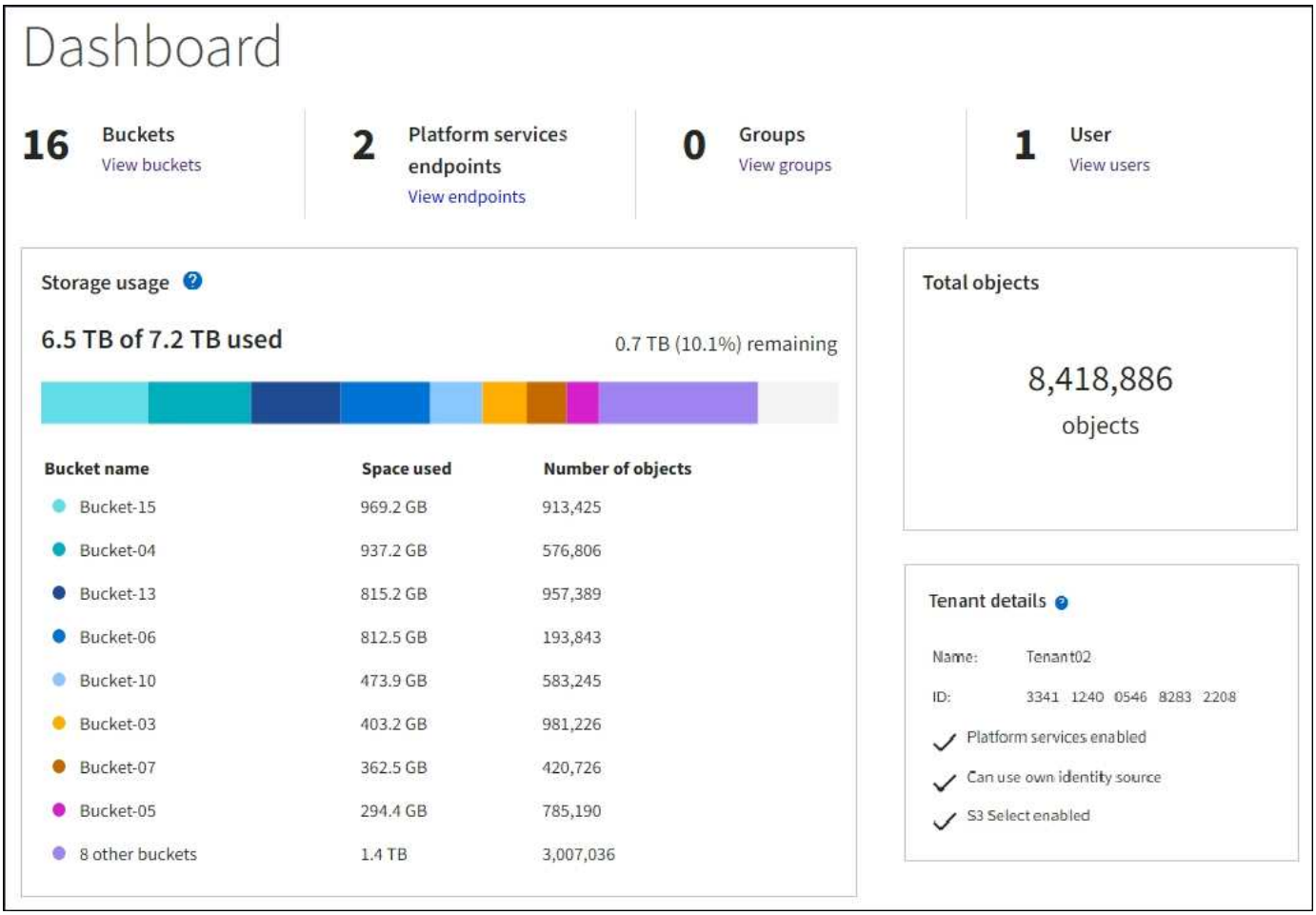
Tenant Manager にサインインしたテナントユーザは管理ノードに接続しています。

Tenant Manager のダッシュボード

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

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

棒グラフの上に表示される値は、テナントのすべてのバケットまたはコンテナに使用されているスペースの合計です。テナントで使用可能な最大ギガバイト数、テラバイト数、またはペタバイト数をアカウント作成時に指定した場合は、使用されているクォータの量と残りのクォータも表示されます。



ストレージメニュー（ **S3** テナントのみ）

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

アクセスキー

S3 テナントユーザは次のようにアクセスキーを管理できます。

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

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

バケット

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

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

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

- S3 イベント通知の設定。この通知は、 AWS Simple Notification Service ™（ SNS ）をサポートするデスティネーションサービスに送信できます。
- CloudMirror レプリケーションの設定。テナントから外部の S3 バケットにオブジェクトが自動的にレプリケートされるようにすることができます。

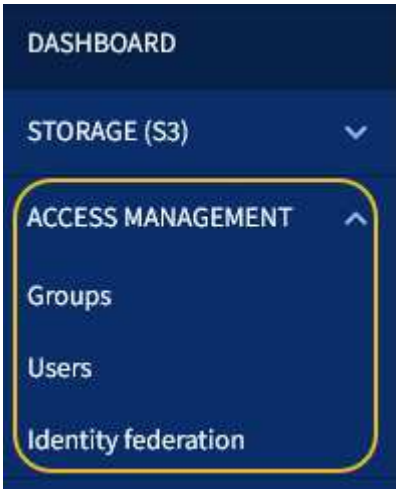
- 検索統合の設定。検索統合は、オブジェクトの作成、削除、またはそのメタデータやタグの更新が行われるたびに、デスティネーションの検索インデックスにオブジェクトメタデータを送信します。

プラットフォームサービスのエンドポイント

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

Access 管理メニュー

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



関連情報

- Grid Manager の詳細を見る
- テナントアカウントを使用する

StorageGRID アクセスを制御します

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

Grid Manager へのアクセスを制御

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

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

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

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

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

シングルサインオンを有効にします

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

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

Grid のパスワードを変更

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

関連情報

- StorageGRID の管理
- テナントアカウントを使用する

テナントとクライアント接続を管理する

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

テナントアカウント

テナントアカウントを使用すると、 StorageGRID システムでオブジェクトの格納と読み出しを実行できるユーザを指定し、どの機能を利用可能とするかを設定できます。テナントアカウントは、 S3 REST API または Swift REST API をサポートするクライアントアプリケーションが、 StorageGRID でオブジェクトの格納や読み出しを行うことを可能にします。テナントアカウントでは、それぞれ S3 クライアントプロトコルまたは Swift クライアントプロトコルのどちらかを使用します。

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

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

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

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

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

StorageGRID ノードへのクライアント接続

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

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

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

  CLB サービスは廃止されました。

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

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

1. 必要に応じてハイアベイラビリティ（ HA ）グループを設定します。HA グループを作成すると、複数の管理ノードとゲートウェイノードのインターフェイスがアクティブ / バックアップ構成に追加されます。クライアント接続は、 HA グループの仮想 IP アドレスを使用して確立されます。
2. ロードバランササービスのエンドポイントを設定する。管理ノードまたはゲートウェイノード上のロードバランササービスは、クライアントアプリケーションからの受信ネットワーク接続を複数のストレージノードに分散します。ロードバランサエンドポイントを作成する際には、ポート番号、エンドポイントで

HTTP / HTTPS 接続を許可するかどうか、エンドポイントを使用するクライアントのタイプ（ S3 または Swift ）、 HTTPS 接続に使用する証明書（該当する場合）を指定します。

3. ノードのクライアントネットワークへの接続がすべてロードバランサエンドポイントで行われるようにする場合は、ノードのクライアントネットワークを信頼されていないものとして指定します。

関連情報

- StorageGRID の管理
- テナントアカウントを使用する
- S3 を使用する
- Swift を使用します
- Tenant Manager を確認します
- ネットワークの設定を行います

ネットワークの設定を行います

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

ドメイン名

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

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

ハイアベイラビリティグループ

ハイアベイラビリティ（ HA ）グループを使用して、 S3 / Swift クライアントに可用性の高いデータ接続を提供したり、 Grid Manager および Tenant Manager への可用性の高い接続を提供したりできます。

HA グループを作成するときは、 1 つ以上のノードのネットワークインターフェイスを選択します。各 HA グループは、選択したノードの共有サービスへのアクセスを提供します。

- ゲートウェイノード、管理ノード、またはその両方のインターフェイスを含む HA グループは、 S3 / Swift クライアントに可用性の高いデータ接続を提供します。
- 管理ノード上のインターフェイスを含む HA グループは、 Grid Manager および Tenant Manager への可用性の高い接続のみを提供します。

インターフェイスは、グリッドネットワーク（ eth0 ）、クライアントネットワーク（ eth2 ）、または VLAN ネットワークに属することができます。

各 HA グループに最大 10 個の仮想 IP （ VIP ）アドレスを割り当てることができます。1 つのインターフェイスをプライマリインターフェイスに指定し、他のインターフェイスに優先順位を付けます。プライマリインターフェイスは、障害が発生しないかぎり、アクティブインターフェイスです。アクティブインターフェイスに障害が発生すると、 VIP アドレスはプライオリティ順に最初のバックアップインターフェイスに移動します。そのインターフェイスに障害が発生すると、 VIP アドレスは次のバックアップインターフェイスに移動します。

リンクコスト

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

ロードバランサエンドポイント

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

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

トラフィック分類

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

VLAN インターフェイス

仮想 LAN （ VLAN ）インターフェイスを作成してトラフィックを分離し、パーティションを作成することで、セキュリティ、柔軟性、パフォーマンスを向上させることができます。各 VLAN インターフェイスは、管理ノードおよびゲートウェイノード上の 1 つ以上の親インターフェイスに関連付けられます。HA グループでは VLAN インターフェイスを使用し、ロードバランサエンドポイントではクライアントトラフィックと管理トラフィックをアプリケーションまたはテナントごとに分離できます。

たとえば、ネットワークで FabricPool トラフィックに VLAN 100 を使用し、アーカイブアプリケーションに VLAN 200 を使用しているとします。

関連情報

- StorageGRID の管理
- テナントとクライアント接続を管理する

セキュリティを設定します

StorageGRID システムのセキュリティを保護するために、 Grid Manager でさまざまなセキュリティ設定を行うことができます。

証明書

StorageGRID では、 2 種類のセキュリティ証明書が使用されます。

- HTTPS 接続を使用する場合は、サーバ証明書が必要です。サーバ証明書は、クライアントとサーバ間のセキュアな接続を確立し、クライアントに対するサーバの ID を認証し、データのセキュアな通信パスを提供するために使用されます。サーバとクライアントには、それぞれ証明書のコピーがあります。
- クライアント証明書は、クライアントまたはユーザ ID をサーバに対して認証し、パスワードだけではなくよりも安全な認証を提供します。クライアント証明書はデータを暗号化しません。

すべての StorageGRID 証明書は、 * configuration * > * Security * > * Certificates * ページで表示できます。

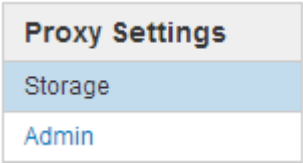
キー管理サーバ

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

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

プロキシ設定

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



信頼されていないクライアントネットワーク

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

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

関連情報

- StorageGRID の管理
- テナントとクライアント接続を管理する

システム設定を構成します

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

表示オプション

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

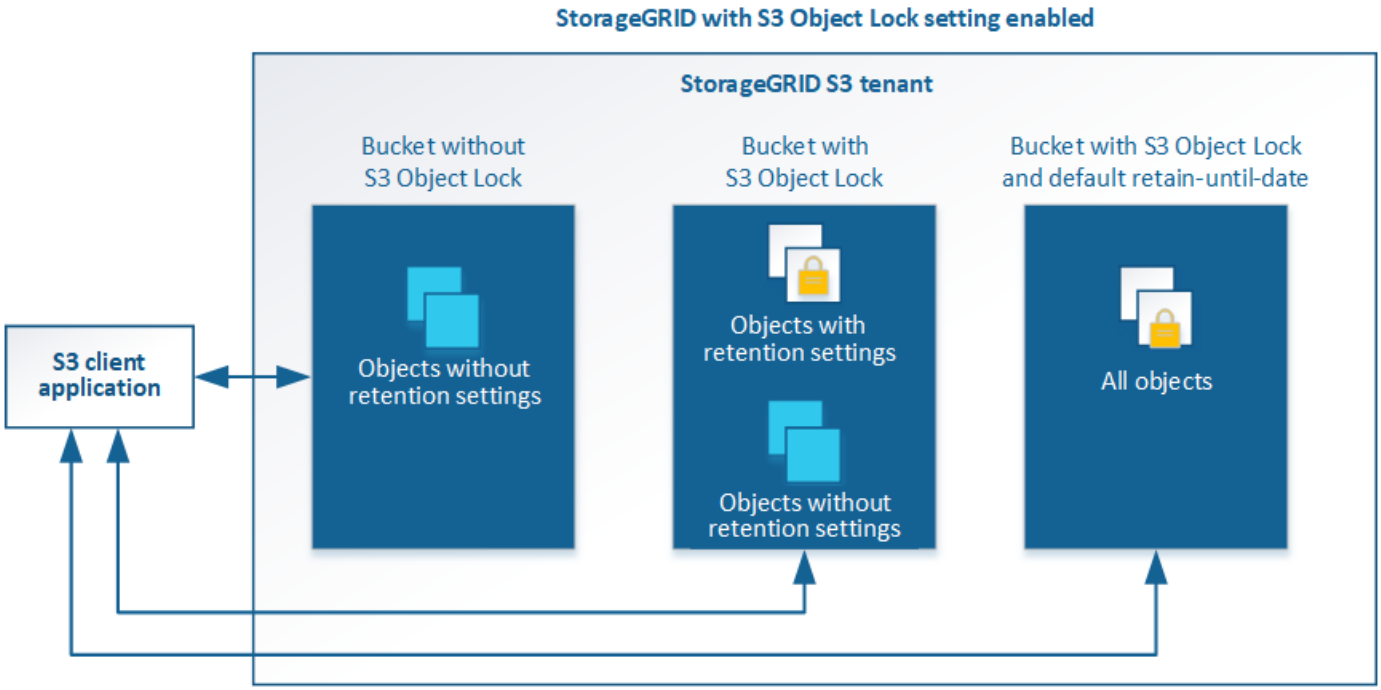
グリッドオプション

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

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

S3 オブジェクトのロック

StorageGRID S3 オブジェクトロック機能は、 Amazon Simple Storage Service （ Amazon S3 ）での S3 オブジェクトロックに相当するオブジェクト保護解決策 です。StorageGRID システムに対してグローバルな S3 オブジェクトロック設定を有効にすると、 S3 テナントアカウントで S3 オブジェクトのロックを有効にした状態でバケットを作成できるようになります。テナントは、 S3 クライアントアプリケーションを使用して、オプションでバケット内のオブジェクトの保持設定（終了日、リーガルホールド、またはその両方）を指定できます。また、 S3 オブジェクトのロックが有効になっている各バケットでは、必要に応じてデフォルトの保持モードと保持期間を使用できます。この期間は、オブジェクトを独自の保持設定なしでバケットに追加した場合に適用されます。



ストレージオプション

ストレージオプションを使用すると、オブジェクトのセグメント化を制御したり、ストレージボリュームのウォーターマーク設定を上書きして、ストレージノードの使用可能なストレージスペースを管理したりできます。

