StorageGRID 12.1 ソフトウェアドキュメント

StorageGRID software

NetApp
July 22, 2026

This PDF was generated from https://docs.netapp.com/ja-jp/storagegrid/index.html on July 22, 2026.
Always check docs.netapp.com for the latest.

目次

StorageGRID 12.1 ソフトウェアドキュメント 1
StorageGRIDアプライアンスハードウェアについて 2
リリースノート 3
StorageGRID 12.1の新機能 3
容量 3
アクセス制御 3
フェデレーション 3
管理性 3
S3を使用したチャンク アップロード署名要求がサポートされるようになりました。 4
セキュリティ 4
テナント 5
Upgrade 5
ユーザーインターフェース 5
StorageGRIDで削除または廃止された機能 6
定義 6
StorageGRIDの機能のサポート終了 6
StorageGRID のGrid Management APIの変更点 8
BMCパスワードとLAN IP設定を変更するための新しいエンドポイント 8
StorageGRID のテナント管理 API の変更 9
オブジェクト複製用の新しいAPI 9
StorageGRID S3 REST API サポートの変更点 9
StorageGRIDシステムの使用を開始する 14
StorageGRID の詳細をご覧ください 14
StorageGRID とは 14
StorageGRID を使用したハイブリッドクラウド 16
StorageGRID のアーキテクチャとネットワークトポロジ 17
グリッドノードおよびサービス 20
StorageGRID によるデータの管理方法 33
StorageGRID の詳細をご覧ください 45
ネットワークのガイドライン 54
StorageGRID のネットワークガイドライン 54
StorageGRID のネットワークタイプ 55
ネットワークトポロジの例 59
StorageGRID のネットワーク要件 65
StorageGRID のネットワーク固有の要件 67
環境固有のネットワークに関する考慮事項 69
StorageGRID のネットワーク インストールとプロビジョニング 73
StorageGRID のインストール後のガイドライン 73
ネットワークポートのリファレンス 74

StorageGRID のクイックスタート 83
StorageGRIDのインストール、アップグレード、ホットフィックス 86
StorageGRIDノードをインストールする 86
StorageGRIDアプライアンスハードウェアについて 86
ソフトウェアベースのノードをインストール 86
グリッドを構成してインストールを完了する 186
StorageGRIDのインストール後の必須およびオプションの手順について学習します 200
StorageGRID ソフトウェアをアップグレードします 201
StorageGRID ソフトウェアをアップグレードします 201
アップグレードを計画して準備 201
ソフトウェアのアップグレード 208
StorageGRIDアップグレードの問題のトラブルシューティング 223
StorageGRIDホットフィックスの適用 226
StorageGRID ホットフィックス手順 226
ホットフィックスを適用したときのStorageGRIDへの影響 227
StorageGRIDホットフィックスに必要な材料を入手 228
StorageGRIDホットフィックスファイルをダウンロードします 229
StorageGRIDホットフィックスを適用する前にシステムの状態を確認してください 230
StorageGRID でホットフィックスを適用します 230
StorageGRIDシステムの設定と管理 235
StorageGRID の管理 235
StorageGRID 管理のクイックスタート 235
Grid Managerの使用を開始する 236
StorageGRID へのアクセスを制御します 264
グリッドフェデレーションを使用する 339
セキュリティを管理します 388
テナントを管理します 461
クライアント接続を設定します 481
ネットワークと接続を管理します 525
ストレージノードを管理します 545
管理ノードを管理する 559
ILM を使用してオブジェクトを管理する 560
StorageGRID で ILM を使用してオブジェクトを管理 560
ILM とオブジェクトライフサイクル 561
StorageGRID でストレージグレードを作成して割り当てる 583
ストレージプールを使用する 586
クラウドストレージプールを使用 595
StorageGRID でイレイジャー コーディング プロファイルを管理 615
StorageGRIDの S3 リージョンを構成する 619
ILM ルールを作成する 621
ILMポリシーを管理します。 638

StorageGRID で ILM ポリシーと ILM ルールを操作する 655
S3 オブジェクトロックを使用する 660
ILM ルールとポリシーの例 669
StorageGRID のシステム強化 691
StorageGRID のシステム強化について学ぶ 691
StorageGRIDソフトウェア アップグレードの強化ガイドライン 691
StorageGRID ネットワークのセキュリティ強化のガイドライン 692
StorageGRID ノードの保護対策のガイドライン 693
StorageGRID における TLS および SSH の強化ガイドライン 698
StorageGRID のログ、パスワード、監査メッセージの強化ガイドライン 699
StorageGRIDとFabricPool 700
FabricPoolでStorageGRIDを使用するための設定ワークフロー 700
StorageGRID を FabricPool クラウド階層として接続するために必要な情報 702
FabricPool セットアップウィザードを使用する 703
StorageGRID を手動で設定します 717
ONTAP System Manager を設定して、StorageGRID を FabricPool クラウド階層として追加します 728
FabricPoolを使用したStorageGRIDのDNSサーバーエントリを設定する 730
FabricPool に関するStorageGRID のベストプラクティス 730
StorageGRIDからFabricPoolデータを削除します 735
StorageGRIDのテナントとクライアントの使用 737
テナントアカウントを使用する 737
StorageGRID テナントアカウントを使用する 737
サインインとサインアウトの方法 738
StorageGRIDのテナントマネージャーダッシュボード 740
テナント管理 API 743
グリッドフェデレーション接続を使用する 748
グループとユーザを管理します 758
S3 アクセスキーを管理します 776
S3 バケットを管理する 781
S3 プラットフォームサービスを管理します 812
S3 REST APIを使用する 847
StorageGRID S3 REST API でサポートされているバージョンとアップデート 847
StorageGRID でサポートされている S3 API リクエスト 851
StorageGRID S3 REST API 構成をテストします 872
StorageGRID での S3 REST API の実装 873
Amazon S3 REST APIのサポート 889
StorageGRIDのカスタム処理 945
アクセスポリシーを管理する 966
StorageGRID監査ログで追跡されるS3操作 994
Swift REST APIの使用（サポート終了） 995
StorageGRID での Swift REST API サポート 995

StorageGRIDシステムの監視とトラブルシューティング 996
StorageGRID システムを監視します 996
AutoSupport を使用します 996
StorageGRID システムを監視する 1010
StorageGRIDでダッシュボードを表示および管理する 1011
Nodes ページを表示します 1013
定期的に監視する情報 1044
アラートの管理 1072
ログファイル参照 1109
ログ管理と外部Syslogサーバーを構成する 1129
メールサーバーの設定 1145
SNMP による監視を使用する 1147
追加の StorageGRID データを収集します 1160
StorageGRID システムのトラブルシューティングを行う 1173
StorageGRID システムのトラブルシューティングを行う 1173
オブジェクトやストレージの問題をトラブルシューティングする 1180
StorageGRID でメタデータの問題のトラブルシューティング 1199
StorageGRID の証明書エラーのトラブルシューティング 1201
StorageGRIDの管理ノードとユーザーインターフェースの問題のトラブルシューティング 1203
StorageGRID のネットワーク、ハードウェア、プラットフォームの問題のトラブルシューティング 1206
StorageGRID の外部 syslog サーバーエラーメッセージのトラブルシューティング 1214
StorageGRIDにおけるロードバランサのキャッシュの問題について学ぶ 1217
監査ログを確認します 1218
監査メッセージとログ 1218
監査メッセージがStorageGRIDシステムを通じて保存用のaudit.logファイルにどのように移動するか 1219
StorageGRID 管理ノードのコマンドラインから監査ログファイルにアクセスする 1222
StorageGRIDにおける監査ログファイルのローテーションについて学ぶ 1223
監査ログファイルの形式 1223
監査メッセージの形式 1236
監査メッセージとオブジェクトライフサイクル 1241
監査メッセージ 1247
StorageGRIDシステムの容量または機能を拡張します 1294
StorageGRIDシステムの拡張について学ぶ 1294
拡張計画 1295
StorageGRIDにおける複製データの拡張計画 1295
StorageGRIDにおける消失訂正符号化（EC）データの拡張計画 1296
StorageGRIDの拡張後の EC 再バランス調整について学ぶ 1297
拡張ガイドライン 1301
StorageGRIDでオブジェクト容量を追加するためのガイドライン 1301
StorageGRIDでメタデータ容量を追加するためのガイドライン 1303
StorageGRIDにグリッドノードを追加するためのガイドライン 1305

StorageGRIDに新しいサイトを追加するためのガイドライン 1305
StorageGRIDシステムの拡張準備 1307
StorageGRID インストールファイルをダウンロードして展開します 1307
ハードウェアとネットワークの確認 1313
Grid ノードまたはサイトを追加 1314
StorageGRIDにグリッド ノードまたは新しいサイトを追加するためのワークフローの概要 1314
StorageGRIDの拡張のためにグリッド ネットワークにサブネットを追加または更新します 1314
StorageGRIDに新しいグリッドノードを展開する 1316
StorageGRID拡張を実行する 1320
ストレージボリュームを追加します 1325
StorageGRIDシステムにストレージボリュームを追加する 1325
StorageGRIDのVMwareストレージノードにストレージボリュームを追加する 1328
StorageGRIDのLinuxストレージノードに直接接続またはSANボリュームを追加する 1330
拡張したシステムを設定します 1333
StorageGRIDで新しく追加されたノードとサイトを構成する 1333
StorageGRID拡張後にストレージノードがアクティブであることを確認する 1335
Prometheus メトリックをStorageGRIDの新しい管理ノードにコピーする 1335
監査ログをStorageGRIDの新しい管理ノードにコピーする 1336
StorageGRIDシステムにノードを追加した後、消失訂正符号化データを再バランスします。 1338
StorageGRIDの拡張エラーのトラブルシューティング 1341
StorageGRIDシステムの保守 1342
StorageGRIDグリッドのメンテナンス 1342
開始する前に 1342
アプライアンスのメンテナンス手順 1342
StorageGRID 復旧パッケージをダウンロードします 1342
ノードまたはサイトの運用を停止 1343
StorageGRIDノードまたはサイトの運用停止 1343
ノードの運用停止 1343
運用停止サイト 1361
グリッド、サイト、またはノードの名前変更 1385
StorageGRID の名前変更手順を使用する 1385
StorageGRID表示名の追加または更新 1389
ノードの手順 1395
StorageGRIDノードのメンテナンス手順 1395
StorageGRIDでADCサービスを移動します 1395
StorageGRIDストレージノードをデータ専用ノードに変換する 1396
リブート、シャットダウン、および電源の手順 1398
ポートの再マッピング手順 1410
Server Managerの手順 1414
ネットワーク手順 1423
StorageGRIDグリッドネットワークのサブネットを更新します 1423

IP アドレスを設定する 1425
既存のノードにインターフェイスを追加 1445
StorageGRIDでDNSサーバーを設定する 1448
単一のStorageGRIDノードのDNS構成を変更する 1449
StorageGRIDでNTPサーバーを管理する 1452
隔離されたStorageGRIDノードのネットワーク接続を復元します 1453
ホストとミドルウェアの手順 1455
StorageGRIDノードを新しいLinuxホストに移行する 1455
StorageGRIDでVMware仮想マシンを自動再起動するように構成します 1457
ノードをリカバリまたは交換 1458
StorageGRIDノードリカバリに関する警告と考慮事項 1458
グリッドノードをリカバリするための前提条件 1458
複数のグリッドノードをホストしているサーバで障害が発生した場合のノードリカバリの順序 1459
リカバリしたノードの IP アドレス 1459
StorageGRIDグリッドノードのリカバリに必要な資料を収集する 1459
StorageGRID インストールファイルをダウンロードして展開します 1460
StorageGRIDノード復旧手順を選択 1466
ストレージノードの障害からリカバリします 1467
StorageGRIDストレージノードの障害から回復する 1467
アプライアンスストレージノードをリカバリします 1468
システムドライブに損傷がない場合は、ストレージボリューム障害からリカバリします 1483
システムドライブ障害からリカバリします 1492
管理ノードの障害からリカバリ 1504
StorageGRIDにおけるプライマリまたは非プライマリ管理ノードの復旧 1504
同じプライマリ管理ノードを使用してプライマリ管理ノードの障害から復旧する 1504
プライマリ管理ノードの障害から非プライマリ管理ノードを使用して復旧する 1513
非プライマリ管理ノードの障害からリカバリします 1520
ゲートウェイノードの障害からリカバリします 1527
StorageGRIDゲートウェイノードの交換 1527
リカバリの開始を選択してStorageGRIDゲートウェイノードを構成します 1528
アーカイブノードの障害からリカバリします 1529
StorageGRIDアーカイブノードの障害から回復する 1529
Linuxノードの交換 1529
StorageGRIDのLinuxノードを置き換える 1530
StorageGRID用の新しいLinuxホストをデプロイします 1530
StorageGRIDノードをホストにリストアします 1531
追加のStorageGRIDノードリカバリ手順を実行する 1536
StorageGRID の VMware ノードをリカバリノードに交換する 1537
StorageGRID の VMware ノードを SG1000 または SG100 に交換する 1538
ステップ1：VMwareノードを交換する 1538
ステップ2：ノードの完全復旧 1543

障害が発生したノードをサービスアプライアンスと交換します 1543
障害が発生したStorageGRIDノードをサービスアプライアンスと交換 1543
StorageGRIDサービスアプライアンスのインストール（プラットフォーム変更のみ） 1544
StorageGRID アプライアンスの再設置の準備（プラットフォーム交換のみ） 1544
サービスアプライアンスでStorageGRIDソフトウェアのインストールを開始する 1545
StorageGRIDサービスアプライアンスのインストールの監視 1548
テクニカルサポートによるStorageGRIDサイトの復旧方法 1549
StorageGRIDソリューションとリソース 1551
NetAppコンソールを使用してStorageGRIDを管理する方法 1552
法的通知 1553
著作権 1553
商標 1553
特許 1553
プライバシーポリシー 1553
APIライセンス 1553
オープンソース 1553

StorageGRID 12.1 ソフトウェアドキュメント

StorageGRIDアプライアンスハードウェアについて

https://docs.netapp.com/us-en/storagegrid-appliances/index.html["StorageGRID アプライアンスのドキュメント"^]
にアクセスして、StorageGRIDストレージおよびサービスアプライアンスのインストール、設定、およびメンテナンスの方法を確認してください。

リリースノート

StorageGRID 12.1の新機能

StorageGRID 12.1では、以下の機能と変更点が導入されます。

最近の StorageGRID 12.1 リリースにおける修正された問題と既知の問題の詳細については、 "StorageGRID 12.1 リリースノート"を参照してください。NetAppアカウントでサインインするか、アカウントを作成してリリースノートにアクセスする必要があります。

容量

ECリバランスは空きスペースを使用するようになりました

ECリバランス機能は、使用済み領域ではなく空き領域を使用するようになりました。"StorageGRIDの拡張後の EC 再バランス調整について学ぶ"を参照してください。

メタデータ許容スペース

メタデータの最大許容容量を3.96 TBから7.92 TBに増やすことができるようになりました。"許可されているメタデータスペースです"を参照してください。

アクセス制御

OIDCを使用した**SSO**

これで"OpenID Connect （OIDC）を使用して StorageGRID でシングル サインオン（SSO）を設定する"できます。

フェデレーション

グローバル ネームスペース

テナントが複数の StorageGRID システムにまたがってバケットにアクセスできるように、グローバル名前空間を設定できるようになりました。"グローバルネームスペースについて"を参照してください。

管理性

ADC サービスの自動移動

"ADCの定足数を満たす必要がある場合"、ADCサービスは、"ストレージノードをデータ専用ノードに変換する"または"ストレージノードの廃止"の際に自動的に移動されるようになりました。

プライマリ管理ノードの復旧

プライマリ以外の管理ノードから、任意のノードを復旧できるようになりました。"プライマリ管理ノードの障害からの復旧"を参照してください。

S3を使用したチャンク アップロード署名要求がサポートされるようになりました。

既存のバケットでS3オブジェクトロックを有効にする

「既存バケットに対する S3 オブジェクトロックを許可する」設定が有効になっている場合、S3 テナントアカウントは既存バケットに対して S3 オブジェクトロックを有効にできるようになります。S3 テナントアカウントが既存のバケットに対して S3 オブジェクトロックを有効にすると、無効にすることはできません。

S3オブジェクトロックが有効なバケットのレプリケーションが許可されました

S3 オブジェクトロックが有効なバケット内のオブジェクトを複製するために CloudMirror を使用できるようになりました。"プラットフォームサービスについて" を参照してください。

空でないバケットに対してクロスグリッドレプリケーションを有効にする

空でないバケットに対して、クロスグリッドレプリケーションを有効にできるようになりました。"グリッド間レプリケーションの要件"を参照してください。

S3 バッチ操作 （FPVR のみ）

S3バッチ操作を使用すると、クロスグリッドレプリケーション用に構成予定のバージョン管理が有効になっているバケット内の既存オブジェクトを複製できます。

この機能には StorageGRID 12.1 の FPVR 承認が必要です。この機能をご利用になるには、担当のアカウント担当者にお問い合わせください。

機能しないS3 REST APIヘッダー

`If-Match`および `If-None-Match`ヘッダーは受け入れられますが、S3 REST API xref:{relative_path}../s3/put-object.html["PutObject"] 、link:../s3/complete-multipart-upload.html["CompleteMultipartUpload"] 、link:../s3/put-object-copy.html["CopyObject"] 、およびlink:../s3/operations-on-objects.html["deleteObject"]では機能しません。

詳細については、"StorageGRID S3 REST API サポートの変更点"を参照してください。

事前計算されたチェックサム値のサポート

S3 REST SPI は、事前計算されたチェックサム値と `x-amz-checksum-type`リクエストヘッダーをサポートするようになりました。"REST API サポートの更新内容"を参照してください。

セキュリティ

マルチ管理者認証

マルチ管理者検証 （MAV） は、StorageGRID システムへの偶発的または不正な変更を防ぐのに役立ちます。"StorageGRID マルチ管理者検証について"を参照してください。

FIPSに関するセキュリティポリシーの更新

FIPSの厳格なポリシー基準が更新されました。"「TLSおよびSSHポリシーの管理」でセキュリティポリシーを選択します。"を参照してください。

テナント

アカウント同期

「アカウントクローン」機能は、特定のテナントアカウント情報を一度だけ複製する機能を指すようになりました。

_アカウント同期_は、1つ以上のグリッドフェデレーション接続内のStorageGRIDシステム間で、テナントアカウント、テナントグループ、テナントユーザー、およびS3アクセスキーを自動的かつ継続的にレプリケートできる新機能です。"StorageGRID のアカウント同期について"を参照してください。

Kafkaエンドポイントとmtls認証

Kafkaエンドポイントで、相互トランスポート層セキュリティ（mTLS）がサポートされるようになりました。"プラットフォームサービスエンドポイントを設定する"を参照してください。

バケットの最大数

StorageGRID システムは、S3 テナントアカウントごとに最大 20,000 個のバケットをサポートするようになりました。

Upgrade

機能の有効化にかかる時間が長くなります

StorageGRID をバージョン 12.1 にアップグレードする際、機能の有効化にかかる時間が 5 分未満から 1 時間に増加しました。"StorageGRIDアップグレードの完了までの時間を見積もる" を参照してください。

ユーザーインターフェース

BMC設定ページ

Grid Manager のノードページに新しい BMC 設定タブが追加され、BMC パスワードのリセットおよび BMC LAN IP 設定の変更が可能になりました。"アプライアンスのBMCパスワードを変更する" および "アプライアンスノードのBMC LAN IP設定を変更する" を参照してください。これらの機能をサポートするために、新しい API エンドポイントも追加されました。"BMCパスワードとLAN IP設定を変更するための新しいエンドポイント" を参照してください。

メール通知

グリッドマネージャーには、アラート、AutoSupport、および複数管理者認証（MAV）のメール通知を設定および管理するための共通のメールページが追加されました。詳細については、"メールサーバーの設定"を参照してください。

リンク費用ページ更新

StorageGRID 12.1では、より詳細なリンクコスト情報と設定が提供されます。"リンクコストを管理します"を参照してください。

USBポート制御

Grid ManagerからUSBポートを有効または無効にできるようになりました。"USBポート経由でリモートアクセスを制御する"を参照してください。

StorageGRIDで削除または廃止された機能

StorageGRID 12.1.0 で削除または非推奨となった機能と性能について説明します。アップグレードを行う前に、削除または非推奨となった機能がクライアントアプリケーションやグリッド構成に影響するかどうかを確認してください。

定義

ハイシ
: 新しい本番環境では、この機能を使用しないでください。既存の運用環境では、引き続きこの機能を使用できます。

サポート終了
: この機能をサポートする最後に出荷されたバージョン。場合によっては、この段階で機能のドキュメントが削除されることがあります。

削除済み
: この機能を*サポートしていない*最初のバージョン。

StorageGRIDの機能のサポート終了

廃止された機能は、N+2メジャーバージョンで削除されます。たとえば、ある機能がバージョンN（たとえば6.3）で廃止された場合、その機能が存在する最後のバージョンはN+1です（たとえば、6.4）。バージョンN+2（たとえば6.5）は、この機能が製品に存在しない場合の最初のリリースです。

詳細については、を参照してください "[Software Version Supportページ"^]。

特定の状況では、NetAppは特定の機能のサポートを指定よりも早く終了する可能性があります。

機能	ハイシ	サポート終了	削除済み	以前のドキュメントへのリンク
AES-128暗号化のグローバルSSE設定	12.1	12.2	12.3	StorageGRID 12.1.0以降、保存された新規オブジェクトデータのAES-128暗号化のサポートは非推奨となりました。AES-128で暗号化された保存済みオブジェクトの取得機能は引き続きサポートされます。

機能	ハイシ	サポート終了	削除済み	以前のドキュメントへのリンク
アラーム、従来型 （アラートではありません）	11.7	11.8	11.9	"アラーム一覧（StorageGRID 11.8）"
アーカイブノードのサポート	11.7	11.8	11.9	"アーカイブノードの運用停止に関する考慮事項（StorageGRID 11.8）" 注：アップグレードを開始する前に、次の作業を行う必要があります。 1. すべてのアーカイブノードを廃止します。 "グリッドノードの運用停止（StorageGRID 11.8ドキュメントサイト）"を参照してください。 2. ストレージプールおよびILMポリシーから、すべてのアーカイブノード参照を削除します。 "NetAppナレッジベース：StorageGRID 11.9ソフトウェアアップグレード解決ガイド"を参照してください。
CIFS / Sambaを使用した監査エクスポート	11.1	11.6	11.7	
CLBサービス	11.4	11.6	11.7	
Dockerコンテナエンジン	11.8	11.9	未定	ソフトウェアのみのデプロイメント用のコンテナ エンジンとしての Docker のサポートは非推奨になりました。Docker は将来のリリースで別のコンテナ エンジンに置き換えられる予定です。参照"ソフトウェアベースノードのソフトウェア要件"現在サポートされている Docker バージョンのリスト。
メール設定（レガシー）	11.9	12.0	12.1	"アラームの通知を設定する（レガシーシステム）（StorageGRID 11.8）"
NFS監査エクスポート	11.8	11.9	12.0	"NFSの監査クライアントアクセスの設定（StorageGRID 11.8）"
ポートの再マップ	12.0	12.1	12.2	
Swift APIのサポート	11.7	11.9	12.0	"Swift REST APIの使用（StorageGRID 11.8）"

機能	ハイシ	サポート終了	削除済み	以前のドキュメントへのリンク
RHEL 8.8	11.9	11.9	12.0	
RHEL 9.0	11.9	11.9	12.0	
RHEL 9.2	11.9	11.9	12.0	
Ubuntu 18.04.	11.9	11.9	12.0	
Ubuntu 20.04.	11.9	11.9	12.0	
Debian 11	11.9	11.9	12.0	

次の項目も参照してください。

- "Grid 管理 API に対する変更"
- "テナント管理 API に変更が加えられました"

StorageGRID のGrid Management APIの変更点

StorageGRID 12.1では、グリッド管理APIのバージョン4を使用しています。バージョン4ではバージョン3は非推奨となりますが、バージョン1、2、3は引き続きサポートされます。

> 非推奨バージョンの管理 API は StorageGRID で引き続き使用できます。ただし、これらのバージョンの API のサポートは、今後の StorageGRID のリリースで削除される予定です。StorageGRID 12.0 以降にアップグレードした後、 `PUT /grid/config/management` API を使用して非推奨の API を無効化できます。

詳細については、を参照してください"グリッド管理 API を使用します"。

BMCパスワードとLAN IP設定を変更するための新しいエンドポイント

以下のエンドポイントが追加され、"アプライアンスの BMC パスワードを変更する"できるようになりました。

```
PUT /bmc-configuration/root-password
```

以下のエンドポイントが追加され、"BMC LAN IP設定を変更または表示する"できるようになりました。

```
PUT /grid/bmc/{node-id}/lan-ip-config
```

```
GET /grid/bmc/{node-id}/lan-ip-config
```

StorageGRID のテナント管理 API の変更

StorageGRID 12.1では、テナント管理APIのバージョン4を使用しています。バージョン4ではバージョン3は非推奨となりますが、バージョン1、2、3は引き続きサポートされます。

> 非推奨バージョンのテナント管理 API は StorageGRID で引き続き使用できます。ただし、これらのバージョンの API のサポートは、今後の StorageGRID のリリースで削除される予定です。StorageGRID 12.0 以降にアップグレードした後、 `PUT /grid/config/management` API を使用して非推奨の API を無効化できます。

詳細については、を参照してください"テナント管理 API について理解する"。

オブジェクト複製用の新しいAPI

使用することができます `/org/cross-grid-replication/{versionId}/replicate`クロスグリッド レプリケーションが新しく構成された既存のバケット上のオブジェクトを手動で複製するための API。

StorageGRID S3 REST API サポートの変更点

StorageGRID で使用される S3 REST API は定期的に更新されます。

リリース	コメント
12.1.0	• `If-Match` `If-Match`ヘッダーの動作は、StorageGRIDの構成によって異なります。このヘッダーを指定すると、エラーメッセージ（`501 Not Implemented`）が返される可能性があります。 `If-Match`ヘッダーが受け入れられたものの機能しない場合、より厳格な`501 Not Implemented`エラー動作を有効にするための手順を示すアラートが表示される可能性があります。 • `If-None-Match` `If-None-Match`ヘッダーの動作は、StorageGRIDの構成によって異なります。このヘッダーを指定すると、エラーメッセージ（`501 Not Implemented`）が返される可能性があります。 `If-None-Match`ヘッダーが受け入れられたものの機能しない場合、より厳格な`501 Not Implemented`エラー動作を有効にするための手順を示すアラートが表示される可能性があります。 • 以下のリクエストおよびサポートされているヘッダーに対して、事前計算されたチェックサム値のサポートを追加しました： ◦ CompleteMultipartUpload： `x-amz-checksum-crc32`、 `x-amz-checksum-crc32c`、および `x-amz-checksum-crc64nvme` ◦ CreateMultipartUpload： `CRC32`、 `CRC32C`、および `CRC64NVME`（`x-amz-checksum-algorithm`用） ◦ CopyObject： `CRC32`、 `CRC32C`、 `CRC64NVME`、および `SHA256`（`x-amz-checksum-algorithm`用） ◦ PutObject： `x-amz-checksum-crc32`、 `x-amz-checksum-crc32c`、および `x-amz-checksum-crc64nvme` ◦ UploadPart： `x-amz-checksum-crc32`、 `x-amz-checksum-crc32c`、および `x-amz-checksum-crc64nvme` • `x-amz-checksum-type`のCreateMultipartUploadおよびCompleteMultipartUploadのサポートを追加しました。 • `s3:x-amz-copy-source`ポリシー条件キーのサポートが追加されました。 • 既存のバケットで S3 オブジェクトロックを有効にできるようにします。

リリース	コメント
12.0	• 管理インターフェースのクロスオリジン リソース共有 (CORS) のサポートが追加されました。これにより、別のドメインが管理 API を使用してStorageGRID内のデータにアクセスできるようになります。"詳細" 。 • STS AssumeRole およびセッションポリシーのサポートを追加しました。"セッションポリシーの例" を参照してください。テナントグループごとに AssumeRole を設定できます。
11.9	• 次の要求およびサポートされるヘッダーについて、事前に計算されたSHA-256チェックサム値のサポートが追加されました。この機能を使用して、アップロードされたオブジェクトの整合性を検証できます。 ◦ CompleteMultipartUpload： `x-amz-checksum-sha256` ◦ CreateMultipartUpload： `x-amz-checksum-algorithm` ◦ GetObject： `x-amz-checksum-mode` ◦ HeadObject： `x-amz-checksum-mode` ◦ ListParts ◦ PutObject： `x-amz-checksum-sha256` ◦ アップロードパーツ： `x-amz-checksum-sha256` • グリッド管理者がテナントレベルの保持期間と準拠設定を制御できるようになりました。これらの設定はS3オブジェクトロックの設定に影響します。 ◦ バケットのデフォルトの保持モードとオブジェクトの保持モード：GovernanceまたはCompliance（グリッド管理者が許可している場合）。 ◦ バケットのデフォルトの保持期間およびオブジェクトのRetain Until Date：グリッド管理者が設定した最大保持期間の許容値以下にする必要があります。 • コンテンツエンコーディングとストリーミング `x-amz-content-sha256`値のサポートが改善されました `aws-chunked`。制限事項： ◦ 存在する場合は `chunk-signature`オプションで、検証されていません。 ◦ 存在する場合、 `x-amz-trailer`コンテンツは無視されます。
11.8	で使用されている名前に一致するようにS3処理の名前が更新されました "Amazon Web Services （ AWS ）ドキュメント：「 Amazon Simple Storage Service API Reference"。

リリース	コメント
11.7	• "クイックリファレンス：サポートされるS3 API要求"を追加しました。 • S3オブジェクトロックでのガバナンスモードの使用のサポートが追加されました。 • GET Object要求とHEAD Object要求のStorageGRID固有の応答ヘッダーのサポートが追加されました `x-ntap-sg-cgr-replication-status`。このヘッダーは、グリッド間レプリケーションのオブジェクトのレプリケーションステータスを示します。 • SelectObjectContent要求でParquetオブジェクトがサポートされるようになりました。
11.6	• GET Object要求とHEAD Object要求でrequestパラメータを使用できるようになりました `partNumber`。 • S3 オブジェクトロックのデフォルト保持モードとデフォルトの保持期間がバケットレベルでサポートされるようになりました。 • オブジェクトに許可される保持期間の範囲を設定するポリシー条件キーのサポートが追加されました `s3:object-lock-remaining-retention-days`。 • 単一のPUT Object処理のmaximum_recommended_sizeを5GiB（5、368、709、120バイト）に変更しました。5GB より大きいオブジェクトがある場合は、マルチパートアップロードを使用してください。
11.5	• バケットの暗号化の管理のサポートが追加されました。 • S3 オブジェクトのロックと廃止された従来の準拠要求のサポートを追加しました。 • バージョン管理されたバケットでの DELETE Multiple Objects の使用のサポートが追加されました。 • `Content-MD5`要求ヘッダーが正しくサポートされるようになりました。
11.4	• DELETE Bucket tagging 、 GET Bucket tagging 、 PUT Bucket tagging のサポートが追加されました。コスト割り当てタグはサポートされていません。 • StorageGRID 11.4 で作成されたバケットでは、オブジェクトキー名がパフォーマンスのベストプラクティスに適合するように制限する必要はなくなりました。 • イベントタイプでのバケット通知のサポートが追加されました `s3:ObjectRestore:Post`。 • マルチパートの AWS サイズの上限が適用されるようになりました。マルチパートアップロードの各パートのサイズは 5MiB から 5GiB の間にする必要があります。最後の部分は 5MiB より小さくすることができます。 • TLS 1.3のサポートが追加されました

リリース	コメント
11.3	• ユーザ指定のキーによるオブジェクトデータのサーバ側暗号化（ SSE-C ）がサポートされるようになりました。 • DELETE Bucket lifecycle、GET Bucket lifecycle、PUT Bucket lifecycleの各処理（Expirationアクションのみ）と応答ヘッダーのサポートが追加されました `x-amz-expiration`。 • PUT Object 、 PUT Object - Copy 、 Multipart Upload が更新されて、取り込み時に同期配置を使用する ILM ルールの影響を受けるようになりました。 • TLS 1.1 暗号はサポートされなくなりました。
11.2	クラウドストレージプールで POST Object restore を使用できるようになりました。グループポリシーとバケットポリシーの ARN 、ポリシー条件キー、およびポリシー変数で AWS 構文を使用できるようになりました。StorageGRID 構文を使用する既存のグループポリシーとバケットポリシーは引き続きサポートされます。 • 注：カスタム StorageGRID 機能で使用される ARN やその他の構成 JSON / XML での使用に変更はありませんでした。
11.1	Cross-Origin Resource Sharing（CORS）、グリッドノードへのS3クライアント接続でのHTTP、バケットでの準拠設定のサポートが追加されました。
11.0	バケットでのプラットフォームサービス（ CloudMirror レプリケーション、通知、および Elasticsearch 検索統合）の設定がサポートされるようになりました。また、バケットに対するオブジェクトタギングの場所の制約と「available」の整合性がサポートされるようになりました。
10.4	ILM スキャンのバージョン管理、エンドポイントドメインの名前ページの更新、ポリシーの条件と変数、ポリシーの例、および PutOverwriteObject 権限の変更のサポートが追加されました。
10.3	バージョン管理のサポートが追加されました。
10.2	グループとバケットのアクセスポリシー、およびマルチパートコピー（ Upload Part - Copy ）のサポートが追加されました。
10.1	マルチパートアップロード、仮想ホスト型リクエスト、およびv4認証のサポートを追加しました。
10.0	StorageGRIDシステムによる S3 REST API の初期サポート。現在サポートされている *Simple Storage Service API* リファレンス のバージョンは 2006-03-01 です。

詳細については、"S3 REST APIのサポートされているバージョンとアップデート" を参照してください。

StorageGRIDシステムの使用を開始する

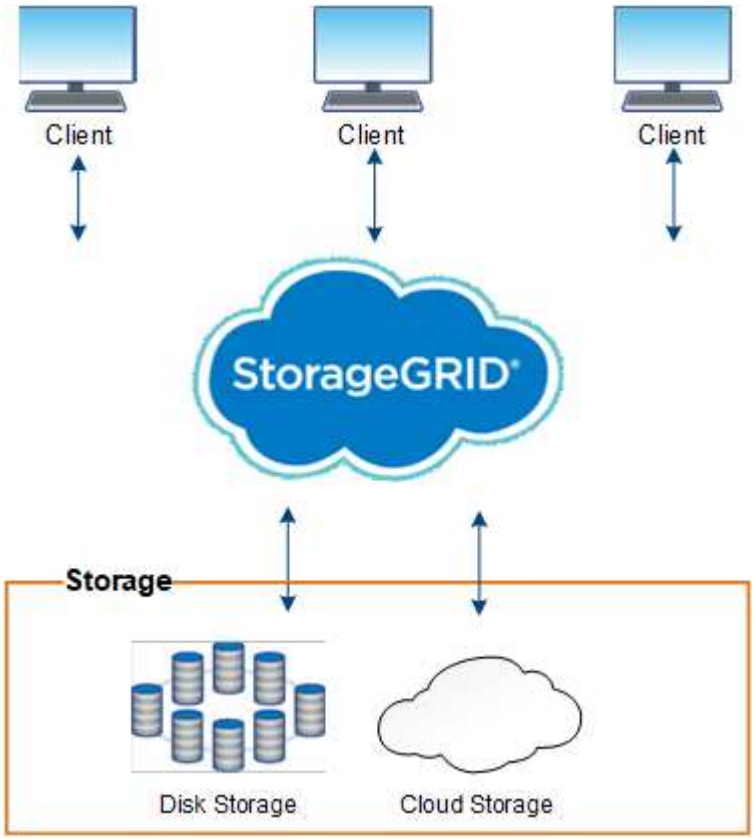
StorageGRID の詳細をご覧ください

StorageGRID とは

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

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

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



アーカイブノードのサポートが廃止されました。S3 APIを使用したアーカイブノードから外部アーカイブストレージシステムへのオブジェクトの移動は、"ILMクラウドストレージプール"より多くの機能を提供するに置き換えられました。

StorageGRID のメリット

StorageGRID システムには次の利点があります。

- 非構造化データ用に地理的に分散したデータリポジトリを拡張性にきわめて優れ、使いやすくなっています。
- Amazon Web Services Simple Storage Service (S3) 標準オブジェクト ストレージ プロトコル。
- ハイブリッドクラウドの実現：ポリシーベースの情報ライフサイクル管理（ ILM ）を使用して、 Amazon Web Services （ AWS ）や Microsoft Azure などのパブリッククラウドにオブジェクトを格納できます。StorageGRID プラットフォームサービスを使用すると、パブリッククラウドに格納されたオブジェクトのコンテンツレプリケーション、イベント通知、メタデータ検索を行うことができます。
- 柔軟なデータ保護で、データの保持性と可用性を確保レプリケーションと階層型イレイジャーコーディングを使用してデータを保護できます。保存データと転送中データの検証により、長期保持の整合性を確保します。
- 動的なデータライフサイクル管理でストレージコストの管理を支援オブジェクトレベルでデータのライフサイクルを管理するILMルールを作成し、データのローカリティ、保持性、パフォーマンス、コスト、 保持期限が設定されます。
- データストレージの高可用性と一部の管理機能。ロードバランシングの統合により、 StorageGRID リソース全体のデータ負荷を最適化します。
- 複数のストレージテナントアカウントをサポート。システムに格納されているオブジェクトをエンティティごとに分離できます。
- 包括的なアラートシステム、グラフィカルダッシュボード、すべてのノードとサイトの詳細なステータスなど、 StorageGRID システムの健全性を監視するための多数のツールが用意されています。
- ソフトウェアベースまたはハードウェアベースの展開をサポート。StorageGRID は次のいずれかに展開できます：
  - VMware で実行される仮想マシン。
  - Linux ホスト上のコンテナエンジン。
  - StorageGRIDエンジニアリングのアプライアンス。
    - ストレージアプライアンスはオブジェクトストレージを提供します。
    - サービスアプライアンスは、グリッド管理サービスとロードバランシングサービスを提供します。
- 以下の規制に関連するストレージ要件に準拠しています。
  - 取引所会員や株式仲買業者を規制するための 17 CFR § 240.17a-4 （ f ）における証券取引委員会（ SEC ）
  - 金融業界規制機関（ FINRA ）ルール 4511 （ c ）。 SEC ルール 17a-4 （ f ）の形式とメディア要件は先延ばしになります。
  - 商品先物取引を規制するための 17 CFR § 1.31 （ c ） - （ d ）規制の商品先物取引委員会（ CFTC ）
- 無停止のアップグレード処理とメンテナンス処理。アップグレード、拡張、運用停止、メンテナンスの実行中も、コンテンツにアクセスできます。
- フェデレーション型ID管理。ユーザ認証のために、Active Directory、OpenLDAP、またはOracle Directory Serviceと統合します。Security Assertion Markup Language 2.0（SAML 2.0）またはOpenID Connect（OIDC）を使用して、StorageGRIDとActive Directory Federation Services (AD FS) などの外部IDプロバイダー間で認証および認可データを交換するシングル サインオン（SSO）をサポートします。

StorageGRID を使用したハイブリッドクラウド

ポリシーベースのデータ管理を実装してクラウドストレージプールにオブジェクトを格納し、StorageGRID プラットフォームサービスを活用し、NetApp FabricPool を使用してONTAP からStorageGRID にデータを階層化することで、ハイブリッドクラウド構成でStorageGRID を使用します。

クラウドストレージプール

クラウドストレージプールを使用すると、StorageGRID システムの外部にオブジェクトを保存できます。たとえば、アクセス頻度の低いオブジェクトを、Amazon S3 Glacier、S3 Glacier Deep Archive、Google Cloud、Microsoft Azure Blob Storage のアーカイブアクセス層などの低コストのクラウドストレージに移動することができます。または、ストレージボリュームまたはストレージノードの障害によって失われたデータを復旧するために使用できる、StorageGRID オブジェクトのクラウドバックアップを保持することもできます。

ディスクストレージやテープストレージなど、サードパーティパートナーのストレージもサポートされています。

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

S3 プラットフォームサービス

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

- CloudMirror レプリケーションサービスでは、指定したオブジェクトが Amazon S3 または別の StorageGRID システムにあるターゲット S3 バケットに自動的にミラーリングされます。
- イベント通知サービスは、指定されたアクションに関するメッセージを、Simple Notification Service (Amazon SNS) イベントの受信をサポートする外部エンドポイントに送信します。
- 検索統合サービスは、オブジェクトのメタデータを外部のElasticsearchサービスに送信し、サードパーティツールを使用してメタデータを検索、視覚化、分析できるようにします。

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

FabricPool を使用したONTAP データ階層化

FabricPool を使用してデータを StorageGRID に階層化することで、 ONTAP ストレージのコストを削減できます。FabricPool を使用すると、オンプレミスまたはオフプレミスの低コストのオブジェクトストレージ階層へデータを自動で階層化できます。

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

関連情報

- "クラウドストレージプールとは"

- "プラットフォームサービスを管理します"
- "StorageGRID for FabricPool を設定します"

StorageGRID のアーキテクチャとネットワークトポロジ

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

について学ぶ"グリッドノードタイプ"。

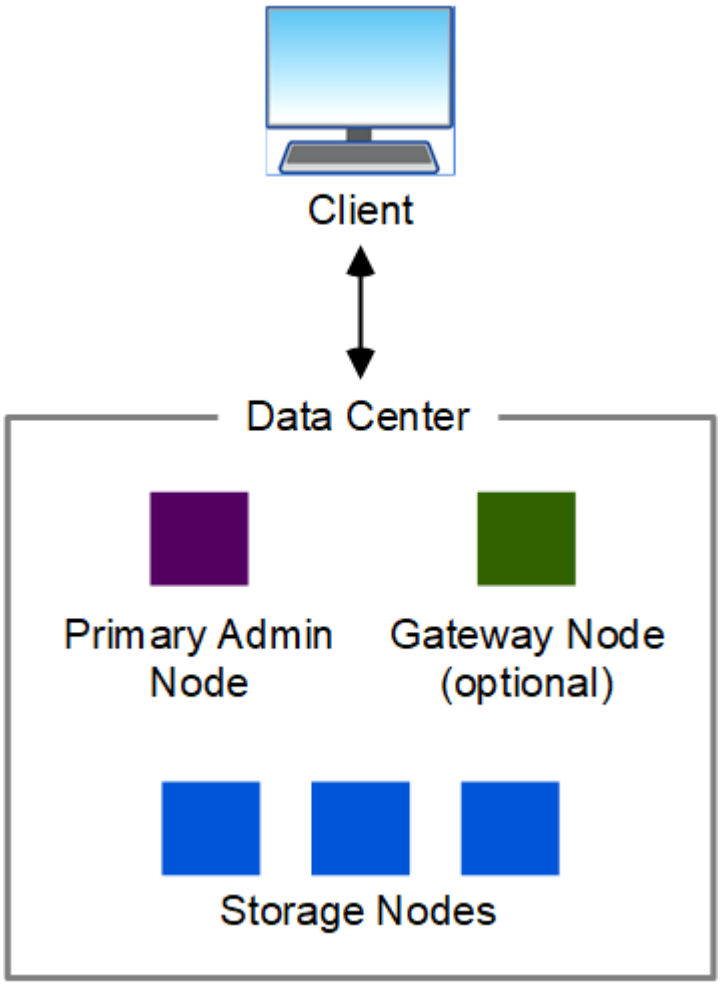
StorageGRID のネットワークトポロジー、要件、およびグリッド通信の詳細については、"ネットワークのガイドライン"を参照してください。

導入トポロジ

StorageGRIDシステムは、単一のデータ センター サイトまたは複数のデータ センター サイトに導入できます。展開あたりのサイトの最大数は 16 です。

単一サイト

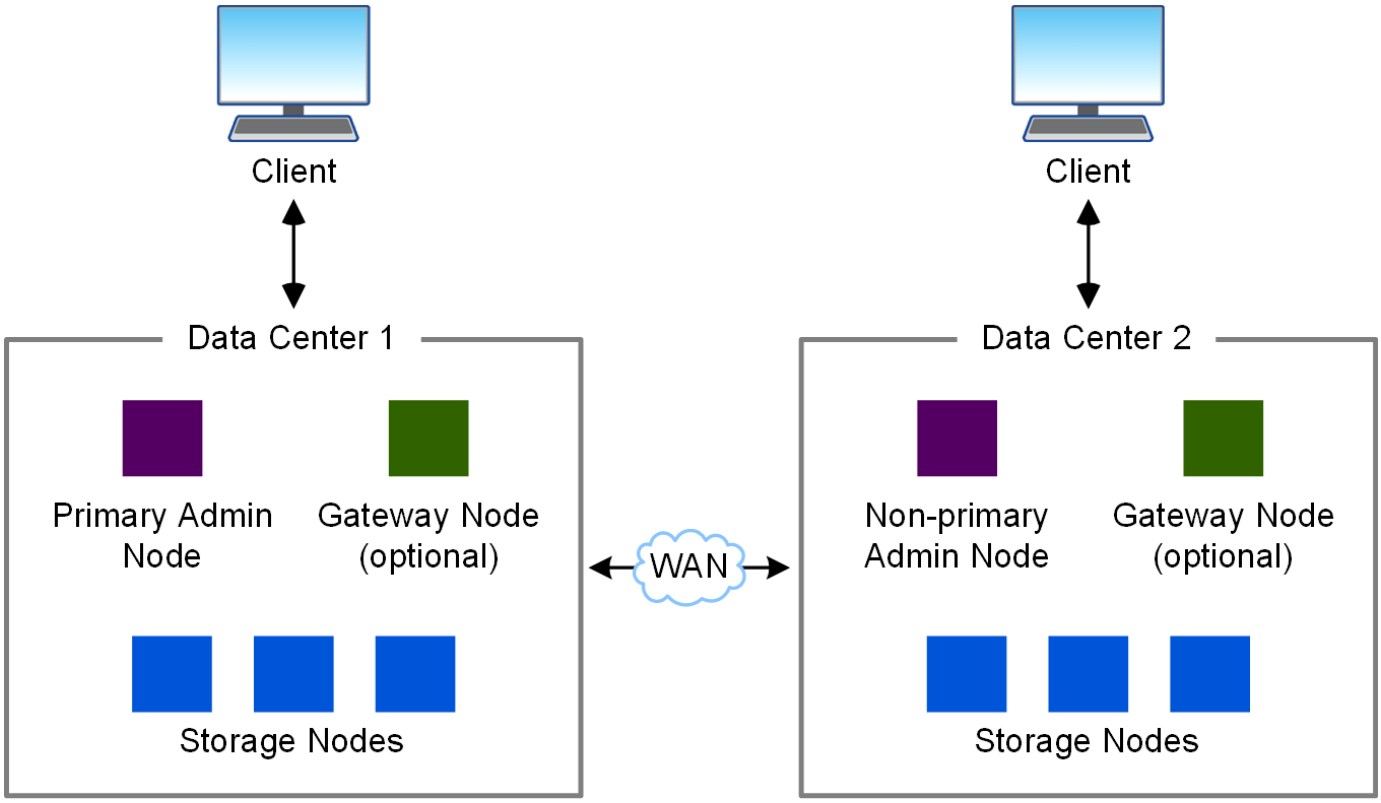
単一サイトに導入する場合は、 StorageGRID システムのインフラと運用が一元化されます。



複数のサイト

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

サイトは、地震断層線や氾濫原など、さまざまな障害領域にわたる地理的に異なる場所に位置することがよくあります。データの共有と災害復旧は、他のサイトへのデータの自動配布によって実現されます。



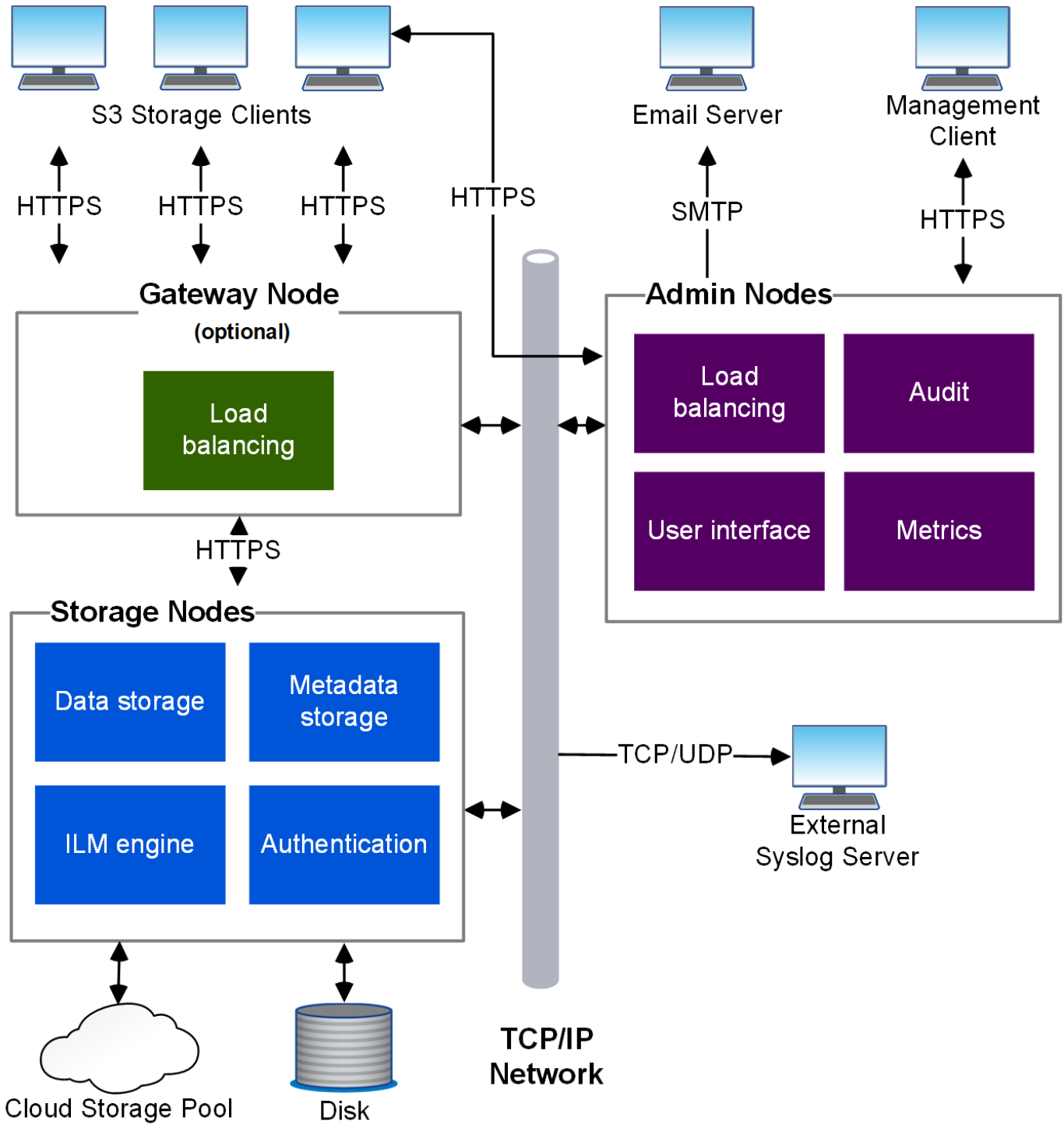
単一のデータ センター内に複数の論理サイトが存在することも可能で、分散レプリケーションと消去コーディングを使用して可用性と回復力を向上させることができます。

グリッドノードの冗長性

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

システムアーキテクチャ

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



S3クライアントは、StorageGRID でオブジェクトを保存および取得します。他のクライアントは、StorageGRID 管理インターフェイスへのアクセスに使用され、必要に応じて監査共有へのアクセスにも使用されます。さらに、StorageGRID はオプションで、外部 SMTP サーバー経由でメールアラートを送信できます。

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

オブジェクトは、ソフトウェアベースまたはハードウェアベースのストレージノード上、あるいは外部のS3バケットまたはAzure Blob Storageコンテナで構成されるクラウドストレージプールに、StorageGRID 内で保

存できます。

グリッドノードおよびサービス

StorageGRID グリッド ノードとサービス

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

グリッドノードのタイプ

StorageGRIDシステムは、次の 3 種類のグリッド ノードを使用します。

管理ノード
: システム構成、監視、ログ記録などの管理サービスを提供します。グリッドマネージャーにサインインすると、管理ノードに接続されます。各グリッドには1つのプライマリ管理ノードが必要であり、冗長性のために追加の非プライマリ管理ノードを設けることができます。どの管理ノードにも接続でき、各管理ノードには StorageGRID システムの同様のビューが表示されます。ただし、ほとんどのメンテナンス手順はプライマリ管理ノードを使用して実行する必要があります。

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

  を参照し "管理ノードとは"

ストレージノード
: オブジェクトデータとメタデータを管理、格納StorageGRIDシステムの各サイトには、少なくとも3つのストレージノードが必要です。

  新しいストレージノードの初期インストール時に、次の用途にのみ使用するように指定できます"メタデータまたはデータを保存する"。

  を参照し "ストレージノードとは"

ゲートウェイノード（オプション）
: クライアントアプリケーションがStorageGRIDへの接続に使用できるロードバランシングインターフェイスを提供します。ロードバランサによってクライアントが最適なストレージノードにシームレスに転送されるため、ノードやサイト全体の障害が透過的に処理されます。

  を参照し "ゲートウェイノードとは"

ハードウェアノードとソフトウェアノード

StorageGRIDノードは、 StorageGRIDアプライアンス ノードまたはソフトウェア ベースのノードとして展開できます。システムあたりのノードの最大数 (すべてのノード タイプを含む) は 220 です。

StorageGRID アプライアンスノード

StorageGRID ハードウェアアプライアンスは、 StorageGRID システム専用に設計されています。一部のアプライアンスはストレージノードとして使用できます。その他のアプライアンスは、管理ノードまたはゲートウェイノードとして使用できます。アプライアンスノードをソフトウェアベースのノードと組み合わせることが

できます。あるいは、外部のハイパーバイザー、ストレージ、コンピューティングハードウェアに依存しない、専用のアプライアンスのみで構成されたグリッドを導入することもできます。

使用可能なアプライアンスの詳細については、以下を参照してください。

- "StorageGRID アプライアンスのドキュメント"
- "NetApp Hardware Universe"

ソフトウェアベースのノード

ソフトウェア ベースのグリッド ノードは、VMware 仮想マシンとして、または Linux ホスト上のコンテナー エンジン内に展開できます。見る"ソフトウェアベースのノードにStorageGRIDをインストールする" 。

を使用して、 "NetApp Interoperability Matrix Tool（IMT）"サポートされているバージョンを確認します。

StorageGRID サービス

StorageGRID サービスの一覧を以下に示します。

サービス	製品説明	場所
アカウントサービスフォワーダ	ロードバランササービスがリモートホスト上のアカウントサービスを照会するためのインターフェイスを提供し、ロードバランサエンドポイントの設定変更をロードバランササービスに通知します。	管理ノードおよびゲートウェイノード上のロードバランササービス
ADC（Administrative Domain Controller）	トポロジ情報を管理し、認証サービスを提供するとともに、 LDR サービスおよび CMN サービスから送られるクエリに応答します。	各サイトにADCサービスを含むストレージノードが少なくとも3つ
AMS（監査管理システム）	監査対象のすべてのシステムイベントとトランザクションを監視し、テキストログファイルに記録します。	管理ノード
アヴァヒ・デーモン	ローカル ネットワーク内の名前解決とサービス検出に使用される mDNS を処理します。	すべてのノード
キャッシュサービス	ロード バランサー (ゲートウェイ) ノード上で実行され、オブジェクト コンテンツのローカル キャッシュを管理します。	ゲートウェイノード
Cassandra	オブジェクト メタデータの分散データベースを管理します。	ストレージノード（データ専用を除く）
Cassandra Reaper	オブジェクトメタデータの自動修復を実行します。	ストレージノード

サービス	製品説明	場所
チャンクサービス	イレイジャーコーディングされたデータフラグメントとパリティフラグメントを管理します。	ストレージノード
CMN（Configuration Management Node）	システム全体の設定とグリッドタスクを管理します。各グリッドには1つのCMNサービスがあります。	プライマリ管理ノード
DDS（Distributed Data Store）	Cassandra データベースとのインターフェイスを提供してオブジェクトメタデータを管理します。	ストレージノード
DMV（Data Mover）	データをクラウドエンドポイントに移動します。	ストレージノード
動的IP（dynip）	IP の動的な変更がないかグリッドを監視し、ローカル設定を更新します。	すべてのノード
gdu-server	グリッドの保守およびプロビジョニング処理を実行するためのバックエンドタスクランナー。 `mgmt-api`およびその他のユーティリティスクリプトからのリクエストを受け付け、検証し、プロビジョニング、拡張、廃止、アップグレードなど、各アクションを適切なGDUタスクハンドラにディスパッチします。	管理ノード
グラファーナ	Grid Manager に表示される指標に使用されます。	管理ノード
高可用性	高可用性グループページで設定されたノード上の高可用性仮想IPアドレスを管理します。このサービスは *keepalived* サービスとも呼ばれています。	管理ノードとゲートウェイノード
ID （ idnt ）	ローカル ユーザーとグループ、認証を管理し、LDAP および Active Directory からのユーザー ID を統合します。	ADCサービスを使用するストレージノード
ラムダ・アービトレーター	S3 Select SelectObjectContent 要求を管理します。	すべてのノード
ロードバランサ（nginx-gw）	クライアントからストレージノードへのS3トラフィックのロードバランシングを提供します。	管理ノードとゲートウェイノード

サービス	製品説明	場所
LDR（Local Distribution Router）	グリッド内のコンテンツの格納と転送を管理します。	ストレージノード
mgmt-api	グリッドマネージャーのバックエンドAPI。グリッドの管理（構成、監視、保守ワークフロー）を行うための認証済みRESTエンドポイントを公開し、検証と権限管理を強制し、長時間実行される操作をオーケストレーションします。Grid Managerインターフェースおよびオートメーションクライアントで使用される主要なコントロールプレーンAPI。	管理ノード
MISCd Information Service Controlデーモン	他のノード上のサービスの照会と管理、およびノードの環境設定の管理（他のノードで実行されているサービスの状態の照会など）を行うためのインターフェイスを提供します。	すべてのノード
nginx	は、各種のグリッドサービス（ Prometheus や動的 IP など）が HTTPS API を介して他のノード上のサービスと通信できるようにするための、認証およびセキュアな通信のメカニズムとして機能します。	すべてのノード
nginx-gw ロードバランサー	クライアントからストレージノードへのS3トラフィックのロードバランシングを提供します。	管理ノードとゲートウェイノード
NMS（ネットワーク管理システム）	Grid Manager を介して表示される監視、レポート、および設定のオプションを強化します。	管理ノード
ノードエクスポーター（Prometheusデータ収集）	Prometheus 時系列メトリック収集のシステムレベルの統計を公開します。	すべてのノード
NTP	ネットワーク タイム プロトコル (NTP) サービス。	すべてのノード
永続性	リブート後も維持する必要があるルートディスク上のファイルを管理します。	すべてのノード
Prometheus	すべてのノードのサービスから時系列の指標を収集します。	管理ノード
RSM（Replicated State Machine）	プラットフォームサービス要求がそれぞれのエンドポイントに送信されるようにします。	ADCサービスを使用するストレージノード

サービス	製品説明	場所
SSM（Server Status Monitor）	ハードウェアの状態を監視して NMS サービスに報告します。	インスタンスがすべてのグリッドノードに存在する
サーバーマネージャー	StorageGRIDサービスを管理します。	すべてのノード
SNMPエージェント	SNMP 要求に応答します。	管理ノード
SNMP ポート管理サービス	SNMP ポートの動的管理を処理します。	すべてのノード
SSH（セキュアシェル）	安全なアクセスとリモート システム管理を処理します。	すべてのノード
SSM (システム ステータス モニター)	ハードウェアの状態を監視して NMS サービスに報告します。	すべてのノード
統計	S3 バケットに関連する追加のメトリクスを記録します。	ストレージノード
トレースエージェント（jaeger-agent）	トレース コレクター (jaeger-collector) によって送信されたトレース情報を受信して処理します。	すべてのノード
トレースコレクター (jaeger-collector)	トレース収集を実行し、テクニカルサポートが使用する情報を収集します。トレースコレクタサービスは、オープンソースのJaegerソフトウェアを使用しています。	管理ノード

StorageGRID 管理ノードとは何ですか？

管理ノードは、システムの設定、監視、ロギングなどの管理サービスを提供します。管理ノードを使用して、S3クライアントトラフィックの負荷を分散することもできます。各グリッドにはプライマリ管理ノードが 1 つ必要で、冗長性を確保するために任意の数の非プライマリ管理ノードを設定できます。

プライマリ管理ノードと非プライマリ管理ノードの違い

Grid Manager または Tenant Manager にサインインすると、管理ノードに接続されます。任意の管理ノードに接続することができ、各管理ノードにはStorageGRIDシステムの同様のビューが表示されます。ただし、プライマリ管理ノードは、非プライマリ管理ノードよりも多くの機能を提供します。たとえば、ほとんどのメンテナンス手順はプライマリ管理ノードから実行する必要があります。

次の表は、プライマリ管理ノードと非プライマリ管理ノードの機能をまとめたものです。

機能	プライマリ管理ノード	非プライマリ管理ノード
サービスを含むAMS	はい	はい
サービスを含むCMN	はい	いいえ
サービスを含むNMS	はい	はい
サービスを含むPrometheus	はい	はい
サービスを含むSSM	はい	はい
サービスと高可用性サービスが含まれます。ロードバランサ	はい	はい
（mgmt-api）をサポートします。管理アプリケーションプログラムインターフェイス	はい	はい
IPアドレスの変更やNTPサーバの更新など、ネットワーク関連のすべてのメンテナンスタスクに使用できる	はい	いいえ
リカバリパッケージをダウンロードできます	はい	はい
ストレージノードの拡張後にECのリバランシングを実行可能	はい	いいえ
ボリュームのリストア手順に使用できます。	はい	はい
1つ以上のノードからログファイルとシステムデータを収集可能	はい	はい
ストレージ、ゲートウェイ、および非プライマリ管理ノードを回復できます	はい	はい
プライマリ管理ノードを回復できる	はい	はい
アラート通知、AutoSupportパッケージ、SNMPトラップと通知を送信	はい。として機能し優先送信者ます。	はい。スタンバイ送信者として機能します。

優先送信者管理ノード

StorageGRID環境に複数の管理ノードが含まれている場合は、プライマリ管理ノードがアラート通知、AutoSupportパッケージ、SNMPトラップおよびインフォームの優先送信者となります。

通常のシステム操作では、優先送信者のみが通知を送信します。ただし、他のすべての管理ノードは優先送信

者を監視します。問題が検出された場合は、他の管理ノードがスタンバイ送信者として機能します。

次の場合には、複数の通知が送信される可能性があります。

- 管理ノードどうしが「孤立」すると、優先送信者とスタンバイ送信者の両方が通知の送信を試み、通知のコピーが複数受信される可能性があります。
- スタンバイ送信者が優先送信者の問題を検出し、通知の送信を開始すると、優先送信者は通知の送信機能を回復する可能性があります。この問題が発生すると、重複した通知が送信される可能性があります。スタンバイ送信者は、優先送信者でエラーが検出されなくなると、通知の送信を停止します。

> AutoSupportパッケージのテスト時には、すべての管理ノードからテストが送信されます。アラート通知をテストするときは、すべての管理ノードにサインインして接続を確認する必要があります。

管理ノードのプライマリサービス

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

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

StorageGRIDストレージ ノードとは何ですか？

ストレージノードは、オブジェクトデータとメタデータを管理および格納します。ストレージノードには、ディスク上のオブジェクトデータとメタデータを格納、移動、検証、読み出すために必要なサービスとプロセスが含まれています。

StorageGRIDシステムの各サイトには、少なくとも3つのストレージノードが必要です。

ストレージノードのタイプ

インストール時に、インストールするストレージノードのタイプを選択できます。これらのタイプは、ソフトウェアベースのストレージノードおよびこの機能をサポートするアプライアンスベースのストレージノードで使用できます。

- データとメタデータを統合したストレージノード
- メタデータのみのストレージノード
- データ専用ストレージノード

ストレージノードタイプは次の状況で選択できます。

- ストレージノードの初回インストール時
- StorageGRIDシステムの拡張時にストレージノードを追加した場合

データとメタデータのストレージノード（組み合わせ）

デフォルトでは、すべての新しいストレージノードはオブジェクトデータとメタデータの両方を保存します。このタイプのストレージノードは、_複合_ストレージノードと呼ばれます。

メタデータのみのストレージノード

グリッドに非常に多数の小さなオブジェクトが格納されている場合は、メタデータ専用のストレージノードを使用すると効果的です。専用のメタデータ容量をインストールすると、非常に多数の小さなオブジェクトに必要なスペースと、それらのオブジェクトのメタデータに必要なスペースのバランスが向上します。また、メタデータのみのストレージノードをハイパフォーマンスアプライアンスでホストすることで、パフォーマンスを向上させることができます。

メタデータのみのストレージノードには、次の特定のハードウェア要件があります。

- StorageGRID アプライアンスを使用する場合、メタデータ専用ノードは、1.9 TB ドライブが 12 台または 3.8 TB ドライブが 12 台搭載された SGF6112 アプライアンスでのみ構成できます。
- ソフトウェアベースのノードを使用する場合は、メタデータのみのノードリソースが既存のストレージノードのリソースと一致していることを確認する必要があります。例えば：
  - 既存のStorageGRIDサイトでSG6000またはSG6100アプライアンスを使用している場合は、ソフトウェアベースのメタデータのみのノードが次の最小要件を満たしている必要があります。
    - 128GBのRAM
    - 8コアCPU
    - 8TB SSDまたはCassandraデータベース用同等のストレージ（rangedb/0）

- 既存のStorageGRIDサイトが 24 GB RAM、8 コア CPU、3 TB または 4 TB のメタデータ ストレージを備えた仮想ストレージ ノードを使用している場合、ソフトウェア ベースのメタデータ専用ノードでは同様のリソース (24 GB RAM、8 コア CPU、4 TB のメタデータ ストレージ (rangedb/0)) を使用する必要があります。

- 新しいStorageGRIDサイトを追加する場合、新しいサイトの合計メタデータ容量は、少なくとも既存のサイトと一致する必要があります。新しいサイトのリソースは、既存のサイトのストレージ ノードと一致する必要があります。

> メタデータのみのストレージノードにはが含まれておりLDRサアヒス、S3クライアント要求を処理できますが、StorageGRIDのパフォーマンスが向上しない場合があります。

データ専用ストレージノード

ストレージノードのパフォーマンス特性が異なる場合は、データ専用のストレージノードを使用するのが理にかなっています。たとえば、パフォーマンスを潜在的に向上させるために、データ専用で大容量の回転式ディスクストレージノードと、メタデータ専用のハイパフォーマンスストレージノードを組み合わせることができます。

さらに、Cassandra から RAM の少ないノードを削除することで、ノードごとのメタデータ容量制限が増加し、メタデータ容量を増やすことができます。。 "オブジェクトメタデータストレージを管理する" 。

複合ストレージノードをデータ専用ストレージノードに変換できます。ストレージノードにADCサービスが含まれており、変換の前提条件が満たされている場合、変換中にサービスは自動的に同じサイト内の別のストレージノードに移動されます。前提条件と詳細な手順については、"ストレージノードをデータ専用ノードに変換する"を参照してください。

グリッドごとおよびサイトごとの必要なストレージノード

トポロジで使用するストレージ ノードを選択するときは、グリッドまたはグリッド内の各サイトに次のものが含まれている必要があることに注意してください。

- サイトあたり（単一または複数サイトグリッド内）: 3ADCストレージ ノード (複合ストレージ ノードとメタデータのみのストレージ ノードの任意の組み合わせが可能)
- 単一サイト グリッド: 少なくとも 2 つのオブジェクト ストレージ ノード (複合ノードとデータ専用ノードの任意の組み合わせが可能)
- マルチサイト グリッド: サイトごとに少なくとも 1 つのオブジェクト ストレージ ノード (組み合わせまたはデータのみのいずれか)

ストレージノードのプライマリサービス

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

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

サービス	キー機能
アカウント（ acct ）	テナントアカウントを管理します。 データ専用ストレージノードはこのサービスをホストしません。
管理ドメインコントローラ（ADC）	トポロジとグリッド全体の構成を管理します。 データ専用ストレージノードはこのサービスをホストしません。 詳細 Administrative Domain Controller （ ADC ）サービスは、グリッドノードとその相互接続を認証します。ADCサービスは、サイトにある少なくとも3つのストレージノードでホストされます。 ADCサービスは、サービスの場所や可用性を含むトポロジー情報を維持します。グリッドノードが他のグリッドノードからの情報を必要とする場合、または他のグリッドノードにアクションを実行させる必要がある場合、ADCサービスに問い合わせて、要求を処理するのに最適なグリッドノードを検索します。さらに、ADCサービスはStorageGRIDデプロイメントの構成バンドルのコピーを保持しており、どのグリッドノードでも現在の構成情報を取得できます。 分散された処理および孤立した処理に対応するため、各 ADC サービスは、証明書、設定バンドル、およびサービスやトポロジに関する情報を、StorageGRID システム内の他の ADC サービスと同期します。 一般に、すべてのグリッドノードは少なくとも 1 つの ADC サービスへの接続を維持し、これにより、グリッドノードは常に最新情報にアクセスします。グリッドノードに接続すると、他のグリッドノードの証明書がキャッシュされるため、ADCサービスを使用できない場合でも既知のグリッドノードで引き続き機能できます。新しいグリッドノードが接続を確立するためには、 ADC サービスを使用する必要があります。 ADC サービスは接続された各グリッドノードからトポロジ情報を収集します。このグリッドノード情報には、 CPU 負荷、使用可能なディスクスペース（ストレージがある場合）、サポートされているサービス、およびグリッドノードのサイト ID が含まれます。その他のサービスは、トポロジクエリを介して ADC サービスにトポロジ情報を要求します。ADC サービスは、 StorageGRID システムから受信した最新情報で各クエリに応答します。
Cassandra	オブジェクトメタデータを格納し、保護します。 データ専用ストレージノードはこのサービスをホストしません。
Cassandra Reaper	オブジェクトメタデータの自動修復を実行します。 データ専用ストレージノードはこのサービスをホストしません。

サービス	キー機能
チャンク	イレイジャーコーディングされたデータフラグメントとパリティフラグメントを管理します。
Data Mover （ DMV ）	クラウドストレージプールにデータを移動します。
Distributed Data Store （ DDS ）	オブジェクトメタデータストレージを監視します。 詳細 各ストレージノードにはDistributed Data Store（DDS）サービスが含まれています。このサービスは、Cassandraデータベースと連携して、StorageGRIDシステムに格納されているオブジェクトメタデータに対してバックグラウンドタスクを実行します。 DDSサービスは、StorageGRIDシステムに取り込まれたオブジェクトの合計数と、システムでサポートされている各インターフェイス（S3）を使用して取り込まれたオブジェクトの合計数を追跡します。
ID （ idnt ）	LDAP および Active Directory から取得したユーザ ID を統合する データ専用ストレージノードはこのサービスをホストしません。

サービス	キー機能
[LDR-SERVICE]Local Distribution Router（LDR）	オブジェクトストレージプロトコル要求を処理し、ディスク上のオブジェクトデータを管理します。

サービス	キー機能
Replicated State Machine （ RSM ）	S3プラットフォームサービス要求がそれぞれのエンドポイントに送信されるようにします。 データ専用ストレージノードはこのサービスをホストしません。
SSM （サーバステータスモニタ）	オペレーティングシステムと基盤のハードウェアを監視します。

StorageGRID ゲートウェイノードとは何ですか？

ゲートウェイノードは、S3クライアントアプリケーションがStorageGRIDへの接続に使用できる専用のロードバランシングインターフェイスを提供します。ロードバランシングは、複数のストレージノードにワークロードを分散することで、速度と接続容量を最大化します。ゲートウェイノードはオプションです。

StorageGRIDロードバランササービスは、すべての管理ノードとすべてのゲートウェイノードに提供されます。クライアント要求の Transport Layer Security （ TLS ）終了を実行し、要求を検査し、ストレージノードへの新しいセキュアな接続を確立します。ロードバランササービスは、クライアントを最適なストレージノードにシームレスに転送するため、ノードやサイト全体の障害が透過的に発生します。

1つ以上のロードバランサエンドポイントを設定して、ゲートウェイノードおよび管理ノード上のロードバランササービスへのアクセスに使用するポートを定義します。ロードバランサエンドポイントでは、クライアントタイプ（S3）、バインドモード、および必要に応じて許可またはブロックされたテナントのリストも定義されます。を参照して "ロードバランシングに関する考慮事項"

必要に応じて、複数のゲートウェイノード（または管理ノード）をハイアベイラビリティ（HA）グループにグループ化できます。HAグループは個別のアクティブインターフェイスで障害が発生した場合は、バックアップインターフェイスでクライアントアプリケーションのワークロードを管理できます。を参照して "ハイアベイラビリティ（HA）グループを管理します"

ゲートウェイノードのプライマリサービス

次の表に、ゲートウェイノードのプライマリサービスを示します。他のほとんどのグリッドサービスが表示されるわけではありません。

サービス	キー機能
キャッシュサービス	オブジェクト コンテンツのローカル キャッシュを管理します。
高可用性	管理ノードとゲートウェイノードのグループのハイアベイラビリティ仮想 IP アドレスを管理します。 • 注：* このサービスは管理ノードにも搭載されています。
LDR	LDR サービスは次のタスクを処理します。 • クエリ • 情報ライフサイクル管理（ILM）のアクティビティ • オブジェクトの削除 • オブジェクトデータのストレージ • 別の LDR サービス（ストレージノード）からのオブジェクトデータの転送 • データストレージ管理 • S3プロトコルインターフェイス 支援 LDR サービスは、S3オブジェクトをネットワークに公開するために使用するポートを一意の UID にマッピングします。 オブジェクトストア LDR サービスの基盤となるデータストレージは、一定数のオブジェクトストア（と管理ノードのボリュームとも呼ばれます）に分割されます。各オブジェクトストアは、ストレージノード内の個別のマウントポイントです。 オブジェクトストアは、ボリューム ID と呼ばれる 0000 ~ 002F の 16 進数で識別されます。最初のオブジェクトストア（ボリューム 0 ）では、 Cassandra データベースのオブジェクトメタデータ用にスペースがリザーブされます。このボリュームの残りのスペースは、オブジェクトデータの保存と保護に使用されます。他のすべてのオブジェクトストアはオブジェクトデータ専用です。オブジェクトデータにはレプリケートコピーとイレイジャーコーディングフラグメントがあります。 StorageGRID は Cassandra データベースにオブジェクトメタデータを格納します。 Cassandra データベースは LDR サービスと連携します。 冗長性を確保してオブジェクトメタデータを損失から保護するために、各サイトでオブジェクトメタデータのコピーが 3 つ保持されます。このレプリケーションは設定できず、自動的に実行されます。詳細については、を参照してください "オブジェクトメタデータストレージを管理する"。

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

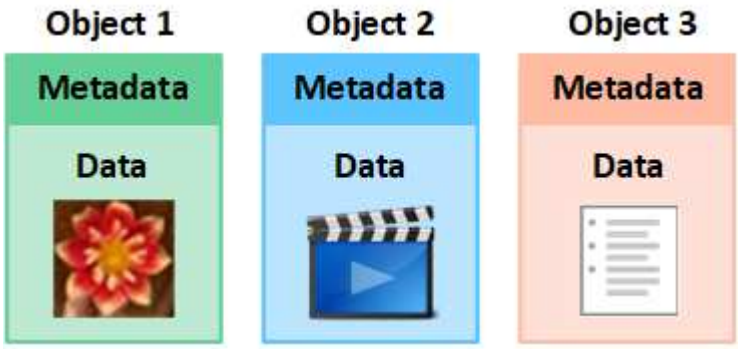
StorageGRID によるデータの管理方法

StorageGRIDオブジェクトとは

オブジェクトストレージでは、ストレージの単位がファイルやブロックではなく、オブジェクトになります。ファイルシステムやブロックストレージのツリー階層とは異なり、オブジェクトストレージでは、フラットで非構造化されたレイアウトでデータが編成されます。

オブジェクトストレージでは、データの物理的な場所と、データを格納および読み出す方法が切り離されています。

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



オブジェクトデータとは

写真、映画、診療記録など、あらゆるものが含まれます。

オブジェクトメタデータとは

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

オブジェクトメタデータには、次のような情報が含まれます。

- システムメタデータ（各オブジェクト（UUID）の一意のID、オブジェクト名、S3バケットの名前、テナントアカウントの名前またはID、オブジェクトの論理サイズ、オブジェクトの作成日時、オブジェクトの

最終変更日時など）。

- 各オブジェクトコピーまたはイレイジャーコーディングフラグメントの現在の格納場所。
- オブジェクトに関連付けられているユーザメタデータ。

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

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

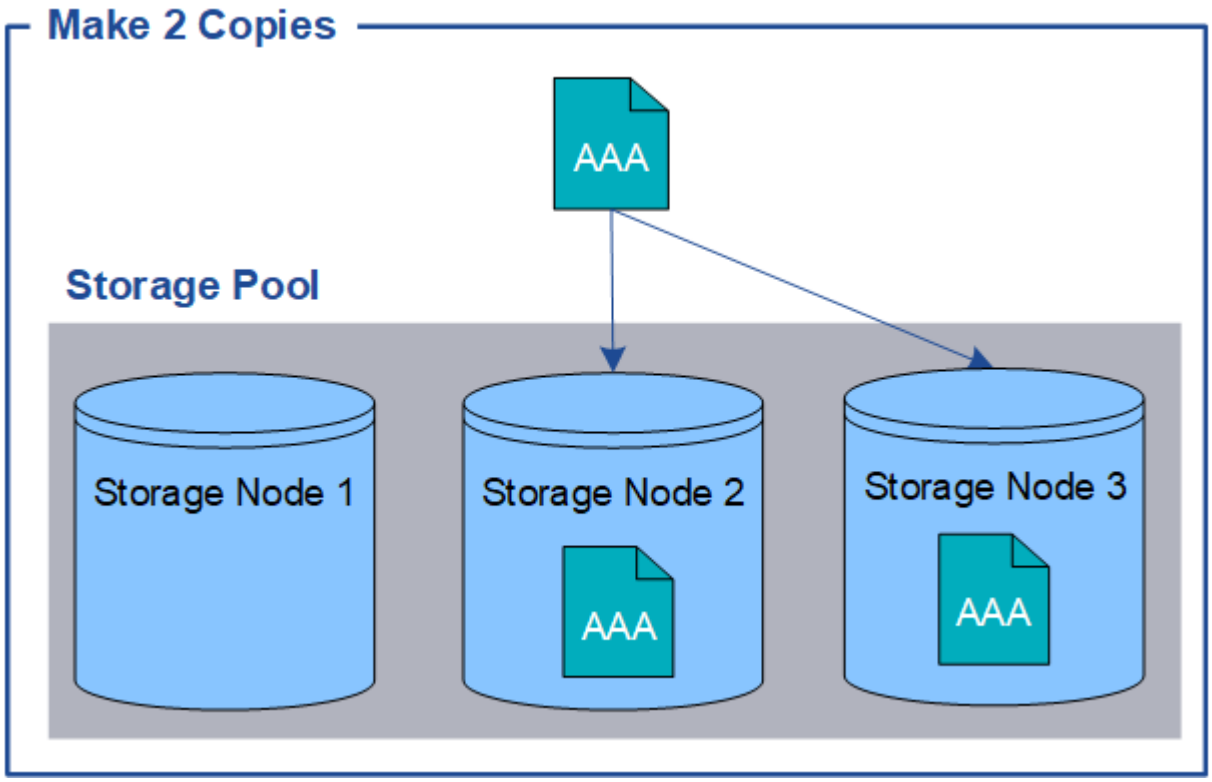
オブジェクトデータはどのように保護されますか？

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

レプリケーション

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

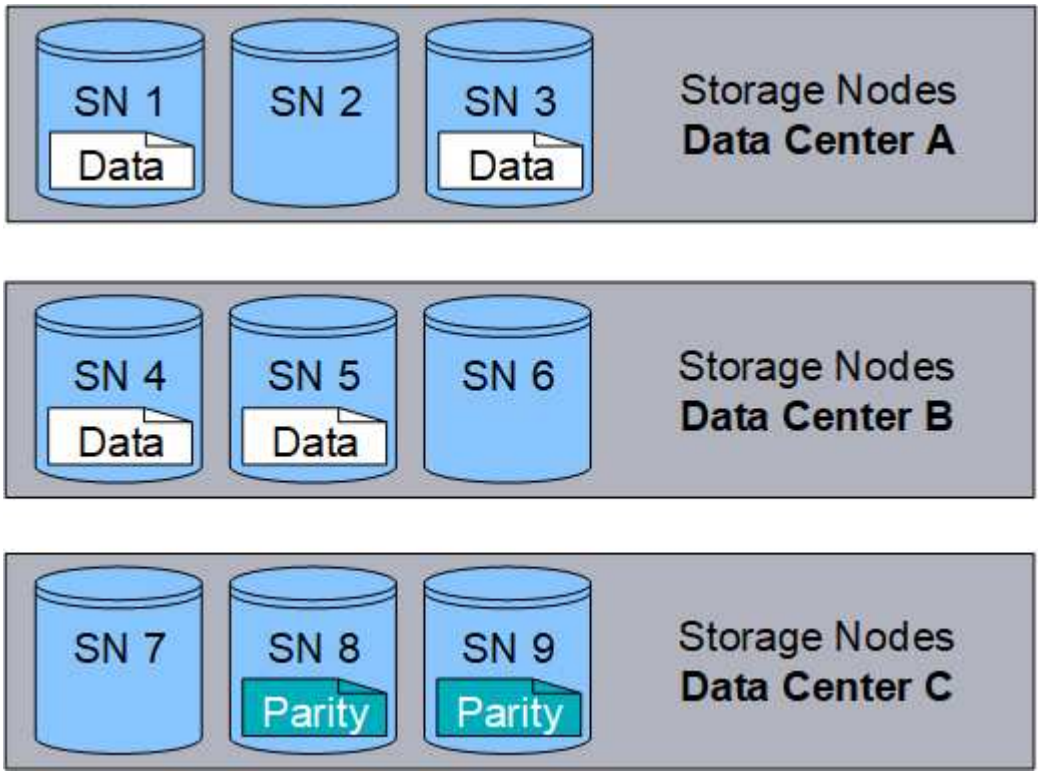
次の例では、 Make 2 Copies ルールによって、 3 つのストレージノードからなるストレージプールに各オブジェクトのレプリケートコピーを 2 つずつ配置するように指定しています。



イレイジャーコーディング

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

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



関連情報

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

StorageGRID でのオブジェクトのライフサイクル

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

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

- 取り込み：S3クライアントアプリケーションからHTTP経由でStorageGRIDシステムにオブジェクトを保存するプロセスです。このステージでは、 StorageGRID システムがオブジェクトの管理を開始します。

- コピー管理：アクティブなILMポリシーのILMルールに従って、StorageGRIDでレプリケートコピーとイレイジャーコーディングコピーを管理するプロセスです。コピー管理ステージでは、StorageGRIDがオブジェクトデータを損失から保護するために、指定した数とタイプのオブジェクトコピーをストレージノードまたはクラウドストレージプールに作成して保持します。
- * Retrieve * ： StorageGRID システムに格納されたオブジェクトにクライアントアプリケーションがアクセスするプロセス。クライアントがオブジェクトを読み取り、オブジェクトがストレージノードまたはクラウドストレージプールから読み出されます。
- * 削除 * ：グリッドからすべてのオブジェクトコピーを削除するプロセス。オブジェクトは、クライアントアプリケーションが StorageGRID システムに削除要求を送信することで削除されるか、オブジェクトの有効期間が終了したときに StorageGRID が実行する自動プロセスによって削除されます。



関連情報

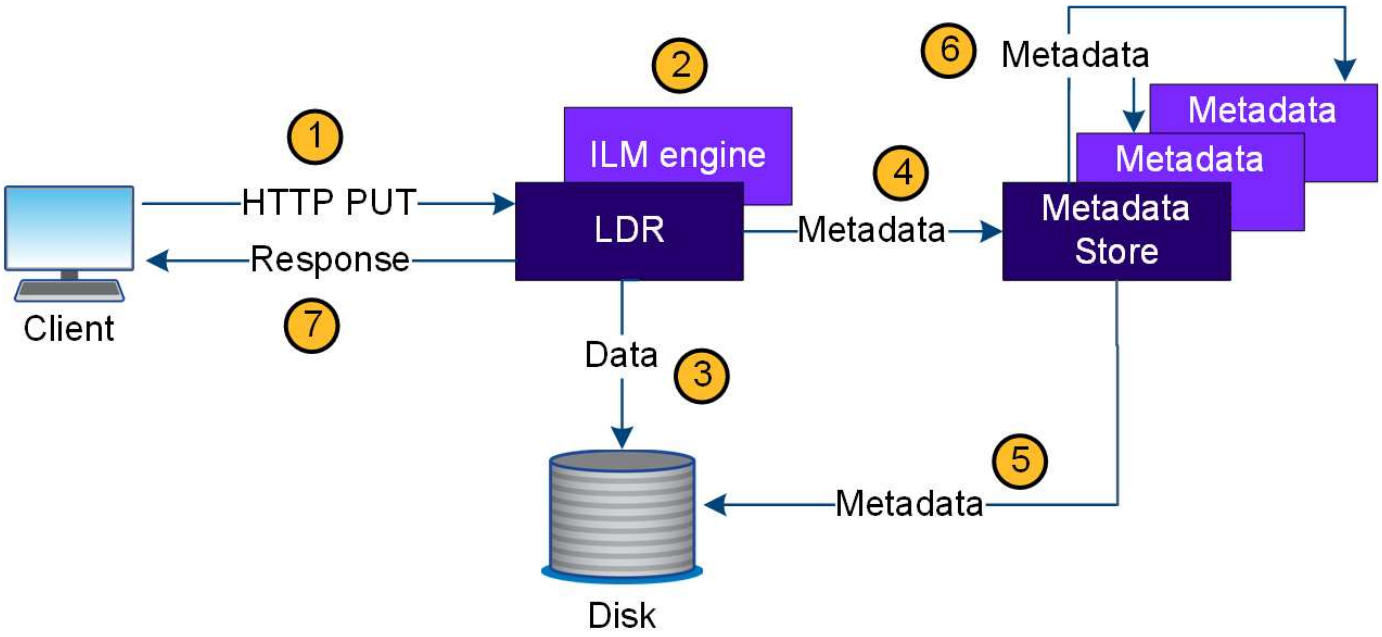
- "ILM を使用してオブジェクトを管理する"
- "情報ライフサイクル管理を使用"

StorageGRIDによるオブジェクト取り込みの処理方法

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

データフロー

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



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

StorageGRIDでオブジェクトコピーを管理する方法

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

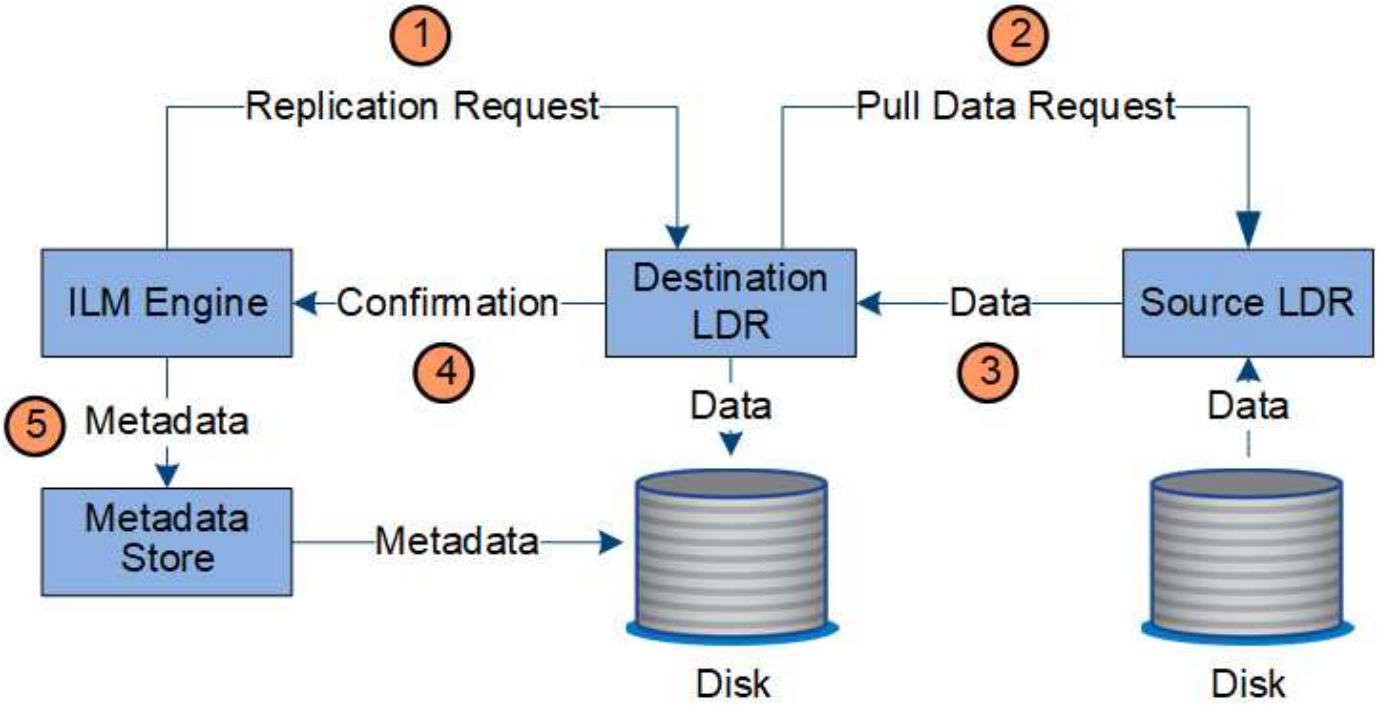
必要なオブジェクトコピーのタイプや場所は、オブジェクトのライフサイクルにおけるタイミングによって異なります。オブジェクトが必要に応じて配置されるように、 ILM ルールが定期的に評価されます。

オブジェクトデータは LDR サービスで管理されます。

コンテンツの保護：レプリケーション

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

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

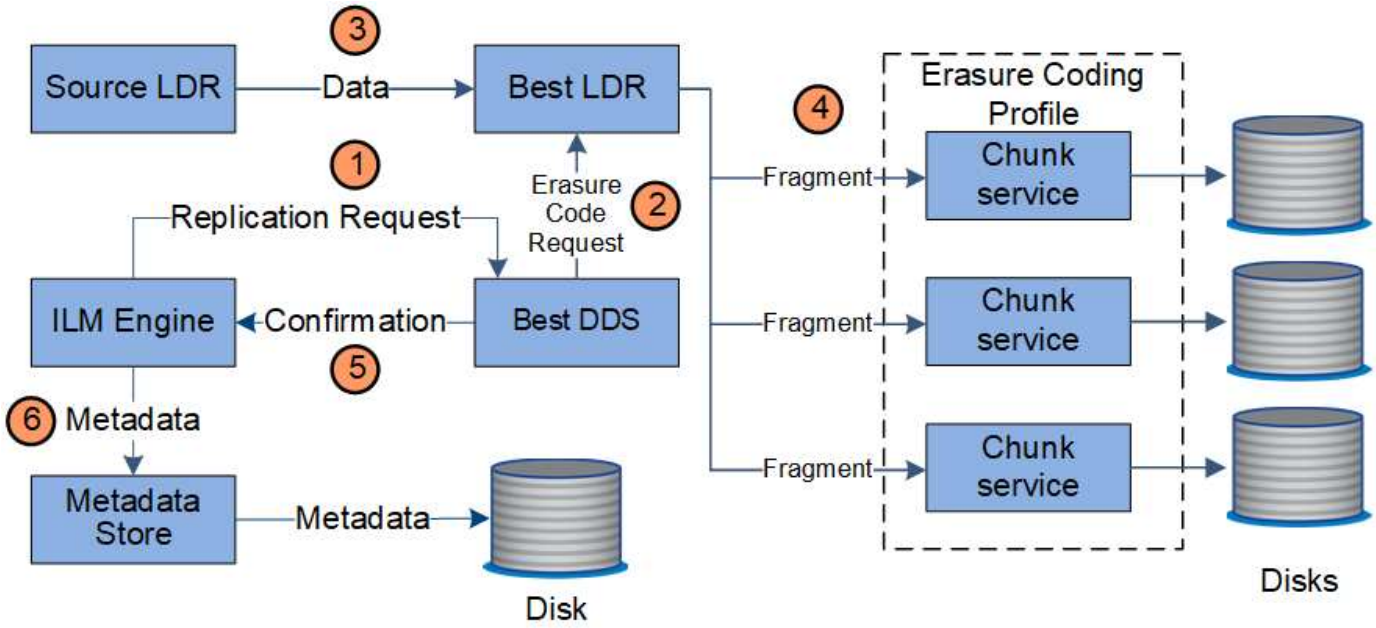


1. ILM エンジンが、 ILM ルールで指定されたストレージプール内で最適なデスティネーション LDR サービスを ADC サービスに照会します。その後、レプリケーションを開始するコマンドをその LDR サービスに送信します。
2. デスティネーション LDR サービスから、 ADC サービスを照会することで最適なソースの場所が特定されます。その後、レプリケーション要求をソース LDR サービスに送信します。
3. ソース LDR サービスからデスティネーション LDR サービスにコピーが送信されます。
4. デスティネーション LDR サービスから ILM エンジンに、オブジェクトデータ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

コンテンツの保護：イレイジャーコーディング

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

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

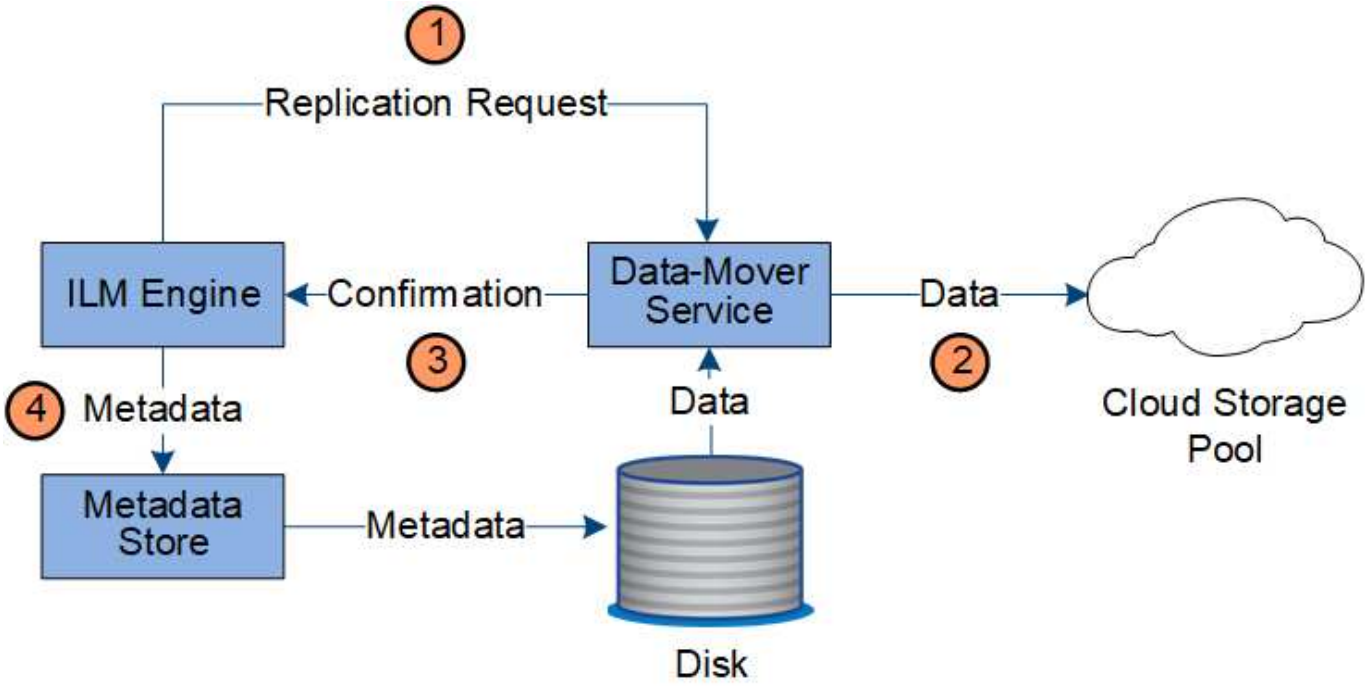


1. ILM エンジンから、 ADC サービスを照会することでイレイジャーコーディング処理の実行に最も適した DDS サービスが特定され、そのサービスに「Initiate」要求が送信されると、ILMエンジンからそのサービスに送信されます。
2. DDS サービスが、オブジェクトデータのイレイジャーコーディングを実行するように LDR に指示します。
3. ソース LDR サービスから、イレイジャーコーディングの対象として選択された LDR サービスにコピーが送信されます。
4. 適切な数のパリティフラグメントとデータフラグメントが作成されると、LDRサービスはそれらのフラグメントをイレイジャー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

コンテンツの保護：クラウドストレージプール

ILMルールのコンテンツ配置指示で、オブジェクトデータの複製コピーをクラウドストレージプールに保存する必要がある場合、オブジェクトデータは、クラウドストレージプール用に指定された外部S3バケットまたはAzure Blob Storageコンテナに複製されます。

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



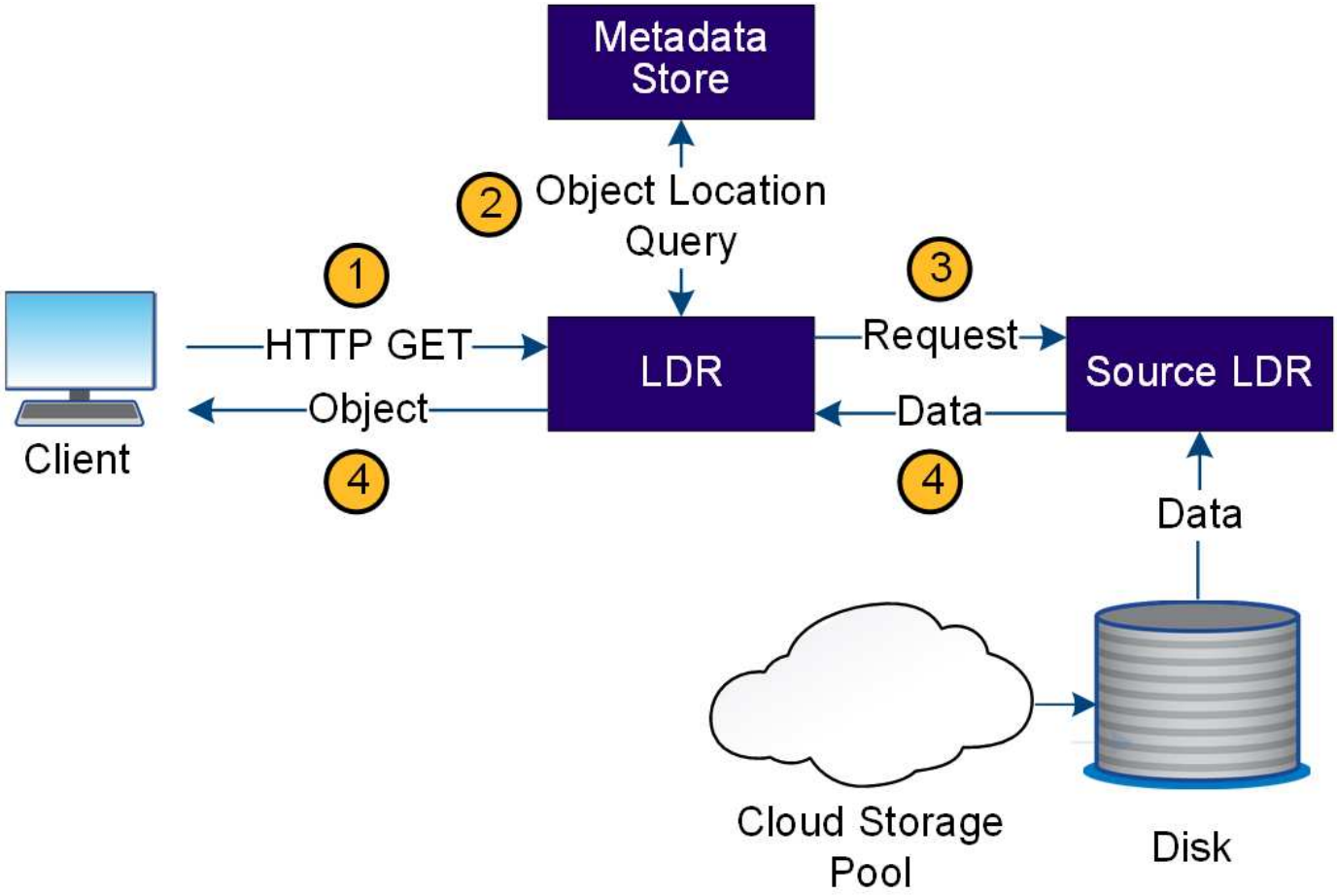
1. ILM エンジンが、クラウドストレージプールにレプリケートするための Data Mover サービスを選択します。
2. Data Mover サービスが、オブジェクトデータをクラウドストレージプールに送信します。
3. Data Mover サービスが、オブジェクトデータが格納されたことを ILM エンジンに通知します。
4. ILM エンジンが、メタデータストアのオブジェクトの場所を示すメタデータを更新します。

StorageGRIDによるオブジェクト取得の処理方法

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

ストレージノードの LDR サービスから、メタデータストアを照会することでオブジェクトデータの場所が特定され、ソース LDR サービスからオブジェクトデータが読み出されます。基本的には、ストレージノードからの読み出しが優先されます。ストレージノードでオブジェクトを使用できない場合、読み出し要求はクラウドストレージプールに転送されます。

AWS GlacierストレージまたはAzure Archive階層に唯一のオブジェクトコピーがある場合、クライアントアプリケーションはS3 RestoreObject要求を問題して、読み出し可能なコピーをクラウドストレージプールにリストアする必要があります。



1. LDR サービスがクライアントアプリケーションから読み出し要求を受信
2. LDR サービスからメタデータストアを照会することで、オブジェクトデータの場所とメタデータが特定されます。
3. LDR サービスからソース LDR サービスに読み出し要求が転送されます。
4. ソースLDRサービスは取得したオブジェクトデータをクエリ先のLDRサービスに返し、システムはオブジェクトをクライアントアプリケーションに返します。

StorageGRIDでオブジェクトの削除を処理する方法

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

削除階層

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

- * S3 オブジェクトのロック * ：グリッドでグローバルな S3 オブジェクトのロック設定が有効になっている場合、 S3 クライアントは S3 オブジェクトのロックを有効にしたバケットを作成し、 S3 REST API を使用して、そのバケットに追加された各オブジェクトバージョンの最新の保持設定とリーガルホールド設

定を指定できます。

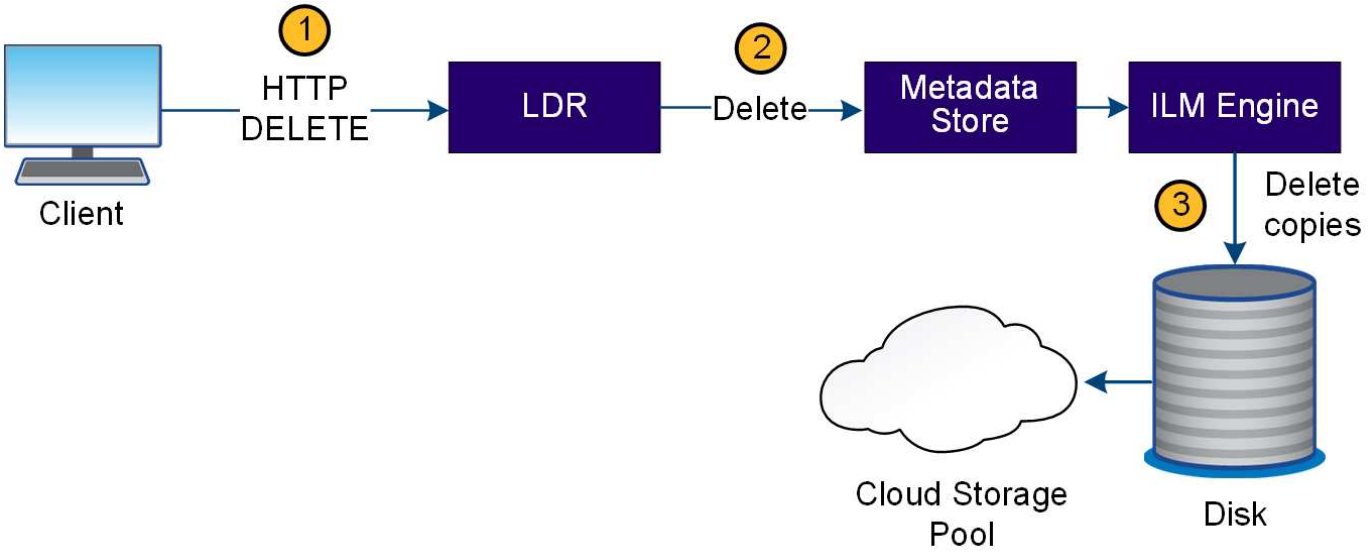
- リーガルホールドの対象となっているオブジェクトバージョンは、どの方法でも削除できません。
- オブジェクトバージョンのretain-until-dateに達する前は、どの方法でもそのバージョンを削除できません。
- S3オブジェクトロックが有効になっているバケット内のオブジェクトは、ILMによって「無期限」に保持されます。ただし、それまでの保持期間が終了したあとは、クライアント要求やバケットライフサイクルの終了によってオブジェクトバージョンを削除できます。
- S3クライアントがデフォルトのretain-until-dateをバケットに適用する場合、オブジェクトごとにretain-until-dateを指定する必要はありません。

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

> S3バケットライフサイクルが設定されている場合は、ライフサイクルフィルタに一致するオブジェクトのILMポリシーがライフサイクル有効期限のアクションで上書きされます。その結果、 ILM のオブジェクト配置手順がすべて終了したあとも、オブジェクトがグリッドに保持されることがあります。

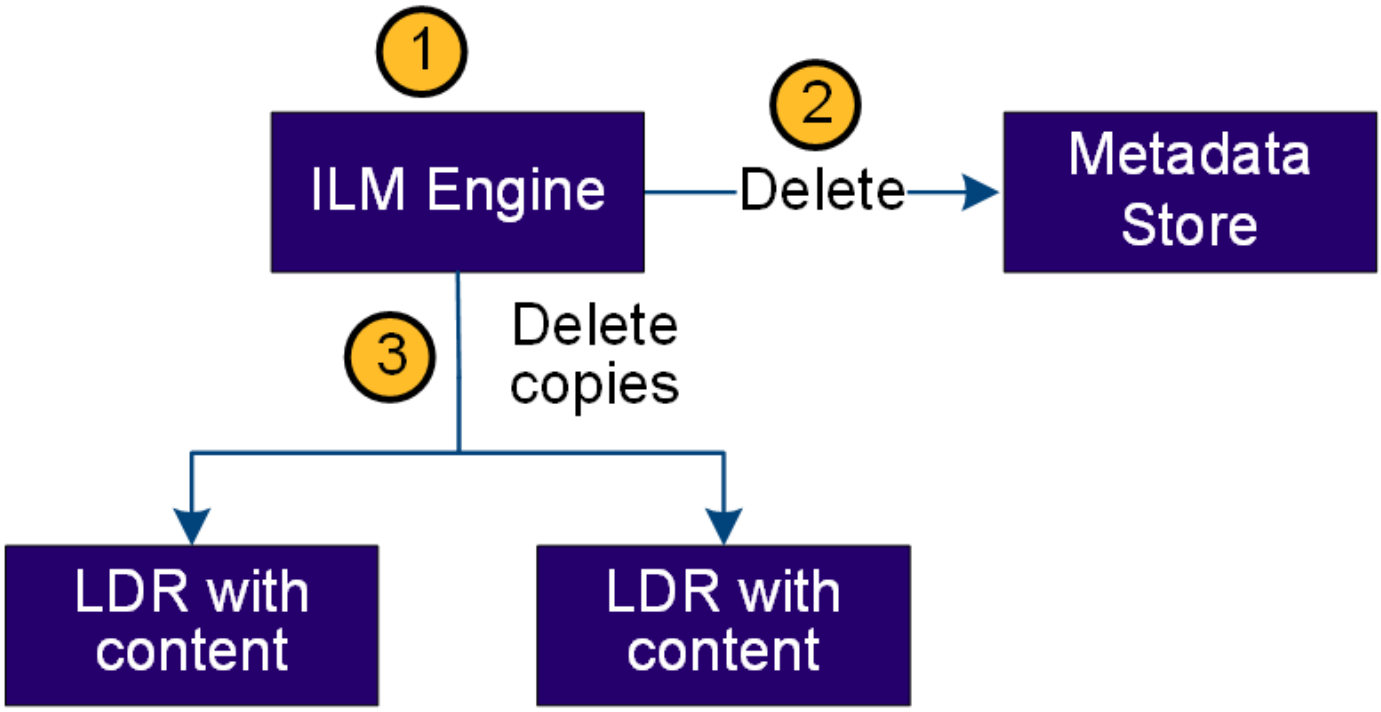
詳細については、を参照してください "オブジェクトの削除方法" 。

クライアント削除のデータフロー



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

ILM による削除のデータフローを示します



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

StorageGRID での情報ライフサイクル管理

情報ライフサイクル管理 (ILM) を使用して、 StorageGRIDシステム内のすべてのオブジェクトの配置、期間、および取り込み動作を制御します。 ILM ルールは、 StorageGRID が時間の経過とともにオブジェクトを保存する方法を決定します。 1 つ以上の ILM ルールを設定し、それらを ILM ポリシーに追加します。グリッドには、一度に複数のアクティブなポリシーを設定できます。

ILM ルールでは次の項目を定義

- どのオブジェクトを保存するか。ルールはすべてのオブジェクトに適用できます。また、フィルターを指定して、ルールが適用されるオブジェクトを識別することもできます。たとえば、ルールは、特定のテナント アカウント、特定の S3 バケット、または特定のメタデータ値に関連付けられたオブジェクトにのみ適用できます。

- ストレージのタイプと場所。オブジェクトはストレージノードまたはクラウドストレージプールに格納できます。
- 作成するオブジェクトコピーのタイプ。レプリケートコピーとイレイジャーコーディングコピーが可能
- レプリケートコピーの場合は、作成されるコピーの数。
- （イレイジャーコーディングコピーの場合）使用されるイレイジャーコーディングスキーム。
- オブジェクトのストレージの場所とコピーのタイプの経時的変化。
- オブジェクトがグリッドに取り込まれるときにオブジェクトデータを保護する方法（同期配置またはデュアルコミット）。

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

ILM ルールの例

たとえば、ILMルールでは次のように指定できます。

- テナントAに属するオブジェクトにのみ適用されます
- それらのオブジェクトのレプリケートコピーを2つ作成し、各コピーを別 々 のサイトに格納します。
- 2つのコピーは「無期限」で保持されます。つまり、StorageGRIDでは自動的に削除されません。これらのオブジェクトは、クライアントの削除要求によって削除されるか、バケットライフサイクルが終了するまで、 StorageGRID によって保持されます。
- 取り込み動作には[Balanced]オプションを使用します。テナントAがオブジェクトをStorageGRID に保存するとすぐに2サイトの配置手順が適用されます。ただし、必要な両方のコピーをすぐに作成できない場合は除きます。

  たとえば、テナント A がオブジェクトを保存したときにサイト 2 に到達できない場合、 StorageGRID はサイト 1 のストレージノードに 2 つの中間コピーを作成します。サイト 2 が使用可能になると、 StorageGRID はそのサイトで必要なコピーを作成します。

ILM ポリシーによるオブジェクトの評価方法

StorageGRIDシステムのアクティブなILMポリシーによって、すべてのオブジェクトの配置、期間、および取り込み動作が制御されます。

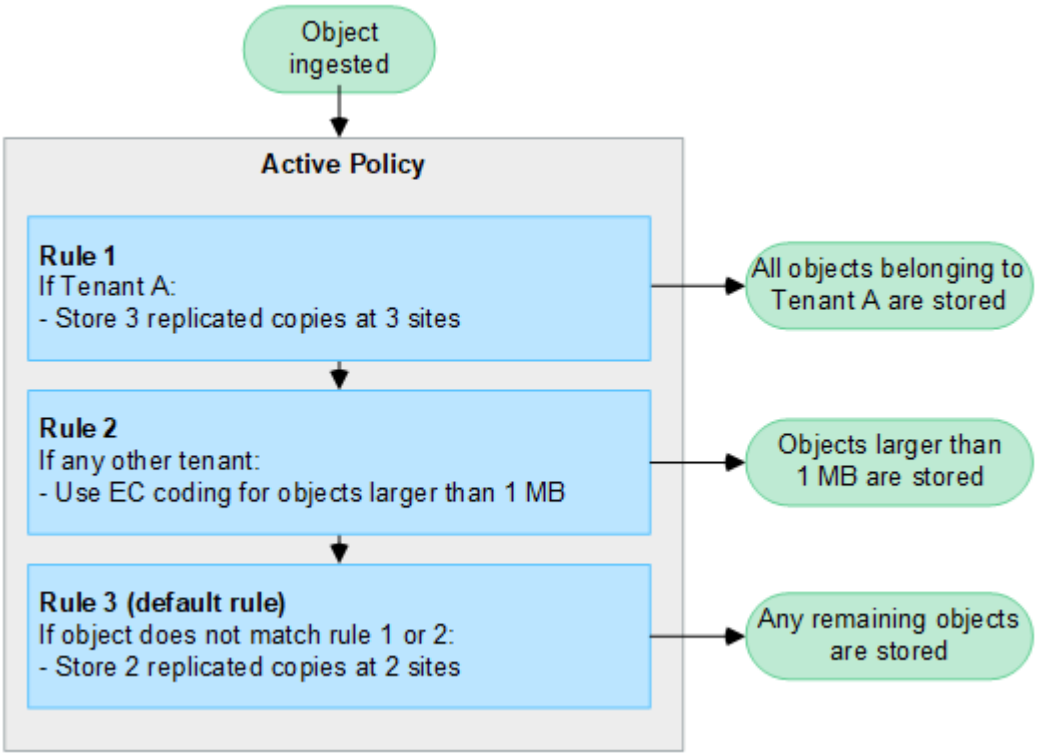
クライアントがオブジェクトを StorageGRID に保存すると、オブジェクトはアクティブポリシー内の順序付けられた ILM ルールに照らして次のように評価されます。

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

ILM ポリシーの例

たとえば、ILMポリシーに次の情報を指定する3つのILMルールを含めることができます。

- ルール**1**：テナント**A**のレプリケートコピー
  - テナントAに属するすべてのオブジェクトを一致します
  - これらのオブジェクトを3つのサイトに3つのレプリケートコピーとして格納します。
  - 他のテナントに属するオブジェクトはルール1に一致しないため、ルール2に照らして評価されます。
- ルール**2**：**1MB**を超えるオブジェクトのイレイジャーコーディング
  - 他のテナントのすべてのオブジェクトが一致します（1MBを超える場合にのみ一致します）。これらのオブジェクトは、 3 つのサイトで 6+3 のイレイジャーコーディングを使用して格納されます。
  - は1MB以下のオブジェクトに一致しないため、これらのオブジェクトはルール3に照らして評価されます。
- ルール**3**：**2**つのデータセンターに**2**つのコピーを作成（デフォルト）
  - は、ポリシー内の最後のデフォルトルールです。フィルタを使用しません。
  - ルール1またはルール2に一致しないすべてのオブジェクト（テナントAに属していない1MB以下のオブジェクト）のレプリケートコピーを2つ作成します。



関連情報

- "ILM を使用してオブジェクトを管理する"

StorageGRID の詳細をご覧ください

StorageGRIDグリッドマネージャの詳細

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

Grid Managerはリリースごとに更新され、このページのスクリーンショットの例とは異なる場合があります。

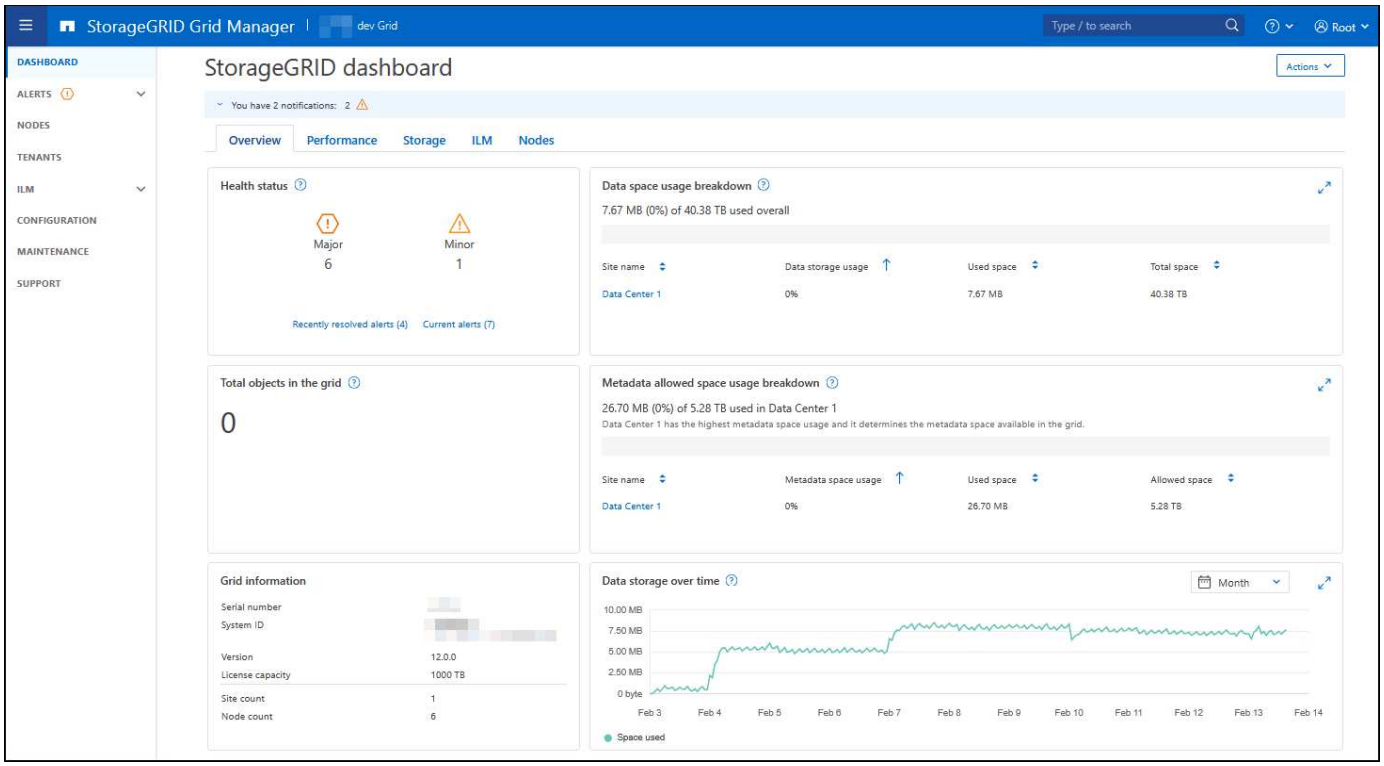
Grid Manager にサインインすると、管理ノードに接続されます。各 StorageGRID システムには、 1 つのプライマリ管理ノードと、任意の数のプライマリ以外の管理ノードが含まれています。どの管理ノードにも接続が可能で、各管理ノードに表示される StorageGRID システムのビューもほぼ同じです。

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

Grid Manager ダッシュボード

グリッドマネージャに初めてサインインしたときに、ダッシュボードを使用して概要を確認できます"システムアクティビティの監視"。

ダッシュボードには、システムの健全性とパフォーマンス、ストレージの使用状況、ILMプロセス、S3処理、およびグリッド内のノードに関する情報が含まれています。システムを効果的に監視するために必要な情報を含むカードのコレクションから選択できます"ダッシュボードの設定"。



各カードに表示されている情報の説明については、そのカードのヘルプアイコン(?)を選択してください。

検索フィールド

ヘッダーバーの * Search * フィールドを使用すると、 Grid Manager 内の特定のページにすばやく移動できます。たとえば、「* km *」と入力すると、キー管理サーバ（KMS）ページにアクセスできます。

- Search * を使用して、 Grid Manager のサイドバーおよび設定、メンテナンス、サポートの各メニューでエントリを検索できます。グリッドノードやテナントアカウントなどの項目を名前で検索することもできます。

ヘルプメニュー

ヘルプメニュー  からアクセスできる項目：

- その"FabricPool"そして"S3のセットアップ"魔法使い
- 現在のリリースのStorageGRIDドキュメントサイト
- "APIドキュメント"
- 現在インストールされているStorageGRIDのバージョンに関する情報

［アラート］メニュー

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

[Alerts]メニューでは、次の操作を実行でき"アラートの管理"ます。

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

[Nodes]ページ

その"[Nodesページ"]グリッド全体、グリッド内の各サイト、およびサイトの各ノードに関する情報を表示します。特定のサイトまたはノードの情報を表示するには、そのサイトまたはノードを選択します。

テナントページ

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

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

ILM メニュー

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

[ILM]メニューでは、ILMを表示および管理できます。

- ルール
- ポリシー
- ポリシータグ
- ストレージプール
- ストレージグレード
- 地域
- オブジェクトメタデータの検索

設定メニュー

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

ネットワークタスク

ネットワークタスクは次のとおりです。

- "ハイアベイラビリティグループを管理します"
- "ロードバランサのエンドポイントを管理する"
- "S3エンドポイントのドメイン名を設定"
- "トラフィック分類ポリシーを管理します"
- "VLAN インターフェイスを設定します"
- "管理インターフェースでStorageGRID CORSを有効にする"

セキュリティタスク

セキュリティタスクは次のとおりです。

- "セキュリティ証明書を管理する"
- "内部ファイアウォールコントロールを管理します"
- "キー管理サーバを設定"
- セキュリティ設定を構成する。"TLSおよびSSHポリシー" 、"ネットワークとオブジェクトのセキュリティオプション" 、"インターフェイスのセキュリティ設定" 、 そして"SSHアクセス オプション"
- 設定を構成する"ストレージプロキシ"または"管理プロキシ"

システムタスク

システムタスクは次のとおりです。

- "グリッドフェデレーション"を使用して、テナントアカウント情報を同期し、2つのStorageGRIDシステム間でオブジェクトデータをレプリケートします
- オプションで、"格納オブジェクトを圧縮します"オプション
- オプションで、"デフォルトのバケット一貫性設定"

- "S3 オブジェクトロックの管理"
- ストレージ設定を理解する"ストレージボリュームのウォーターマーク"
- "イレイジャーコーディングプロファイルの管理"

タスクの監視

監視タスクは次のとおりです。

- "メールサーバーの設定"
- "ログ管理を構成する"
- "SNMP による監視を使用する"

アクセス制御タスク

アクセス制御タスクは次のとおりです。

- "管理者グループを管理する"
- "管理者ユーザーの管理"
- 変更する"プロビジョニングパスフレーズ"または"ノードコンソールのパスワード"
- "アイデンティティフェデレーションを使用する"
- "SSOの設定"
- "複数管理者による検証を設定する"

メンテナンスメニュー

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

タスク

保守作業には次のものが含ま

- "運用停止処理" 未使用のグリッドノードとサイトを削除するには
- "拡張処理"新しいグリッドノードとサイトを追加するには
- "グリッドノードのリカバリ手順"障害が発生したノードを交換してデータをリストアするには
- "プロシージャ名を変更します"グリッド、サイト、およびノードの表示名を変更するには
- "オブジェクトの存在チェック操作"オブジェクトデータの有無（正確性ではない）を確認するため
- 実行する"ローリングリブート"複数のグリッドノードを再起動する
- オブジェクトデータの復元
  - "アプライアンスのストレージボリュームにオブジェクトデータをリストアします"
  - "システムドライブに損傷がない場合は、オブジェクトデータをストレージボリュームにリストアします"

- "オブジェクトデータをストレージボリュームにリストアする（システムドライブの障害）"

システム

実行可能なシステムメンテナンスタスクには、次のものがあります。

- "StorageGRID ライセンス情報を表示します"または"ライセンス情報を更新する"
- 生成とダウンロード"回復パッケージ"
- 選択したアプライアンスでStorageGRID ソフトウェアの更新（ソフトウェアのアップグレード、ホットフィックス、SANtricity OSソフトウェアの更新など）を実行する
  - "アップグレード手順"
  - "Hotfix 手順 の略"
  - "Grid Managerを使用してSG6000ストレージコントローラのSANtricity OSをアップグレードする"
  - "Grid Managerを使用してSG5700ストレージコントローラのSANtricity OSをアップグレードする"

ネットワーク

実行できるネットワークメンテナンス作業には、次のものがあります。

- "DNSサーバの設定"
- "グリッドネットワークサブネットの更新"
- "NTPサーバを管理します。"

サポートメニュー

Support （サポート）メニューには、テクニカルサポートがシステムの分析とトラブルシューティングに役立つオプションが表示されます。

ツール

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

- "AutoSupportの設定"
- "診断を実行します"グリッドの現在の状態
- "ログファイルとシステムデータを収集"
- "サポート指標を確認"

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

その他

[Support]メニューの[Other]セクションでは、次の操作を実行できます。

- 設定"I/Oの優先順位付け"
- 管理"リンクコスト"
- ノードサービスIDを表示する
- 管理"ストレージのウォーターマーク"

StorageGRIDテナントマネージャの詳細

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

Tenant Managerはリリースごとに更新されるため、このページのスクリーンショットの例とは異なる場合があります。

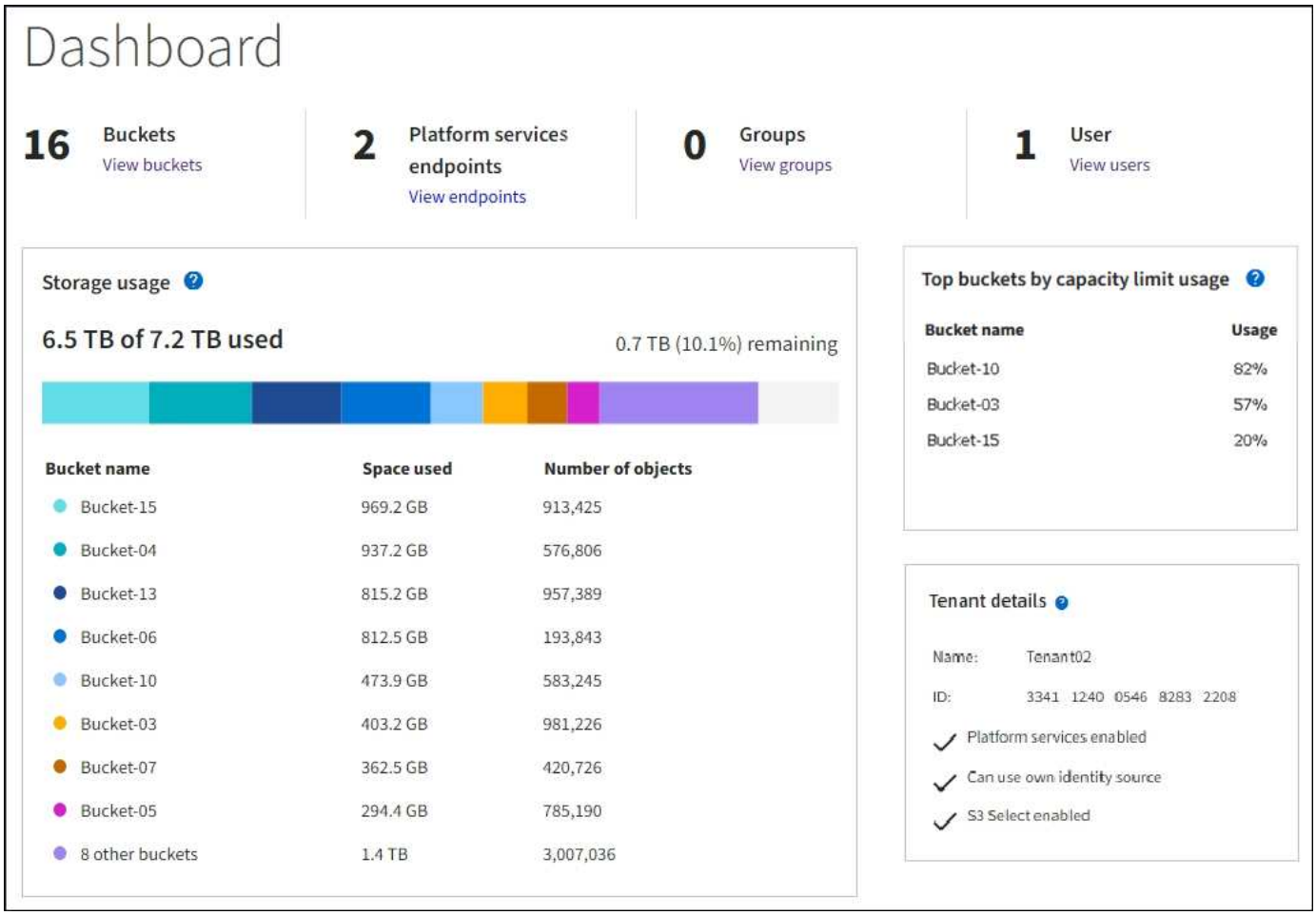
Tenant Manager にサインインしたテナントユーザは管理ノードに接続しています。

Tenant Managerのダッシュボード

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

テナント マネージャー ダッシュボードを使用すると、テナント ユーザーはストレージの使用状況を一目で監視できます。ストレージ使用量パネルには、テナントの最大の S3 バケットのリストが表示されます。使用済みスペースの値は、バケットまたはコンテナ内のオブジェクト データの合計量です。棒グラフは、これらのバケットまたはコンテナの相対的なサイズを表します。

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



[Storage]メニュー（**S3**）

このメニューにより、S3 ユーザーは次の操作を実行できます。

- アクセスキーを管理する
- バケットの作成、管理、削除
- プラットフォームサービスエンドポイントの管理
- 使用が許可されているグリッドフェデレーション接続を表示する

アクセスキー

S3 テナントユーザは次のようにアクセスキーを管理できます。

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

> 他のユーザーのアクセス キーの管理は、[アクセス管理] メニューから行います。

バケット

適切な権限を持つS3テナントユーザは、バケットに対して次のタスクを実行できます。

- バケットを作成する
- 新しいバケットの S3 オブジェクトロックを有効にする（ StorageGRID システムで S3 オブジェクトロックが有効になっていることを前提）
- 整合性の値を更新
- 最終アクセス時間の更新を有効または無効にします
- オブジェクトのバージョン管理を有効または一時停止します
- S3オブジェクトロックのデフォルトの保持期間を更新します
- Cross-Origin Resource Sharing （ CORS ）の設定
- バケット内のすべてのオブジェクトを削除する
- 空のバケットを削除します
- を使用し"S3コンソール"てバケットオブジェクトを管理する

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

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

プラットフォームサービスのエンドポイント

グリッド管理者がテナントアカウントにプラットフォームサービスの使用を有効にした場合は、Manage Endpoints権限を持つS3テナントユーザが各プラットフォームサービスのデスティネーションエンドポイントを設定できます。

グリッドフェデレーション接続

グリッド管理者がテナントアカウントにグリッドフェデレーション接続の使用を許可している場合は、Root Access権限を持つS3テナントユーザが接続名を表示し、クロスグリッドレプリケーションが有効になっている各バケットのバケット詳細ページにアクセスできます。 およびに、接続内のもう一方のグリッドにバケットデータがレプリケートされていたときに発生する最新のエラーを表示します。を参照して "グリッドフェデレーション接続を表示します"

Access 管理メニュー

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

ネットワークのガイドライン

StorageGRID のネットワークガイドライン

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

これらの手順について

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

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

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

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

開始する前に

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

ネットワークを設定する前に、StorageGRIDアーキテクチャを理解しておいてください（を参照）"StorageGRID の詳細をご覧ください"。

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

アプライアンスノードを設置

- "アプライアンスハードウェアを設置"

ソフトウェアベースのノードをインストール

- "ソフトウェアベースのノードにStorageGRIDをインストールする"

StorageGRID ソフトウェアを設定および管理する

- "StorageGRID の管理"
- "リリースノート"。NetAppアカウントでサインインするか、アカウントを作成してリリースノートにアクセスする必要があります。

StorageGRID のネットワークタイプ

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

トラフィックタイプ

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

ネットワークは次の方法で設定できます。

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

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

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

ネットワークインターフェイス

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

ネットワーク	インターフェイス名
グリッドネットワーク（必須）	eth0
管理ネットワーク（オプション）	eth1
クライアントネットワーク（オプション）	eth2

仮想ポートまたは物理ポートをノードネットワークインターフェースにマッピングする方法の詳細については、以下を参照してください。"ソフトウェアベースのノードにStorageGRIDをインストールする" 。

アプライアンスノード

- "SG6160ストレージアプライアンス"
- "SGF6112ストレージアプライアンス"
- "SG6000ストレージアプライアンス"
- "SG5800ストレージアプライアンス"
- "SG5700ストレージアプライアンス"
- "SG110およびSG1100サービスアプライアンス"
- "SG100およびSG1000サービス アプライアンス"

各ノードのネットワーク情報

ノードで有効にするネットワークごとに、次の項目を設定する必要があります。

- IPアドレス
- サブネットマスク
- ゲートウェイのIPアドレス

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

ハイアベイラビリティグループ

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

グリッドネットワーク

グリッドネットワークは必須です。このネットワークは、すべての内部 StorageGRID トラフィックに使用されます。グリッドネットワークは、グリッド内のすべてのノード間、すべてのサイトおよびサブネットを接続します。グリッドネットワーク上のすべてのノードが他のすべてのノードと通信できる必要があります。グリ

ッドネットワークは複数のサブネットで構成できます。NTP などの重要なグリッドサービスを含むネットワークも、グリッドサブネットとして追加できます。

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

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

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

グリッドネットワークゲートウェイに関する次の要件と詳細に注意してください。

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

管理ネットワーク

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

管理ネットワークを有効にするグリッドノードを選択できます。

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

- Grid Manager および Tenant Manager のユーザインターフェイスにアクセスします。
- NTP サーバ、 DNS サーバ、外部キー管理サーバ（ KMS ）、 Lightweight Directory Access Protocol （ LDAP ）サーバなどの重要なサービスへのアクセス
- 管理ノード上の監査ログへのアクセス。
- 保守とサポートのための Secure Shell Protocol （ SSH ）アクセス。

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

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

- 管理ネットワークサブネットの外部から接続を行う場合や複数の管理ネットワークサブネットを設定する

場合は、管理ネットワークゲートウェイが必要です。

- ノードの管理ネットワークサブネットリストで設定されているサブネットごとに静的ルートが作成されます。

クライアントネットワーク

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

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

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

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

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

クライアントネットワークゲートウェイについては、次の点に注意してください。

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

オプションの **VLAN** ネットワーク

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

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

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

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

> VLAN インターフェイスは管理ノードとゲートウェイノードにのみ追加できます。ストレージノードへのクライアントアクセスまたは管理アクセスにVLANインターフェイスを使用することはできません。

手順とガイドラインについては、を参照してください"VLAN インターフェイスを設定します"。

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

ネットワークトポロジの例

StorageGRID の **Grid Network** トポロジ

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

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

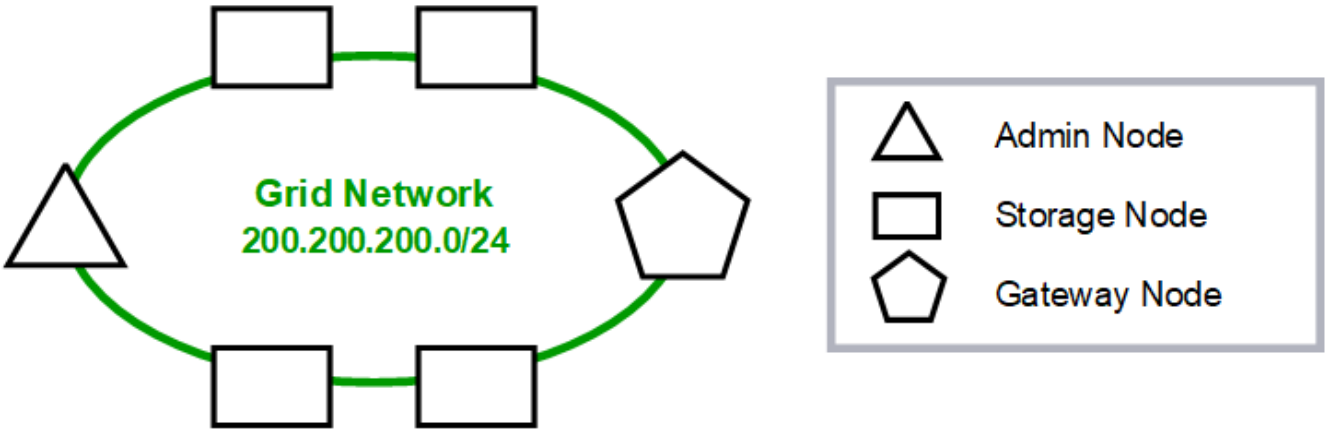
設定時に、グリッドネットワークサブネットリスト（ GNSL ）にすべてのグリッドネットワークサブネットを追加する必要があります。このリストには、すべてのサイトのすべてのサブネットが含まれ、 NTP 、 DNS 、 LDAP などの重要なサービスへのアクセスを提供する外部サブネットも含まれます。

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

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

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

Topology example: Grid Network only



Provisioned

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

System Generated

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

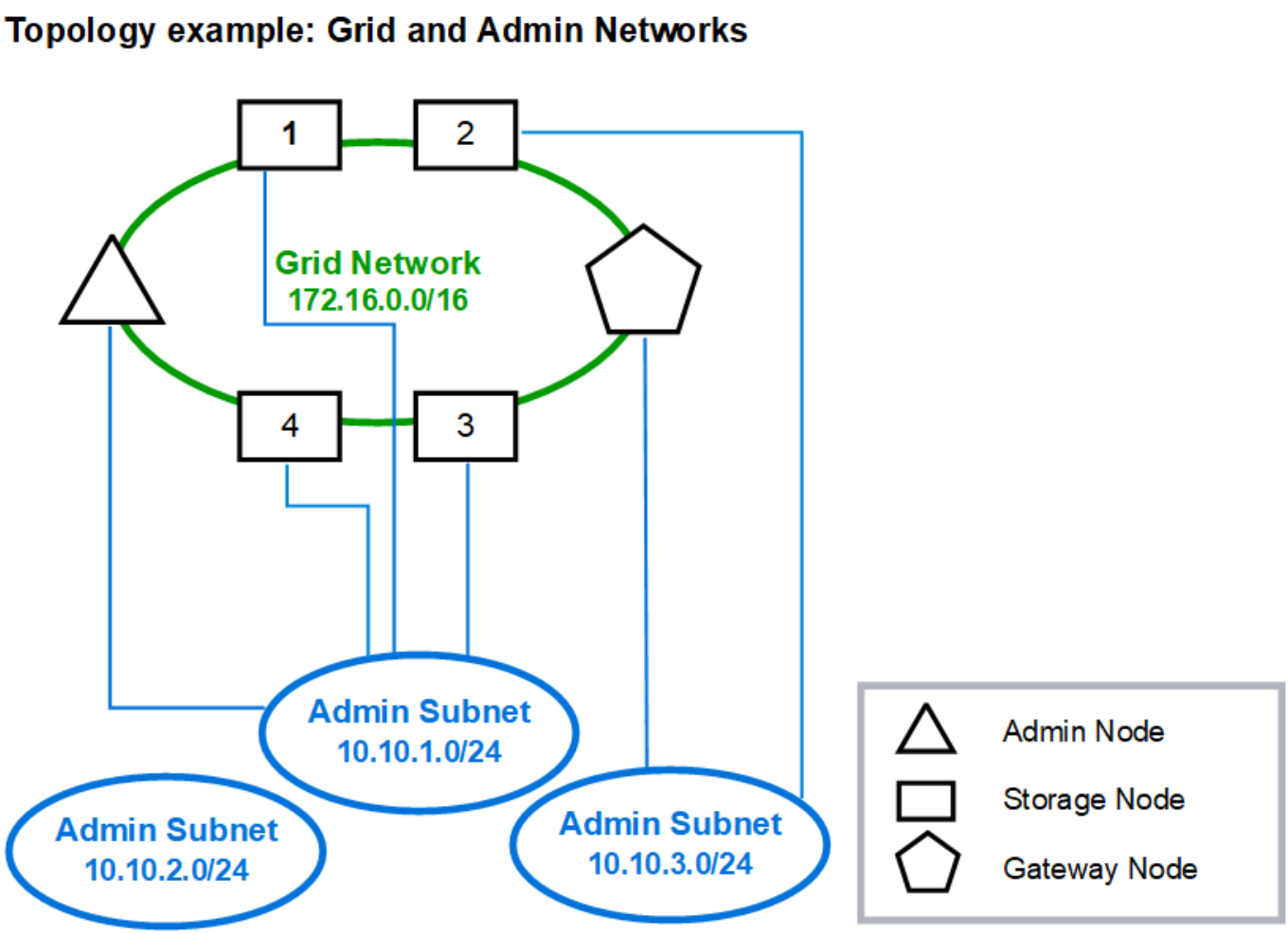
StorageGRID の管理ネットワーク トポロジ

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

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

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

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



Provisioned

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

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

System Generated

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

StorageGRID のクライアント ネットワーク トポロジ

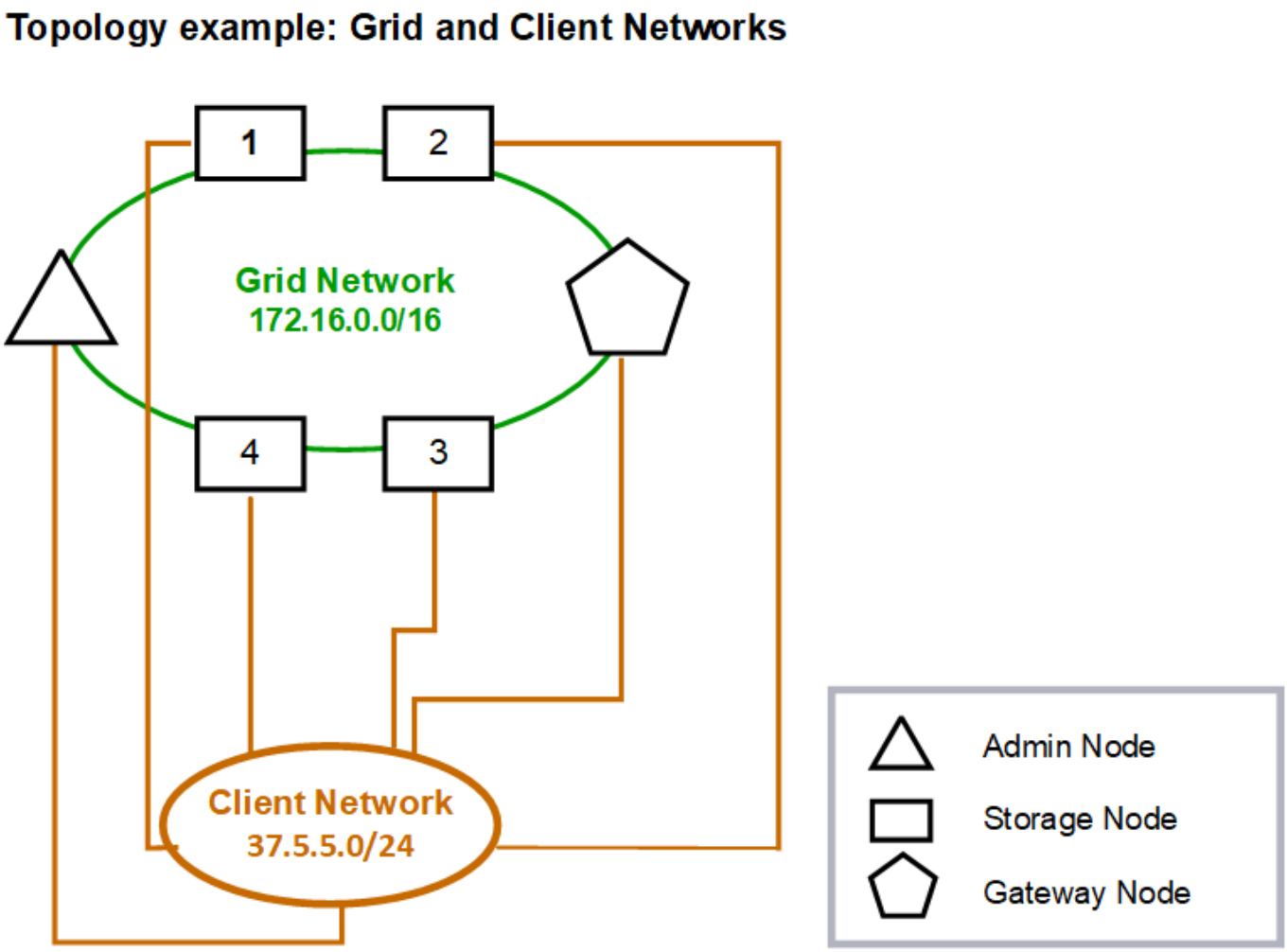
クライアントネットワークの使用はオプションです。クライアントネットワークを使用すると、クライアントネットワークトラフィック（S3など）をグリッドの内部トラフィックから分離できるため、グリッドネットワークのセキュリティが向上します。管理ネットワークが設定されていない場合、管理トラフィックはクライアントネットワークまたはグリッドネットワークのどちらでも処理できます。

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

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

この例では、クライアントネットワークはS3クライアント要求と管理機能に使用され、グリッドネットワー

クは内部のオブジェクト管理処理専用に使用されます。



Provisioned

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

System Generated

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

関連情報

"ノードのネットワーク設定の変更"

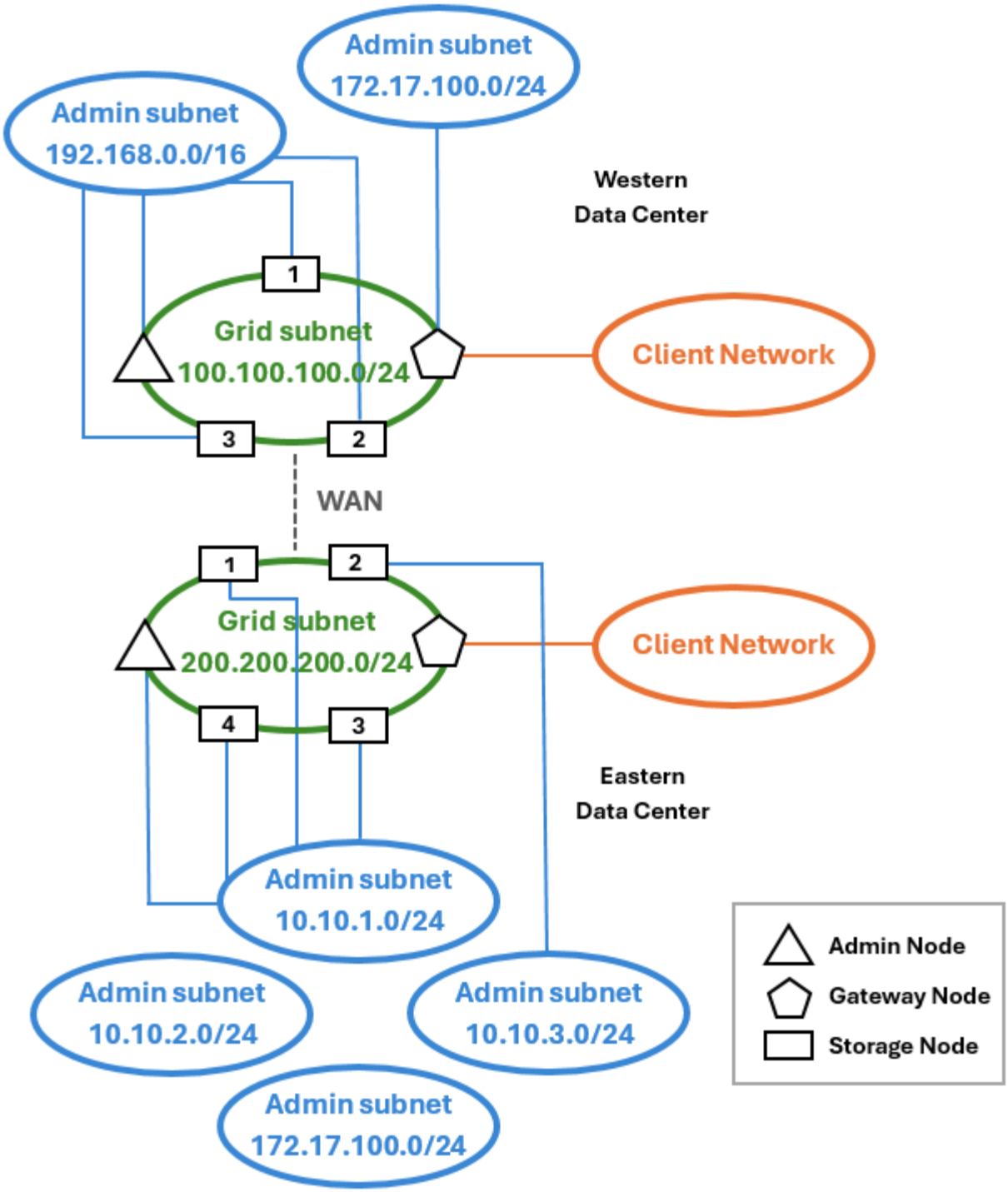
3つの**StorageGRID**ネットワークすべてのネットワーク トポロジ

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

次の例では、

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

トポロジの例：グリッドネットワーク、管理ネットワーク、クライアントネットワーク



StorageGRID のネットワーク要件

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

一般的なネットワーク要件

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

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

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

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

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



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

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

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

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

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

WAN帯域幅の実際の最小要件は、クライアントアクティビティとILM保護方式によって異なります。最小WAN帯域幅要件の見積もりについては、ネットアッププロフェッショナルサービスのコンサルタントにお問い合わせください。

管理ノードとゲートウェイノードの接続

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

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

ネットワークアドレス変換（ **NAT** ）の使用

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

StorageGRID のネットワーク固有の要件

各 StorageGRID ネットワークタイプの要件に従ってください。

ネットワークゲートウェイおよびルータ

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

サブネット

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

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

- ネットワークIPアドレスのサブネットマスクを255.255.255.254または255.255.255.255（CIDR表記では/31または/32）にすることはできません。
- ネットワークインターフェイスのIPアドレスとサブネットマスク（CIDR）によって定義されたサブネットは、同じノードに設定されている他のインターフェイスのサブネットと重複することはできません。
- どのノードのグリッド ネットワーク、管理ネットワーク、またはクライアント ネットワークにも、次の IPv4 アドレスを含むサブネットを使用しないでください。
  - 192,168,130,101

- 192,168,130,121
- 192,168,131,101
- 192,168,131,121
- 192,168,130,102
- 192,168,130,122
- 192,168,131,102
- 192,168,131,122
- 198.51.100.2
- 198.51.100.4

  たとえば、どのノードのグリッド ネットワーク、管理ネットワーク、またはクライアント ネットワークにも次のサブネット範囲を使用しないでください。

  - 192.168.130.0/24 は、このサブネット範囲に IP アドレス 192.168.130.101 と 192.168.130.102 が含まれているためです。
  - 192.168.131.0/24 は、このサブネット範囲に IP アドレス 192.168.131.101 と 192.168.131.102 が含まれているためです。
  - 198.51.100.0/24 は、このサブネット範囲に IP アドレス 198.51.100.2 と 198.51.100.4 が含まれているためです。

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

グリッドネットワーク

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

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

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

管理ネットワーク

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

管理ネットワークの一般的な用途には、管理接続、AutoSupport 、KMSのほか、重要なサーバ（グリッドネットワークまたはクライアントネットワーク経由で接続されていない場合）への接続があります。

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

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

クライアントネットワーク

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

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

関連情報

"ノードのネットワーク設定の変更"

環境固有のネットワークに関する考慮事項

StorageGRID Linuxデプロイメントのネットワーク構成

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

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

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

参照"インストール手順"。

コンテナエンジン導入用のホストネットワーク構成

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

物理ホスト

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

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

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

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

「Linux」は、RHEL、Ubuntu、または Debian のデプロイメントを指します。サポートされているバージョンのリストについては、 "NetApp Interoperability Matrix Tool（IMT）" 。

最小帯域幅の推奨値

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

ノードのタイプ	ネットワークのタイプ		
	グリッド	管理者	クライアント

ノードのタイプ	ネットワークのタイプ		
	最小**LAN**帯域幅	管理者	10Gbps
1Gbps	1Gbps	ゲートウェイ	10Gbps
1Gbps	10Gbps	ストレージ	10Gbps
1Gbps	10Gbps	アーカイブする	10Gbps

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

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

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

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

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

StorageGRIDの導入準備として、 StorageGRIDクラスタ内のホスト上の物理リソースとネットワークリソースを構成するための推奨方法については、以下を参照してください。"ホストネットワークを設定する" 。

プラットフォームサービスとクラウドストレージプール用のネットワークとポート

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

プラットフォームサービス用のネットワーク

およびで説明するように、"テナントのプラットフォームサービスを管理する""プラットフォームサービスを管理します"プラットフォームサービスには、検索統合、イベント通知、CloudMirrorレプリケーションを提供する外部サービスが含まれます。

プラットフォームサービスには、 StorageGRID ADC サービスをホストするストレージノードから外部サービ

スエンドポイントへのアクセスが必要です。アクセスの提供例は次のとおりです。

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

クラウドストレージプールのネットワーク

クラウドストレージプールでは、Amazon S3 GlacierやMicrosoft Azure Blob Storageなど、使用する外部サービスが提供するエンドポイントへのストレージノードからのアクセスも必要です。詳細については、"クラウドストレージプールとは"を参照してください。

プラットフォームサービスとクラウドストレージプールのポート

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

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

エンドポイントの作成時または編集時に別のポートを指定できます。を参照して "ネットワークポートのリファレンス"

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

VLAN およびプラットフォームサービスとクラウドストレージプール

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

StorageGRIDアプライアンス ノードのネットワーク構成

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

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

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

アプライアンスのポートボンディングモードに関する情報を参照してください。

- "ポートボンディングモード（SG6160）"
- "ポートボンディングモード（SGF6112）"
- "ポートボンディングモード（SG6000-CNコントローラ）"

- "ポートボンディングモード（SG5800コントローラ）"
- "ポートボンディングモード（E5700SGコントローラ）"
- "ポートボンディングモード（SG110およびSG1100）"
- "ポートボンディングモード（SG100およびSG1000）"

StorageGRID のネットワーク インストールとプロビジョニング

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

ノードの初期導入

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

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

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

プライマリ管理ノードへの自動ノード登録

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

管理ネットワークまたはクライアントネットワークを無効にします

管理ネットワークまたはクライアントネットワークを無効にする場合は、ノード承認プロセスで設定を削除するか、インストールの完了後にIP変更ツールを使用します（を参照）"IP アドレスを設定する"。

StorageGRID のインストール後のガイドライン

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

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

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

グリッドネットワーク設定がDHCPによって変更されるとノードがリブートします。DHCPの変更が複数のノードに同時に影響すると、システムが停止する可能性があります。

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

ネットワークポートのリファレンス

StorageGRID の内部グリッド ノード通信

StorageGRID の内部ファイアウォールは、グリッドネットワーク上の特定のポートへの受信接続を許可します。ロードバランサエンドポイントで定義されたポートにも接続が許可されます。

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

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

Linux ベースのノードについてはガイドラインを参照してください

エンタープライズ ネットワーク ポリシーによってこれらのポートへのアクセスが制限されている場合は、デプロイメント構成パラメータを使用してデプロイメント時にポートを再マップできます。ポートの再マッピングとデプロイメント構成パラメータの詳細については、以下を参照してください。"ソフトウェアベースのノードにStorageGRIDをインストールする" 。

ポート再マッピングのサポートは非推奨であり、将来のリリースでは削除される予定です。再マップされたポートを削除するには、"ベアメタルホストでのポートの再マッピングを削除します" 。

VMware ベースのノードについてのガイドラインを参照してください

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

エンタープライズ ネットワーク ポリシーによってこれらのポートへのアクセスが制限されている場合は、VMware vSphere Web Client を使用してノードを展開するときにポートを再マップするか、グリッド ノードの展開を自動化するときに構成ファイル設定を使用できます。ポートの再マッピングとデプロイメント構成パラメータの詳細については、"VMware にStorageGRIDをインストールする" 。

ポート再マッピングのサポートは非推奨であり、将来のリリースでは削除される予定です。再マップされたポートを削除するには、"ベアメタルホストでのポートの再マッピングを削除します" 。

アプライアンスノードのガイドライン

これらのいずれかのポートへのアクセスがエンタープライズネットワークポリシーで制限されている場合は、StorageGRID アプライアンスインストーラを使用してポートを再マッピングできます。を参照してください "オプション：アプライアンスのネットワークポートの再マッピング"

ポート再マッピングのサポートは非推奨であり、将来のリリースでは削除される予定です。再マップされたポートを削除するには、"StorageGRIDアプライアンスのポート再マップを削除します" 。

StorageGRID の内部ポート

ポート	**tcp** または **udp** です	開始	宛先	詳細
22	TCP	プライマリ管理ノード	すべてのノード	メンテナンス手順では、プライマリ管理ノードがポート 22 で SSH を使用して他のすべてのノードと通信できる必要があります。他のノードからの SSH トラフィックの許可は任意です。
80	TCP	アプライアンス	プライマリ管理ノードと非プライマリ管理ノード	StorageGRID アプライアンスが、インストールを開始する目的でプライマリ管理ノードと通信するために使用します。
123	UDP	すべてのノード	すべてのノード	ネットワークタイムプロトコルサービス。すべてのノードは、 NTP を使用して他のすべてのノードと時間を同期します。
443	TCP	すべてのノード	プライマリ管理ノードと非プライマリ管理ノード	インストールおよびその他のメンテナンス手順の実行中に、プライマリ管理ノードにステータスを通知するために使用します。
1055	TCP	すべてのノード	プライマリ管理ノードと非プライマリ管理ノード	インストール、拡張、リカバリ、およびその他のメンテナンス手順用の内部トラフィック。
1139	TCP	ストレージノード	ストレージノード	ストレージノード間の内部トラフィック。

ポート	**tcp** または **udp** です	開始	宛先	詳細
1501	TCP	すべてのノード	ADC を採用するストレージノード	レポート、監査、および設定の内部トラフィック。
1502	TCP	すべてのノード	ストレージノード	S3 関連の内部トラフィック。
1504	TCP	すべてのノード	管理ノード	NMS サービスのレポートおよび設定の内部トラフィック。
1505	TCP	すべてのノード	管理ノード	AMS サービスの内部トラフィック。
1506	TCP	すべてのノード	すべてのノード	サーバステータスの内部トラフィック。
1507	TCP	すべてのノード	ゲートウェイノード	ロードバランサの内部トラフィック。
1508	TCP	すべてのノード	プライマリ管理ノード	設定管理の内部トラフィック。
1511	TCP	すべてのノード	ストレージノード	メタデータの内部トラフィック。
5353	UDP	すべてのノード	すべてのノード	インストール、拡張、リカバリ時のフルグリッド IP の変更やプライマリ管理ノードの検出に使用されるマルチキャスト DNS (mDNS) サービスを提供します。 注: このポートの構成はオプションです。
7001	TCP	ストレージノード	ストレージノード	Cassandra TLS ノード間クラスタ通信。
7443	TCP	すべてのノード	プライマリ管理ノードと非プライマリ管理ノード	インストール、拡張、リカバリ、その他のメンテナンス手順、およびエラーレポート用の内部トラフィック。

ポート	**tcp** または **udp** です	開始	宛先	詳細
8011	TCP	すべてのノード	プライマリ管理ノードと非プライマリ管理ノード	インストール、拡張、リカバリ、およびその他のメンテナンス手順用の内部トラフィック。
8443	TCP	プライマリ管理ノード	アプライアンスノード	メンテナンスモードの手順 に関連する内部トラフィック。
9042	TCP	ストレージノード	ストレージノード	Cassandra クライアントポート。
9999	TCP	すべてのノード	すべてのノード	複数のサービスの内部トラフィック。メンテナンス手順、指標、およびネットワークの更新が含まれます。
10226	TCP	ストレージノード	プライマリ管理ノード	StorageGRIDアプライアンスで、EシリーズSANtricity System Managerからプライマリ管理ノードにAutoSupportパッケージを転送するために使用されます。
10342	TCP	すべてのノード	プライマリ管理ノードと非プライマリ管理ノード	インストール、拡張、リカバリ、およびその他のメンテナンス手順用の内部トラフィック。
18000	TCP	すべてのノード	ADC を採用するストレージノード	アカウントサービスの内部トラフィック。
18001	TCP	すべてのノード	ADC を採用するストレージノード	アイデンティティフェデレーションの内部トラフィック。
18002	TCP	すべてのノード	ストレージノード	オブジェクトプロトコルに関連する内部 API トラフィック。
18003	TCP	すべてのノード	ADC を採用するストレージノード	プラットフォームサービスの内部トラフィック。
18017	TCP	管理 / ストレージノード	ストレージノード	クラウドストレージプールの Data Mover サービスの内部トラフィック。

ポート	**tcp** または **udp** です	開始	宛先	詳細
18019	TCP	すべてのノード	すべてのノード	消失訂正符号化とレプリケーションのためのチャンクサービス内部トラフィック
18082	TCP	管理 / ストレージノード	ストレージノード	S3 関連の内部トラフィック。
18086	TCP	すべてのノード	ストレージノード	LDRサービスに関連する内部トラフィック。
18200	TCP	管理 / ストレージノード	ストレージノード	クライアント要求に関する追加の統計。
19000	TCP	管理 / ストレージノード	ADC を採用するストレージノード	Keystone サービスの内部トラフィック。

関連情報

"外部との通信"

StorageGRIDの外部通信

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

ポートへのアクセスを制限します

エンタープライズネットワークポリシーによっていずれかのポートへのアクセスが制限されている場合は、次のいずれかを実行できます。

- ユーザ定義ポートでのアクセスを許可する場合に使用し"ロードバランサエンドポイント"ます。
- ノード導入時にポートを再マッピングします。ただし、ロードバランサエンドポイントを再マッピングしないでください。StorageGRIDノードのポートの再マッピングに関する情報を参照してください。

> ポート再マッピングのサポートは非推奨であり、将来のリリースでは削除される予定です。再マップされたポートを削除するには、"StorageGRIDアプライアンスのポート再マップを削除します"または"ベアメタルホストでのポートの再マッピングを削除します"。

- "Red Hat Enterprise LinuxでのStorageGRIDのポート再マッピングキー"
- "VMwareテノStorageGRIDノホオトノサイマツヒンク"
- "オプション：アプライアンスのネットワークポートの再マッピング"

次の表に、ノードに着信するトラフィックに使用されるポートを示します。

このリストには、として設定されている可能性のあるポートは含まれませ"ロードバランサエンドポイント"ん。

ポート	**tcp** または **udp** です	プロトコル	開始	宛先	詳細
22	TCP	SSH	サービスラップトップ	すべてのノード	コンソール ステップを含む手順では、SSH またはコンソール アクセスが必要です。オプションで、ポート 22 の代わりにポート 2022 を使用することもできます。 注: このポートは、特定のメンテナンス操作のために SSH アクセスを有効にする必要がある場合にのみ必要です。
25	TCP	SMTP	管理ノード	E メールサーバ	アラートおよび E メールベースの AutoSupport に使用されます。Email Servers ページを使用して、デフォルトのポート設定である 25 を上書きできます。
53	TCP / UDP	DNS	すべてのノード	DNSサーバ	DNSに使用されます。
67	UDP	DHCP	すべてのノード	DHCPサービス	必要に応じて、 DHCP ベースのネットワーク設定のサポートに使用します。dhclient サービスは、静的に設定されたグリッドに対しては実行されません。
68	UDP	DHCP	DHCPサービス	すべてのノード	必要に応じて、 DHCP ベースのネットワーク設定のサポートに使用します。dhclient サービスは、静的 IP アドレスを使用するグリッドに対しては実行されません。
80	TCP	HTTP	ブラウザ	管理ノード	ポート 80 は、管理ノードのユーザインターフェイス用のポート 443 にリダイレクトされます。
80	TCP	HTTP	ブラウザ	アプライアンス	ポート 80 は、 StorageGRID アプライアンスインストーラ用のポート 8443 にリダイレクトされます。

ポート	**tcp** または **udp** です	プロトコル	開始	宛先	詳細
80	TCP	HTTP	ADC を採用するストレージノード	AWS	AWSまたはHTTPを使用するその他の外部サービスに送信されるプラットフォームサービスメッセージに使用されます。エンドポイントの作成時に、テナントがデフォルトの HTTP ポート設定である 80 を上書きできる。
80	TCP	HTTP	ストレージノード	AWS	HTTPを使用するAWSターゲットに送信されるCloud Storage Pools要求。クラウドストレージプールの設定時に、グリッド管理者がデフォルトの HTTP ポート設定である 80 を上書きできます。
123	UDP	NTP	プライマリ NTP ノード	外部 NTP	ネットワークタイムプロトコルサービス。プライマリ NTP ソースとして選択されたノードは、クロックの時間と外部 NTP の時間ソースとの同期も行います。
161	TCP / UDP	SNMP	SNMPクライアント	すべてのノード	SNMP ポーリングに使用します。すべてのノードは基本情報を提供し、管理ノードもアラートデータを提供します。設定時のデフォルトの UDP ポートは 161 です。 • 注：このポートは必須です。 SNMP が設定されている場合にのみノードファイアウォールで開かれます。SNMP を使用する場合は、代替ポートを設定できます。 • 注： StorageGRID での SNMP の使用については、ネットアップの営業担当者にお問い合わせください。
162	TCP / UDP	SNMP 通知	すべてのノード	通知の送信先	アウトバウンド SNMP 通知およびトラップのデフォルトの UDP ポートは 162 です。 • 注：このポートは、 SNMP が有効で通知の送信先が設定されている場合にのみ必要です。SNMP を使用する場合は、代替ポートを設定できます。 • 注： StorageGRID での SNMP の使用については、ネットアップの営業担当者にお問い合わせください。
389	TCP / UDP	LDAP	ADC を採用するストレージノード	Active Directory / LDAP	アイデンティティフェデレーション用の Active Directory または LDAP サーバに接続するために使用します。

ポート	**tcp** または **udp** です	プロトコル	開始	宛先	詳細
443	TCP	HTTPS	ブラウザ	管理ノード	Web ブラウザおよび管理 API クライアントが Grid Manager および Tenant Manager にアクセスするために使用します。 注意: Grid Manager ポート 443 または 8443 を閉じると、ブロックされたポートに現在接続しているすべてのユーザー (自分を含む) は、その IP アドレスが特権アドレス リストに追加されていない限り、Grid Manager にアクセスできなくなります。参照"ファイアウォールコントロールを設定します"特権 IP アドレスを構成します。
443	TCP	HTTPS	管理ノード	Active Directory	シングルサインオン（ SSO ）が有効な場合に、 Active Directory に接続する管理ノードで使用します。
443	TCP	HTTPS	ADC を採用するストレージノード	AWS	AWSまたはHTTPSを使用するその他の外部サービスに送信されるプラットフォームサービスメッセージに使用されます。エンドポイントの作成時に、テナントがデフォルトの HTTP ポート設定である 443 を上書きできる。
443	TCP	HTTPS	ストレージノード	AWS	HTTPSを使用するAWSターゲットに送信されるCloud Storage Pools要求。クラウドストレージプールの設定時に、グリッド管理者がデフォルトの HTTPS ポート設定である 443 を上書きできます。
636	TCP / UDP	LDAP	ADC を採用するストレージノード	Active Directory / LDAP	アイデンティティフェデレーション用の Active Directory または LDAP サーバに接続するために使用します。
5353	UDP	mDNS	すべてのノード	すべてのノード	インストール、拡張、リカバリ時のフルグリッド IP の変更やプライマリ管理ノードの検出に使用されるマルチキャスト DNS (mDNS) サービスを提供します。 注: このポートの構成はオプションです。
5696	TCP	KMIP	アプライアンス	KMS	ノードの暗号化用に設定されたアプライアンスから Key Management Server （ KMS ）へのキー管理 Interoperability Protocol （ KMIP ）の外部トラフィック（ StorageGRID アプライアンスインストーラの KMS 構成のページで別のポートを指定している場合を除く）。

ポート	**tcp** または **udp** です	プロトコル	開始	宛先	詳細
8443	TCP	HTTPS	ブラウザ	管理ノード	オプション。 Web ブラウザおよび管理 API クライアントが Grid Manager にアクセスするために使用します。Grid Manager と Tenant Manager の通信を分離するために使用できます。 注意: Grid Manager ポート 443 または 8443 を閉じると、ブロックされたポートに現在接続しているすべてのユーザー (自分を含む) は、その IP アドレスが特権アドレス リストに追加されていない限り、Grid Manager にアクセスできなくなります。参照"ファイアウォールコントロールを設定します"特権 IP アドレスを構成します。
8443	TCP	HTTPS	ブラウザ	アプライアンス	Web ブラウザおよび管理 API クライアントがStorageGRIDアプライアンス インストーラにアクセスするために使用します。 注: ポート 443 は、 StorageGRIDアプライアンス インストーラのポート 8443 にリダイレクトされます。
9022	TCP	SSH	サービスラップトップ	アプライアンス	サポートとトラブルシューティングのために、構成前モードでの StorageGRID アプライアンスへのアクセスを許可します。このポートは、グリッドノード間で、または通常運用時にアクセス可能である必要はありません。
9091	TCP	HTTPS	外部の Grafana サービス	管理ノード	外部の Grafana サービスが StorageGRID Prometheus サービスへのセキュアなアクセスに使用します。 • 注：このポートは、証明書ベースの Prometheus アクセスが有効になっている場合にのみ必要です。
9092	TCP	カフカ	ADC を採用するストレージノード	Kafkaクラスタ	Kafkaクラスタに送信されるプラットフォームサービスメッセージに使用されます。テナントは、エンドポイントの作成時にデフォルトのKafkaポート設定（9092）を上書きできます。
9443	TCP	HTTPS	ブラウザ	管理ノード	オプション。 Web ブラウザおよび管理 API クライアントがテナント マネージャにアクセスするために使用します。Grid Manager と Tenant Manager の通信を分離するために使用できます。

ポート	**tcp** または **udp** です	プロトコル	開始	宛先	詳細
18082	TCP	HTTPS	S3 クライアント	ストレージノード	ストレージノードへのS3クライアントトラフィックの直接転送（HTTPS）。
18084	TCP	HTTP	S3 クライアント	ストレージノード	ストレージノードへのS3クライアントトラフィックの直接転送（HTTP）。
23000-23999	TCP	HTTPS	グリッド間レプリケーションのソースグリッド上のすべてのノード	グリッド間レプリケーション用のデスティネーショングリッド上の管理ノードとゲートウェイノード	この範囲のポートはグリッドフェデレーション接続用に予約されています。特定の接続の両方のグリッドが同じポートを使用します。

StorageGRID のクイックスタート

StorageGRID システムを設定して使用するには、次の手順を実行します。



データの学習、計画、収集

オプションについて理解し、新しいStorageGRID システムを計画するには、ネットアップの営業担当者にお問い合わせください。次のタイプの質問を考えてみましょう。

- 最初から将来にわたって格納するオブジェクトデータの量はどれくらいになると予想されますか？
- サイトはいくつ必要ですか？
- 各サイトに必要なノードの数と種類
- どのStorageGRID ネットワークを使用しますか。
- グリッドを使用してオブジェクトを格納するのは誰ですか？どのアプリケーションを使用するか
- セキュリティやストレージに関する特別な要件はありますか？
- 法的要件や規制要件に準拠する必要がありますか？

必要に応じて、ネットアッププロフェッショナルサービスのコンサルタントと協力してNetApp ConfigBuilder ツールにアクセスし、新しいシステムのインストールと導入の際に使用する設定ワークブックを完成させます。また、このツールを使用して、任意のStorageGRID アプライアンスの設定を自動化することもできます。を参照してください "アプライアンスのインストールと設定を自動化"

"StorageGRID の詳細をご覧ください"と"ネットワークのガイドライン"を確認してください。

2 ノードのインストール

StorageGRID システムは、ハードウェアベースとソフトウェアベースの個 々 のノードで構成されます。最初に各アプライアンスノードのハードウェアを設置し、LinuxまたはVMwareホストをそれぞれ設定します。

インストールを完了するには、各アプライアンスまたはソフトウェアホストにStorageGRID ソフトウェアをインストールし、ノードをグリッドに接続します。この手順では、サイト名とノード名、サブネットの詳細、およびNTPサーバとDNSサーバのIPアドレスを指定します。

詳細はこちら：

- "アプライアンスハードウェアを設置"
- "ソフトウェアベースのノードにStorageGRIDをインストールする"

3 サインインしてシステムの健全性を確認

グリッドのインストールが完了したら、グリッド マネージャーにサインインできます。そこから、新しいシステムの全体的な健全性を確認したり、 AutoSupportとアラートメールを有効にしたり、S3 エンドポイントのドメイン名を設定したりできます。

詳細はこちら：

- "Grid Manager にサインインします"
- "システムヘルスを監視する"
- "AutoSupportの設定"
- "アラート用の E メール通知を設定します"
- "S3エンドポイントのドメイン名を設定"

4 設定と管理

新しいStorageGRID システムで実行する必要がある設定タスクは、グリッドの使用方法によって異なります。少なくとも、システムアクセスのセットアップ、FabricPool ウィザードとS3ウィザードの使用、ストレージとセキュリティのさまざまな設定の管理を行う必要があります。

詳細はこちら：

- "StorageGRID アクセスを制御します"
- "S3セットアップウィザードを使用する"
- "FabricPool セットアップウィザードを使用する"
- "セキュリティを管理します"
- "システムの保護対策"

5 **ILM**のセットアップ

StorageGRID システム内のすべてのオブジェクトの配置と期間を制御するには、1つ以上のILMルールで構成

される情報ライフサイクル管理（ILM）ポリシーを設定します。ILMルールは、オブジェクトデータのコピーを作成および分散する方法と、それらのコピーを一定の期間にわたって管理する方法をStorageGRID に指示します。

詳細はこちら："ILM を使用してオブジェクトを管理する"

6 StorageGRIDを使用

初期設定が完了すると、StorageGRIDテナントアカウントはS3クライアントアプリケーションを使用してオブジェクトの取り込み、読み出し、削除を行うことができます。

詳細はこちら：

- "テナントアカウントを使用する"
- "S3 REST APIを使用する"

7 監視とトラブルシューティング

システムが起動したら、定期的にアクティビティを監視し、アラートをトラブルシューティングして解決する必要があります。外部syslogサーバの設定、SNMPによる監視、追加データの収集などが必要になる場合もあります。

詳細はこちら：

- "StorageGRID を監視します"
- "StorageGRID のトラブルシューティングを行う"

8 拡張、保守、リカバリ

ノードやサイトを追加して、システムの容量や機能を拡張することができます。また、さまざまなメンテナンス手順を実行して、障害からリカバリしたり、StorageGRID システムを最新の状態に維持して効率的に実行したりすることもできます。

詳細はこちら：

- "グリッドを展開する"
- "グリッドのメンテナンス"
- "ノードをリカバリ"

StorageGRIDのインストール、アップグレード、ホットフィックス

StorageGRIDノードをインストールする

StorageGRIDアプライアンスハードウェアについて

`https://docs.netapp.com/us-en/storagegrid-appliances/index.html["StorageGRID アプライアンスのドキュメント"^]`
にアクセスして、StorageGRIDストレージおよびサービスアプライアンスのインストール、設定、およびメンテナンスの方法を確認してください。

ソフトウェアベースのノードをインストール

ソフトウェアベースのノードに**StorageGRID**をインストールするためのクイックスタート

Linux または VMware StorageGRIDノードをインストールするには、次の大まかな手順に従います。

> 「Linux」は、RHEL、Ubuntu、または Debian のデプロイメントを指します。サポートされているバージョンのリストについては、 "NetApp Interoperability Matrix Tool（IMT）" 。

1 準備

- 詳細はこちらをご覧ください "StorageGRID のアーキテクチャとネットワークトポロジ"。
- の詳細については、を"StorageGRID ネットワーク"参照してください。
- を集めて準備します"必要な情報と資料"。
- (VMwareのみ) インストールと構成"VMware vSphereハイパーバイザー、vCenter、およびESXホスト"。
- 必要なを準備します"CPUおよびRAM"。
- を提供し"ストレージとパフォーマンスの要件"ます。
- (Linux のみ)"Linuxサーバの準備" StorageGRIDノードをホストします。

2 導入

グリッドノードを導入する。導入したグリッドノードは、 StorageGRID システムの一部として作成され、 1 つ以上のネットワークに接続されます。

- （Linuxのみ）手順1で準備したホストにソフトウェアベースのグリッドノードを展開するには、Linuxコマンドラインを使用して"ノード構成ファイル"。
- (VMwareのみ) VMware vSphere Web Client、.vmdkファイル、および.ovfファイルテンプレートのセットを使用して、"ソフトウェアベースのノードを仮想マシン（VM）として導入"手順 1 で準備したサーバー上

で。

- StorageGRIDアプライアンスノードを導入するには、に従って "ハードウェア設置のクイックスタート"ください。

3 構成

すべてのノードを導入したら、Grid Managerを使用してに"グリッドを設定し、インストールを完了する"移動します。

インストールを自動化します

「Linux」は、RHEL、Ubuntu、または Debian のデプロイメントを指します。サポートされているバージョンのリストについては、 "NetApp Interoperability Matrix Tool（IMT）" 。

Linux

時間を節約し、整合性を確保するために、StorageGRIDホストサービスのインストールとグリッドノードの設定を自動化できます。

- Ansible、Puppet、Chefなどの標準的なオーケストレーションフレームワークを使用して自動化：
  - Linuxのインストール
  - ネットワークとストレージの構成
  - コンテナエンジンとStorageGRIDホストサービスのインストール
  - 仮想グリッドノードの導入

  見る"StorageGRID ホストサービスのインストールと設定を自動化する" 。
- グリッドノードを展開した後、"StorageGRIDシステムの設定を自動化"インストール アーカイブに提供されている Python 構成スクリプトを使用します。
- "アプライアンスグリッドノードのインストールと設定を自動化する"
- StorageGRID環境の高度な開発者は、を使用してグリッドノードのインストールを自動化します"インストールREST API"。

VMware

時間を節約し、整合性を確保するために、グリッドノードの導入と設定、およびStorageGRIDシステムの設定を自動化できます。

- "VMware vSphereを使用してグリッドノードの導入を自動化"です。
- インストールアーカイブに付属のPython設定スクリプトを使用して、グリッドノードを導入したあとに"StorageGRIDシステムの設定を自動化"実行します。
- "アプライアンスグリッドノードのインストールと設定を自動化する"
- StorageGRID環境の高度な開発者は、を使用してグリッドノードのインストールを自動化します"インストールREST API"。

StorageGRIDに必要な情報と資料

StorageGRIDをインストールする前に、必要な情報や資料を収集して準備します。

必要な情報

ネットワーク計画

各StorageGRIDノードに接続するネットワーク。StorageGRIDは、トラフィックの分離、セキュリティ、および管理上の利便性のために、複数のネットワークをサポートしています。

"ネットワークのガイドライン"を参照してください。

ネットワーク情報

各グリッドノードに割り当てるIPアドレス、およびDNSサーバとNTPサーバのIPアドレス。

グリッドノードヨウノサーバ

導入予定の StorageGRID ノードの数とタイプに応じて、それらをサポートできる十分なリソースを備えた一連のサーバ（物理、仮想、またはその両方）を特定します。

> StorageGRID 環境でStorageGRID アプライアンス（ハードウェア）ストレージノードを使用しない場合は、バッテリバックアップ式書き込みキャッシュ（BBWC）を備えたハードウェアRAIDストレージを使用する必要があります。StorageGRID は、Virtual Storage Area Network（VSAN;仮想ストレージエリアネットワーク）、ソフトウェアRAID、またはRAID保護なしの使用をサポートしていません。

ノードの移行（必要な場合、**Ubuntu** と **Debian** のみ）

"ノード移行の要件"物理ホストでサービスを中断せずに定期的なメンテナンスを実行する場合は、を参照してください。

関連情報

"NetApp Interoperability Matrix Tool"

前提要件

NetApp StorageGRID ライセンス

デジタル署名された有効なNetAppライセンスが必要です。

> StorageGRIDのインストールアーカイブには、グリッドのテストとコンセプトの実証に使用できる非本番環境のライセンスが含まれています。

StorageGRID インストールアーカイブ

"StorageGRIDインストールアーカイブをダウンロードしてファイルを展開する"です。

サービスラップトップ

StorageGRID システムは、サービスラップトップを介してインストールされます。

サービスラップトップには次のものが必要です。

- ネットワークポート
- SSH クライアント（ PuTTY など）
- "サポートされている Web ブラウザ"

StorageGRID のドキュメント

- "リリースノート"。NetAppアカウントでサインインするか、アカウントを作成してリリースノートにアクセスする必要があります。
- "StorageGRID の管理手順"

StorageGRID インストールファイルをダウンロードして展開します

StorageGRID インストールアーカイブをダウンロードし、必要なファイルを展開する必要があります。必要に応じて、インストールパッケージ内のファイルを手動で検証できます。

手順

1. に進みます "ネットアップの StorageGRID ダウンロードページ"。
2. 最新のリリースをダウンロードするボタンを選択するか、ドロップダウンメニューから別のバージョンを選択して、「 * Go * 」を選択します。
3. ネットアップアカウントのユーザ名とパスワードを使用してサインインします。
4. Caution/MustRead文が表示された場合は'その文を読み'チェックボックスをオンにします

   StorageGRID リリースのインストール後に、必要な修正プログラムを適用する必要があります。詳細については、"リカバリとメンテナンスの手順の Hotfix 手順"

5. [End User License Agreement]を読み、チェックボックスをオンにして、*[Accept & Continue]*を選択します。
6. * StorageGRIDのインストール *列で、ソフトウェアベースのノード タイプ (RHEL、Ubuntu、Debian、または VMware) に応じた .tgz または .zip インストール アーカイブを選択します。

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

7. インストールアーカイブを保存します。
8. Linux ノードではコード署名の検証は手動で行います。オプションで、インストール アーカイブを検証する必要がある場合:

   a. StorageGRIDコード署名検証パッケージをダウンロードします。このパッケージのファイル名はの形式を使用し `StorageGRID_<version-number>_Code_Signature_Verification_Package.tar.gz`ます。`<version-number>`はStorageGRIDソフトウェアのバージョンです。

   b. 手順に従ってください"インストールファイルを手動で検証する"。
9. インストールアーカイブからファイルを展開します。
10. 必要なファイルを選択します。

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

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

RHEL

パスとファイル名	製品説明
	StorageGRID ダウンロードファイルに含まれているすべてのファイルについて説明するテキストファイル。
	製品サポートのない無償ライセンス。
	RHELホストにStorageGRIDノードイメージをインストールするためのRPMパッケージ。
	RHELホストにStorageGRIDホストサービスをインストールするためのRPMパッケージ。
導入スクリプトツール	製品説明
	StorageGRID システムの設定を自動化するための Python スクリプト。
	StorageGRID アプライアンスの設定を自動化するための Python スクリプト。
	スクリプトで使用する構成ファイルの例 `configure-storagegrid.py`。
	シングルサインオンが有効な場合にグリッド管理 API にサインインするために使用できる Python スクリプトの例。このスクリプトは、Pingフェデレーション統合にも使用できます。
	スクリプトで使用する空の構成ファイル `configure-storagegrid.py`。
	StorageGRIDコンテナ導入用のRHELホストを設定するためのサンプルのAnsibleのロールとプレイブック。必要に応じて、ロールまたはプレイブックをカスタマイズできます。
	Active DirectoryまたはPingフェデレーションを使用してシングルサインオン（SSO）が有効になっている場合にグリッド管理APIにサインインするために使用できるPythonスクリプトの例。

パスとファイル名	製品説明
	関連するPythonスクリプトによって呼び出され、AzureとのSSO対話を実行するヘルパースクリプト `storagegrid-ssoauth-azure.py`。
	StorageGRID の API スキーマ 注：アップグレードを実行する前に、これらのスキーマを使用して、アップグレード互換性テスト用の非本番環境のStorageGRID 環境がない場合、StorageGRID 管理APIを使用するように記述したコードが新しいStorageGRID リリースと互換性があることを確認できます。

Ubuntu または **Debian**

パスとファイル名	製品説明
	StorageGRID ダウンロードファイルに含まれているすべてのファイルについて説明するテキストファイル。
	テスト環境やコンセプトの実証環境に使用できる、非本番環境のNetAppライセンスファイル。
	Ubuntu ホストまたは Debian ホストに StorageGRID ノードイメージをインストールするための DEB パッケージ。
	ファイルのMD5チェックサム `/debs/storagegrid-webscale-images-version-SHA.deb`。
	Ubuntu ホストまたは Debian ホストに StorageGRID ホストサービスをインストールするための DEB パッケージ。
導入スクリプトツール	製品説明
	StorageGRID システムの設定を自動化するための Python スクリプト。
	StorageGRID アプライアンスの設定を自動化するための Python スクリプト。

パスとファイル名	製品説明
	シングルサインオンが有効な場合にグリッド管理 API にサインインするために使用できる Python スクリプトの例。このスクリプトは、Pingフェデレーション統合にも使用できます。
	スクリプトで使用する構成ファイルの例 `configure-storagegrid.py`。
	スクリプトで使用する空の構成ファイル `configure-storagegrid.py`。
	StorageGRID コンテナ導入用の Ubuntu ホストまたは Debian ホストを設定するためのサンプルの Ansible のロールとプレイブック。必要に応じて、ロールまたはプレイブックをカスタマイズできます。
	Active DirectoryまたはPingフェデレーションを使用してシングルサインオン（SSO）が有効になっている場合にグリッド管理APIにサインインするために使用できるPythonスクリプトの例。
	関連するPythonスクリプトによって呼び出され、AzureとのSSO対話を実行するヘルパースクリプト `storagegrid-ssoauth-azure.py`。
	StorageGRID の API スキーマ 注：アップグレードを実行する前に、これらのスキーマを使用して、アップグレード互換性テスト用の非本番環境のStorageGRID 環境がない場合、StorageGRID 管理APIを使用するように記述したコードが新しいStorageGRID リリースと互換性があることを確認できます。

VMware

パスとファイル名	製品説明
	StorageGRID ダウンロードファイルに含まれているすべてのファイルについて説明するテキストファイル。
	製品サポートのない無償ライセンス。

パスとファイル名	製品説明
	グリッドノード仮想マシンを作成するためのテンプレートとして使用される仮想マシンディスクファイル。
	(.mf`プライマリ管理ノードを導入するためのOpen Virtualization Formatテンプレートファイル）(.ovf`とマニフェストファイル
	テンプレートファイル(.ovf）とマニフェストファイル(.mf）。非プライマリ管理ノードを導入するためのものです。
	テンプレートファイル(.ovf）とマニフェストファイル(.mf）を使用してゲートウェイノードを導入します。
	(.mf`仮想マシンベースのストレージノードを導入するためのテンプレートファイル(.ovf`とマニフェストファイル）
導入スクリプトツール	製品説明
	仮想グリッドノードの導入を自動化するためのBash シェルスクリプト。
	スクリプトで使用する構成ファイルの例 deploy-vsphere-ovftool.sh。
	StorageGRID システムの設定を自動化するためのPython スクリプト。
	StorageGRID アプライアンスの設定を自動化するための Python スクリプト。
	シングルサインオン（SSO）が有効な場合にグリッド管理APIにサインインするために使用できるPythonスクリプトの例。このスクリプトは、Pingフェデレーション統合にも使用できます。
	スクリプトで使用する構成ファイルの例 configure-storagegrid.py。
	スクリプトで使用する空の構成ファイル configure-storagegrid.py。

パスとファイル名	製品説明
	Active DirectoryまたはPingフェデレーションを使用してシングルサインオン（SSO）が有効になっている場合にグリッド管理APIにサインインするために使用できるPythonスクリプトの例。
	関連するPythonスクリプトによって呼び出され、AzureとのSSO対話を実行するヘルパースクリプト `storagegrid-ssoauth-azure.py`。
	StorageGRID の API スキーマ 注：アップグレードを実行する前に、これらのスキーマを使用して、アップグレード互換性テスト用の非本番環境のStorageGRID 環境がない場合、StorageGRID 管理APIを使用するように記述したコードが新しいStorageGRID リリースと互換性があることを確認できます。

StorageGRIDインストールファイルを確認する

必要に応じて、StorageGRIDインストールアーカイブ内のファイルを手動で検証できます。

開始する前に

あなたが持っている"検証パッケージをダウンロードしました"から "ネットアップの StorageGRID ダウンロードページ"。

手順

1. 検証パッケージからアーティファクトを抽出します。

   ```
   tar -xf StorageGRID_12.1.0_Code_Signature_Verification_Package.tar.gz
   ```

2. これらのアーチファクトが抽出されたことを確認します。
   - リーフ証明書： `Leaf-Cert.pem`
   - 証明書チェーン： `CA-Int-Cert.pem`
   - タイムスタンプ応答チェーン： `TS-Cert.pem`
   - チェックサムファイル： `sha256sum`
   - チェックサム署名： `sha256sum.sig`
   - タイムスタンプ応答ファイル： `sha256sum.sig.tsr`
3. チェーンを使用して、リーフ証明書が有効であることを確認します。

   例： `openssl verify -CAfile CA-Int-Cert.pem Leaf-Cert.pem`

予想される出力： `Leaf-Cert.pem: OK`

4. リーフ証明書の期限が切れたためにSTEP_2_FAILEDが発生した場合は、ファイルを使用して `tsr`確認します。

   例： `openssl ts -CAfile CA-Int-Cert.pem -untrusted TS-Cert.pem -verify -data sha256sum.sig -in sha256sum.sig.tsr`

   予想される出力には： `Verification: OK`

5. リーフ証明書から公開鍵ファイルを作成します。

   例： `openssl x509 -pubkey -noout -in Leaf-Cert.pem > Leaf-Cert.pub`

   予想される出力：*NONE*

6. 公開鍵を使用してファイルを `sha256sum.sig`検証し `sha256sum`ます。

   例： `openssl dgst -sha256 -verify Leaf-Cert.pub -signature sha256sum.sig sha256sum`

   予想される出力： `Verified OK`

7. 新しく作成したチェックサムと比較してファイルの内容を確認し `sha256sum`ます。

   例： `sha256sum -c sha256sum`

   予期される出力:+ `<filename>: OK`
   `<filename>`は、ダウンロードしたアーカイブファイルの名前です。

8. "残りの手順を完了する"インストール アーカイブから適切なファイルを抽出して選択します。

StorageGRIDのソフトウェア要件

仮想マシンを使用して、あらゆるタイプのStorageGRIDノードをホストできます。グリッドノードごとに仮想マシンが1つ必要です。

RHEL

RHEL にStorageGRIDをインストールするには、サードパーティのソフトウェア パッケージをいくつかインストールする必要があります。サポートされている一部の Linux ディストリビューションには、これらのパッケージがデフォルトで含まれていません。 StorageGRIDインストールがテストされるソフトウェア パッケージのバージョンには、このページに記載されているものが含まれます。

これらのパッケージのいずれかを必要とするLinuxディストリビューションおよびコンテナランタイムインストールオプションを選択し、それらがLinuxディストリビューションによって自動的にインストールされない場合は、プロバイダまたはLinuxディストリビューションのサポートベンダーから入手可能な場合は、ここに記載されているいずれかのバージョンをインストールします。それ以外の場合は、ベンダーが提供しているデフォルトのパッケージバージョンを使用します。

すべてのインストールオプションには、PodmanまたはDockerのいずれかが必要です。両方のパッケージをインストールしないでください。インストールオプションに必要なパッケージのみをインストールします。

> ソフトウェアのみの環境のコンテナエンジンとしてのDockerのサポートは廃止されました。Dockerは、今後のリリースで別のコンテナエンジンに置き換えられる予定です。

テスト済みの**Python**バージョン

- 3.5.2-2
- 3.6.8-2
- 3.6.8-38
- 3.6.9-1
- 3.7.3-1
- 3.8.10-0
- 3.9.2-1
- 3.9.10-2
- 3.9.16-1
- 3.10.6-1
- 3.11.2-6

テスト済みの**Podman**バージョン

- 3.2.3-0
- 3.4.4 + DS1
- 4.1.1-7
- 4.2.0-11
- 4.3.1 + DS1-8 + B1
- 4.4.1-8
- 4.4.1-12

テスト済みの**Docker**バージョン

Dockerのサポートは廃止され、今後のリリースで削除される予定です。

- Docker - CE 20.10.7
- Docker - CE 20.10.20-3
- Docker - CE 23.0.6-1
- Docker - CE 24.0.2-1
- Docker - CE 24.0.4-1
- Docker - CE 24.0.5-1
- Docker - CE 24.0.7-1
- 1.5-2

Ubuntu と **Debian**

UbuntuまたはDebianにStorageGRIDをインストールするには、サードパーティのソフトウェアパッケージをインストールする必要があります。一部のサポートされているLinuxディストリビューションには、デフォルトでこれらのパッケージが含まれていません。StorageGRIDのインストールがテストされているソフトウェアパッケージのバージョンには、このページに記載されているバージョンも含まれます。

これらのパッケージのいずれかを必要とするLinuxディストリビューションおよびコンテナランタイムインストールオプションを選択し、それらがLinuxディストリビューションによって自動的にインストールされない場合は、プロバイダまたはLinuxディストリビューションのサポートベンダーから入手可能な場合は、ここに記載されているいずれかのバージョンをインストールします。それ以外の場合は、ベンダーが提供しているデフォルトのパッケージバージョンを使用します。

すべてのインストールオプションには、PodmanまたはDockerのいずれかが必要です。両方のパッケージをインストールしないでください。インストールオプションに必要なパッケージのみをインストールします。

ソフトウェアのみの環境のコンテナエンジンとしてのDockerのサポートは廃止されました。Dockerは、今後のリリースで別のコンテナエンジンに置き換えられる予定です。

テスト済みの**Python**バージョン

- 3.5.2-2
- 3.6.8-2
- 3.6.8-38
- 3.6.9-1
- 3.7.3-1
- 3.8.10-0
- 3.9.2-1
- 3.9.10-2
- 3.9.16-1
- 3.10.6-1
- 3.11.2-6

テスト済みの**Podman**バージョン

- 3.2.3-0
- 3.4.4 + DS1
- 4.1.1-7
- 4.2.0-11
- 4.3.1 + DS1-8 + B1
- 4.4.1-8
- 4.4.1-12

テスト済みの**Docker**バージョン

Dockerのサポートは廃止され、今後のリリースで削除される予定です。

- Docker - CE 20.10.7
- Docker - CE 20.10.20-3
- Docker - CE 23.0.6-1
- Docker - CE 24.0.2-1
- Docker - CE 24.0.4-1
- Docker - CE 24.0.5-1
- Docker - CE 24.0.7-1
- 1.5-2

VMware

VMware vSphere ハイパーバイザー

準備が整った物理サーバに VMware vSphere ハイパーバイザーをインストールする必要があります。VMware ソフトウェアをインストールする前に、ハードウェアが正しく設定されている必要があります（ファームウェアバージョンと BIOS 設定を含む）。

- インストールする StorageGRID システムのネットワークをサポートできるように、ハイパーバイザーのネットワークを設定します。

  "ネットワークのガイドライン"

- データストアが、グリッドノードをホストするために必要な仮想マシンと仮想ディスクに十分な大きさであることを確認します。
- 複数のデータストアを作成する場合は、仮想マシン作成時に各グリッドノードに使用するデータストアを簡単に識別できるよう、各データストアに名前を付けます。

ESXホストの構成要件

各 ESX ホストでネットワークタイムプロトコル（ NTP ）を適切に設定する必要があります。ホストの時刻が正しくないと、データ損失などのマイナスの影響が生じる可能性があります。

VMware 構成要件

StorageGRIDノードを導入する前に、VMware vSphereとvCenterをインストールして設定する必要があります。

サポートされるVMware vSphere HypervisorおよびVMware vCenter Serverソフトウェアのバージョンについては、を参照してください "NetApp Interoperability Matrix Tool"。

これらの VMware 製品をインストールするために必要な手順については、 VMware のドキュメントを参照してください。

StorageGRIDのCPUとRAMの要件

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

各 StorageGRID ノードに必要な最小リソースは次のとおりです。

- CPU コア：ノードあたり 8 個
- RAM：使用可能なRAMの合計容量と、システムで実行されているStorageGRID以外のソフトウェアの容量によって異なります。
  - 通常、ノードあたり24GB以上、システムRAMの合計より2~16GB少ない
  - 複数のテナントがそれぞれ最大5,000個のバケットを持つ場合、ノードあたり少なくとも64 GB

> StorageGRID システムは、S3 テナントアカウントごとに最大 20,000 個のバケットをサポートします。

ソフトウェアベースのメタデータのみのノードリソースは、既存のストレージノードリソースと一致している必要があります。例：

- 既存のStorageGRIDサイトでSG6000またはSG6100アプライアンスを使用している場合は、ソフトウェアベースのメタデータのみのノードが次の最小要件を満たしている必要があります。
  - 128GBのRAM
  - 8コアCPU
  - 8TB SSDまたはCassandraデータベース用同等のストレージ（rangedb/0）
- 既存のStorageGRIDサイトが 24 GB RAM、8 コア CPU、3 TB または 4 TB のメタデータ ストレージを備えた仮想ストレージ ノードを使用している場合、ソフトウェア ベースのメタデータ専用ノードでは同様のリソース (24 GB RAM、8 コア CPU、4 TB のメタデータ ストレージ (rangedb/0)) を使用する必要があります。

新しいStorageGRIDサイトを追加するときは、新しいサイトの総メタデータ容量が少なくとも既存のStorageGRIDサイトと一致し、新しいサイトのリソースが既存のStorageGRIDサイトのストレージノードと一致している必要があります。

> 「Linux」は、RHEL、Ubuntu、または Debian のデプロイメントを指します。サポートされているバージョンのリストについては、 "NetApp Interoperability Matrix Tool（IMT）" 。

Linux

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

VMware

VMwareでは、仮想マシンごとに1ノードがサポートされます。StorageGRIDノードが使用可能な物理RAMを超えていないことを確認します。各仮想マシンは、StorageGRIDを実行する専用にする必要があります。

CPUとメモリの使用状況を定期的に監視し、これらのリソースが引き続き作業負荷に対応できることを確認してください。例えば、仮想ストレージノードのRAMとCPUの割り当てを2倍にすると、StorageGRIDアプライアンスノードに提供されるリソースと同様のリソースが提供されます。さらに、ノードあたりのメタデータ量が500 GBを超える場合は、ノードあたりのRAMを48 GB以上に増やすことを検討してください。オブジェクトメタデータストレージの管理、メタデータ予約領域設定の増加、CPUとメモリ使用量の監視に関する情報については、"管理"、"監視"、および"アップグレード" StorageGRIDの手順を参照してください。

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

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

(RHEL、Debian、Ubuntu のみ) 実稼働環境では、同じ物理ストレージ ハードウェアまたは仮想ホスト上で複数のストレージ ノードを実行しないでください。単一のStorageGRID展開内の各ストレージ ノードは、独自の分離された障害ドメインに配置する必要があります。単一のハードウェア障害が単一のストレージ ノードにのみ影響するようにすれば、オブジェクト データの耐久性と可用性を最大限に高めることができます。

"ストレージとパフォーマンスの要件"を参照してください。

StorageGRIDのストレージとパフォーマンスの要件

StorageGRID ノードのストレージ要件を理解し、初期構成と将来のストレージ拡張をサポートするのに十分なスペースがあることを確認する必要があります。

ストレージとパフォーマンスの要件は、ソフトウェア ベースのノード実装によって異なります。

「Linux」は、RHEL、Ubuntu、または Debian のデプロイメントを指します。サポートされているバージョンのリストについては、 "NetApp Interoperability Matrix Tool（IMT）" 。

ストレージカテゴリ

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

- コンテナプール — ノードコンテナ用のパフォーマンス層（10K SAS または SSD）ストレージ。StorageGRID ノードをサポートするホストにコンテナエンジンをインストールして構成する際に、コンテナエンジンのストレージドライバに割り当てられます。

- システムデータ — パフォーマンス層（10K SAS または SSD）ストレージは、システムデータとトランザクションログをノードごとに永続的に保存するためのもので、StorageGRID ホストサービスが使用し、個々のノードにマッピングします。
- * オブジェクトデータ * — オブジェクトデータとオブジェクトメタデータの永続的なストレージを実現するパフォーマンス階層（ 10K SAS または SSD ）のストレージと大容量階層（ NL-SAS / SATA ）のストレージ。

すべてのストレージカテゴリにおいて、RAIDでバックアップされたブロックデバイスを使用する必要があります。冗長構成ではないディスク、SSD、またはJBODはサポートされていません。ストレージの種類に関わらず、共有RAIDストレージまたはローカルRAIDストレージを使用できます。StorageGRID でノードを移行するには、システムデータとオブジェクトデータの両方を共有ストレージに保存する必要があります。詳細については、"ノードコンテナの移行要件"を参照してください。

パフォーマンス要件

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

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

NetApp ONTAPストレージを使用するホストの要件

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

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

必要なホストの数

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

> 本番環境への展開においては、単一の物理ホストまたは仮想ホスト上で複数のストレージノードを実行しないでください。各ストレージノード専用のホストにより、障害発生時の隔離されたドメインが確保されます。

管理ノードやゲートウェイノードなど、他の種類のノードを同じホストにデプロイすることも、必要に応じて専用のホストにデプロイすることもできます。

> ディスクスナップショットを使用してグリッドノードを復元することはできません。代わりに、"グリッドノードのリカバリ"各ノードタイプの手順を参照してください。

各ノードのストレージボリュームの数

以下の表は、各ホストに必要なストレージボリューム（LUN）の数と、各LUNに必要な最小サイズを、そのホストに展開されるノードに基づいて示しています。

テスト済みの最大LUNサイズは100TiBです。

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

LUNの用途	ストレージのカテゴリ	LUN数	LUN あたりの最小サイズ
コンテナエンジンのストレージプール	コンテナプール	1	ノードの総数 × 100GB
`/var/local`ボリューム	システムデータ	このホストのノードごとに 1 個	100GB
ストレージノード	オブジェクトデータ	このホストのストレージノードごとに 3 個 注: LinuxソフトウェアベースのストレージノードとvMwareソフトウェアベースのストレージノードは、1～48個のストレージボリュームを持つことができます。少なくとも3つのストレージボリュームを推奨します。	12 TB（4 TB/LUN、最小） テスト済みの最大LUNサイズ：100 TiB。 詳細については、ストレージノードのストレージ要件 を参照してください。
ストレージノード（メタデータのみ）	オブジェクトメタデータ	1	4 TB/LUN（最小） テスト済みの最大LUNサイズ：100 TiB。 詳細については、ストレージノードのストレージ要件 を参照してください。 注：メタデータのみのストレージノードに必要なrangedbは1つだけです。
管理ノードの監査ログ	システムデータ	このホストの管理ノードごとに 1 個	200GB
管理ノードのテーブル	システムデータ	このホストの管理ノードごとに 1 個	200GB

設定されている監査レベル、S3オブジェクトキー名などのユーザー入力のサイズ、および保持する必要のある監査ログデータの量によっては、各管理ノードの監査ログLUNのサイズを増やす必要がある場合があります。一般的に、グリッドはS3操作1回あたり約1 KBの監査データを生成するため、200 GB のLUNは2～3日間、1日あたり7,000万回の操作、または1秒あたり800回の操作をサポートできます。

ホストの最小ストレージスペース

以下の表は、ノードの種類ごとに必要な最小ストレージ容量を示しています。この表を使用すると、ホストにデプロイされているノードに基づいて、各ストレージカテゴリでホストに提供する必要がある最小ストレージ容量を判断できます。

ディスクスナップショットを使用してグリッドノードを復元することはできません。代わりに、"グリッドノードのリカバリ"各ノードタイプの手順を参照してください。

各ノード ホストには、OS 用に 100 GB の LUN が必要です。

ノードのタイプ	コンテナプール	システムデータ	オブジェクトデータ
ストレージノード	100GB	100GB	4,000GB
管理ノード	100GB	500 GB (3 LUN)	_ 該当なし _
ゲートウェイノード	100GB	100GB	_ 該当なし _

例: ホストまたは仮想マシンのストレージ要件の計算

同じホストまたは仮想マシン上に、ストレージノード、管理ノード、ゲートウェイノードの3つのノードをデプロイする計画を立てているとします。ホストには最低9つのストレージボリュームを提供する必要があります。ノードコンテナには最低 300 GB のパフォーマンス層ストレージ、システムデータとトランザクションログには 700 GB のパフォーマンス層ストレージ、オブジェクトデータには 12 TB の容量層ストレージが必要です。

Linuxホストの例

ノードのタイプ	**LUN**の用途	**LUN**数	**LUN**サイズ
ストレージノード	コンテナエンジンのストレージプール	1	300GB （ 100GB/ ノード）
ストレージノード	`/var/local`ボリューム	1	100GB
ストレージノード	オブジェクトデータ	3	12TB （ 4TB / LUN ）
管理ノード	`/var/local`ボリューム	1	100GB
管理ノード	管理ノードの監査ログ	1	200GB
管理ノード	管理ノードのテーブル	1	200GB
ゲートウェイノード	`/var/local`ボリューム	1	100GB
• 合計 *		**9**	• コンテナプール： * 300GB システムデータ**:** 700 GB • オブジェクトデータ： 12 、 000GB

VMware仮想マシンの例

ノードのタイプ	**LUN**の用途	**LUN**数	**LUN**サイズ
ストレージノード	OSボリューム	1	100GB
ストレージノード	オブジェクトデータ	3	12TB （ 4TB / LUN ）
管理ノード	OSボリューム	1	100GB
管理ノード	管理ノードの監査ログ	1	200GB
管理ノード	管理ノードのテーブル	1	200GB
ゲートウェイノード	OSボリューム	1	100GB

ノードのタイプ	LUNの用途	LUN数	LUNサイズ
• 合計 *		8	システムデータ: 700 GB • オブジェクトデータ：12 、 000GB

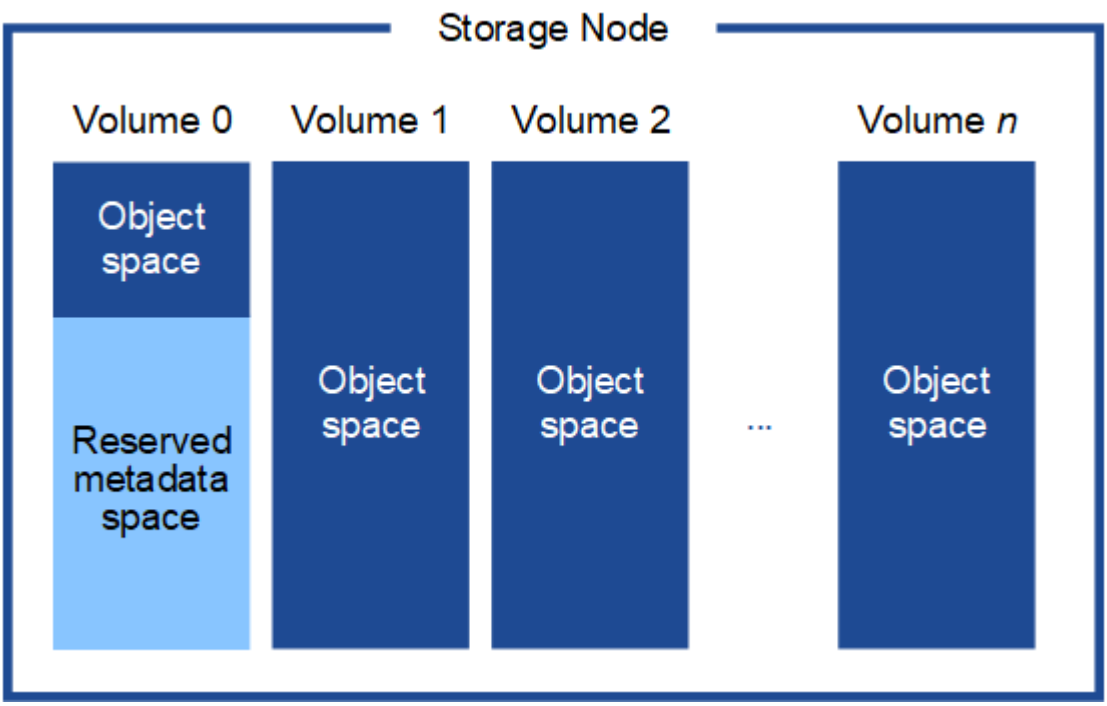
ストレージノードの特定のストレージ要件

LinuxおよびVMwareにおけるストレージノードのストレージ要件は以下のとおりです。

- Linuxソフトウェアベースのストレージノードは、1～48個のストレージボリュームを持つことができます。
- VMwareソフトウェアベースのストレージノードは、1～48個のストレージボリュームを持つことができます。
- 3 つ以上のストレージ ボリュームが推奨されます。
- 各ストレージ ボリュームは 4 TB 以上である必要があります。

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

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



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

メタデータ専用のストレージノードでグリッドをインストールする場合、グリッドにはオブジェクトストレージ用のノードも最低限含まれている必要があります。メタデータ専用ストレージノードの詳細については、"ストレージノードのタイプ"を参照してください。

- 単一サイトのグリッドの場合は、オブジェクトとメタデータ用に少なくとも2つのストレージノードが設定されます。
- マルチサイトグリッドの場合は、サイトごとに少なくとも1つのストレージノードがオブジェクトとメタデータ用に設定されます。

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

- 少なくとも 4TB をボリューム 0 に割り当てる必要があります。

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

  ボリューム0への割り当てが500GB未満の場合（非本番環境での使用のみ）は、ストレージボリュームの容量の10%がメタデータ用にリザーブされます。

- ソフトウェアベースのメタデータのみのノードリソースは、既存のストレージノードリソースと一致している必要があります。例：
  - 既存のStorageGRIDサイトでSG6000またはSG6100アプライアンスを使用している場合は、ソフトウェアベースのメタデータのみのノードが次の最小要件を満たしている必要があります。
    - 128GBのRAM
    - 8コアCPU
    - 8TB SSDまたはCassandraデータベース用同等のストレージ（rangedb/0）
  - 既存のStorageGRIDサイトが 24 GB RAM、8 コア CPU、3 TB または 4 TB のメタデータ ストレージを備えた仮想ストレージ ノードを使用している場合、ソフトウェア ベースのメタデータ専用ノードでは同様のリソース (24 GB RAM、8 コア CPU、4 TB のメタデータ ストレージ (rangedb/0)) を使用する必要があります。

    新しいStorageGRIDサイトを追加するときは、新しいサイトの総メタデータ容量が少なくとも既存のStorageGRIDサイトと一致し、新しいサイトのリソースが既存のStorageGRIDサイトのストレージノードと一致している必要があります。

- 新しいシステム（StorageGRID 11.6以降）をインストールし、各ストレージノードに128GB以上のRAMがある場合は、8TB以上をボリューム0に割り当てます。ボリューム 0 に大きな値を設定すると、各ストレージノードでメタデータに使用できるスペースが増加する可能性があります。
- 同一サイト向けに複数のストレージノードを設定する場合は、可能であればボリューム0にも同じ設定を使用してください。サイトに異なるサイズのストレージノードが含まれている場合、ボリューム0が最小のストレージノードがそのサイトのメタデータ容量を決定します。

詳細については、を参照してください"オブジェクトメタデータストレージを管理する"。

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

「Linux」は、RHEL、Ubuntu、または Debian のデプロイメントを指します。サポートされているバージョンのリストについては、 "NetApp Interoperability Matrix Tool（IMT）" 。

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

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

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

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

移行またはハイパーバイザーのメンテナンスを実行する前に、ノードを正常にシャットダウンしてください。の手順を参照してください"グリッドノードをシャットダウンしています"。

VMware のライブマイグレーションはサポートされていません

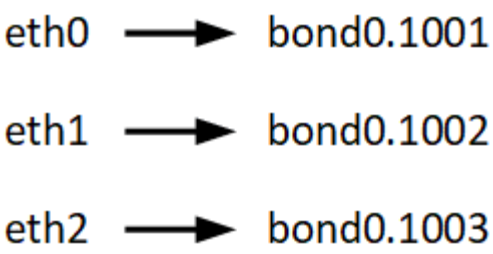
VMware VMでベアメタルインストールを実行する場合、OpenStack Live MigrationとVMwareのライブvMotion原因で仮想マシンのクロック時間がジャンプするため、どのタイプのグリッドノードでもサポートされていません。まれにではありますが、クロック時間が不正確だとデータや設定の更新が失われることがあります。

コールドマイグレーションはサポートされています。コールドマイグレーションでは、 StorageGRID ノードをホスト間で移行する前にシャットダウンします。の手順を参照してください"グリッドノードをシャットダウンしています"。

一貫したネットワークインターフェイス名

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

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



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

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

複数のホスト間でネットワークインターフェイスの名前を統一するには、さまざまな方法があります。いくつかの例については、を参照してください"ホストネットワークを設定する"。

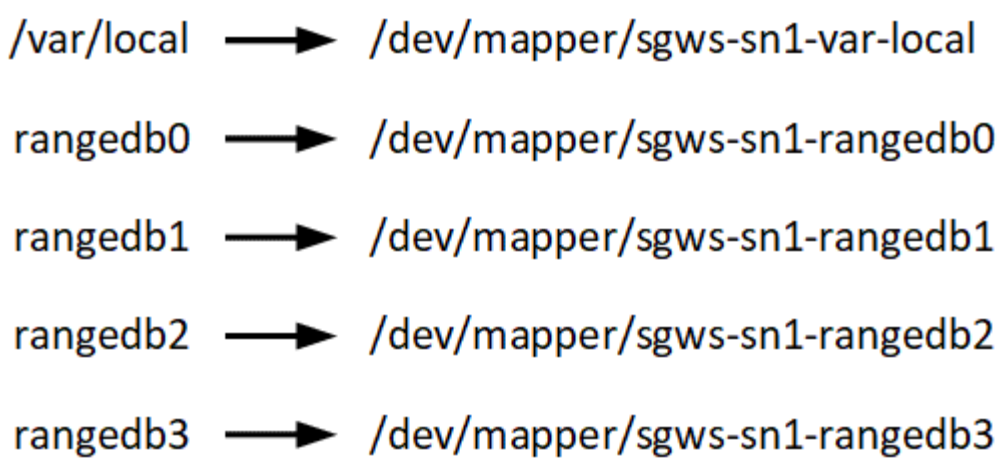
共有ストレージ

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

- 「ノードのエクスポート」処理で、HostAで実行されているノードコンテナから永続的な状態の少量のデータが抽出され、そのノードのシステムデータボリュームにキャッシュされます。そのあと、 HostA のノードコンテナのインスタンス化が解除されます。
- 「ノードのインポート」処理では、HostAと同じネットワークインターフェイスマッピングとブロックストレージマッピングを使用するHostBのノードコンテナがインスタンス化されます。次に、キャッシュされた永続状態データが新しいインスタンスに挿入されます。

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

次の例は、StorageGRIDストレージノード用のブロックデバイスマッピングの1つのソリューションを示しています。これらのホストではDMマルチパスを使用しており、でaliasフィールドを使用し `/etc/multipath.conf` て、すべてのホストで使用可能な一貫性のあるわかりやすい名前をブロックデバイスに提供しています。



StorageGRIDがホスト全体の設定を変更する方法

ベアメタルシステムでは、StorageGRIDによってホスト全体の設定が一部変更され `sysctl` ます。

「Linux」は、RHEL、Ubuntu、または Debian のデプロイメントを指します。サポートされているバージョンのリストについては、 "NetApp Interoperability Matrix Tool（IMT）" 。

次の変更が行われます。

```
# Recommended Cassandra setting: CASSANDRA-3563, CASSANDRA-13008, DataStax
documentation
vm.max_map_count = 1048575

# core file customization
# Note: for cores generated by binaries running inside containers, this
# path is interpreted relative to the container filesystem namespace.
# External cores will go nowhere, unless /var/local/core also exists on
# the host.
kernel.core_pattern = /var/local/core/%e.core.%p

# Set the kernel minimum free memory to the greater of the current value
or
# 512MiB if the host has 48GiB or less of RAM or 1.83GiB if the host has
more than 48GiB of RTAM
vm.min_free_kbytes = 524288

# Enforce current default swappiness value to ensure the VM system has
some
# flexibility to garbage collect behind anonymous mappings. Bump
watermark_scale_factor
```

```
# to help avoid OOM conditions in the kernel during memory allocation
bursts. Bump
# dirty_ratio to 90 because we explicitly fsync data that needs to be
persistent, and
# so do not require the dirty_ratio safety net. A low dirty_ratio combined
with a large
# working set (nr_active_pages) can cause us to enter synchronous I/O mode
unnecessarily,
# with deleterious effects on performance.
vm.swappiness = 60
vm.watermark_scale_factor = 200
vm.dirty_ratio = 90

# Turn off slow start after idle
net.ipv4.tcp_slow_start_after_idle = 0

# Tune TCP window settings to improve throughput
net.core.rmem_max = 8388608
net.core.wmem_max = 8388608
net.ipv4.tcp_rmem = 4096 524288 8388608
net.ipv4.tcp_wmem = 4096 262144 8388608
net.core.netdev_max_backlog = 2500

# Turn on MTU probing
net.ipv4.tcp_mtu_probing = 1

# Be more liberal with firewall connection tracking
net.ipv4.netfilter.ip_conntrack_tcp_be_liberal = 1

# Reduce TCP keepalive time to reasonable levels to terminate dead
connections
net.ipv4.tcp_keepalive_time = 270
net.ipv4.tcp_keepalive_probes = 3
net.ipv4.tcp_keepalive_intvl = 30

# Increase the ARP cache size to tolerate being in a /16 subnet
net.ipv4.neigh.default.gc_thresh1 = 8192
net.ipv4.neigh.default.gc_thresh2 = 32768
net.ipv4.neigh.default.gc_thresh3 = 65536
net.ipv6.neigh.default.gc_thresh1 = 8192
net.ipv6.neigh.default.gc_thresh2 = 32768
net.ipv6.neigh.default.gc_thresh3 = 65536

# Disable IP forwarding, we are not a router
net.ipv4.ip_forward = 0
```

```
# Follow security best practices for ignoring broadcast ping requests
net.ipv4.icmp_echo_ignore_broadcasts = 1

# Increase the pending connection and accept backlog to handle larger
connection bursts.
net.core.somaxconn=4096
net.ipv4.tcp_max_syn_backlog=4096
```

Linux グリッドホストに StorageGRID をインストールします

すべての Linux グリッド ホストにStorageGRIDをインストールする必要があります。サポートされているバージョンの一覧については、 NetApp相互運用性マトリックス ツールを使用してください。

開始する前に

お使いのオペレーティングシステムが、以下に示すStorageGRIDのカーネルバージョンの最小要件を満たしていることを確認してください。コマンドを使用し `uname -r`てオペレーティングシステムのカーネルバージョンを確認するか、OSベンダーに問い合わせてください。

「Linux」は、RHEL、Ubuntu、または Debian のデプロイメントを指します。サポートされているバージョンのリストについては、 "NetApp Interoperability Matrix Tool（IMT）" 。

RHEL

RHELバージョン	最小カーネルバージョン	カーネルパッケージ名
8.8（廃止）	4.18.0～477.10.1.el8_8.x86_64	kernel-4.18.0-477.10.1.el8_8.x86_64
8.10	4.18.0-553.el8_10.x86_64	kernel-4.18.0-553.el8_10.x86_64
9.0（廃止）	5.14.0～70.22.1.el9_0.x86_64	kernel-5.14.0-70.22.1.el9_0.x86_64
9.2（廃止）	5.14.0～284.11.1.el9_2.x86_64	カーネル-5.14.0-284.11.1.el9_2.x86_64
9.4	5.14.0～427.18.1.el9_4.x86_64	カーネル-5.14.0-427.18.1.el9_4.x86_64
9.6	5.14.0-570.18.1.el9_6.x86_64	カーネル-5.14.0-570.18.1.el9_6.x86_64

Ubuntu

注: Ubuntuバージョン18.04および20.04のサポートは廃止され、今後のリリースで削除される予定です。

Ubuntuバージョン	最小カーネルバージョン	カーネルパッケージ名
22.04.1	5.15.0-47-汎用	linux-image-5.15.0-47-generic/jammy-updates、jammy-security、現在は5.15.0-47.51
24.04	6.8.0-31-汎用	linux-image-6.8.0-31-generic/noble、現在は6.8.0-31.31

Debian

注意: Debianバージョン11のサポートは非推奨となり、今後のリリースで削除される予定です。

Debianバージョン	最小カーネルバージョン	カーネルパッケージ名
11（廃止）	5.10.0-18-amd64	linux-image-5.10.0-18-amd64/stable、現在は5.10.150-1
12	6.1.0-9-amd64	linux-image-6.1.0-9-amd64/stable、現在は6.1.27-1

手順

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

   グラフィカルデスクトップ環境をインストールしないでください。

- RHEL をインストールするときに標準の Linux インストーラーを使用している場合は、「コンピューティング ノード」ソフトウェア構成 (使用可能な場合) または「最小インストール」ベース環境を選択します。
- Ubuntu をインストールするときは、標準システムユーティリティ*を選択する必要があります。**Ubuntu** ホストへの **ssh** アクセスを有効にするには、***OpenSSH** サーバー を選択することをお勧めします。その他のオプションはすべてオフのままにできます。

2. RHEL の Extras チャネルを含むすべてのホストがパッケージ リポジトリにアクセスできることを確認します。
3. スワップが有効になっている場合：
   a. 次のコマンドを実行します。 `$ sudo swapoff --all`
   b. からすべてのスワップエントリを削除し `/etc/fstab`て、設定を維持します。

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

Ubuntu および **Debian** 上の **StorageGRID** の **AppArmor** プロファイルについて説明します

自社で導入した Ubuntu 環境を運用し、 AppArmor の必須のアクセス制御システムを使用している場合、ベースシステムにインストールするパッケージに関連付けられた AppArmor プロファイルが、 StorageGRID と一緒にインストールされた対応するパッケージによってブロックされる可能性があります。

デフォルトでは、 AppArmor プロファイルは、ベースのオペレーティングシステムにインストールするパッケージに対してインストールされます。StorageGRID システムコンテナからこれらのパッケージを実行すると、 AppArmor プロファイルがブロックされます。DHCP 、 MySQL 、 NTP 、 tcdump のベースパッケージが AppArmor と競合するほか、これら以外のベースパッケージも競合する可能性があります。

AppArmor プロファイルの対処方法としては、次の 2 つの選択肢があります。

- ベースシステムにインストールされたパッケージのうち、 StorageGRID システムコンテナに含まれるパッケージと重複するパッケージのプロファイルを個々に無効にする。各プロファイルを無効にすると、StorageGRID ログファイルに AppArmor が有効であることを示すエントリが表示されます。

  次のコマンドを使用します。

```
sudo ln -s /etc/apparmor.d/<profile.name> /etc/apparmor.d/disable/
sudo apparmor_parser -R /etc/apparmor.d/<profile.name>
```

- 例： *

```
sudo ln -s /etc/apparmor.d/bin.ping /etc/apparmor.d/disable/
sudo apparmor_parser -R /etc/apparmor.d/bin.ping
```

- AppArmorを完全に無効にします。Ubuntu 9.10以降の場合は、 "Ubuntuオンラインコミュニティ"の手順に従ってください。新しいバージョンのUbuntuでは、AppArmorを完全に無効にできない場合があります。

AppArmorを無効にすると、StorageGRIDログファイルにAppArmorが有効であることを示すエントリは表示されません。

Linux デプロイメント用の StorageGRID ホストネットワークを設定する

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

「Linux」は、RHEL、Ubuntu、または Debian のデプロイメントを指します。サポートされているバージョンのリストについては、 "NetApp Interoperability Matrix Tool（IMT）" 。

開始する前に

- "ネットワークのガイドライン"の情報を確認しました。
- に関する情報を確認しておき"ノードコンテナの移行要件"ます。
- 仮想ホストを使用している場合は、MAC アドレスのクローニングに関する考慮事項と推奨事項ホスト ネットワークを構成する前に。

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

タスクの内容

グリッドノードは、グリッドネットワークにアクセスできる必要があります。また、管理ネットワークとクライアントネットワークにアクセスすることもできます。このアクセスを確立するには、ホストの物理インターフェイスを各グリッドノードの仮想インターフェイスに関連付けるマッピングを作成します。ホストインターフェイスを作成するときにわかりやすい名前を使用すると、すべてのホストへの導入が簡単になり、移行も可能になります。

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

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

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

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

MAC アドレスのクローニングに関する考慮事項と推奨事項

MACアドレスのクローン作成を行うと、コンテナはホストのMACアドレスを使用し、ホストは指定したアドレス、またはランダムに生成されたアドレスのMACアドレスを使用するようになります。

MAC クローニングのイネーブル化

特定の環境においては、MACアドレスのクローニングによってセキュリティを強化できます。これは、管理ネットワーク、グリッドネットワーク、およびクライアントネットワークにそれぞれ専用の仮想NICを使用できるためです。

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

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

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

ネットワークごとに 1 つのキーがあります。

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

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

MAC クローン作成の使用例

MAC クローニングでは、次の 2 つのユースケースを検討します。

- MAC クローニングが有効になっていません：ノード構成ファイルの `_CLONE_MAC`キーが設定されていないか、「false」に設定されている場合、ホストはホスト NIC MAC を使用し、コンテナは StorageGRID によって生成された MAC を持ちます。ただし、 `_NETWORK_MAC`キーに MAC が指定されている場合

を除きます。 `_NETWORK_MAC`キーにアドレスが設定されている場合、コンテナには `_NETWORK_MAC`キーで指定されたアドレスが設定されます。

- MACクローニングが有効な場合：ノード構成ファイルの `_CLONE_MAC`キーが「true」に設定されている場合、コンテナはホストNICのMACを使用し、 `_NETWORK_MAC`キーにMACが指定されていない限り、ホストはStorageGRIDで生成されたMACを使用します。 `_NETWORK_MAC`キーにアドレスが設定されている場合、ホストは生成されたアドレスではなく、指定されたアドレスを使用します。

> MACアドレスのクローニングを使用せず、ハイパーバイザーによって割り当てられたもの以外のMACアドレスに対してすべてのインターフェースがデータを受信および送信できるようにしたい場合は、仮想スイッチおよびポートグループレベルのセキュリティプロパティが、MACアドレスの変更と偽造送信に対して **Accept** に設定されていることを確認してください。仮想スイッチに設定された値は、ポートグループレベルの値によって上書きされる可能性があるため、両方の場所で設定が同じであることを確認してください。

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

MAC クローニングの例

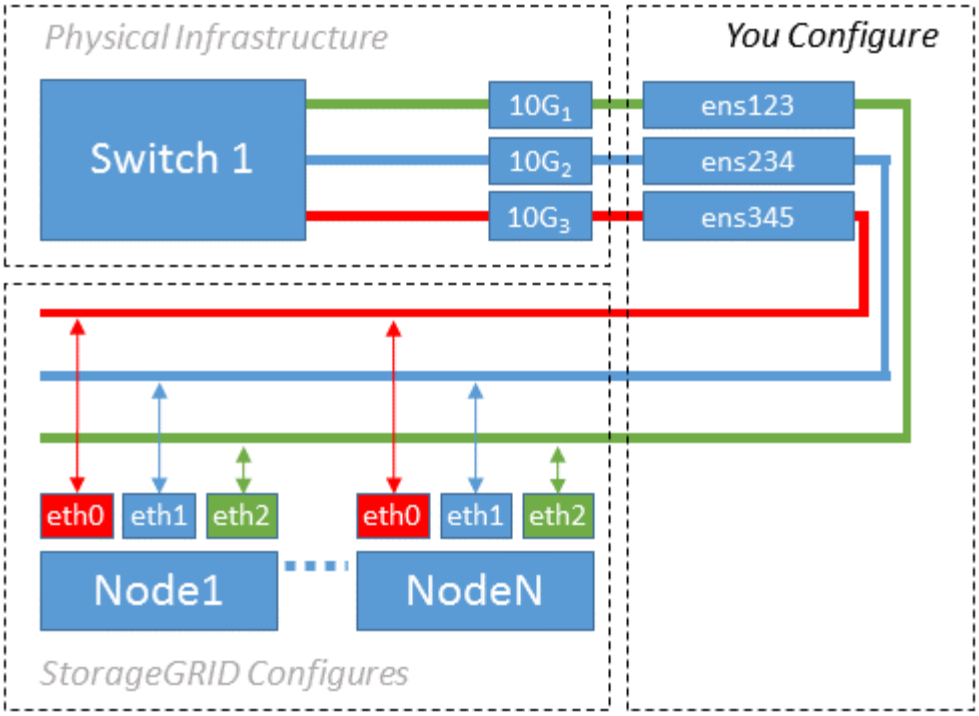
インターフェイスens256およびノード構成ファイルの次のキーに対して、MACアドレス11：22：33：44：55：66のホストでMACクローニングを有効にする例。

- `ADMIN_NETWORK_TARGET = ens256`
- `ADMIN_NETWORK_MAC = b2:9c:02:c2:27:10`
- `ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC = true`

結果：ens256のホストMACはb2：9c：02：c2：27：10、管理ネットワークMACは11：22：33：44：55：66です。

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

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



Linuxオペレーティングシステムは、 `ensXYZ`インストール時または起動時、あるいはインターフェースがホットアドされたときに、インターフェースを自動的に追加します。起動後にインターフェースが自動的に起動するように設定されていることを確認する以外に、構成は必要ありません。後の構成プロセスで正しいマッピングを提供できるように、どの ensXYZ がどのStorageGRIDネットワーク (グリッド、管理、またはクライアント) に対応するかを決定する必要があります。

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

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

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

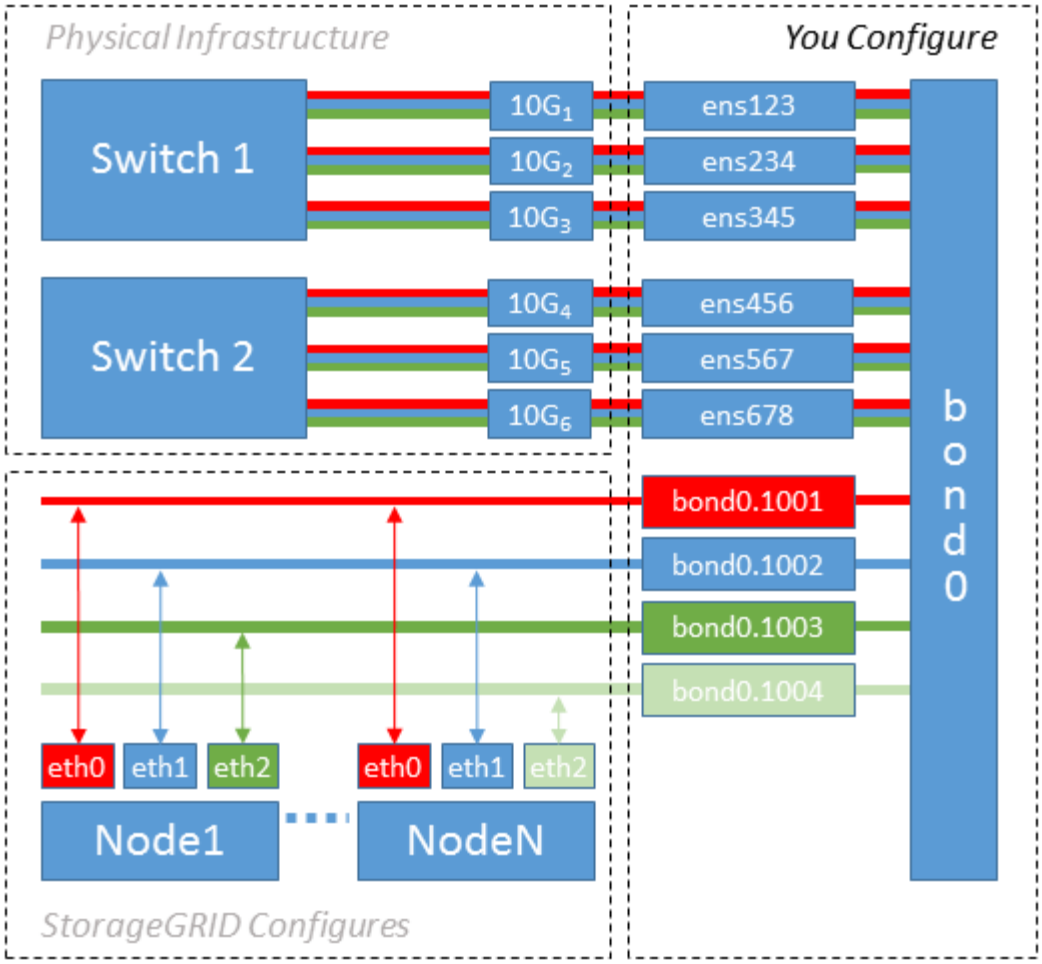
例 2 は、ネットワークインターフェイスのボンディングおよび使用している Linux ディストリビューションでの VLAN インターフェイスの作成に関する十分な知識があることを前提としています。

タスクの内容

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

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

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



手順

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

   すべてのホストのボンドに同じ名前を使用します。例: `bond0` 。

2. このボンドを関連する「物理デバイス」として使用するVLANインターフェイスを、標準のVLANインターフェイスの命名規則に従って作成します `physdev-name.VLAN ID`。

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

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

関連情報

- "UbuntuとDebianの/etc/network/interfacesの例"
- "RHEL の /etc/sysconfig/network-scripts の例"

各 Linux ホストにブロック ストレージ ボリュームを割り当てる必要があります。

開始する前に

以下のトピックで、このタスクを実行するために必要な情報を確認しておきます。

- "ストレージとパフォーマンスの要件"
- "ノードコンテナの移行要件"

> 「Linux」は、RHEL、Ubuntu、または Debian のデプロイメントを指します。サポートされているバージョンのリストについては、 "NetApp Interoperability Matrix Tool（IMT）" 。

タスクの内容

ブロックストレージボリューム（LUN）をホストに割り当てるときは、「ストレージ要件」の表を使用して次の項目を確認してください。

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

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

> これらのボリュームをパーティショニング、フォーマット、マウントする必要はありません。ボリュームがホストから認識できることを確認するだけで済みます。

> メタデータ専用ストレージノードに必要なオブジェクトデータLUNは1つだけです。

(`/dev/sdb`ボリューム名のリストを作成するときは、「`raw`」の特殊なデバイスファイルなどは使用しないでください。これらのファイルはホストのリブート時に変わることがあり、システムの適切な運用に影響します。`iSCSI LUN`と`Device Mapper Multipathing`を使用している場合は、ディレクトリでマルチパスエイリアスを使用することを検討して `/dev/mapper`ください。特に、`SAN`トポロジに共有ストレージへの冗長ネットワークパスが含まれている場合は、この方法が有効です。または、システムによって作成されたソフトリンクを永続的なデバイス名に使用することもできます `/dev/disk/by-path/`。

例：

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

結果はインストールごとに異なります。

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

例：

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

aliasフィールドをこのように使用すると、ホストのディレクトリにブロックデバイスとしてエイリアスが表示される `/dev/mapper`ため、設定やメンテナンスの処理でブロックストレージボリュームを指定する必要があるときに、わかりやすい名前を指定して簡単に検証できます。

StorageGRIDノードの移行とDevice Mapperマルチパスの使用をサポートするために共有ストレージをセットアップする場合は、同じ場所にあるすべてのホストに共通のを作成してインストールできます `/etc/multipath.conf`。各ホストで別のコンテナエンジンのストレージボリュームを使用するだけで済みます。エイリアスを使用し、各コンテナエンジンのストレージボリュームの LUN のエイリアスにターゲットのホスト名を含めると覚えやすいので、この方法で設定することを推奨します。

ソフトウェアのみの環境のコンテナエンジンとしてのDockerのサポートは廃止されました。Dockerは、今後のリリースで別のコンテナエンジンに置き換えられる予定です。

関連情報

- "コンテナエンジンのストレージボリュームを設定します"

- "ストレージとパフォーマンスの要件"
- "ノードコンテナの移行要件"

Linux上の**StorageGRID**用にコンテナエンジンのストレージボリュームを設定する

Docker または Podman コンテナ エンジンをインストールする前に、ストレージ ボリュームをフォーマットしてマウントする必要がある場合があります。

ソフトウェアのみの環境のコンテナエンジンとしてのDockerのサポートは廃止されました。Dockerは、今後のリリースで別のコンテナエンジンに置き換えられる予定です。

「Linux」は、RHEL、Ubuntu、または Debian のデプロイメントを指します。サポートされているバージョンのリストについては、 "NetApp Interoperability Matrix Tool（IMT）" 。

タスクの内容

Docker または Podman ストレージ ボリュームにルート ボリュームを使用する予定で、次のものを含むホスト パーティションに十分な空き容量がある場合は、これらの手順をスキップできます。

- ポッドマン： `/var/lib/containers`
- ドッカー: `/var/lib/docker`

手順

1. コンテナエンジンのストレージボリュームにファイルシステムを作成します。

RHEL

```
sudo mkfs.ext4 container-engine-storage-volume-device
```

Ubuntu または **Debian**

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

2. コンテナエンジンのストレージボリュームをマウントします。

RHEL

- Docker の場合：

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

- Podman の場合：

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

Ubuntu または **Debian**

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

- Podman の場合：

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

3. コンテナ ストレージ ボリューム デバイスのエントリを /etc/fstab に追加します。
   - RHEL: コンテナストレージボリュームデバイス
   - Ubuntu または Debian: docker-storage-volume-device

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

Docker をインストールする

StorageGRIDシステムは、コンテナのコレクションとして Linux 上で実行できます。

- Ubuntu または Debian 用のStorageGRIDをインストールする前に、Docker をインストールする必要があります。
- Docker コンテナ エンジンを使用することを選択した場合は、次の手順に従って Docker をインストールします。さもないと、Podman をインストールします 。

> ソフトウェアのみの環境のコンテナエンジンとしてのDockerのサポートは廃止されました。Dockerは、今後のリリースで別のコンテナエンジンに置き換えられる予定です。

手順

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

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

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

```
sudo systemctl enable docker
```

```
sudo systemctl start docker
```

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

```
sudo docker version
```

   クライアントとサーバのバージョンは1.11.0以降である必要があります。

Podman をインストールします

StorageGRIDシステムはコンテナのコレクションとして実行されます。 Podman コンテナ エンジンを使用することを選択した場合は、次の手順に従って Podman をインストールします。さもないと、Docker をインストールする 。

手順

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

   また、 Podman をインストールする際には、 Podman-Docker パッケージもインストールする必要があります。

2. 次のように入力して、必要なバージョンの Podman および Podman-Docker がインストールされていることを確認します。

```
sudo docker version
```

   Podman-Docker パッケージでは、 Docker コマンドを使用できます。

   クライアントとサーバのバージョンは3.2.3以降である必要があります。

```
Version: 3.2.3
API Version: 3.2.3
Go Version: go1.15.7
Built: Tue Jul 27 03:29:39 2021
OS/Arch: linux/amd64
```

関連情報

"ホストストレージを設定する"

Linuxへの**StorageGRID**ホストサービスのインストール

StorageGRIDホスト サービスをインストールするには、オペレーティング システムの種類に応じたStorageGRIDパッケージを使用します。

「Linux」は、RHEL、Ubuntu、または Debian のデプロイメントを指します。サポートされているバージョンのリストについては、 "NetApp Interoperability Matrix Tool（IMT）" 。

RHEL

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

タスクの内容

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

手順

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

   たとえば、次の手順のコマンド例を使用できるように、これらのコマンドをディレクトリに配置し `/tmp`ます。

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

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

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

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

   パッケージを以外のディレクトリに配置した `/tmp`場合は、使用したパスを反映するようにコマンドを変更します。

Ubuntu または **Debian**

StorageGRID DEB パッケージを使用して、Ubuntu または Debian 用のStorageGRIDホスト サービスをインストールします。

タスクの内容

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

手順

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

   たとえば、次の手順のコマンド例を使用できるように、これらのコマンドをディレクトリに配置し `/tmp`ます。

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

   最初にパッケージをインストールし、 `service`次にパッケージをインストールする必要があり `images`ます。パッケージを以外のディレクトリに配置した `/tmp`場合は、使用したパスを反映するようにコマンドを変更します。

   ```
   sudo dpkg --install /tmp/storagegrid-webscale-images-version-SHA.deb
   ```

   ```
   sudo dpkg --install /tmp/storagegrid-webscale-service-version-SHA.deb
   ```

   StorageGRIDパッケージをインストールする前に、Python 3 がインストールされている必要があります。その `sudo dpkg --install /tmp/storagegrid-webscale-images-version-SHA.deb`これを行わない限り、コマンドは失敗します。

ソフトウェアベースのノードのインストールを自動化する

Linux上の**StorageGRID**ホストサービスのインストールとグリッドノードの構成を自動化

StorageGRID ホストサービスのインストールおよびグリッドノードの設定を自動化することができます。

タスクの内容

「Linux」は、RHEL、Ubuntu、または Debian のデプロイメントを指します。サポートされているバージョンのリストについては、 "NetApp Interoperability Matrix Tool（IMT）" 。

導入を自動化すると、次のいずれかの場合に役立ちます。

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

StorageGRID ホストサービスはパッケージによってインストールされ、構成ファイルによって制御されます。次のいずれかの方法で構成ファイルを作成できます。

- "構成ファイルを作成します"手動インストール中に対話的に実行します。
- 構成ファイルを事前に準備し（またはプログラム化して）、この資料で説明するように、標準のオーケストレーションフレームワークを使用した自動インストールを可能にします。

  StorageGRIDには、StorageGRIDアプライアンスとStorageGRIDシステム全体（「グリッド」）の設定を自動化するためのPythonスクリプトがオプションで用意されています。これらのスクリプトを直接使用することも、スクリプトを調べて、独自に開発したグリッド内導入ツールや設定ツールの使用方法を学ぶこ

ともでき"StorageGRID インストール REST API"ます。

StorageGRID ホストサービスのインストールと設定を自動化する

StorageGRID ホストサービスのインストールは、 Ansible 、 Puppet 、 Chef 、 Fabric 、 SaltStack などの標準のオーケストレーションフレームワークを使用して自動化できます。

StorageGRIDホスト サービスは、DEB (Ubuntu または Debian) または RPM (RHEL) にパッケージ化されており、自動インストールを有効にするために事前に (またはプログラムによって) 準備できる構成ファイルによって駆動されます。すでに標準のオーケストレーション フレームワークを使用して Linux デプロイメントをインストールおよび構成している場合は、プレイブックまたはレシピにStorageGRIDを追加するのは簡単です。

ホストの準備と仮想グリッドノードの導入の手順をすべて自動化することができます。

サンプルの Ansible のロールとプレイブック

サンプルのAnsibleのロールとプレイブックは、インストールアーカイブのフォルダにあります `/extras`。Ansibleプレイブックは、ロールでホストを準備してStorageGRIDをターゲットサーバにインストールする方法を示しています `storagegrid`。必要に応じて、ロールまたはプレイブックをカスタマイズできます。

> ⓘ サンプルのプレイブックには、 StorageGRID ホストサービスを開始する前にネットワークデバイスを作成するために必要な手順は含まれていません。これらの手順は、最終的な確認と使用の前に追加してください。

RHEL

RHELの場合、提供されているインストールタスクは `storagegrid`役割の例を使用する `ansible.builtin.dnf`ローカル RPM ファイルまたはリモート Yum リポジトリからインストールを実行するモジュール。モジュールが利用できないかサポートされていない場合は、次のファイル内の適切なAnsibleタスクを編集して、 `yum`または `ansible.builtin.yum`モジュール:

- `roles/storagegrid/tasks/rhel_install_from_repo.yml`
- `roles/storagegrid/tasks/rhel_install_from_local.yml`

Ubuntu または **Debian**

UbuntuまたはDebianの場合、提供されているインストールタスクは `storagegrid`役割の例を使用する `ansible.builtin.apt`ローカル DEB ファイルまたはリモート apt リポジトリからインストールを実行するモジュール。モジュールが利用できないかサポートされていない場合は、次のファイル内の適切なAnsibleタスクを編集して、 `ansible.builtin.apt`モジュール:

- `roles/storagegrid/tasks/deb_install_from_repo.yml`
- `roles/storagegrid/tasks/deb_install_from_local.yml`

StorageGRID の設定を自動化

グリッドノードを導入したら、 StorageGRID システムの設定を自動化できます。

開始する前に

- インストールアーカイブにある次のファイルの場所を確認しておきます。

ファイル名	製品説明
configure-storagegrid.py	設定を自動化するための Python スクリプト
storagegrid-sample.json を設定します	スクリプトで使用する構成ファイルの例
storagegrid-bank.json を設定する	スクリプトで使用する空の構成ファイルです

- 構成ファイルを作成しておき `configure-storagegrid.json`ます。このファイルを作成するには（`configure-storagegrid.sample.json`、サンプル構成ファイル）または空の構成ファイル）（`configure-storagegrid.blank.json`を変更します。

> 変更したファイルのパスワードセクションから管理パスワードとプロビジョニングパスフレーズを保存します。 `configure-storagegrid.json`構成ファイルを安全な場所に保管します。これらのパスワードは、インストール、拡張、およびメンテナンスの手順に必要です。変更したファイルもバックアップする必要があります `configure-storagegrid.json`構成ファイルを作成して安全な場所に保存します。

タスクの内容

Pythonスクリプトと `configure-storagegrid.json`構成ファイルを使用して、StorageGRIDシステムの設定を自動化できます `configure-storagegrid.py`。

> また、 Grid Manager またはインストール API を使用してシステムを設定することもできます。

手順

1. Python スクリプトを実行するために使用する Linux マシンにログインします。
2. インストールアーカイブを展開したディレクトリに移動します。

   例：

   ```
   cd StorageGRID-Webscale-version/platform
   ```

   `platform`は `rpms`、または `vsphere`です `debs`。

3. Python スクリプトを実行し、作成した構成ファイルを使用します。

   例：

   ```
   ./configure-storagegrid.py ./configure-storagegrid.json --start-install
   ```

結果

設定プロセス中にリカバリパッケージ `.zip`ファイルが生成され、インストールおよび設定プロセスを実行するディレクトリにダウンロードされます。グリッドノードで障害が発生した場合に StorageGRID システムをリカバリできるようにするために、リカバリパッケージファイルをバックアップする必要があります。たとえば、バックアップされたセキュアなネットワーク上の場所や、安全なクラウドストレージ上の場所にコピーします。

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

ランダムパスワードを生成するように指定した場合は、ファイルを開き `Passwords.txt`、StorageGRIDシステムへのアクセスに必要なパスワードを探します。

```
######################################################################
##### The StorageGRID "Recovery Package" has been downloaded as: #####
#####           ./sgws-recovery-package-994078-rev1.zip          #####
#####   Safeguard this file as it will be needed in case of a    #####
#####                 StorageGRID node recovery.                 #####
######################################################################
```

StorageGRID システムがインストールおよび設定されると、確認メッセージが表示されます。

```
StorageGRID has been configured and installed.
```