情報ライフサイクル管理を使用

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

ILM ルールでは次の項目を定義

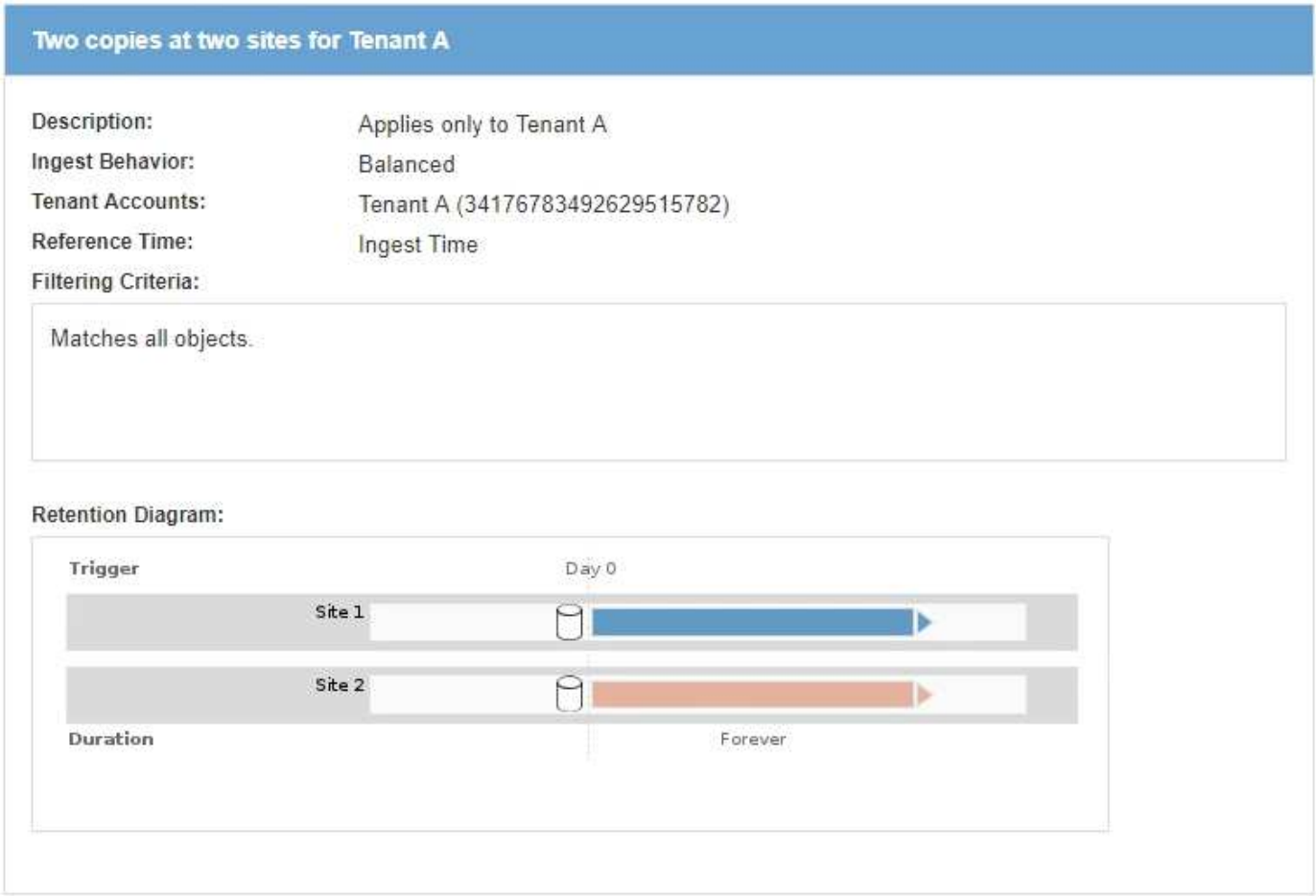
- 格納するオブジェクト。ルールはすべてのオブジェクトに適用することも、ルール環境 を構成するオブジェクトを特定するフィルタを指定することもできます。たとえば、特定のテナントアカウント、特定の S3 バケットまたは Swift コンテナ、または特定のメタデータ値に関連付けられたオブジェクトにのみルールを適用できます。
- ストレージのタイプと場所。オブジェクトは、ストレージノード、クラウドストレージプール、またはアーカイブノードに格納できます。
- 作成するオブジェクトコピーのタイプ。コピーはレプリケートまたはイレイジャーコーディングできます。
- レプリケートコピーの場合は、作成されるコピー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

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

ILM ルールの例

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

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



ILM ポリシーによるオブジェクトの評価方法

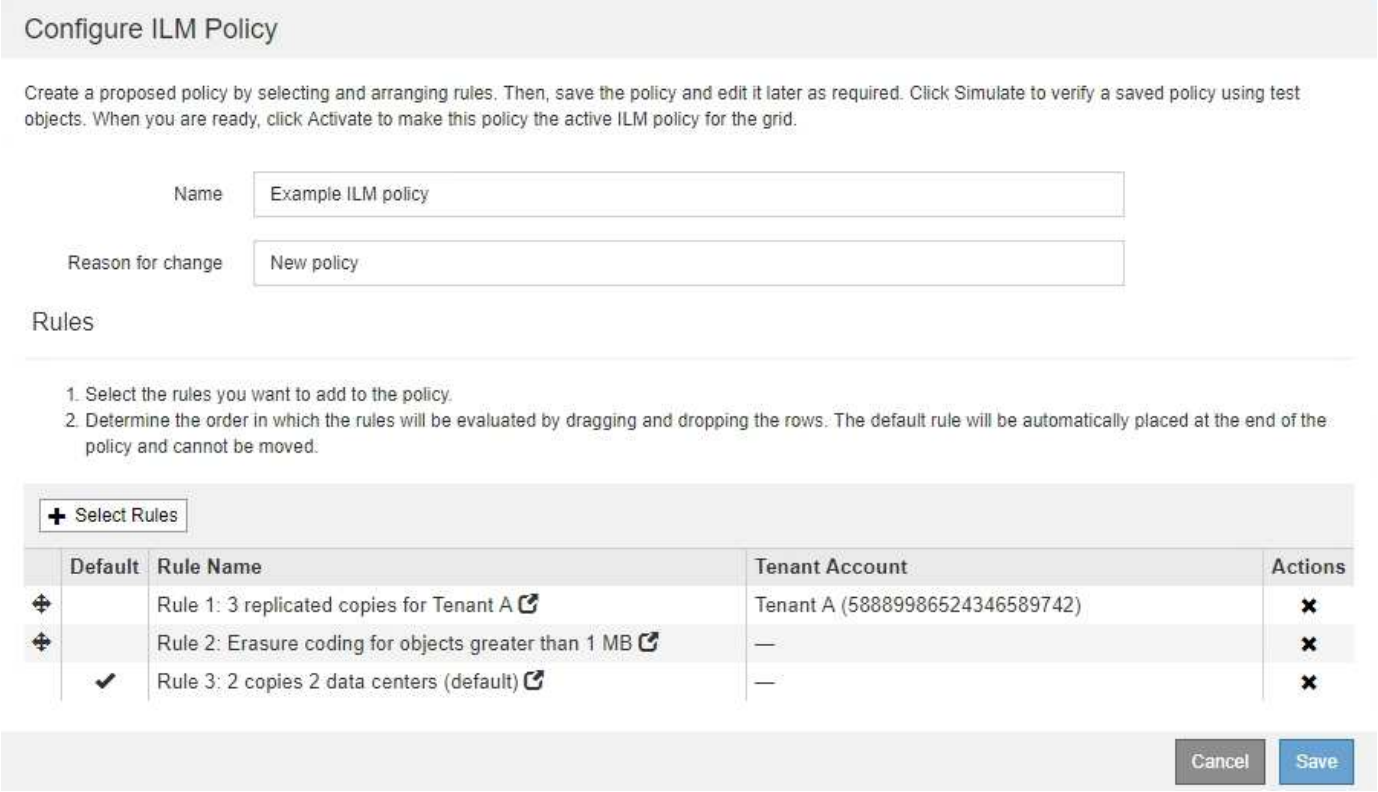
StorageGRID システムのアクティブな ILM ポリシーは、すべてのオブジェクトの配置、期間、データ保護を制御します。

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

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

ILM ポリシーの例

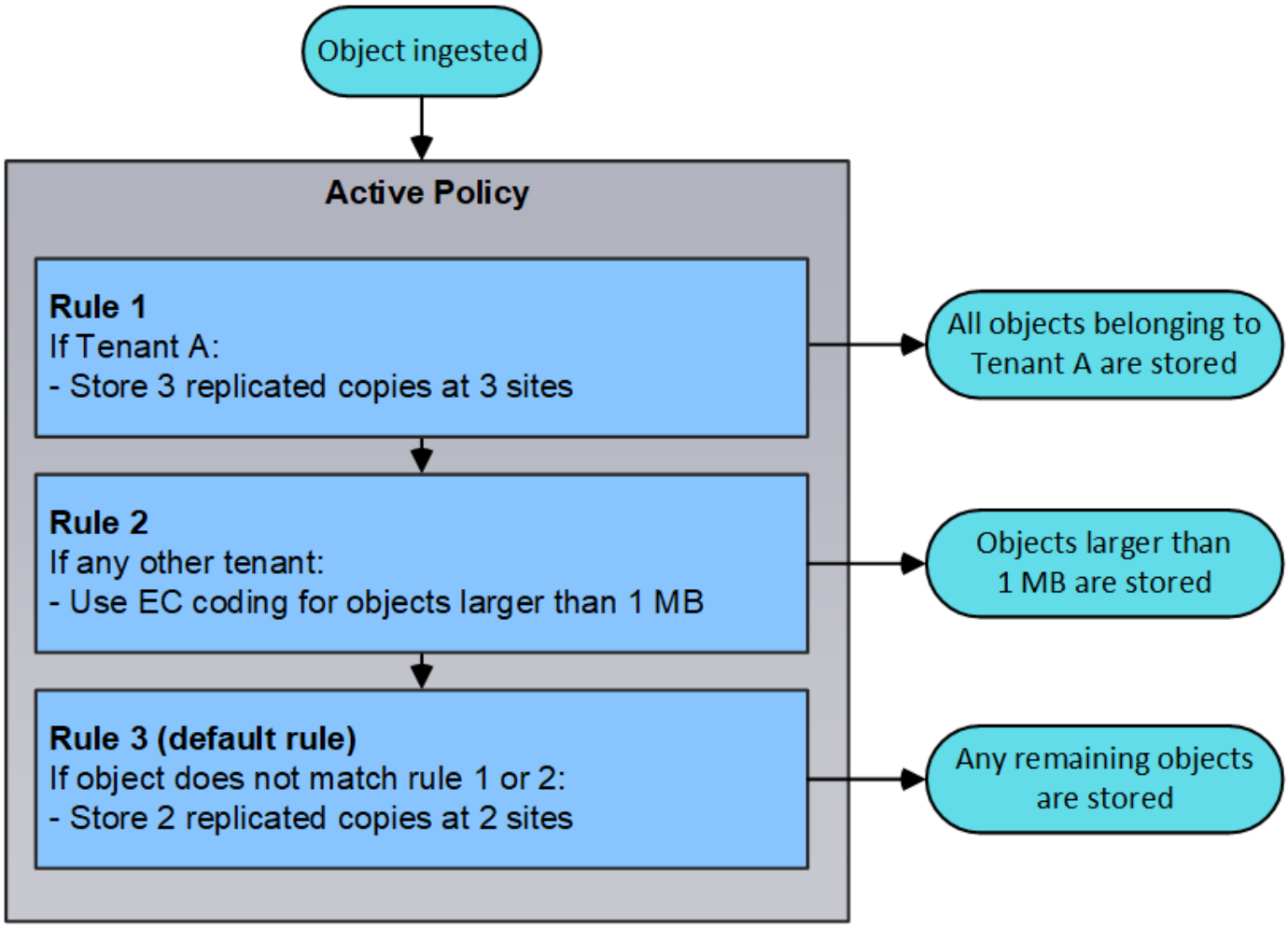
この例の ILM ポリシーは 3 つの ILM ルールを使用します。



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

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

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

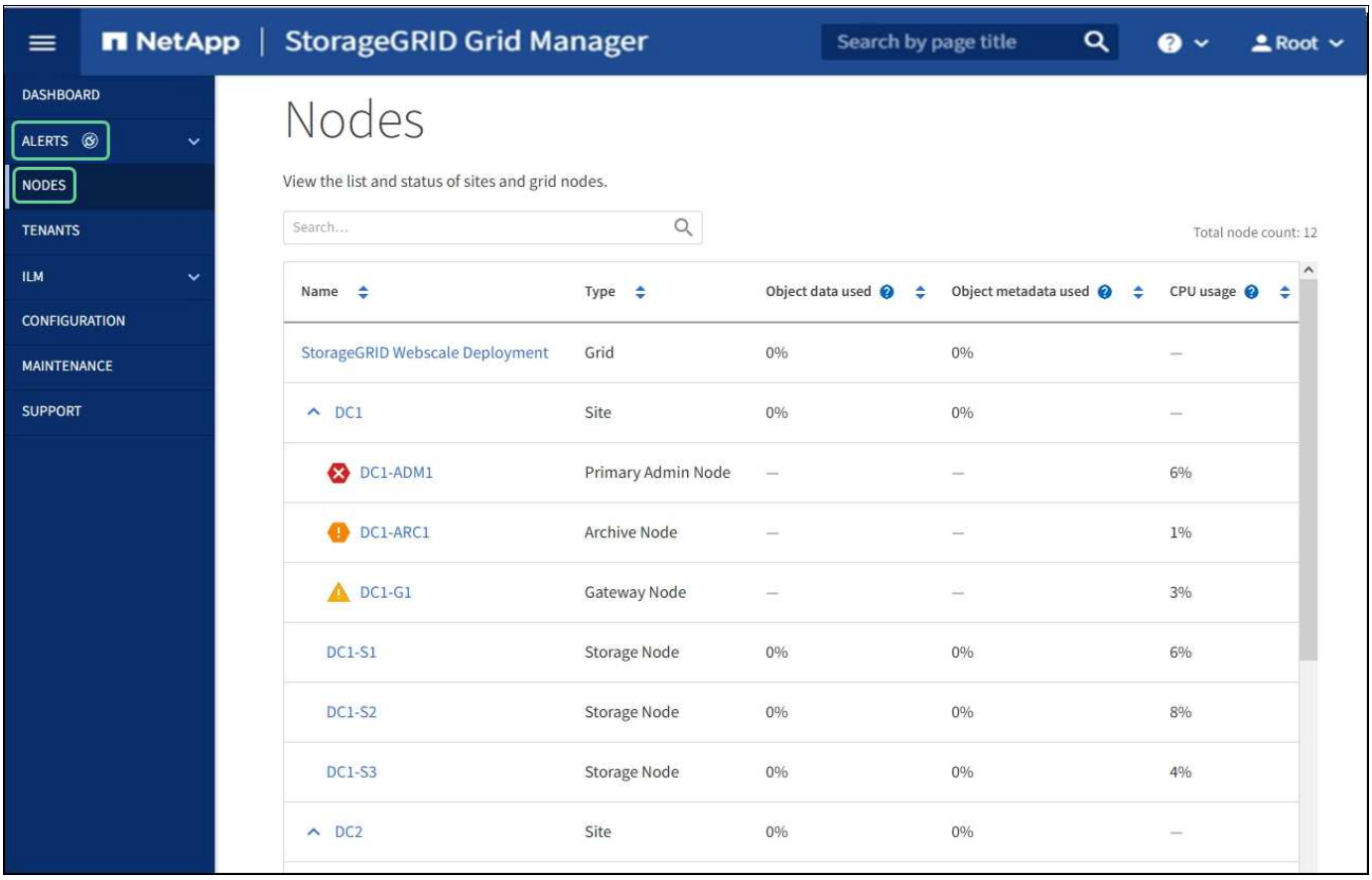


- 関連情報 *
- ILM を使用してオブジェクトを管理する

処理を監視

Nodes ページを表示します

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



Nodes テーブルには、 StorageGRID システム内のすべてのサイトとノードが表示されます。ノードごとに概要情報が表示されます。ノードにアクティブなアラートがある場合は、ノード名の横にアイコンが表示されます。ノードが接続されていてアクティブなアラートがない場合は、アイコンは表示されません。

接続状態アイコン

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

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

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

ノードがグリッドから切断された場合は、基になるアラートが表示される可能性がありますが、「未接続」アイコンのみが表示されます。ノードのアクティブなアラートを表示するには、ノードを選択します。

警告アイコン

ノードにアクティブなアラートがある場合は、ノード名の横に次のアイコンが表示されます。

- * 重要 * ：異常な状態で、 StorageGRID のノードやサービスの通常の動作が停止しています。基盤となる問題 にすぐに対処する必要があります。問題 が解決されないと、サービスの停止やデータの損失を招くおそれがあります。
- * メジャー * ：異常な状態で、現在の処理に影響しているか、重大アラートのしきい値に近づいています。Major アラートを調査し、根本的な問題に対処して、異常な状態が発生した場合に StorageGRID のノードやサービスが正常に動作しなくなる事態を防ぐ必要があります。
- * マイナー * ：システムは正常に動作していますが、継続するとシステムの動作に影響する可能性がある異常な状態が発生しています。自動的にクリアされない Minor アラートを監視し、解決して、深刻な問題が生じないようにする必要があります。

システム、サイト、またはノードの詳細

使用可能な情報を表示するには、グリッド、サイト、またはノードの名前を次のように選択します。

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

Nodes ページのタブ

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

タブ名	説明	に含まれます
概要	• 各ノードの基本情報が表示されます。 • ノードに影響しているアクティブなアラートが表示されます。	すべてのノード
ハードウェア	• 各ノードの CPU 利用率とメモリの使用状況が表示されます • アプライアンスノードについては、ハードウェア情報も表示されます。	すべてのノード
ネットワーク	ネットワークインターフェイス間で送受信されるネットワークトラフィックを示すグラフが表示されます。単一のノードのビューには、そのノードの追加情報 が表示されます。	すべてのノード、各サイト、グリッド全体
ストレージ	• 各ノードのディスクデバイスとボリュームの詳細が表示されます。 • ストレージノード、各サイト、およびグリッド全体の場合、オブジェクトデータストレージとメタデータストレージの使用量の推移を示すグラフが表示されます。	すべてのノード、各サイト、グリッド全体

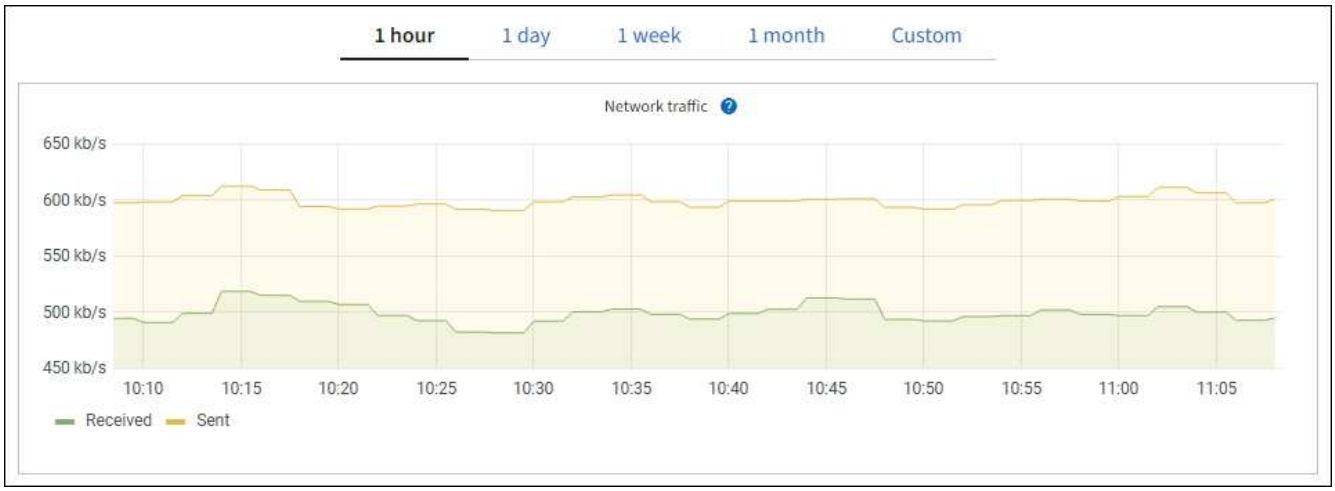
タブ名	説明	に含まれます
オブジェクト	• S3 および Swift の取り込み速度と読み出し速度に関する情報が表示されます。 • ストレージノードの場合、オブジェクト数や、メタデータストアのクエリとバックグラウンド検証に関する情報が表示されます。	ストレージノード、各サイト、グリッド全体
ILM	情報ライフサイクル管理（ ILM ）処理に関する情報が表示されます。 • ストレージノードの場合、 ILM 評価およびイレイジャーコーディングオブジェクトのバックグラウンド検証に関する詳細が表示されます。 • 各サイトおよびグリッド全体の場合、 ILM キューの状況の推移を示すグラフが表示されます。 • グリッド全体の場合、 ILM によるすべてのオブジェクトのフルスキャンが完了するまでの推定時間が表示されます。	ストレージノード、各サイト、グリッド全体
ロードバランサ	ロードバランササービスに関連するパフォーマンスグラフと診断グラフが表示されます。 • 各サイトの場合、そのサイトのすべてのノードの統計が要約して表示されます。 • グリッド全体の場合、すべてのサイトの統計が要約して表示されます。	管理ノードとゲートウェイノード、各サイト、およびグリッド全体
プラットフォームサービス	サイトでの S3 プラットフォームサービスの処理に関する情報が表示されます。	各サイト
SANtricity システムマネージャ	SANtricity システムマネージャへのアクセスを許可します。SANtricity System Manager では、ストレージコントローラのハードウェア診断および環境情報と、ドライブに関連する問題を確認できます。	ストレージアプライアンスノード *注：ストレージアプライアンスのコントローラファームウェアが8.70（11.70）より前の場合、SANtricity のSystem Managerタブは表示されません。

Prometheus 指標

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

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

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



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

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

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

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

StorageGRID 属性

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

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

- * Nodes ページ * ： Nodes ページに表示される値の多くは StorageGRID 属性です。（ Prometheus 指標はノードのページにも表示されます）。
- * アラーム * ：属性が定義されたしきい値に達すると、特定の重大度レベルで StorageGRID アラーム（レガシーシステム）がトリガーされます。
- * グリッドトポロジツリー * ：属性値はグリッドトポロジツリーに表示されます（ * support * > * Tools * > * Grid topology * ）。

- * Events * ：システムイベントは、特定の属性がネットワークエラーなどのエラーや障害をノードに記録したときに発生します。

属性値

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

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

関連情報

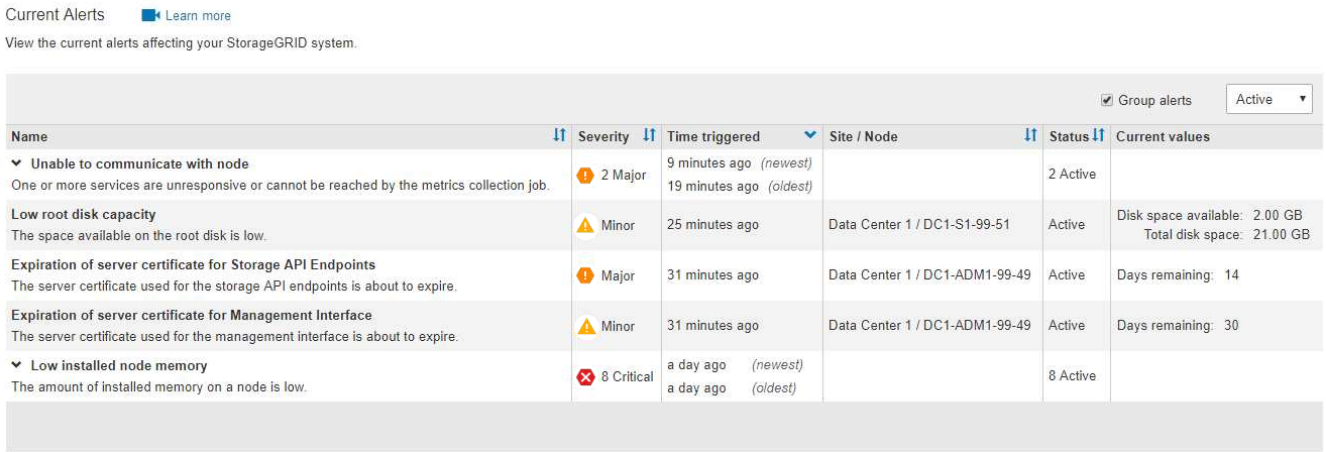
- 監視とトラブルシューティング
- アラートを監視および管理する
- StorageGRID のサポートオプションを使用する

アラートを監視および管理する

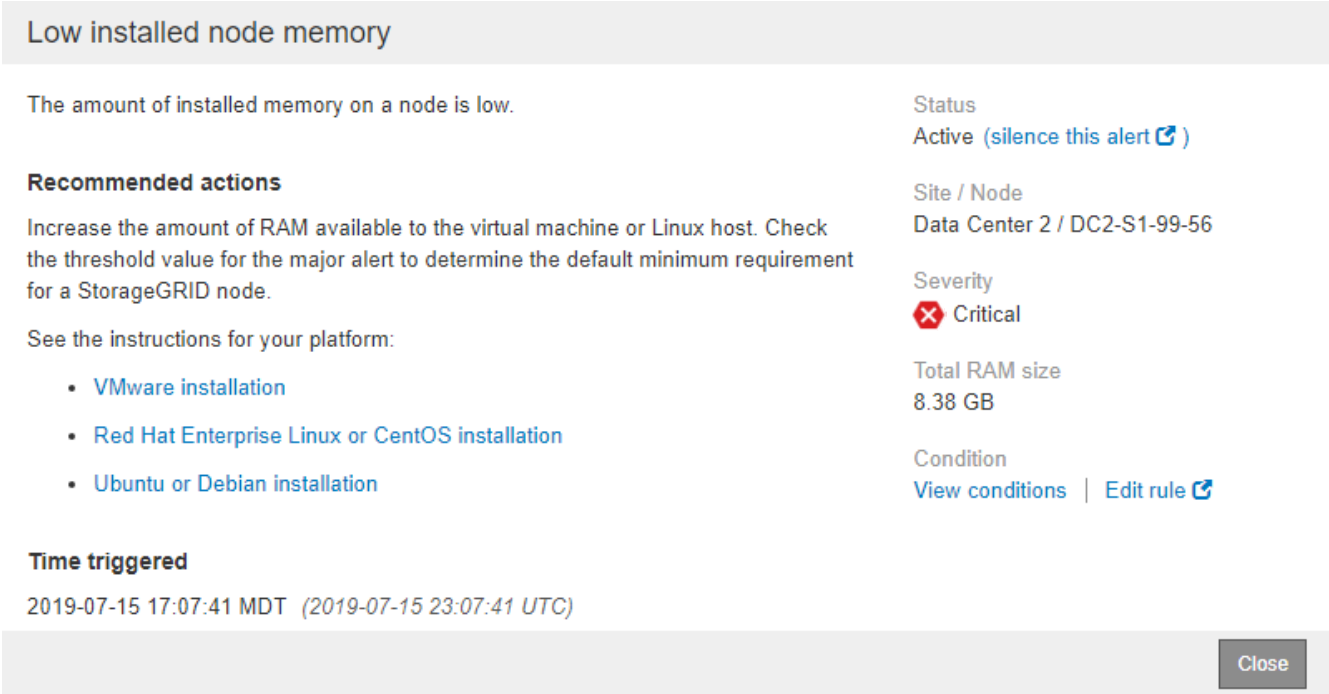
アラートシステムでは、 StorageGRID の運用中に発生する問題を、使いやすいインターフェイスを通じて検出し、評価し、解決することができます。

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

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



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



従来のアラームシステムは廃止されました。このアラームシステムのユーザインターフェイスと API は、今後のリリースで削除される予定です。アラートシステムには大きなメリットがあり、使いやすくなっています。

アラートの管理

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

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

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

```
node_memory_MemTotal < 24000000000
```

関連情報

監視とトラブルシューティング

SNMP による監視を使用する

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

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

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

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

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

トラップ通知およびインフォーム通知は、次の場合に送信されます。

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

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

- 関連情報 *
- 監視とトラブルシューティング

監査メッセージを確認します

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

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

- システム監査メッセージは、監査システム自体、グリッドノードの状態、システム全体のタスクアクティビティ、およびサービスバックアップ処理に関連します。
- オブジェクトストレージの監査メッセージは、オブジェクトの格納と読み出し、グリッドノードからグリッドノードへの転送、検証など、 StorageGRID 内のオブジェクトの格納と管理に関連します。
- クライアント読み取り / 書き込み監査メッセージは、 S3 または Swift クライアントアプリケーションがオブジェクトの作成、変更、または読み出しの要求を行うときに記録されます。
- 管理監査メッセージには、管理 API に対するユーザ要求が記録されます。

各管理ノードで、監査メッセージがテキストファイルに保存されます。監査共有には、アクティブファイル（ audit.log ）と、圧縮された過去の監査ログが含まれています。さらに、グリッド内の各ノードでは、一部の監査メッセージがローカルログファイル（ localaudit.log ）に格納されます。

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

必要に応じて、管理ノードとローカルノードに格納されている監査情報を外部 syslog サーバに送信することができます。外部 syslog サーバを使用すると、監査情報の管理やネットワークトラフィックの削減が容易になります。を参照してください 監査メッセージとログの送信先を設定します を参照してください。

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

関連情報

- 監査ログを確認します
- StorageGRID の管理

メンテナンスを実施します

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

ソフトウェアの更新

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

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

StorageGRID ソフトウェアのアップグレード

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

す。

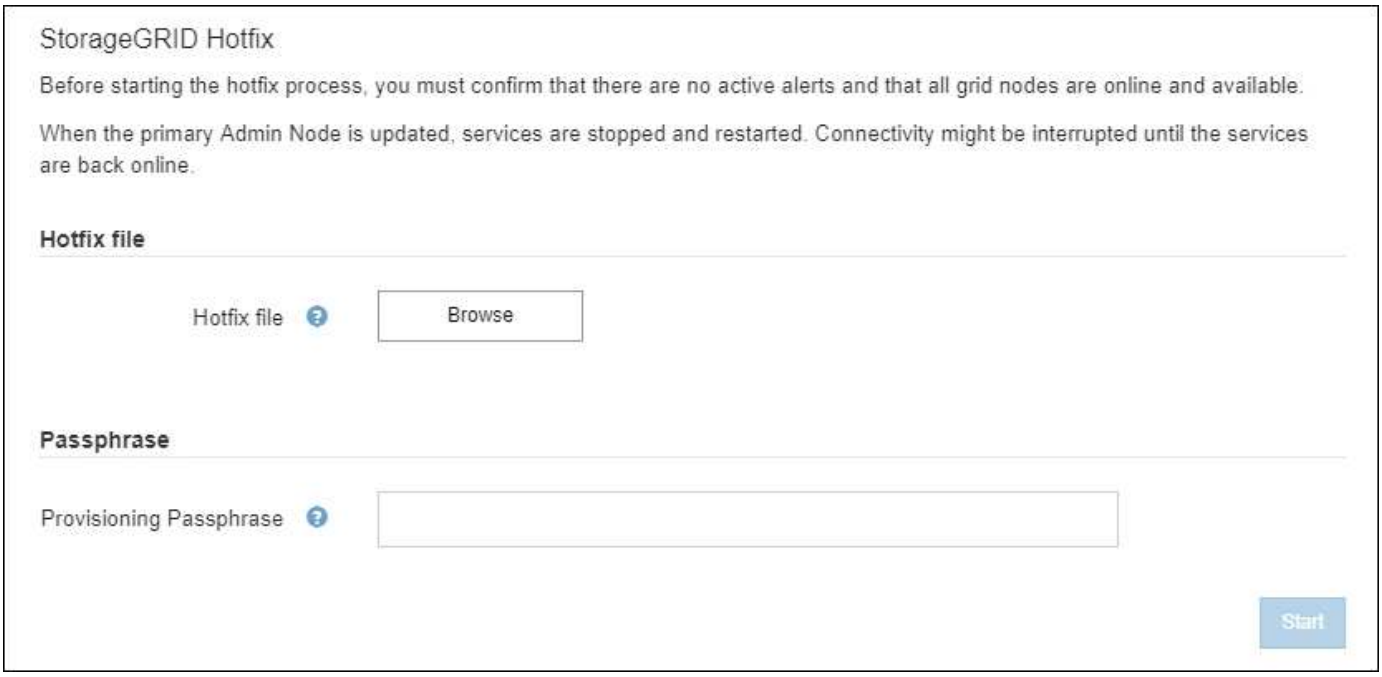
StorageGRID ソフトウェアのアップグレード中も、クライアントアプリケーションはオブジェクトデータの取り込みと読み出しを継続できます。

ホットフィックス

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

StorageGRID のホットフィックスには、フィーチャーパックまたはフィーチャーパックに含まれないソフトウェアの変更が含まれます。今後のリリースにも同じ変更が含まれます。

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



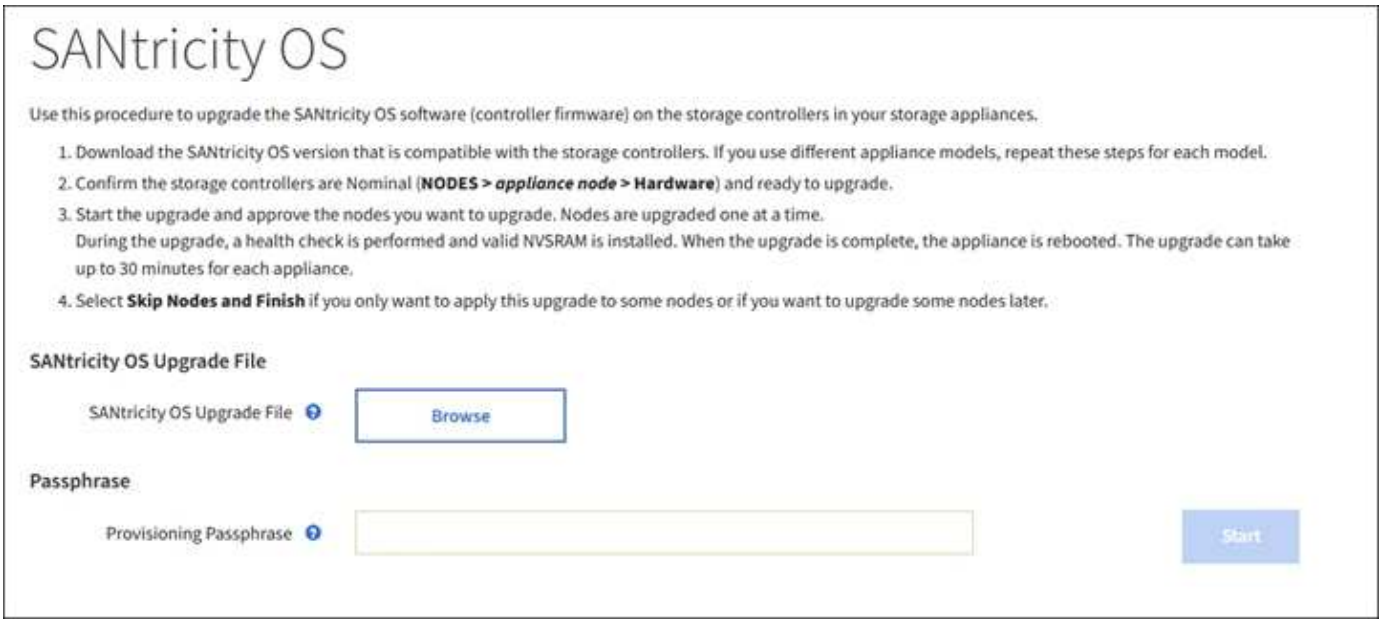
ホットフィックスは、最初にプライマリ管理ノードに適用されます。その後、 StorageGRID システム内のすべてのノードで同じソフトウェアバージョンが実行されるまで、他のグリッドノードへのホットフィックスの適用を承認する必要があります。個々のグリッドノード、グリッドノードのグループ、またはすべてのグリッドノードを選択して、承認順序をカスタマイズできます。