StorageGRIDで**VMware vSphere**を使用してグリッドノードの導入を自動化

VMware OVF Toolを使用すると、グリッドノードの導入を自動化できます。StorageGRID の設定を自動化することもできます。

グリッドノードの導入を自動化

VMware OVF Toolを使用すると、グリッドノードの導入を自動化できます。

開始する前に

- Bash 3.2 以降が搭載された Linux / UNIX システムにアクセスできるようにしておきます。
- VMware vSphereとvCenterを使用している場合
- VMware OVF ツールがインストールされ、正しく構成されています。
- OVFツールを使用してVMware vSphereにアクセスするためのユーザ名とパスワードを確認しておきます。
- OVFファイルからVMを導入して電源をオンにするための十分な権限と、VMに接続するための追加ボリュームを作成するための権限が必要です。詳細については、のドキュメントを参照してください `ovftool`。
- StorageGRID 仮想マシンを導入する vSphere 内の場所の仮想インフラ（ VI ） URL を確認しておきます。この URL は通常、 vApp またはリソースプールです。例：

```
vi://vcenter.example.com/vi/sgws
```

この値は、VMwareユーティリティを使用して確認できます（詳細についてはのドキュメントを参照してください）。

vApp に導入する場合、初回は仮想マシンが自動的に起動されないため、手動で電源をオンにする必要があります。

- 導入構成ファイルに必要なすべての情報を収集しておきます。詳細は、を参照してください"導入環境に関する情報を収集します"。
- VMware 用インストールアーカイブに含まれている次のファイルに StorageGRID からアクセスできるようにしておきます。

ファイル名	製品説明
NetApp-SG-version-sha.vmdk	グリッドノード仮想マシンを作成するためのテンプレートとして使用される仮想マシンディスクファイル。 *注：*このファイルは、ファイルおよび .mf ファイルと同じフォルダにある必要があります .ovf。
vsphere-primary-admin.ovf vsphere-primary-admin.mf	(.mf プライマリ管理ノードを導入するためのOpen Virtualization Formatテンプレートファイル) (.ovf とマニフェストファイル
vsphere-non-primary-admin.ovf vsphere-non-primary-admin.mf	テンプレートファイル(.ovf）とマニフェストファイル(.mf）。非プライマリ管理ノードを導入するためのものです。
vsphere-gateway.ovf vsphere-gateway.mf	テンプレートファイル(.ovf）とマニフェストファイル(.mf）を使用してゲートウェイノードを導入します。
vsphere-storage.ovf vsphere-storage.mf	(.mf 仮想マシンベースのストレージノードを導入するためのテンプレートファイル (.ovf とマニフェストファイル)
deploy-vsphere-ovftool.sh	仮想グリッドノードの導入を自動化するための Bash シェルスクリプト。
deploy-vsphere-ovftool-sample.ini	スクリプトで使用する構成ファイルの例を示します deploy-vsphere-ovftool.sh。

導入環境に応じた構成ファイルを定義します

StorageGRIDの仮想グリッドノードを導入するために必要な情報を構成ファイルで指定します。このファイルは、Bashスクリプトで使用され`deploy-vsphere-ovftool.sh`ます。サンプル構成ファイルを変更して、ファイ

ルを最初から作成する必要がないようにすることができます。

手順

1. サンプルコンフィギュレーションファイルのコピーを作成し(`deploy-vsphere-ovftool.sample.ini`ます）。新しいファイルをという名前でと同じディレクトリに `deploy-vsphere-ovftool.sh`保存します `deploy-vsphere-ovftool.ini。
2. `deploy-vsphere-ovftool.ini`を開きます。
3. VMware 仮想グリッドノードを導入するために必要なすべての情報を入力します。

   詳細は、を参照してください構成ファイルの設定。

4. 必要な情報をすべて入力して確認したら、ファイルを保存して閉じます。

構成ファイルの設定

`deploy-vsphere-ovftool.ini`構成ファイルには、仮想グリッドノードの導入に必要な設定が含まれています。

構成ファイルでは、最初にグローバルパラメータがリストされ、そのあとにノード名で定義されるセクションにノード固有のパラメータがリストされます。ファイルの使用状況：

- *Global parameters* は、すべてのグリッドノードに適用されます。
- _Node-specific parameters_override グローバルパラメータ。

グローバルパラメータ

グローバルパラメータは、個々のセクションの設定で上書きされないかぎり、すべてのグリッドノードに適用されます。複数のノードに適用するパラメータをグローバルパラメータセクションに配置し、個々のノードのセクションで必要に応じてこれらの設定を上書きします。

- * OVFTOOL_ARGUMENTS * ： OVFTOOL_ARGUMENTS をグローバル設定として指定するか、または特定のノードに個別に引数を適用できます。例：

  ```
  OVFTOOL_ARGUMENTS = --powerOn --noSSLVerify --diskMode=eagerZeroedThick
  --datastore='datastore_name'
  ```

  オプションと `--overwrite`オプションを使用して、既存の仮想マシンをシャットダウンして交換できます `--powerOffTarget。

  > ノードを別々のデータストアに導入し、 OVFTOOL_ARGUMENTS をグローバルに指定するのではなくノードごとに指定する必要があります。

- * source *：StorageGRID仮想マシンテンプレート(`.vmdk`ファイルと個 々 のグリッドノードのファイル `.ovf`と `.mf`ファイルのパス。デフォルトでは現在のディレクトリに設定されます。

```
SOURCE = /downloads/StorageGRID-Webscale-version/vsphere
```

- * target * ： StorageGRID の導入先となる VMware vSphere 仮想インフラ（ vi ）の URL 。例：

```
TARGET = vi://vcenter.example.com/vm/sgws
```

- * GRID_NETWORK_CONFIG * ：静的または DHCP のいずれかの IP アドレスの取得に使用される方法。デフォルトはSTATICです。全ノードまたはほとんどのノードが IP アドレスの取得に同じ方法を使用する場合は、ここでその方法を指定できます。その後、個々のノードで別々の設定を指定してグローバル設定を上書きできます。例：

```
GRID_NETWORK_CONFIG = STATIC
```

- * GRID_NETWORK_TARGET * ：グリッドネットワークに使用される既存の VMware ネットワークの名前。全ノードまたはほとんどのノードが同じネットワーク名を使用する場合は、ここでその名前を指定できます。その後、個々のノードで別々の設定を指定してグローバル設定を上書きできます。例：

```
GRID_NETWORK_TARGET = SG Admin Network
```

- * GRID_NETWORK_MASK * ：グリッドネットワークのネットワークマスク。全ノードまたはほとんどのノードが同じネットワークマスクを使用する場合は、ここでそのネットワークマスクを指定できます。その後、個々のノードで別々の設定を指定してグローバル設定を上書きできます。例：

```
GRID_NETWORK_MASK = 255.255.255.0
```

- * GRID_NETWORK_GATEWAY * ：グリッドネットワークのネットワークゲートウェイ。全ノードまたはほとんどのノードが同じネットワークゲートウェイを使用する場合は、ここでそのネットワークゲートウェイを指定できます。その後、個々のノードで別々の設定を指定してグローバル設定を上書きできます。例：

```
GRID_NETWORK_GATEWAY = 10.1.0.1
```

- * GRID_NETWORK_MTU * ：オプション。グリッドネットワークでの最大伝送ユニット（ MTU ）です。この値を指定する場合、 1280 ～ 9216 の範囲で指定する必要があります。例：

```
GRID_NETWORK_MTU = 9000
```

  省略すると、 1400 が使用されます。

  ジャンボフレームを使用する場合は、 MTU を 9000 などのジャンボフレームに適した値に設定します。それ以外の場合は、デフォルト値のままにします。

ネットワークのMTU値は、ノードの接続先であるvSphereの仮想スイッチポートに設定されている値と同じである必要があります。そうしないと、ネットワークパフォーマンスの問題やパケット損失が発生する可能性があります。

ネットワークのパフォーマンスを最大限に高めるには、すべてのノードのグリッドネットワークインターフェイスで MTU 値がほぼ同じになるように設定する必要があります。個々のノードのグリッドネットワークの MTU 設定に大きな違いがある場合は、 * Grid Network MTU mismatch * アラートがトリガーされます。MTU値はすべてのネットワークタイプで同じである必要はありません。

- * ADMIN_NETWORK_CONFIG * ： IP アドレスの取得に使用された方法。無効、静的、または DHCP のいずれかです。デフォルトはdisabledです。全ノードまたはほとんどのノードが IP アドレスの取得に同じ方法を使用する場合は、ここでその方法を指定できます。その後、個々のノードで別々の設定を指定してグローバル設定を上書きできます。例：

```
ADMIN_NETWORK_CONFIG = STATIC
```

- * ADMIN_NETWORK_TARGET * ：管理ネットワークに使用する既存の VMware ネットワークの名前。この設定は、管理ネットワークが無効になっていない場合に必要となります。全ノードまたはほとんどのノードが同じネットワーク名を使用する場合は、ここでその名前を指定できます。グリッドネットワークとは異なり、すべてのノードを同じ管理ネットワークに接続する必要はありません。その後、個々のノードで別々の設定を指定してグローバル設定を上書きできます。例：

```
ADMIN_NETWORK_TARGET = SG Admin Network
```

- * ADMIN_NETWORK_MASK * ：管理ネットワークのネットワークマスク。この設定は、静的 IP アドレスを使用する場合に必要となります。全ノードまたはほとんどのノードが同じネットワークマスクを使用する場合は、ここでそのネットワークマスクを指定できます。その後、個々のノードで別々の設定を指定してグローバル設定を上書きできます。例：

```
ADMIN_NETWORK_MASK = 255.255.255.0
```

- * ADMIN_NETWORK_GATEWAY * ：管理ネットワークのネットワークゲートウェイ。この設定は、 IP アドレスを静的に指定し、かつ ADMIN_NETWORK_ESL 設定で外部サブネットを指定する場合に必要となります（つまり、ADMIN_NETWORK_ESLが空の場合は必要ありません）。全ノードまたはほとんどのノードが同じネットワークゲートウェイを使用する場合は、ここでそのネットワークゲートウェイを指定できます。その後、個々のノードで別々の設定を指定してグローバル設定を上書きできます。例：

```
ADMIN_NETWORK_GATEWAY = 10.3.0.1
```

- * ADMIN_NETWORK_ESL * ：管理ネットワークの外部サブネットリスト（ルート）。 CIDR ルートのデスティネーションをカンマで区切ったリストとして指定します。全ノードまたはほとんどのノードが同じ外部サブネットリストを使用する場合は、ここでそのリストを指定できます。その後、個々のノードで別々の設定を指定してグローバル設定を上書きできます。例：

```
ADMIN_NETWORK_ESL = 172.16.0.0/21,172.17.0.0/21
```

- * ADMIN_NETWORK_MTU * ：オプション。管理ネットワークでの最大伝送ユニット（ MTU ）です。ADMIN_NETWORK_CONFIG = DHCPの場合は指定しないでください。この値を指定する場合、1280 ～ 9216 の範囲で指定する必要があります。省略すると、 1400 が使用されます。ジャンボフレームを使用する場合は、 MTU を 9000 などのジャンボフレームに適した値に設定します。それ以外の場合は、デフォルト値のままにします。全ノードまたはほとんどのノードが管理ネットワークに同じ MTU を使用する場合は、ここでその MTU を指定できます。その後、個々のノードで別々の設定を指定してグローバル設定を上書きできます。例：

```
ADMIN_NETWORK_MTU = 8192
```

- * CLIENT_NETWORK_CONFIG * ： IP アドレスの取得に使用する方法。無効、静的、または DHCP のいずれかになります。デフォルトはdisabledです。全ノードまたはほとんどのノードが IP アドレスの取得に同じ方法を使用する場合は、ここでその方法を指定できます。その後、個々のノードで別々の設定を指定してグローバル設定を上書きできます。例：

```
CLIENT_NETWORK_CONFIG = STATIC
```

- * client_network_target * ：クライアントネットワークに使用する既存の VMware ネットワークの名前。この設定は、クライアントネットワークが無効になっていない場合に必要となります。全ノードまたはほとんどのノードが同じネットワーク名を使用する場合は、ここでその名前を指定できます。グリッドネットワークとは異なり、すべてのノードを同じクライアントネットワークに接続する必要はありません。その後、個々のノードで別々の設定を指定してグローバル設定を上書きできます。例：

```
CLIENT_NETWORK_TARGET = SG Client Network
```

- * CLIENT_NETWORK_MASK * ：クライアントネットワークのネットワークマスク。この設定は、静的 IP アドレスを使用する場合に必要となります。全ノードまたはほとんどのノードが同じネットワークマスクを使用する場合は、ここでそのネットワークマスクを指定できます。その後、個々のノードで別々の設定を指定してグローバル設定を上書きできます。例：

```
CLIENT_NETWORK_MASK = 255.255.255.0
```

- * client_network_gateway * ：クライアントネットワークのネットワークゲートウェイ。この設定は、静的 IP アドレスを使用する場合に必要となります。全ノードまたはほとんどのノードが同じネットワークゲートウェイを使用する場合は、ここでそのネットワークゲートウェイを指定できます。その後、個々のノードで別々の設定を指定してグローバル設定を上書きできます。例：

```
CLIENT_NETWORK_GATEWAY = 10.4.0.1
```

- * CLIENT_NETWORK_MTU * ：オプション。クライアントネットワークでの最大伝送ユニット（ MTU ）です。CLIENT_NETWORK_CONFIG = DHCPの場合は指定しないでください。この値を指定する場合、

1280 ～ 9216 の範囲で指定する必要があります。省略すると、 1400 が使用されます。ジャンボフレームを使用する場合は、 MTU を 9000 などのジャンボフレームに適した値に設定します。それ以外の場合は、デフォルト値のままにします。全ノードまたはほとんどのノードがクライアントネットワークに同じ MTU を使用する場合は、ここでその MTU を指定できます。その後、個々のノードで別々の設定を指定してグローバル設定を上書きできます。例：

```
CLIENT_NETWORK_MTU = 8192
```

- * PORT_REMAP * ：ノードが内部でのグリッドノードの通信または外部との通信に使用するポートを再マッピングします。StorageGRID で使用される 1 つ以上のポートがエンタープライズネットワークポリシーによって制限される場合は、ポートの再マッピングが必要です。StorageGRIDで使用されるポートのリストについては、の内部でのグリッドノードの通信と外部との通信を参照してください"ネットワークのガイドライン"。

  ロードバランサエンドポイントの設定に使用する予定のポートは再マッピングしないでください。

  PORT_REMAP のみを設定すると、指定したマッピングがインバウンド通信とアウトバウンド通信の両方に使用されます。PORT_REMAP_INBOUND を併せて指定した場合は、PORT_REMAP がアウトバウンド通信のみに適用されます。

  使用される形式は、です *network type/protocol/default port used by grid node/new port*。ネットワークタイプはgrid、admin、またはclient、protocolはtcpまたはudpです。

  例：

  ```
  PORT_REMAP = client/tcp/18082/443
  ```

  この例の設定だけを使用した場合は、グリッドノードのインバウンド通信とアウトバウンド通信の両方が、ポート 18082 からポート 443 へと対称的にマッピングされます。この例の設定を PORT_REMAP_INBOUND とともに使用した場合は、アウトバウンド通信がポート 18082 からポート 443 にマッピングされます。

  カンマで区切ったリストを使用して複数のポートを再マッピングすることもできます。

  例：

  ```
  PORT_REMAP = client/tcp/18082/443, client/tcp/18083/80
  ```

- * port_remap_inbound * ：指定したポートのインバウンド通信を再マッピングします。PORT_REMAP_INBOUNDを指定し、PORT_REMAPに値を指定しなかった場合、ポートのアウトバウンド通信は変更されません。

  ロードバランサエンドポイントの設定に使用する予定のポートは再マッピングしないでください。

使用される形式は、です *network type/protocol/_default port used by grid node/new port*。ネットワークタイプはgrid、admin、またはclient、protocolはtcpまたはudpです。

例：

```
PORT_REMAP_INBOUND = client/tcp/443/18082
```

次の例は、ポート 443 に送信されたトラフィックを内部ファイアウォールを通過させ、グリッドノードが S3 要求をリスンしているポート 18082 に転送します。

カンマで区切った複数のインバウンドポートを再マッピングすることもできます。

例：

```
PORT_REMAP_INBOUND = grid/tcp/3022/22, admin/tcp/3022/22
```

- * temporary_password_type *：ノードがグリッドに参加する前に、VMコンソールやStorageGRIDインストールAPIにアクセスする場合、またはSSHを使用してアクセスする場合に使用する一時インストールパスワードのタイプ。

> すべてのノードまたはほとんどのノードで同じタイプの一時インストールパスワードを使用する場合は、グローバルパラメータセクションでタイプを指定します。その後、必要に応じて個 々 のノードに別の設定を使用します。たとえば、**[カスタムパスワードを使用]***をグローバルに選択した場合は、 custom_temporary_password =<password>*を使用して各ノードのパスワードを設定できます。

- temporary_password_type *には、次のいずれかを指定できます。
  - ノード名を使用：ノード名は一時的なインストールパスワードとして使用され、VMコンソール、StorageGRIDインストールAPI、およびSSHへのアクセスを提供します。
  - パスワードを無効にする:一時的なインストールパスワードは使用されません。インストールの問題をデバッグするためにVMにアクセスする必要がある場合は、を参照してください"インストールに関する問題のトラブルシューティング"。
  - カスタムパスワードを使用：* custom_temporary_password =<password>*で指定した値は、一時的なインストールパスワードとして使用され、VMコンソール、StorageGRIDインストールAPI、およびSSHへのアクセスを提供します。

> 必要に応じて、* temporary_password_type パラメータを省略し、custom_temporary_password=<password>*のみを指定できます。

- * custom_temporary_password =<password>*オプション。インストール時にVMコンソール、StorageGRIDインストールAPI、およびSSHにアクセスする際に使用する一時パスワード。TEMPORARY_PASSWORD_TYPE が Use node name または Disable password *に設定されている場合は無視されます。

ノード固有のパラメータ

構成ファイルには、各ノード専用のセクションがあります。各ノードには次の設定が必要です。

- セクションヘッドでは、 Grid Manager に表示されるノード名を定義します。この値を無視するには、ノードに対してオプションの node_name パラメータを指定します。
- * NODE_TYPE * ：VM_Admin_Node、VM_Storage_Node、またはVM_API_Gateway_Node
- * storage_type * ：組み合わせたデータ、またはメタデータ。（オプション）ストレージノードのこのパラメータは、データとメタデータの組み合わせが指定されていない場合はデフォルトで設定されます。詳細については、を参照してください "ストレージノードのタイプ"。
- * GRID_NETWORK_IP * ：グリッドネットワークでのノードの IP アドレス。
- * ADMIN_NETWORK_IP * ：管理ネットワークでのノードの IP アドレス。ノードが管理ネットワークに接続され、かつ ADMIN_NETWORK_CONFIG が STATIC に設定されている場合にのみ必要です。
- * client_network_ip * ：クライアントネットワーク上のノードの IP アドレス。ノードがクライアントネットワークに接続され、かつノードの CLIENT_NETWORK_CONFIG が STATIC に設定されている場合にのみ必要です。
- * ADMIN_IP * ：グリッドネットワークでのプライマリ管理ノードの IP アドレス。プライマリ管理ノードの GRID_NETWORK_IP で指定した値を使用します。このパラメータを省略すると、ノードは mDNS を使用してプライマリ管理ノードの IP を検出しようとします。詳細については、を参照してください "グリッドノードによるプライマリ管理ノードの検出"。

  プライマリ管理ノードでは ADMIN_IP パラメータが無視されます。

- グローバルに設定されていないすべてのパラメータ。たとえば、ノードが管理ネットワークに接続されていて、 ADMIN_NETWORK_NETWORK パラメータをグローバルに指定していない場合は、ノードに対してそれらのパラメータを指定する必要があります。

プライマリ管理ノード

プライマリ管理ノードには次の設定を追加する必要があります。

- * node_type * ： VM_Admin_Node
- * Admin_role * ：プライマリ

次のエントリ例は、プライマリ管理ノードが 3 つのネットワークすべてに接続される場合を示しています。

```
[DC1-ADM1]
  ADMIN_ROLE = Primary
  NODE_TYPE = VM_Admin_Node
  TEMPORARY_PASSWORD_TYPE = Use custom password
  CUSTOM_TEMPORARY_PASSWORD = Passw0rd

  GRID_NETWORK_IP = 10.1.0.2
  ADMIN_NETWORK_IP = 10.3.0.2
  CLIENT_NETWORK_IP = 10.4.0.2
```

プライマリ管理ノードにオプションで追加できる設定は次のとおりです。

- * DISK * ：デフォルトでは、管理ノードに対して監査用とデータベース用の 2 つの 200GB ハードディスクが追加で割り当てられます。DISK パラメータを使用して、この容量を増やすことができます。例：

```
DISK = INSTANCES=2, CAPACITY=300
```

管理ノードの場合は、 INSTANCES を必ず 2 にする必要があります。

ストレージノード

ストレージノードには次の設定を追加する必要があります。

- * node_name * ： VM_Storage_Node

  次のエントリ例は、ストレージノードがグリッドネットワークと管理ネットワークに接続され、クライアントネットワークに接続されない場合を示しています。このノードでは、 ADMIN_IP 設定を使用してグリッドネットワークでのプライマリ管理ノードの IP アドレスを指定しています。

```
[DC1-S1]
  NODE_TYPE = VM_Storage_Node

  GRID_NETWORK_IP = 10.1.0.3
  ADMIN_NETWORK_IP = 10.3.0.3

  ADMIN_IP = 10.1.0.2
```

  2 番目のエントリ例は、ストレージノードがクライアントネットワークに接続される場合を示しています。ここでは、 S3 クライアントアプリケーションがストレージノードへのアクセスに使用できるポートが、ユーザのエンタープライズネットワークポリシーによって 80 または 443 に制限されています。この例の構成ファイルでは、 PORT_REMAP を使用して、ストレージノードがポート 443 で S3 メッセージを送受信できるようにしています。

```
[DC2-S1]
  NODE_TYPE = VM_Storage_Node

  GRID_NETWORK_IP = 10.1.1.3
  CLIENT_NETWORK_IP = 10.4.1.3
  PORT_REMAP = client/tcp/18082/443

  ADMIN_IP = 10.1.0.2
```

  最後の例では、 ssh トラフィックに対してポート 22 からポート 3022 への対称的な再マッピングが作成されますが、インバウンドとアウトバウンドの両方のトラフィックに明示的に値が設定されます。

```
[DC1-S3]
  NODE_TYPE = VM_Storage_Node

  GRID_NETWORK_IP = 10.1.1.3

  PORT_REMAP = grid/tcp/22/3022
  PORT_REMAP_INBOUND = grid/tcp/3022/22

  ADMIN_IP = 10.1.0.2
```

ストレージノードにオプションで追加できる設定は次のとおりです。

- * DISK * ：デフォルトでは、ストレージノードに対して RangeDB 用に 3 つの 4TB ディスクが割り当てられます。DISK パラメータを使用して、この容量を増やすことができます。例：

```
DISK = INSTANCES=16, CAPACITY=4096
```

- * storage_type * ：すべての新しいストレージノードは、オブジェクトデータとメタデータの両方を格納するようにデフォルトで設定されます（_combined_storage Node）。storage_typeパラメータを使用して、データまたはメタデータのみを格納するようにストレージノードのタイプを変更できます。例：

```
STORAGE_TYPE = data
```

ゲートウェイノード

ゲートウェイノードには次の設定を追加する必要があります。

- * node_name * ： VM_API_Gateway

次のエントリ例は、ゲートウェイノードが 3 つのネットワークすべてに接続される場合を示しています。この例では、構成ファイルのグローバルセクションでクライアントネットワークのパラメータが指定されていないため、ノードに対してそれらのパラメータを指定する必要があります。

```
[DC1-G1]
  NODE_TYPE = VM_API_Gateway

  GRID_NETWORK_IP = 10.1.0.5
  ADMIN_NETWORK_IP = 10.3.0.5

  CLIENT_NETWORK_CONFIG = STATIC
  CLIENT_NETWORK_TARGET = SG Client Network
  CLIENT_NETWORK_MASK = 255.255.255.0
  CLIENT_NETWORK_GATEWAY = 10.4.0.1
  CLIENT_NETWORK_IP = 10.4.0.5

  ADMIN_IP = 10.1.0.2
```

非プライマリ管理ノード

非プライマリ管理ノードには次の設定を追加する必要があります。

- * node_type * ： VM_Admin_Node
- * Admin_role * ：非プライマリ

次のエントリ例は、非プライマリ管理ノードがクライアントネットワークに接続されない場合を示しています。

```
[DC2-ADM1]
  ADMIN_ROLE = Non-Primary
  NODE_TYPE = VM_Admin_Node

  GRID_NETWORK_TARGET = SG Grid Network
  GRID_NETWORK_IP = 10.1.0.6
  ADMIN_NETWORK_IP = 10.3.0.6

  ADMIN_IP = 10.1.0.2
```

非プライマリ管理ノードにオプションで追加できる設定は次のとおりです。

- * DISK * ：デフォルトでは、管理ノードに対して監査用とデータベース用の 2 つの 200GB ハードディスクが追加で割り当てられます。DISK パラメータを使用して、この容量を増やすことができます。例：

  ```
  DISK = INSTANCES=2, CAPACITY=300
  ```

  管理ノードの場合は、 INSTANCES を必ず 2 にする必要があります。

Bash スクリプトを実行します

VMware vSphereへのStorageGRIDノードの導入を自動化するために、Bashスクリプトと変更したdeploy-vsphere-ovftool.ini構成ファイルを使用できます `deploy-vsphere-ovftool.sh`。

開始する前に

環境に対応した deploy-vsphere-ovftool.ini 構成ファイルを作成しておきます。

Bashスクリプトのヘルプを使用するには、helpコマンドを入力し(`-h/--help`ます）。例：

```
./deploy-vsphere-ovftool.sh -h
```

または

```
./deploy-vsphere-ovftool.sh --help
```

手順

1. Bash スクリプトの実行に使用する Linux マシンにログインします。
2. インストールアーカイブを展開したディレクトリに移動します。

   例：

   ```
   cd StorageGRID-Webscale-version/vsphere
   ```

3. グリッドノードをすべて導入する場合は、使用する環境に適したオプションを指定して Bash スクリプトを実行します。

   例：

   ```
   ./deploy-vsphere-ovftool.sh --username=user --password=pwd ./deploy-vsphere-ovftool.ini
   ```

4. エラーのために導入できなかったグリッドノードがある場合は、エラーを解決し、そのノードだけを対象に Bash スクリプトを再実行します。

   例：

   ```
   ./deploy-vsphere-ovftool.sh --username=user --password=pwd --single-node="DC1-S3" ./deploy-vsphere-ovftool.ini
   ```

各ノードのステータスが「PASSED」になると、導入は完了です。

```
Deployment Summary
+------------------------------+----------+----------------------+
| node                         | attempts | status               |
+------------------------------+----------+----------------------+
| DC1-ADM1                     |        1 | Passed               |
| DC1-G1                       |        1 | Passed               |
| DC1-S1                       |        1 | Passed               |
| DC1-S2                       |        1 | Passed               |
| DC1-S3                       |        1 | Passed               |
+------------------------------+----------+----------------------+
```

StorageGRID の設定を自動化

グリッドノードを導入したら、 StorageGRID システムの設定を自動化できます。

開始する前に

- インストールアーカイブにある次のファイルの場所を確認しておきます。

ファイル名	製品説明
configure-storagegrid.py	設定を自動化するための Python スクリプト
storagegrid-sample.json を設定します	スクリプトで使用する構成ファイルの例
storagegrid-bank.json を設定する	スクリプトで使用する空の構成ファイルです

- 構成ファイルを作成しておき `configure-storagegrid.json`ます。このファイルを作成するには（`configure-storagegrid.sample.json`、サンプル構成ファイル）または空の構成ファイル）(`configure-storagegrid.blank.json`を変更します。

> 変更したファイルのパスワードセクションから管理パスワードとプロビジョニングパスフレーズを保存します。 `configure-storagegrid.json`構成ファイルを安全な場所に保管します。これらのパスワードは、インストール、拡張、およびメンテナンスの手順に必要です。変更したファイルもバックアップする必要があります `configure-storagegrid.json`構成ファイルを作成して安全な場所に保存します。

タスクの内容

Pythonスクリプトと `configure-storagegrid.json`グリッド構成ファイルを使用して、StorageGRID システムの設定を自動化できます `configure-storagegrid.py`。

> また、 Grid Manager またはインストール API を使用してシステムを設定することもできます。

手順

1. Python スクリプトを実行するために使用する Linux マシンにログインします。

2. インストールアーカイブを展開したディレクトリに移動します。

   例：

   ```
   cd StorageGRID-Webscale-version/platform
   ```

   `platform`は、debs、rpm、またはvsphereです。

3. Python スクリプトを実行し、作成した構成ファイルを使用します。

   例：

   ```
   ./configure-storagegrid.py ./configure-storagegrid.json --start-install
   ```

結果

設定プロセス中にリカバリパッケージ `.zip`ファイルが生成され、インストールおよび設定プロセスを実行するディレクトリにダウンロードされます。グリッドノードで障害が発生した場合に StorageGRID システムをリカバリできるようにするために、リカバリパッケージファイルをバックアップする必要があります。たとえば、バックアップされたセキュアなネットワーク上の場所や、安全なクラウドストレージ上の場所にコピーします。

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

ランダムパスワードを生成するように指定した場合は、ファイルを開き `Passwords.txt`、StorageGRIDシステムへのアクセスに必要なパスワードを探します。

```
#######################################################################
##### The StorageGRID "Recovery Package" has been downloaded as: #####
#####           ./sgws-recovery-package-994078-rev1.zip           #####
#####   Safeguard this file as it will be needed in case of a     #####
#####                 StorageGRID node recovery.                  #####
#######################################################################
```

StorageGRID システムがインストールおよび設定されると、確認メッセージが表示されます。

```
StorageGRID has been configured and installed.
```

関連情報

- "Grid Manager に移動します"
- "インストールREST API"

StorageGRID用のVMware環境に関する情報を収集

グリッドノードを導入する前に、ネットワーク設定と VMware 環境に関する情報を収集する必要があります。

> 一部のノードだけを先にインストールしてから、一部のノードだけをインストールするよりも、すべてのノードを 1 つのインストールする方が効率的です。

VMware の情報

導入環境にアクセスし、 VMware 環境に関する情報、グリッドネットワーク、管理ネットワーク、クライアントネットワーク用に作成されたネットワークに関する情報、およびストレージノードで使用する予定のストレージボリュームタイプに関する情報を収集する必要があります。

VMware 環境に関する次の情報を収集する必要があります。

- 導入を完了するための適切な権限を持つ VMware vSphere アカウントのユーザ名とパスワード。
- 各StorageGRIDノード仮想マシンのホスト、データストア、およびネットワーク構成の情報。

> VMware のライブ vMotion を使用すると仮想マシンのクロック時間が急に進むため、この機能はどのタイプのグリッドノードでもサポートされていません。まれにではありますが、クロック時間が不正確だとデータや設定の更新が失われることがあります。

グリッドネットワークの情報

StorageGRID グリッドネットワーク（必須）用に作成された VMware ネットワークに関する次の情報を収集する必要があります。

- ネットワーク名。
- 静的または DHCP のいずれかの IP アドレスの割り当てに使用する方法。
  - 静的 IP アドレスを使用する場合は、各グリッドノードのネットワークに関する必須の詳細情報（ IP アドレス、ゲートウェイ、ネットワークマスク）。
  - DHCPを使用している場合は、グリッドネットワークでのプライマリ管理ノードのIPアドレス。詳細については、を参照してください "グリッドノードによるプライマリ管理ノードの検出" 。

管理ネットワークの情報

ノードがオプションの StorageGRID 管理ネットワークに接続される場合は、このネットワーク用に作成された VMware ネットワークに関する次の情報を収集する必要があります。

- ネットワーク名。
- 静的または DHCP のいずれかの IP アドレスの割り当てに使用する方法。
  - 静的 IP アドレスを使用する場合は、各グリッドノードのネットワークに関する必須の詳細情報（ IP アドレス、ゲートウェイ、ネットワークマスク）。
  - DHCPを使用している場合は、グリッドネットワークでのプライマリ管理ノードのIPアドレス。詳細

については、を参照してください "グリッドノードによるプライマリ管理ノードの検出" 。

- 管理ネットワークの外部サブネットリスト（ ESL ）。

クライアントネットワークの情報

ノードがオプションの StorageGRID クライアントネットワークに接続される場合は、このネットワーク用に作成された VMware ネットワークに関する次の情報を収集する必要があります。

- ネットワーク名。
- 静的または DHCP のいずれかの IP アドレスの割り当てに使用する方法。
- 静的 IP アドレスを使用する場合は、各グリッドノードのネットワークに関する必須の詳細情報（ IP アドレス、ゲートウェイ、ネットワークマスク）。

追加のインターフェイスに関する情報

ノードのインストール後に、 vCenter で VM にトランクインターフェイスまたはアクセスインターフェイスを追加することもできます。たとえば、管理ノードまたはゲートウェイノードにトランクインターフェイスを追加して、 VLAN インターフェイスを使用して複数のアプリケーションまたはテナントに属するトラフィックを分離できます。または、ハイアベイラビリティ（ HA ）グループで使用するアクセスインターフェイスを追加することもできます。

追加したインターフェイスは、 VLAN インターフェイスのページおよび Grid Manager の HA グループのページに表示されます。

- トランクインターフェイスを追加する場合は、新しい親インターフェイスごとに 1 つ以上の VLAN インターフェイスを設定します。を参照して "VLAN インターフェイスを設定します"
- アクセスインターフェイスを追加した場合は、 HA グループに直接追加する必要があります。を参照して "ハイアベイラビリティグループを設定する"

仮想ストレージノードのストレージボリューム

仮想マシンベースのストレージノードに関する次の情報を収集する必要があります。

- 追加するストレージボリューム（ストレージLUN）の数とサイズ。を参照してください。"ストレージとパフォーマンスの要件"

グリッドの設定情報

グリッドを設定するための情報を収集する必要があります。

- Grid ライセンス
- Network Time Protocol （ NTP ；ネットワークタイムプロトコル）サーバの IP アドレス
- DNSサーバのIPアドレス

Linux デプロイメント用の **StorageGRID** ノード構成ファイルを作成する

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

アンスノードには使用されません。

「Linux」は、RHEL、Ubuntu、または Debian のデプロイメントを指します。サポートされているバージョンのリストについては、 "NetApp Interoperability Matrix Tool（IMT）" 。

ノード構成ファイルの場所

各StorageGRIDノードの構成ファイルを、そのノードを実行するホストのディレクトリに配置し `/etc/storagegrid/nodes` ます。たとえば、`HostA`で管理ノード、ゲートウェイノード、およびストレージノードを`1`つずつ実行する場合は、`3`つのノード構成ファイルを`HostA`のに配置する必要があります `/etc/storagegrid/nodes`。

構成ファイルは、 vim や nano などのテキストエディタを使用して各ホストで直接作成することも、別の場所で作成して各ホストに移動することもできます。

ノード構成ファイルの命名

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

ノード名は次のルールに従って付ける必要があります。

- 一意でなければなりません
- 1 文字目はアルファベットにする必要があります
- A~Z と a~z のアルファベットを使用できます
- 0~9 の数字を使用できます
- 1 つまたは複数のハイフン（ `-` ）を含めることができます。
- 拡張子は含めず、32文字以下にする必要があります。 `.conf`

これらの命名規則に従わない内のファイルは、 `/etc/storagegrid/nodes`ホストサービスによって解析されません。

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

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

たとえば、データセンター1の最初の管理ノードにを使用し、 `dc2-sn3.conf` データセンター`2`の`3`番目のストレージノードにを使用できます `dc1-adm1.conf`。ただし、すべてのノード名がルールに従っていれば、別の名前にしてもかまいません。

ノード構成ファイルの内容

構成ファイルには、1行に1つのキーと1つの値を持つキーと値のペアが含まれています。キーと値のペアごとに、次のルールに従ってください。

- キーと値は等号で区切る必要があり(`=`ます）、およびオプションの空白文字で区切る必要があります。
- キーにスペースを含めることはできません。

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

次の表に、サポートされているすべてのキーの値を示します。各キーには、次のいずれかの指定があります。

- 必須：すべてのノードまたは指定したノードタイプに必須
- ベストプラクティス：オプション（推奨されますが）
- オプション：すべてのノードでオプション

管理ネットワークキー

ADMIN_IP を指定します

値	名称
Linux ベースのノードをインストールするために使用する管理ノードのグリッド ネットワーク IPv4 アドレス。リカバリの場合、プライマリ管理ノードの IP が使用可能な場合はそれを使用し、そうでない場合は非プライマリ管理ノードの IP を使用します。このパラメータを省略すると、ノードは mDNS を使用してプライマリ管理ノードを検出しようとします。 "グリッドノードによるプライマリ管理ノードの検出"	ベストプラクティス

ADMIN_NETWORK_CONFIG

値	名称
DHCP 、 STATIC 、または DISABLED	オプション

ADMIN_NETWORK_ESL

値	名称
このノードが管理ネットワークゲートウェイを使用して通信するサブネット（CIDR表記）をカンマで区切ったリスト。 例： `172.16.0.0/21,172.17.0.0/21`	オプション

ADMIN_NETWORK_GATEWAY

値	名称

このノードのローカルの管理ネットワークゲートウェイの IPv4 アドレス。ADMIN_NETWORK_IP および ADMIN_NETWORK_MASK で定義されるサブネットに属している必要があります。この値は、 DHCP によって設定されたネットワークでは無視されます。
 	
例：
 	
`1.1.1.1`
 	
`10.224.4.81`
	を指定した場合は必須 `ADMIN_NETWORK_ESL`です。それ以外の場合はオプション。

ADMIN_NETWORK_IP

値	名称

このノードの管理ネットワークにおける IPv4 アドレス。このキーが必要なのは、ADMIN_NETWORK_CONFIG = STATICの場合だけです。それ以外の値の場合は指定しないでください。
 	
例：
 	
`1.1.1.1`
 	
`10.224.4.81`
	ADMIN_NETWORK_CONFIG = STATICの場合に必要です。
	
	それ以外の場合はオプション。

ADMIN_NETWORK_MAC

値	名称
コンテナ内の管理ネットワークインターフェイスの MAC アドレス。 このフィールドはオプションです。省略すると、 MAC アドレスが自動的に生成されます。 6 つの 16 進数値をコロンで区切って指定する必要があります。 例： `b2:9c:02:c2:27:10`	オプション

ADMIN_NETWORK_MASK

値	名称

このノードの管理ネットワークにおける IPv4 ネットマスク。ADMIN_NETWORK_CONFIG = STATICの場合はこのキーを指定します。それ以外の値の場合は指定しないでください。
 	
例：
 	
`255.255.255.0`
 	
`255.255.248.0`
	ADMIN_NETWORK_IPを指定し、ADMIN_NETWORK_CONFIG = STATICの場合は必須です。
	
	それ以外の場合はオプション。

ADMIN_NETWORK_MTU を指定します

値	名称

このノードの管理ネットワークでの最大伝送ユニット（ MTU ）。ADMIN_NETWORK_CONFIG = DHCPの場合は指定しないでください。この値を指定する場合、 1280 ～ 9216 の範囲で指定する必要があります。省略すると、 1500 が使用されます。
 	
ジャンボフレームを使用する場合は、 MTU を 9000 などのジャンボフレームに適した値に設定します。それ以外の場合は、デフォルト値のままにします。
 	
• 重要 * ：ネットワークの MTU 値は、ノードが接続されているスイッチポートに設定された値と一致する必要があります。そうしないと、ネットワークパフォーマンスの問題やパケット損失が発生する可能性があります。
 	
例：
 	
`1500`
 	
`8192`
	オプション

ADMIN_NETWORK_TARGET

値	名称

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

ADMIN_NETWORK_TARGET タイプ

値	名称
DedicatedInterface（これが唯一サポートされている値です。）	オプション

ADMIN_NETWORK_TARGET _TYPE_interface_clone_MAC

値	名称
正しいか間違っているか StorageGRID コンテナで管理ネットワークのホストターゲットインターフェイスの MAC アドレスを使用するには、キーを「 true 」に設定して原因 に設定します。 LinuxのMACクローニングの詳細については、以下を参照してください。"MAC アドレスのクローニングに関する考慮事項と推奨事項"	ベストプラクティス

ADMIN_NETWORK_ROLE

値	名称
プライマリまたは非プライマリ このキーが必要なのは、NODE_TYPE = VM_ADMIN_Nodeの場合のみです。それ以外のタイプのノードの場合は指定しないでください。	NODE_TYPE = VM_Admin_Nodeの場合は必須 それ以外の場合はオプション。

ブロックデバイスキー

BLOBK_DEVICE_AUDIT_logs

値	名称

このノードで監査ログの永続的なストレージに使用するブロックデバイススペシャルファイルのパスと名前。
 	
例：
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-adm1-audit-logs`
	NODE_TYPE = VM_Admin_Nodeのノードに必要です。他のノードタイプの場合は指定しないでください。

block_device_rangedb_nnn

値	名称

このノードでオブジェクトの永続的なストレージに使用するブロックデバイススペシャルファイルのパスと名前。このキーが必要なのは、NODE_TYPE = VM_Storage_Nodeのノードだけです。それ以外のタイプのノードの場合は指定しないでください。
 	
BLOCK_DEVICE_RANGEDB_000のみが必須で、それ以外は省略可能です。BLOCK_DEVICE_RANGEDB_000に指定するブロックデバイスは4TB以上である必要があります。それ以外は4TB未満でもかまいません。
 	
隙間を空けてはいけません。BLOCK_DEVICE_RANGEDB_005を指定する場合は、BLOCK_DEVICE_RANGEDB_004も指定されている必要があります。
 	
• 注 * ：既存の環境との互換性を確保するため、アップグレードされたノードでは 2 桁のキーがサポートされています。
 	
例：
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-sn1-rangedb-000`
	必須：
	
	BLOCK_DEVICE_RANGEDB_000
	
	オプション：
	
	BLOCK_DEVICE_RANGEDB_001
	
	BLOCK_DEVICE_RANGEDB_002
	
	BLOCK_DEVICE_RANGEDB_003
	
	BLOCK_DEVICE_RANGEDB_004
	
	BLOCK_DEVICE_RANGEDB_005
	
	BLOCK_DEVICE_RANGEDB_006
	
	BLOCK_DEVICE_RANGEDB_007
	
	BLOCK_DEVICE_RANGEDB_008
	
	BLOCK_DEVICE_RANGEDB_009
	
	BLOCK_DEVICE_RANGEDB_010
	
	BLOCK_DEVICE_RANGEDB_011
	
	BLOCK_DEVICE_RANGEDB_012
	
	BLOCK_DEVICE_RANGEDB_013
	
	BLOCK_DEVICE_RANGEDB_014
	
	BLOCK_DEVICE_RANGEDB_015

BLOBK_DEVICE_tables

値	名称

このノードでデータベーステーブルの永続的なストレージに使用するブロックデバイススペシャルファイルのパスと名前。このキーが必要なのは、NODE_TYPE = VM_ADMIN_Nodeのノードだけです。それ以外のタイプのノードの場合は指定しないでください。
 	
例：
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-adm1-tables`
	必須

BLOBK_DEVICE_VAR_LOCAL です

値	名称

このノードの永続的ストレージに使用するブロックデバイススペシャルファイルのパスと名前 `/var/local`。
 	
例：
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-sn1-var-local`
	必須

クライアントネットワークキー

CLIENT_NETWORK_CONFIG

値	名称
DHCP 、 STATIC 、または DISABLED	オプション

CLIENT_NETWORK_GATEWAY

値	名称

このノードのローカルのクライアントネットワークゲートウェイの IPv4 アドレス。 CLIENT_NETWORK_IP および CLIENT_NETWORK_MASK で定義されるサブネットに属している必要があります。この値は、 DHCP によって設定されたネットワークでは無視されます。
 	
例：
 	
`1.1.1.1`
 	
`10.224.4.81`
	オプション

CLIENT_NETWORK_IP

値	名称

このノードのクライアントネットワークにおける IPv4 アドレス。
 	
このキーが必要なのは、CLIENT_NETWORK_CONFIG = STATICの場合だけです。それ以外の値の場合は指定しないでください。
 	
例：
 	
`1.1.1.1`
 	
`10.224.4.81`
	client_network_config = staticの場合に必要
	
	それ以外の場合はオプション。

CLIENT_NETWORK_MAC

値	名称
コンテナ内のクライアントネットワークインターフェイスの MAC アドレス。 このフィールドはオプションです。省略すると、 MAC アドレスが自動的に生成されます。 6 つの 16 進数値をコロンで区切って指定する必要があります。 例： `b2:9c:02:c2:27:20`	オプション

CLIENT_NETWORK_MASK

値	名称

このノードのクライアントネットワークにおける IPv4 ネットマスク。
 	
CLIENT_NETWORK_CONFIG = STATICの場合にこのキーを指定します。他の値の場合は指定しないでください。
 	
例：
 	
`255.255.255.0`
 	
`255.255.248.0`
	CLIENT_NETWORK_IPを指定し、CLIENT_NETWORK_CONFIG = STATICの場合は必須
	
	それ以外の場合はオプション。

CLIENT_NETWORK_MTU

値	名称

このノードのクライアントネットワークでの最大伝送ユニット（ MTU ）。CLIENT_NETWORK_CONFIG = DHCPの場合は指定しないでください。この値を指定する場合、 1280 ～ 9216 の範囲で指定する必要があります。省略すると、 1500 が使用されます。
 	
ジャンボフレームを使用する場合は、 MTU を 9000 などのジャンボフレームに適した値に設定します。それ以外の場合は、デフォルト値のままにします。
 	
• 重要 * ：ネットワークの MTU 値は、ノードが接続されているスイッチポートに設定された値と一致する必要があります。そうしないと、ネットワークパフォーマンスの問題やパケット損失が発生する可能性があります。
 	
例：
 	
`1500`
 	
`8192`
	オプション

client_network_target です

値	名称

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

client_network_target_type

値	名称
DedicatedInterface（これはサポートされている唯一の値です。）	オプション

client_network_target_type _interface_clone_MAC

値	名称
正しいか間違っているか クライアントネットワークでホストターゲットインターフェイスの MAC アドレスを使用するには、キーを「 true 」に設定して StorageGRID コンテナを原因 します。 LinuxのMACクローニングの詳細については、以下を参照してください。"MAC アドレスのクローニングに関する考慮事項と推奨事項"	ベストプラクティス

グリッドネットワークキー

GRID_NETWORK_CONFIG

値	名称
STATIC または DHCP 指定しない場合のデフォルトはstaticです。	ベストプラクティス

GRID_NETWORK_GATEWAY

値	名称
このノードのローカルのグリッドネットワークゲートウェイの IPv4 アドレス。 GRID_NETWORK_IP および GRID_NETWORK_MASK で定義されるサブネットに属している必要があります。この値は、 DHCP によって設定されたネットワークでは無視されます。 グリッドネットワークのサブネットが 1 つだけでゲートウェイがない場合は、サブネットの標準のゲートウェイアドレス（ X.Y.Z.1 ）か、このノードの GRID_NETWORK_IP の値を使用します。このどちらかの値にしておけば、以降にグリッドネットワークを拡張するときに処理が簡単になります。	必須

GRID_NETWORK_IP

値	名称

このノードのグリッドネットワークにおける IPv4 アドレス。このキーが必要なのは、GRID_NETWORK_CONFIG = STATICの場合のみです。それ以外の値の場合は指定しないでください。
 	
例：
 	
`1.1.1.1`
 	
`10.224.4.81`
	GRID_NETWORK_CONFIG = STATICの場合は必須
	
	それ以外の場合はオプション。

GRID_NETWORK_MAC

値	名称
コンテナ内のグリッドネットワークインターフェイスの MAC アドレス。 6 つの 16 進数値をコロンで区切って指定する必要があります。 例： `b2:9c:02:c2:27:30`	オプション 省略すると、 MAC アドレスが自動的に生成されます。

GRID_NETWORK_MASK

値	名称

このノードのグリッドネットワークにおける IPv4 ネットマスク。GRID_NETWORK_CONFIG = STATICの場合はこのキーを指定します。それ以外の値の場合は指定しないでください。
 	
例：
 	
`255.255.255.0`
 	
`255.255.248.0`
	GRID_NETWORK_IPを指定し、GRID_NETWORK_CONFIG = STATICを指定した場合に必要です。
	
	それ以外の場合はオプション。

GRID_NETWORK_MTU

値	名称

このノードのグリッドネットワークでの最大伝送ユニット（ MTU ）。GRID_NETWORK_CONFIG = DHCPの場合は指定しないでください。この値を指定する場合、 1280 ～ 9216 の範囲で指定する必要があります。省略すると、 1500 が使用されます。
 	
ジャンボフレームを使用する場合は、 MTU を 9000 などのジャンボフレームに適した値に設定します。それ以外の場合は、デフォルト値のままにします。
 	
• 重要 * ：ネットワークの MTU 値は、ノードが接続されているスイッチポートに設定された値と一致する必要があります。そうしないと、ネットワークパフォーマンスの問題やパケット損失が発生する可能性があります。
• 重要 * ：ネットワークパフォーマンスを最大限に高めるには、すべてのノードのグリッドネットワークインターフェイスで MTU 値がほぼ同じになるように設定する必要があります。個々のノードのグリッドネットワークの MTU 設定に大きな違いがある場合は、 * Grid Network MTU mismatch * アラートがトリガーされます。MTU 値はすべてのネットワークタイプで同じである必要はありません。
 	
例：
 	
`1500`
 	
`8192`
	オプション

GRID_NETWORK_TARGET

値	名称

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

GRID_NETWORK_TARGET タイプ

値	名称
DedicatedInterface（これが唯一サポートされている値です。）	オプション

GRID_NETWORK_TARGET _TYPE_interface_clone_MAC

値	名称
正しいか間違っているか グリッドネットワーク上のホストターゲットインターフェイスの MAC アドレスを使用するには、キーの値を「 true 」に設定して StorageGRID コンテナを原因 に設定します。 LinuxのMACクローニングの詳細については、以下を参照してください。"MAC アドレスのクローニングに関する考慮事項と推奨事項"	ベストプラクティス

インストールパスワードキー（一時）

custom_temporary_password_hash

値	名称
プライマリ管理ノードの場合は、インストール時にStorageGRIDインストールAPIのデフォルトの一時パスワードを設定します。 注：インストールパスワードはプライマリ管理ノードにのみ設定します。別のタイプのノードでパスワードを設定しようとすると、ノード構成ファイルの検証に失敗します。 この値を設定しても、インストールが完了しても効果はありません。 このキーを省略すると、デフォルトでは一時パスワードは設定されません。または、StorageGRIDインストールAPIを使用して一時パスワードを設定することもできます。 8文字以上32文字以下のパスワードの形式のSHA-512パスワードハッシュで `$6$<salt>$<password hash>` ある必要があります `crypt()`。 このハッシュは、SHA-512モードのコマンドなどのCLIツールを使用して生成できます `openssl passwd`。	ベストプラクティス

interfacesキー

interface_target_nnnn

値	名称
このノードに追加するインターフェイスの名前とオプションの概要 。各ノードに複数のインターフェイスを追加できます。 _nnnn_には、追加する各interface_targetエントリに一意の番号を指定します。 値には、ベアメタルホスト上の物理インターフェイスの名前を指定します。その後、必要に応じて、カンマを追加してインターフェイスの概要を指定します。このインターフェイスは、 VLAN インターフェイスのページと HA グループのページに表示されます。 例： `INTERFACE_TARGET_0001=ens256, Trunk` トランクインターフェイスを追加する場合は、 StorageGRID で VLAN インターフェイスを設定する必要があります。アクセスインターフェイスを追加する場合は、そのインターフェイスをHAグループに直接追加できます。VLANインターフェイスを設定する必要はありません。	オプション

最大**RAM**キー

MAXIMUM_RAM

値	名称

このノードに使用を許可する RAM の最大容量。このキーを省略した場合、ノードでメモリは制限されません。本番用のノードについて設定するときは、システム RAM の合計容量よりも 24GB 以上、 16~32GB 以上小さい値を指定してください。
 	
• 注 * ： RAM 値は、ノードの実際のメタデータ用リザーブスペースに影響します。を参照してください"Metadata Reserved Spaceとは何かの概要"。
 	
このフィールドの形式はです *numberunit*。 *unit*`には、、 `k、m、または g`を指定できます `b。
 	
例：
 	
`24g`
 	
`38654705664b`
 	
• 注：このオプションを使用する場合は、 memory cgroups のカーネルサポートを有効にする必要があります。
	オプション

ノードタイプキー

Node_type のように指定します

値	名称
ノードのタイプ： • VM_Admin_Nodeの略 • VM_Storage_Nodeの略 • VM_Archive_Nodeの略 • VM_API_Gateway	必須

ストレージタイプ

値	名称
ストレージノードに含まれるオブジェクトのタイプを定義。詳細については、を参照してください "ストレージノードのタイプ"。このキーが必要なのは、NODE_TYPE = VM_Storage_Nodeのノードだけです。それ以外のタイプのノードの場合は指定しないでください。ストレージタイプ： • 組み合わせ（ Combined ） • データ • メタデータ 注：storage_typeを指定しない場合、ストレージノードタイプはデフォルトで組み合わせ（データとメタデータ）に設定されます。	オプション

ポートの再マッピングキー

ポート再マッピングのサポートは非推奨であり、将来のリリースでは削除される予定です。再マップされたポートを削除するには、"ベアメタルホストでのポートの再マッピングを削除します" 。

PORT_REMAP を参照してください

値	名称
ノードが内部でのグリッドノードの通信または外部との通信に使用するポートを再マッピングします。ポートの再マッピングが必要になるのは、またはの説明に従って、StorageGRIDで使用される1つ以上のポートがエンタープライズネットワークポリシーによって制限されている場合です。"内部でのグリッドノードの通信""外部との通信" 重要：ロードバランサエンドポイントの設定に使用する予定のポートを再マッピングしないでください。 • 注： PORT_REMAP のみを設定すると、指定したマッピングがインバウンド通信とアウトバウンド通信の両方に使用されます。PORT_REMAP_INBOUND を併せて指定した場合は、PORT_REMAP がアウトバウンド通信のみに適用されます。 使用される形式は、 `*network type*/*protocol*/*default port used by grid node*/*new port*` です。 `*network type*` はgrid、admin、またはclient、 `*protocol*` はtcpまたはudpです。 例： `PORT_REMAP = client/tcp/18082/443` カンマで区切ったリストを使用して複数のポートを再マッピングすることもできます。 例： `PORT_REMAP = client/tcp/18082/443, client/tcp/18083/80`	オプション

PORT_REMAP_INBOUND

値	名称
指定したポートのインバウンド通信を再マッピングします。PORT_REMAP_INBOUNDを指定し、PORT_REMAPに値を指定しなかった場合、ポートのアウトバウンド通信は変更されません。 重要：ロードバランサエンドポイントの設定に使用する予定のポートを再マッピングしないでください。 使用される形式は、 `*network type*/*protocol*/*remapped port*/*default port used by grid node*` です。 `*network type*` はgrid、admin、またはclient、 `*protocol*` はtcpまたはudpです。 例： `PORT_REMAP_INBOUND = grid/tcp/3022/22` カンマで区切った複数のインバウンドポートを再マッピングすることもできます。 例： `PORT_REMAP_INBOUND = grid/tcp/3022/22, admin/tcp/3022/22`	オプション

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

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

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

プライマリ管理ノードの自動検出は、マルチキャストドメインネームシステム（mDNS）を使用して実行されます。プライマリ管理ノードは、最初に起動されるときに、 mDNS を使用してそのノードの IP アドレスを公開します。同じサブネット上の他のノードは、この IP アドレスを自動的に照会して取得します。ただし、通常、マルチキャストIPトラフィックはサブネット間でルーティングできないため、他のサブネット上のノードはプライマリ管理ノードのIPアドレスを直接取得できません。

自動検出を使用する場合：

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

VMware vSphereを使用して**StorageGRID**の仮想マシンとしてグリッドノードを導入

VMware vSphere Web Client を使用して、各グリッドノードを仮想マシンとして導入します。導入時に、各グリッドノードが作成されて、 1 つ以上の StorageGRID ネットワークに接続されます。

StorageGRIDアプライアンスストレージノードを導入する必要がある場合は、を参照してください "アプライアンスストレージノードを導入する"。

必要に応じて、ノードポートを再マッピングしたり、ノードの CPU やメモリの設定を増やしたりして、電源をオンにすることができます。

開始する前に

- 方法を確認し"設置を計画して準備"、ソフトウェア、CPUとRAM、ストレージとパフォーマンスの要件を把握しておく必要があります。
- VMware vSphere ハイパーバイザーについて理解し、この環境で仮想マシンの導入を経験している必要があります。

この `open-vm-tools`パッケージは、VMware Toolsに似たオープンソースの実装であり、StorageGRID仮想マシンに含まれています。VMware Toolsを手動でインストールする必要はありません。

- VMware 用の正しいバージョンの StorageGRID インストールアーカイブをダウンロードして展開しておきます。

拡張またはリカバリ処理の一環として新しいノードを導入する場合は、グリッドで現在実行されているバージョンの StorageGRID を使用する必要があります。

- StorageGRID仮想マシンディスク(`.vmdk`）ファイルが必要です。

```
NetApp-SG-version-SHA.vmdk
```

- 導入するグリッドノードのタイプごとにファイルと `.mf`ファイルを用意しておき `.ovf`ます。

ファイル名	製品説明
vsphere-primary-admin.ovf vsphere-primary-admin.mf	プライマリ管理ノードのテンプレートファイルとマニフェストファイル。
vsphere-non-primary-admin.ovf vsphere-non-primary-admin.mf	非プライマリ管理ノードのテンプレートファイルとマニフェストファイル。
vsphere-storage.ovf vsphere-storage.mf	ストレージノードのテンプレートファイルとマニフェストファイル。
vsphere-gateway.ovf vsphere-gateway.mf	ゲートウェイノードのテンプレートファイルとマニフェストファイル。

- `.vdmk`、 `.ovf`、および `.mf`のファイルはすべて同じディレクトリにあります。
- 障害ドメインを最小限に抑えるための計画が必要です。たとえば、すべてのゲートウェイノードを単一のvSphere ESXiホストに導入することは避けてください。

本番環境では、1台の仮想マシンで複数のストレージノードを実行しないでください。許容できない障害ドメインの問題が発生する場合は、同じESXiホストで複数の仮想マシンを実行しないでください。

- 拡張またはリカバリ処理でノードを導入する場合は、またはが必要"StorageGRID システムの拡張手順""リカバリとメンテナンスの手順"です。
- NetApp ONTAP システムからストレージが割り当てられた仮想マシンとしてStorageGRID ノードを導入する場合は、ボリュームでFabricPool 階層化ポリシーが有効になっていないことを確認しておきます。たとえば、StorageGRIDノードがVMwareホストで仮想マシンとして実行されている場合は、そのノードのデータストアを作成するボリュームでFabricPool階層化ポリシーが有効になっていないことを確認してください。StorageGRIDノードで使用するボリュームでFabricPool階層化を無効にすると、トラブルシューティングとストレージの処理が簡単になります。

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

タスクの内容

最初に VMware ノードを導入するとき、拡張時に新しい VMware ノードを追加するとき、またはリカバリ処理の一環として VMware ノードを交換するときは、次の手順に従います。手順に記載されている場合を除き、ノードの導入手順は、管理ノード、ストレージノード、ゲートウェイノードを含むすべてのタイプのノードで同じです。

新しい StorageGRID システムを設置する場合は、次の手順を実行します。

- ノードは任意の順序で導入できます。
- 各仮想マシンがグリッドネットワーク経由でプライマリ管理ノードに接続できることを確認する必要があります。
- グリッドを設定する前に、すべてのグリッドノードを導入する必要があります。

拡張またはリカバリ処理を実行する場合は、次の手順を実行します。

- 新しい仮想マシンがグリッドネットワーク経由で他のすべてのノードに接続できることを確認する必要があります。

ノードのポートを再マッピングする必要がある場合は、ポートの再マッピングの設定が完了するまで新しいノードの電源をオンにしないでください。

ポート再マッピングのサポートは非推奨であり、将来のリリースでは削除される予定です。再マップされたポートを削除するには、"ベアメタルホストでのポートの再マッピングを削除します" 。

手順

1. vCenter を使用して OVF テンプレートを導入

   URL を指定する場合は、次のファイルを含むフォルダを指定します。それ以外の場合は、ローカルディレクトリから各ファイルを選択します。

   ```
   NetApp-SG-version-SHA.vmdk
   vsphere-node.ovf
   vsphere-node.mf
   ```

   たとえば、導入する最初のノードがこのファイルに含まれている場合は、次のファイルを使用して StorageGRID システムのプライマリ管理ノードを導入します。

   ```
   NetApp-SG-version-SHA.vmdk
   vsphere-primary-admin.ovf
   vsphere-primary-admin.mf
   ```

2. 仮想マシンの名前を指定します。

   標準的には、仮想マシンとグリッドノードに同じ名前を使用します。

3. 仮想マシンを適切な vApp またはリソースプールに配置します。
4. プライマリ管理ノードを導入する場合は、エンドユーザライセンス契約を読んで同意します。

   vCenter のバージョンによっては、使用する手順の順序は、エンドユーザライセンス契約を承諾し、仮想マシンの名前を指定し、データストアを選択する場合とで異なります。

5. 仮想マシンのストレージを選択します。

   リカバリ処理の一環としてノードを導入する場合は、の手順に従って、ストレージリカバリ手順新しい仮想ディスクの追加、障害が発生したグリッドノードからの仮想ハードディスクの再接続、またはその両方を行います。

   ストレージノードを導入する際は、ストレージボリュームを 3 個以上使用し、各ストレージボリュームのサイズを 4TB 以上にします。ボリューム 0 に少なくとも 4TB 割り当てる必要があります。

   > ストレージノードの .ovf ファイルは、ストレージ用の複数の VMDK を定義します。これらの VMDK がストレージ要件を満たしていない場合は、ノードの電源を入れる前に、それらの VMDK を削除し、ストレージに適切な VMDK または RDM を割り当てる必要があります。VMware 環境で一般に使用され、管理も容易であるのは VMDK ですが、大きなオブジェクトサイズ（たとえば 100MB 超）を使用するワークロードのパフォーマンスは RDM の方が高くなります。

   > 一部の StorageGRID 環境では、一般的な仮想ワークロードよりも大容量のアクティブなストレージボリュームを使用する場合があります。パフォーマンスを最適化するために、などの一部のハイパーバイザーパラメータの調整が必要になる場合があります `MaxAddressableSpaceTB`。パフォーマンスが低下する場合は、仮想化のサポートリソースに問い合わせて、ワークロード固有の構成調整によって環境がメリットを受けるかどうかを確認してください。

6. ネットワークを選択します。

   各ソースネットワークのデスティネーションネットワークを選択して、ノードで使用する StorageGRID ネットワークを決定します。

   - グリッドネットワークは必須です。vSphere 環境でデスティネーションネットワークを選択する必要があります。+グリッドネットワークは、すべての内部StorageGRIDトラフィックに使用されます。グリッド内のすべてのノードが、すべてのサイトとサブネットにわたって接続されます。グリッドネットワーク上のすべてのノードが他のすべてのノードと通信できる必要があります。
   - 管理ネットワークを使用する場合は、 vSphere 環境で別のデスティネーションネットワークを選択します。管理ネットワークを使用しない場合は、グリッドネットワークに対して選択したデスティネーションと同じデスティネーションを選択します。
   - クライアントネットワークを使用する場合は、 vSphere 環境で別のデスティネーションネットワークを選択します。クライアントネットワークを使用しない場合は、グリッドネットワークに対して選択したデスティネーションと同じデスティネーションを選択します。
   - 管理ネットワークまたはクライアントネットワークを使用する場合は、ノードが同じ管理ネットワークまたはクライアントネットワーク上にある必要はありません。

7. [テンプレートのカスタマイズ]*で、必要なStorageGRIDノードプロパティを構成します。

   a. ノード名 * を入力します。

      グリッドノードをリカバリする場合は、リカバリするノードの名前を入力する必要があります。

   b. 新しいノードがグリッドに追加される前にVMコンソールまたはStorageGRIDインストールAPIにアクセスしたり、SSHを使用したりできるように、*[Temporary installation password]*ドロップダウンを使用して一時的なインストールパスワードを指定します。

      一時インストールパスワードは、ノードのインストール時にのみ使用されます。グリッドに追加されたノードに"ノードのコンソールパスワード"は、リカバリパッケージのファイルに含まれているを使用してアクセスできます。 `Passwords.txt`

      - ノード名を使用：*ノード名*フィールドに入力した値は、一時的なインストールパスワードとして使用されます。
      - カスタムパスワードを使用：カスタムパスワードを一時的なインストールパスワードとして使用します。
      - パスワードを無効にする:一時的なインストールパスワードは使用されません。インストールの問題をデバッグするためにVMにアクセスする必要がある場合は、を参照してください"インストールに関する問題のトラブルシューティング"。

   c. *カスタムパスワードを使用*を選択した場合は、*カスタムパスワード*フィールドで使用する一時インストールパスワードを指定します。

   d. * グリッドネットワーク（ eth0 ） * セクションで、 * グリッドネットワーク IP 設定 * に静的または DHCP を選択します。

      - 静的を選択した場合は、 * グリッドネットワーク IP * 、 * グリッドネットワークマスク * 、 * グリッドネットワークゲートウェイ * 、 * グリッドネットワーク MTU * を入力します。
      - DHCP を選択した場合は、 * グリッドネットワーク IP * 、 * グリッドネットワークマスク * 、 * グリッドネットワークゲートウェイ * が自動的に割り当てられます。

   e. 「 * Primary Admin IP * 」フィールドに、グリッドネットワークのプライマリ管理ノードの IP アドレスを入力します。

      プライマリ管理ノードの IP アドレスを省略すると、プライマリ管理ノードまたは ADMIN_IP が設定された少なくとも 1 つのグリッドノードが同じサブネットにある場合は、 IP アドレスが自動的に検出されます。ただし、ここでプライマリ管理ノードの IP アドレスを設定することを推奨します。

   f. 「 * Admin Network （ eth1 ） * 」セクションで、「 * Admin network IP configuration * 」に対して「 static 」、「 dhcp 」、または「 disabled 」を選択します。

      - 管理ネットワークを使用しない場合は、[DISABLED]を選択し、[Admin Network IP]に「* 0.0.0.0 *」と入力します。他のフィールドは空白のままにすることができます。
      - 静的を選択した場合は、 * 管理ネットワーク IP * 、 * 管理ネットワークマスク * 、 * 管理ネットワークゲートウェイ * 、 * 管理ネットワーク MTU * を入力します。
      - 静的を選択した場合は、 * 管理ネットワークの外部サブネットリスト * を入力します。ゲートウェイも設定する必要があります。
      - DHCP を選択した場合は、 * 管理ネットワーク IP * 、 * 管理ネットワークマスク * 、および * 管理ネットワークゲートウェイ * が自動的に割り当てられます。

g. クライアントネットワーク（ eth2 ） * セクションで、 * クライアントネットワーク IP 構成 * の静的、 DHCP 、または無効を選択します。

- クライアントネットワークを使用しない場合は、[DISABLED]を選択し、[Client Network IP]に「* 0.0.0.0 *」と入力します。他のフィールドは空白のままにすることができます。
- 静的を選択した場合は、 * クライアントネットワーク IP * 、 * クライアントネットワークマスク * 、 * クライアントネットワークゲートウェイ * 、および * クライアントネットワーク MTU * を入力します。
- DHCP を選択した場合は、 * クライアントネットワーク IP * 、 * クライアントネットワークマスク * 、および * クライアントネットワークゲートウェイ * が自動的に割り当てられます。

8. 仮想マシンの設定を確認し、必要な変更を行います。
9. 完了する準備ができたら、 [完了] を選択して仮想マシンのアップロードを開始します。
10. [[step_recovery_storage] - リカバリ処理の一環としてこのノードを導入し、フルノードリカバリではない場合は、導入の完了後に次の手順を実行します。

a. 仮想マシンを右クリックし、 * 設定の編集 * を選択します。

b. ストレージに指定されている各デフォルト仮想ハードディスクを選択し、 * 削除 * を選択します。

c. データリカバリの状況に応じて、ストレージ要件に従って新しい仮想ディスクを追加し、以前に削除した障害グリッドノードから保存した仮想ハードディスクを再接続するか、またはその両方を実行します。

次の重要なガイドラインに注意してください。

- 新しいディスクを追加する場合は、ノードのリカバリ前に使用していたものと同じタイプのストレージデバイスを使用する必要があります。
- ストレージノードの .ovf ファイルは、ストレージ用の複数の VMDK を定義します。これらの VMDK がストレージ要件を満たしていない場合は、ノードの電源を入れる前に、それらの VMDK を削除し、ストレージに適切な VMDK または RDM を割り当てる必要があります。VMware 環境で一般に使用され、管理も容易であるのは VMDK ですが、大きなオブジェクトサイズ（たとえば 100MB 超）を使用するワークロードのパフォーマンスは RDM の方が高くなります。

11. このノードで使用するポートを再マッピングする必要がある場合は、次の手順を実行します。

エンタープライズネットワークポリシーによって、StorageGRID が使用する1つ以上のポートへのアクセスが制限されている場合は、ポートを再マッピングする必要があります。StorageGRID が使用するポートについては、"ネットワークのガイドライン"を参照してください。

ロードバランサエンドポイントで使用されるポートは再マッピングしないでください。

a. 新しい VM を選択します。

b. [構成] タブで、 [* 設定 * > * vApp オプション *] を選択します。vapp Options * の場所は、 vCenter のバージョンによって異なります。

c. プロパティ * テーブルで、 PORT_REMAP_INBOUND および PORT_REMAP を確認します。

d. ポートのインバウンド通信とアウトバウンド通信の両方を対称的にマッピングするには、 * PORT_REMAP * を選択します。

ポート再マッピングのサポートは非推奨であり、将来のリリースでは削除される予定です。再マップされたポートを削除するには、"ベアメタルホストでのポートの再マッピングを削除します" 。

PORT_REMAP のみを設定すると、インバウンド通信とアウトバウンド通信の両方で環境 を指定したマッピングが適用されます。PORT_REMAP_INBOUND を併せて指定した場合は、 PORT_REMAP がアウトバウンド通信のみに適用されます。

i. 「 * 値の設定 * 」を選択します。

ii. ポートマッピングを入力します。

```
<network type>/<protocol>/<default port used by grid node>/<new port>
```

`<network type>`はgrid、admin、またはclientで、 `<protocol>`はtcpまたはudpです。

たとえば、 ssh トラフィックをポート 22 からポート 3022 に再マッピングするには、次のように入力します。

```
client/tcp/22/3022
```

カンマで区切ったリストを使用して複数のポートを再マッピングできます。

例：

```
client/tcp/18082/443, client/tcp/18083/80
```

i. 「* OK *」を選択します。

e. ノードへのインバウンド通信に使用するポートを指定するには、 * port_remap_inbound * を選択します。

PORT_REMAP_INBOUNDを指定し、PORT_REMAPに値を指定しなかった場合、ポートのアウトバウンド通信は変更されません。

i. 「 * 値の設定 * 」を選択します。

ii. ポートマッピングを入力します。

```
<network type>/<protocol>/<remapped inbound port>/<default inbound port
used by grid node>
```

`<network type>`はgrid、admin、またはclientで、 `<protocol>`はtcpまたはudpです。

たとえば、ポート 3022 に送信されるインバウンドの SSH トラフィックを再マッピングしてグリッドノードがポート 22 で受信するようにするには、次のように入力します。

```
client/tcp/3022/22
```

カンマで区切った複数のインバウンドポートを再マッピングできます。

例：

```
grid/tcp/3022/22, admin/tcp/3022/22
```

i. 「 * OK 」を選択します

12. ノードの CPU またはメモリをデフォルトの設定から増やす場合は、次の手順を実行します。

a. 仮想マシンを右クリックし、 * 設定の編集 * を選択します。

b. CPU の数またはメモリの容量を必要に応じて変更します。

[メモリ予約 *] を、仮想マシンに割り当てられた * メモリ * と同じサイズに設定します。

c. 「* OK *」を選択します。

13. 仮想マシンの電源をオンにします。

終了後

このノードを拡張またはリカバリ用手順 の一部として導入した場合は、その手順に戻って手順 を完了します。

Linux上のStorageGRIDノードの設定ファイルの例

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

「Linux」は、RHEL、Ubuntu、または Debian のデプロイメントを指します。サポートされているバージョンのリストについては、 "NetApp Interoperability Matrix Tool（IMT）" 。

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

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

プライマリ管理ノードの例

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

- ファイルの内容の例： *

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Primary
TEMPORARY_PASSWORD_TYPE = Use custom password
CUSTOM_TEMPORARY_PASSWORD = Passw0rd
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adm1-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adm1-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adm1-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.2
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1

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

ストレージノードの例

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

- ファイルの内容の例： *

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

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

ゲートウェイノードの例

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

- ファイルの内容の例： *

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

非プライマリ管理ノードの例

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

- ファイルの内容の例： *

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

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

Linux での StorageGRID 設定を検証する

StorageGRIDノードごとに構成ファイルをに作成したら `/etc/storagegrid/nodes`、それらのファイルの内容を検証する必要があります。

「Linux」は、RHEL、Ubuntu、または Debian のデプロイメントを指します。サポートされているバージョンのリストについては、 "NetApp Interoperability Matrix Tool（IMT）" 。

構成ファイルの内容を検証するには、各ホストで次のコマンドを実行します。

```
sudo storagegrid node validate all
```

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

メタデータのみのノードでLUNを1つだけ使用している場合は、警告メッセージが表示されても無視してかまいません。

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

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

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

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

Linuxで**StorageGRID**ホストサービスを開始します

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

「Linux」は、RHEL、Ubuntu、または Debian のデプロイメントを指します。サポートされているバージョンのリストについては、 "NetApp Interoperability Matrix Tool（IMT）" 。

手順

1. 各ホストで次のコマンドを実行します。

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

2. 次のコマンドを実行して、導入の進行状況を確認します。

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

3. いずれかのノードのステータスが「Not Running」または「Stopped」になった場合は、次のコマンドを実行します。

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

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

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

StorageGRID インストール **REST API** について学ぶ

StorageGRID には、インストールタスクを実行するための StorageGRID インストール API が用意されています。

API のドキュメントは、 Swagger オープンソース API プラットフォームで提供されています。Swagger では、ユーザインターフェイスを使用してパラメータやオプションを変更した場合の API の動作を確認しながら、 API の開発を進めることができます。このドキュメントは、標準的なWebテクノロジとJSONデータ形式に精通していることを前提としています。

APIドキュメントWebページで実行するAPI処理はすべてライブ処理です。設定データやその他のデータを誤って作成、更新、または削除しないように注意してください。

各 REST API コマンドは、 API の URL 、 HTTP アクション、必須またはオプションの URL パラメータ、および想定される API 応答で構成されます。

StorageGRID インストール **API**

StorageGRID インストールAPIは、StorageGRID システムを最初に設定するとき、およびプライマリ管理ノードのリカバリを実行する必要がある場合にのみ使用できます。インストール API には、 Grid Manager から HTTPS 経由でアクセスできます。

APIドキュメントにアクセスするには、プライマリ管理ノードでインストールWebページに移動し、メニューバーから*>[APIドキュメント]*を選択します。

StorageGRID インストール API には次のセクションがあります。

- **config**：製品のリリースおよびAPIのバージョンに関連する操作。製品のリリースバージョンと、そのリリースでサポートされているAPIの主要バージョンを一覧表示できます。
- **grid**：グリッドレベルの設定操作。グリッドの詳細、Grid Network のサブネット、グリッドのパスワード、NTP および DNS サーバーの IP アドレスなど、グリッドの設定を取得および更新できます。
- **nodes**: ノードレベルの設定操作。グリッドノードの一覧を取得したり、グリッドノードを削除したり、グリッドノードを設定したり、グリッドノードを表示したり、グリッドノードの設定をリセットしたりできます。
- **provision**: プロビジョニング操作。プロビジョニング操作を開始し、プロビジョニング操作のステータスを確認できます。
- リカバリ：プライマリ管理ノードのリカバリ操作。情報のリセット、リカバリパッケージのアップロード、リカバリの開始、およびリカバリ操作のステータスの確認が可能です。
- **recovery-package**：リカバリパッケージをダウンロードするための操作。
- サイト：サイトレベルの設定操作。サイトの作成、表示、削除、および変更が可能です。
- **temporary-password**: インストール中に mgmt-api を保護するための一時パスワードに対する操作。

StorageGRIDインストールの問題のトラブルシューティング

StorageGRID システムのインストール中に問題が発生した場合は、インストールログファイルにアクセスできます。テクニカルサポートが問題を解決するためにインストールログファイルを使用することもあります。

「Linux」は、RHEL、Ubuntu、または Debian のデプロイメントを指します。サポートされているバージョンのリストについては、 "NetApp Interoperability Matrix Tool（IMT）" 。

Linux

次のインストールログファイルは、各ノードを実行しているコンテナからアクセスできます。

- `/var/local/log/install.log`（すべてのグリッドノードに存在）
- `/var/local/log/gdu-server.log`（プライマリ管理ノードにあります）

次のインストールログファイルは、ホストからアクセスできます。

- `/var/log/storagegrid/daemon.log`
- `/var/log/storagegrid/nodes/node-name.log`

ログファイルへのアクセス方法については、を参照してください"ログファイルとシステムデータを収集"。

VMware

次のファイルは、テクニカルサポートが問題の解決に必要とする場合があるメインのインストールログファイルです。

- `/var/local/log/install.log`（すべてのグリッドノードに存在）
- `/var/local/log/gdu-server.log`（プライマリ管理ノードにあります）

仮想マシンのリソース予約の調整が必要

OVF ファイルでは、各グリッドノードが十分な RAM と CPU を確保して効率よく動作できるようにするためのリソースリザベーションが設定されています。これらのOVFファイルをVMwareに導入して仮想マシンを作成し、事前定義された数のリソースを使用できない場合、仮想マシンは起動しません。

タスクの内容

VM ホストに各グリッドノード用の十分なリソースがあることがわかっている場合は、各仮想マシンに割り当てられているリソースを手動で調整し、仮想マシンの起動を試みます。

手順

1. VMware vSphere ハイパーバイザーのクライアントツリーで、起動されていない仮想マシンを選択します。
2. 仮想マシンを右クリックし、 * 設定の編集 * を選択します。
3. [仮想マシンのプロパティ] ウィンドウで、 [* リソース *] タブを選択します。
4. 仮想マシンに割り当てられているリソースを調整します。
   a. [**CPU**] を選択し、 [予約] スライダを使用して、この仮想マシン用に予約されている MHz を調整します。
   b. [* Memory] を選択し、 [Reservation （予約）] スライダを使用してこの仮想マシン用に予約されている MB を調整します。
5. 「* OK *」を選択します。
6. 必要に応じて、同じ VM ホストでホストされている他の仮想マシンに対して同じ手順を繰り返します。

一時インストールパスワードが無効になりました

VMwareノードを導入するときに、必要に応じて一時的なインストールパスワードを指定できます。新しいノードがグリッドに追加される前にVMコンソールにアクセスするかSSHを使用するには、このパスワードが必要です。

一時インストールパスワードを無効にした場合は、インストールの問題をデバッグするために追加の手順を実行する必要があります。

次のいずれかを実行できます。

- コンソールにアクセスしたり、SSHを使用してインストールの問題をデバッグできるように、VMを再導入します。ただし、一時的なインストールパスワードを指定してください。
- vCenterを使用してパスワードを設定します。
  a. VMの電源をオフにします。
  b. に移動し、[設定]タブを選択して[vApp Options]*を選択します。
  c. 設定する一時インストールパスワードのタイプを指定します。
     - カスタム一時パスワードを設定するには、* custom_temporary_password *を選択します。
     - ノード名を一時パスワードとして使用する場合は、* temporary_password_type *を選択します。
  d. 「 * 値の設定 * 」を選択します。
  e. 一時パスワードを設定します。
     - custom_temporary_password *をカスタムのパスワード値に変更します。
     - temporary_password_type を use node name *の値で更新します。
  f. VMを再起動して新しいパスワードを適用します。

関連情報

- ログファイルへのアクセス方法については、を参照してください"ログファイル参照"。
- "StorageGRID システムのトラブルシューティングを行う"
- サポートが必要な場合は、にお問い合わせください "NetAppサポート"。

スクリプトの例

RHEL上の**StorageGRID**で**4**つの物理インターフェイスを**1**つのボンドに統合する例

以下のサンプルファイルを使用して、 4 つの Linux 物理インターフェイスを 1 つの LACP ボンドにまとめ、 3 つの VLAN インターフェイスを確立して、 StorageGRID のグリッドネットワーク、管理ネットワーク、およびクライアントネットワークのインターフェイス用にボンドを分割します。

物理インターフェイス

リンクの反対側のスイッチでも、 4 つのポートを 1 つの LACP トランクまたはポートチャネルとして扱い、少なくともタグで参照された 3 つの VLAN を通過させる必要があります。

/etc/sysconfig/network-scripts/ifcfg-ens160

```
TYPE=Ethernet
NAME=ens160
UUID=011b17dd-642a-4bb9-acae-d71f7e6c8720
DEVICE=ens160
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

/etc/sysconfig/network-scripts/ifcfg-ens192

```
TYPE=Ethernet
NAME=ens192
UUID=e28eb15f-76de-4e5f-9a01-c9200b58d19c
DEVICE=ens192
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

/etc/sysconfig/network-scripts/ifcfg-ens224

```
TYPE=Ethernet
NAME=ens224
UUID=b0e3d3ef-7472-4cde-902c-ef4f3248044b
DEVICE=ens224
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

/etc/sysconfig/network-scripts/ifcfg-ens256

```
TYPE=Ethernet
NAME=ens256
UUID=7cf7aabc-3e4b-43d0-809a-1e2378faa4cd
DEVICE=ens256
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

ボンドインターフェイス

/etc/sysconfig/network-scripts/ifcfg-bond0

```
DEVICE=bond0
TYPE=Bond
BONDING_MASTER=yes
NAME=bond0
ONBOOT=yes
BONDING_OPTS=mode=802.3ad
```

VLANインターフェイス

/etc/sysconfig/network-scripts/ifcfg-bond0.1001

```
VLAN=yes
TYPE=Vlan
DEVICE=bond0.1001
PHYSDEV=bond0
VLAN_ID=1001
REORDER_HDR=0
BOOTPROTO=none
UUID=296435de-8282-413b-8d33-c4dd40fca24a
ONBOOT=yes
```

/etc/sysconfig/network-scripts/ifcfg-bond0.1002

```
VLAN=yes
TYPE=Vlan
DEVICE=bond0.1002
PHYSDEV=bond0
VLAN_ID=1002
REORDER_HDR=0
BOOTPROTO=none
UUID=dbaaec72-0690-491c-973a-57b7dd00c581
ONBOOT=yes
```

/etc/sysconfig/network-scripts/ifcfg-bond0.1003

```
VLAN=yes
TYPE=Vlan
DEVICE=bond0.1003
PHYSDEV=bond0
VLAN_ID=1003
REORDER_HDR=0
BOOTPROTO=none
UUID=d1af4b30-32f5-40b4-8bb9-71a2fbf809a1
ONBOOT=yes
```

Ubuntu および **Debian** 上の **StorageGRID** の物理インターフェースを集約する例

この `/etc/network/interfaces`ファイルは、物理インターフェイス、ボンドインターフェイス、およびVLANインターフェイスを定義する3つのセクションで構成されています。以下の 3 つのセクションサンプルを 1 つのファイルに統合すれば、 4 つの Linux 物理インターフェイスを 1 つの LACP ボンドにまとめ、そのボンドを StorageGRID のグリッドネットワーク、管理ネットワーク、およびクライアントネットワークのインターフェイスとして使用するための 3 つの VLAN インターフェイスを確立できます。

物理インターフェイス

リンクの反対側のスイッチでも、 4 つのポートを 1 つの LACP トランクまたはポートチャネルとして扱い、少なくともタグで参照された 3 つの VLAN を通過させる必要があります。

```
# loopback interface
auto lo
iface lo inet loopback

# ens160 interface
auto ens160
iface ens160 inet manual
    bond-master bond0
    bond-primary en160

# ens192 interface
auto ens192
iface ens192 inet manual
    bond-master bond0

# ens224 interface
auto ens224
iface ens224 inet manual
    bond-master bond0

# ens256 interface
auto ens256
iface ens256 inet manual
    bond-master bond0
```

ボンドインターフェイス

```
# bond0 interface
auto bond0
iface bond0 inet manual
    bond-mode 4
    bond-miimon 100
    bond-slaves ens160 ens192 end224 ens256
```

VLANインターフェイス

```
# 1001 vlan
auto bond0.1001
iface bond0.1001 inet manual
vlan-raw-device bond0

# 1002 vlan
auto bond0.1002
iface bond0.1002 inet manual
vlan-raw-device bond0

# 1003 vlan
auto bond0.1003
iface bond0.1003 inet manual
vlan-raw-device bond0
```

グリッドを構成してインストールを完了する

StorageGRID Grid Managerに移動します

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

開始する前に

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

手順

1. Webブラウザを開き、次の場所に移動します。

   `https://primary_admin_node_ip`

   ポート 8443 でグリッドマネージャにアクセスすることもできます。

   `https://primary_admin_node_ip:8443`

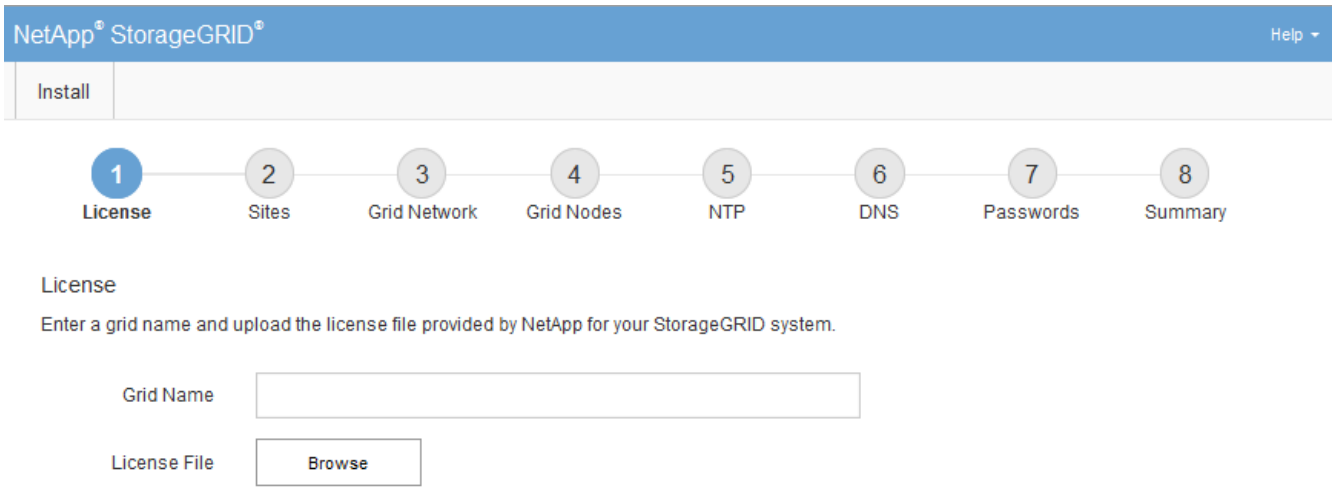
   ネットワーク設定に応じて、グリッドネットワーク上または管理ネットワーク上のプライマリ管理ノード IP の IP アドレスを使用できます。信頼されていない証明書に移動するには、ブラウザのsecurity/advancedオプションの使用が必要になる場合があります。

2. 必要に応じて一時インストーラパスワードを管理します。
   - いずれかの方法ですでにパスワードが設定されている場合は、パスワードを入力して続行します。
     - ユーザが以前にインストーラにアクセスしているときにパスワードを設定した
     - Linuxの場合、パスワードはノード構成ファイルから自動的にインポートされます。`/etc/storagegrid/nodes/<node_name>.conf`
     - VMwareの場合、SSH/コンソールパスワードはOVFプロパティから自動的にインポートされます。

◦ パスワードが設定されていない場合は、必要に応じてStorageGRIDインストーラを保護するためのパスワードを設定します。

3. [Install a StorageGRID system]*を選択します。

   StorageGRID グリッドを設定するためのページが表示されます。



StorageGRID ライセンス情報を指定します

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

手順

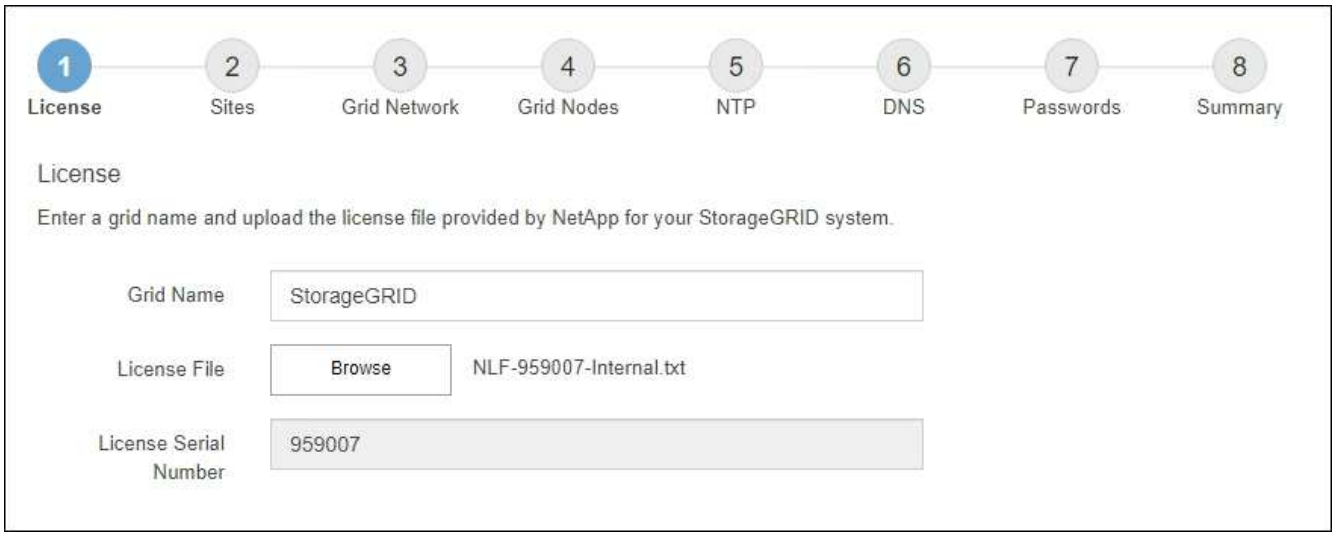
1. [License]ページで、StorageGRID システムのわかりやすい名前を*[Grid Name]*フィールドに入力します。

   インストール後、ノードメニューの上部に名前が表示されます。

2. を選択し、**NetApp**ライセンスファイルを検索し(`**NLF-*unique-id*.txt**`ます）、[開く]*を選択します。

   ライセンスファイルが検証され、シリアル番号が表示されます。

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



3. 「 * 次へ * 」を選択します。

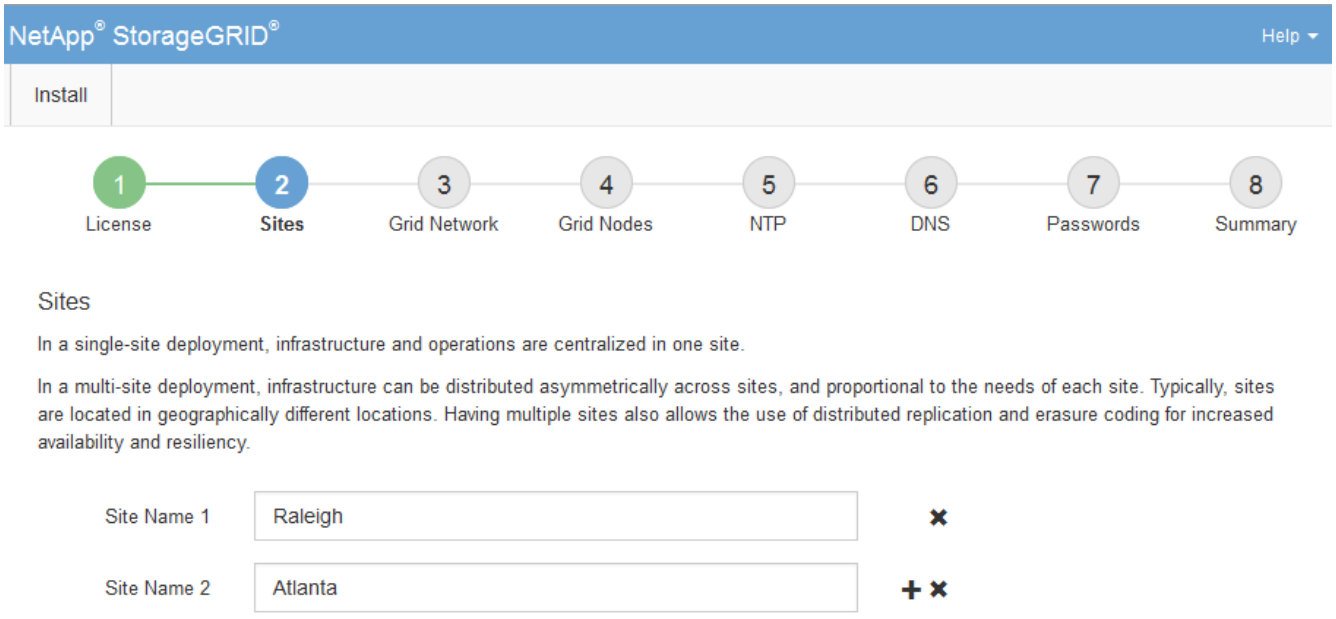
StorageGRID でサイトを追加する

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

手順

1. サイトページで、*サイト名*を入力してください。
2. サイトを追加するには、最後のサイトエントリの横にあるプラス記号を選択し、新しい **Site name** テキストボックスに名前を入力します。

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



3. 「 * 次へ * 」を選択します。

StorageGRID のグリッドネットワークサブネットを指定します

グリッドネットワークで使用されるサブネットを指定する必要があります。

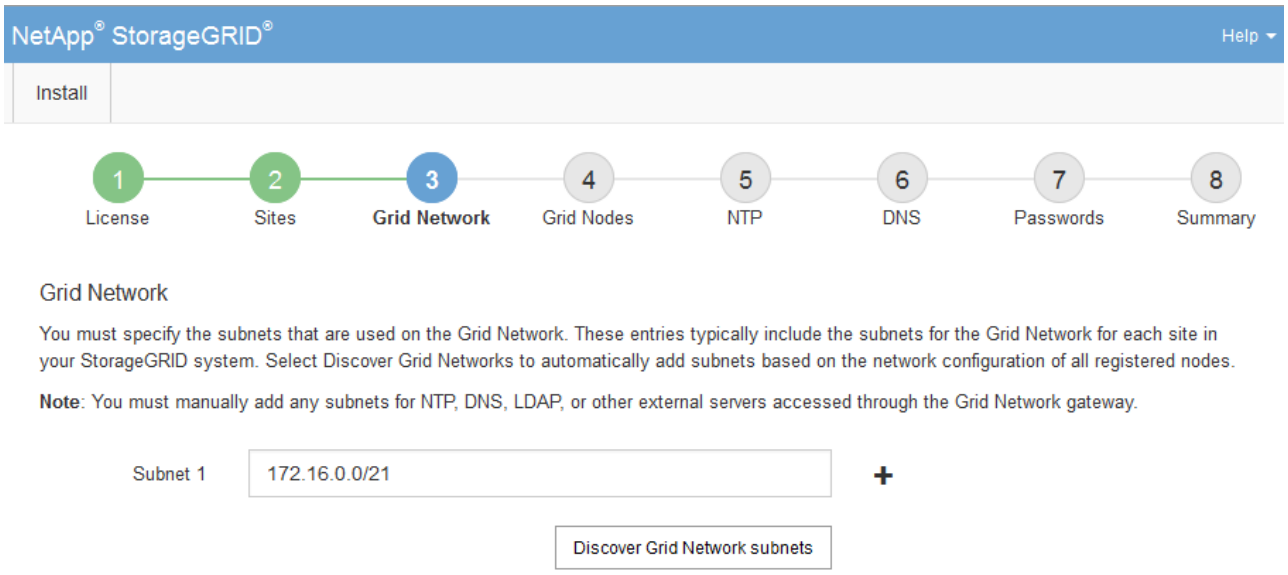
タスクの内容

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

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

手順

1. [* サブネット 1*] テキストボックスで、少なくとも 1 つのグリッドネットワークの CIDR ネットワークアドレスを指定します。
2. 最後のエントリの横にあるプラス記号を選択すると、ネットワークエントリを追加できます。グリッドネットワーク内のすべてのサイトについて、すべてのサブネットを指定する必要があります。
   - 既に少なくとも1つのノードをデプロイしている場合は、*グリッドネットワークサブネットの検出*を選択すると、Grid Managerに登録されているグリッドノードによって報告されたサブネットがグリッドネットワークサブネットリストに自動的に表示されます。
   - グリッドネットワークゲートウェイ経由でアクセスするNTP、DNS、LDAP、またはその他の外部サーバのサブネットを手動で追加する必要があります。



3. 「 * 次へ * 」を選択します。

StorageGRID の保留中のグリッドノードを承認する

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

開始する前に

仮想アプライアンスと StorageGRID アプライアンスのグリッドノードをすべて導入しておきます。

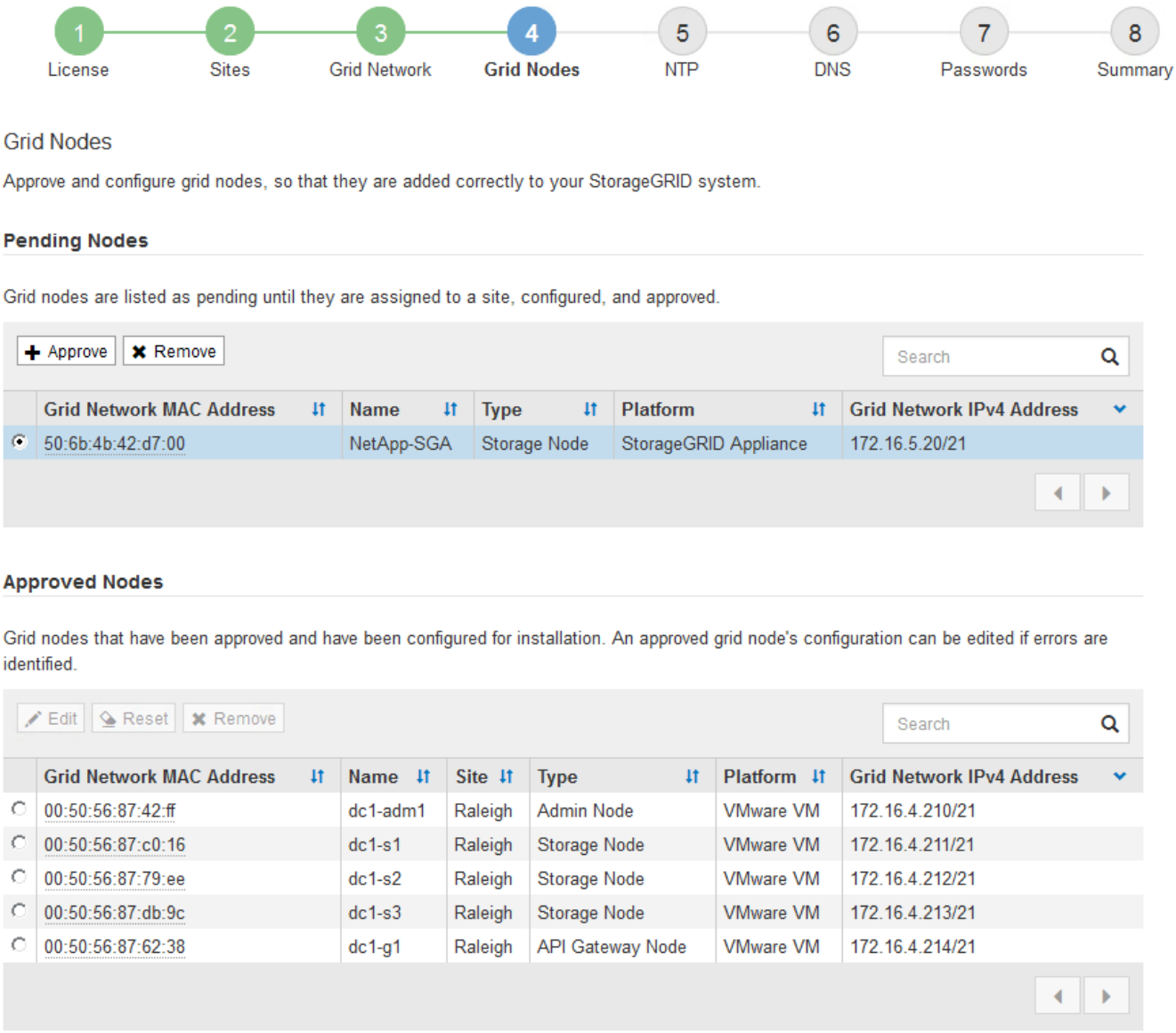
一部のノードだけを先にインストールしてから、一部のノードだけをインストールするよりも、すべてのノードを 1 つのインストールする方が効率的です。

手順

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

見つからないグリッドノードがある場合は、そのノードが正常に導入され、プライマリ管理ノードの正しいグリッドネットワークIPがADMIN_IPに設定されていることを確認します。

2. 承認する保留中のノードの横にあるラジオボタンを選択します。



3. [* 承認（ Approve ）] を選択し
4. [一般設定] で、必要に応じて次のプロパティの設定を変更します。

- * Site * ：このグリッドノードのサイトのシステム名。
- * Name * ：ノードのシステム名。デフォルトでは、ノードの設定時に指定した名前が付けられます。

  システム名はStorageGRID の内部処理に必要であり、インストールの完了後に変更することはできません。ただし、インストールプロセスのこのステップでは、必要に応じてシステム名を変更できます。

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

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

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

- ストレージタイプ（ストレージノードのみ）：新しいストレージノードをデータのみ、メタデータのみ、またはその両方に排他的に使用するように指定します。オプションは、データとメタデータ（「組み合わせ」）、データのみ、*メタデータのみ*です。

  これらのノードタイプの要件については、を参照してください"ストレージノードのタイプ"。

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

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

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

     グリッドサブネットが複数ある場合は、ゲートウェイが必要です。

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

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

   サブネット（ CIDR ） * テキストボックスに、このインターフェイスから発信されるルートの宛先サブネ

ットを入力します。管理サブネットが複数ある場合は、管理ゲートウェイが必要です。

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

アプライアンス： StorageGRID アプライアンスでは、StorageGRID アプライアンスインストーラを使用した初回インストール時に管理ネットワークを設定しなかった場合、この[Grid Manager]ダイアログボックスで管理ネットワークを設定することはできません。代わりに、次の手順を実行する必要があります。

a. アプライアンスをリブートします。アプライアンスインストーラで、 * Advanced * > * Reboot * を選択します。

   リブートには数分かかることがあります。

b. [Configure Networking*] > [**Link Configuration**] を選択し、適切なネットワークを有効にします。

c. [Configure Networking*]>[**IP Configuration**] を選択し、有効なネットワークを設定します。

d. ホームページに戻り、*インストールの開始*を選択してください。

e. Grid Managerで、ノードが[Approved Nodes]テーブルに表示されている場合は、そのノードを削除します。

f. Pending Nodes テーブルからノードを削除します。

g. ノードが Pending Nodes リストに再表示されるまで待ちます。

h. 適切なネットワークを設定できることを確認します。アプライアンスインストーラの[IP Configuration]ページで指定した情報があらかじめ入力されています。

   詳細については、を参照して、 "ハードウェア設置のクイックスタート"使用しているアプライアンスの手順を確認してください。

7. グリッドノードのクライアントネットワークを設定する場合は、必要に応じてクライアントネットワークセクションで設定を追加または更新します。クライアントネットワークを設定する場合はゲートウェイが必要になります。これは、インストール後にノードのデフォルトゲートウェイになります。

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

   アプライアンス： StorageGRID アプライアンスの場合、StorageGRID アプライアンスインストーラを使用した初期インストールでクライアントネットワークが設定されていないと、この[Grid Manager]ダイアログボックスで設定できません。代わりに、次の手順を実行する必要があります。

   a. アプライアンスをリブートします。アプライアンスインストーラで、 * Advanced * > * Reboot * を選択します。

      リブートには数分かかることがあります。

   b. [Configure Networking*] > [**Link Configuration**] を選択し、適切なネットワークを有効にします。

   c. [Configure Networking*]>[**IP Configuration**] を選択し、有効なネットワークを設定します。

   d. ホームページに戻り、*インストールの開始*を選択してください。

e. Grid Managerで、ノードが[Approved Nodes]テーブルに表示されている場合は、そのノードを削除します。

f. Pending Nodes テーブルからノードを削除します。

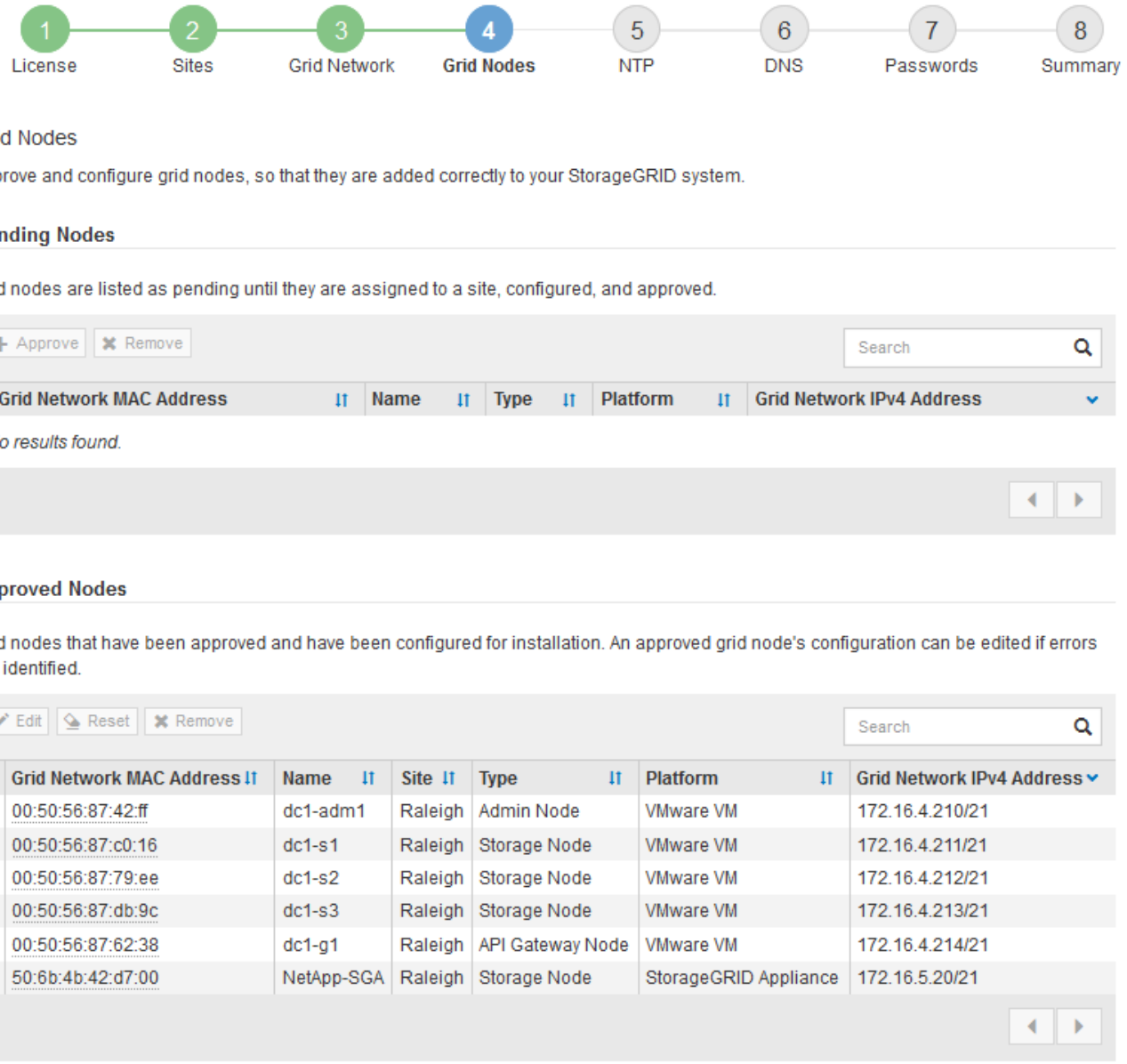
g. ノードが Pending Nodes リストに再表示されるまで待ちます。

h. 適切なネットワークを設定できることを確認します。アプライアンスインストーラの[IP Configuration]ページで指定した情報があらかじめ入力されています。

詳細については、を参照して、 "ハードウェア設置のクイックスタート"使用しているアプライアンスの手順を確認してください。

8. [保存（ Save ）] を選択します。

グリッドノードエントリが [承認済みノード（ Approved Nodes ）] リストに移動します。



9. 承認する保留中のグリッドノードごとに、上記の手順を繰り返します。

グリッドに追加したいノードはすべて承認する必要があります。ただし、概要ページで **Install** を選択する前であれば、いつでもこのページに戻ることができます。承認済みのグリッドノードのプロパティを変更するには、そのラジオボタンを選択し、**Edit** を選択します。

10. グリッドノードの承認が完了したら、*次へ*を選択してください。

StorageGRID のネットワークタイムプロトコルサーバ情報を指定します

別々のサーバで実行された処理を常に同期された状態にするには、 StorageGRID システムの NTP 設定情報を指定する必要があります。

タスクの内容

NTP サーバの IPv4 アドレスを指定する必要があります。

外部 NTP サーバを指定する必要があります。指定した NTP サーバで NTP プロトコルが使用されている必要があります。

時間のずれに伴う問題を防ぐには、 Stratum 3 またはそれより上位の NTP サーバ参照を 4 つ指定する必要があります。

本番レベルのStorageGRID インストール用に外部NTPソースを指定する場合は、Windows Server 2016より前のバージョンのWindowsでWindows Time (W32Time)サービスを使用しないでください。以前のバージョンの Windows のタイムサービスは精度が十分でないため、StorageGRID などの高精度環境での使用は Microsoft でサポートされていません。

"高精度時間のサポート境界"

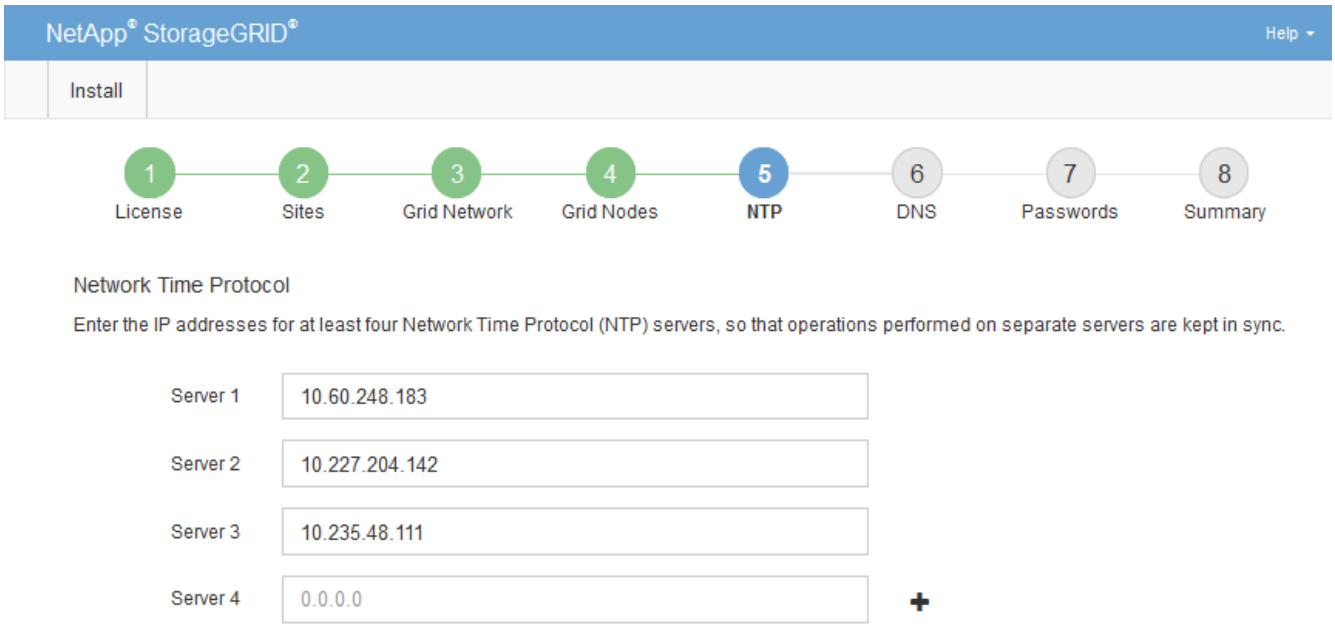
外部 NTP サーバは、以前にプライマリ NTP ロールを割り当てていたノードによって使用されます。

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

(VMware のみ) ハイパーバイザーが仮想マシンと同じ NTP ソースを使用していることを確認したり、VMTools を使用してハイパーバイザーとStorageGRID仮想マシン間の時間同期を無効にしたりするなど、VMware の追加チェックを実行します。

手順

1. [* サーバー 1 * から * サーバー 4 *] テキストボックスに、少なくとも 4 つの NTP サーバーの IPv4 アドレスを指定します。
2. 必要に応じて、最後のエントリの横にあるプラス記号を選択して、サーバエントリを追加します。



3. 「 * 次へ * 」を選択します。

関連情報

"ネットワークのガイドライン"

StorageGRID の**DNS**サーバー情報を指定します

IPアドレスの代わりにホスト名を使用して外部サーバにアクセスできるように、StorageGRID システムのDNS情報を指定する必要があります。

タスクの内容

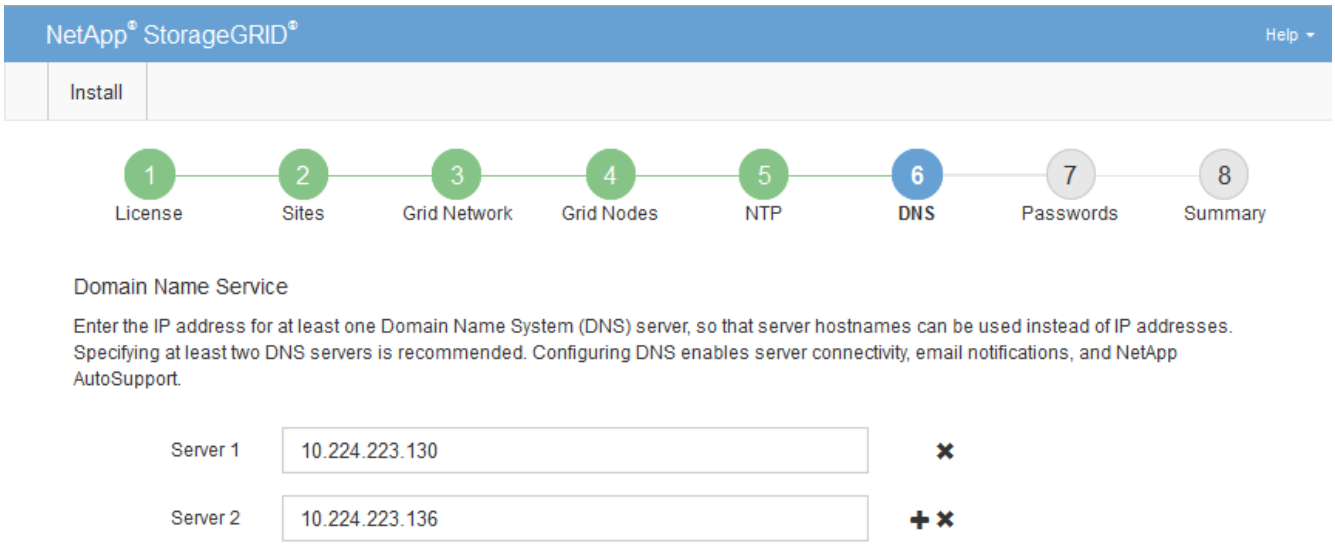
を指定する "DNSサーバ情報"と、Eメール通知やAutoSupportにIPアドレスではなく完全修飾ドメイン名（FQDN）ホスト名を使用できます。

適切に動作するように、2つまたは3つのDNSサーバを指定します。3つ以上を指定すると、一部のプラットフォームではOSに制限があるため、3つだけが使用される可能性があります。ルーティングが制限されている環境では、個 々 のノード（通常はサイトのすべてのノード）で、最大3つのDNSサーバの異なるセットを使用できます"DNSサーバリストをカスタマイズします"。

可能であれば、各サイトがローカルにアクセスできるDNSサーバを使用して、孤立したサイトが外部の宛先のFQDNを解決できるようにします。

手順

1. 「 * サーバー 1 * 」テキストボックスで、少なくとも 1 つの DNS サーバーの IPv4 アドレスを指定します。
2. 必要に応じて、最後のエントリの横にあるプラス記号を選択して、サーバエントリを追加します。



少なくとも 2 つの DNS サーバを指定することを推奨します。DNS サーバは 6 つまで指定できます。

3. 「 * 次へ * 」を選択します。

StorageGRID システムのパスワードを指定します

StorageGRID システムのインストールの一環として、システムの保護とメンテナンス作業に使用するパスワードを入力する必要があります。

タスクの内容

Install Passwords ページを使用して、プロビジョニングパスフレーズとグリッド管理 root ユーザのパスワードを指定します。

- プロビジョニングパスフレーズは暗号化キーとして使用され、 StorageGRID システムでは格納されません。
- リカバリパッケージのダウンロードなど、インストール、拡張、メンテナンスの手順に使用するプロビジョニングパスフレーズが必要です。そのため、プロビジョニングパスフレーズは安全な場所に保存しておくことが重要です。
- 現在のプロビジョニングパスフレーズがある場合は、 Grid Manager からプロビジョニングパスフレーズを変更できます。
- Grid管理rootユーザのパスワードは、Grid Managerを使用して変更できます。
- ランダムに生成されたコマンドラインコンソールとSSHパスワードは、リカバリパッケージのファイルに格納されます `Passwords.txt`。

手順

1. 「プロビジョニングパスフレーズ」に、StorageGRID システムのグリッドトポロジを変更する際に必要となるプロビジョニングパスフレーズを入力します。

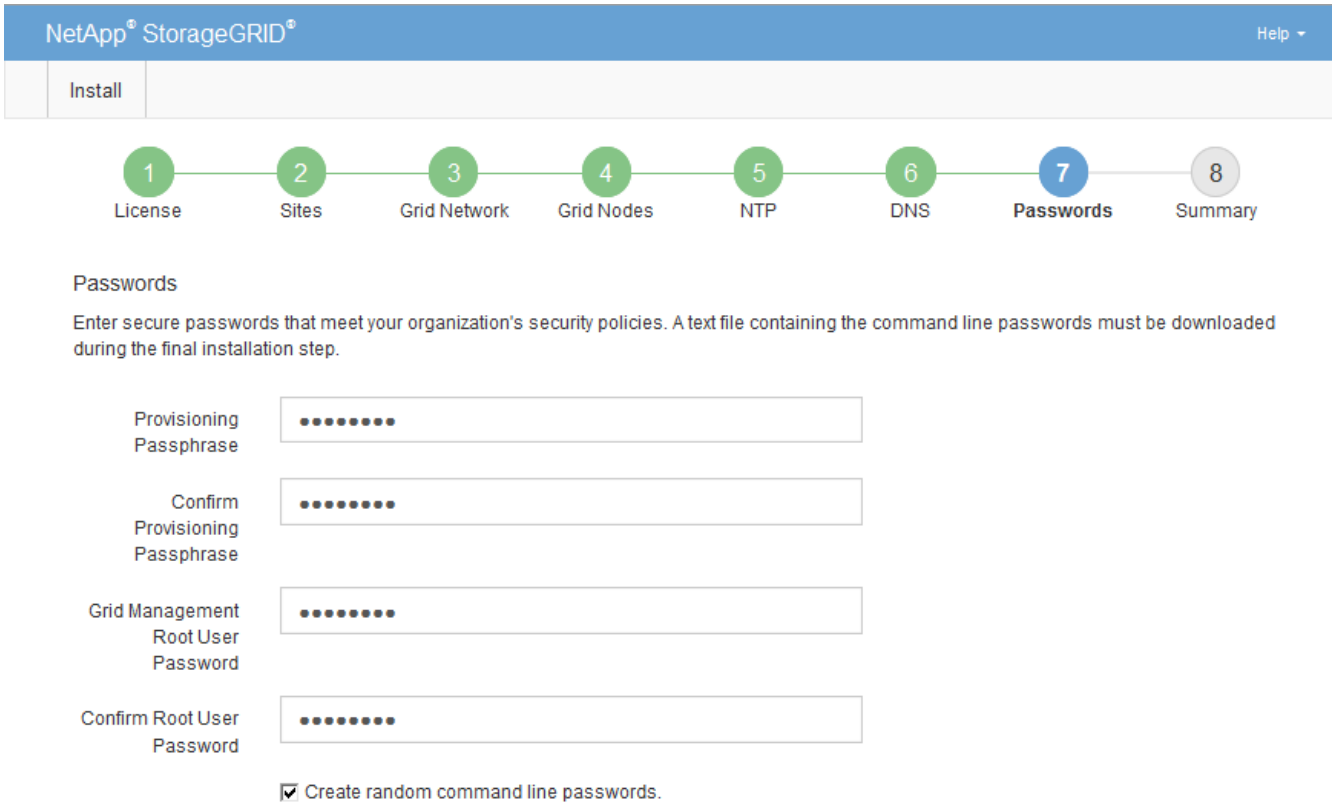
   プロビジョニングパスフレーズは安全な場所に保存してください。

   インストールが完了した後にプロビジョニング パスフレーズを変更する場合は、Grid Manager を使用できます。 構成 > アクセス制御 > グリッド パスワード を選択します。

2. 「プロビジョニングパスフレーズの確認」で、プロビジョニングパスフレーズを再入力して確認してください。
3. [Grid Management Root User Password]*に、Grid Managerに「root」ユーザとしてアクセスする際に使用するパスワードを入力します。

> プロビジョニング パスフレーズを安全な場所に保存します。インストール、拡張、メンテナンスの手順に必要です。

4. Confirm Root User Password * で、 Grid Manager のパスワードを再入力して確認します。



5. コンセプトの実証またはデモ用にGridをインストールする場合は、必要に応じて*[Create random command line passwords]*チェックボックスをオフにします。

本番環境では、セキュリティ上の理由から常にランダムパスワードを使用する必要があります。「root」または「admin」アカウントを使用してコマンドラインからグリッドノードにアクセスする際にデフォルトのパスワードを使用する場合は、「Create random command line passwords」*の選択を解除します。

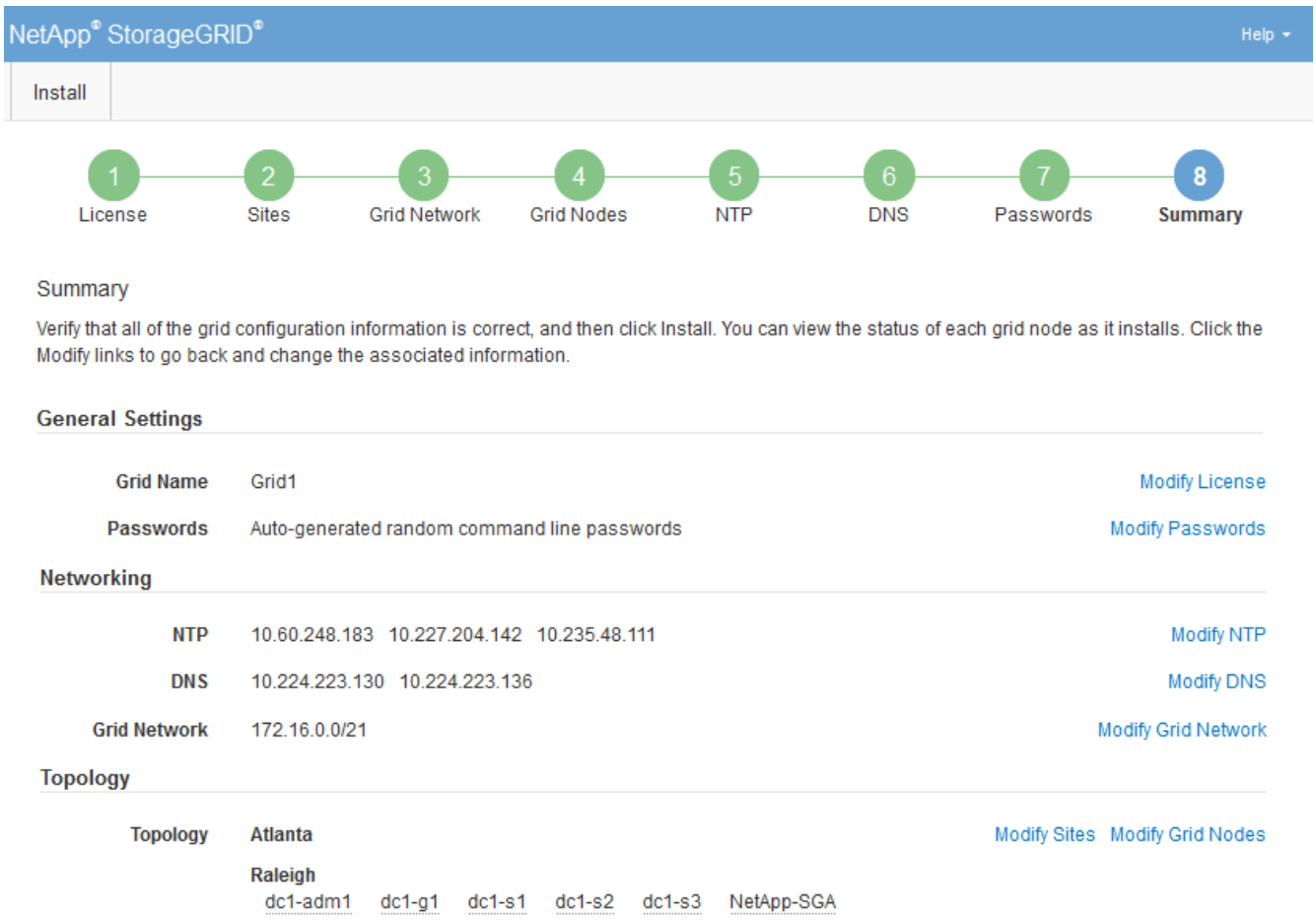
> 概要ページで「インストール」を選択すると、リカバリーパッケージファイル（`sgws-recovery-package-id-revision.zip`）のダウンロードを求められます。インストールを完了するには、"このファイルをダウンロードします"が必要です。システムへのアクセスに必要なパスワードは、リカバリーパッケージファイルに含まれる `Passwords.txt`ファイルに保存されています。

6. 「 * 次へ * 」を選択します。

インストールを正常に完了するために、入力した設定情報をよく確認する必要があります。

手順

1. 「 * 概要 * 」ページを表示します。



2. グリッドの設定情報がすべて正しいことを確認します。Summary （サマリ）ページの Modify （変更）リンクを使用して、戻ってエラーを修正します。
3. 「インストール」を選択します。

> ノードがクライアントネットワークを使用するように構成されている場合、「インストール」を選択すると、そのノードのデフォルトゲートウェイはグリッドネットワークからクライアントネットワークに切り替わります。接続が切断された場合は、アクセス可能なサブネット経由でプライマリ管理ノードにアクセスしていることを確認してください。詳細については、"ネットワークのガイドライン"を参照してください。

4. [リカバリパッケージのダウンロード] を選択します。

グリッドトポロジを定義するポイントまでインストールが進むと、リカバリパッケージファイルをダウンロードするように求められ(`.zip`ます）、このファイルの内容に正常にアクセスできることを確認するメッセージが表示されます。リカバリパッケージファイルのダウンロードが必要となるのは、グリッドノードで障害が発生した場合に StorageGRID システムをリカバリできるようにするためです。インストール

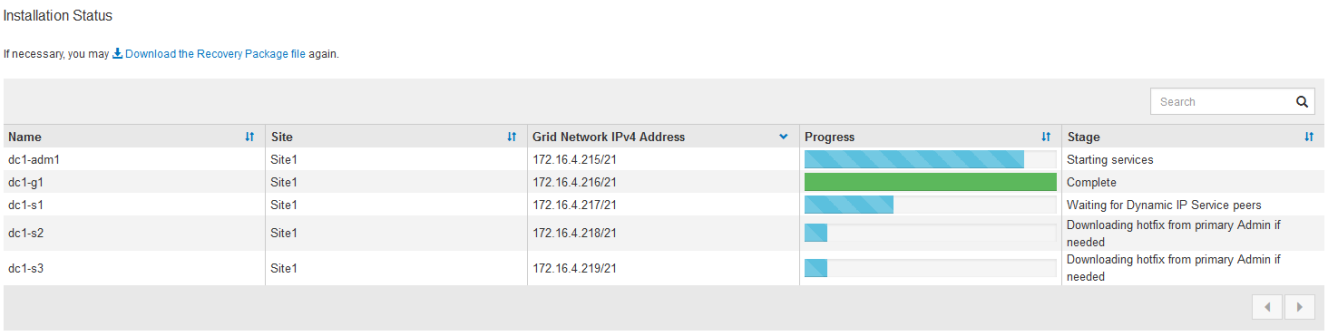
はバックグラウンドで続行されますが、このファイルをダウンロードして確認するまで、インストールを完了してStorageGRID システムにアクセスすることはできません。

5. ファイルの内容を展開できることを確認し `.zip`、安全で安全な別 々 の場所に保存します。

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

6. 「リカバリパッケージファイルのダウンロードと検証が正常に完了しました」チェックボックスを選択し、「次へ」を選択します。

   インストールがまだ進行中の場合は、ステータスページが表示されます。このページには、グリッドノードごとのインストールの進捗状況が表示されます。



   すべてのグリッドノードが完了ステージに到達すると、 Grid Manager のサインインページが表示されます。

7. 「 root 」ユーザおよびインストール時に指定したパスワードを使用して Grid Manager にサインインします。

StorageGRIDのインストール後のネットワークと**DHCP**の要件

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

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

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

> グリッドネットワーク設定がDHCPによって変更されるとノードがリブートします。DHCPの変更が複数のノードに同時に影響すると、システムが停止する可能性があります。

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

StorageGRIDのインストール後の必須およびオプションの手順について学習します

インストールが完了したら、必要な統合タスクと設定タスクを実行します。必要に応じてオプションのタスクを実行できます。

必要な作業

- (VMware のみ) VMware vSphere Hypervisor を自動再起動するように構成します。

  サーバの再起動時に仮想マシンを再起動するようにハイパーバイザーを設定する必要があります。自動再起動を有効にしないと、サーバが再起動したあとも仮想マシンとグリッドノードがシャットダウンされたままになります。詳細については、 VMware vSphere ハイパーバイザーのドキュメントを参照してください。

- "テナントアカウントを作成します"StorageGRIDシステムにオブジェクトを格納するために使用されるS3クライアントプロトコル。
- "システムアクセスを制御します"グループとユーザアカウントを設定する。必要に応じて（Active DirectoryやOpenLDAPなど）、管理者グループおよびユーザをインポートできます"フェデレーテッドアイデンティティソースを設定する"。または、できます"ローカルグループとユーザを作成します"。
- オブジェクトをStorageGRIDシステムにアップロードするために使用するクライアントアプリケーションを統合してテストし"S3 API"ます。
- "情報ライフサイクル管理（ILM）ルールとILMポリシーを設定する"を使用してオブジェクトデータを保護する。
- インストール環境にアプライアンスストレージノードが含まれている場合は、SANtricity OSを使用して次のタスクを実行します。
  - 各 StorageGRID アプライアンスに接続します。
  - AutoSupport データの受信を確認します。

    を参照してください "ハードウェアをセットアップする"

- セキュリティリスクを排除するには、を確認して従い"StorageGRID システムのセキュリティ強化ガイドライン"ます。
- "システムアラートのEメール通知を設定します"です。

任意のタスク

- "グリッドノードのIPアドレスを更新します"展開を計画して回復パッケージを生成してから変更があった場合。
- "ストレージ暗号化を設定します"（必要な場合）。
- "ストレージの圧縮を設定します"必要に応じて、格納オブジェクトのサイズを縮小します。
- "VLAN インターフェイスを設定します"必要に応じて、ネットワークトラフィックを分離して分割します。
- "ハイアベイラビリティグループを設定する"Grid Manager、Tenant Manager、およびS3クライアントの接続の可用性を高めるため（必要な場合）。
- "ロードバランサエンドポイントを設定する"S3クライアント接続（必要な場合）。

StorageGRID ソフトウェアをアップグレードします

StorageGRID ソフトウェアをアップグレードします

以下の手順に従って、 StorageGRID システムを新しいリリースにアップグレードします。

アップグレードを実行すると、StorageGRIDシステム内のすべてのノードがアップグレードされます。

> 緊急にストレージを拡張して容量を増やす必要がある場合（ストレージがほぼいっぱいの場合）は、アップグレードを開始しないでください。アップグレード手順を適時に完了してください。回復が必要な場合は、テクニカル サポートにお問い合わせください。

アップグレードする前に

これらのトピックを確認して、StorageGRID 12.1の新機能と強化点について学び、非推奨または削除された機能があるかどうかを確認し、StorageGRID APIの変更点について調べてください。

- "アップグレード中にシステムが受ける影響"
- "StorageGRID 12.1の新機能"
- "削除または廃止された機能"
- "Grid 管理 API に対する変更"
- "テナント管理 API に変更が加えられました"

アップグレードを計画して準備

StorageGRIDアップグレードの完了までの時間を見積もる

アップグレードにかかる時間に基づいて、アップグレードのタイミングを検討してください。アップグレードの各段階で実行できる処理と実行できない処理に注意してください。

タスクの内容

StorageGRID のアップグレード完了までに必要な時間は、クライアントの負荷やハードウェアのパフォーマンスなどのさまざまな要因によって異なります。

次の表に、アップグレードの主なタスクをまとめ、各タスクに必要なおおよその時間を示します。表に続いて、システムのアップグレード時間を見積もる手順を記載します。

アップグレードタスク	製品説明	おおよその所要時間です	このタスクの実行中です
事前確認を実行してプライマリ管理ノードをアップグレードする	アップグレードの事前確認が実行され、プライマリ管理ノードが停止、アップグレード、および再起動されます。	30分~1時間（サービスアプライアンスノードの所要時間が最も長い） 今回は未解決の事前確認エラーが増加します。	プライマリ管理ノードにはアクセスできません。接続エラーが報告される場合がありますが、これは無視してかまいません。 アップグレードを開始する前にアップグレードの事前確認を実行すると、スケジュールされたアップグレードメンテナンス時間前にエラーを解決できます。
アップグレードサービスを開始します	ソフトウェアファイルが配布され、アップグレードサービスが開始されます。	グリッドノードあたり3分	
他のグリッドノードをアップグレードします	他のすべてのグリッドノードのソフトウェアは、ノードを承認した順序でアップグレードされます。 1 つの管理ノードまたはゲートウェイ ノードは、1 つのストレージ ノードと同時にアップグレードされます。	ノードあたり 15~1 時間。アプライアンスノードで最も時間が必要です 注：アプライアンスノードの場合、StorageGRID アプライアンスインストーラは自動的に最新リリースに更新されます。	• グリッド設定を変更しないでください。 • 監査レベルの設定は変更しないでください。 • ILM設定を更新しないでください。 • ホットフィックス、運用停止、拡張など、他のメンテナンス手順を実行することはできません。 注：リカバリを実行する必要がある場合は、テクニカルサポートにお問い合わせください。
機能を有効にします	新しいバージョンの新機能が有効になります。	最大1時間	• グリッド設定を変更しないでください。 • 監査レベルの設定は変更しないでください。 • ILM設定を更新しないでください。 • 別のメンテナンス手順 を実行することはできません。
最終アップグレード手順	一時ファイルが削除され、新しいリリースへのアップグレードが完了します。	5分	最後のアップグレード手順*タスクが完了したら、すべてのメンテナンス手順を実行できます。

アップグレードにかかる時間を見積もる

手順

1. すべてのグリッドノードをアップグレードするために必要な推定時間。
    a. StorageGRID システムのノード数に 1 時間を掛けます。

原則として、アプライアンスノードのアップグレードにはソフトウェアベースのノードよりも時間がかかります。

b. この時間に、ファイルのダウンロード、事前確認検証の実行、および最終アップグレード手順の完了に必要な時間として1時間を加算します `.upgrade`。

2. Linux ノードがある場合は、 RPM パッケージまたは DEB パッケージをダウンロードしてインストールするために必要な時間として、各ノードに 15 分を追加します。
3. 手順 1 および 2 の結果を追加して、アップグレードの合計推定時間を計算します。

例：**StorageGRID 12.1**へのアップグレードにかかる推定時間

システムにグリッドノードが 14 個あり、そのうち 8 個が Linux ノードであるとします。

1. 14 に 1 時間を掛けます。
2. ダウンロード、事前確認、および最終手順に 1 時間を足します。

   すべてのノードのアップグレードにかかる推定時間は15時間です。

3. Linux ノードに RPM パッケージまたは DEB パッケージをインストールする時間を、 8 に 15 分 / ノードを掛けます。

   この手順の推定時間は 2 時間です。

4. 値をまとめて追加します。

   システムを StorageGRID 12.1.0 にアップグレードするには、最大 18 時間かかる場合があります。

> 必要に応じて、複数のセッションでグリッドノードのサブセットを承認することで、メンテナンス時間をより短い時間に分割できます。たとえば、1つのセッションでサイトAのノードをアップグレードしてから、以降のセッションでサイトBのノードをアップグレードすることができます。アップグレードを複数のセッションで実行する場合は、すべてのノードがアップグレードされるまで新しい機能の使用を開始できないことに注意してください。

StorageGRIDアップグレードがシステムに与える影響

アップグレード時にStorageGRIDシステムがどのような影響を受けるかについて説明します。

アップグレードが完了するまで外部**SSH**アクセスは許可されます

アップグレード中は外部 SSH アクセスが許可されます。アップグレードが完了すると、外部 SSH アクセスはデフォルトでブロックされます。アップグレード後、グリッドマネージャ > *セキュリティ設定*ページにある*SSHブロック*タブを使用して、"外部SSHアクセスを管理する" 。グリッド ノード間の SSH アクセスは影響を受けません。

StorageGRIDのアップグレードは無停止

StorageGRID システムは、アップグレードプロセス中もクライアントアプリケーションからデータを取り込み、読み出すことができます。同じタイプのすべてのノード（ストレージノードなど）のアップグレードを承認すると、ノードが一度に1つずつ停止されるため、すべてのグリッドノードまたは特定のタイプのすべての

グリッドノードが使用できなくなる時間はありません。

継続的な可用性を確保するには、各オブジェクトの複数のコピーを格納するように指定するルールをILMポリシーに含めるようにしてください。また、すべての外部S3クライアントが次のいずれかに要求を送信するように設定されていることを確認する必要があります。

- ハイアベイラビリティ（HA）グループの仮想IPアドレス
- 高可用性を備えたサードパーティ製ロードバランサ
- 各クライアントに複数のゲートウェイノードが必要
- クライアントごとに複数のストレージノード

クライアントアプリケーションが短時間中断される可能性があります

StorageGRIDシステムは、アップグレードプロセス中もクライアントアプリケーションからデータを取り込み、読み出すことができます。ただし、アップグレード中に個 々 のゲートウェイノードまたはストレージノードでサービスの再開が必要になった場合は、それらのノードへのクライアント接続が一時的に中断されることがあります。接続はアップグレードプロセスの完了後にリストアされ、個 々 のノードのサービスが再開されます。

接続の中断が短時間でも許容されない場合は、アップグレードを適用するためにダウンタイムのスケジュールが必要になることがあります。特定のノードが更新されるタイミングをスケジュールするには、選択的な承認を使用できます。

> 複数のゲートウェイとハイアベイラビリティ（HA）グループを使用して、アップグレードプロセス中の自動フェイルオーバーを実現できます。の手順を参照してください"ハイアベイラビリティグループを設定する"。

混合バージョンのノードがあるグリッドではバックグラウンド修復は実行されません

グリッドに混合バージョンのノードが含まれている場合、アップグレード中にバックグラウンド修復は実行されません。サイトの停止中に発生した不整合は、アップグレードが完了するまで修復されません。

アプライアンスファームウェアがアップグレードされている

StorageGRID 12.1 のアップグレード中：

- すべての StorageGRID アプライアンスノードは、StorageGRID アプライアンスインストーラのファームウェアバージョン 12.1 に自動的にアップグレードされます。
- SG6060 および SGF6024 アプライアンスは、BIOS ファームウェア バージョン 3B08.EX およびBMCファームウェア バージョン 4.01.07 に自動的にアップグレードされます。
- SG100 および SG1000 アプライアンスは、BIOS ファームウェア バージョン 3B13.EC およびBMCファームウェア バージョン 4.75.07 に自動的にアップグレードされます。
- SGF6112、SG6160、SG110、SG1100アプライアンスは、BIOSファームウェアバージョン3A14.QDおよびBMCファームウェアバージョン3.21.07に自動的にアップグレードされます。

ILMポリシーはステータスに応じて処理が異なります。

- アップグレード後もアクティブポリシーは変わりません。
- アップグレード時に保持されるのは、最新の10個の履歴ポリシーだけです。

- ドラフトポリシーがある場合は、アップグレード時に削除されます。

アラートがトリガーされる可能性があります

アラートは、サービスの開始と停止、および StorageGRID システムを複数バージョンが混在した環境で使用している場合（一部のグリッドノードで以前のバージョンを実行し、その他のノードはより新しいバージョンにアップグレードしている場合）にトリガーされることがあります。アップグレードの完了後にその他のアラートがトリガーされることがあります。

例えば、サービスが停止すると「ノードと通信できません」というアラートが表示されることがあります。また、一部のノードが StorageGRID 12.0 以降にアップグレードされているが、他のノードがまだ以前のバージョンの StorageGRID を実行している場合に、「Cassandra 通信エラー」というアラートが表示されることがあります。通常、これらのアラートはアップグレードが完了すると解消されます。

StorageGRID 12.0以降へのアップグレード中にストレージノードが停止すると、*ILM配置が不可能*アラートがトリガーされる可能性があります。このアラートは、アップグレード完了後1日間続く場合があります。

アップグレードが完了したら、Grid Managerダッシュボードで*または[現在のアラート]*を選択して、アップグレード関連のアラートを確認できます。

設定の変更は制限されています

> 構成変更に関する制限は、リリースごとに異なります。別の StorageGRID リリースにアップグレードする場合は、そのリリースのアップグレード手順に記載されている制限付き変更のリストを参照してください。

[新しい機能を有効にする *] タスクが完了するまで :

- グリッド設定を変更しないでください。
- 新しい機能を有効または無効にしないでください。
- ILM設定を更新しないでください。ILM の動作が不安定になり、正常に動作しない場合があります。
- ホットフィックスの適用やグリッドノードのリカバリは行わないでください。

> アップグレード中にノードのリカバリが必要な場合は、テクニカルサポートにお問い合わせください。

- アップグレード中は、HAグループ、VLANインターフェース、またはロードバランサーのエンドポイントを管理しないでください。
- アップグレードが完了するまで、HAグループを削除しないでください。他のHAグループ内の仮想IPアドレスにアクセスできなくなる可能性があります。

[* Final Upgrade Steps * （最終アップグレード手順 * ）] タスクが完了するまで：

- 拡張手順 を実行しないでください。
- 運用停止手順 は実行しないでください。

アップグレードする前に、インストールされている**StorageGRID**のバージョンを確認します

アップグレードを開始する前に、以前のバージョンのStorageGRIDに最新のホットフィ

ックスが適用されていることを確認してください。

タスクの内容

StorageGRID 12.1 にアップグレードする前に、グリッドに StorageGRID 12.0 以降がインストールされている必要があります。現在 StorageGRID の以前のバージョンを使用している場合は、グリッドの現在のバージョンが少なくとも StorageGRID 12.0.0 になるまで、以前のすべてのアップグレードファイルと最新のホットフィックス（強く推奨）をインストールする必要があります。

にアップグレードパスの1つを示します例。

> NetApp、次のバージョンにアップグレードする前に、各StorageGRIDバージョンに最新の修正プログラムを適用し、インストールする新しいバージョンごとに最新の修正プログラムを適用することを強くお勧めします。場合によっては、データ損失のリスクを回避するために修正プログラムを適用する必要があります。参照 "NetAppのダウンロード：StorageGRID"詳細については、各修正プログラムのリリース ノートを参照してください。

インストールされたバージョンを確認する

手順

1. を使用してGrid Managerにサインインし"サポートされている Web ブラウザ"ます。
2. Grid Manager の上部から * ヘルプ * > * バージョン情報 * を選択します。
3. バージョン が 11.9.0.8 以降であることを確認します。
4. *バージョン*が11.9.0.8以降でない場合は、 "NetAppのダウンロード：StorageGRID"必要なアップグレードおよび修正プログラム ファイルをダウンロードします。
5. "アップグレードの手順に従ってください"ダウンロードしたリリースごとに。"最新の修正プログラムを適用する"各リリースごとに（強く推奨）。

次のアップグレード例を参照してください。

例: **StorageGRID**バージョン **11.8** から **12.0** にアップグレード

次の例は、StorageGRID 12.1へのアップグレードに備えて、StorageGRID バージョン11.9からバージョン12.0にアップグレードする手順を示しています。

次の順序でソフトウェアをダウンロードしてインストールし、システムをアップグレードする準備をします。

1. StorageGRID 11.8.0メジャーリリースにアップグレードします。
2. 最新のStorageGRID 11.8.0._y_hotfixを適用します。
3. StorageGRID 11.9.0 メジャー リリースにアップグレードします。
4. StorageGRID 11.9.0.8 以降の修正プログラムを適用します。

StorageGRIDソフトウェアのアップグレードに必要な材料を入手する

ソフトウェアのアップグレードを開始する前に、必要な情報や情報をすべて入手しておきます。

項目	脚注
サービスラップトップ	サービスラップトップには次のものが必要です。 • ネットワークポート • SSH クライアント（ PuTTY など）
"サポートされている Web ブラウザ"	通常、ブラウザサポートは StorageGRID リリースごとに変更されます。ブラウザが新しい StorageGRID バージョンに対応していることを確認します。
プロビジョニングパスフレーズ	このパスフレーズは、 StorageGRID システムが最初にインストールされるときに作成されて文書化されます。プロビジョニングパスフレーズはファイルに含まれていません `Passwords.txt`。
Linux RPMまたはDEBアーカイブ	Linuxホストにノードが導入されている場合は、アップグレードを開始する前に実行する必要があります"RPMパッケージまたはDEBパッケージをすべてのホストにダウンロードしてインストールします"。 Linux オペレーティング システムが StorageGRID の最小カーネル バージョン要件を満たしていることを確認します。見る"LinuxホストにStorageGRIDをインストールする" 。
StorageGRID のドキュメント	• "リリースノート"。NetAppアカウントでサインインするか、アカウントを作成してリリースノートにアクセスする必要があります。アップグレードを開始する前に、必ずこれらの内容をよくお読みください。 • "StorageGRID ソフトウェアアップグレード解決ガイド"アップグレード先のメジャーバージョンについて（サインインが必要） • その他（ "StorageGRID のドキュメント"必要に応じて）。

アップグレード前に**StorageGRID**システムの状態を確認してください

StorageGRIDシステムをアップグレードする前に、システムがアップグレードに対応できる状態であることを確認します。システムが正常に動作し、すべてのグリッドノードが動作していることを確認します。

手順

1. を使用してGrid Managerにサインインし"サポートされている Web ブラウザ"ます。
2. アクティブなアラートがないかを確認し、ある場合は解決します。
3. アップグレードの前に、StorageGRID 12.1 に必要なすべてのポートが開いていることを確認するには、"内部でのグリッドノードの通信"および"外部との通信"を参照してください。

> StorageGRID 12.1 へのアップグレード時に追加のポートは必要ありません。

ソフトウェアのアップグレード

StorageGRIDアップグレードのクイックスタート

アップグレードを開始する前に、一般的なワークフローを確認してください。StorageGRID アップグレードページの指示に従って、各アップグレード手順を実行します。

1 Linuxホストノシユンヒ

LinuxホストにStorageGRIDノードが導入されている場合は"RPM パッケージまたは DEB パッケージを各ホストにインストールします"、アップグレードを開始する前に

2 アップグレードファイルとホットフィックスファイルのアップロード

プライマリ管理ノードから、StorageGRID の[Upgrade]ページにアクセスし、必要に応じてアップグレードファイルとホットフィックスファイルをアップロードします。

3 リカバリパッケージをダウンロード

アップグレードを開始する前に、現在のリカバリ パッケージをダウンロードしてください。

4 アップグレードの事前確認を実行

アップグレードの事前確認は問題を検出するのに役立ち、実際のアップグレードを開始する前に問題を解決できます。

5 アップグレードの開始

アップグレードを開始すると、事前確認が再度実行され、プライマリ管理ノードが自動的にアップグレードされます。プライマリ管理ノードのアップグレード中はGrid Managerにアクセスできません。監査ログも使用できなくなります。このアップグレードには最大 30 分かかることがあります。

6 リカバリパッケージをダウンロード

プライマリ管理ノードがアップグレードされたら、新しいリカバリ パッケージをダウンロードします。

7 ノードの承認

個々のグリッドノード、グリッドノードのグループ、またはすべてのグリッドノードを承認できます。

> グリッドノードを停止およびリブートする準備ができていることを確認するまでは、グリッドノードのアップグレードを承認しないでください。

8 サイカイシヨリ

すべてのグリッドノードをアップグレードすると新しい機能が有効になり、運用を再開できます。バックグラウンド*データベースのアップグレード*タスクと*最終アップグレード手順*タスクが完了するまで、運用停止または拡張手順 の実行を待機する必要があります。

関連情報

"アップグレードが完了するまでの推定時間"

StorageGRIDのすべてのLinuxホストにRPMまたはDEBパッケージをダウンロードしてインストールします

LinuxホストにStorageGRIDノードが導入されている場合は、アップグレードを開始する前に、これらの各ホストにRPMパッケージまたはDEBパッケージを追加でダウンロードしてインストールします。

アップグレードファイル、Linuxファイル、ホットフィックスファイルをダウンロードします

Grid ManagerからStorageGRID のアップグレードを実行すると、最初の手順として、アップグレードアーカイブと必要なホットフィックスをダウンロードするように求められます。ただし、Linuxホストをアップグレードするためにファイルをダウンロードする必要がある場合は、必要なファイルをすべて事前にダウンロードすることで時間を節約できます。

手順

1. に進みます "NetAppのダウンロード：StorageGRID"。
2. 最新のリリースをダウンロードするボタンを選択するか、ドロップダウンメニューから別のバージョンを選択して、「 * Go * 」を選択します。

   StorageGRID ソフトウェアのバージョンの形式は、 11.*x.y.* です。StorageGRID ホットフィックスの形式は、 11._x.y.z _ です。
3. ネットアップアカウントのユーザ名とパスワードを使用してサインインします。
4. 「Caution/MustRead」という通知が表示された場合は、ホットフィックス番号をメモし、チェックボックスをオンにします。
5. エンドユーザライセンス契約（EULA）を読み、チェックボックスをオンにして*[同意して続行]*を選択します。

   選択したバージョンのダウンロードページが表示されます。このページには3つの列があります。
6. 2列目（* Upgrade StorageGRID *）から、次の2つのファイルをダウンロードします。
   - 最新リリースのアップグレードアーカイブ（VMware、SG1000、またはSG100プライマリ管理ノード*のセクションにあるファイル）。このファイルはアップグレードを実行するまでは必要ありませんが、今すぐダウンロードすると時間を節約できます。
   - または `.zip`形式のRPMまたはDEBアーカイブ `.tgz`。サービスラップトップでWindowsを実行している場合は、ファイルを選択し`.zip`ます。
     - RHEL

       `StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.zip`

       `StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.tgz`

- UbuntuまたはDebian++
  `StorageGRID-Webscale-version-DEB-uniqueID.zip`
  `StorageGRID-Webscale-version-DEB-uniqueID.tgz`

7. 必要なホットフィックスが原因で「注意」/「必ずお読みください」の通知に同意する必要がある場合は、ホットフィックスをダウンロードしてください。
   a. に戻ります "NetAppのダウンロード：StorageGRID"。
   b. ドロップダウンからホットフィックス番号を選択します。
   c. 注意事項とEULAに再度同意します。
   d. ホットフィックスとそのREADMEをダウンロードして保存します。

      アップグレードを開始すると、StorageGRID の[Upgrade]ページでホットフィックスファイルをアップロードするように求められます。

8. Linux ノードではコード署名の検証は手動で行われます。必要に応じて、インストール アーカイブを検証します。
   a. StorageGRIDコード署名検証パッケージをダウンロードします。このパッケージのファイル名はの形式を使用し `StorageGRID_<version-number>_Code_Signature_Verification_Package.tar.gz`ます。`<version-number>`はStorageGRIDソフトウェアのバージョンです。
   b. 手順に従ってください"インストールファイルを手動で検証する"。

すべての**Linux**ホストにアーカイブをインストールします

StorageGRID ソフトウェアをアップグレードする前に、次の手順を実行します。

手順

1. インストールファイルから RPM パッケージまたは DEB パッケージを展開します。
2. すべての Linux ホストに RPM パッケージまたは DEB パッケージをインストールします。

   Linux用のStorageGRIDホストサービスのインストール手順については、"StorageGRID ホストサービスをインストールする" 。

   新しいパッケージは追加のパッケージとしてインストールされます。

以前のバージョンのインストールアーカイブを削除

Linuxホストのスペースを解放するには、不要になった以前のバージョンのStorageGRIDのインストールアーカイブを削除します。

手順

1. 古いStorageGRIDインストールアーカイブを削除します。

RHEL

1. インストールされているStorageGRIDパッケージのリストを取得します。 `dnf list | grep -i storagegrid`

   例：

```
[root@rhel-example ~]# dnf list | grep -i storagegrid
StorageGRID-Webscale-Images-11-6-0.x86_64 11.6.0-
20220210.0232.8d56cfe @System
StorageGRID-Webscale-Images-11-7-0.x86_64 11.7.0-
20230424.2238.1a2cf8c @System
StorageGRID-Webscale-Images-11-8-0.x86_64 11.8.0-
20240131.0139.e3e0c87 @System
StorageGRID-Webscale-Images-11-9-0.x86_64 11.9.0-
20240826.1753.4aeeb70 @System
StorageGRID-Webscale-Service-11-6-0.x86_64 11.6.0-
20220210.0232.8d56cfe @System
StorageGRID-Webscale-Service-11-7-0.x86_64 11.7.0-
20230424.2238.1a2cf8c @System
StorageGRID-Webscale-Service-11-8-0.x86_64 11.8.0-
20240131.0139.e3e0c87 @System
StorageGRID-Webscale-Service-11-9-0.x86_64 11.9.0-
20240826.1753.4aeeb70 @System
[root@rhel-example ~]#
```

2. 以前のStorageGRIDパッケージを削除します。 `dnf remove images-package service-package`

   > 現在実行しているStorageGRIDのバージョン、またはアップグレード先のStorageGRIDのバージョンのインストールアーカイブは削除しないでください。

   表示される警告は無視してかまいません。これらのファイルは、新しいStorageGRIDパッケージをインストールするときに置き換えられたファイルを参照します。

   例：

```
[root@rhel-example ~]# dnf remove StorageGRID-Webscale-Images-11-6-
0.x86_64 StorageGRID-Webscale-Service-11-6-0.x86_64
Updating Subscription Management repositories.
Unable to read consumer identity

This system is not registered with an entitlement server. You can
use subscription-manager to register.

Dependencies resolved.
```

```
================================================================================
========
Package            Architecture      Version           Repository
Size
================================================================================
========
Removing:
StorageGRID-Webscale-Images-11-6-0 x86_64 11.6.0-
20220210.0232.8d56cfe @System 2.7 G
StorageGRID-Webscale-Service-11-6-0 x86_64 11.6.0-
20220210.0232.8d56cfe @System 7.5 M

Transaction Summary
================================================================================
========
Remove 2 Packages

Freed space: 2.8 G
Is this ok [y/N]: y
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing: 1/1
  Running scriptlet: StorageGRID-Webscale-Service-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64  1/2
  Erasing: StorageGRID-Webscale-Service-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64  1/2
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/ipv6.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/ipv4.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/eui64.pyc
: remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/eui48.pyc
: remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/__init__.
pyc: remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/ip/sets.pyc:
```

```
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/ip/rfc1924.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/ip/nmap.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/ip/iana.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/ip/glob.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/ip/__init__.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/fbsocket.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/eui/ieee.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/eui/__init__.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/core.pyc: remove
failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/contrib/subnet_spl
itter.pyc: remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/contrib/__init__.p
yc: remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/compat.pyc: remove
failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/__init__.pyc:
remove failed: No such file or directory

  Erasing: StorageGRID-Webscale-Images-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64   2/2
  Verifying: StorageGRID-Webscale-Images-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64  1/2
  Verifying: StorageGRID-Webscale-Service-11-6-0-11.6.0-
```

```
20220210.0232.8d56cfe.x86_64  2/2
Installed products updated.

Removed:
  StorageGRID-Webscale-Images-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64
  StorageGRID-Webscale-Service-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64

Complete!
[root@rhel-example ~]#
```

Ubuntu と Debian

1. インストールされているStorageGRIDパッケージのリストを取得します。 `dpkg -l | grep storagegrid`

   例：

```
root@debian-example:~# dpkg -l | grep storagegrid
ii  storagegrid-webscale-images-11-6-0  11.6.0-20220210.0232.8d56cfe
amd64 StorageGRID Webscale docker images for 11.6.0
ii  storagegrid-webscale-images-11-7-0  11.7.0-
20230424.2238.1a2cf8c.dev-signed amd64 StorageGRID Webscale docker
images for 11.7.0
ii  storagegrid-webscale-images-11-8-0  11.8.0-20240131.0139.e3e0c87
amd64 StorageGRID Webscale docker images for 11.8.0
ii  storagegrid-webscale-images-11-9-0  11.9.0-20240826.1753.4aeeb70
amd64 StorageGRID Webscale docker images for 11.9.0
ii  storagegrid-webscale-service-11-6-0 11.6.0-20220210.0232.8d56cfe
amd64 StorageGRID Webscale host services for 11.6.0
ii  storagegrid-webscale-service-11-7-0 11.7.0-20230424.2238.1a2cf8c
amd64 StorageGRID Webscale host services for 11.7.0
ii  storagegrid-webscale-service-11-8-0 11.8.0-20240131.0139.e3e0c87
amd64 StorageGRID Webscale host services for 11.8.0
ii  storagegrid-webscale-service-11-9-0 11.9.0-20240826.1753.4aeeb70
amd64 StorageGRID Webscale host services for 11.9.0
root@debian-example:~#
```

2. 以前のStorageGRIDパッケージを削除します。 `dpkg -r images-package service-package`

   > 現在実行しているStorageGRIDのバージョン、またはアップグレード先のStorageGRIDのバージョンのインストールアーカイブは削除しないでください。

   例：

```
root@debian-example:~# dpkg -r storagegrid-webscale-service-11-6-0
storagegrid-webscale-images-11-6-0
(Reading database ... 38190 files and directories currently
installed.)
Removing storagegrid-webscale-service-11-6-0 (11.6.0-
20220210.0232.8d56cfe) ...
locale: Cannot set LC_CTYPE to default locale: No such file or
directory
locale: Cannot set LC_MESSAGES to default locale: No such file or
directory
locale: Cannot set LC_ALL to default locale: No such file or
directory
dpkg: warning: while removing storagegrid-webscale-service-11-6-0,
directory '/usr/lib/python2.7/dist-
packages/netapp/storagegrid/vendor/latest' not empty so not removed
Removing storagegrid-webscale-images-11-6-0 (11.6.0-
20220210.0232.8d56cfe) ...
root@debian-example:~#
```

1. StorageGRIDコンテナイメージを削除します。

Docker

1. インストールされているコンテナイメージのリストをキャプチャします。 `docker images`

   例：

```
[root@docker-example ~]# docker images
REPOSITORY           TAG             IMAGE ID       CREATED
SIZE
storagegrid-11.9.0   Admin_Node      610f2595bcb4   2 days ago
2.77GB
storagegrid-11.9.0   Storage_Node    7f73d33eb880   2 days ago
2.65GB
storagegrid-11.9.0   API_Gateway     2f0bb79526e9   2 days ago
1.82GB
storagegrid-11.8.0   Storage_Node    7125480de71b   7 months ago
2.54GB
storagegrid-11.8.0   Admin_Node      404e9f1bd173   7 months ago
2.63GB
storagegrid-11.8.0   Archive_Node    c3294a29697c   7 months ago
2.39GB
storagegrid-11.8.0   API_Gateway     1f88f24b9098   7 months ago
1.74GB
storagegrid-11.7.0   Storage_Node    1655350eff6f   16 months ago
2.51GB
storagegrid-11.7.0   Admin_Node      872258dd0dc8   16 months ago
2.48GB
storagegrid-11.7.0   Archive_Node    121e7c8b6d3b   16 months ago
2.41GB
storagegrid-11.7.0   API_Gateway     5b7a26e382de   16 months ago
1.77GB
storagegrid-11.6.0   Admin_Node      ee39f71a73e1   2 years ago
2.38GB
storagegrid-11.6.0   Storage_Node    f5ef895dcad0   2 years ago
2.08GB
storagegrid-11.6.0   Archive_Node    5782de552db0   2 years ago
1.95GB
storagegrid-11.6.0   API_Gateway     cb480ed37eea   2 years ago
1.35GB
[root@docker-example ~]#
```

2. 以前のバージョンのStorageGRIDのコンテナイメージを削除します。 `docker rmi image id`

   現在実行しているStorageGRIDのバージョン、またはアップグレード先のStorageGRIDのバージョンのコンテナイメージは削除しないでください。

例：

```
[root@docker-example ~]# docker rmi cb480ed37eea
Untagged: storagegrid-11.6.0:API_Gateway
Deleted:
sha256:cb480ed37eea0ae9cf3522de1dadfbff0075010d89c1c0a2337a3178051dd
f02
Deleted:
sha256:5f269aabf15c32c1fe6f36329c304b6c6ecb563d973794b9b59e8e5ab8ccc
afa
Deleted:
sha256:47c2b2c295a77b312b8db69db58a02d8e09e929e121352bec713fa12dae66
bde
[root@docker-example ~]#
```

ポドマン

1. インストールされているコンテナイメージのリストをキャプチャします。 `podman images`

   例：

```
[root@podman-example ~]# podman images
REPOSITORY                    TAG           IMAGE ID      CREATED
SIZE
localhost/storagegrid-11.8.0  Storage_Node  7125480de71b  7 months
ago   2.57 GB
localhost/storagegrid-11.8.0  Admin_Node    404e9f1bd173  7 months
ago   2.67 GB
localhost/storagegrid-11.8.0  Archive_Node  c3294a29697c  7 months
ago   2.42 GB
localhost/storagegrid-11.8.0  API_Gateway   1f88f24b9098  7 months
ago   1.77 GB
localhost/storagegrid-11.7.0  Storage_Node  1655350eff6f  16 months
ago  2.54 GB
localhost/storagegrid-11.7.0  Admin_Node    872258dd0dc8  16 months
ago  2.51 GB
localhost/storagegrid-11.7.0  Archive_Node  121e7c8b6d3b  16 months
ago  2.44 GB
localhost/storagegrid-11.7.0  API_Gateway   5b7a26e382de  16 months
ago  1.8 GB
localhost/storagegrid-11.6.0  Admin_Node    ee39f71a73e1  2 years
ago    2.42 GB
localhost/storagegrid-11.6.0  Storage_Node  f5ef895dcad0  2 years
ago    2.11 GB
localhost/storagegrid-11.6.0  Archive_Node  5782de552db0  2 years
ago    1.98 GB
localhost/storagegrid-11.6.0  API_Gateway   cb480ed37eea  2 years
ago    1.38 GB
[root@podman-example ~]#
```

2. 以前のバージョンのStorageGRIDのコンテナイメージを削除します。 `podman rmi image id`

> 現在実行しているStorageGRIDのバージョン、またはアップグレード先のStorageGRIDのバージョンのコンテナイメージは削除しないでください。

例：

```
[root@podman-example ~]# podman rmi f5ef895dcad0
Untagged: localhost/storagegrid-11.6.0:Storage_Node
Deleted:
f5ef895dcad0d78d0fd21a07dd132d7c7f65f45d80ee7205a4d615494e44cbb7
[root@podman-example ~]#
```

StorageGRIDアップグレードを実行する

StorageGRID 12.1 にアップグレードし、同時にそのリリース向けの最新のホットフィックスを適用できます。StorageGRID のアップグレードページには、推奨されるアップグレード手順と、適切なダウンロードページへの直接リンクが記載されています。

開始する前に

すべての考慮事項を確認し、計画と準備の手順をすべて完了しておきます。

> 緊急にストレージを拡張して容量を増やす必要がある場合（ストレージがほぼいっぱいの場合）は、アップグレードを開始しないでください。アップグレード手順を適時に完了してください。回復が必要な場合は、テクニカル サポートにお問い合わせください。

StorageGRID のアップグレードページにアクセスします

最初の手順として、グリッドマネージャのStorageGRID の[Upgrade]ページにアクセスします。

手順

1. を使用してGrid Managerにサインインし"サポートされている Web ブラウザ"ます。
2. メンテナンス > システム > *ソフトウェアアップデート*を選択します。
3. StorageGRID のアップグレードタイルで、*アップグレード*を選択します。

ファイルを選択

StorageGRID アップグレードページの更新パスには、最新の StorageGRID リリースにするためにインストールする必要のあるメジャーバージョン（例：12.1.0）とホットフィックス（例：12.1.0.1）が示されています。推奨バージョンとホットフィックスは、表示されている順序でインストールしてください。

> 更新パスが表示されない場合は、ブラウザがNetAppサポート サイトにアクセスできないか、AutoSupportページ (*[サポート] > [ツール] > [AutoSupport] > [設定]) の [ソフトウェア更新の確認] チェックボックスが無効になっている可能性があります。

手順

1. [ファイルの選択]ステップで、更新パスを確認します。
2. [Download files]セクションで、各*[Download]*リンクを選択して、NetApp Support Site から必要なファイルをダウンロードします。

   更新パスが表示されない場合は、に移動して "NetAppのダウンロード：StorageGRID"新しいバージョンまたはホットフィックスが利用可能かどうかを確認し、必要なファイルをダウンロードします。

   > すべてのLinuxホストにRPMパッケージまたはDEBパッケージをダウンロードしてインストールする必要がある場合は、StorageGRID のアップグレードファイルとホットフィックスファイルが更新パスにすでにリストされている可能性があります。

3. *参照*を選択して、バージョンアップグレードファイルをStorageGRIDにアップロードします：
   `NetApp_StorageGRID_12.1.0_Software_uniqueID.upgrade`

   アップロードとコード署名の検証が完了すると、ファイル名の横に緑色のチェックマークが表示されま

す。

4. ホットフィックスファイルをダウンロードした場合は、*[参照]*を選択してそのファイルをアップロードします。ホットフィックスはバージョンのアップグレード時に自動的に適用されます。
5. 「 * Continue * 」を選択します。

事前確認を実行

事前確認を実行すると、グリッドのアップグレードを開始する前にアップグレードの問題を検出して解決できます。

手順

1. [Run prechecks]*ステップで、最初にグリッドのプロビジョニングパスフレーズを入力します。
2. [リカバリパッケージのダウンロード] を選択します。

   プライマリ管理ノードをアップグレードする前に、リカバリ パッケージ ファイルの現在のコピーをダウンロードする必要があります。リカバリ パッケージ ファイルを使用すると、障害が発生した場合にシステムを復元できます。

3. ファイルをダウンロードしたら、ファイルを含むコンテンツにアクセスできることを確認します `Passwords.txt`。
4. ダウンロードしたファイルを(`.zip`2つの安全で安全な別の場所にコピーします。

   > リカバリ パッケージ ファイルには、 StorageGRIDシステムからデータを取得するために使用できる暗号化キーとパスワードが含まれているため、セキュリティで保護する必要があります。

5. [事前確認を実行]*を選択し、事前確認が完了するまで待ちます。
6. 報告された各事前チェックの詳細を確認し、報告されたエラーをすべて解決してください。StorageGRID 12.1リリースの "StorageGRID ソフトウェアアップグレード解決ガイド"を参照してください。

   システムをアップグレードする前に、precheck_errors_をすべて解決する必要があります。ただし、アップグレード前にprecheck_warnings_に対処する必要はありません。

   > カスタムのファイアウォールポートが開いている場合は、事前確認の実行中に通知されます。アップグレードを続行する前に、テクニカルサポートに連絡する必要があります。

7. 報告された問題を解決するために設定を変更した場合は、*[事前確認を実行]*をもう一度選択して、更新された結果を取得します。

   すべてのエラーが解決されると、アップグレードを開始するように求められます。

プライマリ管理ノードのアップグレードを開始し、アップグレードを開始します

アップグレードを開始すると、アップグレードの事前確認が再度実行され、プライマリ管理ノードが自動的にアップグレードされます。アップグレードのこの部分には最大30分かかることがあります。

プライマリ管理ノードのアップグレード中は、他のGrid Managerページにはアクセスできません。監査ログも使用できなくなります。

手順

1. [アップグレードの開始]*を選択します。

   Grid Managerに一時的にアクセスできなくなることを通知する警告が表示されます。

2. [OK]*を選択して警告を確認し、アップグレードを開始します。
3. アップグレードの事前確認が実行され、プライマリ管理ノードがアップグレードされるまで待ちます。

   事前確認でエラーが報告された場合は、それらを解決し、*[アップグレードの開始]*をもう一度選択します。

   オンラインで準備が完了している別の管理ノードがグリッドにある場合は、そのノードを使用してプライマリ管理ノードのステータスを監視できます。プライマリ管理ノードをアップグレードしたらすぐに、他のグリッドノードを承認できます。

4. 必要に応じて*を選択して[他のノードのアップグレード]*ステップにアクセスします。

他のノードをアップグレードする

すべてのグリッドノードをアップグレードする必要がありますが、複数のアップグレードセッションを実行してアップグレードの順序をカスタマイズすることができます。たとえば、1つのセッションでサイトAのノードをアップグレードしてから、以降のセッションでサイトBのノードをアップグレードすることができます。アップグレードを複数のセッションで実行する場合は、すべてのノードがアップグレードされるまで新しい機能の使用を開始できないことに注意してください。

ノードのアップグレード順序が重要な場合は、ノードまたはノードグループを 1 つずつ承認し、各ノードでアップグレードが完了するまで待ってから、次のノードまたはノードグループを承認します。

グリッドノードでアップグレードを開始すると、そのノードのサービスは停止します。グリッドノードはあとでリブートされます。ノードと通信しているクライアントアプリケーションのサービスの中断を回避するために、ノードを停止およびリブートする準備ができていることを確認できないかぎり、ノードのアップグレードを承認しないでください。必要に応じて、メンテナンス時間をスケジュールするか、お客様に通知します。

手順

1. [他のノードをアップグレード]*手順については、概要を確認します。概要には、アップグレード全体の開始時刻と各メジャーアップグレードタスクのステータスが表示されます。
   - *アップグレードサービスの開始*は、最初のアップグレードタスクです。このタスクでは、ソフトウェアファイルがグリッドノードに配信され、各ノードでアップグレードサービスが開始されます。
   - アップグレード サービスの開始 タスクが完了すると、他のグリッド ノードのアップグレード タスクが開始され、リカバリ パッケージの新しいコピーをダウンロードするように求められます。
2. プロンプトが表示されたら、プロビジョニング パスフレーズを入力し、リカバリ パッケージの新しいコピーをダウンロードします。

プライマリ管理ノードがアップグレードされた後、リカバリ パッケージ ファイルの新しいコピーをダウンロードする必要があります。リカバリ パッケージ ファイルを使用すると、障害が発生した場合にシステムを復元できます。

3. 各タイプのノードのステータステーブルを確認します。非プライマリ管理ノード、ゲートウェイノード、ストレージノードのテーブルが用意されています。

   グリッドノードは、テーブルが最初に表示された時点で次のいずれかの段階になります。

   - アップグレードを開梱しています
   - ダウンロード中
   - 承認待ちです

4. アップグレードするグリッドノードを選択する準備ができたら（または選択したノードの承認を取り消す必要がある場合）、次の手順に従います。

   StorageGRID 12.1 へのアップグレードで、すべてのノードではなく個々のノードを承認する場合は、次のサイトに進む前にサイト全体をアップグレードすることがベストプラクティスです。

タスク	指示
特定のサイトのすべてのノードなど、承認する特定のノードを検索します	[検索]フィールドに検索文字列を入力します
アップグレードするノードをすべて選択します	[すべてのノードを承認]*を選択します
アップグレードの対象として同じタイプのノードをすべて選択する（[All Storage Nodes]など）	ノードタイプの*[すべて承認]*ボタンを選択します 同じタイプの複数のノードを承認すると、ノードは一度に 1 つずつアップグレードされます。
アップグレードする個 々 のノードを選択します	ノードの*[承認]*ボタンを選択します
選択したすべてのノードでアップグレードを延期します	[すべてのノードを承認しない]*を選択します
同じタイプの選択したすべてのノードでアップグレードを延期します	ノードタイプの*[すべて未承認]*ボタンを選択します
個 々 のノードでアップグレードを延期します	ノードの*[未承認]*ボタンを選択します

5. 承認されたノードが次のアップグレード段階に進むまで待ちます。

   - 承認され、アップグレードを待機しています
   - サービスを停止しています

[ステージ]が*[サービスの停止中]*になっているノードを削除することはできません。[未承認]ボタンは無効になっています。

- コンテナを停止しています
- Dockerイメージをクリーンアップしています
- ベースOSパッケージをアップグレードしています

アプライアンスノードがこの段階になると、アプライアンスのStorageGRID アプライアンスインストーラソフトウェアが更新されます。この自動プロセスにより、StorageGRID アプライアンスインストーラのバージョンが StorageGRID ソフトウェアのバージョンと常に同期された状態になります。

- リブートしています

一部のアプライアンスモデルでは、ファームウェアとBIOSをアップグレードするために複数回リブートすることがあります。

- リブート後に手順を実行しています
- サービスを開始しています
- 完了

6. すべてのグリッドノードがアップグレードされるまで、必要な回数だけを繰り返し承認ステップます。

アップグレードを完了する

すべてのグリッドノードのアップグレードステージが完了すると、*[他のグリッドノードをアップグレード]*タスクが[完了]と表示されます。残りのアップグレードタスクはバックグラウンドで自動的に実行されます。

手順

1. *機能の有効化*タスクが完了すると（最大1時間）、アップグレードされたStorageGRIDバージョンの"新機能"をすぐに使用開始できます。

   最後のアップグレード手順*が完了すると、アップグレードが完了します。最初のステップである*ファイルの選択*が緑色の成功バナーで再表示されます。

2. グリッドの動作が正常に戻っていることを確認します。
   a. サービスが正常に動作していること、および予期しないアラートが発生していないことを確認してください。
   b. StorageGRID システムへのクライアント接続が想定どおり動作していることを確認する。

関連情報

"アップグレード中にシステムが受ける影響"

StorageGRIDアップグレードの問題のトラブルシューティング

アップグレードの実行時に問題が発生した場合は、問題 を自分で解決できることがあります。問題 を解決できない場合は、できるだけ多くの情報を収集し、テクニカルサポー

トにお問い合わせください。

アップグレードが完了しない

次のセクションでは、アップグレードが部分的に失敗した場合のリカバリ方法について説明します。

アップグレードの事前確認エラー

問題を検出して解決するために、実際のアップグレードを開始する前にアップグレードの事前確認を手動で実行できます。事前確認で報告されるほとんどのエラーには、問題 の解決方法が表示されます。

プロビジョニングに失敗しました

自動プロビジョニングプロセスが失敗する場合は、テクニカルサポートにお問い合わせください。

グリッドノードがクラッシュするか起動しない

アップグレードプロセス中にグリッドノードがクラッシュする、またはアップグレードの終了後に正常に起動しない場合は、テクニカルサポートに調査を依頼して、根本的な問題を修正してください。

データの取り込みまたは読み出しが中断される

グリッドノードをアップグレードしていないときにデータの取り込みまたは読み出しが予期せず中断される場合は、テクニカルサポートにお問い合わせください。

データベースのアップグレードエラーです

データベースのアップグレードがエラーで失敗した場合は、アップグレードを再試行します。それでも失敗する場合は、テクニカルサポートにお問い合わせください。

関連情報

"ソフトウェアのアップグレード前のシステム状態の確認"

ユーザインターフェイスに関する問題

アップグレードの実行中または実行後に、Grid ManagerまたはTenant Managerで問題が発生する可能性があります。

Grid Managerのアップグレード中に複数のエラーメッセージが表示される

プライマリ管理ノードのアップグレード中にブラウザをリフレッシュしたり、別のGrid Managerページに移動したりすると、「503：Service unavailable」および「Problem connecting to the server」というメッセージが複数表示されることがあります。これらのメッセージは無視してかまいません。ノードがアップグレードされるとすぐに表示されなくなります。

アップグレードを開始してから1時間以上経過してもこれらのメッセージが表示される場合は、何らかの原因でプライマリ管理ノードをアップグレードできなかった可能性があります。問題 を自分で解決できない場合は、テクニカルサポートにお問い合わせください。

Web インターフェイスが想定どおりに応答しません

StorageGRID ソフトウェアのアップグレード後に Grid Manager またはテナントマネージャが想定どおりに応

答しない場合がある。

Web インターフェイスで問題が発生した場合：

- を使用していることを確認し"サポートされている Web ブラウザ"ます。

  通常、ブラウザサポートは StorageGRID リリースごとに変更されます。

- Web ブラウザのキャッシュをクリアします。

  キャッシュをクリアすると、以前のバージョンの StorageGRID ソフトウェアで使用されていた古いリソースが削除され、ユーザインターフェイスが再び正しく動作するようになります。手順については、 Web ブラウザのドキュメントを参照してください。

「Docker image availability check」エラーメッセージ

アップグレードプロセスを開始しようとすると、「The following issues were identified by the Docker image availability check validation suite」というエラーメッセージが表示されることがあります。アップグレードを完了する前に、すべての問題を解決する必要があります。

見つかった問題の解決に必要な変更内容がわからない場合は、テクニカルサポートにお問い合わせください。

メッセージ	原因	解決策
アップグレードバージョンを特定できません。アップグレードバージョン情報ファイルが `{file_path}` 想定される形式と一致しませんでした。	アップグレードパッケージが破損しています。	アップグレードパッケージを再度アップロードしてやり直してください。問題が解決しない場合は、テクニカルサポートにお問い合わせください。
アップグレードバージョン情報ファイル `{file_path}`が見つかりませんでした。アップグレードバージョンを特定できません。	アップグレードパッケージが破損しています。	アップグレードパッケージを再度アップロードしてやり直してください。問題が解決しない場合は、テクニカルサポートにお問い合わせください。
に現在インストールされているリリースバージョンを特定できません `{node_name}`。	ノード上の重要なファイルが破損しています。	テクニカルサポートにお問い合わせください。
のバージョンをリストしようとしているときに接続エラーが発生しました `{node_name}`	ノードがオフラインであるか、接続が中断されました。	すべてのノードがオンラインで、プライマリ管理ノードからアクセスできることを確認して、操作をやり直します。

メッセージ	原因	解決策
ノードのホスト `{node_name}` にStorageGRIDイメージがロードされていませ `{upgrade_version}` ん。アップグレードを続行するには、イメージとサービスがホストにインストールされている必要があります。	ノードを実行しているホストにアップグレード用の RPM パッケージまたは DEB パッケージがインストールされていないか、イメージのインポートがまだ終了していません。 • 注：このエラーは、 Linux でコンテナとして実行されている環境 ノードのみに該当します。	RPM パッケージまたは DEB パッケージが、ノードが実行されているすべての Linux ホストにインストールされていることを確認します。サービスとイメージファイルの両方について、バージョンが正しいことを確認します。数分待ってから再試行してください。 を参照して "Linux ：すべてのホストに RPM パッケージまたは DEB パッケージをインストールします"
ノードチェック中のエラー `{node_name}`	予期しないエラーが発生しました。	数分待ってから再試行してください。
事前確認の実行中に不明なエラーが発生しました。 `{error_string}`	予期しないエラーが発生しました。	数分待ってから再試行してください。

StorageGRIDホットフィックスの適用

StorageGRID ホットフィックス手順

ソフトウェアの問題が検出され、次の機能リリースの前に解決された場合は、StorageGRID システムへのホットフィックスの適用が必要になる場合があります。

StorageGRID のホットフィックスには、フィーチャーパックまたはフィーチャーパックに含まれないソフトウェアの変更が含まれます。今後のリリースにも同じ変更が含まれます。さらに、各ホットフィックスリリースには、その機能またはパッチリリースに含まれる以前のすべてのホットフィックスがまとめて含まれています。

ホットフィックスの適用に関する考慮事項

別のメンテナンス手順 が実行されているときは、StorageGRID ホットフィックスを適用できません。たとえば、運用停止、拡張、またはリカバリ手順 の実行中はホットフィックスを適用できません。

> ノードまたはサイトの運用停止手順 が一時停止されている場合、ホットフィックスを安全に適用できます。また、 StorageGRID アップグレード手順 の最終段階でホットフィックスを適用できる場合があります。詳細については、 StorageGRID ソフトウェアのアップグレード手順を参照してください。

Grid Manager でホットフィックスをアップロードすると、ホットフィックスはプライマリ管理ノードに自動的に適用されます。その後、 StorageGRID システム内の残りのノードへのホットフィックスの適用を承認できます。

1 つ以上のノードへのホットフィックスの適用に失敗した場合は、ホットフィックスの進捗状況テーブルの

Details 列に障害の理由が表示されます。エラーの原因となった問題を解決してから、プロセス全体を再試行する必要があります。ホットフィックスの適用に成功していたノードは、以降のアプリケーションではスキップされます。必要に応じて、すべてのノードが更新されるまで、ホットフィックスの適用を何度でも安全に再試行できます。アプリケーションを完了するには、すべてのグリッドノードにホットフィックスが正常にインストールされている必要があります。

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

リカバリと拡張のためのホットフィックスの適用方法

グリッドにホットフィックスが適用されると、プライマリ管理ノードまたは非プライマリ管理ノードは、復旧操作によって復元されたノード、または拡張によって追加されたノードに、同じホットフィックスバージョンを自動的にインストールします。プライマリ以外の管理ノードにサインインしている場合、プライマリ管理ノードを含む任意のノードを復旧できます。プライマリ以外の管理ノードからノードを復旧した場合、復旧したノードにはその管理ノードがホットフィックスを適用します。

プライマリ管理ノードをStorageGRIDインストーラーから復旧する必要がある場合は、正しいStorageGRIDリリースを手動でインストールしてからホットフィックスを適用する必要があります。プライマリ管理ノードの最終的なStorageGRIDバージョンは、グリッド内の他のノードのバージョンと一致している必要があります。

次の例は、プライマリ管理ノードを復旧する際に、プライマリ以外の管理ノードにサインインしている状態でホットフィックスを適用する方法を示しています。

1. グリッドで StorageGRID 11._A.B_VERSION が実行されており、最新のホットフィックスが適用されているとします。「グリッドバージョン」は11._A.B.y_です。
2. プライマリ管理ノードに障害が発生した場合。
3. プライマリ管理ノードを StorageGRID 11.*A.B_* を使用して再導入し、リカバリ手順 を実行します。

> グリッドのバージョンと一致する必要がある場合は、ノードの導入時にマイナーリリースを使用できます。メジャーリリースを先に導入する必要はありません。

4. 次に、プライマリ管理ノードにホットフィックス 11.*A.B.C.* を適用します。

ホットフィックスを適用したときの**StorageGRID**への影響

ホットフィックスを適用したときに、 StorageGRID システムにどのような影響が生じるのかを理解しておく必要があります。

StorageGRIDのホットフィックスはシステム停止を伴わない

StorageGRIDシステムは、ホットフィックス適用プロセス全体を通じてクライアントアプリケーションからデータを取り込み、読み出すことができます。同じタイプのすべてのノード（ストレージノードなど）をホットフィックスに承認すると、ノードが一度に1つずつ停止されるため、すべてのグリッドノードまたは特定のタイプのすべてのグリッドノードが使用できなくなることはありません。

継続的な可用性を確保するには、各オブジェクトの複数のコピーを格納するように指定するルールをILMポリシーに含めるようにしてください。また、すべての外部S3クライアントが次のいずれかに要求を送信するように設定されていることを確認する必要があります。

- ハイアベイラビリティ（HA）グループの仮想IPアドレス
- 高可用性を備えたサードパーティ製ロードバランサ
- 各クライアントに複数のゲートウェイノードが必要
- クライアントごとに複数のストレージノード

クライアントアプリケーションが短時間中断される可能性があります

StorageGRID システムは、ホットフィックス適用プロセス中もクライアントアプリケーションからデータを取り込み、読み出すことができますが、ホットフィックスが個々のゲートウェイノードまたはストレージノードのサービスを再開する必要がある場合は、それらのノードへのクライアント接続が一時的に中断されることがあります。接続はホットフィックスの適用終了後に再開され、個々のノードのサービスも再開されます。

接続の中断が短時間でも許容されない場合は、ホットフィックス適用時のダウンタイムをスケジュールする必要があります。特定のノードが更新されるタイミングをスケジュールするには、選択的な承認を使用できます。

> 複数のゲートウェイとハイアベイラビリティ（ HA ）グループを使用すると、ホットフィックス適用プロセス中に自動フェイルオーバーを実行できます。の手順を参照してください"ハイアベイラビリティグループを設定する"。

アラートおよび **SNMP** 通知がトリガーされる可能性があります

サービスが再起動されたとき、および StorageGRID システムを複数バージョンが混在した環境で使用している場合（一部のグリッドノードで以前のバージョンを実行し、その他のノードはより新しいバージョンにアップグレードしている場合）には、アラートと SNMP 通知がトリガーされることがあります。通常、これらのアラートと通知はホットフィックスが完了するとクリアされます。

設定の変更は制限されています

StorageGRID にホットフィックスを適用する際は、次の点に注意

- ホットフィックスがすべてのノードに適用されるまで、グリッド設定の変更（グリッドネットワークサブネットの指定や保留中のグリッドノードの承認など）は行わないでください。
- ホットフィックスがすべてのノードに適用されるまで、ILM設定を更新しないでください。

StorageGRIDホットフィックスに必要な材料を入手

ホットフィックスを適用する前に、必要な項目をすべて用意する必要があります。

項目	脚注
StorageGRID ホットフィックスファイル	StorageGRID ホットフィックスファイルをダウンロードする必要があります。

項目	脚注
• ネットワークポート • "サポートされている Web ブラウザ" • SSH クライアント（ PuTTY など）	
復旧パッケージ(.zip）ファイル	修正プログラムを適用する前に、"最新のリカバリパッケージファイルをダウンロードする"ホットフィックス中に問題が発生した場合に備えて。次に、修正プログラムを適用した後、回復パッケージ ファイルの新しいコピーをダウンロードし、安全な場所に保存します。更新されたリカバリ パッケージ ファイルを使用すると、障害が発生した場合にシステムを復元できます。
Passwords.txt ファイル	オプションであり、SSH クライアントを使用して手動で修正プログラムを適用する場合にのみ使用されます。その `Passwords.txt`ファイルは回復パッケージの一部です `.zip`ファイル。
プロビジョニングパスフレーズ	このパスフレーズは、 StorageGRID システムが最初にインストールされるときに作成されて文書化されます。プロビジョニングパスフレーズはファイルに含まれていません `Passwords.txt`。
関連ドキュメント	`readme.txt`ファイル（ホットフィックス用）。このファイルは、ホットフィックスのダウンロードページにあります。ホットフィックスを適用する前に、ファイルをよく確認して `readme`ください。

StorageGRIDホットフィックスファイルをダウンロードします

ホットフィックスを適用する前に、ホットフィックスファイルをダウンロードする必要があります。

手順

1. に進みます "NetAppのダウンロード：StorageGRID"。
2. [利用可能なソフトウェア] の下にある下矢印をクリックすると、ダウンロード可能なホットフィックスのリストが表示されます。

   ホットフィックスファイルのバージョンの形式は 11.4_.x.y__ です。

3. 更新に含まれている変更を確認します。

   がインストールされていてホットフィックスを適用する必要がある場合は"プライマリ管理ノードをリカバリしました"、他のグリッドノードにインストールされている同じバージョンのホットフィックスを選択します。

   a. ダウンロードするホットフィックスのバージョンを選択し、 * Go * を選択します。

b. NetAppアカウントのユーザ名とパスワードを使用してサインインします。

c. エンドユーザライセンス契約を読んで同意します。

選択したバージョンのダウンロードページが表示されます。

d. ホットフィックスファイルをダウンロードし `readme.txt`て、ホットフィックスに含まれる変更の概要を確認します。

4. ホットフィックスのダウンロードボタンを選択してファイルを保存します。

> このファイルの名前は変更しないでください。

> macOSデバイスを使用している場合は、ホットフィックスファイルが自動的にファイルとして保存されることがあります `.txt`。その場合は、拡張子を付けずにファイルの名前を変更する必要があり `.txt`ます。

5. ダウンロードする場所を選択し、「 * 保存 * 」を選択します。

StorageGRIDホットフィックスを適用する前にシステムの状態を確認してください

システムにホットフィックスを適用する準備ができていることを確認する必要があります。

手順

1. を使用してGrid Managerにサインインし"サポートされている Web ブラウザ"ます。
2. 可能であれば、システムが正常に稼働し、すべてのグリッドノードがグリッドに接続されていることを確認します。

接続されているノードには、ノードページに緑色のチェックマークが表示されます。

3. 可能であれば、現在のアラートがないかを確認し、ある場合は解決します。
4. 手順 のアップグレード、リカバリ、拡張、運用停止など、他のメンテナンス手順が実行中でないことを確認します。

アクティブなメンテナンス手順が完了してからホットフィックスを適用してください。

別のメンテナンス手順 が実行されているときは、StorageGRID ホットフィックスを適用できません。たとえば、運用停止、拡張、またはリカバリ手順 の実行中はホットフィックスを適用できません。

> ノードまたはサイトの場合は"運用停止手順 が一時停止されています"、ホットフィックスを安全に適用できます。また、 StorageGRID アップグレード手順 の最終段階でホットフィックスを適用できる場合があります。の手順を参照してください"StorageGRID ソフトウェアのアップグレード"。

StorageGRID でホットフィックスを適用します

ホットフィックスは、最初にプライマリ管理ノードに自動的に適用されます。その後、

すべてのノードが同じバージョンのソフトウェアを実行するまでの間、他のグリッドノードへのホットフィックスの適用を承認する必要があります。個々のグリッドノード、グリッドノードのグループ、またはすべてのグリッドノードを選択して、承認順序をカスタマイズできます。

開始する前に

- を確認しておきます"ホットフィックスの適用に関する考慮事項"。
- プロビジョニングパスフレーズを用意します。
- Rootアクセス権限またはMaintenance権限が必要です。

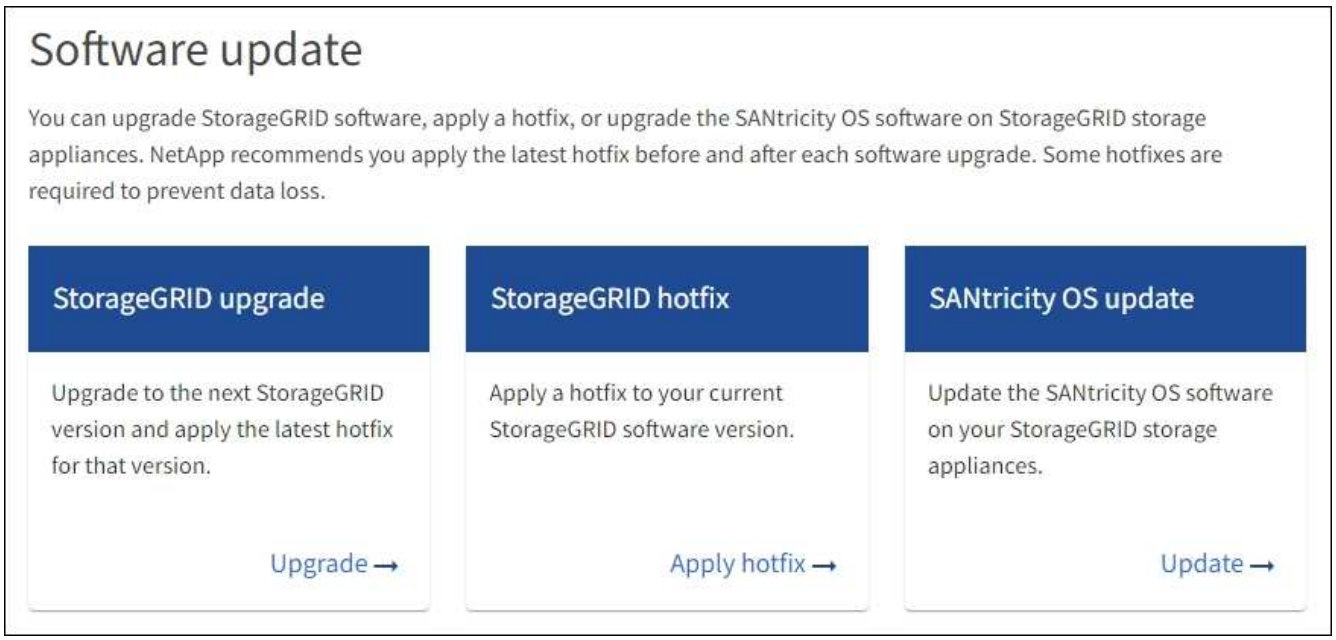
タスクの内容

- ホットフィックスのノードへの適用は遅延できますが、ホットフィックスの適用はすべてのノードにホットフィックスを適用するまで完了しません。
- ホットフィックスプロセスが完了するまで、StorageGRID ソフトウェアのアップグレードやSANtricity OSの更新は実行できません。

手順

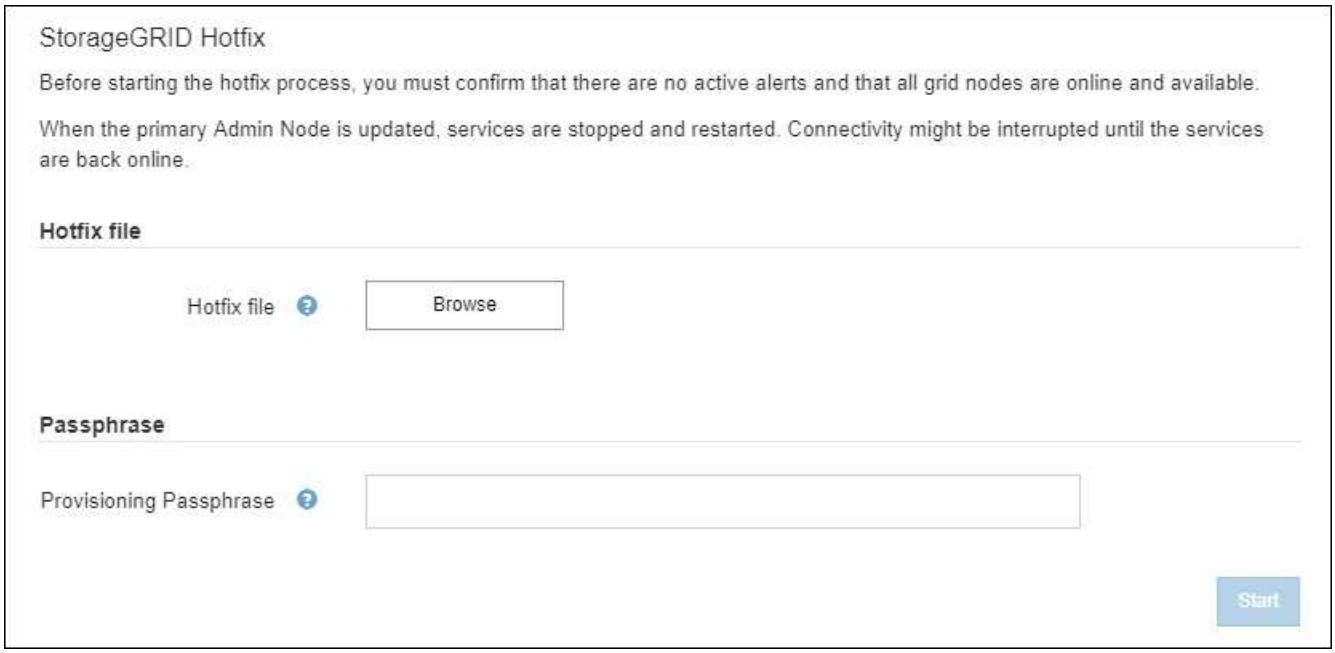
1. を使用してGrid Managerにサインインし"サポートされている Web ブラウザ"ます。
2. メンテナンス > システム > *ソフトウェアアップデート*を選択します。

   Software Update ページが表示されます。



3. [* ホットフィックスの適用 *] を選択します。

   StorageGRID Hotfix ページが表示されます。



を選択します"]

4. NetApp Support Site からダウンロードしたホットフィックスファイルを選択します。

   a. [* 参照 *] を選択します。

   b. ファイルを探して選択します。

      `hotfix-install-version`

   c. 「 * 開く * 」を選択します。

      ファイルがアップロードされます。アップロードが完了すると、ファイル名が [詳細] フィールドに表示されます。

      ファイル名は検証プロセスの一部であるため、変更しないでください。

5. プロビジョニングパスフレーズをテキストボックスに入力します。

   「 * Start * （スタート * ）」ボタンが有効になります。

6. 「 * Start （開始）」を選択します

   プライマリ管理ノードのサービスを再起動する際にブラウザの接続が一時的に失われる可能性があることを示す警告が表示されます。

7. [OK] を選択して、プライマリ管理ノードへのホットフィックスの適用を開始します。

   ホットフィックスの適用が開始されると、次

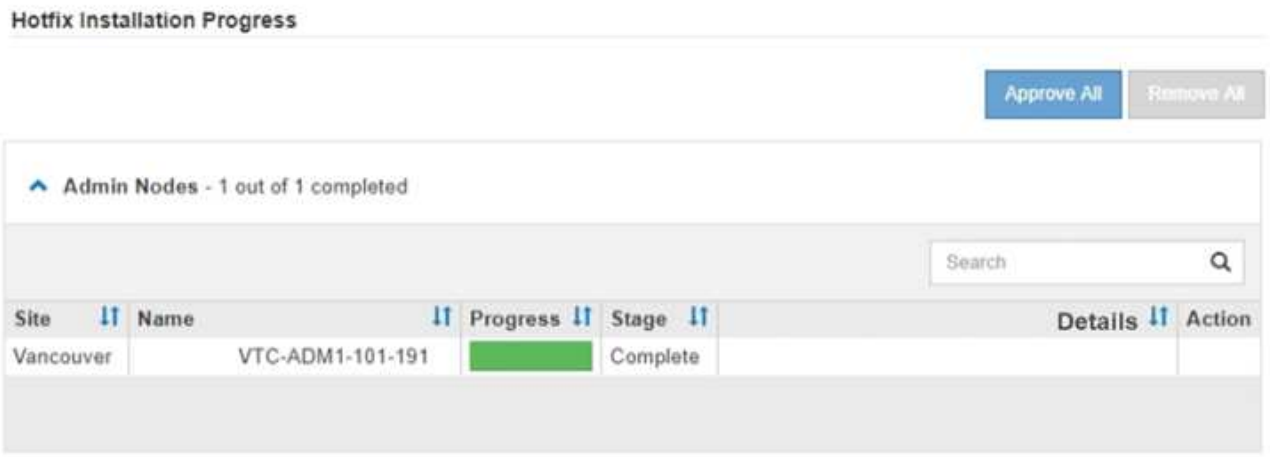
   a. コード署名の検証を含む、修正プログラムの検証が実行されます。

      エラーが報告された場合は解決し、ホットフィックスファイルを再アップロードして、 * Start * を再度選択します。

b. ホットフィックスのインストールの進行状況の表が表示されます。

この表には、グリッド内のすべてのノードと、ホットフィックスのインストールの現在のステージがノードごとに表示されます。テーブル内のノードは、タイプ（管理ノード、ゲートウェイノード、ストレージノード）別にグループ化されています。

c. 進行状況バーが完了すると、プライマリ管理ノードが「Complete」と表示されます。



8. 必要に応じて、各グループ内のノードのリストを * Site * 、 * Name * 、 * Progress * 、 * Stage * 、または * Details * で昇順または降順にソートします。または、 * 検索 * ボックスに用語を入力して特定のノードを検索します。
9. 更新する準備ができたグリッドノードを承認します。同じタイプの承認済みノードが一度に 1 つずつアップグレードされます。

> ノードを更新する準備ができていることを確認するまでは、ノードのホットフィックスを承認しないでください。グリッドノードにホットフィックスを適用すると、そのノード上の一部のサービスが再開されることがあります。このような処理を実行すると、ノードと通信しているクライアントで原因 サービスが中断する可能性があります。

- 1 つまたは複数の * 承認 * ボタンを選択して、 1 つまたは複数のノードをホットフィックスキューに追加します。
- 各グループ内の * すべて承認 * ボタンを選択して、同じタイプのすべてのノードをホットフィックスキューに追加します。[* 検索 * （ * Search * ）] ボックスに検索条件を入力した場合は、 [すべて承認（ Approve All * ）] ボタンをクリックすると、検索条件で選択したすべてのノードが環境 されます。

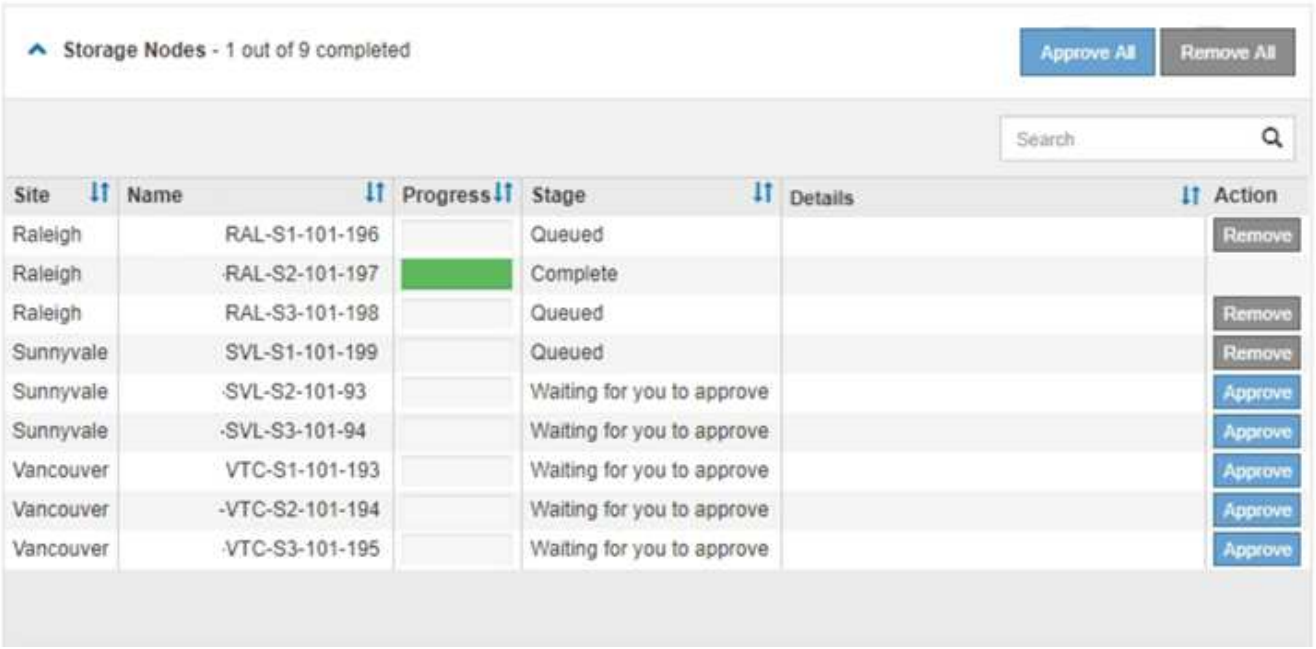
> ページ上部の * すべて承認 * ボタンをクリックすると、ページにリストされているすべてのノードが承認されます。一方、テーブルグループの上部にある * すべて承認 * ボタンをクリックすると、そのグループ内のすべてのノードのみが承認されます。ノードのアップグレード順序が重要な場合は、ノードまたはノードグループを 1 つずつ承認し、各ノードでアップグレードが完了するまで待ってから、次のノードを承認します。

- ページ上部の最上位レベルの * すべて承認 * ボタンを選択して、グリッド内のすべてのノードをホットフィックスキューに追加します。

別のソフトウェア更新を開始する前に、 StorageGRID ホットフィックスを完了する必要があります。ホットフィックスを完了できない場合は、テクニカルサポートにお問い合わせください。

- ノードまたはすべてのノードをホットフィックスキューから削除するには、「 * Remove * 」または「 * Remove All * 」を選択します。

  [Stage]が[Queued]を超えると、*[Remove]*ボタンが非表示になり、ホットフィックスプロセスからノードを削除できなくなります。



10. 承認された各グリッドノードにホットフィックスが適用されるまで待ちます。

    ホットフィックスがすべてのノードに正常にインストールされると、ホットフィックスのインストールの進捗状況の表が閉じます。緑のバナーは、ホットフィックスが完了した日時を示します。

11. ホットフィックスをどのノードにも適用できなかった場合は、各ノードのエラーを確認し、問題 を解決してから、上記の手順を繰り返します。

    手順 は、ホットフィックスがすべてのノードに正常に適用されるまで完了しません。必要に応じて、完了するまでホットフィックスの適用を何度でも安全に再試行できます。

StorageGRIDシステムの設定と管理

StorageGRID の管理

StorageGRID 管理のクイックスタート

以下の手順に従って、 StorageGRID システムを設定および管理します。

StorageGRID システムの概要を理解し、Linux コマンドシェル、ネットワーク、サーバーハードウェアのセットアップと構成について十分な知識を持っていることを確認してください。

1. **Grid Manager** の使用を開始する
   - "グリッドマネージャーのユーザーインターフェースを使用するための基本的な手順を学びましょう"
   - "ライセンス情報について"
   - "グリッド管理APIの使用方法について"
2. **StorageGRID** へのアクセスを制御する
   - "パスフレーズ、パスワード、および権限について"
   - "IDフェデレーションの設定"
   - "管理者グループを管理する"
   - "ユーザの管理"
   - "シングル サインオン（SSO）を設定する"
3. グリッドフェデレーションを使用する
   - "グリッドフェデレーション接続の設定"
   - "アカウント同期について"
   - "クロスグリッドレプリケーションの詳細"
   - "グローバル名前空間を設定する"
4. セキュリティを管理する
   - "StorageGRID の暗号化方式を確認します"
   - "証明書の管理"
   - "セキュリティを設定します"
   - "キー管理サーバを設定"
   - "プロキシ設定を管理します"

- "ファイアウォールを制御します"

5 テナントの管理

- "テナントアカウントの概要と管理"
- "テナントのプラットフォームサービスを管理する"
- "テナントアカウント用の S3 Select を管理します"

6 クライアント接続を構成する

- "S3クライアントのセキュリティについて"
- "S3セットアップウィザードを使用します"
- "ハイアベイラビリティグループを管理します"
- "S3エンドポイントのドメイン名を設定"

7 ネットワークと接続を管理する

- "ネットワークの設定"
- "VLAN インターフェイスを設定します"
- "トラフィック分類ポリシーを管理します"
- "リンクコストを管理します"

8 ノードを管理する

- "ストレージノードを管理します"
- "管理ノードを管理する"

Grid Managerの使用を開始する

StorageGRIDのWebブラウザ要件

サポートされている Web ブラウザを使用する必要があります。

Webブラウザ	サポートされる最小バージョン
Google Chrome	138
Microsoft Edge	138
Mozilla Firefox	140

ブラウザウィンドウを推奨幅に設定します。

ブラウザの幅	ピクセル
最小	一、〇 二四
最適	1280

StorageGRID Grid Manager に Sign in します

Grid Manager のサインインページにアクセスするには、サポートされている Web ブラウザのアドレスバーに管理ノードの完全修飾ドメイン名（ FQDN ）または IP アドレスを入力します。

各 StorageGRID システムには、 1 つのプライマリ管理ノードと、任意の数のプライマリ以外の管理ノードが含まれています。任意の管理ノードでグリッドマネージャにサインインして、 StorageGRID システムを管理できます。ただし、一部のメンテナンス手順はプライマリ管理ノードからしか実行できません。

HAグループに接続します

管理ノードがハイアベイラビリティ（ HA ）グループに含まれている場合は、 HA グループの仮想 IP アドレスまたは仮想 IP アドレスにマッピングされる完全修飾ドメイン名を使用して接続します。プライマリ管理ノードが使用できない場合を除いてプライマリ管理ノード上のグリッド Manager にアクセスするよう、プライマリ管理ノードをグループのプライマリインターフェイスとして選択する必要があります。を参照して "ハイアベイラビリティグループを管理します"

SSOを使用します

サインインの手順は、以下の場合、若干異なります。"シングルサインオン（SSO）が設定されている" 。

最初の管理ノードでGrid Managerにサインインします

開始する前に

- ログインクレデンシャルが必要です。
- を使用している"サポートされている Web ブラウザ"。
- Web ブラウザでクッキーが有効になっている必要があります。
- 少なくとも1つの権限が割り当てられたユーザグループに属している必要があります。
- Grid ManagerのURLが必要です。

  `https://FQDN_or_Admin_Node_IP/`

  完全修飾ドメイン名、管理ノードのIPアドレス、または管理ノードのHAグループの仮想IPアドレスを使用できます。

  HTTPSのデフォルトのポート（443）以外のポートでGrid Managerにアクセスするには、URLにポート番号を追加します。

  `https://FQDN_or_Admin_Node_IP:port/`

手順

1. サポートされている Web ブラウザを起動します。
2. ブラウザのアドレスバーに、Grid ManagerのURLを入力します。
3. セキュリティアラートが表示された場合は、ブラウザのインストールウィザードを使用して証明書をインストールします。を参照して "セキュリティ証明書を管理する"
4. Grid Manager にサインインします。

   表示されるサインイン画面は、StorageGRID 用にシングルサインオン（SSO）が設定されているかどうかによって異なります。

   SSOを使用しない

   a. Grid Manager のユーザ名とパスワードを入力します。
   b. 「サインイン」を選択します。

   SSOを使用する

   - StorageGRID がSSOを使用しており、このブラウザで初めてURLにアクセスした場合は、次の手順を実行します。
     i. 「サインイン」を選択します。[Account]フィールドに0を入力したままにしておくことができます。
     ii. 組織の SSO サインイン ページで標準の SSO 資格情報を入力します。

     たとえば、 StorageGRIDが SSO を使用しており、以前に Grid Manager またはテナント アカウントにアクセスしたことがある場合は、次のようになります。

     A. 0 （**Grid Manager**のアカウント**ID**）を入力するか、最近のアカウントのリストに表示されている場合は Grid Manager *を選択します。
     B. 「サインイン」を選択します。
     C. 組織の SSO サインインページで通常使用している SSO クレデンシャルを使用してサインインします。

サインインすると、ダッシュボードを含むGrid Managerのホームページが表示されます。提供される情報については、を参照してください"ダッシュボードを表示および管理します"。

別の管理ノードにサインインします

次の手順に従って、別の管理ノードにサインインします。

SSOを使用しない

手順

1. ブラウザのアドレスバーに、他の管理ノードの完全修飾ドメイン名または IP アドレスを入力します。必要に応じてポート番号を追加します。
2. Grid Manager のユーザ名とパスワードを入力します。
3. 「サインイン」を選択します。

SSOを使用する

SSOを使用しているStorageGRID で1つの管理ノードにサインインしている場合は、再度サインインしなくても他の管理ノードにアクセスできます。

手順

1. ブラウザのアドレスバーに、もう一方の管理ノードの完全修飾ドメイン名またはIPアドレスを入力します。
2. SSOセッションの有効期限が切れている場合は、クレデンシャルを再度入力します。

StorageGRID Grid Manager からログアウトします

グリッドマネージャの操作が完了したら、サインアウトして、権限のないユーザがStorageGRID システムにアクセスできないようにする必要があります。ブラウザのクッキーの設定によっては、ブラウザを閉じてもシステムからサインアウトされない場合があります。

手順

1. 右上のユーザ名を選択します。
2. [サインアウト]*を選択します。

オプション	製品説明
SSO は使用されていません	管理ノードからサインアウトされます。 Grid Manager のサインインページが表示されます。 • 注： * 複数の管理ノードにサインインした場合、各ノードからサインアウトする必要があります。
SSOが有効	アクセスしていたすべての管理ノードからサインアウトされます。StorageGRID のサインインページが表示されます。**Grid Manager** は、 [Recent Accounts] * ドロップダウンにデフォルトとして表示され、 [**Account ID**] フィールドには 0 と表示されます。 注意: SSOが有効になっていて、テナントマネージャにもサインインしている場合は、"テナントアカウントからサインアウトします" に"SSOからサインアウトします"。

StorageGRID Grid Managerのパスワードを変更する

Grid Manager のローカルユーザは自分のパスワードを変更できます。

開始する前に

Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。

タスクの内容

フェデレーテッドユーザとしてStorageGRID にサインインする場合やシングルサインオン（SSO）が有効になっている場合は、Grid Managerでパスワードを変更することはできません。代わりに、 Active Directory や OpenLDAP などの外部 ID ソースでパスワードを変更する必要があります。

手順

1. Grid Manager のヘッダーで、 * _ your name_* > * Change password * を選択します。
2. 現在のパスワードを入力します。
3. 新しいパスワードを入力します。

   パスワードは 8 文字以上 32 文字以下にする必要があります。パスワードでは大文字と小文字が区別されます。

4. 新しいパスワードをもう一度入力します。
5. [保存（ Save ）] を選択します。

StorageGRID ライセンス情報を表示します

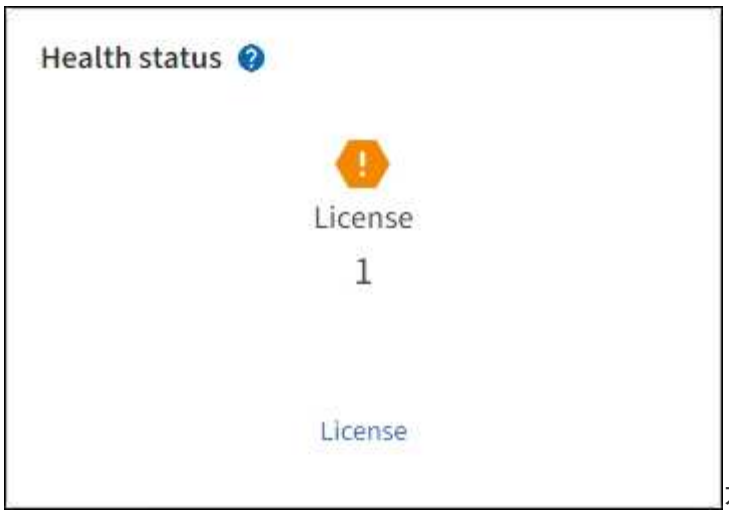
グリッドの最大ストレージ容量など、 StorageGRID システムのライセンス情報を必要に応じていつでも表示できます。

開始する前に

Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。

タスクの内容

このStorageGRID システムのソフトウェアライセンスを持つ問題 がある場合は、ダッシュボードの[Health]ステータスカードにライセンスステータスアイコンと*[License]リンクが表示されます。番号は、ライセンス関連の問題の数を示します。



カードのライセンスステータス"]

手順

1. 次のいずれかを実行して[License]ページにアクセスします。
   - メンテナンス > システム > *ライセンス*を選択します。
   - ダッシュボードの[Health]ステータスカードで、ライセンスステータスアイコンまたは*[License]*リンクを選択します。

     このリンクは、ライセンスを持つ問題 が存在する場合にのみ表示されます。
2. 現在のライセンスの読み取り専用の詳細を表示します。
   - StorageGRID システム ID 。この StorageGRID インストールの一意の ID 番号です
   - ライセンスのシリアル番号
   - ライセンスタイプ（* Perpetual または Subscription *）
   - グリッドのライセンスが付与されているストレージ容量
   - サポートされるストレージ容量
   - ライセンスの終了日。永久ライセンスの場合は「N/A *」と表示されます。
   - サポート終了日

     この日付は現在のライセンスファイルから読み取られたもので、ライセンスファイルを取得後にサポート サービス契約を延長または更新した場合は、古くなっている可能性があります。この値を更新するには、"StorageGRID ライセンス情報を更新します"を参照してください。また、Digital Advisor を使用して実際の契約終了日を確認することもできます。
   - ライセンステキストファイルの内容

StorageGRID ライセンス情報を更新します

ライセンス内容に変更があった場合は、 StorageGRID システムのライセンス情報を更新する必要があります。たとえば、グリッド用のストレージ容量を追加で購入した場合は、ライセンス情報を更新する必要があります。

開始する前に

- StorageGRID システムに適用する新しいライセンスファイルを用意しておきます。
- そうだな "特定のアクセス権限"
- プロビジョニングパスフレーズを用意します。

手順

1. メンテナンス > システム > *ライセンス*を選択します。
2. [ライセンスの更新]セクションで、*[参照]*を選択します。
3. 新しいライセンスファイルを探して選択し(`.txt`ます）。

   新しいライセンスファイルが検証され、表示されます。

4. プロビジョニングパスフレーズを入力します。
5. [保存（ Save ）] を選択します。

API を使用します

StorageGRID Grid Management APIを使用する

Grid Manager のユーザインターフェイスの代わりにグリッド管理 REST API を使用して、システム管理タスクを実行できます。たとえば、 API を使用して処理を自動化したり、ユーザなどの複数のエンティティを迅速に作成したりできます。

トップレベルのリソース

グリッド管理 API で使用可能な最上位のリソースは次のとおりです。

- `/grid`：Grid Managerユーザのみがアクセスでき、設定されているグループ権限に基づいてアクセスできます。
- `/org`：テナントアカウントのローカルまたはフェデレーテッドLDAPグループに属するユーザのみがアクセスできます。詳細については、を参照してください "テナントアカウントを使用する"。
- `/private`：Grid Managerユーザのみがアクセスでき、設定されているグループ権限に基づいてアクセスできます。プライベート API は予告なく変更される場合があります。StorageGRID プライベートエンドポイントは、要求の API バージョンも無視します。

問題 **API** 要求

グリッド管理 API では、 Swagger オープンソース API プラットフォームを使用します。Swagger のわかりやすいユーザインターフェイスを使用して、開発者および一般のユーザは StorageGRID で API を使用してリアルタイムの処理を実行できます。

Swagger のユーザインターフェイスでは、各 API 処理に関する詳細情報とドキュメントを参照できます。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- そうだな "特定のアクセス権限"

APIドキュメントWebページで実行するAPI処理はすべてライブ処理です。設定データやその他のデータを誤って作成、更新、または削除しないように注意してください。

手順

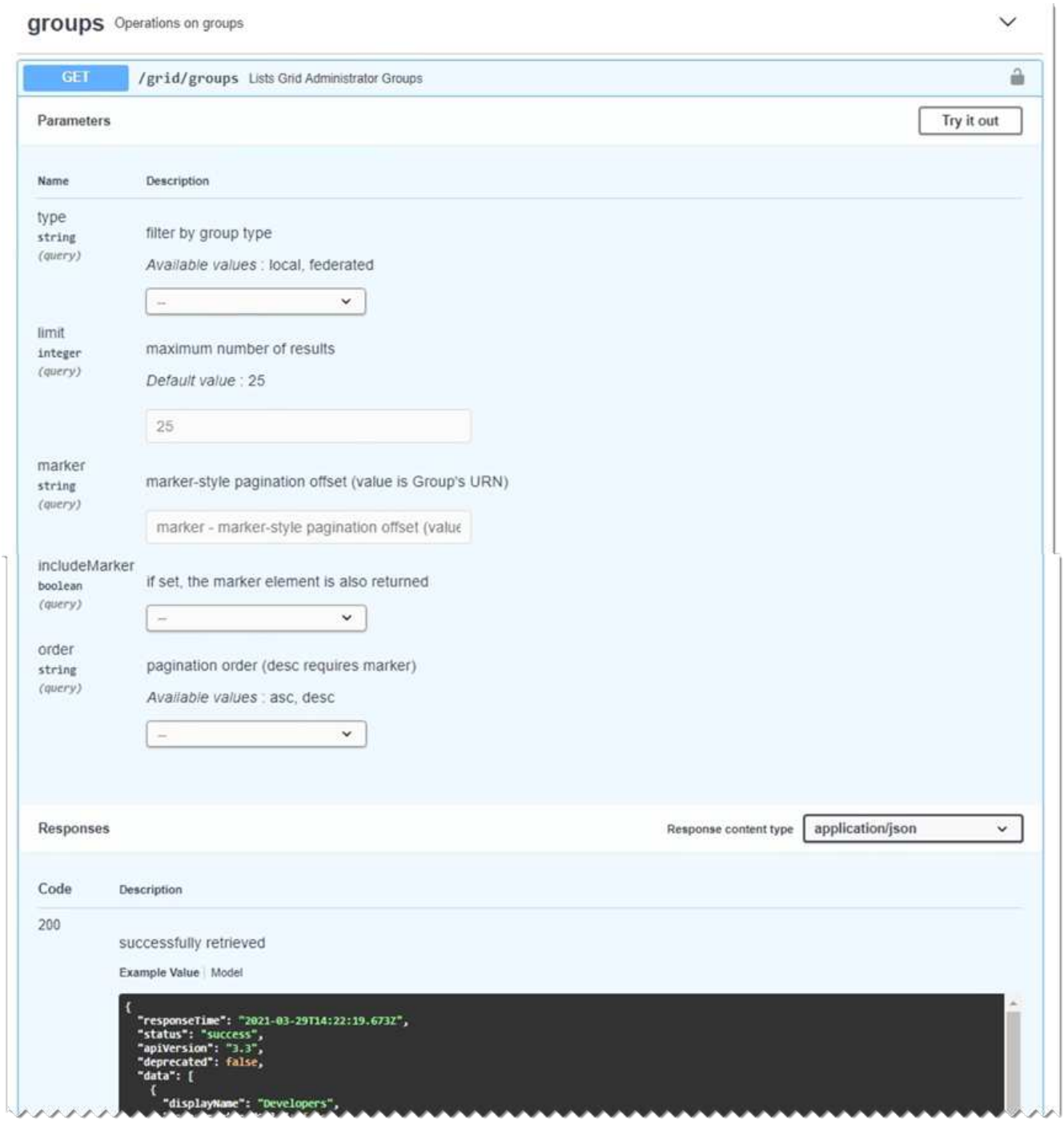
1. グリッドマネージャーのヘッダーからヘルプアイコン を選択し、「API documentation」を選択します。
2. プライベート API を使用して操作を実行するには、 StorageGRID 管理 API ページで * プライベート API ドキュメントへ移動 * を選択します。

   プライベート API は予告なく変更される場合があります。StorageGRID プライベートエンドポイントは、要求の API バージョンも無視します。

3. 目的の処理を選択します。

   API 処理を拡張すると、 GET 、 PUT 、 UPDATE 、 DELETE など、使用可能な HTTP アクションを確認できます。

4. HTTP アクションを選択して、要求の詳細を確認します。これには、エンドポイント URL 、必須またはオプションのパラメータのリスト、要求の本文の例（必要な場合）、想定される応答が含まれます。



5. グループやユーザの ID など、要求で追加のパラメータが必要かどうかを確認します。次に、これらの値を取得します。必要な情報を取得するために、先に別の API 要求の問題 が必要になることがあります。
6. 要求の本文の例を変更する必要があるかどうかを判断します。その場合は、 * Model * を選択して各フィールドの要件を確認できます。
7. [* 試してみてください *] を選択します。
8. 必要なパラメータを指定するか、必要に応じて要求の本文を変更します。
9. [* Execute] を選択します。
10. 応答コードを確認し、要求が成功したかどうかを判断します。

グリッド管理 API では、使用可能な処理が次のセクションに分類されます。

このリストには、パブリック API で使用可能な処理のみが含まれます。

- * accounts *：新しいアカウントの作成や特定のアカウントのストレージ使用状況の取得など、ストレージテナントアカウントを管理する処理。
- * alert-history *：解決済みのアラートに対する処理。
- * alert-receivers *：アラート通知受信者（Eメール）に対する処理。
- * alert-rules *：アラートルールに対する処理。
- * alert-silences *：アラートサイレンスに対する処理。
- * alerts *：アラートに対する処理。
- **audit**:監査構成を一覧表示および更新する操作。
- **auth**：ユーザセッション認証を実行する処理。

  グリッド管理 API は、ベアラートークン認証方式をサポートしています。サインインするには、認証要求のJSON本文（つまり）でユーザ名とパスワードを指定します `POST /api/v3/authorize`。ユーザが認証されると、セキュリティトークンが返されます。このトークンは、後続の API 要求（「 Authorization ： Bearer_token_ 」）のヘッダーで指定する必要があります。トークンは16時間後に期限切れになります。

  StorageGRID システムでシングルサインオンが有効になっている場合は、別の手順による認証が必要です。「シングルサインオンが有効な場合のAPIへのログイン」を参照してください。

  認証セキュリティの向上については、「クロスサイトリクエストフォージェリからの保護」を参照してください。

- * client-certificates *：外部の監視ツールを使用してStorageGRID に安全にアクセスできるように、クライアント証明書を設定する処理。
- * config *：製品リリースおよびGrid管理APIのバージョンに関連する処理。製品のリリースバージョンおよびそのリリースでサポートされているグリッド管理 API のメジャーバージョンをリストし、廃止されたバージョンの API を無効にすることができます。
- * deactivated-features *：非アクティブ化された可能性がある機能を表示する操作。
- * dns-servers *：設定されている外部DNSサーバをリストおよび変更する処理。
- * drive-details *：特定のストレージアプライアンスモデルのドライブに対する処理。
- * endpoint-domain-names *：S3エンドポイントのドメイン名をリストおよび変更する処理。
- イレイジャーコーディング：イレイジャーコーディングプロファイルに対する処理。
- **expansion**:拡張の操作(プロシージャレベル)。
- * expansion-nodes *：拡張の処理（ノードレベル）。
- * expansion-sites *：拡張の処理（サイトレベル）。
- * grid-networks *：グリッドネットワークリストをリストおよび変更する処理。

- * grid-passwords *：Gridパスワード管理の処理。
- * groups *：ローカルのグリッド管理者グループを管理する処理、およびフェデレーテッドグリッド管理者グループを外部のLDAPサーバから取得する処理。
- *identity-source *：外部のアイデンティティソースを設定する処理、およびフェデレーテッドグループとユーザ情報を手動で同期する処理。
- * ILM *：情報ライフサイクル管理（ILM）の処理。
- * in-progress-procedures *：現在進行中のメンテナンス手順を取得します。
- * license *：StorageGRID ライセンスを取得および更新する処理。
- * logs *：ログファイルを収集およびダウンロードする処理。v
- * metrics *：StorageGRID メトリックに対する処理。特定の時点におけるインスタントメトリッククエリ、および一定期間にわたるメトリッククエリを含みます。グリッド管理 API は、バックエンドのデータソースとして Prometheus システム監視ツールを使用します。Prometheus クエリの構築については、Prometheus の Web サイトを参照してください。

  名前にが含まれる指標は*`private`*内部使用のみを目的としています。これらの指標は、StorageGRID のリリース間で予告なく変更される可能性があります。

- * node-details *：ノードの詳細に対する処理。
- * node-health *：ノードの健常性ステータスに対する処理。
- * node-storage-state *：ノードのストレージステータスに対する処理。
- *ntp-servers *：外部のネットワークタイムプロトコル（NTP）サーバをリストまたは更新する処理。
- * objects *：オブジェクトおよびオブジェクトメタデータに対する処理。
- * recovery*：リカバリ手順 の処理。
- **recovery-package**: リカバリ パッケージをダウンロードする操作。
- **regions**:リージョンを表示および作成する操作。
- * s3-object-lock *：グローバルS3オブジェクトロック設定に対する処理。
- * server-certificate *：Grid Managerサーバ証明書を表示および更新する処理。
- **snmp**:現在のSNMP設定に対する操作。
- * storage-watermarks *：ストレージノードのウォーターマーク。
- * traffic-classes *：トラフィック分類ポリシーの処理。
- * untrusted-client-network *：信頼されていないクライアントネットワーク構成に対する処理。
- * users *：Grid Managerユーザを表示および管理する処理。

StorageGRID におけるグリッド管理 **API** のバージョン管理

グリッド管理 API では、バージョン管理を使用して無停止アップグレードがサポートされます。

たとえば、このリクエストURLはAPIのバージョン4を指定します。

`https://hostname_or_ip_address/api/v4/authorize`

APIのメジャーバージョンは、古いバージョンと互換性がない_変更を行うと更新されます。APIのマイナーバージョンは、_が古いバージョンと互換性がある_に変更されると更新されます。互換性のある変更には、新しいエンドポイントやプロパティの追加などがあります。

次の例は、変更のタイプに基づいて API バージョンがどのように更新されるかを示しています。

API に対する変更のタイプ	古いバージョン	新しいバージョン
旧バージョンと互換性があります	2.1	2.2
旧バージョンとの互換性がありません	2.1	3.0

StorageGRIDソフトウェアを初めてインストールすると、最新バージョンのAPIのみが有効になります。ただし、 StorageGRID の新機能リリースにアップグレードした場合、少なくとも StorageGRID の機能リリース 1 つ分の間は、古い API バージョンにも引き続きアクセスできます。

> サポートされるバージョンを設定できます。詳細については、Swagger APIドキュメントの* config *セクションを参照してください"Grid 管理 API"。すべてのAPIクライアントを新しいバージョンを使用するように更新したら、古いバージョンのサポートを無効にする必要があります。

古い要求は、次の方法で廃止とマークされます。

- 応答ヘッダーが「 Deprecated ： true 」となる。
- JSON 応答の本文に「 deprecated ： true 」が追加される
- 廃止の警告が nms.log に追加される。例：

```
Received call to deprecated v2 API at POST "/api/v2/authorize"
```

現在のリリースでサポートされている **API** のバージョンを確認します

API要求を使用して `GET /versions`、サポートされているAPIのメジャーバージョンのリストを返します。この要求は、Swagger APIドキュメントの* config *セクションにあります。

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2023-06-27T22:13:50.750Z",
  "status": "success",
  "apiVersion": "4.0",
  "data": [
    2,
    3,
    4
  ]
}
```

要求の **API** バージョンを指定します

APIのバージョンは(`/api/v4`、パスパラメータを使用して指定できます）またはヘッダー(`Api-Version: 4`を指定できます。両方の値を指定した場合は、ヘッダー値がパス値よりも優先されます。

```
curl https://[IP-Address]/api/v4/grid/accounts

curl -H "Api-Version: 4" https://[IP-Address]/api/grid/accounts
```

StorageGRID でクロスサイトリクエストフォージェリ（**CSRF**）から保護する

CSRF トークンを使用してクッキーによる認証を強化すると、 StorageGRID に対するクロスサイトリクエストフォージェリ（ CSRF ）攻撃を防ぐことができます。Grid Manager と Tenant Manager はこのセキュリティ機能を自動的に有効にします。他の API クライアントは、サインイン時にこの機能を有効にするかどうかを選択できます。

攻撃者が別のサイト（たとえば、 HTTP フォーム POST を使用して）への要求をトリガーできる場合、サインインしているユーザのクッキーを使用して特定の要求を原因 が送信できます。

StorageGRID では、 CSRF トークンを使用して CSRF 攻撃を防ぐことができます。有効にした場合、特定のクッキーの内容が特定のヘッダーまたは特定の POST パラメータの内容と一致する必要があります。

この機能をイネーブルにするには、認証時にパラメータをに `true`設定し `csrfToken`ます。デフォルトはです `false`。

```
curl -X POST --header "Content-Type: application/json" --header "Accept:
application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

trueの場合、 `GridCsrfToken`Grid Managerへのサインインにはランダムな値でクッキーが設定され、Tenant Managerへのサインインにはランダムな値でクッキーが設定さ `AccountCsrfToken`れます。

クッキーが存在する場合は、システムの状態を変更できるすべての要求（ POST 、 PUT 、 PATCH 、 DELETE ）には次のいずれかが含まれている必要があります。

- `X-Csrf-Token`ヘッダーの値がCSRFトークンクッキーの値に設定されたヘッダー。
- エンドポイントがフォームエンコードされた本文を受け入れる場合： `csrfToken`フォームエンコードされた要求本文パラメータ。

その他の例および詳細については、オンラインの API ドキュメントを参照してください。

CSRFトークンクッキーが設定されている要求では、CSRF攻撃に対する追加の保護としてJSON要求本文が必要な要求に対して「Content-Type:application/json」ヘッダーも適用されます。

シングルサインオンが有効な場合は、 **API** を使用します

StorageGRID API を使用する場合、 **Single Sign-On** が有効になっている（**Active Directory**）

もしあなたが"シングルサインオン（ SSO ）の設定と有効化"Active Directory を SSO プロバイダーとして使用する場合は、一連の API 要求を発行して、グリッド管理 API またはテナント管理 API に有効な認証トークンを取得する必要があります。

シングルサインオンが有効な場合は、 **API** にサインインします

ここで説明する手順は、 Active Directory を SSO アイデンティティプロバイダとして使用する場合に該当します。

開始する前に

- StorageGRID ユーザグループに属するフェデレーテッドユーザの SSO ユーザ名とパスワードが必要です。
- テナント管理 API にアクセスする場合は、テナントアカウント ID を確認しておきます。

タスクの内容

認証トークンを取得するには、次のいずれかの例を使用します。

- その `storagegrid-ssoauth.py`StorageGRIDインストール ファイル ディレクトリにある Python スクリプト (./rpms`RHELの場合、 `./debs` UbuntuまたはDebianの場合、 `./vsphere` VMware の場合)。
- cURL 要求のワークフローの例。

  cURL ワークフローは、実行に時間がかかりすぎるとタイムアウトする場合があります。「」というエラーが表示される場合があり `A valid SubjectConfirmation was not found on this Response`ます。

  cURL ワークフローの例では、パスワードが他のユーザに表示されないように保護されていません。

URLエンコードに問題がある場合は、次のエラーが表示されることがあります。 `Unsupported SAML`

`version`

手順

1. 認証トークンを取得するには、次のいずれかの方法を選択します。
   - Pythonスクリプトを使用し `storagegrid-ssoauth.py`ます。手順2に進みます。
   - curl 要求を使用します。手順3に進みます。
2. スクリプトを使用する `storagegrid-ssoauth.py`場合は、スクリプトをPythonインタープリタに渡してスクリプトを実行します。

   プロンプトが表示されたら、次の引数の値を入力します。

   - SSO 方式。ADFS または ADFS と入力します。
   - SSOユーザ名
   - StorageGRID がインストールされているドメイン
   - StorageGRID のアドレス
   - テナント管理 API にアクセスする場合は、テナントアカウント ID 。

   ```
   python3 storagegrid-ssoauth.py
   sso_method: adfs
   saml_user: my-sso-username
   saml_domain: my-domain
   sg_address: storagegrid.example.com
   tenant_account_id: 12345
   Enter the user's SAML password:
   ********************************************************************************

   ********************************************************************************
   StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
   ```

   StorageGRID 認証トークンが出力に表示されます。SSO を使用していない場合の API の使用方法と同様に、トークンを他の要求に使用できるようになりました。

3. cURL 要求を使用する場合は、次の手順 を使用します。
   a. サインインに必要な変数を宣言します。

   ```
   export SAMLUSER='my-sso-username'
   export SAMLPASSWORD='my-password'
   export SAMLDOMAIN='my-domain'
   export TENANTACCOUNTID='12345'
   export STORAGEGRID_ADDRESS='storagegrid.example.com'
   export AD_FS_ADDRESS='adfs.example.com'
   ```

   > グリッド管理APIにアクセスするには、として0を使用し `TENANTACCOUNTID`ます。

b. 署名済みの認証URLを受信するには、にPOST要求を実行し `/api/v3/authorize-saml`、応答からJSONエンコードを削除します。

次の例は、の署名付き認証URLに対するPOST要求を示してい `TENANTACCOUNTID`ます。結果はに渡され `python -m json.tool`、JSONエンコードが削除されます。

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
  -H "accept: application/json" -H  "Content-Type: application/json"
\
  --data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

この例の応答には、 URL エンコードされた署名済み URL が含まれていますが、 JSON エンコードされたレイヤは含まれていません。

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZHLbsIwEEV%2FJTuv7...
sSl%2BfQ33cvfwA%3D&RelayState=12345",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

c. 後続のコマンドで使用できるように、応答からを保存し `SAMLRequest`ます。

```
export SAMLREQUEST='fZHLbsIwEEV%2FJTuv7...sSl%2BfQ33cvfwA%3D'
```

d. AD FS からクライアント要求 ID を含む完全な URL を取得します。

1 つは、前の応答の URL を使用してログインフォームを要求する方法です。

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=
$SAMLREQUEST&RelayState=$TENANTACCOUNTID" | grep 'form method="post"
id="loginForm"'
```

応答にはクライアント要求 ID が含まれています。

```
<form method="post" id="loginForm" autocomplete="off"
novalidate="novalidate" onKeyPress="if (event && event.keyCode == 13)
Login.submitLoginRequest();" action="/adfs/ls/?
SAMLRequest=fZHRToMwFIZfhb...UJikvo77sXPw%3D%3D&RelayState=12345&clie
nt-request-id=00000000-0000-0000-ee02-0080000000de" >
```

e. 応答からクライアント要求 ID を保存します。

```
export SAMLREQUESTID='00000000-0000-0000-ee02-0080000000de'
```

f. 前の応答のフォームアクションにクレデンシャルを送信します。

```
curl -X POST "https://$AD_FS_ADDRESS
/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client
-request-id=$SAMLREQUESTID" \
--data "UserName=$SAMLUSER@$SAMLDOMAIN&Password=
$SAMLPASSWORD&AuthMethod=FormsAuthentication" --include
```

AD FS からヘッダーに追加情報 が含まれた 302 リダイレクトが返されます。

> SSO システムで多要素認証（ MFA ）が有効になっている場合、フォームポストには 2 つ目のパスワードまたはその他のクレデンシャルも含まれます。

```
HTTP/1.1 302 Found
Content-Length: 0
Content-Type: text/html; charset=utf-8
Location:
https://adfs.example.com/adfs/ls/?SAMLRequest=fZHRToMwFIZfhb...UJikvo
77sXPw%3D%3D&RelayState=12345&client-request-id=00000000-0000-0000-
ee02-0080000000de
Set-Cookie: MSISAuth=AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY=; path=/adfs;
HttpOnly; Secure
Date: Tue, 06 Nov 2018 16:55:05 GMT
```

g. 応答からクッキーを保存し `MSISAuth`ます。

```
export MSISAuth='AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY='
```

h. 認証 POST からクッキーを使用して、指定した場所に GET 要求を送信します。

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=
$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client-request-
id=$SAMLREQUESTID" \
--cookie "MSISAuth=$MSISAuth" --include
```

応答ヘッダーには、あとでログアウトに使用する AD FS セッション情報が含まれます。応答の本文には、非表示のフォームフィールドに SAMLResponse が含まれています。

```
HTTP/1.1 200 OK
Cache-Control: no-cache,no-store
Pragma: no-cache
Content-Length: 5665
Content-Type: text/html; charset=utf-8
Expires: -1
Server: Microsoft-HTTPAPI/2.0
P3P: ADFS doesn't have P3P policy, please contact your site's admin
for more details
Set-Cookie:
SamlSession=a3dpbnRlcnMtUHJpbWFyeS1BZG1pbi0xNzgmRmFsc2Umcng4NnJDZmFKV
XFxVWx3bkl1MnFuUSUzZCUzZCYmJiYmXzE3MjAyZTA5LThmMDgtNDRkZC04Yzg5LTQ3ND
UxYzA3ZjkzYw==; path=/adfs; HttpOnly; Secure
Set-Cookie: MSISAuthenticated=MTEvNy8yMDE4IDQ6MzI6NTkgUE0=;
path=/adfs; HttpOnly; Secure
Set-Cookie: MSISLoopDetectionCookie=MjAxOC0xMS0wNzoxNjozMjo1OVpcMQ==;
path=/adfs; HttpOnly; Secure
Date: Wed, 07 Nov 2018 16:32:59 GMT

<form method="POST" name="hiddenform"
action="https://storagegrid.example.com:443/api/saml-response">
  <input type="hidden" name="SAMLResponse"
value="PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4=" /><input
type="hidden" name="RelayState" value="12345" />
```

i. 非表示フィールドからを保存し `SAMLResponse`ます。

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. 保存したを使用して `SAMLResponse`、StorageGRID認証トークンを生成するStorageGRID要求を行い`/api/saml-response`ます。

で `RelayState`、テナントアカウントIDを使用するか、グリッド管理APIにサインインする場合は0を使用します。

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
  -H "accept: application/json" \
  --data-urlencode "SAMLResponse=$SAMLResponse" \
  --data-urlencode "RelayState=$TENANTACCOUNTID" \
  | python -m json.tool
```

応答には認証トークンが含まれています。

```
{
    "apiVersion": "3.0",
    "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
    "responseTime": "2018-11-07T21:32:53.486Z",
    "status": "success"
}
```

a. 応答に認証トークンをとして保存し `MYTOKEN`ます。

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

SSOが使用されていない場合のAPIの使用方法と同様に、を他の要求に使用できるようになりまし `MYTOKEN`た。

シングルサインオンが有効な場合は、 **API** からサインアウトします

シングルサインオン（ SSO ）が有効になっている場合は、グリッド管理 API またはテナント管理 API からサインアウトするための一連の API 要求を問題 で処理する必要があります。ここで説明する手順は、 Active Directory を SSO アイデンティティプロバイダとして使用する場合に該当します

タスクの内容

必要に応じて、組織のシングルログアウトページからログアウトすることで、StorageGRID APIからサインアウトできます。または、 StorageGRID からシングルログアウト（ SLO ）を実行することもできます。この場合、有効な StorageGRID ベアラトークンが必要です。

手順

1. 署名されたログアウト要求を生成するには、「cookie "sso=true」をSLO APIに渡します。

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

ログアウト URL が返されます。

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3
D",
    "responseTime": "2018-11-20T22:20:30.839Z",
    "status": "success"
}
```

2. ログアウト URL を保存します。

```
export LOGOUT_REQUEST
='https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%
3D'
```

3. 要求をログアウト URL に送信し、 SLO を実行して StorageGRID にリダイレクトします。

```
curl --include "$LOGOUT_REQUEST"
```

302 応答が返されます。リダイレクト先は API のみのログアウトには適用されません。

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: MSISSignoutProtocol=U2FtbA==; expires=Tue, 20 Nov 2018
22:35:03 GMT; path=/adfs; HttpOnly; Secure
```

4. StorageGRID Bearer トークンを削除します。

StorageGRID Bearer トークンを削除すると、 SSO を使用しない場合と同じように動作します。「cookie "sso=true"」が指定されていない場合、ユーザはSSO状態に影響を与えずにStorageGRIDからログアウトされます。

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

ユーザがサインアウトされたことを示す応答が `204 No Content`返されます。

```
HTTP/1.1 204 No Content
```

シングル サインオン が有効になっている場合は **StorageGRID API** を使用します（**Entra ID**）

もしあなたが"シングルサインオン（ SSO ）の設定と有効化"Entra ID を SSO プロバイダーとして使用する場合、2 つのサンプル スクリプトを使用して、グリッド管理 API またはテナント管理 API に有効な認証トークンを取得できます。

Entra IDシングルサインオンが有効になっている場合は、**API**に**Sign in**。

これらの手順は、Entra IDをSSO IDプロバイダーとして使用している場合に適用されます。

開始する前に

- StorageGRID ユーザグループに属するフェデレーテッドユーザの SSO E メールアドレスとパスワードが必要です。
- テナント管理 API にアクセスする場合は、テナントアカウント ID を確認しておきます。

タスクの内容

認証トークンを取得するには、次のサンプルスクリプトを使用します。

- `storagegrid-ssoauth-azure.py`Pythonスクリプト
- `storagegrid-ssoauth-azure.js`Node.jsスクリプト

両方のスクリプトはStorageGRIDインストールファイルディレクトリにあります。(`./rpms` RHELの場合、`./debs` UbuntuまたはDebianの場合、 `./vsphere` VMware の場合)。

Entra IDとのAPI統合を独自に作成するには、 `storagegrid-ssoauth-azure.py`スクリプト。 Python スクリプトは、 StorageGRIDに 2 つのリクエストを直接送信します (最初に SAMLRequest を取得し、後で認証トークンを取得します)。また、Node.js スクリプトを呼び出して Entra ID と対話し、SSO 操作を実行します。

SSO 操作は一連の API リクエストを使用して実行できますが、実行するのは簡単ではありません。 Puppeteer Node.js モジュールは、Entra ID SSO インターフェースをスクレイピングするために使用されます。

URLエンコードに問題がある場合は、次のエラーが表示されることがあります。 `Unsupported SAML version`

手順

1. 必要な依存関係を次のようにインストールします。
   a. Node.jsをインストールします（を参照 "https://nodejs.org/en/download/"）。
   b. 必要な Node.js モジュール（ puppeteer および jsdom ）を取り付けます。

      ```
      npm install -g <module>
      ```

2. Python スクリプトを Python インタープリタに渡して、スクリプトを実行します。

   次に、Python スクリプトは対応する Node.js スクリプトを呼び出して、Entra ID SSO のやり取りを実行

します。

3. プロンプトが表示されたら、次の引数の値を入力します（または、パラメータを使用して渡します）。
   - Entra ID へのサインインに使用する SSO メールアドレス
   - StorageGRID のアドレス
   - テナント管理 API にアクセスする場合は、テナントアカウント ID
4. プロンプトが表示されたらパスワードを入力し、要求された場合は Entra ID に MFA 認証を提供できるように準備してください。

```
c:\Users\user\Documents\azure_sso>py storagegrid-azure-ssoauth.py --sso-email-address user@my-domain.com
--sg-address storagegrid.examp.e.com --tenant-account-id 0
Enter the user's SSO password:
********************************************************************************

Watch for and approve a 2FA authorization request
********************************************************************************
StorageGRID Auth Token: {'responseTime': '2021-10-04T21:30:48.807Z', 'status': 'success', 'apiVersion':
'3.4', 'data': '4807d93e-a3df-48f2-9680-906cd255979e'}
```

> このスクリプトでは、 MFA が Microsoft Authenticator を使用して実行されていることを前提として他の形式のMFAをサポートするようにスクリプトを変更する必要がある場合があります（テキストメッセージで受信したコードの入力など）。

StorageGRID 認証トークンが出力に表示されます。SSO を使用していない場合の API の使用方法と同様に、トークンを他の要求に使用できるようになりました。

シングル サインオンが有効になっている場合は **StorageGRID API** を使用します（**PingFederate**）

もしあなたが"シングルサインオン（ SSO ）の設定と有効化"PingFederate を SSO プロバイダーとして使用する場合は、一連の API 要求を発行して、Grid Management API または Tenant Management API に有効な認証トークンを取得する必要があります。

シングルサインオンが有効な場合は、 **API** にサインインします

これらの手順は、 SSO アイデンティティプロバイダとして PingFederate を使用している場合に適用されます

開始する前に

- StorageGRID ユーザグループに属するフェデレーテッドユーザの SSO ユーザ名とパスワードが必要です。
- テナント管理 API にアクセスする場合は、テナントアカウント ID を確認しておきます。

タスクの内容

認証トークンを取得するには、次のいずれかの例を使用します。

- その `storagegrid-ssoauth.py`StorageGRIDインストール ファイル ディレクトリにある `Python` スクリプト (./rpms`RHELの場合、 `./debs` UbuntuまたはDebianの場合、 `./vsphere` VMware の場合)。
- cURL 要求のワークフローの例。

  cURL ワークフローは、実行に時間がかかりすぎるとタイムアウトする場合があります。「」というエラ

ーが表示される場合があり `A valid SubjectConfirmation was not found on this Response`ます。

> cURL ワークフローの例では、パスワードが他のユーザに表示されないように保護されていません。

URLエンコードに問題がある場合は、次のエラーが表示されることがあります。 `Unsupported SAML version`

手順

1. 認証トークンを取得するには、次のいずれかの方法を選択します。
   - Pythonスクリプトを使用し `storagegrid-ssoauth.py`ます。手順2に進みます。
   - curl 要求を使用します。手順3に進みます。
2. スクリプトを使用する `storagegrid-ssoauth.py`場合は、スクリプトをPythonインタープリタに渡してスクリプトを実行します。

   プロンプトが表示されたら、次の引数の値を入力します。

   - SSO 方式。「PingFederate」の任意のバリエーション（PingFederate、PingFederateなど）を入力できます。
   - SSOユーザ名
   - StorageGRID がインストールされているドメイン。このフィールドは PingFederate には使用されません。空白のままにするか、任意の値を入力できます。
   - StorageGRID のアドレス
   - テナント管理 API にアクセスする場合は、テナントアカウント ID 。

   ```
   python3 storagegrid-ssoauth.py
   sso_method: pingfederate
   saml_user: my-sso-username
   saml_domain:
   sg_address: storagegrid.example.com
   tenant_account_id: 12345
   Enter the user's SAML password:
   ********************************************************************************

   ********************************************************************************
   StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
   ```

   StorageGRID 認証トークンが出力に表示されます。SSO を使用していない場合の API の使用方法と同様に、トークンを他の要求に使用できるようになりました。

3. cURL 要求を使用する場合は、次の手順 を使用します。
   a. サインインに必要な変数を宣言します。

```
export SAMLUSER='my-sso-username'
export SAMLPASSWORD='my-password'
export TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.example.com'
```

グリッド管理APIにアクセスするには、として0を使用し `TENANTACCOUNTID`ます。

b. 署名済みの認証URLを受信するには、にPOST要求を実行し `/api/v3/authorize-saml`、応答からJSONエンコードを削除します。

次の例は、 TENANTACCOUNTID の署名済み認証 URL を取得するための POST 要求です。結果は python-m json ツールに渡され、 JSON エンコードが削除されます。

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
  -H "accept: application/json" -H  "Content-Type: application/json"
\
  --data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

この例の応答には、 URL エンコードされた署名済み URL が含まれていますが、 JSON エンコードされたレイヤは含まれていません。

```
{
    "apiVersion": "3.0",
    "data": "https://my-pf-baseurl/idp/SSO.saml2?...",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

c. 後続のコマンドで使用できるように、応答からを保存し `SAMLRequest`ます。

```
export SAMLREQUEST="https://my-pf-baseurl/idp/SSO.saml2?..."
```

d. 応答とクッキーをエクスポートし、応答をエコーします。

```
RESPONSE=$(curl -c - "$SAMLREQUEST")
```

```
echo "$RESPONSE" | grep 'input type="hidden" name="pf.adapterId"
id="pf.adapterId"'
```

e. 'pf.adapterID' 値をエクスポートし、応答をエコーします。

```
export ADAPTER='myAdapter'
```

```
echo "$RESPONSE" | grep 'base'
```

f. 「 href 」値をエクスポートし（末尾のスラッシュ / を削除）、応答をエコーします。

```
export BASEURL='https://my-pf-baseurl'
```

```
echo "$RESPONSE" | grep 'form method="POST"'
```

g. 「 action 」の値をエクスポートします。

```
export SSOPING='/idp/.../resumeSAML20/idp/SSO.ping'
```

h. クレデンシャルとともに Cookie を送信する：

```
curl -b <(echo "$RESPONSE") -X POST "$BASEURL$SSOPING" \
--data "pf.username=$SAMLUSER&pf.pass=
$SAMLPASSWORD&pf.ok=clicked&pf.cancel=&pf.adapterId=$ADAPTER"
--include
```

i. 非表示フィールドからを保存し `SAMLResponse`ます。

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. 保存したを使用して `SAMLResponse`、StorageGRID認証トークンを生成するStorageGRID要求を行い`/api/saml-response`ます。

で `RelayState`、テナントアカウントIDを使用するか、グリッド管理APIにサインインする場合は0を使用します。

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
  -H "accept: application/json" \
  --data-urlencode "SAMLResponse=$SAMLResponse" \
  --data-urlencode "RelayState=$TENANTACCOUNTID" \
  | python -m json.tool
```

応答には認証トークンが含まれています。

```
{
    "apiVersion": "3.0",
    "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
    "responseTime": "2018-11-07T21:32:53.486Z",
    "status": "success"
}
```

a. 応答に認証トークンをとして保存し `MYTOKEN`ます。

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

SSOが使用されていない場合のAPIの使用方法と同様に、を他の要求に使用できるようになりまし `MYTOKEN`た。

シングルサインオンが有効な場合は、 **API** からサインアウトします

シングルサインオン（ SSO ）が有効になっている場合は、グリッド管理 API またはテナント管理 API からサインアウトするための一連の API 要求を問題 で処理する必要があります。これらの手順は、 SSO アイデンティティプロバイダとして PingFederate を使用している場合に適用されます

タスクの内容

必要に応じて、組織のシングルログアウトページからログアウトすることで、StorageGRID APIからサインアウトできます。または、 StorageGRID からシングルログアウト（ SLO ）を実行することもできます。この場合、有効な StorageGRID ベアラトークンが必要です。

手順

1. 署名されたログアウト要求を生成するには、「cookie "sso=true」をSLO APIに渡します。

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

ログアウト URL が返されます。

```
{
    "apiVersion": "3.0",
    "data": "https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D",
    "responseTime": "2021-10-12T22:20:30.839Z",
    "status": "success"
}
```

2. ログアウト URL を保存します。

```
export LOGOUT_REQUEST='https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D'
```

3. 要求をログアウト URL に送信し、 SLO を実行して StorageGRID にリダイレクトします。

```
curl --include "$LOGOUT_REQUEST"
```

302 応答が返されます。リダイレクト先は API のみのログアウトには適用されません。

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: PF=QoKs...SgCC; Path=/; Secure; HttpOnly; SameSite=None
```

4. StorageGRID Bearer トークンを削除します。

StorageGRID Bearer トークンを削除すると、 SSO を使用しない場合と同じように動作します。「cookie "sso=true"」が指定されていない場合、ユーザはSSO状態に影響を与えずにStorageGRIDからログアウトされます。

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

ユーザがサインアウトされたことを示す応答が `204 No Content`返されます。

```
HTTP/1.1 204 No Content
```

グリッド管理 API を使用すると、 StorageGRID システムの特定の機能を完全に非アクティブ化できます。機能を非アクティブ化すると、その機能に関連するタスクを実行する権限をユーザに割り当てることができなくなります。

タスクの内容

非活動化されたフィーチャーシステムを使用すると、 StorageGRID システムの特定のフィーチャーへのアクセスを禁止できます。機能の非アクティブ化は、 root ユーザまたは * Root Access * 権限を持つ管理者グループに属するユーザがその機能を使用できないようにする唯一の方法です。

この機能がどのように役立つかを理解するために、次のシナリオを検討してください。

_Company A は、テナントアカウントを作成して StorageGRID システムのストレージ容量をリースするサービスプロバイダです。容量をリースしている顧客のオブジェクトのセキュリティを保護するために、 A 社では、アカウントの導入後に自社の従業員がテナントアカウントにアクセスできないようにしたいと考えています。 _

_ 企業 A は、グリッド管理 API で Deactivate Features システムを使用することで、この目的を達成できます。Grid Manager（UIとAPIの両方）で「Change tenant root password」機能を完全に非アクティブ化することで、A社の管理者ユーザ（rootユーザおよび* Root access *権限を持つグループに属するユーザを含む）がテナントアカウントのrootユーザのパスワードを変更できないようにします。_

手順

1. Swagger のグリッド管理 API のドキュメントにアクセスします。を参照して "グリッド管理 API を使用します"
2. Deactivate Features エンドポイントを探します。
3. テナントの root パスワードの変更などの機能を非アクティブ化するには、次のような本文を API に送信します。

   ```
   { "grid": {"changeTenantRootPassword": true} }
   ```

   要求が完了すると、テナントの root パスワードの変更機能が無効になります。Change tenant root password *管理権限はユーザインターフェイスに表示されなくなり、テナントのrootパスワードを変更しようとするAPI要求は「403 Forbidden」で失敗します。

非アクティブ化した機能を再アクティブ

デフォルトでは、グリッド管理 API を使用して、非アクティブ化した機能を再アクティブ化できます。ただし、非アクティブ化された機能が再アクティブ化されないようにするには、 * activateFeatures * 機能自体を非アクティブ化します。

> *activateFeatures*機能を再度有効にすることはできません。この機能を非アクティブ化すると、非アクティブ化した他の機能を永続的に再アクティブ化できなくなることに注意してください。失われた機能をリストアするには、テクニカルサポートにお問い合わせください。

手順

1. Swagger のグリッド管理 API のドキュメントにアクセスします。
2. Deactivate Features エンドポイントを探します。

3. すべての機能を再アクティブ化するには、次のような本文を API に送信します。

```
{ "grid": null }
```

この要求が完了すると、テナントの root パスワード変更機能を含むすべての機能が再アクティブ化されます。ユーザに * Root access * 権限または * Change tenant root password * 管理権限が割り当てられている場合、テナントの root パスワードを変更する API 要求はすべてユーザインターフェイスに表示され、テナントの root パスワードを変更する API 要求は成功します。



前述の例は、 _all_deactivated 機能を再アクティブ化します。非アクティブ化したままにする必要がある他の機能が非アクティブ化されている場合は、 PUT 要求でそれらを明示的に指定する必要があります。たとえば、Change tenant root password機能を再アクティブ化し、引き続きstorageadmin管理権限を非アクティブ化するには、次のPUT要求を送信します。+

```
{ "grid": {"storageAdmin": true} }
```

StorageGRID へのアクセスを制御します

StorageGRID アクセスを制御します

グループやユーザーを作成またはインポートし、各グループに権限を割り当てることで、StorageGRID へのアクセス権を持つユーザーと、ユーザーが実行できるタスクを制御できます。オプションで、シングル サインオン（SSO）の有効化、クライアント証明書の作成、グリッドパスワードの変更、およびマルチ管理者認証の使用が可能です。

Grid Manager へのアクセスを制御

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

を使用する"アイデンティティフェデレーション"と、セットアップが"グループ" "ユーザ"高速化され、使い慣れたクレデンシャルを使用してStorageGRIDにサインインできます。Active Directory 、 OpenLDAP 、または Oracle Directory Server を使用する場合は、アイデンティティフェデレーションを設定できます。



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

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

必要に応じて、グループを読み取り専用に設定することができます。読み取り専用グループのユーザは、設定と機能のみを表示できます。Grid Managerまたはグリッド管理APIでは、変更を加えたり処理を実行したりすることはできません。

シングルサインオンを有効にします

StorageGRID システムは、Security Assertion Markup Language 2.0（SAML 2.0）または OpenID Connect（OIDC）標準を使用したシングル サインオン（SSO）をサポートしています。"SSOを設定して有効にします"を実行すると、すべてのユーザーは、Grid Manager、Tenant Manager、Grid Management API、または

Tenant Management API にアクセスする前に、外部の ID プロバイダーによって認証される必要があります。ローカルユーザーは StorageGRID にサインインできません。

プロビジョニングパスフレーズを変更します

プロビジョニング パスフレーズは、多くのインストールおよびメンテナンス手順、およびStorageGRIDリカバリ パッケージのダウンロードに必要です。パスフレーズは、 StorageGRIDシステムのグリッド トポロジ情報と暗号化キーのバックアップをダウンロードする場合にも必要です。あなたはできる"パスフレーズを変更します"必要に応じて。

ノードのコンソールパスワードを変更します

グリッド内の各ノードにはノード コンソール パスワードがあり、SSH を使用して「admin」としてノードにログインするか、VM/物理コンソール接続で root ユーザーとしてログインする必要があります。必要に応じて、"ノードのコンソールパスワードを変更します"各ノードに対して。

複数管理者による認証を使用する

マルチ管理者検証（MAV）を使用すると、特定のStorageGRID操作を指定された管理者の承認後にのみ実行できるようにすることができます。MAVは、侵害された管理者、悪意のある管理者、または経験の浅い管理者が、望ましくない変更を行ったり、データを削除したりすることを防止します。

StorageGRID プロビジョニング パスフレーズを変更する

StorageGRIDプロビジョニング パスフレーズを変更するには、この手順を使用します。パスフレーズは、回復、拡張、およびメンテナンスの手順に必要です。パスフレーズは、グリッド トポロジ情報、グリッド ノード コンソール パスワード、およびStorageGRIDシステムの暗号化キーを含むリカバリ パッケージ バックアップをダウンロードする場合にも必要です。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- Maintenance または Root アクセス権限が必要です。
- 現在のプロビジョニングパスフレーズを用意します。

タスクの内容

プロビジョニングパスフレーズは、多くのインストールおよびメンテナンス手順で必要であり、"リカバリパッケージのダウンロード" 。プロビジョニングパスフレーズは、 `Passwords.txt`ファイル。プロビジョニングパスフレーズを必ず文書化し、安全な場所に保管してください。

手順

1. 構成 > アクセス制御 > グリッド パスワード を選択します。
2. で、[変更]*を選択します
3. 現在のプロビジョニングパスフレーズを入力します。
4. 新しいパスフレーズを入力します。パスフレーズは 8 文字以上 32 文字以下にする必要があります。パスフレーズでは大文字と小文字が区別されます。

プロビジョニング パスフレーズを安全な場所に保存します。インストール、拡張、メンテナンスの手順に必要です。

5. 新しいパスフレーズをもう一度入力し、「 * 保存 * 」を選択します。

   プロビジョニングパスフレーズの変更が完了すると、成功を示す緑のバナーが表示されます。



6. リカバリパッケージ * を選択します。
7. 新しいプロビジョニング パスフレーズを入力して、新しいリカバリ パッケージをダウンロードします。

プロビジョニング パスフレーズを変更した後は、すぐに新しいリカバリ パッケージをダウンロードする必要があります。リカバリ パッケージ ファイルを使用すると、障害が発生した場合にシステムを復元できます。

StorageGRIDでノードコンソールのパスワードを変更する

グリッド内の各ノードにはノード コンソール パスワードがあり、これを使用してノードにログインします。デフォルトでは、各ノードには一意のパスワードがあります。各パスワードを新しい一意のパスワードに変更することも、すべてのノードのパスワードを変更してグローバル パスワードを使用することもできます。パスワードはリカバリ パッケージに保存されます。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"Maintenance権限またはRoot Access権限"。
- 現在のプロビジョニングパスフレーズを用意します。

タスクの内容

ノード コンソール パスワードは、SSH を使用して「admin」としてノードにログインするか、VM/物理コンソール接続で root ユーザーとしてログインするために使用します。次のいずれかのオプションを使用して、ノード コンソールのパスワードを変更できます。

- 各ノードにランダムなパスワードを自動的に適用する
- すべてのノードに1つのグローバルパスワードを指定して適用する
- 1 つ以上のノードに一意のパスワードを指定して適用します

パスワードは更新された `Passwords.txt`リカバリ パッケージ内のファイル。パスワードはファイル内の「パスワード」列にリストされます。

その"SSHアクセスパスワード"ノード間の通信に使用される SSH キーは、ノード コンソールのパスワードとは別です。この手順では、SSH アクセス パスワードは変更されません。

ウィザードにアクセスします

手順

1. 構成 > アクセス制御 > グリッド パスワード を選択します。
2. で、[変更する]*を選択します。

現在のリカバリパッケージをダウンロードします

ノード コンソールのパスワードを変更する前に、現在のリカバリ パッケージをダウンロードしてください。いずれかのノードでパスワード変更プロセスが失敗した場合は、このファイル内のパスワードを使用できます。

手順

1. グリッドのプロビジョニングパスフレーズを入力します。
2. [リカバリパッケージのダウンロード] を選択します。
3. リカバリパッケージファイルをコピーする(`.zip`) を 2 つの安全でセキュリティ保護された別の場所に保管します。

> リカバリ パッケージ ファイルには、 StorageGRIDシステムからデータを取得するために使用できる暗号化キーとパスワードが含まれているため、セキュリティで保護する必要があります。

4. 「 * Continue * 」を選択します。

新しいパスワードを入力してください

1. 使用するパスワード変更方法を選択します。
   - 自動: StorageGRID は、すべてのノードに新しいランダムなコンソール パスワードを自動的に割り当てます。
   - カスタム: コンソールのパスワードを入力します。

自動

1. 「 * Continue * 」を選択します。

カスタム

1. 次のいずれかを選択します。
   - グローバル コンソール パスワード: すべてのノードに同じコンソール パスワードを適用します。
   - 一意のコンソール パスワード: 1 つ以上のノードに異なるパスワードを適用します。
2. グローバル コンソール パスワード を選択した場合は、すべてのノードに使用するパスワードを入力します。
3. 一意のコンソール パスワード を選択した場合は、1 つ以上のノードに対して一意のパスワードを入力します。
4. 「 * Continue * 」を選択します。

1. 確認ダイアログが表示されたら、 StorageGRIDがノード コンソールのパスワードの変更を開始する準備ができたら、[はい] を選択します。

   このプロセスは開始後にキャンセルすることはできません。

   StorageGRID は、新しいパスワードを含む新しいリカバリ パッケージを生成します。

2. 新しいリカバリ パッケージの準備ができたら、[新しいリカバリ パッケージをダウンロード] を選択し、リカバリ パッケージを保存します。
3. ファイルを開き `.zip`ます。
4. の内容にアクセスできることを確認します。これには、ノードコンソールの新しいパスワードが含まれています。ファイルも含ま `Passwords.txt`れます。
5. 新しいリカバリパッケージファイルをコピーします(`.zip`) を 2 つの安全でセキュリティ保護された別の場所に保管します。

   古いリカバリ パッケージを上書きしないでください。

   リカバリ ファイルには、 StorageGRIDシステムからデータを取得するために使用できる暗号化キーとパスワードが含まれているため、セキュリティで保護する必要があります。

6. 新しいリカバリ パッケージをダウンロードし、その内容を確認したことを示すには、チェックボックスを選択します。
7. 「 * Continue * 」を選択します。

   StorageGRID は各ノードのパスワードを更新します。

   更新プロセス中にエラーが発生した場合、進行状況バーにパスワードの変更に失敗したノードの数が表示されます。システムは、パスワードの変更に失敗したノードに対してプロセスを自動的に再試行します。一部のノードでパスワードが変更されていない状態でプロセスが終了した場合は、[再試行] ボタンが表示されます。

8. 1 つ以上のノードでパスワードの更新に失敗した場合：
   a. 表に表示されたエラーメッセージを確認します。
   b. 問題を解決します。
   c. [* Retry*] を選択します。

      再試行すると、前回のパスワード変更で失敗したノード上のノードコンソールパスワードのみが変更されます。

9. 進行状況バーに残りの更新がないことが示されたら、[完了] を選択します。
10. すべてのノードのノードコンソールのパスワードが変更されたら、最初にダウンロードしたリカバリパッケージ 。

StorageGRID 管理ノードの SSH アクセス パスワードを変更する

管理ノードのSSHアクセスパスワードを変更すると、グリッド内の各ノードの一意の内部SSHキーセットも更新されます。プライマリ管理ノードは、これらのSSHキーを使用して、セキュアなパスワードレス認証を使用してノードにアクセスします。

SSHキーを使用して、VMまたは物理コンソール接続でノードに、またはrootユーザとしてログインし `admin` ます。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"Maintenance権限またはRoot Access権限"。
- 現在のプロビジョニングパスフレーズを用意します。

タスクの内容

管理ノードの新しいアクセスパスワードと各ノードの新しい内部キーは、 `Passwords.txt`リカバリ パッケージ内のファイル。キーはそのファイルの「パスワード」列にリストされています。

ノード間の通信に使用する SSH キー用に、個別の SSH アクセスパスワードがあります。これらはこの手順では変更されません。

ウィザードにアクセスします

手順

1. 構成 > アクセス制御 > グリッド パスワード を選択します。
2. [SSHキーの変更]*で、*変更する*を選択します。

現在のリカバリパッケージをダウンロードします

SSH アクセス キーを変更する前に、現在のリカバリ パッケージをダウンロードしてください。いずれかのノードでキー変更プロセスが失敗した場合は、このファイル内のキーを使用できます。

手順

1. グリッドのプロビジョニングパスフレーズを入力します。
2. [リカバリパッケージのダウンロード] を選択します。
3. リカバリパッケージファイルをコピーする(`.zip`) を 2 つの安全でセキュリティ保護された別の場所に保管します。

> リカバリ パッケージ ファイルには、 StorageGRIDシステムからデータを取得するために使用できる暗号化キーとパスワードが含まれているため、セキュリティで保護する必要があります。

4. 「 * Continue * 」を選択します。
5. 確認ダイアログが表示されたら、SSHアクセスキーの変更を開始する準備ができている場合は*[はい]*を選択します。

> このプロセスは開始後にキャンセルすることはできません。

SSHアクセスキーの変更

SSH アクセス キーの変更プロセスが開始されると、新しいキーを含む新しい回復パッケージが生成されます。その後、各ノードでキーが更新されます。

手順

1. 新しい回復パッケージが生成されるまで待ちます。これには数分かかる場合があります。
2. 新しいリカバリパッケージのダウンロードボタンが有効になったら、*新しいリカバリパッケージのダウンロード*を選択し、新しいリカバリパッケージファイルを保存します。(`.zip`) を 2 つの安全でセキュリティ保護された別の場所に保管します。
3. ダウンロードが完了したら、次の手順を実行

   a. ファイルを開き `.zip`ます。

   b. 新しいSSHアクセスキーを含むファイルなどのコンテンツにアクセスできることを確認します `Passwords.txt`。

   c. 新しいリカバリパッケージファイルをコピーします(`.zip`) を 2 つの安全でセキュリティ保護された別の場所に保管します。

   > ! 古いリカバリ パッケージを上書きしないでください。

   リカバリ パッケージ ファイルには、 StorageGRIDシステムからデータを取得するために使用できる暗号化キーとパスワードが含まれているため、セキュリティで保護する必要があります。

4. 各ノードでキーが更新されるまで待ちます。更新には数分かかることがあります。

   すべてのノードでキーを変更すると、成功を示す緑色のバナーが表示されます。

   更新プロセス中にエラーが発生した場合は、バナーメッセージにキーが変更されなかったノードの数が表示されます。キーの変更に失敗したノードでは、プロセスが自動的に再試行されます。一部のノードでキーが変更されていない状態でプロセスが終了すると、* Retry *ボタンが表示されます。

   1つ以上のノードでキーの更新に失敗した場合：

   a. 表に表示されたエラーメッセージを確認します。

   b. 問題を解決します。

   c. [* Retry*] を選択します。

      再試行すると、前回のキー変更で失敗したノードのSSHアクセスキーだけが変更されます。

5. すべてのノードのSSHアクセスキーが変更されたら、最初にダウンロードしたリカバリパッケージ 。
6. 必要に応じて、[メンテナンス] > [システム] > [回復パッケージ] を選択して、新しい回復パッケージの追加コピーをダウンロードします。

StorageGRIDでIDフェデレーションを使用する

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

Grid Manager のアイデンティティフェデレーションを設定する

管理者グループとユーザーを Active Directory、Microsoft Entra ID、OpenLDAP、Oracle Directory Server などの別のシステムで管理する場合は、Grid Manager で ID フェデレーションを構成できます。

開始する前に

- グリッドマネージャーにサインインするには、"サポートされている Web ブラウザ" 。
- あなたは"特定のアクセス権限"。
- アイデンティティ プロバイダーとして、Active Directory、Microsoft Entra ID、OpenLDAP、または Oracle Directory Server を使用しています。

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

- OpenLDAP を使用する場合は、 OpenLDAP サーバを設定する必要があります。を参照して OpenLDAP サーバの設定に関するガイドライン
- シングルサインオン（SSO）を有効にする予定の場合は、"シングルサインオンの要件と考慮事項" 。
- LDAP サーバとの通信に Transport Layer Security （ TLS ）を使用する場合は、アイデンティティプロバイダが TLS 1.2 または 1.3 を使用しています。を参照して "発信 TLS 接続でサポートされる暗号"

タスクの内容

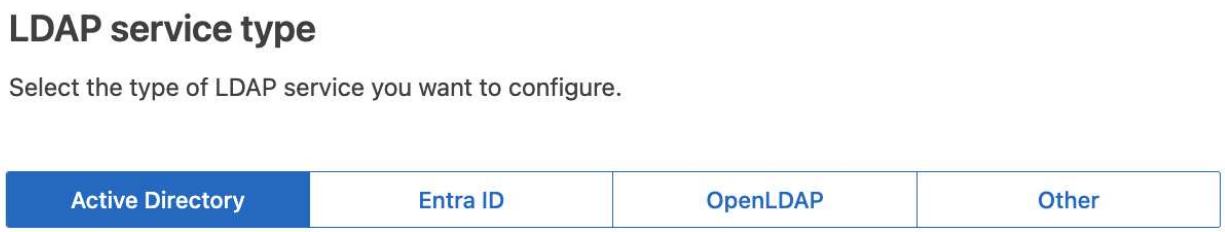
Active Directory、Microsoft Entra ID、OpenLDAP、Oracle Directory Server などの別のシステムからグループをインポートする場合は、Grid Manager の ID ソースを構成できます。次の種類のグループをインポートできます。

- 管理者グループ。管理者グループ内のユーザは、グループに割り当てられた管理権限に基づいて、 Grid Manager にサインインしてタスクを実行できます。
- 独自のアイデンティティソースを使用しないテナントのテナントユーザグループ。テナントグループ内のユーザは、 Tenant Manager でグループに割り当てられた権限に基づいてタスクを実行し、 Tenant Manager にサインインしてタスクを実行できます。詳細については、および"テナントアカウントを使用する"を参照してください"テナントアカウントを作成する"。

設定を入力します

手順

1. 構成 > アクセス制御 > **ID** フェデレーション を選択します。
2. ［ * アイデンティティフェデレーションを有効にする * ］ を選択
3. LDAP サービスタイプセクションで、設定する LDAP サービスのタイプを選択します。



Oracle Directory Server を使用する LDAP サーバーの値を設定するには、 * その他 * を選択します。

4. [* その他 *] を選択した場合は、 [LDAP 属性] セクションのフィールドに入力します。それ以外の場合は、次の手順に進みます。
   - ユーザーの一意の名前: LDAP ユーザーの一意の識別子を含む属性の名前。この属性は、 `sAMAccountName` Active Directoryおよび `uid`OpenLDAP 用。 `Oracle Directory Server`を構成する場合は、次のように入力します。 `uid`。
   - ユーザー **UUID**: LDAP ユーザーの永続的な一意の識別子を含む属性の名前。この属性は、 `objectGUID` Active Directoryおよび `entryUUID`OpenLDAP 用。 `Oracle Directory Server`を構成する場合は、次のように入力します。 `nsuniqueid`。指定された属性の各ユーザーの値は、16 バイト形式または文字列形式の 32 桁の 16 進数である必要があります。ハイフンは無視されます。
   - グループの一意の名前: LDAP グループの一意の識別子を含む属性の名前。この属性は、 `sAMAccountName` Active Directoryおよび `cn`OpenLDAP 用。 `Oracle Directory Server`を構成する場合は、次のように入力します。 `cn`。
   - グループ **UUID**: LDAP グループの永続的な一意の識別子を含む属性の名前。この属性は、 `objectGUID` Active Directoryおよび `entryUUID`OpenLDAP 用。 `Oracle Directory Server`を構成する場合は、次のように入力します。 `nsuniqueid`。指定された属性の各グループの値は、16 バイト形式または文字列形式の 32 桁の 16 進数である必要があります。ハイフンは無視されます。
5. すべての LDAP サービスタイプについて、 LDAP サーバの設定セクションに必要な LDAP サーバおよびネットワーク接続情報を入力します。
   - * Hostname * ： LDAP サーバの完全修飾ドメイン名（ FQDN ）または IP アドレス。
   - * Port * ： LDAP サーバへの接続に使用するポート。

     STARTTLS のデフォルトポートは 389 、 LDAPS のデフォルトポートは 636 です。ただし、ファイアウォールが正しく設定されていれば、任意のポートを使用できます。

   - * Username * ： LDAP サーバに接続するユーザの識別名（ DN ）の完全パス。

     Active Directory の場合は、ダウンレベルログオン名またはユーザープリンシパル名を指定することもできます。

     指定するユーザには、グループおよびユーザを表示する権限、および次の属性にアクセスする権限が必要です。

     - `sAMAccountName`または `uid`
     - `objectGUID`、 `entryUUID`、または `nsuniqueid`

- `cn`
- `memberOf`または `isMemberOf`
- * Active Directory *： `objectSid`、 `primaryGroupID`、 `userAccountControl`、および `userPrincipalName`
- エントラ**ID**: `accountEnabled`そして `userPrincipalName`

◦ * Password * ：ユーザ名に関連付けられたパスワード。

> ⓘ 今後パスワードを変更する場合は、このページでパスワードを更新する必要があります。

◦ * Group Base DN * ：グループを検索する LDAP サブツリーの識別名（ DN ）の完全パス。Active Directory では、ベース DN に対して相対的な識別名（ DC=storagegrid 、 DC=example 、 DC=com など）のグループをすべてフェデレーテッドグループとして使用できます。

> ⓘ * グループの一意な名前 * 値は、所属する * グループベース DN * 内で一意である必要があります。

◦ * User Base DN * ：ユーザを検索する LDAP サブツリーの識別名（ DN ）の完全パス。

> ⓘ * ユーザーの一意な名前 * 値は、それぞれが属する * ユーザーベース DN * 内で一意である必要があります。

◦ ユーザー名のバインド形式（オプション）：パターンを自動的に決定できない場合にStorageGRID が使用するデフォルトのユーザー名パターン。

StorageGRID がサービスアカウントにバインドできない場合にユーザがサインインできるようにするため、 * バインドユーザ名形式 * を指定することを推奨します。

次のいずれかのパターンを入力します。

- **UserPrincipalName** パターン **(AD** および **Entra ID)**: `[USERNAME]@example.com`
- ダウンレベル ログオン名パターン **(AD** および **Entra ID)**: `example\[USERNAME]`
- 識別名パターン： `CN=[USERNAME],CN=Users,DC=example,DC=com`

  記載されているとおりに * [username] * を含めます。

6. Transport Layer Security （ TLS ）セクションで、セキュリティ設定を選択します。
   ◦ **STARTTLS** を使用する: STARTTLS を使用して、LDAP サーバーとの通信を保護します。これは、Active Directory、OpenLDAP、またはその他の場合に推奨されるオプションですが、このオプションは Microsoft Entra ID ではサポートされていません。
   ◦ **LDAPS** を使用する: LDAPS (LDAP over SSL) オプションは、TLS を使用して LDAP サーバーへの接続を確立します。 Microsoft Entra ID の場合はこのオプションを選択する必要があります。
   ◦ **TLS** を使用しない: StorageGRIDシステムと LDAP サーバー間のネットワーク トラフィックは保護されません。このオプションは Microsoft Entra ID ではサポートされていません。

Active Directory サーバーが LDAP 署名を強制している場合、「TLS を使用しない」オプションの使用はサポートされません。 STARTTLS または LDAPS を使用する必要があります。

7. STARTTLS または LDAPS を選択した場合は、接続の保護に使用する証明書を選択します。
   - * オペレーティングシステムの CA 証明書を使用 * ：オペレーティングシステムにインストールされているデフォルトの Grid CA 証明書を使用して接続を保護します。
   - * カスタム CA 証明書を使用 * ：カスタムセキュリティ証明書を使用します。

     この設定を選択した場合は、カスタムセキュリティ証明書をコピーして CA 証明書テキストボックスに貼り付けます。

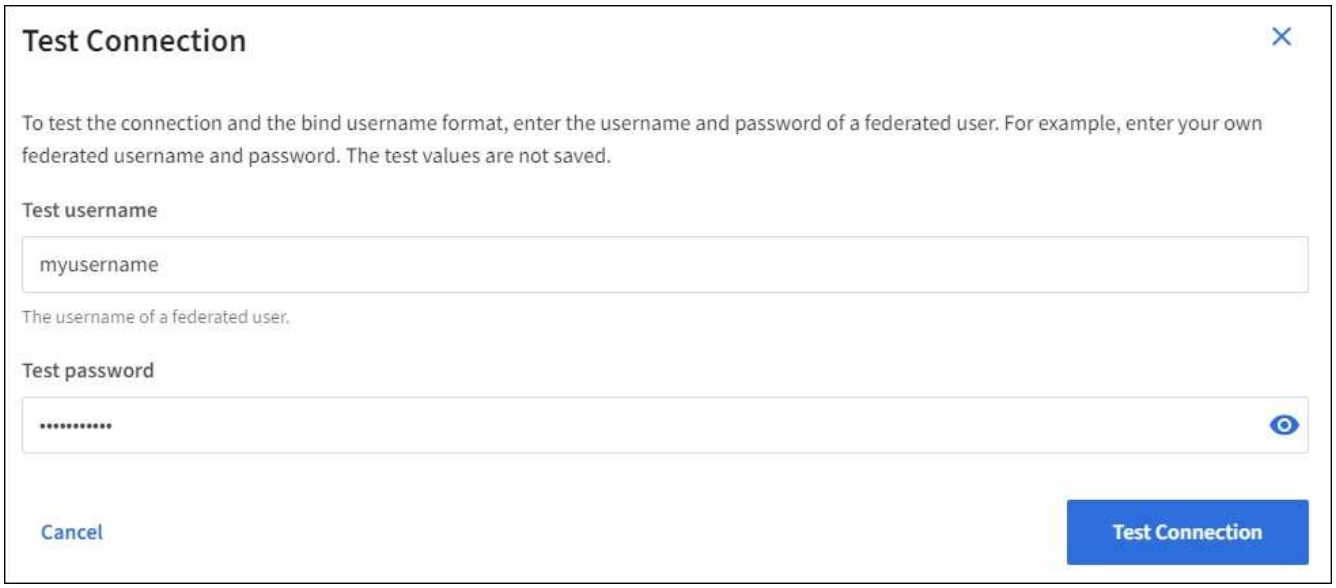
接続をテストして設定を保存します

すべての値を入力したら、設定を保存する前に接続をテストする必要があります。StorageGRID では、LDAP サーバの接続設定とバインドユーザ名の形式が指定されている場合は検証されます。

手順

1. [接続のテスト *] を選択します。
2. バインドユーザー名の形式を指定しなかった場合:
   - 接続設定が有効な場合は、「Test connection successful」というメッセージが表示されます。[保存（ Save ）] を選択して、構成を保存します。
   - 接続設定が無効な場合は、「test connection could not be established」というメッセージが表示されます。[閉じる（ Close ）] を選択します。その後、問題を解決して接続を再度テストします。
3. バインドユーザ名の形式を指定した場合は、有効なフェデレーテッドユーザのユーザ名とパスワードを入力します。

   たとえば、自分のユーザ名とパスワードを入力します。ユーザ名に特殊文字（@、/など）を使用しないでください。



   - 接続設定が有効な場合は、「Test connection successful」というメッセージが表示されます。[保存（

Save ）] を選択して、構成を保存します。

- 接続設定、バインドユーザ名形式、またはテストユーザ名とパスワードが無効な場合は、エラーメッセージが表示されます。問題を解決してから、もう一度接続をテストしてください。

アイデンティティソースとの強制同期

StorageGRID システムは、アイデンティティソースからフェデレーテッドグループおよびユーザを定期的に同期します。ユーザの権限をすぐに有効にしたり制限したりする必要がある場合は、同期を強制的に開始できます。

手順

1. アイデンティティフェデレーションページに移動します。
2. ページの上部にある「 * サーバーを同期」を選択します。

環境によっては、同期プロセスにしばらく時間がかかることがあります。

アイデンティティフェデレーション同期エラー * アラートは、アイデンティティソースからフェデレーテッドグループとユーザを同期する問題 がある場合にトリガーされます。

アイデンティティフェデレーションを無効にする

グループおよびユーザーの ID フェデレーションを一時的または永続的に無効にすることができます。アイデンティティ フェデレーションが無効になっている場合、 StorageGRIDとアイデンティティ ソース間の通信は行われません。ただし、構成した設定はすべて保持されるため、将来的に ID フェデレーションを簡単に再度有効にすることができます。

タスクの内容

アイデンティティフェデレーションを無効にする前に、次の点に注意してください。

- フェデレーテッドユーザはサインインできなくなります。
- 現在サインインしているフェデレーテッドユーザは、セッションが有効な間は StorageGRID システムに引き続きアクセスできますが、セッションが期限切れになると以降はサインインできなくなります。
- StorageGRIDシステムとアイデンティティ ソース間の同期は行われず、同期されていないアカウントに対してアラートは発生しません。
- シングル サインオン (SSO) ステータスが 有効 または サンドボックス モード の場合、**ID** フェデレーションを有効にする チェックボックスは無効になります。 ID フェデレーションを無効にする前に、シングル サインオン ページの SSO ステータスを 無効 にする必要があります。見る"シングルサインオンを無効にします" 。

手順

1. アイデンティティフェデレーションページに移動します。
2. [アイデンティティフェデレーションを有効にする]*チェックボックスをオフにします。

OpenLDAP サーバの設定に関するガイドライン

アイデンティティフェデレーションに OpenLDAP サーバを使用する場合は、 OpenLDAP サーバで特定の設定が必要です。

Active Directory または Microsoft Entra ID 以外の ID ソースの場合、 StorageGRID は外部的に無効にされているユーザーへの S3 アクセスを自動的にブロックしません。 S3 アクセスをブロックするには、ユーザーの S3 キーを削除するか、すべてのグループからユーザーを削除します。

memberof オーバーレイと **refint** オーバーレイ

memberof オーバーレイと refint オーバーレイを有効にする必要があります。詳細については、のリバースグループメンバーシップのメンテナンス手順を参照してくださいhttp://www.openldap.org/doc/admin24/index.html["OpenLDAP のドキュメント：バージョン 2.4 管理者ガイド"^]。

インデックス作成

次の OpenLDAP 属性とインデックスキーワードを設定する必要があります。

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

また、パフォーマンスを最適化するには、 Username のヘルプで説明されているフィールドにインデックスを設定してください。

のリバースグループメンバーシップのメンテナンスに関する情報を参照してくださいhttp://www.openldap.org/doc/admin24/index.html["OpenLDAP のドキュメント：バージョン 2.4 管理者ガイド"^]。

関連情報

"外部との通信に使用するポート"

StorageGRID で管理者グループを管理する

管理者グループを作成して、 1 人以上の管理者ユーザのセキュリティ権限を管理できます。StorageGRID システムへのアクセスを許可するには、ユーザがグループに属している必要があります。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- そうだな "特定のアクセス権限"
- フェデレーテッドグループをインポートする場合は、アイデンティティフェデレーションを設定済みで、フェデレーテッドグループが設定済みのアイデンティティソースにすでに存在している必要があります。

管理者グループを作成します

管理者グループを使用すると、 Grid Manager およびグリッド管理 API のどのユーザがどの機能や処理にアクセスできるかを決定できます。

ウィザードにアクセスします

手順

1. 構成 > アクセス制御 > *管理者グループ*を選択します。
2. 「 * グループを作成 * 」を選択します。

グループタイプを選択します

ローカルグループを作成するか、フェデレーテッドグループをインポートできます。

- ローカルユーザに権限を割り当てる場合は、ローカルグループを作成します。
- アイデンティティソースからユーザをインポートするためのフェデレーテッドグループを作成します。

ローカルグループ

手順

1. * ローカルグループ * を選択します。
2. グループの表示名を入力します。必要に応じてあとから更新できます。たとえば、「Maintenance Users」や「ILM Administrators」などです。
3. グループの一意の名前を入力します。この名前は後で更新できません。
4. 「 * Continue * 」を選択します。

フェデレーテッドグループ

手順

1. [フェデレーショングループ] を選択します。
2. インポートするグループの名前を、設定されているアイデンティティソースに表示されているとおりに入力します。
   - Active Directory および Microsoft Entra ID の場合は、sAMAccountName を使用します。
   - OpenLDAP の場合は、 CN （共通名）を使用します。
   - 別の LDAP を使用する場合は、 LDAP サーバに適切な一意の名前を使用します。
3. 「 * Continue * 」を選択します。

グループの権限を管理します

手順

1. * アクセスモード * では、グループ内のユーザが Grid Manager およびグリッド管理 API で設定の変更や処理を実行できるかどうか、あるいは設定と機能のみを表示できるかどうかを選択します。
   - * 読み取り / 書き込み * （デフォルト）：ユーザは設定を変更し、管理権限で許可されている操作を実行できます。
   - * 読み取り専用 * ：ユーザーは設定と機能のみを表示できます。Grid Managerまたはグリッド管理APIでは、変更を加えたり処理を実行したりすることはできません。ローカルの読み取り専用ユーザは自分のパスワードを変更できます。

ユーザーが複数のグループに属していて、いずれかのグループが * 読み取り専用 * に設定されている場合、ユーザーは選択したすべての設定と機能に読み取り専用でアクセスできます。

2. 1つ以上を選択し"管理者グループの権限"ます。

   各グループに 1 つ以上の権限を割り当てる必要があります。そうしないと、グループに属するユーザは StorageGRID にサインインできません。

3. ローカルグループを作成する場合は、「 * Continue * 」を選択します。フェデレーテッドグループを作成する場合は、 * Create group * および * Finish * を選択します。

ユーザの追加（ローカルグループのみ）

手順

1. 必要に応じて、このグループに対して 1 人以上のローカルユーザを選択します。

   ローカルユーザをまだ作成していない場合は、ユーザを追加せずにグループを保存できます。このグループは、ユーザページでユーザに追加できます。詳細は、を参照してください "ユーザの管理" 。

2. [グループの作成 *] と [完了 *] を選択します。

管理者グループを表示および編集します

既存のグループの詳細の表示、グループの変更、またはグループの複製を行うことができます。

- すべてのグループの基本情報を表示するには '[グループ] ページの表を確認します
- 特定のグループのすべての詳細を表示したり、グループを編集したりするには、 * アクション * メニューまたは詳細ページを使用します。

タスク	**[Actions]**メニュー	詳細ページ
グループの詳細を表示します	a. グループのチェックボックスをオンにします。 b. [* アクション * > * グループの詳細を表示 *] を選択します。	テーブルでグループ名を選択します。
表示名の編集（ローカルグループのみ）	a. グループのチェックボックスをオンにします。 b. [* アクション * > * グループ名の編集 *] を選択します。 c. 新しい名前を入力します。 d. 「変更を保存」を選択します。	a. グループ名を選択して詳細を表示します。 b. 編集アイコン を選択します。 c. 新しい名前を入力します。 d. 「変更を保存」を選択します。

タスク	[Actions]メニュー	詳細ページ
アクセスモードまたは権限を編集します	a. グループのチェックボックスをオンにします。 b. [* アクション * > * グループの詳細を表示 *] を選択します。 c. 必要に応じて、グループのアクセスモードを変更します。 d. 必要に応じて、を選択または選択解除し"管理者グループの権限"ます。 e. 「変更を保存」を選択します。	a. グループ名を選択して詳細を表示します。 b. 必要に応じて、グループのアクセスモードを変更します。 c. 必要に応じて、を選択または選択解除し"管理者グループの権限"ます。 d. 「変更を保存」を選択します。

グループを複製します

手順

1. グループのチェックボックスをオンにします。
2. [* アクション * > * グループの複製 *] を選択します。
3. グループ複製ウィザードを完了します。

グループを削除します

管理者グループを削除すると、システムからそのグループを削除し、グループに関連付けられているすべての権限を削除できます。管理者グループを削除すると、そのグループからすべてのユーザが削除されますが、ユーザは削除されません。

手順

1. [Groups]ページで、削除する各グループのチェックボックスをオンにします。
2. [* アクション * > * グループの削除 *] を選択します。
3. 「 * グループを削除する * 」を選択します。

StorageGRID の管理者グループ権限

管理者ユーザグループを作成する場合は、 Grid Manager の特定の機能へのアクセスを制御する権限を 1 つ以上選択します。その後、作成した 1 つ以上の管理者グループに各ユーザを割り当てて、ユーザが実行できるタスクを決定できます。

各グループに 1 つ以上の権限を割り当てる必要があります。そうしないと、そのグループに属するユーザは Grid Manager またはグリッド管理 API にサインインできません。

デフォルトでは、少なくとも 1 つの権限が割り当てられたグループに属するユーザは次のタスクを実行できます。

- Grid Manager にサインインします
- ダッシュボードを表示します
- ノードページを表示します

- 現在のアラートと解決済みのアラートを表示します
- 自分のパスワードを変更する（ローカルユーザのみ）
- [Configuration]ページと[Maintenance]ページに表示される特定の情報を確認します

権限とアクセスモードの相互作用

すべての権限について、グループの * アクセスモード * 設定は、ユーザーが設定を変更して操作を実行できるかどうか、または関連する設定と機能のみを表示できるかどうかを決定します。ユーザーが複数のグループに属していて、いずれかのグループが * 読み取り専用 * に設定されている場合、ユーザーは選択したすべての設定と機能に読み取り専用でアクセスできます。

以降のセクションでは、管理者グループの作成時または編集時に割り当てることができる権限について説明します。明示的に言及されていない機能には、 * Root Access * 権限が必要です。

ルートアクセス

この権限は、すべてのグリッド管理機能へのアクセスを許可します。

テナントの **root** パスワードを変更する

この権限は、テナントページの * root パスワードの変更 * オプションへのアクセスを許可し、テナントのローカル root ユーザのパスワードを変更できるユーザを制御することを可能にします。この権限は、 S3 キーのインポート機能が有効になっている場合に S3 キーの移行にも使用されます。この権限がないユーザには、 * rootパスワードの変更*オプションが表示されません。

> Change root password * オプションが含まれている tenants ページへのアクセスを許可するには、 * Tenant accounts * 権限を割り当てます。

ILM

この権限は、次の * ILM * メニュー・オプションへのアクセスを提供します。

- ルール
- ポリシー
- ポリシータグ
- ストレージプール
- ストレージグレード
- 地域
- オブジェクトメタデータの検索

> ストレージ グレードを管理するには、ユーザーに その他のグリッド構成 権限が必要です。

メンテナンス

これらのオプションを使用するには、 Maintenance 権限が必要です。

- 設定 > アクセス制御

    - Grid のパスワード
- 設定 > ネットワーク
    - S3エンドポイントのドメイン名
- メンテナンス > タスク
    - 運用停止
    - 拡張
    - オブジェクトの存在チェック
    - リカバリ
- メンテナンス > システム
    - リカバリパッケージ
    - ソフトウェアの更新
- サポート > ツール
    - ログ

Maintenance権限がないユーザは、次のページを表示できますが、編集はできません。

- メンテナンス > ネットワーク
    - DNSサーバ
    - グリッドネットワーク
    - NTPサーバ
- メンテナンス > システム
    - ライセンス
- 設定 > ネットワーク
    - S3エンドポイントのドメイン名
- 設定 > セキュリティ
    - 証明書
- 設定 > 監視
    - 監査と syslog サーバ

アラートの管理

この権限では、アラートを管理するためのオプションにアクセスできます。サイレンス、アラート通知、アラートルールを管理するには、この権限が必要です。

指標クエリ

この権限により、次の項目にアクセスできます。

- サポート > ツール > メトリクス ページ
- グリッド管理APIの*[Metrics]*セクションを使用したカスタムのPrometheus指標クエリ

- Grid Managerの指標を含むダッシュボードカード

オブジェクトメタデータの検索

この権限は、 * ILM * > * Object metadata lookup * ページへのアクセスを提供します。

その他のグリッド設定

この権限により、次の追加のグリッド構成オプションにアクセスできます。

- **ILM**
  - ストレージグレード
- 設定 > システム
- サポート > その他
  - I/Oの優先順位付け
  - ノードサービス
  - ストレージウォーターマーク

リンクコストにはルートアクセスが必要です。

ストレージアプライアンス管理者

この権限により、次のことが可能

- Grid Managerを使用して、ストレージアプライアンス上のEシリーズSANtricity System Managerにアクセスする。
- これらの処理をサポートするアプライアンスの[Manage Drives]タブで、トラブルシューティングとメンテナンスのタスクを実行する機能。

テナントアカウント

この権限により、次のことが可能になります。

- [Tenants]ページにアクセスします。このページで、テナントアカウントを作成、編集、削除できます
- 既存のトラフィック分類ポリシーを表示します
- テナントの詳細を含むGrid Managerのダッシュボードカードを表示します

StorageGRID でユーザーを管理する

ローカルユーザとフェデレーテッドユーザを表示できます。また、ローカルユーザを作成してローカル管理者グループに割り当て、そのユーザがアクセスできる Grid Manager 機能を決定することもできます。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- そうだな "特定のアクセス権限"

ローカルユーザを作成します

1 人以上のローカルユーザを作成し、各ユーザを 1 つ以上のローカルグループに割り当てることができます。このグループの権限は、ユーザがアクセスできる Grid Manager および Grid 管理 API 機能を制御します。

作成できるのはローカルユーザのみです。外部のアイデンティティソースを使用して、フェデレーテッドユーザとフェデレーテッドグループを管理します。

Grid Managerには、「root」という名前の事前定義されたローカルユーザが含まれています。rootユーザは削除できません。

シングルサインオン（SSO）が有効になっている場合、ローカルユーザはStorageGRID にサインインできません。

ウィザードにアクセスします

手順

1. 構成 > アクセス制御 > *管理者ユーザー*を選択します。
2. 「 * ユーザーの作成 * 」を選択します。

ユーザクレデンシャルを入力します

手順

1. ユーザのフルネーム、一意なユーザ名、およびパスワードを入力します。
2. 必要に応じて、このユーザに Grid Manager または Grid 管理 API へのアクセスを禁止する場合は「 * Yes 」を選択します。
3. 「 * Continue * 」を選択します。

グループに割り当てます

手順

1. 必要に応じて、ユーザを 1 つ以上のグループに割り当てて、そのユーザの権限を決定します。

   まだグループを作成していない場合は、グループを選択せずにユーザを保存できます。このユーザーは、[グループ] ページでグループに追加できます。

   ユーザが複数のグループに属している場合は、権限の累積数が算出されます。詳細は、を参照してください "管理者グループを管理する" 。

2. [Create user*] を選択し、 [**Finish**] を選択します。

ローカルユーザを表示および編集します

既存のローカルユーザとフェデレーテッドユーザの詳細を表示できます。ローカルユーザを変更して、ユーザのフルネーム、パスワード、またはグループメンバーシップを変更できます。また、ユーザが Grid Manager およびグリッド管理 API にアクセスすることを一時的に禁止することもできます。

編集できるのはローカルユーザのみです。外部のアイデンティティソースを使用してフェデレーテッドユーザを管理します。

- すべてのローカルユーザとフェデレーテッドユーザの基本情報を表示するには、ユーザページのテーブルを確認してください。
- 特定のユーザの詳細をすべて表示したり、ローカルユーザを編集したり、ローカルユーザのパスワードを変更したりするには、 * Actions * メニューまたは詳細ページを使用します。

  編集内容は、次回ユーザがグリッドマネージャからサインアウトして再度サインインしたときに適用されます。

ローカルユーザは、Grid Managerのバナーの*[パスワードの変更]*オプションを使用して自分のパスワードを変更できます。

タスク	**[Actions]**メニュー	詳細ページ
ユーザの詳細を表示します	a. ユーザのチェックボックスを選択します。 b. [* アクション * > * ユーザーの詳細を表示 *] を選択します。	テーブルでユーザの名前を選択します。
フルネームの編集（ローカルユーザのみ）	a. ユーザのチェックボックスを選択します。 b. * アクション * > * フルネームの編集 * を選択します。 c. 新しい名前を入力します。 d. 「変更を保存」を選択します。	a. 詳細を表示するユーザの名前を選択します。 b. 編集アイコン を選択します。 c. 新しい名前を入力します。 d. 「変更を保存」を選択します。
StorageGRID アクセスを拒否または許可します	a. ユーザのチェックボックスを選択します。 b. [* アクション * > * ユーザーの詳細を表示 *] を選択します。 c. [アクセス] タブを選択します。 d. ユーザが Grid Manager または Grid 管理 API にサインインできないようにするには「 * Yes 」を選択します。サインインできるようにするには、「 * No * 」を選択します。 e. 「変更を保存」を選択します。	a. 詳細を表示するユーザの名前を選択します。 b. [アクセス] タブを選択します。 c. ユーザが Grid Manager または Grid 管理 API にサインインできないようにするには「 * Yes 」を選択します。サインインできるようにするには、「 * No * 」を選択します。 d. 「変更を保存」を選択します。

タスク	**[Actions]**メニュー	詳細ページ
パスワードを変更（ローカルユーザのみ）	a. ユーザのチェックボックスを選択します。 b. [* アクション * > * ユーザーの詳細を表示 *] を選択します。 c. [パスワード] タブを選択します。 d. 新しいパスワードを入力します。 e. 「 * パスワードの変更 * 」を選択します。	a. 詳細を表示するユーザの名前を選択します。 b. [パスワード] タブを選択します。 c. 新しいパスワードを入力します。 d. 「 * パスワードの変更 * 」を選択します。
変更グループ（ローカルユーザのみ）	a. ユーザのチェックボックスを選択します。 b. [* アクション * > * ユーザーの詳細を表示 *] を選択します。 c. [グループ] タブを選択します。 d. 必要に応じて、グループ名のあとのリンクを選択し、新しいブラウザタブでグループの詳細を表示します。 e. 「 * グループを編集」を選択して、別のグループを選択します。 f. 「変更を保存」を選択します。	a. 詳細を表示するユーザの名前を選択します。 b. [グループ] タブを選択します。 c. 必要に応じて、グループ名のあとのリンクを選択し、新しいブラウザタブでグループの詳細を表示します。 d. 「 * グループを編集」を選択して、別のグループを選択します。 e. 「変更を保存」を選択します。

フェデレーションユーザーのインポート

1 人以上のフェデレーション ユーザー (最大 100 人) を [ユーザー] ページに直接インポートできます。

手順

1. 構成 > アクセス制御 > *管理者ユーザー*を選択します。
2. *フェデレーション ユーザーのインポート*を選択します。
3. 1 人以上のフェデレーション ユーザーの UUID またはユーザー名を入力します。

   複数のエントリの場合は、各 UUID またはユーザー名を新しい行に追加します。

4. *インポート*を選択します。

   1 人以上のユーザーの「ユーザー」フィールドへのインポートが失敗した場合は、次の手順を実行します。

   a. *インポートされていないユーザー*を展開し、*ユーザーのコピー*を選択します。
   b. 前へ*を選択し、コピーしたユーザーを*フェデレーション ユーザーのインポート ダイアログ ボックスに貼り付けて、インポートを再試行します。

[フェデレーション ユーザーのインポート**]** ダイアログ ボックスを閉じると、正常にインポートされたユーザーの [ユーザー] ページにフェデレーション ユーザー情報が表示されます。

ユーザを複製します

既存のユーザを複製して、同じ権限を持つ新しいユーザを作成することができます。

手順

1. ユーザのチェックボックスを選択します。
2. * アクション * > * ユーザーの複製 * を選択します。
3. 複製ユーザーウィザードを完了します。

ユーザを削除します

ローカルユーザを削除して、そのユーザをシステムから完全に削除できます。

rootユーザは削除できません。

手順

1. [Users]ページで、削除する各ユーザのチェックボックスをオンにします。
2. * アクション * > * ユーザーの削除 * を選択します。
3. 「 * ユーザーの削除 * 」を選択します。

シングルサインオン（ **SSO** ）を使用

StorageGRID SSO について学ぶ

シングル サインオン (SSO) が有効になっている場合、ユーザーは、組織によって実装された SSO サインイン プロセスを使用して資格情報が承認されている場合にのみ、Grid Manager、Tenant Manager、Grid Management API、または Tenant Management API にアクセスできます。ローカル ユーザーはStorageGRIDにサインインできません。

StorageGRID システムは、Security Assertion Markup Language 2.0（SAML 2.0）標準または OpenID Connect を使用したシングル サインオン（SSO）をサポートしています。

シングルサインオン（ SSO ）を有効にする前に、 SSO が有効になった場合に StorageGRID のサインインとサインアウトのプロセスにどのような影響があるかを確認してください。

SSO が有効な場合はサインインします

SSO が有効な場合に StorageGRID にサインインすると、組織の SSO ページにリダイレクトされてクレデンシャルが検証されます。

手順

1. Web ブラウザで、 StorageGRID 管理ノードの完全修飾ドメイン名または IP アドレスを入力します。

   StorageGRID のサインインページが表示されます。

   - このブラウザで初めて URL にアクセスする場合は、アカウント ID の入力を求められます。
   - 以前に Grid Manager または Tenant Manager にアクセスしたことがある場合は、最近のアカウントを選択するか、アカウント ID を入力するように求められます。

テナントアカウントの完全なURL（完全修飾ドメイン名またはIPアドレスのあとにを追加したもの）を入力すると、StorageGRIDのサインインページは表示されません `/?accountId=20-digit-account-id`。代わりに、組織のSSOサインインページにすぐにリダイレクトされ、そこでできますSSO クレデンシャルを使用してサインインします。

2. Grid Manager と Tenant Manager のどちらにアクセスするかを指定します。
   - Grid Manager にアクセスするには、 * Account ID * フィールドを空白のままにします。アカウント ID に「 * 0 」と入力するか、最近のアカウントのリストに * Grid Manager * が表示されている場合はそれを選択します。
   - Tenant Manager にアクセスするには、 20 桁のテナントアカウント ID を入力するか、最近のアカウントのリストにテナントが表示されている場合は名前でテナントを選択します。
3. 「サインイン」を選択します

   StorageGRID は、組織の SSO サインインページにリダイレクトします。例：

4. [[signin_soS] SSO クレデンシャルを使用してサインインします。

   SSO クレデンシャルが正しい場合：

   a. アイデンティティプロバイダ（ IdP ）が StorageGRID に認証応答を返します。
   b. StorageGRID が認証応答を検証します。
   c. 応答が有効で、 StorageGRID アクセス権限のあるフェデレーテッドグループに属している場合は、選択したアカウントに応じて、 Grid Manager またはテナントマネージャにサインインされます。

   サービスアカウントにアクセスできない場合でも、 StorageGRID アクセス権限を持つフェデレーテッドグループに属する既存のユーザであれば、サインインできます。

5. 必要に応じて、他の管理ノードにアクセスします。または、適切な権限がある場合は Grid Manager またはテナントマネージャにアクセスします。

   SSOクレデンシャルを再入力する必要はありません。

SSO が有効な場合はサインアウトします

StorageGRID で SSO が有効になっている場合にサインアウトするとどうなるかは、サインイン先とサインアウト元によって異なります。

手順

1. ユーザインターフェイスの右上隅にある[サインアウト]リンクを探します。
2. [サインアウト]*を選択します。

   StorageGRID のサインインページが表示されます。[Recent Accounts] * ドロップダウンが更新されて、 * Grid Manager * またはテナント名が表示されるようになり、これらのユーザインターフェイスにあとからすばやくアクセスできるようになります。

次の表は、単一のブラウザセッションを使用している場合にサインアウトしたときの動作をまとめたものです。複数のブラウザセッションで StorageGRID にサインインしている場合は、すべてのブラウザセッションから個別にサインアウトする必要があります。

サインイン先	サインアウト元	サインアウトされる対象
1 つ以上の管理ノードでグリッドマネージャを使用します	任意の管理ノード上の Grid Manager	すべての管理ノード上の Grid Manager 注意: SSO に Entra ID を使用する場合、すべての管理ノードからサインアウトするまでに数分かかることがあります。
1 つ以上の管理ノード上の Tenant Manager	任意の管理ノード上の Tenant Manager	すべての管理ノード上の Tenant Manager
Grid Manager と Tenant Manager の両方	Grid Manager	Grid Manager のみ。SSO からサインアウトするには、 Tenant Manager からもサインアウトする必要があります。

StorageGRID SSO の要件と考慮事項

StorageGRID システムでシングルサインオン（SSO）を有効にする前に、要件と考慮事項を確認してください。

アイデンティティプロバイダの要件

StorageGRID は複数の SSO ID プロバイダー（IdP）をサポートしています。

OIDC

以下の SSO IdPs は OpenID Connect （OIDC） でサポートされています：

- Active Directory フェデレーションサービス（ AD FS ）
- Microsoft Entra ID
- Keycloak
- PingFederate
- Okta

SAML

以下の SSO IdPs は、Security Assertion Markup Language 2.0 （SAML 2.0） でサポートされています：

- Active Directory フェデレーションサービス（ AD FS ）
- Microsoft Entra ID
- PingFederate

SSO アイデンティティプロバイダを設定する前に、 StorageGRID システムのアイデンティティフェデレーションを設定する必要があります。アイデンティティフェデレーションに使用する LDAP サービスのタイプによって、実装できる SSO のタイプが制御されます。

LDAP サービスタイプが設定されました	**SSO** アイデンティティプロバイダのオプション
Active Directory	• Active Directory • Keycloak • Okta • エントラID • PingFederate
エントラID	エントラID

AD FS の要件

次のいずれかのバージョンの AD FS を使用できます。

- Windows Server 2022 AD FS
- Windows Server 2019 AD FS
- Windows Server 2016 AD FS

Windows Server 2016では、以上を使用している必要があります "KB3201845 の更新プログラム"。

その他の要件

- Transport Layer Security （ TLS ） 1.2 または 1.3
- Microsoft .NET Framework バージョン 3.5.1 以降

Entra IDに関する考慮事項

SSO タイプとして Entra ID を使用し、ユーザーのユーザー プリンシパル名にプレフィックスとして sAMAccountName が使用されていない場合、 StorageGRID がLDAP サーバーとの接続を失うとログインの問題が発生する可能性があります。ユーザーがサインインできるようにするには、LDAP サーバーへの接続を復元する必要があります。

サーバ証明書の要件

デフォルトでは、 StorageGRID は各管理ノードで管理インターフェイス証明書を使用して、グリッド マネージャ、テナント マネージャ、グリッド管理 API、およびテナント管理 API へのアクセスを保護します。StorageGRIDに対して証明書利用者信頼 (AD FS)、エンタープライズ アプリケーション (Entra ID)、またはサービス プロバイダー接続 (PingFederate) を構成する場合は、サーバー証明書をStorageGRID要求の署名証明書として使用します。

まだ"管理インターフェイス用のカスタム証明書を設定しました"実行していない場合は、今実行する必要があります。インストールしたカスタムサーバ証明書はすべての管理ノードで使用され、すべての StorageGRID 証明書利用者信頼、エンタープライズアプリケーション、または SP 接続で使用できます。

> 管理ノードのデフォルトサーバ証明書を証明書利用者信頼、エンタープライズアプリケーション、または SP 接続で使用することは推奨されません。ノードに障害が発生した場合にそのノードをリカバリすると、新しいデフォルトサーバ証明書が生成されます。リカバリしたノードにサインインするには、証明書利用者信頼、エンタープライズアプリケーション、または SP 接続を新しい証明書で更新する必要があります。

管理ノードのサーバ証明書にアクセスするには、ノードのコマンドシェルにログインしてディレクトリに移動 `/var/local/mgmt-api`します。カスタムサーバ証明書の名前はです `custom-server.crt`。ノードのデフォルトのサーバ証明書の名前はです `server.crt`。

ポートの要件

シングルサインオン（ SSO ）は、制限された Grid Manager ポートまたは Tenant Manager ポートでは使用できません。ユーザをシングルサインオンで認証する場合は、デフォルトの HTTPS ポート（ 443 ）を使用する必要があります。を参照して "外部ファイアウォールでアクセスを制御します"

フェデレーションユーザーが**StorageGRID**にサインインできることを確認してください

シングルサインオン（ SSO ）を有効にする前に、少なくとも 1 人のフェデレーテッドユーザが既存のテナントアカウント用に Grid Manager および Tenant Manager にサインインできることを確認する必要があります。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- そうだな "特定のアクセス権限"

- アイデンティティフェデレーションがすでに設定されている。

手順

1. 既存のテナントアカウントがある場合は、テナントが独自のアイデンティティソースを使用していないことを確認します。

   SSO を有効にすると、 Tenant Manager で設定されたアイデンティティソースが Grid Manager で設定されたアイデンティティソースによって上書きされます。テナントのアイデンティティソースに属するユーザは、 Grid Manager アイデンティティソースのアカウントがないかぎり、サインインできなくなります。

   a. 各テナントアカウントの Tenant Manager にサインインします。
   b. アクセス管理 > *アイデンティティ連携*を選択します。
   c. [アイデンティティフェデレーションを有効にする]*チェックボックスが選択されていないことを確認します。
   d. 該当する場合は、このテナントアカウントに使用されている可能性のあるフェデレーテッドグループが不要になったことを確認し、チェックボックスをオフにして*[保存]*を選択します。

2. フェデレーテッドユーザが Grid Manager にアクセスできることを確認します。
   a. グリッド マネージャーから、構成 > アクセス制御 > 管理者グループ を選択します。
   b. Active Directory アイデンティティソースから少なくとも 1 つのフェデレーテッドグループがインポートされていて、そのグループに Root アクセス権限が割り当てられていることを確認します。
   c. サインアウトします。
   d. フェデレーテッドグループ内のユーザとして Grid Manager に再度サインインできることを確認します。

3. 既存のテナントアカウントがある場合は、次の手順を実行して、 Root アクセス権限を持つフェデレーテッドユーザがサインインできることを確認します。
   a. グリッド マネージャーから、[テナント] を選択します。
   b. テナントアカウントを選択し、 * Actions * > * Edit * を選択します。
   c. Enter details （詳細の入力）タブで、 * Continue （続行） * を選択します。
   d. チェックボックスがオンになっている場合は、チェックボックスをオフにして[Save]*を選択します。

      Tenant ページが表示されます。

   e. テナントアカウントを選択し、 * サインイン * を選択して、ローカルの root ユーザとしてテナントアカウントにサインインします。
   f. テナント マネージャーから、アクセス管理 > グループ を選択します。
   g. Grid Manager から少なくとも 1 つのフェデレーテッドグループにこのテナントに対する Root アクセス権限が割り当てられていることを確認します。
   h. サインアウトします。
   i. フェデレーテッドグループ内のユーザとしてテナントに再度サインインできることを確認します。

関連情報

- "シングルサインオンの要件と考慮事項"

- "管理者グループを管理する"
- "テナントアカウントを使用する"

OIDCを使用してSSOを設定する

StorageGRID で OIDC を使用したシングル サインオンの設定について

StorageGRID でシングル サインオン（SSO）を設定すると、StorageGRID（サービス プロバイダー）と SSO ID プロバイダーがユーザ認証リクエストについて安全に通信できるようになります。

StorageGRID では、OpenID Connect（OIDC）または SAML を使用してシングル サインオンを設定できます。OIDC を使用して StorageGRID でシングル サインオンを設定するには、以下の概要手順に従うか、"SAMLを使用したSSOの設定"について確認してください。



IDプロバイダーの設定

使用するSSO IDプロバイダーに応じて、IDフェデレーションLDAPサービスタイプとしてActive DirectoryまたはEntra IDのいずれかを選択できます。

- Active Directory Federation Service (AD FS) の場合、AD FS、Entra ID、Keycloak、Okta、または PingFederate アイデンティティ プロバイダーを使用できます。
- Entra IDでは、Entra IDのIDプロバイダーのみを使用できます。

SSO IDプロバイダーのソフトウェアを使用して、グリッド内の各管理ノードのOIDCを設定します。

- Active Directory の "各管理ノードごとにアプリケーショングループを作成する" について学ぶ
- Entra ID の"各管理ノード用のアプリケーションを作成する"について学ぶ
- Keycloakの"各管理ノードのクライアントを作成する"について学ぶ
- "各管理ノードごとにOktaアプリケーションを作成する"について学ぶ
- PingFederate の "各管理ノードに対してサービスプロバイダー接続を作成する" について学ぶ



SSOの設定

OIDC 用の SSO 設定ウィザードを選択します。次に、ID プロバイダーで SSO を設定し、サンドボックス モードに入って StorageGRID ユーザーに対して有効化する前に SSO の設定とテストを行います。

"OIDCを使用したSSOの設定"について学ぶ



SSOを有効にする

各管理ノードへのサインインに SSO を使用できることを確認したら、すべての StorageGRID ユーザーに対して SSO を有効にしてください。

"StorageGRID ユーザーのシングル サインオンの有効化"について学ぶ

StorageGRID の **AD FS** に **OIDC** 用のアプリケーショングループを作成する

システム内のOpenID Connect（OIDC）用管理ノードごとにアプリケーショングループを作成するには、Active Directory Federation Services（AD FS）を使用する必要があります。

開始する前に

- システム内の各管理ノードについて、完全修飾ドメイン名（またはIPアドレス）と証明書利用者識別子が必要です。

> StorageGRID システムの各管理ノードには、アプリケーショングループが必要です。これにより、ユーザーはどの管理ノードにも安全にサインインおよびサインアウトできます。すべての管理ノードに対して単一のアプリケーショングループを作成するか（推奨）、管理ノードごとに異なるアプリケーショングループを作成することができます。

- AD FSでアプリケーショングループを作成した経験があるか、Microsoft AD FSのドキュメントにアクセスできる環境にあること。
- AD FS 管理スナップインを使用していて、 Administrators グループに属している必要があります。

タスクの内容

これらの手順は、Windows Server 2022 AD FS に適用されます。AD FS の異なるバージョンを使用している場合は、手順に若干の違いがあります。ご不明な点がある場合は、Microsoft AD FS のドキュメントを参照してください。

ステップ**1**：アプリケーショングループを作成する

Windows PowerShell を使用して、アプリケーショングループを迅速に作成できます。

手順

1. Windows Server Manager で、 * Tools * > * AD FS Management * を選択します。
2. 「Application Groups」>「Add Application Group」を選択します。
3. *名前*には、依拠当事者識別子を入力してください。
4. テンプレートで、「クライアント/サーバーアプリケーション」>「Web APIにアクセスするサーバーアプリケーション」を選択します。
5. 「 * 次へ * 」を選択します。
6. クライアント識別子の値を記録してください。
7. リダイレクト**URI** に、管理ノードの FQDN （または IP アドレス） `callback`および `logged-out` URI を入力します：
   - `https://<FQDN>/api/v4/oidc-callback` または `https://<IP_address>/api/v4/oidc-callback`
   - `https://<FQDN>/api/v4/oidc-logged-out` または `https://<IP_address>/api/v4/oidc-logged-out`

   すべての管理ノードに同じアプリケーショングループを使用している場合は、各管理ノードのURIを入力してください。各管理ノードに異なるアプリケーショングループを使用している場合は、対応する管理ノードのURIのみを入力してください。

8. 「 * 追加」を選択します。
9. 「共有シークレットを生成」を選択し、「シークレット」の値を記録してから、「次へ」を選択します。
10. **Identifier** のクライアント識別子を入力してください。
11. 「追加」を選択し、次に「次へ」を選択します。
12. 「全員を許可する」を選択します。
13. クライアントアプリケーション（呼び出し元） でサーバーアプリケーションが選択されていることを確認してください。
14. 許可されたスコープ で、以下のオプションのみが選択されていることを確認してください：
    - allatclaims
    - email
    - openid
    - プロフィール
15. 「次へ」>「次へ」を選択します。
16. *閉じる*を選択します。

ステップ**2**：発行変換ルールを設定する

アプリケーショングループごとに発行変換ルールを設定します。

手順

1. 「AD FS Management」ページで、アプリケーショングループを右クリックし、「Properties」を選択します。
2. 以前に作成した Web API を選択し、編集 を選択します。
3. 「発行変換ルール」>「ルールの追加…」を選択します。
4. 「クレームルールテンプレート：」で、「Send LDAP Attribute as Claims」を選択します。
5. 「 * 次へ * 」を選択します。
6. クレームルール名を入力してください。
7. 属性ストアとして **Active Directory** を選択します。
8. 送信クレームタイプにLDAP属性マッピングを追加します：
    - `E-Mail Addresses - E-Mail Address`
    - `Token-Groups - Unqualified Names - Group`
9. [完了] を選択します。
10. **Apply** > **OK** > **OK** を選択します。

次の手順

アプリケーショングループを作成した後、"OIDCを使用してSSOを構成する"。

StorageGRID の **OIDC** 向け **Entra ID** でエンタープライズアプリケーションを作成する

Entra IDを使用して、システム内のOpenID Connect（OIDC）用管理ノードごとにエンタープライズアプリケーションを作成します。

開始する前に

- システム内の各管理ノードについて、証明書利用者識別子と完全修飾ドメイン名（FQDN）またはIPアドレスを確認しておく必要があります。

> StorageGRID システムの各管理ノードには、エンタープライズアプリケーションが必要です。これにより、ユーザーはどの管理ノードにも安全にサインインおよびサインアウトできるようになります。すべての管理ノードに対して単一のエンタープライズアプリケーションを作成すること（推奨）も、管理ノードごとに異なるエンタープライズアプリケーションを作成することもできます。

- Entra ID でアプリケーションを作成した経験があります。
- 有効なサブスクリプションを持つ Entra ID アカウントをお持ちです。
- Entra ID アカウントには、グローバル管理者、クラウド アプリケーション管理者、アプリケーション管理者、またはサービス プリンシパルの所有者のいずれかのロールがあります。

ステップ**1**：**Entra ID** にアクセスする

手順

1. にログインし "Azure ポータル"ます。
2. "Microsoft Entra ID"を選択します。
3. "アプリ登録"を選択します。

ステップ**2**：新しいアプリケーションを登録する

システム内の各管理ノードに対して、新しいエンタープライズアプリケーションを登録してください。

手順

1. Entra ID Enterprise アプリケーション ペインで、「アプリケーション登録」 > 「新規登録」を選択します。
2. *名前*には、依拠当事者識別子を入力してください。
3. サポートされているアカウントの種類 の下で、アプリケーションを使用したり API にアクセスしたりできるアカウントの種類を選択します。たとえば、シングルテナントのみ **- <tenant_name>**。
4. 「リダイレクトURI」で、「プラットフォームを選択」>「Web」を選択します。
5. 管理ノードのFQDN（またはIPアドレス）リダイレクトURIを入力してください： `https://<FQDN>/api/v4/oidc-callback`または `https://<IP_address>/api/v4/oidc-callback`

   すべての管理ノードに同じエンタープライズアプリケーションを使用している場合は、各管理ノードのURIを入力してください。各管理ノードごとに異なるエンタープライズアプリケーションを使用している場合は、対応する管理ノードのURIのみを入力してください。

6. 「登録」を選択します。

7. 新規アプリケーション登録の概要ページで、アプリケーション（クライアント）**ID** と ディレクトリ（テナント）**ID** を記録してください。

ステップ**3**：クライアントシークレットを設定する

新しいアプリケーションごとにクライアントシークレットを登録してください。

手順

1. 新しいアプリケーション登録の概要ページで、管理 > 証明書とシークレット > 新しいクライアントシークレット を選択します。
2. クライアントシークレットを入力し、希望する有効期限を設定してください。
3. クライアントシークレットを作成するには、*追加*を選択します。
4. 秘密の*値*をコピーします。

> クライアントシークレットページを更新したり、別のページに移動したりすると、シークレットの値は表示されなくなります。

ステップ**4**：**API**権限を設定する

各新規アプリケーションのAPI権限を設定します。

手順

1. 新しいアプリケーション登録の概要ページで、管理 > **API**権限 > 権限の追加 を選択します。
2. 「Microsoft APIs」>「Microsoft Graph」>「Delegated permissions」を選択します。
3. **OpenId permissions** を展開し、**email**、**offline_access**、**openid**、**profile** を選択します。
4. 「権限を追加」を選択します。
5. *<tenant> に管理者の同意を付与する*を選択し、*はい*を選択します。

ステップ**5**：ログアウト後のリダイレクト**URI**を追加する

新規アプリケーションごとに、ログアウト後のリダイレクトURIを追加してください。

手順

1. 新規アプリケーション登録の概要ページで、**Manage** > **Authentication** を選択します。
2. 「リダイレクトURIの追加」 > 「Web」を選択します。
3. 管理ノードの FQDN（または IP アドレス）リダイレクト URI を入力してください： `https://<FQDN>/api/v4/oidc-logged-out`または `https://<IP_address>/api/v4/oidc-logged-out`

   すべての管理ノードに同じアプリケーショングループを使用している場合は、各管理ノードのURIを入力してください。各管理ノードに異なるアプリケーショングループを使用している場合は、対応する管理ノードのURIのみを入力してください。

4. 「設定」を選択します。

次の手順

エンタープライズアプリケーションを作成した後、"OIDCを使用してSSOを構成する"。

StorageGRID の **OIDC** 用クライアントを **Keycloak** で作成する

Keycloakを使用して、StorageGRIDシステムのOpenID Connect （OIDC）用の各管理ノードのクライアント接続を作成します。

開始する前に

- Keycloakでクライアントを作成した経験がある、またはKeycloakのドキュメントにアクセスできる環境にあること。
- ディレクトリ検索とログイン認証情報専用のアカウント（Bind DN）が用意されています。
- Keycloak の管理者アクセス権を持っています。

タスクの内容

StorageGRID システムの各管理ノードには、クライアント接続が必要です。これにより、ユーザーはどの管理ノードにも安全にサインインおよびサインアウトできるようになります。すべての管理ノードに対して単一のクライアント接続を作成することも（推奨）、管理ノードごとに異なるクライアント接続を作成することもできます。

特に指定がない限り、デフォルト設定を使用してください。場合によっては、組織が要求する設定を使用できます。

ステップ**1**：必要に応じてレルムを作成する

LDAPプロバイダーとOIDCクライアントを設定するには、Keycloakレルムを作成するか、Keycloakのデフォルトレルムを使用します。

手順

1. 「レルムの作成」を選択します。
2. 領域の名前を入力してください。
3. 「有効」を選択します。
4. 「 * Create * 」を選択します。

ステップ**2**：**LDAP**プロバイダーの設定

KeycloakがActive Directory フェデレーションサービス（AD FS）LDAPサーバに接続できるように、LDAPプロバイダーを設定します。

手順

1. 「User federation」＞「Add Ldap providers」を選択します。
2. 設定タブで：
   a. 以下の推奨値を入力してください：
      - UI表示名：一意の値を入力してください。
      - ベンダー：**Active Directory**
      - 接続URL： `ldap://<ldap_IP_address>`または `ldaps://<ldap_IP_address>`

- 接続プーリング：**ON**
- バインドDN：バインドDNを入力してください
- バインド認証情報：パスワードを入力してください
- 編集モード：**READ_ONLY**
- ユーザーDN：例： `CN=Users、 DC=saml、 DC=sgws`
- ユーザー名のLDAP属性：**sAMAccountName**
- RDN LDAP属性：**cn**
- UUID LDAP属性：**objectGUID**
- ユーザーオブジェクトクラス： `person、 organizationalPerson、 user`
- ユーザーLDAPフィルタ： `(sAMAccountName=*)`
- 検索範囲：サブツリー
- ページネーション: **ON**
- ユーザーのインポート: **ON**
- 同期登録：**ON**
- 検索時に無効なユーザーを削除する：**ON**

b. 「接続テスト」と「認証テスト」を選択してください。

続行する前に、発生する可能性のある問題をすべて解決してください。

3. [保存（ Save ）] を選択します。

ステップ**3**：**LDAP**マッピングの設定

LDAPマッピングを設定して、ADを属性としてKeycloakにマッピングします。

手順

1. 「ユーザーフェデレーション」>「LDAP」に移動します。
2. 作成したLDAPプロバイダーを選択します。
3. 「マッパー」タブで、「マッパーの追加」>「新しいマッパーの作成」を選択します。
4. マッパータイプには、**user-attribute-ldap-mapper** を選択してください。
5. 「保存」を選択し、以下の情報を入力してください：
   - ユーザーモデル属性: **userPrincipalName**
   - LDAP属性：**userPrincipalName**
   - 読み取り専用: **ON**
   - LDAPから常に値を読み取る：**ON**
   - LDAPでは必須：**OFF**
   - デフォルト値を強制的に設定する：**ON**
   - バイナリ属性：**OFF**

6. [保存（ Save ）] を選択します。

ステップ**4**：**OIDC**クライアントを作成する

お使いのシステム用のOIDCクライアントを作成してください。

手順

1. 「クライアント」＞「クライアントの作成」に移動します。
2. 一般設定については、以下の情報を入力してください。
   - 名前：クライアントの表示名を入力してください。
   - クライアントタイプ：**OIDC Connect**
   - クライアントID：一意の値を入力してください。この値を後で使用するために保存してください。
3. 「 * 次へ * 」を選択します。
4. 機能設定については、以下の情報を入力してください。
   - クライアント認証： **ON**
   - 標準フロー：有効化
   - 直接アクセス権限：有効
   - サービスアカウントの役割：有効にする
5. 「 * 次へ * 」を選択します。
6. ログイン設定には、リダイレクト URI を入力します：

> 管理インターフェイスに1つ以上のロードバランサーエンドポイントが設定されている場合は、各ポートのリダイレクトURIを追加します。例： `https://<Admin_IP_address_or_FQDN>:<port>/api/v4/oidc-callback`および `\https://<Admin_IP_address_or_FQDN>:<port>/api/v4/oidc-logged-out`

   - 有効なリダイレクトURI： `https://<Admin_IP_address_or_FQDN>/api/v4/oidc-callback`および `\https://<Admin_IP_address_or_FQDN>/api/v4/oidc-logged-out`
   - 有効なログアウト後のリダイレクトURI： `https://<Admin_IP_address_or_FQDN>/api/v4/oidc-logged-out`
   - Webオリジン： `https://<Admin_IP_address_or_FQDN>`
7. [保存（ Save ）] を選択します。

ステップ**5**：クライアントシークレットを生成する

作成したOIDCクライアント用のクライアントシークレットを生成します。

手順

1. 「クライアント」に移動し、作成したOIDCクライアントを選択します。
2. 「認証情報」タブで、以下の情報を入力してください：
   - クライアント認証：**Client Id and Secret**

- クライアントシークレット：クライアントシークレットを生成または設定します。この値を後で使用するために保存してください。

ステップ**6**：スコープを定義する

Keycloakでスコープを定義します。

手順

1. **Client scopes** > **Create client scope** に移動し、以下の情報を入力してください：
   - タイプ：**None**
   - プロトコル：**OpenID Connect**
   - 同意画面に表示：有効
   - OpenIDプロバイダーメタデータに含める：有効
2. [保存（ Save ）] を選択します。
3. 「マッパー」タブで、「新しいマッパーの設定」>「ユーザー属性」を選択し、以下の情報を入力します：
   - 名前：一意の値を入力してください。
   - ユーザー属性：**userPrincipalName**
   - トークンクレーム名：**upn**
   - クレームJSONタイプ：**String**
   - IDトークンに追加：**ON**
   - アクセストークンに追加：**ON**
   - ユーザー情報に追加: **ON**
   - トークンイントロスペクションに追加: **ON**
4. [保存（ Save ）] を選択します。
5. 「クライアント」に移動し、作成したOIDCクライアントを選択します。
6. **Client Scopes** > **Add client scope** を選択します。
7. 作成したクライアントスコープを選択します。
8. 「 * 追加」を選択します。

ステップ**7**：**OIDC**を使用して**SSO**を設定する準備をする

Keycloakを使用してOIDCでSSOを構成するために必要な情報をStorageGRIDシステムに保存します。

手順

1. 作成した OIDC クライアントからクライアントIDとクライアントシークレットを保存したことを確認してください。
2. レルムのOpenID Connect検出エンドポイントを保存します。これは `well-known`設定エンドポイントで確認できます：

```
https://<keycloak_host_ip/keycloak_host_name>/realms/<realm_name>/.well-
```

known/openid-configuration

必要に応じてネットワークポートを含めます。

```
https://<keycloak_host_ip/keycloak_host_name>:<https_port>/realms/<realm_name>
/.well-known/openid-configuration
```

次の手順

OIDCクライアントを作成した後、"OIDCを使用してSSOを構成する"。

StorageGRID で**OIDC**用の**Okta**アプリケーションを作成する

StorageGRID システムのすべての管理ノードに対して、OpenID Connect （OIDC） 用の Okta アプリケーションを作成します。

開始する前に

- Oktaアプリケーションの作成経験がある、またはOktaのドキュメントにアクセスできる環境にあること。
- Okta の管理者アクセス権を持っている必要があります。

タスクの内容

Oktaアプリケーションには、すべての管理ノードのサインインおよびサインアウトのリダイレクトURIが含まれている必要があります。リダイレクトURIを使用することで、ユーザーはどの管理ノードにも安全にサインインおよびサインアウトできます。すべての管理ノードに対して単一のOktaアプリケーションを作成することも（推奨）、管理ノードごとに異なるアプリケーションを作成することもできます。

特に指定がない限り、デフォルト設定を使用してください。場合によっては、組織が要求する設定を使用できます。

ステップ**1**：**Okta**アプリケーションを作成する

Okta UIを使用してOktaアプリケーションを作成します。

手順

1. Oktaで、アプリケーション > *アプリケーション*に移動します。
2. 「アプリ連携の作成」を選択し、以下の情報を入力してください：
   - サインイン方法：**OIDC - OpenID Connect**
   - アプリケーションの種類：**Web**アプリケーション
3. 「 * 次へ * 」を選択します。
4. 「アプリ統合」フィールドにアプリケーションの名前を入力してください。
5. コアグラントに対して、Authorization Code が選択されている（デフォルト）ことを確認してください。
6. 各管理ノードのサインインおよびサインアウトのリダイレクトURIを追加します。
   - サインインリダイレクトURI： `https://<Admin_IP_address_or_FQDN>/api/v4/oidc-callback`
   - サインアウトリダイレクトURI： `https://<Admin_IP_address_or_FQDN>/api/v4/oidc-logged-out`

管理インターフェイスに1つ以上のロードバランサーエンドポイントが設定されている場合は、各ポートのリダイレクトURIを追加します。例：`https://<Admin_IP_address_or_FQDN>:<port>/api/v4/oidc-callback`および `\https://<Admin_IP_address_or_FQDN>:<port>/api/v4/oidc-logged-out`

7. *保存*を選択します。クライアント ID とクライアントシークレットの値を後で使用するために保存します。

ステップ**2**：フェデレートグループを追加する

Active Directory Federation Service (AD FS) サーバーのグループを作成するか、既存のグループを StorageGRID に使用します。

手順

1. GRID Managerで、「構成」>「管理者グループ」>「グループの作成」>「グループの連携」を選択します。
2. AD FSサーバーグループ名を入力してください。
3. アクセスモードには「読み書き」を、権限には「ルートアクセス」を選択します。
4. 「 * グループを作成 * 」を選択します。

ステップ**3**：**AD FS**サーバーグループとユーザーをインポートする

AD FSサーバーにOkta Active Directoryクライアントをインストールします。次に、AD FSサーバーのグループとユーザーをインポートします。

手順

1. Okta で、「Directory」>「Directory Integrations」>「Add Directory」>「Add Active Directory」に移動します。
2. 「Active Directory の設定」>「エージェントのダウンロード」を選択してください。
3. セットアップ手順をすぐに実行してください。

   遅延すると、セットアップが停止し、最初からやり直す必要が生じる可能性があります。

   a. Active Directoryドメインを選択します。
   b. 既存のユーザーをリンクするのではなく、OktaService アカウントを作成します。
   c. ユーザーを含む組織単位と、グループを含む組織単位を選択してください。
   d. OktaのユーザーとしてAD UPNを使用するユーザープリンシパル名（UPN）を選択してください。例：user@domain.com

4. **Okta AD Agent Management Utility** アプリケーションを検索してください。次に、アプリケーションを実行し、ステータスメッセージ `The agent is running`が表示されることを確認してください。

   Okta ADクライアントは、AD FSサーバーの同期とOktaへのインポートを実行する際には常に実行されている必要があります。

5. Oktaで、「ディレクトリ」>「ディレクトリ統合」に移動します。
6. 作成したディレクトリ統合を選択します。
7. 「インポート」>「今すぐインポート」を選択します。
8. インポートするユーザーを選択し、*割り当ての確認*を選択してください。
9. 「ディレクトリ」＞「People」に移動し、ユーザーが正常にインポートされたことを確認してください。

   ユーザーのステータスが「アクティブ」でない場合は、*アクティブ化*を選択し、ユーザーのステータスが「アクティブ」になるまでページを更新し続けてください。
10. ディレクトリ ＞ グループ に移動し、インポートしたユーザーのグループが自動的にインポートされていることを確認してください。
11. グループを選択し、インポートしたユーザーがそのグループに属していることを確認してください。

ステップ**4**：クレームを設定する

アクセストークンにAD FSサーバーグループを含めるためのクレームを設定します。次に、クレームにインポートされたユーザーとOktaアプリケーションのインポートされたグループが含まれていることを確認します。

手順

1. Oktaで、「ディレクトリ」>「グループ」に移動します。
2. インポートしたユーザーに対して、インポートしたグループを選択してください。
3. 「アプリケーション」>「アプリケーションの割り当て」>「割り当て」を選択します。
4. 「Security」＞「API」に移動してください。
5. *デフォルト*の認証サーバーを選択してください。
6. 「Claims」>「Add Claim」を選択してください。次に、以下の認証情報を使用してクレームを作成します。
   - 名前：グループ
   - トークンタイプに含める：**ID**トークン **-** 常に
   - 値の型: 式
   - 値: **Groups.startsWith("active_directory","",100)**
   - 対象範囲：あらゆる範囲
7. 「Security」＞「API」に移動してください。
8. *デフォルト*の認証サーバーを選択してください。
9. **Token Preview** タブを選択し、Request Properties に以下の認証情報を入力します：
   - OAuth/OIDCクライアント：**<application name>**
   - Grant type：**Authorization Code**
   - ユーザー：インポートされたユーザー （**E**メールアドレス）
   - スコープ：**email**、**profile**、**openid**
10. [* Execute] を選択します。

インポートされたグループは、ペイロードの「Preview id_token」タブに表示されます。

次の手順

Oktaアプリケーションを作成した後、"OIDCを使用してSSOを構成する"。

StorageGRID の **OIDC** 向けに **PingFederate** でサービスプロバイダー接続を作成する

PingFederate を使用して、システム内の各管理ノード用に OpenID Connect （OIDC）のサービスプロバイダー （SP） 接続を作成します。

開始する前に

- PingFederate サーバーで SP 接続を作成した経験があります。
- PingFederateサーバ用のがありhttps://docs.pingidentity.com/pingfederate/latest/administrators_reference_guide/pf_administrators_reference_guide.html["管理者向けリファレンスガイド"^]ます。PingFederate ドキュメントでは、詳細な手順と説明を説明しています。
- あなたは"管理者権限"PingFederate サーバー用。

タスクの内容

これらの手順は、StorageGRID のSSOプロバイダーとしてPingFederate サーバーバージョン12.1.10を設定する方法をまとめたものです。別のバージョンのPingFederateを使用している場合は、これらの手順を適宜調整する必要があります。ご使用のリリースに関する詳細な手順については、PingFederate サーバーのドキュメントを参照してください。

特に指定がない限り、デフォルト設定を使用してください。場合によっては、認証方法の設定など、組織で必要とされる設定を使用できます。

ステップ **1**：データストア　を作成する

まだ作成していない場合は、PingFederateをAD FSのLDAPサーバに接続するためのデータストアを作成してください。

手順

1. システム ＞ データと資格情報ストア に移動します。
2. 「新しいデータストア」を選択します。
3. 「タイプ」で「ディレクトリ（LDAP）」を選択します。
4. 「 * 次へ * 」を選択します。
5. LDAP設定の下：
   - ホスト名、ユーザー**DN**（ユーザー名）、および*パスワード*の値を入力してください。

     StorageGRID で"アイデンティティフェデレーションの設定"際に使用した値を使用してください。
   - Active Directoryの場合は、*LDAPタイプ*を選択してください。

ステップ**2**：パスワード認証情報バリデーター　を作成する

パスワード認証情報バリデータをまだ作成していない場合は、作成します。

手順

1. **Password Credential Validators** > **Create New instance** を選択します。
2. 「タイプ」タブで、以下の情報を入力します：
   a. インスタンス名とインスタンスID：両方に同じ値を使用できます。
   b. タイプ：*LDAP Username Password Credential Validator*を選択してください。
3. 「 * 次へ * 」を選択します。
4. 「インスタンス構成」タブで、以下の情報を入力します：
   - LDAPデータストア：作成したデータストアを選択します。
   - 検索ベース：LDAPの構成 の情報を入力します。
   - 検索フィルター：**sAMAccountName=${username}** と入力します。
   - 検索範囲：*サブツリー*を選択してください。
5. 「 * 次へ * 」を選択します。
6. 拡張契約タブで、以下の属性を追加します： `memberOf`、 `objectGUID`、 `sAMAccountName`、 `sn`、および `userPrincipalName`
7. 「次へ」 > 「保存」を選択します。

ステップ**3**：**IdP**アダプタインスタンス　を作成する

まだ作成していない場合は、IdP（アイデンティティプロバイダー）アダプターインスタンスを作成してください。

> StorageGRID システムの各管理ノードには、IdP 接続が必要です。これにより、ユーザーはどの管理ノードにも安全にサインインおよびサインアウトできます。すべての管理ノードに対して単一の IdP 接続を作成すること（推奨）も、管理ノードごとに異なる IdP 接続を作成することもできます。

手順

1. 「 * 認証 * > * 統合 * > * IdP アダプタ * 」に移動します。
2. [新規インスタンスの作成（ Create New Instance ）] を選択します
3. 「タイプ」タブで、以下の情報を入力します：
   - インスタンス名とインスタンスID：両方に同じ値を使用できます。
   - タイプ：*HTML Form IdP Adapter*を選択してください。
4. 「 * 次へ * 」を選択します。
5. 「IdP Adapter」タブで、「Credential Validators」に新しい行を追加するを選択します。
6. 作成したパスワードクレデンシャルバリデータを選択します。
7. 「 * 次へ * 」を選択します。

8. 拡張契約タブで、パスワードクレデンシャルバリデータにマッピングした属性を追加します。
9. 「 * 次へ * 」を選択します。
10. アダプター属性タブで、Pseudonym の **username** 属性を選択します。
11. 「次へ」>「次へ」を選択します。
12. 概要を確認し、*保存*を選択します。

ステップ**4**：**OAuth**サーバーと認証サーバーの設定を構成する

StorageGRID が受け入れるグラントタイプをサポートするように認証サーバーを設定します。

手順

1. システム > *認証サーバー設定*に移動します。
2. REUSE EXISTING PERSISTENT ACCESS GRANTS FOR GRANT TYPES について、以下のオプションが選択されていることを確認してください。
   - 暗黙
   - 認証コード
   - リソース所有者のパスワード認証情報

   > ⓘ 会社がRESOURCE OWNER PASSWORD CREDENTIALSの使用を制限している場合、AUTHORIZATION CODEのみを使用できます。

3. OAuth 管理 Web サービス設定については、作成した パスワードクレデンシャルバリデータ を選択してください。

ステップ**5**：スコープを定義する

PingFederate でスコープを定義します。

手順

1. システム > **OAuth**設定 > スコープ管理 に移動します。
2. 「共通スコープ」タブで、**openid**、**email**、**profile** の値が存在しない場合は追加します。

ステップ**6**：**IdP**アダプタマッピングの設定

IdPアダプタマッピングを設定して、IdPからの属性を、アクセストークンやリフレッシュトークンなど、クライアントに発行される永続的な権限にマッピングします。

手順

1. **Authentication** > **Policy Contract Grant Mapping** に移動します。
2. 「IdP Adapter Grant Mapping」を選択します。
3. SOURCE ADAPTER INSTANCE ドロップダウンから、作成した HTMLフォームアダプタ を選択します。
4. 「マッピングの追加」 > 「契約履行」を選択します。
5. ソースで、USER_KEYとUSER_NAMEに*アダプター*を選択します。

6. 「値」で、USER_KEYに「sAMAccountName」を、USER_NAMEに「username」を選択します。
7. 「次へ」>「次へ」を選択して概要ページへ移動します。
8. [保存（ Save ）] を選択します。

ステップ**7**：リソース所有者の認証情報マッピングを設定する

認証時にユーザー認証情報が正しく検証されるように、リソース所有者認証情報のマッピングを設定してください。

手順

1. **Authentication** > **Policy Contract Grant Mapping** に移動します。
2. 「Resource Owner Credentials Grant Mapping」を選択します。
3. SOURCE PASSWORD VALIDATOR INSTANCE ドロップダウンから、作成した パスワードクレデンシャルバリデータ を選択します。
4. 「マッピングの追加」 >「契約履行」を選択します。
5. USER_KEY のマッピングを追加します：
   - 「ソース」で「Password Credential Validator」を選択します。
   - 「値」で **sAMAccountName** を選択します。
6. 「次へ」>「次へ」を選択して概要ページへ移動します。
7. [保存（ Save ）] を選択します。

ステップ **8:** 署名証明書の作成またはインポート

署名証明書を作成またはインポートしていない場合は、作成します。

手順

1. 「 * Security * > * Signing & Decryption keys & Certificates * 」に移動します。
2. 「新規作成」を選択し、以下の情報を入力します。
   - 共通名（CN）：これはサーバーの完全修飾ドメイン名（FQDN）である必要があります。
   - 組織名（Org）：組織の名前を入力してください。
   - 国：2文字の国コードを入力してください。例えば、アメリカ合衆国の場合は US と入力します。
   - 鍵アルゴリズム：適切な鍵アルゴリズム（例：**RSA**）を選択してください。
   - 鍵サイズ：**2048** ビットに設定してください。
   - 署名アルゴリズム：安全な暗号化操作を保証するために、署名アルゴリズムとして「RSA with SHA256」を選択してください。

ステップ**9**：アクセストークン管理の設定

StorageGRIDは、PingFederateでAPIリクエストを認証および認可するためにアクセストークンを使用します。

手順

1. アプリケーション > アクセストークン管理 に移動します。
2. [新規インスタンスの作成（ Create New Instance ）] を選択します
3. 「タイプ」タブで、以下の情報を入力します：
   - インスタンス名とインスタンスID：両方に同じ値を使用できます。
   - タイプ：値が **JSON Web Tokens** であることを確認してください。
4. 「 * 次へ * 」を選択します。
5. インスタンス構成タブで、証明書について以下の情報を入力します。
   - キーID：キーの一意の識別子を入力してください。
   - 証明書：作成した証明書を追加します。
   - JWSアルゴリズム：*SHA256を使用したRSA*を選択してください。
   - 有効な署名証明書キーID：この手順で作成した*KEY ID*を選択してください。
6. 「次へ」>「次へ」を選択します。
7. アクセストークン属性コントラクトタブで、サブジェクト属性名に*USER_KEY*を、コントラクトの拡張に*username*を選択します。
8. 「 * 追加」を選択します。
9. 概要ページへ移動するには、「次へ」＞「次へ」＞「次へ」を選択してください。
10. [保存（ Save ）] を選択します。

ステップ**10**：アクセストークンマッピングの設定

作成したアクセストークンを使用するように、アクセストークンマッピングを設定します。

手順

1. 「アプリケーション」＞「アクセストークンのマッピング」に移動します。
2. 「アクセストークンのマッピング」を選択します。
3. 「マッピングを追加」を選択します。
4. コンテキストには、*デフォルト*を選択します。
5. Access Token Manager には、作成した アクセストークン を選択します。
6. 「次へ」 > 「Contract Fulfillment」を選択します：
7. ソースの「ユーザー名」で **Persistent Grant** を選択します。
8. 「値」で、ユーザー名として「**USER_KEY**」を選択してください。
9. 「次へ」 > 「保存」を選択します。

ステップ**11**：**OpenID Connect** ポリシーを設定する

OpenID仕様に従ってマッピングされた属性へのクライアントアクセスに関するOpenID Connectポリシーを定義します。

手順

1. 「アプリケーション」＞「OAuthクライアント」に移動してください。
2. **OpenId Connect Policy Management** > **Add Policy** を選択します。
3. 「ポリシーの管理」タブで、以下の情報を入力します：
   - ポリシーID：ポリシーの一意の識別子。
   - ポリシー名：ポリシーの内容を説明する名称。
   - アクセストークンマネージャー：作成したアクセストークンを選択します。
   - ID TOKEN LIFETIME：ID トークンの有効期間を設定します。例：60 分または 1 時間。
   - IDトークンにユーザー情報を含める：IDトークンにユーザーの詳細を含める場合は、このボックスを選択してください。
4. 「 * 次へ * 」を選択します。
5. 「属性契約」タブで、作成した データストア に不要な既存の属性をすべて削除します。Ping Authentication から StorageGRID に渡す属性のみを保持します。

   これは非常に重要なステップです。これは、IDトークンにどの属性値を含めるかを決定します。StorageGRID は、認証プロセス中にこれらの値を継承します。

6. 「次へ」>「次へ」を選択します。
7. 「属性ソースとユーザー検索」タブで、*「属性ソースの追加」*を選択します。次に、以下の情報を入力します。
   - ATTRIBUTE SOURCE ID と ATTRIBUTE SOURCE DESCRIPTION：両方に同じ値を使用できます。
   - アクティブデータストア：作成したデータストアを選択します。
8. 「 * 次へ * 」を選択します。
9. LDAP ディレクトリ検索タブで、次の手順を実行します。
   a. 「 * ベース DN * 」を入力します。この DN は、 LDAP サーバの StorageGRID で入力した値と完全に一致している必要があります。
   b. 「ルートオブジェクトクラス」ドロップダウンから、**objectClass** を選択します。
   c. 「ATTRIBUTE」ドロップダウンから、マッピングするオブジェクトクラスごとに属性を追加します。例：
      - InetOrgPerson：displayName、givenName、またはHomePhoneを追加します。
      - ユーザー: LocalID または userPrincipalName （upn）を追加します。
      - 上部：memberOf または名前を追加します。
      - 人物：sn を追加します。
10. 「 * 次へ * 」を選択します。
11. LDAP Filter タブで、 * sAMAccountName = $ ｛userName｝ * と入力します。

    LDAPフィルターをカスタマイズして、StorageGRIDが組織固有のActive DirectoryまたはLDAP構造に基づいてユーザー属性を取得できるようにする必要があります。ご使用の環境に適したフィルタ式を入手するには、LDAP/AD管理者にご相談ください。

12. 「保存」を選択して、概要を確認してください。

13. 「契約履行」タブで、以下の情報を入力してください：
    - ソース：作成したLDAPデータストアを選択します。
    - 値：各属性コントラクトをそれぞれの値にマッピングします。
14. 「次へ」>「次へ」を選択します。
15. 概要を確認し、*保存*を選択します。
16. 「アプリケーション」>「OAuthクライアント」>「OpenID Connectポリシー管理」に移動します。
17. 作成したポリシーがデフォルトポリシーとして設定されていることを確認してください。

ステップ12：OAuthサーバー用のOAuthクライアントを作成する

必要なクライアント認証情報を設定し、PingFederate と StorageGRID 間の接続を承認するために、新しい OAuth クライアントを作成します。

手順

1. 「アプリケーション」＞「OAuthクライアント」に移動してください。
2. 「クライアントの追加」を選択し、以下の情報を入力します：
    - クライアントID：固有の値を入力してください。
    - クライアント認証：*クライアントシークレット*を選択します。
    - クライアントシークレット：シークレットの変更 > シークレットの生成 を選択します。

      これにより、クライアント用の秘密鍵が生成されます。このキーは後で使用するために保存してください。

    - リダイレクト URI：StorageGRID の返却 URL を「リダイレクト URI」セクションに入力します。これらの URL は、StorageGRID で OAuth 用に設定された URL と一致する必要があります。例：
    - `https://<Admin IP or Hostname>/api/v4/oidc-callback`
    - `https://<Admin IP or Hostname>/api/v4/oidc-logged-out`
    - 許可されるグラントの種類：以下のオプションを選択してください。
        - 認証コード：これにより OAuth フローが開始されます。
        - リフレッシュトークン：アクセストークンの有効期限が切れたときに新しいトークンを取得します。
        - リソース所有者のパスワード認証情報：認証のためにユーザー認証情報に直接アクセスする必要がある場合。
    - OPENID CONNECT：IDトークン署名アルゴリズムとして「SHA-256を使用したRSA」を選択してください。
    - ログアウトモード：**OIDC Back-Channel** を選択してください。
    - フロントチャネルログアウトURI、バックチャネルログアウトURI、およびポストログアウトリダイレクトURI：StorageGRID ログアウトURIを追加します： `https://<Admin IP or Hostname>/api/v4/oidc-logged-out`
3. [保存（ Save ）] を選択します。

次の手順

SP接続を作成した後、"OIDCを使用してSSOを構成する"。

OIDC を使用して **StorageGRID** で **SSO** を設定する

OpenID Connect (OIDC) の SSO 設定ウィザードに従い、サンドボックスモードに入って設定とテストを行います。すべての StorageGRID ユーザーに対してシングル サインオン（SSO）を有効にする前に、設定とテストを実施してください。SSO を有効にした後、必要に応じてサンドボックスモードに戻り、設定を変更したり再テストしたりできます。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"rootアクセス権限"。
- StorageGRID システムの SSO ID プロバイダーで OIDC クライアントを設定しました。
- StorageGRID システムに"アイデンティティフェデレーションが設定された"があります。

ステップ**1**：**ID**プロバイダーの詳細を入力する

ウィザードにアクセスし、「IDプロバイダーの詳細を入力する」ページの各項目を入力します。

手順

1. SSO設定を構成するウィザードにアクセスします。
   a. 構成 > アクセス制御 > シングル サインオン を選択します。シングル サインオン ページが表示されます。

      [SSO 設定の構成] ボタンが無効になっている場合は、ID プロバイダーをフェデレーション ID ソースとして構成していることを確認します。。 "シングルサインオンの要件と考慮事項" 。

   b. *SSO設定の構成*を選択します。 「ID プロバイダーの詳細を提供する」ページが表示されます。
2. プロトコル で **OIDC** を選択します。
3. ドロップダウンリストから * SSO タイプ * を選択します。
4. StorageGRID 要求への応答としてアイデンティティプロバイダが SSO 設定情報を送信するときに、接続の保護に使用する TLS 証明書を指定します。
   - * オペレーティング・システムの CA 証明書を使用 * ：オペレーティング・システムにインストールされているデフォルトの CA 証明書を使用して、接続を保護します。
   - * カスタム CA 証明書を使用 * ：カスタム CA 証明書を使用して接続を保護します。

     この設定を選択した場合：

     i. CA証明書の場所を参照します。
     ii. CA証明書ファイルをアップロードします。
   - **TLS** を使用しない：接続を保護するために TLS 証明書を使用しません。

CA証明書を変更した場合は、すぐに"管理ノードでmgmt-apiサービスを再起動します。"Grid ManagerでSSOが成功するかどうかをテストします。

5. *続行*を選択します。 「証明書利用者識別子の提供」ページが表示されます。

ステップ2：クライアント情報を入力する

ウィザードの「クライアント情報の入力」ステップで、各項目を入力してください。

手順

1. StorageGRID の 依拠当事者識別子 を指定します。この値は、各 OIDC 構成に使用する名前を制御します。
   - たとえば、グリッドに管理ノードが1つしかなく、今後管理ノードを追加する予定がない場合は、または `StorageGRID`と入力し `SG`ます。
   - グリッドに複数の管理ノードが含まれている場合は、識別子に文字列 `[HOSTNAME]`を含めてください。例： `SG-[HOSTNAME]`。この文字列を含めると、グリッド内の各管理ノードのホスト名に基づいて、そのノードの OIDC 構成を示すテーブルが作成されます。

StorageGRIDシステムの管理ノードに対してOIDCを設定する必要があります。これにより、ユーザーはどの管理ノードにも安全にサインインおよびサインアウトできるようになります。すべての管理ノードで同じOIDC構成を使用することも（推奨）、各管理ノードに異なるOIDC構成を設定することもできます。

2. 各依拠当事者識別子について、クライアント**ID**、クライアントシークレット、および*OpenIDエンドポイントURL*を入力してください。
3. *保存してサンドボックスモードに入る*を選択します。

ステップ3：テスト構成

サンドボックスモードに入ると、選択したSSOタイプの構成を完了してテストできます。

サンドボックスモードを使用すると、設定のやり取りを簡単に実行し、SSOを有効にする前にすべての設定をテストできます。StorageGRIDは、必要に応じてサンドボックスモードを維持できます。ただし、サインインできるのはフェデレーションユーザーとローカルユーザーのみです。

手順

1. 「SSO の構成」ページで、ウィザードの「構成のテスト」手順のリンクを見つけます。

   URL は、 [* フェデレーションサービス名 * （ * Federation service name * ）] フィールドに入力した値から取得されます。

2. リンクを選択するか、URLをコピーして新しいタブに貼り付けて、IDプロバイダーのサインオンページにアクセスしてください。
3. フェデレーションユーザー名とパスワードを入力してください。
   - SSOのサインインとログアウトが正常に完了すると、緑色のバナーが表示されます。
   - SSO 処理が失敗すると、エラーメッセージが表示されます。問題 を修正し、ブラウザのクッキーを消去してやり直してください。

4. ウィザードの手順に従って、グリッド内の各管理ノードのテスト構成ページにアクセスしてください。
5. 手順 2 および 3 を繰り返して、各管理ノードの SSO 接続を確認します。

ステップ**4**：シングル サインオンを有効にする

各管理ノードへのサインインにSSOを使用できることを確認したら、StorageGRIDシステム全体でSSOを有効にできます。

> SSOが有効になっている場合、すべてのユーザーは、グリッドマネージャ、テナントマネージャ、グリッド管理API、およびテナント管理APIにアクセスするためにSSOを使用する必要があります。ローカルユーザーはStorageGRIDにアクセスできなくなります。StorageGRIDは、サポートされているすべてのSSOプロバイダーに対応した認証スクリプトの例を提供していません。

手順

1. SSO 構成ウィザードのテスト構成手順で、**SSO** を有効にする を選択します。
2. 警告メッセージを確認し、*SSO を有効にする*を選択します。

   シングル サインオンが有効になりました。シングル サインオン ページが表示され、先ほど構成した SSO の詳細が表示されます。

3. 設定を編集するには、[編集] を選択します。
4. シングル サインオンを無効にするには、*無効にする*を選択してください。

> Azure ポータルを使用しており、Entra ID にアクセスするために使用するのと同じコンピューターからStorageGRID にアクセスする場合は、Azure ポータル ユーザーが承認されたStorageGRIDユーザー (StorageGRIDにインポートされたフェデレーション グループ内のユーザー) であることを確認するか、 StorageGRIDにサインインする前に Azure ポータルからログアウトしてください。

SAMLを使用して**SSO**を設定する

SAMLを使用して**StorageGRID**でシングル サインオンを設定する方法について説明します

StorageGRID でシングル サインオン（SSO）を設定すると、StorageGRID（サービス プロバイダー）と SSO ID プロバイダーがユーザ認証リクエストについて安全に通信できるようになります。

StorageGRID では、OpenID Connect（OIDC）または SAML を使用してシングル サインオンを設定できます。SAML を使用して StorageGRID でシングル サインオンを設定するには、以下の概要手順に従うか、"OIDCを使用したSSOの設定"について確認してください。

1 **SSO**の設定

SAML の SSO 設定ウィザードを選択します。次に、ID プロバイダーで SSO を設定し、サンドボックス モードに切り替えます。

"SAMLを使用したSSOの設定"について学ぶ

2 IDプロバイダーの設定

使用するSSO IDプロバイダーに応じて、IDフェデレーションLDAPサービスタイプとしてActive DirectoryまたはEntra IDのいずれかを選択できます。

- Active Directory Federation Service (AD FS) の場合、AD FS、Entra ID、またはPingFederate アイデンティティプロバイダーを使用できます。
- Entra IDでは、Entra IDのIDプロバイダーのみを使用できます。

SSO IDプロバイダーのソフトウェアを使用して、グリッド内の各管理ノードのSAMLを設定します。

- Active Directory の "各管理ノードごとにアプリケーショングループを作成する" について学ぶ
- Entra ID の"各管理ノード用のアプリケーションを作成する"について
- PingFederate の "各管理ノードに対してサービスプロバイダー接続を作成する" について学ぶ

3 テスト構成

各管理ノードの SAML を設定したら、SSO 設定ウィザードに戻り、設定をテストしてください。

"SSOの設定をテストする"について学ぶ

4 SSOを有効にする

すべての StorageGRID ユーザーに対してシングル サインオンを有効にします。

"StorageGRID ユーザーのシングル サインオンの有効化"について学ぶ

SAMLを使用して**StorageGRID**で**SSO**を設定する

SAML の SSO 設定ウィザードに従い、サンドボックスモードに入って、すべての StorageGRID ユーザーに対して有効にする前にシングル サインオン（SSO）の設定とテストを行います。SSO を有効にした後、必要に応じてサンドボックスモードに戻り、設定を変更したり再テストしたりできます。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"rootアクセス権限"。
- StorageGRID システムにアイデンティティフェデレーションを設定しておきます。
- アイデンティティ フェデレーション **LDAP** サービス タイプ では、使用する予定の SSO アイデンティティ プロバイダーに基づいて、Active Directory または Entra ID のいずれかを選択しました。

LDAP サービスタイプが設定されました	SSO アイデンティティプロバイダのオプション
Active Directory フェデレーションサービス（ AD FS ）	• Active Directory • エントラID • PingFederate
エントラID	エントラID

タスクの内容

SSO が有効な場合、ユーザが管理ノードにサインインしようとすると、 StorageGRID から SSO アイデンティティプロバイダに認証要求が送信されます。次に、 SSO アイデンティティプロバイダは、認証要求が成功したかどうかを示す認証応答を StorageGRID に返します。成功した要求の場合：

- Active Directory または PingFederate からの応答には、ユーザの Universally Unique Identifier （ UUID ）が含まれています。
- Entra ID からの応答には、ユーザー プリンシパル名 (UPN) が含まれます。

StorageGRID （サービスプロバイダー）と SSO ID プロバイダーがユーザ認証リクエストについて安全に通信できるようにするには、次のタスクを実行します。

1. StorageGRIDで設定を構成します。
2. SSO IDプロバイダーのソフトウェアを使用して、各管理ノードの証明書利用者信頼 （AD FS）、エンタープライズアプリケーション （Entra ID）、またはサービスプロバイダー （PingFederate） を作成します。
3. StorageGRIDに戻り、SSO を有効にします。

サンドボックス モードを使用すると、この双方向の構成を簡単に実行でき、SSO を有効にする前にすべての設定をテストできます。サンドボックス モードを使用している場合、ユーザーは SSO を使用してサインインできません。

ステップ**1**：**ID**プロバイダーの詳細を入力する

ウィザードにアクセスし、「IDプロバイダーの詳細を入力する」ページの各項目を入力します。

手順

1. ウィザードにアクセスする：
   a. 構成 > アクセス制御 > シングル サインオン を選択します。シングル サインオン ページが表示されます。

      [SSO 設定の構成] ボタンが無効になっている場合は、ID プロバイダーをフェデレーション ID ソースとして構成していることを確認します。。 "シングルサインオンの要件と考慮事項" 。

   b. *SSO設定の構成*を選択します。 「ID プロバイダーの詳細を提供する」ページが表示されます。
2. 「プロトコル」で「SAML」を選択します。
3. ドロップダウンリストから * SSO タイプ * を選択します。

4. SSO タイプとして Active Directory を選択した場合は、Active Directory フェデレーション サービス (AD FS) に表示されるとおりに、ID プロバイダーの フェデレーション サービス名 を入力します。

   フェデレーションサービス名を確認するには、 Windows Server Manager に移動します。[ツール *>*AD FS 管理 *] を選択します。[アクション] メニューから、 [* フェデレーションサービスのプロパティの編集 *] を選択します。フェデレーションサービス名が 2 番目のフィールドに表示されます。

5. StorageGRID 要求への応答としてアイデンティティプロバイダが SSO 設定情報を送信するときに、接続の保護に使用する TLS 証明書を指定します。

   - * オペレーティング・システムの CA 証明書を使用 * ：オペレーティング・システムにインストールされているデフォルトの CA 証明書を使用して、接続を保護します。
   - * カスタム CA 証明書を使用 * ：カスタム CA 証明書を使用して接続を保護します。

     この設定を選択した場合は、カスタム証明書のテキストをコピーし、 * CA 証明書 * テキストボックスに貼り付けます。

   - **TLS** を使用しない：接続を保護するために TLS 証明書を使用しません。

     CA証明書を変更した場合は、すぐに"管理ノードでmgmt-apiサービスを再起動します。"Grid ManagerでSSOが成功するかどうかをテストします。

6. *続行*を選択します。 「証明書利用者識別子の提供」ページが表示されます。

ステップ **2**：依拠パーティの信頼、エンタープライズ アプリケーション、または **SP** 接続の提供

選択したSSOタイプに基づいて、ウィザードのステップ2の各項目を入力してください。

Active Directory

「依拠当事者識別子の提供」の手順で、該当する項目をすべて入力してください。

手順

1. StorageGRIDの **Relying party identifier** を指定します。この値は、AD FS 内の各証明書利用者信頼に使用する名前を制御します。
   - たとえば、グリッドに管理ノードが1つしかなく、今後管理ノードを追加する予定がない場合は、または `StorageGRID`と入力し `SG`ます。
   - グリッドに複数の管理ノードが含まれている場合は、文字列 `[HOSTNAME]`識別子内。例：`SG-[HOSTNAME]`。この文字列を含めると、ノードのホスト名に基づいて、グリッド内の各管理ノードの依存パーティ ID を示すテーブルが作成されます。

   > 証明書利用者信頼は StorageGRID システム内の管理ノードごとに作成する必要があります。管理ノードごとに証明書利用者信頼を作成することで、ユーザは管理ノードに対して安全にサインイン / サインアウトすることができます。

2. *保存してサンドボックスモードに入る*を選択します。

エントラ**ID**

「エンタープライズアプリケーションの構成」ステップの各項目を入力してください。

手順

1. エンタープライズ アプリケーション セクションで、 StorageGRIDの エンタープライズ アプリケーション名 を指定します。この値は、Entra ID 内の各エンタープライズ アプリケーションに使用する名前を制御します。
   - たとえば、グリッドに管理ノードが1つしかなく、今後管理ノードを追加する予定がない場合は、または `StorageGRID`と入力し `SG`ます。
   - グリッドに複数の管理ノードが含まれている場合は、文字列 `[HOSTNAME]`識別子内。例：`SG-[HOSTNAME]`。この文字列を含めると、ノードのホスト名に基づいて、システム内の各管理ノードのエンタープライズ アプリケーション名を示すテーブルが作成されます。

   > StorageGRID システムで管理ノードごとにエンタープライズアプリケーションを作成する必要があります。管理ノードごとにエンタープライズアプリケーションを用意することで、ユーザはどの管理ノードに対しても安全にサインイン / サインアウトすることができます。

2. 表に記載されている各管理ノードのエンタープライズアプリケーションを作成するには、"Entra IDでエンタープライズアプリケーションを作成する"の手順に従ってください。
3. Entra ID から、各エンタープライズ アプリケーションのフェデレーション メタデータ URL をコピーします。次に、この URL をStorageGRIDの対応する **Federation metadata URL** フィールドに貼り付けます。
4. すべての管理ノードのフェデレーション メタデータ URL をコピーして貼り付けた後、[保存してサンドボックス モードに入る] を選択します。

PingFederate

*SP接続IDの指定*ステップのフィールドに入力します。

手順

1. Service Provider （ SP ；サービスプロバイダ）セクションで、 StorageGRID の * SP 接続 ID * を指定します。この値は、 PingFederate の各 SP 接続に使用する名前を制御します。
   - たとえば、グリッドに管理ノードが1つしかなく、今後管理ノードを追加する予定がない場合は、または `StorageGRID`と入力し `SG`ます。
   - グリッドに複数の管理ノードが含まれている場合は、文字列 `[HOSTNAME]`識別子内。例： `SG-[HOSTNAME]` 。この文字列を含めると、ノードのホスト名に基づいて、システム内の各管理ノードのSP接続 ID を示すテーブルが作成されます。

   StorageGRID システムで管理ノードごとに SP 接続を作成する必要があります。管理ノードごとに SP 接続を確立することで、ユーザは管理ノードに対して安全にサインイン / サインアウトすることができます。

2. 各管理ノードのフェデレーションメタデータの URL を * Federation metadata url * フィールドで指定します。

   次の形式を使用します。

   ```
   https://<Federation Service
   Name>:<port>/pf/federation_metadata.ping?PartnerSpId=<SP Connection
   ID>
   ```

3. *保存してサンドボックスモードに入る*を選択します。

ステップ **3**：証明書利用者の信頼、エンタープライズ アプリケーション、または **SP** 接続の設定

構成を保存してサンドボックス モードに入ると、選択した SSO タイプの構成を完了してテストできます。

StorageGRID は、必要な限りサンドボックス モードのままにすることができます。ただし、サインインできるのはフェデレーション ユーザーとローカル ユーザーのみです。

Active Directory

手順

1. Active Directory フェデレーションサービス（ AD FS ）に移動します。
2. 「SSO の構成」ページの表に示されている各証明書利用者 ID を使用して、 StorageGRIDの 1 つ以上の証明書利用者信頼を作成します。

   次の表に示す管理ノードごとに信頼を 1 つ作成する必要があります。

   手順については、"AD FS に証明書利用者信頼を作成します"を参照してください。

エントラ**ID**

手順

1. 現在サインインしている管理ノードのシングルサインオンページから、 SAML メタデータをダウンロードして保存するボタンを選択します。
2. グリッド内の他の管理ノードについて、上記の手順を繰り返します。
   a. ノードにサインインします。
   b. 構成 > アクセス制御 > シングル サインオン を選択します。
   c. そのノードの SAML メタデータをダウンロードして保存します。
3. Azure ポータルに移動します。
4. "Entra IDでエンタープライズアプリケーションを作成する"の手順に従って、各管理ノードのSAMLメタデータファイルを対応するEntra IDエンタープライズアプリケーションにアップロードしてください。

PingFederate

手順

1. 現在サインインしている管理ノードのシングルサインオンページから、 SAML メタデータをダウンロードして保存するボタンを選択します。
2. グリッド内の他の管理ノードについて、上記の手順を繰り返します。
   a. ノードにサインインします。
   b. 構成 > アクセス制御 > シングル サインオン を選択します。
   c. そのノードの SAML メタデータをダウンロードして保存します。
3. 「 PingFederate 」に移動します。
4. "StorageGRID 用に 1 つ以上の SP 接続を作成します"。各管理ノードのSP接続ID（「SSO設定」ページの表に表示）と、その管理ノード用にダウンロードしたSAMLメタデータを使用してください。

   次の表に示す管理ノードごとに 1 つの SP 接続を作成する必要があります。

ステップ**4**：設定のテスト

StorageGRIDシステム全体にシングル サインオンの使用を強制する前に、各管理ノードに対してシングル サインオンとシングル ログアウトが正しく設定されていることを確認してください。

Active Directory

手順

1. 「SSO の構成」ページで、ウィザードの「構成のテスト」手順のリンクを見つけます。

   URL は、 [* フェデレーションサービス名 * （ * Federation service name * ）] フィールドに入力した値から取得されます。

2. リンクを選択するか、 URL をコピーしてブラウザに貼り付け、アイデンティティプロバイダのサインオンページにアクセスします。
3. SSO を使用して StorageGRID にサインインできることを確認するには、 * 次のいずれかのサイトにサインイン * を選択し、プライマリ管理ノードの証明書利用者 ID を選択して * サインイン * を選択します。
4. フェデレーテッドユーザのユーザ名とパスワードを入力します。
   - SSO サインインおよびログアウト処理が成功すると、成功のメッセージが表示されます。
   - SSO 処理が失敗すると、エラーメッセージが表示されます。問題 を修正し、ブラウザのクッキーを消去してやり直してください。
5. 同じ手順を繰り返して、グリッド内の管理ノードごとに SSO 接続を確認します。

エントラ**ID**

手順

1. Azure ポータルのシングルサインオンページに移動します。
2. [このアプリケーションをテストする *] を選択します。
3. フェデレーテッドユーザのクレデンシャルを入力します。
   - SSO サインインおよびログアウト処理が成功すると、成功のメッセージが表示されます。
   - SSO 処理が失敗すると、エラーメッセージが表示されます。問題 を修正し、ブラウザのクッキーを消去してやり直してください。
4. 同じ手順を繰り返して、グリッド内の管理ノードごとに SSO 接続を確認します。

PingFederate

手順

1. 「SSO の構成」ページで、サンドボックス モード メッセージの最初のリンクを選択します。

   一度に 1 つのリンクを選択してテストします。

2. フェデレーテッドユーザのクレデンシャルを入力します。
   - SSO サインインおよびログアウト処理が成功すると、成功のメッセージが表示されます。
   - SSO 処理が失敗すると、エラーメッセージが表示されます。問題 を修正し、ブラウザのクッキーを消去してやり直してください。
3. 次のリンクを選択して、グリッド内の各管理ノードの SSO 接続を確認します。

   「ページの有効期限が切れました」というメッセージが表示された場合は、ブラウザで「 * 戻る * 」ボタンを選択し、クレデンシャルを再送信してください。

ステップ**5**：シングル サインオンを有効にする

各管理ノードへのサインインにSSOを使用できることを確認したら、StorageGRIDシステム全体でSSOを有効にできます。

SSO が有効になっている場合は、すべてのユーザが SSO を使用して Grid Manager 、テナントマネージャ、グリッド管理 API 、およびテナント管理 API にアクセスする必要があります。ローカルユーザは StorageGRID にアクセスできなくなります。

手順

1. SSO 構成ウィザードのテスト構成手順で、**SSO** を有効にする を選択します。
2. 警告メッセージを確認し、*SSO を有効にする*を選択します。

   シングル サインオンが有効になりました。シングル サインオン ページが表示され、先ほど構成した SSO の詳細が表示されます。

3. 設定を編集するには、[編集] を選択します。
4. シングル サインオンを無効にするには、[**SSO** を無効にする] を選択します。

Azure ポータルを使用しており、Entra ID にアクセスするために使用するのと同じコンピューターからStorageGRID にアクセスする場合は、Azure ポータル ユーザーが承認されたStorageGRIDユーザー (StorageGRIDにインポートされたフェデレーション グループ内のユーザー) であることを確認するか、 StorageGRIDにサインインする前に Azure ポータルからログアウトしてください。

次の手順

SAMLを使用してSSOを設定した後、管理ノードのIDプロバイダーを設定します。

IDプロバイダーが…	必要があります…
Active Directory	"各管理ノードのアプリケーショングループを作成する"
エントラID	"各管理ノードのアプリケーションを作成する"
PingFederate	"各管理ノードのサービスプロバイダー接続を作成する"

StorageGRID の **SAML** 用に **AD FS** で証明書利用者信頼を作成する

システム内の各管理ノードのSAMLに対して、Active Directory フェデレーションサービス（AD FS）を使用して証明書利用者信頼を作成する必要があります。証明書利用者信頼を作成するには、PowerShellコマンドを使用する方法、StorageGRID からSAMLメタデータをインポートする方法、またはデータを手動で入力する方法があります。

開始する前に

- StorageGRID のシングルサインオンを設定し、 SSO タイプとして **AD FS** を選択しました。
- Grid Manager に "サンドボックスモードに入りました" があります。

- システム内の各管理ノードの完全修飾ドメイン名 (または IP アドレス) と証明書利用者識別子がわかっています。これらの値は、 StorageGRID のSSO 設定ページの管理ノードの詳細テーブルで確認できます。

> ⓘ 証明書利用者信頼は StorageGRID システム内の管理ノードごとに作成する必要があります。管理ノードごとに証明書利用者信頼を作成することで、ユーザは管理ノードに対して安全にサインイン / サインアウトすることができます。

- AD FS での証明書利用者信頼の作成経験があるか、または Microsoft AD FS のドキュメントを参照できる必要があります。
- AD FS 管理スナップインを使用していて、 Administrators グループに属している必要があります。
- 証明書利用者信頼を手動で作成する場合は、 StorageGRID 管理インターフェイス用にカスタム証明書をアップロードするか、コマンドシェルから管理ノードにログインする方法を確認しておきます。

タスクの内容

以下の手順は、 Windows Server 2016 AD FS に該当します。別のバージョンの AD FS を使用している場合は、手順 にわずかな違いがあります。不明な点がある場合は、 Microsoft AD FS のドキュメントを参照してください。

Windows PowerShell を使用して証明書利用者信頼を作成します

Windows PowerShell を使用して証明書利用者信頼を簡単に作成できます。

手順

1. Windows のスタートメニューから PowerShell アイコンを右クリックし、 * 管理者として実行 * を選択します。
2. PowerShell コマンドプロンプトで、次のコマンドを入力します。

```
Add-AdfsRelyingPartyTrust -Name "Admin_Node_Identifer" -MetadataURL
"https://Admin_Node_FQDN/api/saml-metadata"
```

   - には *Admin_Node_Identifier*、管理ノードの証明書利用者IDを[Single Sign-on]ページに表示されるとおりに入力します。たとえば、 `SG-DC1-ADM1`です。
   - には *Admin_Node_FQDN*、同じ管理ノードの完全修飾ドメイン名を入力します。（必要に応じて、ノードの IP アドレスを代わりに使用できます。ただし、 IP アドレスを入力した場合、その IP アドレスが変わったときには証明書利用者信頼を更新または再作成する必要があります）。

3. Windows Server Manager で、 * Tools * > * AD FS Management * を選択します。

   AD FS 管理ツールが表示されます。

4. 「 * AD FS * > * 証明書利用者信頼」を選択します。

   証明書利用者信頼のリストが表示されます。

5. 新しく作成した証明書利用者信頼にアクセス制御ポリシーを追加します。
   a. 作成した証明書利用者信頼を検索します。
   b. 信頼を右クリックし、 * アクセス制御ポリシーの編集 * を選択します。
   c. アクセス制御ポリシーを選択します。

d. [* 適用（ Apply ）] を選択し、 [* OK] を選択します

6. 新しく作成した証明書利用者信頼に要求発行ポリシーを追加します。
   a. 作成した証明書利用者信頼を検索します。
   b. 信頼を右クリックし、 ［ * クレーム発行ポリシーの編集 * ］ を選択します。
   c. [* ルールの追加 *] を選択します。
   d. ［ ルールテンプレートの選択 ］ ページで、リストから ［ * LDAP 属性をクレームとして送信 * ］ を選択し、 ［ * 次へ * ］ を選択します。
   e. ［ ルールの設定 ］ ページで、このルールの表示名を入力します。

      たとえば、* ObjectGUID to Name ID*または* UPN to Name ID*などです。

   f. 属性ストアで、 * Active Directory * を選択します。
   g. [マッピング]テーブルの[LDAP属性]列に「* objectGUID 」と入力するか、[ユーザープリンシパル名]* を選択します。
   h. マッピングテーブルの発信クレームタイプ列で、ドロップダウンリストから * 名前 ID * を選択します。
   i. 「完了」を選択し、「 * OK 」を選択します。
7. メタデータが正常にインポートされたことを確認します。
   a. 証明書利用者信頼を右クリックしてプロパティを開きます。
   b. [**Endpoints**] 、 [***Identifiers**] 、および [**Signature**] タブのフィールドに値が入力されていることを確認します。

      メタデータが見つからない場合は、フェデレーションメタデータのアドレスが正しいことを確認するか、値を手動で入力します。

8. 上記の手順を繰り返して、 StorageGRID システム内のすべての管理ノードに対して証明書利用者信頼を設定します。
9. 完了したら、StorageGRID に戻り、"すべての証明書利用者信頼をテストする"正しく設定されていることを確認してください。

フェデレーションメタデータをインポートして、証明書利用者信頼を作成します

各証明書利用者信頼の値をインポートするには、各管理ノードの SAML メタデータにアクセスします。

手順

1. Windows Server Manager で、 * Tools * を選択し、 * AD FS Management * を選択します。
2. Actions （アクション）で、 * Add （証明書利用者信頼の追加） * を選択します。
3. [ようこそ] ページで、 [* クレーム対応 *] を選択し、 [開始 *] を選択します。
4. [* オンラインまたはローカルネットワーク上で公開されている証明書利用者に関するデータをインポートする *] を選択します。
5. * フェデレーションメタデータアドレス（ホスト名または URL ） * に、この管理ノードの SAML メタデータの場所を入力します。

`https://Admin_Node_FQDN/api/saml-metadata`

には *Admin_Node_FQDN*、同じ管理ノードの完全修飾ドメイン名を入力します。（必要に応じて、ノードの IP アドレスを代わりに使用できます。ただし、 IP アドレスを入力した場合、その IP アドレスが変わったときには証明書利用者信頼を更新または再作成する必要があります）。

6. 証明書利用者信頼の追加ウィザードを実行し、証明書利用者信頼を保存して、ウィザードを閉じます。

> 表示名を入力するときは、管理ノードの証明書利用者 ID を使用します。これは、 Grid Manager のシングルサインオンページに表示される情報とまったく同じです。たとえば、 `SG-DC1-ADM1`です。

7. クレームルールを追加します。
   a. 信頼を右クリックし、 ［ * クレーム発行ポリシーの編集 * ］ を選択します。
   b. [* ルールを追加 * （ Add rule * ）] を
   c. ［ ルールテンプレートの選択 ］ ページで、リストから ［ * LDAP 属性をクレームとして送信 * ］ を選択し、 ［ * 次へ * ］ を選択します。
   d. ［ ルールの設定 ］ ページで、このルールの表示名を入力します。

      たとえば、* ObjectGUID to Name ID*または* UPN to Name ID*などです。

   e. 属性ストアで、 * Active Directory * を選択します。
   f. [マッピング]テーブルの[LDAP属性]列に「* objectGUID 」と入力するか、[ユーザープリンシパル名]*を選択します。
   g. マッピングテーブルの発信クレームタイプ列で、ドロップダウンリストから * 名前 ID * を選択します。
   h. 「完了」を選択し、「 * OK 」を選択します。
8. メタデータが正常にインポートされたことを確認します。
   a. 証明書利用者信頼を右クリックしてプロパティを開きます。
   b. [**Endpoints**] 、 [***Identifiers**] 、および [**Signature**] タブのフィールドに値が入力されていることを確認します。

      メタデータが見つからない場合は、フェデレーションメタデータのアドレスが正しいことを確認するか、値を手動で入力します。

9. 上記の手順を繰り返して、 StorageGRID システム内のすべての管理ノードに対して証明書利用者信頼を設定します。
10. 完了したら、StorageGRID に戻り、"すべての証明書利用者信頼をテストする"正しく設定されていることを確認してください。

証明書利用者信頼を手動で作成します

証明書利用者信頼のデータをインポートしないことを選択した場合は、値を手動で入力できます。

手順

1. Windows Server Manager で、 * Tools * を選択し、 * AD FS Management * を選択します。

2. Actions （アクション）で、 * Add （証明書利用者信頼の追加） * を選択します。
3. [ようこそ] ページで、 [* クレーム対応 *] を選択し、 [開始 *] を選択します。
4. [* 証明書利用者に関するデータを手動で入力する *] を選択し、 [* 次へ *] を選択します。
5. 証明書利用者信頼の追加ウィザードを実行します。

   a. この管理ノードの表示名を入力します。

      整合性を確保するために、管理ノードの証明書利用者 ID を使用してください。この ID は、 Grid Manager のシングルサインオンページに表示されます。たとえば、 `SG-DC1-ADM1`です。

   b. オプションのトークン暗号化証明書を設定する手順は省略してください。

   c. [URLの設定]ページで、* SAML 2.0 WebSSOプロトコルのサポートを有効にする*チェックボックスをオンにします。

   d. 管理ノードの SAML サービスエンドポイントの URL を入力します。

      `https://Admin_Node_FQDN/api/saml-response`

      には *Admin_Node_FQDN*、管理ノードの完全修飾ドメイン名を入力します。（必要に応じて、ノードの IP アドレスを代わりに使用できます。ただし、 IP アドレスを入力した場合、その IP アドレスが変わったときには証明書利用者信頼を更新または再作成する必要があります）。

   e. Configure Identifiers ページで、同じ管理ノードの証明書利用者 ID を指定します。

      Admin_Node_Identifier

      には *Admin_Node_Identifier*、管理ノードの証明書利用者IDを[Single Sign-on]ページに表示されるとおりに入力します。たとえば、 `SG-DC1-ADM1`です。

   f. 設定を確認し、証明書利用者信頼を保存して、ウィザードを閉じます。

      [クレーム発行ポリシーの編集] ダイアログボックスが表示されます。

      ダイアログボックスが表示されない場合は、信頼を右クリックし、 * クレーム発行ポリシーの編集 * を選択します。

6. ［ クレームルール ］ ウィザードを開始するには、 ［ * ルールの追加 * ］ を選択します。

   a. ［ ルールテンプレートの選択 ］ ページで、リストから ［ * LDAP 属性をクレームとして送信 * ］ を選択し、 ［ * 次へ * ］ を選択します。

   b. ［ ルールの設定 ］ ページで、このルールの表示名を入力します。

      たとえば、* ObjectGUID to Name ID*または* UPN to Name ID*などです。

   c. 属性ストアで、 * Active Directory * を選択します。

   d. [マッピング]テーブルの[LDAP属性]列に「* objectGUID 」と入力するか、[ユーザープリンシパル名]*を選択します。

   e. マッピングテーブルの発信クレームタイプ列で、ドロップダウンリストから * 名前 ID * を選択します。

f. 「完了」を選択し、「 * OK 」を選択します。

7. 証明書利用者信頼を右クリックしてプロパティを開きます。
8. [* Endpoints] タブで、シングルログアウト（ SLO ）のエンドポイントを設定します。
   a. 「 * SAML を追加」を選択します。
   b. [* Endpoint Type*>*SAML Logout*] を選択します。
   c. 「 * Binding * > * Redirect * 」を選択します。
   d. [**Trusted URL**] フィールドに、この管理ノードからのシングルログアウト（ SLO ）に使用する URL を入力します。

      `https://Admin_Node_FQDN/api/saml-logout`

   には *Admin_Node_FQDN*、管理ノードの完全修飾ドメイン名を入力します。（必要に応じて、ノードの IP アドレスを代わりに使用できます。ただし、 IP アドレスを入力した場合、その IP アドレスが変わったときには証明書利用者信頼を更新または再作成する必要があります）。

   a. 「* OK *」を選択します。
9. [* Signature*] タブで、この証明書利用者信頼の署名証明書を指定します。
   a. カスタム証明書を追加します。
      - StorageGRID にアップロードしたカスタム管理証明書がある場合は、その証明書を選択します。
      - カスタム証明書がない場合は、管理ノードにログインし、管理ノードのディレクトリに移動して `/var/local/mgmt-api`証明書ファイルを追加し `custom-server.crt`ます。

        管理ノードのデフォルト証明書を使用する(`server.crt`ことは推奨されません。管理ノードで障害が発生した場合、ノードをリカバリする際にデフォルトの証明書が再生成されるため、証明書利用者信頼を更新する必要があります。

   b. [* 適用（ Apply ）] を選択し、 [* OK] を選択します。

      証明書利用者のプロパティが保存されて閉じられます。
10. 上記の手順を繰り返して、 StorageGRID システム内のすべての管理ノードに対して証明書利用者信頼を設定します。
11. 完了したら、StorageGRID に戻り、"すべての証明書利用者信頼をテストする"正しく設定されていることを確認してください。

StorageGRID の **SAML** 用に **Entra ID** でエンタープライズアプリケーションを作成する

Entra IDを使用して、システム内のSAML用管理ノードごとにエンタープライズアプリケーションを作成します。

開始する前に

- StorageGRIDのシングル サインオンの構成を開始し、SSO タイプとして **Entra ID** を選択しました。
- Grid Manager に "サンドボックスモードに入りました" があります。
- システム内の各管理ノードには エンタープライズ アプリケーション名 があります。これらの値

は、「SSO の構成」ページの管理ノードの詳細テーブルからコピーできます。

> StorageGRID システムで管理ノードごとにエンタープライズアプリケーションを作成する必要があります。管理ノードごとにエンタープライズアプリケーションを用意することで、ユーザはどの管理ノードに対しても安全にサインイン / サインアウトすることができます。

- Entra ID でエンタープライズ アプリケーションを作成した経験があります。
- 有効なサブスクリプションを持つ Entra ID アカウントをお持ちです。
- Entra ID アカウントには、グローバル管理者、クラウド アプリケーション管理者、アプリケーション管理者、またはサービス プリンシパルの所有者のいずれかのロールがあります。

ステップ**1**：**Entra ID** にアクセスする

手順

1. にログインし "Azure ポータル"ます。
2. 移動先 "エントラID"。
3. を選択します "エンタープライズアプリケーション"。

ステップ**2**：エンタープライズアプリケーションを作成し、**StorageGRID SSO**構成を保存する

Entra ID の SSO 構成をStorageGRIDに保存するには、Entra ID を使用して各管理ノードのエンタープライズアプリケーションを作成する必要があります。 Entra ID からフェデレーション メタデータ URL をコピーし、[SSO の構成] ページの対応する フェデレーション メタデータ **URL** フィールドに貼り付けます。

手順

1. 管理ノードごとに次の手順を繰り返します。
   a. Entra ID Enterprise アプリケーション ペインで、新しいアプリケーション を選択します。
   b. 「 * 独自のアプリケーションを作成する * 」を選択します。
   c. 名前には、[SSO の構成] ページの管理ノードの詳細テーブルからコピーした エンタープライズ アプリケーション名 を入力します。
   d. ギャラリー (ギャラリー以外) で見つからない他のアプリケーションを統合 * ラジオボタンを選択したままにします。
   e. 「 * Create * 」を選択します。
   f. 2 の * Get started * リンクを選択します。シングルサインオン * ボックスを設定するか、左マージンの * シングルサインオン * リンクを選択します。
   g. [* SAML *] ボックスを選択します。
   h. 「 * アプリフェデレーションメタデータ URL * 」をコピーします。この URL は「 * ステップ 3 SAML 署名証明書 * 」にあります。
   i. [SSO の構成] ページに移動し、使用した エンタープライズ アプリケーション名 に対応する フェデレーション メタデータ **URL** フィールドに URL を貼り付けます。
2. 各管理ノードのフェデレーション メタデータ URL を貼り付け、SSO 構成に必要なその他の変更をすべて行った後、[SSO の構成] ページで [保存] を選択します。

ステップ**3**：各管理ノードの**SAML**メタデータをダウンロードする

SSO 設定を保存したら、 StorageGRID システム内の管理ノードごとに SAML メタデータファイルをダウンロードできます。

手順

1. 管理ノードごとに上記の手順を繰り返します。
   a. 管理ノードから StorageGRID にサインインします。
   b. 構成 > アクセス制御 > シングル サインオン を選択します。
   c. ボタンを選択して、その管理ノードの SAML メタデータをダウンロードします。
   d. Entra ID にアップロードするファイルを保存します。

ステップ**4**：**SAML**メタデータを各エンタープライズアプリケーションにアップロードする

各StorageGRID管理ノードの SAML メタデータ ファイルをダウンロードした後、Entra ID で次の手順を実行します。

手順

1. Azure ポータルに戻ります。
2. エンタープライズアプリケーションごとに、次の手順を繰り返します。

   以前にリストに追加したアプリケーションを表示するには、 [エンタープライズアプリケーション] ページの更新が必要な場合があります。

   a. エンタープライズアプリケーションのプロパティページに移動します。
   b. [Assignment Required*] を [**No**] に設定します（個別に割り当てを設定する場合を除く）。
   c. シングルサインオンページに移動します。
   d. SAML の設定を完了します。
   e. メタデータファイルのアップロードボタンを選択し、対応する管理ノード用にダウンロードした SAML メタデータファイルを選択します。
   f. ファイルがロードされたら、「 * 保存」を選択し、「 * X * 」を選択してパネルを閉じます。SAML を使用してシングルサインオンを設定するページに戻ります。
3. "各アプリケーションをテストする"。

StorageGRID の **SAML** 用に **PingFederate** でサービスプロバイダー接続を作成する

PingFederate を使用して、システム内の SAML 用の各管理ノードのサービスプロバイダー （SP） 接続を作成します。処理を高速化するために、StorageGRID から SAML メタデータをインポートします。

開始する前に

- StorageGRID にシングルサインオンを設定し、 SSO タイプとして「 Ping federate * 」を選択しました。
- Grid Manager に "サンドボックスモードに入りました" があります。

- システム内の各管理ノードには * SP接続 ID* があります。これらの値は、「SSO の構成」ページの「管理ノード」の詳細テーブルで確認できます。
- システムの管理ノードごとに * SAML メタデータ * をダウンロードしておきます。
- PingFederate サーバーで SP 接続を作成した経験があります。
- PingFederateサーバ用のがありhttps://docs.pingidentity.com/pingfederate/latest/administrators_reference_guide/pf_administrators_reference_guide.html["管理者向けリファレンスガイド"^]ます。PingFederate ドキュメントでは、詳細な手順と説明を説明しています。
- あなたは"管理者権限"PingFederate サーバー用。

タスクの内容

ここでは、 StorageGRID の SSO プロバイダとして PingFederate Server バージョン 10.3 を設定する方法を簡単に説明します。別のバージョンの PingFederate を使用している場合は、これらの指示を適用する必要があります。ご使用のリリースの詳細な手順については、 PingFederate Server のマニュアルを参照してください。

PingFederate の前提条件を完了します

StorageGRID に使用する SP 接続を作成する前に、 PingFederate で前提条件のタスクを完了する必要があります。SP 接続を設定するときは、これらの前提条件の情報を使用します。

データストアの作成**[[data-store]**

まだ作成していない場合は、 PingFederate を AD FS LDAP サーバーに接続するデータストアを作成します。StorageGRIDで使用した値を使用し"アイデンティティフェデレーションの設定"ます。

- * タイプ * ：ディレクトリ（ LDAP ）
- * LDAP タイプ * ： Active Directory
- * バイナリ属性名 *: 「 LDAP バイナリ属性」タブに * objectGUID * を正確に入力します。

パスワードクレデンシャルバリデータの作成

パスワード認証情報バリデータをまだ作成していない場合は、作成します。

- * 「 * 」と入力します。 LDAP ユーザ名パスワード資格情報検証ツール
- * データストア *: 作成したデータストアを選択します。
- * 検索ベース * ： LDAP から情報を入力します（例： DC=SAML 、 DC=sgws ）。
- * 検索フィルタ * ： sAMAccountName = $ ｛ userName ｝
- * スコープ * ：サブツリー

IdPアダプタインスタンス**[**アダプタインスタンス**]**を作成します

IdP アダプタのインスタンスをまだ作成していない場合は作成します。

手順

1. 「 * 認証 * > * 統合 * > * IdP アダプタ * 」に移動します。

2. [新規インスタンスの作成（ Create New Instance ）] を選択します
3. [タイプ] タブで、 [* HTML フォーム IdP アダプタ *] を選択します。
4. [IdP アダプタ] タブで、 [資格情報検証ツール] に新しい行を追加する *] を選択します。
5. 選択してくださいパスワードクレデンシャルバリデータあなたが作成したもの。
6. [アダプタの属性] タブで、 **pseudonym** * の ***username** 属性を選択します。
7. [保存（ Save ）] を選択します。

署名証明書の作成またはインポート**[signing-certificate]**

署名証明書を作成またはインポートしていない場合は、作成します。

手順

1. 「 * Security * > * Signing & Decryption keys & Certificates * 」に移動します。
2. 署名証明書を作成またはインポートします。

PingFederate で **SP** 接続を作成します

PingFederate で SP 接続を作成すると、管理ノード用に StorageGRID からダウンロードした SAML メタデータがインポートされます。メタデータファイルには、必要な値の多くが含まれています。

> ユーザが任意のノードに対して安全にサインインおよびサインアウトできるように、StorageGRID システム内の管理ノードごとに SP 接続を作成する必要があります。次の手順に従って、最初の SP 接続を作成します。次に、に進み、追加の SP 接続を作成します必要な追加の接続を作成します。

SP 接続タイプを選択します

手順

1. [* アプリケーション * > * 統合 * > * SP 接続 *] に移動します。
2. [接続の作成 *] を選択します。
3. 「 * この接続にテンプレートを使用しない * 」を選択します。
4. ブラウザ SSO プロファイル * および * SAML 2.0 * をプロトコルとして選択します。

SP メタデータをインポートします

手順

1. メタデータのインポートタブで、 * ファイル * を選択します。
2. 管理ノードの SSO の構成ページからダウンロードした SAML メタデータ ファイルを選択します。
3. [Metadata Summary]と[General Info]タブに表示される情報を確認します。

   パートナーのエンティティ ID と接続名は、 StorageGRID SP 接続 ID に設定されています。（例： 10.96.105.200-DC1-ADM1-105-200 ）。ベース URL は、 StorageGRID 管理ノードの IP です。

4. 「 * 次へ * 」を選択します。

IdP ブラウザの SSO を設定する

手順

1. ブラウザ SSO タブで、 * ブラウザ SSO の設定 * を選択します。
2. SAML プロファイルタブで、 * SP が開始した SSO * 、 * SP - 初期 SLO * 、 * IdP が開始した SSO * 、および * IdP によって開始された SLO * オプションを選択します。
3. 「 * 次へ * 」を選択します。
4. [Assertion Lifetime （アサーションの有効期間）] タブで、変更を行いません。
5. [アサーションの作成] タブで、 [* アサーションの作成の設定 *] を選択します。
   a. [ID マッピング] タブで、 [* 標準 *] を選択します。
   b. [属性契約（ Attribute Contract ）] タブで、属性契約として * sama_subject * を使用し、インポートされた名前形式を指定しません。
6. [Extend the Contract]で、*[Delete]*を選択して、使用されていないを削除し `urn:oid`ます。

アダプタインスタンスをマッピングします

手順

1. [Authentication Source Mapping] タブで、 [* Map New Adapter Instance] を選択します。
2. [Adapter instance]タブで、作成したを選択しアダプタインスタンスます。
3. [マッピング方法] タブで、 [データストアから追加属性を取得する *] を選択します。
4. [属性ソースとユーザールックアップ] タブで、 [属性ソースの追加] を選択します。
5. [Data Store]タブで、説明を入力し、追加したを選択しますデータストア。
6. LDAP ディレクトリ検索タブで、次の手順を実行します。
   - 「 * ベース DN * 」を入力します。この DN は、 LDAP サーバの StorageGRID で入力した値と完全に一致している必要があります。
   - 検索範囲（ Search Scope ）で、 * サブツリー * （ * Subtree * ）を選択します。
   - [ルートオブジェクトクラス]で、*objectGUID*または*userPrincipalName*のいずれかの属性を検索して追加します。
7. [LDAP Binary Attribute Encoding Types] タブで、 *objectGUID * 属性として *Base64 * を選択します。
8. LDAP Filter タブで、 * sAMAccountName = $ ｛ userName ｝ * と入力します。
9. [Attribute Contract Fulfillment]タブで、[Source]ドロップダウンから*を選択し、**[Value]**ドロップダウンから objectGUID または userPrincipalName *を選択します。
10. 属性ソースを確認して保存します。
11. Failsave Attribute Source タブで、 * Abort the SSO Transaction * を選択します。
12. 概要を確認し、「 * Done * 」を選択します。
13. 「 Done （完了）」を選択します。

プロトコルを設定します

手順

1. * SP Connection * > * Browser SSO * > * Protocol Settings * タブで、 * Configure Protocol Settings * を選択します。
2. [アサーションコンシューマサービスURL]タブで、StorageGRID SAMLメタデータからインポートされたデフォルト値を受け入れます（バインドの場合は* POST 、エンドポイント**URL**の場合は `/api/saml-response`）。
3. [SLOサービスURLs]タブで、StorageGRID SAMLメタデータ（バインドの場合は* redirect*、エンドポイントURLの場合は* redirect*）からインポートされたデフォルト値を受け入れます `/api/saml-logout`。
4. [Allowable SAML Bindings]タブで、[**artifact**]および[**SOAP**]を選択解除します。必要なのは、 * POST * および * redirect * のみです。
5. [Signature Policy]タブで、[* Require Authn Requests to be Signed]チェックボックスと[* Always Sign Assertion]チェックボックスをオンのままにします。
6. ［ 暗号化ポリシー ］ タブで、 ［ * なし * ］ を選択します。
7. 概要を確認し、「 * Done * 」を選択してプロトコル設定を保存します。
8. 概要を確認し、「完了」を選択して、ブラウザ SSO 設定を保存します。

クレデンシャルを設定

手順

1. ［ SP 接続 ］ タブで ' ［ * 資格情報 * ］ を選択します
2. 資格情報タブで、 * 資格情報の設定 * を選択します。
3. 選択してください署名証明書作成またはインポートした。
4. 「 * 次へ * 」を選択して、「 * 署名検証設定の管理 * 」に移動します。
   a. [信頼モデル] タブで、 [*Unanchored] を選択します。
   b. [Signature Verification Certificate] タブで、 StorageGRID SAML メタデータからインポートした署名証明書情報を確認します。
5. 概要画面を確認し、 ［ * 保存 * ］ を選択して SP 接続を保存します。

追加の **SP** 接続を作成します

最初の SP 接続をコピーして、グリッド内の管理ノードごとに必要な SP 接続を作成できます。コピーごとに新しいメタデータをアップロードします。

> 異なる管理ノードの SP 接続では、パートナーのエンティティ ID 、ベース URL 、接続 ID 、接続名、署名の検証を除き、同じ設定を使用します。 と SLO 応答 URL 。

手順

1. * Action * > * Copy * を選択して、追加の管理ノードごとに最初の SP 接続のコピーを作成します。
2. コピーの接続 ID と接続名を入力し、 * 保存 * を選択します。
3. 管理ノードに対応するメタデータファイルを選択します。
   a. 「 * アクション * > * メタデータで更新 * 」を選択します。
   b. 「 * ファイルを選択」を選択し、メタデータをアップロードします。

c. 「 * 次へ * 」を選択します。

d. [保存（ Save ）] を選択します。

4. 未使用の属性によるエラーを解決します。

a. 新しい接続を選択します。

b. ブラウザ SSO の設定 > アサーションの作成の設定 > 属性契約 * を選択します。

c. urn ： Oid * のエントリを削除します。

d. [保存（ Save ）] を選択します。

StorageGRIDでSSOを無効にする

不要になった場合はシングルサインオン（ SSO ）を無効にすることができます。アイデンティティフェデレーションを無効にする場合は、事前にシングルサインオンを無効にする必要があります。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- そうだな "特定のアクセス権限"

手順

1. 構成 > アクセス制御 > シングル サインオン を選択します。

   [Single Sign-On] ページが表示されます。

2. 「無効にする」を選択します。
3. 「 * はい * 」を選択します。

   ローカルユーザがサインインできるようになったことを示す警告メッセージが表示されます。

次回 StorageGRID にサインインすると、 StorageGRID のサインインページが表示され、ローカルユーザまたはフェデレーテッド StorageGRID ユーザのユーザ名とパスワードを入力する必要があります。

StorageGRID 管理ノードの SSO を一時的に無効にして再度有効にします

シングルサインオン（ SSO ）システムが停止すると、 Grid Manager にサインインできない場合があります。この場合は、 1 つの管理ノードに対して SSO を一時的に無効にしてから再度有効にすることができます。SSO を無効にしてから再度有効にするには、ノードのコマンドシェルにアクセスする必要があります。

開始する前に

- そうだな "特定のアクセス権限"
- あなたはファイルを持ってい `Passwords.txt`ます。
- ローカルの root ユーザのパスワードを確認しておきます。

タスクの内容

1 つの管理ノードに対して SSO を無効にすると、ローカルの root ユーザとして Grid Manager にサインインできます。StorageGRID システムを保護するために、ノードのコマンドシェルを使用してサインアウト後すぐに管理ノードの SSO を再度有効にする必要があります。

1 つの管理ノードに対して SSO を無効にしても、グリッド内の他の管理ノードの SSO 設定には影響しません。Grid Managerの[Single Sign-on]ページの[Enable SSO]*チェックボックスは選択されたままになり、既存のSSO設定は更新しないかぎり維持されます。

手順

1. 管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@Admin_Node_IP`
   b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

      rootとしてログインすると、プロンプトがからに `#`変わります `$`。

2. SSO の設定に応じて、次のいずれかのコマンドを実行します。

   SAML

   `disable-saml`

   OIDC

   `disable-oidc`

   環境 this admin Node only コマンドのメッセージが表示されます。

3. SSO を無効にすることを確認します。

   ノードでシングルサインオンが無効になったことを示すメッセージが表示されます。

4. Web ブラウザから、同じ管理ノード上の Grid Manager にアクセスする。

   SSO を無効にしたため、 Grid Manager のサインインページが表示されます。

5. ユーザ名「 root 」とローカルの root ユーザのパスワードを使用してサインインします。
6. SSO 設定の修正が必要なために SSO を一時的に無効にした場合は、次の手順を実行します
   a. 構成 > アクセス制御 > シングル サインオン を選択します。
   b. 正しくない SSO 設定または古い SSO 設定を変更します。
   c. [保存（ Save ）] を選択します。

      シングルサインオンページから * Save * を選択すると、グリッド全体で SSO が自動的に再有効化されます。

7. 他の理由で Grid Manager へのアクセスが必要であったために SSO を一時的に無効にした場合は、次の手

順を実行します。

a. 必要なタスクを実行します。
b. [サインアウト]*を選択し、Grid Managerを閉じます。
c. 管理ノードで SSO を再度有効にします。次のいずれかの手順を実行します。

- 次のコマンドを実行します。 `enable-saml`

  環境 this admin Node only コマンドのメッセージが表示されます。

SSO を有効にすることを確認します。

ノードでシングルサインオンが有効になったことを示すメッセージが表示されます。

- グリッドノードをリブートします。 `reboot`

8. Web ブラウザから、同じ管理ノードから Grid Manager にアクセスする。
9. StorageGRID のサインインページが表示され、グリッドマネージャにアクセスするには SSO クレデンシャルを入力する必要があることを確認します。

複数管理者による認証を使用する

StorageGRID マルチ管理者検証について

StorageGRID管理者は、マルチ管理者検証（MAV）を使用して、特定の操作が指定された管理者の承認後にのみ実行されるようにすることができます。MAVは、StorageGRIDシステムへの偶発的または不正な変更を防ぐのに役立ちます。

MAVはデフォルトでは無効になっています。

MAV構成 - 概要

MAVを設定するには、以下のタスクを実行します：

- 1つ以上の管理者グループを作成します。MAVの管理者は承認権限と拒否権限を持ちます。
- 複数管理者による認証機能を有効にします。
- 保護された操作のセットから選択します。

初期設定を実行したり、後で変更を加えたりするには、ユーザーはルートアクセス権限を持っている必要があります。

MAVにおける保護された操作の処理方法

MAVが有効になっている場合、保護されたすべての操作を完了するには、以下の手順が必要です：

1. ユーザーが操作を開始すると、リクエストが生成されます。
2. 操作を実行する前に、少なくとも1名のMAV管理者の承認が必要です。
3. 承認されると、MAV保護された操作は自動的に実行されます。

StorageGRID マルチ管理者検証（MAV）システムの設定には、MAV 管理者グループとユーザーの作成および管理、MAV 機能の有効化、保護対象操作の選択または構成が含まれます。

MAVの管理者は、保護された操作に対して承認権限と拒否権限を持ちます。

開始する前に

- あなたはを持っています"rootアクセス権限"。
- プライマリ管理ノードからGrid Managerにサインインしています。

ステップ1：MAV管理者グループとユーザーを作成する

既存の管理者をMAVグループに追加するか、または新しい管理者を作成できます。

Active Directory (AD) ユーザーを MAV 管理者として構成できます。AD ユーザーは StorageGRID 管理者として構成する必要があります。

手順

1. MAV管理者グループを作成するには、"ローカルグループまたはフェデレーテッドグループを作成する"の手順に従ってください。
2. グループ権限については、**Root access** または **Multi-admin verification requests** を選択してください。
3. ローカルユーザーまたはフェデレーションユーザーをグループに追加するか、新しいローカルユーザーを作成して、"ローカルユーザーを作成する"の手順に従ってグループに追加します。

ステップ2：MAVを有効または無効にする

マルチ管理者認証（MAV）を明示的に有効にする必要があります。MAVが有効になっている状態で、保留中のMAVリクエストがある場合にMAVを無効にすると、保留中のリクエストが削除される旨の通知が表示されます。

手順

1. **Configuration** > **Access control** > **Multi-admin verification** > **MAV settings** を選択します。
2. 複数管理者による認証を有効にするには、「MAV を有効にする」チェックボックスを選択してください。
3. 承認者グループセクションには、MAV管理者グループと承認者が一覧表示されます。
4. 「操作」セクションで、MAVで保護する操作のチェックボックスを選択します。
5. （オプション）保留中の承認リクエストについて MAV 管理者に通知するためにメール通知を使用する場合：
   a. メールサーバーを設定していない場合は、次の手順に従ってください："メールサーバーの設定"。
   b. 送信者のメールアドレスを入力してください。
   c. メール通知の受信者を1人以上入力してください。
6. 変更を保存するには、*保存*を選択してください。

メール通知を設定しない場合、MAV管理者はGrid Managerダッシュボードを表示したり、承認キューで保留中の承認リクエストを確認したりできます。承認キューを確認するには、複数管理者認証ページで「その他のリクエスト」を選択してください。

ステップ**3**：保護された操作を管理する

複数管理者による認証を有効にすると、MAVで保護する操作のチェックボックスをオンまたはオフにすることで、保護対象の操作を管理できます。

StorageGRID 12.1 では、保護される操作は ILM ポリシーの有効化のみです。MAV を有効にする場合は、ILM ポリシーの有効化のチェックボックスを選択する必要があります。

MAVリクエストには、以下のいずれかのステータスがあります：

- 保留中。リクエストが開始されました。
- 期限切れ。リクエストは30日以内に対応されませんでした。または、Root アクセス権限を持つユーザーが MAV を無効にした場合、保留中のすべてのリクエストが期限切れになります。
- 取り下げ済み。ユーザーがリクエストを取り下げました。
- 承認済み。MAV管理者が保留中のリクエストを承認しました。
- 却下されました。MAV管理者が保留中のリクエストを却下しました。

MAVメール通知のトラブルシューティング

MAV管理者が保留中のリクエストに関するメール通知を受信しない場合は、以下の手順に従って問題を解決してください。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"アラートまたはRoot Access権限を管理します。"。

手順

1. 設定を確認します。
   a. 設定 > 監視 > メールサーバー を選択します。
   b. E メール（ SMTP ）サーバの設定が正しいことを確認します。
   c. 受信者の有効な E メールアドレスが指定されていることを確認します。
2. スパムフィルタを確認し、 E メールが迷惑メールフォルダに送信されていないことを確認します。
3. メール管理者に問い合わせて、送信者アドレスからのメールがブロックされていないことを確認してください。
4. 管理ノードのログファイルを収集し、テクニカルサポートに連絡します。

   テクニカルサポートは、ログの情報を参考に問題の原因を特定します。たとえば、指定したサーバに接続するときに、 prometheus.log ファイルにエラーが表示されることがあります。

   "ログファイルとシステムデータを収集"を参照してください。

StorageGRID で**MAV**で保護された操作の承認を申請する

StorageGRID の管理者またはユーザーとして、MAV で保護された操作を StorageGRID で開始すると、リクエストが自動的に生成されます。操作には承認が必要であることを知らせるメッセージが表示されます。

StorageGRID システムは、MAV によって保護される操作を定義します。MAV で保護された操作を開始すると、承認のために MAV 管理者へリクエストが送信されます。

手順

StorageGRID システムは、MAV で保護された操作を開始したことを通知します。

1. 必要に応じて、以下のいずれかの作業を実行してください。
   a. **Configuration** > **Access control** > **Multi-admin verification** > **My requests** を選択して、リクエストのステータスを確認してください。
      - 保留中。リクエストが開始されました。
      - 期限切れ。リクエストは30日以内に対応されませんでした。または、Root アクセス権限を持つユーザーが MAV を無効にした場合、保留中のすべてのリクエストが期限切れになります。
      - 取り下げ済み。ユーザーがリクエストを取り下げました。
      - 承認済み。MAV管理者が保留中のリクエストを承認しました。
      - 却下されました。MAV管理者が保留中のリクエストを却下しました。
   b. **Configuration** > **Access control** > **Multi-admin verification** > **Other requests** を選択して、他のユーザーの保留中のリクエストを確認してください。
   c. 操作をキャンセルするには、マイリクエスト > キャンセルしたいリクエスト > 取り消し を選択します。

MAV管理者がリクエストを承認すると、操作は自動的に実行されます。

リクエストが却下された場合、操作は実行されません。必要に応じて、新しいリクエストを送信できます。

StorageGRID で **MAV** で保護された操作リクエストを管理する

MAV 管理者として、StorageGRID で MAV で保護された操作のリクエストを管理できます。自分または他のユーザーの保留中のリクエストを表示したり、リクエストを承認または拒否したり、過去のリクエスト履歴を表示したりできます。

開始する前に

- あなたは MAV 管理者グループに属しており、"rootアクセス権限" を持っています。
- プライマリ管理ノードからGrid Managerにサインインしています。

手順

1. MAVリクエストに関するメール通知を受け取った場合は、「Configuration」>「Multi-admin verification」>「Other requests」を選択してください。

   さらに、グリッドマネージャーのダッシュボードには、保留中のMAVリクエストに関する通知が表示されます。

2. 管理する各リクエストのラジオボタンを選択してください。
3. 選択したリクエストを承認または拒否するには、*承認*または*拒否*を選択してください。
4. 過去のリクエスト履歴を表示するには、*履歴*を選択してください。

グリッドフェデレーションを使用する

StorageGRID グリッド フェデレーションについて学ぶ

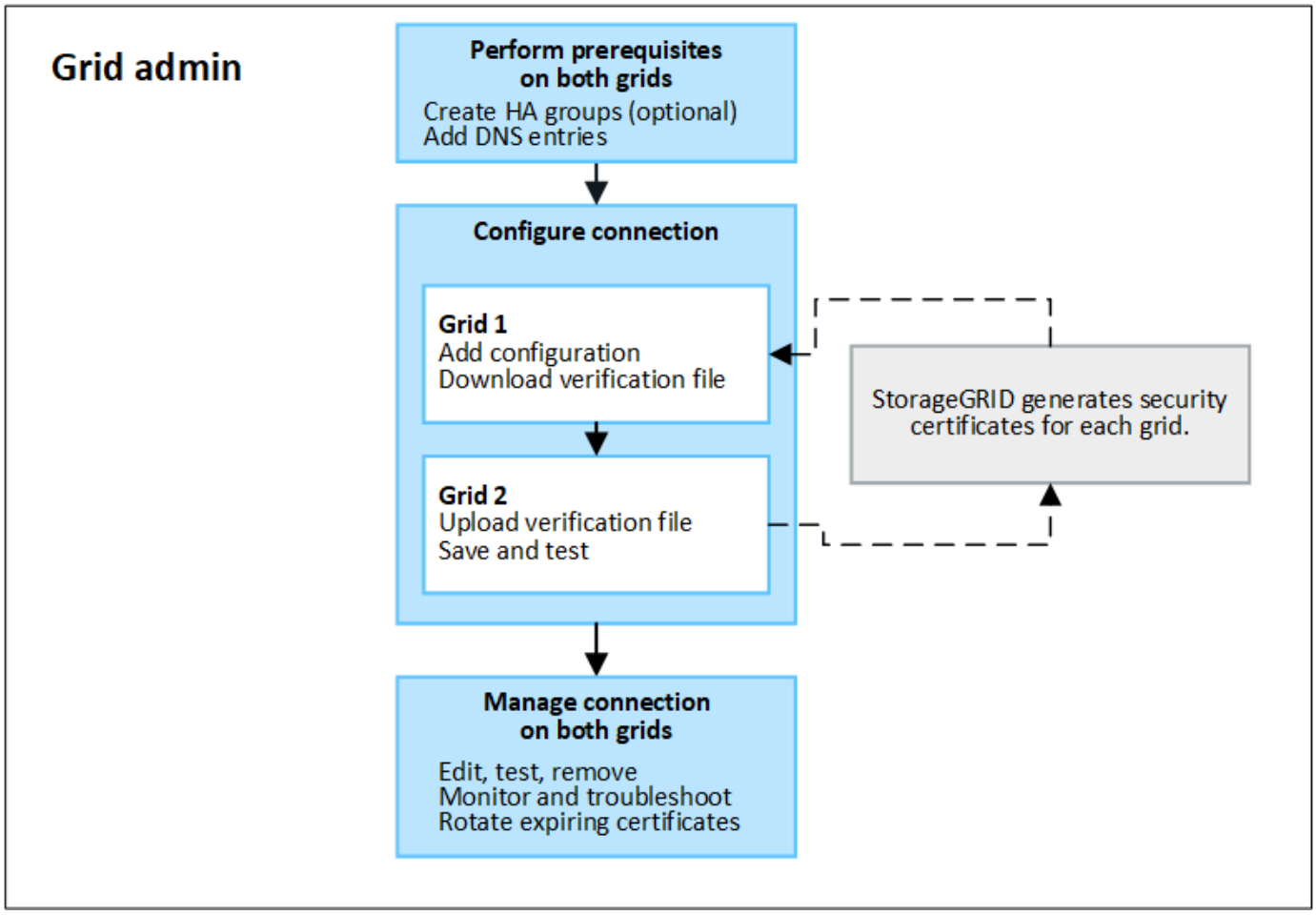
グリッドフェデレーションを使用すると、テナントを同期し、ディザスタリカバリのために複数の StorageGRID システム間でオブジェクトをレプリケートできます。

グリッドフェデレーション接続とは何ですか？

グリッドフェデレーション接続は、2つのStorageGRID システムの管理ノードとゲートウェイノードの間の双方向の信頼されたセキュアな接続です。

グリッドフェデレーションのワークフロー

次のワークフロー図は、2つのグリッド間のグリッドフェデレーション接続を設定する手順をまとめたものです。



- グリッドフェデレーションに使用されるグリッドでは、同じバージョンのが実行されているか、メジャーバージョンの違いが1つ以上ないStorageGRIDが実行されている必要があります。

  バージョン要件の詳細については、 "リリースノート"を参照してください。NetAppアカウントでサインインするか、アカウントを作成してリリースノートにアクセスする必要があります。

- グリッドは、他のグリッドへの1つ以上のグリッドフェデレーション接続を持つことができます。各グリッドフェデレーション接続は、他の接続とは独立しています。たとえば、Grid 1がGrid 2と1つの接続を持ち、Grid 3と2つ目の接続を持つ場合、Grid 2とGrid 3の間に暗黙的な接続はありません。
- グリッドフェデレーション接続は双方向です。接続が確立されたら、どちらのグリッドからも接続を監視および管理できます。
- "アカウント同期"または"グリッド間レプリケーション"を使用するには、グリッドフェデレーション接続が少なくとも1つ存在する必要があります。

ネットワークとIPアドレスの要件

- グリッドフェデレーション接続は、グリッドネットワーク、管理ネットワーク、またはクライアントネットワークで確立できます。
- グリッドフェデレーション接続は、あるグリッドを別のグリッドに接続します。各グリッドの設定では、管理ノード、ゲートウェイノード、またはその両方で構成されるもう一方のグリッド上のグリッドフェデレーションエンドポイントを指定します。
- ベストプラクティスとして、ゲートウェイノードと管理ノードを各グリッドで接続することを推奨"ハイアベイラビリティ（HA）グループ"します。HAグループを使用すると、ノードを使用できなくなってもグリッドフェデレーション接続をオンラインのまま維持できます。いずれかのHAグループのアクティブインターフェイスで障害が発生した場合は、バックアップインターフェイスを使用して接続を確立できます。
- 単一の管理ノードまたはゲートウェイノードのIPアドレスを使用するグリッドフェデレーション接続を作成することは推奨されません。ノードが使用できなくなると、グリッドフェデレーション接続も使用できなくなります。
- "グリッド間レプリケーション"オブジェクトの数を増やすには、各グリッドのストレージノードが、もう一方のグリッドに設定されている管理ノードとゲートウェイノードにアクセスできる必要があります。グリッドごとに、すべてのストレージノードが、接続に使用する管理ノードまたはゲートウェイノードとしてへの広帯域幅ルートを持っていることを確認します。

FQDNを使用して接続の負荷を分散します

本番環境では、Fully Qualified Domain Name（FQDN；完全修飾ドメイン名）を使用して接続内の各グリッドを識別します。次に、次のように適切なDNSエントリを作成します。

- Grid 1のFQDNを、Grid 1のHAグループの1つ以上の仮想IP（VIP）アドレス、またはGrid 1の1つ以上の管理ノードまたはゲートウェイノードのIPアドレスにマッピングします。
- Grid 2のFQDNを、Grid 2の1つ以上のVIPアドレス、またはGrid 2内の1つ以上の管理ノードまたはゲートウェイノードのIPアドレスにマッピングします。

複数のDNSエントリを使用する場合、接続を使用する要求は次のようにロードバランシングされます。

- 複数のHAグループのVIPアドレスにマッピングされたDNSエントリは、HAグループ内のアクティブノード間で負荷分散されます。

- 複数の管理ノードまたはゲートウェイノードのIPアドレスにマッピングされたDNSエントリは、マッピングしたノード間で負荷分散されます。

ポートの要件

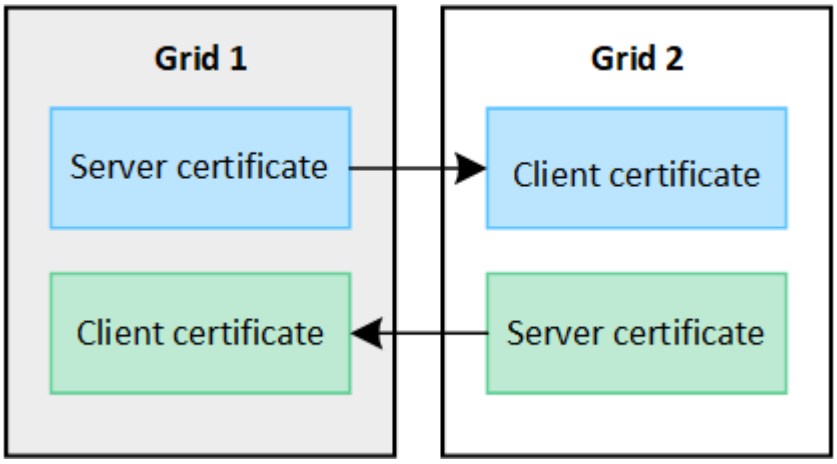
グリッドフェデレーション接続を作成するときは、未使用のポート番号（23000~23999）を指定できます。この接続の両方のグリッドが同じポートを使用します。

どちらのグリッドでも、このポートを他の接続に使用しているノードがないことを確認する必要があります。

証明書の要件

グリッドフェデレーション接続を設定すると、StorageGRID によって次の4つのSSL証明書が自動的に生成されます。

- グリッド1からグリッド2に送信される情報を認証および暗号化するためのサーバ証明書とクライアント証明書
- グリッド2からグリッド1に送信される情報を認証および暗号化するためのサーバ証明書とクライアント証明書



デフォルトでは、証明書の有効期間は730日間（2年間）です。これらの証明書の有効期限が近づくと、* Expiration of grid federation certificate *アラートによって証明書のローテーションを要求されます。これはGrid Managerを使用して実行できます。

> 接続のいずれかの側の証明書が期限切れになると、接続は動作を停止します。証明書が更新されるまで、データレプリケーションは保留されます。

詳細

- "グリッドフェデレーション接続を作成する"
- "グリッドフェデレーション接続を管理します"
- "グリッドフェデレーションエラーをトラブルシューティングする"

StorageGRID のアカウント同期について

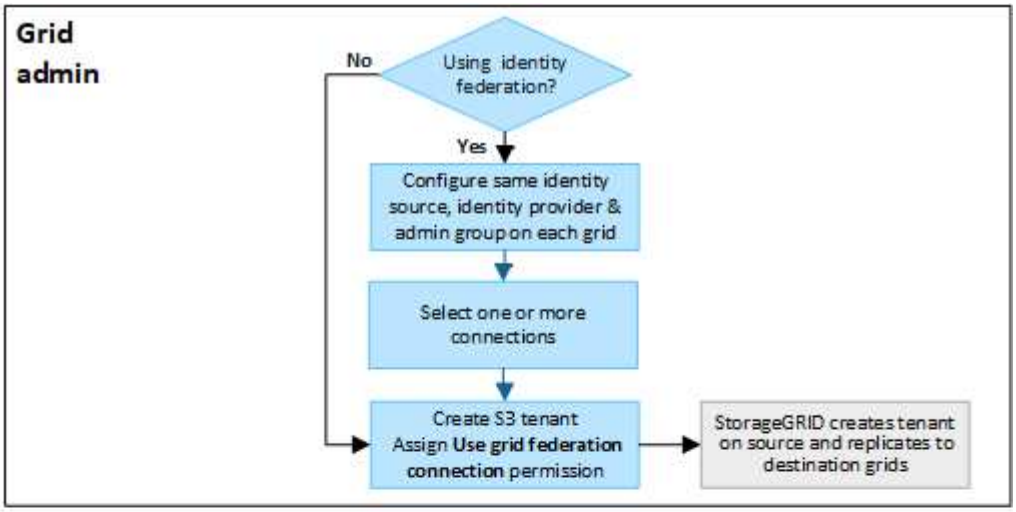
アカウント同期とは、1つ以上の"グリッドフェデレーション接続"内のStorageGRIDシステム間で、テナントアカウント、テナントグループ、テナントユーザー、およびオプシ

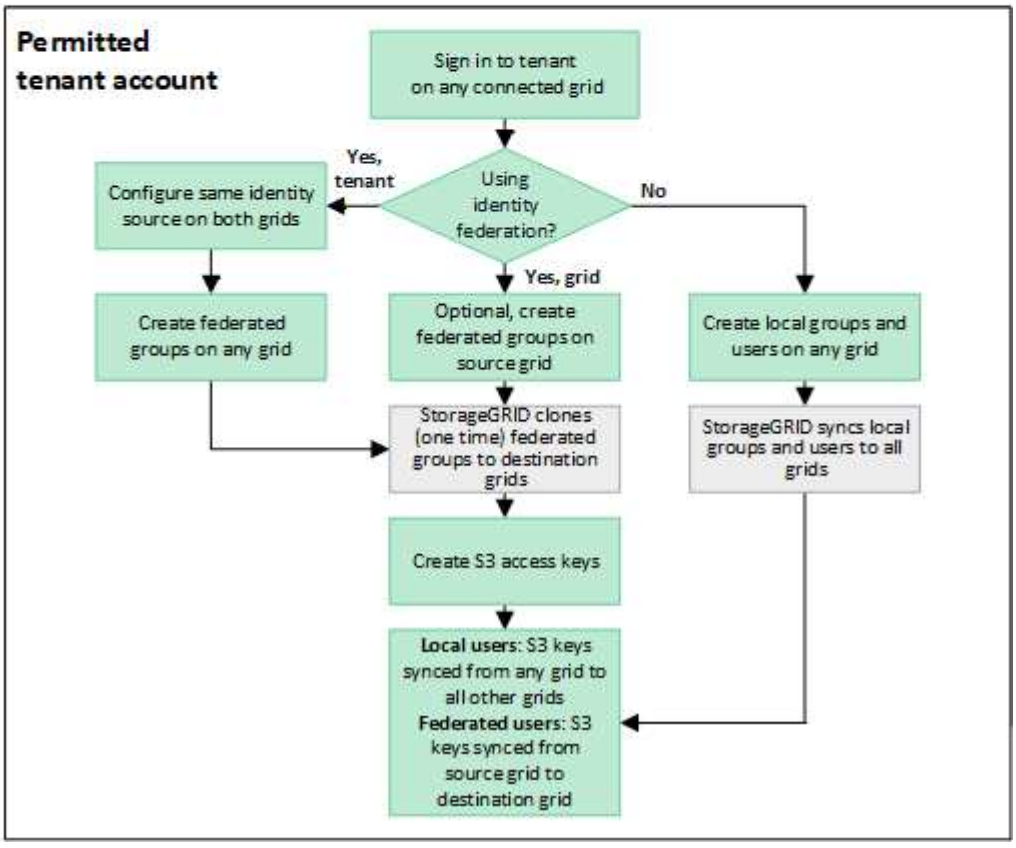
ョンでS3アクセスキーを自動的かつ継続的に連続レプリケーションすることです。

"グリッド間レプリケーション"にはアカウント同期が必要です。StorageGRID システム間でアカウント情報を同期することで、テナントのユーザーとグループが、接続されている任意のグリッド上の対応するバケットとオブジェクトにアクセスできるようになります。

アカウント同期のワークフロー

ワークフロー図は、グリッド管理者と許可されたテナントがアカウント同期を設定するために実行する手順を示しています。これらの手順は、"グリッドフェデレーション接続が設定されました"の後に実行されます。





グリッド管理者が実行する手順は、のStorageGRIDシステムでシングルサインオン（SSO）を使用するかアイデンティティフェデレーションを使用するかによって異なり"グリッドフェデレーション接続"ます。

アカウント同期のための **SSO** の設定（オプション）

グリッドフェデレーション接続のいずれかのStorageGRID システムでSSOを使用する場合は、両方のグリッドでSSOを使用する必要があります。グリッドフェデレーション用のテナントアカウントを作成する前に、テナントのソースグリッドとデスティネーショングリッドのグリッド管理者が次の手順を実行する必要があります。

手順

1. 両方のグリッドに同じアイデンティティソースを設定します。を参照して "アイデンティティフェデレーションを使用する"
2. 両方のグリッドに同じ SSO ID プロバイダー (IdP) を構成します。見る"シングルサインオンを設定します"。
3. "同じ管理者グループを作成します"両方のグリッドで同じフェデレーテッドグループをインポートする。

   テナントを作成するときに、このグループを選択して、ソースとデスティネーションの両方のテナントアカウントに対する初期のRootアクセス権限を割り当てます。

   > テナントを作成する前にこの管理者グループが両方のグリッドに存在していない場合、テナントはデスティネーションにレプリケートされません。

アカウント同期のためのグリッドレベルの **ID** フェデレーションを設定する（オプション）

どちらかのStorageGRID システムがSSOなしでアイデンティティフェデレーションを使用する場合は、両方のグリッドでアイデンティティフェデレーションを使用する必要があります。グリッドフェデレーション用のテナントアカウントを作成する前に、テナントのソースグリッドとデスティネーショングリッドのグリッド管理者が次の手順を実行する必要があります。

手順

1. 両方のグリッドに同じアイデンティティソースを設定します。を参照して "アイデンティティフェデレーションを使用する"
2. 必要に応じて、あるフェデレーテッドグループにソースとデスティネーションの両方のテナントアカウントに対する最初のRoot Access権限が付与される場合は、同じフェデレーテッドグループをインポートすることで、両方のグリッドで権限が付与され"同じ管理者グループを作成します"ます。

   > 両方のグリッドに存在しないフェデレーテッドグループにRoot Access権限を割り当てた場合、テナントはデスティネーショングリッドにレプリケートされません。

3. フェデレーテッドグループに両方のアカウントに対する最初のRoot Access権限を付与しない場合は、ローカルrootユーザのパスワードを指定します。

許可された**S3**テナントアカウントを作成します

SSOまたはアイデンティティフェデレーションを必要に応じて設定したら、グリッド管理者が次の手順を実行して、バケットオブジェクトを他のStorageGRID システムにレプリケートできるテナントを特定します。

手順

1. テナントのアカウント同期操作のソースグリッドとして使用するグリッドを決定します。

   テナントが最初に作成されたグリッドは、テナントの_source grid_と呼ばれます。テナントがレプリケートされるグリッドは、テナントの_destination grid_と呼ばれます。

2. そのグリッドで、新しいS3テナントアカウントを作成するか、既存のアカウントを編集します。
3. Use grid federation connection *権限を割り当てます。
4. テナントアカウントで独自のフェデレーテッドユーザを管理する場合は、* Use own identity source *権限を割り当てます。

   この権限が割り当てられている場合、フェデレーショングループを作成する前に、送信元と宛先のテナントアカウントの両方で同じIDソースを設定する必要があります。ソーステナントに追加されたフェデレーショングループは、両方のグリッドが同じIDソースを使用しない限り、宛先テナントに同期できません。

5. 特定のグリッドフェデレーション接続を選択します。
6. 新しいテナントまたは変更したテナントを保存します。

   [Use grid federation connection]*権限が設定された新しいテナントが保存されると、StorageGRID は次のように、そのテナントのレプリカをもう一方のグリッドに自動的に作成します。

   - 両方のテナントアカウントで、アカウントID、名前、ストレージクォータ、および権限が同じになります。
   - テナントに対してルートアクセス権限を持つフェデレーショングループを選択した場合、そのグループは宛先テナントに複製されます。ただし、フェデレーショングループおよびユーザーについては、継続的な同期は行われません。クローンは一度のみ実行されます。
   - テナントに対してルートアクセス権限を持つローカルユーザーを選択した場合、そのユーザーは宛先テナントに同期されます。

詳細については、"グリッドフェデレーションで許可されるテナントを管理します"を参照してください。

許可されているテナントアカウントのワークフロー

*グリッドフェデレーション接続の使用*権限を持つテナントが宛先グリッドにレプリケートされた後、許可されたテナントアカウントは、テナントグループ、ユーザー、およびS3アクセスキーを同期するために、以下の手順を実行できます。

手順

1. 接続されているいずれかのグリッド上で、テナントアカウントにサインインしてください。
2. 許可されている場合は、送信元テナントアカウントと宛先テナントアカウントの両方でIDフェデレーションを設定してください。
3. 接続されたグリッド上でグループとユーザーを作成できます。

   テナントに新しいグループまたはユーザーが作成されると、StorageGRID はそれらを宛先テナントに自動的に同期します。

4. S3アクセスキーを作成
5. 必要に応じて、S3アクセスキーをソーステナントから宛先テナントに同期します。

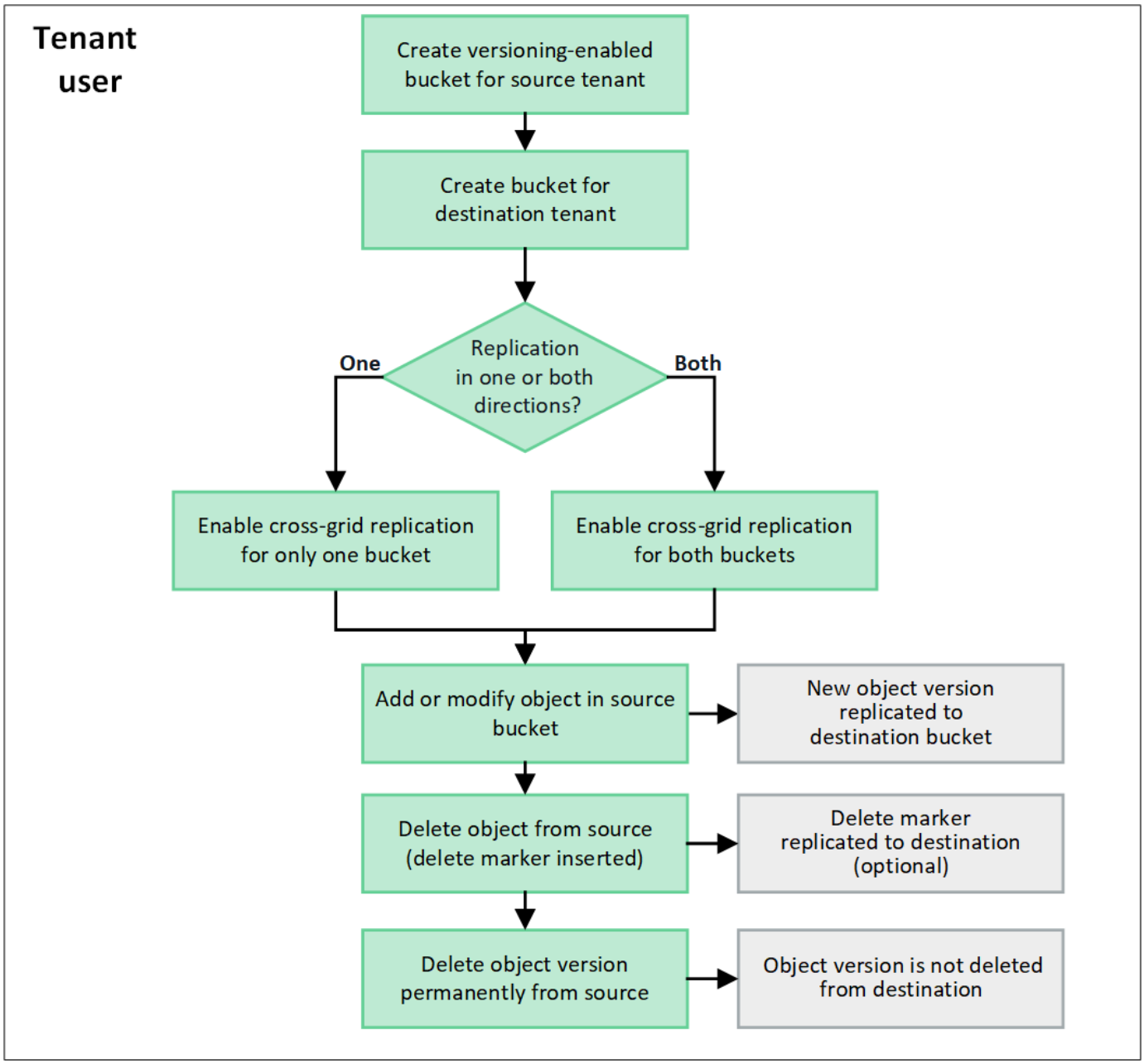
許可されたテナントアカウントのワークフローの詳細、およびグループ、ユーザー、S3 アクセスキーの同期方法については、"テナントグループとユーザーを同期する"を参照してください。

StorageGRID のクロスグリッドレプリケーションについて学ぶ

クロスグリッドレプリケーションとは、"グリッドフェデレーション接続"で接続された 2 つの StorageGRID システム内の選択した S3 バケット間でオブジェクトを自動的にレプリケートすることです。"アカウント同期"は、クロスグリッドレプリケーションに必要です。

グリッド間レプリケーションのワークフロー

ワークフロー図は、2 つのグリッド上のバケット間のクロスグリッド レプリケーションを構成する手順をまとめたものです。



グリッド間レプリケーションの要件

テナントアカウントに「グリッドフェデレーション接続を使用する」権限があり、1つ以上の"グリッドフェデレーション接続"を使用できる場合、ルートアクセス権限を持つテナントユーザーは、各グリッド上の対応するテナントアカウントにバケット（「ソース」バケットと「宛先」バケット）を作成できます。これらのバケット：

- それぞれ異なる名前を持つことができます
- 異なる地域を持つことができる
- バージョン管理が有効になっている必要があります
- 以下のいずれかの S3 オブジェクトロック構成が必要です：
  - 送信元：無効、宛先：無効
  - ソース：有効、宛先：有効
  - 送信元: 無効、宛先: 有効

両方のバケットを作成したら、どちらか一方、または両方のバケットに対してクロスグリッドレプリケーションを設定できます。

詳細

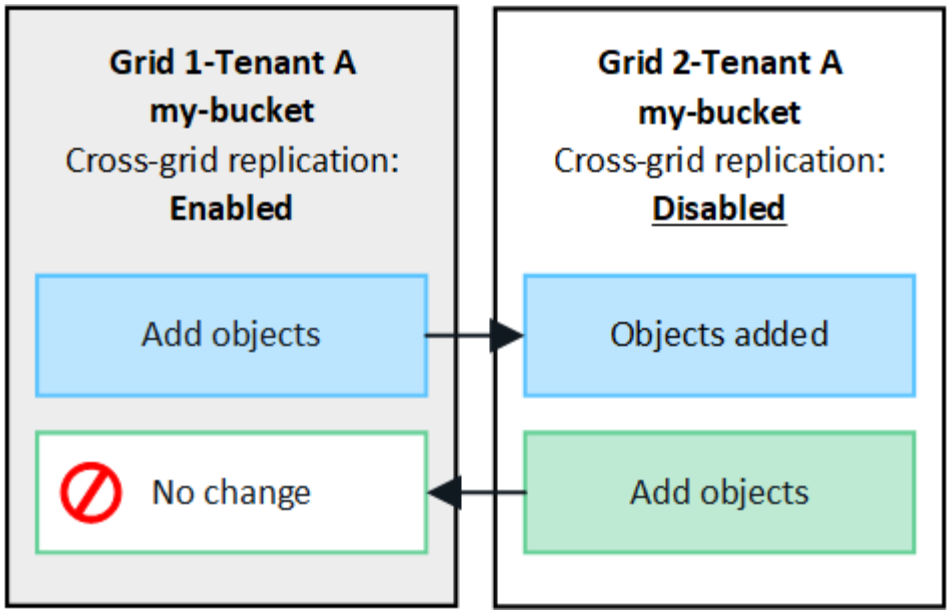
"グリッド間レプリケーションを管理します"

グリッド間レプリケーションの仕組み

クロスグリッド レプリケーションを一方向または双方向で実行するように構成できます。

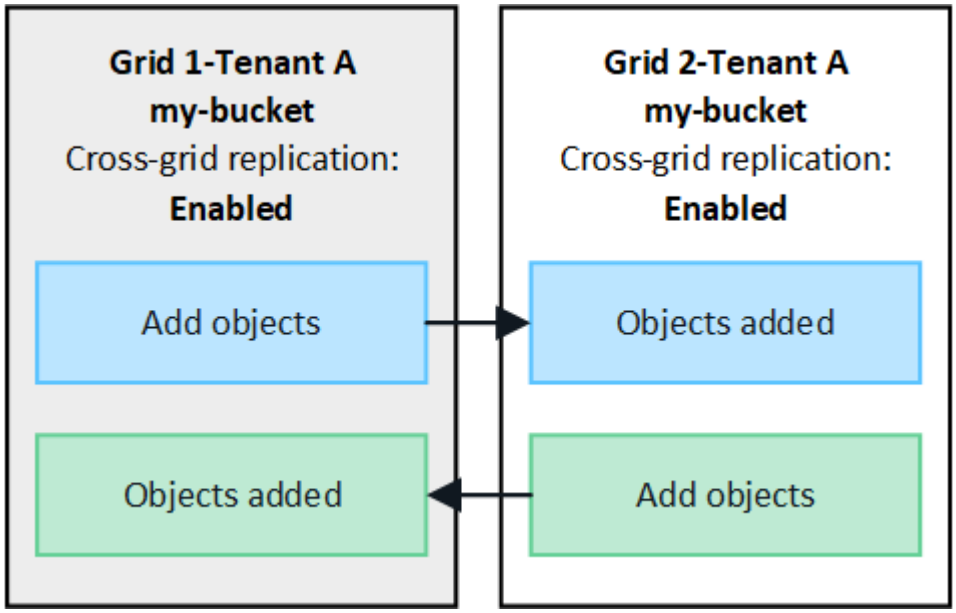
一方向のレプリケーション

1 つのグリッドのみのバケットに対してグリッド間レプリケーションを有効にすると、そのバケット (ソースバケット) に追加されたオブジェクトは、他のグリッドの対応するバケット (宛先バケット) に複製されます。ただし、宛先バケットに追加されたオブジェクトはソースに複製されません。図では、クロスグリッドレプリケーションが有効になっています。 `my-bucket`グリッド 1 からグリッド 2 への移動は可能ですが、逆方向では有効になっていません。



双方向のレプリケーション

両方のグリッドで同じバケットに対してクロスグリッドレプリケーションを有効にすると、一方のバケットに追加されたオブジェクトがもう一方のグリッドにレプリケートされます。次の図では、で双方向のグリッド間レプリケーションが有効になってい `my-bucket`ます。



オブジェクトが取り込まれるとどうなりますか？

S3クライアントが、クロスグリッドレプリケーションが有効になっているバケットにオブジェクトを追加すると、次の処理が実行されます。

1. StorageGRID は、ソースバケットからデスティネーションバケットにオブジェクトを自動的にレプリケートします。このバックグラウンドレプリケーション処理の実行時間は、保留中の他のレプリケーション処理の数など、いくつかの要因によって異なります。

   S3 クライアントは、GetObject または HeadObject リクエストを発行してオブジェクトのレプリケーショ

ン ステータスを確認できます。レスポンスにはStorageGRID固有の `x-ntap-sg-cgr-replication-status`応答ヘッダー。次のいずれかの値を持ちます。

グリッド	レプリケーションのステータス
ソース	• * Completed *：すべてのグリッド接続でレプリケーションが完了しました。 • * pending *：オブジェクトは少なくとも1つのグリッド接続にレプリケートされていません。 • 失敗: どのグリッド接続でもレプリケーションは保留中ではなく、少なくとも 1 つの接続で永続的な障害が発生しました。ユーザーはエラーを解決する必要があります。
デスティネーション	**replica**:オブジェクトはソースグリッドからレプリケートされました。

StorageGRIDはサポートしていません `x-amz-replication-status`ヘッダ。

2. StorageGRIDは、他のオブジェクトと同様に、各グリッドのアクティブなILMポリシーを使用してオブジェクトを管理します。たとえば、グリッド1のオブジェクトAは2つのレプリケートコピーとして格納されて無期限に保持されるのに対し、グリッド2にレプリケートされたオブジェクトAのコピーは2+1のイレイジャーコーディングを使用して格納され、3年後に削除されるとします。

オブジェクトが削除されるとどうなりますか？

で説明したように"データフローを削除します"、StorageGRIDは次のいずれかの理由でオブジェクトを削除できます。

- S3クライアントが削除要求を実行します。
- Tenant Managerユーザが、バケットからすべてのオブジェクトを削除するオプションを選択しまし"バケット内のオブジェクトを削除する"た。
- バケットにはライフサイクル設定があり、有効期限が切れます。
- オブジェクトのILMルールの最後の期間が終了し、それ以上の配置が指定されていない。

[Delete objects in bucket]処理、バケットライフサイクルの有効期限、またはILM配置の有効期限が原因でStorageGRID がオブジェクトを削除しても、レプリケートオブジェクトがグリッドフェデレーション接続の他のグリッドから削除されることはありません。ただし、S3クライアントによる削除によってソースバケットに追加された削除マーカーは、必要に応じてデスティネーションバケットにレプリケートできます。

クロスグリッドレプリケーションが有効になっているバケットからS3クライアントがオブジェクトを削除した場合の動作を理解するには、バージョン管理が有効になっているバケットからS3クライアントがオブジェクトを削除する仕組みを次のように確認してください。

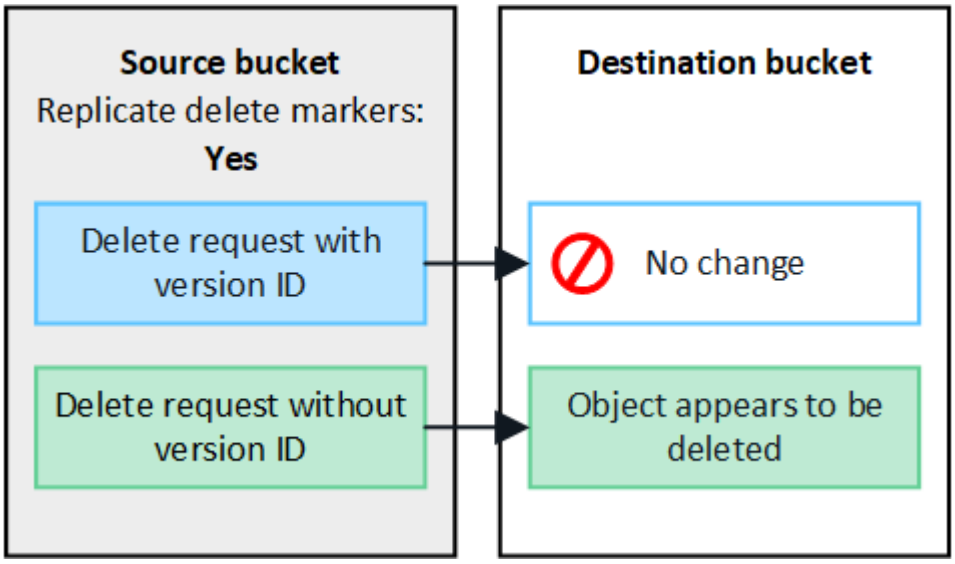
- S3クライアントがバージョンIDを含む削除要求を実行すると、そのバージョンのオブジェクトが完全に削除されます。バケットに削除マーカーは追加されません。
- S3 クライアントがバージョン ID を含まない削除リクエストを発行した場合、 StorageGRID はオブジェクト バージョンを削除しません。代わりに、バケットに削除マーカーを追加します。削除マーカーにより、 StorageGRID はオブジェクトが削除されたかのように動作します。

- バージョンIDのないGetObjectリクエストは失敗します。 `404 No Object Found`
- 有効なバージョン ID を持つ GetObject 要求は成功し、要求されたオブジェクト バージョンを返します。

S3クライアントがクロスグリッドレプリケーションが有効になっているバケットからオブジェクトを削除すると、StorageGRID は次のように削除要求をデスティネーションにレプリケートするかどうかを判断します。

- 削除リクエストにバージョン ID が含まれている場合、そのオブジェクト バージョンはソース グリッドから完全に削除されます。ただし、 StorageGRID はバージョン ID を含む削除要求を複製しないため、同じオブジェクト バージョンが宛先から削除されません。
- 削除リクエストにバージョン ID が含まれていない場合、 StorageGRID は、バケットのクロスグリッド レプリケーションの構成に基づいて、オプションで削除マーカーを複製できます。
  - 削除マーカーをレプリケートするように選択した場合（デフォルト）は、削除マーカーがソースバケットに追加され、デスティネーションバケットにレプリケートされます。実際には、オブジェクトは両方のグリッドで削除されているように見えます。
  - 削除マーカーを複製しないことを選択した場合、削除マーカーはソースバケットに追加されますが、宛先バケットには複製されません。実際には、ソース グリッドで削除されたオブジェクトは、宛先グリッドでは削除されません。

図では、*削除マーカーの複製*が*はい*に設定されています。"クロスグリッドレプリケーションが有効になりました" 。バージョン ID を含むソース バケットの削除リクエストでは、宛先バケットからオブジェクトは削除されません。バージョン ID を含まないソース バケットの削除リクエストは、宛先バケット内のオブジェクトを削除するように見えます。



オブジェクトの削除をグリッド間で同期したままにする場合は、両方のグリッドでバケットに対応するを作成します"S3ライフサイクル設定"。

暗号化されたオブジェクトのレプリケート方法

グリッド間レプリケーションを使用してグリッド間でオブジェクトをレプリケートする場合は、個 々 のオブジェクトを暗号化するか、デフォルトのバケット暗号化を使用するか、またはグリッド全体の暗号化を設定できます。バケットに対してグリッド間レプリケーションを有効にする前後に、デフォルトのバケットまたはグリッド全体の暗号化設定を追加、変更、または削除できます。

個 々 のオブジェクトを暗号化するには、SSE（StorageGRIDで管理されるキーによるサーバ側の暗号化）を使用してオブジェクトをソースバケットに追加します。要求ヘッダーを使用し `x-amz-server-side-encryption`、を指定します `AES256`。を参照して "サーバ側の暗号化を使用します"

> SSE-C (顧客提供のキーを使用したサーバー側暗号化) の使用は、クロスグリッド レプリケーションではサポートされていません。取り込み操作は失敗します。

バケットでデフォルトの暗号化を使用するには、PutBucketEncryption要求を使用して、パラメータを`AES256`に設定します `SSEAlgorithm`。バケットレベルの暗号化は、要求ヘッダーを指定せずに取り込まれたオブジェクトに適用され `x-amz-server-side-encryption`ます。を参照して "バケットの処理"

グリッドレベルの暗号化を使用するには、* stored object encryption オプションを AES-256 *に設定します。グリッドレベルの暗号化は、バケットレベルで暗号化されていないオブジェクト、または要求ヘッダーなしで取り込まれたオブジェクトに適用され `x-amz-server-side-encryption`ます。を参照して "ネットワークとオブジェクトのオプションを設定します"

> SSE は AES-128 をサポートしていません。 **AES-128** オプションを使用してソース グリッドに対して 保存されたオブジェクトの暗号化 オプションが有効になっている場合、AES-128 アルゴリズムの使用はレプリケートされたオブジェクトに伝播されません。代わりに、複製されたオブジェクトは、宛先のデフォルトのバケットまたはグリッド レベルの暗号化設定（使用可能な場合）を使用します。

ソースオブジェクトの暗号化方法を決定する際に、StorageGRID は次のルールを適用します。

1. 取り込みヘッダーがある場合は、そのヘッダーを使用し `x-amz-server-side-encryption`ます。
2. 取り込みヘッダーが存在しない場合は、バケットのデフォルトの暗号化設定（構成されている場合）を使用します。
3. バケット設定が構成されていない場合は、グリッド全体の暗号化設定（構成されている場合）を使用します。
4. グリッド全体の設定が存在しない場合は、ソース オブジェクトを暗号化しないでください。

StorageGRID では、レプリケートオブジェクトの暗号化方法を決定する際に、次の順序でルールが適用されます。

1. ソースオブジェクトがAES-128暗号化を使用している場合を除き、ソースオブジェクトと同じ暗号化を使用します。
2. ソース オブジェクトが暗号化されていないか、AES-128 を使用している場合は、宛先バケットのデフォルトの暗号化設定（構成されている場合）を使用します。
3. 宛先バケットに暗号化設定がない場合、宛先のグリッド全体の暗号化設定（構成されている場合）を使用します。
4. グリッド全体の設定が存在しない場合は、宛先オブジェクトを暗号化しないでください。

S3 オブジェクトロックを使用したクロスグリッドレプリケーション

次の状況では、S3 オブジェクト ロックが有効になっているStorageGRIDバケット間でクロス グリッド レプリケーションを設定できます。

ソースバケットの **S3** オブジェクトロックがかかっている場合...	そして、送信先バケットの **S3** オブジェクトロックは...
有効	有効
無効	有効

既存のバケットに対して S3 Object Lock を有効にすることができますが、これは後々設定ミスにつながる可能性があります。

ソースバケットでS3オブジェクトロックが有効になっている場合は、宛先バケットでも有効になっていることを確認してください。宛先バケットでS3オブジェクトロックが無効になっている場合、レプリケーション中にエラーが発生します。"グリッド間レプリケーションのアラートとエラー"を参照してください。

ソースバケットの S3 オブジェクトロックが有効になっている場合:

- オブジェクトは、次の順序で保存先で保持設定を使用してロックされます。
  a. ソース オブジェクトの保持ヘッダー値:

     `x-amz-object-lock-mode`

     `x-amz-object-lock-retain-until-date`

  b. ソースバケットのデフォルトの保持期間（設定されている場合）。
  c. 宛先バケットのデフォルトの保持期間（設定されている場合）。

  宛先バケットのデフォルトの保持は、ソース オブジェクトから複製された保持設定を上書きしません。
- 宛先オブジェクトの法的保留ステータスを設定するには、 `x-amz-object-lock-legal-hold`オブジェクトをアップロードするとき。
- 宛先テナントまたはバケットがソースオブジェクトの S3 オブジェクトロック設定をサポートしていない場合は、エラーが発生します。参照"クロスグリッド レプリケーションのアラートとエラー。"

ソースバケットの S3 オブジェクトロックが無効になっている場合:

- 宛先バケットのデフォルトの保持期間を設定して、宛先オブジェクトに S3 オブジェクトロックの保持期間設定を適用できます。
- 宛先オブジェクトは法的保留ステータスを設定できません。

PutObjectTaggingと**DeleteObjectTagging**はサポートされない

PutObjectTagging要求とDeleteObjectTagging要求は、グリッド間レプリケーションが有効になっているバケット内のオブジェクトではサポートされません。

S3クライアントがPutObjectTaggingまたはDeleteObjectTaggingリクエストを発行すると、 `501 Not Implemented`が返されます。メッセージは `Put(Delete) ObjectTagging isn't available for buckets that have cross-grid replication configured`。

PutObjectRetentionとPutObjectLegalHoldはサポートされていません

PutObjectRetention および PutObjectLegalHold リクエストは、クロスグリッド レプリケーションが有効になっているバケット内のオブジェクトでは完全にはサポートされません。

S3 クライアントが PutObjectRetention または PutObjectLegalHold リクエストを発行すると、ソース オブジェクトの設定は変更されますが、その変更は宛先には適用されません。

セグメント化されたオブジェクトのレプリケート方法

ソース グリッドの最大セグメント サイズは、宛先グリッドに複製されるオブジェクトに適用されます。オブジェクトが別のグリッドに複製される場合、ソース グリッドの 最大セグメント サイズ 設定 (**[構成] > *システム] > *ストレージ オプション**) が両方のグリッドで使用されます。たとえば、ソース グリッドの最大セグメント サイズが 1 GB で、宛先グリッドの最大セグメント サイズが 50 MB であるとします。ソース グリッドに 2 GB のオブジェクトを取り込むと、そのオブジェクトは 2 つの 1 GB セグメントとして保存されます。また、グリッドの最大セグメント サイズは 50 MB ですが、宛先グリッドには 2 つの 1 GB セグメントとして複製されます。

StorageGRIDにおけるグリッド間複製とCloudMirror複製の比較

グリッドフェデレーションの使用を開始する際に、との類似点と相違点を確認して"グリッド間レプリケーション""StorageGRID CloudMirror レプリケーションサービス"ください。

> クロスグリッド レプリケーションによってレプリケートされたバケットでは CloudMirror を使用することはできません。また、その逆も同様です。

	グリッド間レプリケーション	**CloudMirror** レプリケーションサービス
主な目的は何ですか？	1つのStorageGRID システムがディザスタリカバリシステムとして機能します。バケット内のオブジェクトは、グリッド間で一方向または両方向にレプリケートできます。	テナントで、StorageGRID （ソース）内のバケットから外部のS3バケット（デスティネーション）にオブジェクトを自動的にレプリケートできます。 CloudMirror レプリケーションは、独立した S3 インフラストラクチャ内にオブジェクトの独立したコピーを作成します。この独立したコピーはバックアップとしては使用されませんが、クラウドでさらに処理されることがよくあります。

	グリッド間レプリケーション	**CloudMirror** レプリケーションサービス
セットアップ方法は？	1. 2つのグリッド間のグリッドフェデレーション接続を設定します。 2. 新しいテナントアカウントを追加すると、他のグリッドと自動的に同期されます。 3. 新しいテナントグループとユーザーを追加すると、それらも同期されます。 4. 各グリッドに対応するバケットを作成し、一方向または両方向でグリッド間レプリケーションを実行できるようにします。	1. テナントユーザは、Tenant ManagerまたはS3 APIを使用してCloudMirrorエンドポイント（IPアドレス、クレデンシャルなど）を定義することによってCloudMirrorレプリケーションを設定します。 2. そのテナントアカウントが所有するバケットは、CloudMirrorエンドポイントを指すように設定できます。
設定は誰が担当しますか？	• グリッド管理者が接続とテナントを設定します。 • テナントユーザは、グループ、ユーザ、キー、およびバケットを設定します。	通常はテナントユーザです。
デスティネーションは何ですか？	グリッドフェデレーション接続内のもう一方のStorageGRID システム上の、対応する同一のS3バケット。	• 互換性のある任意のS3インフラ（Amazon S3を含む）。 • Google Cloud Platform（GCP）
オブジェクトのバージョン管理は必要ですか。	はい。ソースバケットとデスティネーションバケットの両方でオブジェクトのバージョン管理を有効にする必要があります。	いいえ。CloudMirrorレプリケーションでは、ソースとデスティネーションの両方で、バージョン管理に対応していないバケットとバージョン管理に対応していないバケットを任意に組み合わせて使用できます。
オブジェクトをデスティネーションに移動する原因は何ですか？	オブジェクトは、グリッド間レプリケーションが有効になっているバケットに追加されると自動的にレプリケートされます。	CloudMirrorエンドポイントが設定されたバケットにオブジェクトが追加されると、オブジェクトが自動的にレプリケートされます。CloudMirrorエンドポイントを設定する前にソースバケットに存在していたオブジェクトは、変更しないかぎりレプリケートされません。
オブジェクトのレプリケート方法	グリッド間レプリケーションでバージョン管理オブジェクトが作成され、バージョンIDがソースバケットからデスティネーションバケットにレプリケートされます。これにより、両方のグリッドでバージョンの順序を維持できます。	CloudMirrorレプリケーションではバージョン管理が有効なバケットは必要ないため、CloudMirrorではサイト内のキーの順序のみを維持できます。別のサイトにあるオブジェクトへの要求の順序が維持される保証はありません。

	グリッド間レプリケーション	**CloudMirror** レプリケーションサービス
オブジェクトをレプリケートできない場合はどうなりますか。	オブジェクトは、メタデータストレージの制限に従ってレプリケーションのキューに登録されます。	オブジェクトは、プラットフォームサービスの制限に従ってレプリケーションのキューに登録されます（を参照"プラットフォームサービスの使用に関する推奨事項"）。
オブジェクトのシステムメタデータはレプリケートされているか？	はい。オブジェクトが他のグリッドにレプリケートされると、そのシステムメタデータもレプリケートされます。メタデータは両方のグリッドで同一になります。	いいえ。オブジェクトが外部バケットにレプリケートされると、そのシステムメタデータが更新されます。メタデータは場所によって異なり、取り込み時間や独立したS3インフラの動作によって異なります。
オブジェクトの読み出し方法	アプリケーションは、いずれかのグリッドのバケットに要求することで、オブジェクトを読み出すことができます。	アプリケーションは、StorageGRID またはS3デスティネーションに要求を行うことで、オブジェクトの読み出しや読み取りを行うことができます。たとえば、 CloudMirror レプリケーションを使用してパートナー組織にオブジェクトをミラーリングするとします。パートナーは、独自のアプリケーションを使用して、 S3 デスティネーションからオブジェクトを直接読み取ったり更新したりできます。StorageGRID を使用する必要はありません。
オブジェクトが削除された場合の動作	• バージョンIDを含む削除要求は、デスティネーショングリッドにレプリケートされません。 • バージョンIDが含まれていない削除要求では、ソースバケットに削除マーカーが追加され、必要に応じてデスティネーショングリッドにレプリケートできます。 • グリッド間レプリケーションが一方向のみに設定されている場合は、ソースに影響を与えずにデスティネーションバケット内のオブジェクトを削除できます。	結果は、ソースバケットとデスティネーションバケットのバージョン管理状態によって異なります（同じである必要はありません）。 • 両方のバケットがバージョン管理に対応している場合は、削除要求によって両方の場所に削除マーカーが追加されます。 • ソースバケットのみがバージョン管理に対応している場合、削除要求ではソースに削除マーカーが追加されますが、デスティネーションには追加されません。 • どちらのバケットもバージョン管理に対応していない場合、削除要求によってソースからはオブジェクトが削除されますが、デスティネーションからは削除されません。 同様に、デスティネーションバケット内のオブジェクトもソースに影響を与えることなく削除できます。

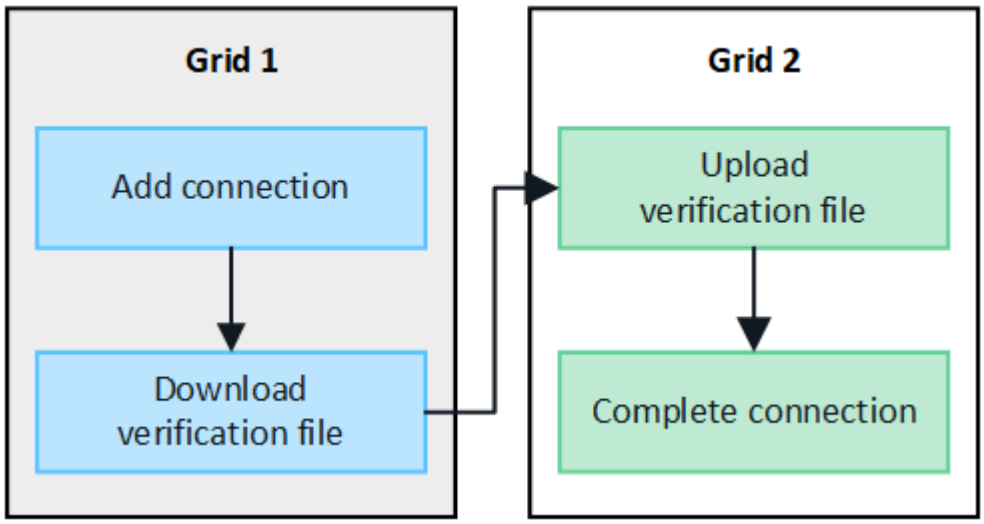
StorageGRID グリッド フェデレーション接続を作成する

テナントの詳細を同期してオブジェクトデータをレプリケートする場合

は、StorageGRID システム間でグリッドフェデレーション接続を作成できます。

図に示すように、グリッド連携接続の作成には、両方のグリッドでの手順が含まれます。一方のグリッドに接続を追加し、もう一方のグリッドで接続を完了します。どちらのグリッドからでも開始できます。

オプションで、"グリッドフェデレーション接続の作成、編集、および保守を自動化する"。



開始する前に

- グリッドフェデレーション接続を設定するためのを確認しておきます"考慮事項と要件"。
- 各グリッドにIPアドレスまたはVIPアドレスの代わりに完全修飾ドメイン名（FQDN）を使用する場合は、使用する名前を確認し、各グリッドのDNSサーバに適切なエントリがあることを確認しておきます。
- を使用している"サポートされている Web ブラウザ"。
- 両方のグリッドのRootアクセス権限とプロビジョニングパスフレーズが必要です。

接続を追加します

次の手順は、2つのStorageGRID システムのどちらかで実行します。

手順

1. いずれかのグリッドのプライマリ管理ノードからGrid Managerにサインインします。
2. 構成 > システム > グリッド フェデレーション を選択します。
3. [接続の追加]*を選択します。
4. 接続名を入力してください。これは、この接続を識別するための固有の名前です。例えば、 `Grid 1-Grid 2`。
5. "グローバル名前空間を構成する"を使用する場合は、*グローバル名前空間を有効にする*を選択してください。
6. 「 * Continue * 」を選択します。
7. グリッドの詳細を以下のように入力してください：

フィールド	製品説明
このグリッドのFQDNまたはIP	次のいずれか • 現在サインインしているグリッドのFQDN • このグリッド上のHAグループのVIPアドレスです • このグリッド上の管理ノードまたはゲートウェイノードのIPアドレス。IPは、デスティネーショングリッドが到達可能な任意のネットワーク上に設定できます。
ポート	この接続に使用するポート。23000～23999の任意の未使用ポート番号を入力できます。 この接続の両方のグリッドが同じポートを使用します。どちらのグリッドでも、このポートを他の接続に使用しているノードがないことを確認する必要があります。
このグリッドの証明書有効日数	接続内のこのグリッドのセキュリティ証明書を有効にする日数。デフォルト値は730日（2年）ですが、1～762日の任意の値を入力できます。 接続を保存すると、StorageGRID で各グリッドのクライアント証明書とサーバ証明書が自動的に生成されます。
このグリッドのプロビジョニングパスフレーズ	サインインしているグリッドのプロビジョニングパスフレーズ。
もう一方のグリッドのFQDNまたはIP	次のいずれか • 接続先のグリッドのFQDN • もう一方のグリッド上のHAグループのVIPアドレスです • もう一方のグリッド上の管理ノードまたはゲートウェイノードのIPアドレス。IPは、ソースグリッドが到達可能な任意のネットワーク上に設定できます。

1. [保存して続行]*を選択します。
2. [検証ファイルのダウンロード]ステップで、*[検証ファイルのダウンロード]*を選択します。

   もう一方のグリッドで接続が完了すると、どちらのグリッドからも検証ファイルをダウンロードできなくなります。

3. ダウンロードしたファイル(`*connection-name*.grid-federation`を見つけ、安全な場所に保存します。

   > このファイルには秘密情報（別名でマスク）やその他の機密情報が含まれて `*`おり、安全に保存および送信する必要があります。

4. [Close]*を選択して、[Grid Federation]ページに戻ります。

5. 新しい接続が表示され、*接続ステータス*が*接続待ち*になっていることを確認します。
6. もう一方のグリッドのファイルをグリッド管理者に提供し `*connection-name*.grid-federation`ます。

接続を完了します

接続先のStorageGRID システム（もう一方のグリッド）で次の手順を実行します。

手順

1. プライマリ管理ノードからGrid Managerにサインインします。
2. 構成 > システム > グリッド フェデレーション を選択します。
3. [Upload verification file]*を選択して、[Upload]ページにアクセスします。
4. [検証ファイルのアップロード]*を選択します。次に、最初のグリッドからダウンロードしたファイルを参照して選択し(`*connection-name*.grid-federation`ます）。

   接続の詳細が表示されます。

5. 必要に応じて、このグリッドのセキュリティ証明書に別の有効な日数を入力します。[Certificate Valid Days]*エントリは、最初のグリッドに入力した値にデフォルトで設定されますが、各グリッドでは異なる有効期限を使用できます。

   一般に、接続の両側の証明書には同じ日数を使用します。

   > 接続のいずれかの側の証明書が期限切れになると、接続は動作を停止し、証明書が更新されるまでレプリケーションは保留になります。

6. 現在サインインしているグリッドのプロビジョニングパスフレーズを入力します。
7. [保存してテスト]*を選択します。

   証明書が生成され、接続がテストされます。接続が有効な場合は、成功を示すメッセージが表示され、[Grid Federation]ページに新しい接続がリストされます。は[接続済み]*になります。

   エラーメッセージが表示された場合は、問題に対処します。を参照して "グリッドフェデレーションエラーをトラブルシューティングする"

8. 最初のグリッドのグリッドフェデレーションページに移動し、ブラウザを更新します。[接続ステータス]*が[接続済み]*になっていることを確認します。
9. 接続が確立されたら、検証ファイルのすべてのコピーを安全に削除します。

   この接続を編集すると、新しい検証ファイルが作成されます。元のファイルは再利用できません。

終了後

- の考慮事項を確認します"許可されたテナントの管理"。
- "新しいテナントアカウントを1つ以上作成します"をクリックし、*[Use grid federation connection]*権限を割り当てて、新しい接続を選択します。
- "接続を管理します"必要に応じて。接続値の編集、接続のテスト、接続証明書のローテーション、接続の削除を行うことができます。

- "接続を監視します"通常のStorageGRID監視アクティビティの一部として使用します。
- "接続のトラブルシューティングを行います"アカウント同期やクロスグリッドレプリケーションに関連するアラートやエラーの解決を含みます。

StorageGRID でグリッドフェデレーション接続を自動化する

バージョン12.1以降を実行している2つ以上のStorageGRIDシステムをインストールして設定したら、 `manage-grid-federation.py` Pythonスクリプトと JSON設定ファイルを使用して、グリッドフェデレーション接続の作成、編集、およびメンテナンスを自動化できます。

開始する前に

- すべてのグリッドで StorageGRID 12.1 以降が稼働しています。
- いずれかのグリッドでシングル サインオン（SSO）が有効になっている場合は、無効にしてください。
- Python 3.6以降がインストールされたLinuxマシンをお持ちです。
- インストールアーカイブ内の以下のファイルの場所を確認しておいてください。

ファイル名	製品説明
manage-grid-federation.py	グリッドフェデレーション接続管理を自動化するために使用されるPythonスクリプト
manage-grid-federation.sample.json	スクリプトで使用する構成ファイルの例

- あなたは `manage-grid-federation.json`設定ファイルを作成しました。このファイルを作成するには、サンプル設定ファイル `manage-grid-federation.sample.json`を変更してください。

> グリッド管理者パスワードとプロビジョニングパスフレーズを `manage-grid-federation.json`設定ファイルから安全な場所に保存してください。ファイルに認証情報が省略されている場合、スクリプトは対話形式で認証情報の入力を求めます。変更した設定ファイルのバックアップを安全な場所に保存しておくことも重要です。

設定ファイルフィールド

JSON設定ファイルはオブジェクトの配列です。各オブジェクトは1つのグリッドを表し、以下のフィールドをサポートします：

フィールド	必須	製品説明
`hostname`	はい	グリッドの管理者ノードのホスト名またはIPアドレス
`grid_name`	はい	グリッドの表示名（最大12文字）
ユーザ名	いいえ	グリッド管理者ユーザー名（省略した場合は対話形式で入力を求められます）
`password`	いいえ	グリッド管理者パスワード（省略した場合は対話形式で入力を求められます）

フィールド	必須	製品説明
パスフレーズ	いいえ	プロビジョニングパスフレーズ（省略した場合、対話形式で入力が求められます）
`ca_bundle`	いいえ	SSL検証用のカスタムCA証明書バンドルへのパス
リージョン	いいえ	グローバル名前空間接続に使用するデフォルトのS3リージョン
`CNAME`	いいえ	グローバル名前空間接続に必要なCNAME
`globalEndpoint`	いいえ	目的のグローバル名前空間エンドポイント

グローバル名前空間フィールドのいずれかを設定する場合（(`region`、 `CNAME`、`globalEndpoint`）、各グリッドに対して3つすべてを指定する必要があります。リージョンと CNAME がグリッド全体で一意であることを確認し、 `globalEndpoint`の値はすべてのグリッドで同一である必要があります。

タスクの内容

`manage-grid-federation.py` Python スクリプトと `manage-grid-federation.json`設定ファイルを使用して、グリッドフェデレーション接続管理を自動化できます。このスクリプトは以下の操作を実行します：

- グリッド管理APIを使用して各グリッドに対して認証を行います。
- すべてのグリッドが StorageGRID 12.1 以降を実行していることを確認します
- すべてのグリッドでシングル サインオンが無効になっていることを確認します。
- 既存のグリッドフェデレーション接続とS3構成を取得します
- 設定時にS3リージョン、CNAME、およびグローバルネームスペースエンドポイントの設定を更新します。
- まだ接続されていないグリッドペアに対して、新しいグリッドフェデレーション接続を作成します。
- 表示名またはグローバル名前空間設定が変更された場合に、既存の接続を編集します。
- すべての接続とそのステータスの概要を表示します

グリッドフェデレーション接続は、グリッドマネージャーのUIまたはグリッド管理APIを直接使用して管理することもできます。

手順

1. Python スクリプトを実行するために使用する Linux マシンにログインします。
2. スクリプトが格納されているディレクトリに移動してください。

   例：

   ```
   cd StorageGRID-Webscale-version/platform
   ```

ここで **platform** は `debs`、 `rpms`、または `vsphere`です。

3. Python スクリプトを実行し、作成した構成ファイルを使用します。

   例：

   ```
   ./manage-grid-federation.py -i manage-grid-federation.json
   ```

   以下のコマンドラインオプションを使用できます：

オプション	デフォルト	製品説明
`-i、--input-json-file`	（必須）	グリッドのリストを含むJSON設定ファイルへのパス
`-b, --base-port`	23001	新規グリッドフェデレーション接続の開始ポート番号
`--no-verify-ssl`	SSL検証が有効になっています	ローカルとグリッド間の接続におけるSSL証明書の検証を無効にします

既存の接続を編集する

スクリプトが既存の接続に変更が必要であることを検出した場合（例えば、グリッド表示名が変更された場合や、グローバル名前空間設定を更新する必要がある場合など）、提案された編集内容の概要を表示し、処理を進める前に確認を求めます。

グローバル名前空間が有効になっているグリッドで S3 構成の更新（(`region`、 `CNAME`、または `globalEndpoint`）が必要な場合、スクリプトは変更を適用するためにグローバル名前空間を一時的に無効にする必要があります。この場合、確認プロンプトには一時的なルーティング障害に関する警告が表示されます。

```
*** Global Namespace Disable Required ***
Global Namespace must be disabled to update region/CNAME/globalEndpoint
settings.
Routing requests will not work until Global Namespace is re-enabled.
Grids requiring S3 updates: grid1.example.com, grid2.example.com
Proceed with these edits and the temporary routing outage? [y/N]:
```

S3の設定更新中はグローバルネームスペースが一時的に無効になるため、グローバルネームスペースのルーティング要求は機能しません。この作業はメンテナンス期間中に計画してください。

終了後

グリッドフェデレーション接続が確立および構成されると、スクリプトに次のような確認概要が表示されます：

```
===== Newly Established Connections =====
 • Grid-A and Grid-B — grid-a.example.com and grid-b.example.com on port
23001

Total new connections: 1

===== All Grid-Federation Connections =====
  Name              Source                Target                Port
Status    Global Namespace
  ----------------  --------------------  --------------------  -----
--------  ----------------
  Grid-A and Grid-B grid-a.example.com    grid-b.example.com    23001  new
enabled

Total connections listed: 1

===== Grid S3 Configuration Summary =====
 grid-a.example.com:
    Default Region: us-east-1
    CNAME: s3-a.example.com
    Global namespace endpoint: gn.example.com
 grid-b.example.com:
    Default Region: us-west-1
    CNAME: s3-b.example.com
    Global namespace endpoint: gn.example.com
```

終了ステータス

コード	製品説明
0	スクリプトは正常に完了しました
1	検証に失敗したか、グリッドAPI呼び出しでエラーが返されました（ログ出力を確認してください）

接続が失敗した場合、スクリプトは残りのペアの処理を続行し、出力の「Failed Connections」セクションにすべての失敗を報告します。エラーメッセージを確認し、スクリプトを再実行する前に問題を解決してください。

グリッドフェデレーションのグローバルネームスペースについて

グローバルネームスペースにより、テナントは複数の StorageGRID システムにまたがるバケットにアクセスできます。グリッドフェデレーション接続でグローバルネームスペースが有効になっている場合、グローバルネームスペースエンドポイントを対象とする S3 CreateBucket および ListBuckets リクエストは、任意のグリッドのロードバランサーエンドポイントに送信でき、リクエスト内の署名リージョンに基づいて適切なグリッド

に自動的にルーティングされます。

グローバル名前空間とは何ですか？

グローバルネームスペースにより、テナントは複数の StorageGRID システムにまたがるバケットにアクセスできます。グリッドフェデレーション接続でグローバルネームスペースが有効になっている場合、グローバルネームスペースエンドポイントを対象とする S3 CreateBucket および ListBuckets リクエストは、任意のグリッドのロードバランサーエンドポイントに送信でき、リクエスト内の署名リージョンに基づいて適切なグリッドに自動的にルーティングされます。

> バケットURLを特定のグリッドにDNSマッピングするために、DNSリゾルバを設定する必要があります。必要に応じて、ネットワーク管理者に相談し、DNSリゾルバが正しく設定されていることを確認してください。"DNS解決を設定する"を参照してください。

StorageGRID はグローバル名前空間内のグリッド間で一意のバケット名を強制しないため、同じ名前のバケットが異なるグリッド上に存在できます。リクエスト内の署名リージョンは、どのグリッドがバケットを所有し、リクエストを受信すべきかを判断するために使用されます。

たとえば、グリッドAがリージョン `us-east-1`を使用し、グリッドBがリージョン `us-west-1`を使用する場合、リージョン `us-west-1`を指定して任意のグリッドに送信されたCreateBucketリクエストは、自動的にグリッドBにルーティングされます。

グリッドフェデレーションの詳細については、"グリッドフェデレーションとは"を参照してください。

グローバル名前空間の例

グリッド**1**

- デフォルトリージョン： `region-1`
- デフォルトのCNAME： `s3.region-1.company.com`
- グローバルエンドポイント： `s3.company.com`

グリッド **2**

- デフォルトのリージョン： `region-2`
- デフォルトのCNAME： `s3.region-2.company.com`
- グローバルエンドポイント： `s3.company.com`

グリッド**3**

- デフォルトのリージョン： `region-3`
- デフォルトのCNAME： `s3.region-3.company.com`
- グローバルエンドポイント： `s3.company.com`

CreateBucket および **ListBuckets** オペレーション

バケットを作成する場合(`bucket123`）署名リージョン付き `region-2`グローバルエンドポイントをターゲットとする `s3.company.com`、リクエストを受け取ったグリッドはすべて、Grid 2上にバケットを作成します。

バケット固有の操作と一般的なオブジェクト操作

特定のグリッド上にバケットが作成されると、DNSリゾルバはバケットのURLをバケットとグリッドのCNAMEに解決します。

上記の例では、DNSリゾルバは `bucket123.s3.company.com` を `bucket123.s3.grid3.company.com`（バケットとグリッドのCNAME）に解決する必要があります。つまり、すべてのリクエストは追加のルーティングを必要とせずに、そのグリッドに直接送信されます。

例

`PutObject to bucket123.s3.company.com` 解決先： `bucket123.s3.grid3.company.com`

グローバルネームスペースを使用したS3の動作

グローバルネームスペースが完全に設定されると、以下のS3の動作が適用されます。

リージョン強制

グローバル名前空間エンドポイントへのすべての S3 リクエストは、"CreateBucket" および "ListBuckets" を除き、V4 認証ヘッダー内の署名リージョンがグリッドのデフォルトリージョンと一致する必要があります。

- 署名リージョンが一致しない場合、リクエストは次のエラーで拒否されます：

```
An error occurred (AuthorizationHeaderMalformed) when calling the
<operation> operation: The authorization header is malformed; the region
'<signing-region>' is wrong; expecting '<grid-default-region>'
```

- リージョンの適用は、グローバル名前空間が有効になる前に作成されたバケットを含め、グリッド上のすべてのバケットに適用されます。
- 地域制限はV4認証要求にのみ適用されます。匿名リクエストおよびV2リクエストは、地域制限の対象外です。

CreateBucket ルーティング

CreateBucket グローバル名前空間エンドポイント（`s3.company.com`）に送信されるリクエストは、任意のグリッドのロードバランサーエンドポイントにルーティングできます。リクエストは、リクエスト内の署名リージョンとデフォルトリージョンが一致するグリッドに自動的にルーティングされます。

例：

- グリッドAのデフォルトリージョンは `us-east-1`、グリッドBのデフォルトリージョンは `us-west-1` です。
- クライアントはCreateBucketリクエストを `s3.company.com` に送信します。署名リージョンは `us-west-1` です。
- ラウンドロビンDNSはリクエストをグリッドAに転送します。
- グリッドAはリクエストをグリッドBにルーティングします。
- バケットはグリッドB上に作成されます。

CreateBucket の追加の考慮事項：

- `LocationConstraint`要素は、グリッドのデフォルト領域または非デフォルト領域のいずれにも設定できます。これは、バケットを作成するグリッドではなく、ILM ポリシーにのみ影響します（`us-east-1`を使用した AWS の動作とは異なります）。
- リクエスト内の署名領域によって、どのグリッドがバケットを作成するかが決まります（署名領域は、ターゲットグリッドのデフォルト領域と一致する必要があります）。
- 署名済みのV4リクエストがサポートされています。
- 匿名リクエストおよびV2リクエストは、グローバルネームスペースルーティングではサポートされていません。

ListBucketsルーティング

ListBuckets グローバル名前空間エンドポイントに送信されたリクエストは、署名リージョンを使用して正しいグリッドを決定する CreateBucket リクエストと同様にルーティングされます。

HEAD Bucket も ListBuckets 応答のいずれにも、グリッドのデフォルトリージョンは含まれません。デフォルトのリージョンは署名リージョンによって暗黙的に指定され、グリッドのデフォルトリージョンと一致するように強制されます。

アカウントとアクセスキーの管理

テナントアカウントと S3 アクセスキーは、"アカウント同期"を使用してすべてのグリッド間で同期できますが、各グリッドがそれぞれ独自のアクセスキーセットを持っている場合でも、グローバル名前空間は機能します。個別のアクセスキーを使用する場合は、S3 クライアントが各グリッドにリクエストを送信する際に正しいアクセスキーを使用していることを確認してください。

次の手順

これで"グローバル名前空間を設定する"する準備が整いました。

グリッドフェデレーション用のグローバルネームスペースを設定する

複数の StorageGRID システムにまたがるバケットへのテナントアクセスを可能にするグローバル名前空間を設定します。

グローバル名前空間の詳細については、"グリッドフェデレーションのグローバルネームスペースについて"を参照してください。

開始する前に

- 各グリッドのGrid Managerに"サポートされている Web ブラウザ"を使用してサインインしています。
- 各グリッドの"rootアクセス権限"があります。
- グリッドフェデレーション接続の"考慮事項と要件"を確認しました。

グローバルネームスペースを構成するための要件

- グローバル名前空間内のすべてのグリッドは、グリッド間のすべてのペアにおいて、グローバル名前空間が有効になっているグリッドフェデレーション接続を持つ必要があります。
- 単一のグローバルネームスペースに参加できるグリッドの最大数は11（ローカルグリッド1つとリモート

グリッド10個）です。

> 10グリッド制限は、StorageGRID デプロイメントでサポートされるグリッドフェデレーション接続の最大総数によって制限されます。合計接続制限は、グローバル名前空間が有効になっていない接続も含め、デプロイメント内の*すべての*グリッドフェデレーション接続に適用されます。そのため、完全に接続されたグローバル名前空間とその他のグリッドフェデレーション接続の合計が、この全体的な制限を超えないようにする必要があります。

- S3クライアントは、署名バージョン4（SigV4）認証を使用する必要があります。匿名リクエストおよび署名バージョン2リクエストは、グローバルネームスペースルーティング操作ではサポートされていません。
  - 通常の署名付きリクエストは、 "リクエストの認証：認証ヘッダーの使用（AWS Signature Version 4）"に記載されているとおりに指定されます。
  - 事前署名済みのリクエストは、 "リクエストの認証：クエリパラメータの使用（AWS署名バージョン4）"に記載されているとおりに指定されます。

必要な接続数

グローバル名前空間では、すべてのグリッドのペアが接続されている必要があります。必要な接続数は、グリッドの数によって異なります。

グリッドの数	必要な接続数
2	1
3	3
4	6
5	10
n	$n \times (n - 1) / 2$

ステップ**1**：各グリッドに固有のデフォルトリージョンを設定する

グローバル名前空間内の各グリッドには、一意のデフォルト領域が必要です。デフォルト領域は、バケットを所有するグリッドを識別します。

CreateBucket および ListBuckets リクエストはこのリージョンに基づいてルーティングされ、その他のすべてのリクエストは送信先のデフォルトのリージョンと一致する必要があります。

詳細については、"S3リージョンを設定する"を参照してください。

手順

1. 各グリッドで、"デフォルトリージョンを一意の値に設定する"。たとえば、Grid A を `us-east-1`に設定し、Grid B を `us-west-1`に設定します。

ILMポリシーの目的で、"CreateBucket リクエスト"内の `LocationConstraint`要素を使用して設定されたデフォルト以外のリージョンを引き続き使用できます。デフォルト以外のリージョンは、グローバルネームスペース内のグリッド間で一意であるかどうかの検証は行われません。

2. グローバル名前空間内のすべてのグリッドに対して、この手順を繰り返します。各グリッドには、異なるデフォルト領域を設定する必要があります。
3. 必要に応じて追加のリージョンを設定してください。

ステップ**2**：**S3**グローバルネームスペース設定を構成する

グローバル名前空間内の各グリッドに、2つのS3エンドポイントドメイン名を追加します。

- すべてのグリッドで共通のグローバル名前空間エンドポイント
- グリッド固有のCNAME

外部DNSを設定することで、グローバル名前空間エンドポイントが1つ以上のグリッドに解決され、固有のCNAMEエンドポイントが特定のグリッドに解決されるようにします。

S3グローバルネームスペース設定を構成する前に、デフォルトリージョンを設定する必要があります。グローバル名前空間設定を有効にすると、正しいリージョンが指定されていない場合、S3リクエストは失敗します。すべてのS3リクエストは、グリッドのデフォルトリージョンで署名する必要があります。

手順

1. 各グリッドで、**Configuration** > **Network** > **S3 endpoint domain names** > **Domain names** を選択します。
2. すべてのグリッドで共通のグローバル名前空間エンドポイントドメイン名を追加します。例：`s3.example.com`。
3. グリッドに固有のCNAMEを追加します。例えば、 `s3.company.com`。
4. [保存（ Save ）] を選択します。
5. 「グローバル名前空間設定」を選択します。
   a. グローバル名前空間エンドポイントを選択してください。
   b. グリッド固有のCNAMEドメイン名を選択してください。
6. [保存（ Save ）] を選択します。
7. クライアントが使用するサーバー証明書に、新しいS3エンドポイントのドメイン名が含まれていることを確認してください。
   - クライアントが独自の証明書を使用するロードバランサエンドポイントに接続する場合は、"エンドポイントに関連付けられている証明書を更新します"。
   - クライアントがグローバルS3 API証明書を使用するロードバランサエンドポイントに接続するか、またはストレージノードに直接接続する場合は、を"グローバルS3 API証明書の更新"実行します。
8. グローバル名前空間内のすべてのグリッドに対して、これらの手順を繰り返してください。

詳細については、"S3エンドポイントのドメイン名を設定"を参照してください。

ステップ**3**：グローバル名前空間を有効にしたグリッドフェデレーション接続を作成する

すべてのグリッドでS3エンドポイントのドメイン名とデフォルトリージョンが設定されたら、グローバルネームスペースを有効にしたグリッドフェデレーション接続を作成できます。

タスクの内容

グリッドフェデレーション接続を作成し、グローバル名前空間を有効にすると、グローバル名前空間エンドポイント、CNAME、およびデフォルトリージョンの各フィールドには、前の手順で設定した値が自動的に入力されます。これらのフィールドが正しく設定されていない場合、グリッドマネージャーはグローバル名前空間の有効化を防止します。

> グローバル名前空間を使用したグリッドフェデレーション接続が作成された後、その接続内のグリッドのグローバル名前空間エンドポイント、CNAME、およびデフォルトリージョンは変更できません。

手順

1. 最初のグリッドでは、"グリッドフェデレーション接続を作成する"に記載されている手順に従ってください。
2. 接続の詳細を入力する際は、グローバル名前空間を有効にする を選択してください。

   グローバル名前空間エンドポイント、CNAME、およびデフォルトリージョンの各フィールドには、前の手順で設定した値が自動的に入力されます。いずれかの値が欠落しているか無効な場合、問題を解決するまでグローバル名前空間を有効にすることはできません。

3. 検証ファイルをダウンロードし、もう一方のグリッドにアップロードすることで、接続を完了してください。
4. グローバル名前空間内のすべてのグリッドのペアに対して、上記の手順を繰り返します。

   例えば、3つのグリッドがある場合、3つの接続（グリッドA–グリッドB、グリッドA–グリッドC、グリッドB–グリッドC）が必要です。グリッドが4つある場合、接続は6つ必要です。グローバル名前空間には、最大10個のグリッドを作成できます。必要な接続数を参照してください。

ステップ**4**：ロードバランサーのエンドポイントを設定する

"ロードバランサーエンドポイントを設定する" グローバル名前空間内の各グリッドについて。これらのエンドポイントには、すべて同じポートを使用してください。

> DNS解決を設定する前に、ロードバランサーのエンドポイントを設定してください。

ステップ**5**：**DNS**解決の設定

StorageGRID はグローバル名前空間用の組み込み DNS リゾルバを提供していません。S3 リクエストを正しいグリッドにルーティングするには、外部 DNS インフラストラクチャを設定する必要があります。

DNSリゾルバは次の要件を満たす必要があります：

1. グローバル名前空間エンドポイント（例： `s3.example.com`）を、通常はラウンドロビンDNSを使用して、1つまたは複数のグリッドのロードバランサーエンドポイントに解決します。
2. 各グリッドの固有の CNAME （例： `s3.grid-a.example.com`）を、その特定のグリッドのロードバランサーエンドポイントに解決します。

3. 仮想ホスト型バケットリクエストの場合（例： `bucket.s3.example.com`）、組織のルーティングポリシーを使用して、バケット名を適切なグリッドのCNAMEにマッピングします。

   StorageGRID は、どのグリッドがバケットを所有しているかを検出するための DNS ベースのメカニズムを提供していません。バケットの所有権に基づく自動ルーティングが必要な場合は、"テナント管理 API" を使用して ListBucket リクエストを発行し、バケットの UUID を返します。バケットの UUID からグリッドへの内部マッピングを維持してください。外部 DNS は、StorageGRID に直接クエリを実行するのではなく、そのマッピングを使用してください。

関連情報

- "グリッドフェデレーションとは"
- "グリッドフェデレーション接続を作成する"
- "S3エンドポイントのドメイン名を設定"
- "グリッドフェデレーション接続を管理します"

StorageGRID グリッド フェデレーション接続を管理

StorageGRID システム間のグリッドフェデレーション接続の管理には、接続の詳細の編集、証明書のローテーション、テナント権限の削除、未使用の接続の削除が含まれます。

開始する前に

- いずれかのグリッドで、を使用してGrid Managerにサインインしておき"サポートされている Web ブラウザ"ます。
- サインインしているグリッドのが"rootアクセス権限"必要です。

グリッドフェデレーション接続を編集します

グリッドフェデレーション接続を編集するには、接続内のいずれかのグリッドのプライマリ管理ノードにサインインします。最初のグリッドに変更を加えたら、新しい検証ファイルをダウンロードして、もう一方のグリッドにアップロードする必要があります。

> ⓘ 接続設定を編集している間は、アカウント同期やクロスグリッドレプリケーションのリクエストは、既存の接続設定を引き続き使用します。接続は一度に1つずつ編集し、接続ごとに1つの検証ファイルをリモートグリッドにアップロードする必要があります。編集内容は、リモートグリッドにアップロードされた後に適用されます。

接続の編集を開始します

手順

1. いずれかのグリッドのプライマリ管理ノードからGrid Managerにサインインします。
2. *ノード*を選択し、システム内の他のすべての管理ノードがオンラインであることを確認します。

グリッドフェデレーション接続を編集すると、StorageGRID は最初のグリッドのすべての管理ノードに「候補構成」ファイルを保存しようとします。このファイルをすべての管理ノードに保存できない場合は、*[保存してテスト]*を選択すると警告メッセージが表示されます。

3. 構成 > システム > グリッド フェデレーション を選択します。
4. [グリッドフェデレーション]ページの*[アクション]*メニューまたは特定の接続の詳細ページを使用して、接続の詳細を編集します。入力する内容については、を参照してください"グリッドフェデレーション接続を作成する"。

[Actions]メニュー

a. 接続のラジオボタンを選択します。
b. **>**[編集]*を選択します。
c. 新しい情報を入力します。

詳細ページ

a. 接続名を選択して詳細を表示します。
b. 「 * 編集 * 」を選択します。
c. 新しい情報を入力します。

5. サインインしているグリッドのプロビジョニングパスフレーズを入力します。
6. [保存して続行]*を選択します。

新しい値は保存されますが、別のグリッドに新しい検証ファイルをアップロードするまで接続に適用されません。

7. [検証ファイルのダウンロード]*を選択します。

後でこのファイルをダウンロードするには、接続の詳細ページに移動します。

8. ダウンロードしたファイル(`*connection-name*.grid-federation`を見つけ、安全な場所に保存します。

検証ファイルには秘密が含まれているため、安全に保存および送信する必要があります。

9. [Close]*を選択して、[Grid Federation]ページに戻ります。
10. が[編集保留中]*になっていることを確認します。

接続の編集を開始したときに接続ステータスが* Connected 以外の場合、 Pending edit *に変更されません。

11. もう一方のグリッドのファイルをグリッド管理者に提供し `*connection-name*.grid-federation`ます。

接続の編集を終了します

他のグリッドに検証ファイルをアップロードして、接続の編集を完了します。

手順

1. プライマリ管理ノードからGrid Managerにサインインします。
2. 構成 > システム > グリッド フェデレーション を選択します。
3. [検証ファイルのアップロード]*を選択して、アップロードページにアクセスします。
4. [検証ファイルのアップロード]*を選択します。次に、最初のグリッドからダウンロードしたファイルを参照して選択します。
5. 現在サインインしているグリッドのプロビジョニングパスフレーズを入力します。
6. [保存してテスト]*を選択します。

   編集した値を使用して接続を確立できる場合は、成功のメッセージが表示されます。それ以外の場合は、エラーメッセージが表示されます。メッセージを確認し、問題があれば対処します。