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

SANtricity OS のアップグレード

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

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

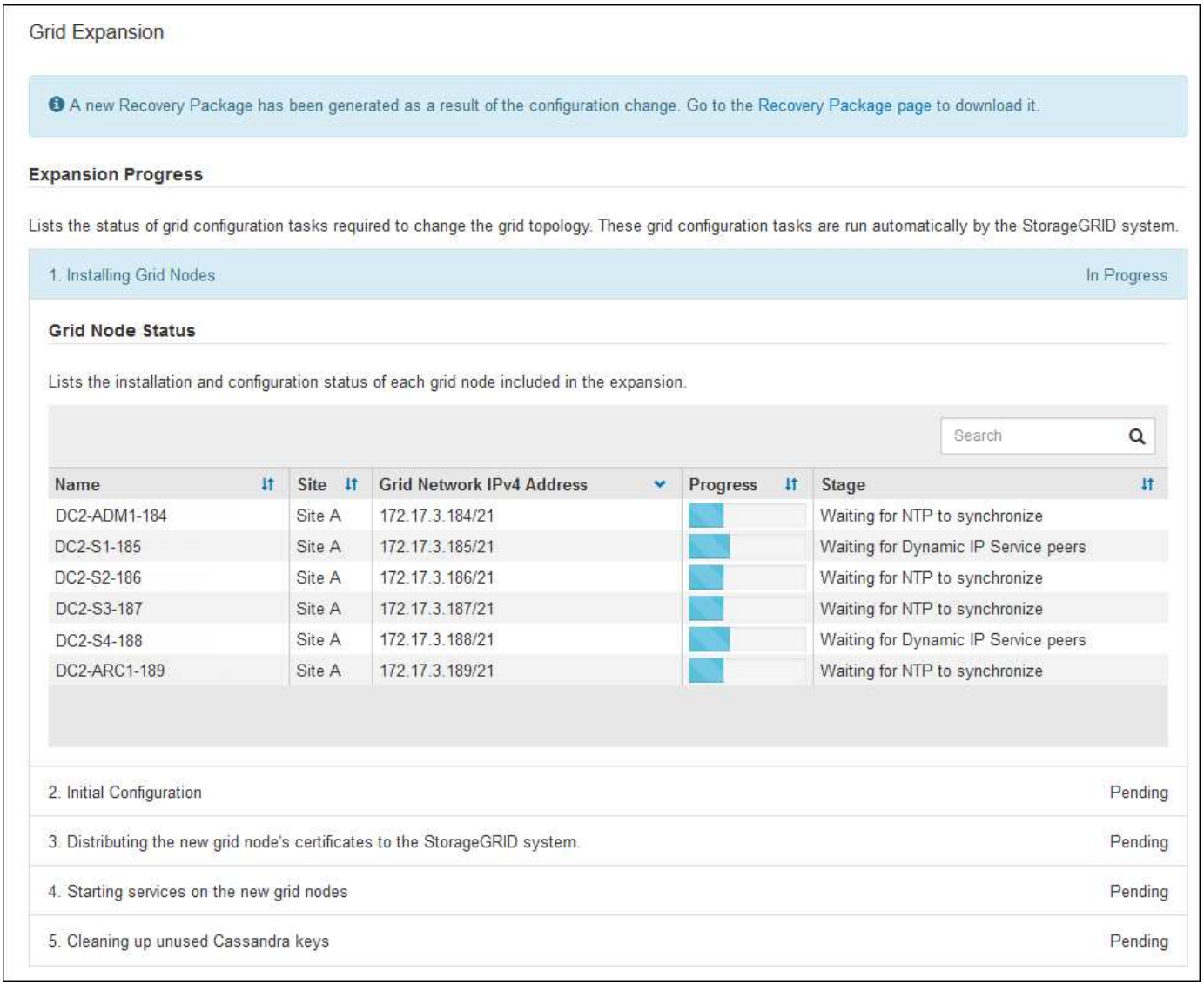


ファイルをアップロードしたあと、個々のストレージノードまたはすべてのノードでアップグレードを承認できます。ノードを選択的に承認できるため、アップグレードのスケジュールを簡単に設定できます。アップグレード用にノードを承認すると、システムによってヘルスチェックが実行され、ノードに適用できる場合はアップグレードがインストールされます。

拡張手順

StorageGRID システムを拡張するには、ストレージノードにストレージボリュームを追加するか、既存のサイトに新しいグリッドノードを追加するか、新しいデータセンターサイトを追加します。SG6060またはSG6060Xストレージアプライアンスを使用するストレージノードがある場合は、拡張シェルフを1台または2台追加してノードのストレージ容量を2倍または3倍にすることができます。

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

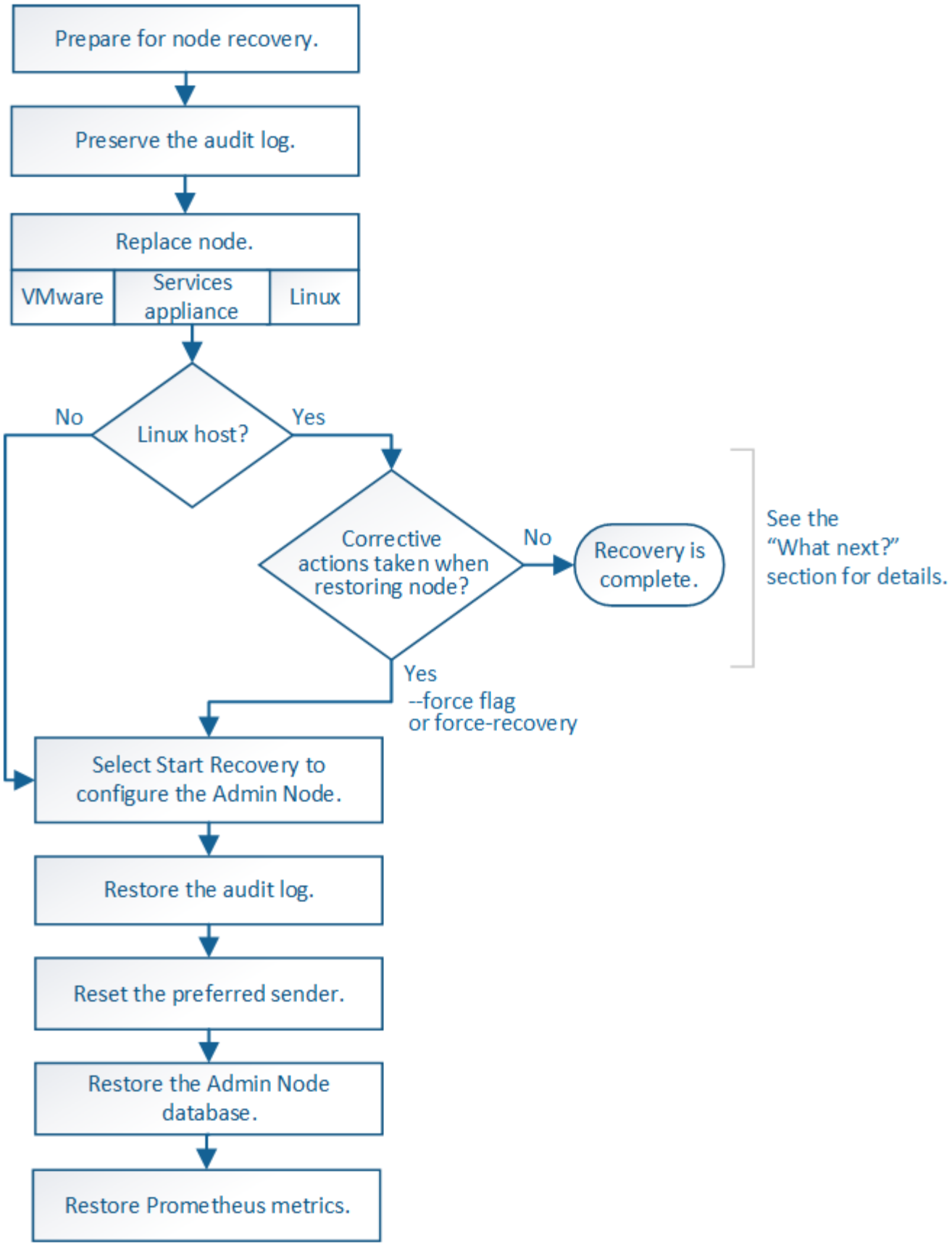


ノードのリカバリ手順

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

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

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



運用停止手順

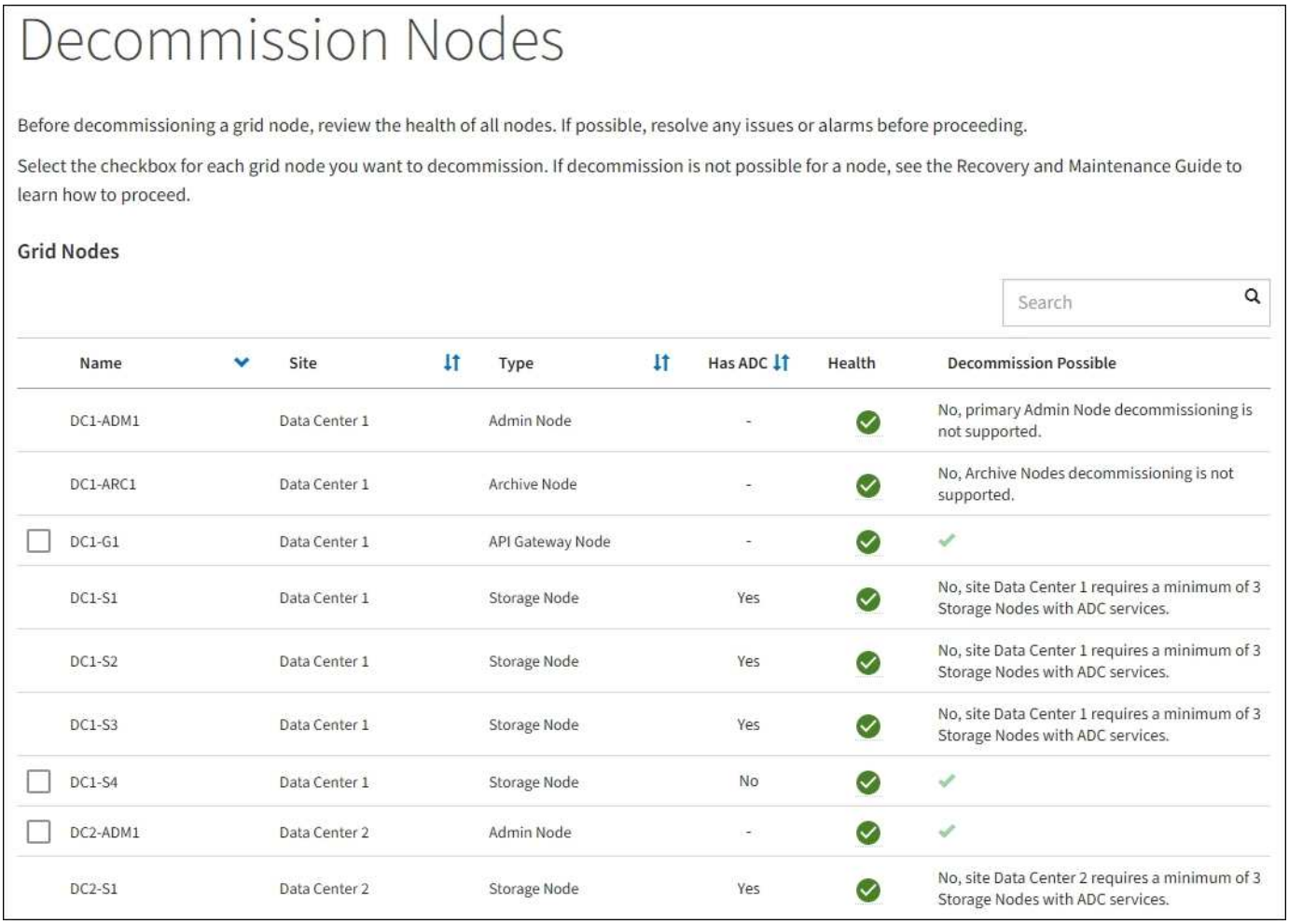
グリッドノードまたはデータセンターサイト全体を StorageGRID システムから完全に削除できます。

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

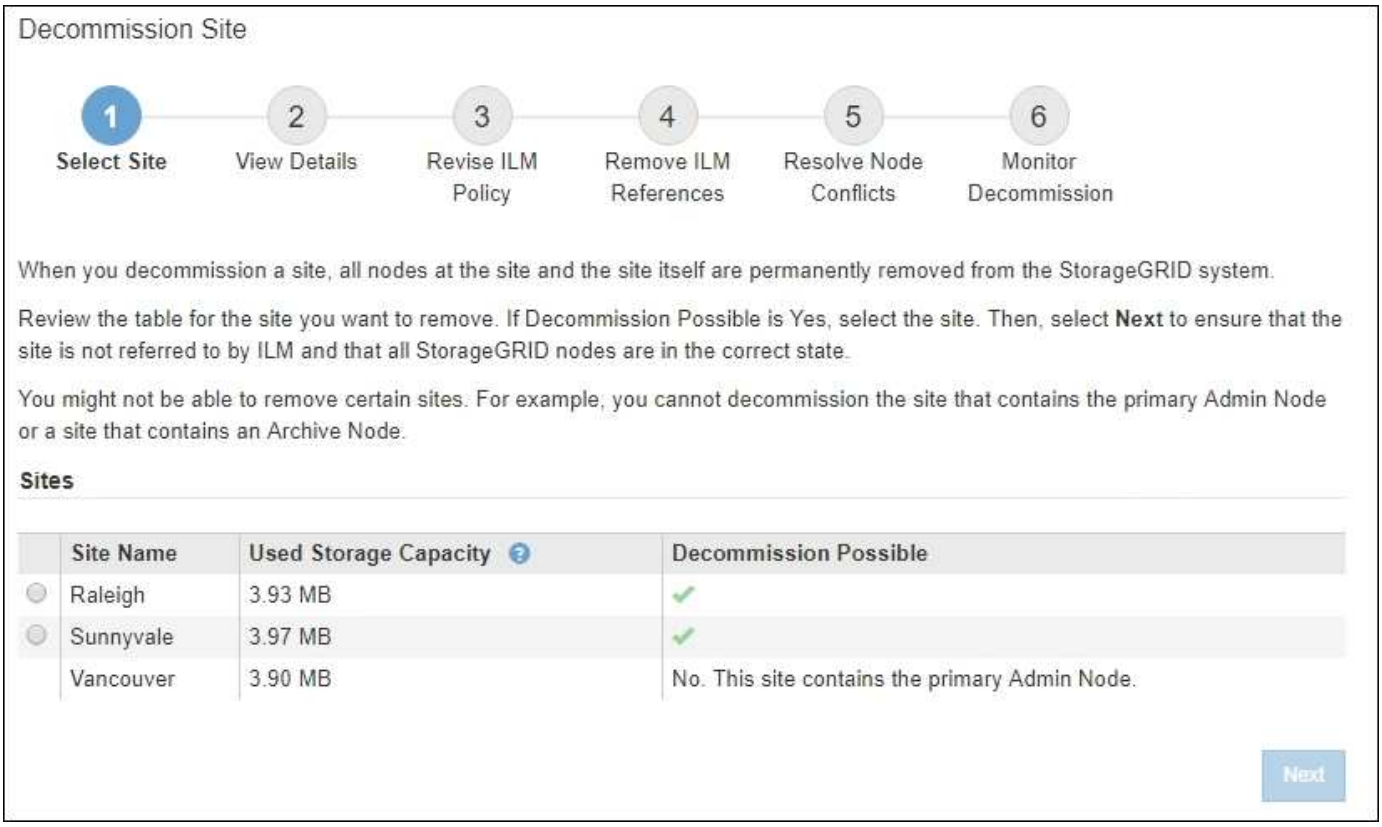
- システムに大きなストレージノードを追加したあとに、オブジェクトを保持したまま小さなストレージノードを 1 つ以上削除する場合。
- 総ストレージ容量を減らす必要がある場合。
- ゲートウェイノードまたは非プライマリ管理ノードが不要になった場合。
- 切断されていて、リカバリしたりオンラインに戻したりすることができないノードがグリッドに含まれている場合。

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

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



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



ネットワークのメンテナンス手順

実行する必要があるネットワークメンテナンス手順には、次のものがあります。

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

ホストレベルおよびミドルウェアの手順

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

アプライアンスノードのクローニング

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

グリッドノードの手順

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

関連情報

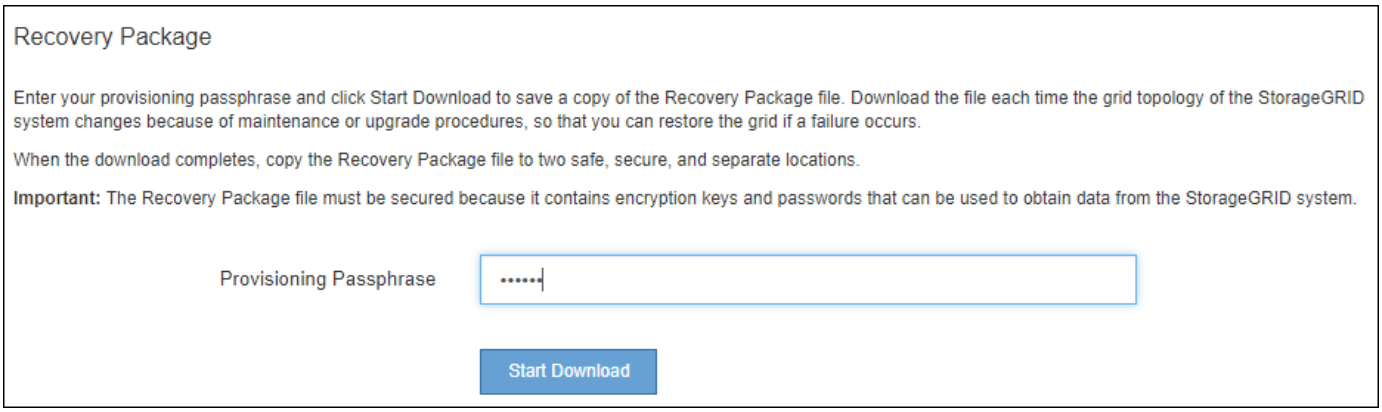
- StorageGRID の管理
- ソフトウェアをアップグレードする
- グリッドを展開します
- リカバリとメンテナンス

リカバリパッケージをダウンロードします

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

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

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



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

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

関連情報

- ソフトウェアをアップグレードする

- グリッドを展開します
- リカバリとメンテナンス

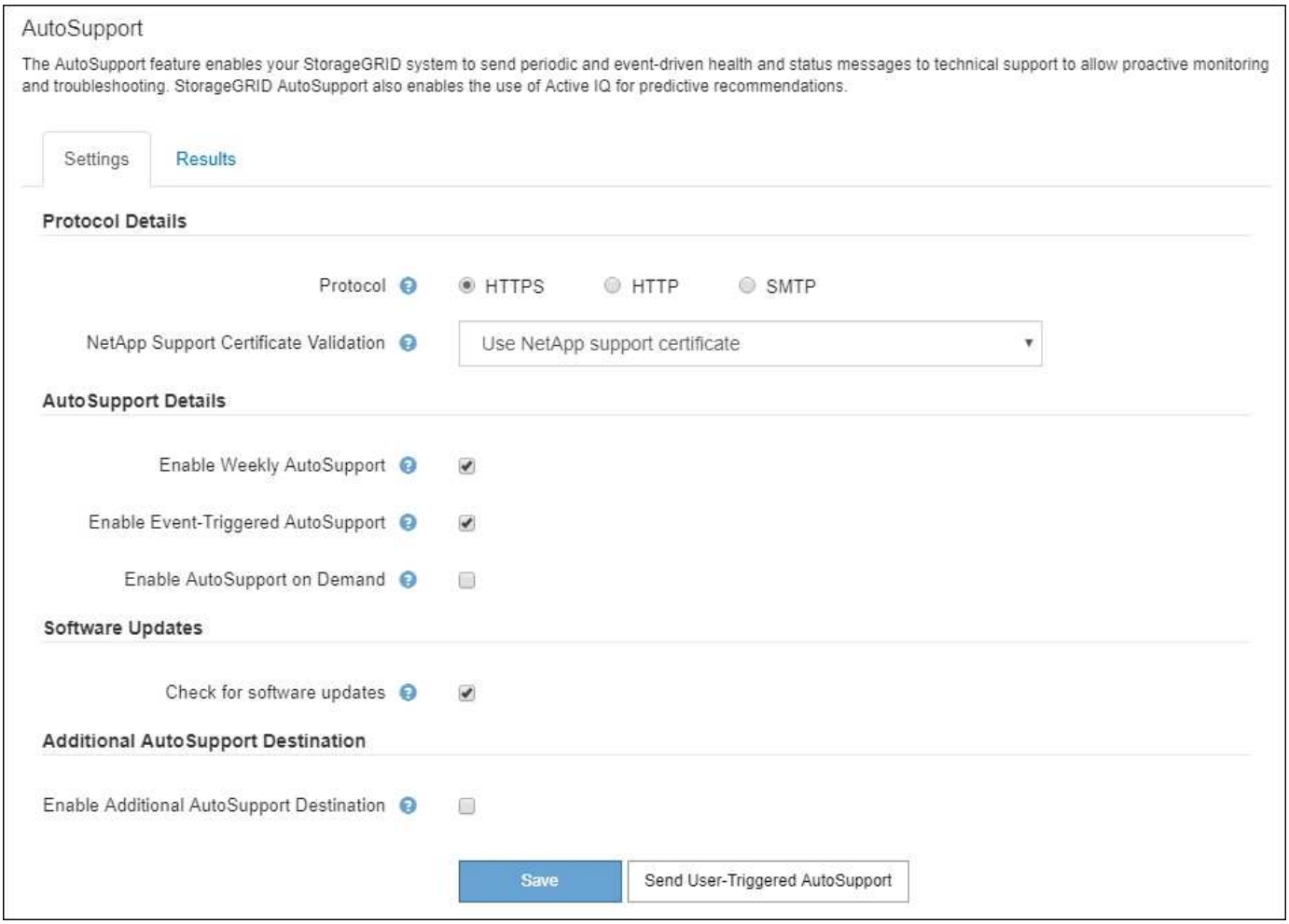
StorageGRID のサポートオプションを使用する

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

AutoSupport を設定します

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

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



AutoSupport メッセージに含まれる情報

AutoSupport メッセージには次のような情報が含まれます。

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

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

メッセージを閉じても、 AutoSupport が無効なままであっても、ブラウザキャッシュがクリアされるまでは再度表示されません。

Digital Advisorを使用します

Active IQデジタルアドバイザはクラウドベースで、NetAppのインストールベースから得られた予測分析と集合知を活用します。継続的なリスク評価、予測アラート、規範となるガイダンス、自動化されたアクションによって、問題が発生する前に予防できます。これにより、システムの健全性が向上し、システムの可用性が向上します。

デジタルアドバイザのダッシュボードと機能をNetAppサポートサイトで使用する場合は、AutoSupportを有効にする必要があります。

"Digital Advisorドキュメント"