7. ウィザードを閉じて[Grid Federation]ページに戻ります。
8. [接続ステータス]*が[接続済み]*になっていることを確認します。
9. 最初のグリッドのグリッドフェデレーションページに移動し、ブラウザを更新します。[接続ステータス]*が[接続済み]*になっていることを確認します。
10. 接続が確立されたら、検証ファイルのすべてのコピーを安全に削除します。

グリッドフェデレーション接続をテストします

手順

1. プライマリ管理ノードからGrid Managerにサインインします。
2. 構成 > システム > グリッド フェデレーション を選択します。
3. [グリッドフェデレーション]ページの*[アクション]*メニューまたは特定の接続の詳細ページを使用して、接続をテストします。

   [Actions]メニュー

   a. 接続のラジオボタンを選択します。
   b. **>**[テスト]*を選択します。

   詳細ページ

   a. 接続名を選択して詳細を表示します。
   b. [接続のテスト *] を選択します。

4. 接続ステータスを確認します。

接続ステータス	製品説明
接続済み	両方のグリッドが接続され、正常に通信しています。

接続ステータス	製品説明
エラー	接続にエラーが発生しています。たとえば、証明書の有効期限が切れているか、設定値が無効になっている場合などです。
編集を保留中です	このグリッドで接続を編集しましたが、接続は既存の設定を使用しています。編集を完了するには、新しい検証ファイルをもう一方のグリッドにアップロードします。
接続を待機しています	このグリッドで接続が設定されていますが、もう一方のグリッドでは接続が完了していません。このグリッドから検証ファイルをダウンロードし、別のグリッドにアップロードします。
不明	接続の状態が不明です。ネットワーク問題 またはオフラインノードが原因である可能性があります。

5. 接続ステータスが*エラー*の場合は、問題を解決します。次に、もう一度*[Test connection]*を選択して、問題 が修正されたことを確認します。

[[rotate_grid_fed_certificates]接続証明書のローテーション

各グリッドフェデレーション接続は、自動生成された4つのSSL証明書を使用して接続を保護します。各グリッドの2つの証明書が有効期限に近づくと、* Expiration of grid federation certificate *アラートによって証明書のローテーションを促すメッセージが表示されます。

> 接続のいずれかの側の証明書が期限切れになると、接続は動作を停止し、証明書が更新されるまでレプリケーションは保留になります。

手順

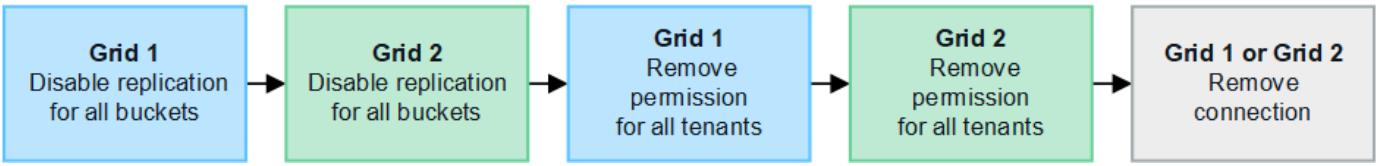
1. いずれかのグリッドのプライマリ管理ノードからGrid Managerにサインインします。
2. 構成 > システム > グリッド フェデレーション を選択します。
3. [Grid Federation]ページのいずれかのタブで、接続名を選択して詳細を表示します。
4. ［証明書］タブを選択します。
5. [証明書の回転]*を選択します。
6. 新しい証明書を有効にする日数を指定します。
7. サインインしているグリッドのプロビジョニングパスフレーズを入力します。
8. [証明書の回転]*を選択します。
9. 必要に応じて、接続のもう一方のグリッドで上記の手順を繰り返します。

   一般に、接続の両側の証明書には同じ日数を使用します。

グリッドフェデレーション接続を削除します

接続のいずれかのグリッドからグリッドフェデレーション接続を削除できます。次の図に示すように、両方のグリッドで前提条件となる手順を実行して、どちらのグリッドのテナントでも接続が使用されていないことを

確認する必要があります。



接続を削除する前に、次の点に注意してください。

- 接続を削除しても、グリッド間ですでにコピーされている項目は削除されません。たとえば、テナントの権限が削除されても、両方のグリッドに存在するテナントユーザ、グループ、およびオブジェクトはどちらのグリッドからも削除されません。これらのアイテムを削除する場合は、両方のグリッドから手動で削除する必要があります。
- 接続を削除すると、レプリケーションを保留している（取り込まれたがもう一方のグリッドにまだレプリケートされていない）オブジェクトのレプリケーションが永続的に失敗します。

すべてのテナントバケットでレプリケーションを無効にします

手順

1. いずれかのグリッドから、プライマリ管理ノードからGrid Managerにサインインします。
2. 構成 > システム > グリッド フェデレーション を選択します。
3. 接続名を選択して詳細を表示します。
4. [Permitted Tenants]*タブで、接続がテナントで使用されているかどうかを確認します。
5. テナントが表示されている場合は、すべてのテナントに、接続内の両方のグリッドですべてのバケットを使用するように指示し"グリッド間レプリケーションを無効にします"ます。

> テナントバケットでグリッド間レプリケーションが有効になっている場合は、* Use grid federation connection *権限を削除することはできません。各テナントアカウントは、両方のグリッドでバケットのグリッド間レプリケーションを無効にする必要があります。

各テナントの権限を削除します

すべてのテナントバケットでグリッド間レプリケーションを無効にしたら、両方のグリッドのすべてのテナントから* Use grid federation permission *を削除します。

手順

1. 構成 > システム > グリッド フェデレーション を選択します。
2. 接続名を選択して詳細を表示します。
3. 各テナントについて、**[Permitted Tenants]***タブで、各テナントから[Use Grid Federation connection]*権限を削除します。を参照して "許可されたテナントを管理する"
4. もう一方のグリッドで許可されたテナントについて、上記の手順を繰り返します。

接続を削除します

手順

1. どちらのグリッドでも接続を使用しているテナントがない場合は、*[削除]*を選択します。

2. 確認メッセージを確認し、*[削除]*を選択します。
    - 接続を削除できる場合は、成功を示すメッセージが表示されます。これで、グリッドフェデレーション接続が両方のグリッドから削除されます。
    - 接続を削除できない場合（まだ使用中、接続エラーなど）、エラーメッセージが表示されます。次のいずれかを実行できます。
        - エラーを解決します（推奨）。を参照して "グリッドフェデレーションエラーをトラブルシューティングする"
        - 力で接続を取り外します。次のセクションを参照してください。

グリッドフェデレーション接続を強制的に削除します

必要に応じて、ステータスが*connected*でない接続を強制的に削除できます。

強制的に削除すると、ローカルグリッドからのみ接続が削除されます。接続を完全に削除するには、両方のグリッドで同じ手順を実行します。

手順

1. 確認ダイアログボックスで*[強制削除]*を選択します。

    成功を示すメッセージが表示されます。このグリッドフェデレーション接続は使用できなくなります。ただし、テナントバケットでグリッド間レプリケーションが引き続き有効になっている場合や、接続内のグリッド間で一部のオブジェクトコピーがすでにレプリケートされている場合があります。

2. 接続のもう一方のグリッドで、プライマリ管理ノードからGrid Managerにサインインします。
3. 構成 > システム > グリッド フェデレーション を選択します。
4. 接続名を選択して詳細を表示します。
5. **[削除]***および[はい]*を選択します。
6. このグリッドから接続を削除するには、*[強制削除]*を選択します。

StorageGRID グリッド フェデレーションで許可されたテナントを管理する

S3テナントアカウントが複数の StorageGRID システム間で1つ以上のグリッドフェデレーション接続を使用することを許可できます。テナントが接続を使用することを許可されている場合、テナントの詳細情報を編集したり、テナントの接続使用許可を永久に削除したりするには、特別な手順が必要です。

開始する前に

- いずれかのグリッドで、を使用してGrid Managerにサインインしておき"サポートされている Web ブラウザ"ます。
- サインインしているグリッドのが"rootアクセス権限"必要です。
- 2つのグリッドの間にあります"グリッドフェデレーション接続を作成しました"。
- "アカウント同期"および"グリッド間レプリケーション"のワークフローを確認しました。
- 必要に応じて、接続内の両方のグリッドに対してシングル サインオン（SSO）またはIDフェデレーションを設定済みであることを確認してください。参照してください："グリッドフェデレーションのアカウント同期について"

許可されたテナントを作成します

新規または既存のテナントアカウントがアカウント同期とクロスグリッドレプリケーションにグリッドフェデレーション接続を使用できるようにするには、"新しいS3テナントを作成します"または"テナントアカウントを編集する"の一般的な手順に従い、以下の点に注意してください：

- テナントは、接続のどちらのグリッドからも作成できます。テナントが作成されるグリッドは、_tenantのソースグリッド_です。
- 接続のステータスは* connected *である必要があります。
- テナントを作成または編集して* Use grid federation connection *権限を有効にし、最初のグリッドに保存すると、同じテナントが自動的にもう一方のグリッドにレプリケートされます。テナントがレプリケートされているグリッドは、_テナントのデスティネーショングリッド_です。
- 両方のグリッドのテナントには、同じ20桁のアカウントID、名前、概要 、クォータ、および権限が割り当てられます。必要に応じて、*概要 *フィールドを使用して、ソーステナントとデスティネーションテナントを特定できます。たとえば、Grid 1に作成されたテナントの概要 は、Grid 2にレプリケートされたテナントの「This tenant was created on Grid 1」にも表示されます。
- セキュリティ上の理由から、ローカルrootユーザのパスワードはデスティネーショングリッドにコピーされません。

> ローカルrootユーザがデスティネーショングリッドでレプリケートされたテナントにサインインできるようにするには、そのグリッドのグリッド管理者が事前に必要です"ローカルrootユーザのパスワードを変更します"。

- 新しいテナントまたは編集したテナントが両方のグリッドで利用可能になると、テナントユーザは次の処理を実行できます。
  - 接続されているどのグリッドからでも、グループとローカルユーザーを作成できます。これらは、接続されている他のすべてのグリッドと自動的に同期されます。"テナントグループとユーザーを同期する"を参照してください。
  - ローカルユーザー向けに新しい S3 アクセスキーを作成します。テナントでアクセスキーの同期が有効になっている場合、これらのキーは接続されている他のグリッドに自動的に同期されます。

> フェデレーションユーザー用のS3アクセスキーは、作成時にソースからターゲットへ一度だけ複製されます。これらのS3アクセスキーが削除された場合、これらの変更は他のグリッドに同期されません。他のグリッド上のS3アクセスキーは手動で削除する必要があります。

  - 接続の両方のグリッドに同一のバケットを作成し、一方向または両方向のグリッド間レプリケーションを有効にします。を参照して "グリッド間レプリケーションを管理します"

許可されたテナントを表示します

グリッドフェデレーション接続の使用が許可されているテナントの詳細を確認できます。

手順

1. *テナント*を選択します。
2. [Tenants]ページで、テナント名を選択してテナントの詳細ページを表示します。
3. 必要に応じて「グリッドフェデレーション」タブを選択して、"グリッドフェデレーション接続を監視する"。

許可されたテナントを編集します

Use grid federation connection *権限があるテナントを編集する必要がある場合は、の一般的な手順に従って、"テナントアカウントを編集しています"次の点に注意してください。

- テナントが「グリッドフェデレーション接続を使用する」権限を持っている場合：
- 接続内のどのグリッドからでも、テナントの詳細を編集できます。テナントレベルの設定（名前、説明、割り当て量など）の変更、およびグループ、ローカルユーザー、ローカルユーザーが所有する S3 アクセスキーの変更は、接続されているすべてのグリッドに自動的に同期されます。
- *許可されたグリッドフェデレーション接続*は、_ソースグリッドでのみ_変更できます。
- 新しいグリッドフェデレーション接続を追加できます。

> 既存の接続を解除することはできません。接続を削除するには、テナントの詳細ページに移動し、*グリッドフェデレーション*タブを選択して、権限を削除します。

- テナントの編集中に新しい接続を追加すると、そのテナントは、その新しい接続で指定されたリモートグリッドに複製されます。

許可されたテナントを削除します

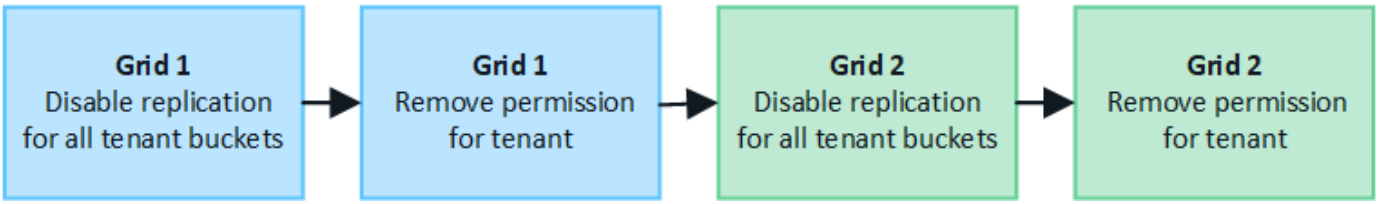
> ソースグリッドから元のテナントを削除するか、宛先グリッドから同期されたテナントを削除すると、そのテナントはすべてのグリッドから削除されるため、そのアカウントは使用できなくなります。

Use grid federation connection *権限が割り当てられているテナントを削除する必要がある場合は、の一般的な手順に従って、"テナントアカウントを削除しています"次の点に注意してください。

- ソースグリッドからテナントを削除する前に、ソースグリッド上の当該アカウントのすべてのバケットを削除する必要があります。
- 同期先グリッドから同期済みテナントを削除する前に、同期先グリッド上の該当アカウントのすべてのバケットを削除する必要があります。
- 元のテナントまたは同期されたテナントのいずれかを削除すると、そのアカウントはクロスグリッドレプリケーションに使用できなくなります。
- ソースグリッドまたは宛先グリッド上の元のテナントを削除すると、宛先グリッドに同期されていたテナントグループ、ユーザー、およびキーも削除されます。

グリッドフェデレーション接続の使用権限の削除

テナントがグリッドフェデレーション接続を使用できないようにするには、* Use grid federation connection *権限を削除する必要があります。



グリッドフェデレーション接続を使用するテナントの権限を削除する前に、次の点に注意してください。

- テナントのバケットでグリッド間レプリケーションが有効になっている場合は、* Use grid federation connection *権限を削除できません。テナントアカウントでは、まずすべてのバケットでグリッド間レプリケーションを無効にする必要があります。
- [Use grid federation connection]*権限を削除しても、グリッド間ですでにレプリケートされている項目は削除されません。たとえば、テナントの権限が削除されても、両方のグリッドに存在するテナントユーザ、グループ、およびオブジェクトはどちらのグリッドからも削除されません。これらのアイテムを削除する場合は、両方のグリッドから手動で削除する必要があります。
- 同じグリッドフェデレーション接続でこの権限を再度有効にする場合は、先にデスティネーショングリッドでこのテナントを削除してください。そうしないと、この権限を再度有効にするとエラーが発生します。

> *グリッドフェデレーション接続を使用する*権限を再度有効にすると、ローカルグリッドがソースグリッドとなり、選択したグリッドフェデレーション接続で指定されたリモートグリッドへの同期が開始されます。テナントアカウントが既にリモートグリッド上に存在する場合、同期処理中に競合エラーが発生します。

開始する前に

- を使用している"サポートされている Web ブラウザ"。
- 両方のグリッド用にが用意されてい"rootアクセス権限"ます。

テナントバケットのレプリケーションを無効にする

最初に、すべてのテナントバケットでグリッド間レプリケーションを無効にします。

手順

1. いずれかのグリッドから、プライマリ管理ノードからGrid Managerにサインインします。
2. 構成 > システム > グリッド フェデレーション を選択します。
3. 接続名を選択して詳細を表示します。
4. [Permitted Tenants]*タブで、テナントが接続を使用しているかどうかを確認します。
5. テナントが表示されている場合は、接続内の両方のグリッド上のすべてのバケットに対してテナントに指示し"グリッド間レプリケーションを無効にします"ます。

> テナントバケットでグリッド間レプリケーションが有効になっている場合は、* Use grid federation connection *権限を削除することはできません。テナントは、両方のグリッドでバケットのグリッド間レプリケーションを無効にする必要があります。

テナントの権限を削除します

テナントバケットでグリッド間レプリケーションを無効にしたら、グリッドフェデレーション接続を使用するテナントの権限を削除できます。

手順

1. プライマリ管理ノードからGrid Managerにサインインします。
2. [Grid Federation]ページまたは[Tenants]ページから権限を削除します。

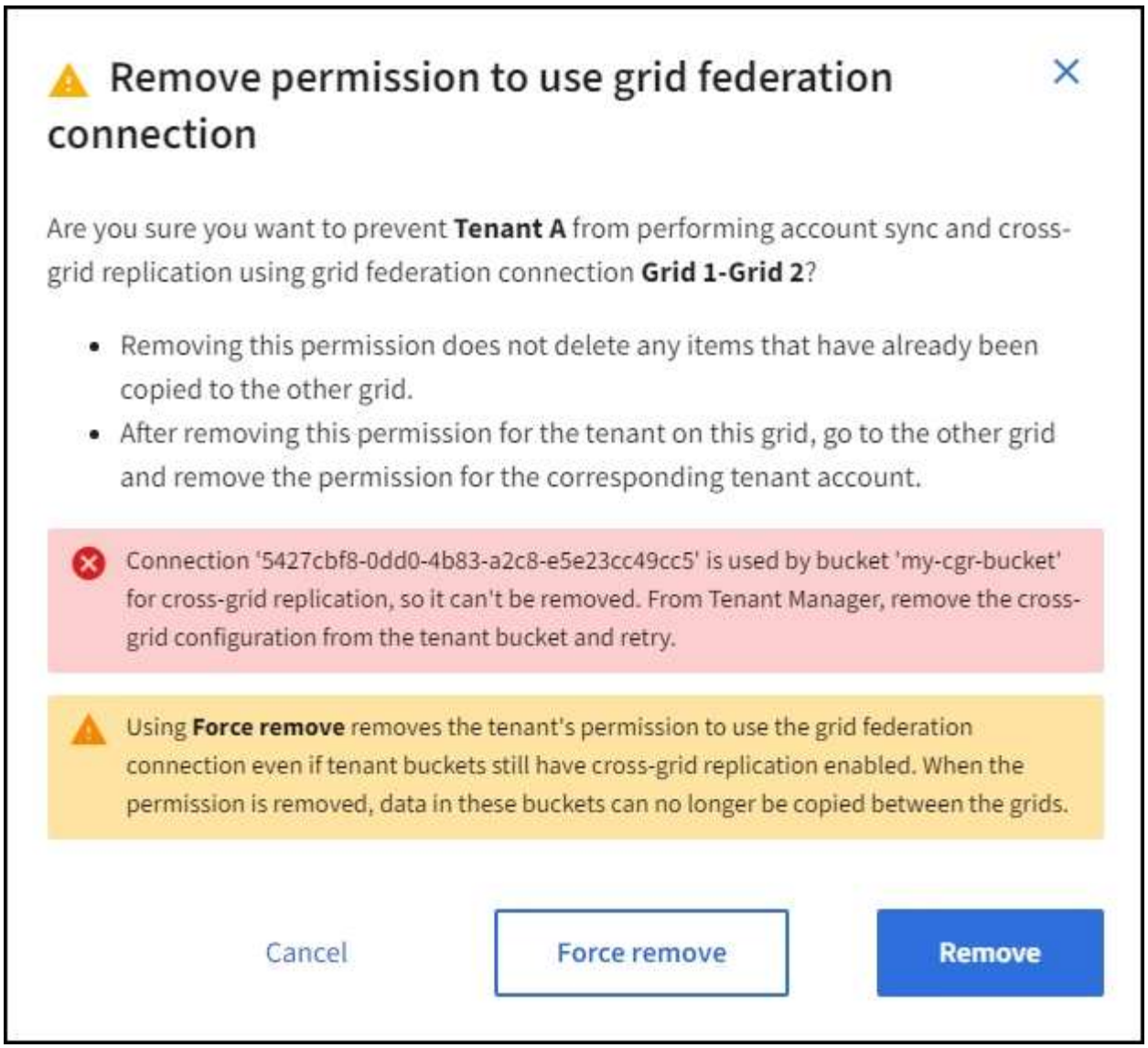
グリッドフェデレーションページ

a. 構成 > システム > グリッド フェデレーション を選択します。
b. 接続名を選択して詳細ページを表示します。
c. [Permitted Tenants]*タブで、テナントのラジオボタンを選択します。
d. [Remove Permission]*を選択します。

テナントページ

a. *テナント*を選択します。
b. テナントの名前を選択して詳細ページを表示します。
c. [グリッドフェデレーション]*タブで、接続のラジオボタンを選択します。
d. [Remove Permission]*を選択します。

3. 確認ダイアログボックスで警告を確認し、*[削除]*を選択します。
   - 権限を削除できる場合は、詳細ページに戻り、成功を示すメッセージが表示されます。このテナントはグリッドフェデレーション接続を使用できなくなります。
   - 1つ以上のテナントバケットでグリッド間レプリケーションが有効になっている場合は、エラーが表示されます。



次のいずれかを実行できます。

- （推奨）。Tenant Managerにサインインし、テナントのバケットごとにレプリケーションを無効にします。を参照して "グリッド間レプリケーションを管理します"次に、手順を繰り返して* Use grid connection *権限を削除します。
- 権限を強制的に削除します。次のセクションを参照してください。

4. もう一方のグリッドに移動して上記の手順を繰り返し、もう一方のグリッド上の同じテナントに対する権限を削除します。

権限を強制的に削除します

テナントバケットでグリッド間レプリケーションが有効になっている場合でも、必要に応じて、グリッドフェデレーション接続を使用するテナントの権限を強制的に削除できます。

テナントの権限を強制的に削除する前に、の一般的な考慮事項と次の追加の考慮事項に注意してください権限を削除しています。

- [Use grid federation connection]*権限を強制的に削除した場合、他のグリッドへのレプリケーションを保留中の（取り込まれたがまだレプリケートされていない）オブジェクトは引き続きレプリケートされま

す。これらのインプロセスオブジェクトがデスティネーションバケットに到達しないようにするには、もう一方のグリッドに対するテナントの権限も削除する必要があります。

- [Use grid federation connection]*権限を削除したあとにソースバケットに取り込まれたオブジェクトは、デスティネーションバケットにレプリケートされません。

手順

1. プライマリ管理ノードからGrid Managerにサインインします。
2. 構成 > システム > グリッド フェデレーション を選択します。
3. 接続名を選択して詳細ページを表示します。
4. [Permitted Tenants]*タブで、テナントのラジオボタンを選択します。
5. [Remove Permission]*を選択します。
6. 確認ダイアログボックスで警告を確認し、*[強制的に削除]*を選択します。

   成功を示すメッセージが表示されます。このテナントはグリッドフェデレーション接続を使用できなくなります。

7. 必要に応じて、もう一方のグリッドに移動して上記の手順を繰り返し、もう一方のグリッドの同じテナントアカウントに対する権限を強制的に削除します。たとえば、処理中のオブジェクトがデスティネーションバケットに到達しないように、もう一方のグリッドで上記の手順を繰り返します。

StorageGRID でグリッドフェデレーションのエラーをトラブルシューティングします

グリッド連携接続、アカウント同期、およびグリッド間レプリケーションに関連するアラートやエラーのトラブルシューティングが必要になる場合があります。

グリッドフェデレーション接続のアラートとエラー

グリッドフェデレーション接続でアラートを受信したり、エラーが発生したりすることがあります。

接続問題 を解決するための変更を行った後、接続をテストして、接続ステータスが*接続済み*に戻ることを確認します。手順については、を参照してください"グリッドフェデレーション接続を管理します"。

Grid Federation Connection Failureアラート

問題

Grid federation connection failure *アラートがトリガーされました。

詳細

グリッド間のグリッド連携接続が機能していない可能性があります。

推奨される対処方法

1. 両方のグリッドの[Grid Federation]ページで設定を確認します。すべての値が正しいことを確認します。を参照して "グリッドフェデレーション接続を管理します"
2. 接続に使用した証明書を確認します。有効期限が切れたグリッドフェデレーション証明書に関するアラートがないこと、および各証明書の詳細が有効であることを確認してください。の接続証明書のローテーション手順を参照してください"グリッドフェデレーション接続を管理します"。
3. 両方のグリッドのすべての管理ノードとゲートウェイノードがオンラインで使用可能であることを確認し

ます。これらのノードに影響している可能性があるアラートを解決してから再試行してください。

4. ローカルまたはリモートのグリッドの完全修飾ドメイン名（FQDN）を指定した場合は、DNSサーバがオンラインで使用可能であることを確認します。ネットワーク、IPアドレス、およびDNSの要件については、を参照してください"グリッドフェデレーションとは"。

Gridフェデレーション証明書の有効期限に関するアラート

問題

Expiration of grid federation certificate *アラートがトリガーされました。

詳細

このアラートは、1つ以上のグリッドフェデレーション証明書の有効期限が近づいていることを示しています。

推奨される対処方法

の接続証明書のローテーション手順を参照してください"グリッドフェデレーション接続を管理します"。

グリッドフェデレーション接続の編集中にエラーが発生しました

問題

グリッドフェデレーション接続を編集するときに、*[保存してテスト]*を選択すると、「1つ以上のノードで候補構成ファイルを作成できませんでした」という警告メッセージが表示されます。

詳細

グリッドフェデレーション接続を編集すると、StorageGRID は最初のグリッドのすべての管理ノードに「候補構成」ファイルを保存しようとします。管理ノードがオフラインの場合など、このファイルをすべての管理ノードに保存できない場合は、警告メッセージが表示されます。

推奨される対処方法

1. 接続を編集するために使用しているグリッドから、*ノード*を選択します。
2. そのグリッドのすべての管理ノードがオンラインであることを確認します。
3. オフラインになっているノードがある場合は、それらのノードをオンラインに戻し、接続の編集をやり直します。

アカウント同期エラー

同期されたテナントアカウントにサインインできません

問題

同期済みのテナントアカウントにはサインインできません。テナントマネージャーのサインインページに表示されるエラーメッセージは「このアカウントの認証情報が無効です。もう一度お試しください。」

詳細

テナントのローカルルートユーザーおよびその他のローカルユーザーに設定したパスワードは、自動的に同期されます。ただし、そのグリッド上のテナントアカウントにサインインする前に、宛先グリッド上のテナントのローカルルートユーザーのパスワードを変更する必要がある場合があります。

推奨される対処方法

rootユーザがテナントのデスティネーショングリッドにサインインする前に、グリッド管理者がデスティネーショングリッドで最初にサインインする必要があります"ローカルrootユーザのパスワードを変更します"。

同期なしで作成されたテナント

問題

「グリッドフェデレーション接続を使用する」権限で新しいテナントを作成すると、「同期なしでテナントが作成されました」というメッセージが表示されます。

詳細

この問題 は、接続ステータスの更新が遅延した場合に発生する可能性があります原因 。これにより、正常でない接続が*接続済み*として表示される可能性があります。

推奨される対処方法

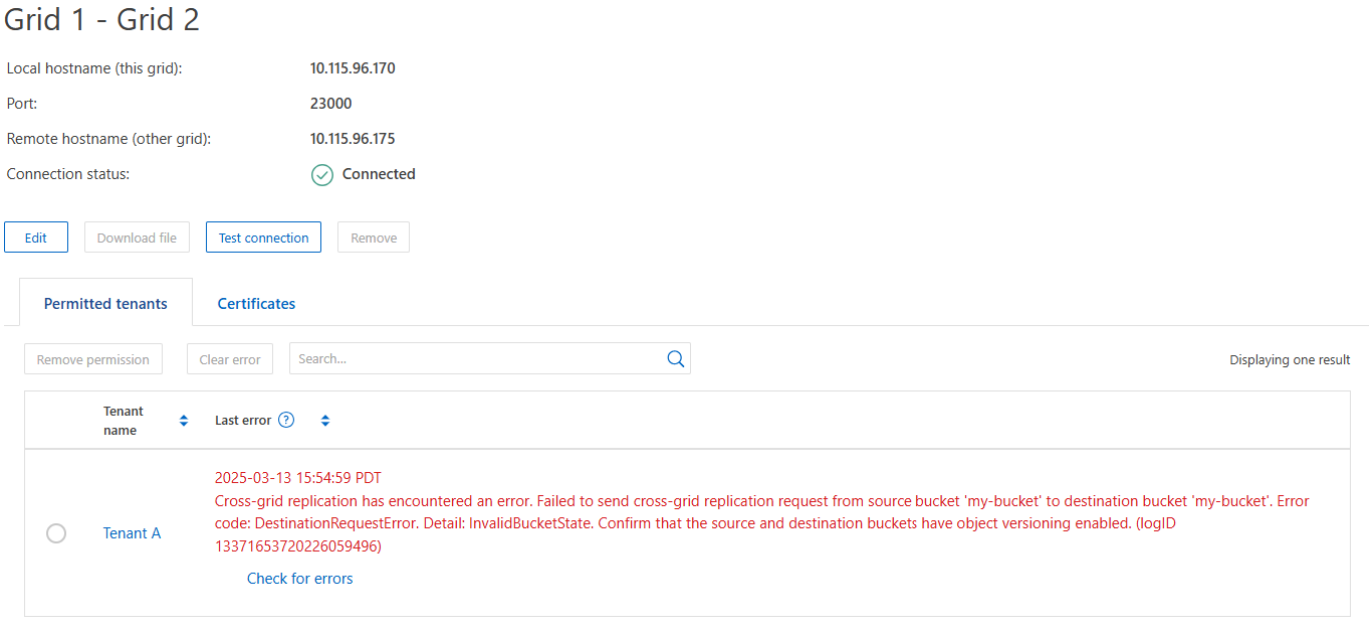
1. エラーメッセージに表示された理由を確認し、接続を妨げる可能性のあるネットワークまたはその他の問題を解決します。を参照して グリッドフェデレーション接続のアラートとエラー
2. 手順に従ってでグリッドフェデレーション接続をテストし"グリッドフェデレーション接続を管理します"、問題が解決されたことを確認します。
3. テナントのソース グリッドから、テナント を選択します。
4. 同期に失敗したテナントアカウントを特定してください。
5. テナント名を選択して詳細ページを表示します。
6. 「同期を再試行」を選択します。エラーが解決された場合、テナントアカウントは他のグリッドと同期されます。

グリッド間レプリケーションのアラートとエラー

接続またはテナントについて表示された最後のエラー

問題

接続の場合"グリッドフェデレーション接続の表示"（または接続の場合"許可されたテナントの管理"）、接続の詳細ページの* Last error *列にエラーが表示されます。例：



列に表示されるメッセージを示すスクリーンショット"]

詳細

各グリッド フェデレーション接続の 最後のエラー 列には、テナントのデータが他のグリッドに複製されているときに発生した最新のエラー (ある場合) が表示されます。この列には、最後に発生したグリッド間レプリケーション エラーのみが表示されます。以前に発生した可能性のあるエラーは表示されません。この列のエラーは、次のいずれかの理由で発生する可能性があります。

- ソース オブジェクトのバージョンが見つかりませんでした。
- ソースバケットが見つかりませんでした。
- デスティネーションバケットが削除されました。
- デスティネーションバケットが別のアカウントで再作成されました。
- デスティネーションバケットのバージョン管理が中断されています。
- デスティネーションバケットが同じアカウントで再作成されましたが、現在バージョン管理されていません。
- ソース オブジェクトの S3 オブジェクト ロック設定が、宛先グリッドのテナント レベルの保持設定に準拠していません。
- ソース オブジェクトには S3 オブジェクト ロック設定があり、宛先バケットでは S3 オブジェクト ロックが無効になっています。

推奨される対処方法

「* Last error *」列にエラーメッセージが表示された場合は、次の手順を実行します。

1. メッセージテキストを確認します。
2. 推奨された措置をすべて実行してください。

   例えば、クロスグリッドレプリケーションの宛先バケットでバージョン管理が一時停止されていた場合は、そのバケットのバージョン管理を再度有効にします。または、クロスグリッドレプリケーションの宛先バケットで S3 Object Lock が無効になっている場合は、そのバケットで S3 Object Lock を有効にします。

3. テーブルから接続またはテナントアカウントを選択します。
4. [Clear error]*を選択します。
5. メッセージをクリアしてシステムのステータスを更新するには、*はい*を選択します。
6. 5~6分待ってから、新しいオブジェクトをバケットに取り込みます。エラーメッセージが再表示されないことを確認します。

> エラーメッセージがクリアされるように、メッセージのタイムスタンプから5分以上経過してから新しいオブジェクトを取り込んでください。

> エラーをクリアしたあとに、同じくエラーが発生している別のバケットにオブジェクトを取り込んだ場合は、新しい* Last error *が表示されることがあります。

7. バケットエラーが原因でレプリケートに失敗したオブジェクトがないかどうかを確認するには、を参照してください"失敗したレプリケーション処理を特定して再試行します"。

Cross-grid replication permanent failureアラート

問題

Cross-grid replication permanent failure *アラートがトリガーされました。

詳細

このアラートは、ユーザによる解決が必要な理由で、2つのグリッド上のバケット間でテナントオブジェクトをレプリケートできない場合に表示されます。このアラートの主な原因は、ソースまたはデスティネーションのバケットが変更されたことです。

推奨される対処方法

1. アラートがトリガーされたグリッドにサインインします。
2. 構成 > システム > グリッド フェデレーション に移動し、アラートにリストされている接続名を見つけます。
3. [Permitted Tenants]タブで、* Last error *列を確認し、エラーが発生しているテナントアカウントを特定します。
4. 障害の詳細については、の手順を参照"グリッドフェデレーション接続を監視する"して、グリッド間レプリケーションの指標を確認してください。
5. 影響を受ける各テナントアカウント：
   a. テナントがグリッド間レプリケーションのデスティネーショングリッドでのクォータを超えていないことを確認するには、の手順を参照してください"テナントのアクティビティを監視する"。
   b. 必要に応じて、デスティネーショングリッドでのテナントのクォータを増やして、新しいオブジェクトを保存できるようにします。
6. 影響を受ける各テナントについて、両方のグリッドでTenant Managerにサインインしてバケットのリストを比較できるようにします。
7. クロスグリッドレプリケーションが有効になっている各バケットについて、次の点を確認します。
   - もう一方のグリッドには、同じテナントに対応するバケットがあります（正確な名前を使用する必要があります）。
   - どちらのバケットでもオブジェクトのバージョン管理が有効になっています（どちらのグリッドでも

バージョン管理を一時停止することはできません）。

- どちらのバケットも「* Deleting objects：read-only *」状態ではありません。

8. 問題が解決されたことを確認するには、の手順を参照し"グリッドフェデレーション接続を監視する"てクロスグリッドレプリケーションの指標を確認するか、次の手順を実行します。

   a. [Grid Federation]ページに戻ります。

   b. 影響を受けるテナントを選択し、* Last error 列で Clear Error *を選択します。

   c. メッセージをクリアしてシステムのステータスを更新するには、*はい*を選択します。

   d. 5~6分待ってから、新しいオブジェクトをバケットに取り込みます。エラーメッセージが再表示されないことを確認します。

   エラーメッセージがクリアされるように、メッセージのタイムスタンプから5分以上経過してから新しいオブジェクトを取り込んでください。

   解決後にアラートがクリアされるまでに最大1日かかることがあります。

   a. に進み、"失敗したレプリケーション処理を特定して再試行します"他のグリッドにレプリケートできなかったオブジェクトを特定するかマーカーを削除し、必要に応じてレプリケーションを再試行します。

Cross-grid replication resource unavailableアラート

問題

Cross-grid replication resource unavailable *アラートがトリガーされました。

詳細

このアラートは、リソースを使用できないためにグリッド間のレプリケーション要求が保留中であることを示しています。たとえば、ネットワークエラーが発生している可能性があります。

推奨される対処方法

1. アラートを監視して、問題 が自動的に解決するかどうかを確認します。
2. 問題 が解消されない場合は、いずれかのグリッドに同じ接続に対する* Grid federation connection failure アラートが表示されているか、またはノードに対して Unable to communicate with node *アラートが表示されているかを確認します。このアラートは、アラートを解決すると解決される場合があります。
3. 障害の詳細については、の手順を参照"グリッドフェデレーション接続を監視する"して、グリッド間レプリケーションの指標を確認してください。
4. アラートを解決できない場合は、テクニカルサポートにお問い合わせください。

問題 の解決後、グリッド間レプリケーションは通常どおり続行されます。

失敗した**StorageGRID**レプリケーション処理を特定して再試行する

Cross-grid replication permanent failure *アラートを解決したら、他のグリッドへのレプリケートに失敗したオブジェクトまたは削除マーカーがないかどうかを確認する必要があります。その後、これらのオブジェクトを再取り込みするか、グリッド管理APIを使用してレプリケーションを再試行できます。

Cross-grid replication permanent failure *アラートは、ユーザの介入が必要な理由で2つのグリッド上のバケット間でテナントオブジェクトをレプリケートできないことを示しています。このアラートの主な原因は、ソースまたはデスティネーションのバケットが変更されたことです。詳細については、を参照してください "グリッドフェデレーションエラーをトラブルシューティングする"。

レプリケートに失敗したオブジェクトがないかどうかを確認します

他のグリッドにレプリケートされていないオブジェクトまたは削除マーカーがないかどうかを確認するには、監査ログでメッセージを検索し"CGRR（クロスグリッドレプリケーション要求）"ます。このメッセージは、StorageGRID がオブジェクト、マルチパートオブジェクト、または削除マーカーをデスティネーションバケットにレプリケートできなかった場合にログに追加されます。

を使用すると、結果を読みやすい形式に変換できます"audit-explainツール"。

開始する前に

- Root Access 権限が割り当てられている。
- あなたはファイルを持ってい `Passwords.txt`ます。
- プライマリ管理ノードのIPアドレスを確認しておきます。

手順

1. プライマリ管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`
   b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

      rootとしてログインすると、プロンプトがからに `#`変わります `$`。

2. audit.logでCGRRメッセージを検索し、audit-explainツールを使用して結果をフォーマットします。

   たとえば、このコマンドは過去30分間のすべてのCGRRメッセージをgrepし、audit-explainツールを使用します。

   ```
   # awk -vdate=$(date -d "30 minutes ago" '+%Y-%m-%dT%H:%M:%S') '$1$2 >= date { print }' audit.log | grep CGRR | audit-explain
   ```

   このコマンドの結果は次の例のようになります。この例には、6つのCGRRメッセージのエントリがあります。この例では、オブジェクトをレプリケートできなかったため、すべてのグリッド間レプリケーション要求で一般的なエラーが返されています。最初の3つのエラーは「オブジェクトのレプリケート」処理に関するもので、最後の3つのエラーは「マーカーのレプリケート」処理に関するものです。

```
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
object" bucket:bucket123 object:"audit-0"
version:QjRBNDIzODAtNjQ3My0xMUVELTg2QjEtODJBMjAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
object" bucket:bucket123 object:"audit-3"
version:QjRDOTRCOUMtNjQ3My0xMUVELTkzM0YtOTg1MTAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
delete marker" bucket:bucket123 object:"audit-1"
version:NUQ0OEYxMDAtNjQ3NC0xMUVELTg2NjMtOTY5NzAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
delete marker" bucket:bucket123 object:"audit-5"
version:NUQ1ODUwQkUtNjQ3NC0xMUVELTg1NTItRDkwNzAwQkI3NEM4 error:general
error
```

各エントリには、次の情報が含まれています。

フィールド	製品説明
CGRRクロスグリッドレプリケーション要求	要求の名前
テナント	テナントのアカウントID
接続	グリッドフェデレーション接続のID
操作	試行されたレプリケーション操作のタイプ。 • オブジェクトをレプリケートします • 削除マーカーを複製します • マルチパートオブジェクトをレプリケートします
バケット	バケット名
オブジェクト	オブジェクト名
バージョン	オブジェクトのバージョンID

フィールド	製品説明
エラー	エラーのタイプ。グリッド間レプリケーションに失敗した場合は、「General error」というエラーが表示されます。

失敗したレプリケーションを再試行します

デスティネーションバケットにレプリケートされなかったオブジェクトのリストを生成して削除マーカーを削除し、根本的な問題を解決したら、次のいずれかの方法でレプリケーションを再試行できます。

- 各オブジェクトをソースバケットに再度取り込みます。
- の説明に従って、グリッド管理プライベートAPIを使用します。

手順

1. Grid Managerの上部でヘルプアイコンを選択し、*[API documentation]*を選択します。
2. [Go to private API documentation]*を選択します。

   「プライベート」とマークされたStorageGRID APIエンドポイントは、予告なく変更される場合があります。StorageGRID プライベートエンドポイントは、要求の API バージョンも無視します。

3. [cross-grid-replication-advanced]*セクションで、次のエンドポイントを選択します。

   ```
   POST /private/cross-grid-replication-retry-failed
   ```

4. [* 試してみてください *] を選択します。
5. body テキストボックスで、 versionId *のサンプルエントリを、失敗したグリッド間レプリケーション要求に対応するaudit.logのバージョンIDに置き換えます。

   文字列は必ず二重引用符で囲んでください。

6. [* Execute] を選択します。
7. サーバ応答コードが「* 204 *」であることを確認します。これは、オブジェクトまたは削除マーカーが他のグリッドへのクロスグリッドレプリケーションのために保留中としてマークされていることを示します。

   Pendingは、クロスグリッドレプリケーション要求が処理のために内部キューに追加されたことを示します。

レプリケーションの再試行を監視します

レプリケーションの再試行処理を監視して、処理が完了していることを確認する必要があります。

オブジェクトまたは削除マーカーが他のグリッドにレプリケートされるまでに数時間以上かかることがあります。

再試行処理は、次の2つの方法で監視できます。

- S3または"GetObject"要求を使用"ヘッドオブジェクト"応答には、次のいずれかの値を持つStorageGRID固有の応答ヘッダーが含まれ `x-ntap-sg-cgr-replication-status`ます。

グリッド	レプリケーションのステータス
ソース	• 完了:レプリケーションは成功しました。 • * pending*：オブジェクトはまだレプリケートされていません。 • **failure**:レプリケーションが永続的なエラーで失敗しました。ユーザーはエラーを解決する必要があります。
デスティネーション	**replica**:オブジェクトはソースグリッドからレプリケートされました。

- の説明に従って、グリッド管理プライベートAPIを使用します。

手順

1. プライベートAPIドキュメントの* cross-grid-replication-advanced *セクションで、次のエンドポイントを選択します。

   ```
   GET /private/cross-grid-replication-object-status/{id}
   ```

2. [* 試してみてください *] を選択します。
3. [Parameter]セクションに、要求で使用したバージョンIDを入力し `cross-grid-replication-retry-failed`ます。
4. [* Execute] を選択します。
5. サーバ応答コードが*200*であることを確認します。
6. レプリケーションステータスを確認します。次のいずれかになります。
   - * pending*：オブジェクトはまだレプリケートされていません。
   - 完了:レプリケーションは成功しました。
   - **failed**:レプリケーションは永続的なエラーで失敗しました。ユーザーはエラーを解決する必要があります。

セキュリティを管理します

StorageGRID でセキュリティを管理する

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

暗号化を管理します

StorageGRID には、データを暗号化するためのいくつかのオプションがあります。データ保護の要件を満たすものを特定する必要があります"使用可能な暗号化方式を確認します"。

証明書の管理

を使用すると、HTTP接続またはサーバに対するクライアントIDまたはユーザIDの認証に使用するクライアント証明書を使用できます"サーバ証明書を設定および管理します"。

キー管理サーバを設定

を使用する"キー管理サーバ"と、アプライアンスがデータセンターから取り外された場合でも、StorageGRIDデータを保護できます。アプライアンスボリュームが暗号化されると、ノードがKMSと通信できないかぎり、アプライアンスのデータにアクセスすることはできません。

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

プロキシ設定を管理します

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

ファイアウォールを制御します

システムのセキュリティを強化するために、で特定のポートを開いたり閉じたりして、StorageGRID管理ノードへのアクセスを制御でき"外部ファイアウォール"ます。各ノードのを設定して、各ノードへのネットワークアクセスを制御することもできます"内部ファイアウォール"。導入に必要なポート以外のすべてのポートでアクセスを禁止できます。

StorageGRID の暗号化方式を確認します

StorageGRID には、データを暗号化するためのいくつかのオプションがあります。使用可能な方法を確認して、データ保護の要件を満たす方法を決定する必要があります。

次の表に、 StorageGRID で使用できる暗号化方式の概要を示します。

暗号化オプション	仕組み	環境
Grid Manager からキー管理サーバ（ KMS ）を取得します	StorageGRIDサイトのユーザ"キー管理サーバを設定"と "アプライアンスのノード暗号化を有効にします"。次に、アプライアンスノードが KMS に接続して、 Key Encryption Key （ KEK ；キー暗号化キー）を要求します。このキーは、各ボリュームのデータ暗号化キー（ DEK ）を暗号化および復号化します。	インストール中にノード暗号化 * が有効になっているアプライアンスノード。アプライアンスのすべてのデータは、物理的な損失やデータセンターからの削除から保護されます。 注：KMSを使用した暗号化キーの管理は、ストレージノードとサービスアプライアンスでのみサポートされます。

暗号化オプション	仕組み	環境
StorageGRIDアプライアンスインストーラの[Drive Encryption]ページ	アプライアンスにハードウェア暗号化をサポートするドライブが含まれている場合は、インストール時にドライブパスフレーズを設定できます。ドライブパスフレーズを設定すると、パスフレーズを知らない限り、システムから削除されたドライブから有効なデータを復元することはできません。インストールを開始する前に、**[ハードウェアの設定]**>*[ドライブ暗号化]*に移動し、ノード内のすべてのStorageGRIDが管理する自己暗号化ドライブを環境に設定します。	自己暗号化ドライブを搭載したアプライアンス。セキュリティ保護されたドライブ上のデータは、すべて物理的な損失やデータセンターからの削除から保護されます。 ドライブ暗号化はSANtricity管理ドライブには適用されません。自己暗号化ドライブとSANtricityコントローラを搭載したストレージアプライアンスを使用している場合は、SANtricityでドライブセキュリティを有効にすることができます。
SANtricity System Manager のドライブセキュリティ	StorageGRIDアプライアンスでドライブセキュリティ機能が有効になっている場合は、を使用してセキュリティキーを作成および管理できます "SANtricityシステムマネージャ"。このキーは、セキュリティ保護されたドライブ上のデータにアクセスするために必要です。	Full Disk Encryption（FDE）ドライブまたは自己暗号化ドライブを搭載したストレージアプライアンス。セキュリティ保護されたドライブ上のデータは、すべて物理的な損失やデータセンターからの削除から保護されます。一部のストレージアプライアンスまたはサービスアプライアンスでは使用できません。
格納オブジェクトの暗号化	オプションは、Grid Managerで有効にし"格納オブジェクトの暗号化"ます。有効にすると、バケットレベルまたはオブジェクトレベルで暗号化されていない新しいオブジェクトが取り込み時に暗号化されます。	新しく取り込まれたS3オブジェクトデータ。 既存の格納オブジェクトは暗号化されません。オブジェクトメタデータやその他の機密データは暗号化されません。
S3 バケットの暗号化	PutBucketEncryption要求を問題して、バケットの暗号化を有効にします。オブジェクトレベルで暗号化されていない新しいオブジェクトは、取り込み時に暗号化されます。	新たに取り込まれた S3 オブジェクトデータのみ。 バケットに対して暗号化を指定する必要があります。既存のバケットオブジェクトは暗号化されません。オブジェクトメタデータやその他の機密データは暗号化されません。 "バケットの処理"

暗号化オプション	仕組み	環境
S3 オブジェクトのサーバ側の暗号化（ SSE ）	オブジェクトを格納するS3要求を実行し、要求ヘッダーを含め `x-amz-server-side-encryption`ます。	新たに取り込まれた S3 オブジェクトデータのみ。 オブジェクトに対して暗号化を指定する必要があります。オブジェクトメタデータやその他の機密データは暗号化されません。 キーは StorageGRID で管理されます。 "サーバ側の暗号化を使用します"
ユーザ指定のキーによる S3 オブジェクトのサーバ側暗号化（ SSE-C ）	オブジェクトを格納する S3 要求を問題 し、 3 つの要求ヘッダーを含めます。 • `x-amz-server-side-encryption-customer-algorithm` • `x-amz-server-side-encryption-customer-key` • `x-amz-server-side-encryption-customer-key-MD5`	新たに取り込まれた S3 オブジェクトデータのみ。 オブジェクトに対して暗号化を指定する必要があります。オブジェクトメタデータやその他の機密データは暗号化されません。 キーは StorageGRID の外部で管理されます。 "サーバ側の暗号化を使用します"
外部ボリュームまたはデータストアの暗号化	導入プラットフォームで暗号化がサポートされている場合は、StorageGRID の外部の暗号化方式を使用して、ボリュームまたはデータストア全体を暗号化できます。	すべてのボリュームまたはデータストアが暗号化されていることを前提として、すべてのオブジェクトデータ、メタデータ、およびシステム構成データ。 外部暗号化方式を使用すると、暗号化アルゴリズムと暗号キーを厳密に制御できます。は、記載されている他の方法と組み合わせることができます。

暗号化オプション	仕組み	環境
StorageGRID の外部でのオブジェクトの暗号化	StorageGRID に取り込まれる前にオブジェクトデータとメタデータを暗号化するには、 StorageGRID の外部の暗号化メソッドを使用します。	オブジェクトデータとメタデータのみ（システム設定データは暗号化されません）。 外部暗号化方式を使用すると、暗号化アルゴリズムと暗号キーを厳密に制御できます。は、記載されている他の方法と組み合わせることができます。 "Amazon Simple Storage Service - ユーザガイド：クライアント側の暗号化を使用したデータの保護"

複数の暗号化方式を使用します

要件に応じて、一度に複数の暗号化方式を使用できます。例：

- KMSを使用してアプライアンスノードを保護できます。また、SANtricity System Managerのドライブセキュリティ機能を使用して、同じアプライアンス内の自己暗号化ドライブのデータを二重に暗号化することもできます。
- KMSを使用してアプライアンスノード上のデータを保護できます。また、[Stored Object Encryption]オプションを使用して、取り込み時にすべてのオブジェクトを暗号化することもできます。

暗号化を必要とするオブジェクトがごく一部しかない場合は、暗号化をバケットレベルまたは個々のオブジェクトレベルで制御することを検討してください。複数レベルの暗号化を有効にすると、パフォーマンスコストが増加します。

関連情報

"FIPS認定の暗号化オプションについて学ぶ"

証明書の管理

StorageGRIDでセキュリティ証明書を管理する

セキュリティ証明書は、 StorageGRID コンポーネント間、および StorageGRID コンポーネントと外部システム間のセキュアで信頼された接続の確立に使用される小さいデータファイルです。

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

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

クライアントが HTTPS を使用してサーバーに接続すると、サーバーは公開キーを含むサーバー証明書で応答

します。クライアントは、サーバーの署名を証明書のコピーの署名と比較します。署名が一致する場合、クライアントは同じ公開鍵を使用してサーバーとのセッションを開始します。

StorageGRID は、一部の接続（ロードバランサエンドポイントなど）のサーバとして、または他の接続（ CloudMirror レプリケーションサービスなど）のクライアントとして機能します。

- デフォルトの Grid CA 証明書 *

StorageGRID には、システムのインストール中に内部グリッド CA 証明書を生成する証明機関 (CA) が組み込まれています。デフォルトでは、グリッド CA 証明書が、内部StorageGRIDトラフィックのセキュリティ保護に使用されます。外部証明機関 (CA) は、組織の情報セキュリティ ポリシーに完全に準拠したカスタム証明書を発行できます。

非実稼働環境では Grid CA 証明書を使用します。運用環境では、外部の証明機関によって署名されたカスタム証明書を使用します。証明書のない安全でない接続はサポートされていますが、推奨されません。

- カスタムCA証明書は内部証明書を削除しません。ただし、カスタム証明書は、サーバ接続の確認用に指定した証明書である必要があります。
- すべてのカスタム証明書がを満たしている必要があります"サーバ証明書に関するシステムセキュリティ強化ガイドライン"。
- StorageGRID では、 CA からの証明書を 1 つのファイル（ CA 証明書バンドル）にバンドルすることがサポートされています。

> StorageGRID には、すべてのグリッドで同じオペレーティングシステムの CA 証明書も含まれています。本番環境では、オペレーティングシステムの CA 証明書の代わりに、外部の認証局によって署名されたカスタム証明書を指定してください。

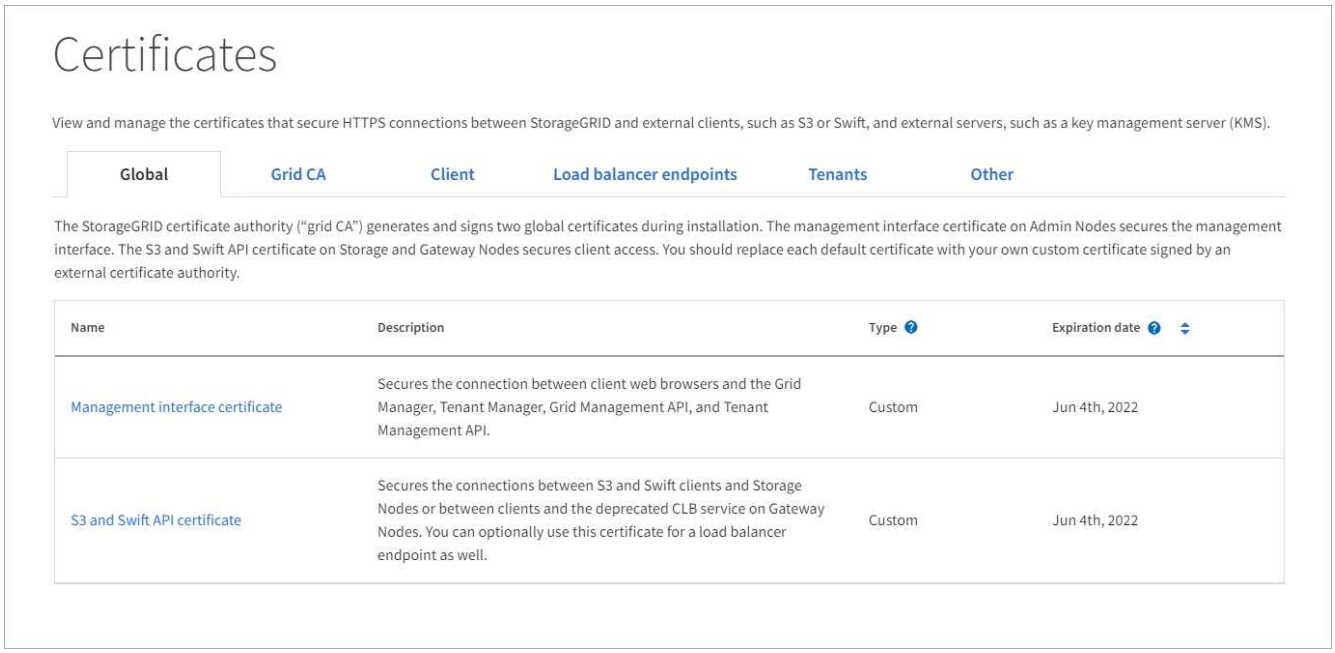
サーバ証明書とクライアント証明書のタイプのバリエーションは、いくつかの方法で実装されます。システムを設定する前に、特定の StorageGRID 構成に必要なすべての証明書を準備しておく必要があります。

アクセスセキュリティ証明書

すべての StorageGRID 証明書に関する情報に一元的にアクセスでき、各証明書の設定ワークフローへのリンクも含まれます。

手順

1. Grid Manager から、構成 > セキュリティ > 証明書 を選択します。



2. [証明書] ページのタブを選択して、各証明書カテゴリの情報を表示し、証明書設定にアクセスします。がある場合は、タブにアクセスできます"適切な権限"。

   - * グローバル * ： Web ブラウザおよび外部 API クライアントからの StorageGRID アクセスを保護します。
   - * Grid CA * ：内部 StorageGRID トラフィックを保護します。
   - * クライアント * ：外部クライアントと StorageGRID Prometheus データベースの間の接続を保護します。
   - ロードバランサエンドポイント：S3クライアントとStorageGRIDロードバランサの間の接続を保護します。
   - * テナント * ：アイデンティティフェデレーションサーバーまたはプラットフォームサービスエンドポイントから S3 ストレージリソースへの接続を保護します。
   - * その他 * ：特定の証明書を必要とする StorageGRID 接続を保護します。

     各タブについては、証明書の詳細へのリンクを次に示します。

グローバル

グローバル証明書によって、Webブラウザおよび外部のS3 APIクライアントからのStorageGRIDアクセスが保護されます。2 つのグローバル証明書は、最初にインストール時に StorageGRID 認証局によって生成されます。本番環境では、外部の認証局によって署名されたカスタム証明書を使用することを推奨します。

- [管理インターフェイスの証明書]: StorageGRID管理インターフェイスへのクライアントWebブラウザ接続を保護します。
- S3 APIシヨウメイシヨ：S3クライアントアプリケーションがオブジェクトデータのアップロードとダウンロードに使用するストレージノード、管理ノード、ゲートウェイノードへのクライアントAPI接続を保護します。

インストールされるグローバル証明書には次の情報が含まれます。

- * 名前 * ：証明書の管理リンクを持つ証明書の名前。
- * 概要 *
- * タイプ * ：カスタムまたはデフォルト。+ グリッドセキュリティを向上させるために、常にカスタム証明書を使用する必要があります。
- * 失効日 * ：デフォルトの証明書を使用している場合、有効期限は表示されません。

次のことができます。

- グリッドセキュリティを向上させるには、外部の認証局によって署名されたカスタム証明書でデフォルト証明書を置き換えます。
  - "StorageGRID で生成されたデフォルトの管理インターフェイス証明書を置き換えます"Grid ManagerとTenant Managerの接続に使用されます。
  - "S3 API証明書を差し替える"ストレージノードとロードバランサエンドポイント（オプション）の接続に使用されます。
- "管理インターフェイスのデフォルトの証明書をリストア"です。
- "デフォルトのS3 API証明書をリストアする"です。
- "スクリプトを使用して、新しい自己署名管理インターフェイス証明書を生成します"です。
- またはをコピーまたはダウンロードし"管理インターフェイスの証明書""S3 APIシヨウメイシヨ"ます。

Grid CA

はGrid CA 証明書、StorageGRIDのインストール時にStorageGRID認証局によって生成され、すべての内部StorageGRIDトラフィックを保護します。

証明書情報には、証明書の有効期限とその内容が含まれます。

できます"グリッドCA証明書をコピーまたはダウンロードします"が、変更することはできません。

クライアント

クライアント証明書外部の認証局によって生成されたを使用して、外部の監視ツールとStorageGRID Prometheusデータベースの間の接続を保護します。

証明書テーブルには、設定されている各クライアント証明書の行があり、証明書の有効期限とともにPrometheus データベースへのアクセスに証明書を使用できるかどうかが示されます。

次のことができます。

- "新しいクライアント証明書をアップロードまたは生成します。"
- 証明書名を選択して証明書の詳細を表示します。表示される情報は次のとおりです。
  - "クライアント証明書の名前を変更します。"
  - "Prometheus のアクセス権限を設定します。"
  - "クライアント証明書をアップロードして置き換えます。"
  - "クライアント証明書をコピーまたはダウンロードします。"
  - "クライアント証明書を削除します。"
- [アクション]*を選択して"編集"、または"添付（ Attach ）" "取り外す"クライアント証明書をすばやく作成します。最大 10 個のクライアント証明書を選択し、 * Actions * > * Remove * を使用して一度に削除できます。

ロードバランサエンドポイント

ロードバランサエンドポイントの証明書S3クライアントと、ゲートウェイノードと管理ノード上のStorageGRIDロードバランササービスの間の接続を保護します。

ロードバランサエンドポイントのテーブルには、設定されている各ロードバランサエンドポイントの行があり、エンドポイントにグローバルS3 API証明書とカスタムロードバランサエンドポイント証明書のどちらが使用されているかが示されます。各証明書の有効期限も表示されます。

> エンドポイント証明書の変更がすべてのノードに適用されるまでに最大 15 分かかることがあります。

次のことができます。

- "ロードバランサエンドポイントを表示します"証明書の詳細を含む。
- "FabricPool のロードバランサエンドポイント証明書を指定します。"
- "グローバルS3 API証明書を使用する"新しいロードバランサエンドポイント証明書を生成する代わりに、

テナント

テナントは、またはプラットフォームサービスエンドポイントの証明書を使用してStorageGRIDとの接続を保護できますアイデンティティフェデレーションサーバの証明書。

テナントテーブルには、テナントごとに 1 つの行があり、各テナントに独自のアイデンティティソースまたはプラットフォームサービスを使用する権限があるかどうかを示します。

次のことができます。

- "Tenant Manager にサインインするテナント名を選択します"
- "テナントのアイデンティティフェデレーションの詳細を表示するテナント名を選択します"
- "テナントプラットフォームサービスの詳細を表示するテナント名を選択します"

- "エンドポイントの作成時にプラットフォームサービスエンドポイント証明書を指定します"

その他

StorageGRID では、特定の目的に他のセキュリティ証明書を使用します。これらの証明書は、機能名で一覧表示されます。その他のセキュリティ証明書には、次のもの

- クラウドストレージプールの証明書
- E メールアラート通知の証明書
- 外部 syslog サーバ証明書
- グリッドフェデレーション接続の証明書
- アイデンティティフェデレーション証明書
- キー管理サーバ（ KMS ）の証明書
- シングルサインオン証明書

情報は、関数が使用する証明書の種類と、そのサーバーおよびクライアント証明書の有効期限を示します。関数名を選択するとブラウザタブが開き、証明書の詳細を表示および編集できます。

> 他の証明書の情報を表示およびアクセスできるのは、をお持ちの場合のみ"適切な権限"です。

次のことができます。

- "S3 、 C2S S3 、または Azure 用のクラウドストレージプール証明書を指定します"
- "アラート E メール通知用の証明書を指定します"
- "外部syslogサーバの証明書を使用する"
- "グリッドフェデレーション接続の証明書をローテーションします"
- "アイデンティティフェデレーション証明書を表示および編集する"
- "キー管理サーバ（ KMS ）のサーバ証明書とクライアント証明書をアップロードします"
- "証明書利用者信頼のSSO証明書を手動で指定します"

セキュリティ証明書の詳細

各タイプのセキュリティ証明書について、実装手順へのリンクとともに以下に説明します。

管理インターフェイスの証明書

証明書のタイプ	製品説明	ナビゲーションの場所	詳細
サーバ	クライアントの Web ブラウザと StorageGRID 管理インターフェイスの間の接続を認証することで、ユーザがセキュリティの警告なしで Grid Manager とテナントマネージャにアクセスできるようにします。 この証明書は、 Grid 管理 API 接続とテナント管理 API 接続も認証します。 インストール時に作成されるデフォルトの証明書を使用することも、カスタム証明書をアップロードすることもできます。	構成 > セキュリティ > *証明書*で、*グローバル*タブを選択し、*管理インターフェース証明書*を選択します。	"管理インターフェイス証明書を設定"

S3 APIシヨウメイシヨ

証明書のタイプ	製品説明	ナビゲーションの場所	詳細
サーバ	ストレージノードとロードバランサエンドポイントへのセキュアなS3クライアント接続を認証します（オプション）。	設定 > セキュリティ > 証明書 で、グローバル タブを選択し、**S3 API** 証明書を選択します。	"S3 API証明書の設定"

Grid CA 証明書

を参照してくださいデフォルトの Grid CA 証明書概要。

管理者クライアント証明書

証明書のタイプ	製品説明	ナビゲーションの場所	詳細
クライアント	StorageGRID が外部クライアントアクセスを認証できるように、各クライアントにインストールします。 • 許可された外部クライアントから StorageGRID Prometheus データベースにアクセスできるようにします。 • 外部ツールを使用して StorageGRID をセキュアに監視できます。	構成 > セキュリティ > 証明書 を選択し、クライアント タブを選択します。	"クライアント証明書を設定"

ロードバランサエンドポイントの証明書

証明書のタイプ	製品説明	ナビゲーションの場所	詳細
サーバ	S3クライアントとゲートウェイノードと管理ノード上のStorageGRIDロードバランササービスの間の接続を認証します。ロードバランサエンドポイントの設定時にロードまたは生成できます。クライアントアプリケーションでは、 StorageGRID に接続する際にロードバランサ証明書を使用してオブジェクトデータを保存および読み出します。 カスタムバージョンのグローバル証明書を使用して、ロードバランササービスへの接続を認証することもできますS3 APIシヨウメイシヨ。グローバル証明書を使用してロードバランサ接続を認証する場合は、ロードバランサエンドポイントごとに個別の証明書をアップロードまたは生成する必要はありません。 • 注： * ロードバランサ認証に使用される証明書は、通常の StorageGRID 処理で最もよく使用される証明書です。	構成 > ネットワーク > ロードバランサエンドポイント	• "ロードバランサエンドポイントを設定する" • "FabricPool のロードバランサエンドポイントを作成します"

クラウドストレージプールのエンドポイントの証明書

証明書のタイプ	製品説明	ナビゲーションの場所	詳細
サーバ	StorageGRID クラウド ストレージ プールから S3 Glacier や Microsoft Azure Blob Storage などの外部ストレージ場所への接続を認証します。クラウドプロバイダの種類ごとに異なる証明書が必要です。	• ilm * > * ストレージ・プール *	"クラウドストレージプールを作成"

E メールアラート通知の証明書

証明書のタイプ	製品説明	ナビゲーションの場所	詳細
サーバとクライアント	アラート通知に使用される SMTP E メールサーバと StorageGRID 間の接続を認証します。 • SMTP サーバとの通信に Transport Layer Security （ TLS ）が必要な場合は、 E メールサーバの CA 証明書を指定する必要があります。 • SMTP E メールサーバで認証用のクライアント証明書が必要な場合にのみ、クライアント証明書を指定してください。	アラート > メール設定	"アラート用の E メール通知を設定します"

外部 **syslog** サーバの証明書

証明書のタイプ	製品説明	ナビゲーションの場所	詳細
サーバ	StorageGRID にイベントを記録する外部 syslog サーバ間で、 TLS 接続または RELP/TLS 接続を認証します。 • 注：外部 syslog サーバへの TCP 、 RELP/TCP 、および UDP 接続には、外部 syslog サーバ証明書は必要ありません。	構成 > 監視 > 監査および**Syslog**サーバー	"外部 syslog サーバを使用します"

[[grid-federation-certificate]グリッドフェデレーション接続証明書

証明書のタイプ	製品説明	ナビゲーションの場所	詳細
サーバとクライアント	グリッドフェデレーション接続で、現在のStorageGRID システムと別のグリッドの間で送信される情報を認証して暗号化します。	構成 > システム > グリッドフェデレーション	• "グリッドフェデレーション接続を作成する" • "接続証明書をローテーションします"

アイデンティティフェデレーション証明書

証明書のタイプ	製品説明	ナビゲーションの場所	詳細
サーバ	Active Directory 、 OpenLDAP 、 Oracle Directory Server などの外部のアイデンティティプロバイダと StorageGRID の間の接続を認証します。アイデンティティフェデレーションに使用します。管理者グループとユーザを外部システムで管理できます。	構成 > アクセス制御 > アイデンティティ連携	"アイデンティティフェデレーションを使用する"

キー管理サーバ（ **KMS** ）の証明書

証明書のタイプ	製品説明	ナビゲーションの場所	詳細
サーバとクライアント	StorageGRID と外部キー管理サーバ（ KMS ）の間の接続を認証します。この接続により、 StorageGRID アプライアンスノードに暗号化キーが提供されます。	構成 > セキュリティ > キー管理サーバー	"キー管理サーバの追加（ KMS ）"

プラットフォームサービスのエンドポイント証明書

証明書のタイプ	製品説明	ナビゲーションの場所	詳細
サーバ	StorageGRID プラットフォームサービスから S3 ストレージリソースへの接続を認証します。	• Tenant Manager * > * storage （ S3 ） * > * Platform services endpoints *	"プラットフォームサービスエンドポイントを作成します" "プラットフォームサービスエンドポイントを編集します"

シングルサインオン（ **SSO** ）証明書

証明書のタイプ	製品説明	ナビゲーションの場所	詳細
サーバ	Active Directory フェデレーションサービス（ AD FS ）やシングルサインオン（ SSO ）要求に使用される StorageGRID などのアイデンティティフェデレーションサービスとの間の接続を認証します。	構成 > アクセス制御 > シングルサインオン	"シングルサインオンを設定します"

証明書の例

例 **1** ：ロードバランササービス

この例では、 StorageGRID がサーバとして機能します。

1. ロードバランサエンドポイントを設定し、 StorageGRID でサーバ証明書をアップロードまたは生成します。
2. ロードバランサエンドポイントへのS3クライアント接続を設定し、同じ証明書をクライアントにアップロードします。
3. クライアントは、データを保存または取得する際に HTTPS を使用してロードバランサエンドポイントに接続します。
4. StorageGRID は、公開鍵を含むサーバ証明書と、秘密鍵に基づく署名を返します。
5. クライアントは、サーバーの署名を証明書のコピーの署名と比較します。署名が一致する場合、クライアントは同じ公開鍵を使用してセッションを開始します。
6. クライアントがオブジェクトデータを StorageGRID に送信

例 **2** ：外部キー管理サーバ（ **KMS** ）

この例では、 StorageGRID がクライアントとして機能します。

1. 外部キー管理サーバソフトウェアを使用する場合は、 StorageGRID を KMS クライアントとして設定し、 CA 署名済みサーバ証明書、パブリッククライアント証明書、およびクライアント証明書の秘密鍵を取得します。
2. Grid Manager を使用して KMS サーバを設定し、サーバ証明書とクライアント証明書およびクライアント秘密鍵をアップロードします。
3. StorageGRID ノードで暗号化キーが必要な場合、証明書からのデータと秘密鍵に基づく署名を含む KMS サーバに要求が送信されます。
4. KMS サーバは証明書の署名を検証し、 StorageGRID を信頼できることを決定します。
5. KMS サーバは、検証済みの接続を使用して応答します。

StorageGRID でサポートされているサーバー証明書のタイプ

StorageGRID システムでは、 RSA または ECDSA （ Elliptic Curve Digital Signature Algorithm ）で暗号化されたカスタム証明書がサポートされます。

セキュリティポリシーの暗号タイプは、サーバ証明書タイプと一致している必要があります。たとえば、RSA暗号にはRSA証明書が必要で、ECDSA暗号にはECDSA証明書が必要です。を参照して "セキュリティ証明書を管理する"サーバ証明書と互換性のないカスタムセキュリティポリシーを設定する場合は、設定できます"一時的にデフォルトのセキュリティポリシーに戻します"。

StorageGRIDによるクライアント接続の保護方法の詳細については、を参照してください"S3クライアントノセキュリテイ"。

StorageGRID で管理インターフェイス証明書を設定する

デフォルトの管理インターフェイス証明書を単一のカスタム証明書に置き換えると、ユーザがグリッドマネージャとテナントマネージャにアクセスする際にセキュリティの警告が表示されなくなります。デフォルトの管理インターフェイス証明書に戻すか、新しい証明書を生成することもできます。

タスクの内容

デフォルトでは、管理ノードごとに、グリッド CA によって署名された証明書が 1 つずつ発行されます。これらの CA 署名証明書は、単一の共通するカスタム管理インターフェイス証明書および対応する秘密鍵に置き換えることができます。

Grid Manager および Tenant Manager への接続時にクライアントがホスト名を確認する必要がある場合は、単一のカスタム管理インターフェイスの証明書がすべての管理ノードに対して使用されるため、ワイルドカード証明書またはマルチドメイン証明書として指定する必要があります。グリッド内のすべての管理ノードに一致するカスタム証明書を定義してください。

設定はサーバ上で行う必要があります。また、使用しているルート認証局（ CA ）によっては、ユーザが Grid Manager および Tenant Manager へのアクセスに使用する Web ブラウザに Grid CA 証明書をインストールすることも必要になります。

失敗したサーバー証明書によって操作が中断されないように、このサーバー証明書の有効期限が近づくと、*管理インターフェイスのサーバー証明書の有効期限*アラートがトリガーされます。必要に応じて、[構成] > [セキュリティ] > [証明書] を選択し、[グローバル] タブで管理インターフェイス証明書の有効期限を確認することで、現在の証明書の有効期限を確認できます。

IP アドレスではなくドメイン名を使用して Grid Manager または Tenant Manager にアクセスする場合は、次のいずれかの場合に証明書のエラーが表示され、バイパスするオプションはありません。

- カスタム管理インターフェイス証明書の有効期限が切れます。
- お前カスタム管理インターフェイス証明書をデフォルトのサーバ証明書に戻しますだ

カスタム管理インターフェイス証明書を追加します

カスタムの管理インターフェイス証明書を追加するには、 Grid Manager を使用して独自の証明書を指定するか、証明書を生成します。

手順

1. 構成 > セキュリティ > *証明書*を選択します。

2. [* グローバル *] タブで、 [* 管理インターフェイス証明書 *] を選択します。
3. [* カスタム証明書を使用する *] を選択します。
4. 証明書をアップロードまたは生成します。

証明書をアップロードする

必要なサーバ証明書ファイルをアップロードします。

a. [証明書のアップロード] を選択します。

b. 必要なサーバ証明書ファイルをアップロードします。

- * サーバ証明書 * ：カスタムサーバ証明書ファイル（ PEM エンコード）。
- 証明書の秘密鍵：カスタムサーバ証明書の秘密鍵ファイル(`.key`）。

> EC 秘密鍵は 224 ビット以上にする必要があります。RSA 秘密鍵は 2048 ビット以上にする必要があります。

- **CA Bundle** ：各中間発行認証局（ CA ）の証明書を含む単一のオプションファイル。このファイルには、PEMでエンコードされた各CA証明書ファイルが、証明書チェーンの順序で連結されている必要があります。

c. [* 証明書の詳細 *] を展開して、アップロードした各証明書のメタデータを表示します。オプションの CA バンドルをアップロードした場合は、各証明書が独自のタブに表示されます。

- 証明書ファイルを保存するには、 * 証明書のダウンロード * を選択します。証明書バンドルを保存するには、 * CA バンドルのダウンロード * を選択します。

  証明書ファイルの名前とダウンロード先を指定します。拡張子を付けてファイルを保存します `.pem`。

  例： `storagegrid_certificate.pem`

- 証明書の内容をコピーして他の場所に貼り付けるには、 * 証明書の PEM のコピー * または * CA バンドル PEM のコピー * を選択してください。

d. [保存（ Save ）] を選択します。+ Grid Manager 、 Tenant Manager 、 Grid Manager API 、または Tenant Manager API への以降のすべての新しい接続にはカスタムの管理インターフェイス証明書が使用されます。

証明書の生成

サーバ証明書ファイルを生成します。

> 本番環境では、外部の認証局によって署名されたカスタム管理インターフェイス証明書を使用することを推奨します。

a. [* 証明書の生成 *] を選択します。

b. 証明書情報を指定します。

フィールド	製品説明
ドメイン名	証明書に含める1つ以上の完全修飾ドメイン名。複数のドメイン名を表すには、ワイルドカードとして * を使用します。

フィールド	製品説明
IP	証明書に含める1つ以上のIPアドレス。
件名（オプション）	証明書所有者のX.509サブジェクト名または識別名（DN）。 このフィールドに値を入力しない場合、生成される証明書では、最初のドメイン名またはIPアドレスがサブジェクト共通名（CN）として使用されます。
有効な日数	作成後に証明書の有効期限が切れる日数。
キー使用の拡張機能を追加します	選択されている場合（デフォルトおよび推奨）、キー使用と拡張キー使用拡張が生成された証明書に追加されます。 これらの拡張機能は、証明書に含まれるキーの目的を定義します。 注:証明書にこれらの拡張機能が含まれている場合、古いクライアントで接続の問題が発生する場合を除き、このチェックボックスをオンのままにします。

c. [*Generate （生成）] を選択します

d. 生成された証明書のメタデータを表示するには、 [証明書の詳細] を選択します。

- 証明書ファイルを保存するには、 [証明書のダウンロード] を選択します。

  証明書ファイルの名前とダウンロード先を指定します。拡張子を付けてファイルを保存します `.pem`。

例： `storagegrid_certificate.pem`

- 証明書の内容をコピーして他の場所に貼り付けるには、 * 証明書の PEM をコピー * を選択します。

e. [保存（ Save ）] を選択します。+ Grid Manager 、 Tenant Manager 、 Grid Manager API 、または Tenant Manager API への以降のすべての新しい接続にはカスタムの管理インターフェイス証明書が使用されます。

5. Web ブラウザが更新されたことを確認するには、ページをリフレッシュしてください。

新しい証明書をアップロードまたは生成したあと、関連する証明書の有効期限アラートがクリアされるまでに最大 1 日かかります。

6. カスタムの管理インターフェイス証明書を追加すると、使用中の証明書の詳細な証明書情報が管理インターフェイスの証明書ページに表示されます。+ 必要に応じて証明書 PEM をダウンロードまたはコピーできます。

管理インターフェイスのデフォルトの証明書をリストア

Grid Manager 接続と Tenant Manager 接続でのデフォルトの管理インターフェイス証明書を使用するように戻すことができます。

手順

1. 構成 > セキュリティ > *証明書*を選択します。
2. [* グローバル *] タブで、 [* 管理インターフェイス証明書 *] を選択します。
3. [* デフォルト証明書を使用する *] を選択します。

   管理インターフェイスのデフォルトの証明書をリストアすると、設定したカスタムサーバ証明書ファイルは削除され、システムからはリカバリできなくなります。以降すべての新しいクライアント接続には、デフォルトの管理インターフェイス証明書が使用されます。

4. Web ブラウザが更新されたことを確認するには、ページをリフレッシュしてください。

スクリプトを使用して、新しい自己署名管理インターフェイス証明書を生成します

ホスト名の厳密な検証が必要な場合は、スクリプトを使用して管理インターフェイス証明書を生成できます。

開始する前に

- そうだな "特定のアクセス権限"
- あなたはファイルを持ってい `Passwords.txt`ます。

タスクの内容

本番環境では、外部の認証局によって署名された証明書を使用することを推奨します。

手順

1. 各管理ノードの完全修飾ドメイン名（ FQDN ）を取得します。
2. プライマリ管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`
   b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

      rootとしてログインすると、プロンプトがからに `#`変わります `$`。
3. 新しい自己署名証明書を使用して StorageGRID を設定します。

   ```
   $ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
   ```

   - では `--domains`、ワイルドカードを使用してすべての管理ノードの完全修飾ドメイン名を表します。たとえば、は `*.ui.storagegrid.example.com`ワイルドカード*を使用してとを `admin2.ui.storagegrid.example.com`表します `admin1.ui.storagegrid.example.com`。
   - に `management`設定 `--type`して、管理インターフェイスの証明書を設定します。この証明書はGrid

ManagerとTenant Managerで使用されます。

- デフォルトでは、生成された証明書の有効期間は 1 年間（ 365 日）です。この期間を過ぎる前に証明書を再作成する必要があります。引数を使用すると、デフォルトの有効期間を上書きできます `--days`。

> 証明書の有効期間は、の実行時から開始され `make-certificate`ます。管理クライアントが StorageGRID と同じ時間ソースと同期されるようにしてください。同期されていないと、クライアントが証明書を拒否する可能性があります。

```
$ sudo make-certificate --domains *.ui.storagegrid.example.com --type
management --days 720
```

出力には、管理 API クライアントで必要なパブリック証明書が含まれています。

4. 証明書を選択してコピーします。

   BEGIN タグと END タグも含めて選択してください。

5. コマンドシェルからログアウトします。 `$ exit`
6. 証明書が設定されたことを確認します。
   a. Grid Manager にアクセスします。
   b. 構成 > セキュリティ > *証明書*を選択します。
   c. [* グローバル *] タブで、 [* 管理インターフェイス証明書 *] を選択します。
7. コピーしたパブリック証明書を使用するように管理クライアントを設定します。BEGIN タグと END タグを含めてください。

管理インターフェイス証明書をダウンロードまたはコピーします

管理インターフェイスの証明書の内容を保存またはコピーして、他の場所で使用することができます。

手順

1. 構成 > セキュリティ > *証明書*を選択します。
2. [* グローバル *] タブで、 [* 管理インターフェイス証明書 *] を選択します。
3. [**Server**] タブまたは [**CA Bundle**] タブを選択し、証明書をダウンロードまたはコピーします。

証明書ファイルまたは **CA** バンドルをダウンロードします

証明書またはCAバンドルファイルをダウンロードし `.pem`ます。オプションの CA バンドルを使用している場合は、バンドル内の各証明書が独自のサブタブに表示されます。

a. [証明書のダウンロード *] または [CA バンドルのダウンロード *] を選択します。

   CA バンドルをダウンロードする場合、 CA バンドルのセカンダリタブにあるすべての証明書が単一のファイルとしてダウンロードされます。

b. 証明書ファイルの名前とダウンロード先を指定します。拡張子を付けてファイルを保存します `.pem`。

   例： `storagegrid_certificate.pem`

証明書または **CA** バンドル **PEM** をコピーしてください

証明書のテキストをコピーして別の場所に貼り付けてください。オプションの CA バンドルを使用している場合は、バンドル内の各証明書が独自のサブタブに表示されます。

a. [Copy certificate PEM* （証明書のコピー）] または [* Copy CA bundle PEM* （ CA バンドル PEM のコピー）

   CA バンドルをコピーする場合、 CA バンドルのセカンダリタブにあるすべての証明書が一緒にコピーされます。

b. コピーした証明書をテキストエディタに貼り付けます。

c. 拡張子を付けてテキストファイルを保存します `.pem`。

   例： `storagegrid_certificate.pem`

StorageGRIDで**S3 API**証明書を設定

ストレージノードまたはロードバランサエンドポイントへのS3クライアント接続に使用されるサーバ証明書を置き換えたりリストアしたりできます。置き換え用のカスタムサーバ証明書は組織に固有のものです。

このバージョンのドキュメントサイトからSwiftの詳細が削除されました。を参照してください "StorageGRID 11.8：S3およびSwift API証明書の設定"

タスクの内容

デフォルトでは、すべてのストレージノードに、グリッド CA によって署名された X.509 サーバ証明書が発行されます。これらの CA 署名証明書は、単一の共通するカスタムサーバ証明書および対応する秘密鍵で置き換えることができます。

1 つのカスタムサーバ証明書がすべてのストレージノードに対して使用されるため、ストレージエンドポイントへの接続時にクライアントがホスト名を確認する必要がある場合は、ワイルドカード証明書またはマルチドメイン証明書として指定する必要があります。グリッド内のすべてのストレージノードに一致するカスタム証明書を定義してください。

サーバでの設定が完了したら、使用しているルート認証局（CA）によっては、システムへのアクセスに使用するS3 APIクライアントにグリッドCA証明書をインストールする必要があります。

> 失敗したサーバー証明書によって操作が中断されないように、ルート サーバー証明書の有効期限が切れそうになると、**S3 API** のグローバル サーバー証明書の有効期限切れ アラートがトリガーされます。必要に応じて、[設定] > [セキュリティ] > [証明書] を選択し、[グローバル] タブで S3 API 証明書の有効期限を確認することで、現在の証明書の有効期限を確認できます。

カスタムのS3 API証明書をアップロードまたは生成できます。

カスタムの**S3 API**証明書を追加する

手順

1. 構成 > セキュリティ > *証明書*を選択します。
2. [グローバル]タブで、* S3 API証明書*を選択します。
3. [* カスタム証明書を使用する *] を選択します。
4. 証明書をアップロードまたは生成します。

証明書をアップロードする

必要なサーバ証明書ファイルをアップロードします。

a. [証明書のアップロード] を選択します。

b. 必要なサーバ証明書ファイルをアップロードします。

- * サーバ証明書 * ：カスタムサーバ証明書ファイル（ PEM エンコード）。
- 証明書の秘密鍵：カスタムサーバ証明書の秘密鍵ファイル(`.key`）。

> EC 秘密鍵は 224 ビット以上にする必要があります。RSA 秘密鍵は 2048 ビット以上にする必要があります。

- **CA Bundle** ：各中間発行認証局の証明書を含む単一のオプションファイル。このファイルには、PEMでエンコードされた各CA証明書ファイルが、証明書チェーンの順序で連結されている必要があります。

c. 証明書の詳細を選択して、アップロードされた各カスタムS3 API証明書のメタデータとPEMを表示します。オプションの CA バンドルをアップロードした場合は、各証明書が独自のタブに表示されます。

- 証明書ファイルを保存するには、 * 証明書のダウンロード * を選択します。証明書バンドルを保存するには、 * CA バンドルのダウンロード * を選択します。

  証明書ファイルの名前とダウンロード先を指定します。拡張子を付けてファイルを保存します `.pem`。

  例： `storagegrid_certificate.pem`

- 証明書の内容をコピーして他の場所に貼り付けるには、 * 証明書の PEM のコピー * または * CA バンドル PEM のコピー * を選択してください。

d. [保存（ Save ）] を選択します。

  カスタムサーバ証明書は、以降の新しいS3クライアント接続に使用されます。

証明書の生成

サーバ証明書ファイルを生成します。

a. [* 証明書の生成 *] を選択します。

b. 証明書情報を指定します。

フィールド	製品説明
ドメイン名	証明書に含める1つ以上の完全修飾ドメイン名。複数のドメイン名を表すには、ワイルドカードとして * を使用します。
IP	証明書に含める1つ以上のIPアドレス。

フィールド	製品説明
件名（オプション）	証明書所有者のX.509サブジェクト名または識別名（DN）。 このフィールドに値を入力しない場合、生成される証明書では、最初のドメイン名またはIPアドレスがサブジェクト共通名（CN）として使用されます。
有効な日数	作成後に証明書の有効期限が切れる日数。
キー使用の拡張機能を追加します	選択されている場合（デフォルトおよび推奨）、キー使用と拡張キー使用拡張が生成された証明書に追加されます。 これらの拡張機能は、証明書に含まれるキーの目的を定義します。 注:証明書にこれらの拡張機能が含まれている場合、古いクライアントで接続の問題が発生する場合を除き、このチェックボックスをオンのままにします。

c. [*Generate （生成）] を選択します

d. [証明書の詳細]*を選択して、生成されたカスタムS3 API証明書のメタデータとPEMを表示します。

- 証明書ファイルを保存するには、 [証明書のダウンロード] を選択します。

  証明書ファイルの名前とダウンロード先を指定します。拡張子を付けてファイルを保存します `.pem`。

例： `storagegrid_certificate.pem`

- 証明書の内容をコピーして他の場所に貼り付けるには、 * 証明書の PEM をコピー * を選択します。

e. [保存（ Save ）] を選択します。

カスタムサーバ証明書は、以降の新しいS3クライアント接続に使用されます。

5. タブを選択して、デフォルトの StorageGRID サーバ証明書、アップロードされた CA 署名証明書、または生成されたカスタム証明書のメタデータを表示します。

新しい証明書をアップロードまたは生成したあと、関連する証明書の有効期限アラートがクリアされるまでに最大 1 日かかります。

6. Web ブラウザが更新されたことを確認するには、ページをリフレッシュしてください。

7. カスタムS3 API証明書を追加すると、[S3 API certificate]ページに、使用中のカスタムS3 API証明書の詳細な証明書情報が表示されます。+ 必要に応じて証明書 PEM をダウンロードまたはコピーできます。

デフォルトの**S3 API**証明書をリストアする

ストレージノードへのS3クライアント接続にデフォルトのS3 API証明書を使用するように戻すことができます。ただし、ロードバランサエンドポイントにはデフォルトのS3 API証明書を使用できません。

手順

1. 構成 > セキュリティ > *証明書*を選択します。
2. [グローバル]タブで、* S3 API証明書*を選択します。
3. [* デフォルト証明書を使用する *] を選択します。

   グローバルS3 API証明書のデフォルトバージョンをリストアすると、設定したカスタムサーバ証明書ファイルは削除され、システムからリカバリできなくなります。ストレージノードへの以降の新しいS3クライアント接続には、デフォルトのS3 API証明書が使用されます。

4. [OK]*を選択して警告を確認し、デフォルトのS3 API証明書をリストアします。

   Root Access権限があり、カスタムのS3 API証明書がロードバランサエンドポイントの接続に使用されていた場合は、デフォルトのS3 API証明書を使用してアクセスできなくなるロードバランサエンドポイントのリストが表示されます。に移動して"ロードバランサエンドポイントを設定する"、影響を受けるエンドポイントを編集または削除します。

5. Web ブラウザが更新されたことを確認するには、ページをリフレッシュしてください。

S3 API証明書をダウンロードまたはコピーする

他の場所で使用できるように、S3 API証明書の内容を保存またはコピーできます。

手順

1. 構成 > セキュリティ > *証明書*を選択します。
2. [グローバル]タブで、* S3 API証明書*を選択します。
3. [**Server**] タブまたは [**CA Bundle**] タブを選択し、証明書をダウンロードまたはコピーします。

証明書ファイルまたは **CA** バンドルをダウンロードします

証明書またはCAバンドルファイルをダウンロードし `.pem`ます。オプションの CA バンドルを使用している場合は、バンドル内の各証明書が独自のサブタブに表示されます。

a. [証明書のダウンロード *] または [CA バンドルのダウンロード *] を選択します。

   CA バンドルをダウンロードする場合、 CA バンドルのセカンダリタブにあるすべての証明書が単一のファイルとしてダウンロードされます。

b. 証明書ファイルの名前とダウンロード先を指定します。拡張子を付けてファイルを保存します `.pem`。

   例： `storagegrid_certificate.pem`

証明書または **CA** バンドル **PEM** をコピーしてください

証明書のテキストをコピーして別の場所に貼り付けてください。オプションの CA バンドルを使用している場合は、バンドル内の各証明書が独自のサブタブに表示されます。

a. [Copy certificate PEM* （証明書のコピー）] または [* Copy CA bundle PEM* （ CA バンドル PEM のコピー）

   CA バンドルをコピーする場合、 CA バンドルのセカンダリタブにあるすべての証明書が一緒にコピーされます。

b. コピーした証明書をテキストエディタに貼り付けます。

c. 拡張子を付けてテキストファイルを保存します `.pem`。

   例： `storagegrid_certificate.pem`

関連情報

- "S3 REST APIを使用する"
- "S3エンドポイントのドメイン名を設定"

StorageGRID グリッド **CA** 証明書をコピーします

StorageGRID は、内部の認証局（ CA ）を使用して内部トラフィックを保護します。独自の証明書をアップロードしても、この証明書は変更されません。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- そうだな "特定のアクセス権限"

タスクの内容

カスタムサーバ証明書が設定されている場合、クライアントアプリケーションはカスタムサーバ証明書を使用してサーバを検証する必要があります。StorageGRID システムから CA 証明書をコピーしない。

手順

1. 構成 > セキュリティ > 証明書 を選択し、グリッド **CA** タブを選択します。
2. [Certificate PEM]セクションで、証明書をダウンロードまたはコピーします。

証明書ファイルをダウンロードします

証明書ファイルをダウンロードし `.pem`ます。

a. [証明書のダウンロード] を選択します。
b. 証明書ファイルの名前とダウンロード先を指定します。拡張子を付けてファイルを保存します `.pem`。

例： `storagegrid_certificate.pem`

証明書 **PEM** をコピーします

証明書のテキストをコピーして別の場所に貼り付けてください。

a. [* 証明書 PEM のコピー *] を選択します。
b. コピーした証明書をテキストエディタに貼り付けます。
c. 拡張子を付けてテキストファイルを保存します `.pem`。

例： `storagegrid_certificate.pem`

FabricPool の **StorageGRID** 証明書を設定します

S3クライアントが厳密なホスト名検証を実行し、厳密なホスト名検証の無効化をサポートしていない場合（FabricPool を使用するONTAP クライアントなど）は、ロードバランサエンドポイントの設定時にサーバ証明書を生成またはアップロードできます。

開始する前に

- そうだな "特定のアクセス権限"
- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。

タスクの内容

ロードバランサエンドポイントを作成する際には、自己署名サーバ証明書を生成するか、既知の認証局（ CA ）によって署名された証明書をアップロードできます。本番環境では、既知の CA によって署名された証明書を使用する必要があります。CA によって署名された証明書は、システムを停止することなくローテーションできます。また、中間者攻撃に対する保護としても優れているため、セキュリティも強化されます。

次の手順は、 FabricPool を使用する S3 クライアントを対象とした一般的なガイドラインです。詳細および手順については、を参照してください"StorageGRID for FabricPool を設定します"。

手順

1. 必要に応じて、 FabricPool で使用するハイアベイラビリティ（ HA ）グループを設定します。
2. FabricPool で使用する S3 ロードバランサエンドポイントを作成します。

HTTPS ロードバランサエンドポイントを作成する際に、サーバ証明書、証明書の秘密鍵、およびオプションの CA バンドルをアップロードするように求められます。

3. ONTAP でクラウド階層として StorageGRID を接続します。

   ロードバランサエンドポイントのポートと、アップロードした CA 証明書で使用する完全修飾ドメイン名を指定します。次に、 CA 証明書を指定します。

   中間 CA が StorageGRID 証明書を発行した場合は、中間 CA 証明書を指定する必要があります。StorageGRID 証明書がルート CA によって直接発行された場合は、ルート CA 証明書を指定する必要があります。

StorageGRID でクライアント証明書を設定

クライアント証明書を使用すると、許可された外部クライアントから StorageGRID の Prometheus データベースにアクセスして、外部ツールで StorageGRID を監視するための安全な方法を提供できます。

外部の監視ツールを使用してStorageGRID にアクセスする必要がある場合は、グリッドマネージャを使用してクライアント証明書をアップロードまたは生成し、証明書の情報を外部ツールにコピーする必要があります。

およびを参照してください"セキュリティ証明書を管理する""カスタムサーバ証明書を設定する"。

失敗したサーバー証明書によって操作が中断されないように、このサーバー証明書の有効期限が近づくと、*証明書ページで構成されたクライアント証明書の有効期限*アラートがトリガーされます。必要に応じて、[構成] > [セキュリティ] > [証明書] を選択し、[クライアント] タブでクライアント証明書の有効期限を確認することで、現在の証明書の有効期限を確認できます。

特別に設定されたアプライアンスノードのデータをキー管理サーバ（KMS）を使用して保護する場合は、に関する具体的な情報を参照してください"KMS クライアント証明書をアップロードする"。

開始する前に

- Root Access 権限が割り当てられている。
- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- クライアント証明書を設定するには：
  - 管理ノードの IP アドレスまたはドメイン名を確認しておきます。
  - StorageGRID 管理インターフェイス証明書を設定している場合は、管理インターフェイス証明書の設定に使用するCA、クライアント証明書、および秘密鍵を用意しておきます。
  - 独自の証明書をアップロードするには、証明書の秘密鍵をローカルコンピュータで使用できます。
  - 秘密鍵は、作成時に保存または記録しておく必要があります。元の秘密鍵がない場合は、新しい秘密鍵を作成する必要があります。
- クライアント証明書を編集するには：
  - 管理ノードの IP アドレスまたはドメイン名を確認しておきます。

- 独自の証明書または新しい証明書をアップロードするには、ローカルコンピュータ上で秘密鍵、クライアント証明書、およびCA（使用している場合）を使用できます。

クライアント証明書を追加します

クライアント証明書を追加するには、次のいずれかの手順を実行します。

- [管理インターフェイス証明書はすでに設定されています]
- CAによって発行されたクライアント証明書
- Grid Managerから証明書が生成されました

管理インターフェイス証明書はすでに設定されています

顧客が指定したCA、クライアント証明書、および秘密鍵を使用して管理インターフェイス証明書がすでに設定されている場合は、この手順 を使用してクライアント証明書を追加します。

手順

1. グリッド マネージャーで、[構成] > [セキュリティ] > [証明書] を選択し、[クライアント] タブを選択します。
2. 「 * 追加」を選択します。
3. 証明書名を入力します。
4. 外部の監視ツールを使用してPrometheus指標にアクセスするには、*[Allow Prometheus]*を選択します。
5. 「 * Continue * 」を選択します。
6. [証明書の接続]*ステップでは、管理インターフェイス証明書をアップロードします。
   a. [証明書のアップロード] を選択します。
   b. [参照]*を選択し、管理インターフェイスの証明書ファイルを選択し(`.pem`ます）。
      - クライアント証明書の詳細 * を選択して、証明書メタデータと証明書 PEM を表示します。
      - 証明書の内容をコピーして他の場所に貼り付けるには、 * 証明書の PEM をコピー * を選択します。
   c. 証明書を Grid Manager に保存するには、 * Create * を選択します。

      新しい証明書が [クライアント] タブに表示されます。
7. 外部監視ツールを設定します（Grafanaなど）。

CAによって発行されたクライアント証明書

管理インターフェイス証明書が設定されていない場合や、CAによって発行されたクライアント証明書と秘密鍵を使用するPrometheusのクライアント証明書を追加する場合は、この手順 を使用して管理者クライアント証明書を追加します。

手順

1. 手順~を実行します"管理インターフェイス証明書を設定します"。
2. グリッド マネージャーで、[構成] > [セキュリティ] > [証明書] を選択し、[クライアント] タブを選択します。

3. 「 * 追加」を選択します。
4. 証明書名を入力します。
5. 外部の監視ツールを使用してPrometheus指標にアクセスするには、*[Allow Prometheus]*を選択します。
6. 「 * Continue * 」を選択します。
7. [証明書の添付]手順では、クライアント証明書、秘密鍵、およびCAバンドルファイルをアップロードします。
   a. [証明書のアップロード] を選択します。
   b. [参照]*を選択し、クライアント証明書、秘密鍵、およびCAバンドルファイルを選択し(`.pem`ます）。
      - クライアント証明書の詳細 * を選択して、証明書メタデータと証明書 PEM を表示します。
      - 証明書の内容をコピーして他の場所に貼り付けるには、 * 証明書の PEM をコピー * を選択します。
   c. 証明書を Grid Manager に保存するには、 * Create * を選択します。

      新しい証明書が[クライアント]タブに表示されます。
8. 外部監視ツールを設定します（Grafanaなど）。

Grid Managerから証明書が生成されました

管理インターフェイス証明書が設定されていない場合やGrid Managerの証明書生成機能を使用するPrometheusのクライアント証明書を追加する場合は、この手順 を使用して管理者クライアント証明書を追加します。

手順

1. グリッド マネージャーで、[構成] > [セキュリティ] > [証明書] を選択し、[クライアント] タブを選択します。
2. 「 * 追加」を選択します。
3. 証明書名を入力します。
4. 外部の監視ツールを使用してPrometheus指標にアクセスするには、*[Allow Prometheus]*を選択します。
5. 「 * Continue * 」を選択します。
6. ステップで、[証明書の生成]*を選択します。
7. 証明書情報を指定します。
   - * Subject *（オプション）：証明書所有者のX.509サブジェクトまたは識別名（DN）。
   - 有効日：生成された証明書の有効日数（生成時から）。
   - キー使用拡張の追加：選択した場合（デフォルトおよび推奨）、キー使用および拡張キー使用拡張が生成された証明書に追加されます。

     これらの拡張機能は、証明書に含まれるキーの目的を定義します。

     証明書にこれらの拡張機能が含まれている場合に古いクライアントで接続の問題が発生する場合を除き、このチェックボックスをオンのままにします

8. [*Generate （生成）] を選択します
9. 証明書メタデータと証明書PEMを表示するには、[クライアント証明書の詳細]を選択します。

   ダイアログを閉じると、証明書の秘密鍵を表示できなくなります。キーを安全な場所にコピーまたはダウンロードします。

   - 証明書の内容をコピーして他の場所に貼り付けるには、 * 証明書の PEM をコピー * を選択します。
   - 証明書ファイルを保存するには、 [証明書のダウンロード] を選択します。

     証明書ファイルの名前とダウンロード先を指定します。拡張子を付けてファイルを保存します `.pem`。

   例： `storagegrid_certificate.pem`

   - 秘密鍵のコピー * を選択して、証明書の秘密鍵をコピーして別の場所に貼り付けます。
   - 秘密鍵をファイルとして保存するには、 * 秘密鍵のダウンロード * を選択します。

     秘密鍵ファイルの名前とダウンロード先を指定します。

10. 証明書を Grid Manager に保存するには、 * Create * を選択します。

    新しい証明書が [クライアント] タブに表示されます。

11. グリッド マネージャーで、[構成] > [セキュリティ] > [証明書] を選択し、[グローバル] タブを選択します。
12. 管理インターフェイス証明書*を選択します。
13. [* カスタム証明書を使用する *] を選択します。
14. 手順からcertificate.pemファイルとprivate_key.pemファイルをアップロードしクライアント証明書の詳細ます。CAバンドルをアップロードする必要はありません。
    a. [証明書のアップロード] を選択し、 [続行] を選択します。
    b. 各証明書ファイルをアップロードし(`.pem`ます）。
    c. 証明書をGrid Managerに保存するには、* Save *を選択します。

       新しい証明書が管理インターフェイスの証明書のページに表示されます。

15. 外部監視ツールを設定します（Grafanaなど）。

外部監視ツールを設定します

手順

1. Grafana などの外部監視ツールで次の設定を行います。
   a. * 名前 * ：接続の名前を入力します。

      StorageGRID ではこの情報は必要ありませんが、接続をテストするための名前を指定する必要があります。

   b. * URL * ：管理ノードのドメイン名または IP アドレスを入力します。HTTPS とポート 9091 を指定し

ます。

例： `https://admin-node.example.com:9091`

c. CA 証明書を使用して、 * TLS クライアント認証 * および * を有効にします。

d. TLS/SSL Auth Detailsの下で、+をコピーして貼り付けます

- 管理インターフェイスのCA証明書を**CA Cert**に追加します
- クライアント証明書をクライアント証明書に送信します
- クライアントキー**への秘密鍵

e. * ServerName* ：管理ノードのドメイン名を入力します。

servername は、管理インターフェイス証明書に表示されるドメイン名と一致する必要があります。

2. StorageGRID またはローカルファイルからコピーした証明書と秘密鍵を保存してテストします。

これで、外部の監視ツールを使用して StorageGRID から Prometheus 指標にアクセスできるようになります。

指標の詳細については、を参照して"StorageGRID の監視手順"ください。

クライアント証明書を編集します

管理者クライアント証明書を編集して、名前を変更したり、 Prometheus アクセスを有効または無効にしたり、現在の証明書の期限が切れたときに新しい証明書をアップロードしたりできます。

手順

1. 構成 > セキュリティ > 証明書 を選択し、クライアント タブを選択します。

証明書の有効期限と Prometheus のアクセス権限を次の表に示します。証明書の有効期限が近づいた場合、またはすでに有効期限が切れた場合は、メッセージが表に表示され、アラートがトリガーされます。

2. 編集する証明書を選択します。
3. 「 * Edit * 」を選択し、「 * 名前と権限を編集 * 」を選択します
4. 証明書名を入力します。
5. 外部の監視ツールを使用してPrometheus指標にアクセスするには、*[Allow Prometheus]*を選択します。
6. 証明書を Grid Manager に保存するには、「 * Continue * 」を選択します。

更新された証明書が [クライアント] タブに表示されます。

新しいクライアント証明書を接続します

現在の証明書の期限が切れたときに新しい証明書をアップロードできます。

手順

1. 構成 > セキュリティ > 証明書 を選択し、クライアント タブを選択します。

証明書の有効期限と Prometheus のアクセス権限を次の表に示します。証明書の有効期限が近づいた場合、またはすでに有効期限が切れた場合は、メッセージが表に表示され、アラートがトリガーされます。

2. 編集する証明書を選択します。
3. 「 * 編集」を選択し、編集オプションを選択します。

証明書をアップロードする

証明書のテキストをコピーして別の場所に貼り付けてください。

a. [証明書のアップロード] を選択し、 [続行] を選択します。

b. クライアント証明書名(`.pem`をアップロードします）。

   クライアント証明書の詳細 * を選択して、証明書メタデータと証明書 PEM を表示します。

   - 証明書ファイルを保存するには、 [証明書のダウンロード] を選択します。

     証明書ファイルの名前とダウンロード先を指定します。拡張子を付けてファイルを保存します `.pem`。

   例： `storagegrid_certificate.pem`

   - 証明書の内容をコピーして他の場所に貼り付けるには、 * 証明書の PEM をコピー * を選択します。

c. 証明書を Grid Manager に保存するには、 * Create * を選択します。

   更新された証明書が [クライアント] タブに表示されます。

証明書の生成

証明書のテキストを生成して他の場所に貼り付けます。

a. [* 証明書の生成 *] を選択します。

b. 証明書情報を指定します。

   - * Subject *（オプション）：証明書所有者のX.509サブジェクトまたは識別名（DN）。
   - 有効日：生成された証明書の有効日数（生成時から）。
   - キー使用拡張の追加：選択した場合（デフォルトおよび推奨）、キー使用および拡張キー使用拡張が生成された証明書に追加されます。

     これらの拡張機能は、証明書に含まれるキーの目的を定義します。

     証明書にこれらの拡張機能が含まれている場合に古いクライアントで接続の問題が発生する場合を除き、このチェックボックスをオンのままにします

c. [*Generate （生成）] を選択します

d. クライアント証明書の詳細 * を選択して、証明書メタデータと証明書 PEM を表示します。

   ダイアログを閉じると、証明書の秘密鍵を表示できなくなります。キーを安全な場所にコピーまたはダウンロードします。

   - 証明書の内容をコピーして他の場所に貼り付けるには、 * 証明書の PEM をコピー * を選択します。
   - 証明書ファイルを保存するには、 [証明書のダウンロード] を選択します。

証明書ファイルの名前とダウンロード先を指定します。拡張子を付けてファイルを保存します `.pem`。

例： `storagegrid_certificate.pem`

- 秘密鍵のコピー * を選択して、証明書の秘密鍵をコピーして別の場所に貼り付けます。
- 秘密鍵をファイルとして保存するには、 * 秘密鍵のダウンロード * を選択します。

  秘密鍵ファイルの名前とダウンロード先を指定します。

e. 証明書を Grid Manager に保存するには、 * Create * を選択します。

新しい証明書が [クライアント] タブに表示されます。

クライアント証明書をダウンロードまたはコピーします

クライアント証明書をダウンロードまたはコピーして、他の場所で使用することができます。

手順

1. 構成 > セキュリティ > 証明書 を選択し、クライアント タブを選択します。
2. コピーまたはダウンロードする証明書を選択します。
3. 証明書をダウンロードまたはコピーします。

証明書ファイルをダウンロードします

証明書ファイルをダウンロードし `.pem`ます。

a. [証明書のダウンロード] を選択します。
b. 証明書ファイルの名前とダウンロード先を指定します。拡張子を付けてファイルを保存します `.pem`。

例： `storagegrid_certificate.pem`

証明書をコピーします

証明書のテキストをコピーして別の場所に貼り付けてください。

a. [* 証明書 PEM のコピー *] を選択します。
b. コピーした証明書をテキストエディタに貼り付けます。
c. 拡張子を付けてテキストファイルを保存します `.pem`。

例： `storagegrid_certificate.pem`

クライアント証明書を削除します

管理者クライアント証明書が不要になった場合は削除できます。

手順

1. 構成 > セキュリティ > 証明書 を選択し、クライアント タブを選択します。
2. 削除する証明書を選択します。
3. 「 * 削除」を選択して確定します。

> 最大 10 個の証明書を削除するには、 [クライアント] タブで削除する各証明書を選択し、 [* アクション * > * 削除 *] を選択します。

証明書を削除したあと、その証明書を使用していたクライアントは、 StorageGRID Prometheus データベースにアクセスするための新しいクライアント証明書を指定する必要があります。

セキュリティを設定します

StorageGRID でTLSおよびSSHポリシーを管理する

TLSおよびSSHポリシーは、クライアントアプリケーションとのセキュアなTLS接続の確立および内部StorageGRID サービスへのセキュアなSSH接続に使用されるプロトコルと暗号を決定します。

セキュリティポリシーは、TLSとSSHによる移動中のデータの暗号化方法を制御します。一般に、お使いのシステムがCCに準拠している必要がある場合、または他の暗号を使用する必要がある場合を除き、最新の互換性（デフォルト）ポリシーを使用してください。

> 一部のStorageGRID サービスは、これらのポリシーで暗号を使用するように更新されていません。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"rootアクセス権限"。

セキュリティポリシーを選択します

手順

1. 構成 > セキュリティ > *セキュリティ設定*を選択します。

   TLSおよびSSHポリシー*タブには、使用可能なポリシーが表示されます。ポリシーのタイルには、現在アクティブなポリシーが緑のチェックマークで表示されます。



2. 利用可能なポリシーの詳細については、タブを確認してください。

最新の互換性（デフォルト）

強力な暗号化が必要で、特別な要件がない場合は、デフォルトのポリシーを使用します。このポリシーは、ほとんどの TLS および SSH クライアントと互換性があります。

レガシー互換性

古いクライアントに追加の互換性オプションが必要な場合は、レガシー互換性ポリシーを使用します。このポリシーの追加オプションにより、モダン互換性ポリシーよりも安全性が低くなる可能性があります。

Common Criteriaの略

Common Criteria 認証が必要な場合は、Common Criteria ポリシーを使用します。

FIPS strict

Common Criteria認証が必要で、ロードバランサエンドポイント、テナントマネージャ、およびグリッドマネージャへの外部クライアント接続にNetApp Cryptographic Security Module（NCSM）3.1.2またはNetApp StorageGRID Kernel Crypto API 6.12.63-1+ntap1モジュールを使用する必要がある場合は、FIPSの厳格なポリシーを使用してください。このポリシーを使用すると、パフォーマンスが低下する可能性があります。

NCSM 3.1.2 と NetApp StorageGRID Kernel Crypto API 6.12.63-1+ntap1 モジュールは、以下の操作で使用されます。

- NCSM
  - 次のサービス間の TLS 接続: ADC、AMS、CMN、DDS、LDR、SSM、NMS、mgmt-api 、nginx、nginx-gw、cache-svc
  - クライアントと nginx-gw サービス (ロードバランサのエンドポイント) 間の TLS 接続
  - クライアントとLDRサービス間のTLS接続
  - SSE-S3、SSE-C、および保存されたオブジェクトの暗号化設定のオブジェクトコンテンツの暗号化
  - SSH 接続

  詳細については、NIST 暗号化アルゴリズム検証プログラム "証明書番号A7816" を参照してください。

- NetApp StorageGRIDカーネル暗号 API モジュール

  NetApp StorageGRIDカーネル暗号化 API モジュールは、VM およびStorageGRIDアプライアンス プラットフォームにのみ存在します。

  - エントロピー収集
  - ノード暗号化

    ※注記：このモジュールは認証申請されていません。

  詳細については、NIST 暗号化アルゴリズム検証プログラム "エントロピー証明書 #E223" を参照してください。

注意: このポリシーを選択すると、"ローリングリブートを実行する"すべてのノードでNCSMをアクティブ化します。再起動を開始および監視するには、[メンテナンス] > [ローリング再起動] を使用します。

カスタム

独自の暗号を適用する必要がある場合は、カスタムポリシーを作成します。

オプションとして、StorageGRID に FIPS 140 暗号化要件がある場合は、FIPS モード機能を有効にして NCSM 3.1.2 および NetApp StorageGRID Kernel Crypto API 6.12.63-1+ntap1 モジュールを使用してください：

a. 設定する `fipsMode`パラメータに `true`。
b. プロンプトが表示されたら、"ローリングリブートを実行する"すべてのノードで暗号化モジュールをアクティブ化します。再起動を開始および監視するには、[メンテナンス] > [ローリング再起動] を使用します。
c. アクティブな FIPS モジュール バージョンを表示するには、[サポート] > [診断] を選択します。

3. 各ポリシーの暗号、プロトコル、およびアルゴリズムの詳細を表示するには、*[詳細を表示]*を選択します。
4. 現在のポリシーを変更するには、*[ポリシーを使用]*を選択します。

   ポリシータイルの*現在のポリシー*の横に緑のチェックマークが表示されます。

カスタムセキュリティポリシーを作成します

独自の暗号を適用する必要がある場合は、カスタムポリシーを作成できます。

手順

1. 作成するカスタムポリシーに最も近いポリシーのタイルで、*[詳細を表示]*を選択します。
2. を選択し、[キャンセル]*を選択します。



3. [カスタムポリシー]タイルで、*[設定と使用]*を選択します。

4. コピーしたJSONを貼り付けて、必要な変更を行います。
5. [ポリシーを使用]*を選択します。

   [カスタムポリシー]タイルの*[現在のポリシー]*の横に緑のチェックマークが表示されます。

6. 必要に応じて、*[設定の編集]*を選択して、新しいカスタムポリシーをさらに変更します。

一時的にデフォルトのセキュリティポリシーに戻します

カスタムセキュリティポリシーを設定した場合、設定したTLSポリシーがと互換性がないと、Grid Managerにサインインできないことがあります"サーバ証明書を設定しました"。

一時的にデフォルトのセキュリティポリシーに戻すことができます。

手順

1. 管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@Admin_Node_IP`
   b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

      rootとしてログインすると、プロンプトがからに `#`変わります `$`。

2. 次のコマンドを実行します。

   ```
   restore-default-cipher-configurations
   ```

3. Web ブラウザから、同じ管理ノード上の Grid Manager にアクセスする。
4. ポリシーを再度設定するには、の手順に従いセキュリティポリシーを選択しますます。

StorageGRID ネットワークとオブジェクトのセキュリティを設定する

ネットワークとオブジェクトのセキュリティを設定して、格納オブジェクトの暗号化、特定のS3要求の防止、ストレージノードへのクライアント接続でHTTPSではなくHTTPを使用できるようにすることができます。

格納オブジェクトの暗号化

格納オブジェクトの暗号化を使用すると、S3経由で取り込まれたすべてのオブジェクトデータを暗号化できます。デフォルトでは、格納オブジェクトは暗号化されませんが、AES‐128またはAES‐256暗号化アルゴリズムを使用してオブジェクトを暗号化することができます。この設定を有効にすると、新たに取り込まれたすべてのオブジェクトが暗号化されますが、既存の格納オブジェクトに対する変更はありません。暗号化を無効にすると、現在暗号化されているオブジェクトは暗号化されたままですが、新しく取り込まれたオブジェクトは暗号化されません

格納オブジェクトの暗号化設定は、バケットレベルまたはオブジェクトレベルの暗号化で暗号化されていないS3オブジェクトにのみ適用されます。

StorageGRID暗号化方式の詳細については、を参照してください"StorageGRID の暗号化方式を確認します"。

クライアントの変更を防止します

[Prevent client modification]は、システム全体の設定です。[Prevent client modification *]オプションを選択すると、次の要求が拒否されます。

S3 REST API

- DeleteBucketヨウキユウ
- 既存オブジェクトのデータ、ユーザ定義メタデータ、または S3 オブジェクトのタグを変更するすべての要求

ストレージノード接続用の**HTTP**を有効にします

デフォルトでは、クライアントアプリケーションは、ストレージノードへの直接接続にHTTPSネットワークプロトコルを使用します。非本番環境のグリッドのテストなどの目的で、これらの接続に対して HTTP を有効にすることもできます。

ストレージノード接続にHTTPを使用するのは、S3クライアントからストレージノードへのHTTP接続を直接確立する必要がある場合のみです。HTTPS接続のみを使用するクライアントや、ロードバランササービスに接続するクライアント（HTTPまたはHTTPSを使用できるため）には、このオプションを使用する必要はありません"各ロードバランサエンドポイントを設定します"。

S3クライアントがHTTPまたはHTTPSを使用してストレージノードに接続するときに使用するポートについては、を参照してください"Summary ：クライアント接続の IP アドレスとポート"。

オプションを選択します

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- Root Access 権限が割り当てられている。

手順

1. 構成 > セキュリティ > *セキュリティ設定*を選択します。
2. [ネットワークとオブジェクト]タブを選択します。
3. 格納オブジェクトを暗号化しない場合は*なし*（デフォルト）設定を使用し、格納オブジェクトを暗号化する場合は* AES-128 または AES-256 *を選択します。
4. 必要に応じて、[Prevent client modification]*を選択し、S3クライアントが特定の要求を実行しないようにします。

   この設定を変更すると、新しい設定が適用されるまで約 1 分かかります。設定した値は、パフォーマンスと拡張用にキャッシュされます。

5. 必要に応じて、クライアントがストレージノードに直接接続し、HTTP接続を使用する場合は、*[ストレージノード接続用のHTTPを有効にする]*を選択します。

要求が暗号化されずに送信されるため、本番環境のグリッドで HTTP を有効にする場合は注意してください。

6. [保存（ Save ）] を選択します。

StorageGRIDインターフェイスのセキュリティ設定を変更する

インターフェイスのセキュリティ設定では、ユーザが指定した時間以上非アクティブであった場合にサインアウトするかどうか、およびスタックトレースをAPIエラー応答に含めるかどうかを制御できます。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- そうだな "rootアクセス権限"

タスクの内容

[セキュリティ設定]ページには、*ブラウザの非アクティブタイムアウト*と*管理APIスタックトレース*の設定が含まれています。

ブラウザの非アクティブタイムアウト

ユーザのブラウザが非アクティブになってからサインアウトされるまでの時間を示します。デフォルトは15分です。

ブラウザの非アクティブ時のタイムアウトは、次の方法でも制御されます。

- システムセキュリティ用の、個別の設定不可能な StorageGRID タイマー。各ユーザの認証トークンは、ユーザがサインインしてから16時間後に期限切れになります。ユーザの認証が期限切れになると、ブラウザの非アクティブタイムアウトが無効になっていたり、ブラウザのタイムアウト値に達していない場合でも、そのユーザは自動的にサインアウトされます。トークンを更新するには、再度サインインする必要があります。
- アイデンティティプロバイダのタイムアウト設定（StorageGRID でシングルサインオン（SSO）が有効になっている場合）。

  SSO が有効になっていて、ユーザーのブラウザがタイムアウトした場合、ユーザーは SSO 資格情報を再入力してStorageGRID に再度アクセスする必要があります。見る"SSOの動作" 。

管理**API**スタックトレース

Grid ManagerおよびTenant Manager APIのエラー応答でスタックトレースを返すかどうかを制御します。

このオプションはデフォルトでは無効になっていますが、テスト環境では有効にすることもできます。一般に、本番環境では、APIエラーが発生したときに内部ソフトウェアの詳細が表示されないように、スタックトレースは無効のままにしておく必要があります。

手順

1. 構成 > セキュリティ > *セキュリティ設定*を選択します。
2. [インターフェイス]*タブを選択します。
3. ブラウザ非アクティブタイムアウトの設定を変更するには、次の手順を実行します。

a. アコーディオンを展開します。

b. タイムアウト期間を変更するには、60秒から7日間の値を指定します。デフォルトのタイムアウトは15分です。

c. この機能を無効にするには、チェックボックスをオフにします。

d. [保存（ Save ）] を選択します。

新しい設定は、現在サインインしているユーザーには影響しません。新しいタイムアウト設定を有効にするには、再度サインインするか、ブラウザを更新する必要があります。

4. 管理APIスタックトレースの設定を変更するには、次の手順を実行します。

a. アコーディオンを展開します。

b. Grid ManagerおよびTenant Manager APIのエラー応答でスタックトレースを返す場合は、チェックボックスを選択します。

APIエラーが発生したときに内部ソフトウェアの詳細が表示されないように、本番環境ではスタックトレースを無効のままにします。

c. [保存（ Save ）] を選択します。

StorageGRIDで外部**SSH**アクセスを管理する

外部アクセスをブロックまたは許可することで、グリッドへの受信トラフィックの SSH アクセスを管理します。 SSH 外部アクセスを管理しても、グリッド内のノード間のトラフィックには影響しません。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- そうだな "rootアクセス権限"

タスクの内容

システムのセキュリティを強化するために、外部からの SSH アクセスはデフォルトでブロックされます。トラブルシューティングなど、着信 SSH アクセスを必要とするタスクを実行する必要がある場合は、一時的に外部アクセスを許可します。タスクが完了したら、外部からのアクセスをブロックします。

手順

1. 構成 > セキュリティ > *セキュリティ設定*を選択します。
2. *SSHをブロック*タブを選択します。
3. 外部 SSH アクセスを管理するには、受信 **SSH** アクセスをブロック オプションを使用します。

a. アクセスをブロックするにはチェックボックスを選択します（デフォルト）。

b. アクセスを許可するにはチェックボックスをオフにします。

サービス ラップトップと他のすべてのグリッド ノード間のポート 22 へのアクセスが必要です。メンテナンス タスクを完了したら、ポート 22 へのアクセスを削除します。

4. [保存（ Save ）] を選択します。

キー管理サーバを設定

StorageGRIDのキー管理サーバーについて学ぶ

キー管理サーバ（ KMS ）は、関連する StorageGRID サイトの StorageGRID アプライアンスノードに Key Management Interoperability Protocol （ KMIP ）を使用して暗号化キーを提供する外部のサードパーティシステムです。

StorageGRIDでは、特定のキー管理サーバのみがサポートされます。サポートされている製品とバージョンのリストについては、を参照して "NetApp Interoperability Matrix Tool（IMT）"ください。

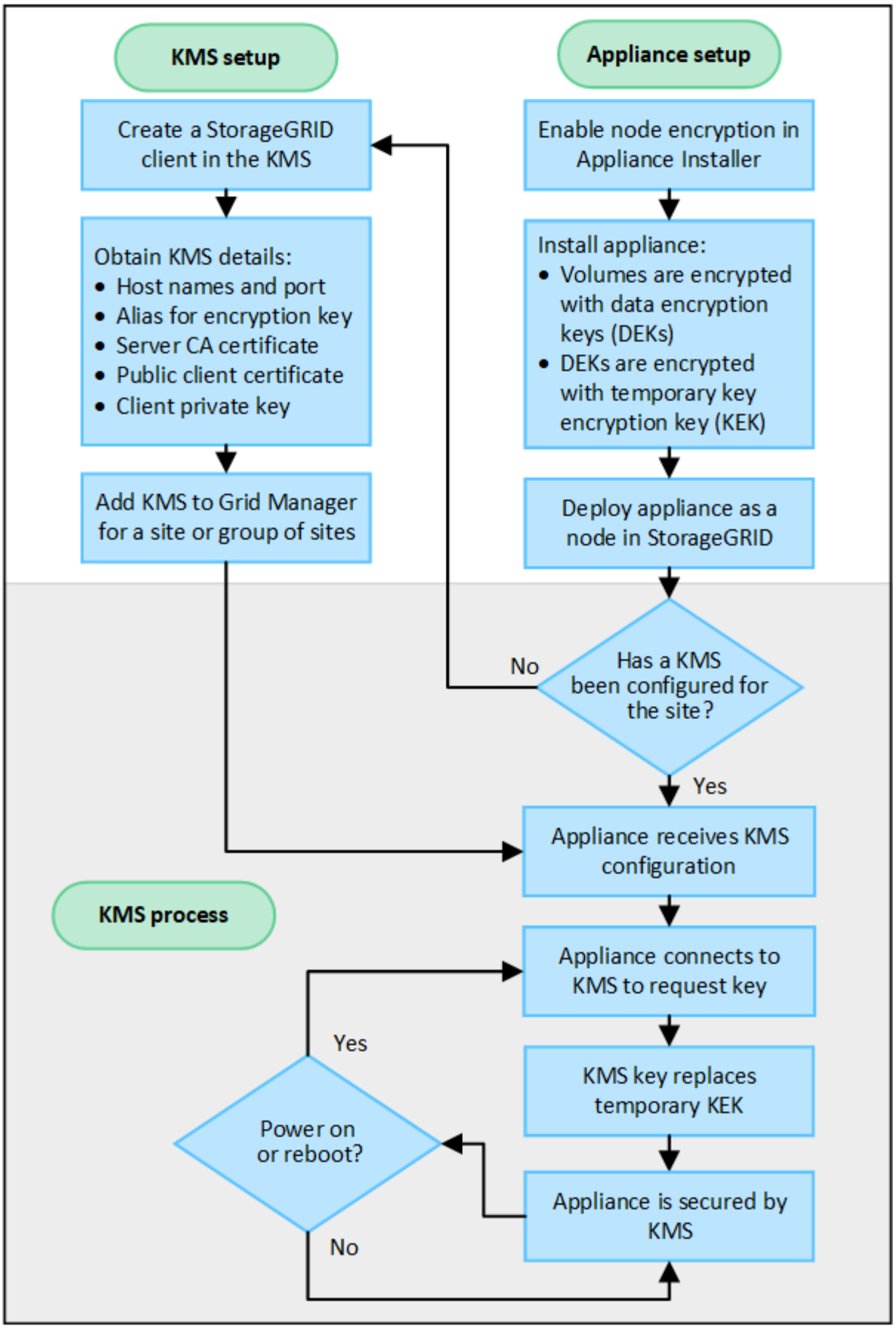
インストール時にノード暗号化 * 設定が有効になっている StorageGRID アプライアンスノードのノード暗号化キーを管理するには、 1 つ以上のキー管理サーバを使用します。これらのアプライアンスノードでキー管理サーバを使用すると、アプライアンスをデータセンターから削除した場合でも、データを保護できます。アプライアンスボリュームが暗号化されると、ノードがKMSと通信できないかぎり、アプライアンスのデータにアクセスすることはできません。

> StorageGRID では、アプライアンスノードの暗号化と復号化に使用する外部キーは作成も管理もされません。外部キー管理サーバを使用して StorageGRID データを保護する場合は、そのサーバの設定方法を理解し、暗号化キーの管理方法を理解しておく必要があります。キー管理タスクの実行については、この手順では説明していません。サポートが必要な場合は、キー管理サーバのドキュメントを参照するか、テクニカルサポートにお問い合わせください。

StorageGRID キー管理サーバとアプライアンスの設定

キー管理サーバ（ KMS ）を使用してアプライアンスノード上の StorageGRID データを保護する前に、 1 つ以上の KMS サーバを設定してアプライアンスノードのノード暗号化を有効にするという 2 つの設定タスクを完了しておく必要があります。これらの 2 つの設定タスクが完了すると、キー管理プロセスが自動的に実行されます。

フローチャートは、 KMS を使用してアプライアンスノード上の StorageGRID データを保護する手順の概要を示しています。



フローチャートには、 KMS のセットアップとアプライアンスのセットアップが並行して行われていることが

示されています。ただし、要件に基づいて、新しいアプライアンスノードのノード暗号化を有効にする前後にキー管理サーバをセットアップできます。

キー管理サーバ（ KMS ）のセットアップ

キー管理サーバのセットアップには、主に次の手順が含まれます。

ステップ	を参照してください
KMS ソフトウェアにアクセスし、各 KMS または KMS クラスタに StorageGRID 用のクライアントを追加します。	"KMS でクライアントとして StorageGRID を設定します"
KMS で StorageGRID クライアントの必要な情報を入手します。	"KMS でクライアントとして StorageGRID を設定します"
Grid Manager に KMS を追加して 1 つのサイトまたはデフォルトのサイトグループに割り当て、必要な証明書をアップロードして、 KMS の設定を保存します。	"キー管理サーバ（ KMS ）を追加する"

アプライアンスをセットアップします

KMS を使用するためにアプライアンスノードをセットアップするには、次の手順に従います。

1. アプライアンスのハードウェア構成フェーズでは、 StorageGRID アプライアンスインストーラを使用してアプライアンスのノード暗号化 * 設定を有効にします。

   > アプライアンスをグリッドに追加したあとに* Node Encryption *設定を有効にすることはできません。また、ノード暗号化が有効になっていないアプライアンスでは外部キー管理を使用できません。

2. StorageGRID アプライアンスインストーラを実行します。インストール時に、次のように各アプライアンスボリュームにランダムデータ暗号化キー（ DEK ）が割り当てられます。
   - DEK は、各ボリュームのデータの暗号化に使用されます。これらのキーは、アプライアンスOSのLinux Unified Key Setup（LUKS）ディスク暗号化を使用して生成され、変更することはできません。
   - 各 DEK は、 KEK （ Master Key Encryption Key ）によって暗号化されます。最初の KEK は、アプライアンスが KMS に接続できるまで DEK を暗号化する一時キーです。
3. StorageGRID にアプライアンスノードを追加します。

詳細は、を参照してください "ノード暗号化を有効にします"。

キー管理の暗号化プロセス（自動的に実行）

キー管理の暗号化には、次の高度な手順が含まれています。これらの手順は自動的に実行されます。

1. ノードの暗号化が有効になっているアプライアンスをグリッドにインストールすると、 StorageGRID は、新しいノードを含むサイトに KMS 設定が存在するかどうかを確認します。

- KMS がすでにサイト用に設定されている場合、アプライアンスは KMS の設定を受信します。
- KMS がサイト用にまだ設定されていない場合は、サイトに KMS を設定し、アプライアンスが KMS の設定を受信するまで、アプライアンス上のデータは一時的な KEK によって暗号化されたままになります。

2. アプライアンスは KMS 設定を使用して KMS に接続し、暗号化キーを要求します。
3. KMS は暗号化キーをアプライアンスに送信します。KMS の新しいキーは一時的な KEK に代わるものであり、アプライアンスボリュームの DEK の暗号化と復号化に使用されるようになりました。

> 暗号化されたアプライアンスノードから設定された KMS に接続する前に存在するデータは、すべて一時キーで暗号化されます。ただし、一時キーを KMS 暗号化キーに置き換えるまでは、アプライアンスボリュームをデータセンターから削除できないようにする必要があります。

4. アプライアンスの電源をオンにするか再接続すると、 KMS に接続してキーを要求します。揮発性メモリに保存されているキーは、電源の喪失や再起動に耐えられません。

StorageGRID キー管理サーバの要件と考慮事項

外部キー管理サーバ（ KMS ）を設定する前に、考慮事項と要件を確認しておく必要があります。

サポートされている**KMIP**のバージョンを教えてください。

StorageGRID は KMIP バージョン 1.4 をサポートしています。

"Key Management Interoperability Protocol （キー管理相互運用性プロトコル）仕様バージョン 1.4"

ネットワークに関する考慮事項

ネットワークのファイアウォールの設定で、各アプライアンスノードが Key Management Interoperability Protocol （ KMIP ）の通信に使用するポートを介して通信できるようにする必要があります。デフォルトの KMIP ポートは 5696 です。

ノード暗号化を使用する各アプライアンスノードに、サイト用に設定した KMS または KMS クラスタへのネットワークアクセスがあることを確認してください。

サポートされている**TLS**のバージョンを教えてください。

アプライアンスノードと設定された KMS の間の通信には、セキュアな TLS 接続が使用されます。StorageGRIDでは、KMSがサポートする内容と使用している内容に基づいて、KMSまたはKMSクラスタへのKMIP接続を確立する際に、TLS 1.2またはTLS 1.3のいずれかのプロトコルをサポートできます"TLSおよびSSHポリシー"。

StorageGRID は、接続時に KMS とプロトコルと暗号 (TLS 1.2) または暗号スイート (TLS 1.3) をネゴシエートします。利用可能なプロトコルバージョンと暗号/暗号スイートを確認するには、 `tlsOutbound`グリッドのアクティブな TLS および SSH ポリシーのセクション (* [構成] > [セキュリティ] [セキュリティ設定])。

サポートされているアプライアンスはどれですか。

キー管理サーバ（ KMS ）を使用して、「ノード暗号化 * 」が有効になっているグリッド内の StorageGRID

アプライアンスの暗号化キーを管理できます。この設定は、 StorageGRID アプライアンスインストーラを使用してアプライアンスをインストールするハードウェア構成の段階でのみ有効にできます。

> アプライアンスをグリッドに追加したあとにノード暗号化を有効にすることはできません。また、ノード暗号化が有効になっていないアプライアンスでは、外部キー管理を使用できません。

StorageGRID アプライアンスおよびアプライアンスノードに対して設定したKMSを使用できます。

次のようなソフトウェアベース（アプライアンス以外）のノードでは、設定されたKMSを使用できません。

- 仮想マシン（ VM ）として導入されたノード
- Linux ホストのコンテナエンジン内に導入されたノード

これらの他のプラットフォームに導入されたノードでは、データストアまたはディスクレベルで StorageGRID 外部の暗号化を使用できます。

キー管理サーバを設定する必要があるのはいつですか？

新規インストールの場合は、テナントを作成する前に Grid Manager で 1 つ以上のキー管理サーバをセットアップするのが一般的です。この順序により、ノード上に格納されるオブジェクトデータよりも先にノードが保護されます。

Grid Manager では、アプライアンスノードのインストール前またはインストール後にキー管理サーバを設定できます。

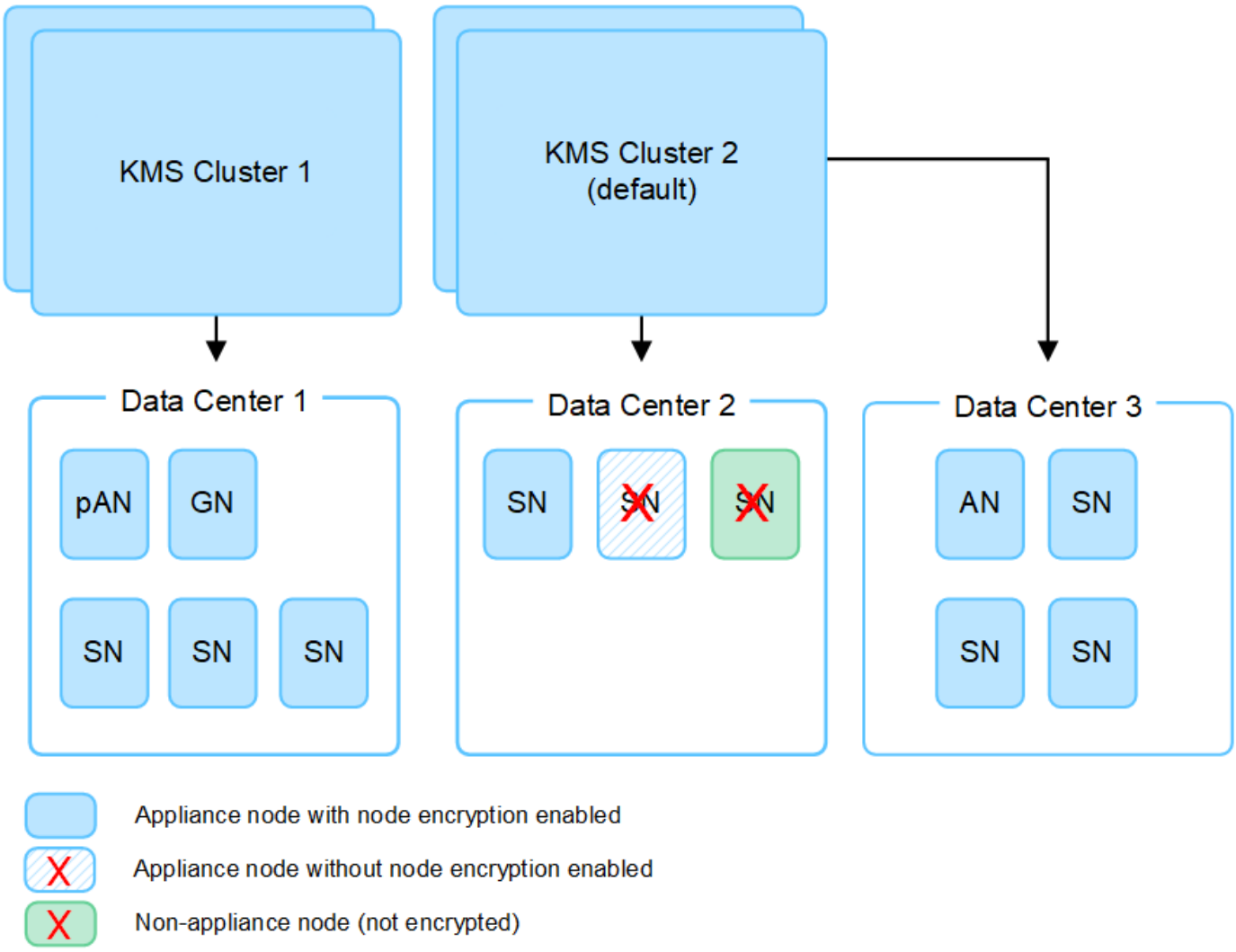
必要なキー管理サーバの数

1 つ以上の外部キー管理サーバを設定して、 StorageGRID システム内のアプライアンスノードに暗号化キーを提供できます。各 KMS は、 1 つのサイトまたはサイトグループにある StorageGRID アプライアンスノードに単一の暗号化キーを提供します。

StorageGRID は KMS クラスタの使用をサポートしています。各 KMS クラスタには、設定と暗号化キーを共有するレプリケートされた複数のキー管理サーバが含まれます。高可用性構成のフェイルオーバー機能が向上するため、 KMS クラスタをキー管理に使用することを推奨します。

たとえば、 StorageGRID システムに 3 つのデータセンターサイトがあるとします。1 つの KMS クラスタを設定して、データセンター 1 のすべてのアプライアンスノードともう 1 つの KMS クラスタのキーを取得し、他のすべてのサイトにあるすべてのアプライアンスノードのキーを取得することができます。2 つ目の KMS クラスタを追加すると、データセンター 2 とデータセンター 3 にデフォルトの KMS を設定できます。

非アプライアンスノード、またはインストール時に* Node Encryption *設定が有効になっていないアプライアンスノードには、KMSを使用できないことに注意してください。



キーをローテーションするとどうなりますか。

セキュリティのベストプラクティスとして、設定した各KMSで定期的に使用する必要があります"暗号化キーのローテーション"。

新しいキーバージョンが利用可能になった場合：

- このサービスは、 KMS に関連付けられているサイトにある暗号化されたアプライアンスノードに自動的に配信されます。キーが回転した後 1 時間以内に分配が行われる必要があります。
- 新しいキーバージョンが配布されたときに暗号化アプライアンスノードがオフラインになっている場合、ノードはリブート後すぐに新しいキーを受け取ります。
- 何らかの理由で新しいバージョンのキーを使用してアプライアンスボリュームを暗号化できない場合は、アプライアンスノードに対して* kms encryption key rotation failed *アラートがトリガーされます。このアラートの解決方法については、テクニカルサポートへの問い合わせが必要になることがあります。

アプライアンスノードは暗号化したあとに再利用できますか。

暗号化されたアプライアンスを別の StorageGRID システムにインストールする必要がある場合は、先にグリッドノードの運用を停止して、オブジェクトデータを別のノードに移動しておく必要があります。その後、StorageGRIDアプライアンスインストーラを使用してを実行できます "KMS構成をクリアします"。KMS

の設定をクリアすると、「ノード暗号化 * 」設定が無効になり、アプライアンスノードと StorageGRID サイトの KMS 設定の間の関連付けが解除されます。

KMS 暗号化キーにアクセスできないため、アプライアンスに残っているデータにはアクセスできなくなり、永続的にロックされます。

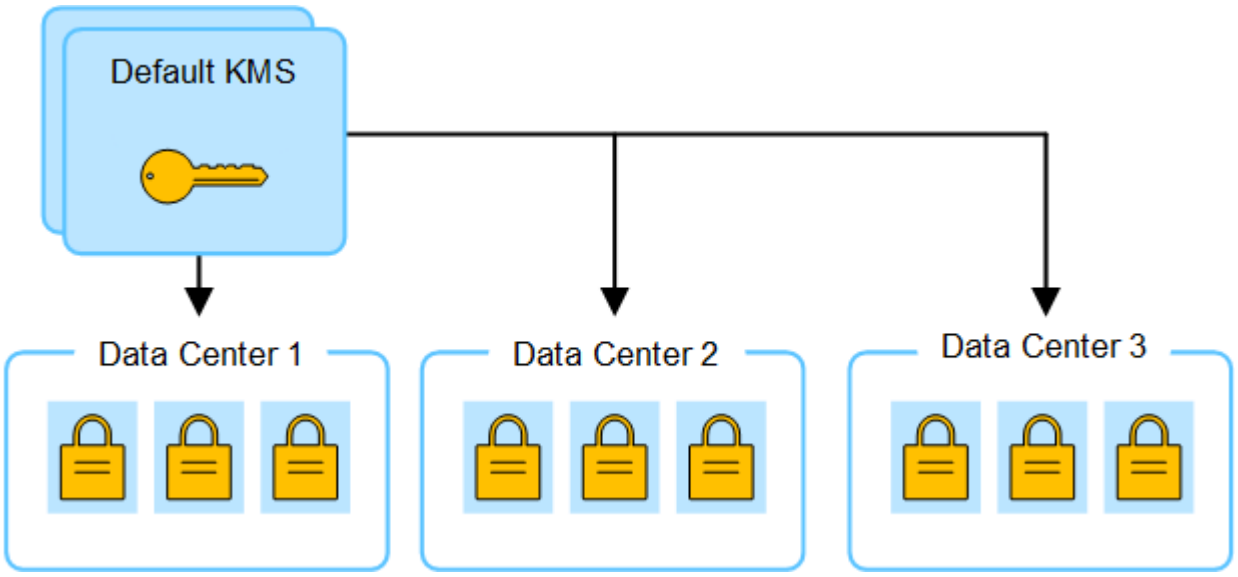
StorageGRID サイトの **KMS** を変更する際の考慮事項

各キー管理サーバ（ KMS ）または KMS クラスタは、 1 つのサイトまたはサイトグループにあるすべてのアプライアンスノードに暗号化キーを提供します。サイトで使用する KMS を変更する必要がある場合は、暗号化キーを KMS から別の KMS にコピーする必要があります。

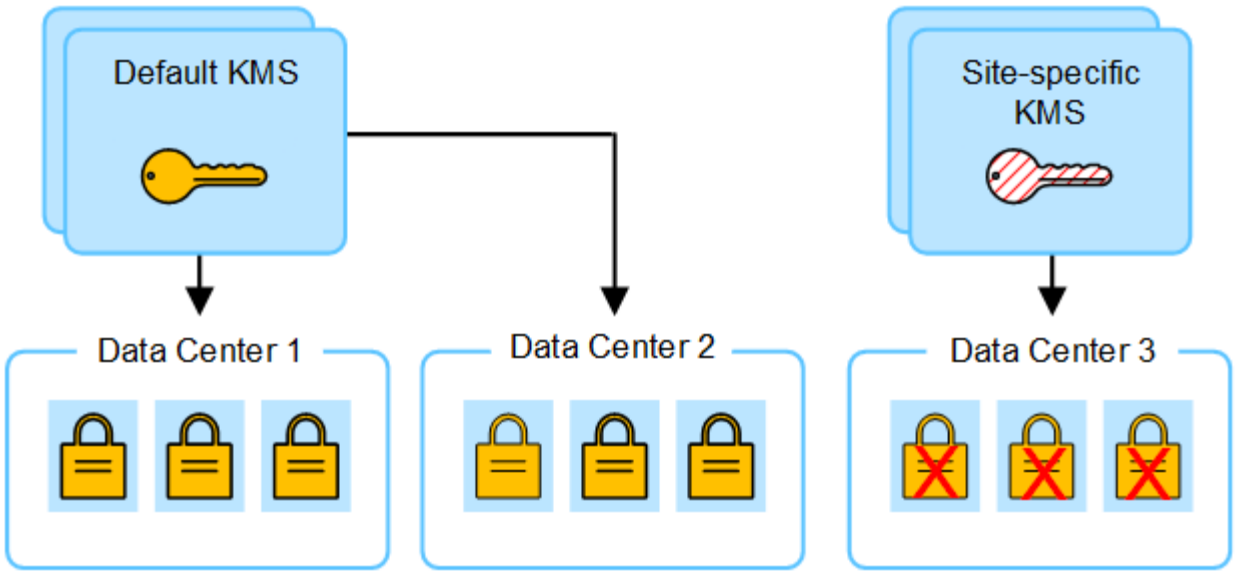
サイトで使用されている KMS を変更する場合は、そのサイトで以前に暗号化したアプライアンスノードを新しい KMS に格納されているキーを使用して復号化できることを確認する必要があります。場合によっては、暗号化キーの現在のバージョンを元の KMS から新しい KMS にコピーする必要があります。サイトで暗号化されたアプライアンスノードを復号化するために、 KMS に正しいキーがあることを確認する必要があります。

例：

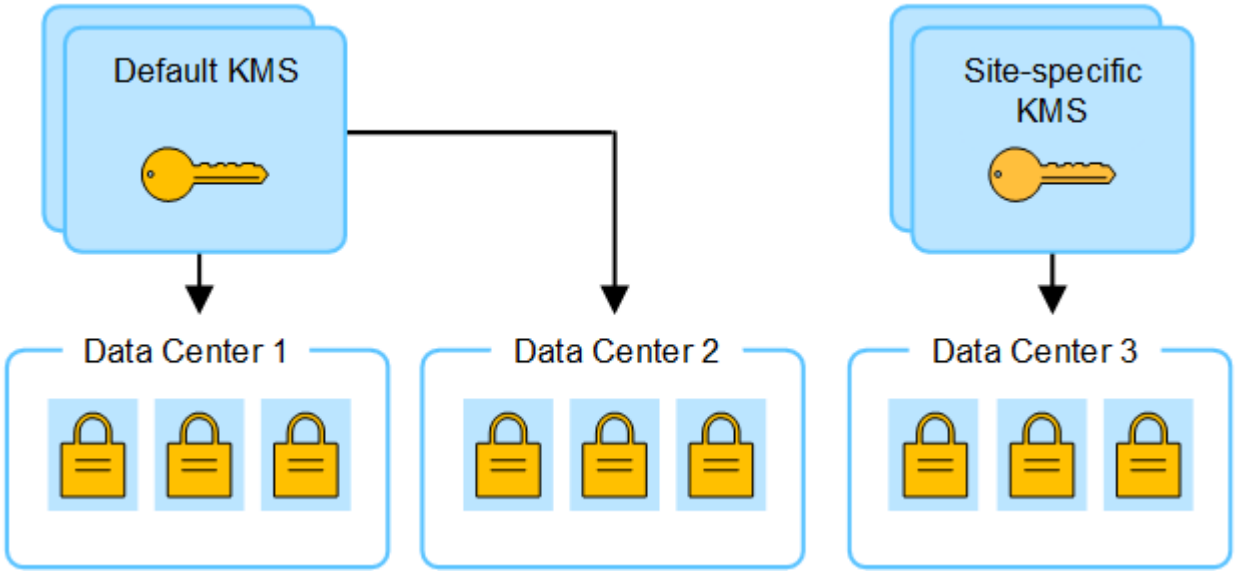
1. 最初に、専用のKMSを持たないすべてのサイトを環境 するデフォルトKMSを構成します。
2. KMS を保存すると、「 Node Encryption * 」設定が有効になっているすべてのアプライアンスノードが KMS に接続して暗号化キーを要求します。このキーは、すべてのサイトのアプライアンスノードの暗号化に使用されます。同じキーを使用して、これらのアプライアンスを復号化する必要もあります。



3. 1 つのサイト（図のデータセンター 3 ）にサイト固有の KMS を追加することにしました。ただし、アプライアンスノードはすでに暗号化されているため、サイト固有の KMS の設定を保存しようとすると検証エラーが発生します。このエラーは、サイト固有の KMS に、そのサイトでノードを復号化するための正しいキーがないことが原因で発生します。



4. 問題 に対応するには、現在のバージョンの暗号化キーをデフォルトの KMS から新しい KMS にコピーします。（技術的には、元のキーを同じエイリアスを持つ新しいキーにコピーします。元のキーは新しいキーの以前のバージョンになります）。サイト固有のKMSに、データセンター3のアプライアンスノードを復号化するための正しいキーが追加され、StorageGRIDに保存できるようになりました。



サイトに使用する **KMS** を変更するユースケース

次の表に、サイトの KMS を変更する一般的なケースに必要な手順をまとめます。

サイトの **KMS** を変更するユースケース	必要な手順
サイト固有の KMS エントリが 1 つ以上あり、それらのエントリの 1 つをデフォルトの KMS として使用する必要があります。	サイト固有の KMS を編集します。[* キー管理対象 *] フィールドで、別の KMS （デフォルト KMS ）で管理されていないサイト * を選択します。サイト固有の KMS がデフォルトの KMS として使用されるようになります。それは専用のKMSを持っていないすべてのサイトに適用されます。 "キー管理サーバ（ KMS ）を編集する"
デフォルトの KMS を使用して、拡張時に新しいサイトを追加する必要があります。新しいサイトにはデフォルトのKMSを使用しないでください。	1. 新しいサイトにあるアプライアンスノードがデフォルトの KMS によって暗号化済みの場合は、 KMS ソフトウェアを使用して、現在のバージョンの暗号化キーをデフォルトの KMS から新しい KMS にコピーします。 2. Grid Manager を使用して新しい KMS を追加し、サイトを選択します。 "キー管理サーバ（ KMS ）を追加する"
サイトの KMS で別のサーバを使用するとします。	1. サイトのアプライアンスノードが既存の KMS によって暗号化済みの場合は、 KMS ソフトウェアを使用して、既存の KMS から新しい KMS に暗号化キーの現在のバージョンをコピーします。 2. Grid Manager を使用して既存の KMS 設定を編集し、新しいホスト名または IP アドレスを入力します。 "キー管理サーバ（ KMS ）を追加する"

KMS でクライアントとして **StorageGRID** を設定します

KMS を StorageGRID に追加する前に、各外部キー管理サーバまたは KMS クラスタのクライアントとして StorageGRID を設定する必要があります。

これらの手順は、タレスCipherTrust ManagerとHashicorp Vaultに適用されます。サポートされている製品とバージョンのリストについては、を参照して "NetApp Interoperability Matrix Tool（IMT）"ください。

手順

1. KMS ソフトウェアから、使用する KMS または KMS クラスタごとに StorageGRID クライアントを作成します。

   各 KMS は、 1 つのサイトまたはサイトグループにある StorageGRID アプライアンスノードの単一の暗号化キーを管理します。

2. 次の2つの方法のいずれかを使用してキーを作成します。

   - KMS製品のキー管理ページを使用します。KMSまたはKMSクラスタごとにAES暗号化キーを作成します。

     暗号化キーは2、048ビット以上で、エクスポート可能である必要があります。

- StorageGRIDにキーを作成してもらいます。のあとにテストして保存すると、プロンプトが表示され"クライアント証明書のアップロード"ます。

3. KMS または KMS クラスタごとに次の情報を記録します。

   KMSをStorageGRIDに追加するときは、次の情報が必要です。

   - 各サーバのホスト名または IP アドレス。
   - KMS で使用される KMIP ポート。
   - KMS 内の暗号化キーのキーエイリアス。

4. KMS または KMS クラスタごとに、認証局（ CA ）が署名したサーバ証明書または PEM でエンコードされた各 CA 証明書ファイルを含む証明書バンドルを、証明書チェーンの順序で連結して取得します。

   サーバ証明書を使用すると、外部 KMS は StorageGRID に対して自身を認証できます。

   - 証明書では、 Privacy Enhanced Mail （ PEM ） Base-64 エンコード X.509 形式を使用する必要があります。
   - 各サーバ証明書の Subject Alternative Name （ SAN ）フィールドには、 StorageGRID が接続する完全修飾ドメイン名（ FQDN ）または IP アドレスを含める必要があります。

     StorageGRID で KMS を設定する場合は、「 * Hostname * 」フィールドに同じ FQDN または IP アドレスを入力する必要があります。

   - サーバ証明書は、 KMS の KMIP インターフェイスで使用されている証明書と一致する必要があります。通常はポート 5696 が使用されます。

5. 外部 KMS によって StorageGRID に発行されたパブリッククライアント証明書とクライアント証明書の秘密鍵を取得します。

   クライアント証明書は、 StorageGRID が KMS に対して自身を認証することを許可します。

StorageGRIDでキー管理サーバーを追加する

StorageGRID キー管理サーバウィザードを使用して、各 KMS または KMS クラスタを追加します。

開始する前に

- を確認しておきます"キー管理サーバを使用する際の考慮事項と要件"。
- "KMS でクライアントとして StorageGRID を設定"各KMSまたはKMSクラスタに必要な情報を確認しておきます。
- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"rootアクセス権限"。

タスクの内容

可能環境 であれば、サイト固有のキー管理サーバを設定してから、別の KMS で管理されていないデフォルトの KMS を設定してください。最初にデフォルトの KMS を作成すると、グリッド内のノードで暗号化されたすべてのアプライアンスがデフォルトの KMS で暗号化されます。サイト固有の KMS をあとで作成するには、まず、暗号化キーの現在のバージョンをデフォルトの KMS から新しい KMS にコピーする必要がありま

す。詳細は、を参照してください "サイトの KMS を変更する際の考慮事項" 。

ステップ**1**：**KMS**の詳細

キー管理サーバの追加ウィザードの手順1（KMSの詳細）で、KMSまたはKMSクラスタの詳細を指定します。

手順

1. 構成 > セキュリティ > *キー管理サーバー*を選択します。

   [設定の詳細]タブが選択された状態で、[キー管理サーバ]ページが表示されます。

2. 「 * Create * 」を選択します。

   キー管理サーバの追加ウィザードの手順1（KMSの詳細）が表示されます。

3. KMS および設定した StorageGRID クライアントの情報を KMS で入力します。

フィールド	製品説明
KMS名	この KMS を特定するのに役立つわかりやすい名前。1~64 文字で指定する必要があります。
キー名	KMS 内の StorageGRID クライアントの正確なキーエイリアス。1~255 文字で指定する必要があります。 注: KMS製品を使用してキーを作成していない場合は、StorageGRIDでキーを作成するように要求されます。
のキーを管理します	この KMS に関連する StorageGRID サイトを参照してください。可能であれば、サイト固有のキー管理サーバを設定してから、環境 で他の KMS で管理されていないすべてのサイトをデフォルトの KMS で設定する必要があります。 • 特定のサイトのアプライアンスノードの暗号化キーをこの KMS で管理する場合は、サイトを選択します。 • 専用のKMSを持たないサイトや、その後の拡張で追加するサイトに適用されるデフォルトKMSを設定するには、*[別のKMSで管理されていないサイト(デフォルトKMS)]*を選択します。 ◦ 注： * 以前にデフォルト KMS で暗号化されていたサイトを選択しても、新しい KMS に元の暗号化キーの現在のバージョンを提供しなかった場合、 KMS の設定を保存すると、検証エラーが発生します。
ポート	KMS サーバが Key Management Interoperability Protocol （ KMIP ）の通信に使用するポート。デフォルトでは、 KMIP 標準ポートである 5696 が使用されます。

フィールド	製品説明
ホスト名	KMS の完全修飾ドメイン名または IP アドレス。 *注：*サーバ証明書のSubject Alternative Name（SAN）フィールドには、ここに入力するFQDNまたはIPアドレスが含まれている必要があります。そうしないと、 StorageGRID は KMS クラスタ内のすべてのサーバに接続できなくなります。

4. KMSクラスタを構成する場合は、*[別のホスト名を追加]*を選択して、クラスタ内の各サーバのホスト名を追加します。
5. 「 * Continue * 」を選択します。

手順**2:**サーバー証明書をアップロードします

キー管理サーバの追加ウィザードの手順2（サーバ証明書をアップロード）で、KMSのサーバ証明書（または証明書バンドル）をアップロードします。サーバ証明書を使用すると、外部 KMS は StorageGRID に対して自身を認証できます。

手順

1. [手順2（サーバ証明書のアップロード）]*で、保存されているサーバ証明書または証明書バンドルの場所を参照します。
2. 証明書ファイルをアップロードします。

   サーバ証明書のメタデータが表示されます。

   証明書バンドルをアップロードした場合は、各証明書のメタデータが独自のタブに表示されます。

3. 「 * Continue * 」を選択します。

手順**3**：クライアント証明書をアップロードする

キー管理サーバの追加ウィザードの手順3（クライアント証明書のアップロード）で、クライアント証明書とクライアント証明書の秘密鍵をアップロードします。クライアント証明書は、 StorageGRID が KMS に対して自身を認証することを許可します。

手順

1. ステップ3（クライアント証明書のアップロード）*で、クライアント証明書の場所を参照します。
2. クライアント証明書ファイルをアップロードします。

   クライアント証明書のメタデータが表示されます。

3. クライアント証明書の秘密鍵の場所を参照します。
4. 秘密鍵ファイルをアップロードします。
5. [テストして保存]*を選択します。

   キーが存在しない場合は、StorageGRIDでキーを作成するように求めるメッセージが表示されます。

キー管理サーバとアプライアンスノードの間の接続をテストします。すべての接続が有効で、正しいキーが KMS にある場合は、新しいキー管理サーバが Key Management Server ページの表に追加されます。

> KMS を追加すると、すぐに [Key Management Server] ページの証明書ステータスが [Unknown （不明）] と表示されます。各証明書の実際のステータスの StorageGRID 取得には 30 分程度かかる場合があります。最新のステータスを表示するには、 Web ブラウザの表示を更新する必要があります。

6. を選択したときにエラーメッセージが表示された場合は、メッセージの詳細を確認し、[OK]*を選択します。

   たとえば、接続テストに失敗した場合は、 422 ： Unprocessable Entity エラーが返されることがあります。

7. 外部接続をテストせずに現在の設定を保存する必要がある場合は、*[強制保存]*を選択します。

   > [Force save]*を選択すると、KMSの構成が保存されますが、各アプライアンスからそのKMSへの外部接続はテストされません。構成を含む問題 がある場合、該当するサイトでノード暗号化が有効になっているアプライアンスノードをリブートできない可能性があります。問題が解決するまでデータにアクセスできなくなる可能性があります。

8. 確認の警告を確認し、設定を強制的に保存する場合は、「 * OK 」を選択します。

   KMS の設定は保存されますが、 KMS への接続はテストされません。

StorageGRID でキー管理サーバーを管理する

キー管理サーバ（KMS）の管理には、詳細の表示と編集、証明書の管理、暗号化されたノードの表示、不要になったKMSの削除が含まれます。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"必要なアクセス権限"。

KMS の詳細を確認します

キーの詳細、サーバ証明書とクライアント証明書の現在のステータスなど、StorageGRIDシステム内の各キー管理サーバ（KMS）に関する情報を表示できます。

手順

1. 構成 > セキュリティ > *キー管理サーバー*を選択します。

   [Key management server]ページに次の情報が表示されます。

   - [Configuration details]タブには、設定済みのキー管理サーバが表示されます。
   - [Encrypted nodes]タブには、ノード暗号化が有効になっているノードが表示されます。

2. 特定のKMSの詳細を表示し、そのKMSに対して操作を実行するには、KMSの名前を選択します。KMSの詳細ページには、次の情報が表示されます。

フィールド	製品説明
のキーを管理します	KMS に関連付けられている StorageGRID サイト。 このフィールドには、特定の StorageGRID サイトの名前、または別の KMS （デフォルト KMS ）で管理されていないサイト * が表示されます
ホスト名	KMS の完全修飾ドメイン名または IP アドレス。 2 台のキー管理サーバからなるクラスタがある場合は、両方のサーバの完全修飾ドメイン名または IP アドレスが表示されます。クラスタに複数のキー管理サーバがある場合は、最初の KMS の完全修飾ドメイン名または IP アドレスと、クラスタ内の追加のキー管理サーバの数が表示されます。 例 `10.10.10.10 and 10.10.10.11`：または `10.10.10.10 and 2 others`。 クラスタ内のすべてのホスト名を表示するには、KMSを選択して*または[アクション]>[編集]*を選択します。

3. KMSの詳細ページでタブを選択すると、次の情報が表示されます。

タブ	フィールド	製品説明
主な詳細	キー名	KMS 内の StorageGRID クライアントのキーエイリアス。
キー UID	キーの最新バージョンの一意の識別子。	最終更新日
キーの最新バージョンの日付と時刻。	サーバ証明書	メタデータ
証明書のメタデータ（シリアル番号、有効期限の日時、証明書PEMなど）。	証明書PEM	証明書のPEM（Privacy Enhanced Mail）ファイルの内容。
クライアント証明書	メタデータ	証明書のメタデータ（シリアル番号、有効期限の日時、証明書PEMなど）。

4. 組織のセキュリティ対策で必要に応じて、*[Rotate key]*を選択するか、KMSソフトウェアを使用してキーの新しいバージョンを作成します。

   キーのローテーションが成功すると、[Key UID]フィールドと[Last modified]フィールドが更新されます。

KMSソフトウェアを使用して暗号化キーをローテーションする場合は、最後に使用したバージョンのキーから新しいバージョンの同じキーにローテーションします。完全に別のキーに回転しないでください。

KMS のキー名 (エイリアス) を変更して、キーの回転を試みないでください。StorageGRID では、以前に使用されていたすべてのキーバージョン（および今後使用するすべてのバージョン）に、同じキーエイリアスを使用して KMS からアクセスできることが必要です。設定されている KMS のキーエイリアスを変更すると、 StorageGRID がデータを復号化できなくなる可能性があります。

証明書の管理

サーバ証明書またはクライアント証明書の問題に迅速に対処します。可能であれば、有効期限が切れる前に証明書を交換してください。

データアクセスを維持するために、証明書の問題はできるだけ早く対処する必要があります。

手順

1. 構成 > セキュリティ > *キー管理サーバー*を選択します。
2. 表で、KMSごとの証明書有効期限の値を確認します。
3. 任意のKMSの証明書の有効期限が不明な場合は、30分ほど待ってからWebブラウザを更新してください。
4. [証明書の有効期限]列に証明書の有効期限が切れているか有効期限に近づいていることが示されている場合は、KMSを選択してKMSの詳細ページに移動します。
   a. [サーバ証明書]*を選択し、[有効期限]フィールドの値を確認します。
   b. 証明書を置き換えるには、*[証明書の編集]*を選択して新しい証明書をアップロードします。
   c. これらのサブステップを繰り返し、サーバー証明書ではなく*クライアント証明書*を選択します。
5. 「* kms CA certificate expiration 」、「 kms client certificate expiration 」、「 kms server certificate expiration *」の各アラートがトリガーされたら、各アラートの概要 をメモして推奨される対処方法を実行します。

   証明書の有効期限の更新がStorageGRIDで取得されるまでに30分ほどかかることがあります。現在の値を確認するには、Webブラウザをリフレッシュしてください。

「* Server certificate status is unknown *」というステータスが表示される場合は、クライアント証明書を必要とせずに、KMSでサーバ証明書の取得が許可されていることを確認してください。

暗号化されたノードを表示する

StorageGRID システムでノード暗号化 * 設定が有効になっているアプライアンスノードに関する情報を表示できます。

手順

1. 構成 > セキュリティ > *キー管理サーバー*を選択します。

   [Key Management Server] ページが表示されます。Configuration Details タブには、設定済みのすべての

キー管理サーバが表示されます。

2. ページの上部で、*[暗号化されたノード]*タブを選択します。

   [Encrypted nodes]タブには、*[Node Encryption]*設定が有効になっているStorageGRID システム内のアプライアンスノードが表示されます。

3. 各アプライアンスノードについて、表の情報を確認します。

列	製品説明
ノード名	アプライアンスノードの名前。
ノードタイプ	ノードのタイプ。 Storage 、 Admin 、または Gateway 。
サイト	ノードがインストールされている StorageGRID サイトの名前。
KMS名	ノードに使用される KMS の説明的な名前。 KMSがリストされていない場合は、[Configuration details]タブを選択してKMSを追加します。 "キー管理サーバ（ KMS ）を追加する"
キー UID	アプライアンスノードでデータの暗号化と復号化に使用する暗号化キーの一意の ID 。キーUID全体を表示するには、テキストを選択します。 ダッシュ（ - - ）は、キー UID が不明であることを示します。アプライアンスノードと KMS 間の接続問題 が原因である可能性があります。
ステータス	KMS とアプライアンスノード間の接続のステータス。ノードが接続されている場合は、タイムスタンプが 30 分ごとに更新されます。KMS の設定変更後に接続ステータスが更新されるまで数分かかることがあります。 *注：*新しい値を表示するには、Webブラウザを更新してください。

4. ステータス列に KMS 問題 と表示されている場合は、問題 にすぐに対処してください。

   通常の KMS 操作中、ステータスは * KMS * に接続されます。ノードがグリッドから切断されると、ノードの接続状態が（意図的に停止しているか不明である）と表示されます。

   その他のステータスメッセージは、同じ名前の StorageGRID アラートに対応します。

   - KMS の設定をロードできませんでした
   - KMS 接続エラー
   - KMS 暗号化キー名が見つかりません
   - KMS 暗号化キーのローテーションに失敗しました
   - KMS キーでアプライアンスボリュームを復号化できませんでした

◦ KMS は設定されていません

これらのアラートに対して推奨される対処方法を実行します。

問題が発生した場合は、データを完全に保護するために、すぐに対処する必要があります。

KMSの編集

証明書の有効期限が近づいている場合など、キー管理サーバの設定の編集が必要になることがあります。

開始する前に

- KMS用に選択したサイトを更新する場合は、を確認しておき"サイトの KMS を変更する際の考慮事項"ます。
- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"rootアクセス権限"。

手順

1. 構成 > セキュリティ > *キー管理サーバー*を選択します。

   [Key management server]ページが表示され、設定済みのすべてのキー管理サーバが表示されます。

2. 編集するKMSを選択し、**[**アクション**]**>*[編集]*を選択します。

   テーブルでKMS名を選択し、KMS詳細ページで*編集*を選択して、KMSを編集することもできます。

3. 必要に応じて、キー管理サーバの編集ウィザードの*ステップ1（KMSの詳細）*で詳細を更新します。

フィールド	製品説明
KMS名	この KMS を特定するのに役立つわかりやすい名前。1~64 文字で指定する必要があります。
キー名	KMS 内の StorageGRID クライアントの正確なキーエイリアス。1~255 文字で指定する必要があります。 キー名の編集が必要になることはほとんどありません。たとえば、エイリアスの名前が KMS で変更された場合や、以前のキーのすべてのバージョンが新しいエイリアスのバージョン履歴にコピーされている場合は、キー名を編集する必要があります。
のキーを管理します	サイト固有のKMSを編集していて、まだデフォルトKMSを持っていない場合は、オプションで*[別のKMSで管理されていないサイト(デフォルトKMS)]*を選択します。このオプションを選択すると、サイト固有のKMSがデフォルトのKMSに変換されます。これは、専用のKMSを持たないすべてのサイトと、拡張で追加されたすべてのサイトに適用されます。 *注:*サイト固有のKMSを編集している場合、別のサイトを選択することはできません。デフォルトのKMSを編集している場合、特定のサイトを選択することはできません。

フィールド	製品説明
ポート	KMS サーバが Key Management Interoperability Protocol （ KMIP ）の通信に使用するポート。デフォルトでは、 KMIP 標準ポートである 5696 が使用されます。
ホスト名	KMS の完全修飾ドメイン名または IP アドレス。 *注：*サーバ証明書のSubject Alternative Name（SAN）フィールドには、ここに入力するFQDNまたはIPアドレスが含まれている必要があります。そうしないと、 StorageGRID は KMS クラスタ内のすべてのサーバに接続できなくなります。

4. KMSクラスタを構成する場合は、*[別のホスト名を追加]*を選択して、クラスタ内の各サーバのホスト名を追加します。
5. 「 * Continue * 」を選択します。

   [キー管理サーバの編集]ウィザードの手順2（サーバ証明書のアップロード）が表示されます。

6. サーバー証明書を置き換える必要がある場合は、 * 参照 * を選択して新しいファイルをアップロードします。
7. 「 * Continue * 」を選択します。

   [Edit a Key Management Server]ウィザードの手順3（クライアント証明書のアップロード）が表示されます。

8. クライアント証明書とクライアント証明書の秘密鍵を置き換える必要がある場合は、 * 参照 * を選択して新しいファイルをアップロードします。
9. [テストして保存]*を選択します。

   キー管理サーバと影響を受けるサイトのすべてのノード暗号化アプライアンスノードの間の接続をテストします。すべてのノード接続が有効で、 KMS に正しいキーがある場合は、キー管理サーバが Key Management Server ページの表に追加されます。

10. エラーメッセージが表示された場合は、メッセージの詳細を確認し、「 * OK * 」を選択します。

    たとえば、この KMS 用に選択したサイトが別の KMS によってすでに管理されている場合や、接続テストに失敗した場合は、「 422 ： Unprocessable Entity 」というエラーが表示されます。

11. 接続エラーを解決する前に現在の設定を保存する必要がある場合は、*[強制保存]*を選択します。

    [Force save]*を選択すると、KMSの構成が保存されますが、各アプライアンスからそのKMSへの外部接続はテストされません。構成を含む問題 がある場合、該当するサイトでノード暗号化が有効になっているアプライアンスノードをリブートできない可能性があります。問題が解決するまでデータにアクセスできなくなる可能性があります。

    KMS の設定が保存されます。

12. 確認の警告を確認し、設定を強制的に保存する場合は、「 * OK 」を選択します。

KMS構成は保存されますが、KMSへの接続はテストされません。

キー管理サーバ（ **KMS** ）を削除する

場合によっては、キー管理サーバの削除が必要になることがあります。たとえば、サイトの運用を停止した場合は、サイト固有の KMS を削除できます。

開始する前に

- を確認しておきます"キー管理サーバを使用する際の考慮事項と要件"。
- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"rootアクセス権限"。

タスクの内容

KMS は以下の場合に削除できます。

- サイトの運用が停止された場合や、ノードの暗号化が有効なアプライアンスノードがサイトに含まれていない場合は、サイト固有の KMS を削除できます。
- ノード暗号化が有効なアプライアンスノードがあるサイトごとにサイト固有の KMS がすでに存在する場合は、デフォルトの KMS を削除できます。

手順

1. 構成 > セキュリティ > *キー管理サーバー*を選択します。

   [Key management server]ページが表示され、設定済みのすべてのキー管理サーバが表示されます。

2. 削除するKMSを選択し、**[**アクション**]**>*[削除]*を選択します。

   テーブルでKMS名を選択し、KMS詳細ページで* Remove *を選択して、KMSを削除することもできます。

3. 次の条件に該当することを確認します。
   - アプライアンスノードでノード暗号化が有効になっていないサイトのサイト固有のKMSを削除する場合。
   - デフォルトのKMSを削除しようとしていますが、ノード暗号化を使用して各サイトにサイト固有のKMSがすでに存在しています。
4. 「 * はい * 」を選択します。

   KMS の設定は削除されます。

プロキシ設定を管理します

StorageGRID ストレージ プロキシを設定する

プラットフォームサービスまたはクラウドストレージプールを使用している場合は、ストレージノードと外部の S3 エンドポイントの間に非透過型プロキシを設定できます。たとえば、インターネット上のエンドポイントなどの外部エンドポイントへプラットフォームサービスメッセージを送信する場合などには、非透過型プロキシが必要です。

設定されているストレージプロキシ設定は、Kafkaプラットフォームサービスエンドポイントには適用されません。

開始する前に

- そうだな "特定のアクセス権限"
- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。

タスクの内容

設定できるストレージプロキシは1つです。

手順

1. 構成 > セキュリティ > *プロキシ設定*を選択します。
2. タブで、[ストレージプロキシを有効にする]*チェックボックスをオンにします。
3. ストレージプロキシのプロトコルを選択します。
4. プロキシサーバのホスト名または IP アドレスを入力します。
5. 必要に応じて、プロキシサーバへの接続に使用するポートを入力します。

   プロトコルのデフォルトポート（HTTPの場合は80、SOCKS5の場合は1080）を使用する場合は、このフィールドを空白のままにします。

6. [保存（ Save ）] を選択します。

   ストレージプロキシが保存されたら、プラットフォームサービスまたはクラウドストレージプールの新しいエンドポイントを設定およびテストできます。

   プロキシの変更が有効になるまでに最大 10 分かかることがあります。

7. プロキシサーバの設定をチェックして、 StorageGRID からのプラットフォームサービス関連メッセージがブロックされないようにします。
8. ストレージプロキシを無効にする必要がある場合は、チェックボックスをオフにして*[保存]*を選択します。

関連情報

"外部との通信に使用するポート"

StorageGRIDで管理プロキシ設定を構成する

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

AutoSupportの詳細については、"AutoSupportの設定"を参照してください。

開始する前に

- そうだな "特定のアクセス権限"
- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。

タスクの内容

単一の管理プロキシの設定を行うことができます。

手順

1. 構成 > セキュリティ > *プロキシ設定*を選択します。

   [Proxy Settings]ページが表示されます。デフォルトでは、タブメニューで[Storage]が選択されています。

2. [Admin]*タブを選択します。
3. [Enable Admin Proxy]*チェックボックスをオンにします。
4. プロキシサーバのホスト名または IP アドレスを入力します。
5. プロキシサーバへの接続に使用するポートを入力します。
6. 必要に応じて、プロキシサーバのユーザ名とパスワードを入力します。

   プロキシサーバでユーザ名またはパスワードが不要な場合は、これらのフィールドを空白のままにします。

7. 次のいずれかを選択します。

   ◦ 管理プロキシへの接続を保護する場合は、*[プロキシ証明書の確認]*を選択します。管理プロキシサーバから提示されたSSL証明書の信頼性を確認するには、CAバンドルをアップロードしてください。

   > プロキシ証明書が検証されている場合、StorageGRID On Demand、Eシリーズ AutoSupport Through StorageGRID、およびAutoSupportの[Upgrade]ページでの更新パスの決定が機能しません。

   CAバンドルをアップロードすると、そのメタデータが表示されます。

   ◦ 管理プロキシサーバとの通信時に証明書を検証しない場合は、*[プロキシ証明書を検証しない]*を選択します。

8. [保存（ Save ）] を選択します。

   管理プロキシが保存されると、管理ノードとテクニカルサポートの間にプロキシサーバが設定されます。

   > プロキシの変更が有効になるまでに最大 10 分かかることがあります。

9. 管理プロキシを無効にする必要がある場合は、**[**管理プロキシを有効にする**]***チェックボックスをオフにして、[保存]*を選択します。

ファイアウォールを制御します

外部ファイアウォールで**StorageGRID**アクセスを制御する

外部ファイアウォールで特定のポートを開いたり閉じたりできます。

StorageGRID 管理ノード上のユーザインターフェイスと API へのアクセスは、外部ファイアウォールで特定のポートを開くか、または閉じることで制御できます。たとえば、システムアクセスを制御する他の方法に加えて、ファイアウォールでテナントが Grid Manager に接続できないようにすることができます。

StorageGRID内部ファイアウォールを設定する場合は、を参照してください"内部ファイアウォールを設定します"。

ポート	製品説明	ポートが開いている場合
443	管理ノードのデフォルトの HTTPS ポート	Web ブラウザと管理 API クライアントは、 Grid Manager 、 Grid 管理 API 、 Tenant Manager 、およびテナント管理 API にアクセスできます。 • 注： * ポート 443 は一部の内部トラフィックにも使用されます。
8443	管理ノード上の制限された Grid Manager ポート	• Web ブラウザと管理 API クライアントは、 HTTPS を使用して Grid Manager とグリッド管理 API にアクセスできます。 • Webブラウザおよび管理APIクライアントは、Tenant Managerまたはテナント管理APIにアクセスできません。 • 内部コンテンツに対する要求は拒否されます。
9443	管理ノード上の制限された Tenant Manager ポート	• Web ブラウザと管理 API クライアントは HTTPS を使用して Tenant Manager とテナント管理 API にアクセスできます。 • Webブラウザおよび管理APIクライアントは、Grid Managerまたはグリッド管理APIにアクセスできません。 • 内部コンテンツに対する要求は拒否されます。

シングルサインオン（ SSO ）は、制限された Grid Manager ポートまたは Tenant Manager ポートでは使用できません。ユーザをシングルサインオンで認証する場合は、デフォルトの HTTPS ポート（ 443 ）を使用する必要があります。

関連情報

- "Grid Manager にサインインします"
- "テナントアカウントを作成する"
- "外部との通信"

StorageGRIDで内部ファイアウォール制御を管理する

StorageGRID には、各ノードに内部ファイアウォールがあります。このファイアウォールを使用すると、ノードへのネットワークアクセスを制御できるため、グリッドのセキュリティが強化されます。ファイアウォールを使用して、特定のグリッド環境に必要なポートを除くすべてのポートでネットワークアクセスを禁止します。[Firewall]コントロールページで行った設定変更は、各ノードに展開されます。

Firewallコントロールページの3つのタブを使用して、グリッドに必要なアクセスをカスタマイズします。

- 特権アドレスリスト：このタブを使用して、選択したポートへのアクセスを許可します。[Manage external access]タブを使用して閉じたポートにアクセスできるIPアドレスまたはサブネットをCIDR表記で追加できます。
- 外部アクセスの管理：このタブを使用して、デフォルトで開いているポートを閉じるか、以前閉じていたポートを再度開きます。
- 信頼されていないクライアントネットワーク：このタブを使用して、ノードがクライアントネットワークからのインバウンドトラフィックを信頼するかどうかを指定します。

  このタブの設定は、[外部アクセスの管理]タブの設定よりも優先されます。

  - 信頼されていないクライアントネットワークを使用するノードは、そのノードに設定されているロードバランサエンドポイントポート（グローバル、ノードインターフェイス、およびノードタイプにバインドされたエンドポイント）の接続のみを受け入れます。
  - ロードバランサエンドポイントのポート_は、[外部ネットワークの管理]タブの設定に関係なく、信頼されていないクライアントネットワークで唯一開いているポート_です。
  - 信頼されている場合は、[Manage external access]タブで開いたすべてのポートおよびクライアントネットワークで開いているロードバランサエンドポイントにアクセスできます。

> あるタブで行った設定は、別のタブで行ったアクセス変更に影響を与える可能性があります。すべてのタブの設定を確認して、ネットワークが想定どおりに動作することを確認してください。

内部ファイアウォールコントロールを設定するには、を参照してください"ファイアウォールコントロールを設定します"。

外部ファイアウォールとネットワークセキュリティの詳細については、を参照してください"外部ファイアウォールでアクセスを制御します"。

[Privileged address list]タブと**[Manage external access]**タブ

特権アドレスリストタブでは、閉じられているグリッドポートへのアクセスを許可する1つ以上のIPアドレスを登録できます。[Manage external access]タブでは、選択した外部ポートまたは開いているすべての外部ポート（デフォルトではグリッド以外のノードからアクセス可能なポート）への外部アクセスを閉じることができます。多くの場合、この2つのタブを一緒に使用して、グリッドに必要な正確なネットワークアクセスをカスタマイズできます。

> 特権IPアドレスには、デフォルトで内部グリッドポートへのアクセスはありません。

例**1:**メンテナンスタスクにジャンプホストを使用します

ネットワーク管理にジャンプホスト（セキュリティ強化ホスト）を使用するとします。次の一般的な手順を使用できます。

1. 特権アドレスリストタブを使用して、ジャンプホストのIPアドレスを追加します。
2. [Manage external access]タブを使用して、すべてのポートをブロックします。

> ポート443と8443をブロックする前に、特権IPアドレスを追加してください。ブロックされたポートに現在接続されているユーザ（ユーザを含む）は、自分のIPアドレスが特権アドレスリストに追加されていないかぎり、Grid Managerにアクセスできません。

設定を保存すると、グリッド内の管理ノードのすべての外部ポートが、ジャンプホストを除くすべてのホストに対してブロックされます。これにより、ジャンプホストを使用して、グリッドでより安全にメンテナンスタスクを実行できるようになります。

例**2**：敏感なポートをロックダウンします

機密ポートとそのポート上のサービスをロックダウンするとします。次の一般的な手順を使用できます。

1. サービスへのアクセスを必要とするホストにのみアクセスを許可するには、特権アドレスリストタブを使用します。
2. [Manage external access]タブを使用して、すべてのポートをブロックします。

> Grid ManagerおよびTenant Managerへのアクセスを割り当てられているポート（事前設定ポートは443および8443）へのアクセスをブロックする前に、権限付きIPアドレスを追加してください。ブロックされたポートに現在接続されているユーザ（ユーザを含む）は、自分のIPアドレスが特権アドレスリストに追加されていないかぎり、Grid Managerにアクセスできません。

設定を保存すると、機密ポートとそのポート上のサービスが特権アドレス リスト上のホストで使用できるようになります。他のすべてのホストは、リクエストがどのインターフェースから送信されたかに関係なく、サービスへのアクセスを拒否されます。

例**3**：未使用のサービスへのアクセスを無効にします

ネットワークレベルでは、使用する予定のない一部のサービスを無効にすることができます。たとえば、HTTP S3クライアントトラフィックをブロックするには、[Manage external access]タブのトグルを使用してポート18084をブロックします。

[信頼されていないクライアントネットワーク**]**タブ

クライアントネットワークを使用している場合は、明示的に設定されたエンドポイントでのみインバウンドクライアントトラフィックを受け入れることで、悪意のある攻撃から StorageGRID を保護できます。

デフォルトでは、各グリッドノードのクライアントネットワークは *trusted_* です。つまり、StorageGRIDはデフォルトで、すべてののグリッドノードへのインバウンド接続を信頼します"使用可能な外部ポート"。

各ノードのクライアントネットワークを「 *untrusted_* 」に指定することで、 StorageGRID システムに対する悪意ある攻撃の脅威を軽減できます。ノードのクライアントネットワークが信頼されていない場合、ノードはロードバランサエンドポイントとして明示的に設定されたポートのインバウンド接続だけを受け入れます。およびを参照してください"ロードバランサエンドポイントを設定する""ファイアウォールコントロールを設定します"。

例 **1** ：ゲートウェイノードが **HTTPS S3** 要求のみを受け入れる

ゲートウェイノードで、 HTTPS S3 要求を除くクライアントネットワーク上のすべてのインバウンドトラフィックを拒否するとします。この場合、次の一般的な手順を実行します。

1. "ロードバランサエンドポイント"ページで、ポート443にHTTPS経由のS3用のロードバランサエンドポイントを設定します。
2. [Firewall control]ページで、[Untrusted]を選択して、ゲートウェイノードのクライアントネットワークを信頼されていないネットワークとして指定します。

設定を保存すると、ポート 443 での HTTPS S3 要求と ICMP エコー（ ping ）要求を除き、ゲートウェイノードのクライアントネットワーク上のすべてのインバウンドトラフィックが破棄されます。

例 **2** ：ストレージノードが **S3** プラットフォームサービス要求を送信する

あるストレージノードからのアウトバウンドS3プラットフォームサービストラフィックは有効にするが、クライアントネットワークではそのストレージノードへのインバウンド接続は禁止するとします。この場合は、次の手順を実行します。

- [Firewall]制御ページの[Untrusted Client Networks]タブで、ストレージノード上のクライアントネットワークが信頼されていないことを指定します。

設定を保存すると、ストレージノードはクライアントネットワークで受信トラフィックを受け入れなくなりますが、設定されているプラットフォームサービスのデスティネーションへのアウトバウンド要求は引き続き許可します。

例**3**：**Grid Manager**へのアクセスをサブネットに制限する

Grid Managerに特定のサブネットに対するアクセスのみを許可するとします。次の手順を実行します。

1. 管理ノードのクライアントネットワークをサブネットに接続します。
2. [Untrusted Client Network]タブを使用して、クライアントネットワークを信頼されていないものとして設定します。
3. 管理インターフェイスのロードバランサエンドポイントを作成する場合は、「port」と入力し、ポートからアクセスする管理インターフェイスを選択します。
4. 信頼されていないクライアントネットワークについては*[はい]*を選択します。
5. [Manage external access]タブを使用して、すべての外部ポートをブロックします（サブネット外のホストに対して特権IPアドレスが設定されているかどうかに関係なく）。

設定を保存すると、指定したサブネットのホストだけがGrid Managerにアクセスできるようになります。他のすべてのホストはブロックされます。

StorageGRID 内部ファイアウォールを設定する

StorageGRID ノードの特定のポートへのネットワークアクセスを制御するようにStorageGRID ファイアウォールを設定できます。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- そうだな "特定のアクセス権限"
- との情報を確認しておき"ファイアウォールコントロールを管理します""ネットワークのガイドライン"ます。
- 管理ノードまたはゲートウェイノードが明示的に設定されたエンドポイントでのみインバウンドトラフィックを受け入れるように設定する場合は、ロードバランサエンドポイントを定義しておきます。

> クライアントネットワークの設定を変更する際、ロードバランサエンドポイントが設定されていないと、既存のクライアント接続が失敗することがあります。

タスクの内容

StorageGRID には、各ノードに内部ファイアウォールがあります。このファイアウォールを使用して、グリッドのノードの一部のポートを開いたり閉じたりできます。[Firewall]制御タブを使用して、グリッドネットワーク、管理ネットワーク、およびクライアントネットワークでデフォルトで開いているポートを開いたり閉じたりできます。閉じているグリッドポートにアクセスできる特権IPアドレスのリストを作成することもできます。クライアントネットワークを使用している場合は、ノードがクライアントネットワークからのインバウンドトラフィックを信頼するかどうかを指定できます。また、クライアントネットワークの特定のポートへのアクセスを設定できます。

グリッドの外部のIPアドレスに対して開くポートの数を絶対に必要なポートだけに制限すると、グリッドのセキュリティが強化されます。3つのファイアウォールコントロールタブのそれぞれの設定を使用して、必要なポートだけが開いていることを確認します。

ファイアウォール制御の使用方法に関する詳細情報（例を含む）については、"ファイアウォールコントロールを管理します"を参照してください。

外部ファイアウォールとネットワークセキュリティの詳細については、"外部ファイアウォールでアクセスを制御します"を参照してください。

ファイアウォールコントロールにアクセスします

手順

1. 構成 > セキュリティ > *ファイアウォール制御*を選択します。

   このページの3つのタブについては、を"ファイアウォールコントロールを管理します"参照してください。

2. 任意のタブを選択して、ファイアウォールコントロールを設定します。

   これらのタブは任意の順序で使用できます。1つのタブで設定した設定では、他のタブで実行できる操作は制限されません。ただし、1つのタブで設定を変更すると、他のタブで設定されたポートの動作が変更される可能性があります。

特権アドレスリスト

特権アドレスリストタブを使用して、デフォルトで閉じられているポート、または外部アクセスの管理タブの設定によって閉じられているポートへのアクセスをホストに許可します。

権限付きIPアドレスとサブネットには、デフォルトで内部のグリッドアクセスはありません。また、[Manage external access]タブでブロックされていても、ロードバランサエンドポイントと、[Privileged address list]タブで開いている追加のポートにアクセスできます。

> 「特権アドレス一覧」タブの設定は、「信頼されていないクライアントネットワーク」タブの設定を上書きできます。

手順

1. 特権アドレスリストタブで、閉じたポートへのアクセスを許可するアドレスまたはIPサブネットを入力します。
2. 必要に応じて、*別のIPアドレスまたはCIDR表記のサブネットを追加*を選択して、追加の特権クライアントを追加できます。

特権リストにできるだけ少ないアドレスを追加します。

3. 必要に応じて、*特権IPアドレスによる StorageGRID 内部ポートへのアクセスを許可する*を選択します。"StorageGRID の内部ポート"を参照してください。

このオプションを使用すると、内部サービスの保護が一部解除されます。可能であれば無効のままにしておきます。

4. [保存（ Save ）] を選択します。

外部アクセスの管理

[Manage external access]タブでポートを閉じると、特権アドレスリストにIPアドレスを追加しないかぎり、グリッド以外のIPアドレスからポートにアクセスすることはできません。閉じることができるのは、デフォルトで開いているポートだけです。また、閉じたポートのみを開くことができます。

[外部アクセスの管理]タブの設定は、[信頼されていないクライアントネットワーク]タブの設定を上書きすることはできません。たとえば、ノードが信頼されていない場合、クライアントネットワークでポートSSH/22が[外部アクセスの管理]タブで開いていてもブロックされます。[Untrusted Client Network]タブの設定は、クライアントネットワークの閉じているポート（443、8443、9443など）よりも優先されます。

手順

1. [外部アクセスの管理]*を選択します。タブには、グリッド内のノードのすべての外部ポート（デフォルトではグリッド以外のノードからアクセス可能なポート）が表示されます。
2. 次のオプションを使用して、開いたり閉じたりするポートを設定します。
   - 各ポートの横にあるトグルを使用して、選択したポートを開いたり閉じたりします。
   - 表にリストされているすべてのポートを開くには、*表示されているすべてのポートを開く*を選択します。
   - 表に示されているすべてのポートを閉じるには、*[表示されているすべてのポートを閉じる]*を選択します。

Grid Manager のポート 443 または 8443 を閉じると、お客様を含め、現在ブロックされたポートに接続しているすべてのユーザーは、特権アドレスリストに IP アドレスが追加されていない限り、Grid Manager へのアクセス権を失います。

テーブルの右側にあるスクロールバーを使用して、使用可能なすべてのポートが表示されていることを確認します。検索フィールドを使用して、ポート番号を入力して外部ポートの設定を検索します。ポート番号の一部を入力できます。たとえば、*2*と入力すると、名前に文字列「2」が含まれるすべてのポートが表示されます。

3. [保存（ Save ）] を選択します

Untrusted Client Networkの略

ノードのクライアントネットワークが信頼されていない場合、ノードはロードバランサエンドポイントとして設定されたポート、およびオプションでこのタブで選択した追加のポートでのみインバウンドトラフィックを

受け入れます。このタブを使用して、拡張時に追加する新しいノードのデフォルト設定を指定することもできます。

ロードバランサエンドポイントが設定されていないと、既存のクライアント接続が失敗する可能性があります。

タブで設定を変更すると、[外部アクセスの管理]*タブの設定が上書きされます。

手順

1. [信頼されていないクライアントネットワーク]*を選択します。
2. [Set New Node Default]セクションで、拡張手順 で新しいノードをグリッドに追加する際のデフォルト設定を指定します。
   - * Trusted *（デフォルト）：拡張でノードを追加すると、そのクライアントネットワークが信頼されます。
   - * Untrusted * ：拡張でノードが追加されるときに、そのクライアントネットワークは信頼されません。

     必要に応じて、このタブに戻って特定の新しいノードの設定を変更できます。

     この設定は、 StorageGRID システム内の既存のノードには影響しません。
3. 次のオプションを使用して、明示的に設定されたロードバランサエンドポイントまたは選択した追加のポートでのみクライアント接続を許可するノードを選択します。
   - テーブルに表示されたすべてのノードを信頼されていないクライアントネットワークのリストに追加するには、*[表示されたノードで信頼されていないクライアントネットワーク]*を選択します。
   - テーブルに表示されたすべてのノードを信頼されていないクライアントネットワークのリストから削除するには、*[表示されたノードで信頼する]*を選択します。
   - 各ノードの横にある切り替えボタンを使用して、選択したノードのクライアントネットワークを[Trusted]または[Untrusted]に設定します。

     たとえば、*表示されているノードで[Untrust on displayed nodes]*を選択してすべてのノードを[Untrusted Client Network]リストに追加し、個 々 のノードの横にある切り替えを使用してその1つのノードを[Trusted Client Network]リストに追加できます。

     テーブルの右側にあるスクロールバーを使用して、使用可能なすべてのノードが表示されていることを確認します。検索フィールドにノード名を入力して、任意のノードの設定を検索します。名前の一部を入力できます。たとえば、「* gw *」と入力すると、名前に文字列「gw」を含むすべてのノードが表示されます。
4. [保存（ Save ）] を選択します。

   新しいファイアウォール設定は即座に適用され、有効になります。ロードバランサーのエンドポイントが設定されていない場合、既存のクライアント接続が失敗する可能性があります。

テナントを管理します

StorageGRID のテナントアカウント

テナントアカウントを使用すると、Simple Storage Service（S3）REST APIを使用して、StorageGRIDシステム内のオブジェクトの格納と読み出しを行うことができます。

このバージョンのドキュメントサイトからSwiftの詳細が削除されました。を参照してください "StorageGRID 11.8：テナントの管理"

グリッド管理者は、S3クライアントがオブジェクトの格納と読み出しに使用するテナントアカウントを作成および管理します。

各テナントアカウントには、フェデレーテッドグループまたはローカルグループ、ユーザ、S3バケット、オブジェクトがあります。

テナントアカウントを使用すると、格納されているオブジェクトをエンティティごとに分離できます。たとえば、次のようなユースケースでは複数のテナントアカウントを使用できます。

- * エンタープライズのユースケース：エンタープライズアプリケーションで StorageGRID システムを管理する場合は、組織内の部門ごとにグリッドのオブジェクトストレージを分離する必要があります。この場合は、マーケティング部門、カスタマーサポート部門、人事部門などのテナントアカウントを作成できます。

  S3 クライアント プロトコルを使用する場合は、S3 バケットとバケット ポリシーを使用して、企業内の部門間でオブジェクトを分離できます。テナント アカウントを使用する必要はありません。実装手順を参照"S3バケットとバケットポリシー"詳細についてはこちらをご覧ください。

- * サービスプロバイダのユースケース：サービスプロバイダとして StorageGRID システムを管理する場合は、グリッド上のストレージをリースするエンティティごとにグリッドのオブジェクトストレージを分離できます。この場合は、 A 社、 B 社、 C 社などのテナントアカウントを作成します。

詳細については、を参照してください "テナントアカウントを使用する"。

テナントアカウントを作成するにはどうすればよいですか？

Grid Managerを使用してテナントアカウントを作成する。テナントアカウントを作成する際には次の情報を指定します。

- テナント名、クライアントタイプ（S3）、オプションのストレージクォータなどの基本情報。
- テナントアカウントに対する権限（テナントアカウントがS3プラットフォームサービスを使用できるか、独自のアイデンティティソースを設定できるか、S3 Selectを使用できるか、グリッドフェデレーション接続を使用できるかなど）。
- テナントの初期ルートアクセス（StorageGRID システムがローカルグループとユーザ、アイデンティティフェデレーション、シングルサインオン（SSO）のいずれを使用しているかに基づく）。

また、S3テナントアカウントが規制要件に準拠する必要がある場合は、StorageGRID システムでS3オブジェクトロック設定を有効にすることができます。S3 オブジェクトのロックを有効にすると、すべての S3 テナントアカウントで準拠バケットを作成、管理できます。

Tenant Managerの用途

テナントアカウントを作成したら、テナントユーザはTenant Managerにサインインして次のタスクを実行できます。

- アイデンティティフェデレーションを設定する（グリッドとアイデンティティソースを共有する場合を除く）
- グループとユーザを管理します
- アカウント同期とグリッド間レプリケーションにはグリッドフェデレーションを使用します
- S3 アクセスキーを管理します
- S3バケットを作成、管理します
- S3プラットフォームサービスを使用する
- S3 Select を使用する
- ストレージの使用状況を監視

S3テナントユーザはTenant Managerを使用してS3アクセスキーとバケットを作成、管理できますが、オブジェクトを取り込み、管理するにはS3クライアントアプリケーションを使用する必要があります。詳細は、を参照してください "S3 REST APIを使用する" 。

StorageGRID テナント アカウントを作成します

StorageGRID システム内のストレージへのアクセスを制御するために、少なくとも 1 つのテナントアカウントを作成する必要があります。

テナントアカウントを作成する手順は、"アイデンティティフェデレーション"そして"シングルサインオン"が構成されているかどうか、およびテナント アカウントの作成に使用する Grid Manager アカウントが、ルートアクセス権限を持つ管理者グループに属しているかどうかを確認します。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"rootアクセスまたはテナントアカウントの権限"。
- Grid Manager 用に設定されているアイデンティティソースをテナントアカウントで使用し、テナントアカウントにフェデレーテッドグループへの root アクセス権限を付与する場合は、そのフェデレーテッドグループを Grid Manager にインポートしておく必要があります。この管理者グループにGrid Manager権限を割り当てる必要はありません。を参照して "管理者グループを管理する"
- S3テナントがグリッドフェデレーション接続を使用してアカウントデータを同期し、バケットオブジェクトを別のグリッドに複製できるようにする場合：
  - そうだな "グリッドフェデレーション接続を設定しました"
  - 接続のステータスは*接続済み*です。
  - Root Access 権限が割り当てられている。
  - の考慮事項を確認しておき"グリッドフェデレーションに許可されたテナントの管理"ます。
  - テナントアカウントがGrid Manager用に設定されたアイデンティティソースを使用する場合は、両方のグリッドのGrid Managerに同じフェデレーテッドグループをインポートしておく必要があります。

テナントを作成するときに、このグループを選択して、ソースとデスティネーションの両方のテナントアカウントに対する初期のRootアクセス権限を割り当てます。

テナントを作成する前にこの管理者グループが両方のグリッドに存在していない場合、テナントはデスティネーションにレプリケートされません。

ウィザードにアクセスします

手順

1. *テナント*を選択します。
2. 「 * Create * 」を選択します。

詳細を入力します

手順

1. テナントの詳細を入力します。

フィールド	製品説明
名前	テナントアカウントの名前。テナント名は一意である必要はありません。作成されたテナントアカウントには、20桁の一意のアカウントIDが割り当てられます。
概要 （オプション）	テナントの特定に役立つ概要 。 グリッドフェデレーション接続を使用するテナントを作成する場合は、必要に応じて、このフィールドを使用してソーステナントとデスティネーションテナントを特定します。たとえば、Grid 1に作成されたテナントの概要は、Grid 2にレプリケートされたテナントの「This tenant was created on Grid 1」にも表示されます。
クライアントタイプ	は* S3 *にする必要があります。
ストレージクォータ（オプション）	このテナントにストレージクォータを設定する場合は、クォータとユニットの数値。

2. 「 * Continue * 」を選択します。

権限を選択

手順

1. 必要に応じて、このテナントに付与する基本的な権限を選択します。

これらの権限の一部には追加の要件があります。詳細については、各権限のヘルプアイコンを選択してください。

権限	選択した項目
プラットフォームサービスを許可します	テナントでは、CloudMirrorなどのS3プラットフォームサービスを使用できます。を参照して "S3 テナントアカウントのプラットフォームサービスを管理します"
独自のアイデンティティソースを使用する	テナントは、フェデレーション グループおよびユーザーに対して独自の ID ソースを構成および管理できます。このオプションは、"SSOを設定しました" StorageGRIDシステム用。
S3を許可するを選択します	テナントは、オブジェクトデータのフィルタリングと読み出しを行うためのS3 SelectObjectContent API要求を問題 できます。を参照して "テナントアカウント用の S3 Select を管理します" 重要：SelectObjectContent要求を実行すると、すべてのS3クライアントとすべてのテナントのロードバランサのパフォーマンスが低下する可能性があります。この機能は、必要な場合にのみ有効にし、信頼できるテナントに対してのみ有効にします。

2. 必要に応じて、このテナントに付与する詳細な権限を選択します。

権限	選択した項目
グリッドフェデレーション接続	テナントは、以下の機能を持つグリッドフェデレーション接続を利用できます。 • このテナントアカウント、およびすべてのテナントグループ、ユーザー、S3アクセスキーが、このグリッドと選択された接続内の他のグリッド間で同期されます。 セキュリティまたはコンプライアンス上の理由で必要な場合は、*アクセスキーの同期を有効にする*の選択を解除できます。 • このテナントで、各グリッド上の対応するバケット間のグリッド間レプリケーションを設定できます。 を参照して "グリッドフェデレーションに許可されたテナントを管理します"
S3 オブジェクトのロック	テナントでS3オブジェクトロックの特定の機能を使用できるようにします。 • *最大保持期間を設定*このバケットに追加された新しいオブジェクトを、取り込まれた時点から保持する期間を定義します。 • *コンプライアンスモードを許可*ユーザーが保持期間中に保護オブジェクトバージョンを上書きまたは削除できないようにします。

3. 「 * Continue * 」を選択します。

手順

1. StorageGRID システムで使用するアイデンティティフェデレーション、シングルサインオン（SSO）、またはその両方に基づいて、テナントアカウントのルートアクセスを定義します。

オプション	手順
アイデンティティフェデレーションが有効になっていない場合	ローカルrootユーザとしてテナントにサインインするときに使用するパスワードを指定します。
アイデンティティフェデレーションが有効になっている場合	a. テナントに対するRoot Access権限を割り当てる既存のフェデレーテッドグループを選択します。 b. 必要に応じて、ローカルrootユーザとしてテナントにサインインする際に使用するパスワードを指定します。
アイデンティティフェデレーションとシングルサインオン（SSO）の両方が有効になっている場合	テナントに対するRoot Access権限を割り当てる既存のフェデレーテッドグループを選択します。ローカルユーザはサインインできません。

2. [テナントの作成] を選択します。

   成功を示すメッセージが表示され、[Tenants]ページに新しいテナントが表示されます。テナントの詳細を表示してテナントアクティビティを監視する方法については、を参照してください"テナントのアクティビティを監視する"。

   テナント設定をグリッド全体に適用する場合、ネットワーク接続、ノードのステータス、およびCassandraの処理によっては、15分以上かかることがあります。

3. テナントに対して「グリッドフェデレーション接続を使用する」権限を選択した場合は、接続先の他のグリッドに同一のテナントが複製されていることを確認してください。両方のグリッド上のテナントは、同じ20桁のアカウントID、名前、説明、割り当て量、および権限を持ちます。

   テナントアカウントがこのグリッドで作成されたが他のグリッドと同期されていないことを示すエラーメッセージが表示された場合は、"グリッドフェデレーションエラーをトラブルシューティングする"の手順を参照してください。

テナントへのサインイン（オプション）

必要に応じて、新しいテナントにサインインして設定を完了するか、あとでテナントにサインインできます。のサインイン手順は、Grid Managerにサインインする際にデフォルトのポート（443）を使用するか制限されたポートを使用するかによって異なります。を参照して "外部ファイアウォールでアクセスを制御します"

今すぐサインインしてください

使用する機能	操作
ポート443にアクセスし、ローカルrootユーザのパスワードを設定します	1. [ルートとしてサインイン]*を選択します。 サインインすると、バケット、アイデンティティフェデレーション、グループ、およびユーザを設定するためのリンクが表示されます。 2. リンクを選択してテナントアカウントを設定します。 各リンクをクリックすると、 Tenant Manager の対応するページが開きます。このページを完了するには、を参照してください"テナントアカウントを使用するための手順"。
ポート443およびローカルrootユーザのパスワードを設定していない	[サインイン]*を選択し、ルートアクセスフェデレーテッドグループのユーザのクレデンシャルを入力します。
制限されたポート	1. [完了]*を選択します 2. このテナントアカウントへのアクセスの詳細を確認するには、[Tenant]テーブルで*[Restricted]*を選択します。 Tenant Manager の URL の形式は次のとおりです。 `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/` ◦ `FQDN_or_Admin_Node_IP`は、管理ノードの完全修飾ドメイン名またはIPアドレスです。 ◦ `port`はテナント専用ポートです。 ◦ `20-digit-account-id`は、テナントの一意のアカウントIDです。

後でサインインします

使用する機能	次のいずれかを実行 ...
ポート443	• グリッド マネージャーから [テナント] を選択し、テナント名の右側にある [**Sign in**] を選択します。 • Web ブラウザにテナントの URL を入力します。 `https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/` ◦ `FQDN_or_Admin_Node_IP`は、管理ノードの完全修飾ドメイン名またはIPアドレスです。 ◦ `20-digit-account-id`は、テナントの一意のアカウントIDです。

使用する機能	次のいずれかを実行 ...
制限されたポート	• グリッド マネージャーから、[テナント] を選択し、[制限] を選択します。 • Web ブラウザにテナントの URL を入力します。 `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id` ◦ `FQDN_or_Admin_Node_IP`は、管理ノードの完全修飾ドメイン名またはIPアドレスです。 ◦ `port`は、テナント専用の制限付きポートです。 ◦ `20-digit-account-id`は、テナントの一意のアカウントIDです。

テナントを設定します

"テナントアカウントを使用する"の手順に従って、テナントグループとユーザー、S3アクセスキー、バケット、プラットフォームサービス、アカウント同期、およびクロスグリッドレプリケーションを管理します。

StorageGRID テナント アカウントを編集する

テナントアカウントを編集して、表示名、ストレージクォータ、またはテナント権限を変更できます。

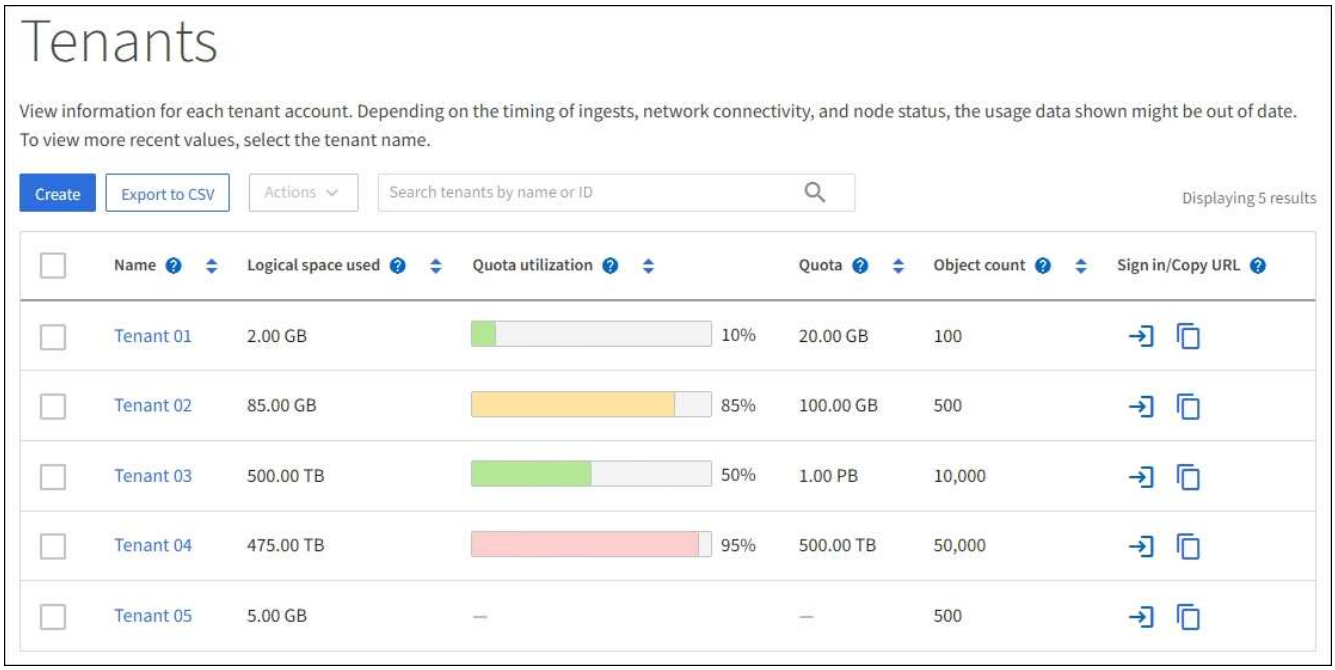
開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"rootアクセスまたはテナントアカウントの権限"。

> テナント設定をグリッド全体に適用する場合、ネットワーク接続、ノードのステータス、およびCassandraの処理によっては、15分以上かかることがあります。

手順

1. *テナント*を選択します。



2. 編集するテナントアカウントを探します。

   検索ボックスを使用して、名前またはテナントIDでテナントを検索します。

3. テナントを選択します。次のいずれかを実行できます。
   - テナントのチェックボックスを選択し、**[操作]**>*[編集]*を選択します。
   - 詳細ページを表示するテナント名を選択し、*[編集]*を選択します。
4. 必要に応じて、次のフィールドの値を変更します。
   - * 名前 *
   - * 概要 *
   - * ストレージクォータ *
5. 「 * Continue * 」を選択します。
6. テナントアカウントの権限を選択または選択解除します。
   - すでに使用しているテナントに対して * Platform services * を無効にすると、テナントが S3 バケット用に設定しているサービスが停止します。エラーメッセージはテナントに送信されません。たとえば、テナントで S3 バケットに CloudMirror レプリケーションが設定されている場合は、引き続きバケットにオブジェクトを格納できますが、エンドポイントとして設定された外部の S3 バケットにはこれらのオブジェクトのコピーが作成されなくなります。を参照して "S3 テナントアカウントのプラットフォームサービスを管理します"
   - [Use own identity source]*の設定を変更して、テナントアカウントで独自のアイデンティティソースを使用するか、Grid Manager用に設定されたアイデンティティソースを使用するかを指定します。

     *独自のアイデンティティソースを使用*が次の場合：

     - [Disabled]（選択）を選択した場合、テナントで独自のアイデンティティソースがすでに有効になっています。Grid Manager 用に設定されたアイデンティティソースを使用するには、テナント側で独自のアイデンティティソースを無効にする必要があります。

- [Disabled]で選択されていない場合、StorageGRID システムでSSOが有効になっています。テナントは、 Grid Manager 用に設定されたアイデンティティソースを使用する必要があります。

- 必要に応じて、[Allow S3 Select]*権限を選択または選択解除します。を参照して "テナントアカウント用の S3 Select を管理します"
- Use grid federation connection *権限を削除するには、次の手順を実行します。
  i. テナント詳細ページで「グリッド連携」タブを選択します。
  ii. 削除する接続を選択してください。
  iii. [Remove Permission]*を選択します。
- [Use grid federation connection]権限を追加するには、次の手順を実行します。
  i. [グリッドフェデレーション]*タブを選択します。
  ii. [グリッドフェデレーション接続を使用する]*チェックボックスをオンにします。
  iii. 必要に応じて、*[既存のローカルユーザとローカルグループをクローニングする]*を選択してリモートグリッドにクローニングします。必要に応じて、実行中のクローニングを停止したり、前回のクローニング処理の完了後に一部のローカルユーザまたはローカルグループのクローニングに失敗した場合にクローニングを再試行したりできます。

  セキュリティまたはコンプライアンス上の理由で必要な場合は、*アクセスキーの同期を有効にする*の選択を解除できます。

- 最大保持期間を設定するか準拠モードを許可するには、次の手順を実行します。

  これらの設定を使用するには、グリッドでS3オブジェクトロックを有効にする必要があります。

  i. [S3 Object Lock]*タブを選択します。
  ii. [Set maximum retention period]*に値を入力し、プルダウンから期間を選択します。
  iii. [準拠モードを許可する]*で、チェックボックスをオンにします。

StorageGRIDテナントのローカルルートユーザーのパスワードを変更する

テナントのローカル root ユーザがアカウントからロックアウトされた場合は、 root ユーザのパスワード変更が必要になることがあります。

開始する前に

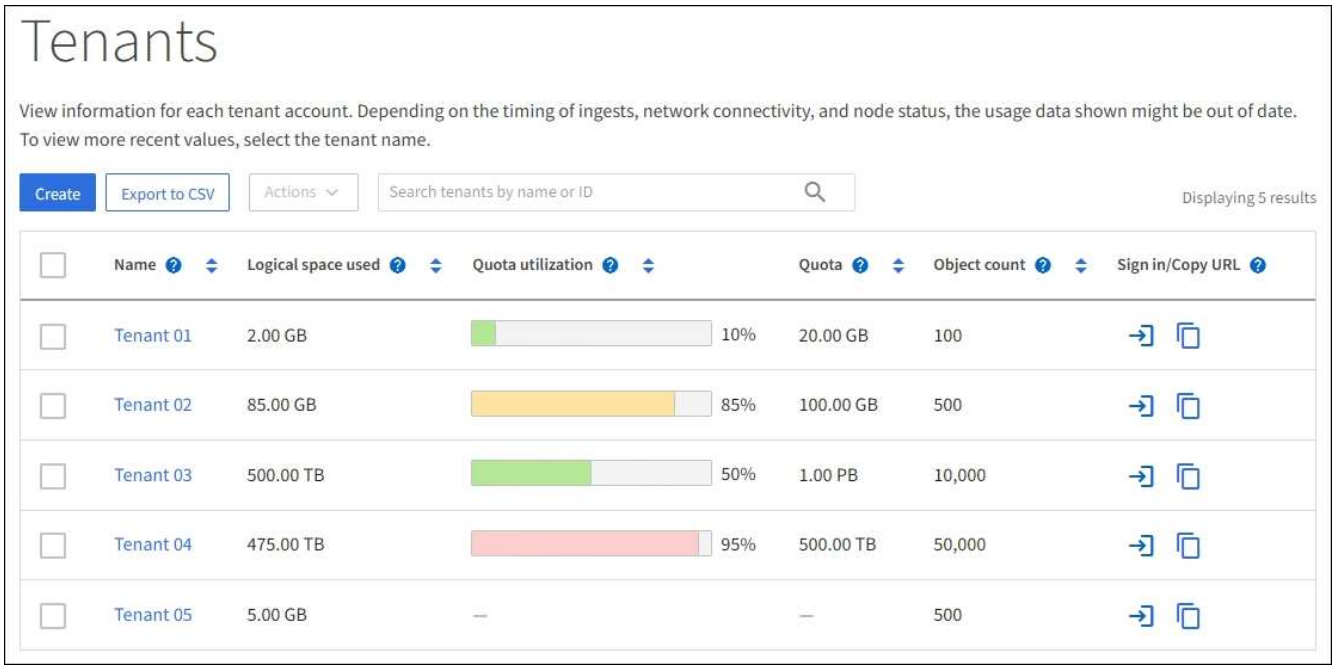
- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- そうだな "特定のアクセス権限"

タスクの内容

StorageGRID システムでシングルサインオン（SSO）が有効になっている場合、ローカルrootユーザはテナントアカウントにサインインできません。root ユーザのタスクを実行するには、テナントの Root Access 権限を持つフェデレーテッドグループにユーザが属している必要があります。

手順

1. *テナント*を選択します。



2. テナントアカウントを選択します。次のいずれかを実行できます。
   - テナントのチェックボックスを選択し、**[操作]>*[rootパスワードの変更]***を選択します。
   - テナントの名前を選択して詳細ページを表示し、**[操作]>*[ルートパスワードの変更]***を選択します。
3. テナントアカウントの新しいパスワードを入力します。
4. [保存（ Save ）] を選択します。

StorageGRID テナント アカウントを削除する

システムに対するテナントのアクセス権を完全に削除する場合は、テナントアカウントを削除します。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- そうだな "特定のアクセス権限"
- テナントアカウントに関連付けられているS3バケットとオブジェクトをすべて削除しておきます。
- テナントがグリッドフェデレーション接続の使用を許可されている場合、"Use grid federation connection 権限が割り当てられたテナントを削除する"に関する考慮事項を確認してください。削除は同期されるため、いずれかのグリッドでテナントが削除されると、選択されたすべてのグリッドで削除されます。

手順

1. *テナント*を選択します。
2. 削除するテナントアカウントを探します。

   検索ボックスを使用して、名前またはテナントIDでテナントを検索します。

3. 複数のテナントを削除するには、チェックボックスをオンにして**>[削除]***を選択します。
4. 単一のテナントを削除するには、次のいずれかを実行します。

- チェックボックスを選択し、[アクション]>*[削除]*を選択します。
- テナント名を選択して詳細ページを表示し、[操作]>*[削除]*を選択します。

5. 「 * はい * 」を選択します。

プラットフォームサービスを管理します

StorageGRID プラットフォーム サービスについて学ぶ

プラットフォームサービスには、 CloudMirror レプリケーション、イベント通知、および検索統合サービスがあります。

S3 テナントアカウントでプラットフォームサービスを有効にする場合は、テナントがそのサービスの使用に必要な外部リソースにアクセスできるようにグリッドを設定する必要があります。

プラットフォームサービスはサポートされていません"ブランチバケット"。

CloudMirror レプリケーション

StorageGRID CloudMirrorレプリケーションサービスは、StorageGRIDバケットから指定された外部のデスティネーションに特定のオブジェクトをミラーリングするために使用します。

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

CloudMirrorレプリケーションには、クロスグリッドレプリケーション機能と重要な類似点と相違点がいくつかあります。詳細については、を参照してください"グリッド間レプリケーションとCloudMirrorレプリケーションを比較してください"。

通知

バケットごとのイベント通知は、オブジェクトに対して実行された特定のアクションに関する通知を、指定された外部 Kafka クラスター、Webhook エンドポイント、または Amazon Simple Notification Service に送信するために使用されます。

たとえば、バケットに追加された各オブジェクトについてアラートが管理者に送信されるように設定できます。この場合、オブジェクトは重大なシステムイベントに関連付けられているログファイルです。

> S3 オブジェクトのロックが有効になっているバケットでイベント通知を設定することはできますが、オブジェクトの S3 オブジェクトロックメタデータ（ Retain Until Date および Legal Hold のステータスを含む）は通知メッセージに含まれません。

検索統合サービス

検索統合サービスは、外部サービスを使用してメタデータを検索または分析できるように、指定されたElasticsearchインデックスにS3オブジェクトメタデータを送信するために使用されます。

たとえば、リモートの Elasticsearch サービスに S3 オブジェクトメタデータを送信するようにバケットを設定できます。次に、 Elasticsearch を使用してバケット間で検索を実行し、オブジェクトメタデータのパターンに対して高度な分析を実行できます。

S3 オブジェクトロックが有効なバケットでは Elasticsearch 統合を設定できますが、オブジェクトの S3 オブジェクトロックメタデータ（ Retain Until Date および Legal Hold のステータスを含む）は通知メッセージに含まれません。

プラットフォームサービスを使用すると、テナントで、外部ストレージリソース、通知サービス、データの検索または分析サービスを利用できるようになります。通常、プラットフォームサービスのターゲットは StorageGRID 環境の外部にあるため、テナントにこれらのサービスの使用を許可するかどうかを決める必要があります。この方法を使用する場合は、テナントアカウントを作成または編集するときにプラットフォームサービスの使用を有効にする必要があります。テナントで生成されたプラットフォームサービスのメッセージが宛先に届くようにネットワークを設定する必要もあります。

プラットフォームサービスの使用に関する推奨事項

プラットフォームサービスを使用する前に、次の推奨事項を確認してください。

- StorageGRID システムの S3 バケットで、バージョン管理と CloudMirror レプリケーションの両方が有効になっている場合は、デスティネーションエンドポイントでも S3 バケットのバージョン管理を有効にします。これにより、 CloudMirror レプリケーションでエンドポイントに同様のオブジェクトバージョンを生成できます。
- CloudMirror のレプリケーション、通知、検索統合を必要とする S3 要求ではアクティブなテナントが 100 個を超えないようにします。アクティブなテナントが 100 を超えると、 S3 クライアントのパフォーマンスが低下する可能性があります。
- 完了できないエンドポイントへの要求は、最大50万件の要求にキューイングされます。この制限はアクティブなテナント間で均等に共有されます。新規テナントは、新規に作成されたテナントに不当なペナルティが課されないように、一時的にこの50万を超えることができます。

関連情報

- "プラットフォームサービスを管理します"
- "ストレージプロキシを設定します"
- "StorageGRID を監視します"

StorageGRID プラットフォーム サービスのネットワークとポート

S3 テナントにプラットフォームサービスの使用を許可する場合は、プラットフォームサービスのメッセージがデスティネーションに配信されるようにグリッドのネットワークを設定する必要があります。

テナントアカウントを作成または更新する際に、 S3 テナントアカウントのプラットフォームサービスを有効にできます。プラットフォームサービスが有効になっている場合、テナントは、その S3 バケットからの CloudMirror レプリケーション、イベント通知、または検索統合のメッセージのデスティネーションとして機能するエンドポイントを作成できます。これらのプラットフォームサービスメッセージは、 ADC サービスを実行しているストレージノードからデスティネーションエンドポイントに送信されます。

たとえば、テナントは次のタイプのデスティネーションエンドポイントを設定できます。

- ローカルでホストされる Elasticsearch クラスタ
- Amazon Simple Notification Serviceメッセージの受信をサポートするローカルアプリケーション
- ローカルでホストされるKafkaクラスタ

- HTTP POST 通知リクエストをサポートする外部またはローカルでホストされる Webhook エンドポイント。

  このエンドポイントは、さまざまな Web サーバー、フレームワーク、または Fluentd などのデータ処理ツールでホストできます。

- StorageGRID の同じインスタンス上または別のインスタンス上の、ローカルにホストされる S3 バケット
- Amazon Web Services 上のエンドポイントなどの外部エンドポイント。

プラットフォームサービスメッセージが確実に配信されるように、 ADC ストレージノードが含まれるネットワークを設定する必要があります。デスティネーションエンドポイントへのプラットフォームサービスメッセージの送信に、次のポートを使用できることを確認する必要があります。

デフォルトでは、プラットフォームサービスメッセージは次のポートで送信されます。

- **80**: httpで始まるエンドポイントURIの場合(ほとんどのエンドポイント)
- * 443 *：httpsで始まるエンドポイントURI（ほとんどのエンドポイント）
- *9092 *：httpまたはhttpsで始まるエンドポイントURIの場合（Kafkaエンドポイントのみ）

エンドポイントの作成や編集を行う際に、テナントで別のポートを指定できます。

> StorageGRID 環境が CloudMirror レプリケーションのデスティネーションとして使用されている場合は、ポート 80 または 443 以外のポートにレプリケーションメッセージが送信される可能性があります。デスティネーション StorageGRID 環境で S3 に使用されているポートがエンドポイントで指定されていることを確認してください。

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

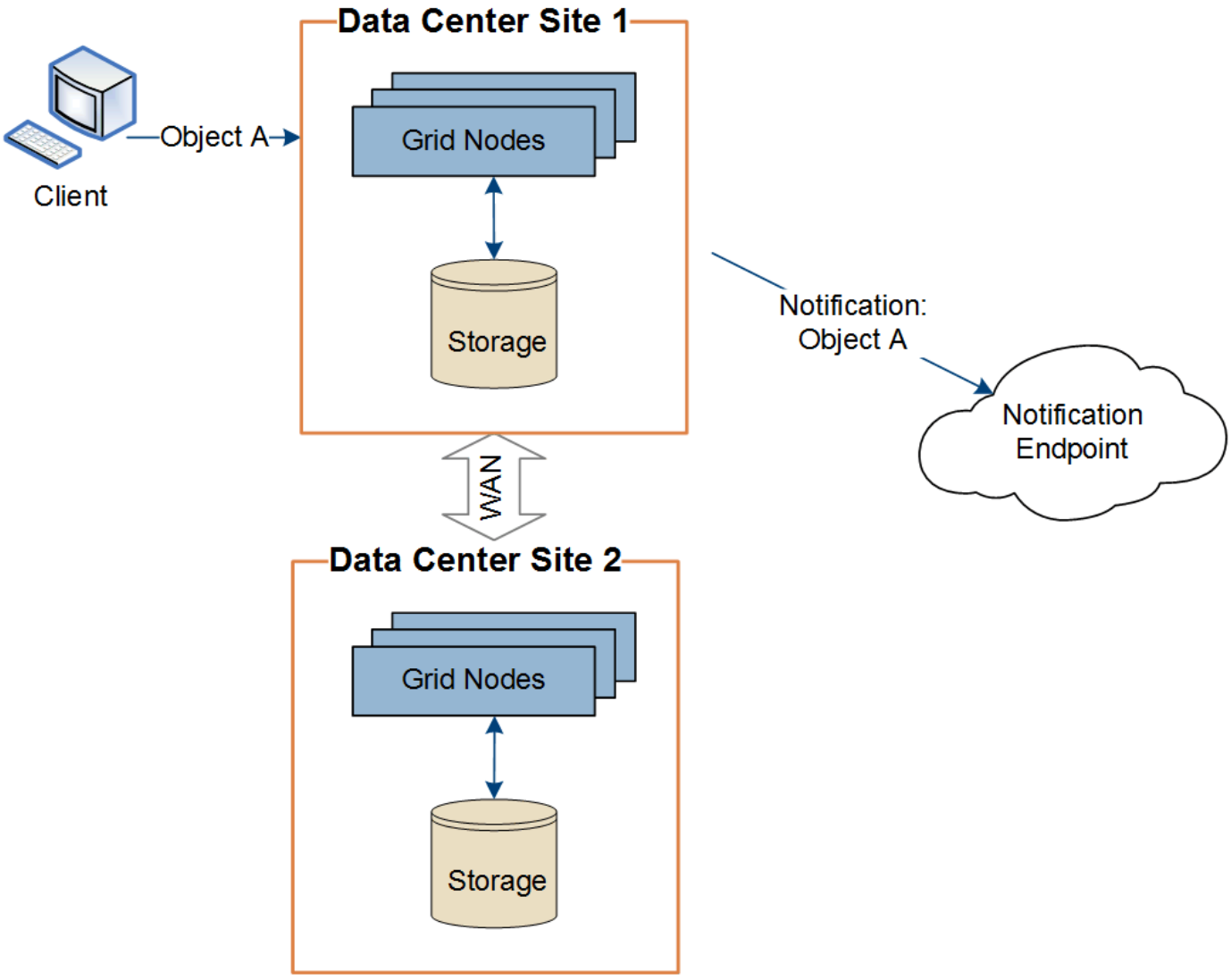
関連情報

- "テナントアカウントを使用する"
- "外部との通信に使用するポート"

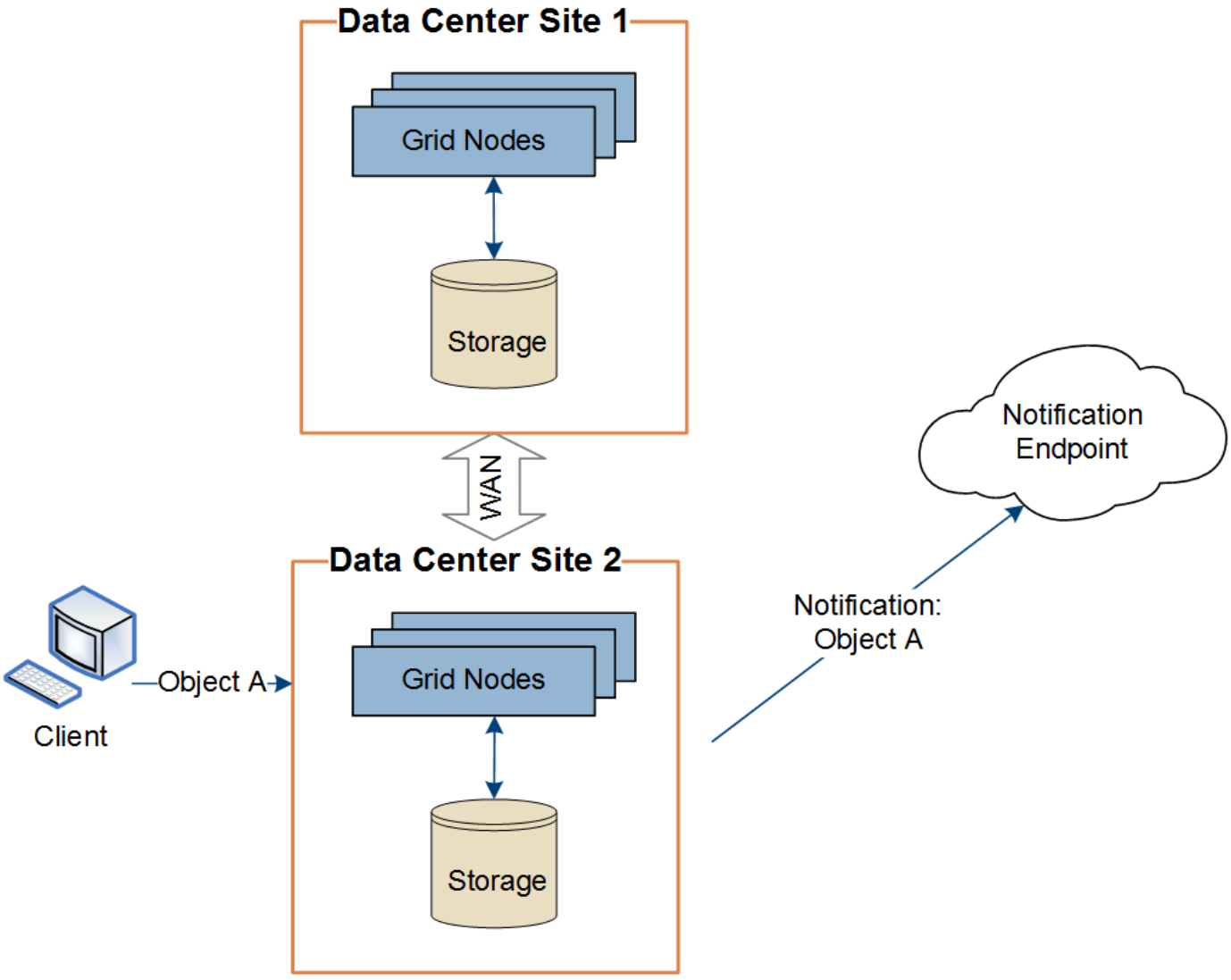
サイトごとの **StorageGRID** プラットフォーム サービス メッセージの配信

プラットフォームサービスの処理はすべてサイト単位で実行されます。

つまり、テナントがクライアントを使用してデータセンターサイト 1 のゲートウェイノードに接続し、オブジェクトに対して S3 API の Create 処理を実行すると、その処理に関する通知はデータセンターサイト 1 からトリガーされて送信されます。



クライアントが続けてデータセンターサイト 2 から同じオブジェクトに対して S3 API の Delete 処理を実行すると、その処理に関する通知はデータセンターサイト 2 からトリガーされて送信されます。



プラットフォームサービスメッセージを宛先に配信できるように、各サイトのネットワークが設定されていることを確認します。

StorageGRID プラットフォーム サービスのトラブルシューティング

プラットフォームサービスで使用されるエンドポイントは、テナントユーザーがテナントマネージャーで作成および管理します。ただし、テナントがプラットフォームサービスの設定や使用に関して問題を抱えている場合は、グリッドマネージャーを使用して問題を解決できる可能性があります。

新しいエンドポイントに関する問題

テナントでプラットフォームサービスを使用するには、 Tenant Manager を使用してエンドポイントを 1 つ以上作成する必要があります。各エンドポイントは、1つのプラットフォームサービスの外部のデスティネーション（StorageGRID S3バケット、Amazon Web Servicesバケット、Amazon Simple Notification Serviceトピック、Kafkaトピック、ローカルまたはAWSでホストされるElasticsearchクラスタなど）です。各エンドポイントには、外部リソースの場所と、そのリソースへのアクセスに必要なクレデンシャルが含まれます。

テナントでエンドポイントを作成すると、 StorageGRID システムによって、そのエンドポイントが存在するかどうかと、指定されたクレデンシャルでアクセスできるかどうかが検証されます。エンドポイントへの接続

は、各サイトの 1 つのノードから検証されます。

エンドポイントの検証が失敗した場合は、その理由を記載したエラーメッセージが表示されます。テナントユーザは、問題 を解決してから、エンドポイントの作成をもう一度実行する必要があります。

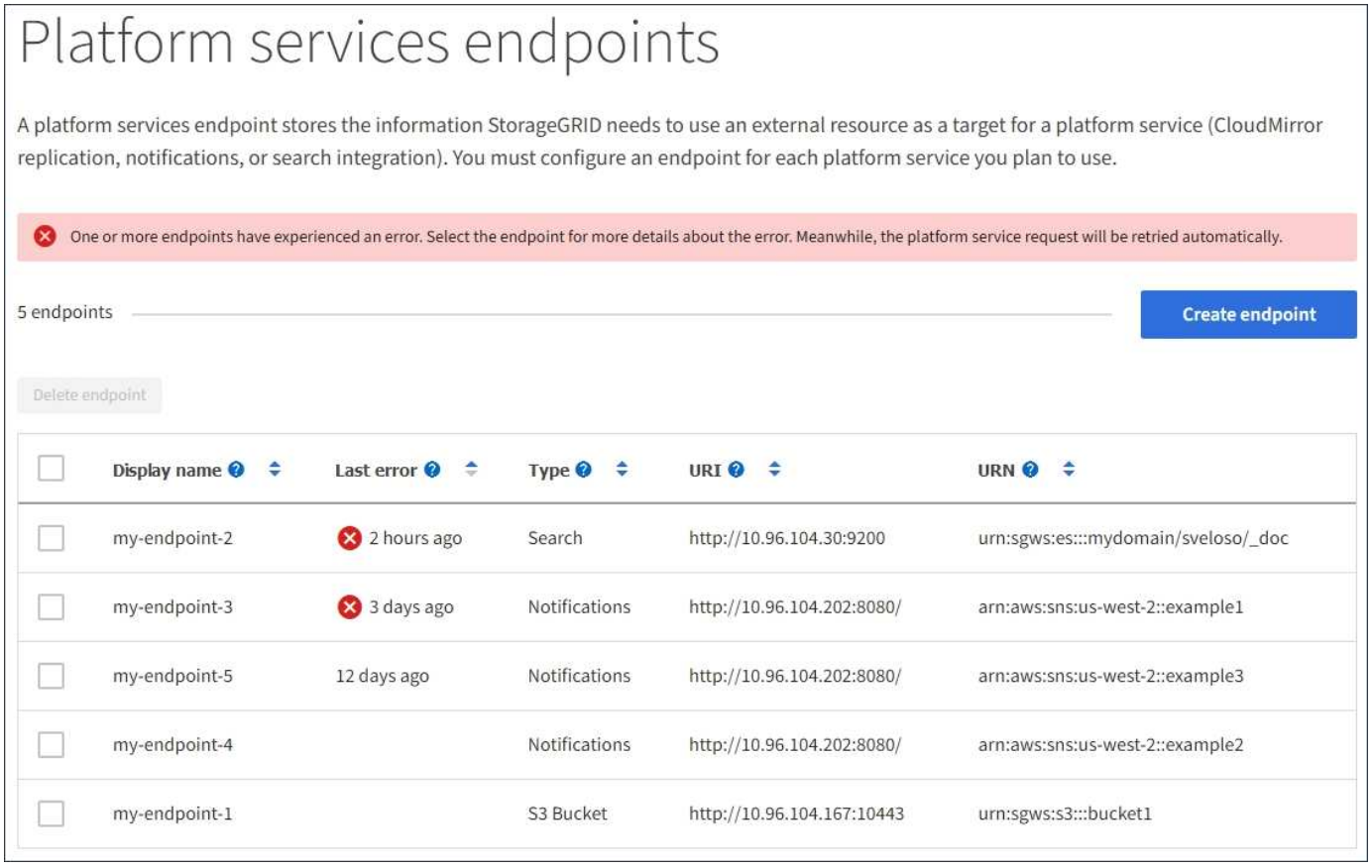
テナントアカウントでプラットフォームサービスが有効になっていないと、エンドポイントの作成が失敗します。

既存のエンドポイントに関する問題

StorageGRID が既存のエンドポイントにアクセスしようとしたときにエラーが発生すると、テナントマネージャのダッシュボードにメッセージが表示されます。

One or more endpoints have experienced an error and might not be functioning properly. Go to the Endpoints page to view the error details. The last error occurred 2 hours ago.

テナントユーザーは、エンドポイントページにアクセスして、各エンドポイントの最新のエラーメッセージを確認し、エラーが発生した日時を特定できます。「最終エラー」列には、各エンドポイントの最新のエラーメッセージが表示され、エラーが発生した日時が示されます。アイコンが表示されているエラーは、過去7日以内に発生したものです。



「 * Last error * 」列の一部のエラーメッセージには、かっこ内にログ ID が含まれている場合があります。グリッド管理者やテクニカルサポートは、この ID を使用して、 bycast.log のエラーに関する詳細情報を確認できます。

プロキシサーバに関連する問題

設定した場合"ストレージプロキシ"ストレージノードとプラットフォーム サービス エンドポイント間で、プロキシ サービスがStorageGRIDからのメッセージを許可していない場合はエラーが発生する可能性があります。これらの問題を解決するには、プロキシ サーバーの設定を確認し、プラットフォーム サービス関連のメッセージがブロックされていないことを確認します。

エラーが発生したかどうかを確認します

過去7日以内にエンドポイントエラーが発生した場合は、Tenant Managerのダッシュボードにアラートメッセージが表示されます。エラーの詳細を確認するには、エンドポイントのページに移動します。

クライアント処理が失敗する

一部のプラットフォームサービスの問題により、 S3 バケットに対する原因 クライアント処理が失敗することがあります。たとえば、内部の Replicated State Machine （ RSM ）サービスが停止した場合や、配信のためにキューに登録されたプラットフォームサービスメッセージが多すぎる場合は、 S3 クライアント処理が失敗します。

サービスのステータスを確認するには、次の手順に従います。

1. ノード > ***site*** > ***Storage Node*** > 概要 を選択します。
2. アラート テーブルでアクティブなアラートを確認します。
3. アクティブなアラートを解決します。必要に応じて、テクニカル サポートにお問い合わせください。

リカバリ可能なエンドポイントエラーとリカバリ不能なエンドポイントエラー

エンドポイントの作成後に、さまざまな理由からプラットフォームサービス要求のエラーが発生することがあります。一部のエラーは、ユーザが対処することでリカバリできます。たとえば、リカバリ可能なエラーは次のような原因で発生する可能性があります。

- ユーザのクレデンシャルが削除されたか、期限切れになっています。
- 宛先バケットが存在しません。
- 通知を配信できません。

StorageGRID でリカバリ可能なエラーが発生した場合は、成功するまでプラットフォームサービス要求が再試行されます。

その他のエラーは回復できません。たとえば、回復不可能なエラーは次の理由で発生する可能性があります。

- エンドポイントが削除されます。
- ウェブフックエンドポイントの宛先は通知リクエストに応答し、 `400 Bad Request`エラー。

StorageGRIDでリカバリ不能なエンドポイントエラーが発生した場合は、次の手順を実行します。

- Grid Managerで、サポート>*ツール*>*メトリクス*>* Grafana *>*プラットフォームサービスの概要*に移動してエラーの詳細を確認します。
- Tenant Managerで、* storage（S3）> Platform Services Endpoints *の順に移動してエラーの詳細を確認します。

- に関連するエラーがないかを確認します `/var/local/log/bycast-err.log`。このログファイルは、ADCサービスがあるストレージノードに格納されます。

プラットフォームサービスメッセージを配信できません

宛先でプラットフォーム サービス メッセージを受け入れられない問題が発生した場合、バケットに対するクライアント操作は成功しますが、プラットフォーム サービス メッセージは配信されません。たとえば、宛先で資格情報が更新され、 StorageGRID が宛先サービスに対して認証できなくなった場合に、このエラーが発生する可能性があります。

関連するアラートを確認します。

プラットフォームサービス要求のパフォーマンスが低下します

要求が送信されるペースがデスティネーションエンドポイントで要求を受信できるペースを超えると、StorageGRID ソフトウェアはバケットの受信 S3 要求を調整する場合があります。スロットルは、デスティネーションエンドポイントへの送信を待機している要求のバックログが生じている場合にのみ発生します。

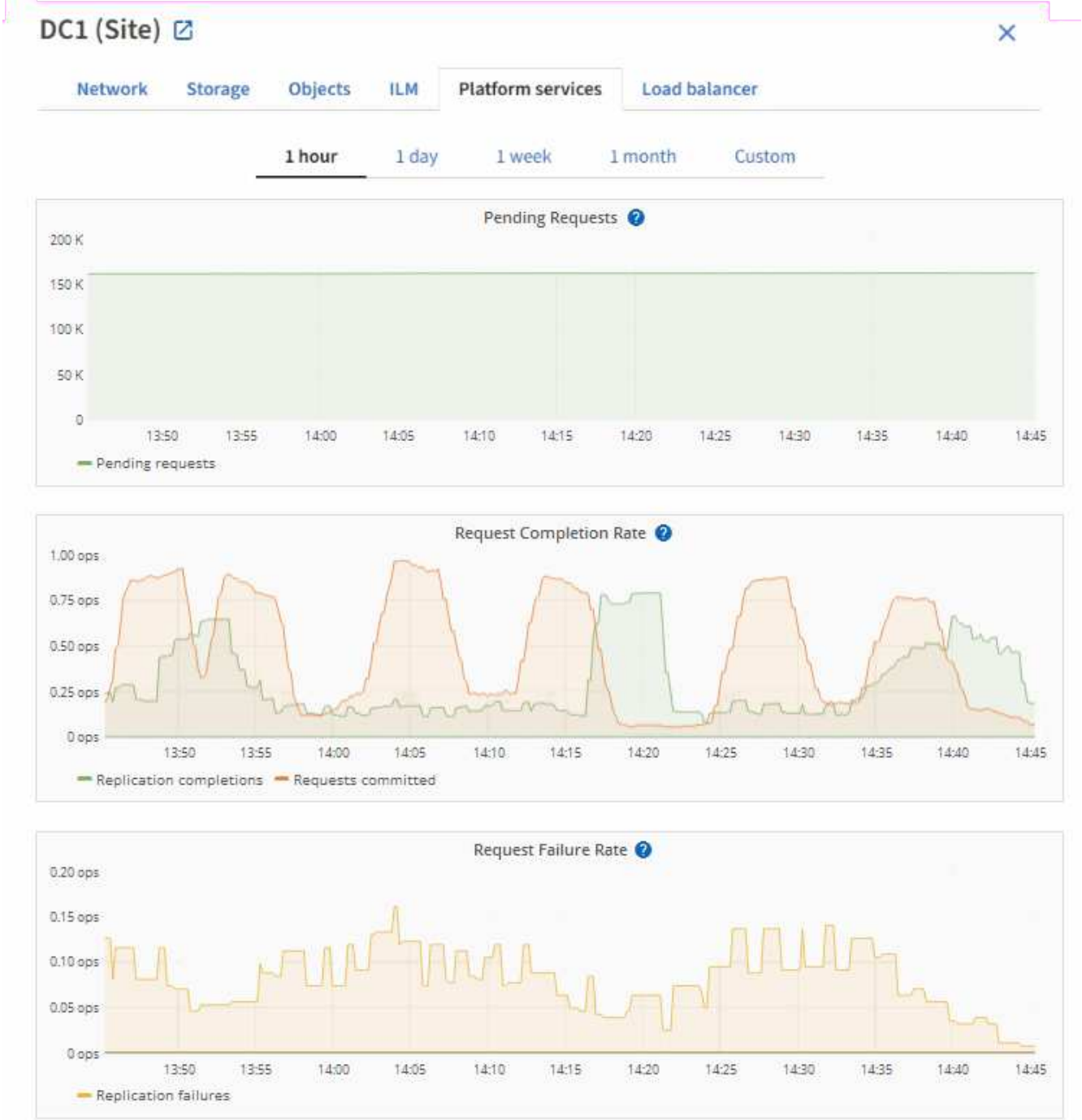
明らかな影響は、受信 S3 要求の実行時間が長くなることだけです。パフォーマンスが大幅に低下していることが検出されるようになった場合は、取り込み速度を下げるか、容量の大きいエンドポイントを使用する必要があります。要求のバックログが増え続けると、クライアント S3 処理（ PUT 要求など）が失敗します。

通常、 CloudMirror 要求には、検索統合やイベント通知の要求よりも多くのデータ転送が含まれるため、デスティネーションエンドポイントのパフォーマンスによる影響を受ける可能性が高くなります。

プラットフォームサービス要求が失敗しました

プラットフォームサービスの要求の失敗率を表示するには、次の手順を実行します。

1. *ノード*を選択します。
2. [**_site *>*Platform Services**] を選択します。
3. エラー率のリクエストチャートを表示します。



Platform services unavailable アラート

「 * Platform services unavailable * 」アラートは、実行中または使用可能な RSM サービスがあるストレージノードが少なすぎるために、サイトでプラットフォームサービスの処理を実行できないことを示しています。

RSM サービスは、プラットフォームサービス要求がそれぞれのエンドポイントに確実に送信されるようにします。

このアラートを解決するには、サイトのどのストレージノードに RSM サービスが含まれているかを特定します（RSMサービスは、ADCサービスを含むストレージノードにあります）。次に、それらのストレージノードの過半数が実行されていて使用可能であることを確認します。

RSM サービスを含む複数のストレージノードでサイトで障害が発生すると、そのサイトに対する保留中のプラットフォームサービス要求はすべて失われます。

プラットフォームサービスエンドポイントに関するその他のトラブルシューティングガイダンス

詳細については、を参照してください"テナントアカウントの使用>プラットフォームサービスエンドポイントのトラブルシューティング"。

関連情報

"StorageGRID システムのトラブルシューティングを行う"

StorageGRID でテナント アカウントの **S3 Select** を管理する

特定の S3 テナントが、個々のオブジェクトに対する S3 Select から問題 SelectObjectContent 要求を使用できるようにすることができます。

S3 Select を使用すると、データベースや関連リソースを導入せずに大量のデータを効率的に検索できます。また、データ取得のコストとレイテンシも削減されます。

S3 Select とは何ですか。

S3 Select では、 S3 クライアントが SelectObjectContent 要求を使用して、オブジェクトから必要なデータのみをフィルタリングして読み出すことができます。S3 Select の StorageGRID 実装には、 S3 Select のコマンドと機能の一部が含まれています。

S3 Select を使用する際の考慮事項と要件

グリッド管理の要件

グリッド管理者は、テナントにS3 Select機能を許可する必要があります。またはの場合に*[Allow S3 Select]*を選択します"テナントを作成します""テナントの編集"。

オブジェクト形式の要件

照会するオブジェクトは、次のいずれかの形式である必要があります。

- * CSV *。そのまま使用することも、GZIPやbzip2のアーカイブに圧縮して使用することもできます。
- 寄木細工。寄木細工オブジェクトの追加要件：
  - S3 Selectでは、GZIPまたはSnappyを使用したカラムナ圧縮のみがサポートされます。S3 Selectでは、寄木細工オブジェクトのオブジェクト全体の圧縮はサポートされません。
  - S3 Selectは寄木細工の出力をサポートしていません。出力形式はCSVまたはJSONで指定する必要があります。
  - 圧縮されていない行グループの最大サイズは512MBです。
  - オブジェクトのスキーマで指定されているデータ型を使用する必要があります。
  - interval、json、list、time、またはUUID論理型は使用できません。

エンドポイントの要件

SelectObjectContent要求はに送信する必要があります"StorageGRID ロードバランサエンドポイント"。

エンドポイントで使用する管理ノードとゲートウェイノードは、次のいずれかである必要があります。

- サービスアプライアンスノード
- VMwareベースのソフトウェアノード
- cgroup v2が有効なカーネルを実行しているベアメタルノード

一般的な考慮事項

クエリをストレージノードに直接送信することはできません。

> SelectObjectContent 要求を使用すると、すべての S3 クライアントおよびすべてのテナントのロードバランサのパフォーマンスを低下させることができます。この機能は、必要な場合にのみ有効にし、信頼できるテナントに対してのみ有効にします。

を参照してください"S3 Select の使用手順"。

表示するには"Grafana チャート"S3 Select の操作を時間経過と共に表示するには、グリッド マネージャーでサポート > ツール > メトリクス を選択します。

クライアント接続を設定します

S3 クライアント接続を **StorageGRID** に設定

グリッド管理者は設定オプションを管理し、S3クライアントアプリケーションがデータの格納と読み出しを行うためにStorageGRIDシステムに接続する方法を制御します。

> このバージョンのドキュメントサイトからSwiftの詳細が削除されました。を参照してください "StorageGRID 11.8：S3およびSwiftクライアント接続の設定"

セツテイタスク

1. クライアントアプリケーションがStorageGRID に接続する方法に基づいて、StorageGRID で前提条件となるタスクを実行します。

必要な作業

以下を入手する必要があります。

- IPアドレス
- ドメイン名
- SSL証明書

任意のタスク

オプションで、以下を設定します。

- アイデンティティフェデレーション
- SSO

1. StorageGRID を使用して、アプリケーションがグリッドに接続するために必要な値を取得します。S3セットアップウィザードを使用するか、各StorageGRID エンティティを手動で設定できます。+

S3セットアップウィザードを使用する

S3セットアップウィザードの手順に従います。

手動で設定

1. ハイアベイラビリティグループの作成
2. ロードバランサエンドポイントを作成する
3. テナントアカウントを作成する
4. バケットとアクセスキーの作成
5. ILMルールとポリシーの設定

1. S3アプリケーションを使用して、StorageGRID への接続を完了します。DNSエントリを作成して、使用するドメイン名にIPアドレスを関連付けます。

   必要に応じて、追加のアプリケーションセットアップを実行します。

2. アプリケーションとStorageGRID で継続的なタスクを実行し、時間の経過に伴うオブジェクトストレージの管理と監視を行います。

クライアントアプリケーションに**StorageGRID** を接続するために必要な情報

StorageGRIDをS3クライアントアプリケーションに接続する前に、StorageGRIDで設定手順を実行して特定の値を取得する必要があります。

どのような価値が必要か？

次の表に、StorageGRIDで設定する必要がある値と、それらの値がS3アプリケーションとDNSサーバで使用される場所を示します。

値	値が設定されます	値が使用されます
仮想IP（VIP）アドレス	[HA group]をクリックしますStorageGRID	DNSエントリ
ポート	StorageGRID > Load Balancer Endpointの順に選択します	クライアントアプリケーション
SSL証明書	StorageGRID > Load Balancer Endpointの順に選択します	クライアントアプリケーション
サーバ名（FQDN）	StorageGRID > Load Balancer Endpointの順に選択します	• クライアントアプリケーション • DNSエントリ
S3アクセスキーIDとシークレットアクセスキー	StorageGRID > Tenant and bucketの順に選択します	クライアントアプリケーション
バケット/コンテナ名	StorageGRID > Tenant and bucketの順に選択します	クライアントアプリケーション

これらの値を取得するにはどうすればよいですか。

要件に応じて、次のいずれかの方法で必要な情報を入手できます。

- *を使用します"S3セットアップウィザード"。S3セットアップウィザードを使用すると、StorageGRID に必要な値を簡単に設定でき、S3アプリケーションの設定時に使用できる1つまたは2つのファイルを出力できます。ウィザードの指示に従って必要な手順を実行し、設定がStorageGRID のベストプラクティスに準拠していることを確認できます。

  S3アプリケーションを設定する場合は、特別な要件がある場合や実装に大幅なカスタマイズが必要な場合を除き、S3セットアップウィザードを使用することを推奨します。

- *を使用します"FabricPool セットアップウィザード"。S3セットアップウィザードと同様に、FabricPool セットアップウィザードを使用して必要な値をすばやく設定し、ONTAP でFabricPool クラウド階層を設定するときに使用できるファイルを出力できます。

  StorageGRID をFabricPool クラウド階層のオブジェクトストレージシステムとして使用する場合は、特別な要件がある場合や実装の大幅なカスタマイズが必要になる場合を除き、FabricPool セットアップウィザードを使用することを推奨します。

- 項目を手動で設定する。S3アプリケーションに接続していて、S3セットアップウィザードを使用しない場合は、設定を手動で実行して必要な値を取得できます。次の手順を実行します。

  a. S3アプリケーションで使用するハイアベイラビリティ（HA）グループを設定します。を参照して "ハイアベイラビリティグループを設定する"

  b. S3アプリケーションが使用するロードバランサエンドポイントを作成します。を参照して "ロードバランサエンドポイントを設定する"

  c. S3アプリケーションが使用するテナントアカウントを作成します。を参照して "テナントアカウント

を作成します"

d. S3テナントの場合は、テナントアカウントにサインインし、アプリケーションにアクセスする各ユーザのアクセスキーIDとシークレットアクセスキーを生成します。を参照して "独自のアクセスキーを作成します"

e. テナントアカウント内にS3バケットを1つ以上作成します。S3の場合は、を参照してください"S3 バケットを作成する"。

f. 新しいテナントまたはバケット/コンテナに属するオブジェクトに対する特定の配置手順を追加するには、新しいILMルールを作成し、そのルールを使用する新しいILMポリシーをアクティブ化します。およびを参照してください"ILM ルールを作成する""ILM ポリシーを作成する"。

StorageGRID の **S3** クライアントのセキュリティ

StorageGRIDテナントアカウントは、S3クライアントアプリケーションを使用してオブジェクトデータをStorageGRIDに保存します。クライアントアプリケーションに実装されているセキュリティ対策を確認する必要があります。

概要

S3 REST APIのセキュリティの実装方法を次に示します。

接続のセキュリティ
: TLS

サーバ認証
: システム CA によって署名された X.509 サーバ証明書、または管理者から提供されたカスタムサーバ証明書

クライアント認証
: S3アカウントのアクセスキーIDとシークレットアクセスキー

クライアント許可
: バケットの所有権と適用可能なすべてのアクセス制御ポリシー

StorageGRIDによるクライアントアプリケーションのセキュリティの仕組み

S3クライアントアプリケーションは、ゲートウェイノードまたは管理ノード上のロードバランササービスに接続するか、またはストレージノードに直接接続できます。

- ロードバランササービスに接続するクライアントでは、ユーザの方法に応じてHTTPSまたはHTTPを使用できます"ロードバランサエンドポイントの設定"。

  HTTPSはTLSで暗号化されたセキュアな通信を提供するため、推奨されます。エンドポイントにセキュリティ証明書を添付する必要があります。

  HTTPは安全性が低く、暗号化されていない通信を提供するため、非本番環境またはテストグリッドにのみ使用する必要があります。

- ストレージノードに接続するクライアントは、HTTPSまたはHTTPも使用できます。

  デフォルトはHTTPSで、推奨されます。

HTTPは安全性が低く、暗号化されていない通信を提供しますが、非本番環境またはテストグリッドではオプションで使用できます"有効"。

- StorageGRID とクライアント間の通信は、 TLS を使用して暗号化されます。
- ロードバランササービスとグリッド内のストレージノードの間の通信は、ロードバランサエンドポイントが HTTP と HTTPS どちらの接続を受け入れるように設定されているかに関係なく暗号化されます。
- REST API処理を実行するには、クライアントがStorageGRIDにを指定する必要があります"HTTP認証ヘッダー"。

セキュリティ証明書とクライアントアプリケーション

いずれの場合も、クライアントアプリケーションは、グリッド管理者がアップロードしたカスタムサーバ証明書または StorageGRID システムが生成した証明書を使用して、 TLS 接続を確立できます。

- ロードバランササービスに接続する場合、クライアントアプリケーションはロードバランサエンドポイント用に設定された証明書を使用します。各ロードバランサエンドポイントには独自の証明書があります。グリッド管理者がアップロードしたカスタムサーバ証明書、またはグリッド管理者がエンドポイントの設定時にStorageGRIDで生成した証明書のいずれかです。

  を参照して "ロードバランシングに関する考慮事項"

- クライアントアプリケーションは、ストレージノードに直接接続する場合、StorageGRID システムのインストール時にストレージノード用に生成されたシステム生成のサーバ証明書（システム認証局によって署名されたもの）を使用します。 または、グリッド管理者がグリッド用に提供した単一のカスタムサーバ証明書。を参照して "カスタムのS3 API証明書を追加する"

TLS 接続の確立に使用する証明書に署名した認証局を信頼するよう、クライアントを設定する必要があります。

TLS ライブラリのハッシュアルゴリズムと暗号化アルゴリズムがサポートされます

StorageGRIDシステムは、クライアント アプリケーションが TLS セッションを確立するときに使用できる暗号スイートのセットをサポートしています。暗号を設定するには、構成 > セキュリティ > セキュリティ設定に移動し、**TLS** および **SSH** ポリシー を選択します。

サポートされる **TLS** のバージョン

StorageGRID では、 TLS 1.2 と TLS 1.3 がサポートされています。

SSLv3 と TLS 1.1 （またはそれ以前のバージョン）はサポートされなくなりました。

S3セットアップウィザードを使用する

StorageGRID S3 セットアップ ウィザードの考慮事項と要件

S3セットアップウィザードを使用して、StorageGRID をS3アプリケーションのオブジェクトストレージシステムとして設定できます。

S3セットアップウィザードを使用するタイミング

S3セットアップウィザードの手順に従って、S3アプリケーションで使用するStorageGRID を設定します。ウィザードを完了すると、ファイルをダウンロードしてS3アプリケーションに値を入力します。ウィザードを使用すると、システムをより迅速に設定し、設定がStorageGRID のベストプラクティスに準拠していることを確認できます。

を使用している場合"rootアクセス権限"は、StorageGRIDグリッドマネージャの使用を開始したときにS3セットアップウィザードを完了することができます。また、ウィザードにアクセスしてあとから完了することもできます。要件に応じて、必要な項目の一部またはすべてを手動で設定し、ウィザードを使用してS3アプリケーションで必要な値をアセンブルすることもできます。

ウィザードを使用する前に

ウィザードを使用する前に、これらの前提条件を満たしていることを確認してください。

IPアドレスを取得し、**VLAN**インターフェイスを設定します

ハイアベイラビリティ（HA）グループを設定する場合は、S3アプリケーションが接続するノードと使用するStorageGRID ネットワークを確認しておきます。また、サブネットCIDR、ゲートウェイIPアドレス、および仮想IP（VIP）アドレスに入力する値も確認しておきます。

仮想LANを使用してS3アプリケーションからトラフィックを分離する場合は、VLANインターフェイスがすでに設定されています。を参照して "VLAN インターフェイスを設定します"

アイデンティティフェデレーションと**SSO**を設定する

StorageGRIDシステムで ID フェデレーションまたはシングル サインオン (SSO) を使用する予定の場合は、これらの機能が有効になっています。また、S3 アプリケーションが使用するテナント アカウントのルート アクセス権を持つフェデレーション グループも把握しています。見る"アイデンティティフェデレーションを使用する"そして"シングルサインオンを設定します"。

ドメイン名を取得して設定します

StorageGRID に使用するFully Qualified Domain Name（FQDN；完全修飾ドメイン名）を確認しておきます。ドメインネームサーバ（DNS）のエントリによって、このFQDNが、ウィザードを使用して作成するHAグループの仮想IP（VIP）アドレスにマッピングされます。

S3仮想ホスト型リクエストを使用する予定がある場合は、"S3エンドポイントのドメイン名が設定されました"が必要です。仮想ホスト型のリクエストを使用することをお勧めします。

ロードバランサとセキュリティ証明書の要件を確認します

StorageGRID ロードバランサを使用する場合は、ロードバランシングに関する一般的な考慮事項を確認しておきます。アップロードする証明書、または証明書の生成に必要な値を用意しておきます。

外部（サードパーティ）のロードバランサエンドポイントを使用する場合は、そのロードバランサの完全修飾ドメイン名（FQDN）、ポート、および証明書が必要です。

グリッドフェデレーション接続を設定します

S3テナントがアカウントデータを同期し、グリッドフェデレーション接続を使用してバケットオブジェクトを別のグリッドに複製できるようにする場合は、ウィザードを開始する前に以下の点を確認してください。

- そうだな "グリッドフェデレーション接続を設定しました"

- 接続のステータスは*接続済み*です。
- Root Access 権限が割り当てられている。

StorageGRID で **S3** セットアップ ウィザードにアクセスして完了します

S3セットアップウィザードを使用して、S3アプリケーションで使用するStorageGRIDを設定できます。セットアップウィザードには、StorageGRID バケットへのアクセスとオブジェクトの保存に必要な値が表示されます。

開始する前に

- あなたはを持っています"rootアクセス権限"。
- でウィザードを使用するためのを確認しておき"考慮事項と要件"ます。

ウィザードにアクセスします

手順

1. を使用してGrid Managerにサインインし"サポートされている Web ブラウザ"ます。
2. *FabricPool and S3 セットアップ ウィザード*のバナーがダッシュボードに表示されている場合は、バナー内のリンクを選択してください。バナーが表示されなくなった場合は、Grid Manager のヘッダーバーにあるヘルプアイコン を選択し、*FabricPool and S3 セットアップ ウィザード*を選択してください。
3. FabricPool とS3のセットアップウィザードのページのS3アプリケーションセクションで、*今すぐ設定*を選択します。

手順**1/6**：**HA**グループを設定する

HAグループは、それぞれにStorageGRID ロードバランササービスが含まれるノードの集まりです。HAグループには、ゲートウェイノード、管理ノード、またはその両方を含めることができます。

HAグループを使用すると、S3データ接続の可用性を維持できます。HAグループのアクティブインターフェイスで障害が発生しても、バックアップインターフェイスでワークロードを管理できるため、S3処理への影響はほとんどありません。

このタスクの詳細については、を参照してください"ハイアベイラビリティグループを管理します"。

手順

1. 外部のロードバランサを使用する場合は、HAグループを作成する必要はありません。[Skip this step]*を選択し、に進みます[手順2/6：ロードバランサエンドポイントの設定]。
2. StorageGRID ロードバランサを使用するには、新しいHAグループを作成するか、既存のHAグループを使用します。

HA グループを作成します

a. 新しいHAグループを作成するには、*[HAグループの作成]*を選択します。

b. [詳細を入力]*ステップで、次のフィールドに値を入力します。

フィールド	製品説明
HAグループ名	このHAグループの一意の表示名。
概要 （オプション）	このHAグループの概要 。

c. [インターフェイスの追加]*手順で、このHAグループで使用するノードインターフェイスを選択します。

列ヘッダーを使用して行をソートするか、検索キーワードを入力してインターフェイスをより迅速に検索します。

ノードは1つ以上選択できますが、ノードごとに選択できるインターフェイスは1つだけです。

d. [* prioritize interfaces]ステップでは、このHAグループのプライマリインターフェイスとバックアップインターフェイスを決定します。

行をドラッグして、*優先順位*列の値を変更します。

リストの最初のインターフェイスはプライマリインターフェイスです。プライマリインターフェイスは、障害が発生しないかぎり、アクティブインターフェイスです。

HAグループに複数のインターフェイスが含まれていて、アクティブインターフェイスで障害が発生した場合、仮想IP（VIP）アドレスは優先順位に従って最初のバックアップインターフェイスに移動します。そのインターフェイスに障害が発生すると、 VIP アドレスは次のバックアップインターフェイスに移動します。障害が解決されると、VIPアドレスは使用可能な最もプライオリティの高いインターフェイスに戻ります。

e. [IPアドレスの入力]*ステップで、次のフィールドに値を入力します。

フィールド	製品説明
サブネットCIDR	VIPサブネットのアドレス（CIDR表記）。IPv4アドレス、スラッシュ、およびサブネットの長さ（0～32）。 ネットワークアドレスにホストビットを設定しないでください。たとえば、 `192.16.0.0/22`です。
ゲートウェイIPアドレス（オプション）	StorageGRID へのアクセスに使用するS3 IPアドレスがStorageGRID VIPアドレスと同じサブネットにない場合は、StorageGRID VIPローカルゲートウェイのIPアドレスを入力します。ローカルゲートウェイの IP アドレスは VIP サブネット内にある必要があります。

フィールド	製品説明
仮想IPアドレス	HAグループ内のアクティブインターフェイスのVIPアドレスを1つ以上10個以下で入力します。すべてのVIPアドレスがVIPサブネット内にある必要があります。 IPv4アドレスを少なくとも1つ指定する必要があります。必要に応じて、追加の IPv4 アドレスと IPv6 アドレスを指定できます。

f. を選択し、[終了]*を選択してS3セットアップウィザードに戻ります。

g. [続行]*を選択して、ロードバランサの手順に進みます。

既存の**HA**グループを使用する

a. 既存のHAグループを使用するには、*[HAグループの選択]*からHAグループ名を選択します。

b. [続行]*を選択して、ロードバランサの手順に進みます。

手順**2/6**：ロードバランサエンドポイントの設定

StorageGRID は、ロードバランサを使用してクライアントアプリケーションからワークロードを管理します。ロードバランシングは、複数のストレージノードにわたって速度と接続容量を最大化します。

すべてのゲートウェイノードと管理ノードに存在するStorageGRID ロードバランササービスを使用することも、外部（サードパーティ）のロードバランサに接続することもできます。StorageGRID ロードバランサを使用することを推奨します。

このタスクの詳細については、を参照してください"ロードバランシングに関する考慮事項"。

StorageGRID ロードバランササービスを使用するには、* StorageGRID load balancer タブを選択し、使用するロードバランサエンドポイントを作成または選択します。外部ロードバランサを使用するには、[外部ロードバランサ]*タブを選択し、設定済みのシステムに関する詳細を入力します。

エンドポイントを作成します

手順

1. ロードバランサエンドポイントを作成するには、*[エンドポイントの作成]*を選択します。
2. Enter endpoint details *ステップで、次のフィールドに値を入力します。

フィールド	製品説明
名前	エンドポイントのわかりやすい名前。
ポート	ロードバランシングに使用する StorageGRID ポート。最初に作成するエンドポイントのデフォルトは10433ですが、未使用の外部ポートを入力できます。80または443を入力すると、ゲートウェイノードでのみエンドポイントが設定されます。これらのポートは管理ノードで予約されているためです。 注意: 他のグリッド サービスで使用されるポートは許可されません。見る"StorageGRID の内部ポート" 。
クライアントタイプ	は* S3 *にする必要があります。
ネットワークプロトコル	「* HTTPS *」を選択します。 注：TLS暗号化なしでのStorageGRID との通信はサポートされていますが、推奨されません。

3. [結合モードの選択]ステップで、結合モードを指定します。バインドモードは、任意のIPアドレスまたは特定のIPアドレスとネットワークインターフェイスを使用してエンドポイントにアクセスする方法を制御します。

モード	製品説明
グローバル（デフォルト）	クライアントは、任意のゲートウェイノードまたは管理ノードのIPアドレス、任意のネットワーク上の任意のHAグループの仮想IP（VIP）アドレス、または対応するFQDNを使用して、エンドポイントにアクセスできます。 このエンドポイントのアクセスを制限する必要がある場合を除き、 * グローバル * 設定（デフォルト）を使用します。
HA グループの仮想 IP	クライアントがこのエンドポイントにアクセスするには、HAグループの仮想IPアドレス（または対応するFQDN）を使用する必要があります。 このバインドモードのエンドポイントでは、エンドポイント用に選択したHAグループが重複しないかぎり、すべて同じポート番号を使用できます。

モード	製品説明
ノードインターフェイス	クライアントがこのエンドポイントにアクセスするには、選択したノードインターフェイスのIPアドレス（または対応するFQDN）を使用する必要があります。
ノードタイプ	選択したノードのタイプに基づいて、クライアントがこのエンドポイントにアクセスするには、いずれかの管理ノードのIPアドレス（または対応するFQDN）か、いずれかのゲートウェイノードのIPアドレス（または対応するFQDN）を使用する必要があります。

4. [Tenant access]ステップで、次のいずれかを選択します。

フィールド	製品説明
Allow all tenants（デフォルト）	すべてのテナントアカウントは、このエンドポイントを使用してバケットにアクセスできます。
選択したテナントを許可します	このエンドポイントを使用してバケットにアクセスできるのは、選択したテナントアカウントのみです。
選択したテナントをブロックします	選択したテナントアカウントは、このエンドポイントを使用してバケットにアクセスできません。他のすべてのテナントでこのエンドポイントを使用できます。

5. [証明書の添付]*ステップで、次のいずれかを選択します。

フィールド	製品説明
証明書のアップロード（推奨）	このオプションは、CA署名済みサーバ証明書、証明書秘密鍵、およびオプションのCAバンドルをアップロードする場合に使用します。
証明書の生成	このオプションは、自己署名証明書を生成する場合に使用します。入力する項目の詳細については、を参照してください"ロードバランサエンドポイントを設定する"。
StorageGRID S3証明書を使用する	このオプションは、StorageGRID グローバル証明書のカスタムバージョンをすでにアップロードまたは生成している場合にのみ使用します。詳細は、を参照してください "S3 API証明書の設定" 。

6. [Finish]*を選択してS3セットアップウィザードに戻ります。
7. [続行]*を選択してテナントとバケットの手順に進みます。

エンドポイント証明書の変更がすべてのノードに適用されるまでに最大 15 分かかることがあります。

既存のロードバランサエンドポイントを使用する

手順

1. 既存のエンドポイントを使用する場合は、*[ロードバランサエンドポイントの選択]*からそのエンドポイントの名前を選択します。
2. [続行]*を選択してテナントとバケットの手順に進みます。

外部のロードバランサを使用する

手順

1. 外部のロードバランサを使用するには、次のフィールドに値を入力します。

フィールド	製品説明
FQDN	外部ロードバランサの完全修飾ドメイン名（FQDN）。
ポート	S3アプリケーションが外部ロードバランサへの接続に使用するポート番号。
証明書	外部ロードバランサのサーバ証明書をコピーして、このフィールドに貼り付けます。

2. [続行]*を選択してテナントとバケットの手順に進みます。

ステップ**3 / 6**：テナントとバケットを作成

テナントは、S3アプリケーションを使用してStorageGRID でオブジェクトの格納と読み出しを行うことができるエンティティです。各テナントには、独自のユーザ、アクセスキー、バケット、オブジェクト、および特定の機能セットがあります。

バケットは、テナントのオブジェクトとオブジェクトメタデータを格納するためのコンテナです。テナントには多数のバケットが含まれている場合もありますが、このウィザードを使用すると、テナントとバケットを最も簡単かつ迅速に作成できます。バケットの追加やオプションの設定があとで必要になった場合は、Tenant Managerを使用できます。

このタスクの詳細については、およびを参照してください"テナントアカウントを作成する""S3 バケットを作成する"。

手順

1. テナントアカウントの名前を入力します。

   テナント名は一意である必要はありません。作成したテナントアカウントには、一意の数値アカウント ID が割り当てられます。

2. StorageGRIDシステムが使用するかどうかに基づいて、テナントアカウントのルートアクセスを定義します。"アイデンティティフェデレーション" 、"シングルサインオン（SSO）" 、またはその両方。

オプション	手順
アイデンティティフェデレーションが有効になっていない場合	ローカルrootユーザとしてテナントにサインインするときに使用するパスワードを指定します。

オプション	手順
アイデンティティフェデレーションが有効になっている場合	a. テナントに含める既存のフェデレーテッドグループを選択します"rootアクセス権限"。 b. 必要に応じて、ローカルrootユーザとしてテナントにサインインする際に使用するパスワードを指定します。
アイデンティティフェデレーションとシングルサインオン（SSO）の両方が有効になっている場合	テナントに含める既存のフェデレーテッドグループを選択します"rootアクセス権限"。ローカルユーザはサインインできません。

3. ルートユーザのアクセスキーIDとシークレットアクセスキーをウィザードで作成する場合は、* Create root user S3 access key automatically *を選択します。

   テナントのユーザをrootユーザだけにする場合は、このオプションを選択します。他のユーザがこのテナントを使用する場合は、"Tenant Managerを使用"キーと権限を設定します。

4. このテナント用のバケットを今すぐ作成する場合は、*[このテナント用にバケットを作成する]*を選択します。

   グリッドでS3オブジェクトロックが有効になっている場合、この手順で作成したバケットではS3オブジェクトロックが有効になりません。このS3アプリケーションでS3 Object Lockバケットを使用する必要がある場合は、ここでバケットを作成することを選択しないでください。代わりに、あとでTenant Managerを使用し"バケットを作成します"ます。

   a. S3アプリケーションが使用するバケットの名前を入力します。たとえば、 `s3-bucket`です。

      バケットの作成後にバケット名を変更することはできません。

   b. このバケットの*[Region]*を選択します。

      (`us-east-1`将来ILMを使用してバケットのリージョンに基づいてオブジェクトをフィルタリングする予定がないかぎり、デフォルトのリージョンを使用します）。

5. [作成して続行]*を選択します。

ステップ**4/6**：データをダウンロードします

ダウンロードデータステップでは、1つまたは2つのファイルをダウンロードして、設定した内容の詳細を保存できます。

手順

1. [Create root user S3 access key automatically]*を選択した場合は、次のいずれかまたは両方を実行します。
   - テナントアカウント名、アクセスキーID、シークレットアクセスキーが記載されたファイルをダウンロードするには、*[アクセスキーのダウンロード]*を選択し `.csv`ます。
   - コピーアイコン（）を選択して、アクセスキーIDとシークレットアクセスキーをクリップボードにコピーします。
2. [設定値をダウンロード]*を選択して、ロードバランサエンドポイント、テナント、バケット、およびroot

ユーザの設定を含むファイルをダウンロードし `.txt`ます。

3. この情報を安全な場所に保存してください。

> 両方のアクセスキーをコピーするまで、このページを閉じないでください。このページを閉じると、キーは使用できなくなります。この情報はStorageGRID システムからデータを取得するために使用できるため、必ず安全な場所に保存してください。

4. プロンプトが表示されたら、チェックボックスをオンにして、キーをダウンロードまたはコピーしたことを確認します。
5. [続行]*を選択してILMルールとポリシーの手順に進みます。

手順**5 / 6**：**S3**の**ILM**ルールと**ILM**ポリシーを確認します

情報ライフサイクル管理（ILM）ルールは、StorageGRID システム内のすべてのオブジェクトの配置、期間、取り込み動作を制御します。StorageGRID に含まれているILMポリシーは、すべてのオブジェクトのレプリケートコピーを2つ作成します。このポリシーは、新しいポリシーを少なくとも1つアクティブ化するまで有効です。

手順

1. ページに表示された情報を確認します。
2. 新しいテナントまたはバケットに属するオブジェクトに対する具体的な手順を追加する場合は、新しいルールと新しいポリシーを作成します。およびを参照してください"ILM ルールを作成する""ILMポリシーを使用する"。
3. [I have review these steps and understand what I need to do]*を選択します。
4. チェックボックスをオンにして、次に何をすべきかを理解していることを示します。
5. を選択して[概要]*に進みます。

ステップ**6 / 6**：まとめの確認

手順

1. 概要を確認します。
2. 次の手順の詳細をメモしておいてください。S3クライアントに接続する前に必要になる可能性がある追加の設定について説明しています。たとえば、*[Sign in as root]*を選択するとTenant Managerに移動し、テナントユーザの追加、バケットの作成、バケットの設定の更新を行うことができます。
3. [完了] を選択します。
4. StorageGRID からダウンロードしたファイルまたは手動で取得した値を使用して、アプリケーションを設定します。

HAグループを管理します

StorageGRID 高可用性グループについて学ぶ

ハイアベイラビリティ（HA）グループは、S3クライアントに可用性の高いデータ接続、およびGrid ManagerとTenant Managerへの可用性の高い接続を提供します。

複数の管理ノードとゲートウェイノードのネットワークインターフェイスをハイアベイラビリティ（ HA ）グ

ループにまとめることができます。HA グループのアクティブインターフェイスで障害が発生した場合、バックアップインターフェイスがワークロードを管理できます。

各 HA グループは、選択したノードの共有サービスへのアクセスを提供します。

- ゲートウェイノード、管理ノード、またはその両方を含むHAグループは、S3クライアントに可用性の高いデータ接続を提供します。
- 管理ノードだけで構成される HA グループは、 Grid Manager と Tenant Manager への可用性の高い接続を提供します。
- サービスアプライアンスとVMwareベースのソフトウェアノードのみを含むHAグループは、の可用性の高い接続を提供できます"S3 Select を使用する S3 テナント"。S3 Select を使用する場合は HA グループを推奨しますが、必須ではありません。

HA グループはどのように作成しますか？

1. 1 つ以上の管理ノードまたはゲートウェイノードのネットワークインターフェイスを選択します。ノードに追加したグリッドネットワーク（ eth0 ）インターフェイス、クライアントネットワーク（ eth2 ）インターフェイス、 VLAN インターフェイス、またはアクセスインターフェイスを使用できます。

   DHCPによってIPアドレスが割り当てられたHAグループにインターフェイスを追加することはできません。

2. プライマリインターフェイスとして指定するインターフェイスは 1 つです。プライマリインターフェイスは、障害が発生しないかぎり、アクティブインターフェイスです。
3. バックアップインターフェイスの優先順位を決定します。
4. グループに仮想 IP （ VIP ）アドレスを 1 ～ 10 個割り当てます。クライアントアプリケーションは、これらの VIP アドレスのいずれかを使用して StorageGRID に接続できます。

手順については、を参照してください"ハイアベイラビリティグループを設定する"。

アクティブインターフェイスとは何ですか。

通常の運用中は、 HA グループのすべての VIP アドレスが優先順位の最初のインターフェイスであるプライマリインターフェイスに追加されます。プライマリインターフェイスが使用可能な状態であれば、クライアントがグループの任意の VIP アドレスに接続するときに使用されます。つまり、通常の動作中は、プライマリインターフェイスがグループの「アクティブ」インターフェイスになります。

同様に、通常動作中は、HAグループの優先度の低いインターフェイスが「バックアップ」インターフェイスとして機能します。これらのバックアップインターフェイスは、プライマリ（現在アクティブ）インターフェイスが使用できなくなるまで使用されません。

ノードの現在の **HA** グループのステータスを表示します

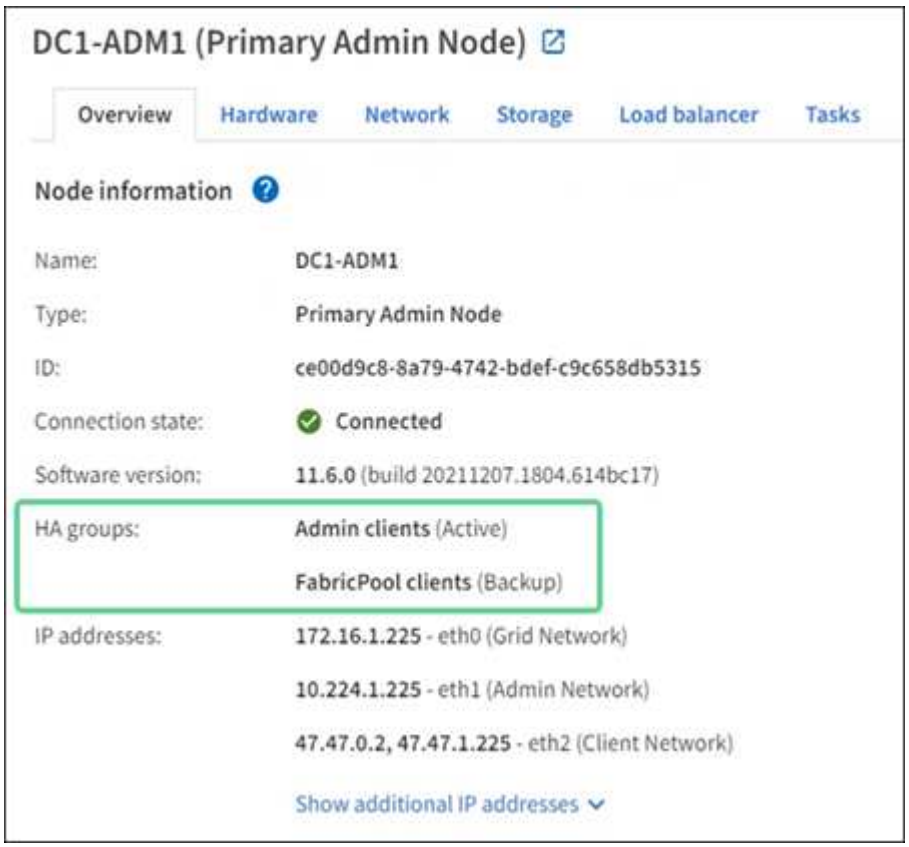
ノードが HA グループに割り当てられているかどうかを確認し、現在のステータスを確認するには、[ノード] > [***node***] を選択します。

概要 * タブに HA グループ * のエントリが含まれている場合、そのノードは表示されている HA グループに割り当てられます。グループ名のあとの値は、 HA グループ内のノードの現在のステータスです。

- * Active * ： HA グループは現在このノードでホストされています。

- * バックアップ * ： HA グループは現在このノードを使用していません。バックアップインターフェイスです。
- 停止：ハイアベイラビリティ（キープアライブ）サービスが手動で停止されているため、このノードでHAグループをホストできません。
- 障害：次の1つ以上の理由により、このノードでHAグループをホストできません：
  - ロードバランサ（ nginx-gw ）サービスがノードで実行されていません。
  - ノードの eth0 または VIP インターフェイスが停止しています。
  - ノードは停止しています。

この例では、プライマリ管理ノードが 2 つの HA グループに追加されています。このノードは、現在、FabricPool クライアントグループのアクティブインターフェイスであり、クライアントグループのバックアップインターフェイスです。



アクティブインターフェイスに障害が発生するとどうなりますか。

VIP アドレスを現在ホストしているインターフェイスは、アクティブインターフェイスです。HA グループに複数のインターフェイスが含まれている場合にアクティブインターフェイスで障害が発生すると、 VIP アドレスは優先順位に従って、使用可能な最初のバックアップインターフェイスに移動します。そのインターフェイスに障害が発生すると、使用可能な次のバックアップインターフェイスに VIP アドレスが移動します。

フェイルオーバーは、次のいずれかの理由でトリガーされる可能性があります。

- インターフェイスが設定されているノードが停止する。
- インターフェイスが設定されているノードと他のすべてのノードとの接続が少なくとも 2 分間失われます。

- アクティブインターフェイスが停止する。
- ロードバランササービスが停止する。
- ハイアベイラビリティサービスが停止します。

> アクティブインターフェイスをホストするノードの外部でネットワーク障害が発生した場合、フェイルオーバーがトリガーされないことがあります。同様に、Grid ManagerまたはTenant Managerのサービスによってフェイルオーバーはトリガーされません。

フェイルオーバープロセスにかかる時間は通常数秒です。クライアントアプリケーションにほとんど影響がなく、通常の再試行で処理を続行できます。

障害が解決され、プライオリティの高いインターフェイスが再び使用可能になると、 VIP アドレスはプライオリティの高いインターフェイスに自動的に移動されます。

StorageGRID HA グループによる高可用性の提供方法

ハイアベイラビリティ（ HA ）グループを使用すると、オブジェクトデータ用および管理用に StorageGRID への可用性の高い接続を提供できます。

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

HA グループは、グループに含まれるすべてのノードが同じサービスを提供する場合にのみ高可用性を提供できます。HA グループを作成するときは、必要なサービスを提供するタイプのノードからインターフェイスを追加してください。

- * 管理ノード * ：ロードバランササービスが含まれ、 Grid Manager またはテナントマネージャへのアクセスを有効にします。
- ゲートウェイノード：ロードバランササービスが含まれます。

HA グループの目的	このタイプのノードを **HA** グループに追加します
Grid Manager へのアクセス	• プライマリ管理ノード（ * プライマリ * ） • 非プライマリ管理ノード • 注： * プライマリ管理ノードがプライマリインターフェイスである必要があります。一部のメンテナンス手順は、プライマリ管理ノードでしか実行できません。
Tenant Manager のみにアクセスします	• プライマリ管理ノードまたは非プライマリ管理ノード
S3 クライアント アクセス - ロードバランサ サービス	• 管理ノード • ゲートウェイノード

HA グループの目的	このタイプのノードを HA グループに追加します
S3クライアントアクセス"S3 選択"	• サービスアプライアンス • VMware ベースのソフトウェアノード • 注： S3 Select を使用する場合は HA グループを推奨しますが、必須ではありません。

Grid Manager または **Tenant Manager** で **HA** グループを使用する場合の制限事項

Grid Manager サービスまたは Tenant Manager サービスに障害が発生した場合は、 HA グループのフェイルオーバーはトリガーされません。

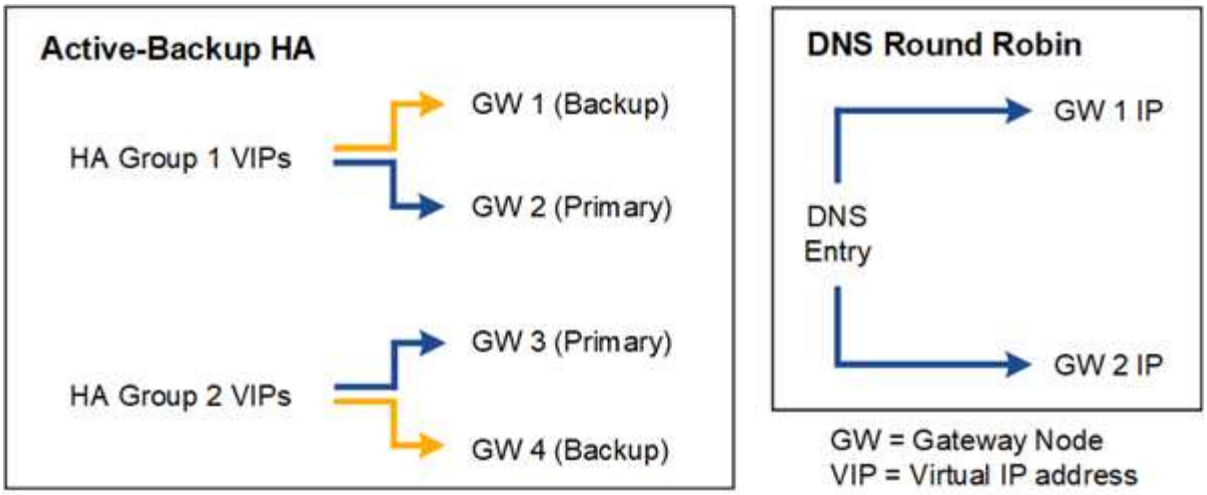
フェイルオーバーの発生時に Grid Manager または Tenant Manager にサインインしている場合はサインアウトされるため、再度サインインしてタスクを再開する必要があります。

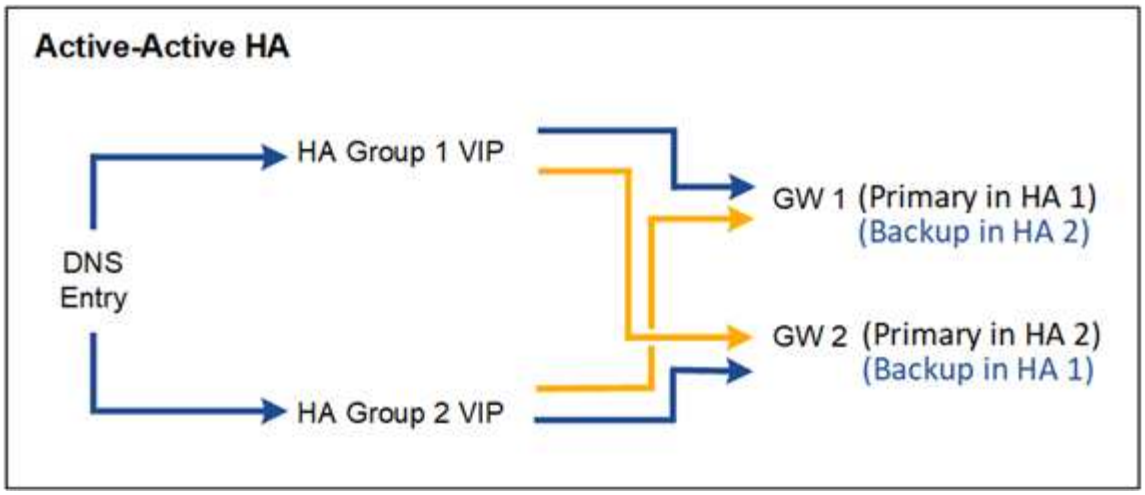
プライマリ管理ノードを使用できないと、一部のメンテナンス手順を実行できません。フェイルオーバー中は、 Grid Manager を使用して StorageGRID システムを監視できます。

StorageGRID 高可用性グループの設定オプション

以下の図は、高可用性（HA）グループを構成するさまざまな方法の例を示しています。それぞれの選択肢には長所と短所があります。

次の図では、 HA グループのプライマリインターフェイスが青、 HA グループのバックアップインターフェイスが黄色で示されています。





次の表は、図に示す各 HA 構成のメリットをまとめたものです。

構成	利点	欠点
アクティブ / バックアップ HA	• StorageGRID で管理され、外部のコンポーネントを必要としません。 • 高速フェイルオーバー。	• HA グループ内の 1 つのノードだけがアクティブです。各 HA グループで少なくとも 1 つのノードがアイドル状態になります。
DNS ラウンドロビン	• 総スループットが向上します。 • アイドル状態のホストはありません。	• クライアントの動作によってはフェイルオーバーが低速になる可能性があります。 • StorageGRID の外部でハードウェアを構成する必要があります。 • ユーザによる健全性チェックが必要です。

構成	利点	欠点
アクティブ / アクティブ HA	• トラフィックが複数の HA グループに分散されます。 • HA グループの数が増えるほど総スループットが向上します。 • 高速フェイルオーバー。	• 設定がより複雑になります。 • StorageGRID の外部でハードウェアを構成する必要があります。 • ユーザによる健全性チェックが必要です。

StorageGRIDで高可用性グループを設定する

ハイアベイラビリティ（ HA ）グループを設定して、管理ノードまたはゲートウェイノード上のサービスへの可用性の高いアクセスを提供できます。

StorageGRIDシステムには最大 255 個の HA グループを設定できます。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"rootアクセス権限"。
- HA グループで VLAN インターフェイスを使用する場合は、 VLAN インターフェイスを作成しておきます。を参照して "VLAN インターフェイスを設定します"
- HA グループ内のノードに対してアクセスインターフェイスを使用する場合は、インターフェイスを作成しておきます。
  - **Linux (**ノードをインストールする前**)**:"ノード構成ファイルを作成"
  - **Linux (**ノードのインストール後**)**:"ノードにトランクまたはアクセスインターフェースを追加する"
  - **VMware (**ノードのインストール後**)**:"ノードにトランクまたはアクセスインターフェースを追加する"

「Linux」は、RHEL、Ubuntu、または Debian のデプロイメントを指します。サポートされているバージョンのリストについては、 "NetApp Interoperability Matrix Tool（IMT）" 。

ハイアベイラビリティグループを作成します

ハイアベイラビリティグループを作成する場合は、 1 つ以上のインターフェイスを選択して優先順位順に編成します。次に、グループに 1 つ以上の VIP アドレスを割り当てます。

HA グループに含まれるゲートウェイノードまたは管理ノードのインターフェイスを指定する必要があります。HA グループでは、 1 つのノードに対して使用できるインターフェイスは 1 つだけですが、同じノードの他のインターフェイスは他の HA グループで使用できます。

ウィザードにアクセスします

手順

1. 構成 > ネットワーク > *高可用性グループ*を選択します。
2. 「 * Create * 」を選択します。

HA グループの詳細を入力します

手順

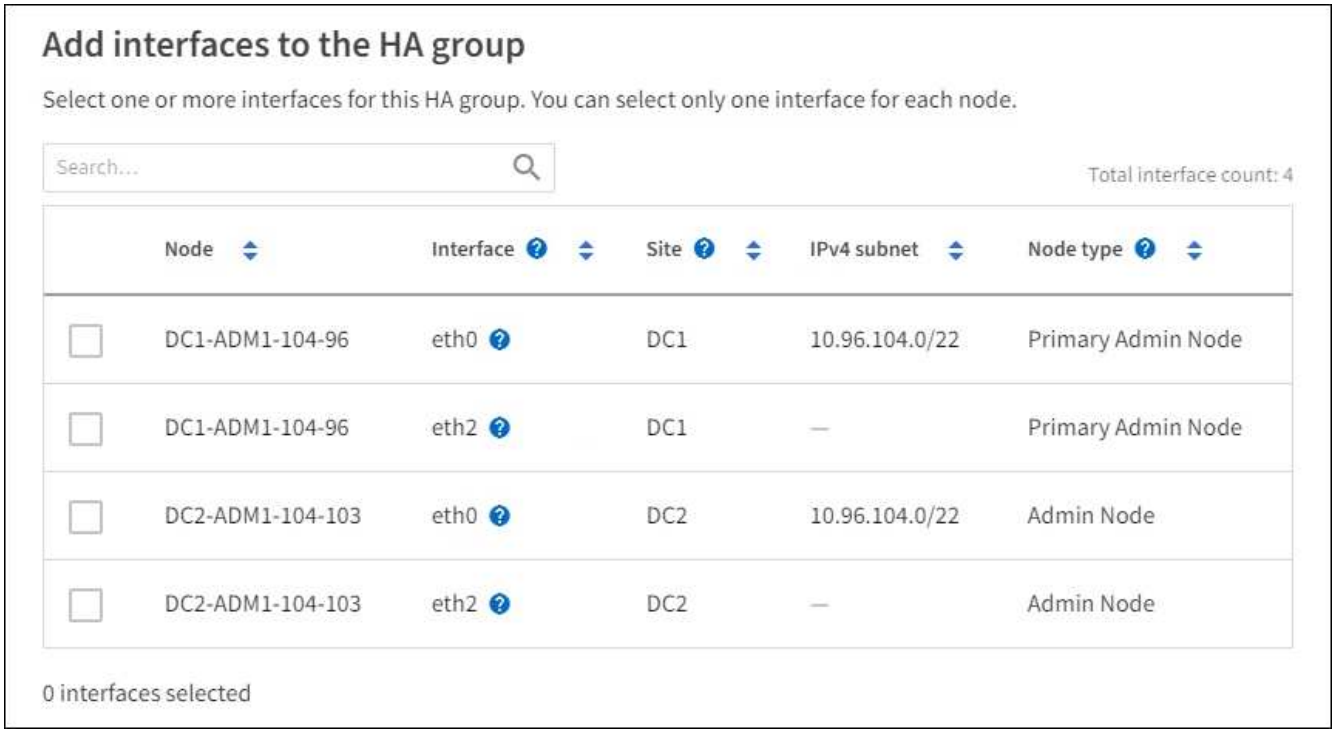
1. HA グループの一意の名前を指定してください。
2. 必要に応じて、 HA グループの概要 を入力します。
3. 「 * Continue * 」を選択します。

HA グループにインターフェイスを追加します

手順

1. この HA グループに追加するインターフェイスを 1 つ以上選択してください。

   列ヘッダーを使用して行をソートするか、検索キーワードを入力してインターフェイスをより迅速に検索します。



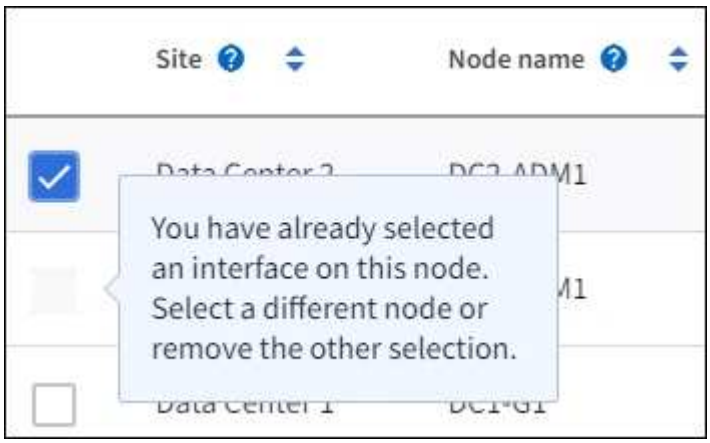
   VLAN インターフェイスを作成したら、新しいインターフェイスがテーブルに表示されるまで最大 5 分間待ちます。

インターフェイスの選択に関するガイドライン

- インターフェイスを少なくとも 1 つ選択してください。
- ノードに対して選択できるインターフェイスは 1 つだけです。
- HA グループがグリッドマネージャとテナントマネージャを含む管理ノードサービスの HA 保護用である場合は、管理ノード上のインターフェイスのみを選択します。
- HAグループがS3クライアントトラフィックのHA保護用の場合は、管理ノード、ゲートウェイノード、またはその両方のインターフェイスを選択します。
- 異なるタイプのノード上のインターフェイスを選択した場合は、情報メモが表示されます。フェイルオーバーが発生すると、以前にアクティブだったノードから提供されたサービスを、新たにアクティ

ブになったノードで使用できなくなる可能性があります。たとえば、バックアップゲートウェイノードは管理ノードサービスのHA保護を提供できません。同様に、バックアップ管理ノードでは、プライマリ管理ノードが提供するすべてのメンテナンス手順を実行できません。

- インターフェイスを選択できない場合、そのチェックボックスは無効になります。詳細については、ツールヒントを参照してください。



- サブネット値またはゲートウェイが選択した別のインターフェイスと競合している場合は、インターフェイスを選択できません。
- 静的IPアドレスが設定されていないインターフェイスは選択できません。

2. 「 * Continue * 」を選択します。

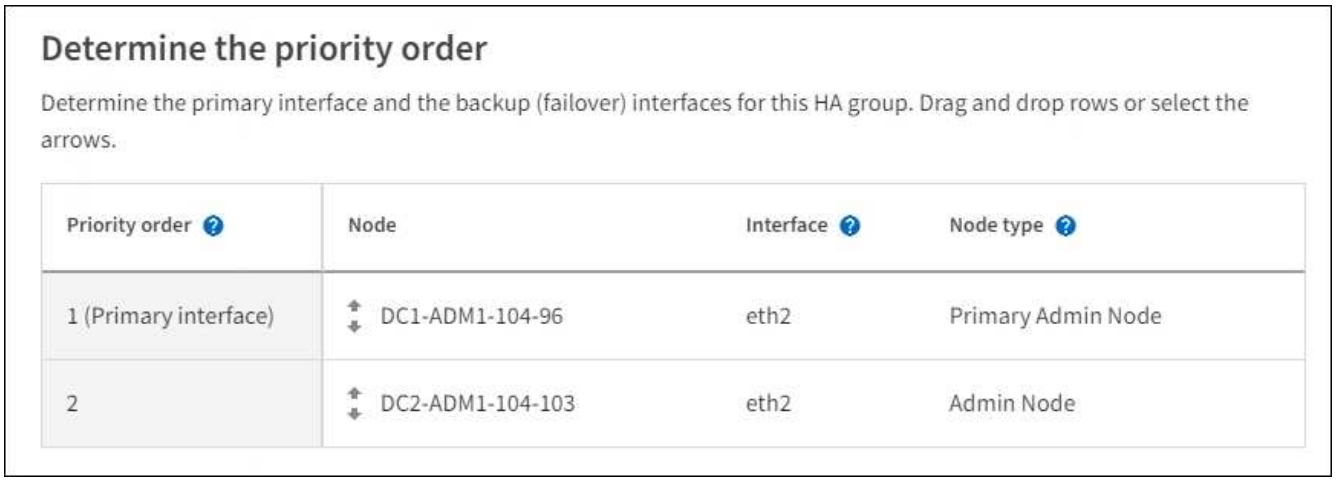
優先順位を決定します

HAグループに複数のインターフェイスが含まれている場合は、プライマリインターフェイスとバックアップ（フェイルオーバー）インターフェイスを判別できます。プライマリインターフェイスに障害が発生すると、VIPアドレスは使用可能な最もプライオリティの高いインターフェイスに移動します。そのインターフェイスに障害が発生すると、 VIP アドレスは次に優先度の高いインターフェイスに移動します。

手順

1. 優先順位*列の行をドラッグして、プライマリインターフェイスとバックアップインターフェイスを決定します。

   リストの最初のインターフェイスはプライマリインターフェイスです。プライマリインターフェイスは、障害が発生しないかぎり、アクティブインターフェイスです。



HA グループが Grid Manager へのアクセスを提供する場合は、プライマリ管理ノード上のインターフェイスを選択してプライマリインターフェイスにする必要があります。一部のメンテナンス手順は、プライマリ管理ノードでしか実行できません。

2. 「 * Continue * 」を選択します。

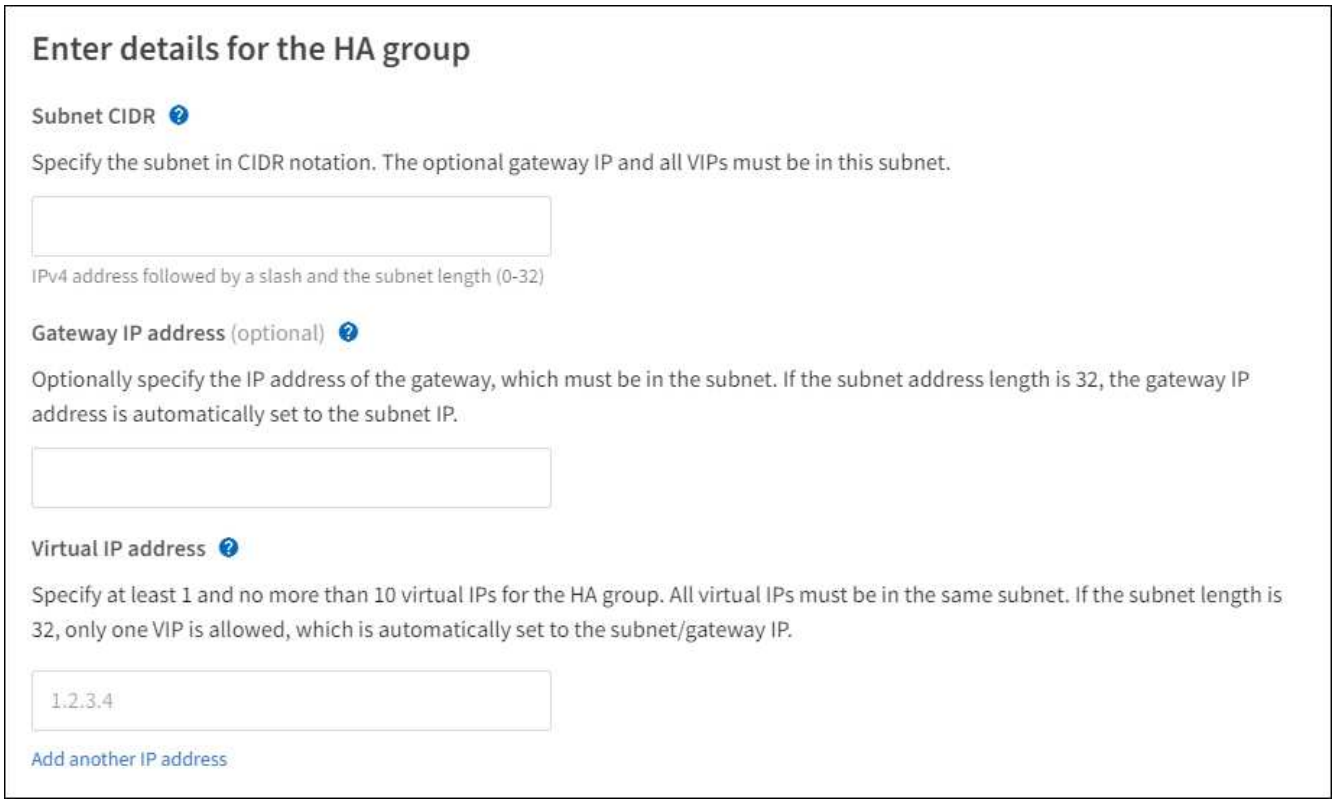
IP アドレスを入力してください

手順

1. [* Subnet CIDR*] フィールドで、 CIDR 表記の VIP サブネット（ IPv4 アドレスの後にスラッシュとサブネットの長さ（ 0 ～ 32 ）を指定します。

   ネットワークアドレスにホストビットを設定しないでください。たとえば、 `192.16.0.0/22`です。

   32 ビットプレフィックスを使用する場合、 VIP ネットワークアドレスはゲートウェイアドレスおよび VIP アドレスとしても機能します。



2. 必要に応じて、S3管理クライアントまたはテナントクライアントが別のサブネットからこれらのVIPアドレスにアクセスする場合は、*[ゲートウェイIPアドレス]*を入力します。ゲートウェイアドレスは VIP サブネット内に設定する必要があります。

   クライアントと管理者のユーザは、このゲートウェイを使用して仮想 IP アドレスにアクセスします。

3. HAグループ内のアクティブインターフェイスのVIPアドレスを1つ以上10個以下で入力します。すべてのVIPアドレスはVIPサブネット内に存在する必要があり、すべてがアクティブインターフェイス上で同時にアクティブになります。

   IPv4 アドレスを少なくとも 1 つ指定する必要があります。必要に応じて、追加の IPv4 アドレスと IPv6 アドレスを指定できます。

4. HA グループの作成 * を選択し、 * 完了 * を選択します。

   HA グループが作成され、設定済みの仮想 IP アドレスを使用できるようになります。

次のステップ

この HA グループをロードバランシングに使用する場合は、ロードバランサエンドポイントを作成してポートとネットワークプロトコルを決定し、必要な証明書を接続します。を参照して "ロードバランサエンドポイントを設定する"

ハイアベイラビリティグループを編集します

ハイアベイラビリティ（ HA ）グループを編集して、グループ名と概要 を変更したり、インターフェイスを追加または削除したり、優先順位を変更したり、仮想 IP アドレスを追加または更新したりできます。

たとえば、サイトまたはノードの運用停止手順 で、選択したインターフェイスに関連付けられているノード

を削除する場合、 HA グループの編集が必要になることがあります。

手順

1. 構成 > ネットワーク > *高可用性グループ*を選択します。

   ハイアベイラビリティグループページには、既存のすべての HA グループが表示されます。

2. 編集するHAグループのチェックボックスを選択します。
3. 更新する内容に基づいて、次のいずれかを実行します。
   - 仮想 IP アドレスを追加または削除するには、 * Actions * > * Edit virtual IP address * を選択します。
   - *Actions * > * Edit HA group * を選択して、グループ名または概要 を更新したり、インターフェイスを追加または削除したり、優先順位を変更したり、 VIP アドレスを追加または削除したりします。
4. [仮想 IP アドレスの編集 *] を選択した場合：
   a. HA グループの仮想 IP アドレスを更新します。
   b. [保存（ Save ）] を選択します。
   c. [完了] を選択します。
5. HA グループの編集 * を選択した場合：
   a. 必要に応じて、グループの名前または概要 を更新します。
   b. 必要に応じて、チェックボックスをオンまたはオフにしてインターフェイスを追加または削除します。

      HA グループが Grid Manager へのアクセスを提供する場合は、プライマリ管理ノード上のインターフェイスを選択してプライマリインターフェイスにする必要があります。一部のメンテナンス手順は、プライマリ管理ノードでしか実行できません

   c. 必要に応じて、行をドラッグして、このHAグループのプライマリインターフェイスとバックアップインターフェイスの優先順位を変更します。
   d. 必要に応じて、仮想 IP アドレスを更新します。
   e. [保存（ Save ）] を選択し、 [完了（ Finish ）] を選択します。

ハイアベイラビリティグループを削除する

ハイアベイラビリティ（ HA ）グループは一度に 1 つ以上削除できます。

ロードバランサエンドポイントにバインドされているHAグループは削除できません。HAグループを削除するには、そのグループを使用しているすべてのロードバランサエンドポイントからそのグループを削除する必要があります。

クライアントの中断を防ぐには、HAグループを削除する前に、該当するS3クライアントアプリケーションを更新してください。各クライアントを更新して、別の IP アドレスを使用して接続します。たとえば、別の HA グループの仮想 IP アドレスや、インストール時にインターフェイスに設定された IP アドレスなどです。

手順

1. 構成 > ネットワーク > *高可用性グループ*を選択します。

2. 削除する各HAグループの*[ロードバランサエンドポイント]*列を確認します。ロードバランサエンドポイントが表示されている場合：

   a. 構成 > ネットワーク > ロードバランサーエンドポイント に移動します。

   b. エンドポイントのチェックボックスを選択します。

   c. [* アクション * （ Actions * ）] > [* エンドポイントバインドモードの編集（ Edit Endpoint binding mode ）]

   d. バインドモードを更新してHAグループを削除します。

   e. 「変更を保存」を選択します。

3. ロードバランサエンドポイントが表示されない場合は、削除する各HAグループのチェックボックスを選択します。

4. >[HAグループの削除]*を選択します。

5. メッセージを確認し、「 * HA グループを削除」を選択して選択を確認します。

   選択したすべての HA グループが削除されます。ハイアベイラビリティグループのページに、成功を示す緑色のバナーが表示されます。

負荷分散の管理

StorageGRID ロード バランシングについて学ぶ

ロードバランシングを使用して、S3クライアントからの取り込みと読み出しのワークロードを処理できます。

ロードバランシングとは何ですか？

クライアントアプリケーションがStorageGRID システムでデータを保存または取得する際、StorageGRID はロードバランサを使用して取り込みと読み出しのワークロードを管理します。ロードバランシングは、複数のストレージノードにワークロードを分散することで、速度と接続容量を最大化します。

StorageGRID ロードバランササービスはすべての管理ノードとすべてのゲートウェイノードにインストールされ、レイヤ 7 のロードバランシングを提供します。クライアント要求の Transport Layer Security （ TLS ）終了を実行し、要求を検査し、ストレージノードへの新しいセキュアな接続を確立します。

各ノード上のロードバランササービスは、クライアントトラフィックをストレージノードに転送する際に独立して動作します。重み付きのプロセスを使用すると、ロードバランササービスは、より多くの要求をより多くの CPU を使用可能なストレージノードにルーティングします。

> 推奨される負荷分散メカニズムとしてはStorageGRID Load Balancer サービスがありますが、代わりにサードパーティのロード バランサを統合することもできます。詳細については、NetAppのアカウント担当者にお問い合わせいただくか、 "StorageGRIDでサードパーティのロードバランサーを使用する"。

必要なロードバランシングノードの数

一般的なベストプラクティスとして、 StorageGRID システムの各サイトにロードバランササービスを使用するノードが 2 つ以上必要です。たとえば、サイトに 2 つのゲートウェイノード、または管理ノードとゲートウェイノードの両方が含まれているとします。サービスアプライアンス、ベアメタルノード、仮想マシン

（VM）ベースのノードのいずれを使用する場合でも、各ロードバランシングノードに適切なネットワーク、ハードウェア、または仮想化インフラがあることを確認します。

ロードバランサエンドポイントとは何ですか？

ロードバランサエンドポイントは、ロードバランササービスを含むノードへのアクセスに送受信クライアントアプリケーション要求が使用するポートとネットワークプロトコル（HTTPSまたはHTTP）を定義します。また、クライアントタイプ（S3）、バインドモード、および許可またはブロックされたテナントのリスト（オプション）も定義します。

ロード バランサ エンドポイントを作成するには、Grid Manager を使用するか、S3 セットアップ ウィザードとFabricPoolウィザードを完了します。

- "ロードバランサエンドポイントを設定する"
- "S3セットアップウィザードを使用します"
- "FabricPool セットアップウィザードを使用します"

ロードバランサのキャッシュに関する考慮事項

キャッシュにより、ワークロードがデータのサブセットで動作し、オブジェクトに複数回アクセスする場合のパフォーマンスが大幅に向上します。さらに、キャッシュにより、完全なグリッド展開を行わなくてもオブジェクト ストレージへのリモート アクセスが可能になります。ロード バランサ キャッシュはゲートウェイ ノードでのみ使用できます。

ロードバランサーのエンドポイントを作成するときは、次の操作を行います。

- キャッシュ可能なワークロードに対してのみキャッシュを有効にします。キャッシュされたデータよりもキャッシュされていないデータに頻繁にアクセスするワークロードは、キャッシュによって処理されなかった場合よりもパフォーマンスが低下します。場合によっては、上書き率や削除率の高いワークロードが、保証されているドライブ書き込み耐久性を超えることもあります。
- キャッシュに適した個々のワークロードをキャッシュするために、追加のエンドポイントまたはノードを追加することを検討してください。
- キャッシュ可能なワークロードとキャッシュ不可能なワークロードには、異なるエンドポイントを使用します。この分離により、キャッシュ メカニズムが適切に適用され、キャッシュ不可能なデータ処理に干渉することがなくなります。
- キャッシュ対応エンドポイントに送信することで、潜在的なキャッシュ可能なワークロードを評価します。キャッシュヒット率を監視および検証して、キャッシュのワークロードの適合性を判断します。この評価は、パフォーマンスを最適化し、キャッシュ リソースを効率的に使用するのに役立ちます。
- "監査ログを確認します"既存のワークロードがキャッシュに適しているかどうかを判断します。指定された期間における、一意のオブジェクトに対する GET の割合を決定します。キャッシュに適するには、この値は 50% 未満である必要があります。

キャッシュに適したワークロードの例

- データレイク
- 高性能コンピューティング（HPC）
- AI/MLトレーニング
- コンテンツ配信ネットワーク（CDN）

- メディア資産管理
- ビデオ制作

> - 複数のオブジェクト バージョンをキャッシュできます。
> - 範囲読み取り操作がサポートされています。

キャッシュに適さないワークロードの例

- Fabric Pool
- バックアップアプリケーション
- ストレージ階層化

> キャッシュで提供されるコンテンツが保存時に暗号化を必要とする場合、 "ノードまたはドライブの暗号化を有効にする"キャッシュノード上。

キャッシュされないオブジェクトとリクエストの種類

- その `response-content-encoding`クエリパラメータ
- その `partNumber`クエリパラメータ
- 条件付きヘッダー
  - `If-Match`
  - `If-Modified-Since`
  - `If-None-Match`
  - `If-Unmodified-Since`
- 次のいずれかを使用して保存時に暗号化されたリクエスト:
  - SSE (StorageGRID管理キーによるサーバー側暗号化)
  - SSE-C（顧客提供のキーによるサーバー側暗号化）
  - 格納オブジェクトの暗号化

キャッシュされていないリクエストは、キャッシュが有効になっていないかのように上流の LDR に転送されます。

関連情報

- "ロードバランサのキャッシュのトラブルシューティング"
- ロード バランサー キャッシュの詳細については、テクニカル サポートにお問い合わせください。

ポートに関する考慮事項

ロードバランサエンドポイントのポートは、最初に作成するエンドポイントのデフォルトで10433になりますが、未使用の外部ポートを1~65535の範囲で指定できます。ポート80または443を使用する場合、エンドポイントはゲートウェイノード上のロードバランササービスのみを使用します。これらのポートは管理ノードで予約されています。複数のエンドポイントに同じポートを使用する場合は、エンドポイントごとに異なるバインディングモードを指定する必要があります。

他のグリッド サービスによって使用されるポートは許可されません。見る"StorageGRID の内部ポート" 。

ネットワークプロトコルに関する考慮事項

ほとんどの場合、クライアントアプリケーションとStorageGRID の間の接続では、Transport Layer Security（TLS）暗号化を使用する必要があります。TLS暗号化を使用せずにStorageGRID に接続することはサポートされていますが、特に本番環境では推奨されません。StorageGRID ロードバランサエンドポイントのネットワークプロトコルを選択する場合は、*[HTTPS]*を選択する必要があります。

ロードバランサエンドポイント証明書に関する考慮事項

ロードバランサエンドポイントのネットワークプロトコルとして* HTTPS *を選択した場合は、セキュリティ証明書を指定する必要があります。ロードバランサエンドポイントの作成時には、次の3つのオプションのいずれかを使用できます。

- 署名済み証明書をアップロードする（推奨）。この証明書には、公的に信頼された認証局または民間の認証局（CA）が署名できます。一般に信頼されているCAサーバ証明書を使用して接続を保護することを推奨します。生成される証明書とは異なり、CAによって署名された証明書は無停止でローテーションでき、有効期限の問題を回避できます。

  ロードバランサエンドポイントを作成する前に、次のファイルを入手する必要があります。

  - カスタムサーバ証明書ファイル。
  - カスタムサーバ証明書の秘密鍵ファイル。
  - 必要に応じて、各中間発行認証局の証明書のCAバンドル。
- 自己署名証明書の生成。
- グローバル**StorageGRID S3**証明書を使用します。この証明書をロードバランサエンドポイント用に選択するには、事前にこの証明書のカスタムバージョンをアップロードまたは生成する必要があります。を参照して "S3 API証明書の設定"

どのような価値が必要か？

証明書を作成するには、S3クライアントアプリケーションがエンドポイントへのアクセスに使用するすべてのドメイン名とIPアドレスを把握しておく必要があります。

証明書の*サブジェクトDN *（識別名）エントリには、クライアントアプリケーションがStorageGRID に使用する完全修飾ドメイン名が含まれている必要があります。例：

```
Subject DN:
/C=Country/ST=State/O=Company,Inc./CN=s3.storagegrid.example.com
```

必要に応じて、ワイルドカードを使用して、ロードバランササービスを実行しているすべての管理ノードおよびゲートウェイノードの完全修飾ドメイン名を表すことができます。たとえば、は `*.storagegrid.example.com`ワイルドカード*を使用してとを `gn1.storagegrid.example.com` 表します `adm1.storagegrid.example.com`。

S3仮想ホスト型リクエストを使用する予定の場合は、ワイルドカード名を含め、設定済みのすべての"S3エンドポイントのドメイン名"に対する*代替名*エントリも証明書に含まれている必要があります。例えば：

```
Alternative Name: DNS:*.s3.storagegrid.example.com
```

ドメイン名にワイルドカードを使用する場合は、を参照してください"サーバ証明書のセキュリティ強化ガイドライン"。

また、セキュリティ証明書の名前ごとにDNSエントリを定義する必要があります。

期限切れになる証明書の管理方法を教えてください。

S3アプリケーションとStorageGRID 間の接続の保護に使用した証明書の有効期限が切れると、アプリケーションからStorageGRID に一時的にアクセスできなくなる可能性があります。

証明書の有効期限の問題を回避するには、次のベストプラクティスに従ってください。

- 証明書の有効期限が近づいていることを警告するアラート（* Expiration of load balancer endpoint certificate や Expiration of global server certificate for S3 API *アラートなど）を注意深く監視します。
- StorageGRID アプリケーションとS3アプリケーションの証明書のバージョンは常に同期しておいてください。ロードバランサエンドポイントに使用する証明書を交換または更新する場合は、S3アプリケーションで使用される同等の証明書を交換または更新する必要があります。
- 公開署名されたCA証明書を使用する。CAによって署名された証明書を使用する場合は、有効期限が近い証明書を無停止で交換できます。
- 自己署名StorageGRID 証明書を生成した証明書の有効期限が近づいている場合は、既存の証明書の有効期限が切れる前に、StorageGRID とS3アプリケーションの両方で証明書を手動で置き換える必要があります。

バインディングモードに関する考慮事項

バインディングモードでは、ロードバランサエンドポイントへのアクセスに使用できるIPアドレスを制御できます。エンドポイントがバインディングモードを使用している場合、クライアントアプリケーションは、許可されたIPアドレスまたはそれに対応するFully Qualified Domain Name（FQDN；完全修飾ドメイン名）を使用している場合にのみ、エンドポイントにアクセスできます。他のIPアドレスまたはFQDNを使用するクライアントアプリケーションはエンドポイントにアクセスできません。

次のいずれかのバインディングモードを指定できます。

- グローバル（デフォルト）：クライアントアプリケーションは、任意のゲートウェイノードまたは管理ノードのIPアドレス、任意のネットワーク上の任意のHAグループの仮想IP（VIP）アドレス、または対応するFQDNを使用してエンドポイントにアクセスできます。エンドポイントのアクセスを制限する必要がないかぎり、この設定を使用します。
- * HAグループの仮想IP *。クライアントアプリケーションは、HAグループの仮想IPアドレス（または対応するFQDN）を使用する必要があります。
- ノードインターフェイス。クライアントは、選択したノードインターフェイスのIPアドレス（または対応するFQDN）を使用する必要があります。
- ノードタイプ。選択したノードのタイプに基づいて、クライアントは管理ノードのIPアドレス（または対応するFQDN）またはゲートウェイノードのIPアドレス（または対応するFQDN）のいずれかを使用する必要があります。

テナントアクセスに関する考慮事項

テナントアクセスは、ロードバランサエンドポイントを使用してバケットにアクセスできるStorageGRID テナントアカウントを制御できるオプションのセキュリティ機能です。すべてのテナントにエンドポイントへのアクセスを許可するか（デフォルト）、各エンドポイントで許可またはブロックされたテナントのリストを指定できます。

この機能を使用すると、テナントとそのエンドポイント間のセキュリティをより適切に分離できます。たとえば、この機能を使用して、あるテナントが所有する最高機密または高度に機密性の高いマテリアルに他のテナントから完全にアクセスできないようにすることができます。

> アクセス制御の目的では、クライアント要求で使用されたアクセスキーからテナントが決定されます。要求の一部としてアクセスキーが提供されていない場合（匿名アクセスなど）は、バケット所有者を使用してテナントが決定されます。

テナントアクセスの例

このセキュリティ機能の仕組みを理解するには、次の例を参考にしてください。

1. 次の2つのロードバランサエンドポイントを作成しておきます。
   - *パブリック*エンドポイント：ポート10443を使用し、すべてのテナントへのアクセスを許可します。
   - * Top secret * endpoint：ポート10444を使用し、* Top secret *テナントにのみアクセスを許可します。他のすべてのテナントはこのエンドポイントへのアクセスをブロックされます。
2. は `top-secret.pdf`、* Top secret *テナントが所有するバケット内にあります。

にアクセスするには `top-secret.pdf`、* Top secret *テナント内のユーザがにGET要求を発行できます `https://w.x.y.z:10444/top-secret.pdf`。このテナントには10444エンドポイントの使用が許可されているため、ユーザはオブジェクトにアクセスできます。ただし、他のテナントに属するユーザが同じURLに対して同じ要求を発行すると、すぐに「Access Denied」というメッセージが表示されます。クレデンシャルと署名が有効であってもアクセスは拒否されます。

CPU の可用性

S3トラフィックをストレージノードに転送する際、各管理ノードとゲートウェイノード上のロードバランササービスは独立して動作します。重み付きのプロセスを使用すると、ロードバランササービスは、より多くの要求をより多くの CPU を使用可能なストレージノードにルーティングします。ノード CPU 負荷情報は数分ごとに更新されますが、重み付けがより頻繁に更新される場合があります。ノードの使用率が 100% になった場合や、ノードの利用率のレポートに失敗した場合でも、すべてのストレージノードには最小限のベースとなる重みの値が割り当てられます。

CPU の可用性に関する情報が、ロードバランササービスが配置されているサイトに制限されている場合があります。

StorageGRIDロード バランサ エンドポイントを設定します

ロードバランサエンドポイントは、S3クライアントがゲートウェイノードと管理ノード上のStorageGRIDロードバランサに接続するときに使用できるポートとネットワークプロトコルを決定します。エンドポイントを使用してGrid Manager、Tenant Manager、またはその両方にアクセスすることもできます。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"rootアクセス権限"。
- を確認しておきます"ロードバランシングに関する考慮事項"。
- ロードバランサエンドポイントに使用するポートを再マッピングしておく必要があります"ポートの再マッピングを削除しました"。
- 使用するハイアベイラビリティ（ HA ）グループを作成しておきます。HA グループを推奨しますが、必須ではありません。を参照して "ハイアベイラビリティグループを管理します"
- ロードバランサエンドポイントをで使用する場合"S3 Select 用の S3 テナント"、ベアメタルノードのIPアドレスまたはFQDNを使用することはできません。S3 Selectに使用されるロードバランサエンドポイントには、サービスアプライアンスとVMwareベースのソフトウェアノードのみが許可されます。
- 使用する VLAN インターフェイスを設定しておきます。を参照して "VLAN インターフェイスを設定します"
- HTTPS エンドポイントを作成する場合（推奨）は、サーバ証明書の情報が必要です。

> ⓘ エンドポイント証明書の変更がすべてのノードに適用されるまでに最大 15 分かかることがあります。

  - 証明書をアップロードするには、サーバ証明書、証明書の秘密鍵、および必要に応じて CA バンドルが必要です。
  - 証明書を生成するには、S3クライアントがエンドポイントへのアクセスに使用するすべてのドメイン名とIPアドレスが必要です。また、件名（識別名）も知っている必要があります。
  - StorageGRID S3 API証明書（ストレージノードへの直接接続にも使用可能）を使用する場合は、デフォルトの証明書を外部の認証局によって署名されたカスタム証明書に置き換えておきます。を参照して "S3 API証明書の設定"

ロードバランサエンドポイントを作成します

各 S3 クライアント ロード バランサ エンドポイントは、ポート、クライアント タイプ (S3)、およびネットワーク プロトコル (HTTP または HTTPS) を指定します。管理インターフェイス ロード バランサ エンドポイントは、ポート、インターフェイス タイプ、および信頼できないクライアント ネットワークを指定します。

ウィザードにアクセスします

手順

1. 構成 > ネットワーク > *ロードバランサーエンドポイント*を選択します。
2. S3 クライアントのエンドポイントを作成するには、**S3** クライアント タブを選択します。
3. Grid Manager、Tenant Manager、またはその両方にアクセスするためのエンドポイントを作成するには、*[Management interface]*タブを選択します。
4. 「 * Create * 」を選択します。

エンドポイントの詳細を入力します

手順

1. 適切な手順を選択して、作成するエンドポイントのタイプの詳細を入力します。

S3 クライアント

フィールド	製品説明
名前	エンドポイントのわかりやすい名前。ロードバランサエンドポイントのページのテーブルに表示されます。
ポート	ロードバランシングに使用する StorageGRID ポート。最初に作成するエンドポイントのデフォルトは10433ですが、未使用の外部ポート（1～65535）を入力できます。 「* 80 」または「 8443 *」と入力した場合、ポート8443を解放していないかぎり、エンドポイントはゲートウェイノードにのみ設定されます。次に、ポート8443をS3エンドポイントとして使用すると、ゲートウェイノードと管理ノードの両方でポートが設定されます。 "グローバル名前空間"のロードバランサーエンドポイントを設定する場合は、各エンドポイントに同じポートを使用してください。
クライアントタイプ	は* S3 *にする必要があります。
ネットワークプロトコル	クライアントがこのエンドポイントに接続するときに使用するネットワークプロトコル。 • セキュアな TLS 暗号化通信を実現するには、「 * HTTPS * 」を選択します（推奨）。エンドポイントを保存するには、セキュリティ証明書を接続する必要があります。 • セキュアで暗号化されていない通信を行うには、「 * HTTP 」を選択します非本番環境のグリッドにのみ HTTP を使用してください。
キャッシュを有効にする	有効または無効にする"ゲートウェイノードでのキャッシュ"このロードバランサエンドポイント用。 キャッシュに問題がある場合は、"ロードバランサのキャッシュのトラブルシューティング" 。

管理インターフェイス

フィールド	製品説明
名前	エンドポイントのわかりやすい名前。ロードバランサエンドポイントのページのテーブルに表示されます。

フィールド	製品説明
ポート	Grid Manager、Tenant Manager、またはその両方へのアクセスに使用するStorageGRIDポート。 • Grid Manager：* 8443* • Tenant Manager：* 9443 * • Grid ManagerとTenant Managerの両方：* 443 * 注：これらのプリセットポートまたは他の使用可能なポートを使用できます。
インターフェイスタイプ	このエンドポイントを使用してアクセスするStorageGRIDインターフェイスのラジオボタンを選択します。
Untrusted Client Networkの略	このエンドポイントに信頼されていないクライアントネットワークからアクセスできるようにする場合は、**[**はい**]***を選択します。それ以外の場合は、No *を選択します。 [はい]*を選択すると、信頼されていないすべてのクライアントネットワークでポートが開いています。 注：ロードバランサエンドポイントの作成時に、信頼されていないクライアントネットワークに対してポートを開いたり閉じたりするように設定できます。

1. 「 * Continue * 」を選択します。

綴じモードを選択します

手順

1. 任意のIPアドレスまたは特定のIPアドレスとネットワークインターフェイスを使用してエンドポイントへのアクセス方法を制御するには、エンドポイントのバインドモードを選択します。

   一部のバインディングモードは、クライアントエンドポイントまたは管理インターフェイスエンドポイントで使用できます。両方のエンドポイントタイプのすべてのモードをここに示します。

モード	製品説明
グローバル（クライアントエンドポイントのデフォルト）	クライアントは、任意のゲートウェイノードまたは管理ノードのIPアドレス、任意のネットワーク上の任意のHAグループの仮想IP（VIP）アドレス、または対応するFQDNを使用して、エンドポイントにアクセスできます。 このエンドポイントのアクセスを制限する必要がないかぎり、*グローバル*設定を使用してください。

モード	製品説明
HA グループの仮想 IP	クライアントがこのエンドポイントにアクセスするには、HAグループの仮想IPアドレス（または対応するFQDN）を使用する必要があります。 このバインドモードのエンドポイントでは、エンドポイント用に選択したHAグループが重複しないかぎり、すべて同じポート番号を使用できます。
ノードインターフェイス	クライアントがこのエンドポイントにアクセスするには、選択したノードインターフェイスのIPアドレス（または対応するFQDN）を使用する必要があります。
ノードタイプ（クライアントエンドポイントのみ）	選択したノードのタイプに基づいて、クライアントがこのエンドポイントにアクセスするには、いずれかの管理ノードのIPアドレス（または対応するFQDN）か、いずれかのゲートウェイノードのIPアドレス（または対応するFQDN）を使用する必要があります。
すべての管理ノード（管理インターフェイスエンドポイントのデフォルト）	クライアントがこのエンドポイントにアクセスするには、いずれかの管理ノードのIPアドレス（または対応するFQDN）を使用する必要があります。

複数のエンドポイントが同じポートを使用する場合、StorageGRID はこの優先順位に従って、使用するエンドポイントを決定します。* HAグループの仮想IP **>***ノードインターフェイス>*ノードタイプ*>*グローバル*。

管理インターフェイスエンドポイントを作成する場合は、管理ノードのみが許可されます。

2. HA グループの仮想 IP * を選択した場合は、 1 つ以上の HA グループを選択します。

   管理インターフェイスエンドポイントを作成する場合は、管理ノードにのみ関連付けられているVIPを選択します。

3. ノードインターフェイス * を選択した場合は、このエンドポイントに関連付ける管理ノードまたはゲートウェイノードごとに 1 つ以上のノードインターフェイスを選択します。
4. [ノードタイプ]*を選択した場合は、プライマリ管理ノードと非プライマリ管理ノードの両方を含む管理ノードまたはゲートウェイノードのいずれかを選択します。

テナントアクセスを制御

> 管理インターフェイスエンドポイントは、エンドポイントにが設定されている場合にのみテナントアクセスを制御できTenant Managerのインターフェイスタイプます。

手順

1. [Tenant access]*ステップで、次のいずれかを選択します。

フィールド	製品説明
Allow all tenants（デフォルト）	すべてのテナントアカウントは、このエンドポイントを使用してバケットにアクセスできます。 テナントアカウントをまだ作成していない場合は、このオプションを選択する必要があります。テナントアカウントを追加したら、ロードバランサエンドポイントを編集して特定のアカウントを許可またはブロックできます。
選択したテナントを許可します	このエンドポイントを使用してバケットにアクセスできるのは、選択したテナントアカウントのみです。
選択したテナントをブロックします	選択したテナントアカウントは、このエンドポイントを使用してバケットにアクセスできません。他のすべてのテナントでこのエンドポイントを使用できます。

2. * HTTP *エンドポイントを作成する場合は、証明書を添付する必要はありません。Create * を選択して、新しいロードバランサエンドポイントを追加します。次に、に進みます終了後。それ以外の場合は、「 * Continue * 」を選択して証明書を添付します。

証明書を添付します

手順

1. * HTTPS * エンドポイントを作成する場合は、エンドポイントに接続するセキュリティ証明書のタイプを選択します。

   この証明書は、S3クライアントと管理ノードまたはゲートウェイノード上のロードバランササービスの間の接続を保護します。

   - * 証明書のアップロード * 。アップロードするカスタム証明書がある場合は、このオプションを選択します。
   - * 証明書の生成 * 。カスタム証明書の生成に必要な値がある場合は、このオプションを選択します。
   - * StorageGRID S3証明書を使用*。ストレージノードへの直接接続にも使用できるグローバルS3 API証明書を使用する場合は、このオプションを選択します。

     グリッドCAによって署名されたデフォルトのS3 API証明書を外部の認証局によって署名されたカスタム証明書に置き換えていないかぎり、このオプションは選択できません。を参照して "S3 API証明書の設定"

   - 管理インターフェイス証明書を使用。管理ノードへの直接接続にも使用できるグローバル管理インターフェイス証明書を使用する場合は、このオプションを選択します。
2. StorageGRID S3証明書を使用しない場合は、証明書をアップロードまたは生成します。

証明書をアップロードする

a. [証明書のアップロード] を選択します。

b. 必要なサーバ証明書ファイルをアップロードします。

- * サーバ証明書 * ： PEM エンコードのカスタムサーバ証明書ファイル。
- 証明書の秘密鍵：カスタムサーバ証明書の秘密鍵ファイル(`.key`）。

> EC 秘密鍵は 224 ビット以上にする必要があります。RSA 秘密鍵は 2048 ビット以上にする必要があります。

- **CA Bundle** ：各中間発行認証局（ CA ）の証明書を含む単一のオプションファイル。このファイルには、PEMでエンコードされた各CA証明書ファイルが、証明書チェーンの順序で連結されている必要があります。

c. [* 証明書の詳細 *] を展開して、アップロードした各証明書のメタデータを表示します。オプションの CA バンドルをアップロードした場合は、各証明書が独自のタブに表示されます。

- 証明書ファイルを保存するには、 * 証明書のダウンロード * を選択します。証明書バンドルを保存するには、 * CA バンドルのダウンロード * を選択します。

  証明書ファイルの名前とダウンロード先を指定します。拡張子を付けてファイルを保存します `.pem`。

  例： `storagegrid_certificate.pem`

- 証明書の内容をコピーして他の場所に貼り付けるには、 * 証明書の PEM のコピー * または * CA バンドル PEM のコピー * を選択してください。

d. 「 * Create * 」を選択します。+ ロードバランサエンドポイントが作成された。カスタム証明書は、S3クライアントまたは管理インターフェイスとエンドポイントの間の以降のすべての新規接続に使用されます。

証明書の生成

a. [* 証明書の生成 *] を選択します。

b. 証明書情報を指定します。

フィールド	製品説明
ドメイン名	証明書に含める1つ以上の完全修飾ドメイン名。複数のドメイン名を表すには、ワイルドカードとして * を使用します。
IP	証明書に含める1つ以上のIPアドレス。
件名（オプション）	証明書所有者のX.509サブジェクト名または識別名（DN）。 このフィールドに値を入力しない場合、生成される証明書では、最初のドメイン名またはIPアドレスがサブジェクト共通名（CN）として使用されます。

フィールド	製品説明
有効な日数	作成後に証明書の有効期限が切れる日数。
キー使用の拡張機能を追加します	選択されている場合（デフォルトおよび推奨）、キー使用と拡張キー使用拡張が生成された証明書に追加されます。 これらの拡張機能は、証明書に含まれるキーの目的を定義します。 注:証明書にこれらの拡張機能が含まれている場合、古いクライアントで接続の問題が発生する場合を除き、このチェックボックスをオンのままにします。

c. [*Generate （生成）] を選択します

d. 生成された証明書のメタデータを表示するには、 [証明書の詳細] を選択します。

- 証明書ファイルを保存するには、 [証明書のダウンロード] を選択します。

  証明書ファイルの名前とダウンロード先を指定します。拡張子を付けてファイルを保存します `.pem`。

  例： `storagegrid_certificate.pem`

- 証明書の内容をコピーして他の場所に貼り付けるには、 * 証明書の PEM をコピー * を選択します。

e. 「 * Create * 」を選択します。

ロードバランサエンドポイントが作成されます。カスタム証明書は、S3クライアントまたは管理インターフェイスとこのエンドポイントの間の以降のすべての新規接続に使用されます。

終了後

手順

1. DNSを使用する場合は、クライアントが接続に使用する各IPアドレスにStorageGRID の完全修飾ドメイン名（FQDN）を関連付けるレコードがDNSに含まれていることを確認します。

   DNS レコードに入力する IP アドレスは、負荷分散ノードの HA グループを使用しているかどうかによって異なります。

   - HAグループを設定した場合、クライアントはそのHAグループの仮想IPアドレスに接続します。
   - HAグループを使用しない場合、クライアントはゲートウェイノードまたは管理ノードのIPアドレスを使用してStorageGRID ロードバランササービスに接続します。

     また、 DNS レコードが、ワイルドカード名を含む、必要なすべてのエンドポイントドメイン名を参照していることを確認する必要があります。

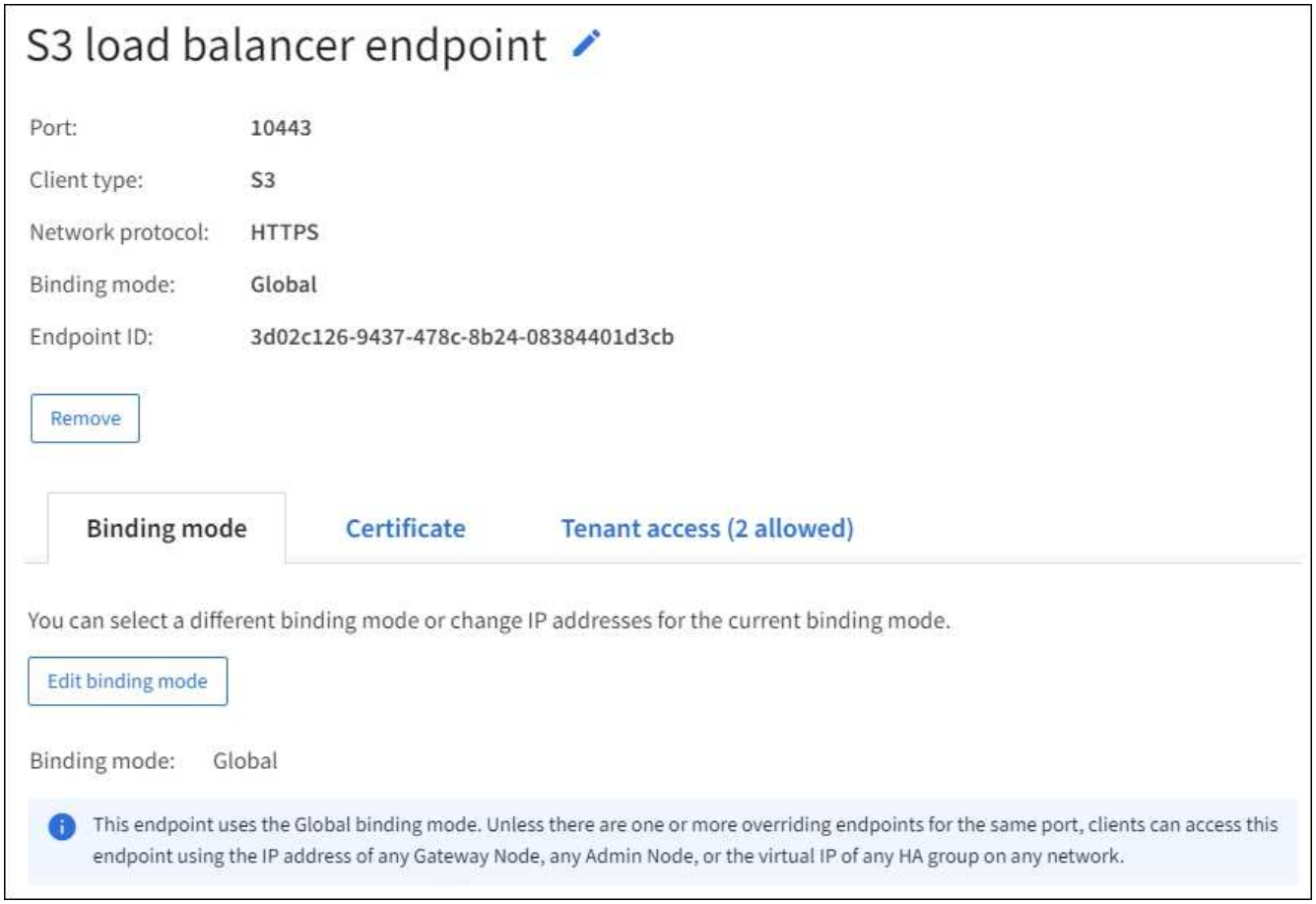
2. エンドポイントへの接続に必要な情報をS3クライアントに提供します。

- ポート番号
- 完全修飾ドメイン名または IP アドレス
- 必要な証明書の詳細

ロードバランサエンドポイントを表示および編集します

既存のロードバランサエンドポイントの詳細を表示できます。これには、セキュアなエンドポイントの証明書メタデータも含まれます。エンドポイントの特定の設定を変更できます。

- すべてのロードバランサエンドポイントの基本情報を表示するには、[Load balancer Endpoints]ページのテーブルを確認します。
- 証明書メタデータを含む、特定のエンドポイントに関するすべての詳細を表示するには、テーブルでエンドポイントの名前を選択します。表示される情報は、エンドポイントのタイプとその設定方法によって異なります。



- エンドポイントを編集するには、[Load balancer Endpoints]ページの*[Actions]*メニューを使用します。

管理インターフェイスエンドポイントのポートの編集中にGrid Managerへのアクセスが失われた場合は、URLとポートを更新してアクセスを回復してください。

エンドポイントの編集後、変更がすべてのノードに適用されるまでに最大 15 分かかる場合があります。

タスク	**[Actions]**メニュー	詳細ページ
エンドポイント名を編集します	a. エンドポイントのチェックボックスを選択します。 b. [* アクション * > * エンドポイント名の編集 *] を選択します。 c. 新しい名前を入力します。 d. [保存（ Save ）] を選択します。	a. エンドポイント名を選択して詳細を表示します。 b. 編集アイコン を選択します。 c. 新しい名前を入力します。 d. [保存（ Save ）] を選択します。
エンドポイントポートの編集	a. エンドポイントのチェックボックスを選択します。 b. **>**[Edit endpoint port]*を選択します。 c. 有効なポート番号を入力してください。 d. [保存（ Save ）] を選択します。	*n/a*
エンドポイントバインドモードを編集します	a. エンドポイントのチェックボックスを選択します。 b. [* アクション * （ Actions * ）] > [* エンドポイントバインドモードの編集（ Edit Endpoint binding mode ）] c. 必要に応じて、バインドモードを更新します。 d. 「変更を保存」を選択します。	a. エンドポイント名を選択して詳細を表示します。 b. 「 * バインドモードを編集」を選択します。 c. 必要に応じて、バインドモードを更新します。 d. 「変更を保存」を選択します。
エンドポイント証明書を編集します	a. エンドポイントのチェックボックスを選択します。 b. [* アクション * > * エンドポイント証明書の編集 *] を選択します。 c. 必要に応じて、新しいカスタム証明書をアップロードまたは生成するか、グローバルS3証明書の使用を開始します。 d. 「変更を保存」を選択します。	a. エンドポイント名を選択して詳細を表示します。 b. [* 証明書 *] タブを選択します。 c. [証明書の編集] を選択します。 d. 必要に応じて、新しいカスタム証明書をアップロードまたは生成するか、グローバルS3証明書の使用を開始します。 e. 「変更を保存」を選択します。

タスク	[Actions]メニュー	詳細ページ
テナントアクセスを編集します	a. エンドポイントのチェックボックスを選択します。 b. >[テナントアクセスの編集]*を選択します。 c. 別のアクセスオプションを選択するか、リストからテナントを選択または削除するか、またはその両方を実行します。 d. 「変更を保存」を選択します。	a. エンドポイント名を選択して詳細を表示します。 b. [テナントアクセス]*タブを選択します。 c. [テナントアクセスの編集]*を選択します。 d. 別のアクセスオプションを選択するか、リストからテナントを選択または削除するか、またはその両方を実行します。 e. 「変更を保存」を選択します。

ロードバランサエンドポイントを削除する

[* アクション * （ Actions * ）] メニューを使用して 1 つ以上のエンドポイントを削除するか、または詳細ページから 1 つのエンドポイントを削除できます。

クライアントの中断を防ぐには、ロードバランサエンドポイントを削除する前に、影響を受けるS3クライアントアプリケーションを更新してください。各クライアントを更新して、別のロードバランサエンドポイントに割り当てられたポートを使用して接続します。必要な証明書情報も必ず更新してください。

管理インターフェイスエンドポイントの削除中にGrid Managerへのアクセスが失われた場合は、URLを更新します。

- 1 つ以上のエンドポイントを削除するには、次の手順
  a. [Load balancer]ページで、削除する各エンドポイントのチェックボックスを選択します。
  b. * アクション * > * 削除 * を選択します。
  c. 「* OK *」を選択します。
- 詳細ページから 1 つのエンドポイントを削除します。
  a. [Load balancer]ページで、エンドポイント名を選択します。
  b. 詳細ページで「 * 削除」を選択します。
  c. 「* OK *」を選択します。

StorageGRIDで**S3**エンドポイントドメイン名を設定する

S3仮想ホスト形式の要求をサポートするには、Grid Managerを使用して、S3クライアントの接続先のS3エンドポイントのドメイン名のリストを設定する必要があります。

エンドポイントドメイン名にIPアドレスを使用することはできません。今後のリリースでは、この設定はできません。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- そうだな "特定のアクセス権限"
- グリッドのアップグレードが進行中でないことを確認します。

> グリッドのアップグレードの実行中は、ドメイン名の設定を変更しないでください。

タスクの内容

クライアントが S3 エンドポイントのドメイン名を使用できるようにするには、次の作業をすべて実行する必要があります。

- Grid Manager を使用して、 S3 エンドポイントのドメイン名を StorageGRID システムに追加します。
- クライアントが必要とするすべてのドメイン名に対してが署名されていることを確認します"クライアントがStorageGRID へのHTTPS接続に使用する証明書"。

  たとえば、エンドポイントがの場合は `s3.company.com`、HTTPS接続に使用される証明書にエンドポイントとエンドポイントのワイルドカードSubject Alternative Name（SAN）：が `*.s3.company.com`含まれていることを確認する必要があります `s3.company.com`。

- クライアントが使用する DNS サーバを設定します。クライアントが接続に使用するIPアドレスのDNSレコードを追加し、レコードが必要なすべてのS3エンドポイントのドメイン名（ワイルドカード名を含む）を参照していることを確認します。

> クライアントは、ゲートウェイノード、管理ノード、またはストレージノードの IP アドレスを使用するか、ハイアベイラビリティグループの仮想 IP アドレスに接続することで、StorageGRID に接続できます。DNS レコードに正しい IP アドレスを追加するためには、クライアントアプリケーションがグリッドに接続する方法を理解しておく必要があります。

グリッドへの HTTPS 接続を使用するクライアント（推奨）では、次のいずれかの証明書を使用できます。

- ロードバランサエンドポイントに接続するクライアントは、そのエンドポイント用のカスタム証明書を使用できます。各ロードバランサエンドポイントは、異なるS3エンドポイントのドメイン名を認識するように設定できます。
- ロードバランサエンドポイントに接続するクライアント、またはストレージノードに直接接続するクライアントは、必要なS3エンドポイントのドメイン名をすべて含めるようにグローバルS3 API証明書をカスタマイズできます。

> S3エンドポイントのドメイン名を追加せずにリストが空の場合、S3仮想ホスト形式の要求のサポートは無効になります。

S3エンドポイントのドメイン名を追加します

手順

1. 構成 > ネットワーク > **S3** エンドポイント ドメイン名 を選択します。
2. ドメイン名を* Domain name 1 フィールドに入力します。ドメイン名をさらに追加するには、[別のドメイン名を追加する]*を選択します。

3. [保存（ Save ）] を選択します。
4. クライアントが使用するサーバ証明書が、必要なS3エンドポイントのドメイン名と一致していることを確認します。
   - クライアントが独自の証明書を使用するロードバランサエンドポイントに接続する場合は、"エンドポイントに関連付けられている証明書を更新します"。
   - クライアントがグローバルS3 API証明書を使用するロードバランサエンドポイントに接続するか、またはストレージノードに直接接続する場合は、を"グローバルS3 API証明書の更新"実行します。
5. エンドポイントのドメイン名要求を解決するために必要な DNS レコードを追加します。

結果

これで、クライアントがエンドポイントを使用すると、 `*bucket.s3.company.com*`DNSサーバが正しいエンドポイントに解決され、証明書によってエンドポイントが認証されます。

S3エンドポイントのドメイン名を変更します

S3アプリケーションで使用されている名前を変更すると、仮想ホスト形式の要求は失敗します。

手順

1. 構成 > ネットワーク > **S3** エンドポイント ドメイン名 を選択します。
2. 編集するドメイン名フィールドを選択し、必要な変更を行います。
3. [保存（ Save ）] を選択します。
4. [はい]*を選択して変更を確定します。

S3エンドポイントのドメイン名を削除します

S3アプリケーションで使用されている名前を削除すると、仮想ホスト形式の要求は失敗します。

手順

1. 構成 > ネットワーク > **S3** エンドポイント ドメイン名 を選択します。
2. ドメイン名の横にある削除アイコン を選択します。
3. [はい]*を選択して削除を確定します。

関連情報

- "S3 REST APIを使用する"
- "IP アドレスを表示します"
- "ハイアベイラビリティグループを設定する"

StorageGRIDクライアント接続のIPアドレスとポート

S3クライアントアプリケーションは、オブジェクトの格納や読み出しを行うために、すべての管理ノードおよびゲートウェイノードに含まれるロードバランササービスまたはすべてのストレージノードに含まれるLocal Distribution Router（LDR）サービスに接続します。

クライアントアプリケーションは、グリッドノードのIPアドレスとそのノード上のサービスのポート番号を使用してStorageGRID に接続できます。必要に応じて、ロードバランシングノードのハイアベイラビリティ（HA）グループを作成して、仮想IP（VIP）アドレスを使用する可用性の高い接続を確立できます。IPアドレスまたはVIPアドレスの代わりに完全修飾ドメイン名（FQDN）を使用してStorageGRID に接続する場合は、DNSエントリを設定できます。

次の表に、クライアントが StorageGRID に接続できるさまざまな方法、および接続のタイプごとに使用される IP アドレスとポートを示します。ロードバランサエンドポイントとハイアベイラビリティ（HA）グループを作成済みの場合は、を参照してGrid Managerでこれらの値を確認してくださいIPアドレスの検索場所。

接続が確立される場所	クライアントが接続するサービス	IPアドレス	ポート
HAグループ	ロードバランサ	HA グループの仮想 IP アドレス	ロードバランサエンドポイントに割り当てられたポート
管理ノード	ロードバランサ	管理ノードの IP アドレス	ロードバランサエンドポイントに割り当てられたポート
ゲートウェイノード	ロードバランサ	ゲートウェイノードの IP アドレス	ロードバランサエンドポイントに割り当てられたポート
ストレージノード	LDR	ストレージノードの IP アドレス	デフォルトの S3 ポート： • HTTPS：18082 • HTTP：18084

URLの例

クライアントアプリケーションをゲートウェイノードのHAグループのロードバランサエンドポイントに接続するには、次の構造のURLを使用します。

```
https://VIP-of-HA-group:LB-endpoint-port
```

たとえば、HAグループの仮想IPアドレスが192.0.2.5で、ロードバランサエンドポイントのポート番号が10443の場合、アプリケーションは次のURLを使用してStorageGRID に接続できます。

```
https://192.0.2.5:10443
```

IPアドレスの検索場所

1. を使用してGrid Managerにサインインし"サポートされている Web ブラウザ"ます。
2. グリッドノードの IP アドレスを確認するには、次の手順を実行します。
   a. *ノード*を選択します。
   b. 接続する管理ノード、ゲートウェイノード、またはストレージノードを選択します。

c. [* Overview * （概要 * ）] タブを選択します。

d. Node Information セクションで、ノードの IP アドレスを確認します。

e. IPv6 アドレスとインターフェイスマッピングを表示するには、 * Show More * を選択します。

クライアントアプリケーションから、リスト内の任意の IP アドレスへの接続を確立できます。

- * eth0 ： * グリッドネットワーク
- * eth1 ： * 管理ネットワーク（オプション）
- * eth2 ： * クライアントネットワーク（オプション）

表示されている管理ノードまたはゲートウェイノードがハイアベイラビリティグループのアクティブノードである場合は、 HA グループの仮想 IP アドレスが eth2 に表示されます。

3. ハイアベイラビリティグループの仮想 IP アドレスを検索するには、次の手順を実行します。

a. 構成 > ネットワーク > *高可用性グループ*を選択します。

b. HA グループの仮想 IP アドレスを表で確認します。

4. ロードバランサエンドポイントのポート番号を確認するには、次の手順を実行します。

a. 構成 > ネットワーク > *ロードバランサーエンドポイント*を選択します。

b. 使用するエンドポイントのポート番号をメモします。

ポート番号が80または443の場合、エンドポイントはゲートウェイノードでのみ設定されます。これらのポートは管理ノードで予約されているためです。それ以外のポートはすべて、ゲートウェイノードと管理ノードの両方に設定されます。

c. テーブルからエンドポイントの名前を選択します。

d. [Client type]*（S3）がエンドポイントを使用するクライアントアプリケーションと一致していることを確認します。

ネットワークと接続を管理します

StorageGRIDネットワーク設定を設定する

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

VLAN インターフェイスを設定します

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

トラフィック分類ポリシー

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

StorageGRID ネットワークのガイドライン

グリッドマネージャを使用して、 StorageGRID のネットワークと接続を設定および管理できます。

S3クライアントの接続方法については、を参照してください"S3クライアント接続の設定"。

デフォルトの **StorageGRID** ネットワーク

StorageGRID では、デフォルトでグリッドノードあたり 3 つのネットワークインターフェイスがサポートされ、各グリッドノードのネットワークをセキュリティやアクセスの要件に応じて設定することができます。

ネットワークトポロジの詳細については、を参照してください"ネットワークのガイドライン"。

グリッドネットワーク

必須。グリッドネットワークは、すべての内部 StorageGRID トラフィックに使用されます。このネットワークによって、グリッド内のすべてのノードが、すべてのサイトおよびサブネットにわたって相互に接続されます。

管理ネットワーク

オプション。通常、管理ネットワークはシステムの管理とメンテナンスに使用されます。クライアントプロトコルアクセスにも使用できます。管理ネットワークは通常はプライベートネットワークであり、サイト間でルーティング可能にする必要はありません。

クライアントネットワーク

オプション。クライアントネットワークはオープンネットワークで、主にS3クライアントアプリケーションへのアクセスに使用されます。そのため、グリッドネットワークを分離してセキュリティを確保できます。クライアントネットワークは、ローカルゲートウェイ経由でアクセス可能なすべてのサブネットと通信できます。

ガイドライン

- StorageGRIDノードには、割り当て先のネットワークごとに専用のネットワークインターフェイス、IPアドレス、サブネットマスク、およびゲートウェイが必要です。
- 1つのグリッドノードに複数のインターフェイスを設定することはできません。
- 各ネットワークのグリッドノードごとに、単一のゲートウェイがサポートされます。このゲートウェイはノードと同じサブネット上に配置する必要があります。必要に応じて、より複雑なルーティングをゲートウェイに実装できます。
- 各ノードでは、各ネットワークが特定のネットワークインターフェイスにマッピングされます。

ネットワーク	インターフェイス名
グリッド	eth0
管理（オプション）	eth1
クライアント（オプション）	eth2

- ノードが StorageGRID アプライアンスに接続されている場合は、ネットワークごとに特定のポートが使用されます。詳細については、使用しているアプライアンスのインストール手順を参照してください。
- デフォルトルートはノードごとに自動的に生成されます。eth2 が有効な場合、 0.0.0.0/0 は eth2 のクライアントネットワークを使用します。eth2 が無効な場合、 0.0.0.0/0 は eth0 のグリッドネットワークを使用します。
- クライアントネットワークは、グリッドノードがグリッドに参加するまで動作状態になりません
- グリッドが完全にインストールされる前にインストールユーザインターフェイスにアクセスできるように、グリッドノード導入時に管理ネットワークを設定できます。

オプションのインターフェイス

必要に応じて、ノードにインターフェイスを追加できます。たとえば、管理ノードまたはゲートウェイノードにトランクインターフェイスを追加して、を使用して"VLANインターフェイス"異なるアプリケーションまたはテナントに属するトラフィックを分離できます。または、で使用するアクセスインターフェイスを追加することもできます"ハイアベイラビリティ（ HA ）グループ"。

トランクインターフェイスまたはアクセスインターフェイスを追加するには、次の項を参照してください。

- * VMware（ノードのインストール後）*："VMware ：ノードにトランクインターフェイスまたはアクセスインターフェイスを追加します"
  - **Linux (**ノードをインストールする前**)**:"ノード構成ファイルを作成"
  - **Linux (**ノードのインストール後**)**:"ノードにトランクまたはアクセスインターフェースを追加する"

「Linux」は、RHEL、Ubuntu、または Debian のデプロイメントを指します。サポートされているバージョンのリストについては、 "NetApp Interoperability Matrix Tool（IMT）" 。

StorageGRIDで**IP**アドレスを表示する

StorageGRID システムの各グリッドノードの IP アドレスを表示できます。その後、このIPアドレスを使用してコマンドラインでグリッドノードにログインし、さまざまなメンテナンス手順を実行できます。

開始する前に

Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。

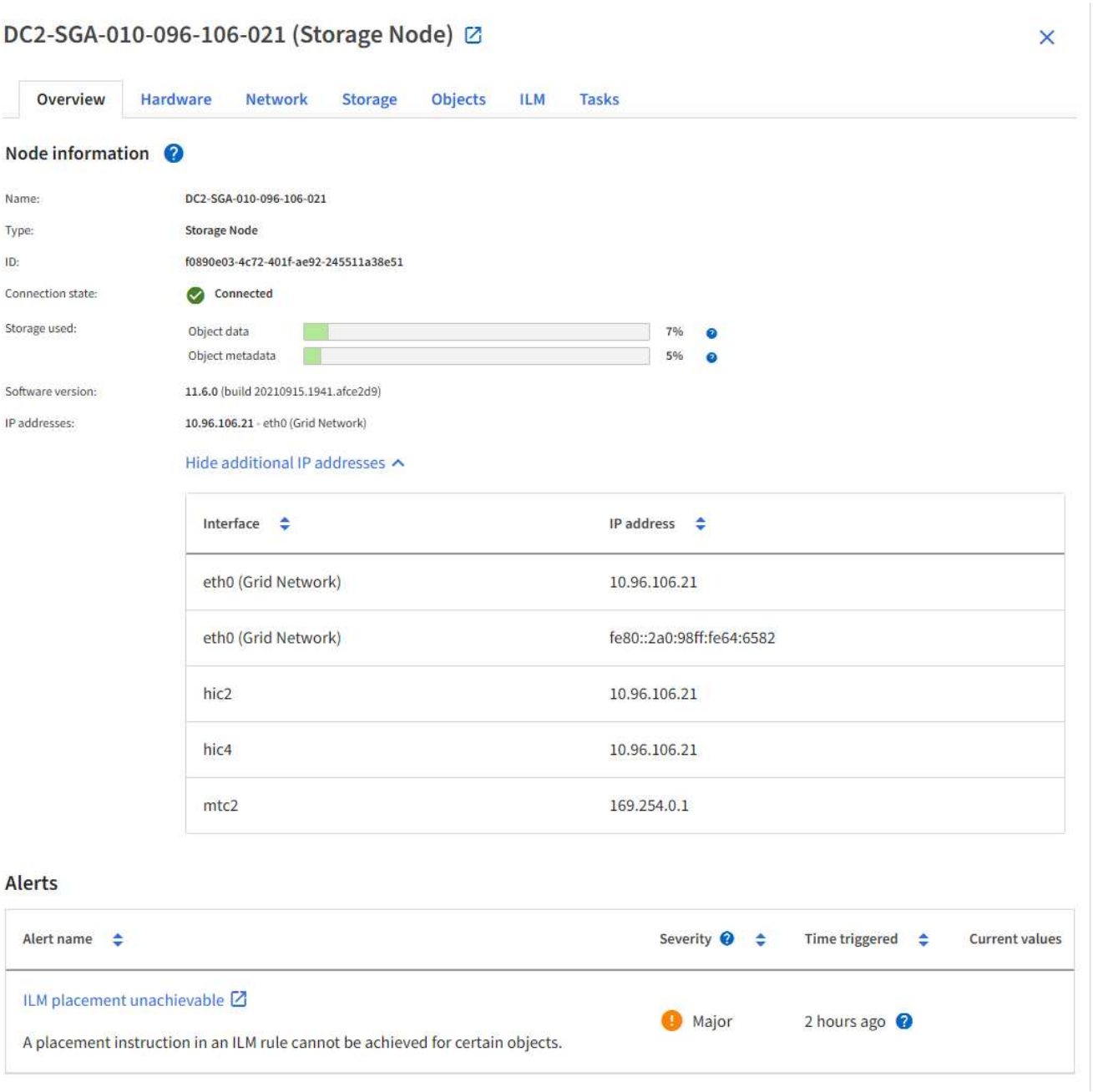
タスクの内容

IPアドレスの変更については、を参照してください"IP アドレスを設定する"。

手順

1. ノード > ***grid node*** > *概要*を選択します。
2. [IP Addresses] のタイトルの右側にある [**Show More**] を選択します。

   このグリッドノードの IP アドレスがテーブルに表示されます。



StorageGRIDで**VLAN**インターフェイスを設定する

管理ノードとゲートウェイ ノードに仮想 LAN (VLAN) インターフェイスを作成し、HA グループとロード バランサ エンドポイントで使用してトラフィックを分離および分割し、セキュリティ、柔軟性、パフォーマンスを向上させます。HA グループ内の選択されたノードは、VLAN インターフェイスを使用して最大 10 個の仮想 IP アドレスを共有できるため、1 つのノードがダウンしても、別のノードが仮想 IP アドレスとの間のトラ

フィックを引き継ぎます。

VLAN インターフェイスに関する考慮事項

- VLAN インターフェイスを作成するには、 VLAN ID を入力し、 1 つ以上のノード上で親インターフェイスを選択します。
- 親インターフェイスは、スイッチでトランクインターフェイスとして設定する必要があります。
- 親インターフェイスは、グリッドネットワーク（ eth0 ）、クライアントネットワーク（ eth2 ）、または VM やベアメタルホスト用の追加のトランクインターフェイス（ ens256 など）です。
- VLAN インターフェイスごとに、特定のノードに対して選択できる親インターフェイスは 1 つだけです。たとえば、同じゲートウェイノードのグリッドネットワークインターフェイスとクライアントネットワークインターフェイスの両方を同じVLANの親インターフェイスとして使用することはできません。
- VLAN インターフェイスが管理ノードトラフィック用で、 Grid Manager および Tenant Manager に関連するトラフィックが含まれている場合は、管理ノード上のインターフェイスのみを選択します。
- VLANインターフェイスがS3クライアントトラフィック用の場合は、管理ノードまたはゲートウェイノードのインターフェイスを選択します。
- トランクインターフェイスを追加する必要がある場合は、次の詳細を参照してください。
  - * VMware（ノードのインストール後）*：VMware ：ノードにトランクインターフェイスまたはアクセスインターフェイスを追加します"
  - **Linux (**ノードをインストールする前**)**:"ノード構成ファイルを作成"
  - **Linux (**ノードのインストール後**)**:"ノードにトランクまたはアクセスインターフェースを追加する"

> 「Linux」は、RHEL、Ubuntu、または Debian のデプロイメントを指します。サポートされているバージョンのリストについては、 "NetApp Interoperability Matrix Tool（IMT）" 。

VLAN インターフェイスを作成します

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"rootアクセス権限"。
- ネットワークでトランクインターフェイスが設定され、 VM または Linux ノードに接続されている。トランクインターフェイスの名前を確認しておきます。
- 設定する VLAN の ID を確認しておきます。

タスクの内容

ネットワーク管理者が、 1 つ以上のトランクインターフェイスと 1 つ以上の VLAN を設定して、異なるアプリケーションまたはテナントに属するクライアントトラフィックまたは管理トラフィックを分離している場合があります。各 VLAN は、数値 ID またはタグで識別されます。たとえば、ネットワークで FabricPool トラフィックに VLAN 100 を使用し、アーカイブアプリケーションに VLAN 200 を使用しているとします。

グリッドマネージャを使用して、クライアントが特定の VLAN 上の StorageGRID にアクセスできるようにする VLAN インターフェイスを作成できます。VLAN インターフェイスを作成するときは、 VLAN ID を指定し、 1 つ以上のノード上で親（トランク）インターフェイスを選択します。

ウィザードにアクセスします

手順

1. 構成 > ネットワーク > **VLAN** インターフェース を選択します。
2. 「 * Create * 」を選択します。

VLAN インターフェイスの詳細を入力します

手順

1. ネットワーク内の VLAN の ID を指定します。1~4094 の値を入力できます。

   VLAN IDは一意である必要はありません。たとえば、あるサイトの管理トラフィックに VLAN ID 200 を使用し、別のサイトのクライアントトラフィックに同じ VLAN ID を使用できます。各サイトに異なる親インターフェイスのセットを持つ個別の VLAN インターフェイスを作成できます。ただし、IDが同じ2つのVLANインターフェイスでノード上の同じインターフェイスを共有することはできません。すでに使用されている ID を指定すると、メッセージが表示されます。

2. 必要に応じて、 VLAN インターフェイスの短い概要 を入力します。
3. 「 * Continue * 」を選択します。

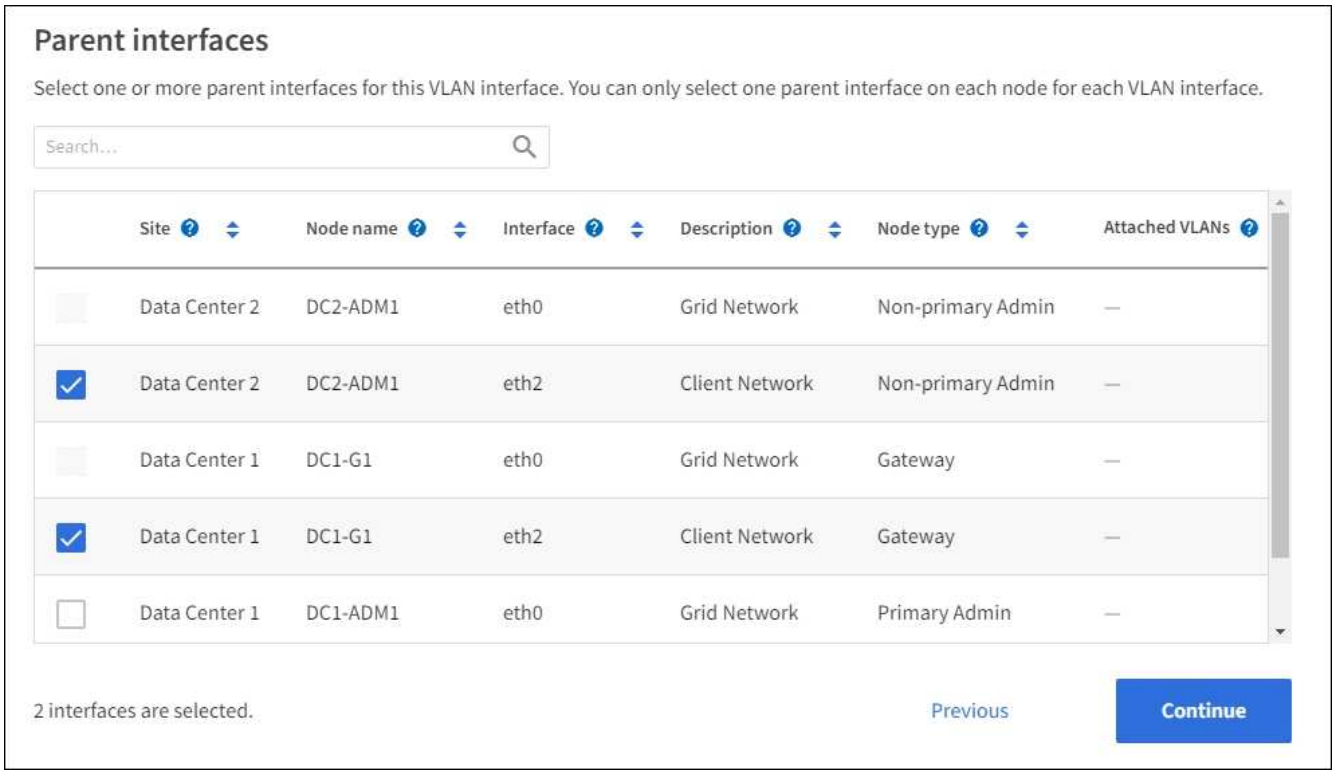
親インターフェイスを選択します

次の表に、グリッドの各サイトのすべての管理ノードとゲートウェイノードで使用可能なインターフェイスを示します。管理ネットワーク（eth1）インターフェイスを親インターフェイスとして使用することはできず、表示されていません。

手順

1. この VLAN を接続する 1 つ以上の親インターフェイスを選択してください。

   たとえば、ゲートウェイノードと管理ノードのクライアントネットワーク（ eth2 ）インターフェイスに VLAN を接続できます。



2. 「 * Continue * 」を選択します。

設定を確認します

手順

1. 構成を確認し、変更を行います。
   - VLAN ID または概要 を変更する必要がある場合は、ページの上部にある *Enter VLAN details * を選択します。
   - 親インターフェイスを変更する必要がある場合は、ページの上部にある「親インターフェイスを選択」を選択するか、「 * 前へ * 」を選択します。
   - 親インターフェースを削除する必要がある場合は、ゴミ箱 を選択してください。
2. [保存（ Save ）] を選択します。
3. 新しいインターフェイスが [高可用性グループ] ページに選択肢として表示され、ノードの [ネットワークインターフェイス] テーブルにリストされるまで、最大 5 分間待機します (**[**ノード**] > [***親インターフェイス ノード**] > [***ネットワーク])。

VLAN インターフェイスを編集します

VLAN インターフェイスを編集する場合、次の種類の変更を行うことができます。

- VLAN ID または概要 を変更します。
- 親インターフェイスを追加または削除します。

たとえば、関連付けられているノードの運用を停止する場合、 VLAN インターフェイスから親インターフェイスを削除できます。

次の点に注意してください。

- HA グループで VLAN インターフェイスを使用している場合、 VLAN ID は変更できません。
- HA グループで親インターフェイスが使用されている場合、親インターフェイスを削除することはできません。

  たとえば、VLAN 200がノードAとBの親インターフェイスに接続されているとします。HAグループがノードAのVLAN 200インターフェイスとノードBのeth2インターフェイスを使用している場合、ノードBの未使用の親インターフェイスは削除できますが、ノードAの使用済みの親インターフェイスは削除できません。

手順

1. 構成 > ネットワーク > **VLAN** インターフェース を選択します。
2. 編集するVLANインターフェイスのチェックボックスを選択します。次に、 * アクション * > * 編集 * を選択します。
3. 必要に応じて、 VLAN ID または概要 を更新します。次に、 [* Continue （続行）] を選択します。

   HA グループで VLAN が使用されている場合、 VLAN ID は更新できません。

4. 必要に応じて、チェックボックスをオンまたはオフにして、親インターフェイスを追加するか、使用されていないインターフェイスを削除します。次に、 [* Continue （続行）] を選択します。
5. 構成を確認し、変更を行います。
6. [保存（ Save ）] を選択します。

VLAN インターフェイスを削除します

1 つ以上の VLAN インターフェイスを削除できます。

HA グループで現在使用されている VLAN インターフェイスは削除できません。HA グループを削除する前に、 VLAN インターフェイスを HA グループから削除する必要があります。

クライアントトラフィックの中断を回避するには、次のいずれかを実行します。

- この VLAN インターフェイスを削除する前に、 HA グループに新しい VLAN インターフェイスを追加してください。
- この VLAN インターフェイスを使用しない新しい HA グループを作成してください。
- 削除する VLAN インターフェイスが現在アクティブインターフェイスである場合は、 HA グループを編集します。削除する VLAN インターフェイスを優先順位リストの一番下に移動します。新しいプライマリインターフェイスとの通信が確立されるまで待ってから、 HA グループから古いインターフェイスを削除します。最後に、そのノードの VLAN インターフェイスを削除します。

手順

1. 構成 > ネットワーク > **VLAN** インターフェース を選択します。
2. 削除する各VLANインターフェイスのチェックボックスを選択します。次に、 * アクション * > * 削除 * を選択します。
3. 「 * はい * 」を選択して選択を確定します。

   選択したすべての VLAN インターフェイスが削除されます。VLAN Interfaces ページに、グリーンの成功バナーが表示されます。

管理インターフェースで**StorageGRID CORS**を有効にする

グリッド管理者は、別のドメインの管理 API を使用してStorageGRID内のデータにアクセスできるようにする場合、 StorageGRIDへの管理 API 要求に対してクロスオリジン リソース共有 (CORS) を有効にすることができます。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- その"rootアクセス権限"すべての CORS 構成リクエストへのアクセスを提供します。

タスクの内容

CORS は、あるドメイン内のクライアント Web アプリケーションが別のドメイン内のリソースにアクセスできるようにするセキュリティ メカニズムです。例えば、ドメイン内のStorageGRIDの監視ダッシュボードを構築したいとします。 `http://www.example.com` 。 StorageGRIDでCORSを有効にすると、 `http://www.example.com` 「グリッドマネージャ」では、 StorageGRIDドメインは、 `http://www.example.com` 。

管理API（mgmt-api）リクエスト `application/json`または `multipart/formdata`リクエスト `Content-Type`CORS ではサポートされています。

手順

1. Grid Manager で、構成 > ネットワーク > 管理インターフェイスの **CORS** 設定 に移動します。
2. **Grid Manager**、**Tenant Manager**、または両方のオプションを選択します。
   - グリッド マネージャー: クロスドメイン グリッド管理 API リクエストに対して CORS を有効にします。
   - テナント マネージャー: クロスドメイン テナント管理 API リクエストに対して CORS を有効にします。
3. ドメイン フィールドに他のドメインの URL を入力します。

   StorageGRIDで複数のドメインの CORS を有効にする場合は、「別のドメインを追加」を選択します。

4. [保存（ Save ）] を選択します。

関連情報

"バケットとオブジェクトのStorageGRID CORSを構成する"

トラフィック分類ポリシーを管理します

StorageGRID のトラフィック分類ポリシー

トラフィック分類ポリシーを使用すると、さまざまなタイプのネットワークトラフィックを識別および監視できます。これらのポリシーは、トラフィックの制限と監視に役立ち、Quality of Service（QoS；サービス品質）サービスを強化できます。

トラフィック分類ポリシーは、ゲートウェイノードおよび管理ノードの StorageGRID ロードバランササービス上のエンドポイントに適用されます。トラフィック分類ポリシーを作成するには、ロードバランサエンドポイントを作成しておく必要があります。

一致ルール

各トラフィック分類ポリシーには、次のエンティティに関連するネットワークトラフィックを識別する 1 つ以上の一致ルールが含まれています。

- バケット
- サブネット
- テナント
- ロードバランサエンドポイント

StorageGRID は、ルールの目的に応じて、ポリシー内のルールに一致するトラフィックを監視します。ポリシーのルールに一致するトラフィックは、そのポリシーによって処理されます。逆に、指定されたエンティティを除くすべてのトラフィックを照合するルールを設定できます。

トラフィック制限

必要に応じて、次の制限タイプをポリシーに追加できます。

- 総帯域幅
- 要求ごとの帯域幅
- 同時要求
- リクエスト率

制限値はロードバランサごとに適用されます。複数のロードバランサに同時にトラフィックが分散されている場合、合計最大速度は指定した速度制限の倍数になります。

> ポリシーを作成して、アグリゲートの帯域幅を制限したり、要求ごとの帯域幅を制限したりできます。ただし、StorageGRID では、両方のタイプの帯域幅を同時に制限することはできません。総帯域幅を制限すると、制限のないトラフィックのパフォーマンスがさらに若干低下する可能性があります。

総帯域幅制限またはリクエストごとの帯域幅制限の場合、リクエストは設定した速度で送受信されます。StorageGRID が適用できる速度は1つのみであるため、マッチャータイプによる最も具体的なポリシー一致が適用されます。リクエストによって消費された帯域幅は、集約帯域幅制限ポリシーを含む、より一般的なマッチングポリシーにはカウントされません。その他のすべての制限タイプについては、クライアントからのリクエストは250ミリ秒遅延され、該当するポリシー制限を超えるリクエストに対しては503 Slow Down応答が返されます。

グリッドマネージャーでは、トラフィックチャートを表示し、ポリシーが想定どおりのトラフィック制限を適用していることを確認できます。

SLA でトラフィック分類ポリシーを使用する

トラフィック分類ポリシーを容量制限およびデータ保護とともに使用して、容量、データ保護、およびパフォーマンスに固有のサービスレベル契約（ SLA ）を適用できます。

次の例は、 SLA の 3 つの階層を示しています。トラフィック分類ポリシーを作成して、各 SLA 層のパフォーマンス目標を達成できます。

サービスレベル階層	容量	データ保護	許容される最大パフォーマンス	コスト
Gold	1 PB のストレージを使用できます	3コピーILMルール	25 、 000 要求 / 秒 5GB/秒（40Gbps）の帯域幅	$$/ 月
シルバー	250TBのストレージを許可	2コピーILMルール	10K要求/秒 1.25GB/秒（10Gbps）の帯域幅	$/ 月
ブロンズ	100TBのストレージを許可	2コピーILMルール	5、000リクエスト/秒 1GB/秒（8Gbps）の帯域幅	月あたりのコスト

StorageGRID トラフィック分類ポリシーを作成する

バケット、バケット正規表現、CIDR、ロードバランサエンドポイント、またはテナントごとにネットワークトラフィックを監視し、必要に応じて制限する場合は、トラフィック分類ポリシーを作成できます。必要に応じて、帯域幅、同時要求数、または要求速度に基づいてポリシーの制限を設定できます。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"rootアクセス権限"。
- 照合するロードバランサエンドポイントを作成しておきます。
- 該当するテナントを作成しておきます。

手順

1. 構成 > ネットワーク > *トラフィック分類*を選択します。
2. 「 * Create * 」を選択します。
3. ポリシーの名前と概要 （オプション）を入力し、* Continue *を選択します。

   たとえば、このトラフィック分類ポリシー環境 の内容と制限する内容を説明します。

4. ポリシーに一致するルールを1つ以上作成するには、*[ルールの追加]*を選択し、以下の詳細を指定します。作成するポリシーには、一致するルールが少なくとも1つ必要です。「 * Continue * 」を選択します。

フィールド	製品説明
タイプ	一致するルール環境 のトラフィックのタイプを選択します。トラフィックタイプには、バケット、バケットの正規表現、CIDR、ロードバランサエンドポイント、テナントがあります。
一致値	選択したタイプに一致する値を入力します。 • Bucket：バケット名を1つ以上入力します。 • Bucket regex：バケット名のセットに一致する正規表現を1つ以上入力します。 正規表現は固定されていません。^anchorを使用してバケット名の先頭に一致させ、$anchorを使用して名前の末尾に一致させます。正規表現マッチングでは、PCRE（Perl互換正規表現）構文のサブセットがサポートされます。 • CIDR：CIDR表記で、目的のサブネットに一致するIPv4サブネットを1つ以上入力します。 • Load balancer endpoint：エンドポイント名を選択します。これは、で定義したロードバランサエンドポイントです"ロードバランサエンドポイントを設定する"。 • Tenant：一致するテナントはアクセスキーIDを使用します。要求にアクセスキーID（匿名アクセスなど）が含まれていない場合は、テナントを特定するためにアクセスされるバケットの所有権が使用されます。
逆一致	定義した[Type]および[Match Value]と一致するすべてのネットワークトラフィック_except_trafficを照合する場合は、*[Inverse Match]*チェックボックスをオンにします。それ以外の場合は'チェックボックスをオフのままにします たとえば、このポリシーをいずれかのロードバランサエンドポイントを除くすべてのロードバランサエンドポイントに適用する場合は、除外するロードバランサエンドポイントを指定し、*[逆一致]*を選択します。 少なくとも 1 つが逆マッチャーである複数のマッチャーを含むポリシーの場合、すべてのリクエストに一致するポリシーを作成しないように注意してください。

5. 必要に応じて、*[制限の追加]*を選択し、以下の詳細を選択して1つ以上の制限を追加し、ルールに一致するネットワークトラフィックを制御します。

> StorageGRID では、制限を追加しなくても指標が収集されるため、トラフィックの傾向を把握できます。

フィールド	製品説明
タイプ	ルールに一致するネットワークトラフィックに適用する制限のタイプ。たとえば、帯域幅や要求レートを制限できます。 注：ポリシーを作成して、総帯域幅を制限したり、要求ごとの帯域幅を制限したりできます。ただし、StorageGRID では、両方のタイプの帯域幅を同時に制限することはできません。集約帯域幅が使用されている場合、要求ごとの帯域幅は使用できません。逆に、要求ごとの帯域幅が使用されている場合、集約帯域幅は使用できません。総帯域幅を制限すると、制限のないトラフィックのパフォーマンスがさらに若干低下する可能性があります。 帯域幅の制限については、設定された制限のタイプに最も一致するポリシーが StorageGRID によって適用されます。たとえば、トラフィックを一方向のみに制限するポリシーがある場合、帯域幅制限が設定されている他のポリシーと一致するトラフィックがあっても、反対方向のトラフィックは無制限になります。StorageGRID では、帯域幅制限に対して次の順序で「最適な」一致が実装されます。 • 正確な IP アドレス（ /32 マスク） • 正確なバケット名 • バケットの正規表現 • テナント • エンドポイント • 正確でない CIDR の一致（ /32 ではない） • 逆一致
環境	これにより、環境 クライアントの読み取り要求（GETまたはHEAD）と書き込み要求（PUT、POST、DELETE）のどちらを制限するか。
値	選択した単位に基づいて、ネットワークトラフィックが制限される値。たとえば、このルールに一致するネットワークトラフィックが10MiB/sを超えないようにするには、「10」と入力して[MiB/s」を選択します 注：単位の設定に応じて、使用可能な単位は2進数（GiBなど）または10進数（GBなど）のいずれかになります。単位の設定を変更するには、Grid Managerの右上にあるユーザードロップダウンを選択し、*ユーザー設定*を選択します。
単位	入力した値を表す単位。

たとえば、SLA 層に 4 GB/秒の帯域幅制限を作成する場合は、4 GB/秒の GET/HEAD と 4 GB/秒の PUT/POST/DELETE の 2 つの集約帯域幅制限を作成します。

6. 「 * Continue * 」を選択します。
7. トラフィック分類ポリシーを読んで確認します。前へ*ボタンを使用して前に戻り、必要に応じて変更を行います。ポリシーに問題がなければ、*[保存して続行]*を選択します。

S3クライアントトラフィックがトラフィック分類ポリシーに従って処理されるようになりました。

終了後

"ネットワークトラフィックの指標を表示します"ポリシーが想定どおりのトラフィック制限を適用していることを確認します。

StorageGRID トラフィック分類ポリシーを編集する

トラフィック分類ポリシーを編集して、その名前または概要 を変更したり、ポリシーのルールや制限を作成、編集、削除したりできます。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"rootアクセス権限"。

手順

1. 構成 > ネットワーク > *トラフィック分類*を選択します。

   [Traffic Classification Policies]ページが表示され、既存のポリシーが表に表示されます。

2. [Actions]メニューまたは詳細ページを使用してポリシーを編集します。入力する内容については、を参照してください"トラフィック分類ポリシーを作成します"。

   [Actions]メニュー

   a. ポリシーのチェックボックスを選択します。

   b. **>**[編集]*を選択します。

   詳細ページ

   a. ポリシー名を選択します。

   b. ポリシー名の横にある*[編集]*ボタンを選択します。

3. [Enter policy name]手順で、必要に応じてポリシー名または概要 を編集し、*[Continue]*を選択します。
4. [一致ルールの追加]ステップで、必要に応じてルールを追加するか、既存のルールの*タイプ*と*一致値*を編集し、*続行*を選択します。
5. [制限の設定]ステップで、必要に応じて制限を追加、編集、または削除し、*[続行]*を選択します。
6. 更新されたポリシーを確認し、*[保存して続行]*を選択します。

   ポリシーに加えた変更が保存され、ネットワークトラフィックはトラフィック分類ポリシーに従って処理されるようになりました。トラフィックチャートを表示して、ポリシーが想定したトラフィック制限を適用していることを確認できます。

StorageGRID トラフィック分類ポリシーを削除する

不要になったトラフィック分類ポリシーは削除できます。削除したポリシーは取得でき

ないため、適切なポリシーを削除してください。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"rootアクセス権限"。

手順

1. 構成 > ネットワーク > *トラフィック分類*を選択します。

   [Traffic Classification Policies]ページが表示され、既存のポリシーが表に示されます。

2. [アクション]メニューまたは詳細ページを使用してポリシーを削除します。

   [Actions]メニュー

   a. ポリシーのチェックボックスを選択します。

   b. * アクション * > * 削除 * を選択します。

   [ポリシーの詳細]ページ

   a. ポリシー名を選択します。

   b. ポリシー名の横にある*[削除]*ボタンを選択します。

3. [はい]*を選択して、ポリシーの削除を確定します。

   ポリシーが削除されます。

StorageGRIDでネットワーク トラフィック指標を表示

トラフィック分類ポリシーページのグラフを表示して、ネットワークトラフィックを監視できます。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"rootアクセスまたはテナントアカウントの権限"。

タスクの内容

既存のトラフィック分類ポリシーについては、ロードバランササービスの指標を表示して、ポリシーがネットワーク全体のトラフィックを正常に制限しているかどうかを確認できます。グラフのデータは、ポリシーの調整が必要かどうかを判断するのに役立ちます。

トラフィック分類ポリシーに制限が設定されていない場合でも、メトリックが収集され、グラフにはトラフィックの傾向を把握するのに役立つ情報が表示されます。

手順

1. 構成 > ネットワーク > *トラフィック分類*を選択します。

   [Traffic Classification Policies]ページが表示され、既存のポリシーがテーブルに表示されます。

2. 指標を表示するトラフィック分類ポリシーの名前を選択します。
3. [Metrics]タブを選択します。

   トラフィック分類ポリシーのグラフが表示されます。このグラフには、選択したポリシーに一致するトラフィックのメトリックだけが表示されます。

   このページには次のグラフが表示されます。

   - [Request rate]：このグラフには、すべてのロードバランサによって処理されたこのポリシーに一致する帯域幅の量が表示されます。受信したデータには、すべての要求の要求ヘッダーと、本文データを含む応答の本文データサイズが含まれます。Sentには、すべての要求の応答ヘッダーと、応答に本文データを含む要求の応答本文のデータサイズが含まれます。

     > ⓘ 要求が完了すると、このチャートには帯域幅の使用量のみが表示されます。低速なオブジェクト要求や大規模なオブジェクト要求では、実際の帯域幅はこのグラフに表示される値と異なる場合があります。

   - エラー応答率：このグラフは、このポリシーに一致する要求がクライアントにエラー（HTTPステータスコード>=400）を返すおおよその速度を示します。
   - Average request duration（non-error）：このグラフには、このポリシーに一致する成功したリクエストの平均期間が表示されます。
   - Policy Bandwidth usage：このグラフには、すべてのロードバランサによって処理されたこのポリシーに一致する帯域幅の量が表示されます。受信したデータには、すべての要求の要求ヘッダーと、本文データを含む応答の本文データサイズが含まれます。Sentには、すべての要求の応答ヘッダーと、応答に本文データを含む要求の応答本文のデータサイズが含まれます。
4. 折れ線グラフにカーソルを合わせると、グラフの特定の部分の値がポップアップで表示されます。
5. [Metrics]タイトルのすぐ下にある* Grafanaダッシュボード*を選択すると、ポリシーのすべてのグラフが表示されます。[* Metrics]タブの4つのグラフに加えて、さらに2つのグラフを表示できます。
   - Write request rate by object size：このポリシーに一致するPUT / POST / DELETE要求の速度。個 々 のセルに配置すると、1秒あたりのレートが表示されます。ホバービューに表示されるレートは整数に切り捨てられ、バケットに0以外の要求がある場合は0と報告されることがあります。
   - Read request rate by object size：このポリシーに一致するGET / HEAD要求のレート。個 々 のセルに配置すると、1秒あたりのレートが表示されます。ホバービューに表示されるレートは整数に切り捨てられ、バケットに0以外の要求がある場合は0と報告されることがあります。
6. または、[サポート] メニューからグラフにアクセスします。
   a. サポート > ツール > *メトリック*を選択します。
   b. [Grafana]セクションから*[Traffic Classification Policy]*を選択します。
   c. ページ左上のメニューからポリシーを選択します。
   d. グラフにカーソルを合わせると、サンプルの日時、カウントに集計されたオブジェクトサイズ、その期間の1秒あたりの要求数を示すポップアップが表示されます。

      トラフィック分類ポリシーは、その ID によって識別されます。ポリシーIDは、トラフィック分類ポリシーページに表示されます。
7. グラフを分析して、ポリシーがトラフィックを制限している頻度と、ポリシーを調整する必要があるかどうかを判断します。

StorageGRIDの送信TLS接続でサポートされている暗号

StorageGRID システムでは、アイデンティティフェデレーションとクラウドストレージプールに使用される外部システムへの Transport Layer Security （ TLS ）接続でサポートされる暗号スイートに制限があります。

サポートされる TLS のバージョン

StorageGRID では、アイデンティティフェデレーションとクラウドストレージプールに使用される外部システムへの接続で TLS 1.2 と TLS 1.3 がサポートされます。

外部システムでの使用がサポートされている TLS 暗号は、さまざまな外部システムとの互換性を確保するように選択されています。このリストは、S3 クライアント アプリケーションでの使用がサポートされている暗号のリストよりも大きくなります。暗号を設定するには、構成 > セキュリティ > セキュリティ設定 に移動し、**TLS** および **SSH** ポリシー を選択します。

> プロトコルバージョン、暗号、鍵交換アルゴリズム、MACアルゴリズムなどのTLS設定オプションは、StorageGRID では設定できません。これらの設定について具体的なご要望がある場合は、ネットアップのアカウント担当者にお問い合わせください。

StorageGRID におけるアクティブ、アイドル、および同時 HTTP 接続の利点

StorageGRID システムのパフォーマンスに影響するのは、 HTTP 接続の設定方法です。設定は、 HTTP 接続がアクティブであるかアイドルであるか、同時に複数の接続を使用するかによって異なります。

次の種類の HTTP 接続について、パフォーマンスのメリットを特定することができます。

- アイドル HTTP 接続
- アクティブ HTTP 接続
- 同時 HTTP 接続

アイドル HTTP 接続を開いておくメリット

クライアント アプリケーションがアイドル状態のときに HTTP 接続を開いたままにして、後のトランザクションを許可します。アイドル状態の HTTP 接続を最大 10 分間開いたままにします。 StorageGRID は、10 分以上開かれアイドル状態になっている HTTP 接続を自動的に閉じる場合があります。

アイドル HTTP 接続を開いておくと、次のようなメリットがあります。

- HTTP トランザクションの実行が StorageGRID 必要と判断されてから StorageGRID システムでトランザクションが実行されるまでのレイテンシが短縮されます

  レイテンシの短縮は、特に TCP / IP 接続と TLS 接続の確立に時間がかかる場合に大きなメリットとなります。

- 実行済みの転送が増えるにしたがって TCP / IP のスロースタートアルゴリズムによってデータ転送速度が向上します
- クライアントアプリケーションと StorageGRID システムの間の接続が中断された、複数の障害状況の瞬時通知

スロースタートの利点とリソースの割り当てのバランスを取りながら、アイドル接続を開いたままにする時間を決定します。

アクティブ **HTTP** 接続のメリット

ストレージノードに直接接続する場合は、HTTP接続でトランザクションを継続的に実行する場合でも、アクティブHTTP接続の継続時間を10分に制限する必要があります。

接続を開いておく最大継続時間は、接続を維持することで得られるメリットと内部システムリソースへの理想的な接続の割り当てとのバランスによって決まります。

ストレージノードへのクライアント接続でアクティブHTTP接続を制限すると、次のようなメリットがあります。

- StorageGRID システム全体で負荷を最適に分散できます。

  時間の経過とともに、負荷分散の要件が変化するため、HTTP 接続が最適ではなくなる可能性があります。クライアント アプリケーションがトランザクションごとに個別の HTTP 接続を確立すると、システムは最適な負荷分散を実行しますが、この方法では永続的な接続に関連する貴重な利点が無効になります。

- クライアントアプリケーションからの HTTP トランザクションを使用可能な空きスペースがある LDR サービスに転送できる
- メンテナンス手順を開始できます。

  メンテナンス手順の中には、実行中のすべての HTTP 接続が完了してからでないと開始されないものがあります。

ロードバランササービスへのクライアント接続では、接続時間を制限することで一部のメンテナンス手順をすぐに開始できます。クライアント接続の時間が制限されていない場合、アクティブな接続が自動的に終了するまでに数分かかることがあります。

同時 **HTTP** 接続のメリット

StorageGRID システムへの TCP / IP 接続を複数開いて並列処理を可能にしておくと、パフォーマンスが向上します。最適な並列接続数は、さまざまな要因によって異なります。

同時 HTTP 接続には、次のようなメリットがあります。

- レイテンシが短縮されます

  他のトランザクションが完了するのを待たずに、トランザクションをすぐに開始できます。

- スループットの向上

  StorageGRID システムでは、トランザクションの並列処理が可能なため、全体的なトランザクションのスループットが向上します。

クライアントアプリケーションで複数の HTTP 接続を確立する必要があります。クライアントアプリケーションでトランザクションの実行が必要になったときは、確立された接続の中からトランザクションの処理に現在使用されていない接続を選択してすぐに使用することができます。

各StorageGRIDシステムのトポロジでは、同時トランザクションと接続のピーク スループットが異なります。ピーク スループットは、コンピューティング、ネットワーク、ストレージ リソース、WAN リンク、およびStorageGRIDシステムがサポートするサーバー、サービス、アプリケーションの数によって異なります。

StorageGRIDシステムは、多くの場合、複数のクライアント アプリケーションをサポートします。同時接続の最大数を決定するときは、この点を考慮してください。クライアント アプリケーションが、それぞれStorageGRIDシステムへの接続を確立する複数のソフトウェア エンティティで構成されている場合は、エンティティ間のすべての接続を合計します。次の状況では、同時接続の最大数を調整する必要が生じる場合があります。

- StorageGRID システムのトポロジによって、システムでサポートできる同時トランザクションや同時接続の最大数が異なります。
- クライアントアプリケーションがネットワークの限られた帯域幅で StorageGRID システムと通信する場合は、個々のトランザクションが妥当な時間で完了するように、必要に応じて同時実行の数を少なくします。
- 多くのクライアントアプリケーションで StorageGRID システムを共有する場合は、システムの制限を超えないように、同時実行の数を少なくする必要があります。

読み取り処理用と書き込み処理用に別々の **HTTP** 接続プールを使用する

読み取り処理と書き込み処理に別々の HTTP 接続プールを使用して、それぞれに使用するプールの容量を制御できます。HTTP 接続のプールを分けることで、トランザクションや負荷分散をより細かく制御できます。

クライアントアプリケーションで生成される負荷には、読み出し中心（読み取り）の負荷と格納中心（書き込み）の負荷があります。読み取りと書き込みで HTTP 接続プールを分けることで、各プールの量を調整してそれぞれのトランザクション専用に使用することができます。

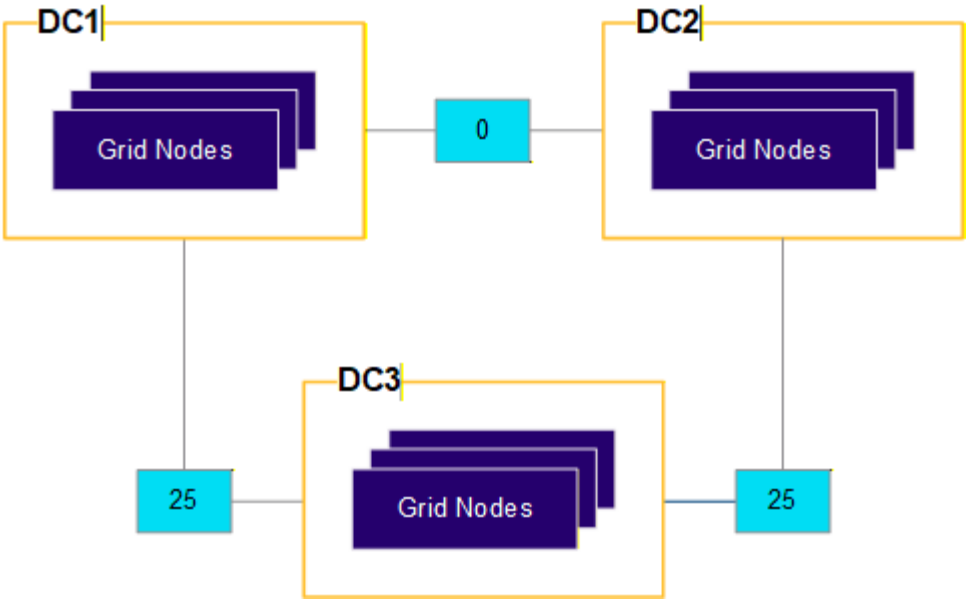
StorageGRIDでリンクコストを管理する

リンクコストを使用すると、複数のデータセンターサイトが存在する場合に、要求されたサービスを提供するデータセンターサイトの優先順位を決定できます。サイト間のレイテンシに合わせてリンクコストを調整できます。

リンクコストとは

- リンクコストは、オブジェクトの読み出しにどのオブジェクトコピーを使用するかを優先的に処理するために使用されます。
- リンクコストは、グリッド管理 API およびテナント管理 API で、使用する内部 StorageGRID サービスを決定するために使用されます。
- リンクコストは、管理ノードおよびゲートウェイノード上のロードバランサーサービスによって、クライアント接続をルーティングするために使用されます。"ロードバランシングに関する考慮事項"を参照してください。

この図は、サイト間のリンクコストが設定された3サイト構成のグリッドを示しています。



- 管理ノードとゲートウェイノード上のロードバランササービスは、同じデータセンターサイトにあるすべてのストレージノード、およびリンクコストが0のデータセンターサイトにクライアント接続を均等に分散します。

  この例で、データセンターサイト 1 （ DC1 ）にあるゲートウェイノードは、 DC1 にあるストレージノードと DC2 にあるストレージノードにクライアント接続を均等に分散します。DC3 にあるゲートウェイノードは、 DC3 にあるストレージノードにのみクライアント接続を送信します。

- 複数のレプリケートコピーが存在するオブジェクトを読み出す場合、 StorageGRID はリンクコストが最も低いデータセンターにあるコピーを読み出します。

  次の例では、DC2にあるクライアントアプリケーションがDC1とDC3の両方に格納されているオブジェクトを読み出す場合、DC1からDC2へのリンクコストは0であり、DC3からDC2へのリンクコスト（25）よりも低いため、オブジェクトはDC1から読み出されます。

リンクコストは、測定単位を伴わない任意の相対的な数値です。たとえば、使用にあたってリンクコスト 50 の優先度はリンクコスト 25 よりも低くなります。次の表に、よく使用されるリンクコストを示します。

リンク	リンクコスト	脚注
物理データセンターサイト間	25（デフォルト）	WAN リンクで接続されたデータセンター。
同じ物理的な場所にある論理データセンターサイト間	0	同じ物理ビルディングまたはキャンパスにある論理データセンターを LAN で接続します。

リンクコストを更新します

データセンターサイト間のリンクコストを更新して、サイト間のレイテンシを反映させることができます。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。

- あなたはを持っています"rootアクセス権限"。

手順

1. サポート > その他 > リンク コスト を選択します。
2. 「サイト/リンク費用」列に記載されている各サイトについて、他のサイトの費用値を0～100の範囲で入力してください。

   送信元が宛先と同じ場合は、リンクコストを変更できません。

3. 変更を破棄するか保存するか：
   - 変更を破棄するには、*変更をクリア*を選択してください。
   - 変更を保存するには、*保存*を選択してください。

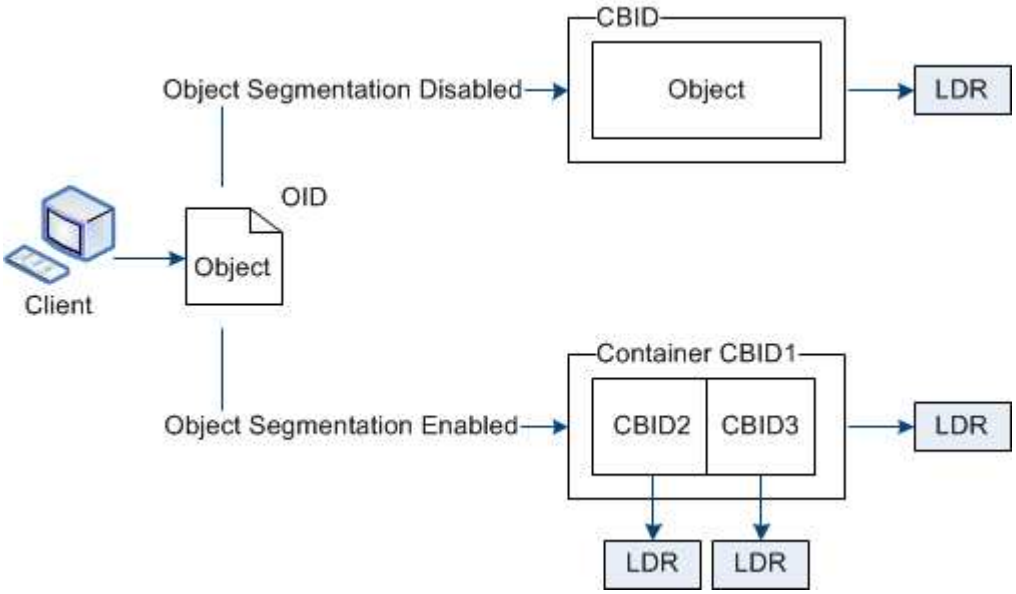
ストレージノードを管理します

[ストレージ]オプションを使用します

StorageGRIDのオブジェクトセグメンテーションについて学ぶ

オブジェクトのセグメント化は、オブジェクトを小さな固定サイズのオブジェクトの集まりに分割して、大きなオブジェクトのストレージとリソースの使用を最適化するプロセスです。S3 のマルチパートアップロードでもセグメント化されたオブジェクトが作成され、各パートを表すオブジェクトが 1 つ作成されます。

オブジェクトが StorageGRID システムに取り込まれると、 LDR サービスはオブジェクトを複数のセグメントに分割し、すべてのセグメントのヘッダー情報をコンテンツとして表示するセグメントコンテナを作成します。



セグメントコンテナを読み出す際、 LDR サービスは各セグメントから元のオブジェクトを組み立て、クライアントに返します。

コンテナとセグメントは、必ずしも同じストレージノードに格納されるとは限りません。コンテナとセグメン

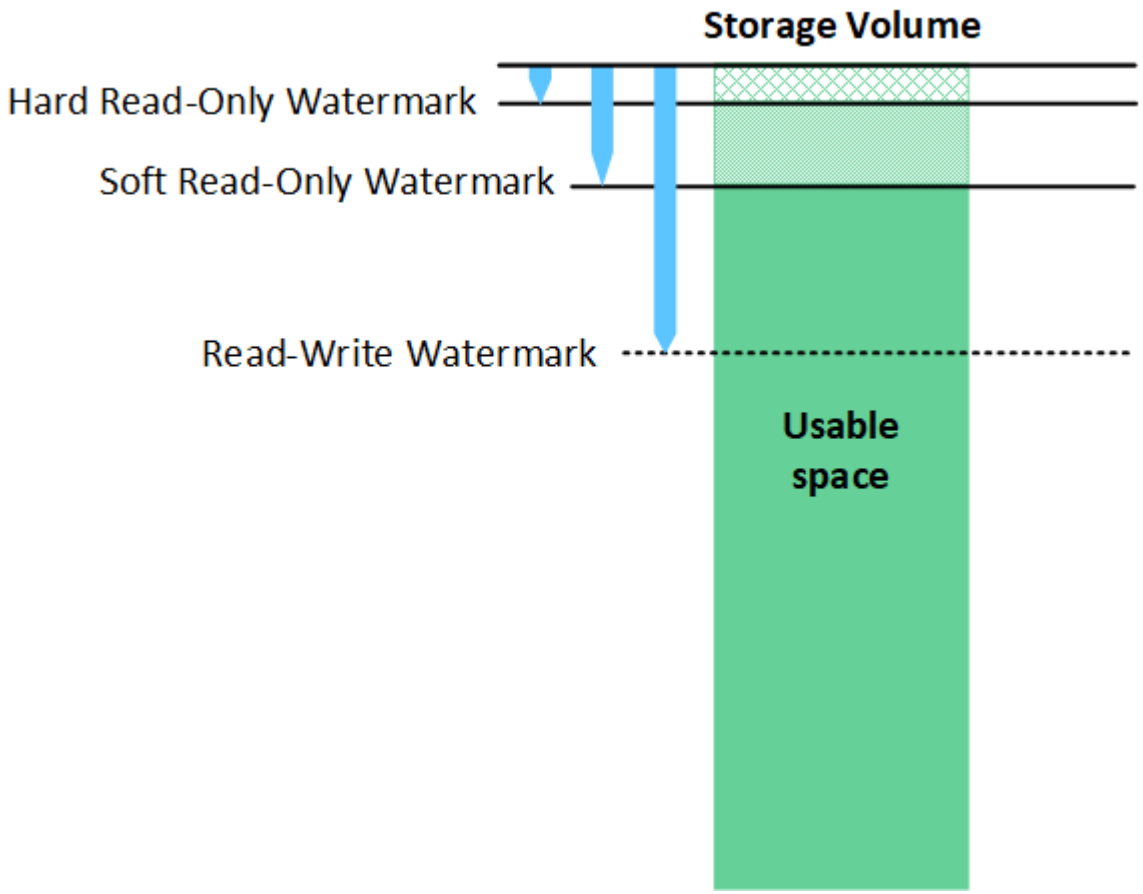
トは、 ILM ルールで指定されたストレージプール内の任意のストレージノードに格納できます。

各セグメントは StorageGRID システムによって個別に処理され、 Managed Objects や Stored Objects などの属性の対象としてカウントされます。たとえば、 StorageGRID システムに格納されているオブジェクトが 2 つのセグメントに分割された場合、取り込みが完了すると次のように Managed Objects の値が 3 つ増えます。

```
segment container + segment 1 + segment 2 = three stored objects
```

StorageGRIDのストレージボリュームのウォーターマークについて学ぶ

StorageGRID では、ストレージボリュームのウォーターマークを 3 つ使用して、スペースの深刻な低下を発生させる前にストレージノードを読み取り専用状態に安全に移行し、読み取り専用状態に移行して再び読み取り / 書き込み可能にすることができます。



ストレージボリュームのウォーターマークは、レプリケートオブジェクトデータとイレイジャーコーディングオブジェクトデータに使用されるスペースにのみ適用されます。ボリューム0でオブジェクトメタデータ用にリザーブされているスペースの詳細については、を参照してください"オブジェクトメタデータストレージを管理する"。

読み取り専用ソフトウォーターマークとは何ですか？

ストレージボリュームのソフト読み取り専用ウォーターマーク*は、オブジェクトデータに使用可能なストレージノードのスペースがフルに近づいていることを示す最初のウォーターマークです。

ストレージノード内の各ボリュームの空きスペースがそのボリュームのソフト読み取り専用ウォーターマークよりも少ない場合、ストレージノードは_読み取り専用モード_に移行します。読み取り専用モードでは、ストレージノードは StorageGRID システムの他の要素にサービスが読み取り専用であることをアドバタイズしますが、保留中の書き込み要求はすべて実行します。

たとえば、ストレージノード内の各ボリュームのソフト読み取り専用ウォーターマークが10GBであるとします。各ボリュームの空きスペースが 10GB 未満になると、ストレージノードはソフト読み取り専用モードに移行します。

読み取り専用ハードウォーターマークとは何ですか？

次のウォーターマークは* storage volume hard read-only watermark *です。これは、オブジェクトデータに使用可能なノードのスペースがフルに近づいていることを示します。

ボリュームの空きスペースがそのボリュームの読み取り専用ハードウォーターマークよりも小さい場合、ボリュームへの書き込みは失敗します。ただし、他のボリュームへの書き込みは、それらのボリュームの空きスペースが読み取り専用ハードウォーターマークよりも少なくなるまで続行できます。

たとえば、ストレージノード内の各ボリュームの読み取り専用ハードウォーターマークが5GBであるとします。各ボリュームの空きスペースが 5GB 未満になると、ストレージノードは書き込み要求を受け付けなくなります。

ハード読み取り専用透かしは、常にソフト読み取り専用透かしより小さくなります。

読み取り/書き込みウォーターマークとは何ですか。

ストレージボリュームの読み取り/書き込みウォーターマーク*は、読み取り専用モードに移行したストレージノードにのみ適用されます。また、ノードが再度読み取り / 書き込み可能になるタイミングを決定します。ストレージノード内のいずれかのストレージボリュームの空きスペースがそのボリュームの読み取り/書き込みウォーターマークを超えると、ノードは自動的に読み取り/書き込み状態に戻ります。

たとえば、ストレージノードが読み取り専用モードに移行したとします。また、各ボリュームの読み取り/書き込みウォーターマークが30GBであるとします。ボリュームの空きスペースが 30GB に増えると、そのノードは再び読み取り / 書き込み可能になります。

読み取り/書き込みウォーターマークは、ソフト読み取り専用ウォーターマークとハード読み取り専用ウォーターマークの両方より常に大きくなります。

ストレージボリュームのウォーターマークを表示する

現在のウォーターマーク設定とシステムに最適化された値を表示できます。最適化された透かしが使用されていない場合は、設定を調整できるかどうかを判断できます。

開始する前に

- StorageGRID 11.6以降へのアップグレードが完了している。
- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"rootアクセス権限"。

現在の透かし設定を表示します

Grid Manager で、現在のストレージのウォーターマーク設定を表示できます。

手順

1. サポート > その他 > *ストレージのウォーターマーク*を選択します。
2. [Storage Watermarks]ページで、[Use optimized values]チェックボックスを確認します。
   - このチェックボックスをオンにすると、ストレージノードのサイズとボリュームの相対容量に基づいて、すべてのストレージノードのすべてのストレージボリュームに対して3つのウォーターマークがすべて最適化されます。

     これがデフォルトで推奨される設定です。これらの値は更新しないでください。必要に応じて、可能です最適化されたストレージウォーターマークを表示する。
   - [最適化された値を使用]チェックボックスがオフの場合、カスタム（最適化されていない）ウォーターマークが使用されます。カスタム透かし設定の使用はお勧めしません。の手順に従って、"ロー読み取り専用のウォーターマーク上書きアラートのトラブルシューティング"設定を調整できるかどうか、または調整する必要があるかどうかを確認します。

     カスタムウォーターマーク設定を指定する場合は、0より大きい値を入力する必要があります。

最適化されたストレージウォーターマークの表示

StorageGRIDでは、2つのPrometheus指標を使用して、ストレージボリュームのソフト読み取り専用ウォーターマークに対して計算された最適化された値が表示されます。グリッド内の各ストレージノードの最適化された最小値と最大値を表示できます。

1. サポート > ツール > *メトリック*を選択します。
2. Prometheus セクションで、 Prometheus ユーザインターフェイスへのリンクを選択します。
3. 推奨されるソフト読み取り専用の最小ウォーターマークを確認するには、次の Prometheus 指標を入力し、 * Execute * を選択します。

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

   最後の列には、各ストレージノードのすべてのストレージボリュームについて、ソフト読み取り専用ウォーターマークの最適化された最小値が表示されます。この値がストレージボリュームのソフト読み取り専用ウォーターマークのカスタム設定よりも大きい場合は、ストレージノードに対して* Low read-only watermark override *アラートがトリガーされます。

4. 推奨されるソフト読み取り専用の最大ウォーターマークを確認するには、次の Prometheus 指標を入力し、 * Execute * を選択します。

   ```
   storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
   ```

   最後の列には、各ストレージノード上のすべてのストレージボリュームについて、ソフト読み取り専用ウォーターマークの最適化された最大値が表示されます。

StorageGRID でのオブジェクト メタデータ ストレージの管理

StorageGRID システムのオブジェクトメタデータ容量は、そのシステムに格納できるオブジェクトの最大数を制御します。StorageGRID システムに新しいオブジェクトを格納するための十分なスペースを確保するには、 StorageGRID がオブジェクトメタデータを格納する場所と方法を理解する必要があります。

オブジェクトメタデータとは

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

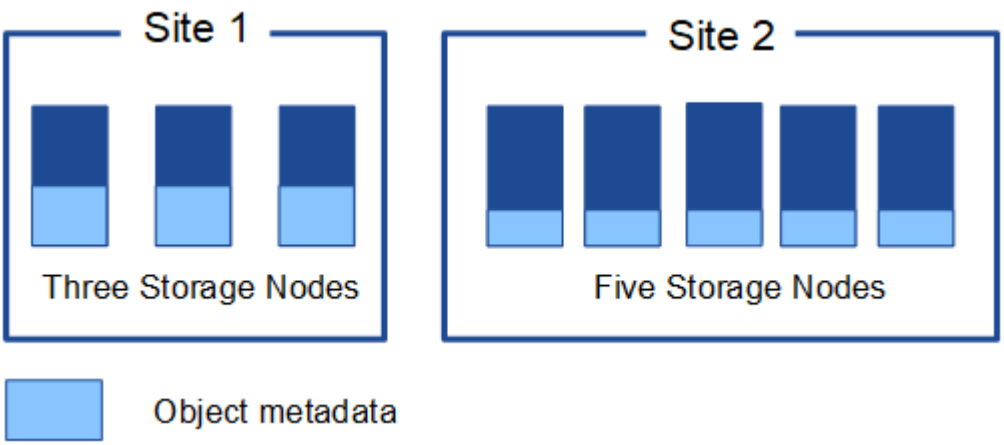
StorageGRID のオブジェクトの場合、オブジェクトメタデータには次の種類の情報が含まれます。

- システムメタデータ（各オブジェクト（UUID）の一意のID、オブジェクト名、S3バケットの名前、テナントアカウントの名前またはID、オブジェクトの論理サイズ、オブジェクトの作成日時、オブジェクトの最終変更日時など）。
- オブジェクトに関連付けられているカスタムユーザメタデータのキーと値のペア。
- S3 オブジェクトの場合、オブジェクトに関連付けられているオブジェクトタグのキーと値のペア。
- レプリケートオブジェクトコピーの場合、各コピーの現在の格納場所。
- イレイジャーコーディングオブジェクトコピーの場合、各フラグメントの現在の格納場所。
- クラウドストレージプール内のオブジェクトコピーの場合、外部バケットの名前とオブジェクトの一意の識別子を含むオブジェクトの場所。
- セグメント化されたオブジェクトやマルチパートオブジェクトの場合、セグメント ID とデータサイズ。

オブジェクトメタデータの格納方法

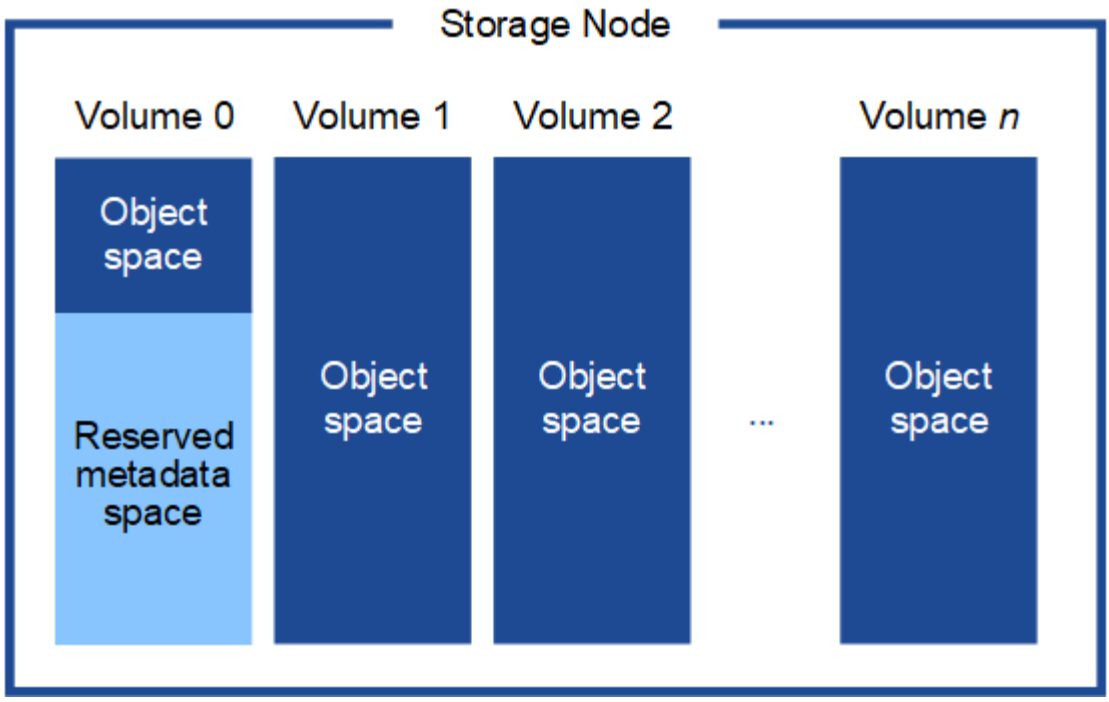
StorageGRID は Cassandra データベースにオブジェクトメタデータを保持し、 Cassandra データベースはオブジェクトデータとは別に格納されます。冗長性を確保し、オブジェクトメタデータを損失から保護するために、 StorageGRID は各サイトのシステム内のすべてのオブジェクトにメタデータのコピーを 3 つずつ格納します。

この図は、 2 つのサイトのストレージノードを表しています。各サイトには同じ量のオブジェクトメタデータが格納され、各サイトのメタデータがそのサイトのすべてのストレージノードに分割されます。



オブジェクトメタデータの格納先

この図は、単一のストレージノードのストレージボリュームを表しています。



図に示すように、 StorageGRID は各ストレージノードのストレージボリューム 0 にオブジェクトメタデータ用のスペースをリザーブします。リザーブスペースを使用してオブジェクトメタデータを格納し、重要なデータベース処理を実行します。ストレージボリューム 0 の残りのスペースとストレージノード内のその他すべてのストレージボリュームは、オブジェクトデータ（レプリケートコピーとイレイジャーコーディングフラグメント）専用に使用されます。

特定のストレージノードでオブジェクトメタデータ用にリザーブされるスペースの量は、いくつかの要因によって異なります。以下にその例を示します。

メタデータリザーブスペースの設定

Metadata reserved space _は、各ストレージノードのボリューム0でメタデータ用にリザーブされるスペースの量を示すシステム全体の設定です。次の表に示すように、この設定のデフォルト値は次の基準に基づいています。

- StorageGRID の最初のインストール時に使用していたソフトウェアバージョン。
- 各ストレージノード上の RAM の容量。

StorageGRID の初期インストールに使用するバージョン	ストレージノード上の **RAM** の容量	**Metadata Reserved Space**のデフォルト設定
12.1	グリッド内の各ストレージノードで 128GB 以上	20 TB （20,000 GB）
	グリッド内の任意のストレージノードで 128GB 未満	3TB （ 3 、 000GB ）
11.5～12.0	グリッド内の各ストレージノードで 128GB 以上	8 TB （ 8 、 000 GB ）

StorageGRID の初期インストールに使用するバージョン	ストレージノード上の **RAM** の容量	**Metadata Reserved Space**のデフォルト設定
	グリッド内の任意のストレージノードで 128GB 未満	3TB （ 3 、 000GB ）
11.1～11.4	いずれかのサイトの各ストレージノードで 128GB 以上	4TB （ 4 、 000GB ）
	各サイトのストレージノードで 128GB 未満	3TB （ 3 、 000GB ）
11.0以前	任意の金額	2TB （ 2 、 000 GB ）

メタデータリザーブスペースの設定を表示

StorageGRIDシステムのMetadata Reserved Space設定を表示するには、次の手順を実行します。

手順

1. 構成 > システム > *ストレージ設定*を選択します。
2. [ストレージ設定]ページで、*[メタデータリザーブスペース]*セクションを展開します。

StorageGRID 11.8以降では、Metadata Reserved Spaceの値が100GB以上1PB以下である必要があります。

各ストレージノードに128 GB以上のRAMが搭載されている新しい StorageGRID 12.1以降のインストールのデフォルト設定は、20,000 GB（20 TB）です。

メタデータ用にリザーブされている実際のスペース

システム全体のMetadata Reserved Space設定とは異なり、オブジェクトメタデータ用の_actual reserved space_forはストレージノードごとに決定されます。あるストレージノードについて、メタデータ用に実際にリザーブされるスペースは、そのノードのボリューム0のサイズ、およびシステム全体でのMetadata Reserved Spaceの設定によって異なります。

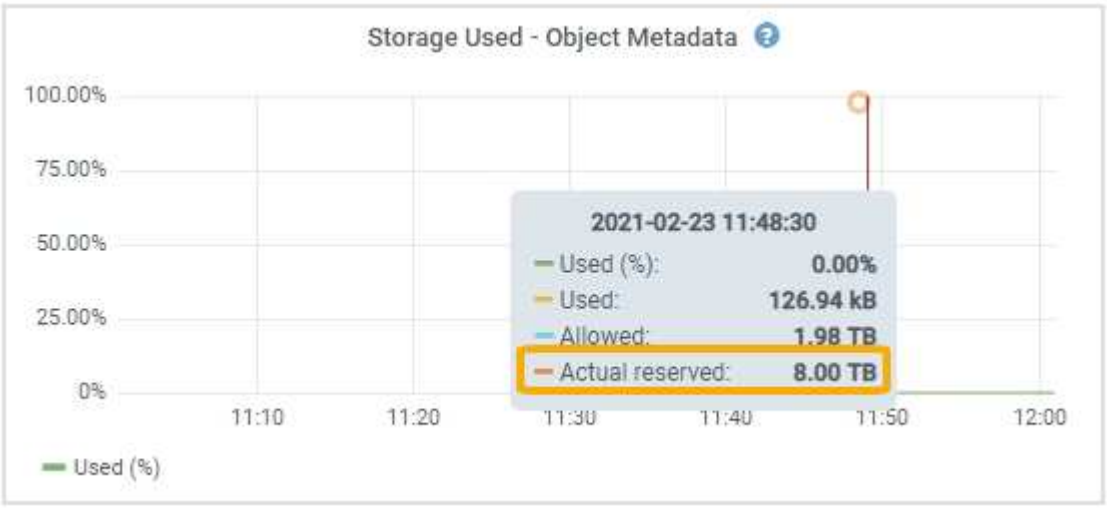
ノードのボリューム **0** のサイズ	メタデータ用にリザーブされている実際のスペース
500 GB未満（非本番環境での使用）	ボリューム 0 の 10%
500GB以上のメタデータ専用ストレージノード	次の値のうち小さい方： • ボリューム0 • メタデータリザーブスペースの設定 注：メタデータのみのストレージノードに必要なrangedbは1つだけです。

メタデータ用に実際にリザーブされているスペースを表示する

特定のストレージノードでメタデータ用に実際にリザーブされているスペースを表示する手順は、次のとおりです。

手順

1. グリッド マネージャーから、[ノード] > [ストレージ ノード] を選択します。
2. [* ストレージ *] タブを選択します。
3. [Storage Used - Object Metadata]グラフにカーソルを合わせ、* Actual Reserved *の値を確認します。



スクリーンショットでは、実際のリザーブ値は 20 TB です。このスクリーンショットは、新しい StorageGRID 12.1 インストールにおける大規模ストレージノード向けのものです。ボリューム 0 は少なくとも 20 TB であるため、デフォルトのシステム全体のメタデータ リザーブ スペース設定を使用します。

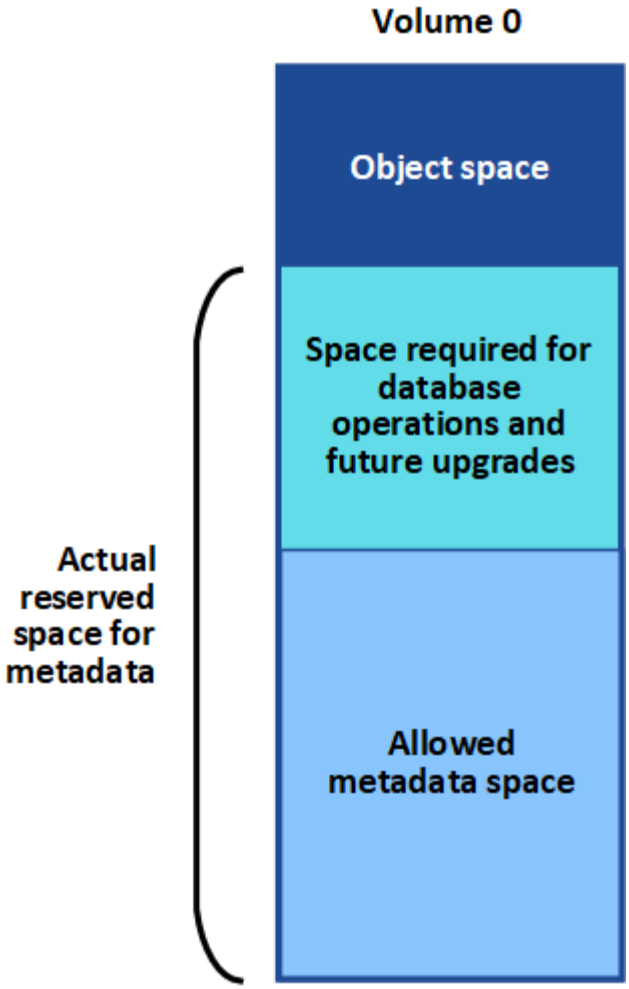
実際のリザーブ スペース（メタデータ）の例

バージョン12.1以降を使用して新しいStorageGRIDシステムをインストールするとします。この例では、各ストレージノードに128 GBを超えるRAMが搭載されており、ストレージノード1（SN1）のボリューム0が6 TBであると仮定します。これらの値に基づくと：

- システム全体の*メタデータ リザーブ スペース*は 20 TB に設定されています。（これは、各ストレージノードの RAM が 128 GB を超える場合に、新しい StorageGRID 12.1 以降をインストールする際のデフォルト値です。）
- SN1のメタデータ用の*実際のリザーブ スペース*は6TBです。（ボリューム0が*メタデータのリザーブ スペース*設定よりも小さいため、ボリューム全体が予約されています。）

許可されているメタデータスペースです

メタデータ用に実際に予約されている各ストレージノードは、オブジェクトメタデータに使用できるスペース（許容されるメタデータスペース _ ）と、重要なデータベース処理（コンパクションや修復など）や将来のハードウェアおよびソフトウェアのアップグレードに必要なスペースに分割されます。許可されるメタデータスペースは、オブジェクトの全体的な容量を決定します。



次の表に、各ストレージノードのメモリ容量とメタデータ用に実際にリザーブされているスペースに基づいてStorageGRID で許容されるメタデータスペース*がどのように計算されるかを示します。

		ストレージノード上のメモリ容量	
	<128 GB	>=128 GB	メタデータ用に実際にリザーブされているスペース
⇐4 TB	メタデータの実際のリザーブ スペースの75%（最大1.32 TB）	メタデータ用の実際のリザーブ スペースの75%（最大1.98 TB）	&GT；4 TB

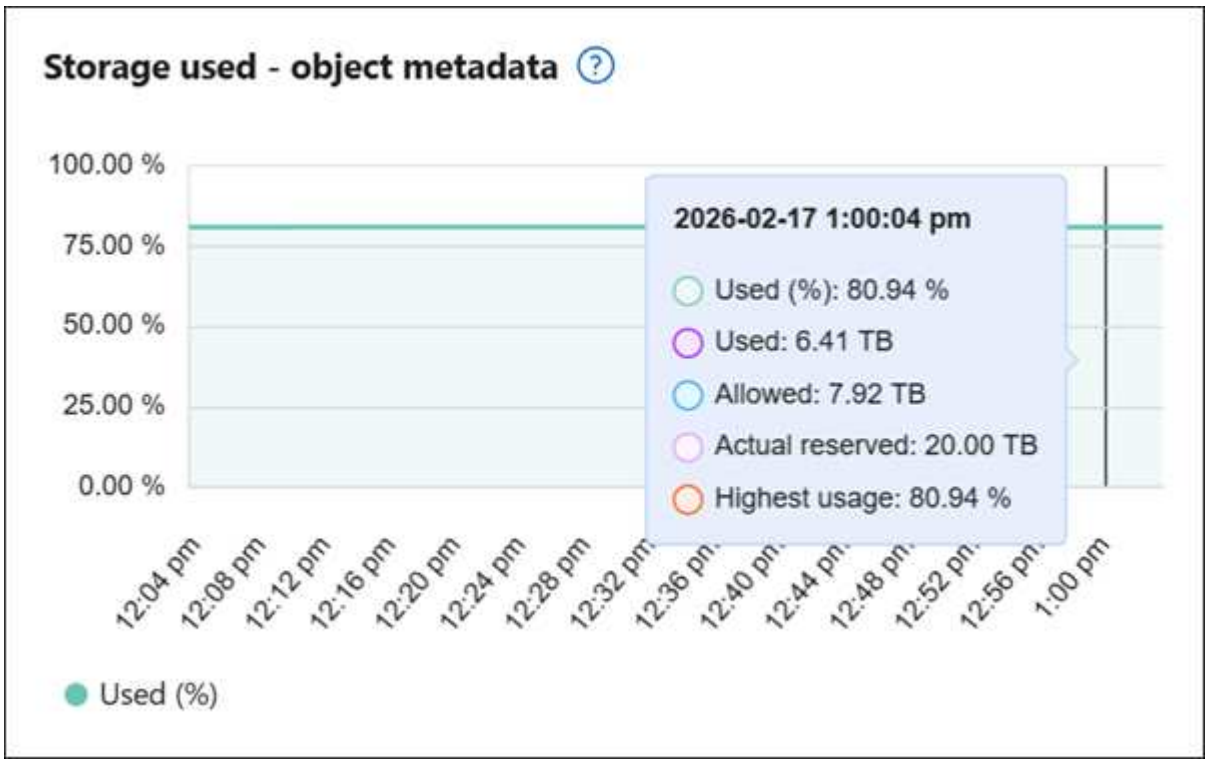
許可されているメタデータスペースを表示する

ストレージノードで許可されているメタデータスペースを表示するには、次の手順を実行します。

手順

1. グリッド マネージャーから、[ノード] を選択します。
2. ストレージノードを選択します。

3. [* ストレージ *] タブを選択します。
4. [Storage Used - object metadata]グラフにカーソルを合わせ、* allowed *の値を確認します。



スクリーンショットでは、*許可*の値は 7.92 TB です。これは、メタデータの実際のリザーブ スペースが 4 TB を超えるストレージノードの最大値です。

「 * Allowed * 」の値は、次の Prometheus 指標に対応します。

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

許可されるメタデータスペースの例

バージョン12.1以降を使用して新しいStorageGRIDシステムをインストールするとします。この例では、各ストレージノードに128 GBを超えるRAMが搭載されており、ストレージノード1（SN1）のボリューム0が6 TBであると仮定します。これらの値に基づくと：

- システム全体の*メタデータ リザーブ スペース*は 20 TB に設定されています。（これは、各ストレージノードの RAM が 128 GB を超える場合に、新しい StorageGRID 12.1 以降をインストールする際のデフォルト値です。）
- SN1のメタデータ用の*実際のリザーブ スペース*は6TBです。（ボリューム0が*メタデータのリザーブ スペース*設定よりも小さいため、ボリューム全体が予約されています。）
- SN1 のメタデータの*許可*容量は 3.75 TB です。これは、メタデータに使用できるスペースの表に示す計算式に基づいています：（メタデータの実際のリザーブ スペース – 1 TB）× 75%、最大 7.92 TB。

サイズの異なるストレージノードがオブジェクト容量に与える影響

前述したように、 StorageGRID は各サイトのストレージノードにオブジェクトメタデータを均等に分散します。このため、サイトにサイズが異なるストレージノードがある場合、サイトで一番小さいノードがサイトの

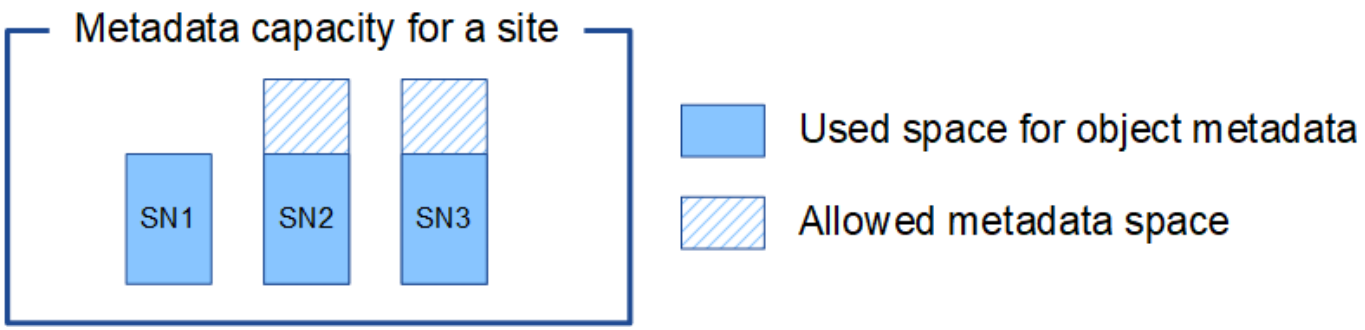
メタデータ容量を決定します。

次の例を考えてみましょう。

- サイズの異なる 3 つのストレージノードを含む単一サイトのグリッドがある。
- Metadata Reserved Space *設定は4TBです。
- ストレージノードには、リザーブされている実際のメタデータスペースと許可されているメタデータスペースについて、次の値があります。

ストレージノード	ボリューム 0 のサイズ	リザーブされている実際のメタデータスペースです	許可されているメタデータスペースです
SN1	2.2TB	2.2TB	1.32TB
SN2	5TB	4TB	1.98TB
SN3	6TB	4TB	1.98TB

オブジェクトメタデータはサイトのストレージノード間で均等に分散されるため、この例の各ノードが格納できるメタデータは 1.32TB です。SN2およびSN3で使用できる追加の0.66TBのメタデータスペースは使用できません。



同様に、 StorageGRID は各サイトで StorageGRID システムのすべてのオブジェクトメタデータを管理するため、 StorageGRID システム全体のメタデータ容量は最小サイトのオブジェクトメタデータ容量で決まります。

また、オブジェクトメタデータの容量はオブジェクトの最大数に制御されるため、一方のノードがメタデータの容量を超えると、実質的にグリッドがフルになります。

関連情報

- 各ストレージノードのオブジェクトメタデータ容量を監視する方法については、の手順を参照してください"StorageGRID の監視"。
- システムのオブジェクトメタデータ容量を増やすには、"グリッドを展開する"新しいストレージノードを追加します。

StorageGRID でメタデータ予約領域の設定を増やす

ストレージノードがRAMおよび使用可能スペースに関する特定の要件を満たしている場

合は、Metadata Reserved Spaceシステム設定を増やすことができます。

必要なもの

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたは"ルートアクセス権限またはその他のグリッド構成権限"。

タスクの内容

システム全体のMetadata Reserved Space設定を手動で8TBに増やすことができます。

次の両方に該当する場合にのみ、「 Metadata Reserved Space 」設定の値を増やすことができます。

- システムの任意のサイトのストレージノードには、それぞれ 128GB 以上の RAM が搭載されています。
- システムの任意のサイトのストレージノードには、ストレージボリューム 0 上に十分な利用可能スペースがあります。

この設定を大きくすると、すべてのストレージノードのストレージボリューム 0 でオブジェクトストレージに使用できるスペースが同時に減少することに注意してください。そのため、想定されるオブジェクトメタデータの要件に基づいて、 Metadata Reserved Space を 8TB 未満の値に設定することを推奨します。

> 一般的には、より低い値ではなく、より高い値を使用することをお勧めします。Metadata Reserved Space 設定が大きすぎる場合は、あとで設定を縮小できます。一方、値をあとで大きくした場合は、オブジェクトデータを移動してスペースを解放しなければならないことがあります。

Metadata Reserved Spaceの設定が特定のストレージノードでオブジェクトメタデータストレージに使用できるスペースに与える影響の詳細については、を参照してください"オブジェクトメタデータストレージを管理する"。

手順

1. 現在の Metadata Reserved Space 設定を確認します。
   a. 構成 > システム > *ストレージ設定*を選択します。
   b. *メタデータ予約領域*の値をメモします。
2. この値を増やすには、各ストレージノードのストレージボリューム 0 に十分な利用可能スペースがあることを確認してください。
   a. *ノード*を選択します。
   b. グリッドの最初のストレージノードを選択します。
   c. Storage （ストレージ）タブを選択します。
   d. Volumes セクションで、 * /var/local/rangedb/0 * エントリを探します。
   e. 使用可能な値が、使用する新しい値と現在の Metadata Reserved Space 値の差以上であることを確認します。

      たとえば、 Metadata Reserved Space 設定が現在 4TB の場合に、 6TB に拡張するには、使用可能な値を 2TB 以上にする必要があります。

   f. すべてのストレージノードに対して上記の手順を繰り返します。

- 1 つ以上のストレージノードに十分な利用可能スペースがない場合は、 Metadata Reserved Space の値を増やすことはできません。この手順は続行しないでください。
- 各ストレージノードのボリューム 0 に十分な利用可能スペースがある場合は、次の手順に進みます。

3. 各ストレージノードに 128GB 以上の RAM があることを確認してください。
   a. *ノード*を選択します。
   b. グリッドの最初のストレージノードを選択します。
   c. [* ハードウェア *] タブを選択します。
   d. メモリ使用状況グラフにカーソルを合わせます。合計メモリ * が 128 GB 以上であることを確認します。
   e. すべてのストレージノードに対して上記の手順を繰り返します。
      - 1 つ以上のストレージノードに使用可能な合計メモリが十分にない場合は、 Metadata Reserved Space の値を増やすことはできません。この手順は続行しないでください。
      - 各ストレージノードの合計メモリが 128GB 以上の場合は、次の手順に進みます。
4. Metadata Reserved Space 設定を更新します。
   a. 構成 > システム > *ストレージ設定*を選択します。
   b. *メタデータ予約領域*を選択します。
   c. 新しい値を入力します。

      たとえば、サポートされている最大値である 8TB を入力するには、「 * 8000000000000 * （ 8 、 0 が 12 個）」と入力します。

   d. [保存（ Save ）] を選択します。

StorageGRID に保存されたオブジェクトを圧縮

オブジェクトの圧縮を有効にすると、StorageGRID に格納されているオブジェクトのサイズを縮小して、オブジェクトによるストレージ消費量を削減できます。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- そうだな "特定のアクセス権限"

タスクの内容

デフォルトでは、オブジェクトの圧縮は無効になっています。圧縮を有効にすると、StorageGRID はロスレス圧縮を使用して各オブジェクトを保存時に圧縮しようとします。

> この設定を変更すると、新しい設定が適用されるまで約 1 分かかります。設定した値は、パフォーマンスと拡張用にキャッシュされます。

オブジェクトの圧縮を有効にする前に、次の点に注意してください。

- 格納されているデータが圧縮可能であることがわかっている場合を除き、*[Compress stored objects]*を選択しないでください。

- StorageGRID にオブジェクトを保存するアプリケーションは、オブジェクトを圧縮してから保存することがあります。クライアントアプリケーションがすでにオブジェクトを圧縮してからStorageGRID に保存している場合は、このオプションを選択してもオブジェクトのサイズがさらに縮小されることはありません。
- StorageGRID でNetApp FabricPool を使用している場合は、[Compress Stored Objects]*を選択しないでください。
- [Compress stored objects]*を選択した場合は、返されるバイト数の範囲を指定するGetObject処理をS3クライアントアプリケーションで実行しないようにしてください。これらの「範囲読み取り」処理は効率的ではありません。StorageGRIDでは、要求されたバイトにアクセスするためにオブジェクトの圧縮を実質的に解除する必要があるためです。非常に大きなオブジェクトから小さい範囲のバイト数を要求するGetObject処理は特に非効率的です。たとえば、50GBの圧縮オブジェクトから10MBの範囲を読み取る処理は非効率的です。

  圧縮オブジェクトから範囲を読み取ると、クライアント要求がタイムアウトする可能性があります。

  オブジェクトを圧縮する必要があり、クライアントアプリケーションが範囲読み取りを使用する必要がある場合は、アプリケーションの読み取りタイムアウトを増やしてください。

手順

1. 構成 > システム > ストレージ設定 > *オブジェクト圧縮*を選択します。
2. [Compress stored objects]*チェックボックスを選択します。
3. [保存（ Save ）] を選択します。

StorageGRID でストレージノード全体を管理

ストレージノードの容量が上限に達した場合は、新しいストレージを追加して StorageGRID システムを拡張する必要があります。ストレージボリュームの追加、ストレージ拡張シェルフの追加、ストレージノードの追加の 3 つのオプションがあります。

ストレージボリュームを追加します

各ストレージノードは最大数のストレージボリュームをサポートします。定義されている最大値はプラットフォームによって異なります。ストレージノードのストレージボリュームが最大数より少ない場合は、ボリュームを追加して容量を増やすことができます。の手順を参照してください"StorageGRID システムの拡張"。

ストレージ拡張シェルフを追加する

一部のStorageGRIDアプライアンスストレージノード（SG6060やSG6160など）では、追加のストレージシェルフをサポートできます。拡張機能が最大容量まで拡張されていない StorageGRID アプライアンスがある場合は、ストレージシェルフを追加して容量を増やすことができます。の手順を参照してください"StorageGRID システムの拡張"。

ストレージノードを追加します

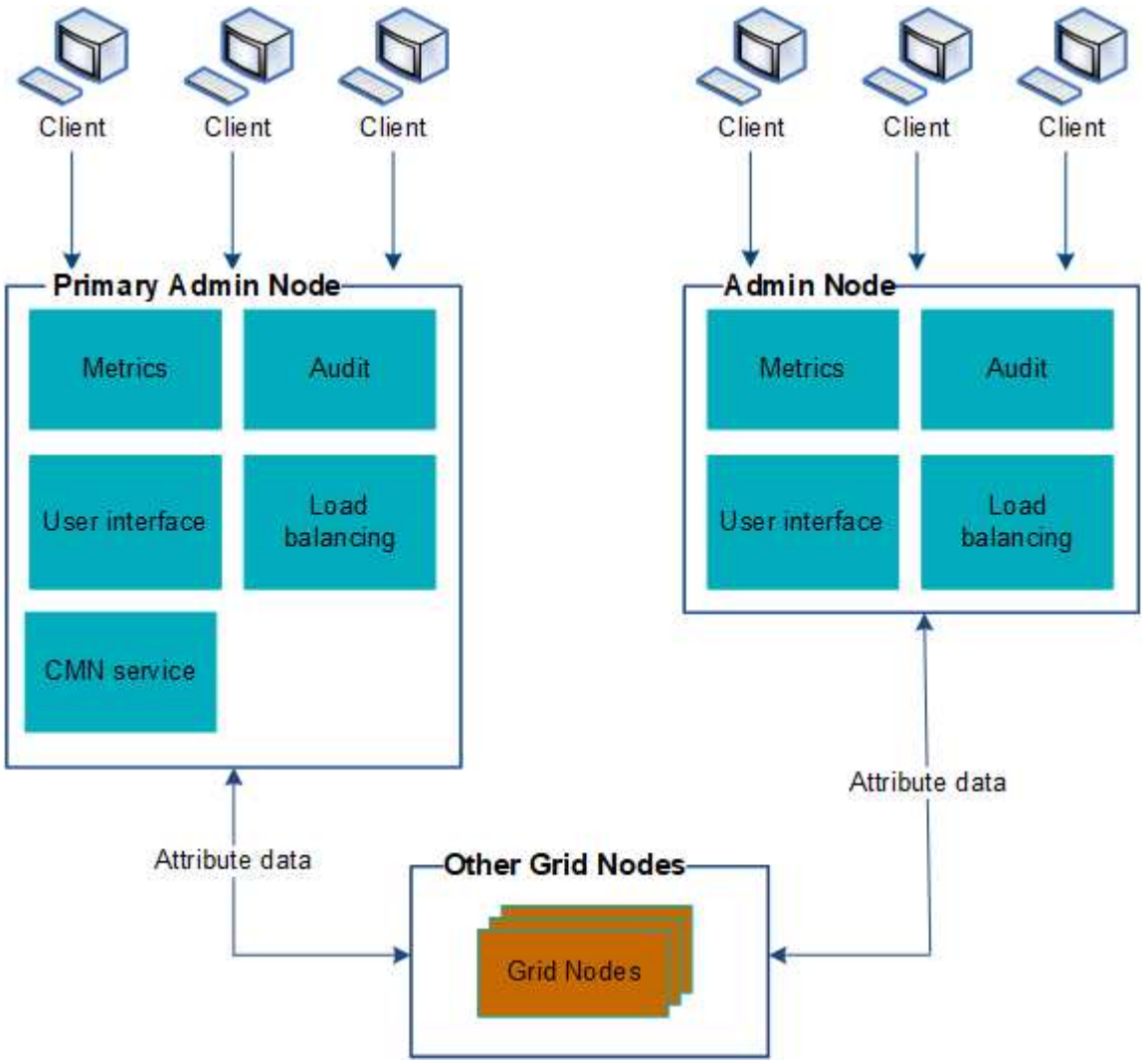
ストレージノードを追加してストレージ容量を増やすことができます。ストレージを追加する場合は、現在アクティブな ILM ルールと容量の要件について慎重に検討する必要があります。の手順を参照してください"StorageGRID システムの拡張"。

管理ノードを管理する

StorageGRID で複数の管理ノードを使用する

StorageGRID システムには複数の管理ノードを含めることができます。これにより、 1 つの管理ノードに障害が発生した場合でも、 StorageGRID システムを継続的に監視して設定することができます。

ある管理ノードが使用できなくなっても属性の処理は続行され、アラートは引き続きトリガーされ、Eメール通知とAutoSupportパッケージは引き続き送信されます。ただし、管理ノードを複数配置しても、通知とAutoSupportパッケージを除き、フェイルオーバー保護は提供されません。



管理ノードに障害が発生した場合、次の 2 つの方法で StorageGRID システムを引き続き表示および設定することができます。

- Web クライアントは使用可能な他の管理ノードに再接続できます。
- システム管理者が管理ノードのハイアベイラビリティグループを設定している場合、 Web クライアントは HA グループの仮想 IP アドレスを使用して引き続き Grid Manager または Tenant Manager にアクセスできます。を参照して "ハイアベイラビリティグループを管理します"

HAグループを使用している場合、アクティブな管理ノードで障害が発生するとアクセスが中断されます。ユーザは、 HA グループの仮想 IP アドレスがグループ内の別の管理ノードにフェイルオーバーしたあとで、再度サインインする必要があります。

一部のメンテナンスタスクはプライマリ管理ノードでしか実行できません。プライマリ管理ノードに障害が発生した場合、そのノードをリカバリするまでは、 StorageGRID システムは完全に機能している状態ではありません。

StorageGRID でプライマリ管理ノードを特定します

プライマリ管理ノードは、非プライマリ管理ノードよりも多くの機能を提供します。たとえば、一部のメンテナンス手順はプライマリ管理ノードを使用して実行する必要があります。

管理ノードの詳細については、を参照してください"管理ノードとは"。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- そうだな "特定のアクセス権限"

手順

1. *ノード*を選択します。
2. 検索ボックスに「* primary *」と入力します。

   検索結果で、[Type]列に「Primary Admin Node」が表示されているノードを特定します。プライマリ管理ノードが1つ表示されます。

ILM を使用してオブジェクトを管理する

StorageGRID で ILM を使用してオブジェクトを管理

ILMポリシーの情報ライフサイクル管理（ILM）ルールは、オブジェクトデータのコピーを作成および分散する方法と、それらのコピーを一定の期間にわたって管理する方法をStorageGRIDに指示します。

これらの手順について

ILMルールとポリシーを設計、実装するには慎重な計画が必要です。運用要件、 StorageGRID システムのトポロジ、オブジェクト保護のニーズ、使用可能なストレージタイプについて理解しておく必要があります。次に、さまざまなタイプのオブジェクトをどのようにコピー、分散、および格納するかを決定する必要があります。

次の手順に従って、次の操作を行います

- を含むStorageGRID ILMについて説明します。"オブジェクトのライフサイクル全体にわたるILMの動作"
- "ストレージプール"、"クラウドストレージプール"、を構成する方法について説明します。"ILM ルール"

- これで1つ以上のサイトのオブジェクトデータを保護する方法について説明します。"ILMポリシーを作成、シミュレート、アクティブ化します"
- "S3オブジェクトロックを使用してオブジェクトを管理します"特定のS3バケット内のオブジェクトが指定した期間削除または上書きされないようにする方法について説明します。

詳細

詳細については、次のビデオをご覧ください。

ILMルールの概要

ILMポリシーの概要

ILM とオブジェクトライフサイクル

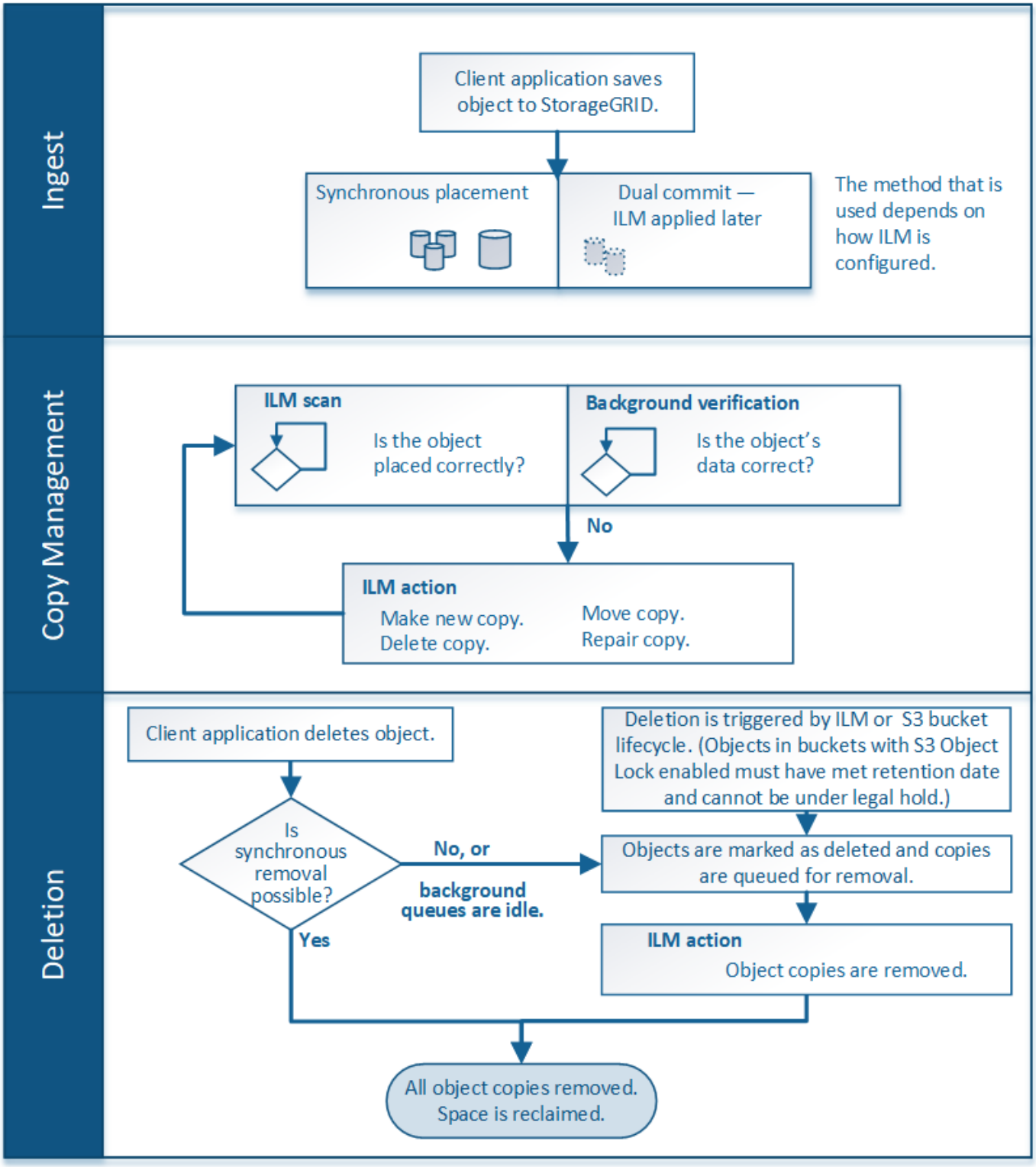
StorageGRID でオブジェクトのライフサイクル全体を通じて **ILM** がどのように動作するか

StorageGRID での ILM を使用したオブジェクト管理方法を理解することは、ポリシーをより効果的に設計するうえで役立ちます。

- 取り込み：S3クライアントアプリケーションがStorageGRIDシステムへの接続を確立してオブジェクトを保存すると取り込みが開始され、StorageGRIDがクライアントに「ingest successful」というメッセージを返すと取り込みが完了します。ILM 要件の指定方法に応じて、 ILM の手順を即座に適用（同期配置）するか、中間コピーを作成して ILM をあとから適用（デュアルコミット）することで、オブジェクトデータは取り込み時に保護されます。
- * コピー管理 * ： ILM の配置手順に指定された数とタイプのオブジェクトコピーを作成すると、StorageGRID はオブジェクトの場所を管理し、オブジェクトを損失から保護します。
  - * ILMのスキャンと評価*：StorageGRIDはグリッドに格納されているオブジェクトのリストを継続的にスキャンし、現在のコピーがILMの要件を満たしているかどうかをチェックします。タイプ、数、または場所が異なるオブジェクトコピーが必要となった場合、 StorageGRID は必要に応じてコピーを作成、削除、または移動します。
  - バックグラウンド検証：StorageGRIDは、オブジェクトデータの整合性をチェックするためにバックグラウンド検証を継続的に実行します。問題が検出されると、 StorageGRID は、現在の ILM 要件を満たす場所に、新しいオブジェクトコピーまたは置き換え用のイレイジャーコーディングオブジェクトフラグメントを自動的に作成します。を参照して "オブジェクトの整合性を検証"
- * オブジェクトの削除 * ： StorageGRID システムからすべてのコピーが削除されると、オブジェクトの管理は終了します。オブジェクトは、クライアントによる削除要求、または S3 バケットライフサイクルの終了が原因の ILM による削除または削除が原因で削除されます。

> S3オブジェクトロックが有効になっているバケット内のオブジェクトは、リーガルホールドの対象になっている場合やretain-until-dateが指定されていてもまだ満たされていない場合は削除できません。

次の図は、オブジェクトのライフサイクル全体にわたる ILM の動作をまとめたものです。



オブジェクトの取り込み方法

StorageGRIDのILM取り込みオプション

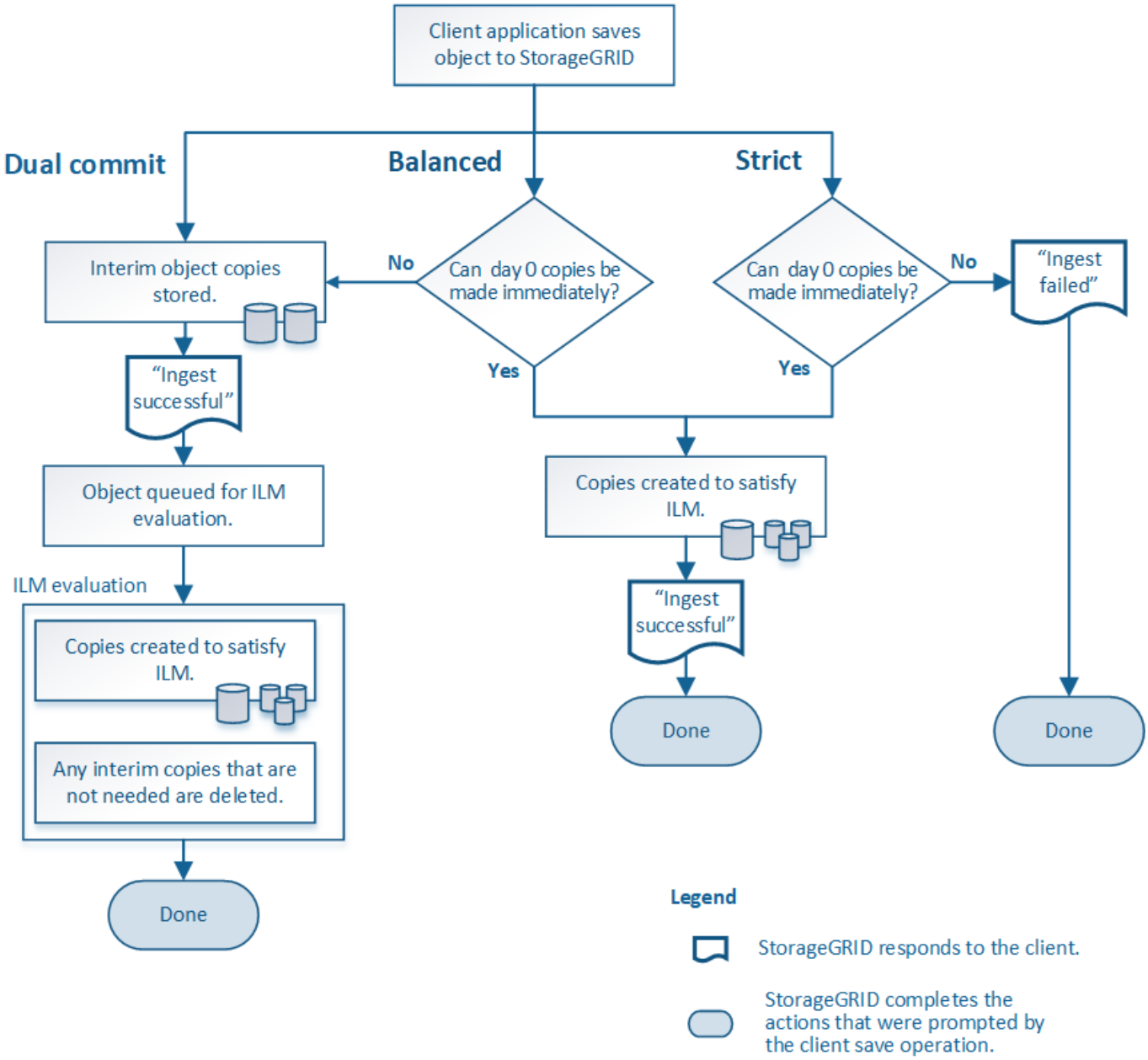
ILMルールを作成するときは、取り込み時にオブジェクトを保護するための3つのオプション（Dual commit、Strict、またはBalanced）のいずれかを指定します。

選択したオプションに応じて、 StorageGRID は、中間コピーを作成してオブジェクトをキューに登録し、あ

とで ILM 評価を実行するか、または同期配置を使用してコピーをただちに作成して ILM 要件を満たします。

取り込みオプションのフローチャート

次のフローチャートは、 3 つの取り込みオプションのそれぞれを使用する ILM ルールにオブジェクトが一致した場合の動作を示しています。



デュアルコミット

[Dual commit]オプションを選択すると、StorageGRIDは2つの異なるストレージノードに中間オブジェクトコピーをただちに作成し、「ingest successful」メッセージをクライアントに返します。オブジェクトは ILM 評価のキューに登録され、ルールの配置手順を満たすコピーはあとで作成されます。デュアルコミットの直後にILMポリシーを処理できないと、サイト障害からの保護の実現に時間がかかることがあります。

次のいずれかの場合に Dual commit オプションを使用します。

- マルチサイトの ILM ルールを使用しており、クライアントの取り込みレイテンシを考慮する必要があります。Dual commitを使用する場合は、デュアルコミットコピーがILMを満たしていない場合にデュアルコミットコピーを作成および削除する追加作業をグリッドで実行できるようにする必要があります。具体的には：
  - ILM のバックログが発生しないように、グリッドの負荷が十分に低い必要があります。
  - グリッドにハードウェアリソース（ IOPS 、 CPU 、メモリ、ネットワーク帯域幅など）が余剰である。
- マルチサイトの ILM ルールを使用していて、通常はサイト間の WAN 接続のレイテンシが高くなっているか、帯域幅が制限されている。このシナリオでは、 Dual commit オプションを使用するとクライアントのタイムアウトを回避できます。Dual commit オプションを選択する前に、現実的なワークロードでクライアントアプリケーションをテストする必要があります。

Balanced（デフォルト）

Balanced オプションを選択した場合も、 StorageGRID は、取り込み時に同期配置を使用してルールの配置手順で指定されたすべてのコピーをただちに作成します。Strictオプションとは対照的に、すべてのコピーをただちに作成できない場合、StorageGRID は代わりにDual commitを使用します。ILMポリシーが複数のサイトに配置を使用していて、サイト障害から即座に保護できない場合は、* ILM placement unachievable *アラートがトリガーされます。

Balanced オプションは、データ保護、グリッドパフォーマンス、および取り込みの成功の最適な組み合わせを実現するために使用します。Balancedは、Create ILM Ruleウィザードのデフォルトのオプションです。

strict

Strict オプションを選択すると、 StorageGRID は取り込み時に同期配置を使用してルールの配置手順で指定されたすべてのオブジェクトコピーをただちに作成します。必要なストレージの場所が一時的に使用できないなどの理由で、StorageGRID がすべてのコピーを作成できない場合、取り込みは失敗します。クライアントは処理を再試行する必要があります。

Strict オプションは、 ILM ルールに指定された場所にのみオブジェクトをただちに格納するための運用または規制上の要件がある場合に使用してください。たとえば、規制要件を満たすために、Strictオプションと高度なフィルタ「Location Constraint」を使用して、特定のデータセンターにオブジェクトが格納されないようにする必要がある場合があります。

を参照して "例 5 ：取り込み動作が Strict の場合の ILM ルールとポリシー"

StorageGRIDにおけるILM取り込みオプションの利点、欠点、制限

取り込み時にデータを保護するための 3 つのオプション（ Balanced 、 Strict 、 Dual commit ）のそれぞれのメリットとデメリットを理解することは、 ILM ルールに選択するオプションを決定する際に役立ちます。

取り込みオプションの概要については、を参照してください"取り込みオプション"。

Balanced オプションと **Strict** オプションのメリット

取り込み時に中間コピーを作成する Dual commit と比較すると、 2 つの同期配置オプションには次のメリットがあります。

- * Better データ セキュリティ * ：オブジェクトデータは、 ILM ルールの配置手順に従ってただちに保護さ

れます。配置手順は、複数の格納場所の障害など、さまざまな障害状況からオブジェクトを保護するように設定できます。Dual commit で保護できるのは、単一のローカルコピーの損失のみです。

- * グリッド処理の効率化 * ：各オブジェクトは、取り込み時に 1 回だけ処理されます。StorageGRID システムで中間コピーを追跡または削除する必要がないため、処理の負荷が軽減され、消費されるデータベーススペースも少なくてすみます。
- * （ Balanced ） Recommended * ： Balanced オプションは、最適な ILM 効率を実現します。Strict取り込み動作が必要な場合、またはグリッドがDual commitの使用条件をすべて満たしている場合を除き、Balancedオプションを使用することを推奨します。
- * （ Strict ）オブジェクトの場所が明らか * ： Strict オプションは、 ILM ルールの配置手順に従ってオブジェクトがただちに格納されることを保証します。

Balanced オプションと **Strict** オプションのデメリット

Dual commit と比較すると、 Balanced オプションと Strict オプションにはいくつかのデメリットがあります。

- * クライアントの取り込み時間が長くなる * ：クライアントの取り込みレイテンシが長くなる可能性があります。BalancedオプションまたはStrictオプションを使用した場合、すべてのイレイジャーコーディングフラグメントまたはレプリケートコピーが作成されて格納されるまで、「ingest successful」メッセージはクライアントに返されません。しかし、ほとんどの場合、オブジェクトデータは最終的な配置までの時間をはるかに短縮できます。
- （**Strict**）取り込みエラーの発生率が高い：Strictオプションを使用すると、StorageGRID がILMルールで指定されたすべてのコピーをすぐに作成できない場合に取り込みが失敗します。必要なストレージの場所が一時的にオフラインになっている場合や、ネットワークでサイト間のオブジェクトコピーが原因 で遅延している場合には、取り込みに失敗する可能性が高くなります。
- * （ Strict ） S3 マルチパートアップロードでは、状況によっては想定どおりに配置されない可能性がある * ： Strict では、オブジェクトが ILM ルールの指定どおりに配置されるか、あるいは取り込みが失敗するかのどちらかの結果が想定されます。ただし、S3マルチパートアップロードの場合は、オブジェクトの各パートの取り込み時にILMが評価され、マルチパートアップロードの完了時にオブジェクト全体に対してILMが評価されます。そのため、次の状況では想定どおりに配置されないことがあります。
  - * S3 マルチパートアップロードの実行中に ILM が変更された場合 * ：各パートはその取り込み時にアクティブなルールに従って配置されるため、マルチパートアップロードが完了した時点でオブジェクトの一部のパートが現在の ILM 要件を満たしていない可能性があります。この場合、オブジェクトの取り込みは失敗しません。代わりに、正しく配置されていないパートはILMルールによる再評価のためにキューに登録され、あとで正しい場所に移動されます。
  - * ILM ルールがサイズでフィルタリングする場合 * ：パーツに対して ILM を評価する際、StorageGRID はオブジェクトのサイズではなくパーツのサイズでフィルタリングします。つまり、オブジェクト全体のILM要件を満たしていない場所にオブジェクトの一部を格納できます。たとえば、10GB 以上のオブジェクトをすべて DC1 に格納し、それより小さいオブジェクトをすべて DC2 に格納するルールの場合、 10 パートからなるマルチパートアップロードの 1GB の各パートは取り込み時に DC2 に格納されます。オブジェクトに対して ILM が評価されると、オブジェクトのすべてのパートが DC1 に移動されます。
- * （ Strict ）オブジェクトタグまたはメタデータが更新され、新たに必要となった配置を実行できなくても取り込みが失敗しない * ： Strict では、オブジェクトが ILM ルールの指定どおりに配置されるか、あるいは取り込みが失敗するかのどちらかの結果が想定されます。ただし、グリッドにすでに格納されているオブジェクトのメタデータまたはタグを更新しても、オブジェクトは再取り込みされません。つまり、更新によってトリガーされたオブジェクト配置の変更はすぐには行われません。通常のバックグラウンド ILM プロセスで ILM が再評価されると、配置変更が行われます。必要な配置変更ができない場合（新たに必要な場所が使用できない場合など）、更新されたオブジェクトは配置変更が可能になるまで現在の配置を保持します。

Balancedオプションと**Strict**オプションを使用したオブジェクトの配置に関する制限事項

BalancedオプションまたはStrictオプションは、次のいずれかの配置手順を含むILMルールには使用できません。

- クラウドストレージプールへの配置： 0 日目
- ルールの[Reference Time]に[User Defined creation time]が設定されている場合のクラウドストレージプール内の配置。

これらの制限は、StorageGRIDがクラウドストレージプールに同期的にコピーを作成できず、ユーザ定義の作成時間が現在の状態に解決される可能性があるためです。

ILMルールと整合性の相互作用によるデータ保護への影響

ILMルールと整合性の選択は、どちらもオブジェクトの保護方法に影響します。これらの設定は対話的に操作できます。

たとえば、ILMルールで選択された取り込み動作はオブジェクトコピーの初期配置に影響し、オブジェクトの格納時に使用される整合性はオブジェクトメタデータの初期配置に影響します。StorageGRIDでは、クライアント要求に対応するためにオブジェクトのデータとメタデータの両方にアクセスする必要があるため、整合性と取り込み動作で同じ保護レベルを選択すると、初期データ保護が向上し、システム応答の予測性が向上します。

StorageGRIDで使用できる整合性の値の概要を次に示します。

- * all *：すべてのノードがオブジェクトメタデータをただちに受信しないと要求が失敗します。
- 強力なグローバル: すべてのサイトにわたるすべてのクライアント要求の書き込み後の読み取り一貫性を保証します。クォーラム セマンティクスが構成されている場合、次の動作が適用されます。
  - グリッドに 3 つ以上のサイトがある場合、クライアント要求に対するサイト障害許容度を許可します。 2 サイト グリッドではサイト障害の許容度はありません。
  - 1 つのサイトがダウンすると、次の S3 操作は成功しません。
    - DeleteBucketEncryption
    - PutBucketBranch
    - PutBucketEncryptionの略
    - PutBucketVersioning
    - PutObjectLegalHold
    - PutObjectLockConfiguration
    - PutObjectRetention

  必要であれば、 "強力なグローバル整合性を実現するStorageGRID Quorumセマンティクスを構成する" 。
- * strong-site *：オブジェクトメタデータがサイト内の他のノードにただちに分散されます。1 つのサイト内のすべてのクライアント要求について、リードアフターライト整合性が保証されます。
- * Read-after-new-write *：新規オブジェクトにはリードアフターライト整合性を提供し、オブジェクトの更新には結果整合性を提供します。高可用性が確保され、データ保護が保証されます。ほとんどの場合に推奨されます。
- * available *：新しいオブジェクトとオブジェクトの更新の両方について、結果整合性を提供します。S3

バケットの場合は、必要な場合にのみ使用します（読み取り頻度の低いログ値を含むバケットや、存在しないキーに対するHEAD処理やGET処理など）。S3 FabricPool バケットではサポートされません。

> 一貫性値を選択する前に、"概要of Consistencyの全文を読む" 。デフォルト値を変更する前に、利点と制限事項を理解しておく必要があります。

整合性ルールと**ILM**ルールの相互作用の例

次の ILM ルールと次の一貫性を持つ 3 つのサイト グリッドがあるとします。

- **ILM** ルール: ローカル サイトに 1 つ、各リモート サイトに 1 つ、合計 3 つのオブジェクト コピーを作成します。厳密な取り込み動作を使用します。
- 一貫性: 強力なグローバル (オブジェクト メタデータは複数のサイトに即座に配布されます)。

クライアントがオブジェクトをグリッドに保存すると、 StorageGRID は3 つのオブジェクト コピーをすべて作成し、メタデータを複数のサイトに配布してから、クライアントに成功を返します。

オブジェクトは、取り込み成功メッセージの時点で損失から完全に保護されます。たとえば、取り込み直後にローカル サイトが失われた場合でも、オブジェクト データとオブジェクト メタデータの両方のコピーがリモート サイトに残ります。オブジェクトは他のサイトから完全に取得可能です。

代わりに同じ ILM ルールと強力なサイト一貫性を使用した場合、オブジェクト データがリモート サイトにレプリケートされた後、オブジェクト メタデータがそこに配布される前に、クライアントは成功メッセージを受信する可能性があります。この場合、オブジェクト メタデータの保護レベルは、オブジェクト データの保護レベルと一致しません。取り込み直後にローカル サイトが失われた場合、オブジェクト メタデータは失われます。オブジェクトを取得できません。

整合性ルールとILMルールの関係は複雑になる可能性があります。サポートが必要な場合は、NetAppにお問い合わせください。

関連情報

"例 5 ：取り込み動作が Strict の場合の ILM ルールとポリシー"

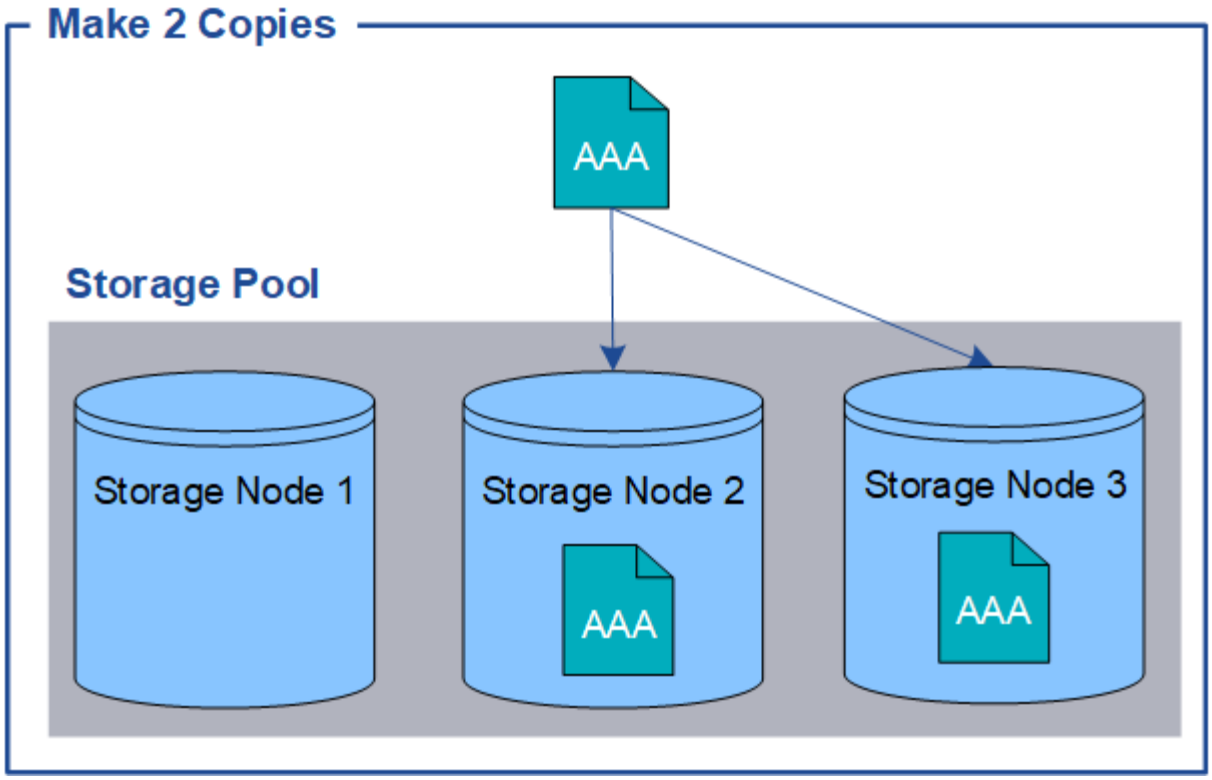
オブジェクトの格納方法（レプリケーションまたはイレイジャーコーディング）

StorageGRIDでのレプリケーションについて学ぶ

レプリケーションは、StorageGRIDがオブジェクトデータを格納するために使用する2つの方法のうちの1つです（もう1つはイレイジャーコーディング）。レプリケーションを使用するILMルールにオブジェクトが一致した場合、オブジェクトデータの完全なコピーが作成されてストレージノードに格納されます。

レプリケートコピーを作成するように ILM ルールを設定する場合は、作成するコピーの数、コピーを配置する場所、およびそれぞれの場所にコピーを格納する期間を指定します。

次の例の ILM ルールは、各オブジェクトのレプリケートコピーを 2 つずつ、 3 つのストレージノードからなるストレージプールに配置するように指定されています。



このルールにオブジェクトが一致した場合、 StorageGRID はオブジェクトのコピーを 2 つ作成して、ストレージプール内の別々のストレージノードにそれぞれのコピーを配置します。この 2 つのコピーは、使用可能な 3 つのストレージノードのうちのいずれか 2 つに配置されます。この場合、ストレージノード 2 と 3 に配置されています。コピーは 2 つあるため、ストレージプール内のいずれかのノードで障害が発生した場合でもオブジェクトを読み出すことができます。

StorageGRID が任意のストレージノードに格納できるレプリケートコピーは 1 つのオブジェクトにつき 1 つだけです。グリッドにストレージノードが 3 つあり、 4 コピーの ILM ルールを作成した場合、作成されるコピーはストレージノードごとに 1 つだけになります。ILM placement unAchievable * アラートがトリガーされ、 ILM ルールを完全に適用できなかったことを示します。

関連情報

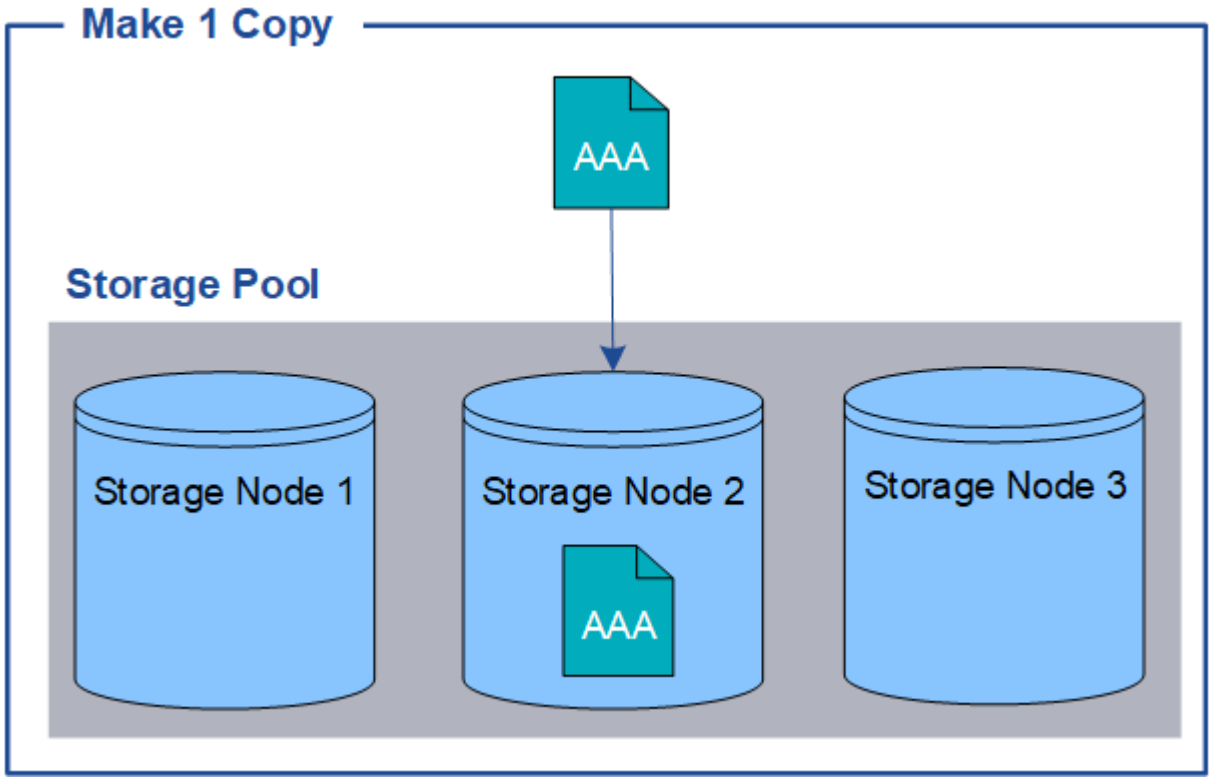
- "イレイジャーコーディングとは"
- "ストレージプールとは"
- "レプリケーションとイレイジャーコーディングを使用してサイト障害から保護"

StorageGRIDにおける単一コピー複製のリスク

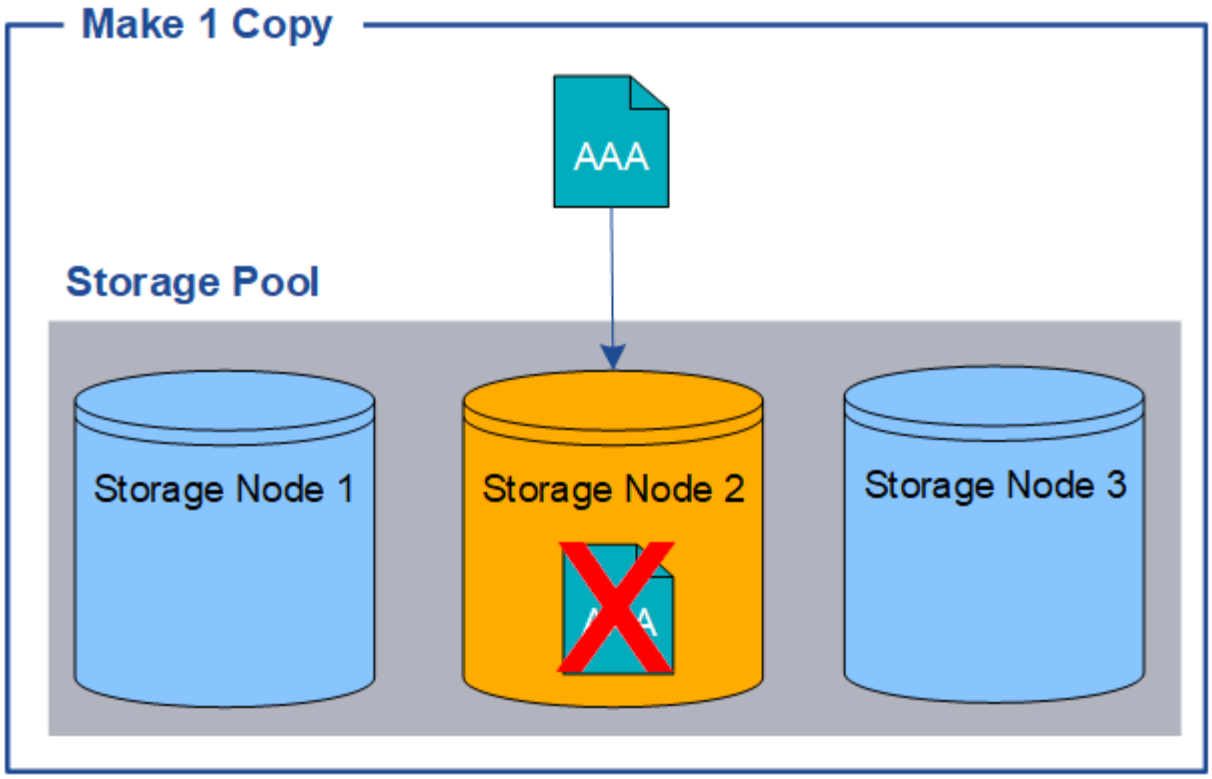
レプリケートコピーを作成する ILM ルールを作成するときは、配置手順の任意の期間に少なくとも 2 つのコピーを指定する必要があります。

任意の期間にレプリケートコピーを1つだけ作成するILMルールは使用しないでください。オブジェクトのレプリケートコピーが 1 つしかない場合、ストレージノードに障害が発生したり、重大なエラーが発生すると、そのオブジェクトは失われます。また、アップグレードなどのメンテナンス作業中は、オブジェクトへのアクセスが一時的に失われます。

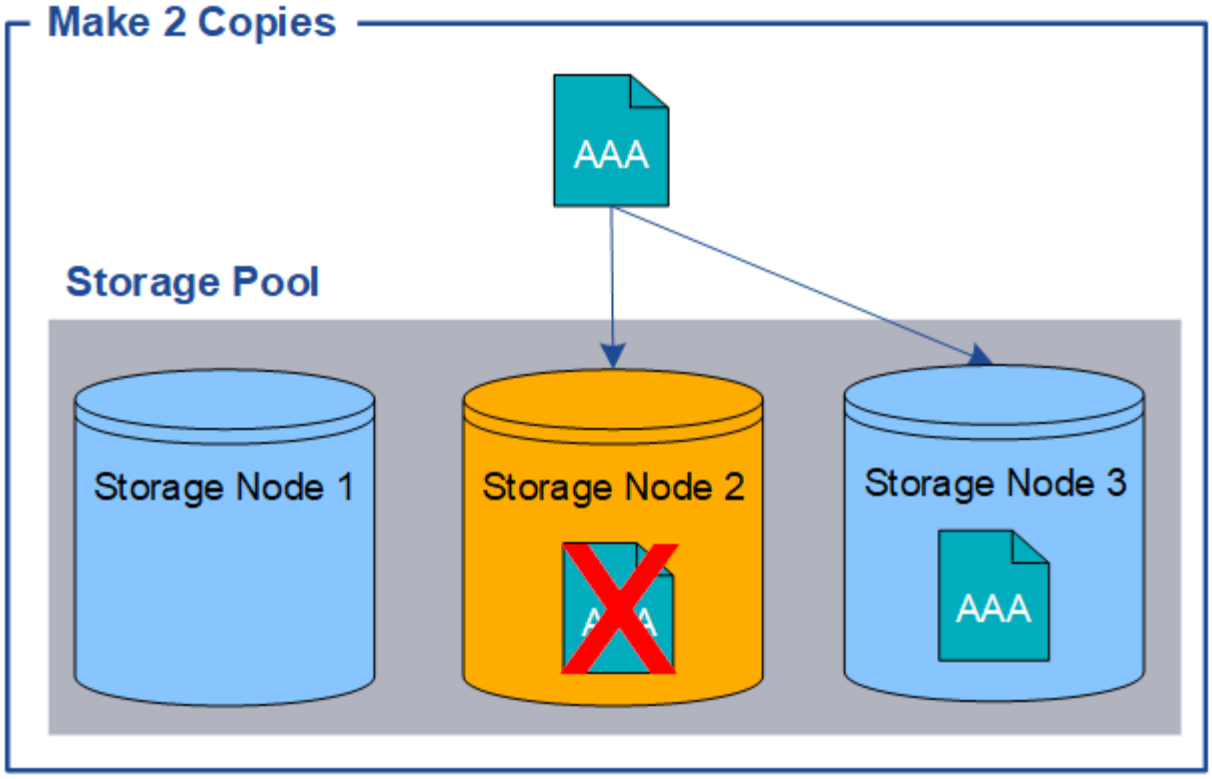
次の例では、 Make 1 Copy ILM ルールによって、 1 つのオブジェクトのレプリケートコピーを 3 つのストレージノードからなるストレージプールに配置するように指定しています。このルールに一致するオブジェクトが取り込まれると、 StorageGRID は 1 つのストレージノードにのみコピーを配置します。



ILM ルールにオブジェクトのレプリケートコピーが 1 つしか作成されていない場合、ストレージノードが使用できなくなるとオブジェクトにアクセスできなくなります。この例では、アップグレードやその他のメンテナンス手順 の実行中など、ストレージノード 2 がオフラインになるとオブジェクト AAA へのアクセスが一時的に失われます。ストレージノード 2 で障害が発生すると、オブジェクト AAA が完全に失われます。



オブジェクトデータの損失を防ぐには、レプリケーションで保護するすべてのオブジェクトのコピーを常に 2 つ以上作成する必要があります。コピーが複数ある場合も、 1 つのストレージノードに障害が発生した場合やオフラインになった場合でもオブジェクトにアクセスできます。



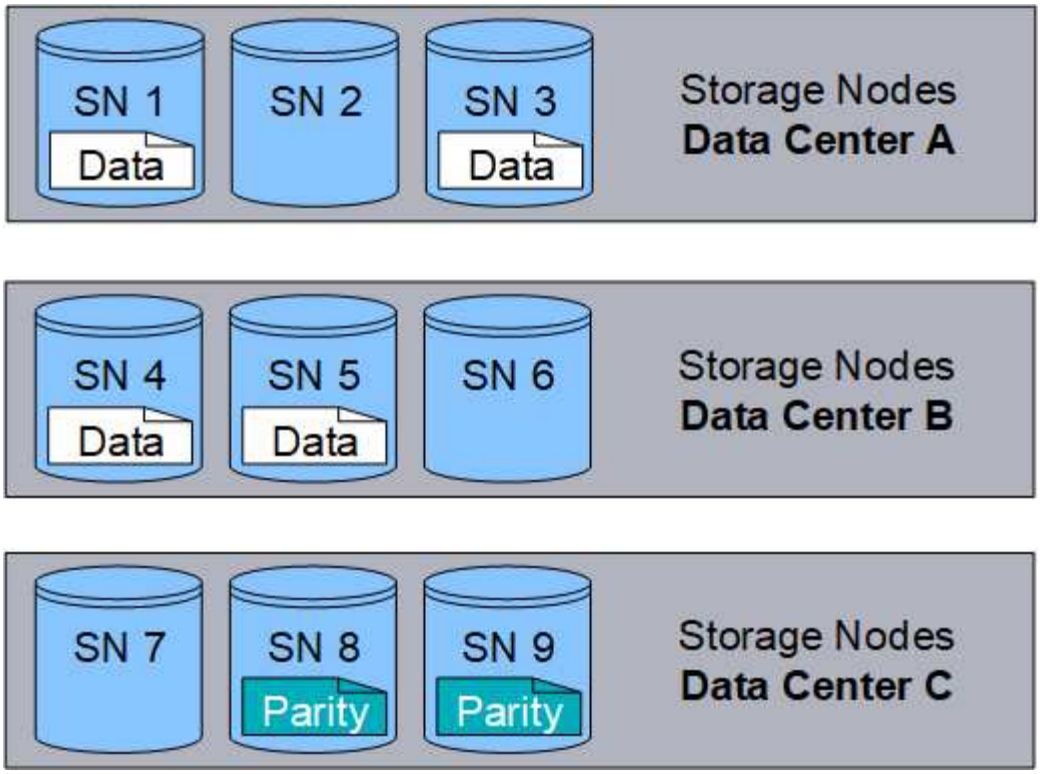
StorageGRID のイレイジャー コーディングについて

イレイジャーコーディングは、StorageGRIDがオブジェクトデータを格納するために使用する2つの方法のうちの1つです（レプリケーションがもう1つの方法です）。イレイジャーコーディングを使用するILMルールにオブジェクトが一致した場合、それらのオブジェクトはデータフラグメントにスライスされ、追加のパリティフラグメントが計算されて、各フラグメントが別 々 のストレージノードに格納されます。

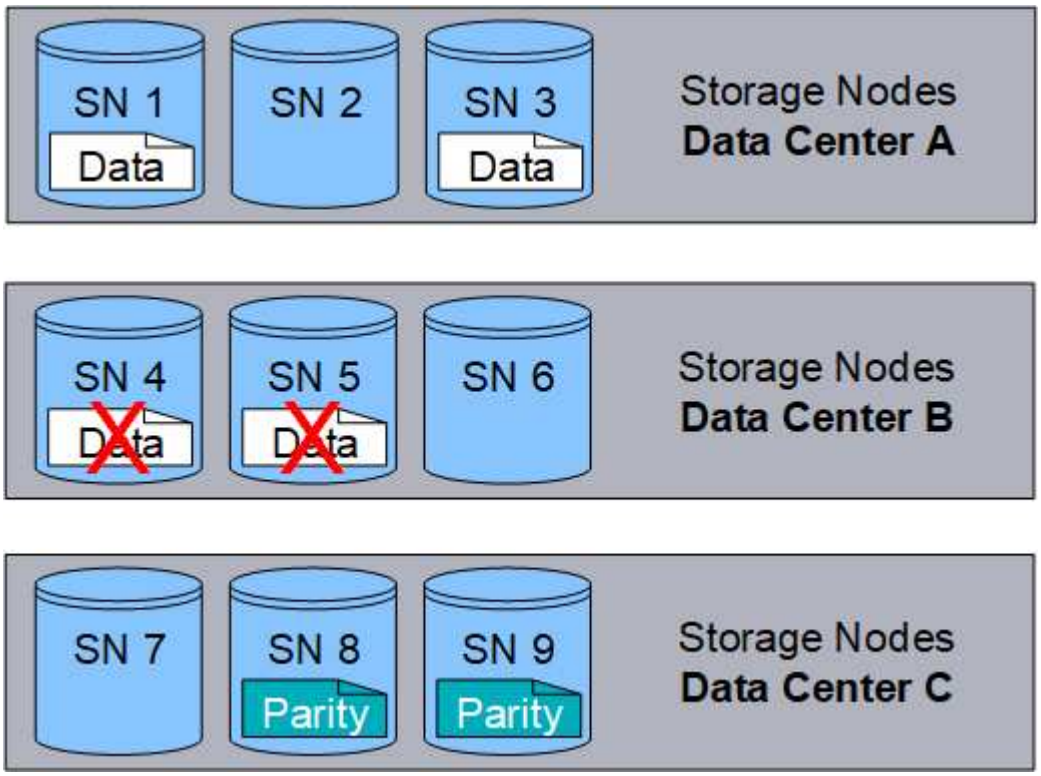
オブジェクトにアクセスすると、格納されているフラグメントを使用してオブジェクトが再アセンブルされます。データフラグメントまたはパリティフラグメントが破損したり失われたりしても、イレイジャーコーディングアルゴリズムが残りのデータフラグメントとパリティフラグメントを使用してそのフラグメントを再作成します。

ILMルールを作成すると、それらのルールをサポートするイレイジャーコーディングプロファイルがStorageGRIDによって作成されます。イレイジャーコーディングプロファイルのリスト、"イレイジャーコーディングプロファイルの名前を変更する"、、または"イレイジャーコーディングプロファイルがどのILMルールでも使用されていない場合は非アクティブ化する"を表示できます。

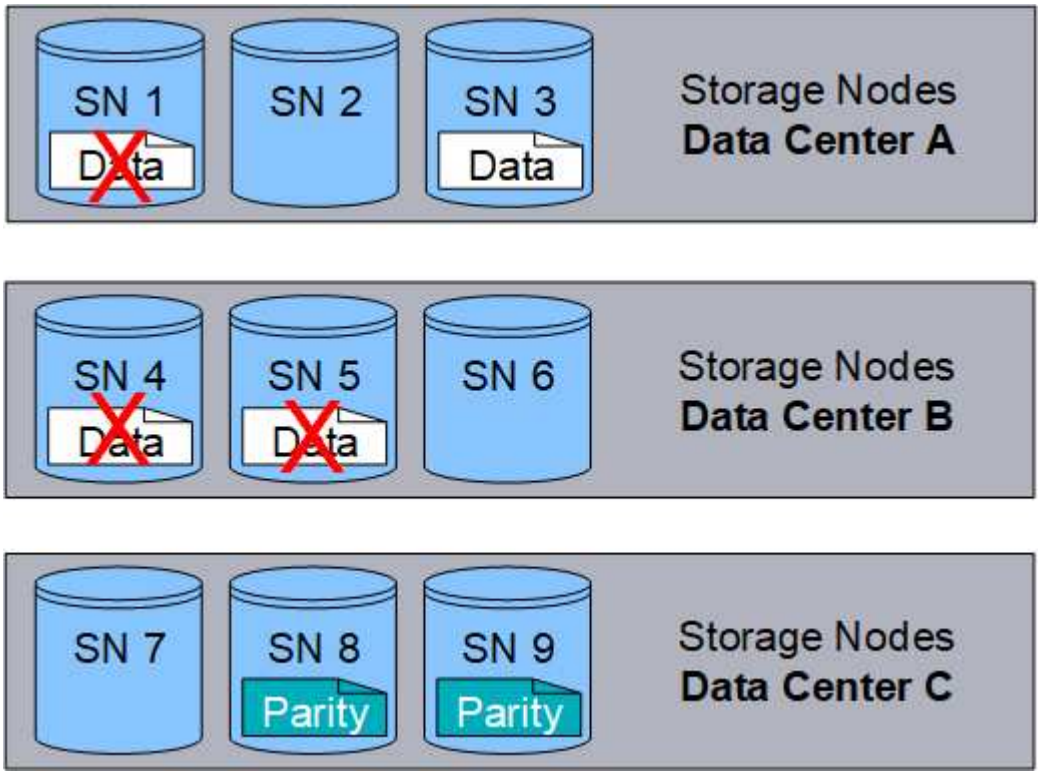
次の例は、オブジェクトのデータに対するイレイジャーコーディングアルゴリズムの使用方法を示しています。この例の ILM ルールでは 4+2 のイレイジャーコーディングスキームを使用します。各オブジェクトは 4 つのデータフラグメントに等分され、オブジェクトデータから 2 つのパリティフラグメントが計算されます。ノードやサイトの障害時にもデータが保護されるよう、 6 つの各フラグメントは 3 つのデータセンターサイトの別々のノードに格納されます。



4+2イレイジャーコーディングスキームはさまざまな方法で設定できます。たとえば、6つのストレージノードで構成される単一サイトのストレージプールを設定できます。では"サイト障害からの保護"、3つのサイトを含むストレージプールを使用し、各サイトに3つのストレージノードを配置できます。6 つのうちのいずれか 4 つのフラグメント（データまたはパリティ）が使用可能であれば、オブジェクトを読み出すことができます。最大 2 つのフラグメントが失われても、オブジェクトデータが失われることはありません。サイト全体が失われても、他のすべてのフラグメントに引き続きアクセスできるかぎり、オブジェクトの読み出しまたは修復が可能です。



3 つ以上のストレージノードが失われると、オブジェクトを読み出せなくなります。



関連情報

- "レプリケーションとは"
- "ストレージプールとは"
- "イレイジャーコーディングスキームとは"
- "イレイジャーコーディングプロファイルの名前を変更する"
- "イレイジャーコーディングプロファイルを非アクティブ化する"

StorageGRIDのイレイジャー コーディング方式について学ぶ

イレイジャーコーディングスキームは、各オブジェクト用に作成されるデータフラグメントとパリティフラグメントの数を制御します。

ILMルールを作成または編集するときに、使用可能なイレイジャーコーディングスキームを選択します。StorageGRIDでは、使用するストレージプールを構成するストレージノードとサイトの数に基づいて、イレイジャーコーディングスキームが自動的に作成されます。

データ保護

StorageGRID システムは、 Reed-Solomon イレイジャーコーディングアルゴリズムを使用します。このアルゴリズムは、オブジェクトを複数のデータフラグメントに分割 `k`し、パリティフラグメントを計算し `m`ます。

`k + m = n`フラグメントはストレージノード全体に分散され、`n`次のようにデータが保護されます。

- オブジェクトを読み出しまたは修復するには k、フラグメントが必要です。
- オブジェクトは失われたフラグメントまたは破損したフラグメントまで保持できます m。の値が大きいほど m、耐障害性が高くなります。

最適なデータ保護は、ストレージプール内のノードまたはボリュームの耐障害性が最も高いイレイジャーコーディングスキームによって実現されます。

ストレージオーバーヘッド

イレイジャーコーディングスキームのストレージオーバーヘッドは(m、パリティフラグメント数をデータフラグメント数で割って計算され(`k`ます。ストレージオーバーヘッドを使用して、各イレイジャーコーディングオブジェクトに必要なディスクスペースを計算できます。

```
disk space = object size + (object size * storage overhead)
```