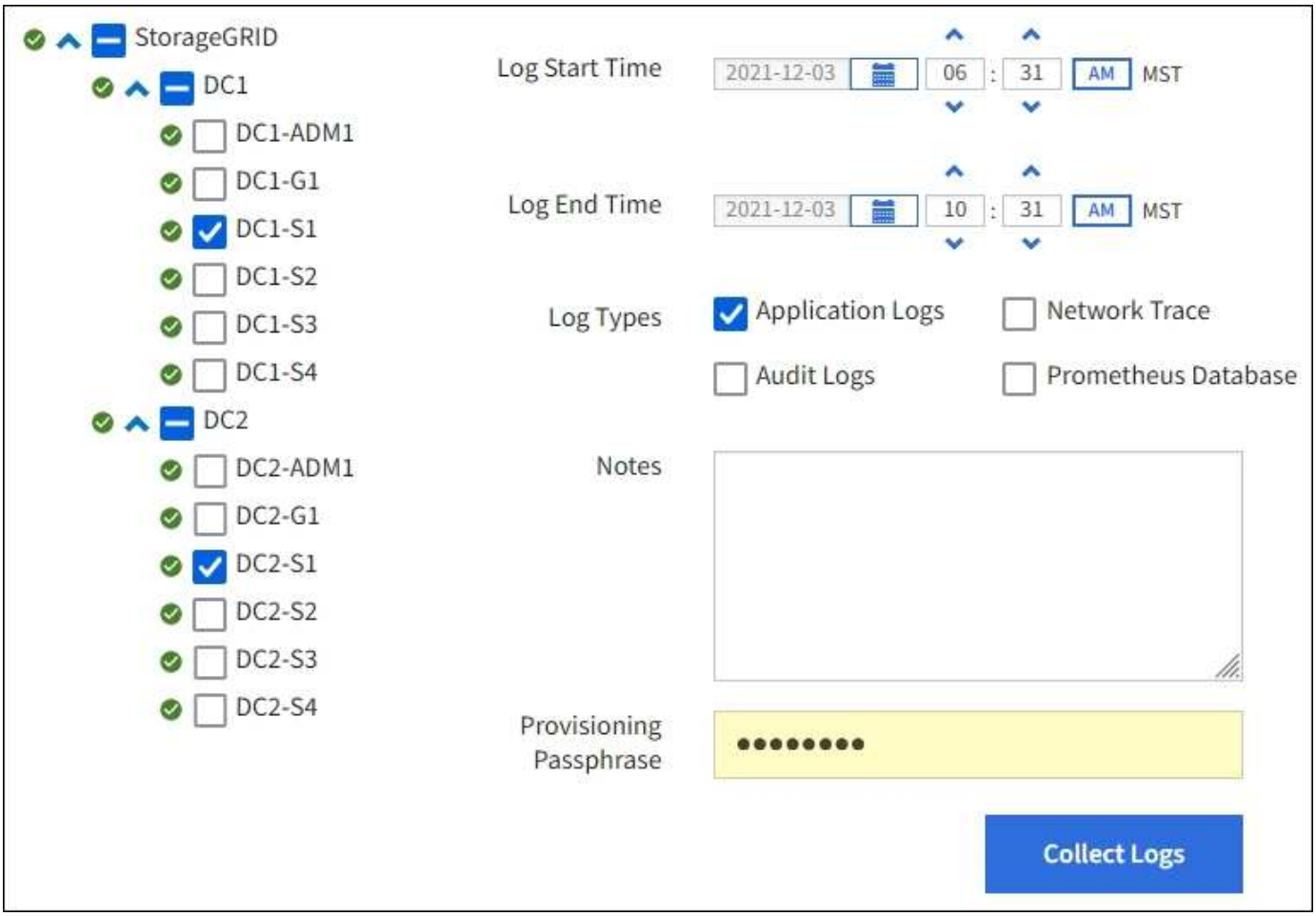
StorageGRID ログを収集

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

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

関連するログファイル、サードパーティアプリケーションに関連するログファイルも作成されます。

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



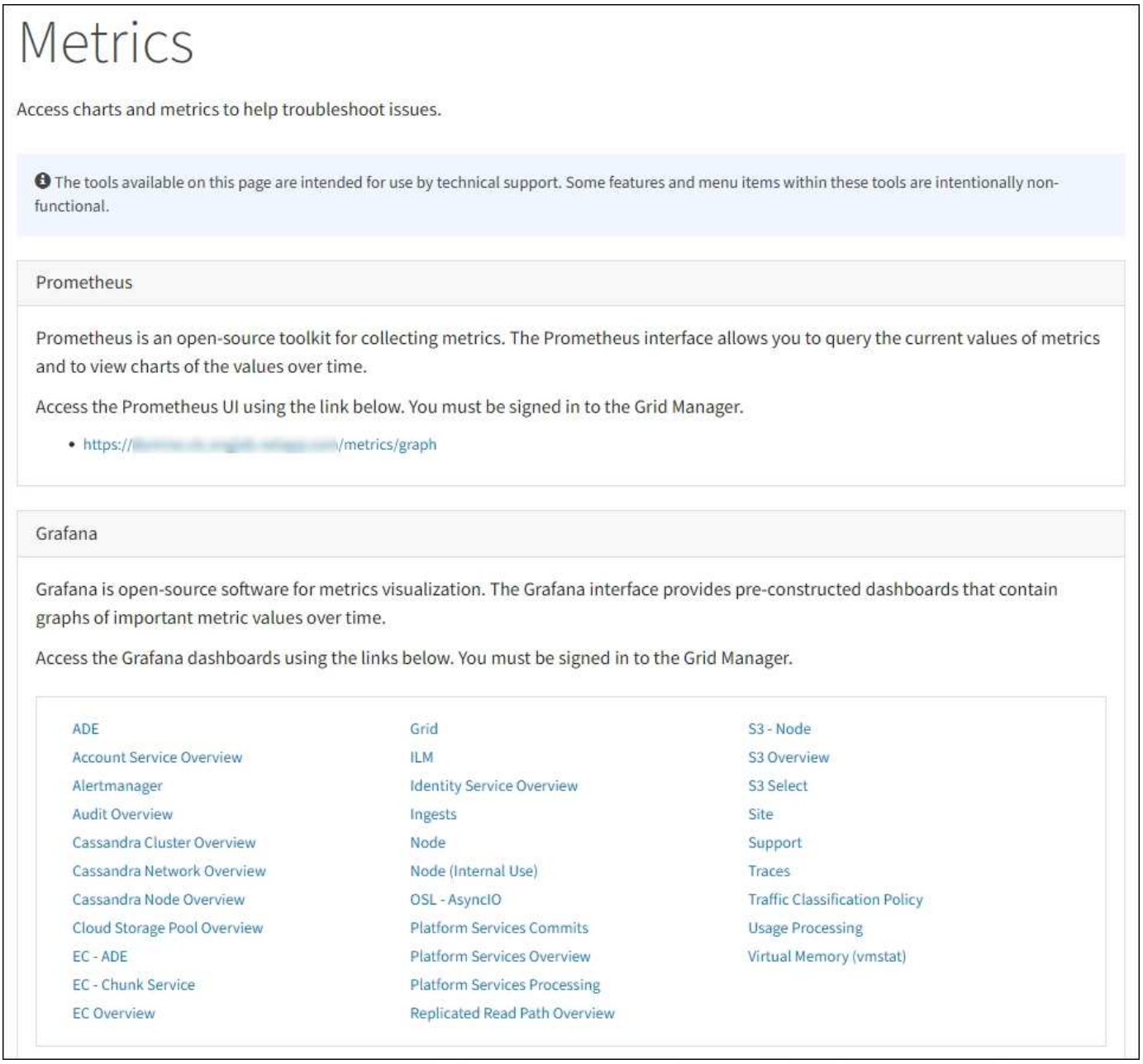
指標を使用して診断を実行

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

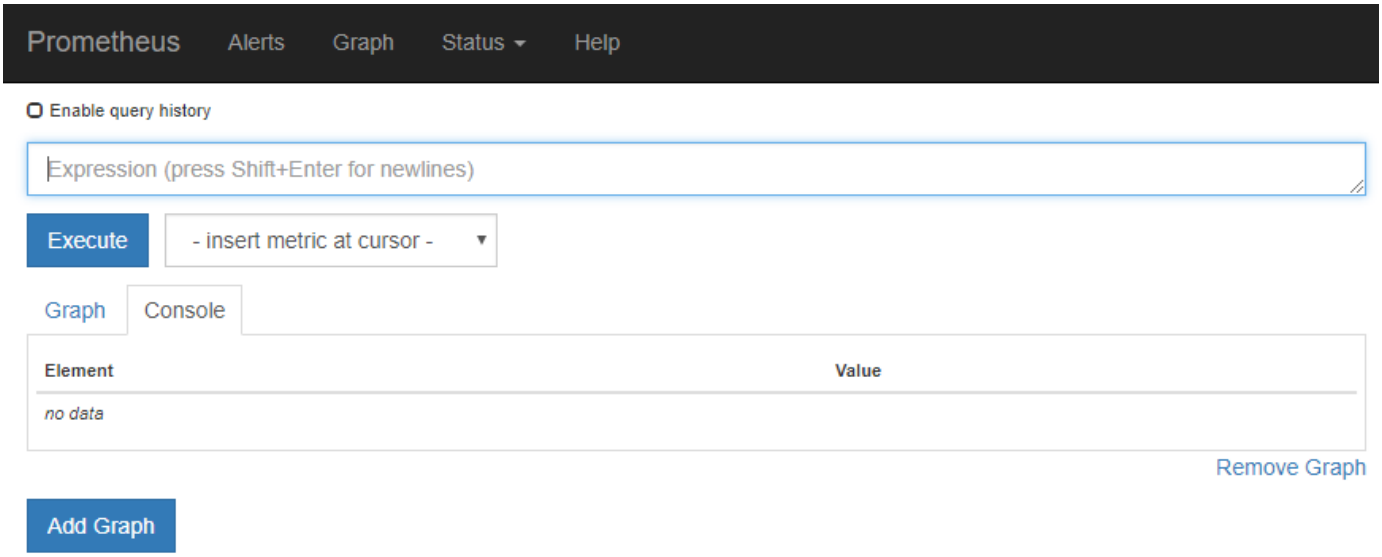
指標ページ

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

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

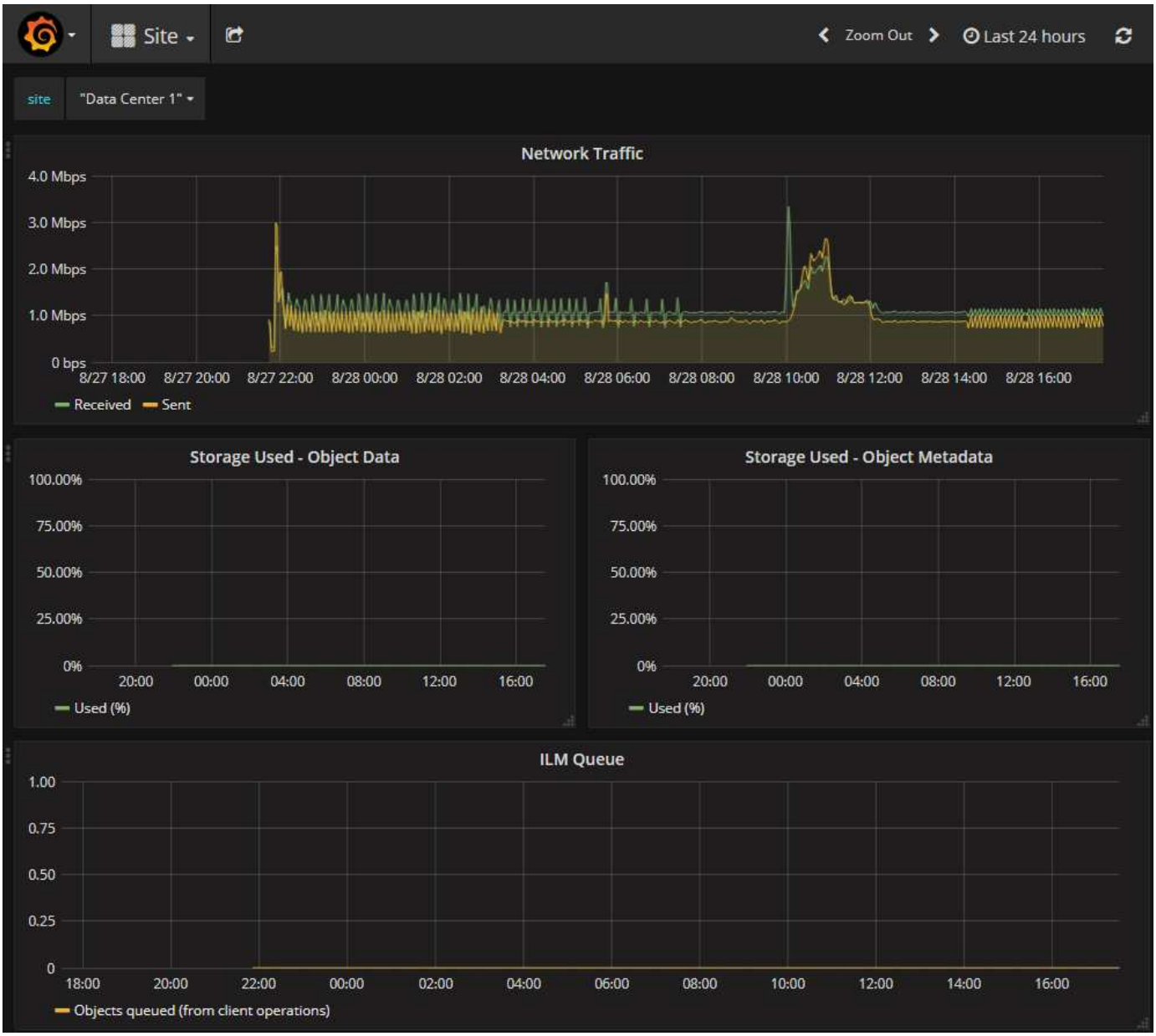


Metrics ページの Prometheus セクションのリンクを使用すると、 StorageGRID 指標の現在の値を照会し、その値の推移をグラフで確認できます。



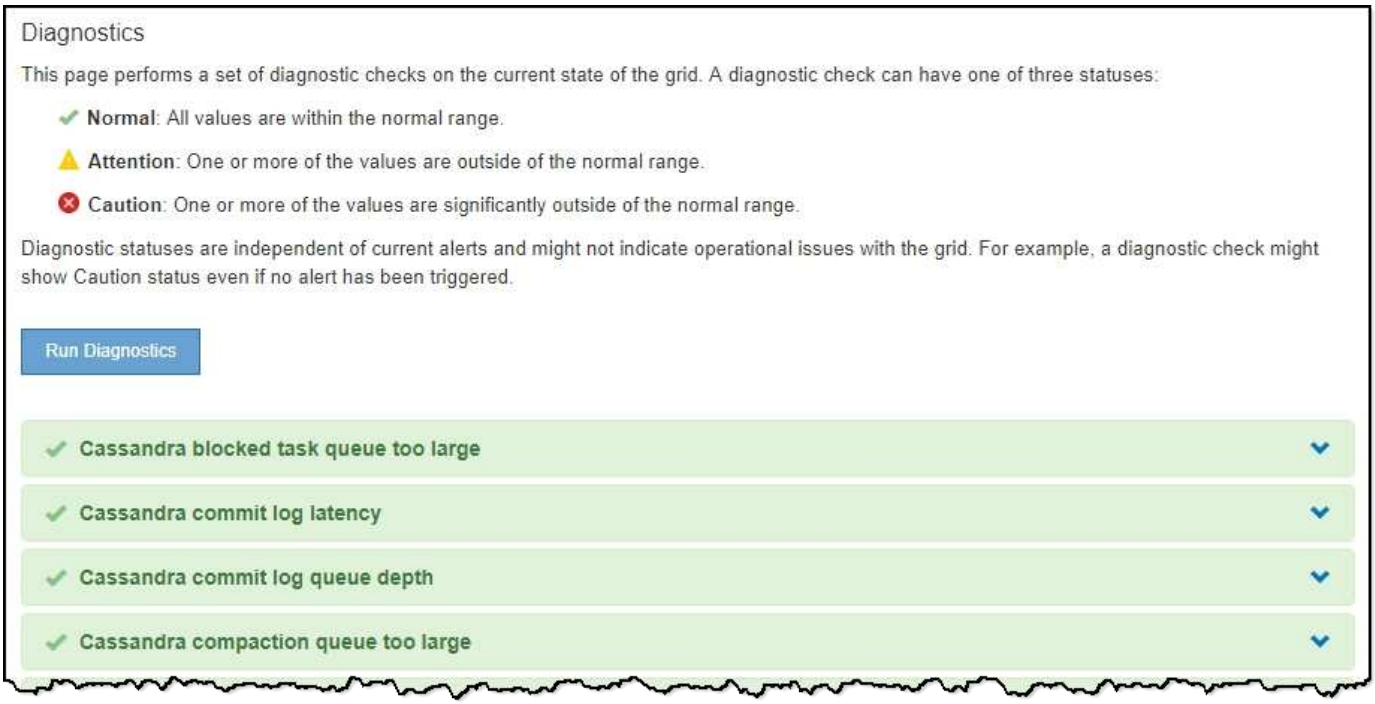
名前に *private* が含まれる指標は内部専用です。 StorageGRID のリリースごとに予告なく変更されることがあります。

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



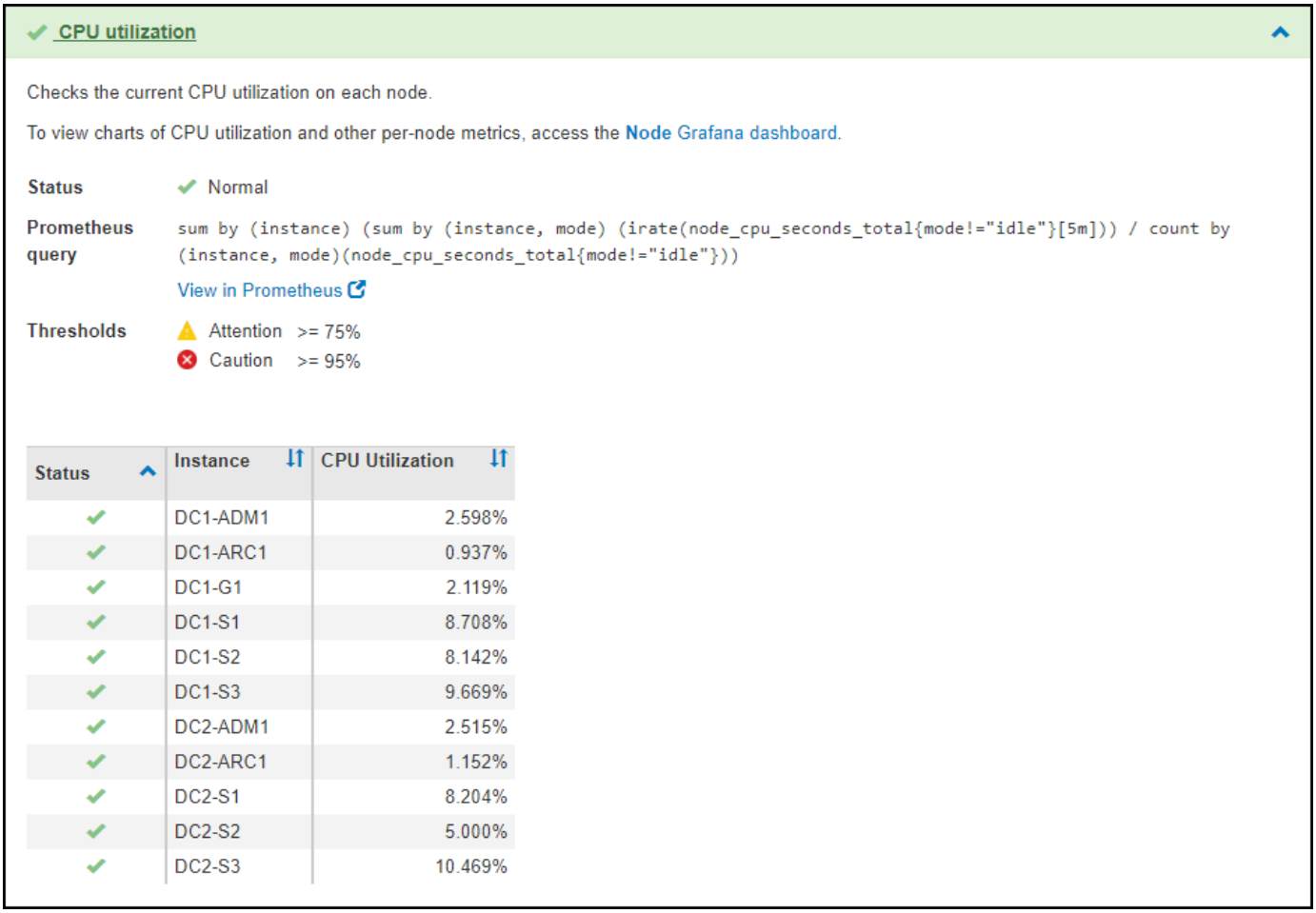
Diagnostics （診断）ページ

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



特定の診断をクリックすると、診断とその現在の結果の詳細が表示されます。

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



関連情報

- StorageGRID の管理
- ネットワークの設定を行います

ネットワークのガイドライン

ネットワークガイドライン：概要

これらのガイドラインを使用して、 StorageGRID アーキテクチャとネットワークトポロジについて学び、ネットワークの設定とプロビジョニングの要件を確認してください。

これらの手順について

これらのガイドラインは、 StorageGRID ノードを導入して設定する前に、 StorageGRID ネットワークインフラの作成に使用できる情報を示しています。これらのガイドラインを使用して、グリッド内のすべてのノード間、およびグリッドと外部のクライアントとサービス間で通信を確実に行うことができます。

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

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

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

作業を開始する前に

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

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

使用する StorageGRID ネットワークとその設定を決定したら、該当する手順に従って StorageGRID ノードを設置および設定できます。

ソフトウェアベースのノードをインストール

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

- Ubuntu または Debian をインストールします
- VMware をインストールする

アプライアンスノードを設置

- SG100 および SG1000 サービスアプライアンス
- SG6000 ストレージアプライアンス
- SG5700 ストレージアプライアンス
- SG5600 ストレージアプライアンス

StorageGRID ソフトウェアを設定および管理する

- StorageGRID の管理
- リリースノート

StorageGRID のネットワークタイプ

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

トラフィックタイプ

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

ネットワークは次の方法で設定できます。

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

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

内部ポートには、グリッドネットワーク経由でのみアクセスできます。外部ポートには、すべてのタイプのネットワークからアクセスできます。この柔軟性により、 StorageGRID 展開の設計と、スイッチおよびファイアウォールでの外部 IP およびポートフィルタリングの設定に複数のオプションを使用できます。を参照してください 内部でのグリッドノードの通信 および 外部との通信。

ネットワークインターフェイス

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

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

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

ソフトウェアベースのノード

- Red Hat Enterprise Linux または CentOS をインストールします
- Ubuntu または Debian をインストールします
- VMware をインストールする

アプライアンスノード

- SG100 および SG1000 サービスアプライアンス
- SG6000 ストレージアプライアンス
- SG5700 ストレージアプライアンス
- SG5600 ストレージアプライアンス

各ノードのネットワーク情報

ノードで有効にするネットワークごとに、次の項目を設定する必要があります。

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

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

イアドレスとして使用する必要があります。

ハイアベイラビリティグループ

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

Grid ネットワーク

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

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

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

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

グリッドネットワークゲートウェイに関する次の要件と詳細に注意してください。

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

管理ネットワーク

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

管理ネットワークを有効にするグリッドノードを選択できます。

管理ネットワークを使用する場合、管理トラフィックとメンテナンストラフィックがグリッドネットワークを経由する必要はありません。管理ネットワークの一般的な用途は次のとおりです。

- Grid Manager および Tenant Manager のユーザインターフェイスにアクセスします。

- NTP サーバ、 DNS サーバ、外部キー管理サーバ（ KMS ）、 Lightweight Directory Access Protocol （ LDAP ）サーバなどの重要なサービスへのアクセス
- 管理ノード上の監査ログへのアクセス。
- 保守とサポートのための Secure Shell Protocol （ SSH ）アクセス。

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

管理ネットワークゲートウェイに関する次の要件および詳細事項に注意してください。

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

クライアントネットワーク

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

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

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

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

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

クライアントネットワークゲートウェイについては、次の点に注意してください。

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

ルートになります。

オプションの **VLAN** ネットワーク

必要に応じて、クライアントトラフィックおよび一部のタイプの管理トラフィックに、仮想 LAN （ VLAN ）ネットワークを使用できます。ただし、グリッドトラフィックに VLAN インターフェイスを使用することはできません。ノード間の内部 StorageGRID トラフィックは、常に eth0 でグリッドネットワークを使用する必要があります。

VLAN の使用をサポートするには、 1 つのノード上の 1 つ以上のインターフェイスをスイッチでトランクインターフェイスとして設定する必要があります。グリッドネットワークインターフェイス（ eth0 ）またはクライアントネットワークインターフェイス（ eth2 ）をトランクとして設定することも、ノードに追加のトランクインターフェイスを設定することもできます。

eth0 がトランクとして設定されている場合、グリッドネットワークトラフィックはスイッチで設定されたトランクのネイティブインターフェイスを経由します。同様に、 eth2 がトランクとして設定されていて、クライアントネットワークも同じノード上で構成されている場合、クライアントネットワークはスイッチ上で構成されているトランクポートのネイティブ VLAN を使用します。

VLAN ネットワークでは、 SSH 、 Grid Manager 、または Tenant Manager のトラフィックに使用するなどのインバウンド管理トラフィックのみがサポートされます。NTP 、 DNS 、 LDAP 、 KMS 、クラウドストレージプールなどのアウトバウンドトラフィックは、 VLAN ネットワーク経由ではサポートされません。

> VLAN インターフェイスは管理ノードとゲートウェイノードにのみ追加できます。VLAN インターフェイスを使用して、クライアントやストレージノードまたはアーカイブノードへの管理者アクセスを行うことはできません。

を参照してください VLAN インターフェイスを設定します を参照してください。

VLAN インターフェイスは HA グループでのみ使用され、アクティブノード上の VIP アドレスに割り当てられます。を参照してください ハイアベイラビリティグループを管理します を参照してください。

関連情報

- ネットワーク要件

ネットワークトポロジの例

グリッドネットワークトポロジ

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

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

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

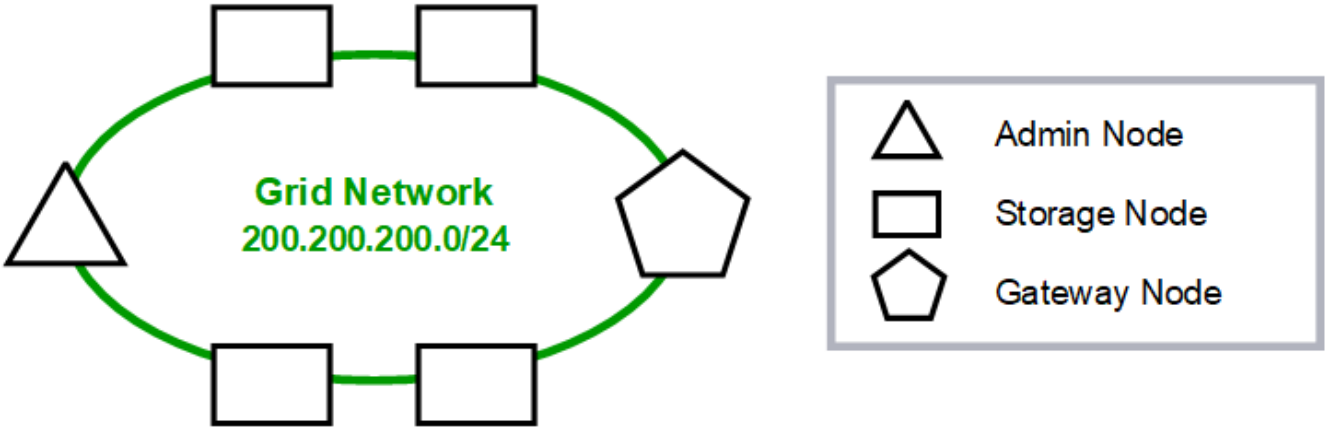
インストール時に、グリッドネットワークのインターフェイスでは、 GNSL に含まれるすべてのサブネットに静的ルートが適用され、設定されている場合はノードのデフォルトルートがグリッドネットワークゲートウ

ェイに設定されます。クライアントネットワークがなく、グリッドネットワークゲートウェイがノードのデフォルトルートである場合、 GNSL は必要ありません。グリッド内の他のすべてのノードへのホストルートも生成されます。

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

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

Topology example: Grid Network only



Provisioned

GNSL → 200.200.200.0/24		
	Grid Network	
Nodes	**IP/mask**	**Gateway**
Admin	200.200.200.32/24	200.200.200.1
Storage	200.200.200.33/24	200.200.200.1
Storage	200.200.200.34/24	200.200.200.1
Storage	200.200.200.35/24	200.200.200.1
Storage	200.200.200.36/24	200.200.200.1
Gateway	200.200.200.37/24	200.200.200.1

System Generated

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

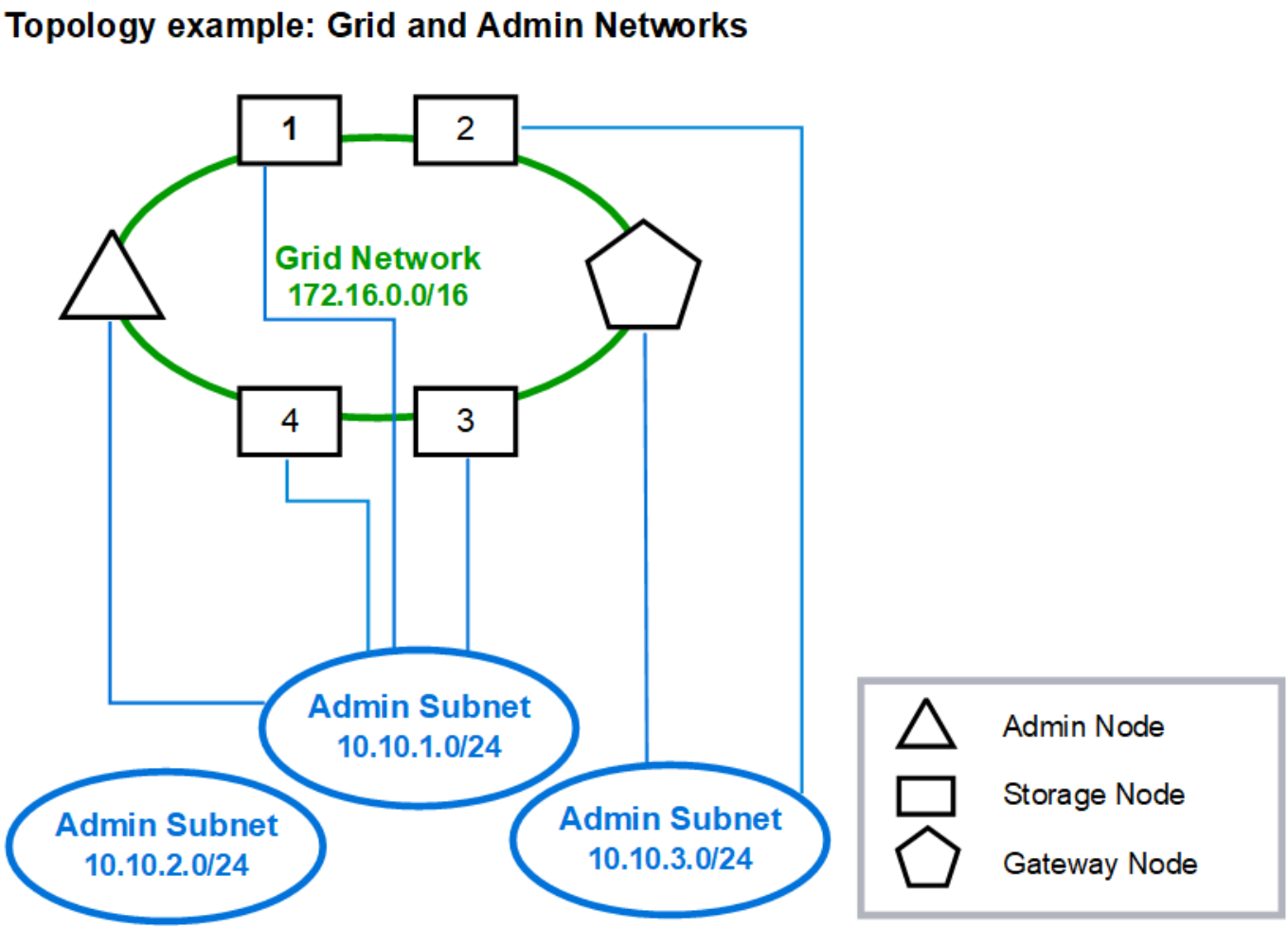
管理ネットワークトポロジ

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

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

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

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



Provisioned

GNSL → 172.16.0.0/16
AESL (all) → 10.10.1.0/24 10.10.2.0/24 10.10.3.0/24

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

System Generated

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

クライアントネットワークトポロジ

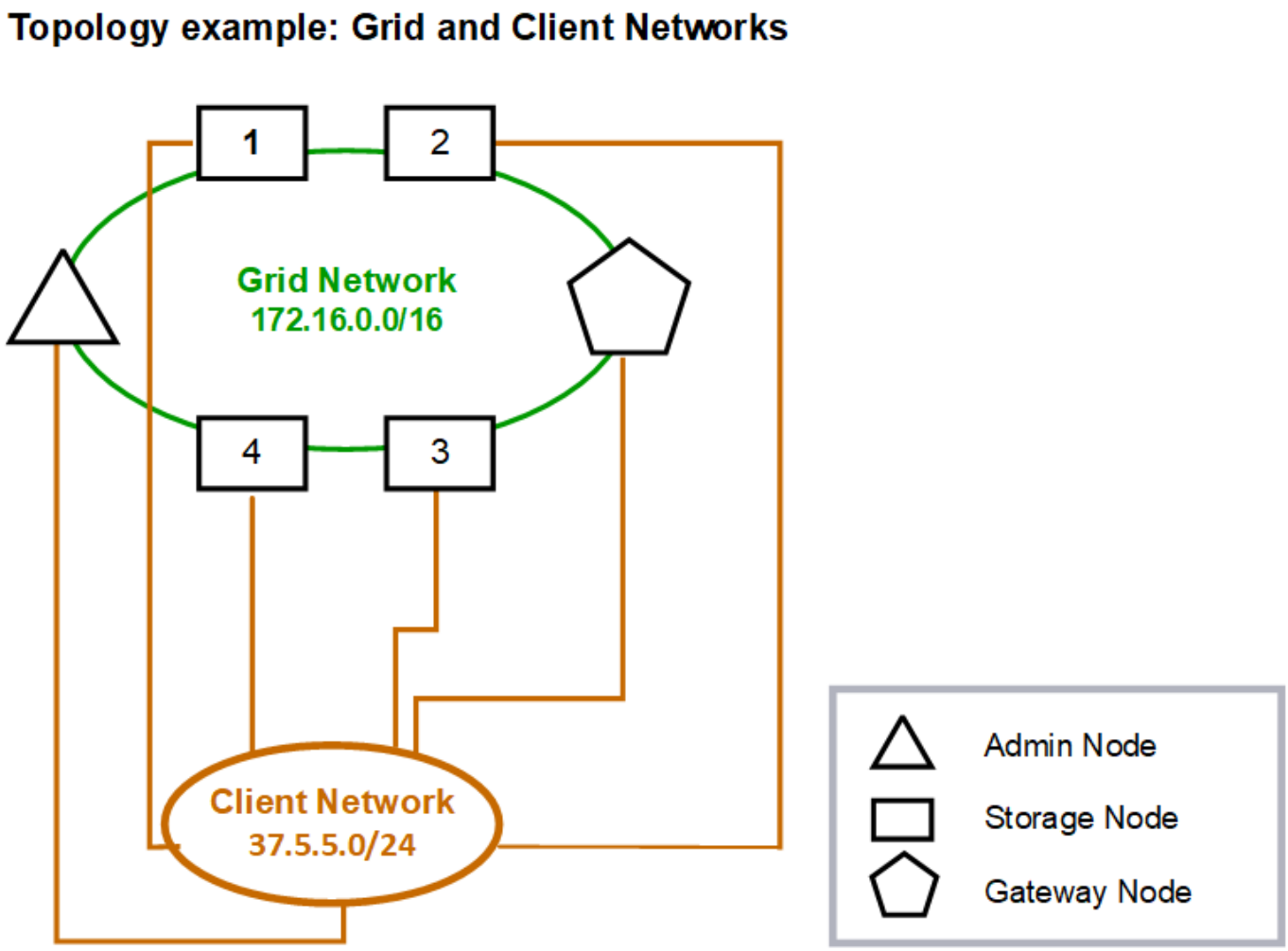
クライアントネットワークの使用はオプションです。クライアントネットワークを使用すると、クライアントネットワークのトラフィック（S3 や Swift など）をグリッドの内部トラフィックから分離できるため、グリッドネットワークのセキュリティを強化できます。管理ネットワークが設定されていない場合、管理トラフィックはクライアントネットワークまたはグリッドネットワークのどちらでも処理できます。

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

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

次の例では、クライアントネットワークが S3 および Swift クライアント要求と管理機能に使用され、グリッ

ドネットワークが内部のオブジェクト管理処理専用となっています。



Provisioned

GNSL → 172.16.0.0/16			
	Grid Network	Client Network	
Nodes	IP/mask	IP/mask	Gateway
Admin	172.16.200.32/24	37.5.5.10/24	37.5.5.1
Storage	172.16.200.33/24	37.5.5.11/24	37.5.5.1
Storage	172.16.200.34/24	37.5.5.12/24	37.5.5.1
Storage	172.16.200.35/24	37.5.5.13/24	37.5.5.1
Storage	172.16.200.36/24	37.5.5.14/24	37.5.5.1
Gateway	172.16.200.37/24	37.5.5.15/24	37.5.5.1

System Generated

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

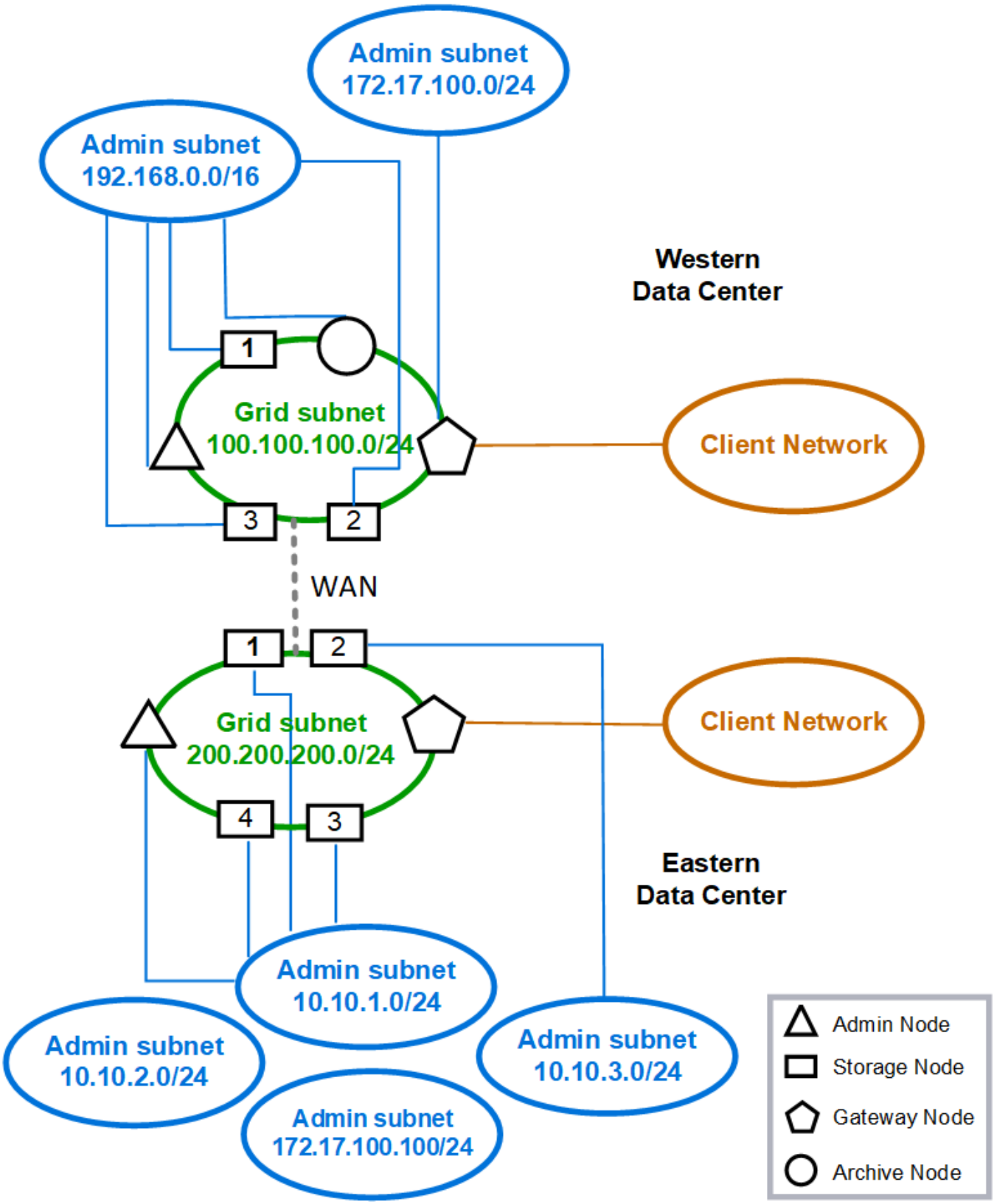
3 つのネットワークすべてのトポロジ

3 つのネットワークをすべて組み合わせて、プライベートグリッドネットワーク、サイトごとに境界を設定した管理ネットワーク、およびオープンなクライアントネットワークで構成されるネットワークトポロジを構成できます。ロードバランサエンドポイントと信頼されていないクライアントネットワークを使用すると、必要に応じてセキュリティを強化できます。

次の例では、

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

Topology example: Grid, Admin, and Client Networks



ネットワーク要件

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

一般的なネットワーク要件

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

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

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

  プライマリ管理ノードが、少なくとも 1 つの NTP サーバにアクセスできる必要があります。

- *DNS サーバ接続 *: 受信 UDP 応答を受信するアウトバウンド UDP 接続。
- *LDAP/Active Directory サーバ接続 *: ストレージノード上のアイデンティティサービスからのアウトバウンド TCP 接続。
- **TCP**: 管理ノードからの AutoSupport 接続を、 support.netapp.com` またはお客様が設定したプロキシのいずれかに送信します。
- * 外部キー管理サーバ * ：ノード暗号化が有効な各アプライアンスノードからのアウトバウンド TCP 接続。
- S3 および Swift クライアントからのインバウンド TCP 接続。
- CloudMirror レプリケーションやクラウドストレージプールなどの StorageGRID プラットフォームサービスからのアウトバウンド要求。

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

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

導入時にオプションの管理ネットワークとクライアントネットワークを設定する準備ができていなかった場合は、設定手順でグリッドノードを承認する際にこれらのネットワークを設定できます。また、インストール後に IP 変更ツールを使用してこれらのネットワークを設定することもできます（を参照） IP アドレスを設定する）。

VLAN インターフェイスでサポートされるのは、 S3 および Swift クライアント接続と、 SSH 、 Grid Manager 、および Tenant Manager 管理接続だけです。NTP 、 DNS 、 LDAP 、 AutoSupport 、 KMS サーバなどへのアウトバウンド接続 クライアント、管理、またはグリッドネットワークのインターフェイスを直接経由する必要があります。インターフェイスが VLAN インターフェイスをサポートするトランクとして設定されている場合、このトラフィックはスイッチで設定されたインターフェイスのネイティブ VLAN を経由します。