たとえば、 4+2 スキームを使用して 10MB のオブジェクト（ストレージオーバーヘッドが 50% ）を格納すると、そのオブジェクトが消費するグリッドストレージは 15MB です。6+3 のストレージオーバーヘッドを含む 6+2 スキームを使用して同じ 10MB のオブジェクトを格納すると、オブジェクトが消費するサイズは約 13.3 MB になります。

ニーズに合ったイレイジャーコーディングスキームのうち、の合計値が最も小さいものを選択します k+m。フラグメント数が少ないイレイジャーコーディングスキームの方が計算効率が高い理由は次のとおりです。

- オブジェクトごとに作成、分散（読み出し）されるフラグメント数を削減
- フラグメントサイズが大きいため、パフォーマンスが向上します。
- ノードの追加に必要なノード数を減らすことができます。"ストレージの追加が必要になった場合の拡張"

ストレージプールに関するガイドライン

イレイジャーコーディングコピーを作成するルールに使用するストレージプールを選択する場合は、ストレージプールについて次のガイドラインに従ってください。

- ストレージプールには 3 つ以上のサイト、または 1 つのサイトだけが含まれている必要があります。

  ストレージプールにサイトが2つ含まれている場合はイレイジャーコーディングを使用できません。

  - 3 つ以上のサイトを含むストレージプールのイレイジャーコーディングスキーム
  - 1 サイトのストレージプールのイレイジャーコーディングスキーム
- All Sitesサイトを含むストレージプールは使用しないでください。
- ストレージプールには、オブジェクトデータを格納できるストレージノードが少なくとも含まれている必要があります *k+m* +1。

ストレージ ノードは、インストール時に、オブジェクト データとメタデータ (「結合された」ストレージ ノード)、オブジェクト メタデータのみ、またはオブジェクト データのみを含むように構成できます。詳細については、 "ストレージノードのタイプ" 。

必要なストレージノードの最小数はです `k+m`。ただし、必要なストレージノードが一時的に使用できない場合に、少なくとも 1 つのストレージノードを追加することで、取り込みエラーや ILM バックログが発生するのを防ぐことができます。

3 つ以上のサイトを含むストレージプールのイレイジャーコーディングスキーム

次の表に、 3 つ以上のサイトを含むストレージプールについて、 StorageGRID で現在サポートされているイレイジャーコーディングスキームを示します。これらのスキームはすべて、サイト障害からの保護を提供します。1 つのサイトが失われてもオブジェクトには引き続きアクセスできます。

サイト障害からの保護を提供するイレイジャーコーディングスキームの場合、各サイトに少なくとも3つのストレージノードが必要なため、ストレージプール内の推奨されるストレージノード数はよりも多くなります `_k+m_ +1`。

イレイジャーコーディングスキーム（ *k* + *m*）	サイトの最小数	各サイトで推奨されるストレージノードの数	推奨されるストレージノードの総数	サイト障害からの保護	ストレージオーバーヘッド
4+2	3	3	9	はい	50%
6+2	4	3	12	はい	33%
8+2	5	3	15	はい	25%
6+3	3	4	12	はい	50%
9+3	4	4	16	はい	33%
2+1	3	3	9	はい	50%
4+1	5	3	15	はい	25%
6+1	7	3	21	はい	17%
7+5	3	5	15	はい	71%

StorageGRID では、サイトごとに少なくとも 3 つのストレージノードが必要です。7+5 スキームを使用するには、各サイトに少なくとも 4 つのストレージノードが必要。サイトごとに 5 つのストレージノードを使用することを推奨します。

サイト保護を提供するイレイジャーコーディングスキームを選択する場合は、次の要素の相対的な重要性を調整します。

- * フラグメント数 * ：フラグメントの総数が少ないほど、一般にパフォーマンスと拡張の柔軟性が向上します。
- フォールトトレランス：パリティセグメントの数が多い（の値が大きい）ことでフォールトトレランスが向上します `m`。
- ネットワークトラフィック：障害からリカバリする場合、フラグメントの数が多い（の合計数が多い）スキームを使用する `k+m`と、ネットワークトラフィックが増加します。
- * ストレージ・オーバーヘッド * ：オーバーヘッドの大きいスキームでは、オブジェクトごとにより多くのストレージ・スペースが必要です。

たとえば、 4+2 と 6+3 のどちらかのスキーム（どちらも 50% のストレージオーバーヘッドがある）を選ぶ場合、フォールトトレランスをさらに高める必要がある場合は 6+3 のスキームを選択します。ネットワークリソースが制限されている場合は、 4+2 のスキームを選択します。他のすべての要素が等しい場合は、フラグメントの合計数が少ないため、 4+2 を選択します。

使用するスキームが不明な場合は、 4+2 または 6+3 を選択するか、テクニカルサポートにお問い合わせください。

1 サイトのストレージプールのイレイジャーコーディングスキーム

1 サイトのストレージプールでは、サイトに十分な数のストレージノードがある場合、 3 つ以上のサイト用に定義されたすべてのイレイジャーコーディングスキームがサポートされます。

必要なストレージノードの最小数はです `k+m`が、ストレージノードを含むストレージプールを `k+m +1`推奨します。たとえば、 2+1 イレイジャーコーディングスキームには少なくとも 3 つのストレージノードからなるストレージプールが必要ですが、推奨されるストレージノード数は 4 つです。

イレイジャーコーディングスキーム（ *k* + *m*）	ストレージノードの最小数	推奨されるストレージノードの数	ストレージオーバーヘッド
4+2	6	7	50%
6+2	8	9	33%
8+2	10	11	25%
6+3	9	10	50%
9+3	12	13	33%
2+1	3	4	50%
4+1	5	6	25%
6+1	7	8	17%
7+5	12	13	71%

レプリケーションとイレイジャーコーディングのどちらを使用してオブジェクトデータを損失から保護するかを決定する前に、イレイジャーコーディングのメリット、デメリット、および要件を理解しておく必要があります。

イレイジャーコーディングのメリット

イレイジャーコーディングは、レプリケーションに比べて信頼性、可用性、ストレージ効率に優れています。

- 信頼性: データが失われることなく耐えられる同時障害の数によって測定されます。
  - レプリケーション: 複数の同一オブジェクトのコピーが異なるノードおよびサイト間に保存されます。
  - 消失訂正符号化: オブジェクトはデータとパリティのフラグメントにエンコードされ、多数のノードとサイトに分散されます。この分散により、サイトとノードの両方の障害からの保護が提供されます。
- 可用性: ストレージ ノードに障害が発生したり、アクセスできなくなった場合にオブジェクトを取得する機能。レプリケーションと比較すると、消去コーディングでは同等のストレージ コストで可用性が向上します。
- ストレージ効率: 同様の可用性と信頼性を実現するために、消去コード化されたオブジェクトは複製されたオブジェクトよりもディスク容量が少なくて済みます。たとえば、2 つのサイトに複製された 10 MB のオブジェクトは 20 MB のディスク領域 (2 つのコピー) を消費しますが、6+3 消失訂正符号化スキームを使用して 3 つのサイト間で消失訂正符号化されたオブジェクトは 15 MB のディスク領域しか消費しません。

> ⓘ イレイジャーコーディングオブジェクトのディスクスペースは、オブジェクトサイズにストレージオーバーヘッドを加えたものです。ストレージオーバーヘッドの割合は、パリティフラグメント数をデータフラグメント数で割って算出します。

イレイジャーコーディングのデメリット

レプリケーションと比較した場合のイレイジャーコーディングのデメリットは次のとおりです。

- イレイジャーコーディングスキームに応じて、ストレージノードとサイトの数を増やすことを推奨します。一方、オブジェクトデータをレプリケートする場合、コピーごとに必要なストレージノードは1つだけです。およびを参照してください"3 つ以上のサイトを含むストレージプールのイレイジャーコーディングスキーム""1 サイトのストレージプールのイレイジャーコーディングスキーム"。
- ストレージの拡張にかかるコストと複雑さが増大します。レプリケーションを使用する環境を拡張するには、オブジェクトコピーを作成するすべての場所にストレージ容量を追加します。イレイジャーコーディングを使用する環境を拡張する場合は、使用中のイレイジャーコーディングスキームと、既存のストレージノードの使用率の両方を考慮する必要があります。たとえば、既存のノードの使用率が100%になるまで待つ場合は、少なくともストレージノードを追加する必要があります `k+m`が、既存のノードの使用率が70%になって拡張する場合は、サイトごとにノードを2つ追加しても、使用可能なストレージ容量を最大化できます。詳細については、を参照してください "イレイジャーコーディングオブジェクトのストレージ容量を追加します"。
- 地理的に分散したサイトでイレイジャーコーディングを使用する場合は、読み出しのレイテンシが上昇します。イレイジャーコーディングされてリモートサイトに分散されたオブジェクトのオブジェクトフラグメントをWAN接続経由で読み出すには、レプリケートされてローカル（クライアントの接続先と同じサイト）で使用可能なオブジェクトよりも時間がかかります。
- 地理的に分散したサイトでイレイジャーコーディングを使用する場合は、特に WAN ネットワーク接続経

由でオブジェクトを頻繁に読み出したり修復したりするケースでは読み出しと修復の WAN ネットワークトラフィックが増大します。

- サイト間で消去コーディングを使用すると、サイト間のネットワーク遅延が増加するため、オブジェクトの最大スループットが大幅に低下します。この減少は TCP ネットワーク スループットの低下によって発生し、 StorageGRIDシステムがオブジェクト フラグメントを保存および取得する速度に影響します。
- コンピューティングリソースの利用率が向上します。

イレイジャーコーディングを使用する状況

次の要件には消去コーディングを使用します。

- 1MB 超のオブジェクト

> イレイジャーコーディングは 1MB を超えるオブジェクトに適しています。非常に小さいイレイジャーコーディングフラグメントを管理するオーバーヘッドを回避するため
> に、200KB未満のオブジェクトにはイレイジャーコーディングを使用しないでください。

- 頻繁に読み出されないコンテンツの長期保存またはコールドストレージ。
- 高いデータ可用性と信頼性。
- サイトやノードの障害に対する保護
- Storage Efficiency：
- 複数のレプリケートコピーではなく 1 つのイレイジャーコーディングコピーのみを使用して効率的にデータを保護する必要のある単一サイト環境
- サイト間レイテンシが 100 ミリ秒未満の複数サイト環境

StorageGRIDがオブジェクトの保持を決定する方法

StorageGRID には、グリッド管理者と個々のテナントユーザが、オブジェクトを格納する期間を指定するためのオプションがあります。通常、テナントユーザが指定した保持手順は、グリッド管理者が指定した保持手順よりも優先されます。

テナントユーザによるオブジェクト保持期間の制御方法

テナントユーザは、次のメソッドを使用してオブジェクトをStorageGRIDに格納する期間を制御できます。

- グリッドでS3オブジェクトロックのグローバル設定が有効になっている場合、S3テナントユーザはS3オブジェクトロックを有効にしてバケットを作成し、各バケットに*デフォルトの保持期間*を選択できます。
- グリッドでグローバルな S3 オブジェクトのロック設定が有効になっている場合、 S3 テナントユーザは S3 オブジェクトのロックを有効にしたバケットを作成し、 S3 REST API を使用して、そのバケットに追加された各オブジェクトバージョンの最新の保持設定とリーガルホールド設定を指定できます。
  - リーガルホールドの対象となっているオブジェクトバージョンは、どの方法でも削除できません。
  - オブジェクトバージョンのretain-until-dateに達する前は、どの方法でもそのバージョンを削除できません。
  - S3オブジェクトロックが有効になっているバケット内のオブジェクトは、ILMによって「無期限」に保持されます。ただし、それまでの保持期間が終了したあとは、クライアント要求やバケットライフ

サイクルの終了によってオブジェクトバージョンを削除できます。を参照して "S3 オブジェクトロックでオブジェクトを管理します"

- S3 テナントユーザは、 Expiration アクションを指定するライフサイクル設定をバケットに追加できます。バケットライフサイクルが存在する場合、クライアントがオブジェクトを削除しないかぎり、StorageGRID は Expiration アクションで指定された日付または日数が経過するまでオブジェクトを格納します。を参照して "S3 ライフサイクル設定を作成する"
- S3クライアントはオブジェクトの削除要求を実行できます。StorageGRID は、オブジェクトを削除するか保持するかを決定する際に、常に S3 バケットライフサイクルまたは ILM よりもクライアントの削除要求を優先します。

グリッド管理者によるオブジェクト保持期間の制御方法

グリッド管理者は、次のメソッドを使用してオブジェクトの保持を制御できます。

- テナントごとにS3オブジェクトロックの最大保持期間を設定します。これにより、テナントユーザはバケットごとにデフォルトの保持期間を設定できます。最大保持期間は、そのバケットに新たに取り込まれたオブジェクト（オブジェクトのretain-until-date）にも適用されます。
- オブジェクトの格納期間を制御するILMの配置手順を作成します。オブジェクトが ILM ルールに一致した場合、 StorageGRID は ILM ルールの最後の期間が経過するまでそのオブジェクトを格納します。配置手順に「forever」が指定されている場合、オブジェクトは無期限に保持されます。
- オブジェクトの保持期間を誰が制御するかに関係なく、格納するオブジェクトコピーのタイプ（レプリケートまたはイレイジャーコーディング）とコピーの場所（ストレージノードまたはクラウドストレージプール）はILM設定によって制御されます。

S3 バケットライフサイクルと **ILM** の相互作用

S3バケットライフサイクルが設定されている場合は、ライフサイクルフィルタに一致するオブジェクトのILMポリシーがライフサイクル有効期限のアクションで上書きされます。その結果、 ILM のオブジェクト配置手順がすべて終了したあとも、オブジェクトがグリッドに保持されることがあります。

オブジェクト保持の例

S3 オブジェクトロック、バケットライフサイクル設定、クライアントの削除要求、 ILM の相互作用について、より深く理解するために次の例を検討してください。

例 **1** ： **S3** バケットライフサイクルのオブジェクト保持期間が **ILM** よりも長い

ILM

2 つのコピーを 1 年間保存（ 365 日）

バケットライフサイクル

2 年（ 730 日）でオブジェクトが期限切れになる

結果

StorageGRID はオブジェクトを 730 日間格納します。StorageGRID は、バケットライフサイクル設定を使用して、オブジェクトを削除するか保持するかを決定します。

ILM よりもバケットライフサイクルのオブジェクト保持期間の方が長い場合でも、格納するコピーの数とタイプを決定する際には引き続き StorageGRID の配置手順が使用されます。この例では、 366 日目から 730 日目までの間、オブジェクトの 2 つのコピーが StorageGRID に引き続き格納されます。

例 **2** ： **S3** バケットライフサイクルのオブジェクト保持期間よりも短い

ILM
2 つのコピーを 2 年間（ 730 日）格納する

バケットライフサイクル
1 年（ 365 日）でオブジェクトを期限切れにする

結果
StorageGRID は 365 日目にオブジェクトのコピーを両方削除します。

例 **3** ：クライアントによる削除は、バケットライフサイクルと **ILM** よりも優先されます

ILM
2つのコピーをストレージノードに「無期限」で格納

バケットライフサイクル
2 年（ 730 日）でオブジェクトが期限切れになる

クライアントの削除要求
発行日： 400 日目

結果
StorageGRID は、クライアントの削除要求に応じて 400 日目にオブジェクトのコピーを両方削除します。

例 **4** ： **S3** オブジェクトロックはクライアントの削除要求を上書きします

S3 オブジェクトのロック
オブジェクトバージョンの retain-until は、 2026-03-31 です。リーガルホールドは有効ではありません。

準拠 **ILM** ルール
2つのコピーをストレージノードに「無期限」で格納

クライアントの削除要求
発行日2024-03-31

結果
retain-until はまだ 2 年前の時点であるため、 StorageGRID はオブジェクトバージョンを削除しません。

StorageGRIDによるオブジェクトの削除方法

StorageGRID は、クライアント要求に直接応答してオブジェクトを削除するか、 S3 バケットライフサイクルの終了または ILM ポリシーの要件に応じて自動的にオブジェクト

を削除します。オブジェクトのさまざまな削除方法と StorageGRID による削除要求の処理方法を理解しておくと、オブジェクトをより効率的に管理できるようになります。

StorageGRID では、次のいずれかの方法でオブジェクトを削除できます。

- 同期削除： StorageGRID がクライアントの削除要求を受け取ると、すべてのオブジェクトコピーがただちに削除されます。コピーが削除されると、削除が成功したことがクライアントに通知されます。
- オブジェクトは削除キューに登録されます。 StorageGRID が削除要求を受け取ると、オブジェクトは削除キューに登録され、削除が成功したことがクライアントにすぐに通知されます。オブジェクトコピーは、あとでバックグラウンド ILM 処理によって削除されます。

StorageGRID では、オブジェクトを削除する際に、削除のパフォーマンスを最適化し、削除のバックログを最小限に抑え、スペースを最も早く解放する方法を使用します。

次の表は、 StorageGRID がどのような場合に各メソッドを使用するかを

削除方法	使用時
オブジェクトは削除キューに登録されます	次の条件のいずれか * が当てはまる場合： • 次のいずれかのイベントによってオブジェクトの自動削除がトリガーされた： ◦ S3 バケットのライフサイクル設定の有効期限または日数に達した。 ◦ ILM ルールに指定された最後の期間が経過した。 注： S3オブジェクトロックが有効になっているバケット内のオブジェクトは、リーガルホールドの対象である場合、またはretain-until-dateが指定されていてもまだ満たされていない場合は削除できません。 • S3クライアントが削除を要求し、次の条件が1つ以上該当します。 ◦ オブジェクトの場所が一時的に使用できない場合など、30秒以内にコピーを削除することはできません。 ◦ バックグラウンド削除キューがアイドル状態である。
オブジェクトをただちに削除（同期削除）	S3クライアントが削除要求を実行し、次の条件*すべて*が満たされている場合： • すべてのコピーを 30 秒以内に削除できる。 • バックグラウンド削除キューには処理するオブジェクトが含まれています。

S3クライアントが削除要求を行うと、StorageGRIDはまずオブジェクトを削除キューに追加します。その後、同期削除の実行に切り替えます。処理対象となるオブジェクトがバックグラウンド削除キューに含まれていることを確認することで、 StorageGRID は、クライアントによる削除のバックログが発生しないようにしつつ、特に同時実行性の低いクライアントに対してより効率的に削除を処理できます。

オブジェクトの削除に必要な時間

StorageGRID によるオブジェクトの削除方法は、システムの動作に影響を及ぼす可能性があります。

- StorageGRID StorageGRID で同期削除が実行されると、結果がクライアントに返されるまでに最大 30 秒かかることがあります。つまり、実際には StorageGRID がオブジェクトを削除キューに登録する場合よりも短時間でコピーが削除されるにもかかわらず、より長くかかっているという印象をクライアントに与える可能性があります。
- 一括削除の実行中に削除のパフォーマンスを綿密に監視している場合、一定数のオブジェクトが削除されたあとに削除速度が低下しているように見えることがあります。この変更は、 StorageGRID がオブジェクトを削除キューへ登録する方法から同期削除に切り替えたときに発生します。削除速度が低下したように見えても、オブジェクトコピーの削除速度が遅くなったわけではありません。一方で、スペースの開放にかかる時間は、平均すると短くなっています。

大量のオブジェクトを削除する場合に、スペースを短時間で解放することが優先されるのであれば、 ILM などの方法を使用してオブジェクトを削除するのではなく、クライアント要求を使用することを検討してください。一般に、クライアントによって削除が実行された場合、 StorageGRID は同期削除を使用できるため、スペースはより短時間で解放されます。

オブジェクトの削除後にスペースを解放するために必要な時間は、いくつかの要因によって異なります。

- オブジェクトコピーが同期的に削除されるか、またはキューに登録されたあとで削除されるか（クライアントの削除要求の場合）。
- グリッド内のオブジェクトの数や、オブジェクトコピーが削除対象キューに登録される場合のグリッドリソースの可用性などのその他の要因（クライアントによる削除およびその他の方法の場合）。

S3 バージョン管理オブジェクトの削除方法

S3 バケットでバージョン管理が有効になっている場合、 StorageGRID は、削除要求に応答する際、要求が S3 クライアント、 S3 バケットライフサイクルの終了、 ILM ポリシーの要件のいずれによるものであるかにかかわらず、 Amazon S3 の動作に従います。

オブジェクトがバージョン管理されている場合、オブジェクトの削除要求ではオブジェクトの現在のバージョンは削除されず、スペースも解放されません。代わりに、オブジェクトの削除要求では、オブジェクトの現在のバージョンとしてゼロバイトの削除マーカーが作成され、以前のバージョンのオブジェクトが「 noncurrent」になります。オブジェクト削除マーカーが最新バージョンであり、最新でないバージョンがない場合、オブジェクト削除マーカーは期限切れのオブジェクト削除マーカーになります。

オブジェクトが削除されていなくても、 StorageGRID は現在のバージョンのオブジェクトが使用できなくなったかのように動作します。そのオブジェクトに対する要求は 404 NotFound を返します。ただし、最新でないオブジェクトデータは削除されていないため、最新でないバージョンのオブジェクトを指定する要求は成功します。

クライアントがバージョンIDを持つオブジェクトバージョンを"ブランチバケット"StorageGRID はオブジェクト バージョンの存在を隠しますが、ブランチ バケットに削除マーカーを作成しません。クライアントがブランチ バケットからバージョン ID のないオブジェクトを削除すると、 StorageGRID は標準の S3 動作に従ってブランチ バケットに削除マーカーを作成します。

バージョン管理オブジェクトを削除するときに領域を解放したり、削除マーカーを削除したりするには、次のいずれかを使用します。

- * S3クライアント要求*：S3 DELETE Object要求にオブジェクトのバージョンIDを指定し(`DELETE /object?versionId=ID`ます）。この要求は、指定したバージョンのオブジェクトコピーだけを削除します（他のバージョンは引き続きスペースを消費します）。
- バケットライフサイクル：バケットライフサイクル設定のアクションを使用します `NoncurrentVersionExpiration`。NoncurrentDays で指定した日数に達すると、 StorageGRID は最新

でないオブジェクトバージョンのコピーをすべて完全に削除します。これらのオブジェクトバージョンはリカバリできません。

バケットライフサイクル設定のアクションは、 `NewerNoncurrentVersions`バージョン管理されたS3バケットに保持する最新でないバージョンの数を指定します。指定した数よりも最新でないバージョンが多い場合は `NewerNoncurrentVersions`StorageGRID、`NoncurrentDays`の値が経過すると古いバージョンが削除されます。しきい値は `NewerNoncurrentVersions`、ILMが提供するライフサイクルルールよりも優先されます。つまり、ILMが削除を要求した場合、しきい値内のバージョンが最新でないオブジェクトが `NewerNoncurrentVersions`保持されます。

期限切れのオブジェクト削除マーカーを削除するには、、 `Days`、またはの `Date`いずれかのタグを指定したアクションを `ExpiredObjectDeleteMarker`使用します `Expiration`。

- * ILM *："アクティブポリシーのクローンを作成する"2つのILMルールを新しいポリシーに追加します。
  - 最初のルール：[Reference Time]に「noncurrent time」を使用して最新でないバージョンのオブジェクトを照合します。で"ILMルールの作成ウィザードの手順1（詳細を入力）"、「Apply this rule to older object versions only（in S3 bucket with versioning enabled）？」という質問に対して* Yes *を選択します。
  - 2つ目のルール：*取り込み時間*を使用して現在のバージョンと一致させます。「noncurrent time」ルールは、ポリシーの「取り込み時間」ルールの上に表示する必要があります。

    期限切れのオブジェクト削除マーカーを削除するには、取り込み時間*ルールを使用して現在の削除マーカーと一致させます。削除マーカーは、 Time Period * of * Days *が経過し、現在の削除メーカーが期限切れになった場合にのみ削除されます(最新でないバージョンはありません)。
- バケット内のオブジェクトを削除：テナントマネージャを使用して、"すべてのオブジェクトバージョンを削除"バケットから削除マーカーを含めます。

バージョン管理オブジェクトが削除されると、StorageGRIDはオブジェクトの現在のバージョンとしてゼロバイトの削除マーカーを作成します。バージョン管理されたバケットを削除する前に、すべてのオブジェクトと削除マーカーを削除する必要があります。

- StorageGRID 11.7以前で作成された削除マーカーは、S3クライアント要求でのみ削除できます。ILM、バケットライフサイクルルール、またはバケット処理のDeleteオブジェクトでは削除されません。
- StorageGRID 11.8以降で作成されたバケットの削除マーカーは、ILM、バケットライフサイクルルール、バケット処理のオブジェクトの削除、またはS3クライアントの明示的な削除によって削除できます。

関連情報

- "S3 REST APIを使用する"
- "例 4 ： S3 バージョン管理オブジェクトの ILM ルールとポリシー"

StorageGRID でストレージグレードを作成して割り当てる

ストレージグレードは、ストレージノードで使用されているストレージのタイプを表します。ILMルールで特定のオブジェクトを特定のストレージノードに配置する場合は、ストレージグレードを作成できます。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。

- そうだな "特定のアクセス権限"

タスクの内容

StorageGRID を初めてインストールすると、システム内のすべてのストレージノードに* default *ストレージグレードが自動的に割り当てられます。必要に応じて、カスタムのストレージグレードを定義して別のストレージノードに割り当てることができます。

カスタムのストレージグレードを使用すると、特定のタイプのストレージノードのみを含むILMストレージプールを作成できます。たとえば、 StorageGRID オールフラッシュストレージアプライアンスなどの最速のストレージノードに特定のオブジェクトを格納できます。

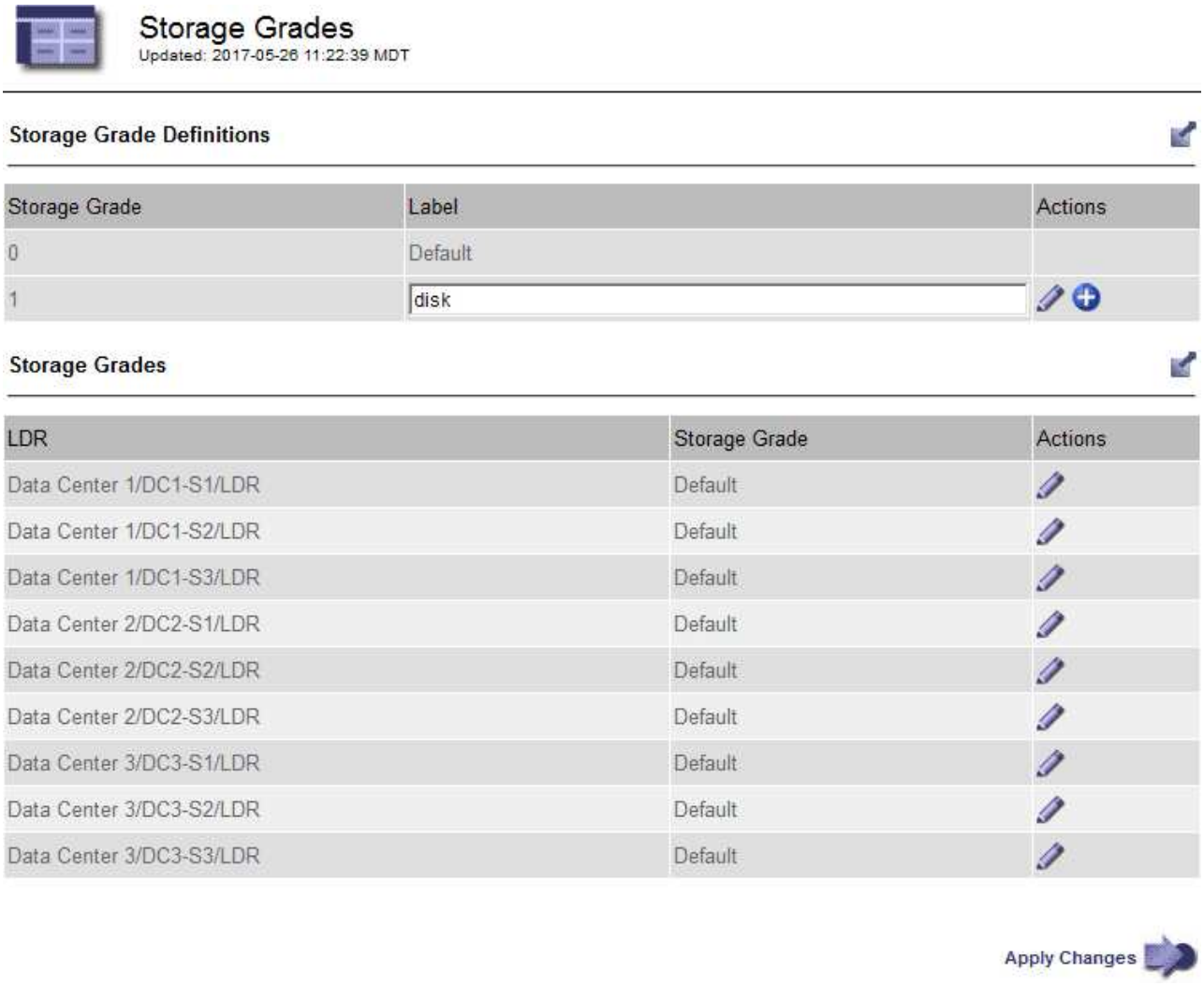
> メタデータのみのストレージ ノードにはストレージ グレードを割り当てることができません。詳細については、 "ストレージノードのタイプ" 。

ストレージグレードが重要でない場合（すべてのストレージノードが同一の場合など）は、この手順を省略して、ストレージグレードの*[すべてのストレージグレードを含む]*選択を使用できます"ストレージプールを作成します"。このオプションを使用すると、ストレージグレードに関係なく、サイトのすべてのストレージノードがストレージプールに含まれるようになります。

> ストレージグレードを必要以上に作成しないでください。たとえば、ストレージノードごとにストレージグレードを作成しないでください。各ストレージグレードを複数のノードに割り当てます。ストレージグレードを 1 つのノードにしか割り当てていない場合、そのノードが使用できなくなると原因 のバックログが発生する可能性があります。

手順

1. ILM * > * ストレージグレード * を選択します。
2. カスタムのストレージグレードを定義：
   a. 追加するカスタムストレージグレードごとに、挿入 アイコン"] を選択して行を追加します。
   b. 説明ラベルを入力します。



ページ"]

c. 「 * 変更を適用する * 」を選択します。

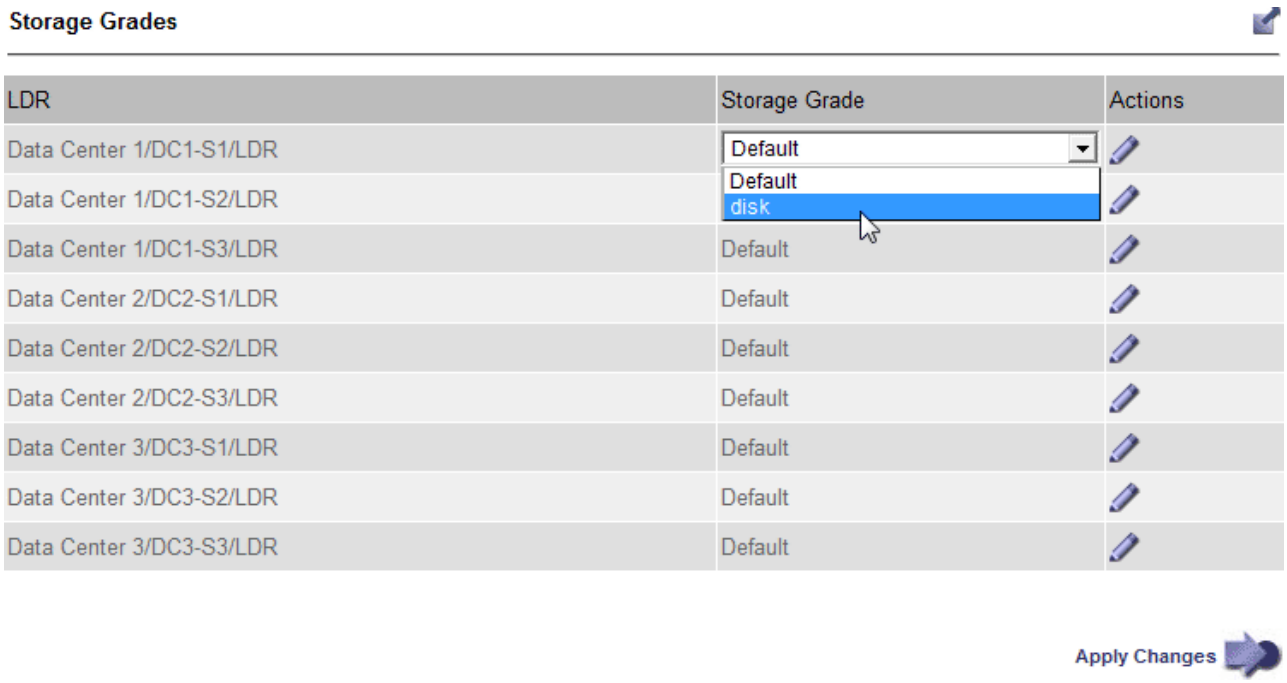
d. 必要に応じて、保存済みのラベルを変更する場合は、編集 を選択し、変更を適用 を選択します。

ストレージグレードを削除することはできません。

3. 新しいストレージグレードをストレージノードに割り当てます。

a. LDRリストからストレージノードを探し、その*編集*アイコンを選択します。

b. リストから適切なストレージグレードを選択します。



ページ"]

特定のストレージノードにストレージグレードを割り当てることができるのは 1 回だけです。障害からリカバリしたストレージノードでは、以前に割り当てられていたストレージグレードが維持されます。ILMポリシーをアクティブ化したあとに、この割り当てを変更しないでください。割り当てが変更されると、新しいストレージグレードに基づいてデータが格納されます。

a. 「 * 変更を適用する * 」を選択します。

ストレージプールを使用する

StorageGRID のストレージプールについて学ぶ

ストレージプールは、ストレージノードを論理的にグループ化したものです。

StorageGRID をインストールすると、サイトごとに1つのストレージプールが自動的に作成されます。ストレージ要件に応じて、追加のストレージプールを設定できます。

ストレージ ノードは、インストール時に、オブジェクト データとメタデータ (「結合された」ストレージ ノード)、オブジェクト メタデータのみ、またはオブジェクト データのみを含むように構成できます。メタデータのみのストレージ ノードは、ストレージ プールでは使用できません。詳細については、 "ストレージノードのタイプ" 。

ストレージプールには 2 つの属性があります。

- * ストレージグレード * ：ストレージノードの場合は、バッキングストレージの相対的なパフォーマンス。
- サイト：オブジェクトが保存されるデータセンター。

ストレージプールは、オブジェクトデータの格納場所と使用するストレージのタイプを決定するためにILMルールで使用されます。レプリケーション用のILMルールを設定する場合は、1つ以上のストレージプールを選

択します。

StorageGRID のストレージプール構成ガイドライン

ストレージプールを構成して使用し、複数のサイトにデータを分散することでデータ損失からデータを保護します。レプリケートコピーとイレイジャーコーディングコピーには、異なるストレージプール構成が必要です。

"レプリケーションとイレイジャーコーディングを使用したサイト障害からの保護の有効化例"を参照してください。

すべてのストレージプールのガイドライン

- ストレージプールの設定は可能なかぎりシンプルにします。必要以上にストレージプールを作成しないでください。
- できるだけ多くのノードを含むストレージプールを作成します。各ストレージプールには 2 つ以上のノードを含める必要があります。ノードが不十分なストレージプールでは、ノードが使用できなくなった場合に原因 ILM バックログが発生する可能性があります。
- 重複する（ 1 つ以上の同じノードを含む）ストレージプールを作成または使用することは避けてください。ストレージプールが重複していると、オブジェクトデータの複数のコピーが同じノードに保存される可能性があります。
- 通常は、All Storage Nodesストレージプール（StorageGRID 11.6以前）やAll Sitesサイトは使用しないでください。これらの項目は自動的に更新され、拡張に追加する新しいサイトが含まれるようになります。これは想定した動作ではない可能性があります。

レプリケートコピーに使用するストレージプールのガイドライン

- を使用したサイト障害からの保護の"レプリケーション"場合は、でサイト固有のストレージプールを1つ以上指定します"各ILMルールの配置手順"。

  StorageGRID のインストール時に、サイトごとに1つのストレージプールが自動的に作成されます。

  各サイトにストレージプールを使用すると、レプリケートされたオブジェクトコピーが想定どおりに配置されるようになります（たとえば、サイト障害から保護するために、各サイトのすべてのオブジェクトのコピーが 1 つずつ）。

- 拡張時にサイトを追加する場合は、新しいサイトのみを含む新しいストレージプールを作成します。次に、"ILMルールを更新"新しいサイトに格納するオブジェクトを制御します。
- コピーの数がストレージプールの数より少ない場合は、プール間のディスク使用量のバランスを取るためにコピーが分散されます。
- ストレージプールが重複している（同じストレージノードを含んでいる）場合は、オブジェクトのすべてのコピーが 1 つのサイトにのみ保存される可能性があります。選択したストレージプールに同じストレージノードが含まれていないことを確認する必要があります。

イレイジャーコーディングされたコピーに使用するストレージプールのガイドラインを次に示します

- を使用してサイト障害から保護するに"イレイジャーコーディング"は、3つ以上のサイトで構成されるストレージプールを作成します。ストレージプールにサイトが2つしかない場合、そのストレージプールをイレイジャーコーディングに使用することはできません。2 つのサイトを含むストレージプールではイレイジャーコーディングスキームを使用できません。

- ストレージプールに含まれるストレージノードとサイトの数によって、使用可能なノードとサイトが決まります"イレイジャーコーディングスキーム"。
- 可能であれば、選択するイレイジャーコーディングスキームに必要な最小数よりも多くのストレージノードをストレージプールに含めてください。たとえば、 6+3 のイレイジャーコーディングスキームを使用する場合は、 9 個以上のストレージノードが必要です。ただし、サイトごとに少なくとも 1 つのストレージノードを追加することを推奨します。
- ストレージノードはサイト間にできるだけ均等に分散します。たとえば、 6+3 のイレイジャーコーディングスキームをサポートするには、 3 つのサイトにそれぞれ 1 つ以上のストレージノードを含むストレージプールを設定します。
- スループット要件が高い場合、サイト間のネットワークレイテンシが100ミリ秒を超える場合は、複数のサイトを含むストレージプールを使用することは推奨されません。レイテンシが上昇すると TCP ネットワークのスループットが低下するため、 StorageGRID がオブジェクトフラグメントを作成、配置、読み出す速度は大幅に低下します。

  スループットの低下は、オブジェクトの取り込みと取得の最大達成可能速度に影響を与え（取り込み動作として「バランス」または「厳密」を選択した場合）、または ILM キューのバックログにつながる可能性があります（取り込み動作として「デュアルコミット」を選択した場合）。"ILMルールの取り込み動作"を参照してください。

> グリッドにサイトが1つしかない場合は、イレイジャーコーディングプロファイルでAll Storage Nodesストレージプール（StorageGRID 11.6以前）またはAll Sitesサイトを使用できません。これにより、2つ目のサイトが追加された場合にプロファイルが無効になるのを防ぐことができます。

StorageGRID のストレージプールによるサイト損失保護

StorageGRID 環境に複数のサイトが含まれている場合は、レプリケーションとイレイジャーコーディングを適切に設定されたストレージプールで使用して、サイト障害から保護することができます。

レプリケーションとイレイジャーコーディングでは、次のように異なるストレージプール構成が必要です。

- レプリケーションを使用してサイト障害から保護するには、StorageGRID のインストール時に自動的に作成されるサイト固有のストレージプールを使用します。次に、各オブジェクトのコピーが各サイトに1つ配置されるように、複数のストレージプールを指定するILMルールを作成します"配置手順"。
- イレイジャーコーディングを使用してサイト障害から保護する場合は、を"複数のサイトで構成されるストレージプールを作成します"参照してください。次に、複数のサイトで構成される1つのストレージプールと使用可能なイレイジャーコーディングスキーマを使用するILMルールを作成します。

> サイト損失保護のためにStorageGRID導入を構成する際には、以下の影響も考慮する必要があります。"取り込みオプション"そして"一貫性"。

レプリケーションの例

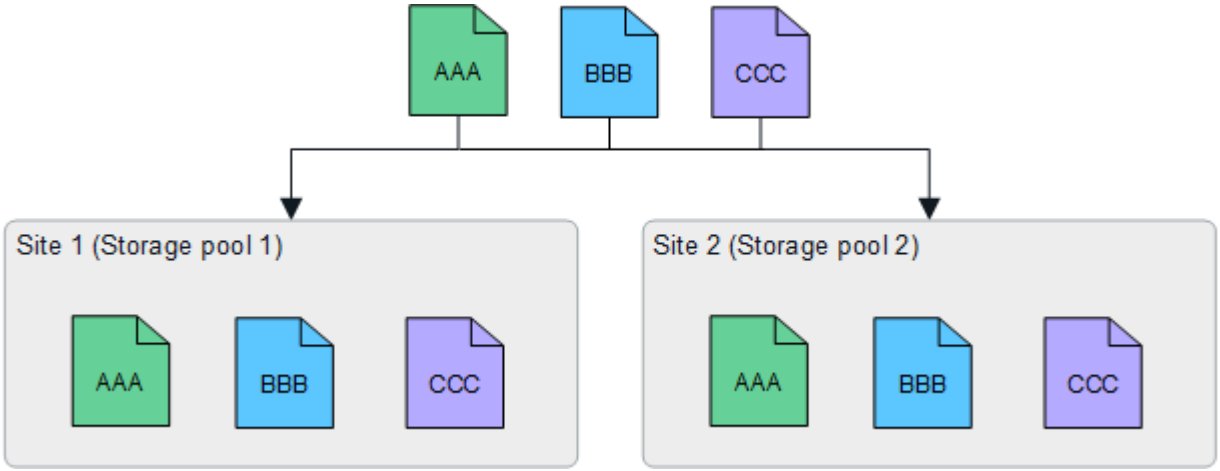
デフォルトでは、StorageGRID のインストール時にサイトごとに1つのストレージプールが作成されます。ストレージプールが1つのサイトだけで構成されていると、レプリケーションを使用してサイト障害から保護するILMルールを設定できます。次の例では、

- ストレージプール1にサイト1が含まれている

- ストレージプール2にサイト2が含まれている
- ILMルールには次の2つの配置が含まれています。
  - サイト1に1つのコピーをレプリケートしてオブジェクトを格納します
  - サイト2に1つのコピーをレプリケートしてオブジェクトを格納します

ILMルールの配置：





一方のサイトが失われると、もう一方のサイトでオブジェクトのコピーを使用できるようになります。

イレイジャーコーディングの例

ストレージプールごとに複数のサイトで構成されるストレージプールを用意すると、イレイジャーコーディングを使用してサイト障害から保護するILMルールを設定できます。次の例では、

- ストレージプール1にサイト1~3が含まれています
- ILMルールには配置が1つ含まれています。3つのサイトからなるストレージプール1で4+2 ECスキームを使用してオブジェクトをイレイジャーコーディングして格納します

ILMルールの配置：



次の例では、

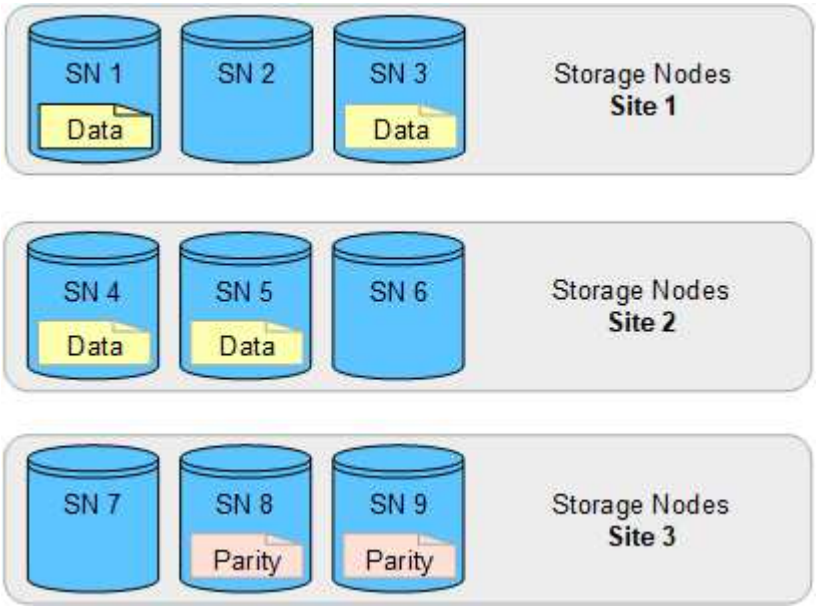
- ILMルールでは4+2のイレイジャーコーディングスキームを使用します。
- 各オブジェクトは 4 つのデータフラグメントに等分され、オブジェクトデータから 2 つのパリティフラグ

メントが計算されます。

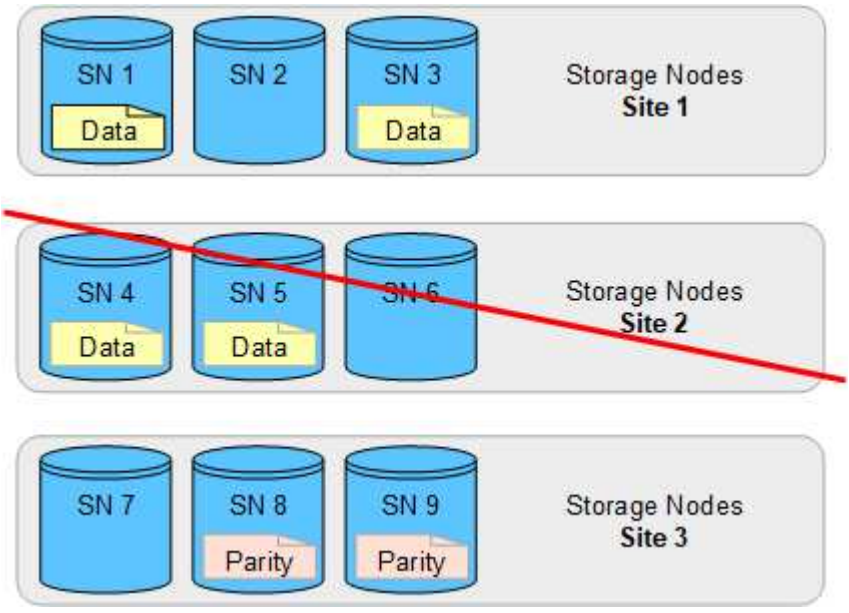
- ノードやサイトの障害時にもデータが保護されるよう、 6 つの各フラグメントは 3 つのデータセンターサイトの別々のノードに格納されます。

> イレイジャーコーディングは、sites_except_twoサイトを任意の数含むストレージプールで許可されます。

4+2のイレイジャーコーディングスキームを使用するILMルール：



一方のサイトが失われても、データは引き続きリカバリできます。



StorageGRID でストレージプールを作成する

ストレージプールを作成することで、 StorageGRID システムがオブジェクトデータを格納する場所と、使用するストレージのタイプを決定します。各ストレージプールには、

サイトとストレージグレードがそれぞれ 1 つ以上含まれています。

新しいグリッドに StorageGRID 12.0 以降をインストールすると、各サイトのストレージプールが自動的に作成されます。ただし、最初に StorageGRID 11.6 以前をインストールした場合は、各サイトのストレージプールは自動的に作成されません。

クラウドストレージプールを作成してStorageGRIDシステムの外部にオブジェクトデータを格納する場合は、を参照してください"クラウドストレージプールの使用に関する情報"。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- そうだな "特定のアクセス権限"
- ストレージプールの作成に関するガイドラインを確認しておく必要があります。

タスクの内容

ストレージプールは、オブジェクトデータの格納場所を決定します。必要なストレージプールの数は、グリッド内のサイトの数と、レプリケートコピーまたはイレイジャーコーディングコピーのタイプによって異なります。

- レプリケーションおよび単一サイトのイレイジャーコーディングの場合は、サイトごとにストレージプールを作成します。たとえば、レプリケートオブジェクトコピーを 3 つのサイトに格納する場合は、ストレージプールを 3 つ作成します。
- 3 つ以上のサイトでイレイジャーコーディングする場合は、サイトごとに 1 つのエントリを含むストレージプールを 1 つ作成します。たとえば、 3 つのサイトにまたがるオブジェクトをイレイジャーコーディングする場合は、ストレージプールを 1 つ作成します。

  イレイジャーコーディングプロファイルで使用するストレージプールにAll Sitesサイトを含めないでください。代わりに、イレイジャーコーディングデータを格納するサイトごとにストレージプールにエントリを追加します。例については、を参照してくださいこの手順を実行します。

- ストレージグレードが複数ある場合は、異なるストレージグレードを含むストレージプールを1つのサイトに作成しないでください。を参照してください"ストレージプールの作成に関するガイドラインを次に示します"。

手順

1. ILM * > * Storage pools * を選択します

   [ストレージプール]タブには、定義済みのすべてのストレージプールが表示されます。

   StorageGRID 11.6以前の新規インストールでは、新しいデータセンターサイトを追加するたびに[All Storage Nodes]ストレージプールが自動的に更新されます。このプールはILMルールで使用しないでください。

2. 新しいストレージプールを作成するには、「 * 作成」を選択します。
3. ストレージプールの一意の名前を入力します。イレイジャーコーディングプロファイルとILMルールを設定する際に識別しやすい名前を使用してください。
4. [*Site *] ドロップダウン・リストから ' このストレージ・プールのサイトを選択します

サイトを選択すると、テーブル内のストレージノードの数が自動的に更新されます。

一般に、どのストレージプールでもAll Sitesサイトを使用しないでください。All Sites ストレージプールを使用する ILM ルールでは、オブジェクトを任意の使用可能なサイトに配置することで、オブジェクトの配置をより細かく制御できます。また、 All Sites ストレージプールは、新しいサイトのストレージノードを即座に使用しますが、これは想定どおりの動作ではない場合があります。

5. [ストレージグレード]*ドロップダウンリストで、ILMルールがこのストレージプールを使用する場合に使用するストレージのタイプを選択します。

   ストレージグレード（_ Includes all storage grades_）には、選択したサイトのすべてのストレージノードが含まれます。グリッド内のストレージノード用にストレージグレードを追加で作成している場合、そのグレードもドロップダウンに表示されます。

6. [[entries]ストレージプールをマルチサイトイレイジャーコーディングプロファイルで使用する場合は、*[Add more nodes]*を選択して、各サイトのエントリをストレージプールに追加します。

   1つのサイトにストレージグレードが異なるエントリを複数追加すると警告が表示されます。

   エントリを削除するには、削除アイコン を選択します。

7. 選択に問題がなければ、 * 保存 * を選択します。

   新しいストレージプールがリストに追加されます。

StorageGRID でストレージプールの詳細を表示する

ストレージプールの詳細を表示して、ストレージプールの使用場所を確認したり、含まれているノードやストレージグレードを確認したりできます。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- そうだな "特定のアクセス権限"

手順

1. ILM * > * Storage pools * を選択します

   [Storage Pools]テーブルには、ストレージノードを含む各ストレージプールに関する次の情報が表示されます。

   - * Name * ：ストレージプールの一意の表示名。
   - ノード数：ストレージプール内のノードの数。
   - ストレージ使用量：このノードでオブジェクトデータに使用されている合計使用可能スペースの割合。この値にはオブジェクトメタデータは含まれません。
   - 合計容量：ストレージプールのサイズ。ストレージプール内のすべてのノードでオブジェクトデータに使用可能なスペースの合計に相当します。
   - * ILM usage *：ストレージプールの現在の使用状況。ストレージプールは、使用されていない場合

や、1つ以上のILMルール、イレイジャーコーディングプロファイル、またはその両方で使用されている場合があります。

2. 特定のストレージプールの詳細を表示するには、そのストレージプールの名前を選択します。

   ストレージプールの詳細ページが表示されます。

3. ストレージプールに含まれるストレージノードの詳細については、*[ノード]*タブを表示します。

   この表には、ノードごとに次の情報が記載されています。

   - ノード名
   - サイト名
   - ストレージグレード
   - Storage usage：オブジェクトデータに使用可能な合計スペースのうち、ストレージノードで使用されているスペースの割合。

   > 同じストレージ使用量 (%) の値は、各ストレージ ノードの「使用済みストレージ - オブジェクト データ」チャートにも表示されます ([ノード] > [ストレージ ノード] > [ストレージ] を選択)。

4. ストレージプールがILMルールまたはイレイジャーコーディングプロファイルで現在使用されているかどうかを確認するには、*[ILM usage（ILM使用状況）]*タブを表示します。
5. 必要に応じて、*[ILM rules]ページ*に移動し、ストレージプールを使用するルールの詳細と管理を確認します。

   を参照してください"ILMルールの操作手順"。

StorageGRID でストレージプールを編集する

ストレージプールを編集して、名前を変更したり、サイトやストレージグレードを更新したりできます。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- そうだな "特定のアクセス権限"
- を確認しておきます"ストレージプールの作成に関するガイドライン"。
- アクティブな ILM ポリシーのルールで使用されているストレージプールを編集する場合は、変更がオブジェクトデータの配置にどのように影響するかを検討しておく必要があります。

タスクの内容

アクティブなILMポリシーで使用されているストレージプールに新しいサイトまたはストレージグレードを追加する場合は、新しいサイトまたはストレージグレードのストレージノードは自動的に使用されないことに注意してください。StorageGRID で新しいサイトまたはストレージグレードを強制的に使用するには、編集したストレージプールを保存したあとに新しいILMポリシーをアクティブ化する必要があります。

手順

1. ILM * > * Storage pools * を選択します
2. 編集するストレージプールのチェックボックスを選択します。

   All Storage Nodesストレージプール（StorageGRID 11.6以前）は編集できません。

3. 「 * 編集 * 」を選択します。
4. 必要に応じて、ストレージプール名を変更します。
5. 必要に応じて、他のサイトとストレージグレードを選択します。

   ストレージプールがイレイジャーコーディングプロファイルで使用されていて、その変更によって原因イレイジャーコーディングスキームが無効になる場合は、サイトまたはストレージグレードを変更できません。たとえば、イレイジャーコーディングプロファイルで使用されているストレージプールにサイトが1つしかないストレージグレードが含まれている場合、サイトが2つのストレージグレードを使用することはできません。これは、変更を行うとイレイジャーコーディングスキームが無効になるためです。

   > 既存のストレージプールに対してサイトを追加または削除しても、既存のイレイジャーコーディングデータは移動されません。サイトから既存のデータを移動する場合は、新しいストレージプールとECプロファイルを作成してデータを再エンコードする必要があります。

6. [保存（ Save ）] を選択します。

終了後

アクティブな ILM ポリシーで使用されているストレージ プールに新しいサイトまたはストレージ グレードを追加した場合は、新しい ILM ポリシーをアクティブ化して StorageGRID が新しいサイトまたはストレージ グレードを使用するよう強制してください。例えば、既存の ILM ポリシーをクローンし、そのクローンをアクティブ化します。"ILM ルールおよび ILM ポリシーの操作"を参照してください。

StorageGRID でストレージプールを削除する

使用されていないストレージプールは削除できます。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"必要なアクセス権限"。

手順

1. ILM * > * Storage pools * を選択します
2. テーブルの[ILM usage]列で、ストレージプールを削除できるかどうかを確認します。

   ILMルールまたはイレイジャーコーディングプロファイルで使用されているストレージプールは削除できません。必要に応じて、**_ storage pool name_**>* ILM usage *を選択して、ストレージプールがどこに使用されているかを確認します。

3. 削除するストレージプールが使用されていない場合は、チェックボックスをオンにします。
4. 「 * 削除」を選択します。
5. 「* OK *」を選択します。

クラウドストレージプールを使用

StorageGRID のクラウドストレージプールについて学ぶ

クラウドストレージプールを使用すると、ILMを使用してオブジェクトデータをStorageGRIDシステムの外部に移動できます。たとえば、アクセス頻度の低いオブジェクトを、Amazon S3 Glacier、S3 Glacier Deep Archive、Google Cloud、Microsoft Azure Blob Storageのアーカイブアクセス層などの低コストのクラウドストレージに移動することができます。または、災害復旧を強化するために、StorageGRIDオブジェクトのクラウドバックアップを保持することもできます。

ILMの観点から見ると、クラウドストレージプールはストレージプールに似ています。オブジェクトをどちらの場所にも保存するには、ILMルールの配置指示を作成する際にプールを選択します。ただし、ストレージプールはStorageGRIDシステム内のストレージノードで構成されているのに対し、クラウドストレージプールは外部バケット（S3）またはコンテナ（Azure Blob Storage）で構成されます。

次の表に、ストレージプールとクラウドストレージプールを比較し、類似点と相違点の概要を示します。

	ストレージプール	クラウドストレージプール
作成方法	Grid Manager で * ILM * > * ストレージプール * オプションを使用している。	Grid Managerで* ILM **>** Storage pools **>** Cloud Storage Pools *オプションを使用する。 クラウドストレージプールを作成する前に、外部のバケットまたはコンテナをセットアップする必要があります。
作成できるプール数	無制限。	最大 10 個。

	ストレージプール	クラウドストレージプール
オブジェクトの格納先	StorageGRID内の1つ以上のストレージノード。	StorageGRIDシステムの外部にあるAmazon S3バケット、Azure Blob Storageコンテナ、またはGoogle Cloud。 クラウドストレージプールが Amazon S3 バケットの場合： • 必要に応じて、 Amazon S3 Glacier や S3 Glacier Deep Archive などの低コストの長期保存用ストレージにオブジェクトを移行するようにバケットライフサイクルを設定できます。外部ストレージシステムでGlacierストレージクラスとS3 RestoreObject APIがサポートされている必要があります。 • AWS Commercial クラウド サービス （ C2S ）で使用するクラウドストレージプールを作成できます。 C2S は AWS Secret Region をサポートします。 クラウドストレージプールが Azure Blob Storage コンテナである場合、StorageGRID はオブジェクトをアーカイブ階層に移行します。 注: 一般的に、クラウド ストレージ プールに使用されるコンテナーに対して、Azure Blob Storage のライフサイクル管理を構成しないでください。RestoreObject クラウド ストレージ プール内のオブジェクトに対する操作は、設定されたライフサイクルによって影響を受ける可能性があります。
オブジェクトの配置を制御する要素	アクティブなILMポリシー内のILMルール。	アクティブなILMポリシー内のILMルール。
使用されるデータ保護方法はどれですか？	レプリケーションまたはイレイジャーコーディング。	レプリケーション：
各オブジェクトに許可されるコピー数	複数。	クラウドストレージプールに 1 つ、また必要に応じて StorageGRID に 1 つ以上のコピーを作成します。 注： 1つのオブジェクトを複数のクラウドストレージプールに同時に格納することはできません。
利点は何ですか？	オブジェクトにいつでもすばやくアクセスできる。	低コストのストレージ。 注：FabricPool データをクラウドストレージプールに階層化することはできません。

StorageGRID におけるクラウドストレージプールオブジェクトのライフサイクル

クラウドストレージプールを実装する前に、クラウドストレージプールのタイプごとに

格納されているオブジェクトのライフサイクルを確認してください。

S3 ：クラウドストレージプールオブジェクトのライフサイクル

S3クラウドストレージプールに格納されるオブジェクトのライフサイクルステージについて説明します。

「Glacier」は、GlacierストレージクラスとGlacier Deep Archiveストレージクラスの両方を表します。例外が1つあります。Glacier Deep Archiveストレージクラスでは、Expeditedリストア階層はサポートされません。Bulk または Standard のみがサポートされます。

Google Cloud Platform （ GCP ）では、 POST Restore 処理を実行しなくても、長期保存からのオブジェクトの読み出しがサポートされます。

1. * StorageGRID * に格納されているオブジェクト

   ライフサイクルを開始するために、クライアントアプリケーションがオブジェクトを StorageGRID に格納します。

2. * オブジェクトを S3 クラウドストレージプールに移動 *

   - S3 クラウドストレージプールを配置場所として使用する ILM ルールにオブジェクトが一致した場合、 StorageGRID はクラウドストレージプールで指定された外部の S3 バケットにオブジェクトを移動します。
   - オブジェクトがS3クラウドストレージプールに移動されると、クライアントアプリケーションは、オブジェクトがGlacierストレージに移行されていないかぎり、StorageGRIDからS3 GetObject要求を使用してオブジェクトを読み出すことができます。

3. * オブジェクトを Glacier に移行（読み出し不可の状態） *

   - 必要に応じて、オブジェクトを Glacier ストレージに移行できます。たとえば外部の S3 バケットが、ライフサイクル設定を使用してオブジェクトを即座または数日後に Glacier ストレージに移行できます。

     オブジェクトを移行する場合は、外部のS3バケットのライフサイクル設定を作成する必要があります。また、Glacierストレージクラスを実装し、S3 RestoreObject APIをサポートするストレージ解決策を使用する必要があります。

   - 移行中、クライアントアプリケーションはS3 HeadObject要求を使用してオブジェクトのステータスを監視できます。

4. * Glacier ストレージからオブジェクトをリストア *

   オブジェクトがGlacierストレージに移行されている場合、クライアントアプリケーションはS3 RestoreObject要求を問題して、読み出し可能なコピーをS3クラウドストレージプールにリストアできます。要求では、クラウドストレージプールでコピーを利用できる日数と、リストア処理に使用するデータアクセス階層（ Expedited 、 Standard 、 Bulk ）を指定します。読み出し可能なコピーの有効期限に達すると、コピーは自動的に読み出し不可能な状態に戻ります。

   StorageGRID内のストレージノードにもオブジェクトのコピーが存在する場合は、RestoreObject要求を実行してGlacierからオブジェクトをリストアする必要はありません。代わりに、GetObject要求を使用してローカルコピーを直接取得できます。

5. * オブジェクトが取得されました *

   オブジェクトがリストアされると、クライアントアプリケーションはGetObject要求を問題して、リストアされたオブジェクトを読み出すことができます。

Azure ：クラウドストレージプールオブジェクトのライフサイクル

Azureクラウドストレージプールに格納されるオブジェクトのライフサイクルステージについて説明します。

1. * StorageGRID * に格納されているオブジェクト

   ライフサイクルを開始するために、クライアントアプリケーションがオブジェクトを StorageGRID に格納します。

2. * オブジェクトを Azure クラウドストレージプールに移動 *

   オブジェクトが、配置場所として Azure クラウド ストレージ プールを使用する ILM ルールに一致する場合、StorageGRID はオブジェクトを、クラウド ストレージ プールで指定された外部の Azure Blob Storage コンテナーに移動します。

3. * オブジェクトをアーカイブ層に移行（読み出し不可の状態） *

   オブジェクトを Azure クラウド ストレージ プールに移動した直後、StorageGRID はオブジェクトを自動的に Azure Blob Storage アーカイブ層に移行します。

4. * アーカイブ層からオブジェクトを復元 *

   オブジェクトがアーカイブ層に移行されている場合、クライアントアプリケーションはS3 RestoreObject要求を問題して、読み出し可能なコピーをAzureクラウドストレージプールにリストアできます。

   StorageGRID が RestoreObject を受信すると、オブジェクトは一時的に Azure Blob Storage Cool ティアに移行されます。RestoreObject リクエストの有効期限に達すると、StorageGRID はオブジェクトをアーカイブ階層に戻します。

   > StorageGRID内のストレージノードにもオブジェクトのコピーが1つ以上存在する場合は、RestoreObject要求を実行してアーカイブアクセス層からオブジェクトをリストアする必要はありません。代わりに、GetObject要求を使用してローカルコピーを直接取得できます。

5. * オブジェクトが取得されました *

   オブジェクトがAzureクラウドストレージプールにリストアされると、クライアントアプリケーションはGetObject要求を問題して、リストアされたオブジェクトを読み出すことができます。

関連情報

"S3 REST APIを使用する"

StorageGRID におけるクラウドストレージプールのユースケース

クラウドストレージプールを使用すると、データを外部の場所にバックアップまたは階層化できます。また、複数のクラウドにデータをバックアップまたは階層化することも

できます。

StorageGRID データを外部の場所にバックアップします

クラウドストレージプールを使用して、 StorageGRID オブジェクトを外部の場所にバックアップできます。

StorageGRID 内のコピーにアクセスできない場合は、クラウドストレージプール内のオブジェクトデータを使用してクライアント要求を処理できます。ただし、クラウドストレージプール内のバックアップオブジェクトコピーにアクセスするには、問題S3 RestoreObject要求が必要になる場合があります。

クラウドストレージプール内のオブジェクトデータは、ストレージボリュームまたはストレージノードの障害が原因で失われたデータを StorageGRID からリカバリする場合にも使用できます。オブジェクトのコピーがクラウドストレージプールにしか残っていない場合、 StorageGRID はオブジェクトを一時的にリストアして、リカバリされたストレージノードに新しいコピーを作成します。

バックアップ解決策 を実装するには

1. 単一のクラウドストレージプールを作成する。
2. ストレージノードにオブジェクトコピーを（レプリケートコピーまたはイレイジャーコーディングコピーとして）同時に格納し、クラウドストレージプールにオブジェクトコピーを 1 つ格納する ILM ルールを設定します。
3. ルールを ILM ポリシーに追加します。次に、ポリシーをシミュレートしてアクティブ化します。

StorageGRID から外部の場所にデータを階層化します

クラウドストレージプールを使用して、 StorageGRID システムの外部にオブジェクトを格納できます。たとえば、保持する必要のあるオブジェクトが多数あり、それらのオブジェクトにアクセスすることはほとんどありません。クラウドストレージプールを使用してオブジェクトを低コストのストレージに階層化し、StorageGRID のスペースを解放できます。

階層化解決策 を実装するには：

1. 単一のクラウドストレージプールを作成する。
2. 使用頻度の低いオブジェクトをストレージノードからクラウドストレージプールに移動する ILM ルールを設定します。
3. ルールを ILM ポリシーに追加します。次に、ポリシーをシミュレートしてアクティブ化します。

複数のクラウドエンドポイントを維持する

オブジェクトデータを複数のクラウドに階層化またはバックアップする場合は、複数のクラウドストレージプールエンドポイントを設定できます。ILMルール内のフィルターを使用すると、各クラウドストレージプールに保存するオブジェクトを指定できます。たとえば、一部のテナントやバケットのオブジェクトを Amazon S3 Glacier に保存し、他のテナントやバケットのオブジェクトを Azure Blob Storage に保存することができます。または、Amazon S3 Glacier と Azure Blob Storage の間でデータを移動することもできます。

> 複数のクラウドストレージプールエンドポイントを使用する場合は、オブジェクトを一度に1つのクラウドストレージプールにしか格納できないことに注意してください。

複数のクラウドエンドポイントを実装するには、次

1. 最大 10 個のクラウドストレージプールを作成できます。
2. 適切なタイミングで適切なオブジェクトデータを各クラウドストレージプールに格納する ILM ルールを設定します。たとえば、バケットAのオブジェクトをクラウドストレージプールAに格納し、バケットBのオブジェクトをクラウドストレージプールBに格納します。または、オブジェクトを一定の時間クラウドストレージプールAに格納してから、クラウドストレージプールBに移動します。
3. ルールを ILM ポリシーに追加します。次に、ポリシーをシミュレートしてアクティブ化します。

StorageGRID におけるクラウドストレージプールの要件と制限

クラウドストレージプールを使用して StorageGRID システムからオブジェクトを移動する場合は、クラウドストレージプールの設定と使用に関する考慮事項を確認しておく必要があります。

一般的な考慮事項

- 一般的に、Amazon S3 Glacier や Azure Blob Storage などのクラウドアーカイブストレージは、オブジェクトデータを安価に保存できる場所です。ただし、クラウドアーカイブストレージからデータを取り出すコストは比較的高額です。全体的なコストを最小限に抑えるには、クラウドストレージプール内のオブジェクトにいつ、どのくらいの頻度でアクセスするかを考慮する必要があります。クラウドストレージプールは、アクセス頻度が低いと予想されるコンテンツにのみ使用することをお勧めします。
- クラウドストレージプールターゲットからオブジェクトを読み出すレイテンシが増加しているため、FabricPool でクラウドストレージプールを使用することはサポートされていません。
- S3オブジェクトロックが有効になっているオブジェクトをクラウドストレージプールに配置することはできません。
- S3オブジェクトロックを使用した次のプラットフォーム、認証、およびプロトコルの組み合わせは、クラウドストレージプールではサポートされていません。
  - プラットフォーム：Google Cloud PlatformとAzure
  - 認証の種類: 匿名アクセス
  - プロトコル：HTTP

クラウドストレージプールに使用するポートに関する考慮事項

指定したクラウドストレージプールとの間でオブジェクトを ILM ルールによって移動できるようにするには、システムのストレージノードが含まれるネットワークを設定する必要があります。次のポートがクラウドストレージプールと通信できることを確認してください。

デフォルトでは、クラウドストレージプールは次のポートを使用します。

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

クラウドストレージプールを作成または編集するときに、別のポートを指定できます。

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

クラウドストレージプールを使用してクラウド内のストレージにアクセスするには、クラウドへのネットワーク接続が必要です。クラウドストレージプールを使用して StorageGRID とクラウドの間で移動するデータ量の予測に基づいて、クラウドへのアクセスに使用するネットワークインフラのコストを考慮し、適切にプロビジョニングする必要があります。

StorageGRID が外部のクラウドストレージプールエンドポイントに接続すると、さまざまな要求を実行して接続を監視し、必要な処理を確実に実行できるようにします。これらの要求には追加コストが伴いますが、クラウドストレージプールの監視にかかるコストは、 S3 または Azure にオブジェクトを格納する場合の全体的なコストのごくわずかです。

外部クラウドストレージプールのエンドポイントから StorageGRID にオブジェクトを戻す必要がある場合、より大きなコストが発生する可能性があります。次のいずれかの場合、オブジェクトが StorageGRID に戻ることがあります。

- オブジェクトの唯一のコピーがクラウドストレージプールにあり、オブジェクトを StorageGRID に格納することにした場合。この場合は、ILMルールとポリシーを再設定します。ILM 評価が実行されると、StorageGRID はクラウドストレージプールからオブジェクトを読み出す要求を複数実行します。次に、StorageGRID は指定された数のレプリケートコピーまたはイレイジャーコーディングコピーをローカルに作成します。オブジェクトが StorageGRID に戻ると、クラウドストレージプール内のコピーは削除されます。
- ストレージノードの障害が原因でオブジェクトが失われた場合。オブジェクトのコピーがクラウドストレージプールにしか残っていない場合、 StorageGRID はオブジェクトを一時的にリストアして、リカバリされたストレージノードに新しいコピーを作成します。

> オブジェクトがクラウドストレージプールから StorageGRID に戻ると、 StorageGRID は各オブジェクトに対してクラウドストレージプールエンドポイントに対して複数の要求を実行します。大量のオブジェクトを移動する場合は、事前にテクニカルサポートに問い合わせて、期間と関連コストの見積もりを依頼してください。

S3 ：クラウドストレージプールバケットに必要な権限

クラウドストレージプールに使用される外部のS3バケットのポリシーで、バケットへのオブジェクトの移動、オブジェクトのステータスの取得、Glacierストレージからのオブジェクトのリストア（必要な場合）などを行う権限をStorageGRIDに付与する必要があります。StorageGRIDにバケットへのフルコントロールアクセスを許可する(`s3:*`のが理想的です）。ただし、許可できない場合は、バケットポリシーでStorageGRIDに次のS3権限を付与する必要があります。

- `s3:AbortMultipartUpload`
- `s3:DeleteObject`
- `s3:GetObject`
- `s3:ListBucket`
- `s3:ListBucketMultipartUploads`
- `s3:ListMultipartUploadParts`
- `s3:PutObject`
- `s3:RestoreObject`

S3：外部バケットのライフサイクルに関する考慮事項

StorageGRIDとクラウドストレージプールに指定された外部のS3バケットとの間のオブジェクトの移動は、StorageGRIDのILMルールとアクティブなILMポリシーによって制御されます。一方、クラウドストレージプールに指定された外部の S3 バケットから Amazon S3 Glacier または S3 Glacier Deep Archive （あるいは Glacier ストレージクラスを実装するストレージ解決策 ）へのオブジェクトの移行は、そのバケットのライフサイクル設定によって制御されます。

クラウドストレージプールからオブジェクトを移行する場合は、外部のS3バケットに適切なライフサイクル設定を作成する必要があります。また、Glacierストレージクラスを実装し、S3 RestoreObject APIをサポートするストレージ解決策を使用する必要があります。

たとえば、 StorageGRID からクラウドストレージプールに移動されたすべてのオブジェクトをすぐに Amazon S3 Glacier ストレージに移行するとします。この場合、単一のアクション（ * Transition * ）を指定する外部の S3 バケットでライフサイクル設定を次のように作成します。

```
<LifecycleConfiguration>
  <Rule>
    <ID>Transition Rule</ID>
    <Filter>
       <Prefix></Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>0</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>
```

このルールは、すべてのバケットオブジェクトを作成された日（ StorageGRID からクラウドストレージプールに移動された日）に Amazon S3 Glacier に移行します。

> 外部バケットのライフサイクルを設定する場合、 * Expiration * アクションを使用してオブジェクトの期限を定義しないでください。Expiration アクション期限切れのオブジェクトを削除するために、外部ストレージシステムを原因 します。期限切れのオブジェクトにあとで StorageGRID からアクセスしようとしても、削除されたオブジェクトは見つかりません。

クラウドストレージプール内のオブジェクトを（Amazon S3 Glacierではなく）S3 Glacier Deep Archiveに移行する場合は、バケットライフサイクルでを指定します `<StorageClass>DEEP_ARCHIVE</StorageClass>`。ただし、この階層を使用してS3 Glacier Deep Archiveからオブジェクトをリストアすることはできません `Expedited`。

Azure ：アクセス層に関する考慮事項

Azure ストレージアカウントを設定する場合は、デフォルトのアクセス層をホットまたはクールに設定できます。クラウドストレージプールで使用するストレージアカウントを作成する場合は、デフォルト階層としてホット階層を使用する必要があります。StorageGRID はオブジェクトをクラウドストレージプールに移動するとすぐに階層をアーカイブに設定しますが、デフォルト設定をホットにしておくことで、最低期間の 30 日前

にクール階層から削除されたオブジェクトに対する早期削除料金が発生しません。

Azure ：ライフサイクル管理はサポートされていません

Cloud Storage Pool で使用するコンテナには、Azure Blob Storage のライフサイクル管理を使用しないでください。ライフサイクル操作が Cloud Storage Pool の操作に干渉する可能性があります。

関連情報

"クラウドストレージプールを作成"

StorageGRID におけるクラウドストレージプールと **CloudMirror** レプリケーション

クラウドストレージプールの使用を開始するにあたって、クラウドストレージプールとStorageGRID CloudMirror レプリケーションサービスの類似点と相違点を理解しておくと役立ちます。

	クラウドストレージプール	**CloudMirror** レプリケーションサービス
主な目的は何ですか？	アーカイブターゲットとして機能します。クラウドストレージプール内のオブジェクトコピーは、オブジェクトの唯一のコピーにすることも、追加のコピーにすることもできます。つまり、2つのコピーをオンサイトに保持する代わりに、1つのコピーをStorageGRID 内に保持してクラウドストレージプールに送信できます。	テナントで、StorageGRID （ソース）内のバケットから外部のS3バケット（デスティネーション）にオブジェクトを自動的にレプリケートできます。独立したS3インフラにオブジェクトの独立したコピーを作成します。
セットアップ方法は？	Grid ManagerまたはグリッドAPIを使用して、ストレージプールと同じ方法で定義されます。ILMルールで配置場所として選択できます。ストレージプールはストレージノードのグループで構成されますが、クラウドストレージプールはリモートの S3 または Azure エンドポイント（ IP アドレス、クレデンシャルなど）を使用して定義されます。	テナントユーザ"CloudMirror レプリケーションを設定します"。Tenant ManagerまたはS3 APIを使用してCloudMirrorエンドポイント（IPアドレス、クレデンシャルなど）を定義します。CloudMirror エンドポイントのセットアップ後、そのテナントアカウントが所有するバケットは、 CloudMirror エンドポイントを参照するように設定できます。
設定は誰が担当しますか？	通常はグリッド管理者	通常はテナントユーザ
デスティネーションは何ですか？	• 互換性のある任意の S3 インフラ（ Amazon S3 を含む） • Azure BLOB アーカイブ層 • Google Cloud Platform（GCP）	• 互換性のある任意の S3 インフラ（ Amazon S3 を含む） • Google Cloud Platform（GCP）

	クラウドストレージプール	**CloudMirror** レプリケーションサービス
オブジェクトをデスティネーションに移動する原因は何ですか？	アクティブなILMポリシー内の1つ以上のILMルール。ILM ルールは、 StorageGRID がクラウドストレージプールに移動するオブジェクトとオブジェクトを移動するタイミングを定義します。	CloudMirrorエンドポイントで設定されたソースバケットに新しいオブジェクトを取り込む処理。CloudMirrorエンドポイントを設定する前にソースバケットに存在していたオブジェクトは、変更しないかぎりレプリケートされません。
オブジェクトの読み出し方法	アプリケーションは、クラウドストレージプールに移動されたオブジェクトを読み出すために、 StorageGRID への要求を行う必要があります。オブジェクトの唯一のコピーがアーカイブストレージに移行された場合、 StorageGRID はオブジェクトのリストアプロセスを管理して読み出し可能にします。	デスティネーションバケット内のミラーコピーは独立したコピーであるため、アプリケーションは、 StorageGRID または S3 デスティネーションに要求を行うことでオブジェクトを読み出すことができます。たとえば、 CloudMirror レプリケーションを使用してパートナー組織にオブジェクトをミラーリングするとします。パートナーは、独自のアプリケーションを使用して、 S3 デスティネーションからオブジェクトを直接読み取ったり更新したりできます。StorageGRID を使用する必要はありません。
デスティネーションから直接読み取ることはできますか。	いいえ。クラウドストレージプールに移動されたオブジェクトは、StorageGRIDによって管理されます。読み取り要求は StorageGRID に転送する必要があります（ StorageGRID がクラウドストレージプールからの読み出しを実行します）。	はい。ミラーコピーは独立したコピーであるためです。
オブジェクトがソースから削除された場合はどうなりますか？	オブジェクトもクラウドストレージプールから削除されます。	削除操作は複製されません。削除したオブジェクトは StorageGRID バケットには存在しなくなりますが、デスティネーションバケットには引き続き存在します。同様に、デスティネーションバケット内のオブジェクトもソースに影響を与えることなく削除できます。
災害後（ StorageGRID システムが動作していない）にどのようにしてオブジェクトにアクセスしますか。	障害が発生した StorageGRID ノードをリカバリする必要があります。このプロセスでは、レプリケートされたオブジェクトのコピーをクラウドストレージプールのコピーを使用してリストアすることができます。	CloudMirror デスティネーション内のオブジェクトコピーは StorageGRID から独立しているため、 StorageGRID ノードがリカバリされる前に直接アクセスできます。

StorageGRID でクラウドストレージプールを作成する

クラウド ストレージ プールは、単一の外部 Amazon S3 バケット、その他の S3 互換プロバイダー、または Azure Blob Storage コンテナーを指定します。

クラウドストレージプールを作成する際に、外部バケットまたはコンテナの名前と場所、StorageGRID がオブジェクトの保存に使用するクラウド プロバイダ タイプ（Amazon S3/GCP または Azure Blob Storage ）、および StorageGRID が外部バケットまたはコンテナにアクセスするために必要な情報を指定します。

クラウドストレージプールは保存後すぐに StorageGRID で検証されます。そのため、クラウドストレージプールに指定されたバケットまたはコンテナが存在し、アクセス可能であることを確認しておく必要があります。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"必要なアクセス権限"。
- を確認しておきます"クラウドストレージプールに関する考慮事項"。
- クラウドストレージプールによって参照される外部のバケットまたはコンテナがすでに存在し、を用意しておきサービスエンドポイント情報ます。
- バケットまたはコンテナにアクセスするには、を認証タイプのアカウント情報選択します。

手順

1. ILM > Storage pools > Cloud Storage Pools *を選択します。
2. [作成]*を選択し、次の情報を入力します。

フィールド	製品説明
クラウドストレージプールの名前	クラウドストレージプールとその目的を簡単に説明する名前。ILM ルールを設定するときに識別しやすい名前を使用してください。
プロバイダタイプ	このクラウドストレージプールに使用するクラウドプロバイダ： • * Amazon S3 / GCP *：Amazon S3、Commercial Cloud Services（C2S ）S3、Google Cloud Platform（GCP）、またはその他のS3互換プロバイダの場合は、このオプションを選択します。 • * Azure Blob Storage *
バケットまたはコンテナ	外部のS3バケットまたはAzureコンテナの名前。クラウドストレージプールの保存後にこの値を変更することはできません。

3. プロバイダタイプの選択に基づいて、サービスエンドポイント情報を入力します。

Amazon S3 / GCP

a. プロトコルに対して、[HTTPS]または[HTTP]を選択します。

> 機密データにHTTP接続を使用しないでください。

b. ホスト名を入力します。例：

```
s3-aws-region.amazonaws.com
```

c. URLスタイルを選択します。

オプション	製品説明
自動検出	指定された情報に基づいて、使用する URL スタイルを自動的に検出します。たとえば、 IP アドレスを指定すると、 StorageGRID はパス形式の URL を使用します。使用するスタイルがわからない場合にのみ、このオプションを選択してください。
virtual-hosted-styleの略	仮想ホスト形式のURLを使用してバケットにアクセスします。仮想ホスト形式のURLでは、ドメイン名の一部にバケット名が含まれます。例： `https://bucket-name.s3.company.com/key-name`
パス形式	パス形式の URL を使用してバケットにアクセスします。パス形式のURLの末尾にはバケット名が含まれます例： `https://s3.company.com/bucket-name/key-name` *注：*パス形式のURLオプションは推奨されておらず、StorageGRIDの今後のリリースで廃止される予定です。

d. 必要に応じて、ポート番号を入力するか、デフォルトのポート（HTTPSの場合は443、HTTPの場合は80）を使用します。

Azure Blobストレージ

a. 次のいずれかの形式を使用して、サービスエンドポイントのURIを入力します。

- `https://host:port`
- `http://host:port`

例： `https://myaccount.blob.core.windows.net:443`

ポートを指定しない場合、HTTPSにはデフォルトでポート443が使用され、HTTPにはポート80が使用されます。

4. *[続行]*を選択します。次に、認証タイプを選択し、クラウドストレージプールエンドポイントに必要な情報を入力します。

アクセスキー

*Amazon S3 / GCP*またはその他の*S3*互換プロバイダの場合

a. * Access key ID *：外部バケットを所有するアカウントのアクセスキーIDを入力します。
b. シークレットアクセスキー：シークレットアクセスキーを入力します。

IAMのあらゆる場所での役割

_ AWS IAMロールAnywhereサービスの場合_

StorageGRIDは、AWSセキュリティトークンサービス（STS）を使用して、AWSリソースにアクセスするための短期間のトークンを動的に生成します。

a. * AWS IAM Roles Anywhereリージョン*：クラウドストレージプールのリージョンを選択します。たとえば、 `us-east-1`です。
b. *トラストアンカーURN *：短期間のSTSクレデンシャルの要求を検証するトラストアンカーのURNを入力します。ルートCAまたは中間CAを指定できます。
c. *プロファイルURN *：IAM Roles Anywhereプロファイルの URNを入力します。このプロファイルには、信頼できるユーザのロールが表示されます。
d. * Role URN *：信頼されたすべてのユーザに想定されるIAMロールのURNを入力します。
e. セッション期間：一時的なセキュリティクレデンシャルとロールセッションの期間を入力します。15分以上12時間以下を入力してください。
f. サーバ**CA**証明書（オプション）：IAM Roles Anywhereサーバを検証するための、PEM形式の1つ以上の信頼されたCA証明書。省略すると、サーバは検証されません。
g. エンドエンティティ証明書：信頼アンカーによって署名されたX509証明書のPEM形式の公開キー。AWS IAMロールAnywhereは、このキーを使用してSTSトークンを発行します。
h. エンドエンティティ秘密鍵：エンドエンティティ証明書の秘密鍵。

CAP（**C2S**アクセスポータル）

_ Commercial Cloud Services（C2S）S3サービス_

a. *一時的なクレデンシャルURL *：StorageGRIDがCAPサーバから一時的なクレデンシャルを取得するために使用する完全なURLを入力します。これには、C2Sアカウントに割り当てられた必須およびオプションのAPIパラメータがすべて含まれます。
b. サーバ**CA**証明書：*[参照]*を選択し、StorageGRIDがCAPサーバの検証に使用するCA証明書をアップロードします。証明書はPEMでエンコードされ、適切な政府認証局（CA）によって発行されている必要があります。
c. クライアント証明書：*[参照]*を選択し、StorageGRIDがCAPサーバに自身を識別するために使用する証明書をアップロードします。クライアント証明書はPEMでエンコードされ、適切な政府認証局（CA）によって発行され、C2Sアカウントへのアクセスが許可されている必要があります。
d. クライアント秘密鍵：*[参照]*を選択し、クライアント証明書用のPEMでエンコードされた秘密鍵をアップロードします。
e. クライアントの秘密鍵が暗号化されている場合は、クライアントの秘密鍵を復号化するためのパスフレーズを入力します。それ以外の場合は、* Client private key passphrase *フィールドを空白のままにします。

クライアント証明書が暗号化される場合は、暗号化に従来の形式を使用します。PKCS#8暗号化形式はサポートされていません。

Azure Blobストレージ

Azure Blob Storage、共有キーのみ_

a. アカウント名：外部コンテナを所有するストレージアカウントの名前を入力します。
b. アカウントキー：ストレージアカウントのシークレットキーを入力します。

これらの値は Azure portal を使用して確認できます。

匿名

追加情報 は必要ありません。

5. 「 * Continue * 」を選択します。次に、使用するサーバ検証のタイプを選択します。

オプション	製品説明
ストレージノードOSでルートCA証明書を使用する	オペレーティングシステムにインストールされているグリッド CA 証明書を使用して接続を保護します。
カスタム CA 証明書を使用する	カスタム CA 証明書を使用する。[Browse]*を選択し、PEMでエンコードされた証明書をアップロードします。
証明書を検証しないでください	このオプションを選択すると、クラウドストレージプールへのTLS接続はセキュアではありません。

6. [保存（ Save ）] を選択します。

クラウドストレージプールを保存すると、 StorageGRID では次の処理が実行されます。

- バケットまたはコンテナとサービスエンドポイントが存在し、指定したクレデンシャルを使用してアクセスできることを検証します。
- クラウドストレージプールとして識別するために、バケットまたはコンテナにマーカーファイルを書き込みます。このファイルは削除しないでください（という名前） `x-ntap-sgws-cloud-pool-uuid`。

  クラウドストレージプールの検証に失敗すると、その理由を記載したエラーメッセージが表示されます。たとえば、証明書エラーが発生した場合や、指定したバケットまたはコンテナが存在しない場合にエラーが報告されることがあります。

7. エラーが発生した場合は、を参照し"クラウドストレージプールのトラブルシューティング手順"、問題を解決してから、クラウドストレージプールの保存を再試行してください。

関連情報

"外部との通信に使用するポート"

StorageGRID でクラウドストレージプールの詳細を表示する

クラウドストレージプールの詳細を表示して、そのプールがどこで使用されているかを確認したり、どのノードとストレージグレードが含まれているかを確認したりできます。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- そうだな "特定のアクセス権限"

手順

1. ILM > Storage pools > Cloud Storage Pools *を選択します。

   [Cloud Storage Pools]テーブルには、ストレージノードを含む各クラウドストレージプールに関する次の情報が表示されます。

   - 名前:プールの一意の表示名。
   - * URI *：クラウドストレージプールのUniform Resource Identifier。
   - プロバイダタイプ：このクラウドストレージプールに使用されているクラウドプロバイダ。
   - * Container *：クラウドストレージプールに使用されるバケットの名前。
   - * ILM usage *：プールの現在の使用状況。クラウドストレージプールは、使用されていない場合や、1つ以上のILMルール、イレイジャーコーディングプロファイル、またはその両方で使用されている場合があります。
   - 前回のエラー：このクラウドストレージプールの健全性チェックで検出された最後のエラー。
2. 特定のクラウドストレージプールの詳細を表示するには、その名前を選択します。

   プールの詳細ページが表示されます。

3. [認証]*タブを表示して、このクラウドストレージプールの認証タイプの詳細を確認し、認証の詳細を編集します。
4. [サーバの検証]タブを表示して、検証の詳細、検証の編集、新しい証明書のダウンロード、証明書PEMのコピーを確認します。
5. クラウドストレージプールがILMルールまたはイレイジャーコーディングプロファイルで現在使用されているかどうかを確認するには、*[ILM usage（ILM usage）]*タブを表示します。
6. 必要に応じて、クラウドストレージプールを使用する* ILMルールページ*に移動し"ルールの詳細と管理"ます。

StorageGRID でクラウドストレージプールを編集する

クラウドストレージプールを編集して、名前、サービスエンドポイント、またはその他の詳細を変更できます。ただし、クラウドストレージプールのS3バケットまたはAzureコンテナを変更することはできません。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。

- そうだな "特定のアクセス権限"
- を確認しておきます"クラウドストレージプールに関する考慮事項"。

手順

1. ILM > Storage pools > Cloud Storage Pools *を選択します。

   Cloud Storage Pools テーブルには、既存のクラウドストレージプールが表示されます。

2. 編集するクラウドストレージプールのチェックボックスを選択し、[操作]>*[編集]*を選択します。

   または、クラウドストレージプールの名前を選択し、*[編集]*を選択します。

3. 必要に応じて、クラウドストレージプール名、サービスエンドポイント、認証クレデンシャル、または証明書の検証方法を変更します。

   > クラウドストレージプールのプロバイダタイプ、S3バケット、Azureコンテナは変更できません。

   以前にサーバ証明書またはクライアント証明書をアップロードした場合は、*[証明書の詳細]*アコーディオンを展開して、現在使用中の証明書を確認できます。

4. [保存（ Save ）] を選択します。

   クラウドストレージプールを保存すると、バケットまたはコンテナとサービスエンドポイントが存在し、指定したクレデンシャルでそれらにアクセスできることが StorageGRID によって検証されます。

   クラウドストレージプールの検証が失敗すると、エラーメッセージが表示されます。たとえば、証明書エラーが発生した場合はエラーが報告されます。

   の手順を参照し"クラウドストレージプールのトラブルシューティング"、問題を解決してから、クラウドストレージプールの保存を再試行してください。

StorageGRID でクラウドストレージプールを削除する

ILMルールで使用されておらず、オブジェクトデータが含まれていないクラウドストレージプールは削除できます。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"必要なアクセス権限"。

必要に応じて、ILMを使用してオブジェクトデータを移動します

削除するクラウドストレージプールにオブジェクトデータが含まれている場合は、ILMを使用してデータを別の場所に移動する必要があります。たとえば、グリッド上のストレージノードや別のクラウドストレージプールにデータを移動できます。

手順

1. ILM > Storage pools > Cloud Storage Pools *を選択します。

2. テーブルの[ILM usage]列で、クラウドストレージプールを削除できるかどうかを確認します。

   ILMルールまたはイレイジャーコーディングプロファイルで使用されているクラウドストレージプールは削除できません。

3. クラウドストレージプールを使用している場合は、**_ cloud storage pool name_**>* ILM usage *を選択します。
4. "各ILMルールをクローニングします"削除するクラウドストレージプールにオブジェクトが現在配置されています。
5. クローニングした各ルールで管理されている既存のオブジェクトの移動先を決定します。

   1つ以上のストレージプール、または別のクラウドストレージプールを使用できます。

6. クローニングした各ルールを編集します。

   Create ILM Ruleウィザードのステップ2で、* Copies at *フィールドから新しい場所を選択します。

7. "新しいILMポリシーを作成する"古いルールを複製したルールに置き換えます。
8. 新しいポリシーをアクティブ化します。
9. ILMによってクラウドストレージプールからオブジェクトが削除され、新しい場所に配置されるまで待ちます。

クラウドストレージプールを削除

クラウドストレージプールが空でILMルールで使用されていない場合は削除できます。

開始する前に

- プールを使用している可能性があるILMルールを削除しておきます。
- S3 バケットまたは Azure コンテナにオブジェクトが含まれていないことを確認します。

  クラウドストレージプールにオブジェクトが含まれている場合、そのストレージプールを削除しようとするとエラーが発生します。を参照して "クラウドストレージプールのトラブルシューティング"

> クラウドストレージプールを作成すると、 StorageGRID はバケットまたはコンテナにマーカーファイルを書き込み、クラウドストレージプールとして識別します。という名前のファイルは削除しないで `x-ntap-sgws-cloud-pool-uuid`ください。

手順

1. ILM **>** Storage pools **>** Cloud Storage Pools *を選択します。
2. [ILM usage]列にクラウドストレージプールが使用されていないことが示されている場合は、チェックボックスをオンにします。
3. * アクション * > * 削除 * を選択します。
4. 「* OK *」を選択します。

以下のトラブルシューティング手順を使用して、クラウドストレージプールを作成、編集、または削除するときに発生する可能性があるエラーを解決します。

エラーが発生したかどうかを確認します

StorageGRIDは、既知のオブジェクトを読み取り、すべてのクラウドストレージプールで簡単な健全性チェックを実行して、 `x-ntap-sgws-cloud-pool-uuid`クラウドストレージプールにアクセスできることと、正常に機能していることを確認します。エンドポイントでエラーが発生すると、StorageGRIDは各ストレージノードから1分ごとに健全性チェックを実行します。エラーが解決されると、健全性チェックは停止します。健全性チェックで問題が検出されると、[Storage pools]ページの[Cloud Storage Pools]テーブルの[Last error]列にメッセージが表示されます。

次の表は、各クラウドストレージプールで検出された最新のエラーと、エラーが発生してからの時間を示しています。

また、過去 5 分以内に新しいクラウドストレージプールのエラーが発生したことが健全性チェックで検出されると、 * クラウドストレージプール接続エラー * アラートがトリガーされます。このアラートのEメール通知を受信した場合は、[ストレージプール]ページ（* ILM > Storage pools *を選択）に移動し、[最後のエラー]列のエラーメッセージを確認して、以下のトラブルシューティングのガイドラインを参照してください。

エラーが解決されたかどうかを確認します

エラーの原因となっている問題を解決したら、エラーが解決されたかどうかを確認できます。[クラウドストレージプール]ページで、エンドポイントを選択し、*[エラーのクリア]*を選択します。StorageGRID がクラウドストレージプールのエラーをクリアしたことを示す確認メッセージが表示されます。

原因となっている問題が解決されると、エラーメッセージは表示されなくなります。ただし、根本的な問題が解決されていない場合（または別のエラーが発生した場合）は、数分以内に[Last error]列にエラーメッセージが表示されます。

エラー：健全性チェックに失敗しました。エンドポイントからのエラーです

次のような場合に、このエラーが発生する可能性があります：

- Amazon S3 バケットをクラウドストレージプールとして使用し始めた後に、デフォルトの保持期間を設定した S3 オブジェクトロックをそのバケットで有効にした場合。このエラーは、PUT 操作に `Content-MD5`などのペイロードチェックサム値を含む HTTP ヘッダーがない場合に発生します。このヘッダー値は、S3 オブジェクトロックが有効になっているバケットへの PUT 操作に対して AWS が要求するものです。

  この問題を解決するには、変更を加えずに"クラウドストレージプールを編集します"の手順に従ってください。この操作により、クラウドストレージプール構成の検証がトリガーされ、クラウドストレージプールエンドポイント構成の S3 オブジェクトロックフラグが自動的に検出および更新されます。

- このバケットをクラウドストレージプールとして使用し始めた後に、StorageGRID S3バケットに対してデフォルトの保持期間を設定したS3オブジェクトロックを有効にした場合。

  この問題を解決するには：

  - HTTP を使用している場合：S3 オブジェクトロックが有効になっているクラウドストレージプールはサポートされていません。エンドポイント接続を編集して、代わりに HTTPS を使用するようにして

ください。

- HTTPS を使用している場合："クラウドストレージプールを編集します" の手順に従い、変更は加えないでください。この操作により、Cloud Storage Pool 構成の検証がトリガーされ、Cloud Storage Pool エンドポイント構成の S3 Object Lock フラグが自動的に検出および更新されます。

さらに問題が発生した場合は、テクニカルサポートにお問い合わせください。

エラー：このクラウドストレージプールには予期しないコンテンツが含まれています

クラウドストレージプールを作成、編集、または削除しようとすると、このエラーが発生する場合があります。このエラーは、バケットまたはコンテナにマーカーファイルが含まれているが、想定されるUUIDのメタデータフィールドがファイルにない場合に発生し `x-ntap-sgws-cloud-pool-uuid`ます。

通常、このエラーが表示されるのは、新しいクラウドストレージプールを作成していて、 StorageGRID の別のインスタンスがすでに同じクラウドストレージプールを使用している場合のみです。

この問題を解決するには、次のいずれかの手順を実行します。

- 新しいクラウドストレージプールを設定する場合に、次の例に示すように、ファイルと追加のオブジェクトキーがバケットに含まれている場合 `x-ntap-sgws-cloud-pool-uuid`は、新しいバケットを作成し、この新しいバケットを使用します。

  追加のオブジェクトキーの例： `my-bucket.3E64CF2C-B74D-4B7D-AFE7-AD28BC18B2F6.1727326606730410`

- ファイルがバケット内の唯一のオブジェクトである場合 `x-ntap-sgws-cloud-pool-uuid`は、このファイルを削除します。

これらの手順がシナリオに当てはまらない場合は、サポートにお問い合わせください。

エラー：クラウドストレージプールを作成または更新できませんでした。エンドポイントからのエラーです

このエラーは、次の状況で発生することがあります。

- クラウドストレージプールを作成または編集するとき。
- 新しいクラウドストレージプールの構成時に、サポートされていないプラットフォーム、認証、またはプロトコルの組み合わせをS3オブジェクトロックと選択した場合。を参照して "クラウドストレージプールに関する考慮事項"

このエラーは、接続または構成の問題が原因でStorageGRIDがクラウドストレージプールに書き込めないことを示しています。

問題 を修正するには、エンドポイントからのエラーメッセージを確認します。

- エラーメッセージにが含まれている場合 `Get *url*: EOF`は、クラウドストレージプールに使用されるサービスエンドポイントで、HTTPSを必要とするコンテナまたはバケットにHTTPが使用されていないことを確認します。
- エラーメッセージにが含まれている場合は `Get *url*: net/http: request canceled while waiting for connection`、クラウドストレージプールに使用されるサービスエンドポイントへのストレージノードのアクセスがネットワーク構成で許可されていることを確認します。
- サポートされていないプラットフォーム、認証、またはプロトコルが原因でエラーが発生した場合は、S3

オブジェクトロックを使用してサポートされている構成に変更し、新しいクラウドストレージプールをもう一度保存してください。

- その他のすべてのエンドポイントエラーメッセージについては、次のいずれか、または複数の操作を試してください。
  - クラウドストレージプール用に入力した名前と同じ名前の外部コンテナまたはバケットを作成して、新しいクラウドストレージプールを再度保存します。
  - クラウドストレージプール用に指定したコンテナまたはバケット名を修正して、新しいクラウドストレージプールを再度保存します。

エラー： **CA** 証明書を解析できませんでした

クラウドストレージプールを作成または編集しようとすると、このエラーが発生する場合があります。このエラーは、クラウドストレージプールの設定時に入力した証明書を StorageGRID が解析できなかった場合に発生します。

問題 を修正するには、指定した CA 証明書に問題がないかどうかを確認します。

エラー：この **ID** のクラウドストレージプールが見つかりませんでした

クラウドストレージプールを編集または削除しようとすると、このエラーが発生する場合があります。このエラーは、次のいずれかの理由でエンドポイントが 404 応答を返した場合に発生します。

- クラウドストレージプールに使用されるクレデンシャルにバケットの読み取り権限がありません。
- クラウドストレージプールに使用されるバケットにマーカーファイルが含まれてい `x-ntap-sgws-cloud-pool-uuid`ません。

問題 を修正するには、次の手順をいくつか実行します。

- 設定したアクセスキーに関連付けられているユーザに必要な権限があることを確認します。
- 必要な権限があるクレデンシャルを使用してクラウドストレージプールを編集します。
- 権限が正しい場合は、サポートにお問い合わせください。

エラー：クラウドストレージプールの内容を確認できませんでした。エンドポイントからのエラーです

クラウドストレージプールを削除しようとすると、このエラーが発生する場合があります。このエラーは、何らかの接続または設定問題 が原因で、 StorageGRID がクラウドストレージプールバケットのコンテンツを読み取れないことを示しています。

問題 を修正するには、エンドポイントからのエラーメッセージを確認します。

エラー： **Objects have already been placed in this bucket**

クラウドストレージプールを削除しようとすると、このエラーが発生する場合があります。ILMによって移動されたデータ、クラウドストレージプールの設定前にバケットにあったデータ、またはクラウドストレージプールの作成後に他のソースによってバケットに配置されたデータが含まれているクラウドストレージプールは削除できません。

問題 を修正するには、次の手順をいくつか実行します。

- 「クラウドストレージプールオブジェクトのライフサイクル」の手順に従って、オブジェクト

をStorageGRIDに戻します。

- 残りのオブジェクトが ILM によってクラウドストレージプールに配置されていないことが確実な場合は、バケットからオブジェクトを手動で削除します。

> ILM によって配置された可能性のあるクラウドストレージプールからは、オブジェクトを手動で削除しないでください。手動で削除したオブジェクトにあとで StorageGRID からアクセスしようとしても、削除したオブジェクトは見つかりません。

エラー：クラウドストレージプールにアクセスしようとして、プロキシで外部エラーが発生しました

このエラーは、ストレージノードとクラウドストレージプールに使用される外部のS3エンドポイントの間に非透過型ストレージプロキシを設定した場合に発生することがあります。このエラーは、外部プロキシサーバがCloud Storage Poolエンドポイントにアクセスできない場合に発生します。たとえば、 DNS サーバがホスト名を解決できない場合や、外部ネットワークの問題 が存在する場合があります。

問題 を修正するには、次の手順をいくつか実行します。

- クラウドストレージプール（ * ILM * > * ストレージプール * ）の設定を確認します。
- ストレージプロキシサーバのネットワーク設定を確認します。

エラー：**X.509**証明書が有効期間外です

クラウドストレージプールを削除しようとすると、このエラーが発生する場合があります。このエラーは、クラウドストレージプール構成を削除する前に、正しい外部クラウドストレージプールが検証され、外部プールが空であることを確認するために、認証にX.509証明書が必要な場合に発生します。

問題 を修正するには、次の手順を実行します。

- 認証用に設定された証明書をクラウドストレージプールに更新します。
- このクラウドストレージプールに対する証明書の有効期限に関するアラートが解決されていることを確認してください。

関連情報

"クラウドストレージプールオブジェクトのライフサイクル"

StorageGRID でイレイジャー コーディング プロファイルを管理

イレイジャーコーディングプロファイルの詳細を表示し、必要に応じてプロファイルの名前を変更できます。現在どのILMルールでも使用されていないイレイジャーコーディングプロファイルは非アクティブ化できます。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"必要なアクセス権限"。

イレイジャーコーディングプロファイルの詳細の表示

イレイジャーコーディングプロファイルの詳細を表示して、プロファイルのステータス、使用されているイレ

イジャーコーディングスキームなどの情報を確認できます。

手順

1. 構成 > システム > *消去コーディング*を選択します。
2. プロファイルを選択します。プロファイルの詳細ページが表示されます。
3. 必要に応じて、[ILM rules]タブで、プロファイルを使用するILMルールと、それらのルールを使用するILMポリシーのリストを確認します。
4. 必要に応じて、プロファイルのストレージプール内の各ストレージノード（ノードが配置されているサイトやストレージの使用状況など）の詳細を[ストレージノード]タブで確認します。

イレイジャーコーディングプロファイルの名前を変更する

イレイジャーコーディングプロファイルの名前を変更すると、プロファイルの内容がわかりやすくなります。

手順

1. 構成 > システム > *消去コーディング*を選択します。
2. 名前を変更するプロファイルを選択します。
3. [名前の変更 *] を選択します。
4. イレイジャーコーディングプロファイルの一意の名前を入力します。

   イレイジャーコーディングプロファイル名は、ILMルールの配置手順でストレージプール名に追加されます。

   > イレイジャーコーディングプロファイル名は一意である必要があります。既存のプロファイルの名前を使用すると、そのプロファイルが非アクティブ化されていても、検証エラーが発生します。

5. [保存（ Save ）] を選択します。

イレイジャーコーディングプロファイルを非アクティブ化する

イレイジャーコーディングプロファイルの使用を予定していない場合や現在どのILMルールでも使用されていない場合は、非アクティブ化できます。

> イレイジャーコーディングデータの修復処理や運用停止手順が実行中でないことを確認する。いずれかの処理の実行中にイレイジャーコーディングプロファイルを非アクティブ化しようとすると、エラーメッセージが返されます。

タスクの内容

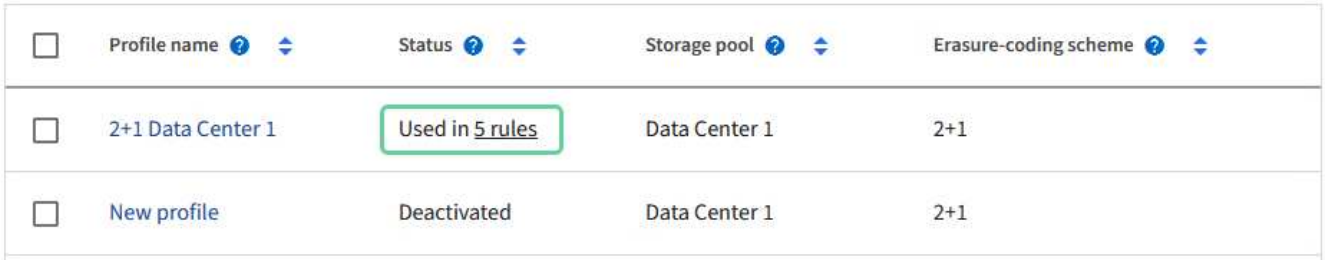
次のいずれかに該当する場合、StorageGRIDではイレイジャーコーディングプロファイルを非アクティブ化できません。

- イレイジャーコーディングプロファイルがILMルールで使用されている。
- イレイジャーコーディングプロファイルはどのILMルールでも使用されなくなりましたが、プロファイルのオブジェクトデータフラグメントとパリティフラグメントは引き続き存在します。

手順

1. 構成 > システム > *消去コーディング*を選択します。
2. [Active]タブの*[Status]*列で、非アクティブ化するイレイジャーコーディングプロファイルがILMルールで使用されていないことを確認します。

   イレイジャーコーディングプロファイルがILMルールで使用されている場合、非アクティブ化することはできません。この例では、2+1のData Center 1プロファイルが少なくとも1つのILMルールで使用されています。



3. プロファイルが ILM ルールで使用されている場合は、次の手順を実行します。
   a. [* ILM*>* Rules] を選択します。
   b. 各ルールを選択し、保持図を確認して、非アクティブ化するイレイジャーコーディングプロファイルがルールで使用されているかどうかを確認します。
   c. 非アクティブ化するイレイジャーコーディングプロファイルがILMルールで使用されている場合は、そのルールがILMポリシーで使用されているかどうかを確認します。
   d. イレイジャーコーディングプロファイルの使用場所に応じて、表の追加の手順を実行します。

プロファイルはどこで使用されていますか？	プロファイルを非アクティブ化する前に実行する追加手順	追加の手順を参照してください
ILM ルールでは使用されません	追加の手順は必要ありません。この手順に進みます。	_ なし _
ILM ポリシーで使用されたことのない ILM ルール	i. 該当する ILM ルールをすべて編集または削除します。ルールを編集する場合は、イレイジャーコーディングプロファイルを使用しているすべての配置を削除します。 ii. この手順に進みます。	"ILM ルールおよび ILM ポリシーの操作"

プロファイルはどこで使用されていますか？	プロファイルを非アクティブ化する前に実行する追加手順	追加の手順を参照してください
アクティブなILMポリシーに含まれるILMルールで使用	i. ポリシーのクローンを作成します。 ii. イレイジャーコーディングプロファイルを使用しているILMルールを削除します。 iii. オブジェクトを確実に保護するために、新しい ILM ルールを 1 つ以上追加します。 iv. 新しいポリシーを保存、シミュレート、およびアクティブ化します。 v. 新しいポリシーが適用され、追加した新しいルールに基づいて既存のオブジェクトが新しい場所に移動されるまで待ちます。 ◦ 注： StorageGRID システムのオブジェクト数とサイズによっては、新しい ILM ルールに基づいてオブジェクトを新しい場所に移動するのに数週間から数カ月かかる場合があります。 データに関連付けられているイレイジャーコーディングプロファイルは安全に非アクティブ化できますが、非アクティブ化処理は失敗します。プロファイルを非アクティブ化する準備ができていない場合は、エラーメッセージが表示されます。 vi. ポリシーから削除したルールを編集または削除します。ルールを編集する場合は、イレイジャーコーディングプロファイルを使用しているすべての配置を削除します。 vii. この手順に進みます。	"ILMポリシーを作成します" "ILM ルールおよび ILM ポリシーの操作"
ILMポリシーに含まれるILMルールで使用	i. ポリシーを編集します。 ii. イレイジャーコーディングプロファイルを使用しているILMルールを削除します。 iii. すべてのオブジェクトが保護されるように 1 つ以上の新しい ILM ルールを追加します。 iv. ポリシーを保存します。 v. ポリシーから削除したルールを編集または削除します。ルールを編集する場合は、イレイジャーコーディングプロファイルを使用しているすべての配置を削除します。 vi. この手順に進みます。	"ILMポリシーを作成します" "ILM ルールおよび ILM ポリシーの操作"

e. [Erasure-Coding Profiles]ページをリフレッシュして、プロファイルがILMルールで使用されていないことを確認します。

4. プロファイルが ILM ルールで使用されていない場合は、ラジオボタンを選択し、 * Deactivate * を選択し

ます。[Deactivate erase-coding profile]ダイアログボックスが表示されます。

> 各プロファイルがどのルールでも使用されていない限り、複数のプロファイルを選択して同時に非アクティブにすることができます。

5. プロファイルを非活動化してもよい場合は、 [* 非活動化 * （ * Deactivate * ）] を選択します。

結果

- StorageGRIDがイレイジャーコーディングプロファイルを非アクティブ化できる場合、ステータスは[Deactivated]になります。これで、どの ILM ルールにもこのプロファイルを選択できなくなりました。非アクティブ化されたプロファイルを再アクティブ化することはできません。
- StorageGRID がプロファイルを非アクティブ化できない場合は、エラー・メッセージが表示されます。たとえば、オブジェクトデータがまだこのプロファイルに関連付けられている場合は、エラーメッセージが表示されます。無効化プロセスを再度実行する前に、数週間待つ必要がある場合があります。

StorageGRIDの S3 リージョンを構成する

ILM ルールでは、S3 バケットが作成されるオプションのリージョンに基づいてオブジェクトをフィルタリングできるため、異なるリージョンのオブジェクトを異なるストレージの場所に保存できます。

S3 バケットのリージョンをルールのフィルタとして使用する場合は、システム内のバケットで使用できるリージョンを最初に作成しておく必要があります。

> バケットの作成後にバケットのリージョンを変更することはできません。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- そうだな "特定のアクセス権限"

タスクの内容

S3 バケットを作成する際は、特定のリージョンにバケットを作成するように指定できます。リージョンを指定すると地理的にユーザにより近い場所にバケットを配置でき、レイテンシの最適化、コストの最小化、規制要件への対応を実現できます。

ILM ルールの作成時には、 S3 バケットに関連付けられているリージョンを高度なフィルタとして使用できます。たとえば、リージョンで作成されたS3バケット内のオブジェクトにのみ適用するルールを設計でき `us-west-2`ます。そのうえで、そのリージョン内のデータセンターサイトにあるストレージノードにオブジェクトのコピーを配置してレイテンシを最適化するように指定できます。

リージョンを設定する場合は、次の注意事項に従ってください。

- デフォルトでは、すべてのバケットがリージョンに属しているとみなされ `us-east-1`ます。
- テナント マネージャまたはテナント管理 API を使用してバケットを作成するとき、または S3 PUT バケット API リクエストの LocationConstraint リクエスト要素を使用してバケットを作成するときに、デフォルト以外のリージョンを指定するには、まずグリッド マネージャを使用してリージョンを作成する必要があります。 PUT Bucket リクエストがStorageGRIDで定義されていないリージョンを使用すると、エラーが発生します。

- S3 バケットの作成時には正確なリージョン名を使用する必要があります。リージョン名では大文字と小文字が区別されます。有効な文字は、数字、アルファベット、およびハイフンです。

  EU は eu-west-1 のエイリアスとはみなされません。 EU または eu-west-1 リージョンを使用する場合は、正確な名前を使用する必要があります。

- ポリシー（アクティブまたは非アクティブ）に割り当てられているルールで使用されているリージョンを削除または変更することはできません。
- 無効なリージョンをILMルールの高度なフィルタとして使用すると、そのルールをポリシーに追加できません。

  ILM ルールでリージョンを詳細フィルタとして使用したが、後でそのリージョンを削除した場合、またはグリッド管理 API を使用してルールを作成し、定義していないリージョンを指定した場合、無効なリージョンが発生する可能性があります。

- あるリージョンを使用して S3 バケットを作成したあとにそのリージョンを削除した場合、高度なフィルタ「 Location Constraint 」を使用してそのバケット内のオブジェクトを検索するにはリージョンを再び追加する必要があります。

手順

1. [* ILM*>* Regions*] を選択します。

   「リージョン」ページが表示されます。

2. *すべての地域*または*デフォルトの地域*タブを選択します。

すべての地域

すべてのリージョン タブには、定義されているデフォルトのリージョンを含む、現在定義されているリージョンが一覧表示されます。

> すべての地域*タブではデフォルトの地域を削除または変更することはできません。デフォルトの地域を変更するには、「*デフォルトの地域」タブを使用します。

a. 地域を追加するには、「別の地域を追加」を選択します。
b. S3 バケットの作成時に使用するリージョンの名前を入力します。

   対応する S3 バケットの作成時には、正確なリージョン名を LocationConstraint 要求の要素として使用する必要があります。

c. 使用されていない領域を削除するには、削除アイコン を選択します。

   いずれかのポリシー（アクティブまたは非アクティブ）で現在使用されているリージョンを削除しようとすると、エラーメッセージが表示されます。

d. 変更が完了したら、 * 保存 * を選択します。

   これで、Create ILM Ruleウィザードのステップ1の[Advanced filters]セクションでリージョンを選択できます。を参照して "ILM ルールで高度なフィルタを使用します"

デフォルトの地域

デフォルト リージョン タブには、現在定義されているデフォルト リージョンが表示されます。これは変更できます。

a. デフォルトのリージョンを変更するには、[デフォルトのリージョン] ドロップダウン リストで使用可能なオプションからリージョン名を選択します。
b. [保存（ Save ）] を選択します。

ILM ルールを作成する

StorageGRIDのILMルールについて学ぶ

オブジェクトを管理するには、一連の情報ライフサイクル管理（ ILM ）ルールを作成して 1 つの ILM ポリシーにまとめます。

システムに取り込まれたすべてのオブジェクトがアクティブポリシーに照らして評価されます。ポリシー内のルールがオブジェクトのメタデータに一致すると、ルールの説明によって、 StorageGRID がそのオブジェクトをコピーして格納するために実行するアクションが決まります。

> オブジェクトメタデータはILMルールで管理されません。代わりに、オブジェクトメタデータはメタデータストア内の Cassandra データベースに格納されます。データを損失から保護するために、オブジェクトメタデータの 3 つのコピーが各サイトで自動的に維持されます。

ILM ルールの要素

ILM ルールには次の 3 つの要素があります。

- * フィルタ条件 * ：ルールの基本フィルタと高度なフィルタにより、ルール環境 で使用するオブジェクトが定義されます。オブジェクトがすべてのフィルタに一致する場合、 StorageGRID はルールを適用し、ルールの配置手順で指定されたオブジェクトコピーを作成します。
- * 配置手順 * ：ルールの配置手順によって、オブジェクトコピーの数、タイプ、および場所が定義されます。各ルールに一連の配置手順を含めることで、時間の経過に伴うオブジェクトコピーの数、タイプ、場所を変更することができます。1 つの配置の期間が終了すると、次の配置手順が次の ILM 評価で自動的に適用されます。
- 取り込み動作：ルールの取り込み動作により、ルールでフィルタされたオブジェクトを取り込み時に保護する方法を選択できます（S3クライアントがオブジェクトをグリッドに保存する場合）。

ILMルールのフィルタリング

ILM ルールを作成する際には、フィルタを指定して環境 ルールを構成するオブジェクトを特定します。

最も単純なケースは、ルールでフィルタを使用しない場合です。環境 のすべてのオブジェクトでフィルタを使用しないルールがある場合は、 ILM ポリシーの最後の（デフォルト）ルールである必要があります。デフォルトルールでは、別のルールのフィルタに一致しないオブジェクトの格納手順が指定されます。

- 基本フィルタを使用すると、大規模なオブジェクトグループに異なるルールを適用できます。これらのフィルタを使用して、特定のテナントアカウント、特定のS3バケット、またはその両方にルールを適用できます。

  基本フィルタを使用すると、多数のオブジェクトに異なるルールを簡単に適用できます。たとえば、会社の財務記録は規制要件を満たすために保存し、マーケティング部門のデータは日々の業務を円滑に進めるために保存しなければならない場合があります。部門ごとに別々のテナントアカウントを作成するか、またはデータを部門ごとに別々の S3 バケットに分離したあとで、すべての財務記録を環境 で処理するルールを 1 つ作成し、環境 ですべてのマーケティングデータを処理するもう 1 つのルールを作成することができます。

- 高度なフィルタにより、きめ細かな制御が可能になります。次のオブジェクトプロパティに基づいてオブジェクトを選択するフィルタを作成できます。
  - 取り込み時間
  - 最終アクセス時間
  - オブジェクト名のすべてまたは一部（キー）
  - 場所の制約（S3のみ）
  - オブジェクトのサイズ
  - ユーザメタデータ
  - オブジェクトタグ（S3のみ）

非常に特定の条件でオブジェクトをフィルタリングできます。たとえば、病院の画像診断部門が保管するオブジェクトは、 30 日以内に頻繁に使用され、その後はあまり使用されない可能性があります。一方、患者の通院情報を格納するオブジェクトは、医療ネットワークの本部請求部門にコピーする必要があります。オブジェクト名、サイズ、 S3 オブジェクトタグ、またはその他の関連条件に基づいて各タイプのオブジェクトを識別するフィルタを作成してから、それぞれのオブジェクトセットを適切に格納するルールを別々に作成できます。

1つのルールで必要に応じてフィルタを組み合わせることができます。たとえば、マーケティング部門では、サイズの大きな画像ファイルをベンダーレコードとは異なる方法で格納しなければならない場合があります。一方、人事部門では、特定の地域の人事レコードとポリシー情報を一元的に格納する必要があります。この場合、テナントアカウントでフィルタリングするルールを作成して各部門からレコードを分離し、各ルールでフィルタを使用してルールが環境 する特定のタイプのオブジェクトを識別できます。

ILMルールの配置手順

配置手順は、オブジェクトデータを格納する場所、タイミング、および方法を決定します。ILM ルールには 1 つ以上の配置手順を含めることができます。各配置手順環境 は一定期間です。

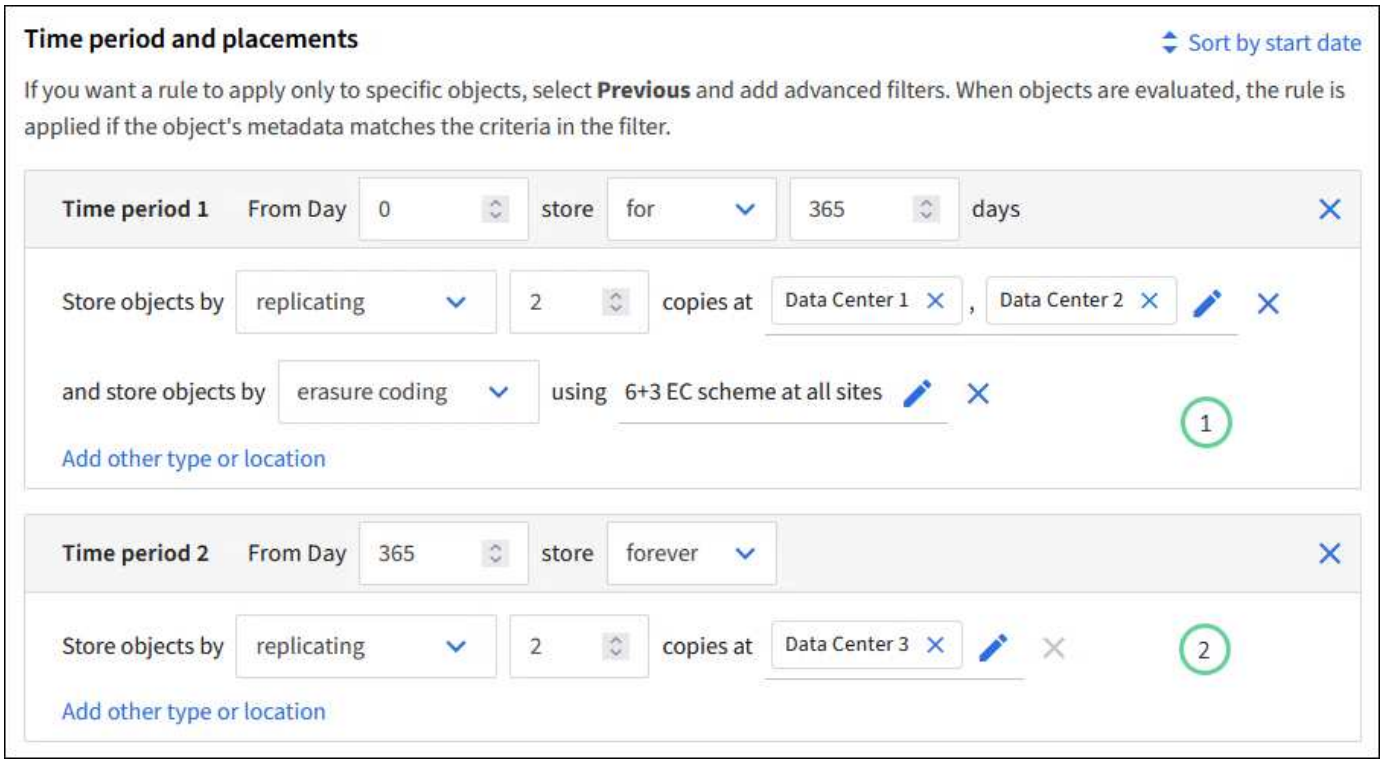
配置手順を作成する場合は、次の点に注意

- 最初に、配置手順を開始するタイミングを決定する参照時間を指定します。参照時間には、オブジェクトが取り込まれたとき、オブジェクトがアクセスされたとき、バージョン管理オブジェクトが noncurrent になったとき、またはユーザ定義の時間が含まれます。
- 次に、基準時間を基準にして配置を適用するタイミングを指定します。たとえば、配置は 0 日目から開始し、オブジェクトが取り込まれた時間から 365 日間継続する場合があります。
- 最後に、コピーのタイプ（レプリケーションまたはイレイジャーコーディング）とコピーの格納場所を指定します。たとえば、 2 つのレプリケートコピーを 2 つの異なるサイトに格納できます。

各ルールでは、 1 つの期間に複数の配置を定義し、期間ごとに異なる配置を定義できます。

- 1つの期間に複数の場所にオブジェクトを配置するには、*他のタイプまたは場所を追加*を選択して、その期間に複数の行を追加します。
- 異なる期間の異なる場所にオブジェクトを配置するには、*別の期間を追加*を選択して次の期間を追加します。次に、期間内に 1 行以上の行を指定します。

この例では、Create ILM Ruleウィザードの[Define placements]ページに表示される2つの配置手順を示しています。



最初の配置指示(1)には、最初の1年間に2つの行があります。

- 1 行目では、 2 つのデータセンターサイトに 2 つのレプリケートオブジェクトコピーが作成されます。
- 2行目は、すべてのデータセンターサイトを使用して6+3のイレイジャーコーディングコピーを作成します。

2番目の配置指示(2)は、1年後に2部のコピーを作成し、それらのコピーを永久に保管します。

ルールに一連の配置手順を定義する場合は、少なくとも 1 つの配置手順が 0 日目に開始し、定義した期間の間にギャップがないことを確認する必要があります。 そして、最終的な配置手順は無期限またはオブジェクトコピーが不要になるまで継続されます。

ルールの各期間が終了すると、次の期間のコンテンツ配置手順が適用されます。新しいオブジェクトコピーが作成され、不要なコピーは削除されます。

ILMルールの取り込み動作

取り込み動作は、ルールの手順に従ってオブジェクトコピーがすぐに配置されるか、または中間コピーが作成されて配置手順があとから適用されるかを制御します。ILM ルールでは、次の取り込み動作を使用できます。

- * Balanced * ： StorageGRID は、取り込み時に ILM ルールで指定されたすべてのコピーを作成しようとします。作成できない場合、中間コピーが作成されてクライアントに成功が返されます。可能な場合は、ILM ルールで指定されたコピーが作成されます。
- * Strict * ： ILM ルールに指定されたすべてのコピーを作成しないと、クライアントに成功が返されません。
- * Dual commit *：StorageGRID はオブジェクトの中間コピーをただちに作成し、クライアントに成功を返します。可能な場合は、 ILM ルールで指定されたコピーが作成されます。

関連情報

- "取り込みオプション"
- "取り込みオプションのメリット、デメリット、および制限事項"
- "整合性とILMルールの相互作用によるデータ保護への影響"

ILM ルールの例

たとえば、ILMルールでは次のように指定できます。

- テナントAに属するオブジェクトにのみ適用されます
- それらのオブジェクトのレプリケートコピーを2つ作成し、各コピーを別 々 のサイトに格納します。
- 2つのコピーは「無期限」で保持されます。つまり、StorageGRIDでは自動的に削除されません。これらのオブジェクトは、クライアントの削除要求によって削除されるか、バケットライフサイクルが終了するまで、 StorageGRID によって保持されます。
- 取り込み動作には[Balanced]オプションを使用します。テナントAがオブジェクトをStorageGRID に保存するとすぐに2サイトの配置手順が適用されます。ただし、必要な両方のコピーをすぐに作成できない場合は除きます。

  たとえば、テナント A がオブジェクトを保存したときにサイト 2 に到達できない場合、 StorageGRID はサイト 1 のストレージノードに 2 つの中間コピーを作成します。サイト 2 が使用可能になると、 StorageGRID はそのサイトで必要なコピーを作成します。

関連情報

- "ストレージプールとは"
- "クラウドストレージプールとは"

StorageGRIDでILMルールの作成ウィザードにアクセスする

ILM ルールを使用して、時間の経過に伴うオブジェクトデータの配置を管理できます。ILMルールを作成するには、Create an ILM ruleウィザードを使用します。

> ポリシーのデフォルトのILMルールを作成する場合は、代わりにの手順を実行し"デフォルトのILMルールの作成手順"ます。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- そうだな "特定のアクセス権限"
- このルールを適用するテナントアカウントを指定する場合は、または各アカウントのアカウントIDが必要"テナントアカウントの権限"です。
- 最終アクセス時間のメタデータでオブジェクトをフィルタリングするようにルールを設定する場合は、S3バケットで最終アクセス時間の更新を有効にする必要があります。
- 使用するクラウドストレージプールを設定しておきます。を参照して "クラウドストレージプールを作成"
- に精通している"取り込みオプション"必要があります。
- S3オブジェクトロックで使用する準拠ルールを作成する必要がある場合は、を"S3 オブジェクトのロックの要件"参照してください。

- オプションとして、ビデオを視聴しました:

  ILMルールの概要

タスクの内容

ILM ルールを作成する場合は、次の点

- StorageGRID システムのトポロジとストレージ構成を考慮します。
- 作成するオブジェクトコピーのタイプ（レプリケートまたはイレイジャーコーディング）と、各オブジェクトに必要なコピー数を検討します。
- StorageGRID システムに接続するアプリケーションで使用されるオブジェクトメタデータのタイプを決定します。ILM ルールは、メタデータに基づいてオブジェクトをフィルタリングします。
- 時間の経過に伴うオブジェクトコピーの配置先を検討します。
- 使用する取り込みオプション（Balanced、Strict、Dual commit）を決定します。

手順

1. [* ILM*>* Rules] を選択します。
2. 「 * Create * 」を選択します。"手順1（詳細を入力）"のCreate an ILM ruleウィザードが表示されます。

StorageGRID ILM ルールの詳細とフィルターを入力してください

[ILMルールの作成]ウィザードの*[詳細を入力]*ステップでは、ルールの名前と概要 を入力し、ルールのフィルタを定義できます。

概要 の入力とルールのフィルタの定義はオプションです。

タスクの内容

オブジェクトをに対して評価すると"ILMルール"、StorageGRIDはオブジェクトメタデータをルールのフィルタと比較します。オブジェクトメタデータがすべてのフィルタに一致した場合、 StorageGRID はルールを使用してオブジェクトを配置します。すべてのオブジェクトに適用するルールを設計したり、 1 つ以上のテナントアカウントやバケット名などの基本的なフィルタや、オブジェクトのサイズやユーザメタデータなどの高度なフィルタを指定したりできます。

手順

1. [* 名前 *] フィールドに、ルールの一意の名前を入力します。
2. 必要に応じて、ルールの短い概要 を * 概要 * フィールドに入力します。

   あとから識別しやすいように、ルールの目的や機能を指定してください。

3. 必要に応じて、このルールを適用するS3テナントアカウントを1つ以上選択します。このルールですべてのテナントを環境 に設定する場合は、このフィールドを空白のままにします。

   Root Access権限またはTenant accounts権限がない場合は、リストからテナントを選択できません。代わりに、テナント ID を入力するか、複数の ID をカンマで区切って入力します。

4. 必要に応じて、このルールを適用するS3バケットを指定します。

[すべてのバケットに適用]*が選択されている場合（デフォルト）、ルールはすべてのS3バケットに適用されます。

5. S3テナントの場合は、必要に応じて*[Yes]*を選択して、バージョン管理が有効になっているS3バケット内の古いオブジェクトバージョンにのみルールを適用します。

   ◦ Yes *を選択すると、の参照時間に「noncurrent time」が自動的に選択されます。"ILMルール作成ウィザードのステップ2"

   [Noncurrent time]は、バージョン管理が有効なバケット内のS3オブジェクトにのみ適用されます。およびを参照してください"バケットの処理、PutBucketVersioning""S3 オブジェクトロックでオブジェクトを管理します"。

   このオプションを使用すると、最新でないオブジェクトバージョンをフィルタリングすることで、バージョン管理オブジェクトによるストレージへの影響を軽減できます。を参照して "例 4 ： S3 バージョン管理オブジェクトの ILM ルールとポリシー"

6. 必要に応じて、*[高度なフィルタを追加する]*を選択して、追加のフィルタを指定します。

   高度なフィルタを設定しない場合は、基本フィルタに一致するすべてのオブジェクトを環境 というルールが適用されます。高度なフィルタリングの詳細については、およびを参照してくださいILM ルールで高度なフィルタを使用します[複数のメタデータタイプと値を指定します]。

7. 「 * Continue * 」を選択します。"ステップ2（配置の定義）"のCreate an ILM ruleウィザードが表示されます。

ILM ルールで高度なフィルタを使用します

高度なフィルタを使用すると、メタデータに基づいて特定のオブジェクトにのみ適用する ILM ルールを作成できます。ルールに対して高度なフィルタを設定するには、照合するメタデータのタイプを選択し、演算子を選択して、メタデータ値を指定します。オブジェクトが評価されると、高度なフィルタに一致するメタデータを含むオブジェクトにのみ ILM ルールが適用されます。

次の表に、高度なフィルタで指定できるメタデータタイプ、各タイプのメタデータに使用できる演算子、および想定されるメタデータ値を示します。

メタデータタイプ	サポートされる演算子	メタデータ値
取り込み時間	• は • ではない • 以前のものです • 以前のものです • 後である • がオンまたは後になっています	オブジェクトが取り込まれた日時。 *注：*新しいILMポリシーをアクティブ化する際のリソースの問題を回避するために、大量の既存オブジェクトの場所を変更する可能性があるルールでは、高度なフィルタとして取り込み時間を使用できます。新しいポリシーが有効になるおおよその時間以上に取り込み時間を設定して、既存のオブジェクトが不要に移動されないようにします。

メタデータタイプ	サポートされる演算子	メタデータ値
キー	• が等しい • 等しくない • 次を含む • 次を含まない • 次の値で始まる • で始まるものではありません • 次の値で終わる • で終わることはありません	一意のS3オブジェクトキーのすべてまたは一部。 たとえば、で終わるオブジェクトやで始まる `test-object/`オブジェクトを照合でき `.txt`ます。
最終アクセス時間	• は • ではない • 以前のものです • 以前のものです • 後である • がオンまたは後になっています	オブジェクトが最後に読み出された（読み取られた、または表示された）日時。 *注：*高度なフィルタとしてを使用する場合は"最終アクセス時間を使用"、S3バケットで最終アクセス時間の更新を有効にする必要があります。
場所の制約（S3のみ）	• が等しい • 等しくない	S3 バケットが作成されたリージョン。表示されるリージョンを定義するには、 * ilm * > * Regions * を使用します。 注: us-east-1 の値は、us-east-1 リージョンで作成されたバケット内のオブジェクトと、リージョンが指定されていないバケット内のオブジェクトに一致します。見る"S3リージョンを設定する" 。
オブジェクトのサイズ	• が等しい • 等しくない • より小さい • 以下 • が次の値より大きい • 以上	オブジェクトのサイズ。 イレイジャーコーディングは 1MB を超えるオブジェクトに適しています。非常に小さいイレイジャーコーディングフラグメントを管理するオーバーヘッドを回避するために、200KB未満のオブジェクトにはイレイジャーコーディングを使用しないでください。

メタデータタイプ	サポートされる演算子	メタデータ値
ユーザメタデータ	• 次を含む • 次の値で終わる • が等しい • が存在します • 次の値で始まる • 次を含まない • で終わることはありません • 等しくない • は存在しません • で始まるものではありません	キーと値のペア。* User metadata name はキー、Metadata Value *は値です。 たとえば、ユーザメタデータがであるオブジェクトでフィルタするには、*ユーザメタデータ `color=blue`名*に `equals`、演算子に、 `blue`* メタデータ値*にを指定します `color`。 *注：*ユーザーメタデータ名では大文字と小文字は区別されません。ユーザーメタデータ値では大文字と小文字が区別されます。
オブジェクトタグ（S3のみ）	• 次を含む • 次の値で終わる • が等しい • が存在します • 次の値で始まる • 次を含まない • で終わることはありません • 等しくない • は存在しません • で始まるものではありません	キーと値のペア。* Object tag name はキー、 Object tag value *は値です。 たとえば、オブジェクトタグがであるオブジェクトでフィルタリングするには `Image=True`、* Object tag name に、演算子に、 **`True`** Object tag value *に `equals`を指定します `Image`。 • 注：* オブジェクトタグ名とオブジェクトタグ値では、大文字と小文字が区別されます。これらの項目は、オブジェクトに対して定義されたとおりに正確に入力する必要があります。

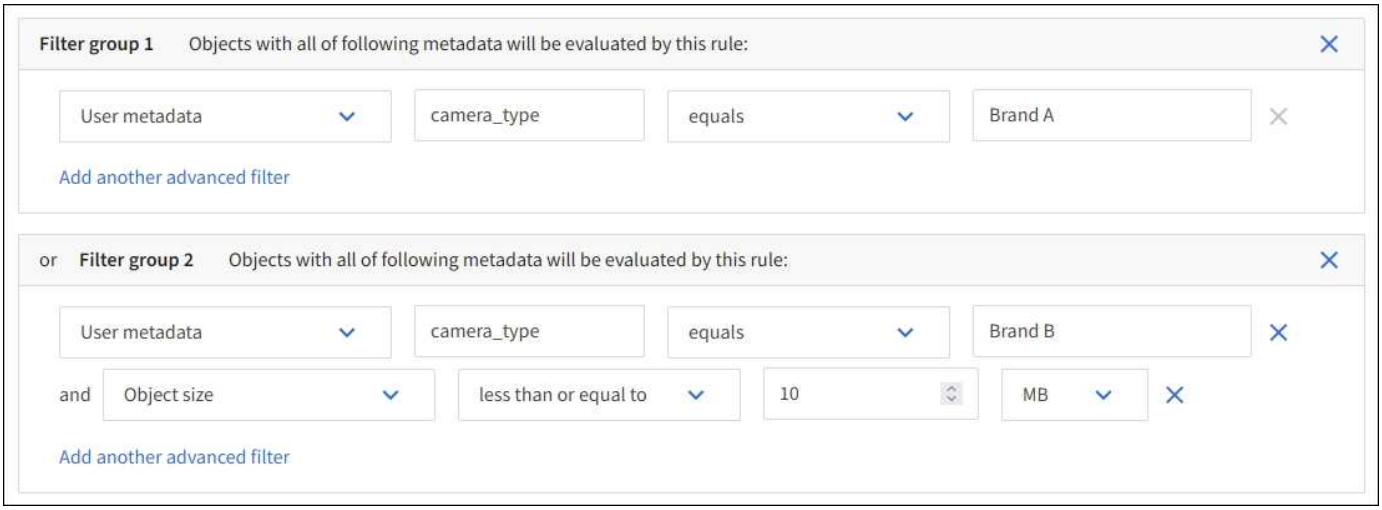
複数のメタデータタイプと値を指定します

高度なフィルタを定義する場合は、複数のタイプのメタデータと複数のメタデータ値を指定できます。たとえば、サイズが10~100MBのオブジェクトに一致するルールを設定する場合は、メタデータタイプ*[オブジェクトサイズ]*を選択し、2つのメタデータ値を指定します。

- 最初のメタデータ値で 10MB 以上のオブジェクトを指定します。
- 2 番目のメタデータ値で 100MB 以下のオブジェクトを指定します。



複数のエントリを使用すると、照合するオブジェクトを正確に制御できます。次の例では、camera_typeユーザメタデータの値がブランドAまたはブランドBであるルール環境オブジェクトを指定しています。ただし、ルールでは、 10MB より小さい Brand B のオブジェクトのみが環境 されます。



StorageGRID ILM ルールの配置指示を定義する

Create ILM Ruleウィザードの* Define placements *ステップでは、オブジェクトを格納する期間、コピーのタイプ（レプリケートまたはイレイジャーコーディング）、格納場所、およびコピー数を決定する配置手順を定義できます。

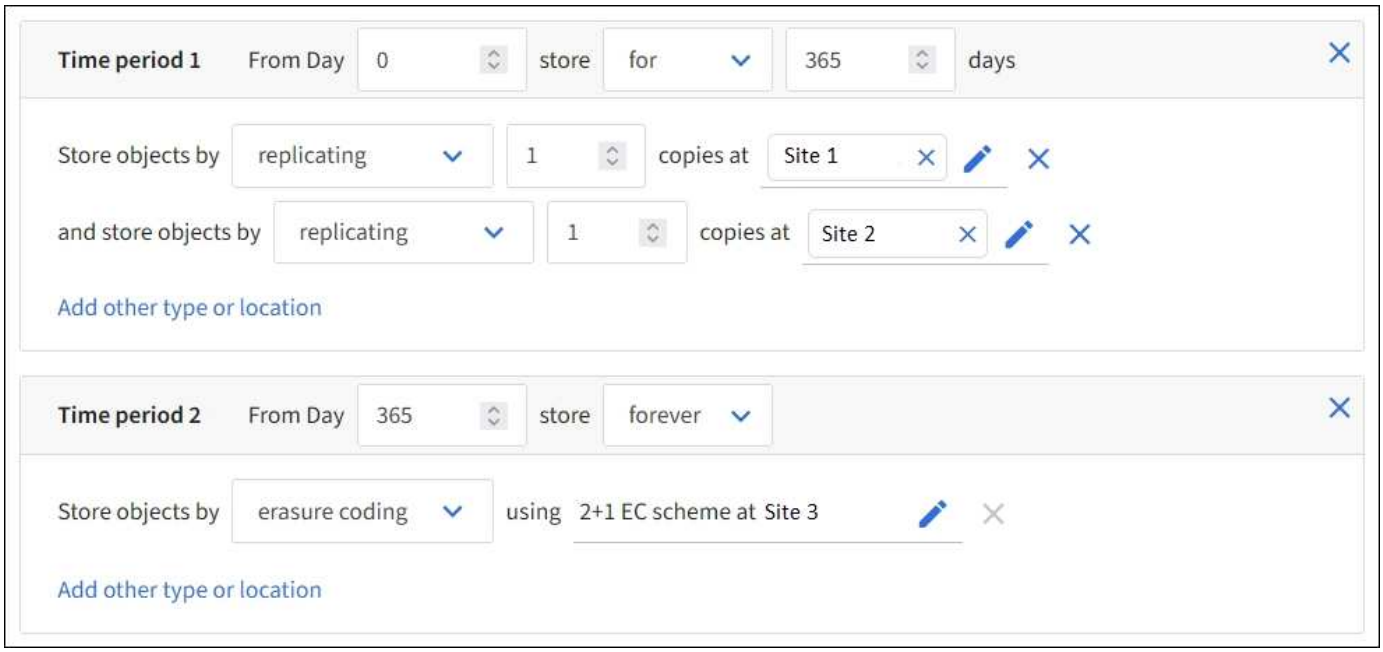
ここに示されているスクリーンショットは一例です。StorageGRIDのバージョンによっては、結果が異なる場合があります。

タスクの内容

ILM ルールには 1 つ以上の配置手順を含めることができます。各配置手順環境 は一定期間です。複数の手順を使用する場合は、期間が連続していて、少なくとも 1 つの手順が 0 日目に開始されている必要があります。手順は無期限に、またはオブジェクトコピーが不要になるまで継続できます。

複数のタイプのコピーを作成する場合や、期間中に別々の場所を使用する場合は、各配置手順に複数の行を追加することができます。

この例では、ILMルールはサイト1にレプリケートコピーを1つ、サイト2にレプリケートコピーを1つ、最初の1年間格納します。1 年後、 2+1 のイレイジャーコーディングコピーが作成され、 1 つのサイトにのみ保存されます。



手順

1. [Reference time]*で、配置手順の開始時間の計算に使用する時間のタイプを選択します。

オプション	製品説明
取り込み時間	オブジェクトが取り込まれた時間。
最終アクセス時間	オブジェクトが最後に読み出された（読み取られた、または表示された）時間。 このオプションを使用するには、S3バケットに対して最終アクセス時間の更新を有効にする必要があります。を参照してください "ILMルールで最終アクセス時間を使用"。
ユーザ定義の作成時間	ユーザ定義のメタデータで指定された時間。
最新でない時間	の質問「Apply this rule to older object versions only（S3バケットでバージョン管理が有効になっている場合）？」で* Yes *を選択すると、「noncurrent time」が自動的に選択されます"ILMルール作成ウィザードのステップ1"。

_compliant_ruleを作成する場合は、*取り込み時間*を選択する必要があります。を参照してください "S3オブジェクトロックでオブジェクトを管理します"。

2. [Time period and placements *]セクションで、最初の期間の開始時刻と期間を入力します。

たとえば、最初の年にオブジェクトを格納する場所（_ from day 0 store for 365 days_）を指定できます。少なくとも 1 つの手順は 0 日目から開始する必要があります。

3. レプリケートコピーを作成する場合は、次の手順を実行します。
   a. ドロップダウンリストで、[Replicating]*を選択します。

b. 作成するコピーの数を選択します。

コピー数を 1 に変更すると、警告が表示されます。ある期間にレプリケートコピーを 1 つしか作成しない ILM ルールには、データが永続的に失われるリスクがあります。を参照してください "シングルコピーレプリケーションを使用しない理由"。

このリスクを回避するには、次のいずれかまたは複数の操作を実行します。

- 期間のコピー数を増やします。
- 他のストレージプールまたはクラウドストレージプールにコピーを追加します。
- ではなく、[イレイジャーコーディング]*を選択します。

このルールですべての期間に対して複数のコピーを作成するようすでに定義されている場合は、この警告を無視してかまいません。

c. [コピー数]*フィールドで、追加するストレージプールを選択します。

- ストレージプールを 1 つしか指定しない場合、 StorageGRID は 1 つのオブジェクトのレプリケートコピーを任意のストレージノードに 1 つだけ格納できます。3つのストレージノードがあるグリッドでコピー数として4を選択した場合、ストレージノードごとに1つのコピーが作成されるのは3つだけです。

ILM placement unAchievable * アラートがトリガーされ、 ILM ルールを完全に適用できなかったことを示します。

- 複数のストレージプールを指定する場合は、次の点に注意してください。 *
  - コピーの数をストレージプールの数よりも多くすることはできません。
  - コピーの数がストレージプールの数と同じ場合は、オブジェクトのコピーが 1 つずつ各ストレージプールに格納されます。
  - コピーの数がストレージプールの数より少ない場合は、取り込みサイトに1つのコピーが格納され、残りのコピーがプール間のディスク使用量のバランスを維持するために分散されます。同時に、どのサイトもオブジェクトのコピーを複数取得できないようにします。
  - ストレージプールが重複している（同じストレージノードを含んでいる）場合は、オブジェクトのすべてのコピーが 1 つのサイトにのみ保存される可能性があります。そのため、All Storage Nodesストレージプール（StorageGRID 11.6以前）と別のストレージプールを指定しないでください。

4. イレイジャーコーディングコピーを作成する場合は、次の手順を実行します。

a. [Store objects by *]ドロップダウンリストで、*イレイジャーコーディング*を選択します。

> イレイジャーコーディングは 1MB を超えるオブジェクトに適しています。非常に小さいイレイジャーコーディングフラグメントを管理するオーバーヘッドを回避するために、200KB未満のオブジェクトにはイレイジャーコーディングを使用しないでください。

b. 200KBを超える値に対してオブジェクトサイズフィルタを追加しなかった場合は、* Previous を選択して手順**1**に戻ります。次に、[高度なフィルタを追加する]を選択し、[オブジェクトサイズ]*フィルタを200KBを超える任意の値に設定します。

c. 追加するストレージプールと使用するイレイジャーコーディングスキームを選択します。

イレイジャーコーディングコピーの格納場所は、イレイジャーコーディングスキームの名前とストレージプールの名前で構成されます。

使用可能なイレイジャーコーディングスキームは、選択したストレージプール内のストレージノードの数によって制限されます。いずれかのを提供するスキームの横にバッジが `Recommended`表示され"最適な保護または最小限のストレージオーバーヘッド"ます。

5. オプション：
   a. 別の場所に追加のコピーを作成するには、*[その他のタイプまたは場所を追加]*を選択します。
   b. 別の期間を追加するには、*[別の期間を追加]*を選択します。

> オブジェクトの削除は次の設定に基づいて実行されます。
>
> - 別の期間が「* forever *」で終わる場合を除き、最後の期間の終了時にオブジェクトが自動的に削除されます。
> - によっては"バケットとテナントの保持期間の設定"、ILMの保持期間が終了してもオブジェクトが削除されない場合があります。

6. オブジェクトをクラウドストレージプールに格納する場合は、次の手順を実行します。
   a. [Store objects by]ドロップダウンリストで、[Replicating *]を選択します。
   b. [Copies at]*フィールドを選択し、クラウドストレージプールを選択します。

      クラウドストレージプールを使用する場合は、次の点に注意してください。

      - 1つの配置手順で複数のクラウドストレージプールを選択することはできません。同様に、クラウドストレージプールとストレージプールを同じ配置手順で選択することはできません。
      - 任意のクラウドストレージプールに格納できるオブジェクトのコピーは 1 つだけです。「 * Copies * 」を 2 以上に設定すると、エラーメッセージが表示されます。
      - どのクラウドストレージプールにも、複数のオブジェクトコピーを同時に格納することはできません。クラウドストレージプールを使用する複数の配置で日付が重複している場合や、同じ配置内の複数の行でクラウドストレージプールを使用している場合は、エラーメッセージが表示されます。
      - オブジェクトがStorageGRIDにレプリケートコピーまたはイレイジャーコーディングコピーとして格納されているときに、そのオブジェクトをクラウドストレージプールに格納できます。ただし、各場所のコピーの数とタイプを指定できるように、その期間の配置手順に複数の行を含める必要があります。

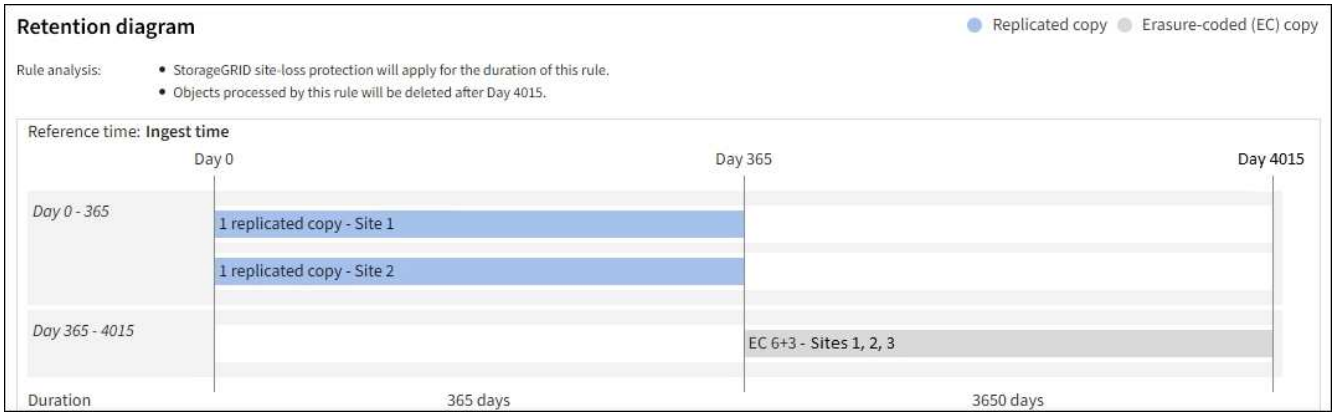
7. [Retention]図で、配置手順を確認します。

   この例では、ILMルールはサイト1にレプリケートコピーを1つ、サイト2にレプリケートコピーを1つ、最初の1年間格納します。1年後にさらに10年間、6+3のイレイジャーコーディングコピーが3つのサイトに保存されます。合計11年が経過すると、オブジェクトはStorageGRID から削除されます。

   保持図の規則解析セクションには'次のような情報が表示されます

   - このルールの期間中は、StorageGRID サイト障害からの保護が適用されます。
   - このルールで処理されるオブジェクトは、4015日目以降に削除されます。

を参照して "サイト障害からの保護を有効にします。"



8. 「 * Continue * 」を選択します。"ステップ3（取り込み動作を選択）"のCreate an ILM ruleウィザードが表示されます。

StorageGRID ILM ルールで最終アクセス時間を使用する

最終アクセス時間をILMルールの参照時間として使用できます。たとえば、過去 3 カ月間に表示されたオブジェクトをローカルストレージノードに残しておき、最近表示されていないオブジェクトをオフサイトの場所に移動することができます。特定の日付に最後にアクセスされたオブジェクトにのみILMルールを適用する場合は、最終アクセス時間を高度なフィルタとして使用することもできます。

タスクの内容

ILMルールで最終アクセス時間を使用する前に、次の考慮事項を確認してください。

- 参照時間として最終アクセス時間を使用する場合は、オブジェクトの最終アクセス時間を変更してもILM評価はすぐにはトリガーされないことに注意してください。オブジェクトの配置が評価され、バックグラウンド ILM がオブジェクトを評価したときに必要に応じてオブジェクトが移動されます。この処理には、オブジェクトがアクセスされてから 2 週間以上かかる場合があります。

  最終アクセス時間に基づいてILMルールを作成する場合は、このレイテンシを考慮し、短期間（1カ月未満）を使用する配置は避けてください。

- 高度なフィルタまたは参照時間として最終アクセス時間を使用する場合は、S3バケットに対して最終アクセス時間の更新を有効にする必要があります。またはを使用できます"テナントマネージャ""テナント管理API"。

  最終アクセス時間の更新は、S3バケットに対してはデフォルトで無効になっています。

  最終アクセス時間の更新を有効にすると、特に小さなオブジェクトを含むシステムのパフォーマンスが低下する可能性があります。これは、オブジェクトが読み出されるたびに StorageGRID が新しいタイムスタンプでオブジェクトを更新する必要があるためです。

次の表に、バケット内のすべてのオブジェクトについて、最終アクセス時間が更新されるかどうかを要求のタイプ別にまとめます。

要求のタイプ	最終アクセス時間の更新が無効になっている場合に最終アクセス時間を更新するかどうか	最終アクセス時間の更新が有効になっている場合に最終アクセス時間を更新するかどうか
オブジェクト、そのアクセス制御リスト、またはメタデータの読み出し要求	いいえ	はい
オブジェクトメタデータの更新要求	はい	はい
バケット間でのオブジェクトのコピー要求	• ソースコピーに対しては、「いいえ」と指定します • デスティネーションコピーについては、はい	• ソースコピーについては、はい • デスティネーションコピーについては、はい
マルチパートアップロードの完了要求	はい、アセンブルされたオブジェクトの場合	はい、アセンブルされたオブジェクトの場合

StorageGRID ILM ルールの取り込み動作を選択します

Create ILM Ruleウィザードの* Select ingest behavior *ステップでは、このルールでフィルタされたオブジェクトを取り込み時に保護する方法を選択できます。

タスクの内容

StorageGRID は、中間コピーを作成してオブジェクトをキューに登録し、あとで ILM 評価を実行するか、またはコピーを作成してルールの配置手順をすぐに満たすことができます。

手順

1. 使用するを選択し"取り込み動作"ます。

   詳細については、を参照してください "取り込みオプションのメリット、デメリット、および制限事項"。

   ルールで次のいずれかの配置が使用されている場合は、BalancedオプションまたはStrictオプションは使用できません。

   - クラウドストレージプール： 0 日目
   - ルールがユーザ定義の作成時間を参照時間として使用している場合のクラウドストレージプール

   を参照して "例 5 ：取り込み動作が Strict の場合の ILM ルールとポリシー"

2. 「 * Create * 」を選択します。

   ILMルールが作成されます。ルールは、に追加されてポリシーがアクティブ化されるまでアクティブになりません"ILMポリシー"。

   ルールの詳細を表示するには、[ILM rules]ページでルールの名前を選択します。

StorageGRIDでデフォルトのILMルールを作成する

ILM ポリシーを作成する前に、デフォルトルールを作成して、ポリシー内の別のルールに一致しないオブジェクトを配置する必要があります。デフォルトのルールではフィルタを使用できません。すべてのテナント、すべてのバケット、およびすべてのオブジェクトバージョンに適用する必要があります。

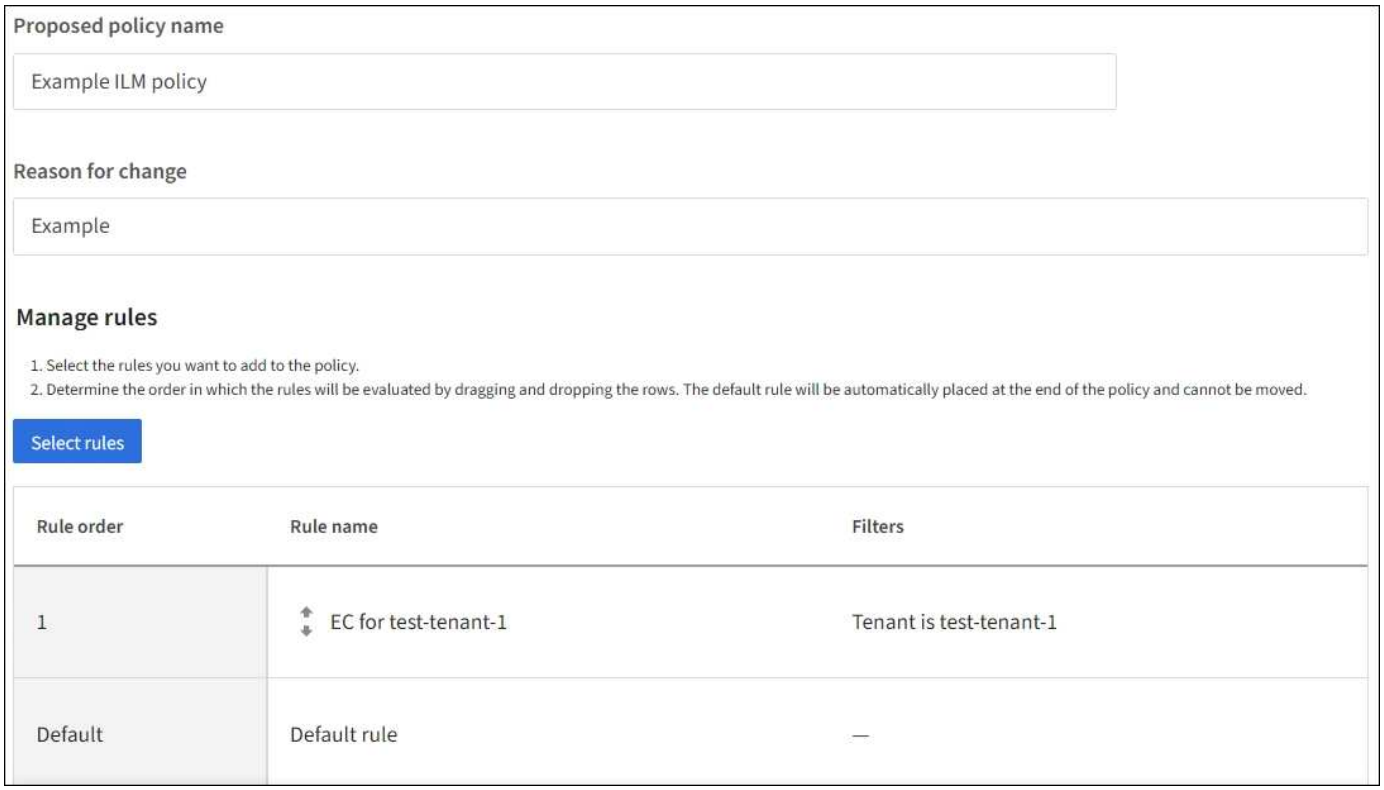
開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- そうだな "特定のアクセス権限"

タスクの内容

デフォルトルールはILMポリシーで最後に評価されるルールであるため、フィルタは使用できません。デフォルトルールの配置手順は、ポリシー内の別のルールに一致しないオブジェクトに適用されます。

このポリシーの例では、最初のルールがtest-tenant-1に属するオブジェクトにのみ適用されます。デフォルトルールである最後のルールは、他のすべてのテナントアカウントに属する環境 オブジェクトです。



デフォルトルールを作成するときは、次の要件に注意してください。

- デフォルトルールは、ポリシーに追加すると最後のルールとして自動的に配置されます。
- デフォルトのルールでは、基本フィルタまたは拡張フィルタは使用できません。
- デフォルトルールはすべてのオブジェクトバージョンに適用する必要があります。
- デフォルトのルールでレプリケートコピーを作成する必要があります。

イレイジャーコーディングコピーを作成するルールをポリシーのデフォルトルールとして使用しないでください。イレイジャーコーディングルールでは、高度なフィルタを使用して、小さいオブジェクトがイレイジャーコーディングされないようにする必要があります。

- 一般に、デフォルトルールではオブジェクトを無期限に保持する必要があります。
- S3オブジェクトロックのグローバル設定を使用している（または有効にする）場合は、デフォルトルールが準拠している必要があります。

手順

1. [* ILM*>* Rules] を選択します。
2. 「 * Create * 」を選択します。

   Create ILM RuleウィザードのStep 1（Enter details）が表示されます。

3. [ルール名]*フィールドにルールの一意の名前を入力します。
4. 必要に応じて、ルールの短い概要 を * 概要 * フィールドに入力します。
5. [Tenant accounts]*フィールドは空白のままにします。

   デフォルトのルールをすべてのテナントアカウントに適用する必要があります。

6. [Bucket name]ドロップダウンでは、[*環境all buckets]*のままにします。

   デフォルトルールはすべてのS3バケットに適用する必要があります。

7. 「このルールを古いオブジェクトバージョンのみに適用する（バージョン管理が有効なS3バケット内）？」という質問は、デフォルトの回答* No *のままにします。
8. 高度なフィルタは追加しないでください。

   デフォルトのルールではフィルタを指定できません。

9. 「 * 次へ * 」を選択します。

   [Step 2（Define placements）]が表示されます。

10. 参照時間（Reference time）で任意のオプションを選択します。

    「このルールは古いオブジェクトバージョンのみに適用しますか？」という質問のデフォルトの回答をそのまま使用している場合は、[Noncurrent Time]はプルダウンリストに含まれません。デフォルトのルールは、すべてのオブジェクトバージョンを適用する必要があります。

11. デフォルトルールの配置手順を指定します。
    - デフォルトルールではオブジェクトを無期限に保持する必要があります。デフォルトルールによってオブジェクトが無期限に保持されない場合、新しいポリシーをアクティブ化すると警告が表示されます。これが想定どおりの動作であることを確認する必要があります。
    - デフォルトのルールでレプリケートコピーを作成する必要があります。

イレイジャーコーディングコピーを作成するルールをポリシーのデフォルトルールとして使用しないでください。イレイジャーコーディングルールでは、小さいオブジェクトがイレイジャーコーディングされないように、「* Object size（MB）greater 200KB *」という高度なフィルタを指定する必要があります。

- S3 オブジェクトのグローバルロック設定を使用している（または有効にする）場合は、デフォルトルールが準拠している必要があります。
  - 2 つ以上のレプリケートオブジェクトコピーまたは 1 つのイレイジャーコーディングコピーを作成する。
  - これらのコピーが、配置手順の各ラインの間、ストレージノード上に存在している必要があります。
  - オブジェクトコピーをクラウドストレージプールに保存することはできません。
  - 配置手順の少なくとも1行は、取り込み時間を参照時間として使用し、0日目から開始する必要があります。
  - 配置手順の少なくとも1行は「forever」にする必要があります。

12. [Retention]の図を参照して配置手順を確認します。
13. 「 * Continue * 」を選択します。

    手順3（取り込み動作を選択）が表示されます。

14. 使用する取り込みオプションを選択し、*[作成]*を選択します。

ILMポリシーを管理します。

StorageGRIDのILMポリシーについて学ぶ

情報ライフサイクル管理（ ILM ）ポリシーは、優先順位が付けられた一連の ILM ルールです。 StorageGRID システムが時間の経過に伴ってオブジェクトデータを管理する方法を決定します。

ILM ポリシーが正しく設定されていないと、リカバリできないデータ損失が発生する可能性があります。ILM ポリシーをアクティブ化する前に、 ILM ポリシーおよびその ILM ルールを慎重に確認し、次に ILM ポリシーをシミュレートします。ILM ポリシーが意図したとおりに機能することを必ず確認してください。

デフォルトのILMポリシー

StorageGRIDをインストールしてサイトを追加すると、次のようにデフォルトのILMポリシーが自動的に作成されます。

- グリッドにサイトが1つある場合、デフォルトのポリシーには、そのサイトの各オブジェクトのコピーを2つレプリケートするデフォルトルールが含まれています。
- グリッドに複数のサイトが含まれている場合、デフォルトルールは各サイトに各オブジェクトのコピーを1つレプリケートします。

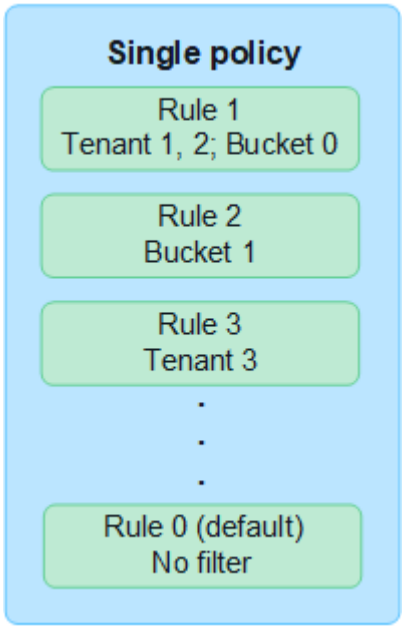
デフォルトのポリシーがストレージ要件を満たしていない場合は、独自のルールとポリシーを作成できます。見る"ILMルールを作成する"そして"ILMポリシーを作成します"。

1つまたは複数のアクティブなILMポリシー

一度に1つ以上のアクティブなILMポリシーを含めることができます。

1つのポリシー

グリッドでシンプルなデータ保護方式を使用し、テナント固有およびバケット固有のルールをいくつか設定する場合は、1つのアクティブなILMポリシーを使用します。ILMルールにフィルタを含めることで、さまざまなバケットやテナントを管理できます。



ポリシーが1つしかなく、テナントの要件が変更された場合は、新しいILMポリシーを作成するか、既存のポリシーのクローンを作成して変更を適用し、シミュレートしてから新しいILMポリシーをアクティブ化する必要があります。ILMポリシーを変更すると、オブジェクトの移動に何日もかかることがあり、原因システムのレイテンシも発生する可能性があります。

複数のポリシー

テナントに異なるQoSオプションを提供するために、一度に複数のアクティブポリシーを設定できます。各ポリシーでは、特定のテナント、S3バケット、オブジェクトを管理できます。特定のテナントまたはオブジェクトセットに対して1つのポリシーを適用または変更しても、他のテナントやオブジェクトに適用されているポリシーは影響を受けません。

ILMポリシータグ

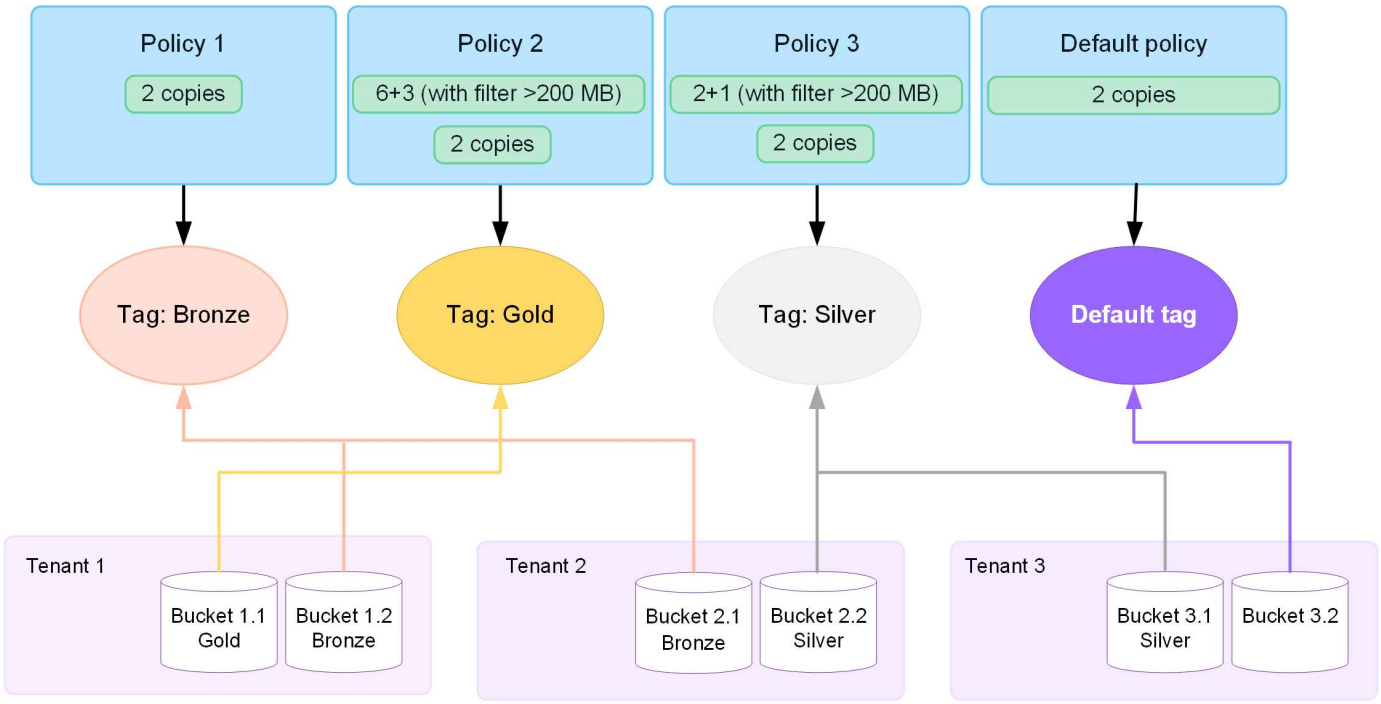
テナントで複数のデータ保護ポリシーをバケット単位で簡単に切り替えられるようにするには、_ILMポリシータグ_を指定して複数のILMポリシーを使用します。各ILMポリシーをタグに割り当て、テナントがバケットにタグを付けてそのバケットにポリシーを適用します。ILMポリシータグはS3バケットにのみ設定できます。

たとえば、Gold、Silver、Bronzeという3つのタグがあるとします。オブジェクトを格納する期間と場所に基づいて、各タグにILMポリシーを割り当てることができます。テナントでは、バケットにタグを付けることで、使用するポリシーを選択できます。Goldタグが付けられたバケットはGoldポリシーで管理され、Goldレベルのデータ保護とパフォーマンスを受け取ります。

あなたはできる"最大10個のポリシータグを作成する"グリッド用です。

デフォルトの**ILM**ポリシータグ

デフォルトのILMポリシータグは、StorageGRIDのインストール時に自動的に作成されます。各グリッドには、デフォルトタグに割り当てられたアクティブポリシーが1つ必要です。デフォルトポリシーは、タグなしのS3バケットに適用されます。



ILM ポリシーによるオブジェクトの評価方法

アクティブなILMポリシーは、オブジェクトの配置、期間、データ保護を制御します。

クライアントがオブジェクトをStorageGRIDに保存すると、ポリシー内の順序付けられた一連のILMルールに照らしてオブジェクトが次のように評価されます。

1. ポリシー内の最初のルールのフィルタがオブジェクトに一致すると、オブジェクトはそのルールの取り込み動作に従って取り込まれ、そのルールの配置手順に従って格納されます。
2. 最初のルールのフィルタがオブジェクトに一致しない場合、オブジェクトはポリシー内の後続の各ルールに照らして（一致するまで）評価されます。
3. どのルールもオブジェクトに一致しない場合は、ポリシー内のデフォルトルールの取り込み動作と配置手順が適用されます。デフォルトルールは、ポリシー内の最後のルールです。デフォルトルールは、すべてのテナント、すべてのS3バケット、およびすべてのオブジェクトバージョンに適用する必要があり、高度なフィルタは使用できません。

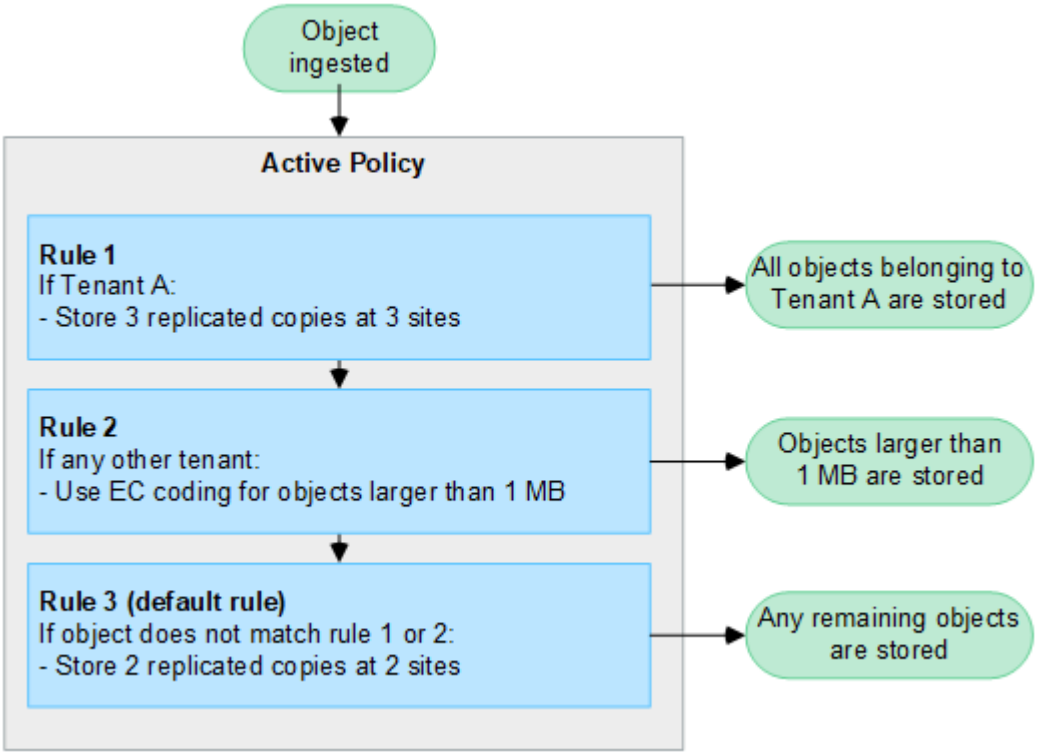
ILM ポリシーの例

たとえば、ILMポリシーに次の情報を指定する3つのILMルールを含めることができます。

- ルール**1**：テナント**A**のレプリケートコピー
  - テナントAに属するすべてのオブジェクトを一致します

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

- ルール**2**：**1MB**を超えるオブジェクトのイレイジャーコーディング
  - 他のテナントのすべてのオブジェクトが一致します（1MBを超える場合にのみ一致します）。これらのオブジェクトは、 3 つのサイトで 6+3 のイレイジャーコーディングを使用して格納されます。
  - は1MB以下のオブジェクトに一致しないため、これらのオブジェクトはルール3に照らして評価されます。
- ルール**3**：**2**つのデータセンターに**2**つのコピーを作成（デフォルト）
  - は、ポリシー内の最後のデフォルトルールです。フィルタを使用しません。
  - ルール1またはルール2に一致しないすべてのオブジェクト（テナントAに属していない1MB以下のオブジェクト）のレプリケートコピーを2つ作成します。



アクティブポリシーと非アクティブポリシーとは何ですか。

すべてのStorageGRIDシステムには、アクティブなILMポリシーが少なくとも1つ必要です。複数のアクティブなILMポリシーが必要な場合は、ILMポリシータグを作成し、各タグにポリシーを割り当てます。テナントはS3バケットにタグを適用します。デフォルトポリシーは、ポリシータグが割り当てられていないバケット内のすべてのオブジェクトに適用されます。

ILMポリシーを初めて作成するときは、1つ以上のILMルールを選択して特定の順序に並べます。ポリシーをシミュレートして動作を確認したら、ポリシーをアクティブ化します。

1つのILMポリシーをアクティブ化すると、StorageGRIDはそのポリシーを使用して、既存のオブジェクトと新しく取り込まれるオブジェクトを含むすべてのオブジェクトを管理します。新しいポリシーの ILM ルールが実装されたときに、既存のオブジェクトが新しい場所に移動されることがあります。

一度に複数のILMポリシーをアクティブ化し、テナントがS3バケットにポリシータグを適用する場合、各バケ

ット内のオブジェクトはタグに割り当てられたポリシーに従って管理されます。

StorageGRIDシステムは、アクティブ化または非アクティブ化されたポリシーの履歴を追跡します。

ILM ポリシーの作成に関する考慮事項

- システム提供のポリシーであるBaseline 2 Copiesポリシーは、テストシステムでのみ使用してください。StorageGRID 11.6以前の場合、このポリシーのMake 2 Copiesルールでは、すべてのサイトが含まれるAll Storage Nodesストレージプールを使用します。StorageGRID システムに複数のサイトがある場合は、 1 つのオブジェクトのコピーが同じサイトに 2 つ配置される可能性があります。

> All Storage Nodesストレージプールは、StorageGRID 11.6以前のインストール時に自動的に作成されます。新しいバージョンのStorageGRID にアップグレードしても、All Storage Nodesプールは引き続き存在します。StorageGRID 11.7以降を新規インストールとしてインストールする場合、All Storage Nodesプールは作成されません。

- 新しいポリシーを設計する際には、グリッドに取り込まれる可能性のあるさまざまなタイプのオブジェクトをすべて考慮してください。それらのオブジェクトに一致し、必要に応じて配置するルールがポリシーに含まれていることを確認してください。
- ILM ポリシーはできるだけシンプルにします。これにより、時間が経って StorageGRID システムに変更が加えられ、オブジェクトデータが意図したとおりに保護されないという危険な状況を回避できます。
- ポリシー内のルールの順序が正しいことを確認してください。ポリシーをアクティブ化すると、新規および既存のオブジェクトがリスト内の順にルールによって評価されます。たとえば、ポリシー内の最初のルールがオブジェクトに一致した場合、そのオブジェクトは他のルールによって評価されません。
- すべてのILMポリシーの最後のルールはデフォルトのILMルールであり、フィルタは使用できません。オブジェクトが別のルールに一致していない場合は、デフォルトルールによって、そのオブジェクトの配置場所と保持期間が制御されます。
- 新しいポリシーをアクティブ化する前に、ポリシーによって既存のオブジェクトの配置が変更されていないかどうかを確認します。既存のオブジェクトの場所を変更すると、新しい配置が評価されて実装される際に一時的なリソースの問題が発生する可能性があります。

StorageGRIDでILMポリシーを作成する

QoS要件を満たすILMポリシーを1つ以上作成します。

アクティブなILMポリシーを1つにすると、すべてのテナントとバケットに同じILMルールを適用できます。

複数のアクティブなILMポリシーを設定することで、特定のテナントやバケットに適切なILMルールを適用して、複数のQoS要件を満たすことができます。

ILMポリシーを作成します

タスクの内容

独自のポリシーを作成する前に、がストレージ要件を満たしていないことを確認して"デフォルトのILMポリシー"ください。

テストシステムでは、システム提供のポリシー（2コピーポリシー（1サイトグリッドの場合）または1サイトあたり1コピー（マルチサイトグリッドの場合）のみを使用してください。StorageGRID 11.6以前の場合、このポリシーのデフォルトルールでは、すべてのサイトが含まれるAll Storage Nodesストレージプールを使用します。StorageGRID システムに複数のサイトがある場合は、 1 つのオブジェクトのコピーが同じサイトに 2 つ配置される可能性があります。

"グローバルS3オブジェクトロック設定が有効になりました"の場合、ILM ポリシーが S3 オブジェクトロックが有効になっているバケットの要件に準拠していることを確認する必要があります。このセクションでは、S3 オブジェクトロックが有効になっていることを示す手順に従ってください。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"必要なアクセス権限"。
- S3オブジェクトロックが有効になっているかどうかに基づいて設定しておき"ILMルールが作成されました"ます。

  S3オブジェクトロックが有効になっていません

  - ポリシーにを追加する必要があり"ILMルールを作成しました"ます。必要に応じて、ポリシーを保存して追加のルールを作成し、ポリシーを編集して新しいルールを追加できます。
  - フィルタが含まれていないがあり"デフォルトの ILM ルールが作成されました"ます。

  S3オブジェクトロックが有効になりました

  - StorageGRID システムの"グローバルS3オブジェクトロック設定はすでに有効になっています"。
  - ポリシーにを追加する必要があり"準拠ILMルールと非準拠ILMルールを作成しました"ます。必要に応じて、ポリシーを保存して追加のルールを作成し、ポリシーを編集して新しいルールを追加できます。
  - に準拠しているポリシーのを指定し"デフォルトの ILM ルールが作成されました"ます。

- オプションとして、ビデオを視聴しました:

ILMポリシーの概要

も参照してください"ILMポリシーを使用する"。

手順

1. 「 * ILM * > * Policies * 」を選択します。

   グローバルなS3オブジェクトロック設定が有効になっている場合は、[ILM policies]ページに、どのILMルールが準拠しているかが示されます。

2. ILMポリシーの作成方法を決定します。

新しいポリシーを作成する

a. [ポリシーの作成]*を選択します。

既存のポリシーをクローニングする

a. 開始するポリシーのチェックボックスを選択し、*[クローン]*を選択します。

既存のポリシーを編集する

a. アクティブでないポリシーは編集できます。最初に使用する非アクティブポリシーのチェックボックスを選択し、*[編集]*を選択します。

3. [ポリシー名]*フィールドに、ポリシーの一意の名前を入力します。
4. 必要に応じて、*[Reason for change]*フィールドに、新しいポリシーを作成する理由を入力します。
5. ポリシーにルールを追加するには、*[ルールの選択]*を選択します。ルール名を選択すると、そのルールの設定が表示されます。

   ポリシーをクローニングする場合は、次の手順を実行します。

   - クローニングするポリシーで使用されているルールが選択されます。
   - クローニングするポリシーで、デフォルトルールではないフィルタを使用していないルールが使用されている場合は、それらのルールを 1 つだけ残して、それを除くすべてのルールを削除するように求められます。
   - デフォルトルールでフィルタを使用している場合は、新しいデフォルトルールを選択するように求められます。
   - デフォルトルールが最後のルールでなかった場合は、新しいポリシーの末尾にルールを移動できます。

S3オブジェクトロックが有効になっていません

a. ポリシーのデフォルトルールを1つ選択します。新しいデフォルトルールを作成するには、*[ILM rules]ページ*を選択します。

   デフォルトルールは、ポリシー内の別のルールに一致しないオブジェクトを環境 します。デフォルトルールはフィルタを使用できず、常に最後に評価されます。

   > Make 2 Copiesルールをポリシーのデフォルトルールとして使用しないでください。Make 2 Copies ルールは、 1 つのストレージプールであるすべてのストレージノードを使用します。このプールにはすべてのサイトが含まれています。StorageGRID システムに複数のサイトがある場合は、 1 つのオブジェクトのコピーが同じサイトに 2 つ配置される可能性があります。

S3オブジェクトロックが有効になりました

a. ポリシーのデフォルトルールを1つ選択します。新しいデフォルトルールを作成するには、*[ILM rules]ページ*を選択します。

   ルールのリストには、準拠しており、フィルタを使用しないルールのみが含まれています。

   > Make 2 Copiesルールをポリシーのデフォルトルールとして使用しないでください。Make 2 Copies ルールは、 1 つのストレージプールであるすべてのストレージノードを使用します。このプールにはすべてのサイトが含まれています。このルールを使用すると、 1 つのオブジェクトの複数のコピーが同じサイトに配置される場合があります。

b. S3非準拠バケット内のオブジェクトに別の「デフォルト」ルールが必要な場合は、*[非準拠S3バケットに対してフィルタなしのルールを含める]*を選択し、フィルタを使用しない非準拠ルールを1つ選択します。

   たとえば、クラウドストレージプールを使用して、S3オブジェクトロックが有効になっていないバケットにオブジェクトを格納できます。

   > フィルタを使用しない非準拠ルールは 1 つだけ選択できます。

も参照してください"例 7 ： S3 オブジェクトロックの準拠 ILM ポリシー"。

6. デフォルトルールの選択が完了したら、* Continue *を選択します。
7. [Other rules]ステップで、ポリシーに追加する他のルールを選択します。これらのルールでは、少なくとも1つのフィルタ（テナントアカウント、バケット名、高度なフィルタ、最新でない参照時間）を使用します。次に、*[選択]*を選択します。

   [Create a policy]ウィンドウに、選択したルールが表示されます。デフォルトのルールは末尾にあり、その上に他のルールがあります。

   S3オブジェクトロックが有効になっていて、非準拠の「デフォルト」ルールも選択した場合、そのルールはポリシーの最後から2番目のルールとして追加されます。

オブジェクトを無期限に保持しないルールがある場合は、警告が表示されます。このポリシーをアクティブ化するときは、デフォルトルールの配置手順が経過したときにStorageGRID でオブジェクトを削除することを確認する必要があります（バケットライフサイクルによってオブジェクトが長期間保持される場合を除く）。

8. デフォルト以外のルールの行をドラッグして、これらのルールを評価する順序を決定します。

   デフォルトのルールは移動できません。S3オブジェクトロックが有効になっている場合は、非準拠の「デフォルト」ルールを選択しても移動できません。

   ILM ルールの順序が正しいことを確認してください。ポリシーをアクティブ化すると、新規および既存のオブジェクトがリスト内の順にルールによって評価されます。

9. 必要に応じて、*[ルールの選択]*を選択してルールを追加または削除します。
10. 完了したら、 * 保存 * を選択します。
11. 上記の手順を繰り返して、追加のILMポリシーを作成します。
12. ILM ポリシーをシミュレートしますです。ポリシーが想定どおりに機能するように、アクティブ化する前に必ずポリシーをシミュレートしてください。

ポリシーをシミュレートする

ポリシーをアクティブ化して本番環境のデータに適用する前に、テストオブジェクトでポリシーをシミュレートします。

開始する前に

テストする各オブジェクトのS3バケット/オブジェクトキーを確認しておきます。

手順

1. S3クライアントまたはを使用して"S3コンソール"、各ルールのテストに必要なオブジェクトを取り込みます。
2. [ILM policies]ページで、ポリシーのチェックボックスを選択し、*[Simulate]*を選択します。
3. [* Object *]フィールドに、テストオブジェクトのS3を入力し `bucket/object-key`ます。たとえば、`bucket-01/filename.png`です。
4. S3のバージョン管理が有効になっている場合は、必要に応じて* Version ID *フィールドにオブジェクトのバージョンIDを入力します。
5. 「 * Simulate * 」を選択します。
6. [Simulation results]セクションで、各オブジェクトが正しいルールに一致したことを確認します。
7. 有効なストレージプールまたはイレイジャーコーディングプロファイルを確認するには、一致したルールの名前を選択してルールの詳細ページに移動します。

   既存のレプリケートオブジェクトとイレイジャーコーディングオブジェクトの配置に対する変更を確認します。既存のオブジェクトの場所を変更すると、新しい配置が評価されて実装される際に一時的なリソースの問題が発生する可能性があります。

結果

ポリシーのルールに変更を加えると、シミュレーション結果に反映され、新しいマッチと以前のマッチが表示

されます。シミュレートポリシーウィンドウには、*すべてクリア*またはシミュレーション結果リスト内の各オブジェクトの削除アイコン✕を選択するまで、テストしたオブジェクトが保持されます。

関連情報

"ILMポリシーのシミュレーション例"

ポリシーをアクティブ化する

1つの新しいILMポリシーをアクティブ化すると、既存のオブジェクトと新しく取り込まれたオブジェクトがそのポリシーで管理されます。複数のポリシーをアクティブ化すると、バケットに割り当てられたILMポリシータグによって管理対象のオブジェクトが決まります。

新しいポリシーをアクティブ化する前に：

1. ポリシーをシミュレートして、想定どおりに動作することを確認します。
2. 既存のレプリケートオブジェクトとイレイジャーコーディングオブジェクトの配置に対する変更を確認します。既存のオブジェクトの場所を変更すると、新しい配置が評価されて実装される際に一時的なリソースの問題が発生する可能性があります。



原因 ポリシーにエラーがあると、回復不能なデータ損失が発生する可能性があります。

タスクの内容

ILM ポリシーをアクティブ化すると、システムは新しいポリシーをすべてのノードに配布します。ただし、すべてのグリッドノードが新しいアクティブポリシーを受信できるようになるまで、新しいポリシーが実際には有効にならない場合があります。グリッドオブジェクトが誤って削除されないように、新しいアクティブポリシーの実装を待機する場合もあります。具体的には：

- データの冗長性や耐久性を高める*ポリシーを変更すると、変更はすぐに実装されます。たとえば、 2 コピーのルールではなく 3 コピーのルールを含む新しいポリシーをアクティブ化した場合、そのポリシーはすぐに実装されます。これは、データの冗長性が向上するためです。
- データの冗長性や保持性を低下させる可能性がある*ポリシーを変更した場合、すべてのグリッドノードが使用可能になるまで変更は実装されません。たとえば、3コピーのルールではなく2コピーのルールを使用する新しいポリシーをアクティブ化すると、その新しいポリシーは[Active policy]タブに表示されますが、すべてのノードがオンラインで使用可能になるまで有効になりません。

手順

1つまたは複数のポリシーをアクティブ化する手順に従います。

1つのポリシーをアクティブ化

アクティブなポリシーを1つだけにする場合は、次の手順を実行します。すでにアクティブなポリシーが1つ以上あり、追加のポリシーをアクティブ化する場合は、次の手順に従って複数のポリシーをアクティブ化します。

1. ポリシーをアクティブ化する準備ができたら、**[ILM]**>*[Policies]*を選択します。

   または、* ILM **>** Policy tags *ページで1つのポリシーをアクティブ化することもできます。

2. [ポリシー]タブで、アクティブ化するポリシーのチェックボックスを選択し、*[アクティブ化]*を選択します。
3. 該当する手順を実行します。
   - ポリシーをアクティブ化するかどうかを確認する警告メッセージが表示されたら、* OK *を選択します。
   - ポリシーの詳細を含む警告メッセージが表示された場合は、次の手順を実行します。
     i. 詳細を確認して、ポリシーでデータが想定どおりに管理されることを確認します。
     ii. デフォルトのルールでオブジェクトが限られた日数だけ格納される場合は、保持図を確認し、その日数をテキストボックスに入力します。
     iii. デフォルトのルールでオブジェクトが無期限に格納され、保持期間が制限されているルールがある場合は、テキストボックスに「* yes *」と入力します。
     iv. [ポリシーのアクティブ化]*を選択します。

複数のポリシーのアクティブ化

複数のポリシーを有効にするには、ポリシー タグを作成し、各タグにポリシーを割り当てる必要があります。グリッドには最大 10 個のポリシー タグを作成できます。

> 複数のポリシー タグが使用されている場合、テナントがバケットにポリシー タグを頻繁に再割り当てすると、グリッドのパフォーマンスに影響が出る可能性があります。信頼できないテナントがある場合は、デフォルト ポリシー タグのみを使用することを検討してください。

1. **>**[Policy tags]*を選択します。
2. 「 * Create * 」を選択します。
3. [ポリシータグの作成]ダイアログボックスで、タグ名とタグの概要（オプション）を入力します。

   > タグの名前と説明はテナントに表示されます。バケットに割り当てるポリシータグをテナントが選択する際に十分な情報に基づいて決定するのに役立つ値を選択してください。たとえば、割り当てられているポリシーによって一定の期間が経過したあとにオブジェクトが削除される場合は、概要でその旨を通知できます。これらのフィールドには機密情報を含めないでください。

4. [タグの作成]*を選択します。
5. ILMポリシータグの表で、プルダウンを使用してタグに割り当てるポリシーを選択します。
6. [ポリシーの制限]列に警告が表示された場合は、*[ポリシーの詳細を表示]*を選択してポリシーを確認

します。

7. 各ポリシーが想定どおりにデータを管理することを確認します。
8. を選択します。または、[変更のクリア]*を選択してポリシーの割り当てを削除します。
9. [Activate policies with new tags]ダイアログボックスで、各タグ、ポリシー、およびルールによるオブジェクトの管理方法の説明を確認します。ポリシーでオブジェクトが想定どおりに管理されるように、必要に応じて変更を行います。
10. ポリシーをアクティブ化する場合は、テキストボックスに「* yes 」と入力し、[ポリシーのアクティブ化]*を選択します。

関連情報

"例 6 ： ILM ポリシーを変更する"

StorageGRID での **ILM** ポリシーシミュレーションの例

ILMポリシーシミュレーションの例では、環境に合わせてシミュレーションを構造化および変更するためのガイドラインを示します。

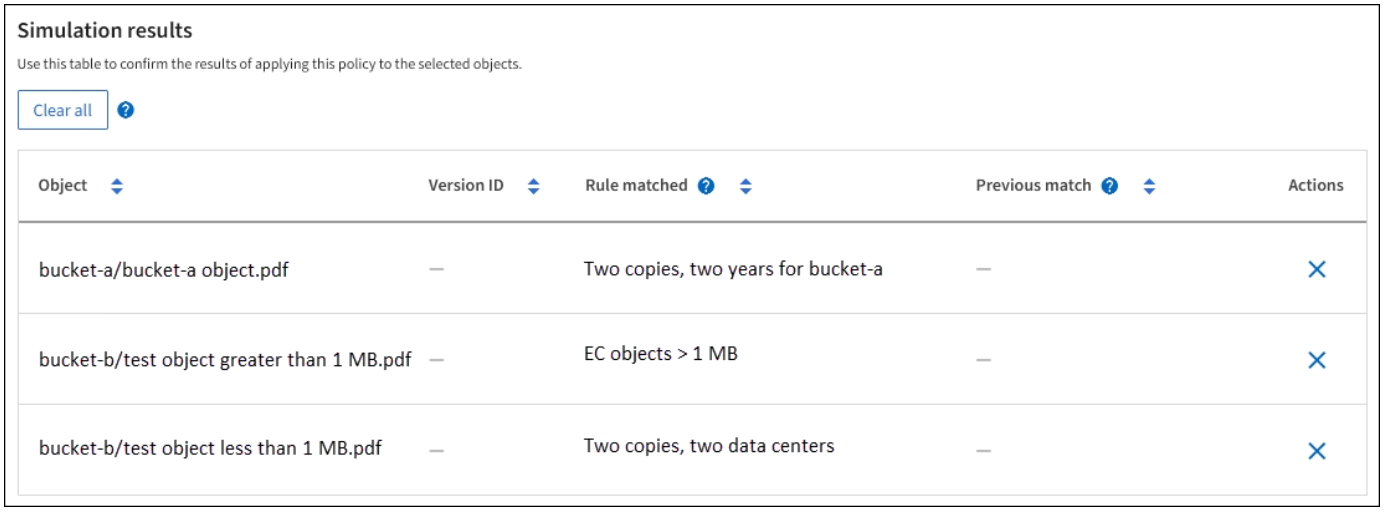
例**1**：**ILM**ポリシーをシミュレートしてルールを検証する

この例では、ポリシーをシミュレートするときにルールを検証する方法について説明します。

この例では、 2 つのバケットに取り込まれたオブジェクトに対して * サンプルの ILM ポリシー * をシミュレートします。このポリシーには、次の 3 つのルールが含まれています。

- 最初のルール「 * 2 copies 、 buckets-a * 」の 2 年間は、 bucket-a のオブジェクトにのみ適用されます
- 2 番目のルール「 * EC objects > 1 MB * 、環境 all buckets] は 1MB を超えるオブジェクトをフィルタリングします。
- 3 つ目のルール「 * 2 つのコピー、 2 つのデータセンター」はデフォルトルールです。フィルタは含まれず、参照時間を noncurrent に指定したものは使用しません。

ポリシーをシミュレートしたら、各オブジェクトが正しいルールに一致したことを確認します。



次の例では、

- `bucket-a/bucket-a object.pdf`のオブジェクトでフィルタリングする最初のルールが正しく一致しました `bucket-a。
- `bucket-b/test object greater than 1 MB.pdf`がにある `bucket-b`ため、最初のルールに一致しませんでした。代わりに、 1MB を超えるオブジェクトをフィルタリングする 2 つ目のルールに正しく一致しました。
- `bucket-b/test object less than 1 MB.pdf`最初の2つのルールのフィルタに一致しなかったため、フィルタが含まれていないデフォルトのルールによって配置されます。

例**2**：**ILM**ポリシーをシミュレートする際にルールの順序を変更する

この例では、ポリシーをシミュレートする際に、ルールの順序を変更して結果を変更する方法を示します。

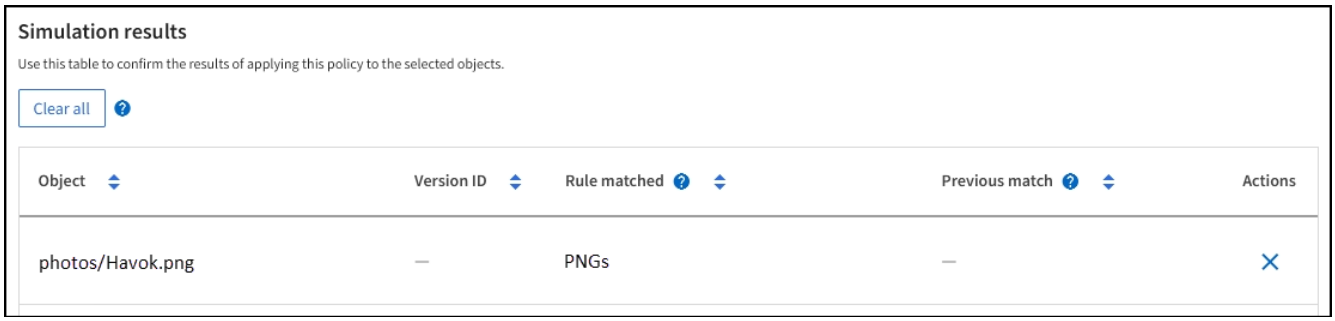
この例では、 * Demo * ポリシーをシミュレートします。このポリシーの目的は次の 3 つのルールで、 series = x -men ユーザメタデータを含むオブジェクトを検索することです。

- 最初のルール「* PNGs *」は、で終わるキー名をフィルタリングし `.png`ます。
- 2つ目のルール「* X-men *」はテナントAのオブジェクトにのみ適用され、ユーザメタデータに対してフィルタを適用します `series=x-men`。
- 最後のルール「* two copies two data centers *」がデフォルトルールで、最初の2つのルールに一致しないオブジェクトに一致します。

手順

1. ルールを追加してポリシーを保存したら、 * Simulate * を選択します。
2. [Object]フィールドにテストオブジェクトの**S3**バケット/オブジェクトキーを入力し、[Simulate]*を選択します。

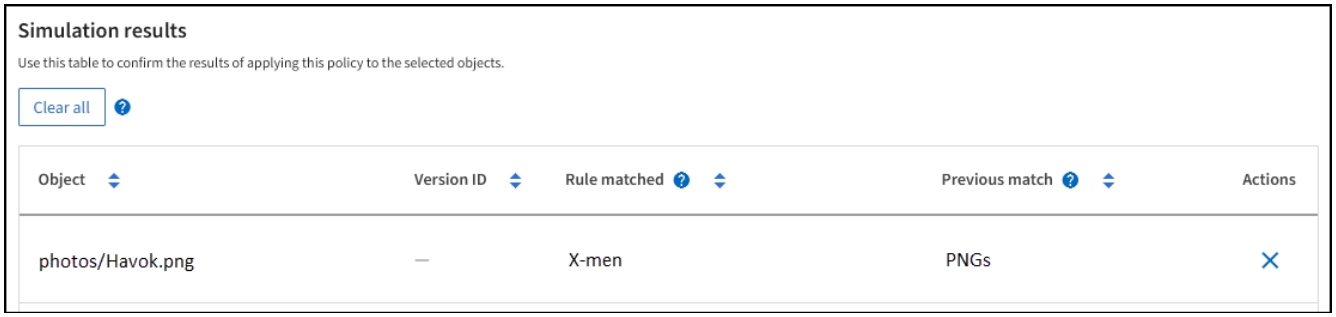
   オブジェクトが* PNGs *ルールに一致したことを示すシミュレーション結果が表示されます `Havok.png`。



   ただし `Havok.png`、は* X-men *ルールをテストすることを目的としています。

3. 問題 を解決するには、ルールの順序を変更します。
   a. [Finish]*を選択して[Simulate ILM Policy]ウィンドウを閉じます。
   b. 「 * Edit * 」を選択して、ポリシーを編集します。
   c. 「 * X-men 」ルールをリストの先頭にドラッグします。
   d. [保存（ Save ）] を選択します。
4. 「 * Simulate * 」を選択します。

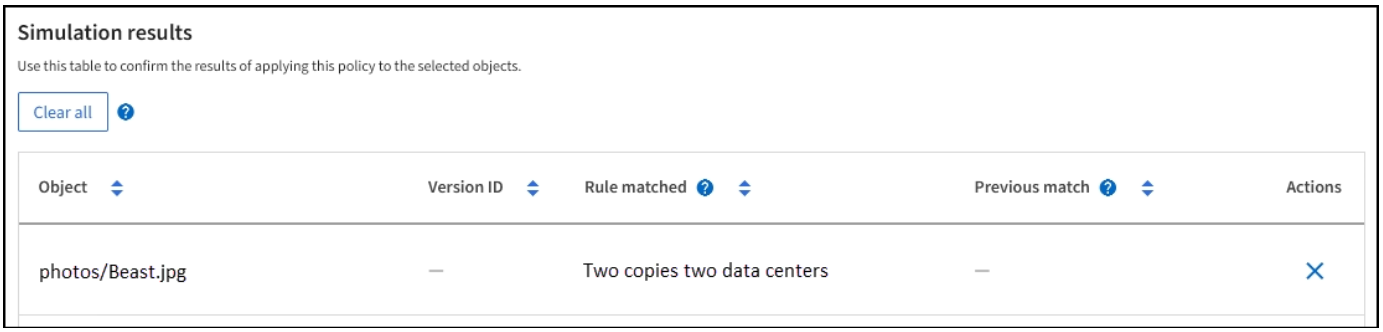
以前にテストしたオブジェクトが更新したポリシーに照らして再評価され、新しいシミュレーション結果が表示されます。この例では、想定どおりにオブジェクトが「X-men」メタデータルールに一致したことが[Rule Matched]列に表示されて `Havok.png`います。[Previous Match]列には、PNGsルールが前回のシミュレーションでオブジェクトに一致したことが表示されます。



例**3**：**ILM**ポリシーをシミュレートするときにルールを修正する

この例では、ポリシーをシミュレートしてポリシー内のルールを修正し、シミュレーションを続行する方法を示します。

この例では、 * Demo * ポリシーをシミュレートします。このポリシーは、ユーザメタデータを含むオブジェクトを検索することを目的として `series=x-men`います。ただし、このポリシーをオブジェクトに対してシミュレートしたときに予期しない結果が発生しました `Beast.jpg`。オブジェクトが「 X-men 」メタデータルールではなくデフォルトルールに一致しましたが、 2 つのデータセンターがコピーされています。



テストオブジェクトがポリシー内の想定したルールに一致しない場合は、ポリシー内の各ルールを調べてエラーを修正する必要があります。

手順

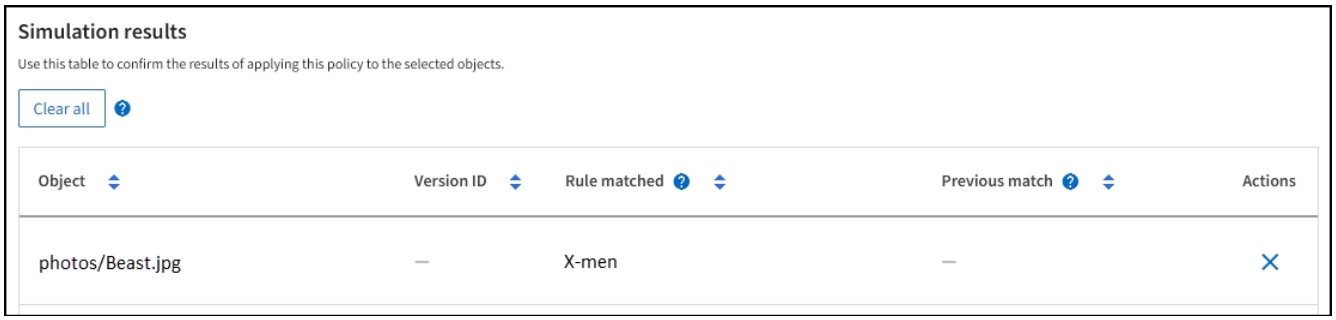
1. を選択して**[**ポリシーのシミュレート**]**ダイアログを閉じます。ポリシーの詳細ページで、[保持図]を選択します。次に、必要に応じて各ルールの[すべて展開]または[詳細を表示]*を選択します。
2. ルールのテナントアカウント、参照時間、およびフィルタ条件を確認します。

   たとえば、「X-men」ルールのメタデータが「x-men」ではなく「x-men01」と入力されたとします。

3. エラーを解決するには、次のようにルールを修正します。
   - ルールがポリシーに含まれている場合は、ルールをクローニングするか、ポリシーから削除して編集します。
   - ルールがアクティブポリシーに含まれている場合は、ルールをクローニングする必要があります。アクティブポリシーのルールを編集したり削除したりすることはできません。

4. もう一度シミュレーションを実行します。

   この例では、修正した「X-men」ルールがユーザメタデータに基づいてオブジェクトに `series=x-men` 想定どおりに一致します `Beast.jpg`。



StorageGRIDでILMポリシータグを管理する

ILMポリシータグの詳細を表示したり、タグを編集したり、タグを削除したりできます。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"必要なアクセス権限"。

ILMポリシータグの詳細の表示

タグの詳細を表示するには：

1. >[Policy tags]*を選択します。
2. テーブルからポリシーの名前を選択します。タグの詳細ページが表示されます。
3. 詳細ページで、割り当てられたポリシーの過去の履歴を表示します。
4. ポリシーを選択して表示します。

ILMポリシータグを編集

> タグの名前と説明はテナントに表示されます。バケットに割り当てるポリシータグをテナントが選択する際に十分な情報に基づいて決定するのに役立つ値を選択してください。たとえば、割り当てられているポリシーによって一定の期間が経過したあとにオブジェクトが削除される場合は、概要でその旨を通知できます。これらのフィールドには機密情報を含めないでください。

既存のタグの概要を編集するには、次の手順を実行します。

1. >[Policy tags]*を選択します。
2. タグのチェックボックスをオンにして、*[編集]*を選択します。

   または、タグの名前を選択します。タグの詳細ページが表示され、そのページで*編集*を選択できます。

3. 必要に応じてタグ概要を変更します。
4. [保存（ Save ）] を選択します。

ILMポリシータグを削除します。

ポリシータグを削除すると、そのタグが割り当てられているバケットにはデフォルトのポリシーが適用されます。

タグを削除するには：

1. **>**[Policy tags]*を選択します。
2. タグのチェックボックスをオンにして、*[削除]*を選択します。確認のダイアログボックスが表示されます。

   または、タグの名前を選択します。タグの詳細ページが表示され、そのページで*[削除]*を選択できます。

3. [はい]*を選択してタグを削除します。

関連情報

"ILMポリシータグの作成について学ぶ"

StorageGRID でオブジェクトメタデータ検索を使用して **ILM** ポリシーを検証する

ILMポリシーをアクティブ化したら、代表的なテストオブジェクトをStorageGRIDシステムに取り込み、オブジェクトメタデータの検索を実行して、コピーが意図したとおりに作成され、正しい場所に配置されていることを確認します。

開始する前に

オブジェクト識別子は次のいずれかになります。

- **UUID**: オブジェクトのユニバーサルユニーク識別子。
- **CBID**: StorageGRID内のオブジェクトの一意の識別子。監査ログからオブジェクトの CBID を取得できます。 CBID はすべて大文字で入力してください。
- **S3** バケットとオブジェクト キー: オブジェクトが S3 インターフェイスを通じて取り込まれると、クライアント アプリケーションはバケットとオブジェクト キーの組み合わせを使用してオブジェクトを保存および識別します。 S3 バケットがバージョン管理されており、バケットとオブジェクト キーを使用して S3 オブジェクトの特定のバージョンを検索する場合は、バージョン **ID** を使用します。

手順

1. オブジェクトを取り込みます。
2. ILM * > * Object metadata lookup * を選択します。
3. [* 識別子 * （ * Identifier * ）] フィールドにオブジェクトの識別子を入力します。UUID、CBID、またはS3バケット/オブジェクトキーを入力できます。
4. 必要に応じて、オブジェクトのバージョン ID を入力します（ S3 のみ）。
5. 「 * 検索 * 」を選択します。

   オブジェクトメタデータの検索結果が表示されます。このページには、次の種類の情報が表示されます。

- システムメタデータ（オブジェクトID（UUID）、結果タイプ（オブジェクト、削除マーカー、S3バケット）、オブジェクトの論理サイズなど）。詳細については、以下のスクリーンショットの例を参照してください。
- オブジェクトに関連付けられているカスタムユーザメタデータのキーと値のペア。
- S3 オブジェクトの場合、オブジェクトに関連付けられているオブジェクトタグのキーと値のペア。
- レプリケートオブジェクトコピーの場合、各コピーの現在の格納場所。
- イレイジャーコーディングオブジェクトコピーの場合、各フラグメントの現在の格納場所。
- クラウドストレージプール内のオブジェクトコピーの場合、外部バケットの名前とオブジェクトの一意の識別子を含むオブジェクトの場所。
- セグメント化されたオブジェクトとマルチパートオブジェクトの場合、セグメント ID とデータサイズを含むオブジェクトセグメントのリスト。100 個を超えるセグメントを持つオブジェクトの場合は、最初の 100 個のセグメントだけが表示されます。
- 未処理の内部ストレージ形式のすべてのオブジェクトメタデータ。この未加工のメタデータには、リリース間で維持されるとはかぎらない内部のシステムメタデータが含まれます。

6. オブジェクトが正しい場所に格納されていること、および正しいタイプのコピーであることを確認します。

   監査オプションが有効になっている場合は、監査ログを監視して「 ORLM Object Rules Met 」というメッセージを探すこともできます。ORLM監査メッセージからは、ILM評価プロセスの詳細なステータスを確認できますが、オブジェクトデータの配置が正しいかどうかやILMポリシーが完全であるかどうかは確認できません。これは自分で評価する必要があります。詳細については、を参照してください "監査ログを確認します"。

次の例では、 2 つのレプリケートコピーとして格納された S3 テストオブジェクトのオブジェクトメタデータの検索結果が表示されています。

> 次のスクリーンショットは一例です。表示される結果は、StorageGRIDのバージョンによって異なります。

System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H$|TFbnQQ}|CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H$|TFboW28|CXG%

Raw Metadata


```
{
    "TYPE": "CTNT",
    "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
    "NAME": "testobject",
    "CBID": "0x8823DE7EC7C10416",
    "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
    "PPTH": "source",
    "META": {
        "BASE": {
            "PAWS": "2",
```


関連情報

"S3 REST APIを使用する"

StorageGRID で ILM ポリシーと ILM ルールを操作する

ストレージ要件の変化に応じて、追加のポリシーを設定したり、ポリシーに関連付けられているILMルールを変更したりしなければならない場合があります。ILM指標を表示してシステムパフォーマンスを判断できます。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- そうだな "特定のアクセス権限"

ILMポリシーを表示します

アクティブ/非アクティブのILMポリシーとポリシーのアクティブ化履歴を表示するには

1. 「 * ILM * > * Policies * 」を選択します。
2. アクティブポリシーと非アクティブポリシーのリストを表示するには、*[Policies]*を選択します。テーブルには、各ポリシーの名前、ポリシーが割り当てられているタグ、およびポリシーがアクティブか非アクティブかが表示されます。
3. ポリシーのアクティブ化の開始日と終了日のリストを表示するには、[Activation history]*を選択します。
4. ポリシー名を選択すると、ポリシーの詳細が表示されます。



ステータスが[Edited]または[Deleted]のポリシーの詳細を表示すると、指定した期間アクティブで、その後編集または削除されたポリシーのバージョンを表示していることを示すメッセージが表示されます。

ILMポリシーを編集します。

編集できるのは、非アクティブなポリシーのみです。アクティブポリシーを編集する場合は、アクティブポリシーを非アクティブ化するか、クローンを作成して編集します。

ポリシーを編集するには：

1. 「 * ILM * > * Policies * 」を選択します。
2. 編集するポリシーのチェックボックスを選択し、*[編集]*を選択します。
3. の手順に従って、ポリシーを編集し"ILMポリシーの作成"ます。
4. ポリシーを再度アクティブ化する前にシミュレートします。



ILM ポリシーが正しく設定されていないと、リカバリできないデータ損失が発生する可能性があります。ILM ポリシーをアクティブ化する前に、 ILM ポリシーおよびその ILM ルールを慎重に確認し、次に ILM ポリシーをシミュレートします。ILM ポリシーが意図したとおりに機能することを必ず確認してください。

ILMポリシーのクローニング

ILMポリシーをクローニングするには：

1. 「 * ILM * > * Policies * 」を選択します。
2. クローニングするポリシーのチェックボックスを選択し、*[クローン]*を選択します。
3. の手順に従って、複製したポリシーから新しいポリシーを作成します"ILMポリシーの作成"。



ILM ポリシーが正しく設定されていないと、リカバリできないデータ損失が発生する可能性があります。ILM ポリシーをアクティブ化する前に、 ILM ポリシーおよびその ILM ルールを慎重に確認し、次に ILM ポリシーをシミュレートします。ILM ポリシーが意図したとおりに機能することを必ず確認してください。

ILMポリシーを削除します。

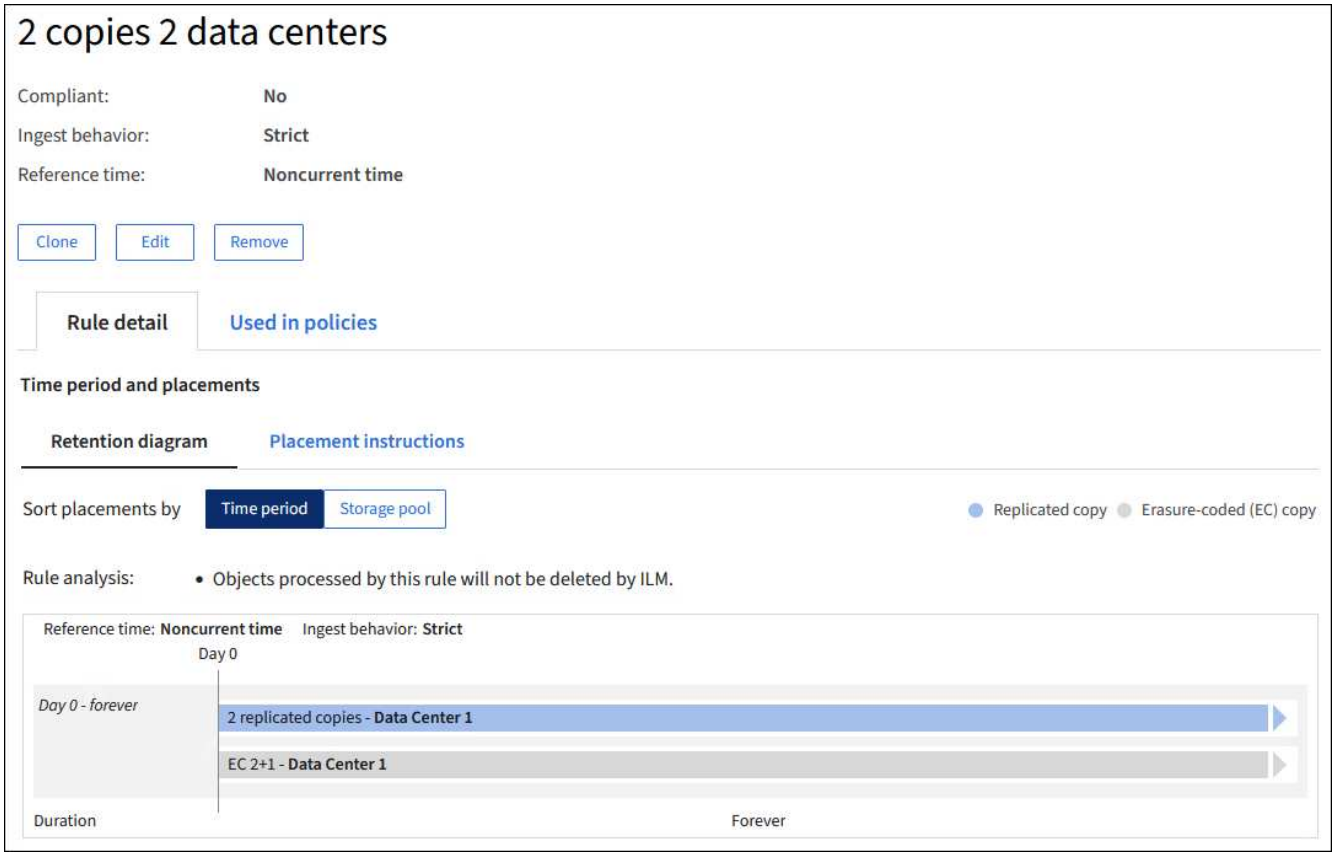
削除できるのは、ILMポリシーが非アクティブな場合のみです。ポリシーを削除するには：

1. 「 * ILM * > * Policies * 」を選択します。
2. 削除する非アクティブポリシーのチェックボックスを選択します。
3. 「 * 削除」を選択します。

ILMルールの詳細を表示します

ILMルールの詳細（保持図やルールの配置手順を含む）を表示するには、次の手順を実行します。

1. [* ILM*>* Rules] を選択します。
2. 詳細を表示するルールの名前を選択します。例：



また、詳細ページを使用してルールをクローニング、編集、削除することもできます。ポリシーで使用されているルールを編集または削除することはできません。

ILM ルールをクローニングします

既存のルールの設定の一部を使用する新しいルールを作成する場合は、既存のルールをクローニングできます。いずれかのポリシーで使用されているルールを編集する必要がある場合は、代わりにルールをクローニングしてクローンに変更を加えます。クローンに変更を加えたら、必要に応じて元のルールをポリシーから削除し、変更後のバージョンで置き換えることができます。

バージョン10.2以前のStorageGRID を使用して作成されたILMルールはクローニングできません。

手順

1. [* ILM*>* Rules] を選択します。
2. クローニングするルールのチェックボックスを選択し、**[クローニング]***を選択します。または、ルール名を選択し、ルールの詳細ページで[クローン]*を選択します。
3. との手順に従って、クローニングされたルールを更新しますILMルールの編集"ILMルールで高度なフィルタを使用する"。

   ILM ルールをクローニングする場合は、新しい名前を入力する必要があります。

ILM ルールを編集する

ILM ルールを編集して、フィルタまたは配置手順を変更しなければならない場合があります。

ILMポリシーで使用されているルールは編集できません。代わりに、クローニングされたコピーに必要な変更を加えることができますルールのクローンを作成。

ILM ポリシーが正しく設定されていないと、リカバリできないデータ損失が発生する可能性があります。ILM ポリシーをアクティブ化する前に、 ILM ポリシーおよびその ILM ルールを慎重に確認し、次に ILM ポリシーをシミュレートします。ILM ポリシーが意図したとおりに機能することを必ず確認してください。

手順

1. [* ILM*>* Rules] を選択します。
2. 編集するルールがILMポリシーで使用されていないことを確認します。
3. 編集するルールが使用中でない場合は、ルールのチェックボックスをオンにして*>[編集]を選択します。または、ルールの名前を選択し、ルールの詳細ページで[編集]*を選択します。
4. ILMルールの編集ウィザードの手順を実行します。必要に応じて、およびの手順を実行し"ILM ルールを作成する""ILMルールで高度なフィルタを使用する"ます。

   ILMルールの編集時に名前を変更することはできません。

ILMルールを削除します

現在のILMルールのリストを管理しやすくするには、使用しないILMルールをすべて削除します。

手順

アクティブポリシーで現在使用されているILMルールを削除するには、次の手順を実行します。

1. ポリシーのクローンを作成します。
2. ポリシークローンからILMルールを削除します。
3. 新しいポリシーを保存、シミュレート、およびアクティブ化して、オブジェクトが想定どおりに保護されるようにします。

4. アクティブでないポリシーで現在使用されているILMルールを削除する手順に進みます。

アクティブでないポリシーで現在使用されているILMルールを削除するには、次の手順を実行します。

1. 非アクティブポリシーを選択します。
2. ポリシーまたはからILMルールを削除しますポリシーを削除します。。
3. 現在使用されていないILMルールを削除する手順に進みます。

現在使用されていないILMルールを削除するには、次の手順を実行します。

1. [* ILM*>* Rules] を選択します。
2. 削除するルールがどのポリシーでも使用されていないことを確認します。
3. 削除するルールが使用中でない場合は、ルールを選択して*>[削除]*を選択します。複数のルールを選択して、すべてのルールを同時に削除できます。
4. [Yes]*を選択して、ILMルールの削除を確定します。

ILM指標を表示します

キューに登録されているオブジェクトの数や評価速度など、ILMの指標を確認できます。これらの指標を監視して、システムのパフォーマンスを判断できます。キューや評価速度が大きい場合は、システムが取り込み速度に対応できていないか、クライアントアプリケーションからの負荷が過剰であるか、何らかの異常な状態が発生している可能性があります。

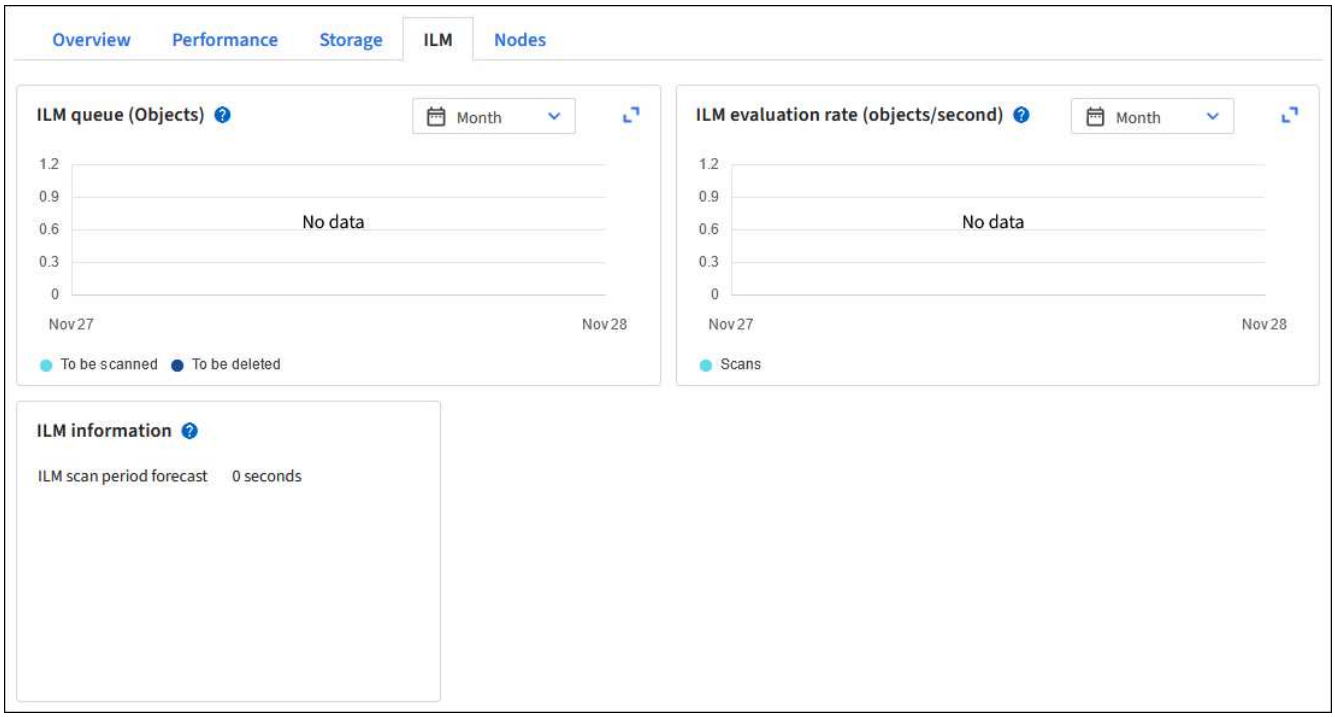
手順

1. >[ILM]*を選択します。

   ダッシュボードはカスタマイズ可能なため、[ILM]タブが使用できない場合があります。

2. [ILM]タブで指標を監視します。

   疑問符 を選択すると、ILMタブの項目の説明を確認できます。



S3 オブジェクトロックを使用する

S3 Object LockがStorageGRIDでオブジェクトを保護する仕組み

グリッド管理者は、StorageGRID システムでS3オブジェクトロックを有効にし、準拠ILMポリシーを実装して、特定のS3バケット内のオブジェクトが一定期間削除または上書きされないようにすることができます。

S3 オブジェクトのロックとは何ですか？

StorageGRID S3 オブジェクトロック機能は、 Amazon Simple Storage Service （ Amazon S3 ）での S3 オブジェクトロックに相当するオブジェクト保護解決策 です。

グローバル S3 オブジェクトロック設定が StorageGRID システムで有効になっている場合、S3 テナントアカウントは、S3 オブジェクトロックが有効または無効のいずれかでバケットを作成できます。既存バケットに対する S3 オブジェクトロックを許可する設定が有効になっている場合、S3 テナントアカウントは既存バケットに対して S3 オブジェクトロックを有効にできます。バケットで S3 オブジェクトロックが有効になっている場合、バケットのバージョン管理が必要となり、自動的に有効になります。S3 テナントアカウントが新規または既存のバケットに対して S3 オブジェクトロックを有効にすると、無効にすることはできません。

- S3オブジェクトロック*が設定されていないバケットには、保持設定が指定されていないオブジェクトのみを含めることができます。保持設定は取り込まれたオブジェクトには適用されません。
- S3 Object Lock *が設定されたバケットには、S3クライアントアプリケーションで保持設定の有無に関係なくオブジェクトを含めることができます。取り込まれた一部のオブジェクトには保持設定が設定されます。
- S3オブジェクトロックでデフォルトの保持が設定されたバケット*では、保持設定を指定したオブジェクトをアップロードし、保持設定を指定せずに新しいオブジェクトをアップロードできます。保持設定がオブジェクトレベルで設定されていないため、新しいオブジェクトではデフォルト設定が使用されます。

デフォルトの保持が設定されている場合、新しく取り込まれたすべてのオブジェクトに保持設定が適用されま

す。オブジェクト保持設定のない既存のオブジェクトは影響を受けません。

保持モード

StorageGRID S3オブジェクトロック機能は、2つの保持モードをサポートしており、さまざまなレベルの保護をオブジェクトに適用できます。これらのモードは、Amazon S3の保持モードに相当します。

- コンプライアンスモードの場合：
  - retain-until-dateに達するまで、オブジェクトを削除できません。
  - オブジェクトのretain-until-dateは増やすことはできますが、減らすことはできません。
  - オブジェクトのretain-until-dateは、その日付に達するまで削除できません。
- ガバナンスモードの場合：
  - 特別な権限を持つユーザは、要求でバイパスヘッダーを使用して、特定の保持設定を変更できます。
  - これらのユーザは、retain-until-dateに達する前にオブジェクトバージョンを削除できます。
  - これらのユーザは、オブジェクトのretain-until-dateを増減、または削除できます。

オブジェクトバージョンの保持設定

S3オブジェクトロックを有効にしてバケットを作成した場合、ユーザはS3クライアントアプリケーションを使用して、バケットに追加される各オブジェクトに次の保持設定を必要に応じて指定できます。

- 保持モード：コンプライアンスまたはガバナンスのいずれか。
- * Retain-until-date *：オブジェクトバージョンのretain-until-dateが将来の日付の場合、オブジェクトは読み出すことはできますが、削除することはできません。
- * リーガルホールド * ：オブジェクトバージョンにリーガルホールドを適用すると、そのオブジェクトがただちにロックされます。たとえば、調査または法的紛争に関連するオブジェクトにリーガルホールドを設定する必要がある場合があります。リーガルホールドには有効期限はありませんが、明示的に削除されるまで保持されます。リーガルホールドは、それまでの保持期間とは関係ありません。

> オブジェクトがリーガルホールドの対象である場合、保持モードに関係なく、誰もオブジェクトを削除できません。

オブジェクト設定の詳細については、"S3 REST APIを使用してS3オブジェクトロックを設定します"を参照してください。

バケットのデフォルトの保持設定

S3オブジェクトロックを有効にしてバケットを作成した場合は、必要に応じて次のバケットのデフォルト設定を指定できます。

- デフォルトの保持モード：コンプライアンスまたはガバナンスのいずれか。
- デフォルトの保持期間：このバケットに追加された新しいオブジェクトバージョンを、追加された日から保持する期間。

デフォルトのバケット設定は、独自の保持設定がない新しいオブジェクトにのみ適用されます。これらのデフォルト設定を追加または変更しても、既存のバケットオブジェクトには影響しません。

"S3 バケットを作成します。"および"S3オブジェクトロックのデフォルトの保持期間を更新します"を参照してください。

S3 オブジェクトロックと従来の準拠の比較

S3 オブジェクトロックは、以前のバージョンの StorageGRID で使用されていた準拠機能に代わる機能です。S3オブジェクトロック機能はAmazon S3の要件に準拠しているため、独自のStorageGRIDコンプライアンス機能（現在は「レガシーコンプライアンス」と呼ばれています）は廃止されました。

> グローバルコンプライアンス設定は非推奨です。以前のバージョンの StorageGRID を使用してこの設定を有効にした場合、S3 オブジェクトロック設定は自動的に有効になります。引き続き StorageGRID を使用して既存の準拠バケットの設定を管理できますが、新しい準拠バケットを作成することはできません。詳細については、 "ネットアップのナレッジベース： StorageGRID 11.5 でレガシー準拠バケットを管理する方法"を参照してください。

以前のバージョンの StorageGRID で従来の準拠機能を使用していた場合、次の表を参照して、 StorageGRID の S3 オブジェクトロック機能と比較する方法を確認してください。

	S3 オブジェクトのロック	コンプライアンス（レガシー）
この機能はグローバルにどのように有効になりますか。	グリッド マネージャーから、構成 > システム > **S3** オブジェクト ロック を選択します。	サポートは終了しました。
バケットで機能を有効にするにはどうすればよいですか？	Tenant Manager 、テナント管理 API 、または S3 REST API を使用して新しいバケットを作成するときは、 S3 オブジェクトロックを有効にする必要があります。	サポートは終了しました。
バケットのバージョン管理はサポートされているか	はい。バケットのバージョン管理は必須であり、バケットで S3 オブジェクトのロックが有効になっている場合は自動的に有効になります。	いいえ。
オブジェクト保持はどのように設定されますか。	retain-until-dateはオブジェクトバージョンごとに設定することも、バケットごとにデフォルトの保持期間を設定することもできます。	ユーザはバケット全体の保持期間を設定する必要があります。保持期間を指定すると、バケット内のすべてのオブジェクトが環境 で保持されます。

	S3 オブジェクトのロック	コンプライアンス（レガシー）
保持期間は変更できますか。	• コンプライアンスモードでは、オブジェクトバージョンのretain-until-dateは増やすことができますが、減らすことはできません。 • ガバナンスモードでは、特別な権限を持つユーザは、オブジェクトの保持設定を変更したり削除したりできます。	バケットの保持期間は延長できますが、短縮することはできません。
リーガルホールドはどこで制御されますか？	バケット内のオブジェクトバージョンにリーガルホールドを適用したり、リーガルホールドを解除したりできます。	リーガルホールドはバケットに適用され、バケット内のすべてのオブジェクトに適用されます。
オブジェクトを削除できるのはいつですか。	• 準拠モードでは、オブジェクトがリーガルホールドの対象でない場合、retain-until-dateに達したあとにオブジェクトバージョンを削除できます。 • ガバナンスモードでは、特別な権限を持つユーザは、オブジェクトがリーガルホールドの対象でない場合、retain-until-dateに達する前にオブジェクトを削除できます。	バケットがリーガルホールドの対象でない場合は、保持期間が過ぎたあとにオブジェクトを削除できます。オブジェクトは自動または手動で削除できます。
バケットライフサイクル設定はサポートされていますか。	はい	いいえ

StorageGRIDのS3 Object Lockワークフロー

グリッド管理者は、テナントユーザと緊密に連携し、保持要件に応じてオブジェクトが保護されるようにする必要があります。

テナント設定をグリッド全体に適用する場合、ネットワーク接続、ノードのステータス、およびCassandraの処理によっては、15分以上かかることがあります。

グリッド管理者とテナントユーザを対象に、S3オブジェクトロック機能を使用するためのタスクの概要を次に示します。

グリッド管理者

- StorageGRIDシステム全体に対してS3オブジェクトロックのグローバル設定を有効にします。
- ユーザーが既存のバケットに対して S3 オブジェクトロックを有効にできるようにします。
- 情報ライフサイクル管理（ILM）ポリシーが_compliant_（に準拠）であることを確認します"S3オブジ

ェクトロックが有効なバケットの要件"。

- 必要に応じて、テナントでComplianceを保持モードとして使用できるようにします。それ以外の場合は、ガバナンスモードのみが許可されます。
- 必要に応じて、テナントの最大保持期間を設定します。

テナントユーザ

- S3オブジェクトロックを使用するバケットとオブジェクトに関する考慮事項を確認してください。
- 必要に応じて、グリッド管理者に連絡して、以下のいずれかの設定を有効にしてください。
  - グローバルS3オブジェクトロック
  - 既存のバケットに対してS3オブジェクトロックを有効にすることを許可する
- S3オブジェクトロックを有効にしてバケットを作成する。
- 既存のバケットでS3オブジェクトロックを有効にします。
- 必要に応じて、バケットのデフォルトの保持設定を指定します。
  - デフォルトの保持モード：GovernanceまたはCompliance（グリッド管理者が許可している場合）。
  - Default retention period：グリッド管理者が設定した最大保持期間以下にする必要があります。
- S3クライアントアプリケーションを使用して、オブジェクトを追加し、必要に応じてオブジェクト固有の保持期間を設定します。
  - 保持モード。ガバナンスまたはコンプライアンス（グリッド管理者によって許可されている場合）。
  - Retain Until Date：グリッド管理者が設定した最大保持期間以下にする必要があります。

関連情報

"S3 Object Lock の要件"について学ぶ

StorageGRID での **S3** オブジェクトロックの要件

グローバルな S3 オブジェクトのロック設定を有効にするための要件、準拠 ILM ルールおよび ILM ポリシーを作成するための要件、および StorageGRID が S3 オブジェクトロックを使用するバケットとオブジェクトに適用する制限事項を確認しておく必要があります。

グローバルな **S3** オブジェクトロック設定を使用するための要件

- S3 テナントが S3 オブジェクトロックを有効にしてバケットを作成できるようにするには、 Grid Manager またはグリッド管理 API を使用してグローバルな S3 オブジェクトロック設定を有効にする必要があります。
- グローバルな S3 オブジェクトのロック設定を有効にすると、すべての S3 テナントアカウントで S3 オブジェクトのロックを有効にしてバケットを作成できるようになります。
- S3オブジェクトロックのグローバル設定を有効にしたあとで、設定を無効にすることはできません。
- すべてのアクティブなILMポリシーのデフォルトルールが_compliant_である（つまり、デフォルトルールはS3 Object Lockが有効なバケットの要件に準拠している必要がある）場合を除き、グローバルS3オブジェクトロックを有効にすることはできません。

- S3オブジェクトロックのグローバル設定が有効になっている場合は、ポリシーのデフォルトルールが準拠していないかぎり、新しいILMポリシーを作成したり既存のILMポリシーをアクティブ化したりすることはできません。グローバルなS3オブジェクトロック設定が有効になると、ILMルールとILMポリシーのページに、どのILMルールが準拠しているかが表示されます。

既存のバケットで**S3 Object Lock**を有効にするための要件

グローバルなS3オブジェクトロック設定が有効になっている場合、既存のバケットでS3オブジェクトロックを有効にする権限を持つすべてのS3テナントアカウントまたはS3ユーザーに、オプションで許可することができます。S3テナントアカウントまたはS3ユーザーが既存のバケットでS3オブジェクトロックを有効にすると、ILMルールによっては、クラウドストレージプールからStorageGRIDへの意図しないデータ移行が発生する可能性があります。

> 意図しないデータ移行は、一度始まってしまうと止めることはできません。

準拠 **ILM** ルールの要件

S3オブジェクトロックのグローバル設定を有効にする場合は、すべてのアクティブなILMポリシーのデフォルトルールが準拠していることを確認する必要があります。準拠ルールは、 S3 オブジェクトのロックが有効になっているバケットと従来の準拠が有効になっている既存のバケットの両方の要件を満たします。

- 2 つ以上のレプリケートオブジェクトコピーまたは 1 つのイレイジャーコーディングコピーを作成する。
- これらのコピーが、配置手順の各ラインの間、ストレージノード上に存在している必要があります。
- オブジェクトコピーをクラウドストレージプールに保存することはできません。
- 配置手順の少なくとも1行は、参照時間として*取り込み時間*を使用して、0日目から開始する必要があります。
- 配置手順の少なくとも1行は「forever」にする必要があります。

ILMポリシーの要件

グローバルなS3オブジェクトロック設定が有効になっている場合は、アクティブと非アクティブのILMポリシーに準拠ルールと非準拠ルールの両方を含めることができます。

- アクティブまたは非アクティブのILMポリシーのデフォルトルールは準拠ルールである必要があります。
- 非準拠ルールは、S3オブジェクトロックが有効になっていないバケット内のオブジェクト、または従来の準拠機能が有効になっていないバケット内のオブジェクトにのみ適用されます。
- 準拠ルールは任意のバケット内のオブジェクトに適用できます。 S3 オブジェクトのロックや従来の準拠を有効にする必要はありません。

"S3オブジェクトロックの準拠ILMポリシーの例"

S3 オブジェクトのロックを有効にした場合のバケットの要件

- StorageGRID システムでグローバルな S3 オブジェクトロック設定が有効になっている場合は、テナントマネージャ、テナント管理 API 、または S3 REST API を使用して、 S3 オブジェクトロックを有効にしたバケットを作成できます。
- バケットで S3 オブジェクトのロックが有効になっている場合は、そのバケットのバージョン管理が StorageGRID で自動的に有効になります。バケットのS3オブジェクトロックを無効にしたり、バージョン管理を一時停止したりすることはできません。

- 必要に応じて、Tenant Manager、テナント管理API、またはS3 REST APIを使用して、各バケットのデフォルトの保持モードと保持期間を指定できます。バケットのデフォルトの保持設定は、バケットに追加された新しいオブジェクトのうち、独自の保持設定がないオブジェクトにのみ適用されます。これらのデフォルト設定は、アップロード時にオブジェクトバージョンごとに保持モードとretain-until-dateを指定することで上書きできます。
- バケットライフサイクル設定は、S3オブジェクトロックが有効なバケットでサポートされます。

S3 オブジェクトのロックが有効になっているバケット内のオブジェクトの要件

- オブジェクトバージョンを保護するには、バケットのデフォルトの保持設定を指定するか、オブジェクトバージョンごとに保持設定を指定します。オブジェクトレベルの保持設定は、S3クライアントアプリケーションまたはS3 REST APIを使用して指定できます。
- 保持設定はオブジェクトのバージョンごとに適用されます。オブジェクトバージョンには、 retain-until date 設定とリーガルホールド設定の両方を設定できます。ただし、オブジェクトバージョンを保持することはできません。また、どちらも保持することはできません。オブジェクトの retain-une-date 設定またはリーガルホールド設定を指定すると、要求で指定されたバージョンのみが保護されます。オブジェクトの以前のバージョンはロックされたまま、オブジェクトの新しいバージョンを作成できます。

S3 オブジェクトのロックが有効なバケット内のオブジェクトのライフサイクル

S3オブジェクトロックが有効なバケットに保存された各オブジェクトは、次の段階を経ます。

1. * オブジェクトの取り込み *

   S3オブジェクトロックが有効になっているバケットにオブジェクトバージョンを追加すると、保持設定は次のように適用されます。

   - オブジェクトに保持設定が指定されている場合は、オブジェクトレベルの設定が適用されます。デフォルトのバケット設定は無視されます。
   - オブジェクトに保持設定が指定されていない場合は、デフォルトのバケット設定が適用されます（存在する場合）。
   - オブジェクトまたはバケットに保持設定が指定されていない場合、オブジェクトはS3オブジェクトロックによって保護されません。

   保持設定が適用されている場合は、オブジェクトとS3ユーザ定義メタデータの両方が保護されます。

2. オブジェクトの保持と削除

   指定した保持期間中、各保護オブジェクトの複数のコピーがStorageGRID によって格納されます。オブジェクトコピーの正確な数、タイプ、格納場所は、アクティブなILMポリシーの準拠ルールによって決まります。retain-until-dateに達する前に保護オブジェクトを削除できるかどうかは、保持モードによって異なります。

   - オブジェクトがリーガルホールドの対象である場合、保持モードに関係なく、誰もオブジェクトを削除できません。

関連情報

- "S3 バケットを作成します。"
- "S3オブジェクトロックのデフォルトの保持期間を更新します"
- "S3 REST APIを使用してS3オブジェクトロックを設定します"

- "例 7 ： S3 オブジェクトロックの準拠 ILM ポリシー"

StorageGRID で **S3** オブジェクトロックを有効にする

オブジェクトデータの保存時に S3 テナントアカウントが規制要件に準拠する必要がある場合は、 StorageGRID システム全体で S3 オブジェクトのロックを有効にする必要があります。グローバルな S3 オブジェクトのロック設定を有効にすると、 S3 テナントユーザは S3 オブジェクトのロックでバケットとオブジェクトを作成および管理できるようになります。

開始する前に

- あなたはを持っています"rootアクセス権限"。
- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- S3オブジェクトロックのワークフローを確認し、考慮事項を理解しておきます。
- 有効なILMポリシーのデフォルトルールが準拠していることを確認しました。詳細については、"デフォルトの ILM ルールを作成します"を参照してください。

タスクの内容

テナントユーザが S3 オブジェクトのロックを有効にした新しいバケットを作成できるようにするには、グリッド管理者がグローバルな S3 オブジェクトロック設定を有効にする必要があります。この設定を有効にすると、無効にすることはできません。

S3オブジェクトロックを有効にした後、グリッド管理者はテナントユーザーが既存のバケットでS3オブジェクトロックを有効にすることを許可することもできます。グリッド管理者はこの設定を有効にした後、無効にすることができます。詳細については、"S3 Object Lock の要件"を参照してください。

S3オブジェクトロックのグローバル設定を有効にしたら、既存のテナントの準拠設定を確認します。この設定を有効にすると、S3オブジェクトロックのテナント単位の設定は、テナント作成時のStorageGRIDリリースによって異なります。

> グローバルコンプライアンス設定は非推奨です。以前のバージョンの StorageGRID を使用してこの設定を有効にした場合、S3 オブジェクトロック設定は自動的に有効になります。引き続き StorageGRID を使用して既存の準拠バケットの設定を管理できますが、新しい準拠バケットを作成することはできません。詳細については、 "ネットアップのナレッジベース： StorageGRID 11.5 でレガシー準拠バケットを管理する方法"を参照してください。

手順

1. 構成 > システム > **S3** オブジェクト ロック を選択します。

   S3 Object Lock Settings （ S3 オブジェクトロック設定）ページが表示されます。

2. StorageGRID システム全体で S3 オブジェクト ロックを有効にするには、**S3** オブジェクト ロックを有効にする を選択します。
3. 必要に応じて、既存のバケットで **S3 Object Lock** を有効にする を選択します。

既存のバケットで S3 オブジェクト ロックを有効にすると、ILM ルールによっては、クラウド ストレージ プールから StorageGRID への意図しないデータ移行が発生する可能性があります。移行が開始されると、この移行を停止することはできません。詳細については、"S3 Object Lock の要件"を参照してください。

4. * 適用 * を選択します。

   確認のダイアログボックスが表示され、S3オブジェクトロックを有効にすると無効にできないことを示すメッセージが表示されます。

5. システム全体に対して S3 オブジェクトロックを永続的に有効にしてもよろしいですか？ * OK * を選択します。

   「 * OK * 」を選択した場合：

   - アクティブなILMポリシーのデフォルトルールが準拠ルールの場合、S3オブジェクトロックはグリッド全体で有効になり、無効にすることはできません。
   - デフォルトルールが準拠していない場合、エラーが表示されます。準拠ルールをデフォルトルールとして含む新しい ILM ポリシーを作成して有効化する必要があります。「OK」を選択します。次に、新しいポリシーを作成し、シミュレーションを実行してから、有効化します。手順については、"ILM ポリシーを作成する"を参照してください。

StorageGRIDで**S3 Object Lock**またはレガシーコンプライアンス設定を更新する際の整合性エラーを解決する

データセンターサイトまたはサイトの複数のストレージノードが使用できなくなった場合は、 S3 テナントユーザが S3 オブジェクトロックまたは従来の準拠設定に変更を適用できるよう支援する必要があります。

S3 オブジェクトロック（または従来の準拠）が有効になっているバケットを使用するテナントユーザは、特定の設定を変更できます。たとえば、 S3 オブジェクトロックを使用するテナントユーザがオブジェクトのバージョンをリーガルホールドの対象にする必要がある場合があります。

テナントユーザが S3 バケットまたはオブジェクトバージョンの設定を更新すると、 StorageGRID はグリッド全体ですぐにバケットまたはオブジェクトメタデータを更新します。データセンターサイトまたは複数のストレージノードを使用できないためにメタデータを更新できない場合は、次のエラーが返されます。

```
503: Service Unavailable
Unable to update compliance settings because the settings can't be
consistently applied on enough storage services. Contact your grid
administrator for assistance.
```

このエラーを解決するには、次の手順を実行します。

1. できるだけ早く、すべてのストレージノードまたはサイトを利用できる状態に戻します。
2. 各サイトで十分な数のストレージノードを利用可能にできない場合は、テクニカルサポートに問い合わせて、ノードをリカバリし、変更がグリッド全体に一貫して適用されるようにしてください。
3. 基盤となる問題 が解決されたら、テナントユーザに設定の変更を再試行するよう通知してください。

関連情報

- "テナントアカウントを使用する"
- "S3 REST APIを使用する"
- "リカバリとメンテナンス"

ILM ルールとポリシーの例

StorageGRID での基本的なオブジェクトの保護と保持に関する **ILM** ルールとポリシー

以下に記載するサンプルルールとポリシーをベースに、それぞれのオブジェクトの保護および保持要件を満たす ILM ポリシーを定義できます。

以下の ILM ルールとポリシーは一例にすぎません。ILM ルールを設定する方法は多数あります。新しいポリシーをアクティブ化する前に、ポリシーをシミュレートして、コンテンツを損失から保護するために意図したとおりに機能することを確認します。

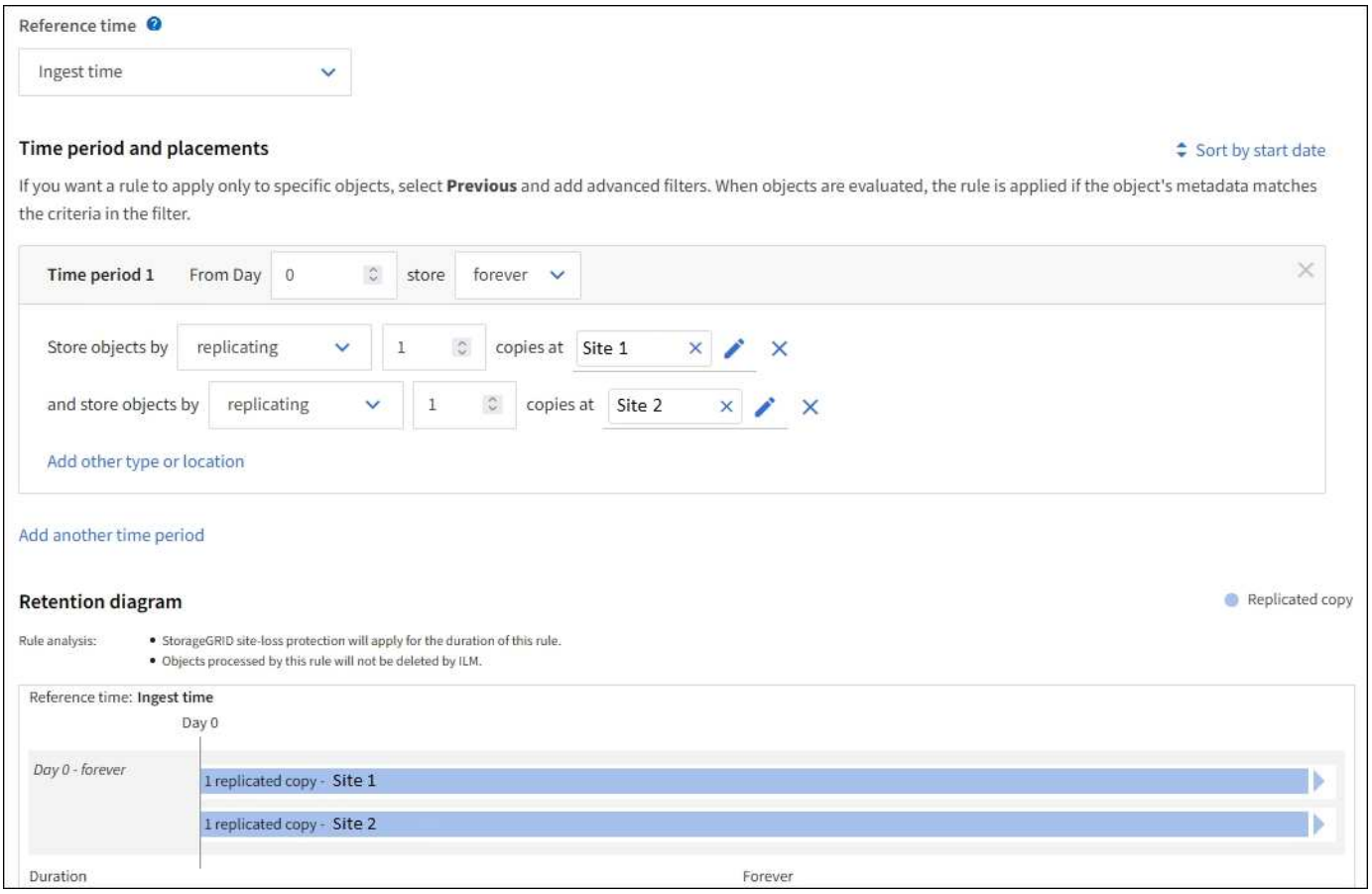
例**1**の**ILM**ルール**1**：オブジェクトデータを**2**つのサイトにコピーします

このILMルールの例では、オブジェクトデータを2つのサイトのストレージプールにコピーします。

ルール定義	値の例
1サイトのストレージプール	サイト1とサイト2という名前の異なるサイトをそれぞれ含む2つのストレージプール。
ルール名	2つのサイトをコピーします
参照時間	取り込み時間
配置	0日目から無期限に、レプリケートコピーを1つサイト1に、レプリケートコピーを1つサイト2に保持します。

保持図の規則解析セクションには'次のような情報が表示されます

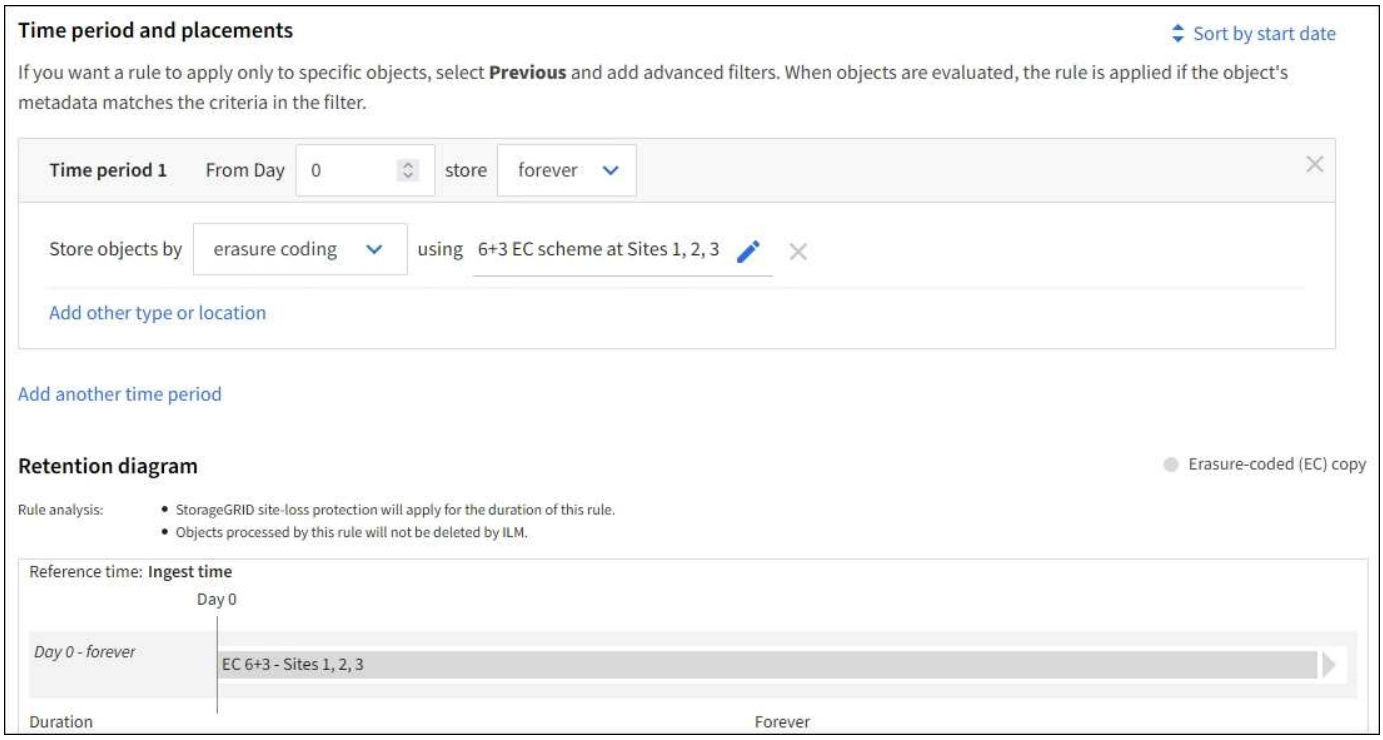
- このルールの期間中は、StorageGRID サイト障害からの保護が適用されます。
- このルールで処理されたオブジェクトはILMで削除されません。



例**1**の**ILM**ルール**2**：イレイジャーコーディングプロファイルとバケットの照合

このILMルールの例では、イレイジャーコーディングプロファイルとS3バケットを使用して、オブジェクトの格納場所と格納期間を決定します。

ルール定義	値の例
複数のサイトで構成されるストレージプール	• 3つのサイトにまたがる1つのストレージプール（サイト1、2、3） • 6+3 イレイジャーコーディングスキームを使用
ルール名	S3 Bucket finance-recordsの略
参照時間	取り込み時間
配置	finance-recordsというS3バケット内のオブジェクトに対して、イレイジャーコーディングコピーをイレイジャーコーディングプロファイルで指定されたプールに1つ作成します。このコピーを無期限に保持します。

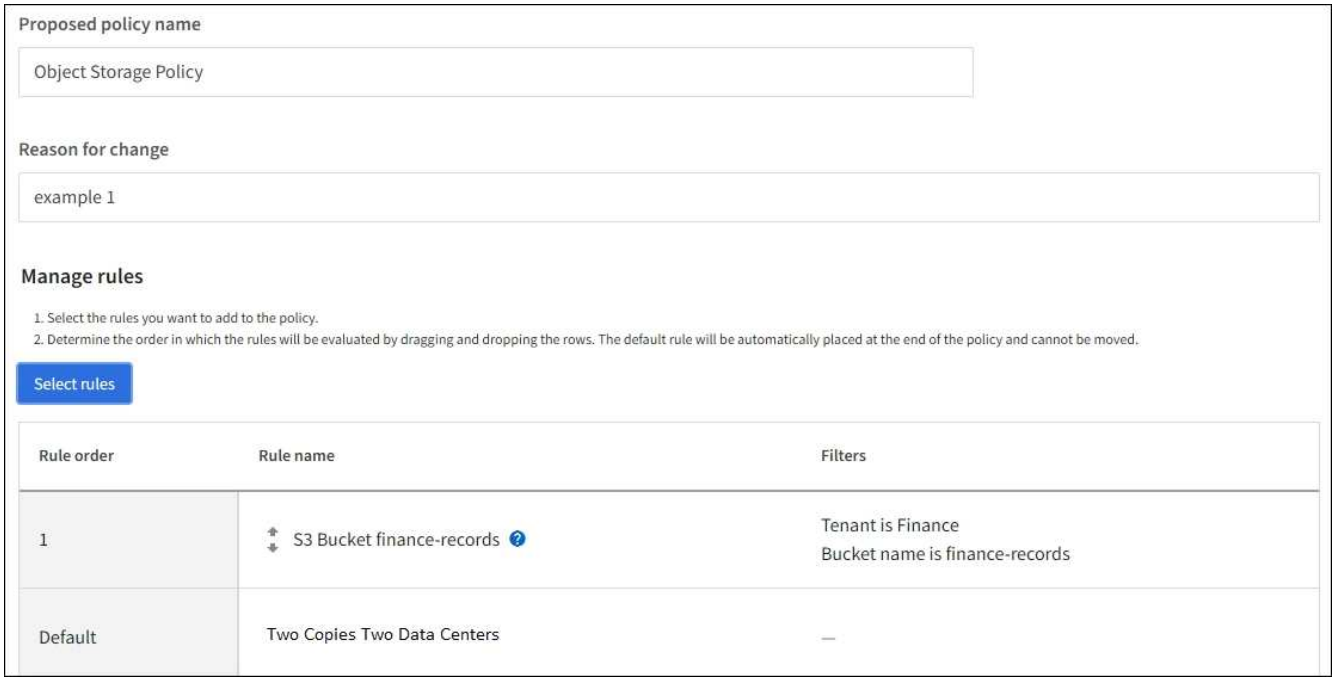


例**1**の**ILM**ポリシー

実際には、StorageGRID システムでは高度で複雑なILMポリシーを設計できますが、ほとんどのILMポリシーはシンプルです。

マルチサイトグリッドの一般的なILMポリシーには、次のようなILMルールが含まれます。

- 取り込み時に、という名前のS3バケットに属するすべてのオブジェクトを、3つのサイトを含むストレージプールに格納します `finance-records`。6+3のイレイジャーコーディングを使用します。
- オブジェクトが最初のILMルールに一致しない場合は、ポリシーのデフォルトのILMルール（2つのコピーが2つのデータセンター）を使用して、そのオブジェクトのコピーをサイト1に1つ、サイト2に1つ格納します。



関連情報

- "ILMポリシーを使用する"
- "ILMポリシーの作成"

StorageGRIDにおける**EC**オブジェクトサイズフィルタリングの**ILM**ルールとポリシー

以下に記載するサンプルルールとポリシーをベースに、オブジェクトサイズでフィルタリングして EC の推奨要件を満たす ILM ポリシーを定義できます。

以下の ILM ルールとポリシーは一例にすぎません。ILM ルールを設定する方法は多数あります。新しいポリシーをアクティブ化する前に、ポリシーをシミュレートして、コンテンツを損失から保護するために意図したとおりに機能することを確認します。

例 **2** の **ILM** ルール **1** ： **1MB** を超えるオブジェクトに **EC** を使用します

この ILM ルールの例では、 1MB を超えるオブジェクトをイレイジャーコーディングします。

イレイジャーコーディングは 1MB を超えるオブジェクトに適しています。非常に小さいイレイジャーコーディングフラグメントを管理するオーバーヘッドを回避するために、200KB未満のオブジェクトにはイレイジャーコーディングを使用しないでください。

ルール定義	値の例
ルール名	EC Only Objects > 1MB
参照時間	取り込み時間
オブジェクトサイズの高度なフィルタ	オブジェクトサイズが1MBを超えています

ルール定義	値の例
配置	3 つのサイトを使用して 2+1 のイレイジャーコーディングコピーを作成



例 **2** の **ILM** ルール **2** ：レプリケートされたコピーを **2** つ

この ILM ルールの例では、レプリケートコピーを 2 つ作成し、オブジェクトサイズではフィルタリングしません。このルールはポリシーのデフォルトルールです。最初のルールでは 1MB を超えるすべてのオブジェクトがフィルタリングされるため、このルールで使用できるのは 1MB 以下の環境 オブジェクトのみです。

ルール定義	値の例
ルール名	2 つのレプリケートコピー
参照時間	取り込み時間
オブジェクトサイズの高度なフィルタ	なし
配置	0日目から無期限に、レプリケートコピーを1つサイト1に、レプリケートコピーを1つサイト2に保持します。

例 **2** の **ILM** ポリシー： **1MB** を超えるオブジェクトに **EC** を使用します

この例の ILM ポリシーには 2 つの ILM ルールが含まれています。

- 最初のルールでは、 1MB を超えるすべてのオブジェクトをイレイジャーコーディングします。
- 2 つ目の（デフォルトの） ILM ルールによって、レプリケートコピーが 2 つ作成されます。1MB を超えるオブジェクトはルール 1 でフィルタリングされているため、ルール 2 では 1MB 以下の環境 オブジェクトのみが除外されます。

StorageGRIDで画像ファイルを保護するための**ILM**ルールとポリシー

次の例のルールとポリシーを使用して、1MBを超えるイメージがイレイジャーコーディングされ、2つのコピーが小さいイメージで作成されるようにすることができます。

以下の ILM ルールとポリシーは一例にすぎません。ILM ルールを設定する方法は多数あります。新しいポリシーをアクティブ化する前に、ポリシーをシミュレートして、コンテンツを損失から保護するために意図したとおりに機能することを確認します。

例 3 の ILM ルール 1 ： 1MB を超える画像ファイルに EC を使用します

この ILM ルールの例では、高度なフィルタリングを使用して、 1MB を超えるすべてのイメージファイルをイレイジャーコーディングします。

> イレイジャーコーディングは 1MB を超えるオブジェクトに適しています。非常に小さいイレイジャーコーディングフラグメントを管理するオーバーヘッドを回避するために、200KB未満のオブジェクトにはイレイジャーコーディングを使用しないでください。

ルール定義	値の例
ルール名	ECイメージファイルが1MBを超えています
参照時間	取り込み時間
オブジェクトサイズの高度なフィルタ	オブジェクトサイズが1MBを超えています
キーの高度なフィルタ	• 末尾は.jpgです • 末尾は.pngです
配置	3 つのサイトを使用して 2+1 のイレイジャーコーディングコピーを作成



このルールはポリシー内の最初のルールとして設定されているため、イレイジャーコーディング配置手順には1MBを超える環境 の.jpgファイルと.pngファイルのみが含まれます。

例 3 の ILM ルール 2 ：残りのすべてのイメージファイルに対してレプリケートコピーを 2 つ作成します

この ILM ルールの例では、高度なフィルタリングを使用して、より小さなイメージファイルをレプリケートするように指定します。ポリシーの最初のルールは 1MB より大きい画像ファイルにすでに一致しているため、このルールは 1MB 以下の環境 画像ファイルを示します。

ルール定義	値の例
ルール名	イメージファイル用に2コピー
参照時間	取り込み時間
キーの高度なフィルタ	• 末尾は.jpgです • 末尾は.pngです
配置	2つのストレージプールにレプリケートコピーを2つ作成します

例 **3** の **ILM** ポリシー：画像ファイルの保護の強化

この例の ILM ポリシーには 3 つのルールが含まれています

- 最初のルールのイレイジャーコーディングでは、 1MB を超えるすべてのイメージファイルをイレイジャーコーディングします。
- 2 番目のルールは、残りのすべてのイメージファイル（ 1MB 以下のイメージ）のコピーを 2 つ作成します。
- デフォルトルールでは、残りのすべてのオブジェクト（画像以外のファイル）が環境 されます。

Rule order	Rule name	Filters
1	EC image files > 1 MB	Object size is greater than 1 MB
2	2 copies for small images	Object size is less than or equal to 200 KB
Default	Default rule	—

StorageGRIDにおける**S3**オブジェクトの非最新バージョンに対する**ILM**ルールとポリシー

バージョン管理が有効なS3バケットでは、参照時間として「noncurrent time」を使用するルールをILMポリシーに含めることで、最新でないオブジェクトバージョンを管理できます。

制限された保持期間を指定したオブジェクトは、指定した期間の経過後に完全に削除されます。オブジェクトが保持される期間を確認してください。

この例に示すように、バージョン管理オブジェクトで使用されるストレージの量を制御するには、最新でないオブジェクトバージョンに別々の配置手順を使用します。

以下の ILM ルールとポリシーは一例にすぎません。ILM ルールを設定する方法は多数あります。新しいポリシーをアクティブ化する前に、ポリシーをシミュレートして、コンテンツを損失から保護するために意図したとおりに機能することを確認します。

最新でないバージョンのオブジェクトに対してILMポリシーのシミュレーションを実行するには、オブジェクトバージョンのUUIDまたはCBIDを確認しておく必要があります。UUIDとCBIDを確認するには、オブジェクトが最新の状態でを使用します"オブジェクトメタデータの検索"。

例 **4** の **ILM** ルール **1** ：コピーを **3** つ、 **10** 年間保存します

この例のILMルールでは、各オブジェクトのコピーが3つのサイトに10年間格納されます。

このルールは、オブジェクトがバージョン管理されているかどうかに関係なく、すべてのオブジェクトを環境します。

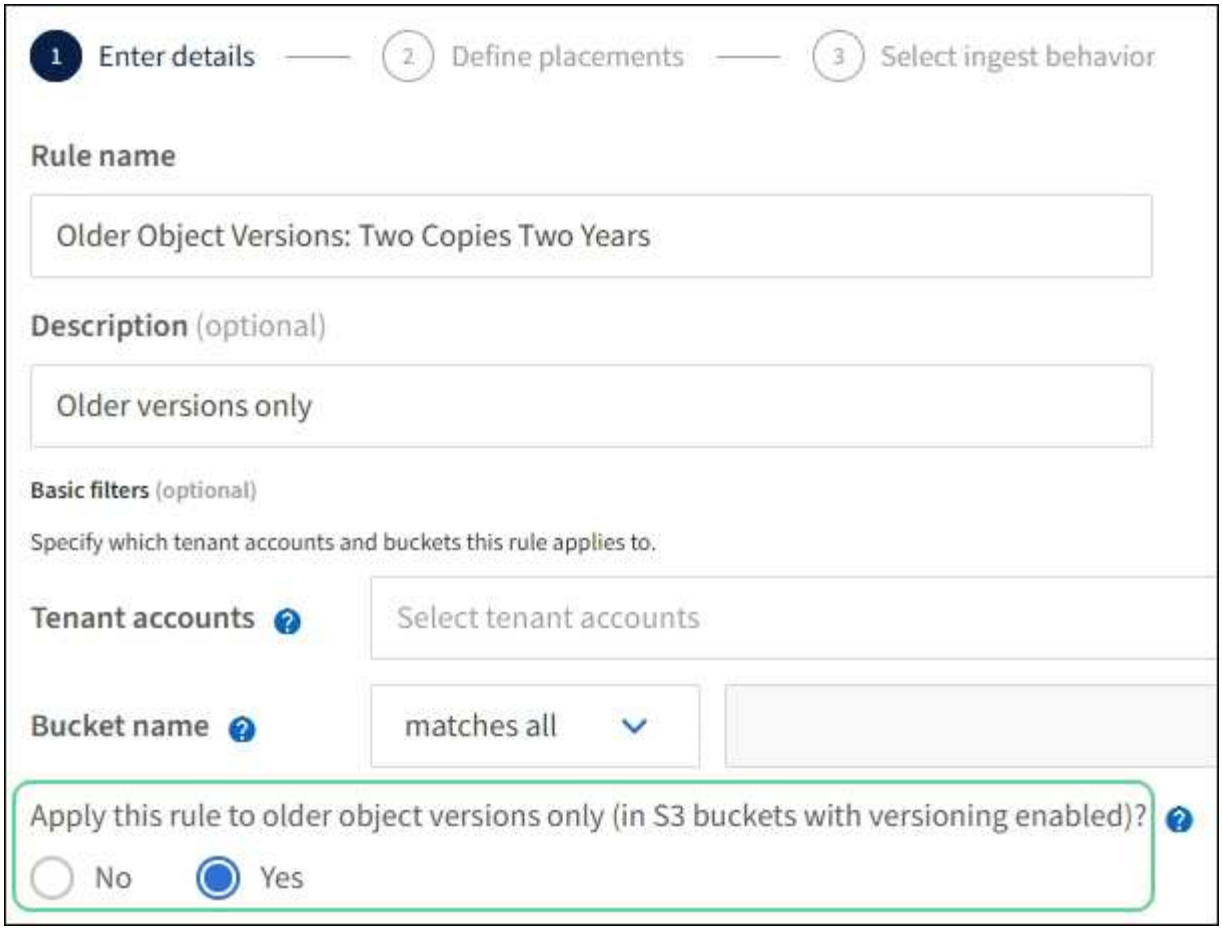
ルール定義	値の例
ストレージプール	サイト1、サイト2、サイト3という名前の異なるデータセンターで構成される3つのストレージプール。
ルール名	3 つのコピー 10 年
参照時間	取り込み時間
配置	0日目から、3つのレプリケートコピーを10年間（3、652日）（サイト1に1つ、サイト2に1つ、サイト3に1つ）保存します。10 年後にオブジェクトのコピーをすべて削除する。

例 **4** の **ILM** ルール **2** ：最新でないバージョンのコピーを **2** つ、 **2** 年間保存します

この例では、最新でないバージョンの S3 バージョン管理オブジェクトのコピーを 2 つ、 2 年間格納します。

ILM ルール 1 ではすべてのバージョンのオブジェクトが環境 されるため、最新でないバージョンをすべて除外する別のルールを作成する必要があります。

「noncurrent time」を参照時間として使用するルールを作成するには、「Apply this rule to older object versions only（S3バケットでバージョン管理が有効になっている場合）？」で* Yes を選択します。 **[Create an ILM rule]**ウィザードの**[Step 1（Enter details）]**で、 Yes *を選択すると、参照時間として_noncurrent time_が自動的に選択され、別の参照時間を選択することはできません。



この例では、最新でないバージョンのコピーが 2 つだけ格納され、その期間は 2 年間です。

ルール定義	値の例
ストレージプール	2つのストレージプールがそれぞれ異なるデータセンター（サイト1とサイト2）にある。
ルール名	最新でないバージョン： 2 コピー 2 年
参照時間	最新でない時間 「Apply this rule to older object versions only（S3バケットでバージョン管理が有効になっている場合）？」という質問で* Yes *を選択すると、自動的に選択されます。 Create an ILM Ruleウィザードを使用します。
配置	最新でない時間に対して（オブジェクトバージョンが最新でなくなった日から）0日目に、最新でないオブジェクトバージョンのレプリケートコピーを2つ（サイト1に1つ、サイト2に1つ）2年間（730日）保持します。2 年後に最新でないバージョンを削除します。

例 **4** の **ILM** ポリシー： **S3** バージョン管理オブジェクト

古いバージョンのオブジェクトを現在のバージョンとは異なる方法で管理する場合は、ILMポリシーで参照時

間に「noncurrent time」を使用するルールを、現在のオブジェクトバージョンに適用されるルールの前に配置する必要があります。

S3 バージョン管理オブジェクトの ILM ポリシーには、次のような ILM ルールが含まれます。

- 古い（最新でない）バージョンの各オブジェクトを、そのバージョンが最新でなくなった日から 2 年間保持します。

> 「noncurrent time」ルールは、ポリシー内で現在のオブジェクトバージョンに適用されるルールの前に配置する必要があります。そうしないと、最新でないオブジェクトバージョンが「noncurrent time」ルールに一致しなくなります。

- 取り込み時に、レプリケートコピーを3つ作成し、3つのサイトそれぞれに1つのコピーを格納します。最新のオブジェクトバージョンのコピーを 10 年間保持します。

この例のポリシーをシミュレートすると、テストオブジェクトは次のように評価されます。

- 最新でないオブジェクトバージョンがすべて最初のルールに一致します。最新でないオブジェクトバージョンが 2 年以上経過している場合は、 ILM によって完全に削除されます（最新でないバージョンのコピーがすべてグリッドから削除されます）。
- 現在のオブジェクトバージョンが 2 つ目のルールに一致します。現在のオブジェクトバージョンが10年間格納されている場合、ILMプロセスはオブジェクトの現在のバージョンとして削除マーカーを追加し、以前のオブジェクトバージョンを「noncurrent」にします。次回のILM評価では、この最新でないバージョンが最初のルールに一致します。その結果、サイト3のコピーがパージされ、サイト1とサイト2の2つのコピーがさらに2年間格納されます。

関連情報

"オブジェクトの削除方法"

StorageGRID の厳格な取り込み動作に関する **ILM** ルールとポリシー

ルールで場所フィルタと Strict 取り込み動作を使用すると、特定のデータセンターの場所にオブジェクトが保存されないようにすることができます。

この例では、規制上の問題により、パリベースのテナントは EU の外部に一部のオブジェクトを格納しないようにしています。他のテナントアカウントのすべてのオブジェクトを含むその他のオブジェクトは、パリデータセンターまたは米国のデータセンターに格納できます。

> 以下の ILM ルールとポリシーは一例にすぎません。ILM ルールを設定する方法は多数あります。新しいポリシーをアクティブ化する前に、ポリシーをシミュレートして、コンテンツを損失から保護するために意図したとおりに機能することを確認します。

関連情報

- "取り込みオプション"
- "Create ILM rule：取り込み動作を選択します"

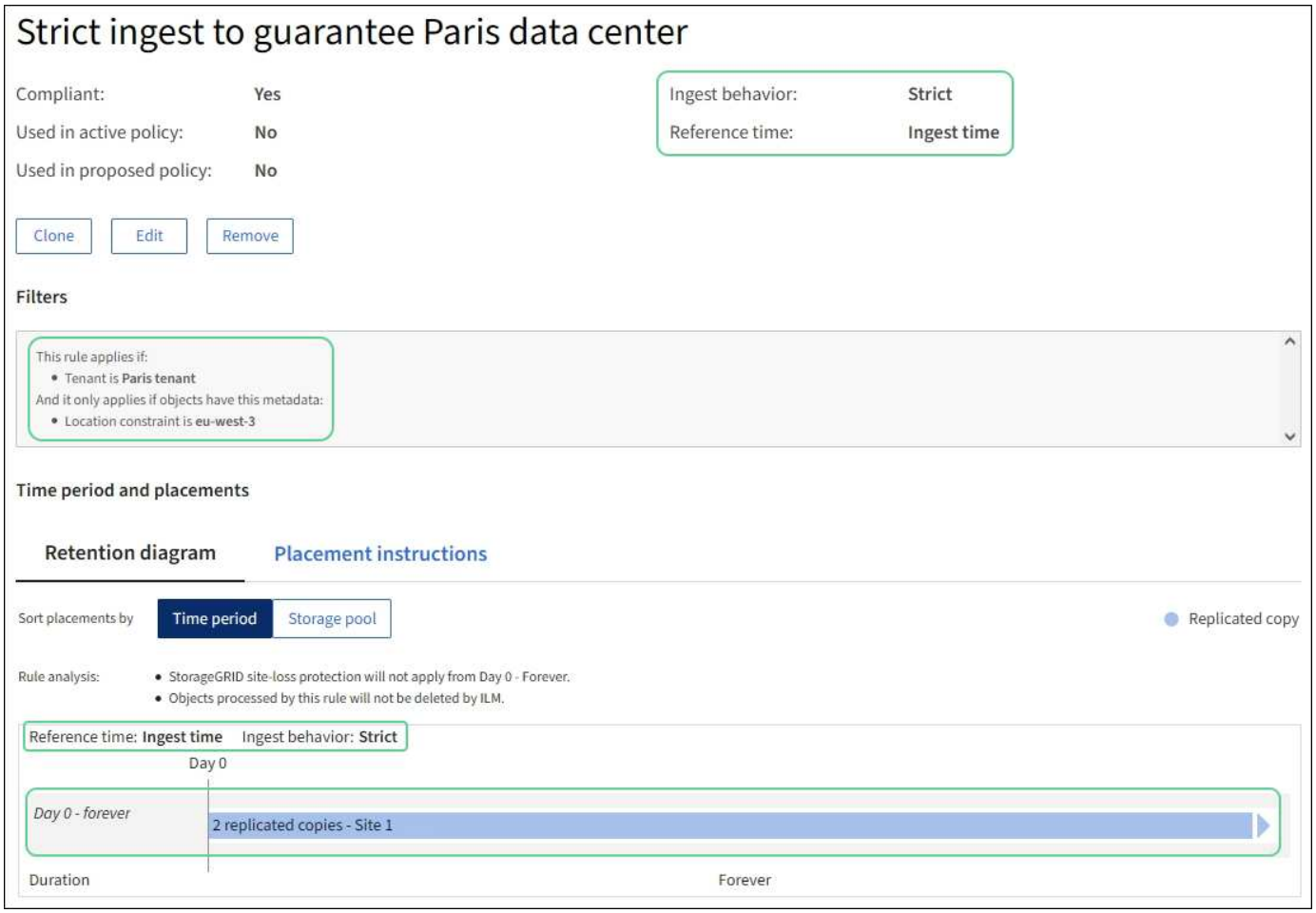
例 **5** の **ILM** ルール **1** ：パリデータセンターを確保するための **Strict** 取り込み

この ILM ルールの例では Strict 取り込み動作を使用して、パリベースのテナントによって S3 バケットに保存されたオブジェクトのリージョンが eu-west-3 リージョン（パリ）に設定されたものが米国のデータセンター

に格納されないようにします。

このルールは、パリテナントに属し、 S3 バケットリージョンが eu-west-3 （パリ）に設定されている環境 オブジェクトを示します。

ルール定義	値の例
テナントアカウント	パリのテナント
高度なフィルタ	ロケーションの制約はeu-west-3に等しくなります
ストレージプール	サイト1（パリ）
ルール名	厳格な取り込みにより、パリのデータセンターを保証します
参照時間	取り込み時間
配置	0日目から2つのレプリケートコピーをサイト1（パリ）に無期限に格納
取り込み動作	厳しい取り込み時に必ずこのルールの配置手順を使用してください。パリデータセンターにオブジェクトのコピーを 2 つ保存できない場合、取り込みは失敗します。



例 **5** の **ILM** ルール **2** ：他のオブジェクトに対してバランスのとれた取り込み

この ILM ルールの例では、 Balanced 取り込み動作を使用して、最初のルールに一致しないオブジェクトの ILM 効率が最適化されます。このルールに一致するすべてのオブジェクトのコピーが 2 つ保存されます。 1 つは米国データセンターに、もう 1 つはパリデータセンターに格納されます。ルールをすぐに満たすことができない場合は、使用可能な任意の場所に中間コピーが格納されます。

このルールは、任意のテナントおよびすべてのリージョンに属する環境 オブジェクトを対象としています。

ルール定義	値の例
テナントアカウント	無視
高度なフィルタ	_ 指定されていません _
ストレージプール	サイト1（パリ）およびサイト2（米国）
ルール名	2 つのコピーで 2 つのデータセンター
参照時間	取り込み時間
配置	0 日目から、 2 つのレプリケートコピーを 2 つのデータセンターに無期限に格納します
取り込み動作	中間（ Balanced ）：このルールに一致するオブジェクトは、可能であればルールの配置手順に従って配置されます。それ以外の場合、中間コピーは任意の空き場所で作成されます。

例 **5** の **ILM** ポリシー：取り込み動作を組み合わせたもの

この例の ILM ポリシーには、取り込み動作が異なる 2 つのルールが含まれています。

2 つの異なる取り込み動作を使用する ILM ポリシーには、次のような ILM ルールが含まれる場合があります。

- パリのテナントに属し、かつ S3 バケットリージョンがパリのデータセンター内でのみ eu-west-3 （パリ）に設定されているオブジェクトを格納します。パリのデータセンターが利用できない場合は取り込みに失敗します。
- その他のすべてのオブジェクト（パリテナントに属しているものの、バケットリージョンが異なるオブジェクトを含む）は、米国のデータセンターとパリのデータセンターの両方に保存します。配置手順を満たすことができない場合は、使用可能な任意の場所に中間コピーを作成します。

この例のポリシーをシミュレートすると、テストオブジェクトは次のように評価されます。

- パリのテナントに属し、 S3 バケットリージョンが eu-west-3 に設定されているオブジェクトはすべて最初のルールに一致し、パリのデータセンターに格納されます。最初のルールでは Strict 取り込みが使用されるため、これらのオブジェクトが米国のデータセンターに格納されることはありません。パリのデータセンターのストレージノードを使用できない場合、取り込みは失敗します。
- その他のオブジェクト（パリのテナントに属するオブジェクトでS3バケットのリージョンがeu-west-3に

設定されていないオブジェクトを含む）はすべて2つ目のルールに一致します。各オブジェクトのコピーが各データセンターに 1 つずつ保存されます。ただし、 2 つ目のルールでは Balanced ing(バランスの取れた取り込み) が使用されるため、 1 つのデータセンターが使用できない場合は、使用可能な任意の場所に 2 つの中間コピーが保存されます。

ILMポリシーの変更が**StorageGRID**パフォーマンスに及ぼす影響

データ保護の変更や新しいサイトの追加が必要な場合は、新しいILMポリシーを作成してアクティブ化できます。

ポリシーを変更する前に、 ILM の配置変更が一時的に StorageGRID システムの全体的なパフォーマンスに及ぼす影響について理解しておく必要があります。

この例では、拡張時に新しいStorageGRID サイトが追加されたため、新しいサイトにデータを格納するために新しいアクティブなILMポリシーを実装する必要があります。新しいアクティブポリシーを実装するには、まず最初に"ポリシーを作成します。"実行します。その後、 "アクティブ化"新しいポリシーを実行する必要があります"シミュレートします"。

以下の ILM ルールとポリシーは一例にすぎません。ILM ルールを設定する方法は多数あります。新しいポリシーをアクティブ化する前に、ポリシーをシミュレートして、コンテンツを損失から保護するために意図したとおりに機能することを確認します。

ILMポリシーの変更がパフォーマンスに与える影響

新しい ILM ポリシーをアクティブ化すると、特に新しいポリシーの配置手順で多数の既存オブジェクトの新しい場所への移動が必要になった場合には、 StorageGRID システムのパフォーマンスに一時的に影響する可能性があります。

新しい ILM ポリシーをアクティブ化すると、 StorageGRID は、そのポリシーを使用して、既存のオブジェクトと新たに取り込まれたオブジェクトを含むすべてのオブジェクトを管理します。新しい ILM ポリシーをアクティブ化する前に、既存のレプリケートオブジェクトとイレイジャーコーディングオブジェクトの配置に対する変更を確認してください。既存のオブジェクトの場所を変更すると、新しい配置が評価されて実装される際に一時的なリソースの問題が発生する可能性があります。

新しいILMポリシーが既存のレプリケートオブジェクトとイレイジャーコーディングオブジェクトの配置に影響しないようにすることができます"取り込み時間フィルタを使用してILMルールを作成する"。たとえば、*取り込み時間_が___<date and time> _*以降であるため、新しいルールは指定した日時以降に取り込まれたオブジェクトにのみ適用されます。

StorageGRID のパフォーマンスに一時的に影響する可能性がある ILM ポリシーの変更には、次のようなものがあります。

- 既存のイレイジャーコーディングオブジェクトに別のイレイジャーコーディングプロファイルを適用する。

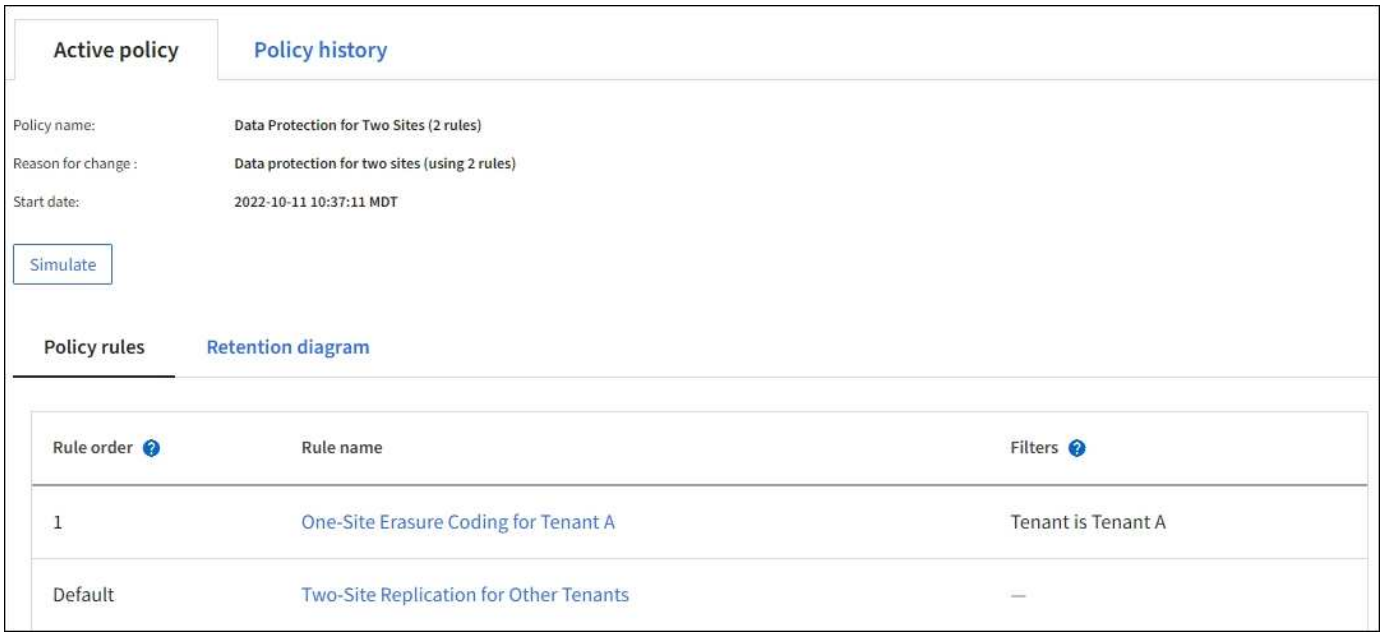
  StorageGRIDでは、イレイジャーコーディングプロファイルはそれぞれ一意であるとみなされ、新しいプロファイルの使用時にイレイジャーコーディングフラグメントは再利用されません。

- 既存のオブジェクトに必要なコピーのタイプを変更する。たとえば、大部分のレプリケートオブジェクトをイレイジャーコーディングオブジェクトに変換する場合などです。

- 既存のオブジェクトのコピーをまったく別の場所に移動する。たとえば、クラウドストレージプールとリモートサイトの間で多数のオブジェクトを移動する場合などです。

例 **6** のアクティブな **ILM** ポリシー： **2** つのサイトでのデータ保護

この例では、アクティブな ILM ポリシーは最初に 2 サイトの StorageGRID システム用に設計され、 2 つの ILM ルールを使用しています。



この ILM ポリシーでは、テナント A に属するオブジェクトが 1 つのサイトで 2+1 のイレイジャーコーディングによって保護され、一方他のすべてのテナントに属するオブジェクトは 2-copy レプリケーションを使用して 2 つのサイト間で保護されます。

ルール **1** ：テナント **A** に **1** つのサイトのイレイジャーコーディング

ルール定義	値の例
ルール名	テナント A の 1 サイトのイレイジャーコーディング
テナントアカウント	テナントA
ストレージプール	サイト1
配置	2+1のイレイジャーコーディングをサイト1に格納し、0日目から無期限に格納します

ルール **2** ：他のテナントに **2** つのサイトをレプリケートする

ルール定義	値の例
ルール名	他のテナント用の 2 サイトレプリケーション

ルール定義	値の例
テナントアカウント	無視
ストレージプール	サイト1とサイト2
配置	2つのレプリケートコピーを0日目から無期限に（サイト1に1つ、サイト2に1つ）

例6のILMポリシー：3サイトでのデータ保護

この例では、3サイトのStorageGRID システムのILMポリシーが新しいポリシーに置き換えられています。

拡張を実行して新しいサイトを追加したあと、グリッド管理者は2つの新しいストレージプールを作成しました。1つはサイト3のストレージプールで、もう1つは3つのサイトすべてを含むストレージプールです（デフォルトの[All Storage Nodes]ストレージプールとは異なります）。次に、2つの新しいILMルールと1つの新しいILMポリシーを作成しました。このポリシーは、3つのサイトすべてのデータを保護するように設計されています。

この新しい ILM ポリシーがアクティブ化されると、テナント A に属するオブジェクトが 3 つのサイトで 2+1 イレイジャーコーディングによって保護され、他のテナント（およびテナント A に属する小さいオブジェクト）に属するオブジェクトは 3 つのサイト間で 3 コピーレプリケーションによって保護されるようになります。

ルール **1** ：テナント **A** に **3** サイトイレイジャーコーディング

ルール定義	値の例
ルール名	テナント A の 3 サイトイレイジャーコーディング
テナントアカウント	テナントA
ストレージプール	3つのサイトすべて（サイト1、サイト2、サイト3を含む）
配置	2+1のイレイジャーコーディングを3つのサイトすべてに0日目から無期限に格納

ルール **2** ：他のテナントに **3** つのサイトをレプリケーションする

ルール定義	値の例
ルール名	他のテナント用に 3 つのサイトにレプリケーション
テナントアカウント	無視
ストレージプール	サイト1、サイト2、およびサイト3

ルール定義	値の例
配置	3つのレプリケートコピーを0日目から無期限に（サイト1に1つ、サイト2に1つ、サイト3に1つ）

例6のILMポリシーのアクティブ化

新しいILMポリシーをアクティブ化すると、新規または更新されたルールの配置手順に基づいて、既存のオブジェクトが新しい場所に移動されたり、既存のオブジェクト用の新しいオブジェクトコピーが作成されたりすることがあります。

原因 ポリシーにエラーがあると、回復不能なデータ損失が発生する可能性があります。ポリシーをアクティブ化する前によく確認およびシミュレートし、想定どおりに機能することを確認してください。

新しい ILM ポリシーをアクティブ化すると、 StorageGRID は、そのポリシーを使用して、既存のオブジェクトと新たに取り込まれたオブジェクトを含むすべてのオブジェクトを管理します。新しい ILM ポリシーをアクティブ化する前に、既存のレプリケートオブジェクトとイレイジャーコーディングオブジェクトの配置に対する変更を確認してください。既存のオブジェクトの場所を変更すると、新しい配置が評価されて実装される際に一時的なリソースの問題が発生する可能性があります。

イレイジャーコーディングの手順が変わったときの動作

この例の現在アクティブなILMポリシーでは、テナントAに属するオブジェクトがサイト1で2+1のイレイジャーコーディングを使用して保護されています。新しいILMポリシーでは、テナントAに属するオブジェクトを、サイト1、2、3で2+1のイレイジャーコーディングを使用して保護します。

新しい ILM ポリシーがアクティブ化されると、次の ILM 処理が実行されます。

- テナント A で取り込まれた新しいオブジェクトは 2 つのデータフラグメントに分割され、 1 つのパリティフラグメントが追加される。その後、3つのフラグメントそれぞれが別 々 のサイトに格納されます。
- テナント A に属する既存のオブジェクトは、実行中の ILM スキャンプロセスで再評価されます。ILMの配置手順では新しいイレイジャーコーディングプロファイルを使用するため、まったく新しいイレイジャーコーディングフラグメントが作成されて3つのサイトに分散されます。

サイト1の既存の2+1フラグメントは再利用されません。StorageGRIDでは、イレイジャーコーディングプロファイルはそれぞれ一意であるとみなされ、新しいプロファイルの使用時にイレイジャーコーディングフラグメントは再利用されません。

レプリケーション手順が変わったときの動作

この例の現在アクティブなILMポリシーでは、他のテナントに属するオブジェクトが、サイト1と2のストレージプールに2つのレプリケートコピーを格納して保護されます。新しいILMポリシーでは、他のテナントに属するオブジェクトを、サイト1、2、3のストレージプールに3つのレプリケートコピーを格納して保護します。

新しい ILM ポリシーがアクティブ化されると、次の ILM 処理が実行されます。

- テナントA以外のテナントが新しいオブジェクトを取り込むと、StorageGRID はコピーを3つ作成して各サイトに1つずつ保存します。
- それらの他のテナントに属する既存のオブジェクトは、 ILM のスキャンプロセスの実行中に再評価されます。サイト1とサイト2の既存のオブジェクトコピーは新しいILMルールのレプリケーション要件を満たしているため、StorageGRID ではサイト3用にオブジェクトの新しいコピーを1つ作成するだけで済みます。

このポリシーをアクティブ化した場合のパフォーマンスへの影響

この例のILMポリシーをアクティブ化すると、このStorageGRIDシステムの全体的なパフォーマンスが一時的に低下します。テナントAの既存オブジェクト用に新しいイレイジャーコーディングフラグメントを作成し、他のテナントの既存オブジェクト用にサイト3にレプリケートコピーを作成するには、通常よりも多くのグリッドリソースが必要になります。

ILM ポリシーが変更されたため、クライアントの読み取り要求と書き込み要求が一時的に通常よりもレイテンシが高くなる可能性があります。配置手順がグリッド全体に完全に実装されたあと、レイテンシは通常レベルに戻ります。

新しいILMポリシーをアクティブ化する際のリソースの問題を回避するために、大量の既存オブジェクトの場所を変更する可能性があるルールでは、高度なフィルタの取り込み時間を使用できます。新しいポリシーが有効になるおおよその時間以上に取り込み時間を設定して、既存のオブジェクトが不要に移動されないようにします。

ILM ポリシーの変更後にオブジェクトが処理される速度を遅くしたり、上げたりする必要がある場合は、テクニカルサポートにお問い合わせください。

StorageGRID での **S3** オブジェクトロックの準拠 **ILM** ポリシー

S3 オブジェクトのロックが有効なバケット内のオブジェクトの保護および保持の要件を満たす ILM ポリシーを定義する際は、以下の例の S3 バケット、 ILM ルール、 ILM ポリシーをベースとして使用できます。

以前の StorageGRID リリースで従来の準拠機能を使用していた場合、この例を使用して、従来の準拠機能が有効になっている既存のバケットを管理することもできます。

以下の ILM ルールとポリシーは一例にすぎません。ILM ルールを設定する方法は多数あります。新しいポリシーをアクティブ化する前に、ポリシーをシミュレートして、コンテンツを損失から保護するために意図したとおりに機能することを確認します。

関連情報

- "S3 オブジェクトロックでオブジェクトを管理します"
- "ILMポリシーを作成します"

S3 オブジェクトのロックのバケットとオブジェクトの例

次の例では、 Bank of ABC という名前の S3 テナントアカウントで、 Tenant Manager を使用して、重要な銀行記録を格納するために S3 オブジェクトロックを有効にしたバケットを作成しています。

バケットの定義	値の例
テナントアカウント名	ABC 銀行
バケット名	銀行記録
バケットのリージョン	us-east-1 （デフォルト）

bank-recordsバケットに追加される各オブジェクトおよびオブジェクトバージョンでは、および `legal hold`の設定に次の値が使用され `retain-until-date`ます。

オブジェクトごとに設定します	値の例
`retain-until-date`	「2030-12-30T23：59：59Z」（2030年12月30日） 各オブジェクトバージョンには独自の設定があり `retain-until-date`ます。この設定は、上げることはできますが、下げることはできません。
`legal hold`	「オフ」（有効ではない） リーガルホールドは、保持期間中いつでも任意のオブジェクトバージョンに適用または解除できます。オブジェクトがリーガルホールドの対象になっている場合は、が到達してもオブジェクトを削除できません `retain-until-date`。

S3オブジェクトロックの**ILM**ルール**1**の例：イレイジャーコーディングプロファイルでバケットを照合

この例の ILM ルールは、 Bank of ABC という名前の S3 テナントアカウントのみに適用されます。バケット内の任意のオブジェクトに一致し、 `bank-records`イレイジャーコーディングを使用して、6+3のイレイジャーコーディングプロファイルを使用して3つのデータセンターサイトのストレージノードにオブジェクトを格納します。このルールは、S3オブジェクトロックを有効にしたバケットの要件を満たしています。つまり、取り込み時間を参照時間として使用して、コピーが0日目から無期限にストレージノードに保持されます。

ルール定義	値の例
ルール名	準拠ルール：bank-records Bucket内のECオブジェクト- Bank of ABC
テナントアカウント	ABC 銀行
バケット名	`bank-records`
高度なフィルタ	オブジェクトサイズ（MB）が1より大きい *注：このフィルタは、1MB以下のオブジェクトにイレイジャーコーディングが使用されないようにします。

ルール定義	値の例
参照時間	取り込み時間
配置	0 日目のストアから永遠に
イレイジャーコーディングプロファイル	• 3 つのデータセンターサイトのストレージノードにイレイジャーコーディングコピーを作成します • 6+3 イレイジャーコーディングスキームを使用

S3 オブジェクトのロックの例の **ILM** ルール **2** ：非準拠ルール

この例の ILM ルールでは、 2 つのレプリケートオブジェクトコピーをストレージノードに最初に格納します。1 年後、クラウドストレージプールに 1 つのコピーを無期限に格納します。このルールはクラウドストレージプールを使用するため、非準拠となり、 S3 オブジェクトロックが有効になっているバケット内のオブジェクトには適用されません。

ルール定義	値の例
ルール名	非準拠ルール：クラウドストレージプールを使用します
テナントアカウント	指定なし
バケット名	指定されていませんが、S3オブジェクトロック（または従来の準拠機能）が有効になっていないバケットにのみ適用されます。
高度なフィルタ	指定なし

ルール定義	値の例
参照時間	取り込み時間
配置	• 0 日目から、 2 つのレプリケートコピーをデータセンター 1 とデータセンター 2 のストレージノードに 365 日間格納します • 1 年後、レプリケートコピーを 1 つクラウドストレージプールに無期限に格納します

S3 オブジェクトのロックの例の **ILM** ルール **3** ：デフォルトルール

この ILM ルールの例では、 2 つのデータセンター内のストレージプールにオブジェクトデータをコピーします。この準拠ルールは、 ILM ポリシーのデフォルトルールとして設計されています。フィルタは含まれず、参照時間が最新でない状態を使用しません。また、 S3 オブジェクトロックが有効なバケットの要件を満たします。 2 つのオブジェクトコピーが 0 日目から無期限にストレージノードに保持され、参照時間として取り込みが使用されます。

ルール定義	値の例
ルール名	デフォルトの準拠ルール：2つのデータセンターに2つコピー
テナントアカウント	指定なし
バケット名	指定なし
高度なフィルタ	指定なし

ルール定義	値の例
参照時間	取り込み時間
配置	0 日目から無期限に、 2 つのレプリケートコピーを保持します。 1 つはデータセンター 1 のストレージノードに、もう 1 つはデータセンター 2 のストレージノードに保持します。

S3 オブジェクトのロックに対する準拠 ILM ポリシーの例

S3 オブジェクトロックが有効になっているバケット内のオブジェクトを含め、システム内のすべてのオブジェクトを効果的に保護する ILM ポリシーを作成するには、すべてのオブジェクトのストレージ要件を満たす ILM ルールを選択する必要があります。その後、ポリシーをシミュレートしてアクティブ化する必要があります。

ポリシーにルールを追加します

この例では、 ILM ポリシーに、次の順序で 3 つの ILM ルールが含まれています。

1. S3 オブジェクトのロックが有効な特定のバケットで 1MB を超えるオブジェクトをイレイジャーコーディングを使用して保護する準拠ルール。オブジェクトは 0 日目から無期限にストレージノードに格納されます。
2. 2 つのレプリケートオブジェクトコピーを作成してストレージノードに 1 年間保存したあと、 1 つのオブジェクトコピーをクラウドストレージプールに無期限に移動する非準拠ルール。S3 オブジェクトロックが有効になっているバケットでは、クラウドストレージプールを使用するため、このルールは適用されません。
3. 2 つのレプリケートオブジェクトコピーを 0 日目からストレージノードに無期限に作成するデフォルトの準拠ルール。

ポリシーをシミュレートする

ポリシーにルールを追加し、デフォルトの準拠ルールを選択して他のルールを整理したら、S3オブジェクトロックを有効にしたバケットのオブジェクトと他のバケットのオブジェクトをテストしてポリシーをシミュレートする必要があります。たとえば、この例のポリシーをシミュレートすると、テストオブジェクトは次のように評価されます。

- 最初のルールは、 Bank of ABC テナントのバケットバンクレコードで 1MB を超えるテストオブジェクトのみに一致します。

- 2 番目のルールは、他のすべてのテナントアカウントの非準拠バケット内のすべてのオブジェクトに一致します。
- デフォルトのルールは次のオブジェクトに一致します。
  - バケットバンク内の1MB以下のオブジェクト- Bank of ABCテナントのレコード。
  - 他のすべてのテナントアカウントで S3 オブジェクトロックが有効になっている他のバケット内のオブジェクト。

ポリシーをアクティブ化する

新しいポリシーによってオブジェクトデータが適切に保護されることを確認したら、アクティブ化します。

S3バケットライフサイクルとILMポリシーがStorageGRIDでどのように相互作用するか

オブジェクトはライフサイクル設定に応じて、S3バケットライフサイクルまたはILMポリシーの保持設定に従います。

ILMポリシーよりも優先するバケットライフサイクルの例

ILMポリシー

- noncurrent-time referenceに基づくルール：0日目にXコピーを20日間保持
- 取り込み時間参照に基づくルール（デフォルト）：0日目にXコピーを50日間保持

バケットライフサイクル

```
"Filter": {"Prefix": "docs/"}, "Expiration": {"Days": 100},
"NoncurrentVersionExpiration": {"NoncurrentDays": 5}
```

結果

- 「docs/text」という名前のオブジェクトが取り込まれます。バケットライフサイクルフィルタの「docs/」プレフィックスに一致します。
  - 100日が経過すると、delete-markerが作成され、「docs/text」がnoncurrentになります。
  - 5日後、「docs/text」は取り込みから合計105日後に削除されます。
  - 取り込みから合計200日後、delete-markerが作成されてから100日後に、期限切れのdelete-markerは削除されます。
- 「video/movie」という名前のオブジェクトが取り込まれます。フィルタに一致しないため、ILM保持ポリシーが使用されています。
  - 50日後、削除マーカーが作成され、「ビデオ/ムービー」が非最新になります。
  - 20日後、取り込みから合計70日後、「ビデオ/ムービー」が削除されます。
  - 取り込みから合計で100日後、delete-markerが作成されてから50日後には、期限切れのdelete-markerが削除されます。

バケットライフサイクルの暗黙的な**keeping-forever**の例

ILMポリシー

- noncurrent-time referenceに基づくルール：0日目にXコピーを20日間保持

- 取り込み時間参照に基づくルール（デフォルト）：0日目にXコピーを50日間保持

バケットライフサイクル

```
"Filter": {"Prefix": "docs/"}, "Expiration": {"ExpiredObjectDeleteMarker":
true}
```

結果

- 「docs/text」という名前のオブジェクトが取り込まれます。バケットライフサイクルフィルタの「docs/」プレフィックスに一致します。

  この `Expiration`アクションは、期限切れの削除マーカーにのみ適用されます。これは、他のすべてを永久に保持することを意味します(「docs /」で始まる)。

  「docs/」で始まる削除マーカーは、期限切れになると削除されます。

- 「video/movie」という名前のオブジェクトが取り込まれます。フィルタに一致しないため、ILM保持ポリシーが使用されています。
  - 50日後、削除マーカーが作成され、「ビデオ/ムービー」が非最新になります。
  - 20日後、取り込みから合計70日後、「ビデオ/ムービー」が削除されます。
  - 取り込みから合計で100日後、delete-markerが作成されてから50日後には、期限切れのdelete-markerが削除されます。

バケットライフサイクルを使用して**ILM**を複製し、期限切れの削除マーカーをクリーンアップする例

ILMポリシー

- noncurrent-time referenceに基づくルール：0日目にXコピーを20日間保持
- 取り込み時の参照に基づくルール（デフォルト）：0日目にX個のコピーを無期限に保持

バケットライフサイクル

```
"Filter": {}, "Expiration": {"ExpiredObjectDeleteMarker": true},
"NoncurrentVersionExpiration": {"NoncurrentDays": 20}
```

結果

- ILMポリシーがバケットライフサイクル内で重複している。
  - ILMポリシーのforeverルールは、オブジェクトを手動で削除し、最新でないバージョンを20日後にクリーンアップするように設計されています。そのため、取り込み時間ルールでは、期限切れの削除マーカーが無期限に保持されます。
  - バケットライフサイクルは、追加時にILMポリシーの動作を複製します `"ExpiredObjectDeleteMarker": true`。削除マーカーは期限切れになると削除されます。
- オブジェクトが取り込まれた。フィルタがない場合は、バケットライフサイクルによってすべてのオブジェクトが環境され、ILMの保持設定が上書きされます。
  - テナントがオブジェクトの削除要求を実行すると、削除マーカーが作成され、オブジェクトがnoncurrentになります。
  - 20日が経過すると、最新でないオブジェクトが削除され、delete-markerの有効期限が切れます。
  - その直後に、期限切れの削除マーカーが削除されます。

StorageGRID のシステム強化

StorageGRID のシステム強化について学ぶ

システムのセキュリティ強化とは、 StorageGRID システムからできるだけ多くのセキュリティリスクを排除するプロセスです。

StorageGRIDをインストールして設定する際には、機密性、整合性、可用性に関する所定のセキュリティ目標を達成するために、これらのガイドラインを使用してください。

システム強化については、すでに業界標準のベスト プラクティスを使用しているはずです。たとえば、StorageGRIDには強力なパスワードを使用し、HTTP ではなく HTTPS を使用し、可能な場合は証明書ベースの認証を有効にします。これらのベスト プラクティスには、物理的なアクセスを制限するとともに、物理的なデータ センターとサポート インフラストラクチャを保護する物理的および環境的なセキュリティが含まれている必要があります。また、事業および地域に適用される規制基準および推奨事項も参照する必要があります。

StorageGRIDはに準拠してい "NetApp Vulnerability Handling Policyの略"ます。報告された脆弱性は、製品セキュリティインシデント対応プロセスに従って検証および解決されます。

StorageGRIDシステムのセキュリティを強化する場合は、次の点を考慮してください。

- * 3つのStorageGRIDネットワークのうち、実装したネットワークはどれですか*。すべての StorageGRID システムでグリッドネットワークを使用する必要がありますが、管理ネットワーク、クライアントネットワーク、またはその両方を使用することもできます。ネットワークごとにセキュリティに関する考慮事項が異なります。
- * StorageGRIDシステムの個 々 のノードに使用するプラットフォームのタイプ*。StorageGRID ノードは、 VMware 仮想マシン、 Linux ホスト上のコンテナエンジン、または専用のハードウェアアプライアンスとして導入できます。プラットフォームのタイプごとに、強化に関するベストプラクティスがあります。
- テナントアカウントの信頼度。テナントアカウントを信頼しないサービスプロバイダである場合は、信頼できる社内テナントのみを使用した場合とはセキュリティ上の問題が異なります。
- *セキュリティ要件と規則*組織は次のとおりです。特定の規制や企業の要件に準拠しなければならない場合があります。

StorageGRIDソフトウェア アップグレードの強化ガイドライン

攻撃を防御するには、 StorageGRID システムおよび関連サービスを最新の状態に保つ必要があります。

StorageGRID ソフトウェアへのアップグレード

StorageGRID ソフトウェアは、可能なかぎり、最新のメジャーリリースまたは以前のメジャーリリースにアップグレードする必要があります。StorageGRID を最新の状態に保つことで、既知の脆弱性がアクティブになる時間を短縮し、攻撃対象領域全体を削減できます。また、StorageGRID の最新リリースには、以前のリリースには含まれていないセキュリティ強化機能が含まれていることがよくあります。

（IMT）を参照して、使用するStorageGRIDソフトウェアのバージョンを確認します "NetApp Interoperability Matrix Tool"。ホットフィックスが必要な場合、NetAppは最新リリース用の更新プログラムの作成を優先します。一部のパッチは、以前のリリースと互換性がない場合があります。

- 最新のStorageGRIDリリースとホットフィックスをダウンロードするには、に進みます "NetAppのダウンロード：StorageGRID"。
- StorageGRIDソフトウェアをアップグレードするには、を参照して"アップグレード手順"ください。
- ホットフィックスを適用するには、を参照して"StorageGRID ホットフィックス手順"ください。

外部サービスへのアップグレード

外部サービスには、 StorageGRID に間接的に影響を及ぼす脆弱性が存在する可能性があります。StorageGRIDが依存するサービスが最新の状態に保たれていることを確認します。これらのサービスには、LDAP、KMS (または KMIP サーバー)、DNS、NTP が含まれます。

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

ハイパーバイザーのアップグレード

StorageGRID ノードが VMware または別のハイパーバイザーで実行されている場合は、ハイパーバイザーのソフトウェアとファームウェアが最新であることを確認する必要があります。

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

*** Linuxノードへのアップグレード***

StorageGRID ノードで Linux ホストプラットフォームを使用している場合は、セキュリティ更新とカーネル更新がホスト OS に適用されていることを確認する必要があります。また、これらの更新プログラムが利用可能になった場合は、脆弱なハードウェアにファームウェアの更新プログラムを適用する必要があります。

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

StorageGRID ネットワークのセキュリティ強化のガイドライン

StorageGRID システムでは、グリッドノードあたり最大 3 つのネットワークインターフェイスがサポートされ、各グリッドノードのネットワークをセキュリティやアクセスの要件に応じて設定することができます。

StorageGRIDネットワークの詳細については、を参照してください"StorageGRID のネットワークタイプ"。

グリッドネットワークのガイドライン

グリッドネットワークはすべての内部 StorageGRID トラフィック用に設定する必要があります。グリッドネットワークのグリッドノードは、いずれも他のすべてのノードと通信できなければなりません。

グリッドネットワークを設定する際は、次のガイドラインに従ってください。

- オープンインターネット上のクライアントなど、信頼できないクライアントからネットワークが保護されていることを確認します。
- 可能な場合は、グリッドネットワークを内部トラフィック専用にします。管理ネットワークとクライアントネットワークの両方に、内部サービスへの外部トラフィックをブロックするファイアウォール制限が追

加されています。グリッドネットワークを使用した外部クライアントトラフィックの処理はサポートされていますが、この使用によって保護レイヤが少なくなります。

- StorageGRID 環境が複数のデータセンターにまたがっている場合は、仮想プライベートネットワーク（ VPN ）またはグリッドネットワーク上で同等の機能を使用して、内部トラフィックをさらに保護します。
- 一部のメンテナンス手順では、プライマリ管理ノードと他のすべてのグリッドノードの間のポート 22 で Secure Shell （ SSH ）アクセスが必要です。外部ファイアウォールを使用して、信頼できるクライアントへの SSH アクセスを制限します。

管理ネットワークのガイドライン

管理ネットワークは、通常、管理タスク（ Grid Manager または SSH を使用する信頼できる従業員）および LDAP 、 DNS 、 NTP 、 KMS （ KMIP サーバ）などの信頼された他のサービスとの通信に使用します。ただし、 StorageGRID ではこの使用が内部的に適用されることはありません。

管理ネットワークを使用する場合は、次のガイドラインに従ってください。

- 管理ネットワーク上のすべての内部トラフィックポートをブロックします。を参照してください"内部ポートのリスト"。
- 信頼されていないクライアントが管理ネットワークにアクセスできる場合は、外部ファイアウォールで管理ネットワーク上の StorageGRID へのアクセスをブロックします。

クライアントネットワークのガイドライン

クライアントネットワークは、通常、テナント、および CloudMirror レプリケーションサービスや別のプラットフォームサービスなどの外部サービスとの通信に使用されます。ただし、 StorageGRID ではこの使用が内部的に適用されることはありません。

クライアントネットワークを使用する場合は、次のガイドラインに従ってください。

- クライアントネットワーク上のすべての内部トラフィックポートをブロックします。を参照してください"内部ポートのリスト"。
- 明示的に設定されたエンドポイントでのみ、インバウンドクライアントトラフィックを受け入れます。の情報を参照してください"ファイアウォールコントロールの管理"。

StorageGRID ノードの保護対策のガイドライン

StorageGRID ノードは、 VMware 仮想マシン、 Linux ホスト上のコンテナエンジン、または専用のハードウェアアプライアンスとして導入できます。プラットフォームのタイプとノードのタイプにはそれぞれ、強化に関するベストプラクティスがあります。

BMCへのリモートIPMIアクセスを制御する

BMC を含むすべてのアプライアンスに対して、リモート IPMI アクセスを有効または無効にすることができます。リモート IPMI インターフェイスを使用すると、BMC アカウントとパスワードを持つすべてのユーザーが StorageGRID アプライアンスへの低レベルのハードウェア アクセスを行えるようになります。BMC へのリモート IPMI アクセスが不要な場合は、このオプションを無効にしてください。

- Grid Manager で BMC へのリモート IPMI アクセスを制御するには、構成 > セキュリティ > セキュリティ設定 > アプライアンス > リモート **IPMI** アクセス に移動します：

- BMCへのIPMIアクセスを無効にするには、*リモートIPMIアクセスを有効にする*チェックボックスをオフにします。
- BMCへのIPMIアクセスを有効にするには、*リモートIPMIアクセスを有効にする*チェックボックスをオンにします。

BMC強化の詳細については、 "ベースボード管理コントローラの強化"サイバーセキュリティ情報シート "国家安全保障局（NSA）"そして "サイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA）"。

アプライアンスの**BMC**パスワードを変更する

アプライアンスの BMC パスワードを変更して、アクセスを制限し、システムのセキュリティを向上させることができます。

1. グリッドマネージャで、ノード > グリッドノード > **BMC**設定 に移動します。
2. 「パスワードの変更」セクションで、*新しいパスワード*に8文字から16文字の長さの新しい BMC パスワードを入力し、*新しいパスワードの確認*にもう一度入力してください。
3. [保存（ Save ）] を選択します。

また、 `PUT /bmc-configuration/root-password` API を使用して BMC パスワードを変更することもできます。

アプライアンスの外部**USB**ポートへのアクセスを制御する

機器のUSBポートを有効にすることで、診断やトラブルシューティングのための技術サポートによるアクセスを許可できます。USBポートへのアクセスが必要ない場合は、セキュリティ上の理由からポートを無効にしてください。USBポートは、初回インストール後またはアップグレード後にデフォルトで有効になります。

- Grid Manager で、**Configuration** > **Security** > **Security settings** > **Appliances** > **USB port access** に移動して、USB ポートを有効または無効にします：
  - 「USB ポートを有効にする」チェックボックスを選択して保存すると、ポートが有効になります。

    USB チェックボックスが以前にオフになって保存されていた場合は、USB ポートを再度有効にするために、**[USB** ポートを有効にする**]** チェックボックスを選択して保存してください。

  - **USB**ポートを有効にする チェックボックスをオフにして保存すると、ポートが無効になります。

ファイアウォールの設定

システム強化プロセスの一環として、外部ファイアウォールの設定を確認し、 IP アドレスとそれが厳密に必要なポートからのみトラフィックが許可されるように変更する必要があります。

StorageGRID には、各ノードに内部ファイアウォールがあります。このファイアウォールを使用すると、ノードへのネットワークアクセスを制御できるため、グリッドのセキュリティが強化されます。特定のグリッド環境に必要なポート以外のすべてのポートでネットワークアクセスを禁止する必要があります"内部ファイアウォールコントロールを管理します"。[Firewall]コントロールページで行った設定変更は、各ノードに展開されます。

具体的には、次の領域を管理できます。

- 特権アドレス：[外部アクセスの管理]タブの設定によって閉じられたポートに、選択したIPアドレスまたはサブネットがアクセスできるようにすることができます。

- 外部アクセスの管理：デフォルトで開いているポートを閉じるか、以前閉じていたポートを再度開くことができます。
- 信頼されていないクライアントネットワーク：ノードがクライアントネットワークからのインバウンドトラフィックを信頼するかどうか、および信頼されていないクライアントネットワークが設定されている場合に開く追加ポートを指定できます。

この内部ファイアウォールは、一部の一般的な脅威に対する追加の保護レイヤを提供しますが、外部ファイアウォールの必要性は排除されません。

StorageGRIDで使用されるすべての内部ポートと外部ポートのリストについては、"StorageGRID の内部ポート"そして"外部との通信に使用するポート"。

未使用のサービスを無効にします

すべてのStorageGRIDノードについて、未使用のサービスへのアクセスを無効にするかブロックする必要があります。たとえば、DHCP を使用する予定がない場合は、グリッド マネージャーを使用してポート 68 を閉じます。 構成 > ファイアウォール制御 > 外部アクセスの管理*を選択します。次に、ポート **68** のステータス トグルを ***Open** から **Closed** に変更します。

仮想化、コンテナ、共有ハードウェア

すべての StorageGRID ノードで、信頼されていないソフトウェアと同じ物理ハードウェア上で StorageGRID を実行しないでください。StorageGRID とマルウェアの両方が同じ物理ハードウェア上に存在する場合、ハイパーバイザーの保護によってStorageGRIDで保護されたデータへのマルウェアのアクセスが防止されるとは限りません。たとえば、 Meltdown と Specter 攻撃は、最新のプロセッサに存在する重要な脆弱性を悪用し、プログラムが同じコンピュータ上のメモリにデータを盗むことを可能にします。

インストール中にノードを保護

ノードがインストールされているときに、信頼されていないユーザがネットワーク経由でStorageGRID ノードにアクセスできないようにします。ノードは、グリッドに参加するまで完全にセキュアになりません。

ハードウェアへの物理的なアクセスを制限する

StorageGRIDハードウェア アプライアンス ノード、およびStorageGRIDを実行している VMware 仮想マシン ホストと Linux ホストへの物理アクセスを、許可された管理者のみに制限する必要があります。物理的なアクセス制御の例としては、ロック、ガード、物理的な障壁、ビデオ監視などがあります。

ハードウェア アプライアンス ノードは、許可された管理者のみがインストールおよび操作できるように設計されています。権限のない管理者がハードウェア アプライアンス ノードにアクセスできないようにします。

管理ノードのガイドライン

管理ノードは、システムの設定、監視、ロギングなどの管理サービスを提供します。Grid Manager または Tenant Manager にサインインすると、管理ノードに接続されます。

StorageGRID システムで管理ノードを保護するには、次のガイドラインに従います。

- 開いているインターネット上の管理ノードなど、信頼されていないクライアントからすべての管理ノードを保護します。グリッドネットワーク上、管理ネットワーク上、またはクライアントネットワーク上のどの管理ノードにも、信頼されていないクライアントがアクセスできないようにします。

- StorageGRID グループは Grid Manager とテナントマネージャの機能へのアクセスを制御します。各ユーザグループにロールに最低限必要な権限を付与し、読み取り専用アクセスモードを使用してユーザによる設定変更を防止します。
- StorageGRID ロードバランサエンドポイントを使用する場合は、信頼されないクライアントトラフィックに管理ノードの代わりにゲートウェイノードを使用します。
- 信頼されていないテナントがある場合は、そのテナントにTenant Managerまたはテナント管理APIへの直接アクセスを許可しないでください。代わりに、信頼されていないテナントがテナントポータルまたはテナント管理 API と連動する外部テナント管理システムを使用するようにします。
- 必要に応じて、管理プロキシを使用して、管理ノードからNetAppサポートへのAutoSupport通信を詳細に制御します。の手順を参照してください"管理プロキシの作成"。
- 必要に応じて、制限された 8443 ポートと 9443 ポートを使用して Grid Manager と Tenant Manager の通信を分離します。共有ポート 443 をブロックして、テナント要求をポート 9443 に制限して追加の保護を確保します。
- 必要に応じて、グリッド管理者とテナントユーザには別々の管理ノードを使用します。

詳細については、の手順を参照してください"StorageGRID の管理"。

ストレージノードに関するガイドライン

ストレージノードは、オブジェクトデータとメタデータを管理および格納します。StorageGRID システムでストレージノードを保護するには、次のガイドラインに従います。

- 信頼できないクライアントがストレージノードに直接接続することを許可しないでください。ゲートウェイノードまたはサードパーティ製のロードバランサーによって提供されるロードバランサーエンドポイントを使用してください。
- 信頼されていないテナントに対してアウトバウンドサービスを有効にしないでください。たとえば、信頼されていないテナントのアカウントを作成する場合は、テナントに独自のアイデンティティソースの使用やプラットフォームサービスの使用を許可しないでください。の手順を参照してください"テナントアカウントを作成する"。
- 信頼されないクライアントトラフィックには、サードパーティのロードバランサを使用します。サードパーティ製のロードバランシングにより、攻撃に対する制御性が向上し、追加の保護レイヤが提供されます。
- 必要に応じて、ストレージプロキシを使用して、クラウドストレージプールとプラットフォームサービスのストレージノードから外部サービスへの通信を詳細に制御します。の手順を参照してください"ストレージプロキシの作成"。
- 必要に応じて、クライアント ネットワークを使用して外部サービスに接続します。次に、[構成] > [セキュリティ] > [ファイアウォール制御] > [信頼されていないクライアント ネットワーク] を選択し、ストレージノード上のクライアント ネットワークが信頼されていないことを示します。ストレージ ノードは、クライアント ネットワーク上の着信トラフィックを受け入れなくなりますが、プラットフォーム サービスへの送信要求は引き続き許可します。

ゲートウェイノードのガイドライン

ゲートウェイノードは、クライアントアプリケーションが StorageGRID への接続に使用できるオプションのロードバランシングインターフェイスです。StorageGRID システムにゲートウェイノードを保護するには、次のガイドラインに従います。

- ロードバランサエンドポイントを設定して使用する。を参照して "ロードバランシングに関する考慮事項"

- クライアントとゲートウェイノードまたはストレージノードの間で、信頼されていないクライアントトラフィックにサードパーティのロードバランサを使用します。サードパーティ製のロードバランシングにより、攻撃に対する制御性が向上し、追加の保護レイヤが提供されます。サードパーティのロードバランサを使用する場合でも、内部のロードバランサエンドポイントを経由するようにネットワークトラフィックを設定したり、ストレージノードに直接送信したりすることができます。
- ロード バランサー エンドポイントを使用している場合は、オプションでクライアントをクライアント ネットワーク経由で接続します。次に、[構成] > [セキュリティ] > [ファイアウォール制御] > [信頼されていないクライアント ネットワーク] を選択し、ゲートウェイ ノード上のクライアント ネットワークが信頼されていないことを示します。ゲートウェイ ノードは、ロード バランサーのエンドポイントとして明示的に構成されたポート上の受信トラフィックのみを受け入れます。

ハードウェアアプライアンスノードのガイドライン

StorageGRID ハードウェアアプライアンスは、 StorageGRID システム専用に設計されています。一部のアプライアンスはストレージノードとして使用できます。その他のアプライアンスは、管理ノードまたはゲートウェイノードとして使用できます。アプライアンスノードをソフトウェアベースのノードと組み合わせることも、自社開発の全アプライアンスグリッドを導入することもできます。

StorageGRID システムにハードウェアアプライアンスノードを固定するには、次のガイドラインに従います。

- アプライアンスでストレージコントローラの管理に SANtricity System Manager を使用している場合は、信頼されていないクライアントからネットワーク経由で SANtricity System Manager にアクセスできないようにします。
- アプライアンスにベースボード管理コントローラ (BMC) が搭載されている場合は、 BMC管理ポートによって低レベルのハードウェア アクセスが許可される場合があるので注意してください。 BMC管理ポートは、安全で信頼できる内部管理ネットワークにのみ接続してください。

  VLAN を確立して、 BMCネットワーク接続を分離し、 BMCインターネット アクセスを信頼できるネットワークに制限できます。 VLAN分離の強制に関する追加情報については、 "ベースボード管理コントローラの強化"サイバーセキュリティ情報シート "国家安全保障局（NSA）"そして "サイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA）"。

  安全で信頼できる内部管理ネットワークが利用できない場合は、 BMC管理ポートを未接続のままにするか、ブロックされたままにしておきます。テクニカル サポートでは、サポート ケース中に一時的なアクセスを要求する場合があります。

- アプライアンスが Intelligent Platform Management Interface （ IPMI ）標準を使用したイーサネット経由でのコントローラハードウェアのリモート管理をサポートする場合は、ポート 623 での信頼されていないトラフィックをブロックします。

  また、リモートIPMIアクセスを無効にする。

> BMCを含むすべてのアプライアンスに対してリモート IPMI アクセスを有効または無効にすることができます。リモート IPMI インターフェイスを使用すると、 BMCアカウントとパスワードを持つすべてのユーザーがStorageGRIDアプライアンスに低レベルのハードウェア アクセスできるようになります。 BMCへのリモート IPMI アクセスが必要ない場合は、次のいずれかの方法でこのオプションを無効にします。+ Grid Manager で、構成 > セキュリティ > セキュリティ設定 > アプライアンス に移動し、リモート **IPMI** アクセスを有効にする チェックボックスをオフにします。 + グリッド管理 API では、プライベート エンドポイントを使用します。 `PUT /private/bmc` 。

- SANtricity System Managerで管理しているSED、FDE、またはFIPS NL-SASドライブを含むアプライアンスモデルの場合は、を参照してください "SANtricityドライブセキュリティの有効化と設定"。
- StorageGRIDアプライアンスインストーラおよびグリッドマネージャを使用して管理するSEDまたはFIPS NVMe SSDを搭載したアプライアンスモデルの場合、 "StorageGRIDドライブ暗号化の有効化と設定" 。
- SED、FDE、またはFIPSドライブを搭載していないアプライアンスの場合は、キー管理サーバー（KMS）を使用して "StorageGRIDソフトウェアノード暗号化を有効にして構成する"。

関連情報

"SANtricity System Managerのドライブセキュリティについて学ぶ"

StorageGRID における TLS および SSH の強化ガイドライン

SSH アクセスを制御し、デフォルトの TLS 証明書を置き換え、TLS および SSH 接続に適切なセキュリティ ポリシーを選択する必要があります。

証明書に関するセキュリティ強化ガイドライン

インストール時に作成されたデフォルトの証明書を独自のカスタム証明書に置き換える必要があります。

多くの組織では、 StorageGRID Web アクセス用の自己署名デジタル証明書が、情報セキュリティポリシーに準拠していません。本番用システムでは、 StorageGRID の認証に使用する CA 署名デジタル証明書をインストールする必要があります。

具体的には、次のデフォルト証明書ではなくカスタムサーバ証明書を使用する必要があります。

- * 管理インターフェイス証明書 * ： Grid Manager 、 Tenant Manager 、 Grid 管理 API 、およびテナント管理 API へのアクセスを保護するために使用します。
- * S3 API証明書*：ストレージノードとゲートウェイノードへのアクセスを保護するために使用します。これらのノードは、S3クライアントアプリケーションがオブジェクトデータをアップロードおよびダウンロードするために使用します。

詳細と手順については、を参照してください"セキュリティ証明書を管理する"。

> StorageGRID では、ロードバランサエンドポイントに使用する証明書は別に管理されます。ロードバランサ証明書を設定するには、を参照してください"ロードバランサエンドポイントを設定する"。

カスタムサーバ証明書を使用する場合は、次のガイドラインに従ってください。

- 証明書には、StorageGRIDのDNSエントリと一致するが必要です `subjectAltName`。詳細については、のセクション4.2.1.6「サブジェクトの別名」を参照してください "RFC 5280: PKIX 証明書と CRL プロファイル"。
- 可能であれば、ワイルドカード証明書は使用しないでください。ただし、S3仮想ホスト形式のエンドポイントの証明書は例外です。この証明書では、バケット名が事前にわからない場合にワイルドカードを使用する必要があります。
- 証明書にワイルドカードを使用する必要がある場合は、リスクを軽減するために追加の手順を実行する必要があります。などのワイルドカードパターンを使用し、他のアプリケーションにはサフィックスを使用し `*.s3.example.com`ない `s3.example.com`でください。このパターンは、などのパス形式のS3

アクセスでも機能します `dc1-s1.s3.example.com/mybucket`。

- 証明書の有効期限を短く（ 2 カ月など）設定し、グリッド管理 API を使用して証明書のローテーションを自動化します。これは、ワイルドカード証明書で特に重要です。

また、クライアントは StorageGRID との通信に厳密なホスト名チェックを使用する必要があります。

TLSおよび**SSH**ポリシーに関するセキュリティ強化ガイドライン

セキュリティポリシーを選択して、クライアントアプリケーションとのセキュアなTLS接続の確立や内部StorageGRID サービスへのセキュアなSSH接続に使用するプロトコルと暗号を決定できます。

セキュリティ ポリシーは、TLS と SSH が移動中のデータを暗号化する方法を制御します。ベストプラクティスとして、アプリケーションの互換性に必要のない暗号化オプションを無効にする必要があります。システムが Common Criteria 準拠、FIPS 140-2 準拠である必要がある場合、または他の暗号を使用する必要がない限り、デフォルトのモダン ポリシーを使用します。

詳細と手順については、を参照してください"TLSおよびSSHポリシーを管理します"。

外部**SSH**アクセスを管理する

システム セキュリティを強化するために、外部からの SSH アクセスはデフォルトでブロックされます。トラブルシューティングなど、着信 SSH アクセスを必要とするタスクを実行する必要がある場合のみ、SSH アクセスを有効にします。参照"外部SSHアクセスを管理する"詳細と手順についてはこちらをご覧ください。

StorageGRID のログ、パスワード、監査メッセージの強化ガイドライン

StorageGRID ネットワークおよびノードに対する強化ガイドラインに加えて、StorageGRID システムの他の領域に対する強化ガイドラインに従う必要があります。

一時インストールパスワード

インストール中にStorageGRIDシステムを保護するには、StorageGRIDインストールUIまたはインストールAPIの一時インストーラパスワードページでパスワードを設定します。このパスワードを設定すると、ユーザインターフェイス、インストールAPI、スクリプトなど、StorageGRIDをインストールするすべての方法に適用され `configure-storagegrid.py`ます。

詳細については、以下を参照してください。

- "ソフトウェアベースのノードにStorageGRIDをインストールする"
- "StorageGRIDアプライアンスの設置"

ログと監査メッセージ

StorageGRID ログおよび監査メッセージ出力は必ず安全な方法で保護してください。StorageGRID のログと監査メッセージは、サポートやシステム可用性の観点から非常に重要な情報を提供します。また、StorageGRID のログおよび監査メッセージの出力に含まれる情報や詳細情報は、一般に機密性が高いため、

セキュリティイベントを外部 syslog サーバに送信するように StorageGRID を設定します。syslog エクスポートを使用する場合は、トランスポートプロトコルに対して TLS と RELP/TLS を選択します。

StorageGRIDログの詳細については、を参照してください"ログファイル参照"。StorageGRID監査メッセージ

の詳細については、を参照してください"監査メッセージ"。

NetApp AutoSupport

StorageGRIDのAutoSupport機能を使用すると、システムの健全性をプロアクティブに監視し、NetApp Support Site、組織内のサポートチーム、またはサポートパートナーにパッケージを自動的に送信できます。デフォルトでは、StorageGRIDを初めて設定すると、NetAppへのAutoSupportパッケージの送信が有効になります。

AutoSupport機能は無効にできます。ただし、 StorageGRID システムで問題 に障害が発生した場合には、AutoSupport を使用して迅速に問題を識別し解決できるため、ネットアップではこの機能を有効にすることを推奨してい

AutoSupportでは、転送プロトコルとしてHTTPS、HTTP、およびSMTPがサポートされます。AutoSupportパッケージは機密性が高いため、NetAppはAutoSupportパッケージをNetAppに送信するためのデフォルトの転送プロトコルとしてHTTPSを使用することを強く推奨します。

Cross-Origin Resource Sharing（CORS）

S3バケットとバケット内のオブジェクトに他のドメインにあるWebアプリケーションからアクセスできるようにするには、そのバケットにCross-Origin Resource Sharing（CORS）を設定します。一般的に、CORSは必要でない限り有効にしないでください。CORS が必要な場合は、信頼できるオリジンに制限します。

手順については、"バケットとオブジェクトのCORSの設定" 。

外部セキュリティデバイス

完全なセキュリティ強化解決策 は、 StorageGRID 以外のセキュリティメカニズムに対応する必要があります。StorageGRID へのアクセスをフィルタリングおよび制限するために追加のインフラデバイスを使用すると、厳格なセキュリティ体制を確立し、維持するための効果的な方法となります。これらの外部セキュリティデバイスには、ファイアウォール、 Intrusion Prevention System （ IPS ；侵入防御システム）、およびその他のセキュリティデバイスが含まれます。

信頼されないクライアントトラフィックには、サードパーティのロードバランサを使用することを推奨します。サードパーティ製のロードバランシングにより、攻撃に対する制御性が向上し、追加の保護レイヤが提供されます。

ランサムウェアの軽減

の推奨事項に従って、ランサムウェア攻撃からオブジェクトデータを保護し "StorageGRID によるランサムウェア対策"ましょう。

StorageGRIDとFabricPool

FabricPoolでStorageGRIDを使用するための設定ワークフロー

NetApp ONTAP ソフトウェアを使用している場合は、NetApp FabricPool を使用して、アクセス頻度の低いデータをNetApp StorageGRID オブジェクトストレージシステムに階層化できます。

次の手順に従って、次の操作を行います

- FabricPool ワークロード用にStorageGRID を設定する際の考慮事項とベストプラクティスを紹介します。
- FabricPool で使用するStorageGRID オブジェクトストレージシステムの設定方法について説明します。
- StorageGRID をFabricPool クラウド階層として接続するときに、ONTAP に必要な値を指定する方法について説明します。

StorageGRID for FabricPool を設定するためのクイックスタート

1 設定を計画する

- アクセス頻度の低い ONTAP データを StorageGRID に階層化するときに使用する FabricPool ボリューム階層化ポリシーを決定します。
- ストレージ容量とパフォーマンスのニーズを満たす StorageGRID システムを計画して設置します。
- StorageGRIDシステムソフトウェア（およびを含む）について理解します"Grid Manager""テナントマネージャ"。
- "HAグループ"、"ロードバランシング"、"ILM"、のFabricPoolのベストプラクティスを確認します"もっと"。
- ONTAP およびFabricPool の使用と設定に関する詳細については、次のリソースを参照してください。

  "TR-4598：『FabricPool Best Practices in ONTAP 』"

  "FabricPoolのONTAPドキュメント"

2 前提条件となるタスクの実行

"StorageGRID をクラウド階層として接続するために必要な情報"次の情報を含むを入手します。

- IPアドレス
- ドメイン名
- SSL証明書

オプションで設定"アイデンティティフェデレーション"そして"シングルサインオン"。

3 **StorageGRID**の設定

StorageGRID を使用して、ONTAP がグリッドに接続するために必要な値を取得します。

すべての項目を設定するには、を使用すること"FabricPool セットアップウィザード"を推奨しますが、必要に応じて各エンティティを手動で設定することもできます。

4 **ONTAP**と**DNS**の設定

ONTAP Toを使用する"クラウド階層を追加します"と、StorageGRID値が使用されます。次に"DNSエントリを設定します"、使用するドメイン名にIPアドレスを関連付けます。

5 監視と管理

システムが起動して稼働したら、ONTAP とStorageGRID で継続的なタスクを実行して、FabricPool データの階層化を長期的に管理および監視します。

FabricPool とは

FabricPool は、ハイパフォーマンスのフラッシュアグリゲートを高パフォーマンス階層として、オブジェクトストアをクラウド階層として使用する ONTAP ハイブリッドストレージ解決策 です。FabricPool 対応アグリゲートを使用すると、パフォーマンス、効率、保護を犠牲にすることなくストレージコストを削減できます。

FabricPool は、クラウド階層（StorageGRID などの外部オブジェクトストア）をローカル階層（ONTAP ストレージアグリゲート）に関連付けて、ディスクの複合コレクションを作成します。FabricPool 内のボリュームは、アクティブ（ホット）データをハイパフォーマンスストレージ（ローカル階層）に保持し、非アクティブ（コールド）データを外部のオブジェクトストア（クラウド階層）に階層化することで、階層化のメリットを活用できます。

アーキテクチャを変更する必要はなく、データとアプリケーションの環境を中央の ONTAP ストレージシステムから引き続き管理できます。

StorageGRID とは

NetApp StorageGRID は、ファイルストレージやブロックストレージなどの他のストレージアーキテクチャとは対照的に、データをオブジェクトとして管理するストレージアーキテクチャです。オブジェクトは単一のコンテナ（バケットなど）内に保持され、他のディレクトリ内のディレクトリ内のファイルとしてネストされることはありません。一般にオブジェクトストレージはファイルストレージやブロックストレージよりもパフォーマンスは低くなりますが、拡張性は大幅に向上します。StorageGRID バケットは、ペタバイト規模のデータと数十億個のオブジェクトを保持できます。

StorageGRID を **FabricPool** クラウド階層として使用する理由

FabricPool では、ONTAP データを複数のオブジェクトストレージプロバイダ（StorageGRID など）に階層化できます。サポートされる 1 秒あたりの最大入出力処理数（ IOPS ）をバケットレベルまたはコンテナレベルで設定する可能性があるパブリッククラウドとは異なり、 StorageGRID のパフォーマンスはシステム内のノード数に応じて拡張されます。StorageGRID を FabricPool クラウド階層として使用すると、コールドデータをプライベートクラウド内に保持することで、最高のパフォーマンスと完全なデータ管理を実現できます。

また、 StorageGRID をクラウド階層として使用する場合は、 FabricPool ライセンスは必要ありません。

StorageGRID を **FabricPool** クラウド階層として接続するために必要な情報

StorageGRID をFabricPool のクラウド階層として接続する前に、StorageGRID で設定手順を実行し、ONTAP で使用する特定の値を取得する必要があります。

どのような価値が必要か？

次の表に、StorageGRID で設定する必要がある値と、それらの値がONTAP およびDNSサーバでどのように使用されるかを示します。

値	値が設定されます	値が使用されます
仮想IP（VIP）アドレス	[HA group]をクリックしますStorageGRID	DNSエントリ
ポート	StorageGRID > Load Balancer Endpointの順に選択します	[System Manager]>[クラウド階層の追加]をクリックしますONTAP
SSL証明書	StorageGRID > Load Balancer Endpointの順に選択します	[System Manager]>[クラウド階層の追加]をクリックしますONTAP
サーバ名（FQDN）	StorageGRID > Load Balancer Endpointの順に選択します	DNSエントリ
アクセスキーIDとシークレットアクセスキー	StorageGRID > Tenant and bucketの順に選択します	[System Manager]>[クラウド階層の追加]をクリックしますONTAP
バケット/コンテナ名	StorageGRID > Tenant and bucketの順に選択します	[System Manager]>[クラウド階層の追加]をクリックしますONTAP

これらの値を取得するにはどうすればよいですか。

要件に応じて、次のいずれかの方法で必要な情報を入手できます。

- を使用します"FabricPool セットアップウィザード"。FabricPool セットアップウィザードを使用すると、StorageGRID で必要な値を簡単に設定でき、ONTAP System Managerの設定に使用できるファイルを出力できます。ウィザードの指示に従って必要な手順を実行し、設定がStorageGRID とFabricPool のベストプラクティスに準拠していることを確認できます。
- 各項目を手動で設定します。次に、ONTAP システムマネージャまたはONTAP CLIに値を入力します。次の手順を実行します。
  a. "FabricPool のハイアベイラビリティ（HA）グループを設定します"です。
  b. "FabricPool のロードバランサエンドポイントを作成します"です。
  c. "FabricPool のテナントアカウントを作成します"です。
  d. テナントアカウントにサインインし"rootユーザのバケットとアクセスキーを作成します"ます。
  e. FabricPoolデータ用のILMルールを作成し、アクティブなILMポリシーに追加します。を参照して"FabricPool データ用のILMを設定します"
  f. 必要に応じて、"FabricPool のトラフィック分類ポリシーを作成します"。

FabricPool セットアップウィザードを使用する

StorageGRID FabricPool セットアップ ウィザードについて学ぶ

FabricPool セットアップウィザードを使用して、StorageGRID をFabricPool クラウド階層用のオブジェクトストレージシステムとして設定できます。セットアップウィザードが完了したら、ONTAP システムマネージャに必要な詳細を入力できます。

FabricPool セットアップウィザードを使用するタイミング

FabricPool セットアップウィザードの手順に従って、FabricPool で使用するStorageGRID を設定し、ILMポリシーやトラフィック分類ポリシーなどの特定のエンティティを自動的に設定します。ウィザードを完了する際に、ONTAP システムマネージャに値を入力するためのファイルをダウンロードします。ウィザードを使用すると、システムをより迅速に設定し、設定がStorageGRID とFabricPool のベストプラクティスに準拠していることを確認できます。

Root Access権限がある場合は、StorageGRID グリッドマネージャの使用を開始したときにFabricPool セットアップウィザードを完了することも、ウィザードにアクセスして完了することもできます。要件に応じて、必要な項目の一部またはすべてを手動で設定し、ウィザードを使用してONTAP で必要な値を1つのファイルにまとめることもできます。



特別な要件がある場合や、実装に大幅なカスタマイズが必要な場合を除き、FabricPool セットアップウィザードを使用します。

ウィザードを使用する前に

必要な準備手順が完了していることを確認します。

ベストプラクティスを確認

- を理解しておく必要"StorageGRID をクラウド階層として接続するために必要な情報"があります。
- 次の項目について、FabricPool のベストプラクティスを確認しておきます。
  - "ハイアベイラビリティ（HA）グループ"
  - "ロードバランシング"
  - "ILMルールとポリシー"

IPアドレスを取得し、**VLAN**インターフェイスを設定します

HAグループを設定する場合は、ONTAP が接続するノードと使用するStorageGRID ネットワークを確認しておきます。また、サブネットCIDR、ゲートウェイIPアドレス、および仮想IP（VIP）アドレスに入力する値も確認しておきます。

仮想LANを使用してFabricPool トラフィックを分離する予定の場合は、VLANインターフェイスがすでに設定されています。を参照して "VLAN インターフェイスを設定します"

アイデンティティフェデレーションと**SSO**を設定する

StorageGRIDシステムで ID フェデレーションまたはシングル サインオン (SSO) を使用する予定の場合は、これらの機能が有効になっています。また、 ONTAPが使用するテナント アカウントのルート アクセス権を持つフェデレーション グループも把握しています。見る"アイデンティティフェデレーションを使用する"そして"シングルサインオンを設定します"。

ドメイン名を取得して設定します

- StorageGRID に使用するFully Qualified Domain Name（FQDN；完全修飾ドメイン名）を確認しておきます。ドメインネームサーバ（DNS）のエントリによって、このFQDNが、ウィザードを使用して作成するHAグループの仮想IP（VIP）アドレスにマッピングされます。を参照して "DNS サーバを設定します"

- S3仮想ホスト型リクエストを使用する予定であれば、"S3エンドポイントのドメイン名が設定されました"。ONTAPはデフォルトではパス形式のURLを使用しますが、仮想ホスト形式のリクエストを使用することをお勧めします。

ロードバランサとセキュリティ証明書の要件を確認します

StorageGRIDロードバランサを使用する場合は、全般を確認しておきます。"ロードバランシングに関する考慮事項"アップロードする証明書、または証明書の生成に必要な値を用意しておきます。

外部（サードパーティ）のロードバランサエンドポイントを使用する場合は、そのロードバランサの完全修飾ドメイン名（FQDN）、ポート、および証明書が必要です。

ILMストレージプールの設定を確認する

StorageGRID 11.6以前を最初にインストールした場合は、使用するストレージプールがすでに設定されています。一般に、ONTAP データの格納に使用するStorageGRID サイトごとにストレージプールを作成する必要があります。

> この前提条件は、StorageGRID 11.7または11.8を最初にインストールした場合は適用されません。これらのバージョンのいずれかを最初にインストールすると、サイトごとにストレージプールが自動的に作成されます。

ONTAP と**StorageGRID** クラウド階層の関係

FabricPool ウィザードの手順に従って、1つのStorageGRID クラウド階層を作成します。この階層には、1つのStorageGRID テナント、1セットのアクセスキー、1つのStorageGRID バケットが含まれます。このStorageGRID クラウド階層を1つ以上のONTAP ローカル階層に接続できます。

クラスタ内の複数のローカル階層に単一のクラウド階層を接続することを推奨します。ただし、要件に応じて、1つのクラスタ内のローカル階層に対して複数のバケットまたは複数のStorageGRID テナントを使用することもできます。異なるバケットやテナントを使用すると、ONTAP ローカル階層間でデータアクセスとデータアクセスを分離できますが、設定や管理はやや複雑です。

複数のクラスタにあるローカル階層に単一のクラウド階層を接続することは推奨されません。

> NetApp MetroCluster™およびFabricPoolミラーでStorageGRIDを使用する場合のベストプラクティスについては、を参照してください "TR-4598：『FabricPool Best Practices in ONTAP 』"。

オプション：ローカル階層ごとに異なるバケットを使用します

ONTAP クラスタのローカル階層に複数のバケットを使用するには、ONTAP で複数のStorageGRID クラウド階層を追加します。各クラウド階層は、同じHAグループ、ロードバランサエンドポイント、テナント、アクセスキーを共有しますが、別 々 のコンテナ（StorageGRID バケット）を使用します。一般的な手順は次のとおりです。

1. StorageGRID グリッドマネージャから、1つ目のクラウド階層に対してFabricPool セットアップウィザードを実行します。
2. ONTAP System Managerで、クラウド階層を追加し、StorageGRID からダウンロードしたファイルを使用して必要な値を指定します。

3. StorageGRID テナントマネージャから、ウィザードで作成されたテナントにサインインし、2つ目のバケットを作成します。
4. FabricPool ウィザードをもう一度実行します。既存のHAグループ、ロードバランサエンドポイント、およびテナントを選択します。次に、手動で作成した新しいバケットを選択します。新しいバケット用の新しいILMルールを作成し、ILMポリシーをアクティブ化してそのルールを追加します。
5. ONTAP で、新しいバケット名を指定して2つ目のクラウド階層を追加します。

オプション：ローカル階層ごとに異なるテナントとバケットを使用します

ONTAP クラスタ内のローカル階層に対して複数のテナントと異なるアクセスキーセットを使用するには、ONTAP で複数のStorageGRID クラウド階層を追加します。各クラウド階層は同じHAグループとロードバランサエンドポイントを共有しますが、使用するテナント、アクセスキー、コンテナ（StorageGRID バケット）は異なります。一般的な手順は次のとおりです。

1. StorageGRID グリッドマネージャから、1つ目のクラウド階層に対してFabricPool セットアップウィザードを実行します。
2. ONTAP System Managerで、クラウド階層を追加し、StorageGRID からダウンロードしたファイルを使用して必要な値を指定します。
3. FabricPool ウィザードをもう一度実行します。既存のHAグループとロードバランサエンドポイントを選択します。新しいテナントとバケットを作成する。新しいバケット用の新しいILMルールを作成し、ILMポリシーをアクティブ化してそのルールを追加します。
4. ONTAP で、新しいアクセスキー、シークレットキー、およびバケット名を指定して、2つ目のクラウド階層を追加します。

StorageGRID FabricPool セットアップ ウィザードにアクセスして完了する

FabricPool セットアップウィザードを使用して、StorageGRID をFabricPool クラウド階層用のオブジェクトストレージシステムとして設定できます。

開始する前に

- FabricPoolセットアップウィザードを使用するためのを確認しておき"考慮事項と要件"ます。

> 他のS3クライアントアプリケーションで使用するStorageGRIDを設定する場合は、に進みます"S3セットアップウィザードを使用する"。

- あなたはを持っています"rootアクセス権限"。

ウィザードにアクセスします

FabricPool セットアップウィザードは、StorageGRID グリッドマネージャの使用を開始したときに完了することも、ウィザードにアクセスして完了することもできます。

手順

1. を使用してGrid Managerにサインインし"サポートされている Web ブラウザ"ます。
2. *FabricPool and S3 セットアップ ウィザード*のバナーがダッシュボードに表示されている場合は、バナー内のリンクを選択してください。バナーが表示されなくなった場合は、Grid Manager のヘッダーバーにあるヘルプアイコン を選択し、*FabricPool and S3 セットアップ ウィザード*を選択してください。

3. FabricPool とS3のセットアップウィザードのページのFabricPool セクションで、* Configure Now *を選択します。

   *ステップ1/9：HAグループの設定*が表示されます。

手順**1/9**：**HA**グループを設定する

ハイアベイラビリティ（HA）グループは、それぞれにStorageGRID ロードバランササービスが含まれるノードの集まりです。HAグループには、ゲートウェイノード、管理ノード、またはその両方を含めることができます。

HAグループを使用すると、FabricPool データ接続の可用性を維持できます。HAグループは、仮想IPアドレス（VIP）を使用してロードバランササービスへの可用性の高いアクセスを提供します。HAグループのアクティブインターフェイスで障害が発生しても、バックアップインターフェイスでワークロードを管理できるため、FabricPool の処理への影響はほとんどありません

このタスクの詳細については、およびを参照してください"ハイアベイラビリティグループを管理します""ハイアベイラビリティグループのベストプラクティス"。

手順

1. 外部のロードバランサを使用する場合は、HAグループを作成する必要はありません。[Skip this step]*を選択し、に進みます[手順2/9：ロードバランサエンドポイントの設定]。
2. StorageGRID ロードバランサを使用するには、新しいHAグループを作成するか、既存のHAグループを使用します。

HA グループを作成します

a. 新しいHAグループを作成するには、*[HAグループの作成]*を選択します。

b. [詳細を入力]*ステップで、次のフィールドに値を入力します。

フィールド	製品説明
HAグループ名	このHAグループの一意の表示名。
概要 （オプション）	このHAグループの概要 。

c. [インターフェイスの追加]*手順で、このHAグループで使用するノードインターフェイスを選択します。

列ヘッダーを使用して行をソートするか、検索キーワードを入力してインターフェイスをより迅速に検索します。

ノードは1つ以上選択できますが、ノードごとに選択できるインターフェイスは1つだけです。

d. [* prioritize interfaces]ステップでは、このHAグループのプライマリインターフェイスとバックアップインターフェイスを決定します。

行をドラッグして、*優先順位*列の値を変更します。

リストの最初のインターフェイスはプライマリインターフェイスです。プライマリインターフェイスは、障害が発生しないかぎり、アクティブインターフェイスです。

HAグループに複数のインターフェイスが含まれていて、アクティブインターフェイスで障害が発生した場合、仮想IP（VIP）アドレスは優先順位に従って最初のバックアップインターフェイスに移動します。そのインターフェイスに障害が発生すると、 VIP アドレスは次のバックアップインターフェイスに移動します。障害が解決されると、 VIP アドレスは利用可能な最優先インターフェイスに戻ります。

e. [IPアドレスの入力]*ステップで、次のフィールドに値を入力します。

フィールド	製品説明
サブネットCIDR	VIPサブネットのアドレス（CIDR表記）。IPv4アドレス、スラッシュ、およびサブネットの長さ（0～32）。 ネットワークアドレスにホストビットを設定しないでください。たとえば、 `192.16.0.0/22`です。
ゲートウェイIPアドレス（オプション）	オプション。StorageGRID へのアクセスに使用するONTAP IPアドレスがStorageGRID VIPアドレスと同じサブネット上にない場合は、StorageGRID VIPローカルゲートウェイのIPアドレスを入力します。ローカルゲートウェイの IP アドレスは VIP サブネット内にある必要があります。

フィールド	製品説明
仮想IPアドレス	HAグループ内のアクティブインターフェイスのVIPアドレスを1つ以上10個以下で入力します。すべてのVIPアドレスはVIPサブネット内に存在する必要があり、すべてがアクティブインターフェイス上で同時にアクティブになります。 IPv4アドレスを少なくとも1つ指定する必要があります。必要に応じて、追加の IPv4 アドレスと IPv6 アドレスを指定できます。

f. を選択し、[終了]*を選択してFabricPool セットアップウィザードに戻ります。

g. [続行]*を選択して、ロードバランサの手順に進みます。

既存の**HA**グループを使用する

a. 既存のHAグループを使用する場合は、*[HAグループの選択]*ドロップダウンリストからHAグループ名を選択します。

b. [続行]*を選択して、ロードバランサの手順に進みます。

手順**2/9**：ロードバランサエンドポイントの設定

StorageGRID は、ロードバランサを使用して、FabricPool などのクライアントアプリケーションからワークロードを管理します。ロードバランシングは、複数のストレージノードにわたって速度と接続容量を最大化します。

すべてのゲートウェイノードと管理ノードに存在するStorageGRID ロードバランササービスを使用することも、外部（サードパーティ）のロードバランサに接続することもできます。StorageGRID ロードバランサを使用することを推奨します。

このタスクの詳細については、一般およびを参照してください"ロードバランシングに関する考慮事項""FabricPool のロードバランシングのベストプラクティス"。

手順

1. StorageGRID ロードバランサエンドポイントを選択または作成するか、外部のロードバランサを使用します。

エンドポイントを作成します

a. [* エンドポイントの作成 *] を選択します。

b. Enter endpoint details *ステップで、次のフィールドに値を入力します。

フィールド	製品説明
名前	エンドポイントのわかりやすい名前。
ポート	ロードバランシングに使用する StorageGRID ポート。最初に作成するエンドポイントのデフォルトは10433ですが、未使用の外部ポートを入力できます。80または443を入力すると、ゲートウェイノードでのみエンドポイントが設定されます。これらのポートは管理ノードで予約されているためです。 *注：*他のグリッドサービスで使用されるポートは許可されません。を参照してください"ネットワークポートのリファレンス"。
クライアントタイプ	は* S3 *にする必要があります。
ネットワークプロトコル	「* HTTPS *」を選択します。 注：TLS暗号化なしでのStorageGRID との通信はサポートされていますが、推奨されません。

c. [結合モードの選択]ステップで、結合モードを指定します。バインドモードは、任意のIPアドレスまたは特定のIPアドレスとネットワークインターフェイスを使用してエンドポイントにアクセスする方法を制御します。

モード	製品説明
グローバル（デフォルト）	クライアントは、任意のゲートウェイノードまたは管理ノードのIPアドレス、任意のネットワーク上の任意のHAグループの仮想IP（VIP）アドレス、または対応するFQDNを使用して、エンドポイントにアクセスできます。 このエンドポイントのアクセスを制限する必要がある場合を除き、 * グローバル * 設定（デフォルト）を使用します。
HA グループの仮想 IP	クライアントがこのエンドポイントにアクセスするには、HAグループの仮想IPアドレス（または対応するFQDN）を使用する必要があります。 このバインドモードのエンドポイントでは、エンドポイント用に選択したHAグループが重複しないかぎり、すべて同じポート番号を使用できます。

モード	製品説明
ノードインターフェイス	クライアントがこのエンドポイントにアクセスするには、選択したノードインターフェイスのIPアドレス（または対応するFQDN）を使用する必要があります。
ノードタイプ	選択したノードのタイプに基づいて、クライアントがこのエンドポイントにアクセスするには、いずれかの管理ノードのIPアドレス（または対応するFQDN）か、いずれかのゲートウェイノードのIPアドレス（または対応するFQDN）を使用する必要があります。

d. [Tenant access]*ステップで、次のいずれかを選択します。

フィールド	製品説明
Allow all tenants（デフォルト）	すべてのテナントアカウントは、このエンドポイントを使用してバケットにアクセスできます。 *[Allow all tenants]*は、ほとんどの場合、FabricPool に使用するロードバランサエンドポイントに適したオプションです。 新しいStorageGRID システムに対してFabricPool セットアップウィザードを使用しており、テナントアカウントをまだ作成していない場合は、このオプションを選択する必要があります。
選択したテナントを許可します	このエンドポイントを使用してバケットにアクセスできるのは、選択したテナントアカウントのみです。
選択したテナントをブロックします	選択したテナントアカウントは、このエンドポイントを使用してバケットにアクセスできません。他のすべてのテナントでこのエンドポイントを使用できます。

e. [証明書の添付]*ステップで、次のいずれかを選択します。

フィールド	製品説明
証明書のアップロード（推奨）	このオプションは、CA署名済みサーバ証明書、証明書秘密鍵、およびオプションのCAバンドルをアップロードする場合に使用します。
証明書の生成	このオプションは、自己署名証明書を生成する場合に使用します。入力する項目の詳細については、を参照してください"ロードバランサエンドポイントを設定する"。
StorageGRID S3証明書を使用する	このオプションは、StorageGRID グローバル証明書のカスタムバージョンをすでにアップロードまたは生成している場合にのみ使用できます。詳細は、を参照してください "S3 API証明書の設定" 。

f. [完了]*を選択して、FabricPool セットアップウィザードに戻ります。

g. [続行]*を選択してテナントとバケットの手順に進みます。

エンドポイント証明書の変更がすべてのノードに適用されるまでに最大 15 分かかることがあります。

既存のロードバランサエンドポイントを使用する

a. [ロードバランサエンドポイントの選択]*ドロップダウンリストから既存のエンドポイントの名前を選択します。

b. [続行]*を選択してテナントとバケットの手順に進みます。

外部のロードバランサを使用する

a. 外部ロードバランサについて、次のフィールドに値を入力します。

フィールド	製品説明
FQDN	外部ロードバランサの完全修飾ドメイン名（FQDN）。
ポート	FabricPool が外部ロードバランサへの接続に使用するポート番号。
証明書	外部ロードバランサのサーバ証明書をコピーして、このフィールドに貼り付けます。

b. [続行]*を選択してテナントとバケットの手順に進みます。

手順**3/9**：テナントとバケット

テナントは、S3アプリケーションを使用してStorageGRID でオブジェクトの格納と読み出しを行うことができるエンティティです。各テナントには、独自のユーザ、アクセスキー、バケット、オブジェクト、および特定の機能セットがあります。FabricPool で使用するバケットを作成する前に、StorageGRID テナントを作成する必要があります。

バケットは、テナントのオブジェクトとオブジェクトメタデータを格納するためのコンテナです。一部のテナントには多数のバケットが含まれている場合もありますが、ウィザードでは一度に1つのテナントと1つのバケットのみを作成または選択できます。Tenant Managerは、あとで必要なバケットを追加するために使用できます。

FabricPool で使用する新しいテナントとバケットを作成するか、既存のテナントとバケットを選択できます。新しいテナントを作成すると、テナントのrootユーザのアクセスキーIDとシークレットアクセスキーが自動的に作成されます。

このタスクの詳細については、およびを参照してください"FabricPool のテナントアカウントを作成します""S3 バケットを作成してアクセスキーを取得する"。

手順

新しいテナントとバケットを作成するか、既存のテナントを選択します。

新しいテナントとバケット

1. 新しいテナントとバケットを作成するには、*[Tenant name]*を入力します。たとえば、 `FabricPool tenant`です。
2. StorageGRIDシステムが使用するかどうかに基づいて、テナントアカウントのルートアクセスを定義します。"アイデンティティフェデレーション" 、"シングルサインオン（SSO）" 、またはその両方。

オプション	手順
アイデンティティフェデレーションが有効になっていない場合	ローカルrootユーザとしてテナントにサインインするときに使用するパスワードを指定します。
アイデンティティフェデレーションが有効になっている場合	a. テナントに対するRoot Access権限を割り当てる既存のフェデレーテッドグループを選択します。 b. 必要に応じて、ローカルrootユーザとしてテナントにサインインする際に使用するパスワードを指定します。
アイデンティティフェデレーションとシングルサインオン（SSO）の両方が有効になっている場合	テナントに対するRoot Access権限を割り当てる既存のフェデレーテッドグループを選択します。ローカルユーザはサインインできません。

3. [Bucket name]*には、FabricPool がONTAP データの格納に使用するバケットの名前を入力します。たとえば、 `fabricpool-bucket`です。

   バケットの作成後にバケット名を変更することはできません。

4. このバケットの*[Region]*を選択します。

   (`us-east-1`将来ILMを使用してバケットのリージョンに基づいてオブジェクトをフィルタリングする予定がないかぎり、デフォルトのリージョンを使用します）。

5. [作成して続行]*を選択してテナントとバケットを作成し、データのダウンロード手順に進みます

テナントとバケットを選択します

既存のテナントアカウントで、バージョン管理が有効になっていないバケットが少なくとも1つ必要です。既存のテナントアカウントのバケットが存在しない場合、そのテナントアカウントを選択することはできません。

1. [Tenant name]*ドロップダウンリストから既存のテナントを選択します。
2. [Bucket name]ドロップダウンリストから既存のバケットを選択します。

   FabricPool ではオブジェクトのバージョン管理がサポートされないため、バージョン管理が有効になっているバケットは表示されません。

FabricPool で使用するS3オブジェクトロックが有効になっているバケットは選択しないでください。

3. [続行]*を選択して、データのダウンロード手順に進みます。

ステップ**4/9: ONTAP** 設定をダウンロードします

この手順では、ONTAP システムマネージャに値を入力するためのファイルをダウンロードします。

手順

1. 必要に応じて、コピーアイコン（）を選択して、アクセスキーIDとシークレットアクセスキーの両方をクリップボードにコピーします。

   これらの値はダウンロードファイルに含まれていますが、個別に保存することもできます。

2. [Download ONTAP settings]*を選択して、これまでに入力した値を含むテキストファイルをダウンロードします。

   この `ONTAP_FabricPool_settings_*bucketname*.txt`ファイルには、StorageGRIDをFabricPoolクラウド階層のオブジェクトストレージシステムとして設定するために必要な次の情報が含まれています。

   - ロードバランサ接続の詳細（サーバ名（FQDN）、ポート、証明書など）
   - バケット名
   - テナントアカウントのrootユーザのアクセスキーIDとシークレットアクセスキー

3. コピーしたキーとダウンロードしたファイルを安全な場所に保存します。

   両方のアクセスキーをコピーするか、ONTAP 設定をダウンロードするか、またはその両方が完了するまで、このページを閉じないでください。このページを閉じると、キーは使用できなくなります。この情報はStorageGRID システムからデータを取得するために使用できるため、必ず安全な場所に保存してください。

4. アクセスキーIDとシークレットアクセスキーをダウンロードまたはコピーしたことを確認するチェックボックスを選択します。

5. [続行]*を選択してILMストレージプールの手順に進みます。

手順**5/9**：ストレージプールを選択します

ストレージプールはストレージノードのグループです。ストレージプールを選択するときは、StorageGRIDがONTAP から階層化されたデータを格納するために使用するノードを決定します。

この手順の詳細については、を参照してください"ストレージプールを作成します"。

手順

1. [サイト]*ドロップダウンリストから、ONTAP から階層化するデータに使用するStorageGRID サイトを選択します。

2. [ストレージプール]*ドロップダウンリストから、そのサイトのストレージプールを選択します。

   サイトのストレージプールには、そのサイトのすべてのストレージノードが含まれます。

3. [Continue（続行）]*を選択してILMルールの手順に進みます。

手順6 / 9：FabricPool のILMルールを確認します

情報ライフサイクル管理（ILM）ルールは、StorageGRID システム内のすべてのオブジェクトの配置、期間、および取り込み動作を制御します。

FabricPool セットアップウィザードでは、FabricPool で使用する推奨されるILMルールが自動的に作成されます。このルールは、指定したバケットにのみ適用されます。1つのサイトで2+1のイレイジャーコーディングを使用して、ONTAP から階層化されたデータを格納します。

この手順の詳細については、およびを参照して"ILM ルールを作成する""FabricPool データでILMを使用するためのベストプラクティス"ください。

手順

1. ルールの詳細を確認します。

フィールド	製品説明
ルール名	自動的に生成され、変更できません
製品説明	自動的に生成され、変更できません
フィルタ	バケット名 このルールは、指定したバケットに保存されている環境 オブジェクトのみです。
参照時間	取り込み時間 配置手順は、オブジェクトがバケットに最初に保存されたときに開始されます。
配置手順	2+1のイレイジャーコーディングを使用

2. 保持図を*と[Storage Pool]*でソートして配置手順を確認します。
   - ルールの* Time Period は Day 0 - Forever です。 0日目*は、ONTAP からデータが階層化されるときにルールが適用されることを意味します。*無期限*は、StorageGRID ILMがONTAPから階層化されたデータを削除しないことを意味します。
   - ルールの*ストレージプール*は、選択したストレージプールです。* EC 2+1 *は、2+1イレイジャーコーディングを使用してデータが格納されることを意味します。各オブジェクトは、2つのデータフラグメントと1つのパリティフラグメントとして保存されます。各オブジェクトの3つのフラグメントが、1つのサイトの別 々 のストレージノードに保存されます。
3. このルールを作成する場合は*[作成して続行]*を選択し、ILMポリシーの手順に進みます。

手順7 / 9：ILMポリシーを確認してアクティブ化します

FabricPoolセットアップウィザードでFabricPool用のILMルールを作成すると、ILMポリシーが作成されます。このポリシーをアクティブ化する前に、ポリシーを慎重にシミュレートして確認する必要があります。

この手順の詳細については、およびを参照して"ILM ポリシーを作成する""FabricPool データでILMを使用するためのベストプラクティス"ください。

> 新しいILMポリシーをアクティブ化すると、StorageGRID はそのポリシーを使用して、既存のオブジェクトと新しく取り込まれるオブジェクトを含むグリッド内のすべてのオブジェクトの配置、期間、およびデータ保護を管理します。場合によっては、新しいポリシーをアクティブ化すると原因 、既存のオブジェクトを新しい場所に移動できるようになります。

> データ損失を回避するために、FabricPoolクラウド階層のデータが期限切れになるILMルールを使用しないでください。FabricPoolオブジェクトがStorageGRID ILMによって削除されないようにするには、保持期間を* forever *に設定します。

手順

1. 必要に応じて、システムによって生成された*ポリシー名*を更新します。デフォルトでは、アクティブポリシーまたは非アクティブポリシーの名前に「+ FabricPool」が追加されますが、独自の名前を指定することもできます。
2. 非アクティブポリシー内のルールのリストを確認します。
   - アクティブでないILMポリシーがグリッドにない場合は、アクティブなポリシーをクローニングして新しいルールを上部に追加することで、アクティブなポリシーが作成されます。
   - アクティブでないILMポリシーがグリッドにすでに設定されており、そのポリシーでアクティブなILMポリシーと同じルールと順序が使用されている場合は、アクティブでないポリシーの先頭に新しいルールが追加されます。
   - 非アクティブポリシーに含まれるルールや順序がアクティブポリシーと異なる場合、ウィザードはアクティブポリシーをクローニングして新しいルールを上部に追加することで、新しい非アクティブポリシーを作成します。
3. 新しい非アクティブポリシー内のルールの順序を確認します。

   FabricPool ルールは最初のルールであるため、FabricPool バケット内のオブジェクトはすべて、ポリシー内の他のルールが評価される前に配置されます。他のバケット内のオブジェクトは、ポリシー内の後続のルールによって配置されます。

4. 保持図を確認して、さまざまなオブジェクトがどのように保持されるかを確認します。
   a. [すべて展開]*を選択すると、非アクティブポリシー内の各ルールの保持図が表示されます。
   b. 保持図を確認するには、**[Time Period]***と[Storage pool]*を選択します。FabricPoolバケットまたはテナントに適用されるルールでオブジェクトが*無期限に保持されることを確認します。
5. 非アクティブポリシーを確認したら、*[アクティブ化して続行]*を選択してポリシーをアクティブ化し、トラフィック分類の手順に進みます。

> ILMポリシーにエラーがあると、原因 で修復不能なデータ損失が発生する可能性があります。アクティブ化する前にポリシーをよく確認してください。

ステップ**8 / 9**：トラフィック分類ポリシーを作成します

オプションとして、FabricPool セットアップウィザードでは、FabricPool ワークロードの監視に使用できるトラフィック分類ポリシーを作成できます。システムによって作成されたポリシーでは、一致ルールを使用して、作成したバケットに関連するすべてのネットワークトラフィックが識別されます。このポリシーはトラフィックのみを監視します。FabricPool またはその他のクライアントのトラフィックは制限されません。

この手順の詳細については、を参照してください"FabricPool のトラフィック分類ポリシーを作成します"。

手順

1. ポリシーを確認します。
2. このトラフィック分類ポリシーを作成する場合は、*[作成して続行]*を選択します。

   FabricPool がStorageGRID へのデータの階層化を開始したらすぐに、[Traffic Classification Policies]ページに移動して、このポリシーのネットワークトラフィック指標を確認できます。あとでルールを追加して他のワークロードを制限し、FabricPool ワークロードの帯域幅がほとんどになるようにすることもできます。

3. それ以外の場合は、*この手順をスキップ*を選択します。

ステップ**9 / 9**：まとめの確認

概要には、ロードバランサ、テナント、バケットの名前、トラフィック分類ポリシー、アクティブなILMポリシーなど、設定した項目の詳細が表示されます。

手順

1. 概要を確認します。
2. [完了] を選択します。

次のステップ

FabricPool ウィザードを完了したら、次の追加手順を実行します。

手順

1. に進み、"ONTAP システムマネージャを設定します"保存された値を入力し、接続のONTAP側を完了します。StorageGRID をクラウド階層として追加し、そのクラウド階層をローカル階層に接続してFabricPoolを作成し、ボリューム階層化ポリシーを設定する必要があります。
2. に移動"DNSサーバの設定"し、StorageGRIDサーバ名（完全修飾ドメイン名）を使用する各StorageGRID IPアドレスに関連付けるレコードがDNSに含まれていることを確認します。
3. StorageGRID監査ログやその他のグローバル設定オプションのベストプラクティスについては、を参照して"StorageGRID および FabricPool に関するその他のベストプラクティスです"ください。

StorageGRID を手動で設定します

StorageGRIDでFabricPool用の高可用性（HA）グループを作成する

FabricPool で使用するように StorageGRID を設定する場合は、必要に応じて 1 つ以上のハイアベイラビリティ（ HA ）グループを作成できます。HAグループは、それぞれにStorageGRID ロードバランササービスが含まれるノードの集まりです。HAグループには、ゲートウェイノード、管理ノード、またはその両方を含めることができます。

HAグループを使用すると、FabricPool データ接続の可用性を維持できます。HAグループは、仮想IPアドレス（VIP）を使用してロードバランササービスへの可用性の高いアクセスを提供します。HAグループのアクティブインターフェイスで障害が発生しても、バックアップインターフェイスでワークロードを管理できるため、FabricPool の処理への影響はほとんどありません。

このタスクの詳細については、を参照してください"ハイアベイラビリティグループを管理します"。FabricPoolセットアップウィザードを使用してこのタスクを実行するには、に進みます"FabricPool セットアップウィザードにアクセスして完了します"。

開始する前に

- を確認しておきます"ハイアベイラビリティグループのベストプラクティス"。
- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"rootアクセス権限"。
- VLAN を使用する場合は、 VLAN インターフェイスを作成しておきます。を参照して "VLAN インターフェイスを設定します"

手順

1. 構成 > ネットワーク > *高可用性グループ*を選択します。
2. 「 * Create * 」を選択します。
3. [詳細を入力]*ステップで、次のフィールドに値を入力します。

フィールド	製品説明
HAグループ名	このHAグループの一意の表示名。
概要 （オプション）	このHAグループの概要 。

4. [インターフェイスの追加]*手順で、このHAグループで使用するノードインターフェイスを選択します。

   列ヘッダーを使用して行をソートするか、検索キーワードを入力してインターフェイスをより迅速に検索します。

   ノードは1つ以上選択できますが、ノードごとに選択できるインターフェイスは1つだけです。

5. [* prioritize interfaces]ステップでは、このHAグループのプライマリインターフェイスとバックアップインターフェイスを決定します。

   行をドラッグして、*優先順位*列の値を変更します。

   リストの最初のインターフェイスはプライマリインターフェイスです。プライマリインターフェイスは、障害が発生しないかぎり、アクティブインターフェイスです。

   HAグループに複数のインターフェイスが含まれていて、アクティブインターフェイスで障害が発生した場合、仮想IP（VIP）アドレスは優先順位に従って最初のバックアップインターフェイスに移動します。そのインターフェイスに障害が発生すると、 VIP アドレスは次のバックアップインターフェイスに移動します。障害が解決されると、 VIP アドレスは利用可能な最優先インターフェイスに戻ります。

6. [IPアドレスの入力]*ステップで、次のフィールドに値を入力します。

フィールド	製品説明
サブネットCIDR	VIPサブネットのアドレス（CIDR表記）。IPv4アドレス、スラッシュ、およびサブネットの長さ（0～32）。 ネットワークアドレスにホストビットを設定しないでください。たとえば、 `192.16.0.0/22`です。
ゲートウェイIPアドレス（オプション）	オプション。StorageGRID へのアクセスに使用するONTAP IPアドレスがStorageGRID VIPアドレスと同じサブネット上にない場合は、StorageGRID VIPローカルゲートウェイのIPアドレスを入力します。ローカルゲートウェイの IP アドレスは VIP サブネット内にある必要があります。
仮想IPアドレス	HAグループ内のアクティブインターフェイスのVIPアドレスを1つ以上10個以下で入力します。すべてのVIPアドレスがVIPサブネット内にある必要があります。 IPv4アドレスを少なくとも1つ指定する必要があります。必要に応じて、追加の IPv4 アドレスと IPv6 アドレスを指定できます。

7. HA グループの作成 * を選択し、完了 * を選択します。

StorageGRID で **FabricPool** 用のロード バランシング エンドポイントを作成する

StorageGRID は、ロードバランサを使用して、FabricPool などのクライアントアプリケーションからワークロードを管理します。ロードバランシングは、複数のストレージノードにわたって速度と接続容量を最大化します。

FabricPool で使用するStorageGRID を設定する場合は、ロードバランサエンドポイントを設定し、ロードバランサエンドポイント証明書をアップロードまたは生成する必要があります。これは、ONTAP とStorageGRID の間の接続を保護するために使用します。

FabricPoolセットアップウィザードを使用してこのタスクを実行するには、に進みます"FabricPool セットアップウィザードにアクセスして完了します"。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"rootアクセス権限"。
- 一般およびを確認しておく必要"FabricPool のロードバランシングのベストプラクティス"があり"ロードバランシングに関する考慮事項"ます。

手順

1. 構成 > ネットワーク > *ロードバランサーエンドポイント*を選択します。
2. 「 * Create * 」を選択します。
3. Enter endpoint details *ステップで、次のフィールドに値を入力します。

フィールド	製品説明
名前	エンドポイントのわかりやすい名前。
ポート	ロードバランシングに使用する StorageGRID ポート。最初に作成するエンドポイントのデフォルトは10433ですが、未使用の外部ポートを入力できます。80または443を入力すると、エンドポイントはゲートウェイノードでのみ設定されます。これらのポートは管理ノードで予約されています。 *注：*他のグリッドサービスで使用されるポートは許可されません。を参照してください"ネットワークポートのリファレンス"。 この番号は、StorageGRID をFabricPool クラウド階層として接続するときにONTAP に指定します。
クライアントタイプ	S3 を選択します。
ネットワークプロトコル	「* HTTPS *」を選択します。 注：TLS暗号化なしでのStorageGRID との通信はサポートされていますが、推奨されません。

4. [結合モードの選択]ステップで、結合モードを指定します。バインドモードは、任意のIPアドレスまたは特定のIPアドレスとネットワークインターフェイスを使用してエンドポイントにアクセスする方法を制御します。

モード	製品説明
グローバル（デフォルト）	クライアントは、任意のゲートウェイノードまたは管理ノードのIPアドレス、任意のネットワーク上の任意のHAグループの仮想IP（VIP）アドレス、または対応するFQDNを使用して、エンドポイントにアクセスできます。 このエンドポイントのアクセスを制限する必要がある場合を除き、 * グローバル * 設定（デフォルト）を使用します。
HA グループの仮想 IP	クライアントがこのエンドポイントにアクセスするには、HAグループの仮想IPアドレス（または対応するFQDN）を使用する必要があります。 このバインドモードのエンドポイントでは、エンドポイント用に選択したHAグループが重複しないかぎり、すべて同じポート番号を使用できます。
ノードインターフェイス	クライアントがこのエンドポイントにアクセスするには、選択したノードインターフェイスのIPアドレス（または対応するFQDN）を使用する必要があります。

モード	製品説明
ノードタイプ	選択したノードのタイプに基づいて、クライアントがこのエンドポイントにアクセスするには、いずれかの管理ノードのIPアドレス（または対応するFQDN）か、いずれかのゲートウェイノードのIPアドレス（または対応するFQDN）を使用する必要があります。

5. [Tenant access]*ステップで、次のいずれかを選択します。

フィールド	製品説明
Allow all tenants（デフォルト）	すべてのテナントアカウントは、このエンドポイントを使用してバケットにアクセスできます。 *[Allow all tenants]*は、ほとんどの場合、FabricPool に使用するロードバランサエンドポイントに適したオプションです。 テナントアカウントをまだ作成していない場合は、このオプションを選択する必要があります。
選択したテナントを許可します	このエンドポイントを使用してバケットにアクセスできるのは、選択したテナントアカウントのみです。
選択したテナントをブロックします	選択したテナントアカウントは、このエンドポイントを使用してバケットにアクセスできません。他のすべてのテナントでこのエンドポイントを使用できます。

6. [証明書の添付]*ステップで、次のいずれかを選択します。

フィールド	製品説明
証明書のアップロード（推奨）	このオプションは、CA署名済みサーバ証明書、証明書秘密鍵、およびオプションのCAバンドルをアップロードする場合に使用します。
証明書の生成	このオプションは、自己署名証明書を生成する場合に使用します。入力する項目の詳細については、を参照してください"ロードバランサエンドポイントを設定する"。
StorageGRID S3証明書を使用する	このオプションは、StorageGRID グローバル証明書のカスタムバージョンをすでにアップロードまたは生成している場合にのみ使用できます。詳細は、を参照してください "S3 API証明書の設定" 。

7. 「 * Create * 」を選択します。

エンドポイント証明書の変更がすべてのノードに適用されるまでに最大 15 分かかることがあります。

StorageGRID で **FabricPool** のテナント アカウントを作成する

Grid Manager で FabricPool 用のテナントアカウントを作成する必要があります。

テナントアカウントを使用すると、クライアントアプリケーションで StorageGRID に対してオブジェクトの格納や読み出しを行うことができます。各テナントアカウントには、専用のアカウント ID 、許可されたグループとユーザ、バケット、オブジェクトがあります。

このタスクの詳細については、を参照してください"テナントアカウントを作成する"。FabricPoolセットアップウィザードを使用してこのタスクを実行するには、に進みます"FabricPool セットアップウィザードにアクセスして完了します"。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- そうだな "特定のアクセス権限"

手順

1. *テナント*を選択します。
2. 「 * Create * 」を選択します。
3. [Enter details]ステップで、次の情報を入力します。

フィールド	製品説明
名前	テナントアカウントの名前。テナント名は一意である必要はありません。作成したテナントアカウントには、一意の数値アカウント ID が割り当てられます。
概要 （オプション）	テナントの特定に役立つ概要 。
クライアントタイプ	FabricPool の場合は* S3 *にする必要があります。
ストレージクォータ（オプション）	FabricPool の場合は、このフィールドを空白のままにします。

4. [アクセス許可の選択]ステップでは、次の手順
   a. [プラットフォームサービスを許可する]*を選択しないでください。

      FabricPool テナントでは、通常、CloudMirrorレプリケーションなどのプラットフォームサービスを使用する必要はありません。

   b. 必要に応じて、*[Use own identity source]*を選択します。
   c. [Allow S3 Select]*を選択しないでください。

      通常、FabricPool テナントではS3 Selectを使用する必要はありません。

   d. オプションで、*グリッドフェデレーション接続を使用する*を選択すると、テナントがアカウント同期およびグリッド間レプリケーションのために"グリッドフェデレーション接続"を使用できるようになります。次に、使用するグリッドフェデレーション接続を選択します。

5. ルートアクセスの定義ステップでは、 StorageGRIDシステムがテナントアカウントの初期ルートアクセス権限を持つユーザーを指定します。"アイデンティティフェデレーション" 、"シングルサインオン（SSO）" 、またはその両方。

オプション	手順
アイデンティティフェデレーションが有効になっていない場合	ローカルrootユーザとしてテナントにサインインするときに使用するパスワードを指定します。
アイデンティティフェデレーションが有効になっている場合	a. テナントに対するRoot Access権限を割り当てる既存のフェデレーテッドグループを選択します。 b. 必要に応じて、ローカルrootユーザとしてテナントにサインインする際に使用するパスワードを指定します。
アイデンティティフェデレーションとシングルサインオン（SSO）の両方が有効になっている場合	テナントに対するRoot Access権限を割り当てる既存のフェデレーテッドグループを選択します。ローカルユーザはサインインできません。

6. [テナントの作成] を選択します。

StorageGRID で **FabricPool** 用の **S3** バケットを作成してアクセス キーを取得

FabricPool ワークロードで StorageGRID を使用する前に、 FabricPool データ用の S3 バケットを作成する必要があります。また、 FabricPool に使用するテナントアカウントのアクセスキーとシークレットアクセスキーを取得する必要があります。

このタスクの詳細については、およびを参照してください"S3 バケットを作成する""独自の S3 アクセスキーを作成します"。FabricPoolセットアップウィザードを使用してこのタスクを実行するには、に進みます"FabricPool セットアップウィザードにアクセスして完了します"。

開始する前に

- FabricPool で使用するテナントアカウントを作成しておきます。
- テナントアカウントへのrootアクセスが必要です。

手順

1. Tenant Manager にサインインします。

   次のいずれかを実行できます。

   - Grid Manager の Tenant Accounts ページで、テナントの * Sign In * リンクを選択し、クレデンシャルを入力します。
   - Web ブラウザでテナントアカウントの URL を入力し、クレデンシャルを入力します。

2. FabricPool データ用の S3 バケットを作成する。

   使用する ONTAP クラスタごとに一意のバケットを作成する必要があります。

   a. ダッシュボードで* View Buckets を選択するか、 storage（S3）> Buckets *を選択します。

b. [* バケットの作成 *] を選択します。

c. FabricPool で使用するStorageGRID バケットの名前を入力します。たとえば、 `fabricpool-bucket`です。

> バケットの作成後にバケット名を変更することはできません。

d. このバケットのリージョンを選択します。

デフォルトでは、すべてのバケットは `us-east-1`地域。デフォルトのリージョンが以下のリージョン以外に設定されている場合 `us-east-1`、ドロップダウンではこの他の領域が最初に選択されます。

e. 「 * Continue * 」を選択します。

f. [* バケットの作成 *] を選択します。

> FabricPool バケットで*を選択しないでください。同様に、**FabricPool**バケットを編集して available やデフォルト以外の整合性を使用しないでください。**FabricPool**バケットに推奨されるバケットの整合性は Read-after-new-write *です。これは新しいバケットのデフォルトの整合性です。

3. アクセスキーとシークレットアクセスキーを作成します。

a. 「 * storage （ S3 ） * > * My access keys * 」を選択します。

b. 「 * キーの作成 * 」を選択します。

c. [アクセスキーの作成 *] を選択します。

d. アクセスキー ID とシークレットアクセスキーを安全な場所にコピーするか、「 * Download.csv * 」を選択してアクセスキー ID とシークレットアクセスキーを含むスプレッドシートファイルを保存します。

これらの値は、 ONTAP で StorageGRID を FabricPool クラウド階層として設定するときに入力します。

> 今後StorageGRID で新しいアクセスキーとシークレットアクセスキーを生成する場合は、新しいキーをONTAP に入力してからStorageGRID から古い値を削除します。そうしないと、ONTAP からStorageGRID に一時的にアクセスできなくなる可能性があります。

FabricPoolデータ用の**StorageGRID ILM**を設定する

このシンプルなサンプルポリシーを、独自のILMルールとポリシーの出発点として使用できます。

この例では、コロラド州デンバーの 1 つのデータセンターに 4 つのストレージノードがある StorageGRID システムの ILM ルールと ILM ポリシーを設計していることを前提としています。この例のFabricPoolデータでは、というバケットを使用して `fabricpool-bucket`います。

以下の ILM ルールとポリシーは一例にすぎません。ILM ルールを設定する方法は多数あります。新しいポリシーをアクティブ化する前に、ポリシーをシミュレートして、コンテンツを損失から保護するために意図したとおりに機能することを確認します。詳細については、を参照してください"ILM を使用してオブジェクトを管理する"。

データ損失を回避するために、FabricPoolクラウド階層のデータが期限切れになるILMルールを使用しないでください。FabricPoolオブジェクトがStorageGRID ILMによって削除されないようにするには、保持期間を* forever *に設定します。

開始する前に

- を確認しておきます"FabricPool データでILMを使用するためのベストプラクティス"。
- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"ILMまたはRoot Access権限"。
- StorageGRID 11.7より前のバージョンからStorageGRID 12.1にアップグレードした場合は、使用するストレージプールが構成済みです。一般的に、データの保存に使用するStorageGRIDサイトごとにストレージプールを作成する必要があります。（バージョン11.7以降、ストレージプールはサイトごとに自動的に作成されます。）

この前提条件は、StorageGRID 11.7または11.8を最初にインストールした場合は適用されません。これらのバージョンのいずれかを最初にインストールすると、サイトごとにストレージプールが自動的に作成されます。

手順

1. のデータにのみ適用するILMルールを作成し `fabricpool-bucket`ます。この例では、イレイジャーコーディングコピーを作成します。

ルール定義	値の例
ルール名	2+1のイレイジャーコーディング（FabricPool データ用
バケット名	`fabricpool-bucket` FabricPool テナントアカウントでフィルタリングすることもできます。
高度なフィルタ	オブジェクトサイズが0.2MBを超えています。 注： FabricPool は4MBのオブジェクトのみを書き込みますが、このルールではイレイジャーコーディングを使用するため、オブジェクトサイズフィルタを追加する必要があります。
参照時間	取り込み時間

ルール定義	値の例
期間と配置	From Day 0は永久に保存されます デンバーで2+1 ECスキームを使用してイレイジャーコーディングしてオブジェクトを格納し、それらのオブジェクトをStorageGRIDに無期限に保持 データ損失を回避するために、FabricPoolクラウド階層のデータが期限切れになるILMルールを使用しないでください。
取り込み動作	バランス

2. 最初のルールに一致しないオブジェクトのレプリケートコピーを2つ作成するデフォルトのILMルールを作成します。基本フィルタ（テナントアカウントまたはバケット名）や高度なフィルタは選択しないでください。

ルール定義	値の例
ルール名	2 つのレプリケートコピー
バケット名	_ なし _
高度なフィルタ	_ なし _
参照時間	取り込み時間
期間と配置	From Day 0は永久に保存されます デンバーに2つのコピーをレプリケートしてオブジェクトを格納
取り込み動作	バランス

3. ILMポリシーを作成し、2つのルールを選択します。レプリケーションルールではフィルタを使用しないため、ポリシーのデフォルト（最後の）ルールを使用できます。
4. テストオブジェクトをグリッドに取り込みます。
5. ポリシーをテストオブジェクトでシミュレートして動作を確認します。
6. ポリシーをアクティブ化する。

このポリシーをアクティブ化すると、 StorageGRID はオブジェクトデータを次のように配置します。

- のFabricPoolから階層化されたデータ `fabricpool-bucket`は、2+1イレイジャーコーディングスキームを使用してイレイジャーコーディングされます。2 つのデータフラグメントと 1 つのパリティフラグメントが 3 つの異なるストレージノードに配置されます。
- 他のすべてのバケット内のオブジェクトがレプリケートされます。2 つのコピーが作成され、 2 つの異な

るストレージノードに配置されます。

- コピーはStorageGRIDで無期限に保持されます。StorageGRID ILMではこれらのオブジェクトは削除されません。

StorageGRIDで**FabricPool**のトラフィック分類ポリシーを作成する

必要に応じて、 StorageGRID トラフィック分類ポリシーを設計して、 FabricPool ワークロードのサービス品質を最適化できます。

このタスクの詳細については、を参照してください"トラフィック分類ポリシーを管理します"。FabricPoolセットアップウィザードを使用してこのタスクを実行するには、に進みます"FabricPool セットアップウィザードにアクセスして完了します"。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"rootアクセス権限"。

タスクの内容

FabricPool のトラフィック分類ポリシーを作成する場合のベストプラクティスは、次のようにワークロードによって異なります。

- FabricPool のプライマリワークロードのデータをStorageGRID に階層化する場合は、FabricPool ワークロードの帯域幅がほとんどになるようにする必要があります。トラフィック分類ポリシーを作成して、他のすべてのワークロードを制限できます。

  一般に、 FabricPool の読み取り処理は、書き込み処理よりも優先順位を付けることが重要です。

  たとえば、他の S3 クライアントがこの StorageGRID システムを使用している場合は、トラフィック分類ポリシーを作成する必要があります。他のバケット、テナント、 IP サブネット、またはロードバランサエンドポイントのネットワークトラフィックを制限できます。

- 通常、FabricPoolワークロードにQoS制限を課すことはなく、他のワークロードだけを制限します。
- 他のワークロードに適用される制限には、ワークロードの動作を考慮する必要があります。また、グリッドのサイジングと機能、および想定される利用率に応じて、制限が適用されます。

手順

1. 構成 > ネットワーク > *トラフィック分類*を選択します。
2. 「 * Create * 」を選択します。
3. ポリシーの名前と概要 （オプション）を入力し、* Continue *を選択します。
4. [一致ルールの追加]ステップで、少なくとも1つのルールを追加します。
   a. [ルールの追加]*を選択します
   b. [Type]で、*[Load balancer endpoint]*を選択し、FabricPool 用に作成したロードバランサエンドポイントを選択します。

      FabricPool テナントアカウントまたはバケットを選択することもできます。

c. このトラフィックポリシーで他のエンドポイントのトラフィックを制限する場合は、* Inverse Match * を選択します。

5. 必要に応じて、1つ以上の制限を追加して、ルールに一致するネットワークトラフィックを制御します。

> StorageGRID では、制限を追加しなくても指標が収集されるため、トラフィックの傾向を把握できます。

a. [制限の追加]*を選択します。

b. 制限するトラフィックのタイプと適用する制限を選択します。

6. 「 * Continue * 」を選択します。

7. トラフィック分類ポリシーを読んで確認します。前へ*ボタンを使用して前に戻り、必要に応じて変更を行います。ポリシーに問題がなければ、*[保存して続行]*を選択します。

終わったら

"ネットワークトラフィックの指標を表示します"ポリシーが想定どおりのトラフィック制限を適用していることを確認します。

ONTAP System Manager を設定して、StorageGRID を FabricPool クラウド階層として追加します

必要なStorageGRID 情報を入手したら、ONTAP に移動してStorageGRID をクラウド階層として追加できます。

開始する前に

- FabricPoolセットアップウィザードが完了すると、 `ONTAP_FabricPool_settings_*bucketname*.txt`ファイルがダウンロードされます。
- StorageGRID を手動で設定した場合は、StorageGRID に使用する完全修飾ドメイン名（FQDN）またはStorageGRID HAグループの仮想IP（VIP）アドレス、ロードバランサエンドポイントのポート番号、ロードバランサ証明書が必要です。 テナントアカウントのrootユーザのアクセスキーIDとシークレットキー、およびそのテナントでONTAP が使用するバケットの名前。

ONTAP システムマネージャにアクセスします

ここでは、ONTAP System Managerを使用してStorageGRID をクラウド階層として追加する方法について説明します。ONTAP CLIを使用して同じ設定を行うことができます。手順については、を参照してください "FabricPoolのONTAPドキュメント"。

手順

1. StorageGRID に階層化するONTAP クラスタのSystem Managerにアクセスします。
2. クラスタの管理者としてサインインします。
3. >[階層]>[クラウド階層の追加]*に移動します。
4. オブジェクトストアプロバイダのリストから* StorageGRID *を選択します。

StorageGRID 値を入力します

詳細については、を参照してください "FabricPoolのONTAPドキュメント" 。

手順

1. ファイルまたは手動で取得した値を使用して、[クラウド階層の追加]フォームに入力し `ONTAP_FabricPool_settings_*bucketname*.txt`ます。

フィールド	製品説明
名前	このクラウド階層の一意の名前を入力してください。デフォルト値をそのまま使用できます。
URLスタイル	"S3エンドポイントのドメイン名が設定されました"の場合は、仮想ホスト型**URL** を選択してください。 パス形式の**URL** は ONTAP のデフォルトですが、StorageGRID では仮想ホスト形式のリクエストの使用が推奨されます。サーバー名（**FQDN**） フィールドにドメイン名の代わりに IP アドレスを指定する場合は、パス形式の**URL** を使用する必要があります。
サーバ名（FQDN）	StorageGRID に使用する完全修飾ドメイン名（FQDN）またはStorageGRID HAグループの仮想IP（VIP）アドレスを入力します。たとえば、`s3.storagegrid.*company*.com`です。 次の点に注意してください。 • ここで指定するIPアドレスまたはドメイン名は、StorageGRID ロードバランサエンドポイント用にアップロードまたは生成した証明書と一致している必要があります。 • ドメイン名を指定する場合は、StorageGRID への接続に使用する各IPアドレスにDNSレコードをマッピングする必要があります。を参照して "DNSサーバの設定"
SSL	有効（デフォルト）
オブジェクトストアの証明書	StorageGRIDロードバランサエンドポイントに使用する証明書PEM（および `-----END CERTIFICATE-----`）を貼り付けます `-----BEGIN CERTIFICATE-----`。 • 注：中間 CA が StorageGRID 証明書を発行した場合は、中間 CA 証明書を指定する必要があります。StorageGRID 証明書がルート CA によって直接発行された場合は、ルート CA 証明書を指定する必要があります。
ポート	StorageGRID ロードバランサエンドポイントで使用するポートを入力します。ONTAP はStorageGRID に接続するときにこのポートを使用します。たとえば、10433と入力します。

フィールド	製品説明
アクセスキーとシークレットキー	StorageGRID テナントアカウントのrootユーザのアクセスキーIDとシークレットアクセスキーを入力します。 ヒント：今後StorageGRID で新しいアクセスキーとシークレットアクセスキーを生成する場合は、新しいキーをONTAP に入力してから、StorageGRID から古い値を削除します。そうしないと、ONTAP からStorageGRID に一時的にアクセスできなくなる可能性があります。
コンテナ名	このONTAP 階層で使用するために作成したStorageGRID バケットの名前を入力します。

2. ONTAP で最後のFabricPool 設定を完了します。
   a. 1つ以上のアグリゲートをクラウド階層に接続します。
   b. 必要に応じて、ボリューム階層化ポリシーを作成します。

FabricPoolを使用したStorageGRIDのDNSサーバーエントリを設定する

ハイアベイラビリティグループ、ロードバランサエンドポイント、およびS3エンドポイントのドメイン名を設定したら、DNSにStorageGRID に必要なエントリが含まれていることを確認する必要があります。セキュリティ証明書の名前ごと、および使用するIPアドレスごとに、DNSエントリを含める必要があります。

を参照して "ロードバランシングに関する考慮事項"

StorageGRID サーバ名のDNSエントリ

StorageGRID サーバ名（完全修飾ドメイン名）を使用する各StorageGRID IPアドレスに関連付けるDNSエントリを追加します。DNSに入力するIPアドレスは、ロードバランシングノードのHAグループを使用しているかどうかによって異なります。

- HAグループを設定している場合、ONTAP はそのHAグループの仮想IPアドレスに接続します。
- HAグループを使用しない場合は、ONTAP からゲートウェイノードまたは管理ノードのIPアドレスを使用してStorageGRID ロードバランササービスに接続できます。
- サーバ名が複数のIPアドレスに解決されると、ONTAP はすべてのIPアドレス（最大16個のIPアドレス）を使用してクライアント接続を確立します。接続が確立されると、ラウンドロビン方式でIPアドレスが取得されます。

仮想ホスト型リクエスト用のDNSエントリ

"S3エンドポイントのドメイン名"を定義済みで、仮想ホスト型のリクエストを使用する場合は、ワイルドカード名を含む必要なすべての S3 エンドポイントドメイン名の DNS エントリを追加してください。

FabricPool に関するStorageGRID のベストプラクティス

FabricPoolを使用したStorageGRID高可用性（HA）グループのベストプラクティス

StorageGRID をFabricPool クラウド階層として接続する前に、StorageGRID のハイアベイラビリティ（HA）グループについて確認し、FabricPool でHAグループを使用する場合のベストプラクティスを確認してください。

HA グループとは何ですか？

ハイアベイラビリティ（HA）グループは、複数のStorageGRID ゲートウェイノード、管理ノード、またはその両方のインターフェイスの集まりです。HAグループは、クライアントデータ接続の可用性を維持するのに役立ちます。HAグループのアクティブインターフェイスで障害が発生しても、FabricPool の処理にほとんど影響を与えずにバックアップインターフェイスでワークロードを管理できます。

各 HA グループは、関連付けられたノード上の共有サービスへの可用性の高いアクセスを提供します。たとえば、ゲートウェイノード上のインターフェイスのみ、または管理ノードとゲートウェイノードの両方で構成される HA グループは、共有のロードバランササービスへの可用性の高いアクセスを提供します。

ハイアベイラビリティグループの詳細については、を参照してください"ハイアベイラビリティ（HA）グループを管理します"。

HAグループを使用する

FabricPool 用のStorageGRID HAグループを作成するためのベストプラクティスは、ワークロードによって異なります。

- プライマリワークロードのデータでFabricPool を使用する場合は、データの読み出しが中断されないように、少なくとも2つのロードバランシングノードを含むHAグループを作成する必要があります。
- FabricPool の snapshot-only のボリューム階層化ポリシーまたは非プライマリのローカルのパフォーマンス階層（ディザスタリカバリ先や NetApp SnapMirror ® デスティネーションなど）を使用する予定の場合は、 1 つのノードだけで HA グループを設定できます。

ここでは、アクティブ / バックアップ HA の HA グループの設定（一方のノードがアクティブでもう一方のノードがバックアップ）について説明します。ただし、 DNS ラウンドロビンまたはアクティブ / アクティブ HA を使用することもできます。これらの他のHA構成の利点については、を参照してください"HA グループの設定オプション"。

FabricPoolを使用したStorageGRIDロード バランシングのベストプラクティス

StorageGRID をFabricPool クラウド階層として接続する前に、FabricPool でロードバランサを使用する際のベストプラクティスを確認してください。

StorageGRIDロードバランサとロードバランサ証明書に関する一般的な情報については、を参照してください"ロードバランシングに関する考慮事項"。

FabricPool に使用するロードバランサエンドポイントへのテナントアクセスのベストプラクティス

特定のロードバランサエンドポイントを使用してバケットにアクセスできるテナントを制御できます。すべてのテナントを許可するか、一部のテナントを許可するか、または一部のテナントをブロックすることができます。FabricPool で使用する負荷分散エンドポイントを作成する場合は、*[すべてのテナントを許可する]*を選択します。ONTAP はStorageGRID バケットに格納されているデータを暗号化するため、この追加のセキュリティレイヤによって提供されるセキュリティはほとんどありません。

FabricPool で使用するStorageGRID ロードバランサエンドポイントを作成するときは、ONTAP でStorageGRID を認証するためのセキュリティ証明書を指定します。

ほとんどの場合、ONTAP とStorageGRID 間の接続では、Transport Layer Security（TLS）暗号化を使用する必要があります。TLS暗号化なしでのFabricPool の使用はサポートされていますが、推奨されませんStorageGRID ロードバランサエンドポイントのネットワークプロトコルを選択する場合は、*[HTTPS]*を選択します。次に、StorageGRID でONTAP を認証するためのセキュリティ証明書を指定します。

ロードバランシングエンドポイントのサーバ証明書の詳細を確認するには、次の手順を実行します。

- "セキュリティ証明書を管理する"
- "ロードバランシングに関する考慮事項"
- "サーバ証明書のセキュリティ強化ガイドライン"

ONTAP に証明書を追加します

StorageGRID をFabricPool クラウド階層として追加する場合は、ルート証明書と下位の認証局（CA）証明書を含む同じ証明書をONTAP クラスタにインストールする必要があります。

証明書の有効期限の管理

> ONTAP とStorageGRID 間の接続の保護に使用されている証明書の有効期限が切れると、FabricPool は一時的に機能を停止し、ONTAP はStorageGRID に階層化されたデータに一時的にアクセスできなくなります。

証明書の有効期限の問題を回避するには、次のベストプラクティスに従ってください。

- 証明書の有効期限が近づいていることを警告するアラート（* Expiration of load balancer endpoint certificate や Expiration of global server certificate for S3 API *アラートなど）を注意深く監視します。
- 証明書のStorageGRID バージョンとONTAP バージョンは常に同期しておいてください。ロードバランサエンドポイントに使用する証明書を交換または更新する場合は、クラウド階層用のONTAP で使用される同等の証明書を置き換えるか更新する必要があります。
- 公開署名されたCA証明書を使用する。CAによって署名された証明書を使用する場合は、グリッド管理APIを使用して証明書のローテーションを自動化できます。これにより、有効期限が近い証明書を無停止で交換できます。
- 自己署名StorageGRID 証明書を生成した証明書の有効期限が近づいている場合は、既存の証明書の有効期限が切れる前に、StorageGRID とONTAP の両方で証明書を手動で置き換える必要があります。自己署名証明書の有効期限が切れている場合は、アクセスが失われないように、ONTAP で証明書の検証をオフにします。

  手順については'を参照して "ネットアップナレッジベース：既存のONTAP FabricPool 環境に新しいStorageGRID 自己署名サーバ証明書を設定する方法"ください

StorageGRID ILMを**FabricPool**データで使用するためのベストプラクティス

FabricPool を使用してStorageGRID にデータを階層化する場合は、StorageGRID の情報ライフサイクル管理（ILM）をFabricPool データで使用するための要件を理解しておく

必要があります。

> FabricPool は、 StorageGRID の ILM ルールやポリシーを認識しません。StorageGRID の ILM ポリシーの設定ミスが原因でデータが失われる可能性があります。詳細については、およびを参照してください"ILMルールを使用したオブジェクトの管理""ILMポリシーの作成"。

FabricPool で**ILM**を使用する場合のガイドライン

FabricPoolセットアップウィザードを使用すると、作成したS3バケットごとに新しいILMルールが自動的に作成され、非アクティブなポリシーに追加されます。ポリシーをアクティブ化するように求められます。自動で作成されたルールは、推奨されるベストプラクティスに従います。1つのサイトで2+1のイレイジャーコーディングを使用します。

FabricPool セットアップウィザードを使用せずにStorageGRID を手動で設定する場合は、次のガイドラインを確認して、ILMルールとILMポリシーがFabricPool のデータやビジネス要件に適していることを確認してください。これらのガイドラインに従って、新しいルールを作成し、アクティブなILMポリシーを更新しなければならない場合があります。

- レプリケーションルールとイレイジャーコーディングルールを任意に組み合わせて、クラウド階層のデータを保護できます。

  コスト効率に優れたデータ保護を実現するために、サイト内で 2+1 のイレイジャーコーディングを使用することを推奨します。イレイジャーコーディングは CPU 使用率は高くなりますが、レプリケーションよりもストレージ容量が大幅に少なくなります。4+1 スキームと 6+1 スキームは 2+1 スキームよりも容量が少ないただし、グリッドの拡張時にストレージノードを追加する必要がある場合、 4+1 スキームと 6+1 スキームの柔軟性は低くなります。詳細については、を参照してください "イレイジャーコーディングオブジェクトのストレージ容量を追加します"。

- FabricPool データに適用するルールは、イレイジャーコーディングを使用するか、少なくとも 2 つのレプリケートコピーを作成する必要があります。

  > ある期間にレプリケートコピーを 1 つしか作成しない ILM ルールには、データが永続的に失われるリスクがあります。オブジェクトのレプリケートコピーが 1 つしかない場合、ストレージノードに障害が発生したり、重大なエラーが発生すると、そのオブジェクトは失われます。また、アップグレードなどのメンテナンス作業中は、オブジェクトへのアクセスが一時的に失われます。

- 必要に応じて"StorageGRIDからFabricPoolデータを削除します"、ONTAPを使用してFabricPoolボリュームのすべてのデータを取得し、高パフォーマンス階層に昇格します。

  > データ損失を回避するために、FabricPoolクラウド階層のデータが期限切れになるILMルールを使用しないでください。StorageGRID ILMによってFabricPoolオブジェクトが削除されないように、各ILMルールの保持期間を* forever *に設定します。

- FabricPool クラウド階層のデータをバケットから別の場所に移動するルールを作成しないでください。クラウドストレージプールを使用してFabricPool データを別のオブジェクトストアに移動することはできません。

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

- ONTAP 9.8 以降では、オプションでオブジェクトタグを作成して階層化データを分類およびソートし、管理を容易にすることができます。たとえば、タグを設定できるのは、 StorageGRID に接続されている FabricPool ボリュームのみです。次に、 StorageGRID で ILM ルールを作成する際に、高度なフィルタ「オブジェクトタグ」を使用してこのデータを選択し、配置します。

FabricPoolを使用した**StorageGRID**グローバル設定のベストプラクティス

FabricPool で使用するStorageGRID システムを設定する場合は、他のStorageGRID オプションの変更が必要になることがあります。グローバル設定を変更する前に、変更が他のS3アプリケーションにどのように影響するかを検討してください。

監査メッセージとログの送信先

FabricPool ワークロードでは多くの場合読み取り処理の割合が高く、大量の監査メッセージが生成される可能性があります。

- FabricPoolまたはその他の S3 アプリケーションのクライアント読み取り操作の記録が不要な場合は、オプションで 構成 > 監視 > 監査および **syslog** サーバー に移動します。監査ログに記録される監査メッセージの数を減らすには、*クライアント読み取り*設定を*エラー*に変更します。見る"ログ管理と外部Syslogサーバーを構成する"詳細については。
- 大規模なグリッドを使用する場合、複数のタイプのS3アプリケーションを使用する場合、またはすべての監査データを保持する場合は、外部のsyslogサーバを設定し、監査情報をリモートで保存します。外部サーバを使用すると、監査データの完全性を損なうことなく、監査メッセージロギングによるパフォーマンスへの影響を最小限に抑えることができます。詳細は、を参照してください "外部 syslog サーバに関する考慮事項" 。

オブジェクトの暗号化

StorageGRIDを設定する際に、他のStorageGRIDクライアントでデータ暗号化が必要な場合は、オプションでを有効にすることができます"格納オブジェクトの暗号化のグローバルオプション"。FabricPool から StorageGRID に階層化されたデータはすでに暗号化されているため、 StorageGRID 設定を有効にする必要はありません。クライアント側の暗号化キーはONTAPが所有します。

オブジェクトの圧縮

StorageGRIDを設定するときは、を有効にしないで"格納オブジェクトを圧縮するグローバルオプション"ください。FabricPool から StorageGRID に階層化されたデータはすでに圧縮されています。StorageGRID オプションを使用しても、オブジェクトのサイズはさらに縮小されません。

S3 オブジェクトのロック

StorageGRIDシステムでグローバルS3オブジェクトロック設定が有効になっている場合は、有効にしないでください。"S3 オブジェクトのロック" FabricPoolバケットを作成するとき。 S3 オブジェクト ロックはFabricPoolバケットではサポートされていません。

バケット整合性

FabricPoolバケットの場合、推奨されるバケット整合性は* Read-after-new-write であり、これは新しいバケットのデフォルトの整合性です。**FabricPool**バケットを編集して available または strong-site *を使用しないでください。

StorageGRID ノードがNetApp ONTAP システムから割り当てられたストレージを使用している場合は、ボリュームでFabricPool 階層化ポリシーが有効になっていないことを確認してください。たとえば、StorageGRID ノードが VMware ホストで実行されている場合は、 StorageGRID ノードのデータストアの作成元ボリュームで FabricPool 階層化ポリシーが有効になっていないことを確認します。StorageGRIDノードで使用するボリュームでFabricPool階層化を無効にすると、トラブルシューティングとストレージの処理が簡単になります。

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

StorageGRIDからFabricPoolデータを削除します

StorageGRIDに現在格納されているFabricPoolデータを削除する必要がある場合は、ONTAPを使用してFabricPoolボリュームのすべてのデータを取得し、高パフォーマンス階層に昇格する必要があります。

開始する前に

- の手順と考慮事項を確認しておき "高パフォーマンス階層にデータを昇格"ます。
- ONTAP 9.8以降を使用している。
- を使用している"サポートされている Web ブラウザ"。
- が搭載されたFabricPoolテナントアカウントのStorageGRIDユーザグループに属している必要があり"すべてのバケットまたはRoot Access権限を管理します"ます。

タスクの内容

ここでは、StorageGRIDからFabricPoolにデータを戻す方法について説明します。この手順は、ONTAPとStorageGRIDのテナントマネージャを使用して実行します。

手順

1. ONTAPから、コマンドを実行し `volume modify`ます。

   新しい階層化を停止するにはに `none`設定し `tiering-policy`、以前に階層化されたすべてのデータをStorageGRIDに戻すにはに `promote`設定 `cloud-retrieval-policy`します。

   を参照してください "FabricPoolボリュームのすべてのデータを高パフォーマンス階層に昇格"

2. 処理が完了するまで待ちます。

   コマンドにオプションを "高パフォーマンス階層への昇格のステータスを確認します"指定して `tiering`使用できます `volume object-store`。

3. 昇格処理が完了したら、FabricPoolテナントアカウントのStorageGRIDテナントマネージャにサインインします。
4. ダッシュボードで* View Buckets を選択するか、 storage（S3）> Buckets *を選択します。
5. FabricPoolバケットが空になったことを確認します。

6. バケットが空の場合は、"バケットを削除します"

終了後

バケットを削除すると、FabricPoolからStorageGRIDへの階層化を続行できなくなります。ただし、ローカル階層は引き続きStorageGRIDクラウド階層に接続されているため、ONTAP System Managerからバケットにアクセスできないことを示すエラーメッセージが返されます。

これらのエラーメッセージが表示されないようにするには、次のいずれかを実行します。

- FabricPoolミラーを使用して、別のクラウド階層をアグリゲートに接続します。
- FabricPoolアグリゲートからFabricPool以外のアグリゲートにデータを移動してから、使用されていないアグリゲートを削除します。

手順については、を参照して "FabricPoolのONTAPドキュメント"ください。

StorageGRIDのテナントとクライアントの使用

テナントアカウントを使用する

StorageGRID テナントアカウントを使用する

テナントアカウントを使用すると、Simple Storage Service（S3）REST APIを使用して、StorageGRIDシステム内のオブジェクトの格納と読み出しを行うことができます。

テナントアカウントとは何ですか？

各テナントアカウントには、フェデレーテッド/ローカルグループ、ユーザ、S3バケット、オブジェクトがあります。

テナントアカウントを使用すると、格納されているオブジェクトをエンティティごとに分離できます。たとえば、次のようなユースケースでは複数のテナントアカウントを使用できます。

- * エンタープライズのユースケース： StorageGRID システムがエンタープライズ内で使用されている場合は、組織の部門ごとにグリッドのオブジェクトストレージを分けることができます。たとえば、マーケティング部門、カスタマーサポート部門、人事部門などのテナントアカウントが存在する場合があります。

> S3 クライアント プロトコルを使用する場合は、S3 バケットとバケット ポリシーを使用して、企業内の部門間でオブジェクトを分離することもできます。個別のテナント アカウントを作成する必要はありません。実装手順を参照"S3バケットとバケットポリシー"詳細についてはこちらをご覧ください。

- * サービスプロバイダのユースケース： * StorageGRID システムがサービスプロバイダによって使用されている場合は、ストレージをリースするエンティティごとにグリッドのオブジェクトストレージを分けることができます。たとえば、会社 A 、会社 B 、会社 C などのテナントアカウントを作成できます。

テナントアカウントを作成する方法

テナントアカウントは、によって作成され"グリッドマネージャを使用した StorageGRID のグリッド管理者"ます。グリッド管理者は、テナントアカウントを作成する際に次の項目を指定します。

- テナント名、クライアントタイプ（S3）、オプションのストレージクォータなどの基本情報。
- テナントアカウントに対する権限（テナントアカウントがS3プラットフォームサービスを使用できるか、独自のアイデンティティソースを設定できるか、S3 Selectを使用できるか、グリッドフェデレーション接続を使用できるかなど）。
- テナントの初期ルートアクセス（StorageGRID システムがローカルグループとユーザ、アイデンティティフェデレーション、シングルサインオン（SSO）のいずれを使用しているかに基づく）。

また、 S3 テナントアカウントが規制要件に準拠する必要がある場合は、グリッド管理者が StorageGRID システムに対して S3 オブジェクトロック設定を有効にすることができます。S3 オブジェクトのロックを有効にすると、すべての S3 テナントアカウントで準拠バケットを作成、管理できます。

のあと"S3 テナントアカウントが作成されます"、Tenant Managerにアクセスして次のタスクを実行できます。

- アイデンティティフェデレーションを設定する（グリッドとアイデンティティソースを共有する場合を除く）
- グループとユーザを管理します
- アカウント同期とグリッド間レプリケーションにはグリッドフェデレーションを使用します
- S3 アクセスキーを管理します
- S3バケットを作成、管理します
- S3プラットフォームサービスを使用する
- S3 Select を使用する
- ストレージの使用状況を監視



S3バケットはTenant Managerを使用して作成および管理できますが、オブジェクトの取り込みと管理にはまたはを"S3コンソール"使用する必要があります"S3 クライアント"。

サインインとサインアウトの方法

StorageGRID Tenant ManagerにSign in

Tenant Managerにアクセスするには、のアドレスバーにテナントのURLを入力し"サポートされている Web ブラウザ"ます。

開始する前に

- ログインクレデンシャルが必要です。
- Tenant Managerにアクセスするためのを、グリッド管理者から入手しておきます。URL は次のいずれかの例のようになります。

```
https://FQDN_or_Admin_Node_IP/

https://FQDN_or_Admin_Node_IP:port/

https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id

https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id
```

URLには、必ず完全修飾ドメイン名（FQDN）、管理ノードのIPアドレス、または管理ノードのHAグループの仮想IPアドレスが含まれます。ポート番号、20桁のテナントアカウントID、またはその両方を指定することもできます。

- URLに20桁のテナントアカウントIDが含まれていない場合は、このアカウントIDが必要です。
- を使用している"サポートされている Web ブラウザ"。
- Web ブラウザでクッキーが有効になっている必要があります。

- ユーザは、のユーザグループに属して"特定のアクセス権限"います。

手順

1. を起動し"サポートされている Web ブラウザ"ます。
2. ブラウザのアドレスバーに、 Tenant Manager にアクセスするための URL を入力します。
3. セキュリティアラートが表示された場合は、ブラウザのインストールウィザードを使用して証明書をインストールします。
4. Tenant Manager にサインインします。

   表示されるサインイン画面は、入力したURLと、StorageGRID 用にシングルサインオン（SSO）が設定されているかどうかによって異なります。

   SSOを使用しない

   StorageGRID がSSOを使用していない場合は、次のいずれかの画面が表示されます。

   - Grid Manager のサインインページが表示されます。[Tenant sign-in]*リンクを選択します。
   - テナント マネージャーのサインイン ページ。 アカウント フィールドはすでに入力されている可能性があります。
     i. テナントの 20 桁のアカウント ID が表示されない場合は、最近のアカウントのリストにテナントアカウントが表示されている場合はその名前を選択するか、アカウント ID を入力します。
     ii. ユーザ名とパスワードを入力します。
     iii. 「サインイン」を選択します。

     Tenant Managerダッシュボードが表示されます。

     iv. 他のユーザーから初期パスワードを受け取った場合は、**_ username_**>* Change password * を選択してアカウントを保護します。

   SSOを使用する

   StorageGRID がSSOを使用している場合は、次のいずれかの画面が表示されます。

   - 組織の SSO ページ。

     標準のSSOクレデンシャルを入力し、*[サインイン]*を選択します。

   - Tenant Manager の SSO サインインページ。
     i. テナントの 20 桁のアカウント ID が表示されない場合は、最近のアカウントのリストにテナントアカウントが表示されている場合はその名前を選択するか、アカウント ID を入力します。
     ii. 「サインイン」を選択します。
     iii. 組織の SSO サインインページで通常使用している SSO クレデンシャルを使用してサインインします。

     Tenant Managerダッシュボードが表示されます。

StorageGRID Tenant Managerからサインアウトします

Tenant Managerの操作が完了したら、サインアウトして、権限のないユーザがStorageGRID システムにアクセスできないようにする必要があります。ブラウザのクッキーの設定によっては、ブラウザを閉じてもシステムからサインアウトされない場合があります。

手順

1. ユーザインターフェイスの右上にあるユーザ名ドロップダウンを探します。
2. ユーザ名を選択し、*[サインアウト]*を選択します。

   - SSO を使用していない場合：

     管理ノードからサインアウトされます。Tenant Manager のサインインページが表示されます。

     > 複数の管理ノードにサインインした場合は、各ノードからサインアウトする必要があります。

   - SSO が有効になっている場合は、次

     アクセスしていたすべての管理ノードからサインアウトされます。StorageGRID のサインインページが表示されます。アクセスしたテナントアカウントの名前がデフォルトで「 Recent Accounts * 」ドロップダウンに表示され、テナントの * アカウント ID * が表示されます。

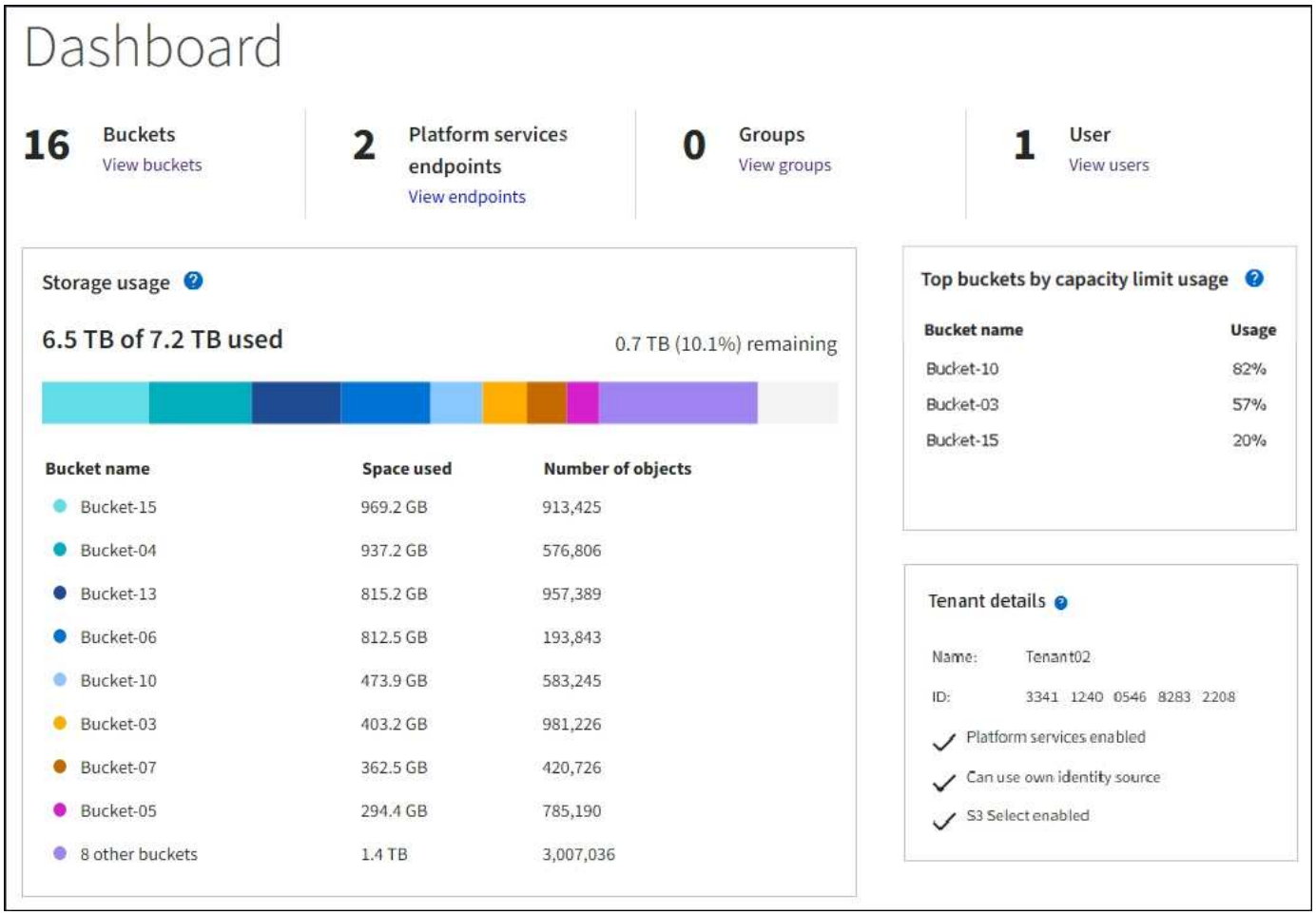
     > SSO が有効で Grid Manager にもサインインしている場合は、 Grid Manager からもサインアウトして SSO からサインアウトする必要があります。

StorageGRIDのテナントマネージャーダッシュボード

テナント マネージャー ダッシュボードには、テナント アカウントの構成の概要と、テナントの S3 バケット内のオブジェクトによって使用されているスペースの量が表示されます。テナントにクォータがある場合は、ダッシュボードには使用されているクォータの量と残っている量が表示されます。テナント アカウントに関連するエラーがある場合は、ダッシュボードにエラーが表示されます。

> このテナントに属するすべてのオブジェクトの論理サイズには、未完了および進行中のマルチパートアップロードが含まれます。このサイズには、ILM ポリシーに使用される追加の物理スペースは含まれません。使用済みスペースの値は推定値です。これらの見積りは、取り込みのタイミング、ネットワーク接続、およびノードの状態によって影響を受けます。

オブジェクトがアップロードされると、ダッシュボードは次の例のようになります。



テナントアカウント情報

ダッシュボードの上部には、設定済みのバケットまたはコンテナ、グループ、およびユーザの数が表示されます。また、プラットフォームサービスエンドポイントが設定されている場合はその数も表示されます。リンクを選択すると詳細が表示されます。

使用していると設定したオプションに応じて"テナント管理権限"、ダッシュボードの残りの部分には、ガイドライン、ストレージの使用状況、オブジェクト情報、およびテナントの詳細のさまざまな組み合わせが表示されます。

ストレージとクォータの使用状況

ストレージ使用状況パネルには、次の情報が表示されます。

- テナントのオブジェクトデータの量。

  アップロードされたオブジェクトデータの合計量を示します。オブジェクトとそのメタデータのコピーを格納するために使用されるスペースは表示されません。

- クォータが設定されている場合は、オブジェクトデータに使用できるスペースの合計容量、および残りのスペースの量と割合。クォータは、取り込むことができるオブジェクトデータの量を制限します。

クォータ使用量は内部の見積もりに基づいており、場合によっては超過する可能性があります。たとえば、テナントがクォータを超えた場合、 StorageGRID はテナントがオブジェクトのアップロードを開始したときにクォータをチェックし、新しい取り込みを拒否します。ただし、 StorageGRID では、クォータを超過したかどうかを判断する際に、現在のアップロードのサイズは考慮されません。オブジェクトが削除されると、クォータ使用量が再計算されるまでテナントが新しいオブジェクトを一時的にアップロードできなくなることがあります。クォータ使用量の計算には10分以上かかることがあります。

- 最大のバケットまたはコンテナの相対サイズを表す棒グラフ。

  任意のグラフセグメントにカーソルを合わせると、そのバケットまたはコンテナで消費されている合計スペースが表示されます。



- 棒グラフに対応するために、オブジェクトデータの合計量と各バケットまたはコンテナのオブジェクト数を含む最大のバケットまたはコンテナのリスト。

Bucket name	Space used	Number of objects
Bucket-02	944.7 GB	7,575
Bucket-09	899.6 GB	589,677
Bucket-15	889.6 GB	623,542
Bucket-06	846.4 GB	648,619
Bucket-07	730.8 GB	808,655
Bucket-04	700.8 GB	420,493
Bucket-11	663.5 GB	993,729
Bucket-03	656.9 GB	379,329
9 other buckets	2.3 TB	5,171,588

  テナントに 9 つ以上のバケットまたはコンテナがある場合は、他のすべてのバケットまたはコンテナがリストの一番下にある 1 つのエントリに結合されます。

Tenant Managerに表示されるストレージ値の単位を変更するには、Tenant Managerの右上にあるユーザドロップダウンを選択し、*[User preferences]*を選択します。

クォータ使用状況アラート

Grid Managerでクォータ使用アラートが有効になっている場合は、クォータが少なくなるか超過すると、次のようにTenant Managerに表示されます。

- テナントのクォータの 90% 以上が使用されると、「テナントクォータ使用率が高い * 」アラートがトリガーされます。

  グリッド管理者にクォータを増やすように依頼することを検討してください。

- クォータを超過すると、新しいオブジェクトをアップロードできないことを通知する通知が表示されます。

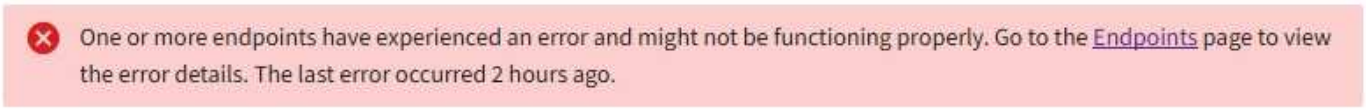
使用容量制限

バケットに容量制限を設定している場合は、Tenant Managerダッシュボードに容量制限の使用量を基準に上位のバケットのリストが表示されます。

バケットに制限が設定されていない場合、その容量は無制限になります。ただし、テナントアカウントに合計ストレージクォータが設定されており、そのクォータに達した場合は、バケットの残りの容量制限に関係なく、それ以上のオブジェクトを取り込むことはできません。

エンドポイントエラー

Grid Managerを使用してプラットフォームサービスで使用する1つ以上のエンドポイントを設定した場合、過去7日以内にエンドポイントエラーが発生すると、Tenant Managerダッシュボードにアラートが表示されます。



に関する詳細を表示するには"プラットフォームサービスエンドポイントエラー"、*[Endpoints]*を選択して[Endpoints]ページを表示します。

テナント管理 API

StorageGRIDテナント管理APIについて学ぶ

Tenant Manager のユーザインターフェイスの代わりにテナント管理 REST API を使用してシステム管理タスクを実行できます。たとえば、 API を使用して処理を自動化したり、ユーザなどの複数のエンティティを迅速に作成したりできます。

テナント管理 API ：

- Swagger オープンソース API プラットフォームを使用します。Swagger では、開発者でもそうでないユーザでも、わかりやすいユーザインターフェイスを利用して API を操作できます。Swagger のユーザインターフェイスでは、各 API 処理に関する詳細情報とドキュメントを参照できます。
- "無停止アップグレードをサポートするためのバージョン管理"を使用します。

Swagger のテナント管理 API のドキュメントにアクセスするには、次の手順を実行します。

1. Tenant Manager にサインインします。
2. Tenant Managerの上部で、ヘルプアイコンを選択し、*[API documentation]*を選択します。

API処理

テナント管理 API では、使用可能な API 処理が次のセクションに分類されます。

- * account *：現在のテナントアカウントに対する処理（ストレージの使用状況情報の取得など）。
- **auth**：ユーザセッション認証を実行する処理。

  テナント管理 API では、 Bearer トークン認証方式がサポートされています。テナントログインの場合は、認証要求（つまり）のJSON本文でユーザ名、パスワード、およびアカウントIDを指定します `POST /api/v3/authorize`。ユーザが認証されると、セキュリティトークンが返されます。このトークンは、後続の API 要求（「 Authorization ： Bearer トークン」）のヘッダーで指定する必要があります。

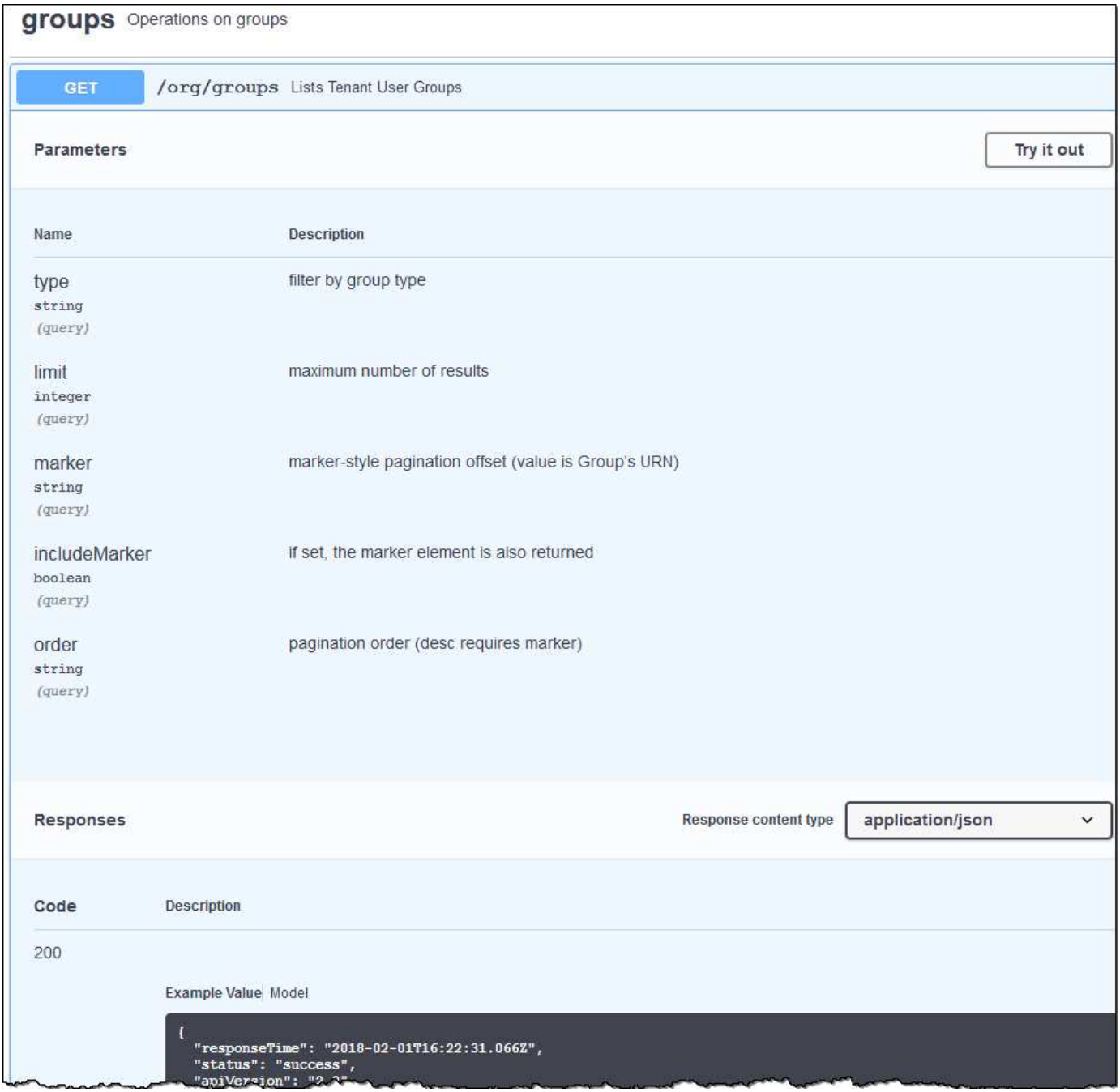
  認証セキュリティの向上については、を参照してください"クロスサイトリクエストフォージェリから保護"。

  > StorageGRID システムでシングルサインオン（ SSO ）が有効になっている場合は、別の手順による認証が必要です。を参照してください"Grid 管理 API の使用手順"。

- * config *：製品リリースおよびテナント管理APIのバージョンに関連する処理。製品リリースバージョンおよびそのリリースでサポートされる API のメジャーバージョンを一覧表示できます。
- コンテナ: S3 バケットに対する操作。
- * deactivated-features *：非アクティブ化された可能性がある機能を表示する操作。
- * endpoints *：エンドポイントを管理する処理。エンドポイントを使用することで、 S3 バケットは外部のサービスを StorageGRID CloudMirror レプリケーション、通知、または検索統合に使用できます。
- * grid-federation-connections *：グリッドフェデレーション接続およびグリッド間レプリケーションに対する処理。
- * groups *：ローカルテナントグループを管理する処理、およびフェデレーテッドテナントグループを外部のアイデンティティソースから取得する処理。
- *identity-source *：外部のアイデンティティソースを設定する処理、およびフェデレーテッドグループとユーザ情報を手動で同期する処理。
- * ILM *：情報ライフサイクル管理（ILM）設定に対する処理。
- * regions *：StorageGRID システムに設定されているリージョンを特定する処理。
- * s3 *：テナントユーザのS3アクセスキーを管理する処理。
- **s3-configurations**：S3 グローバル設定を取得するための操作。
- * s3-object-lock *：グローバルS3オブジェクトロック設定に対する処理。法規制への準拠をサポートするために使用されます。
- * users *：テナントユーザを表示および管理する処理。

処理の詳細

各 API 処理を展開表示すると、 HTTP アクション、エンドポイント URL 、必須またはオプションのパラメータのリスト、要求の本文の例（必要な場合）、想定される応答を確認できます。



問題 **API** 要求

APIドキュメントWebページで実行するAPI処理はすべてライブ処理です。設定データやその他のデータを誤って作成、更新、または削除しないように注意してください。

手順

1. HTTP アクションを選択して、要求の詳細を表示します。
2. グループやユーザの ID など、要求で追加のパラメータが必要かどうかを確認します。次に、これらの値を取得します。必要な情報を取得するために、先に別の API 要求の問題 が必要になることがあります。
3. 要求の本文の例を変更する必要があるかどうかを判断します。その場合は、 * Model * を選択して各フィールドの要件を確認できます。

4. [* 試してみてください *] を選択します。
5. 必要なパラメータを指定するか、必要に応じて要求の本文を変更します。
6. [* Execute] を選択します。
7. 応答コードを確認し、要求が成功したかどうかを判断します。

StorageGRID テナント管理 **API** のバージョン管理

テナント管理 API では、バージョン管理機能を使用して無停止アップグレードがサポートされます。

たとえば、このリクエストURLはAPIのバージョン4を指定します。

```
https://hostname_or_ip_address/api/v4/authorize
```

APIのメジャーバージョンは、古いバージョンと互換性がない_変更を行うと更新されます。APIのマイナーバージョンは、_が古いバージョンと互換性がある_に変更されると更新されます。互換性のある変更には、新しいエンドポイントやプロパティの追加などがあります。

次の例は、変更のタイプに基づいて API バージョンがどのように更新されるかを示しています。

API に対する変更のタイプ	古いバージョン	新しいバージョン
旧バージョンと互換性があります	2.1	2.2
旧バージョンとの互換性がありません	2.1	3.0

StorageGRIDソフトウェアを初めてインストールすると、最新バージョンのAPIのみが有効になります。ただし、 StorageGRID の新機能リリースにアップグレードした場合、少なくとも StorageGRID の機能リリース 1 つ分の間は、古い API バージョンにも引き続きアクセスできます。

> サポートされるバージョンを設定できます。詳細については、Swagger APIドキュメントの* config *セクションを参照してください"Grid 管理 API"。すべてのAPIクライアントを新しいバージョンを使用するように更新したら、古いバージョンのサポートを無効にする必要があります。

古い要求は、次の方法で廃止とマークされます。

- 応答ヘッダーが「 Deprecated ： true 」となる。
- JSON 応答の本文に「 deprecated ： true 」が追加される
- 廃止の警告が nms.log に追加される。例：

```
Received call to deprecated v2 API at POST "/api/v2/authorize"
```

現在のリリースでサポートされている **API** のバージョンを確認します

API要求を使用して `GET /versions`、サポートされているAPIのメジャーバージョンのリストを返します。この要求は、Swagger APIドキュメントの* config *セクションにあります。

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2023-06-27T22:13:50.750Z",
  "status": "success",
  "apiVersion": "4.0",
  "data": [
    2,
    3,
    4
  ]
}
```

要求の **API** バージョンを指定します

APIのバージョンは(`/api/v4`、パスパラメータを使用して指定できます）またはヘッダー(`Api-Version: 4`を指定できます。両方の値を指定した場合は、ヘッダー値がパス値よりも優先されます。

```
curl https://[IP-Address]/api/v4/grid/accounts

curl -H "Api-Version: 4" https://[IP-Address]/api/grid/accounts
```

StorageGRIDでクロスサイトリクエストフォージェリから保護する

CSRF トークンを使用してクッキーによる認証を強化すると、 StorageGRID に対するクロスサイトリクエストフォージェリ（ CSRF ）攻撃を防ぐことができます。Grid Manager と Tenant Manager はこのセキュリティ機能を自動的に有効にします。他の API クライアントは、サインイン時にこの機能を有効にするかどうかを選択できます。

攻撃者が別のサイト（たとえば、 HTTP フォーム POST を使用して）への要求をトリガーできる場合、サインインしているユーザのクッキーを使用して特定の要求を原因 が送信できます。

StorageGRID では、 CSRF トークンを使用して CSRF 攻撃を防ぐことができます。有効にした場合、特定のクッキーの内容が特定のヘッダーまたは特定の POST パラメータの内容と一致する必要があります。

この機能をイネーブルにするには、認証時にパラメータをに `true`設定し `csrfToken`ます。デフォルトはです `false`。

```
curl -X POST --header "Content-Type: application/json" --header "Accept:
application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

trueの場合、 `GridCsrfToken`Grid Managerへのサインインにはランダムな値でクッキーが設定され、Tenant Managerへのサインインにはランダムな値でクッキーが設定さ `AccountCsrfToken`れます。

クッキーが存在する場合は、システムの状態を変更できるすべての要求（ POST 、 PUT 、 PATCH 、 DELETE ）には次のいずれかが含まれている必要があります。

- `X-Csrf-Token`ヘッダーの値がCSRFトークンクッキーの値に設定されたヘッダー。
- エンドポイントがフォームエンコードされた本文を受け入れる場合： `csrfToken`フォームエンコードされた要求本文パラメータ。

CSRF保護を設定するには、またはを使用し"Grid 管理 API""テナント管理 API"ます。

> CSRFトークンクッキーが設定されている要求では、CSRF攻撃に対する追加の保護としてJSON要求本文が必要な要求に対して「Content-Type:application/json」ヘッダーも適用されます。

グリッドフェデレーション接続を使用する

StorageGRID でテナントグループとユーザーを同期する

テナントがグリッドフェデレーション接続を使用するように作成または編集された場合、そのテナントは1つのStorageGRIDシステム（ソーステナント）から他のすべての接続されたStorageGRIDシステム（レプリカテナント）にレプリケートされます。テナントの複製が完了すると、テナントグループ、ユーザー、およびS3アクセスキーが接続されているグリッド間で同期されます。

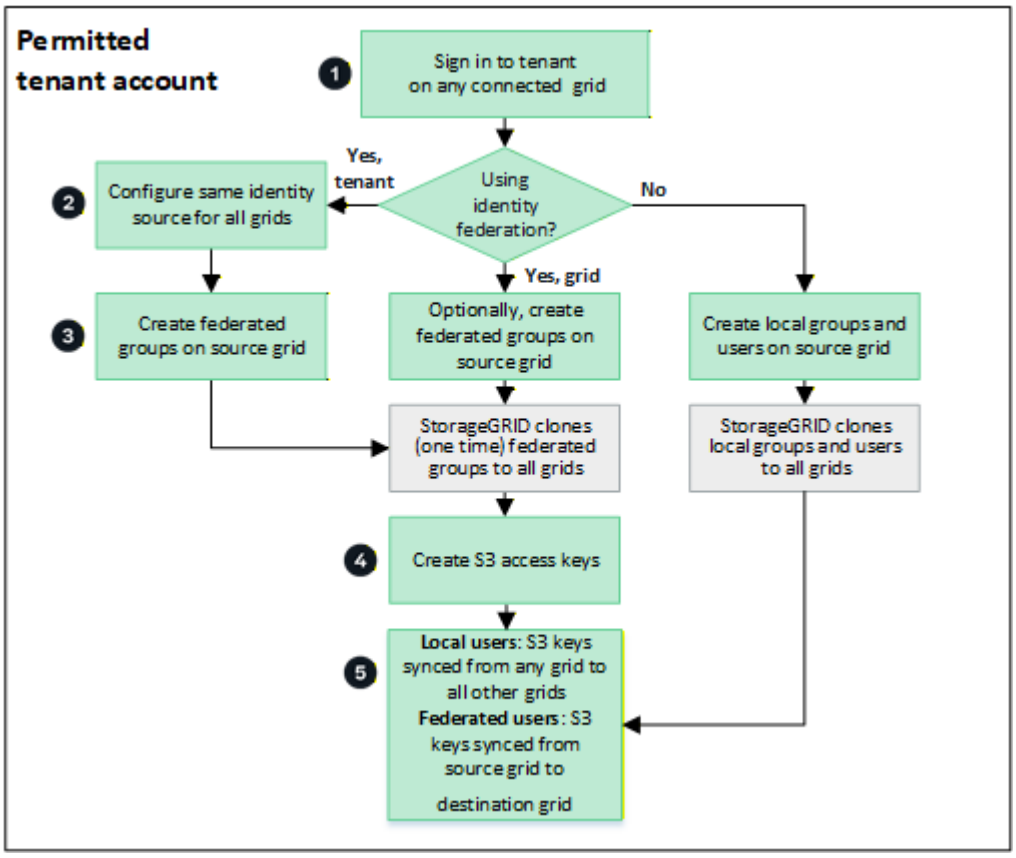
テナントが最初に作成されたStorageGRIDシステムは、テナントの_ソースグリッド_です。テナントは1つ以上の_宛先グリッド_に複製されます。接続されているすべてのグリッド上のテナントアカウントは、同じアカウントID、名前、説明、ストレージクォータ、割り当てられた権限、およびルートユーザーパスワードを持ちます。詳細については、"グリッドフェデレーションのアカウント同期について"および"許可されたテナントを管理する"を参照してください。

テナントアカウント情報の同期は、バケットオブジェクトの"グリッド間レプリケーション"に必要です。すべてのグリッドで同じテナントグループとユーザーを使用することで、接続されているどのグリッドでも、対応するバケットとオブジェクトにアクセスできるようになります。

テナントのアカウント同期ワークフロー

テナントアカウントに*グリッドフェデレーション接続を使用する*権限が付与されている場合は、ワークフロー図を参照して、グループ、ユーザー、およびS3アクセスキーを同期するために実行する手順を確認してく

ださい。



ワークフローの主な手順は次のとおりです。

1 テナントにサインイン

接続されているいずれかのグリッド上で、テナントアカウントにサインインしてください。

2 必要に応じてアイデンティティフェデレーションを設定

テナントアカウントにフェデレーショングループとユーザーを使用するための「独自のIDソースを使用する」権限がある場合は、ソースおよび1つ以上の宛先テナントアカウントに対して、同じIDソース（同じ設定）を構成してください。フェデレーショングループは作成時に複製され、フェデレーションユーザーはキーが作成された時に複製されます。クローンを作成するには、すべてのグリッドで同じIDソースを設定する必要があります。手順については、"アイデンティティフェデレーションを使用する"を参照してください。

3 グループとユーザの作成

接続されたグリッドであれば、どのグリッドからでもグループやユーザーを作成できます。新しいローカルグループを追加すると、StorageGRID は接続されているすべてのグリッドと自動的に同期します。ローカルグループへの変更（編集、削除）も継続的に同期されます。フェデレーテッドグループは作成時に一度だけ複製されます。

- アイデンティティフェデレーションがStorageGRIDシステム全体またはテナントアカウントに対して設定されている場合は、"新しいテナントグループを作成します"アイデンティティソースからフェデレーテッドグループをインポートします。

- ID連携を使用していない場合は、"新しいローカルグループを作成します"その後"ローカルユーザを作成します"。

4 S3アクセスキーの作成

"独自のアクセスキーを作成します"または"別のユーザのアクセスキーを作成します"を任意のグリッドで使用して、接続されているすべてのグリッド上のバケットにアクセスできます。

5 S3アクセスキーを同期する

すべてのグリッドで同じアクセスキーを使用してバケットにアクセスする必要がある場合は、いずれかのグリッドでアクセスキーを作成してください。ローカルユーザーの場合、アクセスキーはデフォルトで自動的に同期されます。フェデレーションユーザーの場合、ソースグリッドで S3 アクセスキーを作成し、アクセスキーの同期を有効にする を選択して、キーをすべての宛先グリッドに同期させる必要があります。

グループ、ユーザー、およびS3アクセスキーはどのように同期されますか？

このセクションを確認して、グループ、ユーザー、およびS3アクセスキーが接続されたグリッド間でどのように同期されるかを理解してください。

ローカルグループは継続的に同期されます

テナントアカウントが作成され、宛先グリッドに複製された後、StorageGRID は接続されているすべてのグリッド間でローカルグループを継続的に同期します。ローカルグループに対するすべての変更（作成、編集、削除操作を含む）は、どのグリッド上で行われた場合でも、接続されている他のすべてのグリッドに自動的に複製されます。

元のグループと同期されたコピーは、どちらも同じアクセスモード、グループ権限、およびS3グループポリシーを持ちます。手順については、"S3 テナント用のグループを作成します"を参照してください。

ローカルユーザーは継続的に同期されます

接続されたグリッド上に新しいローカルユーザーを作成すると、StorageGRID はそのユーザーを接続されている他のすべてのグリッドと自動的に同期します。編集、削除、パスワードのリセットなど、その後の変更も継続的に同期されます。元のユーザーとその同期されたコピーは、同じフルネーム、ユーザー名、および「アクセス拒否」設定を持っています。各グリッド上の同じユーザーは、同じグループにも属しています。手順については、"ユーザの管理"を参照してください。

フェデレーテッドグループは作成時に一度だけ同期されます。

"シングルサインオン"および"アイデンティティフェデレーション"でアカウント同期を使用するための要件が満たされている場合、グリッド上のテナント用に作成（インポート）したフェデレーショングループは、接続されている他のすべてのグリッド上のテナントに自動的に同期されます。

両グループとも、アクセスモード、グループ権限、およびS3グループポリシーは同じです。

ソーステナント用にフェデレーショングループが作成され、他のグリッドと同期されると、フェデレーションユーザーは接続されている任意のグリッド上でテナントにサインインできるようになります。フェデレーショングループに対するその後の変更は、グリッド間で自動的に同期されません。

S3アクセスキーは自動または手動で同期できます

デフォルトでは、StorageGRID は S3 アクセスキーを自動的に同期します。セキュリティ上の理由から、テナントごとに S3 アクセスキーの自動同期を無効にし、各グリッド上でテナントごとに異なるキーを設定することができます。

接続されたグリッドのアクセスキーを管理するには、次のいずれかの方法を実行できます。

- 各グリッドで同じキーを使用する必要がない場合は、自動アクセスキー同期を無効にして、各グリッドで"独自のアクセスキーを作成します"または"別のユーザのアクセスキーを作成します"することができます。

> フェデレーションユーザーのS3アクセスキーを同期すると、ユーザーとS3アクセスキーの両方が同期先のテナントに同期されます。

> ローカルユーザーが所有するS3アクセスキーは、キーが削除された場合も含め、接続されているグリッド間で継続的に同期されます。フェデレーションユーザーが所有するS3アクセスキーは、作成時に一度同期されます。削除を含むその後の変更はレプリケートされません。テナント接続ごとに、アクセスキーの同期を有効または無効にすることができます。

宛先グリッドに追加されたグループとユーザーは同期されます

ローカルグループやユーザーの作成またはインポートなど、接続されているグリッドで行われた変更は、接続されている他のすべてのグリッドに自動的に同期されます。

編集または削除されたローカルグループ、ユーザー、およびアクセスキーは同期されます

ローカルグループ、ローカルユーザー、およびローカルユーザーが所有するS3アクセスキーへの変更は、接続されているすべてのグリッド間で継続的に同期されます。同期される操作には、編集、削除、パスワードのリセットが含まれます。

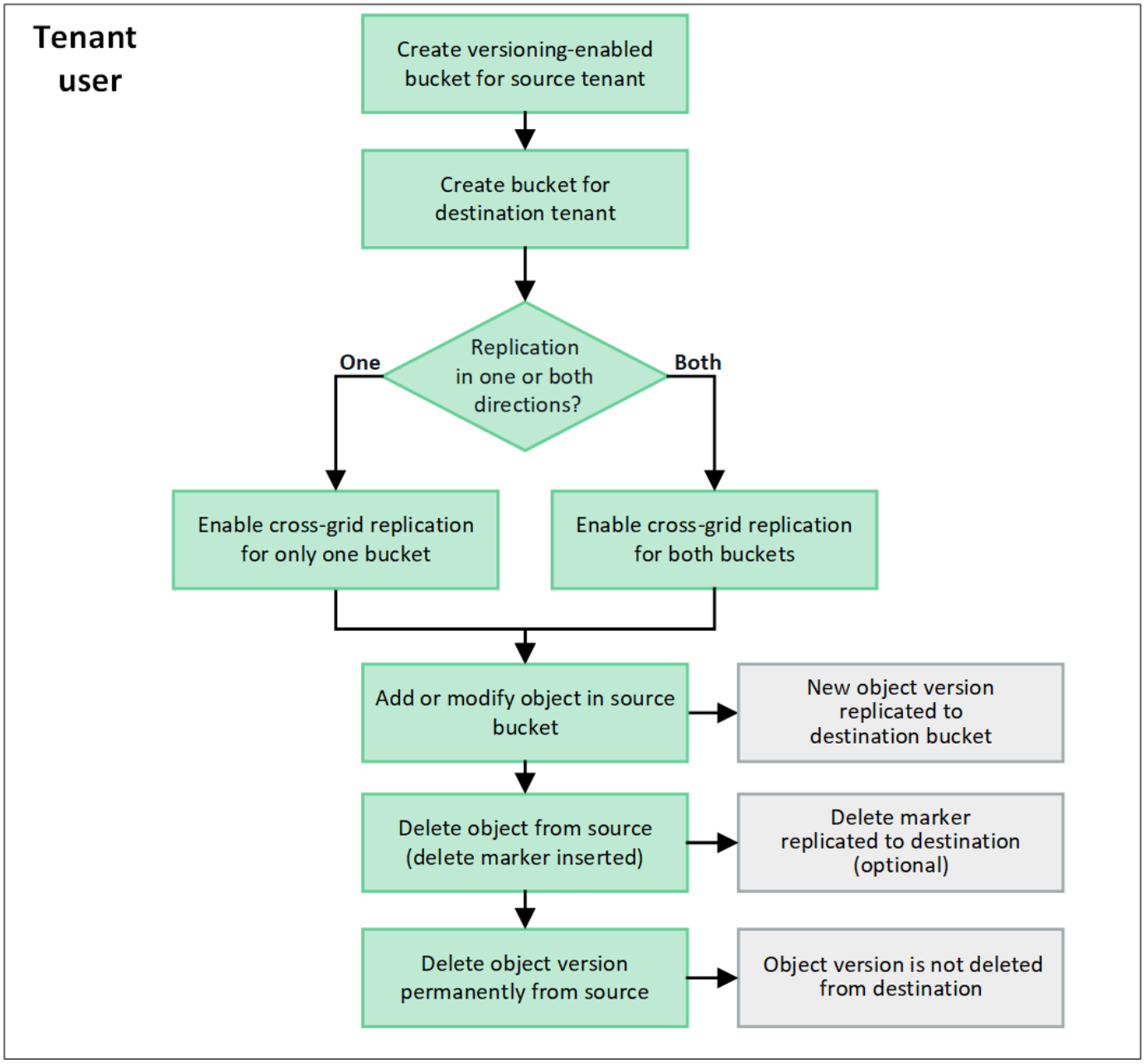
フェデレーショングループおよびフェデレーションユーザーが所有するS3アクセスキーへの変更は、初回作成後は同期されません。

StorageGRID でクロスグリッドレプリケーションを管理する

テナントアカウントの作成時に「Use grid federation connection *」権限が割り当てられていた場合は、グリッド間レプリケーションを使用して、テナントのソースグリッド上のバケットとテナントのデスティネーショングリッド上のバケット間でオブジェクトを自動的にレプリケートできます。グリッド間レプリケーションは、一方または両方の方向で実行できます。

グリッド間レプリケーションのワークフロー

ワークフロー図は、2 つのグリッド上のバケット間のグリッド間レプリケーションを構成するために実行する手順をまとめたものです。これらの手順については、図の下に詳しく説明します。



グリッド間レプリケーションを設定する

クロスグリッド レプリケーションを使用する前に、各グリッドの対応するテナント アカウントにサインインし、2 つのバケットを作成する必要があります。次に、いずれかまたは両方のバケットでクロスグリッド レプリケーションを有効にできます。

開始する前に

- クロスグリッド レプリケーションの要件を確認しました。。 "クロスグリッドレプリケーションとは" 。
- 使用しています"サポートされている Web ブラウザ"。
- テナント アカウントには グリッド フェデレーション接続を使用する 権限があり、両方のグリッドに同一のテナント アカウントが存在します。。 "グリッドフェデレーション接続に許可されているテナントを管理します" 。
- サインインしようとしているテナントユーザーは、両方のグリッドに既に存在し、"rootアクセス権限" 。

- テナントの宛先グリッドにローカル ユーザーとしてサインインしている場合、テナント アカウントのルート ユーザーがそのグリッド上のユーザー アカウントのパスワードを設定しています。

2つのバケットを作成する

最初のステップとして、各グリッドの対応するテナント アカウントにサインインし、各グリッドにバケットを作成します。

手順

1. グリッドフェデレーション接続のいずれかのグリッドから、新しいバケットを作成します。
   a. 両方のグリッドに存在するテナントユーザのクレデンシャルを使用してテナントアカウントにサインインします。

      ローカル ユーザーとしてテナントの宛先グリッドにサインインできない場合は、テナント アカウントのルート ユーザーがユーザー アカウントのパスワードを設定していることを確認します。

   b. の指示に従ってください"S3バケットを作成"。

      バケット名とリージョンはグリッドごとに異なる場合があります。

   c. タブで、[オブジェクトのバージョン管理を有効にする]*を選択します。
   d. StorageGRIDシステムでS3オブジェクトロックが有効になっている場合は、"S3 オブジェクトロックを使用したクロスグリッドレプリケーション" 。
   e. [* バケットの作成 *] を選択します。
   f. [完了] を選択します。
2. これらの手順を繰り返して、グリッド フェデレーション接続内の他のグリッド上の同じテナント アカウントのバケットを作成します。

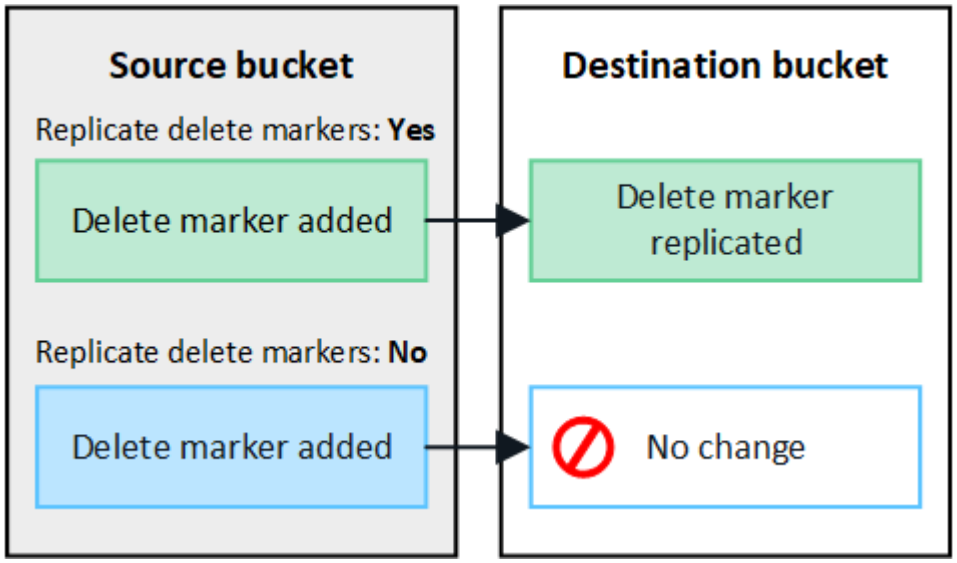
   必要に応じて、各バケットで異なるリージョンを使用できます。

グリッド間レプリケーションを有効にする

手順

1. オブジェクトを複製するグリッドから開始して、"一方向のグリッド間レプリケーション"次を有効にします。
   a. バケットのテナントアカウントにサインインします。
   b. ダッシュボードで* View Buckets を選択するか、 storage（S3）> Buckets *を選択します。
   c. 表からバケット名を選択して、バケットの詳細ページにアクセスします。
   d. [クロスグリッドレプリケーション]*タブを選択します。
   e. [有効化]*を選択し、要件のリストを確認します。
   f. すべての要件を満たしている場合は、使用するグリッドフェデレーション接続を選択します。
   g. 必要に応じて、[Replicate delete markers]の設定を変更して、S3クライアントがバージョンIDを含まない削除要求をソースグリッドに対して実行した場合のデスティネーショングリッドでの動作を確認します。

- * Yes *（デフォルト）：削除マーカーがソースバケットに追加され、デスティネーションバケットにレプリケートされます。
- いいえ: 削除マーカーはソースバケットに追加されますが、宛先バケットには複製されません。



削除リクエストにバージョン ID が含まれている場合、そのオブジェクト バージョンはソース バケットから完全に削除されます。 StorageGRID はバージョン ID を含む削除要求を複製しないため、同じオブジェクト バージョンが宛先から削除されません。

参照"クロスグリッドレプリケーションとは"詳細については。

a. 必要に応じて、*クロスグリッドレプリケーション*監査カテゴリの設定を変更して、監査メッセージの量を管理します。
   - エラー（デフォルト）：失敗したグリッド間レプリケーション要求のみが監査出力に含まれます。
   - * Normal *：グリッドをまたぐレプリケーション要求がすべて含まれるため、監査出力の量が大幅に増加します。
b. [有効にしてテスト]*を選択します。

   しばらくすると、成功メッセージが表示されます。このバケットに追加されたオブジェクトは、他のグリッドに自動的に複製されるようになりました。 クロスグリッド レプリケーション は、バケットの詳細ページで有効な機能として表示されます。

2. 必要に応じて、もう一方のグリッドの対応するバケットに移動し"双方向のグリッド間レプリケーションを有効にします"ます。

グリッド間のレプリケーションをテスト

バケットでクロスグリッドレプリケーションが有効になっている場合は、接続とグリッド間レプリケーションが正しく機能していること、ソースとデスティネーションのバケットがすべての要件を満たしていること（バージョン管理が有効になっている場合など）を確認する必要があります。

開始する前に

- 使用しています"サポートされている Web ブラウザ"。

- が設定されたユーザグループに属している"rootアクセス権限"必要があります。

手順

1. バケットのテナントアカウントにサインインします。
2. ダッシュボードで* View Buckets を選択するか、 storage（S3）> Buckets *を選択します。
3. 表からバケット名を選択して、バケットの詳細ページにアクセスします。
4. [クロスグリッドレプリケーション]*タブを選択します。
5. [接続のテスト *] を選択します。

   接続が正常な場合は、成功バナーが表示されます。それ以外の場合はエラー メッセージが表示され、グリッド管理者はそのメッセージを使用して問題を解決できます。詳細については、"グリッドフェデレーションエラーをトラブルシューティングする" 。

6. グリッド間レプリケーションが両方向で実行されるように設定されている場合は、もう一方のグリッドの対応するバケットに移動して*[Test connection]*を選択し、グリッド間レプリケーションが反対方向で動作していることを確認します。

グリッド間レプリケーションを無効にします

オブジェクトをもう一方のグリッドにコピーする必要がなくなった場合は、グリッド間レプリケーションを永続的に停止できます。

グリッド間レプリケーションを無効にする前に、次の点に注意してください。

- グリッド間のレプリケーションを無効にしても、グリッド間ですでにコピーされているオブジェクトは削除されません。例えば、 `my-bucket`グリッド1にコピーされた `my-bucket`グリッド 2 のバケットのクロスグリッド レプリケーションを無効にしても、そのバケットのクロスグリッド レプリケーションは削除されません。これらのオブジェクトを削除する場合は、手動で削除する必要があります。
- 各バケットでグリッド間レプリケーションが有効になっている場合（双方向でレプリケーションが発生した場合）は、一方または両方のバケットでグリッド間レプリケーションを無効にすることができます。たとえば、グリッド1からグリッド2へのオブジェクトのレプリケーションを無効にしながら、グリッド2から `my-bucket`グリッド1への `my-bucket`オブジェクトのレプリケーションを `my-bucket`続行 `my-bucket`できます。
- グリッド フェデレーション接続を使用するためのテナントの権限を削除する前に、クロス グリッド レプリケーションを無効にする必要があります。。 "許可されたテナントを管理する" 。

開始する前に

- 使用しています"サポートされている Web ブラウザ"。
- が設定されたユーザグループに属している"rootアクセス権限"必要があります。

手順

1. レプリケートするオブジェクトが含まれていないグリッドから、バケットのグリッド間レプリケーションを停止します。
   a. バケットのテナントアカウントにサインインします。
   b. ダッシュボードで* View Buckets を選択するか、 storage（S3）> Buckets *を選択します。
   c. 表からバケット名を選択して、バケットの詳細ページにアクセスします。

d. [クロスグリッドレプリケーション]*タブを選択します。

e. [レプリケーションを無効にする]*を選択します。

f. このバケットのクロスグリッド レプリケーションを無効にする場合は、テキスト ボックスに「はい」と入力し、「無効」を選択します。

しばらくすると、成功のメッセージが表示されます。このバケットに追加された新しいオブジェクトを他のグリッドに自動的にレプリケートすることはできなくなります。*クロスグリッドレプリケーション*は、[Buckets]ページに有効な機能として表示されなくなりました。

2. グリッド間レプリケーションが双方向で実行されるように設定されている場合は、もう一方のグリッドの対応するバケットに移動し、別の方向へのグリッド間レプリケーションを停止します。

StorageGRID でグリッドフェデレーション接続を表示する

テナントアカウントに* Use grid federation connection *権限がある場合は、許可されている接続を表示できます。

開始する前に

- テナントアカウントには、* Use grid federation connection *権限が割り当てられています。
- を使用してTenant Managerにサインインしておき"サポートされている Web ブラウザ"ます。
- が設定されたユーザグループに属している"rootアクセス権限"必要があります。

手順

1. * storage（S3）> Grid federation connections *を選択します。

[Grid Federation Connection]ページが表示され、次の情報を要約した表が含まれます。

列	製品説明
接続名	このテナントには、使用する権限があるグリッドフェデレーション接続。
バケットにクロスグリッドレプリケーションが設定されている	グリッドフェデレーション接続ごとに、グリッド間レプリケーションが有効になっているテナントバケット。これらのバケットに追加されたオブジェクトは、接続内のもう一方のグリッドにレプリケートされます。
前回のエラー	グリッドフェデレーション接続ごとに、データがもう一方のグリッドにレプリケートされていたときに発生する最新のエラー（存在する場合）。を参照して 最後のエラーをクリアします

2. 必要に応じて、にバケット名を選択し"バケットの詳細を表示します"ます。

最後のエラーをクリアします

次のいずれかの理由で、* Last error *列にエラーが表示されることがあります。

- ソースオブジェクトのバージョンが見つかりませんでした。

- ソースバケットが見つかりませんでした。
- デスティネーションバケットが削除されました。
- デスティネーションバケットが別のアカウントで再作成されました。
- デスティネーションバケットのバージョン管理が中断されています。
- デスティネーションバケットが同じアカウントで再作成されましたが、現在バージョン管理されていません。

> この列には、最後に発生したグリッド間レプリケーションエラーのみが表示されます。以前に発生した可能性のあるエラーは表示されません。

手順

1. 「* Last error *」列にメッセージが表示された場合は、メッセージのテキストを確認します。

   たとえば、このエラーは、クロスグリッドレプリケーションのデスティネーションバケットが無効な状態であることを示しています。バージョン管理が中断されたか、S3オブジェクトロックが有効になっている可能性があります。



2. 推奨される対処方法を実行します。たとえば、グリッド間レプリケーションのためにデスティネーションバケットでバージョン管理が一時停止されていた場合は、そのバケットのバージョン管理を再度有効にします。
3. テーブルから接続を選択します。
4. [Clear error]*を選択します。
5. メッセージをクリアしてシステムのステータスを更新するには、*はい*を選択します。
6. 5~6分待ってから、新しいオブジェクトをバケットに取り込みます。エラーメッセージが再表示されないことを確認します。

   > エラーメッセージがクリアされるように、メッセージのタイムスタンプから5分以上経過してから新しいオブジェクトを取り込んでください。

7. バケットエラーが原因でレプリケートに失敗したオブジェクトがないかどうかを確認するには、を参照してください"失敗したレプリケーション処理を特定して再試行します"。

グループとユーザを管理します

StorageGRIDでIDフェデレーションを使用する

アイデンティティフェデレーションを使用すると、テナントグループとテナントユーザを迅速に設定できます。またテナントユーザは、使い慣れたクレデンシャルを使用してテナントアカウントにサインインできます。

Tenant Manager 用のアイデンティティフェデレーションを設定する

テナント グループとユーザーを Active Directory、Microsoft Entra ID、OpenLDAP、Oracle Directory Server などの別のシステムで管理する場合は、Tenant Manager の ID フェデレーションを構成できます。

開始する前に

- テナントマネージャーにサインインするには、"サポートされている Web ブラウザ" 。
- が設定されたユーザグループに属している"rootアクセス権限"必要があります。
- アイデンティティ プロバイダーとして、Active Directory、Microsoft Entra ID、OpenLDAP、または Oracle Directory Server を使用しています。

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

- OpenLDAP を使用する場合は、 OpenLDAP サーバを設定する必要があります。を参照して OpenLDAP サーバの設定に関するガイドライン
- LDAP サーバとの通信に Transport Layer Security （ TLS ）を使用する場合は、アイデンティティプロバイダが TLS 1.2 または 1.3 を使用している必要があります。を参照して "発信 TLS 接続でサポートされる暗号"

タスクの内容

テナントにアイデンティティフェデレーションサービスを設定できるかどうかは、テナントアカウントの設定方法によって異なります。テナントが Grid Manager 用に設定されたアイデンティティフェデレーションサービスを共有する場合があります。[Identity Federation]ページにアクセスしたときにこのメッセージが表示される場合は、このテナントに別のフェデレーテッドアイデンティティソースを設定することはできません。

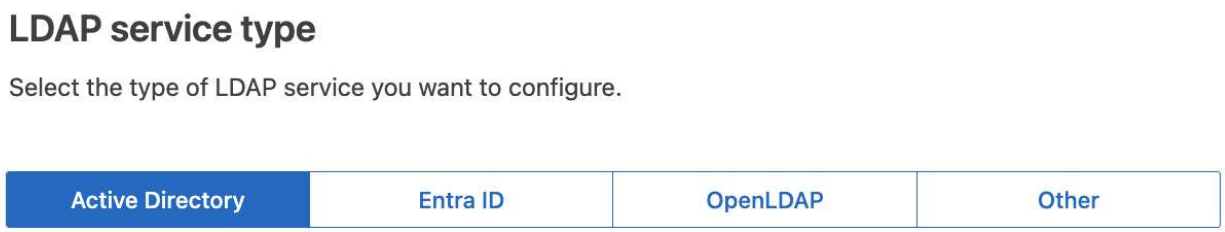
> ⓘ This tenant account uses the LDAP server that is configured for the Grid Manager. Contact the grid administrator for information or to change this setting.