複数サイト用の **WAN** （ **Wide Area Network** ）

複数のサイトで StorageGRID システムを設定する場合は、クライアントトラフィックを考慮する前に、サイト間の WAN 接続の各方向の帯域幅が 25 Mbit/ 秒以上である必要があります。サイト間、ノードまたはサイトの拡張、ノードのリカバリ、その他の処理や構成のデータレプリケーションやイレイジャーコーディングでは、追加の帯域幅が必要になります。

管理ノードとゲートウェイノードの接続

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

ハイアベイラビリティグループに追加する管理ノードとゲートウェイノードには静的 IP アドレスを設定する必要があります。詳細については、を参照してください ハイアベイラビリティグループを管理します。

ネットワークアドレス変換（ **NAT** ）の使用

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

ネットワーク固有の要件

各 StorageGRID ネットワークタイプの要件に従ってください。

ネットワークゲートウェイおよびルータ

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

サブネット

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

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

- ネットワーク IP アドレスのサブネットマスクを 255.255.255.254 または 255.255.255.0 （ CIDR 表記では /31 または /32 ）にすることはできません。
- ネットワークインターフェイスの IP アドレスとサブネットマスク（ CIDR ）によって定義されたサブネ

ットは、同じノードに設定されている他のインターフェイスのサブネットと重複することはできません。

- 各ノードのグリッドネットワークサブネットを GNSL に含める必要があります。
- 管理ネットワークのサブネットは、グリッドネットワークのサブネット、クライアントネットワークのサブネット、または GNSL のサブネットと重複することはできません。
- AESL 内のサブネットを GNSL 内のどのサブネットとも重複させることはできません。
- クライアントネットワークのサブネットは、グリッドネットワークのサブネット、管理ネットワークのサブネット、 GNSL のサブネット、または AESL に含まれるすべてのサブネットと重複することはできません。

Grid ネットワーク

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

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

- グリッドネットワークが複数のサブネットで構成されている場合は、グリッドネットワークサブネットリスト（ GNSL ）に追加します。GNSL のサブネットごとに、すべてのノードにスタティックルートが作成されます。
- グリッドネットワークインターフェイスが VLAN インターフェイスをサポートするトランクとして設定されている場合は、トランクのネイティブ VLAN をグリッドネットワークトラフィックに使用する VLAN にする必要があります。すべてのグリッドノードに、トランクのネイティブ VLAN 経由でアクセスできる必要があります。

管理ネットワーク

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

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

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

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

クライアントネットワーク

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

- クライアントネットワークは、 S3 および Swift クライアントからのトラフィックをサポートするように設計されています。設定すると、クライアントネットワークゲートウェイがノードのデフォルトゲートウェイになります。
- クライアントネットワークを使用する場合は、明示的に設定されたロードバランサエンドポイントでのみインバウンドクライアントトラフィックを受け入れることで、悪意のある攻撃から StorageGRID を保護できます。を参照してください ロードバランサエンドポイントを設定する。
- クライアントネットワークインターフェイスが VLAN インターフェイスをサポートするトランクとして設定されている場合は、クライアントネットワークインターフェイス（ eth2 ）の設定が必要かどうかを検討してください。設定されている場合、クライアントネットワークトラフィックは、スイッチで設定されたトランクネイティブ VLAN を経由します。

環境固有のネットワークに関する考慮事項

Linux の導入

効率性、信頼性、セキュリティのために、 StorageGRID システムはコンテナエンジンの集合として Linux 上で動作します。StorageGRID システムでは、コンテナエンジン関連のネットワーク構成は必要ありません。

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

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

のインストール手順を参照してください Red Hat Enterprise Linux または CentOS または Ubuntu または Debian 導入：

コンテナエンジン導入用のホストネットワーク構成

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

物理ホスト

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

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

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

- ホストに必要なポートを開きます。
- StorageGRID で VLAN インターフェイスを使用する場合は、必要な VLAN へのアクセスを提供するトランクインターフェイスがホストに 1 つ以上必要です。これらのインターフェイスは、 eth0 、 eth2 、または追加のインターフェイスとしてノードコンテナに渡すことができます。トランクインターフェイスまたはアクセスインターフェイスを追加するには、次の項を参照してください。
  - * RHEL または CentOS （ノードのインストール前） * ： ノード構成ファイルを作成
  - * Ubuntu または Debian （ノードをインストールする前） * ： ノード構成ファイルを作成
  - * RHEL 、 CentOS 、 Ubuntu 、または Debian （ノードのインストール後） * ： Linux ：ノードにトランクインターフェイスまたはアクセスインターフェイスを追加します

最小帯域幅の推奨値

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

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

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

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

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

- 管理ノードにグリッドネットワークと管理ネットワークを接続する（必要な帯域幅： 10 + 1 = 11Gbps ）

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

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

StorageGRID クラスタのホストの物理リソースおよびネットワークリソースを設定して StorageGRID を導入する際の準備として、推奨される方法については、次の表を参照してください。

- ホストネットワークの設定（ Red Hat Enterprise Linux または CentOS ）
- ホストネットワークの設定（ Ubuntu または Debian ）

プラットフォームサービスとクラウドストレージプール用のネットワークとポート

StorageGRID プラットフォームサービスまたはクラウドストレージプールを使用する場合は、デスティネーションエンドポイントに到達できるようにグリッドネットワークとファイアウォールを設定する必要があります。

プラットフォームサービス用のネットワーク

を参照してください テナントのプラットフォームサービスを管理する および プラットフォームサービスとは プラットフォームサービスには、検索統合、イベント通知、 CloudMirror レプリケーションを提供する外部サービスが含まれます。

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

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

クラウドストレージプールのネットワーク

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

プラットフォームサービスとクラウドストレージプールのポート

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

- **80**: エンドポイント URI の場合 'http' で始まります
- **442**: エンドポイント URI の場合は 'https' で始まります

エンドポイントの作成時または編集時に別のポートを指定できます。を参照してください ネットワークポー

トのリファレンス。

非透過型プロキシサーバを使用する場合は、も使用する必要があります ストレージプロキシを設定します インターネット上のエンドポイントなどの外部エンドポイントへのメッセージの送信を許可します。

VLAN およびプラットフォームサービスとクラウドストレージプール

プラットフォームサービスやクラウドストレージプールに VLAN ネットワークを使用することはできません。デスティネーションエンドポイントには、グリッドネットワーク、管理ネットワーク、またはクライアントネットワーク経由でアクセスできる必要があります。

アプライアンスノード

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

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

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

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

- SG100 および SG1000 サービスアプライアンス
- SG6000 ストレージアプライアンス
- SG5700 ストレージアプライアンス
- SG5600 ストレージアプライアンス

ネットワークのインストールとプロビジョニング

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

ノードの初期導入

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

ゲートウェイが設定されているグリッドネットワークは、導入時にノードのデフォルトゲートウェイになります。デフォルトゲートウェイを使用すると、グリッドを設定する前に、別々のサブネットにあるグリッドノードがプライマリ管理ノードと通信できるようになります。

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

プライマリ管理ノードへの自動ノード登録

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

管理ネットワークまたはクライアントネットワークを無効にします

管理ネットワークまたはクライアントネットワークを無効にする場合は、ノードの承認プロセス中にそれらのネットワークから設定を削除するか、インストールの完了後に IP 変更ツールを使用できます（を参照） IP アドレスを設定する）。

インストール後のガイドライン

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

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

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

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

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

ネットワークポートのリファレンス

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

に表示された詳細を使用します 内部でのグリッドノードの通信 および 外部との通信 必要な各ポートの設定方法を確認します。

内部でのグリッドノードの通信

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

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

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

Linux ベースのノードについてはガイドラインを参照してください

これらのいずれかのポートへのアクセスがエンタープライズネットワークポリシーで制限されている場合は、導入設定パラメータを使用して導入時にポートを再マッピングできます。ポートの再マッピングおよび導入設定パラメータの詳細については、次のサイトを参照してください。

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

VMware ベースのノードについてのガイドラインを参照してください

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

これらのいずれかのポートへのアクセスがエンタープライズネットワークポリシーによって制限される場合は、ノードを導入する際に VMware vSphere Web Client を使用してポートを再マッピングするか、またはグリッドノードの導入を自動化する際に構成ファイルの設定を使用してポートを再マッピングできます。ポートの再マッピングおよび導入設定パラメータの詳細については、を参照してくださいVMware をインストールする。

アプライアンスノードのガイドライン

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

- SG100 および SG1000 サービスアプライアンス
- SG6000 ストレージアプライアンス
- SG5700 ストレージアプライアンス
- SG5600 ストレージアプライアンス

StorageGRID の内部ポート

ポート	tcp または udp です	移動元	終了：	詳細

22	TCP	プライマリ管理ノード	すべてのノード	メンテナンス手順では、プライマリ管理ノードがポート 22 で SSH を使用して他のすべてのノードと通信できる必要があります。他のノードからの SSH トラフィックの許可は任意です。
80	TCP	アプライアンス	プライマリ管理ノード	StorageGRID アプライアンスが、インストールを開始する目的でプライマリ管理ノードと通信するために使用します。
123	UDP	すべてのノード	すべてのノード	ネットワークタイムプロトコルサービス。すべてのノードは、 NTP を使用して他のすべてのノードと時間を同期します。
443	TCP	すべてのノード	プライマリ管理ノード	インストールおよびその他のメンテナンス手順の実行中に、プライマリ管理ノードにステータスを通知するために使用します。
1139	TCP	ストレージノード	ストレージノード	ストレージノード間の内部トラフィック。
1501 年	TCP	すべてのノード	ADC を採用するストレージノード	レポート、監査、および設定の内部トラフィック。
1502	TCP	すべてのノード	ストレージノード	S3 および Swift 関連の内部トラフィック。
1504.	TCP	すべてのノード	管理ノード	NMS サービスのレポートおよび設定の内部トラフィック。

1505.	TCP	すべてのノード	管理ノード	AMS サービスの内部トラフィック。
1506.	TCP	すべてのノード	すべてのノード	サーバステータスの内部トラフィック。
1507	TCP	すべてのノード	ゲートウェイノード	ロードバランサの内部トラフィック。
1508	TCP	すべてのノード	プライマリ管理ノード	設定管理の内部トラフィック。
1509.	TCP	すべてのノード	アーカイブノード	アーカイブノードの内部トラフィック。
1511.	TCP	すべてのノード	ストレージノード	メタデータの内部トラフィック。
5353	UDP	すべてのノード	すべてのノード	必要に応じて、フルグリッドの IP 変更、およびインストール、拡張、リカバリ時のプライマリ管理ノードの検出に使用します。
7001	TCP	ストレージノード	ストレージノード	Cassandra TLS ノード間クラスタ通信。
7443	TCP	すべてのノード	管理ノード	メンテナンス手順およびエラーレポート用の内部トラフィック。
8443	TCP	プライマリ管理ノード	アプライアンスノード	メンテナンスモードの手順 に関連する内部トラフィック。
9042	TCP	ストレージノード	ストレージノード	Cassandra クライアントポート。
9999	TCP	すべてのノード	すべてのノード	複数のサービスの内部トラフィック。メンテナンス手順、指標、およびネットワークの更新が含まれます。

10226	TCP	ストレージノード	プライマリ管理ノード	StorageGRID アプライアンスが、 E シリーズの SANtricity System Manager からプライマリ管理ノードに AutoSupport メッセージを転送するために使用します。
11139	TCP	アーカイブ / ストレージノード	アーカイブ / ストレージノード	ストレージノードとアーカイブノード間の内部トラフィック。
18000 年	TCP	管理 / ストレージノード	ADC を採用するストレージノード	アカウントサービスの内部トラフィック。
18001	TCP	管理 / ストレージノード	ADC を採用するストレージノード	アイデンティティフェデレーションの内部トラフィック。
18002	TCP	管理 / ストレージノード	ストレージノード	オブジェクトプロトコルに関連する内部 API トラフィック。
18003 年	TCP	管理 / ストレージノード	ADC を採用するストレージノード	プラットフォームサービスの内部トラフィック。
18017 年	TCP	管理 / ストレージノード	ストレージノード	クラウドストレージプールの Data Mover サービスの内部トラフィック。
18019 年になります	TCP	ストレージノード	ストレージノード	イレイジャーコーディング用のチャンクサービスの内部トラフィック。
18082 年	TCP	管理 / ストレージノード	ストレージノード	S3 関連の内部トラフィック。
18083 年	TCP	すべてのノード	ストレージノード	Swift 関連の内部トラフィック。

18200 年	TCP	管理 / ストレージノード	ストレージノード	クライアント要求に関する追加の統計。
19000 年	TCP	管理 / ストレージノード	ADC を採用するストレージノード	Keystone サービスの内部トラフィック。

- 関連情報 *

外部との通信

外部との通信

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

ポートへのアクセスを制限します

エンタープライズネットワークポリシーでいずれかのポートへのアクセスが制限されている場合は、を使用できます ロードバランサエンドポイント ユーザ定義のポートでアクセスを許可します。これで、を使用できます 信頼されていないクライアントネットワーク ロードバランサエンドポイントポートでのみアクセスを許可する場合。

ポートの再マッピング

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

ソフトウェアベースのノード

- Red Hat Enterprise Linux または CentOS をインストールします
- Ubuntu または Debian をインストールします
- VMware をインストールする

アプライアンスノード

- SG100 および SG1000 サービスアプライアンス
- SG6000 ストレージアプライアンス
- SG5700 ストレージアプライアンス
- SG5600 ストレージアプライアンス

外部との通信に使用するポート

次の表に、ノードに着信するトラフィックに使用されるポートを示します。

このリストには、として設定されている可能性のあるポートは含まれていません ロードバランサエンドポイント またはに使用されます "syslogサーバ"。

ポート	**tcp** または **udp** です	プロトコル	移動元	終了：	詳細
22	TCP	SSH	サービスラップトップ	すべてのノード	コンソールの手順を実行するには、 SSH アクセスまたはコンソールアクセスが必要です。必要に応じて、ポート 22 の代わりに 2022 を使用できます。
25	TCP	SMTP	管理ノード	E メールサーバ	アラートおよび E メールベースの AutoSupport に使用されます。Email Servers ページを使用して、デフォルトのポート設定である 25 を上書きできます。
53	TCP / UDP	DNS	すべてのノード	DNS サーバ	ドメインネームシステムに使用します。
67	UDP	DHCP	すべてのノード	DHCP サービス	必要に応じて、 DHCP ベースのネットワーク設定のサポートに使用します。dhclient サービスは、静的に設定されたグリッドに対しては実行されません。
68	UDP	DHCP	DHCP サービス	すべてのノード	必要に応じて、 DHCP ベースのネットワーク設定のサポートに使用します。dhclient サービスは、静的 IP アドレスを使用するグリッドに対しては実行されません。
80	TCP	HTTP	ブラウザ	管理ノード	ポート 80 は、管理ノードのユーザインターフェイス用のポート 443 にリダイレクトされます。
80	TCP	HTTP	ブラウザ	アプライアンス	ポート 80 は、 StorageGRID アプライアンスインストーラ用のポート 8443 にリダイレクトされます。

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

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

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

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

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

ポート	**tcp** または **udp** です	プロトコル	移動元	終了：	詳細
8443	TCP	HTTPS	ブラウザ	管理ノード	任意。Grid Manager にアクセスするために Web ブラウザと管理 API クライアントで使用されます。を使用して、Grid Manager と Tenant Manager の通信を分離できます。
9022	TCP	SSH	サービスラップトップ	アプライアンス	サポートとトラブルシューティングのために、構成前モードでの StorageGRID アプライアンスへのアクセスを許可します。このポートは、グリッドノード間で、または通常運用時にアクセス可能である必要はありません。
9091	TCP	HTTPS	外部の Grafana サービス	管理ノード	外部の Grafana サービスが StorageGRID Prometheus サービスへのセキュアなアクセスに使用します。 • 注：このポートは、証明書ベースの Prometheus アクセスが有効になっている場合にのみ必要です。
ポート 1	TCP	HTTPS	ブラウザ	管理ノード	任意。Tenant Manager にアクセスするために Web ブラウザと管理 API クライアントで使用します。を使用して、Grid Manager と Tenant Manager の通信を分離できます。
18082 年	TCP	HTTPS	S3 クライアント	ストレージノード	ストレージノードへの S3 クライアントトラフィック（HTTPS）。
18083 年	TCP	HTTPS	Swift クライアント	ストレージノード	ストレージノードへの Swift クライアントトラフィック（HTTPS）。
18084 年	TCP	HTTP	S3 クライアント	ストレージノード	ストレージノードへの S3 クライアントトラフィック（HTTP）。

ポート	**tcp** または **udp** です	プロトコル	移動元	終了：	詳細
18085 年になります	TCP	HTTP	Swift クライアント	ストレージノード	ストレージノードへの Swift クライアントトラフィック（HTTP）。

著作権に関する情報

Copyright © 2025 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

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

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

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

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

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

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

商標に関する情報

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