構成を入力します

フェデレーションの識別を設定するときは、StorageGRID がLDAPサービスに接続するために必要な値を指定します。

手順

1. アクセス管理 > *アイデンティティ連携*を選択します。
2. ［ * アイデンティティフェデレーションを有効にする * ］ を選択
3. LDAP サービスタイプセクションで、設定する LDAP サービスのタイプを選択します。



Oracle Directory Server を使用する LDAP サーバーの値を設定するには、 * その他 * を選択します。

4. [* その他 *] を選択した場合は、 [LDAP 属性] セクションのフィールドに入力します。それ以外の場合は、次の手順に進みます。
   - ユーザーの一意の名前: LDAP ユーザーの一意の識別子を含む属性の名前。この属性は、 `sAMAccountName` Active Directoryおよび `uid`OpenLDAP 用。 `Oracle Directory Server`を構成する場合は、次のように入力します。 `uid`。
   - ユーザー **UUID**: LDAP ユーザーの永続的な一意の識別子を含む属性の名前。この属性は、 `objectGUID` Active Directoryおよび `entryUUID`OpenLDAP 用。 `Oracle Directory Server`を構成する場合は、次のように入力します。 `nsuniqueid`。指定された属性の各ユーザーの値は、16 バイト形式または文字列形式の 32 桁の 16 進数である必要があります。ハイフンは無視されます。
   - グループの一意の名前: LDAP グループの一意の識別子を含む属性の名前。この属性は、 `sAMAccountName` Active Directoryおよび `cn`OpenLDAP 用。 `Oracle Directory Server`を構成する場合は、次のように入力します。 `cn`。
   - グループ **UUID**: LDAP グループの永続的な一意の識別子を含む属性の名前。この属性は、 `objectGUID` Active Directoryおよび `entryUUID`OpenLDAP 用。 `Oracle Directory Server`を構成する場合は、次のように入力します。 `nsuniqueid`。指定された属性の各グループの値は、16 バイト形式または文字列形式の 32 桁の 16 進数である必要があります。ハイフンは無視されます。
5. すべての LDAP サービスタイプについて、 LDAP サーバの設定セクションに必要な LDAP サーバおよびネットワーク接続情報を入力します。
   - * Hostname * ： LDAP サーバの完全修飾ドメイン名（ FQDN ）または IP アドレス。
   - * Port * ： LDAP サーバへの接続に使用するポート。

     STARTTLS のデフォルトポートは 389 、 LDAPS のデフォルトポートは 636 です。ただし、ファイアウォールが正しく設定されていれば、任意のポートを使用できます。
   - * Username * ： LDAP サーバに接続するユーザの識別名（ DN ）の完全パス。

     Active Directory の場合は、ダウンレベルログオン名またはユーザープリンシパル名を指定することもできます。

     指定するユーザには、グループおよびユーザを表示する権限、および次の属性にアクセスする権限が必要です。

     - `sAMAccountName`または `uid`
     - `objectGUID`、 `entryUUID`、または `nsuniqueid`

- `cn`
- `memberOf`または `isMemberOf`
- * Active Directory *： `objectSid`、 `primaryGroupID`、 `userAccountControl`、および `userPrincipalName`
- エントラ**ID**: `accountEnabled`そして `userPrincipalName`

◦ * Password * ：ユーザ名に関連付けられたパスワード。

> 今後パスワードを変更する場合は、このページでパスワードを更新する必要があります。

◦ * Group Base DN * ：グループを検索する LDAP サブツリーの識別名（ DN ）の完全パス。Active Directory では、ベース DN に対して相対的な識別名（ DC=storagegrid 、 DC=example 、 DC=com など）のグループをすべてフェデレーテッドグループとして使用できます。

> * グループの一意な名前 * 値は、所属する * グループベース DN * 内で一意である必要があります。

◦ * User Base DN * ：ユーザを検索する LDAP サブツリーの識別名（ DN ）の完全パス。

> * ユーザーの一意な名前 * 値は、それぞれが属する * ユーザーベース DN * 内で一意である必要があります。

◦ ユーザー名のバインド形式（オプション）：パターンを自動的に決定できない場合にStorageGRID が使用するデフォルトのユーザー名パターン。

StorageGRID がサービスアカウントにバインドできない場合にユーザがサインインできるようにするため、 * バインドユーザ名形式 * を指定することを推奨します。

次のいずれかのパターンを入力します。

- **UserPrincipalName** パターン **(AD** および **Entra ID)**: `[USERNAME]@example.com`
- ダウンレベル ログオン名パターン **(AD** および **Entra ID)**: `example\[USERNAME]`
- 識別名パターン： `CN=[USERNAME],CN=Users,DC=example,DC=com`

  記載されているとおりに * [username] * を含めます。

6. Transport Layer Security （ TLS ）セクションで、セキュリティ設定を選択します。

◦ **STARTTLS** を使用する: STARTTLS を使用して、LDAP サーバーとの通信を保護します。これは、Active Directory、OpenLDAP、またはその他の場合に推奨されるオプションですが、このオプションは Microsoft Entra ID ではサポートされていません。

◦ **LDAPS** を使用する: LDAPS (LDAP over SSL) オプションは、TLS を使用して LDAP サーバーへの接続を確立します。 Microsoft Entra ID の場合はこのオプションを選択する必要があります。

◦ **TLS** を使用しない: StorageGRIDシステムと LDAP サーバー間のネットワーク トラフィックは保護されません。このオプションは Microsoft Entra ID ではサポートされていません。

Active Directory サーバーが LDAP 署名を強制している場合、「TLS を使用しない」オプションの使用はサポートされません。 STARTTLS または LDAPS を使用する必要があります。

7. STARTTLS または LDAPS を選択した場合は、接続の保護に使用する証明書を選択します。
   - * オペレーティングシステムの CA 証明書を使用 * ：オペレーティングシステムにインストールされているデフォルトの Grid CA 証明書を使用して接続を保護します。
   - * カスタム CA 証明書を使用 * ：カスタムセキュリティ証明書を使用します。

     この設定を選択した場合は、カスタムセキュリティ証明書をコピーして CA 証明書テキストボックスに貼り付けます。

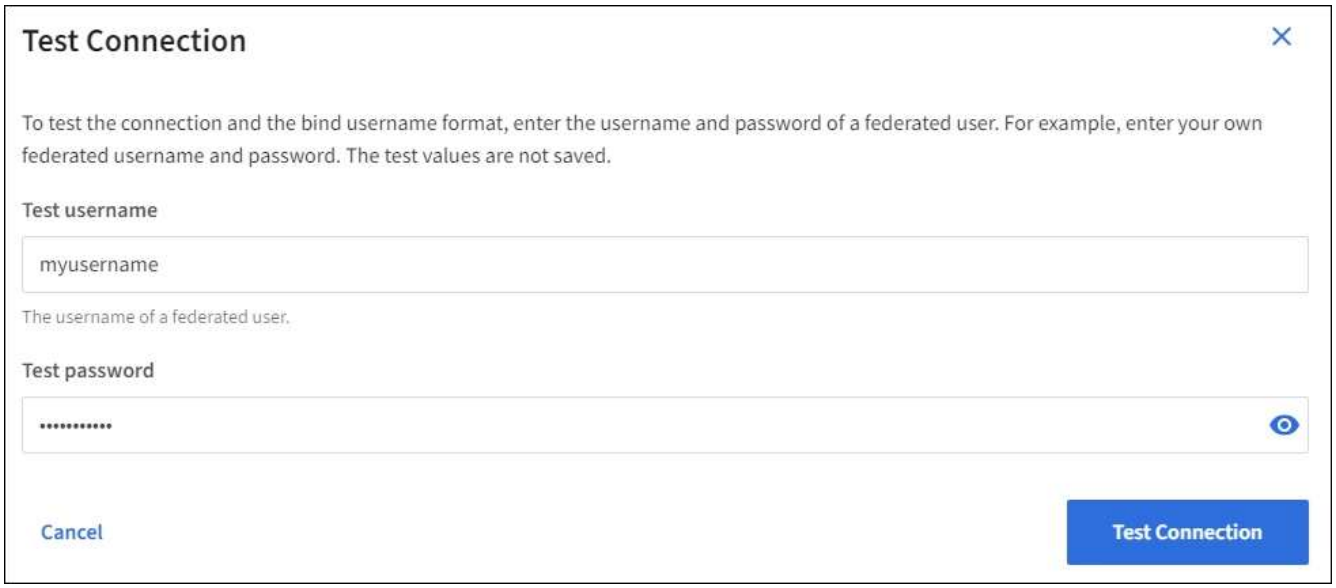
接続をテストして設定を保存します

すべての値を入力したら、設定を保存する前に接続をテストする必要があります。StorageGRID では、LDAP サーバの接続設定とバインドユーザ名の形式が指定されている場合は検証されます。

手順

1. [接続のテスト *] を選択します。
2. バインドユーザー名の形式を指定しなかった場合:
   - 接続設定が有効な場合は、「Test connection successful」というメッセージが表示されます。[保存（ Save ）] を選択して、構成を保存します。
   - 接続設定が無効な場合は、「test connection could not be established」というメッセージが表示されます。[閉じる（ Close ）] を選択します。その後、問題を解決して接続を再度テストします。
3. バインドユーザ名の形式を指定した場合は、有効なフェデレーテッドユーザのユーザ名とパスワードを入力します。

   たとえば、自分のユーザ名とパスワードを入力します。ユーザ名に特殊文字（@、/など）を使用しないでください。



   - 接続設定が有効な場合は、「Test connection successful」というメッセージが表示されます。[保存（

Save ）] を選択して、構成を保存します。

- 接続設定、バインドユーザ名形式、またはテストユーザ名とパスワードが無効な場合は、エラーメッセージが表示されます。問題を解決してから、もう一度接続をテストしてください。

アイデンティティソースとの強制同期

StorageGRID システムは、アイデンティティソースからフェデレーテッドグループおよびユーザを定期的に同期します。ユーザの権限をすぐに有効にしたり制限したりする必要がある場合は、同期を強制的に開始できます。

手順

1. アイデンティティフェデレーションページに移動します。
2. ページの上部にある「 * サーバーを同期」を選択します。

環境によっては、同期プロセスにしばらく時間がかかることがあります。

アイデンティティフェデレーション同期エラー * アラートは、アイデンティティソースからフェデレーテッドグループとユーザを同期する問題 がある場合にトリガーされます。

アイデンティティフェデレーションを無効にする

グループおよびユーザーの ID フェデレーションを一時的または永続的に無効にすることができます。アイデンティティ フェデレーションが無効になっている場合、 StorageGRIDとアイデンティティ ソース間の通信は行われません。ただし、構成した設定はすべて保持されるため、将来的に ID フェデレーションを簡単に再度有効にすることができます。

タスクの内容

アイデンティティフェデレーションを無効にする前に、次の点に注意してください。

- フェデレーテッドユーザはサインインできなくなります。
- 現在サインインしているフェデレーテッドユーザは、セッションが有効な間は StorageGRID システムに引き続きアクセスできますが、セッションが期限切れになると以降はサインインできなくなります。
- StorageGRIDシステムとアイデンティティ ソース間の同期は行われず、同期されていないアカウントに対してアラートは発生しません。
- シングル サインオン (SSO) ステータスが 有効 または サンドボックス モード の場合、**ID** フェデレーションを有効にする チェックボックスは無効になります。 ID フェデレーションを無効にする前に、シングル サインオン ページの SSO ステータスを 無効 にする必要があります。見る"シングルサインオンを無効にします" 。

手順

1. アイデンティティフェデレーションページに移動します。
2. [アイデンティティフェデレーションを有効にする]*チェックボックスをオフにします。

OpenLDAP サーバの設定に関するガイドライン

アイデンティティフェデレーションに OpenLDAP サーバを使用する場合は、 OpenLDAP サーバで特定の設定が必要です。

Active Directory または Microsoft Entra ID 以外の ID ソースの場合、 StorageGRID は外部的に無効にされているユーザーへの S3 アクセスを自動的にブロックしません。 S3 アクセスをブロックするには、ユーザーの S3 キーを削除するか、すべてのグループからユーザーを削除します。

memberof オーバーレイと **refint** オーバーレイ

memberof オーバーレイと refint オーバーレイを有効にする必要があります。詳細については、のリバースグループメンバーシップのメンテナンス手順を参照してくださいhttp://www.openldap.org/doc/admin24/index.html["OpenLDAP のドキュメント：バージョン 2.4 管理者ガイド"^]。

インデックス作成

次の OpenLDAP 属性とインデックスキーワードを設定する必要があります。

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

また、パフォーマンスを最適化するには、 Username のヘルプで説明されているフィールドにインデックスを設定してください。

のリバースグループメンバーシップのメンテナンスに関する情報を参照してくださいhttp://www.openldap.org/doc/admin24/index.html["OpenLDAP のドキュメント：バージョン 2.4 管理者ガイド"^]。

テナントグループを管理する

StorageGRIDで**S3**テナントのグループを作成する

S3 ユーザグループの権限を管理するには、フェデレーテッドグループをインポートするか、ローカルグループを作成します。

開始する前に

- を使用してTenant Managerにサインインしておき"サポートされている Web ブラウザ"ます。
- が設定されたユーザグループに属している"rootアクセス権限"必要があります。
- フェデレーテッドグループをインポートする場合は"アイデンティティフェデレーションが設定された"、そのフェデレーテッドグループが設定済みのアイデンティティソースにすでに存在している必要があります。
- テナントアカウントに グリッドフェデレーション接続の使用 権限があり、"テナントグループとユーザーの同期"のワークフローと考慮事項を確認済みで、テナントのソースグリッドにサインインしています。

グループ作成ウィザードにアクセスします

最初に、グループ作成ウィザードにアクセスします。

手順

1. アクセス管理 > *グループ*を選択します。
2. 「 * グループを作成 * 」を選択します。

グループタイプを選択します

ローカルグループを作成するか、フェデレーテッドグループをインポートできます。

手順

1. [ローカルグループ *] タブを選択してローカルグループを作成するか、または [フェデレーショングループ *] タブを選択して、以前に設定したアイデンティティソースからグループをインポートします。

   StorageGRID システムでシングルサインオン（ SSO ）が有効になっている場合、ローカルグループに属するユーザは Tenant Manager にサインインできません。ただし、クライアントアプリケーションを使用して、グループの権限に基づいてテナントのリソースを管理することはできます。

2. グループの名前を入力します。
   - * ローカルグループ * ：表示名と一意の名前の両方を入力します。表示名はあとで編集できます。

     テナントアカウントで* Use grid federation connection 権限が設定されている場合、デスティネーショングリッドにテナントに同じ unique name *がすでに存在すると、クローニングエラーが発生します。

   - * フェデレーショングループ * ：一意の名前を入力します。Active Directoryの場合、一意の名前は属性に関連付けられた名前です `sAMAccountName`。OpenLDAPの場合、一意の名前は属性に関連付けられた名前です `uid`。
3. 「 * Continue * 」を選択します。

グループの権限を管理します

グループ権限は、ユーザがTenant Managerおよびテナント管理APIで実行できるタスクを制御します。

手順

1. [アクセスモード]*で、次のいずれかを選択します。
   - * Read-write *（デフォルト）：ユーザはTenant Managerにサインインしてテナント設定を管理できます。
   - * 読み取り専用 * ：ユーザーは設定と機能のみを表示できます。Tenant Managerまたはテナント管理APIでは、変更を加えたり処理を実行したりすることはできません。ローカルの読み取り専用ユーザは自分のパスワードを変更できます。

     ユーザが複数のグループに属していて、いずれかのグループが読み取り専用に設定されている場合、選択したすべての設定と機能に読み取り専用でアクセスできます。

2. このグループの権限を1つ以上選択します。

   を参照して "テナント管理権限"

3. 「 * Continue * 」を選択します。

S3グループポリシーを設定

グループポリシーによって、ユーザに付与するS3アクセス権限が決まります。

手順

1. このグループに使用するポリシーを選択します。

グループポリシー	製品説明
S3アクセスがありません	デフォルト。バケットポリシーでアクセスが許可されていないかぎり、このグループのユーザはS3リソースにアクセスできません。このオプションを選択すると、デフォルトでは root ユーザにのみ S3 リソースへのアクセスが許可されます。
読み取り専用アクセス	このグループのユーザには、S3リソースへの読み取り専用アクセスが許可されます。たとえば、オブジェクトをリストして、オブジェクトデータ、メタデータ、タグを読み取ることができます。このオプションを選択すると、テキストボックスに読み取り専用グループポリシーの JSON 文字列が表示されます。この文字列は編集できません。
フルアクセス	このグループのユーザには、バケットを含むS3リソースへのフルアクセスが許可されます。このオプションを選択すると、テキストボックスにフルアクセスグループポリシーの JSON 文字列が表示されます。この文字列は編集できません。
ランサムウェアの軽減	この例では、このテナントのすべてのバケットを環境するポリシーを示します。このグループのユーザは共通の操作を実行できますが、オブジェクトのバージョン管理が有効になっているバケットからオブジェクトを完全に削除することはできません。 このグループポリシーは、* Manage all buckets *権限を持つTenant Managerユーザが上書きできます。[すべてのバケットを管理]権限を信頼できるユーザに制限し、可能な場合は多要素認証（MFA）を使用します。
カスタム	グループ内のユーザには、テキストボックスで指定した権限が付与されます。

2. 「 * Custom * 」を選択した場合は、グループポリシーを入力します。各グループポリシーのサイズは 5 、 120 バイトまでに制限されています。有効な JSON 形式の文字列を入力する必要があります。

   言語の構文や例など、グループポリシーの詳細については、を参照してください"グループポリシーの例"。

3. ローカルグループを作成する場合は、「 * Continue * 」を選択します。フェデレーテッドグループを作成する場合は、 * Create group * および * Finish * を選択します。

ユーザの追加（ローカルグループのみ）

ユーザを追加せずにグループを保存することも、必要に応じて既存のローカルユーザを追加することもできます。

手順

1. 必要に応じて、このグループに対して 1 人以上のローカルユーザを選択します。
2. [グループの作成 *] と [完了 *] を選択します。

   作成したグループがグループのリストに表示されます。

   テナントアカウントに「グリッドフェデレーション接続を使用する」権限があり、テナントのソースグリッド上にいる場合、新しいグループはテナントの宛先グリッドに同期されます。グループの詳細ページの概要セクションには、同期ステータスとして「成功」と表示されます。

StorageGRID テナント管理権限

テナントグループを作成する前に、そのグループに割り当てる権限を検討してください。テナント管理権限は、 Tenant Manager またはテナント管理 API を使用してユーザが実行できるタスクを決定します。ユーザは 1 つ以上のグループに属することができます。権限は、ユーザが複数のグループに属している場合に累積されます。

Tenant Manager にサインインするには、またはテナント管理 API を使用するには、少なくとも 1 つの権限が割り当てられたグループにユーザが属している必要があります。サインインできるすべてのユーザは、次のタスクを実行できます。

- ダッシュボードを表示します
- 自分のパスワードを変更する（ローカルユーザの場合）

すべての権限について、グループのアクセスモード設定によって、ユーザが設定を変更して処理を実行できるかどうか、またはユーザが関連する設定と機能のみを表示できるかどうかが決まります。

ユーザが複数のグループに属していて、いずれかのグループが読み取り専用に設定されている場合、選択したすべての設定と機能に読み取り専用でアクセスできます。

グループには次の権限を割り当てることができます。

権限	製品説明	詳細
ルートアクセス	Tenant Manager とテナント管理 API へのフルアクセスを提供します。	
自分のS3クレデンシャルを管理します	ユーザに自分の S3 アクセスキーの作成および削除を許可します。	この権限がないユーザには、* storage（S3）> My S3 access keys *メニューオプションが表示されません。

権限	製品説明	詳細
すべてのバケットを表示	ユーザーがすべてのバケットとバケット構成を表示できるようにします。	View All Buckets権限またはManage All Buckets権限がないユーザには、* Buckets *メニューオプションは表示されません。 この権限は、すべてのバケットの管理権限に置き換えられます。これは、S3 クライアントまたは S3 コンソールで使用される S3 バケットまたはグループ ポリシーには影響しません。
すべてのバケットを管理	ユーザーがテナント マネージャーとテナント管理 API を使用して、S3 バケットまたはグループ ポリシーに関係なく、S3 バケットを作成および削除したり、テナント アカウント内のすべての S3 バケットの設定を管理したりできるようにします。	View All Buckets権限またはManage All Buckets権限がないユーザには、* Buckets *メニューオプションは表示されません。 この権限は、「すべてのバケットを表示」権限よりも優先されます。これは、S3 クライアントまたは S3 コンソールで使用される S3 バケットまたはグループ ポリシーには影響しません。
エンドポイントを管理します	ユーザに、テナントマネージャまたはテナント管理APIを使用して、StorageGRID プラットフォームサービスのデスティネーションとして使用するプラットフォームサービスエンドポイントを作成または編集することを許可します。	この権限がないユーザーには、*プラットフォームサービスエンドポイント*メニューオプションは表示されません。
S3コンソールタブを使用	View All Buckets権限またはManage All Buckets権限と組み合わせると、ユーザはバケットの詳細ページにあるS3 Consoleタブでオブジェクトの表示と管理を行うことができます。	

StorageGRIDテナントグループを管理

必要に応じてテナントグループを管理し、グループの表示、編集、複製などを行います。

開始する前に

- を使用してTenant Managerにサインインしておき"サポートされている Web ブラウザ"ます。
- が設定されたユーザグループに属している"rootアクセス権限"必要があります。

グループを表示または編集します

各グループの基本情報と詳細を表示および編集できます。

手順

1. アクセス管理 > *グループ*を選択します。
2. [Groups]ページに表示される情報を確認します。このテナントアカウントのすべてのローカルグループとフェデレーテッドグループの基本情報が表示されます。

   テナントアカウントに* Use grid federation connection *権限があり、テナントのソースグリッド上のグループを表示している場合：

   - 宛先グリッドでテナントに同期されていないグループがある場合は、次の手順に従ってくださいグループ同期を再試行する。
3. グループの名前を変更する場合は、次の手順を実行します。
   a. グループのチェックボックスをオンにします。
   b. [* アクション * > * グループ名の編集 *] を選択します。
   c. 新しい名前を入力します。
   d. [変更を保存]*を選択します
4. 詳細を表示したり、追加の編集を行う場合は、次のいずれかを実行します。
   - グループ名を選択します。
   - グループのチェックボックスを選択し、**[操作]**>*[グループの詳細を表示]*を選択します。
5. [Overview]セクションには、グループごとに次の情報が表示されます。
   - 表示名
   - 一意の名前
   - タイプ
   - アクセスモード
   - 権限
   - S3ポリシー
   - このグループのユーザ数
   - テナントアカウントに* Use grid federation connection *権限があり、テナントのソースグリッドでグループを表示している場合は、次のフィールドが追加されます。
     - 同期ステータス（成功*または*失敗）
     - 連携グループの場合、青いバナーは、このグループを編集または削除しても、変更内容が他のグリッドに同期されないことを示しています。
6. 必要に応じてグループ設定を編集します。参照"S3 テナント用のグループを作成します"入力内容の詳細については、こちらをご覧ください。
   a. 概要セクションで、名前または編集アイコン を選択して表示名を変更します。
   b. [グループ権限]タブで権限を更新し、*[変更の保存]*を選択します。
   c. タブで、変更を加えて[変更の保存]*を選択します。

      必要に応じて、別の S3 グループポリシーを選択するか、カスタムポリシーの JSON 文字列を入力します。
7. 既存のローカルユーザをグループに追加するには、次の手順を実行します。

a. [Users]タブを選択します。



b. [ユーザの追加]*を選択します。

c. 追加する既存のユーザーを選択し、*ユーザーの追加*を選択します。

右上に成功メッセージが表示されます。

8. グループからローカルユーザを削除するには、次の手順を実行します

a. [Users]タブを選択します。

b. [ユーザの削除]*を選択します。

c. 削除するユーザを選択し、*[ユーザの削除]*を選択します。

右上に成功メッセージが表示されます。

9. 変更した各セクションで[変更を保存]*が選択されていることを確認します。

グループが重複しています

既存のグループを複製して、新しいグループをより迅速に作成できます。

テナントアカウントに「グリッドフェデレーション接続を使用する」権限が付与されている場合、テナントのソースグリッドからグループを複製すると、複製されたグループはテナントの宛先グリッドに同期されます。

手順

1. アクセス管理 > *グループ*を選択します。
2. 複製するグループのチェックボックスをオンにします。
3. [* アクション * > * グループの複製 *] を選択します。
4. 見る"S3 テナント用のグループを作成します"入力内容の詳細については、こちらをご覧ください。
5. 「 * グループを作成 * 」を選択します。

グループ同期を再試行する

いずれかのグループの同期に失敗した場合、そのグループの同期ステータス列に「Failed」と表示されます。テーブルの上にバナーが表示され、1つ以上のグループの同期に失敗したことを示します。

手順

同期を再試行するには：

1. バナーで「Retry sync」を選択します。この操作は、同期に失敗したすべてのグループの同期を再試行します。
2. 個々のグループの同期を再試行するには、グループ名を選択してください。グループの詳細ページで、*同期を再試行*を選択します。
3. 同期している各グループの詳細ページから、同期操作のステータスを確認できます。

再試行が成功すると、同期に成功した各グループの同期ステータス列に「Succeeded」と表示され、バナーが消えます。

詳細については、"テナントグループとユーザーを同期する"を参照してください。

1つ以上のグループを削除します

1つ以上のグループを削除できます。削除したグループにのみ属しているユーザは、Tenant Managerにサインインしたりテナントアカウントを使用したりできなくなります。

手順

1. アクセス管理 > *グループ*を選択します。
2. 削除する各グループのチェックボックスをオンにします。
3. >[グループの削除]または[アクション]>[グループの削除]*を選択します。

   確認のダイアログボックスが表示されます。
4. または[グループの削除]*を選択します。

AssumeRoleを設定する

開始する前に

AssumeRole を設定するには管理者である必要があります。

タスクの内容

AssumeRole を設定するには、グループがまだ存在しない場合は、想定されるターゲット グループを作成します。グループの S3 ポリシーを編集して、このグループを引き受ける場合に許可されるアクションを指定します。グループの S3 信頼ポリシーを編集して、AssumeRole API を使用してグループを引き継ぐことができる信頼できるユーザーを指定します。

このグループを想定して作成された一時的なセキュリティ資格情報は、限られた期間のみ有効です。セッションは 15 分から 12 時間までで、デフォルトのセッションは 1 時間です。グループの S3 信頼ポリシーからユーザーを削除すると、ユーザーはこのグループを引き受けることができなくなります。

手順

1. アクセス管理 > *グループ*を選択します。
2. グループ名を選択します。
3. **S3** 信頼ポリシー タブを選択します。
4. AssumeRole を実行できるユーザーのリストを含む S3 信頼ポリシーを追加します。
5. 「変更を保存」を選択します。

6. **S3** グループポリシー タブを選択します。
7. S3 ポリシーを編集して、このグループの S3 信頼ポリシーに追加された信頼できるユーザーに必要な S3 アクションのみを指定します。
8. 「変更を保存」を選択します。

AssumeRole S3信頼ポリシーの例

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Principal": {
                "AWS": [
                    "urn:sgws:identity::1234567890:user/user1",
                    "arn:aws:iam::1234567890:user/user2"
                ]
            }
        }
    ]
}
```

プリンシパル：

- `"Principal": "*"` 匿名（署名なし）リクエストを含む、すべてのユーザーに一致します
- `"Principal": { "AWS": "*" }`認証済みのIDまたはユーザーに一致する（匿名リクエストには一致しない）
- バケットポリシーにのみ適用されます
- プリンシパルとは、権限が付与または拒否されるアカウント/ユーザーのことです。

設定が完了すると、S3 信頼ポリシーにリストされているユーザーは AssumeRole を実行し、資格情報を受け取ることができます。最終的な権限は、グループ ポリシー、バケット ポリシー、およびセッション ポリシーによって決定されます。詳細については、 "アクセスポリシーを使用する" 。

StorageGRIDテナントユーザーを管理

ローカルユーザーを作成し、ローカルグループに割り当てることで、これらのユーザーがアクセスできる機能を決定できます。連携ユーザーをインポートすることもできます。テナントマネージャーには、_root_という名前の事前定義されたローカルユーザーが1人含まれています。ローカルユーザーの追加や削除は可能ですが、ルートユーザーを削除することはできません。

StorageGRID システムでシングル サインオン（SSO）が有効になっている場合、ローカルユーザーはテナントマネージャーやテナント管理 API にサインインできませんが、グループ権限に基づいてクライアントアプリケーションを使用してテナントのリソースにアクセスすることは可能です。

開始する前に

- を使用してTenant Managerにサインインしておき"サポートされている Web ブラウザ"ます。
- が設定されたユーザグループに属している"rootアクセス権限"必要があります。
- テナントアカウントに グリッドフェデレーション接続の使用 権限があり、"テナントグループとユーザーの同期"のワークフローと考慮事項を確認済みで、テナントのソースグリッドにサインインしています。

ローカルユーザを作成します

ローカルユーザを作成して1つ以上のローカルグループに割り当て、ユーザのアクセス権限を制御することができます。

どのグループにも属していないS3ユーザには、管理権限やS3グループポリシーが適用されていません。これらのユーザは、バケットポリシーを通じて S3 バケットアクセスを許可されている場合があります。

Create userウィザードにアクセスします

手順

1. アクセス管理 > *ユーザー*を選択します。
2. 「 * ユーザーの作成 * 」を選択します。

資格情報を入力します

手順

1. [ユーザクレデンシャルの入力]*ステップで、次のフィールドに値を入力します。

フィールド	製品説明
フルネーム	このユーザーのフルネーム（ユーザーの名と姓、アプリケーションの名前など）。
ユーザ名	このユーザがサインインに使用する名前。ユーザ名は一意である必要があり、変更することはできません。 注：テナントアカウントに* Use grid federation connection 権限が設定されている場合、デスティネーショングリッドにテナントに同じ Username *がすでに存在すると、クローニングエラーが発生します。
	ユーザがサインイン時に最初に使用するパスワード。

フィールド	製品説明
アクセスを拒否します	このユーザが1つ以上のグループに属している場合でもテナントアカウントにサインインできないようにするには、*[はい]*を選択します。 たとえば、*[はい]*を選択すると、ユーザーのサインイン機能が一時的に中断されます。

2. 「 * Continue * 」を選択します。

グループに割り当てます

手順

1. ユーザを1つ以上のローカルグループに割り当てて、実行できるタスクを決定します。

   グループへのユーザの割り当ては任意です。必要に応じて、グループを作成または編集するときにユーザーを選択できます。

   どのグループにも属していないユーザには、管理権限はありません。アクセス許可は累積的に追加されユーザには、自身が属しているすべてのグループに対するすべての権限が与えられます。を参照して "テナント管理権限"

2. 「 * ユーザーの作成 * 」を選択します。

   テナントアカウントに「グリッドフェデレーション接続を使用する」権限があり、かつテナントのソースグリッド上にいる場合、新しいローカルユーザーはテナントの宛先グリッドに同期されます。ユーザーの詳細ページの概要セクションの「同期ステータス」に「成功」と表示されます。

3. [完了]*を選択して[ユーザー]ページに戻ります。

ローカルユーザを表示または編集します

手順

1. アクセス管理 > *ユーザー*を選択します。
2. [Users]ページに表示される情報を確認します。このテナントアカウントのすべてのローカルユーザとフェデレーテッドユーザの基本情報が表示されます。
3. ユーザのフルネームを変更する場合は、次の手順を実行します。
   a. ユーザのチェックボックスを選択します。
   b. * アクション * > * フルネームの編集 * を選択します。
   c. 新しい名前を入力します。
   d. [変更を保存]*を選択します
4. 詳細を表示したり、追加の編集を行う場合は、次のいずれかを実行します。
   - ユーザ名を選択します。
   - ユーザのチェックボックスを選択し、**[操作]>**[ユーザの詳細を表示]*を選択します。
5. [Overview]セクションには、ユーザごとに次の情報が表示されます。

- フルネーム
- ユーザ名
- ユーザタイプ
- アクセスを拒否しました
- アクセスモード
- グループメンバーシップ

6. 必要に応じてユーザー設定を編集します。入力する項目の詳細については、を参照してくださいローカルユーザを作成します。
   a. 概要セクションで、名前または編集アイコン を選択してフルネームを変更します。

      ユーザー名は変更できません。

   b. タブで、ユーザのパスワードを変更し、[変更を保存]*を選択します。
   c. [アクセス]タブで、**[**いいえ**]**を選択してユーザーがサインインできるようにするか、[はい]を選択してユーザーがサインインできないようにします。次に、*[変更の保存]*を選択します。
   d. [アクセスキー]タブで、*[キーの作成]*を選択し、の手順に従います"別のユーザのS3アクセスキーを作成しています"。
   e. タブで[グループの編集]*を選択して、ユーザーをグループに追加するか、ユーザーをグループから削除します。次に、*変更を保存*を選択します。
7. 変更した各セクションで[変更を保存]*が選択されていることを確認します。

フェデレーションユーザーのインポート

1 人以上のフェデレーション ユーザー (最大 100 人) を [ユーザー] ページに直接インポートできます。

手順

1. アクセス管理 > *ユーザー*を選択します。
2. *フェデレーション ユーザーのインポート*を選択します。
3. 1 人以上のフェデレーション ユーザーの UUID またはユーザー名を入力します。

   複数のエントリの場合は、各 UUID またはユーザー名を新しい行に追加します。

4. *インポート*を選択します。

   1 人以上のユーザーの「ユーザー」フィールドへのインポートが失敗した場合は、次の手順を実行します。

   a. *インポートされていないユーザー*を展開し、*ユーザーのコピー*を選択します。
   b. 前へ*を選択し、コピーしたユーザーを*フェデレーション ユーザーのインポート ダイアログ ボックスに貼り付けて、インポートを再試行します。

[フェデレーション ユーザーのインポート**]** ダイアログ ボックスを閉じると、正常にインポートされたユーザーの [ユーザー] ページにフェデレーション ユーザー情報が表示されます。

ローカルユーザが重複しています

ローカルユーザを複製して新しいユーザを迅速に作成することができます。

> テナントアカウントに「グリッドフェデレーション接続を使用する」権限が付与されている場合、テナントのソースグリッドからユーザーを複製すると、複製されたユーザーはテナントの宛先グリッドに同期されます。

手順

1. アクセス管理 > *ユーザー*を選択します。
2. 複製するユーザのチェックボックスをオンにします。
3. * アクション * > * ユーザーの複製 * を選択します。
4. 入力する項目の詳細については、を参照してくださいローカルユーザを作成します。
5. 「 * ユーザーの作成 * 」を選択します。

ユーザー同期を再試行する

同期に失敗したユーザーについては、そのユーザーの同期ステータス列に「Failed」と表示されます。テーブルの上にバナーが表示され、1人以上のユーザーが同期に失敗したことを示します。

手順

同期を再試行するには：

1. バナーで「Retry sync」を選択します。この操作により、同期に失敗したすべてのユーザーの同期が再試行されます。
2. 個々のユーザーの同期を再試行するには、ユーザー名を選択してください。ユーザー詳細ページで、*同期を再試行*を選択します。
3. 同期している各ユーザーの詳細ページから、同期操作のステータスを確認できます。

再試行が成功すると、同期に成功した各ユーザーの同期ステータス列に「Succeeded」と表示され、バナーが消えます。

詳細については、"テナントグループとユーザーを同期する"を参照してください。

1人以上のローカルユーザを削除します

StorageGRID テナントアカウントにアクセスする必要がなくなった1人以上のローカルユーザを完全に削除できます。

> テナントアカウントに グリッドフェデレーション接続の使用 権限があり、ローカルユーザーを削除すると、StorageGRID は接続先の他のグリッド上の対応するユーザーを削除します。ただし、そのユーザーがターゲットグリッド上のフェデレーションユーザーである場合は除きます。フェデレーションユーザーを削除するには、フェデレーション ID ソースを使用する必要があります。

手順

1. アクセス管理 > *ユーザー*を選択します。

2. 削除する各ユーザのチェックボックスをオンにします。
3. >[ユーザーの削除]または[操作]>[ユーザーの削除]*を選択します。

   確認のダイアログボックスが表示されます。

4. または[ユーザの削除]*を選択します。

S3 アクセスキーを管理します

StorageGRIDでS3アクセスキーを管理

S3 テナントアカウントの各ユーザには、 StorageGRID システムでオブジェクトの格納と読み出しを行うためのアクセスキーが必要です。アクセスキーは、アクセスキー ID とシークレットアクセスキーで構成されます。

S3 アクセスキーは次のように管理できます。

- Manage your own S3 credentials *権限を持つユーザは、自分のS3アクセスキーを作成または削除できます。
- Root access *権限を持つユーザは、S3 rootアカウントとその他すべてのユーザのアクセスキーを管理できます。root アクセスキーは、バケットポリシーで root アクセスキーが明示的に無効になっていないかぎり、テナントのすべてのバケットとオブジェクトへのフルアクセスを提供します。

StorageGRID では、署名バージョン 2 と署名バージョン 4 の認証がサポートされています。クロスアカウントアクセスは、バケットポリシーで明示的に有効になっていないかぎり、許可されません。

StorageGRID で独自の S3 アクセスキーを作成

S3 テナントを使用している場合は、適切な権限があれば、自分の S3 アクセスキーを作成できます。バケットとオブジェクトにアクセスするには、アクセスキーが必要です。

開始する前に

- を使用してTenant Managerにサインインしておき"サポートされている Web ブラウザ"ます。
- が設定されたユーザグループに属している"自分のS3クレデンシャルまたはRoot Access権限を管理します"必要があります。

タスクの内容

テナントアカウントのバケットを作成および管理できる S3 アクセスキーを 1 つ以上作成できます。新しいアクセスキーを作成したら、新しいアクセスキー ID とシークレットアクセスキーでアプリケーションを更新します。セキュリティのため、必要以上のキーを作成しないで、使用していないキーを削除してください。キーが 1 つしかなく、有効期限が近づいている場合は、古いキーが期限切れになる前に新しいキーを作成してから、古いキーを削除します。

各キーには、特定の有効期限または有効期限を設定できません。有効期限については、次のガイドラインに従ってください。

- キーの有効期限を設定して、アクセスを特定の期間に制限します。短い有効期限を設定すると、アクセスキー ID とシークレットアクセスキーが誤って公開されるリスクを低減できます。期限切れのキーは自動的に削除されます。

- 環境のセキュリティリスクが低く、新しいキーを定期的に作成する必要がない場合は、キーの有効期限を設定する必要はありません。あとで新しいキーを作成する場合は、古いキーを手動で削除します。

> アカウントに属する S3 バケットとオブジェクトには、 Tenant Manager でアカウントに表示されるアクセスキー ID とシークレットアクセスキーを使用してアクセスできます。このため、アクセスキーはパスワードと同じように保護する必要があります。定期的にアクセスキーをローテーションし、使用されていないキーはアカウントから削除します。また、他のユーザとはアクセスキーを共有しないでください。

手順

1. 「 * storage （ S3 ） * > * My access keys * 」を選択します。

   [マイアクセスキー] ページが表示され、既存のアクセスキーが一覧表示されます。

2. 「 * キーの作成 * 」を選択します。
3. 次のいずれかを実行します。
   - 有効期限を設定しない * を選択して、有効期限が切れないキーを作成します。（デフォルト）
   - [有効期限の設定 *] を選択し、有効期限の日付と時刻を設定します。

     > 有効期限は、現在の日付から最大5年間です。有効期限は、現在の時刻から少なくとも1分後に設定できます。

4. [アクセスキーの作成 *] を選択します。

   Download access key （アクセスキーのダウンロード）ダイアログボックスが表示され、アクセスキー ID とシークレットアクセスキーが一覧表示されます。

5. アクセスキー ID とシークレットアクセスキーを安全な場所にコピーするか、「 * Download.csv * 」を選択してアクセスキー ID とシークレットアクセスキーを含むスプレッドシートファイルを保存します。

   > この情報をコピーまたはダウンロードするまで、このダイアログボックスを閉じないでください。ダイアログボックスを閉じた後は、キーをコピーまたはダウンロードすることはできません。

6. [完了] を選択します。

   新しいキーは [マイアクセスキー] ページに表示されます。

StorageGRIDでS3アクセスキーを表示する

S3テナントを使用していて、を使用している場合は"適切な権限"、S3アクセスキーのリストを表示できます。有効期限でリストをソートすると、まもなく期限切れになるキーを確認できます。必要に応じて、を使用することも、使用しないことも"キーを削除します"できます"新しいキーを作成します"。

アカウントに属する S3 バケットとオブジェクトには、 Tenant Manager でアカウントに表示されるアクセスキー ID とシークレットアクセスキーを使用してアクセスできます。このため、アクセスキーはパスワードと同じように保護する必要があります。定期的にアクセスキーをローテーションし、使用されていないキーはアカウントから削除します。また、他のユーザとはアクセスキーを共有しないでください。

開始する前に

- を使用してTenant Managerにサインインしておき"サポートされている Web ブラウザ"ます。
- [Manage Your Own S3 credential]が設定されたユーザグループに属している必要があり"アクセス権"ます。

手順

1. 「 * storage （ S3 ） * > * My access keys * 」を選択します。
2. [アクセスキー]ページで、既存のアクセスキーを*または[アクセスキーID]*でソートします。
3. 必要に応じて、新しいキーを作成するか、使用しなくなったキーを削除します。

   既存のキーの有効期限が切れる前に新しいキーを作成した場合は、アカウントのオブジェクトに一時的にアクセスできなくなることなく、新しいキーの使用を開始できます。

   期限切れのキーは自動的に削除されます。

StorageGRID で自分の S3 アクセスキーを削除する

S3 テナントを使用している場合は、適切な権限があれば、自分の S3 アクセスキーを削除できます。アクセスキーを削除すると、テナントアカウント内のオブジェクトとバケットにそのアクセスキーでアクセスできなくなります。

開始する前に

- を使用してTenant Managerにサインインしておき"サポートされている Web ブラウザ"ます。
- あなたはを持っています"Manage Your Own S3 credentialsケンケン"。

アカウントに属する S3 バケットとオブジェクトには、 Tenant Manager でアカウントに表示されるアクセスキー ID とシークレットアクセスキーを使用してアクセスできます。このため、アクセスキーはパスワードと同じように保護する必要があります。定期的にアクセスキーをローテーションし、使用されていないキーはアカウントから削除します。また、他のユーザとはアクセスキーを共有しないでください。

手順

1. 「 * storage （ S3 ） * > * My access keys * 」を選択します。
2. [My access keys]ページで、削除する各アクセスキーのチェックボックスをオンにします。
3. 「 * Delete key （キーの削除）」 * を選択
4. 確認ダイアログボックスで、* Delete key *を選択します。

   ページの右上に確認メッセージが表示されます。

StorageGRID で別のユーザーのS3アクセスキーを作成します

S3 テナントを使用している場合は、適切な権限があれば、バケットやオブジェクトにアクセスする必要があるアプリケーションなど、他のユーザの S3 アクセスキーを作成できます。

開始する前に

- を使用してTenant Managerにサインインしておき"サポートされている Web ブラウザ"ます。
- が設定されたユーザグループに属している"rootアクセス権限"必要があります。

タスクの内容

他のユーザがテナントアカウントのバケットを作成および管理できるように、 1 つ以上の S3 アクセスキーを作成できます。新しいアクセスキーを作成したら、新しいアクセスキー ID とシークレットアクセスキーでアプリケーションを更新します。セキュリティを確保するため、ユーザが必要とする数以上のキーを作成しないでください。また、使用されていないキーは削除してください。キーが 1 つしかなく、有効期限が近づいている場合は、古いキーが期限切れになる前に新しいキーを作成してから、古いキーを削除します。

各キーには、特定の有効期限または有効期限を設定できません。有効期限については、次のガイドラインに従ってください。

- キーの有効期限を設定して、ユーザのアクセスを一定期間に制限します。短い有効期限を設定すると、アクセスキー ID とシークレットアクセスキーが誤って公開されるリスクを低減できます。期限切れのキーは自動的に削除されます。
- 環境のセキュリティリスクが低く、新しいキーを定期的に作成する必要がない場合は、キーの有効期限を設定する必要はありません。あとで新しいキーを作成する場合は、古いキーを手動で削除します。

> ユーザに属する S3 バケットとオブジェクトには、 Tenant Manager でそのユーザに対して表示されるアクセスキー ID とシークレットアクセスキーを使用してアクセスできます。このため、アクセスキーはパスワードと同じように保護する必要があります。定期的にアクセスキーをローテーションし、使用されていないキーはアカウントから削除します。また、他のユーザとはアクセスキーを共有しないでください。

手順

1. アクセス管理 > *ユーザー*を選択します。
2. S3 アクセスキーを管理するユーザを選択します。

   ユーザーの詳細ページが表示されます。
3. [* アクセスキー *] を選択し、 [* キーの作成 *] を選択します。
4. 次のいずれかを実行します。
   - 有効期限のないキーを作成するには、[有効期限を設定しない]*を選択します。（デフォルト）
   - [有効期限の設定 *] を選択し、有効期限の日付と時刻を設定します。

     > 有効期限は、現在の日付から最大5年間です。有効期限は、現在の時刻から少なくとも1分後に設定できます。
5. [アクセスキーの作成 *] を選択します。

Download access key （アクセスキーのダウンロード）ダイアログボックスが表示され、アクセスキー ID とシークレットアクセスキーが一覧表示されます。

6. アクセスキー ID とシークレットアクセスキーを安全な場所にコピーするか、「 * Download.csv * 」を選択してアクセスキー ID とシークレットアクセスキーを含むスプレッドシートファイルを保存します。

> この情報をコピーまたはダウンロードするまで、このダイアログボックスを閉じないでください。ダイアログボックスを閉じた後は、キーをコピーまたはダウンロードすることはできません。

7. [完了] を選択します。

   新しいキーは、ユーザ詳細ページのアクセスキータブに表示されます。

StorageGRID で他のユーザーの S3 アクセスキーを表示する

S3 テナントを使用している場合は、適切な権限があれば、別のユーザの S3 アクセスキーを表示できます。有効期限でリストをソートすると、まもなく期限切れになるキーを確認できます。必要に応じて、新しいキーを作成したり、使用されなくなったキーを削除したりできます。

開始する前に

- を使用してTenant Managerにサインインしておき"サポートされている Web ブラウザ"ます。
- あなたはを持っています"rootアクセス権限"。

> ユーザに属する S3 バケットとオブジェクトには、 Tenant Manager でそのユーザに対して表示されるアクセスキー ID とシークレットアクセスキーを使用してアクセスできます。このため、アクセスキーはパスワードと同じように保護する必要があります。定期的にアクセスキーをローテーションし、使用されていないキーはアカウントから削除します。また、他のユーザとはアクセスキーを共有しないでください。

手順

1. アクセス管理 > *ユーザー*を選択します。
2. [Users]ページで、表示するS3アクセスキーを所有するユーザを選択します。
3. [ユーザの詳細]ページで、*[アクセスキー]*を選択します。
4. キーを * Expiration time * または * Access key ID * でソートします。
5. 必要に応じて、新しいキーを作成し、使用しなくなったキーを手動で削除します。

   既存のキーの有効期限が切れる前に新しいキーを作成した場合、ユーザはアカウントのオブジェクトに一時的にアクセスできなくなることなく、新しいキーの使用を開始できます。

   期限切れのキーは自動的に削除されます。

関連情報

- "別のユーザの S3 アクセスキーを作成します"

- "別のユーザの S3 アクセスキーを削除します"

StorageGRID で他のユーザーの **S3** アクセスキーを削除する

S3 テナントを使用している場合は、適切な権限があれば、別のユーザの S3 アクセスキーを削除できます。アクセスキーを削除すると、テナントアカウント内のオブジェクトとバケットにそのアクセスキーでアクセスできなくなります。

開始する前に

- を使用してTenant Managerにサインインしておき"サポートされている Web ブラウザ"ます。
- あなたはを持っています"rootアクセス権限"。

> ユーザに属する S3 バケットとオブジェクトには、 Tenant Manager でそのユーザに対して表示されるアクセスキー ID とシークレットアクセスキーを使用してアクセスできます。このため、アクセスキーはパスワードと同じように保護する必要があります。定期的にアクセスキーをローテーションし、使用されていないキーはアカウントから削除します。また、他のユーザとはアクセスキーを共有しないでください。

手順

1. アクセス管理 > *ユーザー*を選択します。
2. [Users]ページで、管理するS3アクセスキーを所有するユーザを選択します。
3. [ユーザの詳細]ページで*[アクセスキー]*を選択し、削除する各アクセスキーのチェックボックスをオンにします。
4. * アクション * > * 選択したキーを削除 * を選択します。
5. 確認ダイアログボックスで、* Delete key *を選択します。

   ページの右上に確認メッセージが表示されます。

S3 バケットを管理する

StorageGRID S3バケットを作成する

Tenant Manager を使用して、オブジェクトデータ用の S3 バケットを作成できます。

開始する前に

- を使用してTenant Managerにサインインしておき"サポートされている Web ブラウザ"ます。
- [Root access]または[Manage all buckets]が設定されたユーザグループに属している必要"アクセス権"があります。これらの権限は、グループまたはバケットポリシーの権限の設定よりも優先されます。

> バケットまたはオブジェクトのS3オブジェクトロックプロパティを設定または変更する権限は、"バケットポリシーまたはグループポリシー" 。

- バケットでS3オブジェクトロックを有効にする場合は、グリッド管理者がStorageGRID システムに対してグローバルなS3オブジェクトロック設定を有効にし、S3オブジェクトロックのバケットとオブジェクトの要件を確認しておく必要があります。

- 複数のテナントがそれぞれ最大5,000個のバケットを持つ場合、グリッド内の各ストレージノードには最低64 GBのRAMが必要です。

> StorageGRIDシステムは、S3テナントアカウントごとに最大20,000個のバケットをサポートします。各グリッドには、"ブランチバケット"を含め、最大100,000個のバケットを含めることができます。また、"枝のバケット深度"にも制限があります。

ウィザードにアクセスします

手順

1. ダッシュボードで* View Buckets を選択するか、 storage（S3）> Buckets *を選択します。
2. [* バケットの作成 *] を選択します。

詳細を入力します

手順

1. バケットの詳細を入力します。

フィールド	製品説明
バケット名	次のルールを満たすバケットの名前。 • StorageGRID システム全体で（テナントアカウント内だけではなく）一意である必要があります。 • DNS に準拠している必要があります。 • 3文字以上63文字以下にする必要があります。 • 各ラベルの先頭と末尾の文字は小文字のアルファベットか数字にする必要があり、使用できる文字は小文字のアルファベット、数字、ハイフンのみです。 • 仮想ホスト形式の要求にピリオドを含めることはできません。ピリオドを使用すると、サーバワイルドカード証明書の検証で原因 の問題が発生します。 詳細については、 "バケットの命名規則に関する Amazon Web Services （ AWS ）のドキュメント"を参照してください。 注：バケットの作成後にバケット名を変更することはできません。
地域	バケットのリージョン。 利用可能なリージョンはStorageGRID管理者が管理します。バケットのリージョンは、オブジェクトに適用されるデータ保護ポリシーに影響を与える可能性があります。デフォルトでは、すべてのバケットは `us-east-1`地域。デフォルトのリージョンが以下のリージョン以外に設定されている場合 `us-east-1`、ドロップダウンではこの他の領域が最初に選択されます。 注：バケットの作成後にリージョンを変更することはできません。

2. 「 * Continue * 」を選択します。

設定の管理

手順

1. 必要に応じて、バケットのオブジェクトのバージョン管理を有効にします。

   このバケット内の各オブジェクトのすべてのバージョンを格納する場合は、オブジェクトのバージョン管理を有効にします。そのあと、必要に応じて以前のバージョンのオブジェクトを読み出すことができます。

   次の場合には、オブジェクトのバージョン管理を有効にする必要があります。

   - バケットはクロスグリッドレプリケーションに使用されます。
   - 作成したい"ブランチバケット"このバケツから。

2. S3オブジェクトロックのグローバル設定が有効になっている場合は、必要に応じて、バケットのS3オブジェクトロックを有効にして、Write-Once-Read-Many（WORM）モデルを使用してオブジェクトを格納します。

   バケットのS3オブジェクトロックは、一定の規制要件を満たすためにオブジェクトを一定期間保持する必要がある場合にのみ有効にしてください。S3オブジェクトロックは永続的な設定で、オブジェクトの削除や上書きを一定期間または無期限に防ぐことができます。

   > バケットでS3オブジェクトロックの設定を有効にしたあとに無効にすることはできません。このバケットには、適切な権限を持つユーザがオブジェクトを追加して変更できないようにすることができます。これらのオブジェクトやバケット自体を削除できない場合があります。

   バケットで S3 オブジェクトのロックを有効にすると、バケットのバージョン管理が自動的に有効になります。

3. [S3オブジェクトロックを有効にする]*を選択した場合は、必要に応じてこのバケットに対して*デフォルトの保持*を有効にします。

   > グリッド管理者は、に対する権限をユーザに付与する必要があります"S3オブジェクトロックの特定の機能を使用する"。

   default retention *を有効にすると、バケットに追加された新しいオブジェクトが自動的に削除または上書きされなくなります。デフォルトの保持*設定は、独自の保持期間を持つオブジェクトには適用されません。

   a. default retention が有効になっている場合は、バケットの default retention mode *を指定します。

デフォルトの保持モード	製品説明
ガバナンス	• 権限を持つユーザ `s3:BypassGovernanceRetention`は、要求ヘッダーを使用して保持設定を省略でき `x-amz-bypass-governance-retention: true`ます。 • これらのユーザは、retain-until-dateに達する前にオブジェクトバージョンを削除できます。 • これらのユーザは、オブジェクトのretain-until-dateを増減、または削除できます。
コンプライアンス	• retain-until-dateに達するまで、オブジェクトを削除できません。 • オブジェクトのretain-until-dateは増やすことはできますが、減らすことはできません。 • オブジェクトのretain-until-dateは、その日付に達するまで削除できません。 注：グリッド管理者が準拠モードの使用を許可する必要があります。

b. default retention が有効になっている場合は、バケットの default retention period *を指定します。

Default retention period *は、このバケットに追加された新しいオブジェクトを取り込んだ時点から保持する期間です。グリッド管理者が設定したテナントの最大保持期間以下の値を指定します。

A_maximum_retention periodは、グリッド管理者がテナントを作成するときに設定されます。指定できる値は1~100年です。_default_retention periodを設定する場合、最大保持期間に設定された値を超えることはできません。必要に応じて、最大保持期間を増減するようにグリッド管理者に依頼します。

4. 必要に応じて、「容量制限を有効にする」を選択し、値を入力して、容量単位を選択します。

容量制限は、このバケットのオブジェクトに使用できる最大容量です。この値は、物理容量（ディスク上のサイズ）ではなく、論理容量（オブジェクトサイズ）を表します。

制限が設定されていない場合、このバケットの容量は無制限です。詳細については、を参照してください"ヨウリヨウセイケンシヨウ" 。

5. オプションで、「オブジェクト数の制限を有効にする」を選択します。

オブジェクト数の制限は、このバケットに含めることができるオブジェクトの最大数です。この値は論理量 (オブジェクト数) を表します。制限が設定されていない場合、オブジェクト数は無制限になります。

6. [* バケットの作成 *] を選択します。

バケットが作成され、バケットページのテーブルに追加されます。

7. 必要に応じて、*[Go to bucket details page]*を選択し"バケットの詳細を表示します"て追加の設定を実行します。

また、"ブランチバケットを作成する"必要に応じて。

StorageGRID で **S3** バケットの詳細を表示する

テナントアカウント内のバケットを表示できます。

開始する前に

- を使用してTenant Managerにサインインしておき"サポートされている Web ブラウザ"ます。
- が設定されたユーザグループに属している"rootアクセス、Manage All Buckets、View All Buckets権限"必要があります。これらの権限は、グループポリシーまたはバケットポリシーの権限設定よりも優先されます。

手順

1. ダッシュボードで* View Buckets を選択するか、 storage（S3）> Buckets *を選択します。

   [Buckets]ページが表示されます。

2. 各バケットの概要テーブルを確認します。

   必要に応じて、任意の列で情報をソートしたり、リストを前後にページ移動したりできます。

   > 表示される[Object Count]、[Space Used]、および[Usage]の値は推定値です。これらの推定値は、取り込みのタイミング、ネットワーク接続、ノードのステータスによって左右されます。バケットでバージョン管理が有効になっている場合は、削除したオブジェクトのバージョンがオブジェクト数に含まれます。

   名前
   : バケットの一意の名前。変更することはできません。

   有効な機能
   : バケットで有効になっている機能のリスト。

   S3 オブジェクトのロック
   : バケットでS3オブジェクトロックが有効になっているかどうか。

     この列は、グリッドでS3オブジェクトロックが有効になっている場合にのみ表示されます。この列には、古い準拠バケットの情報も表示されます。

   地域
   : バケットのリージョン。変更できません。この列はデフォルトでは非表示になっています。

   オブジェクト数
   : このバケット内のオブジェクトの数。バケットでバージョン管理が有効になっている場合は、最新でないオブジェクトバージョンがこの値に含まれます。

     オブジェクトが追加または削除されたときに、この値がすぐに更新されないことがあります。

   使用済みスペース
   : バケット内のすべてのオブジェクトの論理サイズ。論理サイズには、レプリケートコピーやイレイジャーコーディングコピー、またはオブジェクトメタデータに必要な実際のスペースは含まれていません。

この値の更新には最大10分かかることがあります。

使用法

バケットの容量制限に対して使用されている割合（設定されている場合）。

使用量の値は内部の見積もりに基づいており、場合によっては超過する可能性があります。たとえば、StorageGRIDはテナントがオブジェクトのアップロードを開始すると容量制限をチェックし（設定されている場合）、テナントが容量制限を超えた場合はこのバケットへの新しい取り込みを拒否します。ただし、StorageGRIDでは、容量制限を超えたかどうかを判断する際に、現在のアップロードのサイズは考慮されません。オブジェクトが削除されると、容量制限の使用量が再計算されるまで、テナントが新しいオブジェクトをこのバケットにアップロードできなくなることがあります。計算には10分以上かかることがあります。

この値は論理サイズを示し、オブジェクトとそのメタデータの格納に必要な物理サイズではありません。

容量

バケットの容量制限（設定されている場合）。

作成日

バケットが作成された日時。この列はデフォルトでは非表示になっています。

3. 特定のバケットの詳細を表示するには、テーブルでバケット名を選択します。
   a. Webページの上部にある概要情報を表示して、バケットの詳細（リージョンやオブジェクト数など）を確認します。
   b. 容量制限の使用状況とオブジェクト数制限の使用状況のバーを表示します。使用率が 100% または 100% に近い場合は、制限を増やすか、一部のオブジェクトを削除することを検討してください。
   c. 必要に応じて、**[Delete objects in bucket]***および[Delete bucket]*を選択します。



これらの各オプションを選択する際に表示される注意事項に細心の注意を払ってください。詳細については、以下を参照してください。

- "バケット内のすべてのオブジェクトを削除する"
- "バケットを削除する"（バケットは空にする必要があります）

   d. 必要に応じて、各タブでバケットの設定を表示または変更します。
      - * S3コンソール*：バケットのオブジェクトを表示します。詳細については、を参照してください "S3コンソールを使用"。
      - バケットオプション：オプション設定を表示または変更します。S3オブジェクトロックなどの一部の設定は、バケットの作成後に変更できません。
        - "バケットの整合性の管理"
        - "最終アクセス時間の更新"
        - "容量制限"
        - "オブジェクト数の制限"
        - "オブジェクトのバージョン管理"

        - "S3 オブジェクトのロック"
        - "デフォルトのバケット保持"
        - "グリッド間レプリケーションを管理します"（テナントに許可されている場合）
    - プラットフォームサービス："プラットフォームサービスを管理します"（テナントで許可されている場合）
    - バケットアクセス：オプション設定を表示または変更します。特定のアクセス権限が必要です。
        - 設定"バケットとオブジェクトの CORS"そのため、バケットとバケット内のオブジェクトは他のドメインの Web アプリケーションからアクセスできるようになります。
        - "ユーザアクセスの制御"（S3バケットとそのバケット内のオブジェクト）。
    - ブランチ: バケットのブランチ バケットのリストを表示します。"新しいブランチバケットを作成するか、ブランチバケットを管理する" 。

StorageGRIDブランチバケットについて学ぶ

ブランチ バケットは、特定の時間に存在していたバケット内のオブジェクトへのアクセスを提供します。

既存のバケットからブランチ バケットを作成します。ブランチ バケットを作成すると、その作成元となった元のバケットは ベース バケット と呼ばれます。さらに、別のブランチ バケットからブランチ バケットを作成することもできます。

ブランチ バケットは保護されたデータへのアクセスを提供しますが、バックアップとしては機能しません。引き続きデータを保護するには、ベース バケットで次の機能を使用します。

- "S3 オブジェクトのロック"
- "グリッド間レプリケーション"ベースバケット用
- "バケットポリシー"バージョン管理されたバケットで古いオブジェクトのバージョンをクリーンアップする

ブランチ バケットの次の特性に注意してください。

- ブランチバケット内のオブジェクトにアクセスするには、"オブジェクトをダウンロードするためのS3コンソール" 。
- クライアントがブランチバケット内のオブジェクトにアクセスすると、ブランチバケットの"アクセスポリシー"ベース バケットのポリシーではなく、アクセスを許可するか拒否するかを決定します。
- ベースバケットに作成されたオブジェクトは、"ILM ルール"ベースバケットに適用します。ブランチ バケットに作成されたオブジェクトは、ILM ルールがブランチ バケットにどのように適用されるかに基づいて評価されます。
- ブランチ バケットでは、クロス グリッド レプリケーションはサポートされていません。
- プラットフォーム サービスはブランチ バケットではサポートされていません。

ブランチバケットの使用例

- 破損が発生する前の時点からブランチ バケットを作成し、破損したオブジェクトを含むベース バケットではなくブランチ バケットをアプリケーションに指定することで、ブランチ バケットを使用して破損したオブジェクトを削除できます。

- バージョン管理されたバケットにデータを保存しています。偶発的な脆弱性があり、時間 *T* 以降に多くの不要なオブジェクトが取り込まれました。 Before 時間値 *T* のブランチ バケットを作成し、クライアント操作をそのブランチ バケットにリダイレクトできます。その後、Before 時間 *T* より前に取り込まれたオブジェクトのみがクライアントに公開されます。
- バージョン管理されたバケットにデータを保存しています。*T1* と *T2* の間に、偶発的な脆弱性により、多くの不要なオブジェクトが取り込まれてしまいました。*Exclude* の時間値 *T1* と *T2* 用にブランチバケットを作成し、クライアント操作をそのブランチバケットにリダイレクトすることができます。これにより、*T1* より前と *T2* より後に取り込まれたオブジェクトのみがクライアントに公開されます。

ブランチバケット内のオブジェクトに対する操作

- ブランチ バケットに対する PUT オブジェクト操作により、ブランチ内にオブジェクトが作成されます。
- ブランチ バケットに対する GET オブジェクト操作は、ブランチからオブジェクトを取得します。オブジェクトがブランチ バケットに存在しない場合、オブジェクトはベース バケットから取得されます。
- ブランチ バケットからのオブジェクトの削除は次のように行われます。

操作	ターゲット	結果	ベースバケット内のオブジェクトの可視性	ブランチバケット内のオブジェクトの可視性
バージョンIDなしで削除	ベースバケット	削除マーカーはベースバケットに対してのみ作成されます	HEAD/GETはオブジェクトが存在しないと返しますが、特定のバージョンには引き続きアクセスできます。	HEAD/GETはオブジェクトが存在することを返し、特定のバージョンにはまだアクセスできます。 削除マーカーはブランチバケットの後に作成される `beforeTime`。
バージョンIDで削除	ベースバケット	ベースバケットとブランチバケットの両方で特定のオブジェクトバージョンが削除されます	HEAD/GETはオブジェクトバージョンが存在しないという結果を返します	HEAD/GETはオブジェクトバージョンが存在しないという結果を返します
バージョンIDなしで削除	ブランチバケット	削除マーカーはブランチバケットに対してのみ作成されます	HEAD/GET はオブジェクトを返します (ベースバケット オブジェクトは影響を受けません)	HEAD/GETはオブジェクトが存在しないと返します
バージョンIDで削除	ブランチバケット	特定のオブジェクトバージョンはブランチバケットに対してのみ削除されます	HEAD/GET は特定のオブジェクト バージョンを返します (ベース バケット オブジェクトは影響を受けません)	HEAD/GETはオブジェクトバージョンが存在しないという結果を返します

参照"S3 バージョン管理オブジェクトの削除方法"。

テナント マネージャを使用して、ブランチ バケットの詳細を作成および表示します。

開始する前に

- テナントマネージャーにサインインするには、"サポートされている Web ブラウザ" 。
- ルートアクセス権を持つユーザーグループに属しているか、"Manage All Buckets権限" 。これらの権限は、グループまたはバケット ポリシーの権限設定をオーバーライドします。
- ブランチを作成したいベースバケットには"バージョン管理が有効"。
- あなたはベース バケットの所有者です。

タスクの内容

ブランチ バケットについては次の情報に注意してください。

ブランチバケット深さ制限

ブランチバケットには、最大20個のベースバケットを含めることができます。ブランチバケットの深さが増すと、S3アクセスのレイテンシが増加する可能性があります。特にListObjectVersionsの呼び出しにおいて顕著です。

- 通常のバケット（最初にベースバケットとして作成されたバケット）であるベースバケットからブランチバケットを作成した場合、新しいブランチバケットにはベースバケットが1つあります。
- ベースバケット自体がブランチバケットである場合、新しいブランチバケットはそのブランチバケットのすべてのベースバケットを継承します。ユーザーはベースバケットを1つだけ直接指定すればよく、継承されるベースバケットは暗黙的に指定されます。
- 基本バケットの総数（明示的および暗黙的）は20を超えることはできません。

  例えば、バケット*A*がバージョン管理が有効になっている通常のバケットであると仮定します。

  - ブランチバケット **B** は **A** から作成され、ベースバケットは **A** です。
  - **B** から作成されたブランチバケット **C** には、**B** （明示的）と **A** （暗黙的）の 2 つのベースバケットがあります。
  - **C** から作成されたブランチバケット **D** には、**C** （明示的）、**B** （暗黙的）、**A** （暗黙的） の 3 つのベースバケットがあります。
  - このパターンは、最大深度20ベースバケットまで続きます。

S3オブジェクトロックの権限

バケットまたはオブジェクトの S3 オブジェクト ロック プロパティを設定する権限は、"バケットポリシーまたはグループポリシー"によって付与されます。

一時停止されたバージョン管理

ベース バケットのバージョン管理を一時停止すると、ベース バケットの内容はブランチ バケットに表示されなくなります。

ブランチ バケットを設定して作成した後は、設定を変更することはできません。

ブランチバケットを作成する

手順

1. ダッシュボードで* View Buckets を選択するか、 storage（S3）> Buckets *を選択します。
2. ブランチを作成するバケット (「ベース バケット」) を選択します。
3. バケットの詳細ページで、ブランチ > *ブランチ バケットの作成*を選択します。

   ベース バケットでバージョン管理が有効になっていない場合、ブランチ バケットの作成 ボタンは無効になります。

詳細を入力します

手順

1. ブランチ バケットの詳細を入力します。

フィールド	製品説明
ブランチバケット名	次の規則に準拠するブランチ バケットの名前: • StorageGRID システム全体で（テナントアカウント内だけではなく）一意である必要があります。 • DNS に準拠している必要があります。 • 3文字以上63文字以下にする必要があります。 • 各ラベルの先頭と末尾の文字は小文字のアルファベットか数字にする必要があり、使用できる文字は小文字のアルファベット、数字、ハイフンのみです。 • 仮想ホスト形式の要求にピリオドを含めることはできません。ピリオドを使用すると、サーバワイルドカード証明書の検証で原因 の問題が発生します。 詳細については、を参照して "バケットの命名規則に関する Amazon Web Services （ AWS ）のドキュメント"ください。 注意: ブランチ バケットを作成した後は、名前を変更することはできません。
リージョン（ブランチバケットでは変更できません）	ブランチ バケットのリージョン。 ブランチ バケットのリージョンはベース バケットのリージョンと一致する必要があるため、このフィールドはブランチ バケットでは無効になります。

フィールド	製品説明
ブランチバケットタイプ	• 読み取り/書き込み: ブランチ バケット内のオブジェクトまたはオブジェクト バージョンを追加または削除できます。 • 読み取り専用: ブランチ バケット内のオブジェクトを変更することはできません。 注: ブランチ バケットが空の場合にのみ、ブランチ バケット タイプを読み取り専用に設定できます。既存のブランチ バケットのタイプが読み取り/書き込みに設定されていて、まだ書き込んでいない場合は、タイプを読み取り専用に変更できます。

2. 「 * Continue * 」を選択します。

時間フィルター

ベースバケット内のオブジェクトバージョンを含める期間を選択してください。任意の時間フィルターを使用する場合は、以下の範囲内の日付を選択してください。

- 最小日付：2010年1月1日（UTC）
- 最大日付：本日（UTC）から5年間

実行前
: ブランチバケットを使用すると、*Before* 時刻より前に作成されたオブジェクトバージョンにアクセスできます。

実行後
: ブランチバケットを使用すると、*After* 時間以降に作成されたオブジェクトバージョンにアクセスできます。

間
: ブランチバケットは、*From* と *To* の間に作成されたオブジェクトバージョンへのアクセスを提供します。

除外する
: ブランチバケットでは、*Exclude from* と *Exclude to* の時間の間に作成されたオブジェクトバージョンへのアクセスは提供されません。

オブジェクト設定を管理する（オプション）

ブランチ バケットのオブジェクト設定は、ベース バケット内のオブジェクト バージョンには影響しません。

手順

1. グローバル S3 オブジェクト ロック設定が有効になっている場合は、オプションでブランチ バケットの S3 オブジェクト ロックを有効にします。 S3 オブジェクトロックを有効にするには、ブランチバケットが読み取り/書き込みバケットである必要があります。

   特定の規制要件を満たすためなど、オブジェクトを一定期間保持する必要がある場合にのみ、ブランチバケットの S3 オブジェクトロックを有効にします。 S3 オブジェクト ロックは、一定期間または無期限に

オブジェクトが削除または上書きされるのを防ぐのに役立つ永続的な設定です。

> バケットに対して S3 オブジェクトロック設定を有効にすると、無効にすることはできません。適切な権限を持つユーザーは誰でも、変更できないオブジェクトをブランチ バケットに追加できます。これらのオブジェクトまたはブランチ バケット自体を削除できない可能性があります。

2. **S3** オブジェクトロックを有効にする を選択した場合は、オプションでブランチバケットの デフォルトの保持期間 を有効にします。

> グリッド管理者は、に対する権限をユーザに付与する必要があります"S3オブジェクトロックの特定の機能を使用する"。

デフォルトの保持 が有効になっている場合、ブランチ バケットに追加された新しいオブジェクトは、削除または上書きされないように自動的に保護されます。 *デフォルトの保持期間*設定は、独自の保持期間を持つオブジェクトには適用されません。

a. デフォルトの保持*が有効になっている場合は、ブランチ バケットの *デフォルトの保持モード を指定します。

デフォルトの保持モード	製品説明
ガバナンス	• 権限を持つユーザ `s3:BypassGovernanceRetention`は、要求ヘッダーを使用して保持設定を省略でき `x-amz-bypass-governance-retention: true`ます。 • これらのユーザは、retain-until-dateに達する前にオブジェクトバージョンを削除できます。 • これらのユーザは、オブジェクトのretain-until-dateを増減、または削除できます。
コンプライアンス	• retain-until-dateに達するまで、オブジェクトを削除できません。 • オブジェクトのretain-until-dateは増やすことはできますが、減らすことはできません。 • オブジェクトのretain-until-dateは、その日付に達するまで削除できません。 注：グリッド管理者が準拠モードの使用を許可する必要があります。

b. デフォルトの保持*が有効になっている場合は、ブランチ バケットの *デフォルトの保持期間 を指定します。

デフォルトの保持期間 は、ブランチ バケットに追加された新しいオブジェクトが取り込まれた時点から保持される期間を示します。グリッド管理者によって設定されたテナントの最大保持期間以下の値を指定します。

A_maximum_retention periodは、グリッド管理者がテナントを作成するときに設定されます。指定できる値は1~100年です。_default_retention periodを設定する場合、最大保持期間に設定された値を超えること

はできません。必要に応じて、最大保持期間を増減するようにグリッド管理者に依頼します。

3. 必要に応じて、「容量制限を有効にする」を選択します。

   容量制限は、ブランチ バケットに使用できる最大容量です。この値は物理的な量 (ディスク上のサイズ) ではなく、論理的な量 (オブジェクトのサイズ) を表します。

   制限が設定されていない場合、ブランチ バケットの容量は無制限になります。参照"ヨウリヨウセイケンシヨウ"詳細についてはこちらをご覧ください。

   > この設定は、ブランチ バケットに直接取り込まれたオブジェクトにのみ適用され、ブランチ バケットを介してベース バケットから表示されるオブジェクトには適用されません。

4. 必要に応じて、「オブジェクト数の制限を有効にする」を選択します。

   オブジェクト数の制限は、ブランチ バケットに含めることができるオブジェクトの最大数です。この値は論理量 (オブジェクト数) を表します。制限が設定されていない場合、オブジェクト数は無制限になります。

   > この設定は、ブランチ バケットに直接取り込まれたオブジェクトにのみ適用され、ブランチ バケットを介してベース バケットから表示されるオブジェクトには適用されません。

5. [* バケットの作成 *] を選択します。

   ブランチ バケットが作成され、[バケット] ページのテーブルに追加されます。

6. オプションで*バケットの詳細ページに移動*を選択して"ブランチバケットの詳細を表示する"追加の構成を実行します。

   バケットの詳細ページでは、読み取り専用バケットの場合、オブジェクトの変更に関連する一部の構成オプションが無効になっています。

StorageGRID バケットに **ILM** ポリシータグを適用する

オブジェクトストレージ要件に基づいて、バケットに適用するILMポリシータグを選択します。

ILMポリシーは、オブジェクトデータの格納場所と一定期間後に削除するかどうかを制御します。グリッド管理者は、複数のアクティブポリシーを使用している場合に、ILMポリシーを作成してILMポリシータグに割り当てます。

> バケットのポリシータグは頻繁に再割り当てしないでください。そうしないと、パフォーマンスの問題が発生する可能性があり

開始する前に

- を使用してTenant Managerにサインインしておき"サポートされている Web ブラウザ"ます。
- が設定されたユーザグループに属している"rootアクセス、Manage All Buckets、View All Buckets権限"必要があります。これらの権限は、グループポリシーまたはバケットポリシーの権限設定よりも優先されます。

手順

1. ダッシュボードで* View Buckets を選択するか、 storage（S3）> Buckets *を選択します。

   [Buckets]ページが表示されます。必要に応じて、任意の列で情報をソートしたり、リストを前後にページ移動したりできます。

2. ILMポリシータグを割り当てるバケットの名前を選択します。

   すでにタグが割り当てられているバケットに対するILMポリシータグの割り当てを変更することもできます。

   「オブジェクト数」と「使用済みスペース」の値が概算値として表示されます。これらの推定値は、取り込みのタイミング、ネットワーク接続、ノードのステータスによって左右されます。バケットでバージョン管理が有効になっている場合は、削除したオブジェクトのバージョンがオブジェクト数に含まれます。

3. [Bucket options]タブで、ILMポリシータグのアコーディオンを展開します。このアコーディオンは、グリッド管理者がカスタムポリシータグの使用を有効にしている場合にのみ表示されます。
4. 各ポリシータグの概要を読んで、バケットに適用するタグを特定します。

   バケットのILMポリシータグを変更すると、バケット内のすべてのオブジェクトのILMによる再評価がトリガーされます。新しいポリシーで一定期間オブジェクトが保持されると、古いオブジェクトは削除されます。

5. バケットに割り当てるタグのラジオボタンを選択します。
6. 「変更を保存」を選択します。ILMポリシーのタグ名のキーと値を使用して、バケットに新しいS3バケットタグが設定され `NTAP-SG-ILM-BUCKET-TAG`ます。

   S3アプリケーションが誤って新しいバケットタグを上書きまたは削除しないようにしてください。バケットに新しいTagSetを適用するときにこのタグを省略すると、バケット内のオブジェクトはデフォルトのILMポリシーに照らして評価されます。

   ILMポリシータグの設定と変更には、ILMポリシータグが検証されるTenant Manager APIまたはTenant Manager APIのみを使用します。S3 PutBucketTagging APIやS3 DeleteBucketTagging APIを使用してILMポリシータグを変更しないで `NTAP-SG-ILM-BUCKET-TAG`ください。

   バケットに割り当てられているポリシータグを変更すると、新しいILMポリシーを使用してオブジェクトが再評価される間、一時的にパフォーマンスに影響します。

StorageGRIDバケットポリシーを管理

S3バケットとそのバケット内のオブジェクトに対するユーザアクセスを制御できます。

開始する前に

- を使用してTenant Managerにサインインしておき"サポートされている Web ブラウザ"ます。
- が設定されたユーザグループに属している"rootアクセス権限"必要があります。View All Buckets権限

とManage All Buckets権限では、表示のみが許可されます。

- 必要な数のストレージノードとサイトが使用可能であることを確認しておきます。どのサイトでも複数のストレージノードを使用できない場合やサイトを使用できない場合は、それらの設定を変更できない可能性があります。

手順

1. [Buckets]*を選択し、管理するバケットを選択します。
2. バケットの詳細ページで、* Bucket access > Bucket policy *を選択します。
3. 次のいずれかを実行します。
   - [ポリシーを有効にする]*チェックボックスを選択して、バケットポリシーを入力します。次に、有効なJSON形式の文字列を入力します。

     各バケットポリシーのサイズ制限は20、480バイトです。
   - 文字列を編集して既存のポリシーを変更します。
   - [ポリシーを有効にする]*の選択を解除してポリシーを無効にします。

言語の構文や例など、バケットポリシーの詳細については、を参照してください"バケットポリシーの例"。

StorageGRIDバケットの整合性を管理

整合性の値を使用して、バケット設定を変更できるかどうかを指定したり、バケット内のオブジェクトの可用性と異なるストレージノードやサイト間でのオブジェクトの整合性のバランスを調整したりできます。クライアントアプリケーションの運用上のニーズを満たすために、整合性の値をデフォルト値とは異なる値に変更することができます。

開始する前に

- を使用してTenant Managerにサインインしておき"サポートされている Web ブラウザ"ます。
- が設定されたユーザグループに属している"すべてのバケットまたはRoot Access権限を管理します"必要があります。これらの権限は、グループまたはバケットポリシーの権限の設定よりも優先されます。

バケットの整合性に関するガイドライン

バケットの整合性は、そのS3バケット内のオブジェクトに影響しているクライアントアプリケーションの整合性を判断するために使用されます。一般に、バケットには* Read-after-new-write *整合性を使用する必要があります。

バケット整合性の変更

Read-after-new-write *整合性がクライアントアプリケーションの要件を満たしていない場合は、バケットの整合性を設定するかヘッダーを使用して整合性を変更できます `Consistency-Control`。 `Consistency-Control`ヘッダーはバケットの整合性よりも優先されます。

> バケットの整合性を変更した場合、変更後に取り込まれたオブジェクトのみが変更後の設定を満たすことが保証されます。

手順

1. ダッシュボードで* View Buckets を選択するか、 storage（S3）> Buckets *を選択します。
2. 表からバケット名を選択します。

   バケットの詳細ページが表示されます。

3. [Bucket options]タブで、[**]アコーディオンを選択します。
4. このバケット内のオブジェクトに対して実行される処理の整合性を選択します。
   - **all**:最高レベルの一貫性を提供します。すべてのノードが即座にデータを受け取り、受け取れない場合は要求が失敗します。
   - * strong-global *：すべてのサイトのすべてのクライアント要求について、リードアフターライト整合性が保証されます。
   - *strong-site *：サイト内のすべてのクライアント要求に対してリードアフターライト整合性が保証されます。
   - * Read-after-new-write *（デフォルト）：新規オブジェクトにはリードアフターライト整合性を提供し、オブジェクトの更新には結果整合性を提供します。高可用性が確保され、データ保護が保証されます。ほとんどの場合に推奨されます。
   - * available *：新しいオブジェクトとオブジェクトの更新の両方について、結果整合性を提供します。S3バケットの場合は、必要な場合にのみ使用します（読み取り頻度の低いログ値を含むバケットや、存在しないキーに対するHEAD処理やGET処理など）。S3 FabricPool バケットではサポートされません。
5. 「変更を保存」を選択します。

バケット設定を変更した場合の動作

バケットには、バケットとバケット内のオブジェクトの動作に影響する複数の設定があります。

次のバケット設定では、デフォルトで* Strong * consistencyが使用されます。どのサイトでも複数のストレージノードを使用できない場合やサイトを使用できない場合は、それらの設定を変更できない可能性があります。

- "バックグラウンドでの空のバケット削除"
- "最終アクセス時間"
- "バケットライフサイクル"
- "バケットポリシー"
- "バケットのタグ付け"
- "バケットのバージョン管理"
- "S3 オブジェクトのロック"
- "バケット暗号化"

> バケットのバージョン管理、S3オブジェクトロック、およびバケット暗号化の整合性の値を強くない値に設定することはできません。

次のバケット設定では整合性が強くなく、変更の可用性も高くなります。これらの設定の変更が反映されるまでに時間がかかることがあります。

- "プラットフォームサービスの設定：通知、レプリケーション、検索の統合"
- "バケットとオブジェクトのStorageGRID CORSを構成する"
- バケットの整合性を変更

> バケット設定の変更時に使用したデフォルトの整合性がクライアントアプリケーションの要件を満たしていない場合は、のヘッダーを"S3 REST API"使用するか、のオプションまたは `force`オプションを使用し `reducedConsistency`て整合性を変更できます `Consistency-Control`"テナント管理 API"。

StorageGRIDで最終アクセス時刻の更新を有効または無効にする

グリッド管理者が StorageGRID システムの情報ライフサイクル管理（ ILM ）ルールを作成する際に、オブジェクトを別の格納場所に移動するかどうかを決定する際にオブジェクトの最終アクセス日時を使用するように指定できます。S3 テナントを使用している場合は、 S3 バケット内のオブジェクトに対して最終アクセス日時の更新を有効にすることで、このようなルールを活用できます。

以下の手順は、[最終アクセス時間]*オプションを高度なフィルタまたは参照時間として使用するILMルールを少なくとも1つ含むStorageGRID システムにのみ該当します。StorageGRID システムにこのようなルールが含まれていない場合は、この手順を無視してかまいません。詳細は、を参照してください "ILMルールで最終アクセス時間を使用" 。

開始する前に

- を使用してTenant Managerにサインインしておき"サポートされている Web ブラウザ"ます。
- が設定されたユーザグループに属している"すべてのバケットまたはRoot Access権限を管理します"必要があります。これらの権限は、グループまたはバケットポリシーの権限の設定よりも優先されます。

タスクの内容

最終アクセス時間*は、**ILM**ルールの Reference time *配置手順で使用できるオプションの1つです。ルールの[Reference time]を[Last access time]に設定すると、オブジェクトが最後に読み出された（読み取りまたは表示された）日時に基づいてオブジェクトを特定の格納場所に配置するようにグリッド管理者が指定できます。

たとえば、最近表示したオブジェクトを高速ストレージに保持するには、次のように指定した ILM ルールを作成できます。

- 過去 1 カ月間に読み出されたオブジェクトは、ローカルストレージノードに保持する。
- 過去 1 カ月間に読み出されなかったオブジェクトは、オフサイトの場所に移動する。

デフォルトでは、最終アクセス時間の更新は無効です。StorageGRID システムに*最終アクセス時間*オプションを使用するILMルールが含まれている場合に、このバケット内のオブジェクトにこのオプションを適用するには、そのルールで指定されたS3バケットに対して最終アクセス時間の更新を有効にする必要があります。

> オブジェクトが読み出されるときに最終アクセス日時を更新すると、特に小さなオブジェクトについては StorageGRID のパフォーマンスが低下する可能性があります。

最終アクセス時間の更新では、オブジェクトが読み出されるたびに StorageGRID で以下の追加手順が実行されるため、パフォーマンスが低下します。

- 新しいタイムスタンプでオブジェクトを更新します
- 現在の ILM ルールとポリシーに照らしてオブジェクトが再評価されるように、 ILM キューにオブジェクトを追加します

次の表に、最終アクセス時間が有効または無効な場合のバケット内のすべてのオブジェクトに適用される動作をまとめます。

要求のタイプ	最終アクセス時間が無効な場合の動作（デフォルト）		最終アクセス時間が有効な場合の動作	
	最終アクセス時間の更新	ILM 評価キューへのオブジェクトの追加	最終アクセス時間の更新	ILM 評価キューへのオブジェクトの追加
HEAD操作が発行されたときにオブジェクトのメタデータを取得する要求	いいえ	いいえ	いいえ	いいえ
オブジェクト、そのアクセス制御リスト、またはメタデータの読み出し要求	いいえ	いいえ	はい	はい
オブジェクトメタデータの更新要求	はい	はい	はい	はい
オブジェクトまたはオブジェクトバージョンのリスト要求	いいえ	いいえ	いいえ	いいえ
バケット間でのオブジェクトのコピー要求	• ソースコピーに対しては、「いいえ」と指定します • デスティネーションコピーについては、はい	• ソースコピーに対しては、「いいえ」と指定します • デスティネーションコピーについては、はい	• ソースコピーについては、はい • デスティネーションコピーについては、はい	• ソースコピーについては、はい • デスティネーションコピーについては、はい
マルチパートアップロードの完了要求	はい、アセンブルされたオブジェクトの場合	はい、アセンブルされたオブジェクトの場合	はい、アセンブルされたオブジェクトの場合	はい、アセンブルされたオブジェクトの場合

手順

1. ダッシュボードで* View Buckets を選択するか、 storage（S3）> Buckets *を選択します。
2. 表からバケット名を選択します。

   バケットの詳細ページが表示されます。

3. [Bucket options]タブで、[Last access time updates]*アコーディオンを選択します。
4. 最終アクセス時間の更新を有効または無効にします。
5. 「変更を保存」を選択します。

StorageGRID の **S3** バケットのオブジェクトバージョニングを変更する

S3テナントを使用している場合は、S3バケットのバージョン管理状態を変更できます。

開始する前に

- を使用してTenant Managerにサインインしておき"サポートされている Web ブラウザ"ます。
- が設定されたユーザグループに属している"すべてのバケットまたはRoot Access権限を管理します"必要があります。これらの権限は、グループまたはバケットポリシーの権限の設定よりも優先されます。
- 必要な数のストレージノードとサイトが使用可能であることを確認しておきます。どのサイトでも複数のストレージノードを使用できない場合やサイトを使用できない場合は、それらの設定を変更できない可能性があります。

タスクの内容

バケットでオブジェクトのバージョン管理を有効または一時停止することができます。バケットのバージョン管理を有効にすると、バージョン管理されていない状態に戻ることはできません。ただし、バケットのバージョン管理は一時停止できます。

- 無効 : バージョン管理は一度も有効になっていません
- 有効：バージョン管理が有効になっています
- 中断：バージョン管理は以前有効になっていて、中断されています

詳細については、次を参照してください。

- "オブジェクトのバージョン管理"
- "S3 バージョン管理オブジェクトの ILM ルールとポリシー（例 4 ）"
- "オブジェクトの削除方法"

手順

1. ダッシュボードで* View Buckets を選択するか、 storage（S3）> Buckets *を選択します。
2. 表からバケット名を選択します。

   バケットの詳細ページが表示されます。
3. タブで、[Object versioning]*アコーディオンを選択します。
4. このバケット内のオブジェクトのバージョン管理の状態を選択します。

   グリッド間レプリケーションに使用されるバケットでは、オブジェクトのバージョン管理を有効にしておく必要があります。S3 オブジェクトのロックまたはレガシーのコンプライアンスが有効になっている場合、 * オブジェクトのバージョン管理 * オプションは無効になります。

オプション	製品説明
バージョン管理を有効にする	このバケット内の各オブジェクトのすべてのバージョンを格納する場合は、オブジェクトのバージョン管理を有効にします。そのあと、必要に応じて以前のバージョンのオブジェクトを読み出すことができます。 バケットにすでに含まれていたオブジェクトは、ユーザによる変更時にバージョン管理されます。
バージョン管理を一時停止	新しいオブジェクトバージョンを作成しない場合は、オブジェクトのバージョン管理を一時停止します。既存のオブジェクトバージョンは引き続き取得できます。

5. 「変更を保存」を選択します。

S3オブジェクトロックを使用して**StorageGRID**でオブジェクトを保持します

バケットとオブジェクトが保持に関する規制要件に準拠する必要がある場合は、S3オブジェクトロックを使用できます。

グリッド管理者に、S3 Object Lockの特定の機能を使用する権限を付与する必要があります。

S3 オブジェクトのロックとは何ですか？

StorageGRID S3 オブジェクトロック機能は、 Amazon Simple Storage Service （ Amazon S3 ）での S3 オブジェクトロックに相当するオブジェクト保護解決策 です。

グローバル S3 オブジェクトロック設定が StorageGRID システムで有効になっている場合、S3 テナントアカウントは、S3 オブジェクトロックが有効または無効のいずれかでバケットを作成できます。既存バケットに対する S3 オブジェクトロックを許可する設定が有効になっている場合、S3 テナントアカウントは既存バケットに対して S3 オブジェクトロックを有効にできます。バケットで S3 オブジェクトロックが有効になっている場合、バケットのバージョン管理が必要となり、自動的に有効になります。S3 テナントアカウントが新規または既存のバケットに対して S3 オブジェクトロックを有効にすると、無効にすることはできません。

- S3オブジェクトロック*が設定されていないバケットには、保持設定が指定されていないオブジェクトのみを含めることができます。保持設定は取り込まれたオブジェクトには適用されません。
- S3 Object Lock *が設定されたバケットには、S3クライアントアプリケーションで保持設定の有無に関係なくオブジェクトを含めることができます。取り込まれた一部のオブジェクトには保持設定が設定されます。
- S3オブジェクトロックでデフォルトの保持が設定されたバケット*では、保持設定を指定したオブジェクトをアップロードし、保持設定を指定せずに新しいオブジェクトをアップロードできます。保持設定がオブジェクトレベルで設定されていないため、新しいオブジェクトではデフォルト設定が使用されます。

デフォルトの保持が設定されている場合、新しく取り込まれたすべてのオブジェクトに保持設定が適用されます。オブジェクト保持設定のない既存のオブジェクトは影響を受けません。

保持モード

StorageGRID S3オブジェクトロック機能は、2つの保持モードをサポートしており、さまざまなレベルの保護をオブジェクトに適用できます。これらのモードは、Amazon S3の保持モードに相当します。

- コンプライアンスモードの場合：
  - retain-until-dateに達するまで、オブジェクトを削除できません。
  - オブジェクトのretain-until-dateは増やすことはできますが、減らすことはできません。
  - オブジェクトのretain-until-dateは、その日付に達するまで削除できません。
- ガバナンスモードの場合：
  - 特別な権限を持つユーザは、要求でバイパスヘッダーを使用して、特定の保持設定を変更できます。
  - これらのユーザは、retain-until-dateに達する前にオブジェクトバージョンを削除できます。
  - これらのユーザは、オブジェクトのretain-until-dateを増減、または削除できます。

オブジェクトバージョンの保持設定

S3オブジェクトロックを有効にしてバケットを作成した場合、ユーザはS3クライアントアプリケーションを使用して、バケットに追加される各オブジェクトに次の保持設定を必要に応じて指定できます。

- 保持モード：コンプライアンスまたはガバナンスのいずれか。
- * Retain-until-date *：オブジェクトバージョンのretain-until-dateが将来の日付の場合、オブジェクトは読み出すことはできますが、削除することはできません。
- * リーガルホールド * ：オブジェクトバージョンにリーガルホールドを適用すると、そのオブジェクトがただちにロックされます。たとえば、調査または法的紛争に関連するオブジェクトにリーガルホールドを設定する必要がある場合があります。リーガルホールドには有効期限はありませんが、明示的に削除されるまで保持されます。リーガルホールドは、それまでの保持期間とは関係ありません。

> ⓘ オブジェクトがリーガルホールドの対象である場合、保持モードに関係なく、誰もオブジェクトを削除できません。

オブジェクト設定の詳細については、"S3 REST APIを使用してS3オブジェクトロックを設定します"を参照してください。

バケットのデフォルトの保持設定

S3オブジェクトロックを有効にしてバケットを作成した場合は、必要に応じて次のバケットのデフォルト設定を指定できます。

- デフォルトの保持モード：コンプライアンスまたはガバナンスのいずれか。
- デフォルトの保持期間：このバケットに追加された新しいオブジェクトバージョンを、追加された日から保持する期間。

デフォルトのバケット設定は、独自の保持設定がない新しいオブジェクトにのみ適用されます。これらのデフォルト設定を追加または変更しても、既存のバケットオブジェクトには影響しません。

"S3 バケットを作成します。"および"S3オブジェクトロックのデフォルトの保持期間を更新します"を参照してください。

S3オブジェクトロックタスク

グリッド管理者とテナントユーザを対象に、S3オブジェクトロック機能を使用するためのタスクの概要を次

に示します。

グリッド管理者

- StorageGRIDシステム全体に対してS3オブジェクトロックのグローバル設定を有効にします。
- ユーザーが既存のバケットに対して S3 オブジェクトロックを有効にできるようにします。
- 情報ライフサイクル管理（ILM）ポリシーが_compliant_（に準拠）であることを確認します"S3オブジェクトロックが有効なバケットの要件"。
- 必要に応じて、テナントでComplianceを保持モードとして使用できるようにします。それ以外の場合は、ガバナンスモードのみが許可されます。
- 必要に応じて、テナントの最大保持期間を設定します。

テナントユーザ

- S3オブジェクトロックを使用するバケットとオブジェクトに関する考慮事項を確認してください。
- 必要に応じて、グリッド管理者に連絡して、以下のいずれかの設定を有効にしてください。
  - グローバルS3オブジェクトロック
  - 既存のバケットに対してS3オブジェクトロックを有効にすることを許可する
- S3オブジェクトロックを有効にしてバケットを作成する。
- 既存のバケットでS3オブジェクトロックを有効にします。
- 必要に応じて、バケットのデフォルトの保持設定を指定します。
  - デフォルトの保持モード：GovernanceまたはCompliance（グリッド管理者が許可している場合）。
  - Default retention period：グリッド管理者が設定した最大保持期間以下にする必要があります。
- S3クライアントアプリケーションを使用して、オブジェクトを追加し、必要に応じてオブジェクト固有の保持期間を設定します。
  - 保持モード。ガバナンスまたはコンプライアンス（グリッド管理者によって許可されている場合）。
  - Retain Until Date：グリッド管理者が設定した最大保持期間以下にする必要があります。

S3 オブジェクトのロックを有効にした場合のバケットの要件

- StorageGRID システムでグローバルな S3 オブジェクトロック設定が有効になっている場合は、テナントマネージャ、テナント管理 API 、または S3 REST API を使用して、 S3 オブジェクトロックを有効にしたバケットを作成できます。
- バケットで S3 オブジェクトのロックが有効になっている場合は、そのバケットのバージョン管理が StorageGRID で自動的に有効になります。バケットのS3オブジェクトロックを無効にしたり、バージョン管理を一時停止したりすることはできません。
- 必要に応じて、Tenant Manager、テナント管理API、またはS3 REST APIを使用して、各バケットのデフォルトの保持モードと保持期間を指定できます。バケットのデフォルトの保持設定は、バケットに追加された新しいオブジェクトのうち、独自の保持設定がないオブジェクトにのみ適用されます。これらのデフォルト設定は、アップロード時にオブジェクトバージョンごとに保持モードとretain-until-dateを指定することで上書きできます。
- バケットライフサイクル設定は、S3オブジェクトロックが有効なバケットでサポートされます。

S3 オブジェクトのロックが有効になっているバケット内のオブジェクトの要件

- オブジェクトバージョンを保護するには、バケットのデフォルトの保持設定を指定するか、オブジェクトバージョンごとに保持設定を指定します。オブジェクトレベルの保持設定は、S3クライアントアプリケーションまたはS3 REST APIを使用して指定できます。
- 保持設定はオブジェクトのバージョンごとに適用されます。オブジェクトバージョンには、 retain-until date 設定とリーガルホールド設定の両方を設定できます。ただし、オブジェクトバージョンを保持することはできません。また、どちらも保持することはできません。オブジェクトの retain-une-date 設定またはリーガルホールド設定を指定すると、要求で指定されたバージョンのみが保護されます。オブジェクトの以前のバージョンはロックされたまま、オブジェクトの新しいバージョンを作成できます。

S3 オブジェクトのロックが有効なバケット内のオブジェクトのライフサイクル

S3オブジェクトロックが有効なバケットに保存された各オブジェクトは、次の段階を経ます。

1. * オブジェクトの取り込み *

   S3オブジェクトロックが有効になっているバケットにオブジェクトバージョンを追加すると、保持設定は次のように適用されます。

   - オブジェクトに保持設定が指定されている場合は、オブジェクトレベルの設定が適用されます。デフォルトのバケット設定は無視されます。
   - オブジェクトに保持設定が指定されていない場合は、デフォルトのバケット設定が適用されます（存在する場合）。
   - オブジェクトまたはバケットに保持設定が指定されていない場合、オブジェクトはS3オブジェクトロックによって保護されません。

   保持設定が適用されている場合は、オブジェクトとS3ユーザ定義メタデータの両方が保護されます。

2. オブジェクトの保持と削除

   指定した保持期間中、各保護オブジェクトの複数のコピーがStorageGRID によって格納されます。オブジェクトコピーの正確な数、タイプ、格納場所は、アクティブなILMポリシーの準拠ルールによって決まります。retain-until-dateに達する前に保護オブジェクトを削除できるかどうかは、保持モードによって異なります。

   - オブジェクトがリーガルホールドの対象である場合、保持モードに関係なく、誰もオブジェクトを削除できません。

従来の準拠バケットは引き続き管理できますか。

S3 オブジェクトロック機能は、以前のバージョンの StorageGRID で使用されていた準拠機能に代わる機能です。以前のバージョンの StorageGRID を使用して準拠バケットを作成した場合は、引き続きこれらのバケットの設定を管理できますが、新しい準拠バケットは作成できなくなります。手順については、を参照してくださいhttps://kb.netapp.com/Advice_and_Troubleshooting/Hybrid_Cloud_Infrastructure/StorageGRID/How_to_manage_legacy_Compliant_buckets_in_StorageGRID_11.5["ネットアップのナレッジベース： StorageGRID 11.5 でレガシー準拠バケットを管理する方法"^]。

関連情報

"S3 Object Lock の要件"について学ぶ

StorageGRIDでS3オブジェクトロックのデフォルトの保持期間を更新

バケットの作成時にS3 Object Lockを有効にした場合は、バケットを編集してデフォルトの保持設定を変更できます。デフォルトの保持を有効（または無効）にしたり、デフォルトの保持モードと保持期間を設定したりできます。

開始する前に

- を使用してTenant Managerにサインインしておき"サポートされている Web ブラウザ"ます。
- が設定されたユーザグループに属している"すべてのバケットまたはRoot Access権限を管理します"必要があります。これらの権限は、グループまたはバケットポリシーの権限の設定よりも優先されます。
- S3オブジェクトロックはStorageGRID システムに対してグローバルに有効になり、バケットの作成時に有効にしました。を参照して "S3オブジェクトロックを使用してオブジェクトを保持します"

手順

1. ダッシュボードで* View Buckets を選択するか、 storage（S3）> Buckets *を選択します。
2. 表からバケット名を選択します。

   バケットの詳細ページが表示されます。
3. [Bucket options]タブで、[S3 Object Lock]*アコーディオンを選択します。
4. 必要に応じて、このバケットの*デフォルトの保持*を有効または無効にします。

   この設定の変更は、バケットにすでに含まれているオブジェクトや、保持期間が独自に設定されている可能性のあるオブジェクトには適用されません。
5. default retention が有効になっている場合は、バケットの default retention mode *を指定します。

デフォルトの保持モード	製品説明
ガバナンス	• 権限を持つユーザ `s3:BypassGovernanceRetention`は、要求ヘッダーを使用して保持設定を省略でき `x-amz-bypass-governance-retention: true`ます。 • これらのユーザは、retain-until-dateに達する前にオブジェクトバージョンを削除できます。 • これらのユーザは、オブジェクトのretain-until-dateを増減、または削除できます。
コンプライアンス	• retain-until-dateに達するまで、オブジェクトを削除できません。 • オブジェクトのretain-until-dateは増やすことはできますが、減らすことはできません。 • オブジェクトのretain-until-dateは、その日付に達するまで削除できません。 注：グリッド管理者が準拠モードの使用を許可する必要があります。

6. default retention が有効になっている場合は、バケットの default retention period *を指定します。

Default retention period *は、このバケットに追加された新しいオブジェクトを取り込んだ時点から保持する期間です。グリッド管理者が設定したテナントの最大保持期間以下の値を指定します。

A_maximum_retention periodは、グリッド管理者がテナントを作成するときに設定されます。指定できる値は1~100年です。_default_retention periodを設定する場合、最大保持期間に設定された値を超えることはできません。必要に応じて、最大保持期間を増減するようにグリッド管理者に依頼します。

7. 「変更を保存」を選択します。

StorageGRIDで**S3**バケットの**CORS**を設定する

S3バケットとバケット内のオブジェクトに他のドメインにあるWebアプリケーションからアクセスできるようにするには、そのバケットにCross-Origin Resource Sharing（CORS）を設定します。

開始する前に

- を使用してTenant Managerにサインインしておき"サポートされている Web ブラウザ"ます。
- GET CORS設定要求の場合は、を持つユーザグループに属してい"Manage All BucketsまたはView All Buckets権限"ます。これらの権限は、グループまたはバケットポリシーの権限の設定よりも優先されます。
- PUT CORS設定要求の場合、ユーザはを持つユーザグループに属してい"Manage All Buckets権限"ます。この権限は、グループポリシーまたはバケットポリシーの権限設定よりも優先されます。
- では"rootアクセス権限"、すべてのCORS設定要求にアクセスできます。

タスクの内容

Cross-Origin Resource Sharing （ CORS ）は、あるドメインのクライアント Web アプリケーションが別のドメインのリソースにアクセスできるようにするセキュリティ機能です。たとえば、という名前のS3バケットを使用してグラフィックを格納するとし `Images`ます。バケットの`CORS`を設定すると `Images`、そのバケット内のイメージをWebサイトに表示できるように `http://www.example.com`なります。

バケットの**CORS**を有効にします

手順

1. テキストエディタを使用して、必要なXMLを作成します。次の例は、 S3 バケットの CORS を有効にするために使用される XML を示しています。具体的には：
   - すべてのドメインがバケットにGET要求を送信できるようにする
   - ドメインがGET、POST、およびDELETE要求の送信のみを許可する `http://www.example.com`
   - すべての要求ヘッダーを許可

```
<CORSConfiguration
    xmlns="http://s3.amazonaws.com/doc/2020-10-22/">
    <CORSRule>
        <AllowedOrigin>*</AllowedOrigin>
        <AllowedMethod>GET</AllowedMethod>
        <AllowedHeader>*</AllowedHeader>
    </CORSRule>
    <CORSRule>
        <AllowedOrigin>http://www.example.com</AllowedOrigin>
        <AllowedMethod>GET</AllowedMethod>
        <AllowedMethod>POST</AllowedMethod>
        <AllowedMethod>DELETE</AllowedMethod>
        <AllowedHeader>*</AllowedHeader>
    </CORSRule>
</CORSConfiguration>
```

CORS設定XMLの詳細については、を参照してください "Amazon Web Services（AWS）ドキュメント：「Amazon Simple Storage Service User Guide」"。

2. ダッシュボードで* View Buckets を選択するか、 storage（S3）> Buckets *を選択します。
3. 表からバケット名を選択します。

   バケットの詳細ページが表示されます。

4. [Bucket access]タブで、[Cross-Origin Resource Sharing（CORS）]*アコーディオンを選択します。
5. [Enable CORS]チェックボックスをオンにします。
6. CORS設定XMLをテキストボックスに貼り付けます。
7. 「変更を保存」を選択します。

CORS設定を変更します

手順

1. テキストボックスのCORS設定XMLを更新するか、* Clear *を選択してやり直します。
2. 「変更を保存」を選択します。

CORS設定を無効にします

手順

1. [Enable CORS]チェックボックスをオフにします。
2. 「変更を保存」を選択します。

関連情報

"管理インターフェース用にStorageGRID CORSを構成する"

StorageGRID S3バケットからオブジェクトを削除する

Tenant Managerを使用して、1つ以上のバケット内のオブジェクトを削除できます。

考慮事項と要件

これらの手順を実行する前に、次の点に注意してください。

- バケット内のオブジェクトを削除すると、StorageGRID はStorageGRID システム内のすべてのノードとサイトから、選択した各バケット内のすべてのオブジェクトとすべてのオブジェクトバージョンを完全に削除します。StorageGRID は、関連するオブジェクトメタデータも削除します。この情報を回復することはできません。
- オブジェクト、オブジェクトコピー、および同時処理の数によっては、バケット内のすべてのオブジェクトの削除に数分、数日、場合によっては数週間かかることがあります。
- バケットにが含まれている場合は"S3オブジェクトロックが有効になりました"、_years_の場合、バケットは* Deleting objects：read-only *の状態のままになることがあります。

> S3オブジェクトロックを使用するバケットは、すべてのオブジェクトの保持期限に達してリーガルホールドが解除されるまで、* Deleting objects：read-only *状態のままです。

- オブジェクトの削除中、バケットの状態は* Deleting objects：read-only *です。この状態の場合、バケットに新しいオブジェクトを追加することはできません。
- すべてのオブジェクトが削除されると、バケットは読み取り専用状態のままになります。次のいずれかを実行できます。
  - バケットを書き込みモードに戻し、新しいオブジェクトに再利用します
  - バケットを削除します
  - バケット名はあとで使用できるように、読み取り専用モードのままにしておきます
- バケットでオブジェクトのバージョン管理が有効になっている場合は、StorageGRID 11.8以降で作成された削除マーカーを削除するには、[Delete objects in bucket]処理を使用します。
- バケットでオブジェクトのバージョン管理が有効になっている場合、StorageGRID 11.7以前で作成された削除マーカーは削除されません。のバケット内のオブジェクトの削除に関する情報を参照してください"S3 バージョン管理オブジェクトの削除方法"。
- を使用する場合は"グリッド間レプリケーション"、次の点に注意してください。
  - このオプションを使用しても、他のグリッドのバケットからオブジェクトは削除されません。
  - ソースバケットに対してこのオプションを選択すると、もう一方のグリッドのデスティネーションバケットにオブジェクトを追加すると* Cross-grid replication failure *アラートがトリガーされます。保証できない場合は、すべてのバケットオブジェクトが削除される前に、他のグリッドのバケットにオブジェクトが追加されないように"グリッド間レプリケーションを無効にします"してください。

開始する前に

- を使用してTenant Managerにサインインしておき"サポートされている Web ブラウザ"ます。
- が設定されたユーザグループに属している"rootアクセス権限"必要があります。この権限は、グループポリシーまたはバケットポリシーの権限設定よりも優先されます。

手順

1. ダッシュボードで* View Buckets を選択するか、 storage（S3）> Buckets *を選択します。

バケットページが表示され、既存の S3 バケットがすべて表示されます。

2. 特定のバケットの*[Actions]*メニューまたは詳細ページを使用します。

[Actions]メニュー

a. オブジェクトを削除する各バケットのチェックボックスを選択します。

b. **>**[Delete objects in bucket]*を選択します。

詳細ページ

a. 詳細を表示するバケット名を選択します。

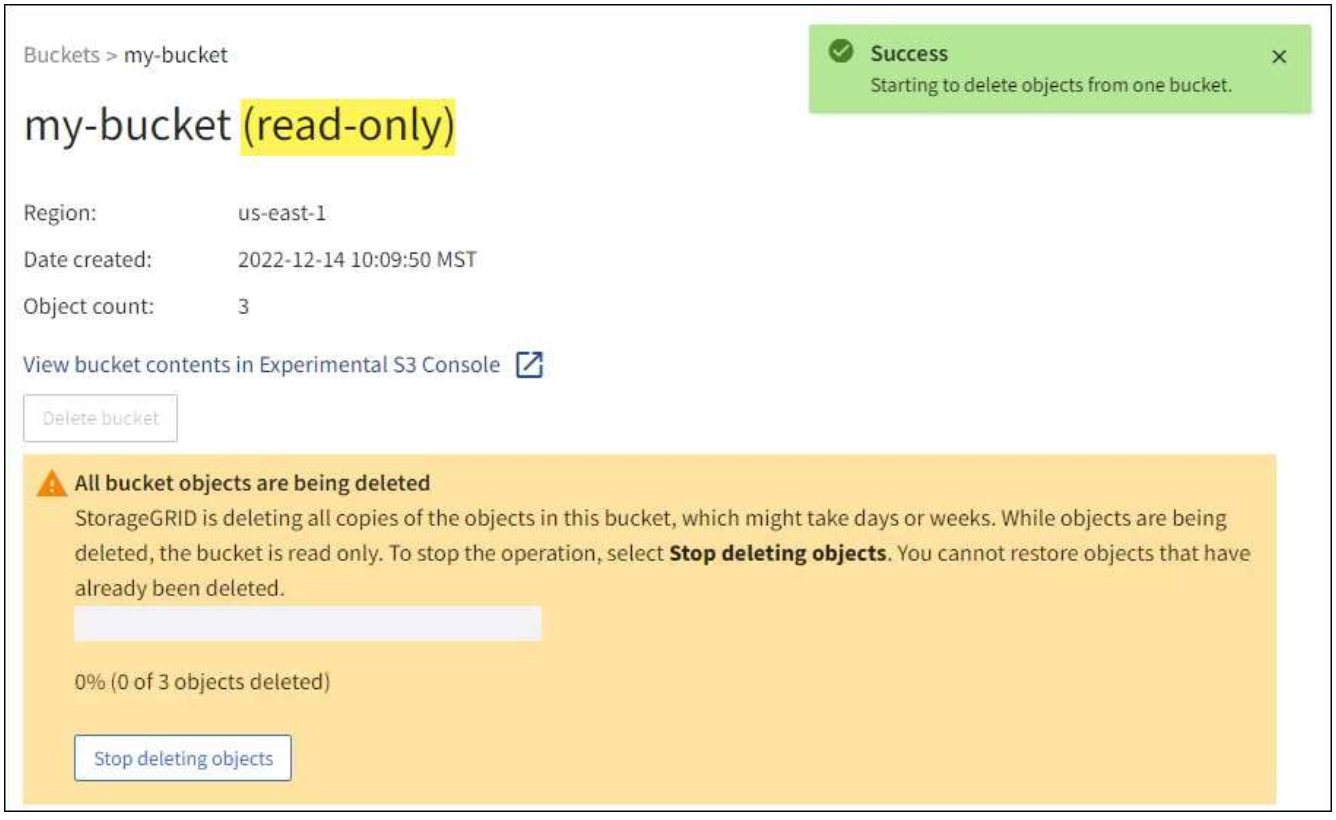
b. [Delete objects in bucket]*を選択します。

3. 確認ダイアログボックスが表示されたら、詳細を確認し、* Yes と入力して OK *を選択します。

4. 削除処理が開始されるまで待ちます。

数分後：

- バケットの詳細ページに黄色のステータスバナーが表示されます。進行状況バーは、削除されたオブジェクトの割合を表します。
- 「（読み取り専用）」は、バケットの詳細ページでバケット名のあとに表示されます。
- [Buckets]ページでバケット名の横に「（**Deleting objects：read-only**）」と表示されます。

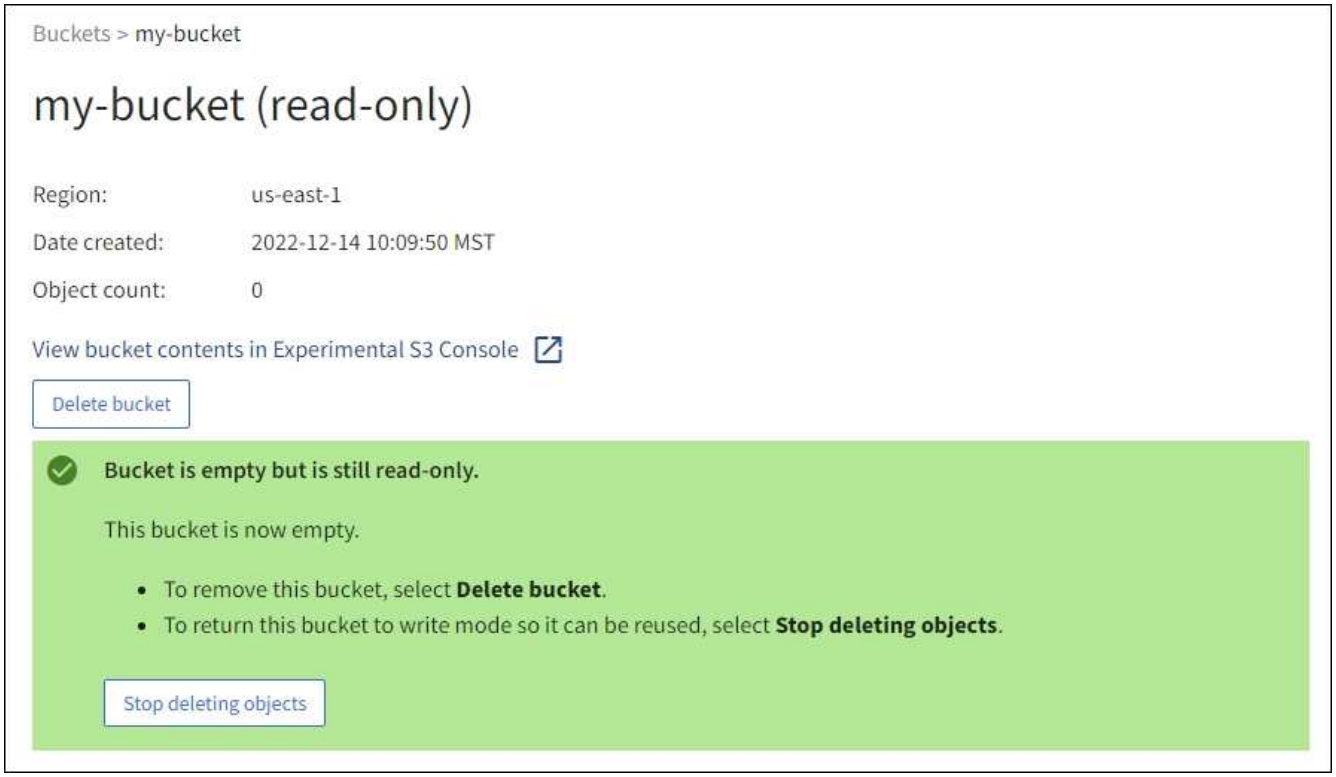


5. 処理の実行中に必要に応じて、**[**オブジェクトの削除の停止**]***を選択してプロセスを停止します。次に、必要に応じて[Delete objects in bucket]*を選択してプロセスを再開します。

[Stop deleting objects]*を選択すると、バケットは書き込みモードに戻りますが、削除されたオブジェクトにアクセスしたりリストアしたりすることはできません。

6. 処理が完了するまで待ちます。

   バケットが空の場合、ステータスバナーは更新されますが、バケットは読み取り専用のままです。



7. 次のいずれかを実行します。

   - ページを終了して、バケットを読み取り専用モードのままにします。たとえば、空のバケットを読み取り専用モードのままにしておくと、あとで使用できるようにバケット名を予約できます。
   - バケットを削除します。1つのバケットを削除する場合は、**[Delete bucket]***を選択します。複数のバケットを削除する場合は、**[Buckets]**ページに戻って[Actions]>[Delete * Buckets]を選択します。

     すべてのオブジェクトの削除後にバージョン管理されたバケットを削除できない場合は、削除マーカーが残っていることがあります。バケットを削除するには、残りのすべての削除マーカーを削除する必要があります。

   - バケットを書き込みモードに戻し、必要に応じて新しいオブジェクト用に再利用します。1つのバケットに対して[Stop deleting objects]を選択するか、**[Buckets]**ページに戻って、複数のバケットに対して**[Action]**>*[Stop deleting objects]*を選択します。

StorageGRID S3 バケットを削除する

Tenant Manager を使用して、空の S3 バケットを削除できます。

開始する前に

- を使用してTenant Managerにサインインしておき"サポートされている Web ブラウザ"ます。

- が設定されたユーザグループに属している"すべてのバケットまたはRoot Access権限を管理します"必要があります。これらの権限は、グループまたはバケットポリシーの権限の設定よりも優先されます。
- 削除するバケットが空です。削除するバケットが_not_emptyの場合は、"バケットからオブジェクトを削除する"

タスクの内容

以下の手順では、 Tenant Manager を使用して S3 バケットを削除する方法について説明します。またはを使用してS3バケットを削除することもできます"テナント管理 API""S3 REST API"。

オブジェクト、最新でないオブジェクトバージョン、またはマーカーが含まれているS3バケットは削除できません。S3バージョン管理オブジェクトの削除方法については、を参照してください"オブジェクトの削除方法"。

手順

1. ダッシュボードで* View Buckets を選択するか、 storage（S3）> Buckets *を選択します。

   バケットページが表示され、既存の S3 バケットがすべて表示されます。

2. 特定のバケットの*[Actions]*メニューまたは詳細ページを使用します。

   [Actions]メニュー

   a. 削除する各バケットのチェックボックスを選択します。

   b. >[Delete Buckets]*を選択します。

   詳細ページ

   a. 詳細を表示するバケット名を選択します。

   b. [Delete bucket]*を選択します。

3. 確認ダイアログボックスが表示されたら、*[はい]*を選択します。

   StorageGRID は、各バケットが空であることを確認してから、各バケットを削除します。この処理には数分かかることがあります。

   バケットが空でない場合は、エラーメッセージが表示されます。バケットを削除する前に、バケットを削除する必要があります"バケット内のすべてのオブジェクトと削除マーカーを削除する"。

StorageGRIDで**S3**コンソールを使用する

S3コンソールを使用して、S3バケット内のオブジェクトを表示および管理できます。

S3コンソールでは、次の操作を実行できます。

- アップロード、ダウンロード、名前変更、コピー、移動、 オブジェクトの削除
- オブジェクトバージョンの表示、リバート、ダウンロード、削除
- プレフィックスでオブジェクトを検索
- オブジェクトタグを管理します

- オブジェクトのメタデータを表示します
- 表示、作成、名前変更、コピー、移動、 フォルダの削除

> S3コンソールでは、最も一般的なケースのユーザエクスペリエンスが向上しています。すべての状況において、CLIやAPIの処理に代わるものではありません。
>
> S3コンソールを使用すると処理に時間がかかりすぎる場合（分や時間など）は、次の点を考慮してください。
>
> - 選択したオブジェクトの数を減らす
> - グラフィカルでない方法（APIまたはCLI）を使用したデータへのアクセス

開始する前に

- を使用してTenant Managerにサインインしておき"サポートされている Web ブラウザ"ます。
- オブジェクトを管理する場合は、Root Access権限のあるユーザグループに属している必要があります。または、Use S3 Console Tab権限とView All Buckets権限またはManage All Buckets権限のいずれかのユーザグループに属している必要があります。を参照して "テナント管理権限"
- ユーザーに対して S3 グループまたはバケット ポリシーが設定されています。見る"バケットとグループのアクセスポリシーを使用" 。
- ユーザのアクセスキー ID とシークレットアクセスキーを確認しておきます。必要に応じて、この情報を含むファイルが作成され `.csv`ます。を参照してください"アクセスキーの作成手順"。

手順

1. ストレージ > バケット > バケット名 を選択します。
2. [S3][Console]タブを選択します。
3. アクセスキーIDとシークレットアクセスキーをフィールドに貼り付けます。それ以外の場合は、*アクセスキーのアップロード*を選択してファイルを選択し `.csv`ます。
4. 「サインイン」を選択します。
5. バケットオブジェクトのテーブルが表示されます。必要に応じてオブジェクトを管理できます。

追加情報

- 接頭辞で検索：接頭辞検索機能は、現在のフォルダに対して特定の単語で始まるオブジェクトのみを検索します。検索には、他の場所でその単語を含むオブジェクトは含まれません。このルールは、フォルダ内のオブジェクトも環境します。たとえば、を検索する `folder1/folder2/somefile-`と、フォルダ内にあり、で始まる `somefile-`オブジェクトが返され `folder1/folder2/`ます。
- ドラッグアンドドロップ:コンピューターのファイルマネージャからS3コンソールにファイルをドラッグアンドドロップできます。ただし、フォルダをアップロードすることはできません。
- フォルダの操作:フォルダを移動、コピー、または名前変更すると、フォルダ内のすべてのオブジェクトが一度に1つずつ更新されるため、時間がかかる場合があります。
- バケットのバージョン管理が無効な場合の完全削除：バージョン管理が無効なバケット内のオブジェクトを上書きまたは削除すると、処理は永続的に実行されます。を参照して "バケットのオブジェクトのバージョン管理を変更する"

S3 プラットフォームサービスを管理します

S3 プラットフォームサービス

StorageGRIDのプラットフォームサービスについて学ぶ

プラットフォームサービスを実装する前に、これらのサービスの使用に関する概要と考慮事項を確認してください。

S3の詳細については、を参照してください"S3 REST APIを使用する"。

プラットフォームサービスの概要

StorageGRID プラットフォームサービスでは、イベント通知やS3オブジェクトとオブジェクトメタデータのコピーを外部のデスティネーションに送信できるため、ハイブリッドクラウド戦略の実装に役立ちます。

通常、プラットフォームサービスのターゲットは StorageGRID 環境の外部にあるため、プラットフォームサービスを使用することで外部ストレージリソース、通知サービス、検索または分析サービスの機能と柔軟性をデータに対して利用できます。

単一のS3バケットに対して、プラットフォームサービスの任意の組み合わせを設定できます。たとえば、StorageGRID S3バケットで"CloudMirrorサービス"と"通知"の両方を設定することで、特定のオブジェクトをAmazon Simple Storage Service （S3）にミラーリングしながら、AWSの費用を追跡するためのサードパーティの監視アプリケーションに各オブジェクトの通知を送信できます。

> プラットフォームサービスの使用は、 StorageGRID 管理者がグリッドマネージャまたはグリッド管理 API を使用してテナントアカウントごとに有効にする必要があります。

プラットフォームサービスの設定方法

プラットフォームサービスは、"テナントマネージャ"または"テナント管理 API"。各エンドポイントは、StorageGRID S3 バケット、Amazon Web Services バケット、Amazon SNS トピック、Webhook エンドポイント、ローカル、AWS、またはその他の場所でホストされている Elasticsearch クラスターなどの外部の宛先を表します。

外部エンドポイントを作成したら、バケットにXML設定を追加してプラットフォームサービスを有効にできます。XML 設定は、バケットが処理を実行するオブジェクト、実行する処理、およびサービスに使用するエンドポイントを特定します。

設定するプラットフォームサービスごとに XML 設定を追加する必要があります。例：

- キーがで始まるすべてのオブジェクト `/images`をAmazon S3バケットにレプリケートする場合は、ソースバケットにレプリケーション設定を追加する必要があります。
- これらのオブジェクトがバケットに格納されたときに通知も送信するには、通知設定を追加する必要があります。
- これらのオブジェクトのメタデータのインデックスを作成する場合は、検索統合の実装に使用するメタデータ通知設定を追加する必要があります。

設定 XML の形式は、 StorageGRID プラットフォームサービスの実装に使用する S3 REST API に従います。

プラットフォームサービス	S3 REST API	を参照してください
CloudMirror レプリケーション	• GetBucketReplicationの略 • PutBucketReplicationの略	• "CloudMirror レプリケーション" • "バケットの処理"
通知	• GetBucketNotificationConfigurationを参照してください • PutBucketNotificationConfigurationの略	• "通知" • "バケットの処理"
検索統合	• GET Bucket metadata notification configuration のコマンドです • PUT Bucket metadata notification configuration のコマンドです	• "検索統合" • "StorageGRIDのカスタム処理"

プラットフォームサービスの使用に関する考慮事項

考慮事項	詳細
デスティネーションエンドポイントの監視	各デスティネーションエンドポイントの可用性を監視する必要があります。長時間にわたってデスティネーションエンドポイントへの接続が失われ、要求のバックログが大量に発生している場合、 StorageGRID に対する以降のクライアント要求（ PUT 要求など）は失敗します。エンドポイントがアクセス可能になったら、失敗した要求を再試行する必要があります。
デスティネーションエンドポイントのスロットル	要求が送信されるペースがデスティネーションエンドポイントで要求を受信できるペースを超えると、 StorageGRID ソフトウェアはバケットの受信 S3 要求を調整する場合があります。スロットルは、デスティネーションエンドポイントへの送信を待機している要求のバックログが生じている場合にのみ発生します。 明らかな影響は、受信 S3 要求の実行時間が長くなることだけです。パフォーマンスが大幅に低下していることが検出されるようになった場合は、取り込み速度を下げるか、容量の大きいエンドポイントを使用する必要があります。要求のバックログが増え続けると、クライアント S3 処理（ PUT 要求など）が失敗します。 通常、 CloudMirror 要求には、検索統合やイベント通知の要求よりも多くのデータ転送が含まれるため、デスティネーションエンドポイントのパフォーマンスによる影響を受ける可能性が高くなります。

考慮事項	詳細
順序保証	StorageGRID では、 1 つのサイト内のオブジェクトに対する処理の順序が保証されます。あるオブジェクトに対するすべての処理が同じサイト内で実行されるかぎり、最終的なオブジェクトの（レプリケーションの）状態は常に StorageGRID の状態と同じになります。 StorageGRID は、 StorageGRID サイト間で処理が行われる場合、最善の順序で要求を処理しようと試みます。たとえば、最初にサイト A にオブジェクトを書き込んだあと、サイト B で同じオブジェクトを上書きした場合、 CloudMirror によって最終的にデスティネーションバケットにレプリケートされるオブジェクトが新しいほうのオブジェクトであるとはかぎりません。
ILM ベースのオブジェクト削除	AWS CRRとAmazon Simple Notification Serviceの削除動作と一致するように、StorageGRID ILMルールに基づいてソースバケット内のオブジェクトが削除された場合、CloudMirror要求とイベント通知要求は送信されません。たとえば、ILM ルールによって 14 日後にオブジェクトが削除された場合、 CloudMirror 要求やイベント通知要求は送信されません。 一方、 ILM に基づいてオブジェクトが削除された場合、検索統合要求は送信されます。
Kafkaエンドポイントの使用	Kafkaエンドポイントの認証では、次の認証タイプが使用されます。これらのタイプは、Amazon SNSなどの他のエンドポイントの認証に使用されるタイプとは異なり、ユーザ名とパスワードのクレデンシャルが必要です。 • SASL/プレーン • SASL/SCRAM-SHA-256 • SASL/SCRAM-SHA-512 *注：*構成済みのストレージプロキシ設定は、Kafkaプラットフォームサービスエンドポイントには適用されません。

CloudMirror レプリケーションサービスの使用に関する考慮事項

考慮事項	詳細
レプリケーションのステータス	StorageGRIDはヘッダーをサポートしていません `x-amz-replication-status`。
オブジェクトのサイズ	CloudMirror レプリケーションサービスでデスティネーションバケットにレプリケートできるオブジェクトの最大サイズは 5TiB で、maximum_supported_object サイズと同じです。 注：1回のPutObject処理の最大推奨サイズは5GiB（5、368、709、120バイト）です。5GB より大きいオブジェクトがある場合は、マルチパートアップロードを使用してください。

考慮事項	詳細
バケットのバージョン管理とバージョン ID	StorageGRID でソース S3 バケットのバージョン管理を有効にした場合、デスティネーションバケットのバージョン管理も有効にする必要があります。 バージョン管理を使用する場合、S3プロトコルの制限により、宛先バケット内のオブジェクトバージョンの順序はベストエフォートであり、CloudMirror サービスによって保証されるものではないことに注意してください。また、宛先バケットは独自の設定を保持するため、バージョン管理機能を提供しない場合があります。 注：StorageGRID のソースバケットのバージョンIDは、デスティネーションバケットのバージョンIDとは関係ありません。
オブジェクトバージョンのタグ付け	S3プロトコルの制限により、バージョンIDを提供するPutObjectTagging要求やDeleteObjectTagging要求はCloudMirrorサービスではレプリケートされません。ソースとデスティネーションのバージョンIDは関連付けられていないため、特定のバージョンIDへのタグの更新を確実にレプリケートする方法はありません。 一方、CloudMirrorサービスでは、バージョンIDを指定しないPutObjectTagging要求またはDeleteObjectTagging要求はレプリケートされません。これらの要求は、最新のキー（バケットがバージョン管理されている場合は最新のバージョン）のタグを更新します。（タグの更新ではなく）タグを使用した通常の取り込みもレプリケートされます。
マルチパートアップロードと `ETag`値	マルチパートアップロードを使用してアップロードされたオブジェクトをミラーリングした場合、 CloudMirror サービスではパートが保持されません。その結果 `ETag`、ミラーリングされたオブジェクトの値は、元のオブジェクトの値とは異なり `ETag`ます。
SSE-C （ユーザ指定のキーによるサーバ側の暗号化）で暗号化されたオブジェクト	CloudMirrorサービスでは、SSE-Cで暗号化されたオブジェクトはサポートされていません。CloudMirrorレプリケーションのソースバケットにオブジェクトを取り込む際に、要求にSSE-C要求ヘッダーが含まれていると処理が失敗します。
S3 オブジェクトのロックが有効になっているバケット	StorageGRID のソース S3 バケットで S3 Object Lock が有効になっている場合は、デフォルトの保持期間が設定された宛先バケットに対しても S3 Object Lock を有効にする必要があります。 S3 Object Lockが有効になっているソースバケットと宛先バケットに対して、_オブジェクトデータ_のレプリケーションがサポートされます。ただし、宛先バケットはオブジェクト保持に関する独自の設定を維持するため、コンプライアンスやバージョン管理を提供しない場合があります。

StorageGRID CloudMirror レプリケーションサービスについて学ぶ

S3バケットに追加されたオブジェクトを指定して1つ以上の外部のデスティネーションバケットにStorageGRIDでレプリケートする場合は、あるS3バケットに対してCloudMirrorレプリケーションを有効にすることができます。

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

CloudMirror レプリケーションは、ソースバケットで S3 オブジェクトロックが有効になっており、エンドポイントが Amazon または StorageGRID の S3 バケットである場合にのみサポートされます。オブジェクトロックの設定は、バケットエンドポイントにレプリケートされません。

CloudMirrorとILM

CloudMirrorレプリケーションは、グリッドのアクティブなILMポリシーとは独立して動作します。CloudMirror サービスは、ソースバケットに格納された時点でオブジェクトをレプリケートし、できるだけ早くデスティネーションバケットに配信します。レプリケートオブジェクトの配信は、オブジェクトの取り込みが成功したときにトリガーされます。

CloudMirrorとグリッド間レプリケーション

CloudMirrorレプリケーションには、クロスグリッドレプリケーション機能と重要な類似点と相違点があります。を参照してください "グリッド間レプリケーションとCloudMirrorレプリケーションを比較してください"。

CloudMirrorおよびS3バケット

通常、 CloudMirror レプリケーションは外部の S3 バケットをデスティネーションとして使用するように設定します。ただし、他の StorageGRID 環境や任意の S3 互換サービスを使用するようにレプリケーションを設定することもできます。

既存のバケット

既存のバケットに対してCloudMirrorレプリケーションを有効にすると、そのバケットに追加された新しいオブジェクトのみがレプリケートされます。バケット内の既存のオブジェクトはレプリケートされません。既存のオブジェクトのレプリケーションを強制的に実行するには、オブジェクトのコピーを実行して既存のオブジェクトのメタデータを更新します。

CloudMirrorレプリケーションを使用してオブジェクトをAmazon S3デスティネーションにコピーする場合は、Amazon S3で各PUT要求ヘッダー内のユーザ定義メタデータのサイズが2KBに制限されることに注意してください。オブジェクトのユーザ定義メタデータが 2KB を超える場合、そのオブジェクトはレプリケートされません。

複数のデスティネーションバケット

1つのバケット内のオブジェクトを複数のデスティネーションバケットにレプリケートするには、レプリケーション設定XMLで各ルールのデスティネーションを指定します。オブジェクトを複数のバケットに同時にレプリケートすることはできません。

バージョン管理に対応している/していないバケット

バージョン管理に対応しているバケットとそうでないバケットでCloudMirrorレプリケーションを設定できます。デスティネーションバケットは、バージョン管理に対応している場合としていない場合があります。バージョン管理に対応しているバケットとしていないバケットを組み合わせて使用することができます。たとえば、バージョン管理に対応しているバケットをバージョン管理に対応していないソースバケットのデスティネーションとして指定することも、その逆を指定することもできます。また、バージョン管理に対応していないバケット間でもレプリケートできます。

削除、レプリケーションループ、およびイベント

削除の動作

は、Amazon S3サービスのCross-Region Replication（CRR；クロスリージョンレプリケーション）の削除動作と同じです。ソースバケット内のオブジェクトを削除しても、デスティネーションのレプリケートオブジェクトは削除されません。ソースとデスティネーションの両方のバケットがバージョン管理に対応している場合は、削除マーカーがレプリケートされます。デスティネーションバケットがバージョン管理に対応していない場合、ソースバケット内のオブジェクトを削除しても削除マーカーはデスティネーションバケットにレプリケートされず、デスティネーションオブジェクトも削除されません。

レプリケーションループからの保護

StorageGRIDは、デスティネーションバケットにレプリケートされたオブジェクトを「レプリカ」としてマークします。デスティネーションStorageGRIDバケットはレプリカとしてマークされたオブジェクトを再びレプリケートしないため、誤ってレプリケーションがループすることはありません。このレプリカマーキングはStorageGRIDの内部機能であり、Amazon S3バケットをデスティネーションとして使用するときにAWS CRRを使用することを妨げません。

レプリカをマークするために使用されるカスタムヘッダーはです `x-ntap-sg-replica`。このマーキングは ' カスケード・ミラーを防止しますStorageGRID では、2つのグリッド間の双方向CloudMirrorがサポートされます。

デスティネーションバケットのイベント

デスティネーションバケット内のイベントは一意であることや順序が保証されるわけではありません。確実に配信することを目的とした処理の結果として、ソースオブジェクトの同一のコピーが複数デスティネーションに配信されることがあります。まれに、複数の異なる StorageGRID サイトから同じオブジェクトが同時に更新された場合、デスティネーションバケットでの処理の順序がソースバケットでのイベントの順序と一致しないことがあります。

S3バケットの**StorageGRID**イベント通知について学ぶ

StorageGRID が指定されたイベントに関する通知を宛先の Kafka クラスター、Webhook エンドポイント、または Amazon Simple Notification Service に送信するようにする場合は、S3 バケットのイベント通知を有効にすることができます。

たとえば、バケットに追加された各オブジェクトについてアラートが管理者に送信されるように設定できます。この場合、オブジェクトは重大なシステムイベントに関連付けられているログファイルです。

イベント通知は通知設定に従ってソースバケットで作成され、デスティネーションに配信されます。オブジェクトに関連付けられているイベントが成功すると、そのイベントに関する通知が作成されて配信のためにキューに登録されます。

通知の一意性と順序は保証されません。確実に配信することを目的とした処理の結果として、 1 つのイベントに関する通知が複数デスティネーションに配信されることがあります。また配信は非同期で実行されるため、特に異なる StorageGRID サイトで開始された処理の場合、デスティネーションでの通知の時間的順序がソースバケットでのイベントの順序と一致する保証はありません。Amazon S3のドキュメントに記載されているように、イベントメッセージでキーを使用して特定のオブジェクトのイベントの順序を決定できます `sequencer`。

StorageGRIDのイベント通知はAmazon S3 APIに従いますが、いくつかの制限事項があります。

- 次のイベントタイプがサポートされています。

- S3：ObjectCreated：
- S3：ObjectCreated：PUT
- S3：ObjectCreated：Post
- S3：ObjectCreated：コピー
- S3：ObjectCreated：CompleteMultipartUpload
- S3：ObjectRemoved：
- S3：ObjectRemoved：削除
- S3：ObjectRemoved：DeleteMarkerCreated
- S3：ObjectRestore：POSTコマンド

- StorageGRID から送信されるイベント通知は標準のJSON形式を使用しますが、次の表に示すように、一部のキーを含めずに特定の値を使用するキーもあります。

キー名	**StorageGRID** 値
eventSource	`sgws:s3`
awsRegion のようになります	含まれていません
x-amz-id-2	含まれていません
ARN	`urn:sgws:s3:::bucket_name`

StorageGRID検索統合サービスについて学ぶ

オブジェクトメタデータに外部の検索およびデータ分析サービスを使用する必要がある場合は、 S3 バケットの検索統合を有効にすることができます。

検索統合サービスはカスタムのStorageGRIDサービスです。オブジェクトの作成や削除、またはそのメタデータやタグの更新が行われるたびに、S3オブジェクトメタデータを非同期的に自動的にデスティネーションエンドポイントに送信します。その後、デスティネーションサービスが提供する高度な検索、データ分析、視覚化、機械学習のツールを使用して、オブジェクトデータを検索、分析し、情報を把握できます。

たとえば、リモートの Elasticsearch サービスに S3 オブジェクトメタデータを送信するようにバケットを設定できます。次に、 Elasticsearch を使用してバケット間で検索を実行し、オブジェクトメタデータのパターンに対して高度な分析を実行できます。

S3オブジェクトロックが有効になっているバケットではElasticsearch統合を設定できますが、Elasticsearchに送信されるメタデータには、オブジェクトのS3オブジェクトロックメタデータ（Retain Until DateおよびLegal Holdステータスを含む）は含まれません。

検索統合サービスではオブジェクトメタデータがデスティネーションに送信されるため、その設定XMLは「_metadata_notification設定XML」と呼ばれます。この設定XMLは、enable_event_notificationsに使用される「通知設定XML」とは異なります。

検索統合と**S3**バケット

検索統合サービスはバージョン管理に対応している / していないに関わらずすべてのバケットに対して有効にすることができ検索統合を設定するには、対象のオブジェクトおよびオブジェクトメタデータのデスティネーションを指定したメタデータ通知設定 XML をバケットに関連付けます。

メタデータ通知はJSONドキュメントの形式で生成され、バケット名、オブジェクト名、バージョンID（存在する場合）が指定されます。各メタデータ通知には、すべてのオブジェクトのタグとユーザメタデータに加えて、オブジェクトのシステムメタデータの標準セットが含まれています。

> タグとユーザメタデータの場合、 StorageGRID は文字列または S3 イベント通知として Elasticsearch に日付と番号を渡します。これらの文字列を日付または数値として解釈するように Elasticsearch を設定するには、動的フィールドマッピングおよびマッピング日付形式に関する Elasticsearch の手順に従ってください。検索統合サービスを設定する前に、インデックスの動的フィールドマッピングを有効にする必要があります。ドキュメントのインデックス作成後は、インデックス内のドキュメントのフィールドタイプを編集することはできません。

通知の検索

メタデータ通知は次の場合に生成され、配信のためにキューに登録されます。

- オブジェクトが作成されます。
- オブジェクトが削除されたとき。グリッドの ILM ポリシーの処理が実行された結果、オブジェクトが削除される場合も含まれます。
- オブジェクトのメタデータまたはタグが追加、更新、または削除されたとき。変更された値だけでなく、すべてのメタデータとタグが常に更新時に送信されます。

バケットにメタデータ通知設定 XML を追加すると、新しく作成したオブジェクトや、データ、ユーザメタデータ、またはタグの更新によって変更したオブジェクトに関する通知が送信されます。ただし、バケットにすでに含まれていたオブジェクトについては通知は送信されません。バケットに含まれるすべてのオブジェクトのオブジェクトメタデータを確実にデスティネーションに送信するには、次のいずれかを行う必要があります。

- バケットの作成後、オブジェクトを追加する前に、検索統合サービスを設定する。
- すでにバケットに含まれているすべてのオブジェクトに対して、メタデータ通知メッセージをデスティネーションに送信するトリガーとなる処理を実行する。

検索統合サービスと**Elasticsearch**

StorageGRID 検索統合サービスは、デスティネーションとして Elasticsearch クラスタをサポートします。他のプラットフォームサービスと同様、 URN がサービスの設定 XML で使用されているエンドポイントにデスティネーションが指定されます。を使用して "NetApp Interoperability Matrix Tool"、サポートされているElasticsearchのバージョンを確認します。

プラットフォームサービスエンドポイントの管理

StorageGRID でプラットフォームサービスエンドポイントを設定する

バケットのプラットフォームサービスを設定する前に、少なくとも 1 つのエンドポイントをプラットフォームサービスのデスティネーションとして設定する必要があります。

プラットフォームサービスへのアクセスは、 StorageGRID 管理者がテナント単位で有効にします。プラットフォームサービスエンドポイントを作成または使用するには、ストレージノードが外部のエンドポイントリソースにアクセスできるようネットワークが設定されているグリッドで、Manage EndpointsまたはRoot Access権限を持つテナントユーザである必要があります。1つのテナントに対して設定できるプラットフォームサービスエンドポイントは最大500個です。詳細については、 StorageGRID 管理者にお問い合わせください。

プラットフォームサービスエンドポイントとは何ですか。

プラットフォームサービスエンドポイントは、StorageGRIDが外部のデスティネーションにアクセスするために必要な情報を指定します。

たとえば、StorageGRID バケットからAmazon S3バケットにオブジェクトをレプリケートする場合は、StorageGRID がAmazonのデスティネーションバケットにアクセスするために必要な情報とクレデンシャルを含むプラットフォームサービスエンドポイントを作成します。

プラットフォームサービスのタイプごとに独自のエンドポイントが必要なため、使用する各プラットフォームサービスについて少なくとも 1 つのエンドポイントを設定する必要があります。プラットフォームサービスエンドポイントの定義が完了したら、サービスを有効にするための設定 XML でエンドポイントの URN をデスティネーションとして指定します。

同じエンドポイントを複数のソースバケットのデスティネーションとして使用できます。たとえば、複数のバケット間で検索を実行できるように、複数のソースバケットが同じ検索統合エンドポイントにオブジェクトメタデータを送信するように設定できます。複数のエンドポイントをターゲットとして使用するようにソースバケットを設定することもできます。これにより、オブジェクトの作成に関する通知をあるAmazon Simple Notification Service（Amazon SNS）トピックに送信したり、オブジェクトの削除に関する通知を別のAmazon SNSトピックに送信したりできます。

CloudMirror レプリケーション用のエンドポイント

StorageGRID は、 S3 バケットを表すレプリケーションエンドポイントをサポートします。このバケットは、Amazon Web Services 、同一またはリモートの StorageGRID 環境、あるいは別のサービスでホストされている可能性があります。

通知用のエンドポイント

StorageGRID は、Amazon SNS、Kafka、Webhook エンドポイントをサポートしています。 Simple Queue Service (SQS) および AWS Lambda エンドポイントはサポートされていません。

検索統合サービスのエンドポイント

StorageGRID は、 Elasticsearch クラスタを表す検索統合エンドポイントをサポートします。Elasticsearchクラスタは、ローカルデータセンターに配置することも、AWSクラウドなどの別の場所でホストすることもできます。

検索統合エンドポイントは、 Elasticsearch の特定のインデックスとタイプを参照します。StorageGRID でエンドポイントを作成する前に、 Elasticsearch でインデックスを作成しておく必要があります。作成していない場合、エンドポイントの作成に失敗します。エンドポイントを作成する前にタイプを作成する必要はありません。StorageGRID は、オブジェクトメタデータをエンドポイントに送信するときに必要に応じてタイプを作成します。

関連情報

"StorageGRID の管理"

プラットフォームサービスエンドポイントを作成するときは、 Unique Resource Name （ URN ）を指定する必要があります。プラットフォームサービスの設定XMLを作成するときは、URNを使用してエンドポイントを参照します。各エンドポイントの URN は一意である必要があります。

プラットフォームサービスエンドポイントは、作成時に StorageGRID で検証されます。プラットフォームサービスエンドポイントを作成する前に、エンドポイントで指定されたリソースが存在し、アクセス可能であることを確認してください。

URN 要素

プラットフォームサービスエンドポイントのURNは、次のようにまたは `urn:mysite` で始まる必要があります `arn:aws`。

- サービスがAmazon Web Services（AWS）でホストされている場合は、 `arn:aws`
- サービスがGoogle Cloud Platform（GCP）でホストされている場合は、 `arn:aws`
- サービスがローカルでホストされている場合は、 `urn:mysite`

たとえば、StorageGRIDでホストされるCloudMirrorエンドポイントのURNを指定する場合、URNはで始まることがあります `urn:sgws`。

URN の次の要素では、次のようにプラットフォームサービスのタイプを指定します。

サービス	タイプ
CloudMirror レプリケーション	`s3`
通知	`sns`、 `kafka` 、 または `webhook`
検索統合	`es`

たとえば、StorageGRIDでホストされるCloudMirrorエンドポイントのURNを引き続き指定するには、GETに `urn:sgws:s3` を追加します `s3`。

ほとんどのエンドポイントでは、URNの最後の要素は宛先URIの特定のターゲットリソースを識別します。たとえば、 `sns-topic-name` 。

Webhook エンドポイントの場合、ターゲット リソースは宛先 URI 自体です。

サービス	特定のリソース
CloudMirror レプリケーション	`bucket-name`

サービス	特定のリソース
通知	`sns-topic-name`または `kafka-topic-name` 注: Webhook エンドポイントの場合、エンドポイントの URN が一意である限り、URN の最後の要素は任意の文字列にすることができます。
検索統合	`domain-name/index-name/type-name` • 注： Elasticsearch クラスタが * NOT * である場合、インデックスを自動的に作成するように設定されているため、エンドポイントを作成する前にインデックスを手動で作成する必要があります。

AWS と **GCP** でホストされるサービスの **URN**

AWS と GCP のエンティティの場合、完全な URN は有効な AWS ARN です。例：

- CloudMirror レプリケーション：

```
arn:aws:s3:::bucket-name
```

- 通知：

```
arn:aws:sns:region:account-id:topic-name
```

- 検索統合：

```
arn:aws:es:region:account-id:domain/domain-name/index-name/type-name
```

AWSの検索統合エンドポイントの場合は、次に示すようにリテラル文字列をに `domain-name`含める必要があります `domain/`。

ローカルでホストされるサービスの **URN**

クラウド サービス ではなくローカルでホストされるサービスを使用する場合は、 URN の 3 番目と最後の必須要素が含まれていて、有効かつ一意な URN が作成されるのであれば、どのような方法で URN を指定してもかまいません。となっている要素はオプションで空白にすることも、リソースを識別して一意な URN の作成に役立つ任意の情報を指定することもできます。例：

- CloudMirror レプリケーション：

```
urn:mysite:s3:::bucket-name
```

StorageGRIDでホストされるCloudMirrorエンドポイントの場合は、次の文字で始まる有効なURNを指定でき `urn:sgws`ます。

```
urn:sgws:s3:::bucket-name
```

- 通知：

  Amazon Simple Notification Serviceエンドポイントを指定します。

  ```
  urn:aws:sns:region:account-id:sns-topic-name
  ```

  Kafkaエンドポイントを指定します。

  ```
  urn::kafka:::kafka-topic-name
  ```

  オプションで、Kafkaエンドポイントを指定する際に `mysite`を含めることができます：`urn:mysite:kafka:::kafka-topic-name`

  Webhook エンドポイントを指定します。

  ```
  urn:mysite:webhook:::webhook-name
  ```

- 検索統合：

  ```
  urn:mysite:es:::domain-name/index-name/type-name
  ```

  ローカルでホストされる検索統合エンドポイントの場合、 `domain-name`エンドポイントのURNが一意であるかぎり、要素には任意の文字列を指定できます。

StorageGRIDプラットフォームサービスエンドポイントを作成する

プラットフォームサービスを有効にする前に、正しいタイプのエンドポイントを少なくとも 1 つ作成しておく必要があります。

開始する前に

- を使用してTenant Managerにサインインしておき"サポートされている Web ブラウザ"ます。
- テナントアカウントのプラットフォームサービスがStorageGRID 管理者によって有効にされている。
- が設定されたユーザグループに属している"エンドポイントまたはRoot Access権限を管理します"必要があります。
- プラットフォーム サービス エンドポイントによって参照されるリソースが作成されました。

- CloudMirror レプリケーション： S3 バケット
- イベント通知: Amazon Simple Notification Service (Amazon SNS) トピック、Kafka トピック、または Webhook エンドポイント
- 検索通知: 宛先クラスターがインデックスを自動的に作成するように構成されていない場合は、Elasticsearch インデックス。

- デスティネーションリソースに関する情報を確認しておきます。
  - Uniform Resource Identifier （ URI ）のホストとポート

    StorageGRID システムでホストされているバケットを CloudMirror レプリケーションのエンドポイントとして使用する場合は、グリッド管理者に問い合わせて入力が必要な値を決定してください。

  - Unique Resource Name （ URN ）

    "プラットフォームサービスのエンドポイントの URN を指定してください"

  - 認証クレデンシャル（必要な場合）：

    検索統合エンドポイント

    検索統合エンドポイントには、次のクレデンシャルを使用できます。

    - Access Key ：アクセスキー ID とシークレットアクセスキー
    - 基本 HTTP 認証：ユーザ名とパスワード

    CloudMirrorレプリケーションエンドポイント

    CloudMirrorレプリケーションエンドポイントの場合は、次のクレデンシャルを使用できます。

    - Access Key ：アクセスキー ID とシークレットアクセスキー
    - CAP （ C2S Access Portal ）：一時的なクレデンシャル URL 、サーバ証明書とクライアント証明書、クライアントキー、およびオプションのクライアント秘密鍵パスフレーズ。

    Amazon SNSエンドポイント

    Amazon SNSエンドポイントの場合は、次のクレデンシャルを使用できます。

    - Access Key ：アクセスキー ID とシークレットアクセスキー

    Kafkaエンドポイント

    Kafkaエンドポイントの場合は、次のクレデンシャルを使用できます。

    - SASL/plain：ユーザ名とパスワード
    - SASL/SCRAM-SHA-256：ユーザ名とパスワード
    - SASL/SCRAM-SHA-512：ユーザ名とパスワード

  - セキュリティ証明書（証明書の検証が必要な場合）

- Elasticsearchセキュリティ機能が有効になっている場合は、接続テスト用のmonitor cluster権限と、ドキュメント更新用のwrite index権限、またはindex権限とdelete index権限の両方があります。

手順

1. ストレージ（ S3 ） * > * プラットフォームサービスのエンドポイント * を選択します。プラットフォームサービスエンドポイントページが表示されます。
2. [* エンドポイントの作成 *] を選択します。
3. エンドポイントとその目的を簡単に説明する表示名を入力します。

   エンドポイントがサポートするプラットフォーム サービスのタイプは、エンドポイント ページにリストされるときにエンドポイント名の横に表示されるため、名前にその情報を含める必要はありません。

4. [* URI*] フィールドに、エンドポイントの Unique Resource Identifier （ URI ）を指定します。

   次のいずれかの形式を使用します。

   ```
   https://host:port
   http://host:port
   ```

   ポートを指定しない場合は、次のデフォルトポートが使用されます。

   - HTTPS URIにはポート443、HTTP URIにはポート80（ほとんどのエンドポイント）
   - HTTPSおよびHTTP URI用のポート9092（Kafkaエンドポイントのみ）

   たとえば、 StorageGRID でホストされているバケットの URI は次のようになります。

   ```
   https://s3.example.com:10443
   ```

   この例のは `s3.example.com`StorageGRIDハイアベイラビリティ（HA）グループの仮想IP（VIP）のDNSエントリ、 `10443`はロードバランサエンドポイントで定義されたポートです。

   > ⓘ 単一点障害（Single Point of Failure）を回避するために、可能なかぎりロードバランシングノードのHAグループに接続する必要があります。

   同様に、 AWS でホストされているバケットの URI は次のようになります。

   ```
   https://s3-aws-region.amazonaws.com
   ```

   > ⓘ エンドポイントがCloudMirrorレプリケーションサービスに使用される場合は、URIにバケット名を含めないでください。バケット名は「 * URN * 」フィールドに含める必要があります。

5. エンドポイントの Unique Resource Name （ URN ）を入力します。

エンドポイントの作成後にエンドポイントのURNを変更することはできません。

6. 「 * Continue * 」を選択します。
7. [認証タイプ]*の値を選択します。

Webhookエンドポイントの認証が必要な場合は、Mutual Transport Layer Security（mTLS）を設定します。ステップ9 。

検索統合エンドポイント

検索統合エンドポイントのクレデンシャルを入力またはアップロードします。

指定するクレデンシャルには、デスティネーションリソースに対する書き込み権限が必要です。

認証タイプ	製品説明	クレデンシャル
匿名	デスティネーションへの匿名アクセスを許可します。セキュリティが無効になっているエンドポイントでのみ機能します。	認証なし。
アクセスキー	AWS 形式のクレデンシャルを使用してデスティネーションとの接続を認証します。	• アクセスキーID • シークレットアクセスキー
基本 HTTP	ユーザ名とパスワードを使用して、デスティネーションへの接続を認証します。	• ユーザ名 • パスワード

CloudMirrorレプリケーションエンドポイント

CloudMirrorレプリケーションエンドポイントのクレデンシャルを入力またはアップロードします。

指定するクレデンシャルには、デスティネーションリソースに対する書き込み権限が必要です。

認証タイプ	製品説明	クレデンシャル
匿名	デスティネーションへの匿名アクセスを許可します。セキュリティが無効になっているエンドポイントでのみ機能します。	認証なし。
アクセスキー	AWS 形式のクレデンシャルを使用してデスティネーションとの接続を認証します。	• アクセスキーID • シークレットアクセスキー

認証タイプ	製品説明	クレデンシャル
CAP （ C2S Access Portal ）	証明書とキーを使用してデスティネーションへの接続を認証します。	• 一時的な資格情報 URL • サーバ CA 証明書（ PEM ファイルのアップロード） • クライアント証明書（ PEM ファイルのアップロード） • クライアント秘密鍵（ PEM ファイルのアップロード、 OpenSSL 暗号化形式、または暗号化されていない秘密鍵形式） • クライアント秘密鍵のパスフレーズ（オプション）

Amazon SNSエンドポイント

Amazon SNSエンドポイントのクレデンシャルを入力またはアップロードします。

指定するクレデンシャルには、デスティネーションリソースに対する書き込み権限が必要です。

認証タイプ	製品説明	クレデンシャル
匿名	デスティネーションへの匿名アクセスを許可します。セキュリティが無効になっているエンドポイントでのみ機能します。	認証なし。
アクセスキー	AWS 形式のクレデンシャルを使用してデスティネーションとの接続を認証します。	• アクセスキーID • シークレットアクセスキー

Kafkaエンドポイント

Kafkaエンドポイントのクレデンシャルを入力またはアップロードします。

指定するクレデンシャルには、デスティネーションリソースに対する書き込み権限が必要です。

認証タイプ	製品説明	クレデンシャル
匿名	デスティネーションへの匿名アクセスを許可します。セキュリティが無効になっているエンドポイントでのみ機能します。	認証なし。
SASL/プレーン	プレーンテキストのユーザ名とパスワードを使用して、宛先への接続を認証します。	• ユーザ名 • パスワード

認証タイプ	製品説明	クレデンシャル
SASL/SCRAM-SHA-256	チャレンジ応答プロトコルとSHA-256ハッシュを使用してユーザ名とパスワードを使用し、宛先への接続を認証します。	• ユーザ名 • パスワード
SASL/SCRAM-SHA-512	チャレンジ応答プロトコルとSHA-512ハッシュを使用してユーザ名とパスワードを使用し、宛先への接続を認証します。	• ユーザ名 • パスワード

ユーザ名とパスワードがKafkaクラスタから取得した委任トークンから取得されたものである場合は、* Use delegation taken authentication *を選択します。

8. 「 * Continue * 」を選択します。
9. エンドポイントへの TLS 接続を検証する方法を選択するには、[証明書の検証] のラジオ ボタンを選択します。

ほとんどのエンドポイント

検索統合、CloudMirror レプリケーション、Amazon SNS、または Kafka エンドポイントの TLS 接続を確認します。

証明書検証のタイプ	製品説明
TLS	エンドポイント リソースへの TLS 接続のサーバー証明書を検証します。
無効	証明書の検証は無効です。このオプションは安全ではありません。
カスタム CA 証明書を使用する	カスタム CA 証明書は、エンドポイントに接続するときにサーバーの ID を確認するために使用されます。
オペレーティングシステムの CA 証明書を使用します	オペレーティングシステムにインストールされているデフォルトの Grid CA 証明書を使用して接続を保護します。

Webhookと**Kafka**エンドポイント

ウェブフックまたはKafkaエンドポイントのTLS接続を確認してください。

証明書検証のタイプ	製品説明
TLS	エンドポイント リソースへの TLS 接続のサーバー証明書を検証します。
mTLS	エンドポイント リソースへの相互 TLS 接続のクライアント証明書とサーバー証明書を検証します。
無効	証明書の検証は無効です。このオプションは安全ではありません。
カスタム CA 証明書を使用する	カスタム CA 証明書は、エンドポイントに接続するときにサーバーの ID を確認するために使用されます。
オペレーティングシステムの CA 証明書を使用します	オペレーティングシステムにインストールされているデフォルトの Grid CA 証明書を使用して接続を保護します。 注：Webhookエンドポイントにはこのオプションはありません。

mTLS を選択すると、これらのオプションが利用可能になります。

証明書検証のタイプ	製品説明
サーバー証明書を検証しない	サーバー証明書の検証を無効にします。つまり、サーバーの ID は検証されません。このオプションは安全ではありません。

証明書検証のタイプ	製品説明
クライアント証明書	クライアント証明書は、エンドポイントに接続するときにクライアントの ID を確認するために使用されます。
クライアントの秘密鍵	クライアント証明書の秘密キー。暗号化する場合は、従来の形式 PKCS #1 を使用する必要があります (PKCS #8 形式はサポートされていません)。
クライアントの秘密鍵のパスフレーズ	クライアントの秘密鍵を復号化するためのパスフレーズ。秘密鍵が暗号化されていない場合は空白のままにします。

10. [* テストとエンドポイントの作成 *] を選択します。
    - 指定したクレデンシャルを使用してエンドポイントにアクセスできた場合は、成功を伝えるメッセージが表示されます。エンドポイントへの接続は、各サイトの 1 つのノードから検証されます。
    - エンドポイントの検証が失敗した場合は、エラーメッセージが表示されます。エラーを修正するためにエンドポイントを変更する必要がある場合は、 * エンドポイントの詳細に戻る * を選択して情報を更新します。次に、「 * Test 」を選択し、エンドポイントを作成します。 *

> テナントアカウントでプラットフォームサービスが有効になっていないと、エンドポイントの作成が失敗します。StorageGRID 管理者にお問い合わせください。

エンドポイントの設定が完了したら、その URN を使用してプラットフォームサービスを設定できます。

関連情報

- "プラットフォームサービスのエンドポイントの URN を指定してください"
- "CloudMirror レプリケーションを設定します"
- "イベント通知の設定"
- "検索統合サービスを設定する"
- "外部との通信に使用するポート"

StorageGRIDプラットフォームサービスエンドポイントの接続をテストします

プラットフォームサービスへの接続が変更された場合は、エンドポイントへの接続をテストして、デスティネーションリソースが存在すること、および指定したクレデンシャルでアクセスできることを確認できます。

開始する前に

- を使用してTenant Managerにサインインしておき"サポートされている Web ブラウザ"ます。
- が設定されたユーザグループに属している"エンドポイントまたはRoot Access権限を管理します"必要があります。

タスクの内容

StorageGRID は、クレデンシャルに正しい権限があるかどうかを検証しません。

手順

1. ストレージ（ S3 ） * > * プラットフォームサービスのエンドポイント * を選択します。

   Platform services Endpoints ページが表示され、設定済みのプラットフォームサービスエンドポイントのリストが表示されます。

2. 接続をテストするエンドポイントを選択します。

   エンドポイントの詳細ページが表示されます。

3. [接続のテスト *] を選択します。

   - 指定したクレデンシャルを使用してエンドポイントにアクセスできた場合は、成功を伝えるメッセージが表示されます。エンドポイントへの接続は、各サイトの 1 つのノードから検証されます。
   - エンドポイントの検証が失敗した場合は、エラーメッセージが表示されます。エラーを修正するためにエンドポイントを変更する必要がある場合は、「 * Configuration * 」を選択して情報を更新します。次に、 [テスト] を選択し、変更を保存します。 *

StorageGRIDでプラットフォームサービスエンドポイントを編集する

プラットフォームサービスエンドポイントの設定を編集して、名前、 URI 、またはその他の詳細を変更できます。たとえば、期限切れのクレデンシャルを更新したり、フェールオーバー用のバックアップ Elasticsearch インデックスを指すように URI を変更したりすることが必要な場合があります。プラットフォームサービスエンドポイントのURNは変更できません。

開始する前に

- を使用してTenant Managerにサインインしておき"サポートされている Web ブラウザ"ます。
- が設定されたユーザグループに属している"エンドポイントまたはRoot Access権限を管理します"必要があります。

手順

1. ストレージ（ S3 ） * > * プラットフォームサービスのエンドポイント * を選択します。

   Platform services Endpoints ページが表示され、設定済みのプラットフォームサービスエンドポイントのリストが表示されます。

2. 編集するエンドポイントを選択します。

   エンドポイントの詳細ページが表示されます。

3. 「 * Configuration * 」を選択します。
4. 必要に応じて、エンドポイントの設定を変更します。

   エンドポイントの作成後にエンドポイントのURNを変更することはできません。

   a. エンドポイントの表示名を変更するには、編集アイコン を選択します。
   b. 必要に応じて、 URI を変更します。

c. 必要に応じて、認証タイプを変更します。

- アクセスキー認証の場合は、必要に応じて「 * S3 キーの編集」を選択し、新しいアクセスキー ID とシークレットアクセスキーを貼り付けることで、キーを変更します。変更をキャンセルする必要がある場合は、 * Revert S3 key edit * を選択します。
- CAP （ C2S Access Portal ）認証の場合は、一時的なクレデンシャル URL またはオプションのクライアント秘密鍵パスフレーズを変更し、必要に応じて新しい証明書と鍵ファイルをアップロードします。

> クライアント秘密鍵は、 OpenSSL 暗号化形式または暗号化されていない秘密鍵形式である必要があります。

d. 必要に応じて、証明書の検証方法を変更します。

5. [変更のテストと保存 *] を選択します。
   - 指定したクレデンシャルを使用してエンドポイントにアクセスできた場合は、成功を伝えるメッセージが表示されます。エンドポイントへの接続は、各サイトの 1 つのノードから検証されます。
   - エンドポイントの検証が失敗した場合は、エラーメッセージが表示されます。エンドポイントを変更してエラーを修正し、 [変更のテストと保存] を選択します。

StorageGRIDプラットフォームサービスエンドポイントを削除する

関連するプラットフォームサービスが不要になった場合は、エンドポイントを削除できます。

開始する前に

- を使用してTenant Managerにサインインしておき"サポートされている Web ブラウザ"ます。
- が設定されたユーザグループに属している"エンドポイントまたはRoot Access権限を管理します"必要があります。

手順

1. ストレージ（ S3 ） * > * プラットフォームサービスのエンドポイント * を選択します。

   Platform services Endpoints ページが表示され、設定済みのプラットフォームサービスエンドポイントのリストが表示されます。

2. 削除する各エンドポイントのチェックボックスを選択します。

> 使用中のプラットフォームサービスエンドポイントを削除すると、エンドポイントを使用するすべてのバケットに対して、関連するプラットフォームサービスが無効になります。完了していない要求はすべて破棄されます。新しい要求は、削除された URN を参照しないようにバケット設定を変更するまで、引き続き生成されます。StorageGRID はこれらの要求を回復不能なエラーとして報告します。

3. [* アクション * > * エンドポイントの削除 *] を選択します。

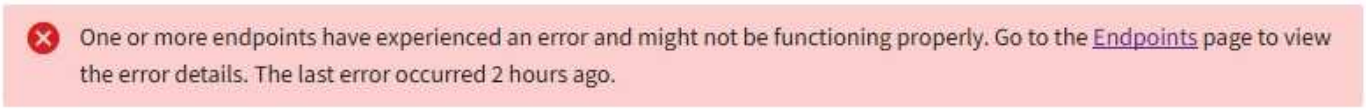
   確認メッセージが表示されます。

4. [* エンドポイントの削除 *] を選択します。

StorageGRID がプラットフォームサービスエンドポイントと通信しようとしたときにエラーが発生すると、ダッシュボードにメッセージが表示されます。Platform services Endpoints ページの Last error 列は、エラーが発生してからの時間を示します。エンドポイントのクレデンシャルに関連付けられている権限が正しくない場合は、エラーは表示されません。

エラーが発生したかどうかを確認します

過去7日以内にプラットフォームサービスエンドポイントエラーが発生した場合は、Tenant Managerダッシュボードにアラートメッセージが表示されます。プラットフォームサービスのエンドポイントページに移動して、エラーの詳細を確認できます。



ダッシュボードに表示されるのと同じエラーは、[Platform services Endpoints]ページの上部にも表示されます。詳細なエラーメッセージを表示するには、次の手順を実行します

手順

1. エンドポイントのリストで、エラーが発生したエンドポイントを選択します。
2. エンドポイントの詳細ページで、「接続」を選択します。このタブには、エンドポイントに関する最新のエラーのみが表示され、エラーが発生した日時も示されます。赤いXアイコンを含むエラーは、過去7日以内に発生したものです。

エラーがまだ最新であるかどうかを確認します

一部のエラーは、解決後も「 * Last error * 」列に引き続き表示される場合があります。エラーが現在発生しているかどうかを確認したり、解決済みのエラーをテーブルから強制的に削除したりするには、次の手順を実行します。

手順

1. エンドポイントを選択します。

   エンドポイントの詳細ページが表示されます。

2. 接続 > 接続テスト * を選択します。

[接続のテスト *] を選択すると、 StorageGRID はプラットフォームサービスエンドポイントが存在すること、および現在のクレデンシャルでアクセスできることを検証します。エンドポイントへの接続は、各サイトの 1 つのノードから検証されます。

エンドポイントエラーの解決

エンドポイントの詳細ページの「 * Last error * 」メッセージを使用して、エラーの原因を特定できます。一部のエラーでは、問題 を解決するためにエンドポイントの編集が必要になります。たとえば、 StorageGRID に正しいアクセス権限がないか、アクセスキーが期限切れになっているためにデスティネーションの S3 バケットにアクセスできない場合、 CloudMirror のエラーが発生することがあります。メッセージは「Either the

endpoint credentials or the destination access needs to be updated」で、詳細は「AccessDenied」または「InvalidAccessKeyId」です。

エラーを解決するためにエンドポイントを編集する必要がある場合は、「 * 変更のテストと保存 * 」を選択すると、 StorageGRID によって更新されたエンドポイントが検証され、現在のクレデンシャルで到達できることが確認されます。エンドポイントへの接続は、各サイトの 1 つのノードから検証されます。

手順

1. エンドポイントを選択します。
2. エンドポイントの詳細ページで、 * 構成 * を選択します。
3. 必要に応じてエンドポイントの設定を編集します。
4. 接続 **>** 接続テスト * を選択します。

必要な権限がないエンドポイントクレデンシャルです

StorageGRID によるプラットフォームサービスエンドポイントの検証では、エンドポイントのクレデンシャルを使用してデスティネーションリソースに接続できること、および基本的な権限チェックを実行できることが確認されます。ただし、 StorageGRID では、特定のプラットフォームサービス処理に必要なすべての権限が検証されるわけではありません。そのため、プラットフォームサービスを使用しようとしたときにエラー（「403 Forbidden」など）が表示された場合は、エンドポイントのクレデンシャルに関連付けられている権限を確認してください。

関連情報

- "StorageGRIDの管理>プラットフォームサービスのトラブルシューティング"
- "プラットフォームサービスエンドポイントを作成します"
- "プラットフォームサービスエンドポイントの接続をテストします"
- "プラットフォームサービスエンドポイントを編集します"

StorageGRIDで**CloudMirror**レプリケーションを設定する

バケットに対してCloudMirrorレプリケーションを有効にするには、有効なバケットレプリケーション設定XMLを作成して適用します。

開始する前に

- テナントアカウントのプラットフォームサービスがStorageGRID 管理者によって有効にされている。
- レプリケーションソースとして機能するバケットがすでに作成されている。
- CloudMirrorレプリケーションのデスティネーションとして使用するエンドポイントがすでに存在し、そのURNが必要です。
- が設定されたユーザグループに属している"すべてのバケットまたはRoot Access権限を管理します"必要があります。これらの権限は、 Tenant Manager を使用してバケットを設定する際にグループポリシーまたはバケットポリシーの権限設定よりも優先されます。

タスクの内容

CloudMirror レプリケーションでは、ソースバケットからエンドポイントで指定されたデスティネーションバケットにオブジェクトがコピーされます。

バケットレプリケーションとその設定方法の一般的な情報については、を参照してください "Amazon Simple Storage Service（S3）のドキュメント：「オブジェクトのレプリケート"。StorageGRIDでのGetBucketReplication、DeleteBucketReplication、およびPutBucketReplicationの実装方法については、を参照してください"バケットの処理"。

> CloudMirrorレプリケーションには、クロスグリッドレプリケーション機能と重要な類似点と相違点があります。詳細については、を参照してください"グリッド間レプリケーションとCloudMirrorレプリケーションを比較してください"。

CloudMirrorレプリケーションを設定する場合は、次の要件と特性に注意してください。

- 有効なバケットレプリケーション設定XMLを作成して適用する場合は、各デスティネーションにS3バケットエンドポイントのURNを使用する必要があります。
- レプリケーションは、Amazon S3 または StorageGRID S3 バケットで S3 オブジェクトロックが有効になっているソースバケットまたは宛先バケットに対してのみサポートされます。オブジェクトロックヘッダーは、宛先オブジェクトにレプリケートされません。
- オブジェクトを含むバケットでCloudMirrorレプリケーションを有効にすると、バケットに追加された新しいオブジェクトがレプリケートされますが、バケット内の既存のオブジェクトはレプリケートされません。レプリケーションをトリガーするには、既存のオブジェクトを更新する必要があります。
- CloudMirror レプリケーションを設定した後に宛先バケットで S3 オブジェクトロックを有効にした場合、レプリケーションを再開できるようにするために "エンドポイントを再保存する" が必要になることがあります。
- レプリケーション設定 XML でストレージクラスを指定した場合は、デスティネーション S3 エンドポイントに対して処理を実行する際に StorageGRID でそのクラスが使用されます。指定したストレージクラスは、デスティネーションエンドポイントでもサポートされている必要があります。デスティネーションシステムのベンダーからの推奨事項がある場合は、それに準拠してください。

手順

1. ソースバケットのレプリケーションを有効にします。
   - S3 レプリケーション API で指定されているように、レプリケーションを有効にするために必要なレプリケーション設定 XML をテキストエディタで作成します。
   - XML を設定する場合は、次の点に
     - StorageGRID では、 V1 のレプリケーション設定のみがサポートされます。これは、StorageGRIDがルールに要素を使用することをサポートして `Filter`おらず、オブジェクトバージョンの削除に関するV1の規則に従います。詳細については、レプリケーション設定に関する Amazon のドキュメントを参照してください。
     - デスティネーションとして S3 バケットエンドポイントの URN を使用してください。
     - 必要に応じて要素を追加し `<StorageClass>`、次のいずれかを指定します。
       - `STANDARD`：デフォルトのストレージクラス。オブジェクトをアップロードするときにストレージクラスを指定しない場合は、 `STANDARD`ストレージクラスが使用されます。
       - `STANDARD_IA`:(標準-アクセス頻度が低い)アクセス頻度は低いものの、必要に応じて高速アクセスが必要なデータには、このストレージクラスを使用します。
       - `REDUCED_REDUNDANCY`：このストレージクラスは、重要でない、再現可能なデータに使用し、ストレージクラスよりも冗長性が低いデータを格納する場合に使用します `STANDARD`。
     - 設定XMLでを指定すると、 `Role`無視されます。この値は StorageGRID では使用されません。

```
<ReplicationConfiguration>
    <Role></Role>
    <Rule>
        <Status>Enabled</Status>
        <Prefix>2020</Prefix>
        <Destination>
           <Bucket>urn:sgws:s3:::2017-records</Bucket>
           <StorageClass>STANDARD</StorageClass>
         </Destination>
     </Rule>
</ReplicationConfiguration>
```

2. ダッシュボードで* View Buckets を選択するか、 storage（S3）> Buckets *を選択します。
3. ソースバケットの名前を選択します。

   バケットの詳細ページが表示されます。

4. プラットフォームサービス * > * レプリケーション * を選択します。
5. [レプリケーションを有効にする]*チェックボックスを選択します。
6. レプリケーション設定 XML をテキストボックスに貼り付け、 * 変更を保存 * を選択します。

   StorageGRID 管理者がグリッドマネージャまたはグリッド管理 API を使用して各テナントアカウントのプラットフォームサービスを有効にしておく必要があります。設定 XML の保存時にエラーが発生した場合は、 StorageGRID 管理者にお問い合わせください。

7. レプリケーションが正しく設定されていることを確認します。
   a. レプリケーション設定で指定されたレプリケーションの要件を満たすオブジェクトをソースバケットに追加します。

      前述の例では、プレフィックス「2020」に一致するオブジェクトがレプリケートされます。

   b. オブジェクトがデスティネーションバケットにレプリケートされたことを確認します。

      サイズの小さいオブジェクトについては、レプリケーションの所要時間が短くなります。

関連情報

"プラットフォームサービスエンドポイントを作成します"

StorageGRID でイベント通知を設定

バケットの通知を有効にするには、通知設定XMLを作成し、Tenant Managerを使用してそのXMLをバケットに適用します。

開始する前に

- テナントアカウントのプラットフォームサービスがStorageGRID 管理者によって有効にされている。

- 通知のソースとして機能するバケットを作成しておきます。
- イベント通知のデスティネーションとして使用するエンドポイントがすでに存在し、URNが設定されている必要があります。
- が設定されたユーザグループに属している"すべてのバケットまたはRoot Access権限を管理します"必要があります。これらの権限は、 Tenant Manager を使用してバケットを設定する際にグループポリシーまたはバケットポリシーの権限設定よりも優先されます。

タスクの内容

通知設定 XML をソース バケットに関連付けることで、イベント通知を設定します。通知設定 XML は、バケット通知を設定するための S3 規則に従い、宛先の Amazon SNS トピック、Kafka トピック、または Webhook エンドポイントをエンドポイントの URN として指定します。

イベント通知とその設定方法の一般的な情報については、を参照して "Amazonのドキュメント"ください。StorageGRIDでS3バケットの通知設定APIを実装する方法については、を参照して"S3 クライアントアプリケーションを実装するための手順"ください。

バケットのイベント通知を設定するときは、次の要件と特性に注意してください。

- 有効な通知設定XMLを作成して適用する場合は、各デスティネーションのイベント通知エンドポイントのURNを使用する必要があります。
- S3オブジェクトロックが有効なバケットでイベント通知を設定できますが、オブジェクトのS3オブジェクトロックメタデータ（Retain Until DateやLegal Holdステータスを含む）は通知メッセージに含まれません。
- イベント通知を設定すると、ソースバケット内のオブジェクトに対して指定されたイベントが発生するたびに通知が生成され、送信先として使用される Amazon SNS トピック、Kafka トピック、または Webhook エンドポイントに送信されます。
- オブジェクトを含むあるバケットのイベント通知を有効にした場合、通知は通知設定の保存後に実行された処理に対してのみ送信されます。

手順

1. ソースバケットの通知を有効にします。
    - イベント通知を有効にするために必要な通知設定 XML を、 S3 通知 API で指定されている内容に従ってテキストエディタで作成します。
    - XML を設定するにあたっては、デスティネーショントピックとしてイベント通知エンドポイントの URN を使用します。

```
<NotificationConfiguration>
  <TopicConfiguration>
     <Id>Image-created</Id>
     <Filter>
        <S3Key>
          <FilterRule>
            <Name>prefix</Name>
            <Value>images/</Value>
          </FilterRule>
        </S3Key>
    </Filter>
    <Topic>arn:aws:sns:us-east-1:050340950352:sgws-topic</Topic>
    <Event>s3:ObjectCreated:*</Event>
   </TopicConfiguration>
 </NotificationConfiguration>
```

2. Tenant Manager で、 * Storage （ S3 ） * > * Buckets * を選択します。
3. ソースバケットの名前を選択します。

   バケットの詳細ページが表示されます。

4. プラットフォームサービス > イベント通知 * を選択します。
5. [イベント通知を有効にする]*チェックボックスをオンにします。
6. 通知設定 XML をテキストボックスに貼り付け、 * 変更を保存 * を選択します。

   StorageGRID 管理者がグリッドマネージャまたはグリッド管理 API を使用して各テナントアカウントのプラットフォームサービスを有効にしておく必要があります。設定 XML の保存時にエラーが発生した場合は、 StorageGRID 管理者にお問い合わせください。

7. イベント通知が正しく設定されていることを確認します。

   a. 設定 XML で設定した通知をトリガーする要件を満たす操作をソースバケット内のオブジェクトに対して実行します。

      この例では、プレフィックスが付いたオブジェクトが作成されるたびにイベント通知が送信され `images/` ます。

   b. 通知が宛先の Amazon SNS トピック、Kafka トピック、または Webhook エンドポイントに配信されたことを確認します。

      たとえば、デスティネーショントピックがAmazon SNSでホストされている場合は、通知が配信されたときにEメールを送信するようにサービスを設定できます。

```
{
   "Records":[
      {
         "eventVersion":"2.0",
         "eventSource":"sgws:s3",
         "eventTime":"2017-08-08T23:52:38Z",
         "eventName":"ObjectCreated:Put",
         "userIdentity":{
            "principalId":"11111111111111111"
         },
         "requestParameters":{
            "sourceIPAddress":"193.51.100.20"
         },
         "responseElements":{
            "x-amz-request-id":"122047343"
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"Image-created",
            "bucket":{
               "name":"test1",
               "ownerIdentity":{
                  "principalId":"11111111111111111"
               },
               "arn":"arn:sgws:s3:::test1"
            },
            "object":{
               "key":"images/cat.jpg",
               "size":0,
               "eTag":"d41d8cd98f00b204e9800998ecf8427e",
               "sequencer":"14D90402421461C7"
            }
         }
      }
   ]
}
```

+
デスティネーショントピックに通知が届いた場合は、 StorageGRID 通知のソースバケットが正しく設定されています。

関連情報

- "バケットの通知について理解します"
- "S3 REST APIを使用する"

- "プラットフォームサービスエンドポイントを作成します"

StorageGRID で検索統合サービスを設定します

バケットの検索統合を有効にするには、検索統合XMLを作成し、Tenant Managerを使用してそのXMLをバケットに適用します。

開始する前に

- テナントアカウントのプラットフォームサービスがStorageGRID 管理者によって有効にされている。
- コンテンツにインデックスを付けるS3バケットを作成しておきます。
- 検索統合サービスのデスティネーションとして使用するエンドポイントがすでに存在し、URNが設定されている必要があります。
- が設定されたユーザグループに属している"すべてのバケットまたはRoot Access権限を管理します"必要があります。これらの権限は、 Tenant Manager を使用してバケットを設定する際にグループポリシーまたはバケットポリシーの権限設定よりも優先されます。

タスクの内容

ソースバケットに対して検索統合サービスを設定した場合、オブジェクトを作成またはオブジェクトのメタデータ / タグを更新すると、オブジェクトメタデータがデスティネーションエンドポイントに送信されます。

すでにオブジェクトが含まれているバケットで検索統合サービスを有効にすると、既存のオブジェクトに関するメタデータ通知は自動的には送信されません。これらの既存のオブジェクトを更新して、デスティネーションの検索インデックスにメタデータが追加されるようにします。

手順

1. バケットの検索統合を有効にします。
    - 検索統合を有効にするために必要なメタデータ通知 XML をテキストエディタで作成します。
    - XML を設定するにあたっては、デスティネーションとして検索統合エンドポイントの URN を使用します。

      オブジェクトはオブジェクト名のプレフィックスでフィルタリングできます。たとえば、プレフィックスがであるオブジェクトのメタデータをあるデスティネーションに送信し、プレフィックスがであるオブジェクトのメタデータを別のデスティネーション `videos`に送信できます `images`。プレフィックスが重複している設定は有効ではなく、送信時に拒否されます。たとえば、プレフィックスがのオブジェクト用のルールとプレフィックスがのオブジェクト用のルールを `test2`含む設定 `test`は許可されません。

      必要に応じて、を参照してメタデータ設定XMLの例ください。

```
<MetadataNotificationConfiguration>
 <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
       <Urn>/Urn>
       </Destination>
 </Rule>
</MetadataNotificationConfiguration>
```

メタデータ通知設定XMLの要素は次のとおりです。

名前	製品説明	必須
MetadataNotificationConfiguration のページです	メタデータ通知でオブジェクトとデスティネーションの指定に使用されるルール用のコンテナタグ。 1 つ以上の Rule 要素を含みます。	はい
ルール	指定したインデックスにメタデータを追加する必要があるオブジェクトを特定するルール用のコンテナタグ。 プレフィックスが重複しているルールは拒否されます。 MetadataNotificationConfiguration 要素に含まれています。	はい
ID	ルールの一意の識別子。 Rule 要素に含まれています。	いいえ
ステータス	Status には「 Enabled 」または「 Disabled 」を指定できます。無効になっているルールについては操作が実行されません。 Rule 要素に含まれています。	はい
プレフィックス	プレフィックスと一致するオブジェクトにルールが適用され、そのメタデータが指定したデスティネーションに送信されます。 すべてのオブジェクトを照合するには、空のプレフィックスを指定します。 Rule 要素に含まれています。	はい

名前	製品説明	必須
デスティネーション	ルールのデスティネーションのコンテナタグ。 Rule 要素に含まれています。	はい
URN	オブジェクトメタデータが送信されるデスティネーションの URN 。次のプロパティを持つ StorageGRID エンドポイントの URN を指定する必要があります。 • `es`3番目の要素である必要があります。 • URNは、メタデータが格納されるインデックスとタイプ（の形式）で終わる必要があります `domain-name/myindex/mytype`。 エンドポイントは、 Tenant Manager またはテナント管理 API を使用して設定します。形式は次のとおりです。 • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` エンドポイントは設定 XML を送信する前に設定する必要があります。そうしないと、 404 エラーで設定が失敗します。 Urn は Destination 要素に含まれています。	はい

2. Tenant Manager で、 * Storage （ S3 ） * > * Buckets * を選択します。
3. ソースバケットの名前を選択します。

   バケットの詳細ページが表示されます。

4. プラットフォームサービス > 検索統合 * を選択します
5. [検索統合を有効にする]*チェックボックスをオンにします。
6. テキストボックスにメタデータ通知設定を貼り付け、 * 変更を保存 * を選択します。

   StorageGRID 管理者がグリッドマネージャまたは管理 API を使用して各テナントアカウントのプラットフォームサービスを有効にしておく必要があります。設定 XML の保存時にエラーが発生した場合は、 StorageGRID 管理者にお問い合わせください。

7. 検索統合サービスが正しく設定されていることを確認します。
   a. 設定 XML で指定されたメタデータ通知をトリガーする要件を満たすオブジェクトをソースバケットに追加します。

      前述の例では、バケットに追加されたすべてのオブジェクトがメタデータ通知をトリガーします。

   b. オブジェクトのメタデータとタグを含む JSON ドキュメントが、エンドポイントで指定された検索インデックスに追加されたことを確認します。

終了後

必要に応じて、次のいずれかの方法でバケットの検索統合を無効にできます。

- Storage（S3）> Buckets を選択し、 Enable search integration *チェックボックスをオフにします。
- S3 API を直接使用している場合は、 DELETE Bucket メタデータ通知要求を使用します。S3 クライアントアプリケーションを実装する手順を参照してください。

例：すべてのオブジェクトに適用されるメタデータ通知設定

この例では、すべてのオブジェクトのオブジェクトメタデータが同じデスティネーションに送信されます。

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
           <Urn>urn:myes:es:::sgws-notifications/test1/all</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

例：**2**つのルールを使用したメタデータ通知の設定

この例では、プレフィックスに一致するオブジェクトのオブジェクトメタデータが `/images`1つ目のデスティネーションに送信され、プレフィックスに一致するオブジェクトのオブジェクトメタデータが `/videos`2つ目のデスティネーションに送信されます。

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Images-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/images</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Videos-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/videos</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

メタデータ通知の形式

バケットで検索統合サービスを有効にすると、オブジェクトのメタデータまたはタグの追加、更新、削除が行われるたびに、 JSON ドキュメントが生成されてデスティネーションエンドポイントに送信されます。

次の例は、という名前のバケットにキーを持つオブジェクトが作成され `test` たときに生成される `JSON` の例を示しています。 `SGWS/Tagging.txt` `test` バケットはバージョン管理されていないため `versionId` 、タグは空です。

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region":"us-east-1",
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

JSONドキュメントに含まれるフィールド

ドキュメント名には、バケット名、オブジェクト名、バージョン ID （存在する場合）が含まれます。

バケットとオブジェクトの情報

`bucket`：バケットの名前

`key`:オブジェクトキー名

`versionID`：オブジェクトのバージョン。バージョン管理されたバケット内のオブジェクトの場合

`region`：例：Bucket region `us-east-1`

システムメタデータ

`size`：HTTPクライアントに表示されるオブジェクトのサイズ（バイト）

`md5`:オブジェクトハッシュ

ユーザメタデータ

`metadata`：オブジェクトのすべてのユーザメタデータ（キーと値のペア）

`key:value`

タグ

`tags`：オブジェクトに定義されたすべてのオブジェクトタグ（キーと値のペア）

`key:value`

Elasticsearchで結果を表示する方法

タグとユーザメタデータの場合、 StorageGRID は文字列または S3 イベント通知として Elasticsearch に日付

と番号を渡します。これらの文字列を日付または数値として解釈するように Elasticsearch を設定するには、動的フィールドマッピングおよびマッピング日付形式に関する Elasticsearch の手順に従ってください。検索統合サービスを設定する前に、インデックスの動的フィールドマッピングを有効にします。ドキュメントのインデックス作成後は、インデックス内のドキュメントのフィールドタイプを編集することはできません。

S3 REST APIを使用する

StorageGRID S3 REST API でサポートされているバージョンとアップデート

StorageGRID は、 Representational State Transfer （ REST ）の Web サービスのセットとして実装される Simple Storage Service （ S3 ）をサポートします。

S3 REST APIのサポートにより、S3 Webサービス用に開発されたサービス指向アプリケーションを、StorageGRID システムを使用するオンプレミスのオブジェクトストレージに接続できます。クライアントアプリケーションで現在S3 REST API呼び出しを使用している場合は、変更を最小限に抑える必要があります。

サポートされるバージョン

StorageGRID は、STS、S3、HTTP の次の特定のバージョンをサポートしています。

項目	バージョン
STS AssumeRole API 仕様	"Amazon Web Services (AWS) ドキュメント: Amazon Assumerole API リファレンス" AssumeRoleの詳細については、以下を参照してください。"AssumeRoleを設定する" 。
S3 API仕様	"AWS ドキュメント: Amazon Simple Storage Service API リファレンス"
HTTP	1.1 HTTP の詳細については、 HTTP/1.1 （ RFC 7230~7235 ）を参照してください。 "IETF RFC 2616 ：『 Hypertext Transfer Protocol （ HTTP/1.1 ）』" • 注： StorageGRID は、 HTTP/1.1 パイプラインをサポートしません。

S3 REST APIのサポートが更新されました

リリース	コメント
12.1.0	• `If-Match` `If-Match`ヘッダーの動作は、StorageGRIDの構成によって異なります。このヘッダーを指定すると、エラーメッセージ（`501 Not Implemented`）が返される可能性があります。 `If-Match`ヘッダーが受け入れられたものの機能しない場合、より厳格な`501 Not Implemented`エラー動作を有効にするための手順を示すアラートが表示される可能性があります。 • `If-None-Match` `If-None-Match`ヘッダーの動作は、StorageGRIDの構成によって異なります。このヘッダーを指定すると、エラーメッセージ（`501 Not Implemented`）が返される可能性があります。 `If-None-Match`ヘッダーが受け入れられたものの機能しない場合、より厳格な`501 Not Implemented`エラー動作を有効にするための手順を示すアラートが表示される可能性があります。 • 以下のリクエストおよびサポートされているヘッダーに対して、事前計算されたチェックサム値のサポートを追加しました： ◦ CompleteMultipartUpload： `x-amz-checksum-crc32`、 `x-amz-checksum-crc32c`、および `x-amz-checksum-crc64nvme` ◦ CreateMultipartUpload： `CRC32`、 `CRC32C`、および `CRC64NVME`（`x-amz-checksum-algorithm`用） ◦ CopyObject： `CRC32`、 `CRC32C`、 `CRC64NVME`、および `SHA256`（`x-amz-checksum-algorithm`用） ◦ PutObject： `x-amz-checksum-crc32`、 `x-amz-checksum-crc32c`、および `x-amz-checksum-crc64nvme` ◦ UploadPart： `x-amz-checksum-crc32`、 `x-amz-checksum-crc32c`、および `x-amz-checksum-crc64nvme` • `x-amz-checksum-type`のCreateMultipartUploadおよびCompleteMultipartUploadのサポートを追加しました。 • `s3:x-amz-copy-source`ポリシー条件キーのサポートが追加されました。 • 既存のバケットで S3 オブジェクトロックを有効にできるようにします。

リリース	コメント
12.0	• 管理インターフェースのクロスオリジン リソース共有 (CORS) のサポートが追加されました。これにより、別のドメインが管理 API を使用してStorageGRID内のデータにアクセスできるようになります。"詳細" 。 • STS AssumeRole およびセッションポリシーのサポートを追加しました。"セッションポリシーの例" を参照してください。テナントグループごとに AssumeRole を設定できます。
11.9	• 次の要求およびサポートされるヘッダーについて、事前に計算されたSHA-256チェックサム値のサポートが追加されました。この機能を使用して、アップロードされたオブジェクトの整合性を検証できます。 ◦ CompleteMultipartUpload： `x-amz-checksum-sha256` ◦ CreateMultipartUpload： `x-amz-checksum-algorithm` ◦ GetObject： `x-amz-checksum-mode` ◦ HeadObject： `x-amz-checksum-mode` ◦ ListParts ◦ PutObject： `x-amz-checksum-sha256` ◦ アップロードパーツ： `x-amz-checksum-sha256` • グリッド管理者がテナントレベルの保持期間と準拠設定を制御できるようになりました。これらの設定はS3オブジェクトロックの設定に影響します。 ◦ バケットのデフォルトの保持モードとオブジェクトの保持モード：GovernanceまたはCompliance（グリッド管理者が許可している場合）。 ◦ バケットのデフォルトの保持期間およびオブジェクトのRetain Until Date：グリッド管理者が設定した最大保持期間の許容値以下にする必要があります。 • コンテンツエンコーディングとストリーミング `x-amz-content-sha256`値のサポートが改善されました `aws-chunked`。制限事項： ◦ 存在する場合は `chunk-signature`オプションで、検証されていません。 ◦ 存在する場合、 `x-amz-trailer`コンテンツは無視されます。
11.8	で使用されている名前に一致するようにS3処理の名前が更新されました "Amazon Web Services （ AWS ）ドキュメント：「 Amazon Simple Storage Service API Reference"。

リリース	コメント
11.7	• "クイックリファレンス：サポートされるS3 API要求"を追加しました。 • S3オブジェクトロックでのガバナンスモードの使用のサポートが追加されました。 • GET Object要求とHEAD Object要求のStorageGRID固有の応答ヘッダーのサポートが追加されました `x-ntap-sg-cgr-replication-status`。このヘッダーは、グリッド間レプリケーションのオブジェクトのレプリケーションステータスを示します。 • SelectObjectContent要求でParquetオブジェクトがサポートされるようになりました。
11.6	• GET Object要求とHEAD Object要求でrequestパラメータを使用できるようになりました `partNumber`。 • S3 オブジェクトロックのデフォルト保持モードとデフォルトの保持期間がバケットレベルでサポートされるようになりました。 • オブジェクトに許可される保持期間の範囲を設定するポリシー条件キーのサポートが追加されました `s3:object-lock-remaining-retention-days`。 • 単一のPUT Object処理のmaximum_recommended_sizeを5GiB（5、368、709、120バイト）に変更しました。5GB より大きいオブジェクトがある場合は、マルチパートアップロードを使用してください。
11.5	• バケットの暗号化の管理のサポートが追加されました。 • S3 オブジェクトのロックと廃止された従来の準拠要求のサポートを追加しました。 • バージョン管理されたバケットでの DELETE Multiple Objects の使用のサポートが追加されました。 • `Content-MD5`要求ヘッダーが正しくサポートされるようになりました。
11.4	• DELETE Bucket tagging 、 GET Bucket tagging 、 PUT Bucket tagging のサポートが追加されました。コスト割り当てタグはサポートされていません。 • StorageGRID 11.4 で作成されたバケットでは、オブジェクトキー名がパフォーマンスのベストプラクティスに適合するように制限する必要はなくなりました。 • イベントタイプでのバケット通知のサポートが追加されました `s3:ObjectRestore:Post`。 • マルチパートの AWS サイズの上限が適用されるようになりました。マルチパートアップロードの各パートのサイズは 5MiB から 5GiB の間にする必要があります。最後の部分は 5MiB より小さくすることができます。 • TLS 1.3のサポートが追加されました

リリース	コメント
11.3	• ユーザ指定のキーによるオブジェクトデータのサーバ側暗号化（ SSE-C ）がサポートされるようになりました。 • DELETE Bucket lifecycle、GET Bucket lifecycle、PUT Bucket lifecycleの各処理（Expirationアクションのみ）と応答ヘッダーのサポートが追加されました `x-amz-expiration`。 • PUT Object 、 PUT Object - Copy 、 Multipart Upload が更新されて、取り込み時に同期配置を使用する ILM ルールの影響を受けるようになりました。 • TLS 1.1 暗号はサポートされなくなりました。
11.2	クラウドストレージプールで POST Object restore を使用できるようになりました。グループポリシーとバケットポリシーの ARN 、ポリシー条件キー、およびポリシー変数で AWS 構文を使用できるようになりました。StorageGRID 構文を使用する既存のグループポリシーとバケットポリシーは引き続きサポートされます。 • 注：カスタム StorageGRID 機能で使用される ARN やその他の構成 JSON / XML での使用に変更はありませんでした。
11.1	Cross-Origin Resource Sharing（CORS）、グリッドノードへのS3クライアント接続でのHTTP、バケットでの準拠設定のサポートが追加されました。
11.0	バケットでのプラットフォームサービス（ CloudMirror レプリケーション、通知、および Elasticsearch 検索統合）の設定がサポートされるようになりました。また、バケットに対するオブジェクトタギングの場所の制約と「available」の整合性がサポートされるようになりました。
10.4	ILM スキャンのバージョン管理、エンドポイントドメインの名前ページの更新、ポリシーの条件と変数、ポリシーの例、および PutOverwriteObject 権限の変更のサポートが追加されました。
10.3	バージョン管理のサポートが追加されました。
10.2	グループとバケットのアクセスポリシー、およびマルチパートコピー（ Upload Part - Copy ）のサポートが追加されました。
10.1	マルチパートアップロード、仮想ホスト型リクエスト、およびv4認証のサポートを追加しました。
10.0	StorageGRIDシステムによる S3 REST API の初期サポート。現在サポートされている *Simple Storage Service API* リファレンス のバージョンは 2006-03-01 です。

StorageGRID でサポートされている S3 API リクエスト

このページでは、StorageGRID がAmazon Simple Storage Service（S3）APIをどのようにサポートしているかをまとめます。

このページには、StorageGRID でサポートされている S3 操作のみが記載されています。リストに記載されていない S3 操作は、 `501 Not Implemented`が返されるか、意図しない動作が発生する可能性があります。

各処理のAWSドキュメントを参照するには、見出しのリンクを選択します。

一般的な**URI**クエリパラメータと要求ヘッダー

特に記載がない限り、次の一般的なURIクエリパラメータがサポートされます。

- `versionId`（オブジェクトの処理に必要な場合）

特に記載がないかぎり、次の一般的な要求ヘッダーがサポートされます。

- `Authorization`
- `Connection`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Date`
- `Expect`
- `Host`
- `x-amz-date`

関連情報

- "S3 REST APIの実装の詳細"
- "Amazon Simple Storage Service API Reference：Common Request Headers"

"AbortMultipartUpload"

URIクエリパラメータと要求ヘッダー

StorageGRIDでは、この要求のすべてに加えて、次の追加のURIクエリパラメータがサポートされ共通のパラメータとヘッダーます。

- `uploadId`

リクエストの本文

なし

StorageGRID のドキュメント

"マルチパートアップロードの処理"

"CompleteMultipartUpload"

URIクエリパラメータと要求ヘッダー

StorageGRIDでは、この要求のすべてに加えて、次の追加のURIクエリパラメータがサポートされ共通のパラ

メータとヘッダーます。

- uploadId
- x-amz-checksum-crc32
- x-amz-checksum-crc32c
- x-amz-checksum-crc64nvme
- x-amz-checksum-sha256
- x-amz-checksum-type
- x-amz-storage-class

本文**XML**タグを要求します

StorageGRID は、次の要求本文XMLタグをサポートしています。

- ChecksumCRC32
- ChecksumCRC32C
- ChecksumCRC64NVME
- ChecksumSHA256
- CompleteMultipartUpload
- ETag
- Part
- PartNumber

StorageGRID のドキュメント

"CompleteMultipartUpload"

"CopyObject"

URIクエリパラメータと要求ヘッダー

StorageGRIDは、この要求のすべてに加えて、次の追加ヘッダーをサポートし共通のパラメータとヘッダーます。

- x-amz-checksum-algorithm
- x-amz-copy-source
- x-amz-copy-source-if-match
- x-amz-copy-source-if-modified-since
- x-amz-copy-source-if-none-match
- x-amz-copy-source-if-unmodified-since
- x-amz-copy-source-server-side-encryption-customer-algorithm
- x-amz-copy-source-server-side-encryption-customer-key
- x-amz-copy-source-server-side-encryption-customer-key-MD5

- `x-amz-metadata-directive`
- `x-amz-object-lock-legal-hold`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-server-side-encryption`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-storage-class`
- `x-amz-tagging`
- `x-amz-tagging-directive`
- `x-amz-meta-<metadata-name>`

リクエストの本文

なし

StorageGRID のドキュメント

"CopyObject"

"CreateBucket"

URIクエリパラメータと要求ヘッダー

StorageGRIDは、この要求のすべてに加えて、次の追加ヘッダーをサポートし共通のパラメータとヘッダーます。

- `x-amz-bucket-object-lock-enabled`

リクエストの本文

StorageGRID は、実装時にAmazon S3 REST APIで定義されたすべての要求本文パラメータをサポートします。

StorageGRID のドキュメント

"バケットの処理"

"CreateMultipartUpload"

URIクエリパラメータと要求ヘッダー

StorageGRIDは、この要求のすべてに加えて、次の追加ヘッダーをサポートし共通のパラメータとヘッダーます。

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`

- `Content-Language`
- `Expires`
- `x-amz-checksum-algorithm`
- `x-amz-checksum-type`
- `x-amz-server-side-encryption`
- `x-amz-storage-class`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-tagging`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`
- `x-amz-meta-<metadata-name>`

リクエストの本文

なし

StorageGRID のドキュメント

"CreateMultipartUpload"

"DeleteBucket"

URIクエリパラメータと要求ヘッダー

StorageGRIDはこの要求に対してすべてをサポートします共通のパラメータとヘッダー。

StorageGRID のドキュメント

"バケットの処理"

"DeleteBucketCors"

URIクエリパラメータと要求ヘッダー

StorageGRIDはこの要求に対してすべてをサポートします共通のパラメータとヘッダー。

リクエストの本文

なし

StorageGRID のドキュメント

"バケットの処理"

"DeleteBucketEncryption"

URIクエリパラメータと要求ヘッダー

StorageGRIDはこの要求に対してすべてをサポートします共通のパラメータとヘッダー。

リクエストの本文

なし

StorageGRID のドキュメント

"バケットの処理"

"DeleteBucketLifecycle"

URIクエリパラメータと要求ヘッダー

StorageGRIDはこの要求に対してすべてをサポートします共通のパラメータとヘッダー。

リクエストの本文

なし

StorageGRID のドキュメント

- "バケットの処理"
- "S3 ライフサイクル設定を作成する"

"DeleteBucketPolicy"

URIクエリパラメータと要求ヘッダー

StorageGRIDはこの要求に対してすべてをサポートします共通のパラメータとヘッダー。

リクエストの本文

なし

StorageGRID のドキュメント

"バケットの処理"

"DeleteBucketReplication"

URIクエリパラメータと要求ヘッダー

StorageGRIDはこの要求に対してすべてをサポートします共通のパラメータとヘッダー。

リクエストの本文

なし

StorageGRID のドキュメント

"バケットの処理"

"DeleteBucketTagging"

URIクエリパラメータと要求ヘッダー

StorageGRIDはこの要求に対してすべてをサポートします共通のパラメータとヘッダー。

リクエストの本文

なし

StorageGRID のドキュメント

"バケットの処理"

"deleteObject"

URIクエリパラメータと要求ヘッダー

StorageGRIDは、この要求のすべてに加えて、次の追加要求ヘッダーをサポートし共通のパラメータとヘッダーます。

- `x-amz-bypass-governance-retention`

リクエストの本文

なし

StorageGRID のドキュメント

"オブジェクトの処理"

"オブジェクトの削除"

URIクエリパラメータと要求ヘッダー

StorageGRIDは、この要求のすべてに加えて、次の追加要求ヘッダーをサポートし共通のパラメータとヘッダーます。

- `x-amz-bypass-governance-retention`

リクエストの本文

StorageGRID は、実装時にAmazon S3 REST APIで定義されたすべての要求本文パラメータをサポートします。

StorageGRID のドキュメント

"オブジェクトの処理"

"DeleteObjectTagging"

StorageGRIDはこの要求に対してすべてをサポートします共通のパラメータとヘッダー。

リクエストの本文

なし

StorageGRID のドキュメント

"オブジェクトの処理"

"GetBucketAcl"

URIクエリパラメータと要求ヘッダー

StorageGRIDはこの要求に対してすべてをサポートします共通のパラメータとヘッダー。

リクエストの本文

なし

StorageGRID のドキュメント

"バケットの処理"

"GetBucketCors"

URIクエリパラメータと要求ヘッダー

StorageGRIDはこの要求に対してすべてをサポートします共通のパラメータとヘッダー。

リクエストの本文

なし

StorageGRID のドキュメント

"バケットの処理"

"GetBucketEncryptionの略"

URIクエリパラメータと要求ヘッダー

StorageGRIDはこの要求に対してすべてをサポートします共通のパラメータとヘッダー。

リクエストの本文

なし

StorageGRID のドキュメント

"バケットの処理"

"GetBucketLifecycleConfiguration"

URIクエリパラメータと要求ヘッダー

StorageGRIDはこの要求に対してすべてをサポートします共通のパラメータとヘッダー。

リクエストの本文

なし

StorageGRID のドキュメント

- "バケットの処理"
- "S3 ライフサイクル設定を作成する"

"GetBucketLocation"

URIクエリパラメータと要求ヘッダー

StorageGRIDはこの要求に対してすべてをサポートします共通のパラメータとヘッダー。

リクエストの本文

なし

StorageGRID のドキュメント

"バケットの処理"

"GetBucketNotificationConfigurationを参照してください"

URIクエリパラメータと要求ヘッダー

StorageGRIDはこの要求に対してすべてをサポートします共通のパラメータとヘッダー。

リクエストの本文

なし

StorageGRID のドキュメント

"バケットの処理"

"GetBucketPolicy"

URIクエリパラメータと要求ヘッダー

StorageGRIDはこの要求に対してすべてをサポートします共通のパラメータとヘッダー。

リクエストの本文

なし

StorageGRID のドキュメント

"バケットの処理"

"GetBucketReplicationの略"

URIクエリパラメータと要求ヘッダー

StorageGRIDはこの要求に対してすべてをサポートします共通のパラメータとヘッダー。

リクエストの本文

なし

StorageGRID のドキュメント

"バケットの処理"

"GetBucketTagging"

URIクエリパラメータと要求ヘッダー

StorageGRIDはこの要求に対してすべてをサポートします共通のパラメータとヘッダー。

リクエストの本文

なし

StorageGRID のドキュメント

"バケットの処理"

"GetBucketVersioning"

URIクエリパラメータと要求ヘッダー

StorageGRIDはこの要求に対してすべてをサポートします共通のパラメータとヘッダー。

リクエストの本文

なし

StorageGRID のドキュメント

"バケットの処理"

"GetObject"

URIクエリパラメータと要求ヘッダー

StorageGRIDでは、この要求のすべてに加えて、次の追加のURIクエリパラメータがサポートされ共通のパラメータとヘッダーます。

- `x-amz-checksum-mode`
- `partNumber`
- `response-cache-control`
- `response-content-disposition`
- `response-content-encoding`
- `response-content-language`
- `response-content-type`
- `response-expires`

追加の要求ヘッダーは次のとおりです。

- `Range`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `If-Match`
- `If-Modified-Since`
- `If-None-Match`
- `If-Unmodified-Since`

リクエストの本文
なし

StorageGRID のドキュメント
"GetObject"

"GetObjectAcl"

URIクエリパラメータと要求ヘッダー
StorageGRIDはこの要求に対してすべてをサポートします共通のパラメータとヘッダー。

リクエストの本文
なし

StorageGRID のドキュメント
"オブジェクトの処理"

"GetObjectLegalHold"

URIクエリパラメータと要求ヘッダー
StorageGRIDはこの要求に対してすべてをサポートします共通のパラメータとヘッダー。

リクエストの本文
なし

StorageGRID のドキュメント
"S3 REST APIを使用してS3オブジェクトロックを設定します"

"GetObjectLockConfigurationの略"

URIクエリパラメータと要求ヘッダー
StorageGRIDはこの要求に対してすべてをサポートします共通のパラメータとヘッダー。

リクエストの本文
なし

StorageGRID のドキュメント
"S3 REST APIを使用してS3オブジェクトロックを設定します"

"GetObjectRetention"

URIクエリパラメータと要求ヘッダー
StorageGRIDはこの要求に対してすべてをサポートします共通のパラメータとヘッダー。

リクエストの本文
なし

StorageGRID のドキュメント

"S3 REST APIを使用してS3オブジェクトロックを設定します"

"GetObjectTagging"

URIクエリパラメータと要求ヘッダー

StorageGRIDはこの要求に対してすべてをサポートします共通のパラメータとヘッダー。

リクエストの本文

なし

StorageGRID のドキュメント

"オブジェクトの処理"

"ヘッドバケット"

URIクエリパラメータと要求ヘッダー

StorageGRIDはこの要求に対してすべてをサポートします共通のパラメータとヘッダー。

リクエストの本文

なし

StorageGRID のドキュメント

"バケットの処理"

"ヘッドオブジェクト"

URIクエリパラメータと要求ヘッダー

StorageGRIDは、この要求のすべてに加えて、次の追加ヘッダーをサポートし共通のパラメータとヘッダーます。

- `x-amz-checksum-mode`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `If-Match`
- `If-Modified-Since`
- `If-None-Match`
- `If-Unmodified-Since`
- `Range`

リクエストの本文

なし

StorageGRID のドキュメント

"ヘッドオブジェクト"

"ListBuckets"

URIクエリパラメータと要求ヘッダー

StorageGRIDはこの要求に対してすべてをサポートします共通のパラメータとヘッダー。

リクエストの本文

なし

StorageGRID のドキュメント

"サービス> ListBucketsの操作"

"ListMultipartUploads"

URIクエリパラメータと要求ヘッダー

StorageGRIDは、この要求のすべてに加えて、次の追加パラメータをサポートし共通のパラメータとヘッダーます。

- `encoding-type`
- `key-marker`
- `max-uploads`
- `prefix`
- `upload-id-marker`

リクエストの本文

なし

StorageGRID のドキュメント

"ListMultipartUploads"

"ListObjects"

URIクエリパラメータと要求ヘッダー

StorageGRIDは、この要求のすべてに加えて、次の追加パラメータをサポートし共通のパラメータとヘッダーます。

- `delimiter`
- `encoding-type`
- `marker`
- `max-keys`
- `prefix`

リクエストの本文

なし

StorageGRID のドキュメント

"バケットの処理"

"ListObjectsV2"

URIクエリパラメータと要求ヘッダー

StorageGRIDは、この要求のすべてに加えて、次の追加パラメータをサポートし共通のパラメータとヘッダーます。

- `continuation-token`
- `delimiter`
- `encoding-type`
- `fetch-owner`
- `max-keys`
- `prefix`
- `start-after`

リクエストの本文

なし

StorageGRID のドキュメント

"バケットの処理"

"ListObjectVersions"

URIクエリパラメータと要求ヘッダー

StorageGRIDは、この要求のすべてに加えて、次の追加パラメータをサポートし共通のパラメータとヘッダーます。

- `delimiter`
- `encoding-type`
- `key-marker`
- `max-keys`
- `prefix`
- `version-id-marker`

リクエストの本文

なし

StorageGRID のドキュメント

"バケットの処理"

"ListParts"

URIクエリパラメータと要求ヘッダー

StorageGRIDは、この要求のすべてに加えて、次の追加パラメータをサポートし共通のパラメータとヘッダーます。

- `max-parts`
- `part-number-marker`
- `uploadId`

リクエストの本文

なし

StorageGRID のドキュメント

"ListMultipartUploads"

"PutBucketCorsの略"

URIクエリパラメータと要求ヘッダー

StorageGRIDはこの要求に対してすべてをサポートします共通のパラメータとヘッダー。

リクエストの本文

StorageGRID は、実装時にAmazon S3 REST APIで定義されたすべての要求本文パラメータをサポートします。

StorageGRID のドキュメント

"バケットの処理"

"PutBucketEncryptionの略"

URIクエリパラメータと要求ヘッダー

StorageGRIDはこの要求に対してすべてをサポートします共通のパラメータとヘッダー。

本文**XML**タグを要求します

StorageGRID は、次の要求本文XMLタグをサポートしています。

- `ApplyServerSideEncryptionByDefault`
- `Rule`
- `ServerSideEncryptionConfiguration`
- `SSEAlgorithm`

StorageGRID のドキュメント

"バケットの処理"

"PutBucketLifecycleConfiguration"

URIクエリパラメータと要求ヘッダー

StorageGRIDはこの要求に対してすべてをサポートします共通のパラメータとヘッダー。

本文**XML**タグを要求します

StorageGRID は、次の要求本文XMLタグをサポートしています。

- `And`
- `Days`
- `Expiration`
- `ExpiredObjectDeleteMarker`
- `Filter`
- `ID`
- `Key`
- `LifecycleConfiguration`
- `NewerNoncurrentVersions`
- `NoncurrentDays`
- `NoncurrentVersionExpiration`
- `Prefix`
- `Rule`
- `Status`
- `Tag`
- `Value`

StorageGRID のドキュメント

- "バケットの処理"
- "S3 ライフサイクル設定を作成する"

"PutBucketNotificationConfigurationの略"

URIクエリパラメータと要求ヘッダー

StorageGRIDはこの要求に対してすべてをサポートします共通のパラメータとヘッダー。

本文**XML**タグを要求します

StorageGRID は、次の要求本文XMLタグをサポートしています。

- `Event`
- `Filter`
- `FilterRule`

- `Id`
- `Name`
- `NotificationConfiguration`
- `Prefix`
- `S3Key`
- `Suffix`
- `Topic`
- `TopicConfiguration`
- `Value`

StorageGRID のドキュメント

"バケットの処理"

"PutBucketPolicy"

URIクエリパラメータと要求ヘッダー

StorageGRIDはこの要求に対してすべてをサポートします共通のパラメータとヘッダー。

リクエストの本文

サポートされているJSON本体フィールドの詳細については、以下を参照してください。"バケットとグループのアクセスポリシーを使用" 。

"PutBucketReplicationの略"

URIクエリパラメータと要求ヘッダー

StorageGRIDはこの要求に対してすべてをサポートします共通のパラメータとヘッダー。

本文**XML**タグを要求します

- `Bucket`
- `Destination`
- `Prefix`
- `ReplicationConfiguration`
- `Rule`
- `Status`
- `StorageClass`

StorageGRID のドキュメント

"バケットの処理"

"PutBucketTaggingの略"

URIクエリパラメータと要求ヘッダー

StorageGRIDはこの要求に対してすべてをサポートします共通のパラメータとヘッダー。

リクエストの本文

StorageGRID は、実装時にAmazon S3 REST APIで定義されたすべての要求本文パラメータをサポートします。

StorageGRID のドキュメント

"バケットの処理"

"PutBucketVersioning"

URIクエリパラメータと要求ヘッダー

StorageGRIDはこの要求に対してすべてをサポートします共通のパラメータとヘッダー。

本文パラメータを要求します

StorageGRID は、次の要求本文パラメータをサポートしています。

- `VersioningConfiguration`
- `Status`

StorageGRID のドキュメント

"バケットの処理"

"PutObject"

URIクエリパラメータと要求ヘッダー

StorageGRIDは、この要求のすべてに加えて、次の追加ヘッダーをサポートし共通のパラメータとヘッダーます。

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-checksum-crc32`
- `x-amz-checksum-crc32c`
- `x-amz-checksum-crc64nvme`
- `x-amz-checksum-sha256`
- `x-amz-server-side-encryption`
- `x-amz-storage-class`
- `x-amz-server-side-encryption-customer-algorithm`

- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-tagging`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`
- `x-amz-meta-<metadata-name>`

リクエストの本文

- オブジェクトのバイナリデータ

StorageGRID のドキュメント

"PutObject"

"PutObjectLegalHold"

URIクエリパラメータと要求ヘッダー

StorageGRIDはこの要求に対してすべてをサポートします共通のパラメータとヘッダー。

リクエストの本文

StorageGRID は、実装時にAmazon S3 REST APIで定義されたすべての要求本文パラメータをサポートします。

StorageGRID のドキュメント

"S3 REST APIを使用してS3オブジェクトロックを設定します"

"PutObjectLockConfiguration"

URIクエリパラメータと要求ヘッダー

StorageGRID は、このリクエストに対して_ほとんどの_共通のパラメータとヘッダーをサポートしています。

リクエストの本文

StorageGRID は、実装時点で Amazon S3 REST API によって定義されたリクエストボディパラメータの_ほとんど_をサポートしていますが、以下の例外があります：

グリッド管理者から許可が与えられていない限り、PutObjectLockConfiguration を使用して既存のバケットで S3 オブジェクトロックを有効にすることはできません。

StorageGRID のドキュメント

"S3 REST APIを使用してS3オブジェクトロックを設定します"

"PutObjectRetention"

URIクエリパラメータと要求ヘッダー

StorageGRIDは、この要求のすべてに加えて、次の追加ヘッダーをサポートし共通のパラメータとヘッダーます。

- `x-amz-bypass-governance-retention`

リクエストの本文

StorageGRID は、実装時にAmazon S3 REST APIで定義されたすべての要求本文パラメータをサポートします。

StorageGRID のドキュメント

"S3 REST APIを使用してS3オブジェクトロックを設定します"

"PutObjectTagging"

URIクエリパラメータと要求ヘッダー

StorageGRIDはこの要求に対してすべてをサポートします共通のパラメータとヘッダー。

リクエストの本文

StorageGRID は、実装時にAmazon S3 REST APIで定義されたすべての要求本文パラメータをサポートします。

StorageGRID のドキュメント

"オブジェクトの処理"

"RestoreObject"

URIクエリパラメータと要求ヘッダー

StorageGRIDはこの要求に対してすべてをサポートします共通のパラメータとヘッダー。

リクエストの本文

サポートされている本文フィールドの詳細については、を参照してください"RestoreObject"。

"SelectObjectContent の順に選択します"

URIクエリパラメータと要求ヘッダー

StorageGRIDはこの要求に対してすべてをサポートします共通のパラメータとヘッダー。

リクエストの本文

サポートされている本文フィールドの詳細については、以下を参照してください。

- "S3 Select を使用する"
- "SelectObjectContent の順に選択します"

"パーツのアップロード"

URIクエリパラメータと要求ヘッダー

StorageGRIDでは、この要求のすべてに加えて、次の追加のURIクエリパラメータがサポートされ共通のパラメータとヘッダーます。

- `partNumber`
- `uploadId`

追加の要求ヘッダーは次のとおりです。

- `x-amz-checksum-crc32`
- `x-amz-checksum-crc32c`
- `x-amz-checksum-crc64nvme`
- `x-amz-checksum-sha256`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`

リクエストの本文

- 部品のバイナリデータ

StorageGRID のドキュメント

"パーツのアップロード"

"パーツコピーをアップロード"

URIクエリパラメータと要求ヘッダー

StorageGRIDでは、この要求のすべてに加えて、次の追加のURIクエリパラメータがサポートされ共通のパラメータとヘッダーます。

- `partNumber`
- `uploadId`

追加の要求ヘッダーは次のとおりです。

- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-modified-since`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-range`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-copy-source-server-side-encryption-customer-algorithm`
- `x-amz-copy-source-server-side-encryption-customer-key`
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`

リクエストの本文

なし

StorageGRID のドキュメント

"パーツコピーをアップロード"

StorageGRID S3 REST API 構成をテストします

Amazon Web Servicesコマンドラインインターフェイス（AWS CLI）を使用して、システムへの接続をテストし、オブジェクトの読み取りと書き込みが可能であることを確認できます。

開始する前に

- からAWS CLIをダウンロードしてインストールしておき "aws.amazon.com/cli"ます。
- 必要に応じて、を指定します"ロードバランサエンドポイントを作成しました"。それ以外の場合は、接続するストレージノードのIPアドレスと使用するポート番号がわかっている必要があります。を参照して " クライアント接続用のIPアドレスとポート"
- そうだな "S3テナントアカウントが作成されました"
- テナントとにサインインしておき"アクセスキーの作成"ます。

これらの手順の詳細については、を参照してください"クライアント接続を設定します"。

手順

1. StorageGRID システムで作成したアカウントを使用するようにAWS CLIを設定します。
   a. 構成モードに切り替えます。 `aws configure`
   b. 作成したアカウントのアクセスキーIDを入力します。
   c. 作成したアカウントのシークレットアクセスキーを入力します。
   d. 使用するデフォルトのリージョンを入力します。たとえば、 `us-east-1`です。
   e. 使用するデフォルトの出力形式を入力するか、 * Enter * キーを押して JSON を選択します。
2. バケットを作成します。

   この例では、IPアドレス10.96.101.17とポート10443を使用するようにロードバランサエンドポイントが設定されていると想定しています。

   ```
   aws s3api --endpoint-url https://10.96.101.17:10443
   --no-verify-ssl create-bucket --bucket testbucket
   ```

   バケットの作成が完了すると、次の例のようにバケットの場所が返されます。

   ```
   "Location": "/testbucket"
   ```

3. オブジェクトをアップロードします。

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
put-object --bucket testbucket --key s3.pdf --body C:\s3-
test\upload\s3.pdf
```

オブジェクトのアップロードが完了すると、オブジェクトデータのハッシュである Etag が返されます。

4. バケットの内容をリストして、オブジェクトがアップロードされたことを確認します。

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
list-objects --bucket testbucket
```

5. オブジェクトを削除します。

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-object --bucket testbucket --key s3.pdf
```

6. バケットを削除します。

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-bucket --bucket testbucket
```

StorageGRID での S3 REST API の実装

StorageGRID S3 REST APIが競合するクライアント要求を解決する方法

同じキーに書き込む 2 つのクライアントなど、競合するクライアント要求は、「 latest-wins 」ベースで解決されます。

「 latest-wins 」評価は、 S3 クライアントが処理を開始するタイミングではなく、 StorageGRID システムが特定の要求を完了したタイミングで行われます。

StorageGRID S3 REST APIが可用性と一貫性のバランスをとる方法

整合性では、オブジェクトの可用性と、異なるストレージノードおよびサイト間でのオブジェクトの整合性のバランスが維持されます。アプリケーションの必要に応じて整合性を変更できます。

デフォルトでは、 StorageGRID は新しく作成されたオブジェクトの書き込み後の読み取り一貫性を保証します。正常に完了した PUT に続く GET では、新しく書き込まれたデータを読み取ることができます。既存のオブジェクトの上書き、メタデータの更新、および削除は、最終的に一貫性が保たれます。

別の整合性でオブジェクトの処理を実行する場合は、次の操作を実行できます。

- 一貫性を指定する各バケット。
- の整合性を指定し各API処理ます。
- 次のいずれかのタスクを実行して、グリッド全体のデフォルトの整合性を変更します。
  - グリッド マネージャーで、構成 > システム > ストレージ設定 > デフォルトのバケット一貫性 に移動します。
  - です。

> グリッド全体の整合性に対する変更は、設定の変更後に作成されたバケットにのみ適用されます。変更の詳細を確認するには、にある監査ログを参照して `/var/local/log`ください（* consistencyLevel *を検索）。

整合性の値

一貫性は、 StorageGRID がオブジェクトを追跡するために使用するメタデータがノード間でどのように分散されるかに影響します。一貫性は、クライアント要求に対するオブジェクトの可用性に影響します。

バケットまたはAPI処理の整合性は、次のいずれかの値に設定できます。

- * all *：すべてのノードがオブジェクトメタデータをただちに受信しないと要求が失敗します。
- 強力なグローバル: すべてのサイトにわたるすべてのクライアント要求の書き込み後の読み取り一貫性を保証します。クォーラム セマンティクスが構成されている場合、次の動作が適用されます。
  - グリッドに 3 つ以上のサイトがある場合、クライアント要求に対するサイト障害許容度を許可します。 2 サイト グリッドではサイト障害の許容度はありません。
  - 1 つのサイトがダウンすると、次の S3 操作は成功しません。
    - DeleteBucketEncryption
    - PutBucketBranch
    - PutBucketEncryptionの略
    - PutBucketVersioning
    - PutObjectLegalHold
    - PutObjectLockConfiguration
    - PutObjectRetention

  必要であれば、 "強力なグローバル整合性を実現するStorageGRID Quorumセマンティクスを構成する" 。
- * strong-site *：オブジェクトメタデータがサイト内の他のノードにただちに分散されます。1 つのサイト内のすべてのクライアント要求について、リードアフターライト整合性が保証されます。
- * Read-after-new-write *：新規オブジェクトにはリードアフターライト整合性を提供し、オブジェクトの更新には結果整合性を提供します。高可用性が確保され、データ保護が保証されます。ほとんどの場合に推奨されます。
- * available *：新しいオブジェクトとオブジェクトの更新の両方について、結果整合性を提供します。S3 バケットの場合は、必要な場合にのみ使用します（読み取り頻度の低いログ値を含むバケットや、存在しないキーに対するHEAD処理やGET処理など）。S3 FabricPool バケットではサポートされません。

「Read-after-new-write」整合性と「available」整合性を使用

HEAD処理またはGET処理で「Read-after-new-write」整合性が使用されている場合、StorageGRIDは次のように複数の手順で検索を実行します。

- まず、低い整合性レベルを使用してオブジェクトを検索します。
- そのルックアップが失敗すると、次の整合性値でルックアップが繰り返され、strong-globalの動作と同等の整合性が得られるようになります。

HEAD処理またはGET処理で「Read-after-new-write」整合性が使用されているが、オブジェクトが存在しない場合、オブジェクト検索の整合性は常にstrong-globalの動作と同じになります。この整合性のためには、オブジェクトメタデータのコピーが各サイトで複数ある必要があるため、同じサイトで使用できないストレージノードが複数ある場合に「500 Internal Server Error」が大量に発生する可能性があります。

Amazon S3と同様の整合性の保証が必要ないかぎり、整合性を「available」に設定することで、HEAD処理とGET処理でのこれらのエラーを回避できます。HEAD処理またはGET処理で「available」整合性が使用されている場合、StorageGRIDでは結果整合性のみが提供されます。整合性が向上しても失敗した処理が再試行されることはないため、オブジェクトメタデータのコピーが複数ある必要はありません。

[api-operation-consistency-control]] API処理の整合性を指定します。

個 々 のAPI処理に対して整合性を設定するには、処理でサポートされている整合性の値を要求ヘッダーで指定する必要があります。この例では、GetObject処理の整合性を「strong-site」に設定しています。

```
GET /bucket/object HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Consistency-Control: strong-site
```

PutObject処理とGetObject処理では、同じ整合性を使用する必要があります。

バケットの一貫性を指定する

バケットに整合性を設定するには、StorageGRID要求を使用し"PUT Bucket consistency"ます。または、Tenant Managerから実行することもできます"バケットの整合性を変更する"。

バケットに整合性を設定する場合は、次の点に注意してください。

- バケットに整合性を設定することで、バケット内のオブジェクトまたはバケット設定に対して実行されるS3処理に使用する整合性が決まります。バケット自体に対する処理には影響しません。
- 個 々 のAPI処理の整合性がバケットの整合性よりも優先されます。
- 通常、バケットではデフォルト整合性の「Read-after-new-write」を使用する必要があります。要求が正しく動作しない場合は、可能であればアプリケーションクライアントの動作を変更します。または、API要求ごとに整合性を指定するようにクライアントを設定します。バケットレベルの整合性は最後の手段として設定してください。

一貫性とILMルールの相互作用がデータ保護にどのように影響するか

選択した整合性とILMルールは、どちらもオブジェクトの保護方法に影響します。これらの設定は対話的に操作できます。

たとえば、オブジェクトの格納時に使用される整合性はオブジェクトメタデータの初期配置に影響し、ILMルールで選択された取り込み動作はオブジェクトコピーの初期配置に影響します。StorageGRIDでは、クライアント要求に対応するためにオブジェクトのメタデータとそのデータの両方にアクセスする必要があるため、整合性と取り込み動作で同じ保護レベルを選択すると、初期データ保護が向上し、システム応答の予測性が向上します。

ILMルールで使用できる項目は次の"取り込みオプション"とおりです。

デュアルコミット

StorageGRIDはオブジェクトの中間コピーをただちに作成し、クライアントに成功を返します。可能な場合は、 ILM ルールで指定されたコピーが作成されます。

strict

クライアントに成功が返される前に、ILMルールで指定されたすべてのコピーが作成されている必要があります。

バランス

StorageGRIDは、取り込み時にILMルールで指定されたすべてのコピーの作成を試みます。作成できない場合は中間コピーが作成され、クライアントに成功が返されます。可能な場合は、 ILM ルールで指定されたコピーが作成されます。

整合性とILMルールの相互作用の例

次の ILM ルールと次の一貫性を持つ 3 つのサイト グリッドがあるとします。

- **ILM** ルール: ローカル サイトに 1 つ、各リモート サイトに 1 つ、合計 3 つのオブジェクト コピーを作成します。厳密な取り込み動作を使用します。
- 一貫性: 強力なグローバル (オブジェクト メタデータは複数のサイトに即座に配布されます)。

クライアントがオブジェクトをグリッドに保存すると、 StorageGRID は3 つのオブジェクト コピーをすべて作成し、メタデータを複数のサイトに配布してから、クライアントに成功を返します。

オブジェクトは、取り込み成功メッセージの時点で損失から完全に保護されます。たとえば、取り込み直後にローカル サイトが失われた場合でも、オブジェクト データとオブジェクト メタデータの両方のコピーがリモート サイトに残ります。オブジェクトは他のサイトから完全に取得可能です。

代わりに同じ ILM ルールと強力なサイト一貫性を使用した場合、オブジェクト データがリモート サイトにレプリケートされた後、オブジェクト メタデータがそこに配布される前に、クライアントは成功メッセージを受信する可能性があります。この場合、オブジェクト メタデータの保護レベルは、オブジェクト データの保護レベルと一致しません。取り込み直後にローカル サイトが失われた場合、オブジェクト メタデータは失われます。オブジェクトを取得できません。

整合性ルールとILMルールの関係は複雑になる可能性があります。サポートが必要な場合は、NetAppにお問い合わせください。

StorageGRIDでのオブジェクトバージョン管理の使用方法

各オブジェクトの複数のバージョンを保持する場合は、バケットのバージョン管理状態を設定できます。バケットのバージョン管理を有効にすると、オブジェクトが誤って削除されないように保護したり、以前のバージョンのオブジェクトを読み出してリストアしたりできます。

StorageGRID システムでは、バージョン管理のほとんどの機能をサポートしていますが、いくつかの制限事項があります。StorageGRIDでは、オブジェクトごとに最大10、000個のバージョンがサポートされます。

オブジェクトのバージョン管理は、 StorageGRID の情報ライフサイクル管理（ ILM ）または S3 バケットのライフサイクル設定と組み合わせることができます。バージョン管理はバケットごとに明示的に有効にする必要があります。バケットでバージョン管理を有効にすると、バケットに追加される各オブジェクトにバージョンIDが割り当てられ、このIDがStorageGRIDシステムによって生成されます。

MFA （多要素認証） Delete の使用はサポートされていません。

> バージョン管理は、 StorageGRID バージョン 10.3 以降で作成されたバケットでのみ有効にすることができます。

ILM とバージョン管理

ILM ポリシーはオブジェクトの各バージョンに適用されます。ILM のスキャン処理では、すべてのオブジェクトが継続的にスキャンされ、現在の ILM ポリシーに照らして再評価されます。ILM ポリシーに対する変更は、それまでに取り込まれたすべてのオブジェクトに適用されます。バージョン管理が有効になっている場合は、それまでに取り込まれたバージョンも対象にILM のスキャン処理により、過去に取り込まれたオブジェクトに変更後の新しい ILM の内容が適用さ

バージョン管理が有効なバケット内のS3オブジェクトについては、バージョン管理のサポートにより、参照時間に「noncurrent time」を使用するILMルールを作成できます（の「Apply this rule to older object versions only？」という質問に対して* Yes *を選択します"ILMルール作成ウィザードのステップ1"）。オブジェクトが更新されると、それまでのバージョンは noncurrent になります。「noncurrent time」フィルタを使用すると、以前のバージョンのオブジェクトによるストレージへの影響を軽減するポリシーを作成できます。

> マルチパートアップロード処理を使用してオブジェクトの新しいバージョンをアップロードすると、オブジェクトの元のバージョンの noncurrent の時間には、マルチパートアップロードの完了時ではなく、新しいバージョンのマルチパートアップロードが作成された時点が反映されます。ただし、オリジナルバージョンの最新でない時間は、現行バージョンの時間よりも数時間 ~ 数日早い場合があります。

関連情報

- "S3 バージョン管理オブジェクトの削除方法"
- "S3 バージョン管理オブジェクトの ILM ルールとポリシー（例 4 ）"です。

S3 REST APIを使用してStorageGRID S3 Object Lockを設定する

StorageGRID システムでS3オブジェクトロックのグローバル設定が有効になっている場合は、S3オブジェクトロックを有効にしてバケットを作成できます。デフォルトの保持設定はバケットごとに指定することも、オブジェクトバージョンごとに指定することも

できます。

StorageGRIDは `x-amz-sdk-checksum-algorithm`リクエストヘッダーをサポートしていません。

バケットで**S3**オブジェクトロックを有効にする方法

StorageGRID システムでグローバルな S3 オブジェクトのロック設定が有効になっている場合は、各バケットの作成時に S3 オブジェクトのロックを必要に応じて有効にすることができます。

S3オブジェクトロックは永続的な設定で、バケットの作成時にのみ有効にできます。バケットの作成後にS3オブジェクトロックを追加または無効にすることはできません。

バケットに対してS3オブジェクトロックを有効にするには、次のいずれかの方法を使用します。

- Tenant Manager を使用してバケットを作成します。を参照して "S3 バケットを作成する"
- CreateBucket要求と要求ヘッダーを使用してバケットを作成し `x-amz-bucket-object-lock-enabled`ます。を参照して "バケットの処理"
- テナントマネージャーからバケット設定を管理します。"S3オブジェクトロックのデフォルトの保持期間を更新します"を参照してください。

S3オブジェクトロックにはバケットのバージョン管理が必要です。バージョン管理はバケットの作成時に自動的に有効になります。バケットのバージョン管理を一時停止することはできません。を参照して "オブジェクトのバージョン管理"

バケットのデフォルトの保持設定

バケットでS3オブジェクトロックが有効になっている場合は、必要に応じてバケットのデフォルトの保持を有効にし、デフォルトの保持モードとデフォルトの保持期間を指定できます。

デフォルトの保持モード

- コンプライアンスモードの場合：
  - retain-until-dateに達するまで、オブジェクトを削除できません。
  - オブジェクトのretain-until-dateは増やすことはできますが、減らすことはできません。
  - オブジェクトのretain-until-dateは、その日付に達するまで削除できません。
- ガバナンスモードの場合：
  - 権限を持つユーザ `s3:BypassGovernanceRetention`は、要求ヘッダーを使用して保持設定を省略でき `x-amz-bypass-governance-retention: true`ます。
  - これらのユーザは、retain-until-dateに達する前にオブジェクトバージョンを削除できます。
  - これらのユーザは、オブジェクトのretain-until-dateを増減、または削除できます。

デフォルトの保持期間

各バケットのデフォルトの保持期間は、年または日数で指定できます。

バケットのデフォルトの保持期間を設定するには、次のいずれかの方法を使用します。

- Tenant Managerからバケット設定を管理します。およびを参照してください"S3 バケットを作成します。""S3オブジェクトロックのデフォルトの保持期間を更新します"。
- 問題デフォルトのモードとデフォルトの日数または年数を指定するための、バケットに対するPutObjectLockConfiguration要求。

PutObjectLockConfiguration

PutObjectLockConfiguration要求を使用すると、S3オブジェクトロックが有効になっているバケットに対して、デフォルトの保持モードとデフォルトの保持期間を設定および変更できます。以前に設定したデフォルトの保持設定を削除することもできます。

新しいオブジェクトバージョンがバケットに取り込まれると、 `x-amz-object-lock-mode`と `x-amz-object-lock-retain-until-date`が指定されていない場合、デフォルトの保持モードが適用されます。 `x-amz-object-lock-retain-until-date`が指定されていない場合、デフォルトの保持期間を使用して保持期限日が計算されます。

オブジェクトバージョンの取り込み後にデフォルトの保持期間が変更された場合、オブジェクトバージョンの保持期限は変更されず、新しいデフォルトの保持期間を使用して再計算されることはありません。

この処理を完了するには、権限またはrootアカウントが必要です `s3:PutBucketObjectLockConfiguration`。

PutObjectLockConfiguration リクエストには、以下のリクエストヘッダーのいずれかを指定する必要があります：

```
Content-MD5
x-amz-checksum-*
```

StorageGRID は、この操作では x-amz-checksum-* ヘッダーの内容を検証しません。

要求例

この例では、バケットに対してS3オブジェクトロックを有効にし（グリッド管理者が許可を与えている場合）、デフォルトの保持モードをCOMPLIANCEに、デフォルトの保持期間を6年に設定します。

```
PUT /bucket?object-lock HTTP/1.1
Accept-Encoding: identity
Content-Length: 308
Host: host
Content-MD5: request header
User-Agent: s3sign/1.0.0 requests/2.24.0 python/3.8.2
X-Amz-Date: date
X-Amz-Content-SHA256: authorization-string
Authorization: authorization-string

<ObjectLockConfiguration>
    <ObjectLockEnabled>Enabled</ObjectLockEnabled>
    <Rule>
        <DefaultRetention>
            <Mode>COMPLIANCE</Mode>
            <Years>6</Years>
        </DefaultRetention>
    </Rule>
</ObjectLockConfiguration>
```

バケットのデフォルトの保持期間を確認する方法

バケットでS3オブジェクトロックが有効になっているかどうかを確認し、デフォルトの保持モードと保持期間を確認するには、次のいずれかの方法を使用します。

- Tenant Managerでバケットを表示します。を参照して "S3バケットを表示します"
- 問題GetObjectLockConfiguration要求。

GetObjectLockConfigurationの略

GetObjectLockConfiguration要求を使用すると、S3 Object Lockがバケットで有効になっているかどうかを確認できます。有効になっている場合は、バケットにデフォルトの保持モードと保持期間が設定されているかどうかを確認できます。

新しいオブジェクトバージョンがバケットに取り込まれると、 `x-amz-object-lock-mode`が指定されていない場合、デフォルトの保持モードが適用されます。デフォルトの保持期間は、 `x-amz-object-lock-retain-until-date`が指定されていない場合に保持期限日を計算するために使用されます。

この処理を完了するには、権限またはrootアカウントが必要です `s3:GetBucketObjectLockConfiguration`。

要求例

```
GET /bucket?object-lock HTTP/1.1
Host: host
Accept-Encoding: identity
User-Agent: aws-cli/1.18.106 Python/3.8.2 Linux/4.4.0-18362-Microsoft
botocore/1.17.29
x-amz-date: date
x-amz-content-sha256: authorization-string
Authorization: authorization-string
```

応答例

```
HTTP/1.1 200 OK
x-amz-id-2:
iVmcB7OXXJRkRH1FiVq1151/T24gRfpwpuZrEG11Bb9ImOMAAe98oxSpXlknabA0LTvBYJpSIX
k=
x-amz-request-id: B34E94CACB2CEF6D
Date: Fri, 04 Sep 2020 22:47:09 GMT
Transfer-Encoding: chunked
Server: AmazonS3

<?xml version="1.0" encoding="UTF-8"?>
<ObjectLockConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
    <ObjectLockEnabled>Enabled</ObjectLockEnabled>
    <Rule>
        <DefaultRetention>
            <Mode>COMPLIANCE</Mode>
            <Years>6</Years>
        </DefaultRetention>
    </Rule>
</ObjectLockConfiguration>
```

オブジェクトの保持設定を指定する方法

S3オブジェクトロックが有効なバケットには、S3オブジェクトロックの保持設定の有無に関係なく、オブジェクトを組み合わせて含めることができます。

オブジェクトレベルの保持設定は、S3 REST APIを使用して指定します。オブジェクトの保持設定は、バケットのデフォルトの保持設定よりも優先されます。

オブジェクトごとに次の設定を指定できます。

- 保持モード：コンプライアンスまたはガバナンスのいずれか。
- * retain-until-date *：StorageGRID がオブジェクトバージョンを保持する期間を指定する日付。
  - コンプライアンスモードでは、retain-until-dateが将来の日付の場合、オブジェクトを読み出すことはできますが、変更や削除はできません。retain-until-dateは増やすことができますが、この日付を減ら

すことも削除することもできません。

- ガバナンスモードでは、特別な権限を持つユーザーは、retain-until-date設定をバイパスできます。保持期間が経過する前にオブジェクトバージョンを削除できます。また、retain-until-dateを増減したり、削除したりすることもできます。

- * リーガルホールド * ：オブジェクトバージョンにリーガルホールドを適用すると、そのオブジェクトがただちにロックされます。たとえば、調査または法的紛争に関連するオブジェクトにリーガルホールドを設定する必要がある場合があります。リーガルホールドには有効期限はありませんが、明示的に削除されるまで保持されます。

  オブジェクトのリーガルホールド設定は、保持モードやretain-until-dateとは関係ありません。オブジェクトのバージョンがリーガルホールドの対象になっている場合、そのバージョンは誰も削除できません。

バケットにオブジェクトバージョンを追加するときにS3オブジェクトロック設定を指定するには、"PutObject"、または"CopyObject" "CreateMultipartUpload"要求を実行します。

次のものを使用できます。

- `x-amz-object-lock-mode`コンプライアンスまたはガバナンス（大文字と小文字が区別されます）。

  を指定する場合は `x-amz-object-lock-mode`、も指定する必要があります `x-amz-object-lock-retain-until-date`。

- `x-amz-object-lock-retain-until-date`

  - retain-until-dateの値は、の形式で指定する必要があります `2020-08-10T21:46:00Z`。秒数には分数を指定できますが、保持される 10 進数は 3 桁（ミリ秒単位）だけです。その他のISO 8601形式は使用できません。
  - retain-une-date は将来の日付にする必要があります。

- `x-amz-object-lock-legal-hold`

  リーガルホールドがオン（大文字と小文字が区別される）の場合、オブジェクトはリーガルホールドの対象になります。リーガルホールドがオフの場合、リーガルホールドは適用されません。それ以外の値を指定すると、 400 Bad Request （ InvalidArgument ）エラーが発生します。

次のいずれかの要求ヘッダーを使用する場合は、次の制限事項に注意してください。

- PutObject リクエストに x-amz-object-lock-* リクエストヘッダーが含まれている場合は、次のリクエストヘッダーのいずれかを含める必要があります：

  ```
  Content-MD5
  x-amz-checksum-*
  ```

  これらのヘッダーは、CopyObject または CreateMultipartUpload には必要ありません。

- バケットで S3 オブジェクトロックが有効になっておらず、x-amz-object-lock-* リクエストヘッダーが存在する場合、400 Bad Request （InvalidRequest）エラーが返されます。

- PutObject要求では、を使用してAWSの動作を照合できます `x-amz-storage-class: REDUCED_REDUNDANCY`。ただし、 S3 オブジェクトのロックが有効になっているバケットにオブジェク

トが取り込まれると、 StorageGRID は常にデュアルコミットの取り込みを実行します。

- 後続のGETまたはHeadObjectバージョンの応答には、ヘッダー、 `x-amz-object-lock-retain-until-date`、および `x-amz-object-lock-legal-hold`（設定されていて、要求の送信者に正しい権限がある場合） `s3:Get*`が含まれます `x-amz-object-lock-mode`。

ポリシー条件キーを使用して、オブジェクトの最小保持期間と最大保持期間を制限でき `s3:object-lock-remaining-retention-days`ます。

オブジェクトの保持設定を更新する方法

既存のオブジェクトのバージョンのリーガルホールドや保持の設定を更新する必要がある場合、次のオブジェクトサブリソース処理を実行できます。

- `PutObjectLegalHold`

  新しいリーガルホールドの値が on の場合、オブジェクトはリーガルホールドの対象になります。リーガルホールドの値がオフの場合、リーガルホールドは解除されます。

- `PutObjectRetention`
  - mode値はcomplianceまたはgovernanceです（大文字と小文字が区別されます）。
  - retain-until-dateの値は、の形式で指定する必要があります `2020-08-10T21:46:00Z`。秒数には分数を指定できますが、保持される 10 進数は 3 桁（ミリ秒単位）だけです。その他のISO 8601形式は使用できません。
  - オブジェクトバージョンに既存の retain-until がある場合は、オブジェクトバージョンを増やすことはできますが、増やすことはできません。新しい値は将来の必要があります。

リクエストには、以下のいずれかのリクエストヘッダーを指定する必要があります。

```
Content-MD5
x-amz-checksum-*
```

StorageGRID は、これらの操作では x-amz-checksum-* ヘッダーの内容を検証しません。

ガバナンスモードの使用方法

権限を持つユーザ `s3:BypassGovernanceRetention`は、ガバナンスモードを使用するオブジェクトのアクティブな保持設定をバイパスできます。`DELETE`処理や`PutObjectRetention`処理には要求ヘッダーを含める必要があります `x-amz-bypass-governance-retention:true`。これらのユーザは、次の追加操作を実行できます。

- 保持期間が経過する前にオブジェクトバージョンを削除するには、DeleteObject処理またはDeleteObjects処理を実行します。

  リーガルホールドの対象になっているオブジェクトは削除できません。リーガルホールドをオフにする必要があります。

`x-amz-bypass-governance-retention`ヘッダーは、S3 Object Lockのないオブジェクトには影響を与えません。

- オブジェクトの保持期間が経過する前にオブジェクトバージョンのモードをガバナンスからコンプライアンスに変更するPutObjectRetention処理を実行します。

  コンプライアンスモードからガバナンスモードに変更することはできません。

- PutObjectRetention処理を実行して、オブジェクトバージョンの保持期間を増減、または削除します。

関連情報

- "S3 オブジェクトロックでオブジェクトを管理します"
- "S3オブジェクトロックを使用してオブジェクトを保持します"
- "Amazon Simple Storage Serviceユーザガイド：オブジェクトのロック"

StorageGRIDのS3ライフサイクル設定について学ぶ

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

このセクションの簡単な例では、S3ライフサイクル設定によって、特定のS3バケットから特定のオブジェクトが削除（期限切れ）されるタイミングをどのように制御できるかを示しています。このセクションの例は、あくまで説明のためのものです。S3ライフサイクル設定の作成に関する詳細については、 "Amazon Simple Storage Service ユーザーガイド：オブジェクトのライフサイクル管理"を参照してください。StorageGRID は有効期限アクションのみをサポートしており、移行アクションはサポートしていません。

ライフサイクル構成とは

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

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

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

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

ジェクトのバージョンが無期限に保持されることが暗黙的に示されます。を参照して "S3バケットライフサイクルとILMポリシーの優先度の例"

そのため、 ILM ルールの配置手順がオブジェクトに引き続き適用されていても、オブジェクトがグリッドから削除されることがあります。あるいは、 ILM 配置手順がすべて終了したあとも、オブジェクトがグリッドに保持される場合があります。詳細については、を参照してください "オブジェクトのライフサイクル全体にわたる ILM の動作"。

> バケットライフサイクル設定は S3 オブジェクトロックが有効になっているバケットで使用できますが、従来の準拠バケットではバケットライフサイクル設定がサポートされません。

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

- DeleteBucketLifecycle
- GetBucketLifecycleConfiguration
- PutBucketLifecycleConfiguration

ライフサイクル構成を作成します

ライフサイクル設定を作成するための最初の手順として、 1 つ以上のルールを含む JSON ファイルを作成します。たとえば、この JSON ファイルには次の 3 つのルールが含まれています。

1. ルール1は、プレフィックス/に一致し、 `key2`値がの `tag2`オブジェクトにのみ適用され `category1`ます。パラメータは `Expiration`、フィルタに一致するオブジェクトが2020年8月22日の午前0時に期限切れになるように指定します。
2. ルール2は、プレフィックスが/に一致するオブジェクトにのみ適用され `category2`ます。パラメータは `Expiration`、フィルタに一致するオブジェクトが、取り込まれてから100日後に期限切れになるように指定します。

   > 日数を指定するルールは、オブジェクトが取り込まれた時点を基準とした相対的なルールです。現在の日付が取り込み日と日数を超えている場合は、ライフサイクル設定の適用後すぐに一部のオブジェクトがバケットから削除される可能性があります。

3. ルール3は、プレフィックスが/に一致するオブジェクトにのみ適用され `category3`ます。 `Expiration`パラメータは、一致するオブジェクトの最新でないバージョンが最新でなくなってから50日後に期限切れになるように指定します。

```
{
    "Rules": [
        {
            "ID": "rule1",
            "Filter": {
                "And": {
                    "Prefix": "category1/",
                    "Tags": [
                        {
                            "Key": "key2",
                            "Value": "tag2"
                        }
                    ]
                }
            },
            "Expiration": {
                "Date": "2020-08-22T00:00:00Z"
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule2",
            "Filter": {
                "Prefix": "category2/"
            },
            "Expiration": {
                "Days": 100
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule3",
            "Filter": {
                "Prefix": "category3/"
            },
            "NoncurrentVersionExpiration": {
                "NoncurrentDays": 50
            },
            "Status": "Enabled"
        }
    ]
}
```

バケットにライフサイクル設定を適用

ライフサイクル設定ファイルを作成したら、PutBucketLifecycleConfiguration要求を発行してバケットに適用します。

この要求は、サンプルファイルのライフサイクル設定をという名前のバケット内のオブジェクトに適用し`testbucket`ます。

```
aws s3api --endpoint-url <StorageGRID endpoint> put-bucket-lifecycle-
configuration
--bucket testbucket --lifecycle-configuration file://bktjson.json
```

ライフサイクル設定がバケットに正常に適用されたことを確認するには、GetBucketLifecycleConfiguration要求を問題します。例：

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-
configuration
 --bucket testbucket
```

成功応答には、適用したライフサイクル設定が表示されます。

バケットライフサイクルの有効期限が環境 オブジェクトであることを検証します

PutObject、HeadObject、またはGetObjectのいずれか環境の要求を発行するときに、ライフサイクル設定の有効期限ルールが特定のオブジェクトであるかどうかを確認できます。ルールが適用される場合は、オブジェクトの有効期限と一致した有効期限ルールを示すパラメータが応答に含まれ`Expiration`ます。

> バケットライフサイクルはILMよりも優先されるため、`expiry-date`オブジェクトが実際に削除される日付が表示されます。詳細については、を参照してください "オブジェクト保持期間の決定方法"。

たとえば、次のPutObject要求は2020年6月22日に発行され、バケットにオブジェクトを配置したとし`testbucket`ます。

```
aws s3api --endpoint-url <StorageGRID endpoint> put-object
--bucket testbucket --key obj2test2 --body bktjson.json
```

成功の応答は、オブジェクトの有効期限が 100 日（ 2020 年 10 月 1 日）に切れ、ライフサイクル設定のルール 2 に一致したことを示します。

```
{
      *"Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:49 GMT\", rule-
id=\"rule2\"",
      "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
}
```

たとえば、次のHeadObject要求を使用して、testbucketバケット内の同じオブジェクトのメタデータを取得しました。

```
aws s3api --endpoint-url <StorageGRID endpoint> head-object
--bucket testbucket --key obj2test2
```

成功の応答にはオブジェクトのメタデータが含まれ、オブジェクトが 100 日で期限切れになり、ルール 2 に一致したことが示されます。

```
{
      "AcceptRanges": "bytes",
      *"Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:48 GMT\", rule-
id=\"rule2\"",
      "LastModified": "2020-06-23T09:07:48+00:00",
      "ContentLength": 921,
      "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
      "ContentType": "binary/octet-stream",
      "Metadata": {}
}
```

バージョン管理が有効なバケットの場合 `x-amz-expiration`、応答ヘッダーはオブジェクトの現在のバージョンにのみ適用されます。

StorageGRIDでS3 REST APIを実装する際の推奨事項

StorageGRID で使用するために S3 REST API を実装する場合は、次の推奨事項を考慮してください。

存在しないオブジェクトに対する **HEAD** の推奨事項

アプリケーションが、実際には存在しないと思われるパスにオブジェクトが存在するかどうかを定期的に確認する場合は、「使用可能」を使用する必要があります。"一貫性" 。たとえば、アプリケーションが PUT を実行する前に場所を HEAD する場合は、「Available」一貫性を使用する必要があります。

そうしないと、同じサイトに複数のストレージノードが使用できない場合やリモートサイトに到達できない場合に、HEAD処理でオブジェクトが見つからないと「500 Internal Server Error」が大量に返されることがあります。

要求を使用して各バケットに「available」整合性を設定すること"PUT Bucket consistency"も、個 々 のAPI処理の要求ヘッダーで整合性を指定することもできます。

オブジェクトキーの推奨事項

オブジェクトキー名については、バケットが最初に作成された日時に基づいて次の推奨事項に従ってください。

StorageGRID 11.4以前で作成されたバケット

- オブジェクトキーの最初の4文字にランダムな値を使用しないでください。これは、 AWS が以前に推奨していたキープレフィックスの推奨事項とは異なります。代わりに、など、ランダムではなく一意ではないプレフィックスを使用します `image`。
- 以前のAWSの推奨事項に従ってキープレフィックスにランダムな一意の文字を使用する場合は、オブジェクトキーの前にディレクトリ名を付けます。つまり、次の形式を使用します。

  ```
  mybucket/mydir/f8e3-image3132.jpg
  ```

  次の形式は使用しないでください。

  ```
  mybucket/f8e3-image3132.jpg
  ```

StorageGRID 11.4以降で作成されたバケット

パフォーマンスのベストプラクティスに合わせてオブジェクトキー名を制限する必要はありません。ほとんどの場合、オブジェクトキー名の最初の4文字にはランダムな値を使用できます。

> ただし、短期間ですべてのオブジェクトを継続的に削除するS3ワークロードは例外です。このユースケースのパフォーマンスへの影響を最小限に抑えるには、キー名の先頭部分を数千個のオブジェクトごとに、日付などの値を変更します。たとえば、S3クライアントが1秒あたり2、000個のオブジェクトを書き込むのが一般的で、ILMまたはバケットライフサイクルポリシーで3日後にすべてのオブジェクトが削除されるとします。パフォーマンスへの影響を最小限に抑えるには、次のようなパターンを使用してキーに名前を付けます。
> `/mybucket/mydir/yyyymmddhhmmss-random_UUID.jpg`

「範囲読み取り」に関する推奨事項

が有効になっている場合"格納オブジェクトを圧縮するグローバルオプション"は、返されるバイト数の範囲を指定するGetObject処理をS3クライアントアプリケーションで実行しないでください。これらの「範囲読み取り」処理は効率的ではありません。StorageGRIDでは、要求されたバイトにアクセスするためにオブジェクトの圧縮を実質的に解除する必要があるためです。非常に大きなオブジェクトから小さい範囲のバイト数を要求するGetObject処理は特に非効率的です。たとえば、50GBの圧縮オブジェクトから10MBの範囲を読み取る処理は非効率的です。

圧縮オブジェクトから範囲を読み取ると、クライアント要求がタイムアウトする可能性があります。

> オブジェクトを圧縮する必要があり、クライアントアプリケーションが範囲読み取りを使用する必要がある場合は、アプリケーションの読み取りタイムアウトを増やしてください。

Amazon S3 REST APIのサポート

StorageGRID における **S3 REST API** のサポートされている操作と制限

StorageGRID システムは Simple Storage Service API （ API バージョン 2006-03-01 ）を実装しており、ほとんどの処理をサポートしていますが、いくつかの制限事項があります。S3 REST API クライアントアプリケーションを統合するときは、実装の詳細を理解しておく必要があります。

StorageGRID システムは、仮想ホスト形式のリクエストとパス形式のリクエストの両方をサポートしています。

日付の処理

S3 REST API の StorageGRID 実装では、有効な HTTP の日付形式のみをサポートしています。

StorageGRID システムでは、日付の値を設定できるすべてのヘッダーで、有効な HTTP の日付形式のみがサポートされます。日付の時刻の部分は、 Greenwich Mean Time （ GMT ；グリニッジ標準時）の形式で指定するか、タイムゾーンのオフセットなし（ +0000 を指定）の Universal Coordinated Time （ UTC ；協定世界時）の形式で指定できます。リクエストにヘッダーを含めると、 `x-amz-date`Dateリクエストヘッダーで指定した値が上書きされます。AWS署名バージョン4を使用する場合 `x-amz-date`は、dateヘッダーがサポートされないため、署名済み要求にヘッダーが含まれている必要があります。

代表的な要求ヘッダー

StorageGRIDシステムでは、1つの例外を除き、で定義されている共通の要求ヘッダーがサポートされ "Amazon Simple Storage Service API Reference：Common Request Headers"ます。

要求ヘッダー	インプリメンテーション
許可	AWS 署名バージョン 2 は完全にサポートされます AWS 署名バージョン 4 は次の例外を除いてサポートされます。 • で実際のペイロードチェックサム値を指定すると `x-amz-content-sha256`、ヘッダーに値が指定されているかのように、値が検証されずに受け入れられ `UNSIGNED-PAYLOAD`ます。ストリーミングを意味するヘッダー値 `aws-chunked`（streaming-AWS4-HMAC-SHA256-payloadなど）を指定する `x-amz-content-sha256`と、チャンクシグネチャはチャンクデータに対して検証されません。

共通の応答ヘッダー

StorageGRID システムでは、以下の例外を除き、 _Simple Storage Service API Reference_で 定義されている共通の応答ヘッダーがすべてサポートされます。

応答ヘッダー	インプリメンテーション
x-amz-id-2	未使用

StorageGRID S3 REST APIによるリクエストの認証方法

StorageGRID システムでは、 S3 API を使用したオブジェクトへのアクセスについて、認証アクセスと匿名アクセスの両方をサポートしています。

S3 API では、 S3 API 要求の認証で署名バージョン 2 と署名バージョン 4 がサポートされます。

認証された要求は、アクセスキー ID とシークレットアクセスキーを使用して署名する必要があります。

StorageGRIDシステムでは、HTTPヘッダーとクエリパラメータの2つの認証方式がサポートされています。
`Authorization`

HTTP Authorization ヘッダーを使用します

S3 APIのすべての処理でHTTP `Authorization`ヘッダーが使用されます。ただし、バケットポリシーで許可されている匿名の要求は除きます。 `Authorization`ヘッダーには、要求の認証に必要なすべての署名情報が含まれます。

クエリパラメータを使用します

クエリパラメータを使用すると、 URL に認証情報を追加できます。これは署名付き URL と呼ばれ、特定のリソースへの一時的なアクセスを許可する場合に使用できます。指定されたURLを持つユーザは、リソースにアクセスする際にシークレットアクセスキーを知っている必要はありません。これにより、リソースへのサードパーティの制限付きアクセスを提供できます。

StorageGRID でサポートされているサービス操作

StorageGRID システムでは、サービスに対して次の処理をサポートしています。

操作	インプリメンテーション
ListBuckets （以前の名前はGET Service）	Amazon S3 REST API のすべての動作が実装されています。予告なく変更される場合があります。
GET Storage Usage の略	StorageGRID要求では"GET Storage Usage の略"、アカウントで使用されているストレージの合計容量と、アカウントに関連付けられているバケットごとに表示されます。これは、パス/とカスタムクエリパラメータ(`?x-ntap-sg-usage`）が追加されたサービスに対する処理です。
オプション/	クライアントアプリケーションからストレージノードのS3ポートに要求を発行して（S3認証クレデンシャルは不要）、ストレージノードが使用可能かどうかを確認できます `OPTIONS /`。この要求は監視に使用できるほか、外部のロードバランサがストレージノードの停止を特定する目的でも使用できます。

StorageGRIDにおけるS3バケットの操作と実装の詳細

StorageGRID システムは、S3 テナントアカウントごとに最大 20,000 個のバケットをサポートします。

各グリッドには、最大100,000個のバケットを含めることができます。

複数のテナントがそれぞれ最大5,000個のバケットを持つ場合、グリッド内の各ストレージノードは最低64 GBのRAMを搭載する必要があります。

バケット名の制限は AWS US Standard リージョンの制限に従いますが、S3 仮想ホスト型リクエストをサポートするために、さらに DNS 命名規則に基づいて制限する必要があります。

詳細については、以下を参照してください。

- "Amazon Simple Storage Serviceユーザガイド：バケットのクォータ、制限事項"

- "S3エンドポイントのドメイン名を設定"

ListObjects (GET Bucket) および ListObjectVersions (GET Bucket object versions) オペレーションはStorageGRIDをサポートします"整合性の値"。

個々のバケットについて、最終アクセス時刻の更新が有効になっているか無効になっているかを確認できます。"GET Bucket last access time のように指定します"を参照してください。

次の表に、 StorageGRID での S3 REST API バケット処理の実装方法を示します。これらの処理を実行するには、アカウントに必要なアクセスクレデンシャルが付与されている必要があります。

操作	インプリメンテーション
CreateBucket	新しいバケットを作成します。バケットを作成すると、そのバケットの所有者になります。 注：S3ディレクトリバケットはサポートされていません。 • バケット名は次のルールを満たす必要があります。 ◦ StorageGRID システム全体で（テナントアカウント内だけではなく）一意である必要があります。 ◦ DNS に準拠している必要があります。 ◦ 3文字以上63文字以下にする必要があります。 ◦ 1 つ以上のラベルを連続して指定できます。隣接するラベルはピリオドで区切ります。各ラベルの先頭と末尾の文字は小文字のアルファベットか数字にする必要があり、使用できる文字は小文字のアルファベット、数字、ハイフンのみです。 ◦ テキスト形式の IP アドレスのようにはできません。 ◦ 仮想ホスト形式の要求でピリオドを使用しないでください。ピリオドを使用すると、サーバワイルドカード証明書の検証で原因 の問題が発生します。 • デフォルトではリージョン内にバケットが作成され `us-east-1` ますが、要求の本文の `request` 要素を使用して別のリージョンを指定できます `LocationConstraint`。要素を使用する場合 `LocationConstraint` は、Grid Managerまたはグリッド管理APIを使用して定義されたリージョンの正確な名前を指定する必要があります。使用するリージョン名がわからない場合は、システム管理者にお問い合わせください。 注：CreateBucketリクエストで StorageGRID に定義されていないリージョンを使用すると、エラーが発生します。 • `x-amz-bucket-object-lock-enabled`リクエストヘッダーを含めることで、S3 Object Lockを有効にしたバケットを作成できます。"S3 REST APIを使用してS3オブジェクトロックを設定します"を参照してください。 S3オブジェクトロックにはバケットのバージョン管理が必要ですが、S3オブジェクトロックを有効にしてバケットを作成すると、自動的に有効になります。 S3オブジェクトロックは、バケット作成時または後から有効にすることができます。
DeleteBucket	バケットを削除します。
DeleteBucketCors	バケットのCORS設定を削除します。

操作	インプリメンテーション
DeleteBucketEncryption	バケットからデフォルトの暗号化を削除します。既存の暗号化オブジェクトは暗号化されたままですが、バケットに追加された新しいオブジェクトは暗号化されません。
DeleteBucketLifecycle	バケットからライフサイクル設定を削除します。"S3 ライフサイクル設定を作成する"を参照してください。
DeleteBucketPolicy	バケットに関連付けられているポリシーを削除します。
DeleteBucketReplication	バケットに関連付けられているレプリケーション設定を削除します。
DeleteBucketTagging	サブリソースを使用し `tagging`てバケットからすべてのタグを削除します。 注意：このバケットにデフォルト以外の ILM ポリシータグが設定されている場合、値が割り当てられた `NTAP-SG-ILM-BUCKET-TAG`バケットタグが存在します。 `NTAP-SG-ILM-BUCKET-TAG`バケットタグが存在する場合は、DeleteBucketTaggingリクエストを発行しないでください。代わりに、`NTAP-SG-ILM-BUCKET-TAG`タグとその割り当てられた値のみを指定してPutBucketTaggingリクエストを発行し、バケットから他のすべてのタグを削除してください。 `NTAP-SG-ILM-BUCKET-TAG`バケットタグを変更または削除しないでください。
GetBucketAcl	バケットの所有者にバケットへのフルアクセスがあることを示す応答が返され、所有者のID、表示名、および権限が表示されます。
GetBucketCors	バケットの設定を返し `cors`ます。
GetBucketEncryptionの略	バケットのデフォルトの暗号化設定を返します。
GetBucketLifecycleConfiguration （以前のGET Bucket lifecycle）	バケットのライフサイクル構成を返します。"S3 ライフサイクル設定を作成する"を参照してください。
GetBucketLocation	`LocationConstraint`要素を使用して `CreateBucket` リクエストで設定されたリージョンを返します。バケットのリージョンが `us-east-1`（デフォルト）の場合、`LocationConstraint`には空の値が返されます。

操作	インプリメンテーション
GetBucketNotificationConfigurationを参照してください （以前の名前のGET Bucket通知）	バケットに関連付けられている通知設定を返します。
GetBucketPolicy	バケットに関連付けられているポリシーを返します。
GetBucketReplicationの略	バケットに関連付けられているレプリケーション設定を返します。
GetBucketTagging	サブリソースを使用し `tagging`てバケットのすべてのタグを返します。 注意：このバケットにデフォルト以外の ILM ポリシータグが設定されている場合、値が割り当てられた `NTAP-SG-ILM-BUCKET-TAG`バケットタグが存在します。このタグは変更または削除しないでください。
GetBucketVersioning	この実装では、サブリソースを使用して `versioning`バケットのバージョン管理の状態を返します。 • *blank*：バージョン管理が一度も有効になっていない（バケットは「バージョン管理されていない」） • 有効：バージョン管理が有効になっています • 中断：バージョン管理は以前有効になっていて、中断されています
GetObjectLockConfigurationの略	バケットのデフォルトの保持モードとデフォルトの保持期間（設定されている場合）を返します。 "S3 REST APIを使用してS3オブジェクトロックを設定します"を参照してください。
ヘッドバケット	バケットが存在し、そのバケットにアクセスする権限があるかどうかを確認します。 この処理から返される情報は次の • `x-ntap-sg-bucket-id`：バケットのUUID（UUID形式）。 • `x-ntap-sg-trace-id`：関連付けられた要求の一意のトレースID。

操作	インプリメンテーション
listObjectsおよびListObjectsV2 （以前の名前はGET Bucket）	バケット内のオブジェクトの一部またはすべて（最大1、000）を返します。オブジェクトのストレージクラスには、ストレージクラスオプションを使用してオブジェクトを取り込んだ場合でも、次の2つの値のいずれかが設定され `REDUCED_REDUNDANCY`ます。 • `STANDARD`オブジェクトがストレージノードで構成されるストレージプールに格納されていることを示します。 • `GLACIER`が表示されます。これは、クラウドストレージプールで指定された外部バケットにオブジェクトが移動されたことを示します。 バケットに同じプレフィックスの削除済みキーが大量に含まれている場合は、キーを含まないキーが応答に含まれることがあります `CommonPrefixes`。 HeadObject および ListObject リクエストの場合、 StorageGRID は異なる精度で LastModified タイムスタンプを返しますが、AWS は同じ精度でタイムスタンプを返します。次の例をご覧ください。 • StorageGRIDヘッドオブジェクト: "LastModified": "2024-09-26T16:43:24+00:00" • StorageGRIDリストオブジェクト: "LastModified": "2024-09-26T16:43:24.931000+00:00" • AWS ヘッドオブジェクト: "LastModified": "2023-10-17T00:19:54+00:00" • AWS リストオブジェクト: "LastModified": "2023-10-17T00:19:54+00:00"
ListObjectVersions （以前のGET Bucket Object versions）	バケットに対する読み取りアクセスが許可されている場合、サブリソースを指定してこの処理を実行すると、 `versions`バケット内のオブジェクトのすべてのバージョンのメタデータがリストされます。
PutBucketCorsの略	クロスオリジン要求を処理できるように、バケットのCORS設定を設定します。Cross-Origin Resource Sharing （ CORS ）は、あるドメインのクライアント Web アプリケーションが別のドメインのリソースにアクセスできるようにするセキュリティ機能です。たとえば、という名前のS3バケットを使用してグラフィックを格納するとし `images`ます。バケットの`CORS`設定を設定すると `images`、そのバケット内の画像をWebサイトに表示できるように `http://www.example.com`なります。
PutBucketEncryptionの略	既存のバケットのデフォルトの暗号化状態を設定します。バケットレベルの暗号化が有効な場合は、バケットに追加されたすべての新しいオブジェクトが暗号化されます。 StorageGRID では、 StorageGRID で管理されるキーによるサーバ側の暗号化がサポートされます。サーバ側の暗号化設定ルールを指定する場合は、パラメータをに `AES256`設定し `SSEAlgorithm`、パラメータは使用しないで `KMSMasterKeyID`ください。 オブジェクトのアップロード要求ですでに暗号化が指定されている場合（要求に要求ヘッダーが含まれている場合）は、バケットのデフォルトの暗号化設定は無視され `x-amz-server-side-encryption-*`ます。

操作	インプリメンテーション
PutBucketLifecycleConfiguration （以前のPUT Bucket lifecycle）	バケットの新しいライフサイクル設定を作成するか、既存のライフサイクル設定と置き換えます。StorageGRID では、 1 つのライフサイクル設定で最大 1 、 000 個のライフサイクルルールがサポートされます。各ルールには、次の XML 要素を含めることができます。 • 有効期限（日数、日付、ExpiredObjectDeleteMarker） • NoncurrentVersionExpiration（NewerNoncurrentVersions、NoncurrentDays ） • フィルタ（プレフィックス、タグ） • ステータス • ID StorageGRID では、次のアクションはサポートされません。 • AbortIncompleteMultipartUpload • 移行 "S3 ライフサイクル設定を作成する"を参照してください。バケットライフサイクルの有効期限アクションがILM配置指示とどのように相互作用するかを理解するには、"オブジェクトのライフサイクル全体にわたる ILM の動作"を参照してください。 • 注：バケットライフサイクル設定は S3 オブジェクトロックが有効なバケットで使用できますが、従来の準拠バケットではバケットライフサイクル設定がサポートされません。

操作	インプリメンテーション

PutBucketNotificationConfigurationの略
 	
（以前の名前のPUT Bucket通知）
	要求の本文に含まれる通知設定XMLを使用してバケットの通知を設定します。実装に関する次の詳細事項に注意してください。
	
	• StorageGRID は、送信先として Amazon Simple Notification Service (Amazon SNS) トピック、Kafka トピック、または Webhook エンドポイントをサポートします。 Simple Queue Service (SQS) または AWS Lambda エンドポイントはサポートされていません。
	• 通知のデスティネーションは、 StorageGRID エンドポイントの URN として指定する必要があります。エンドポイントは、 Tenant Manager またはテナント管理 API を使用して作成できます。
	
	通知設定が機能するためには、エンドポイントが存在している必要があります。エンドポイントが存在しない場合は `400 Bad Request`、コードとともにエラーが返され `InvalidArgument`ます。
	
	• 次のイベントタイプに対して通知を設定することはできません。これらのイベントタイプは * サポートされていません。
	◦ `s3:ReducedRedundancyLostObject`
	◦ `s3:ObjectRestore:Completed`
	• StorageGRID から送信されるイベント通知は標準のJSON形式を使用しますが、次のリストに示すように、一部のキーが含まれず、他のキーには特定の値が使用されます。
	◦ * eventSource*
	
	`sgws:s3`
	
	◦ * awsRegion *
	
	含まれません
	
	◦ * x-amz-id-2 *
	
	含まれません
	
	◦ * arn *
	
	`urn:sgws:s3:::bucket_name`

PutBucketPolicy	バケットに適用されるポリシーを設定します。"バケットとグループのアクセスポリシーを使用"を参照してください。

操作	インプリメンテーション
PutBucketReplicationの略	要求の本文に含まれるレプリケーション設定XMLを使用してバケットを設定します"StorageGRID CloudMirrorレプリケーション"。CloudMirror レプリケーションについては、実装に関する次の詳細事項に注意してください。 • StorageGRID はレプリケーション構成の V1 のみをサポートしています。つまり、StorageGRID はルールに対して `Filter`要素の使用をサポートしておらず、オブジェクトバージョンの削除については V1 の規約に従います。詳細については、 "Amazon Simple Storage Serviceユーザガイド：レプリケーションの設定"を参照してください。 • バケットレプリケーションは、バージョン管理されているバケットでもバージョン管理されていないバケットでも設定でき • レプリケーション設定 XML の各ルールで異なるデスティネーションバケットを指定できます。1 つのソースバケットを複数のデスティネーションバケットにレプリケートできます。 • 宛先バケットは、Tenant Manager またはTenant Management APIで指定されているStorageGRIDエンドポイントのURNとして指定する必要があります。"CloudMirror レプリケーションを設定します"を参照してください。 レプリケーション設定が機能するためには、エンドポイントが存在している必要があります。エンドポイントが存在しない場合、要求はとして失敗し `400 Bad Request`ます。次のエラーメッセージが表示されます。 `Unable to save the replication policy. The specified endpoint URN does not exist: URN.` • 設定XMLでを指定する必要はありません `Role`。この値は StorageGRID では使用されず、送信されても無視されます。 • 設定XMLでストレージクラスを省略した場合、StorageGRIDではデフォルトでストレージクラスが使用され `STANDARD`ます。 • ソースバケットからオブジェクトを削除する場合、またはソースバケット自体を削除する場合、クロスリージョンレプリケーションは次のように動作します。 ◦ レプリケートの前にオブジェクトまたはバケットを削除した場合、オブジェクトまたはバケットはレプリケートされず、通知も送信されません。 ◦ レプリケートのあとにオブジェクトまたはバケットを削除すると、StorageGRID は、 V1 のクロスリージョンレプリケーションに対する Amazon S3 の通常の削除動作に従います。

操作	インプリメンテーション
PutBucketTaggingの略	サブリソースを使用して、 `tagging`バケットの一連のタグを追加または更新します。バケットタグを追加する場合は、次の制限事項に注意してください。 • StorageGRID と Amazon S3 はどちらもバケットごとに最大 50 個のタグをサポートします。 • バケットに関連付けられているタグには、一意のタグキーが必要です。タグキーには Unicode 文字を 128 文字まで使用できます。 • タグ値には、 Unicode 文字を 256 文字以内で指定します。 • キーと値では大文字と小文字が区別されます。 注意：このバケットにデフォルト以外の ILM ポリシータグが設定されている場合、値が割り当てられた `NTAP-SG-ILM-BUCKET-TAG`バケットタグが存在します。 `NTAP-SG-ILM-BUCKET-TAG`バケットタグが、割り当てられた値とともにすべての PutBucketTagging リクエストに含まれていることを確認してください。このタグは変更または削除しないでください。 注：この処理を実行すると、バケットにすでに設定されている現在のタグが上書きされます。セットから既存のタグを省略すると、それらのタグはバケットから削除されます。
PutBucketVersioning	サブリソースを使用 `versioning`して、既存のバケットのバージョン管理状態を設定します。バージョン管理の状態は、次のいずれかの値に設定できます。 • Enabled ：バケット内のオブジェクトに対してバージョン管理を有効にします。バケットに追加されるすべてのオブジェクトに、一意のバージョン ID が割り当てられます。 • Suspended ：バケット内のオブジェクトに対してバージョン管理を無効にします。バケットに追加されたすべてのオブジェクトにバージョンIDが割り当てられ `null`ます。
PutObjectLockConfiguration	• バケットのデフォルトの保持モードとデフォルトの保持期間を設定または削除します。 • グリッド管理者が許可を与えている場合、既存のバケットに対してS3オブジェクトロックを有効にします。 デフォルトの保持期間が変更された場合、既存のオブジェクトバージョンの保持期限は変更されず、新しいデフォルトの保持期間を使用して再計算されることはありません。 詳細については、"S3 REST APIを使用してS3オブジェクトロックを設定します"を参照してください。

オブジェクトの処理

このセクションでは、 StorageGRID システムでオブジェクトの S3 REST API 処理を実装する方法について説明します。

すべてのオブジェクトの処理に次の条件が適用されます。

- StorageGRID"整合性の値"次の例外を除き、オブジェクトに対するすべての操作でサポートされます。
  - GetObjectAcl
  - `OPTIONS /`
  - PutObjectLegalHold
  - PutObjectRetention
  - SelectObjectContent の順に選択します
- 同じキーに書き込む 2 つのクライアントなど、競合するクライアント要求は、「 latest-wins 」ベースで解決されます。「 latest-wins 」評価は、 S3 クライアントが処理を開始するタイミングではなく、 StorageGRID システムが特定の要求を完了したタイミングで行われます。
- StorageGRID バケット内のオブジェクトは、匿名ユーザまたは別のアカウントが作成したオブジェクトも含めて、すべてバケット所有者によって所有されます。

次の表に、 StorageGRID での S3 REST API オブジェクト処理の実装方法を示します。

操作	インプリメンテーション
deleteObject	DeleteObject要求を処理すると、StorageGRIDはすべての格納場所からオブジェクトのすべてのコピーをただちに削除しようとします。成功すると、 StorageGRID はただちにクライアントに応答を返します。30秒以内にすべてのコピーを削除できない場合（場所が一時的に使用できない場合など）、StorageGRID は削除対象のコピーをキューに登録し、クライアントに成功を通知します。 制限事項 • 多要素認証（MFA）と応答ヘッダー `x-amz-mfa`はサポートされていません。 • `If-Match`および `If-None-Match`ヘッダーの動作は、StorageGRIDの構成によって異なります。これらのヘッダーを指定すると、エラーメッセージ（501 Not Implemented）が返される場合があります。 `If-Match`または `If-None-Match`ヘッダーが受け入れられても機能しない場合、より厳格な501 Not Implementedエラー動作を有効にする手順を含むアラートがトリガーされる可能性があります。 `x-amz-bypass-governance-retention` ヘッダーは、S3 Object Lockのないオブジェクトには影響を与えません。 バージョン管理 特定のバージョンを削除するには、リクエスタがバケットの所有者であり、サブリソースを使用する必要があり `versionId`ます。このサブリソースを使用すると、バージョンが完全に削除されます。が削除マーカーに対応している場合は `versionId`、に設定された応答ヘッダー `x-amz-delete-marker`が返されます `true`。 • バージョン管理が有効になっているバケットでサブリソースを使用せずにオブジェクトを削除すると、 `versionId`削除マーカーが生成されます。削除マーカーのが `versionId`応答ヘッダーを使用して返され `x-amz-version-id`、 `x-amz-delete-marker`応答ヘッダーがに設定されて返されます `true`。 • バージョン管理が中断されているバケットでサブリソースを使用せずにオブジェクトを削除すると、 `versionId`既存の「null」バージョンまたは「null」削除マーカーが完全に削除され、新しい「null」削除マーカーが生成されます。 `x-amz-delete-marker`応答ヘッダーがに設定されて返され `true`ます。 • 注 * ：特定の場合、 1 つのオブジェクトに複数の削除マーカーが存在することがあります。 ガバナンスモードでオブジェクトバージョンを削除する方法については、を参照してください"S3 REST APIを使用してS3オブジェクトロックを設定します"。

操作	インプリメンテーション
オブジェクトの削除 （以前の名前はDELETE Multiple Objects）	多要素認証（MFA）と応答ヘッダー `x-amz-mfa`はサポートされていません。 同じ要求メッセージで複数のオブジェクトを削除できます。 `x-amz-bypass-governance-retention`ヘッダーは、S3 Object Lockのないオブジェクトには影響を与えません。 ガバナンスモードでオブジェクトバージョンを削除する方法については、を参照してください"S3 REST APIを使用してS3オブジェクトロックを設定します"。
DeleteObjectTagging	サブリソースを使用して、 `tagging`オブジェクトからすべてのタグを削除します。 バージョン管理 要求にクエリパラメータが指定されていない場合、 `versionId`バージョン管理されたバケット内のオブジェクトの最新バージョンからすべてのタグが削除されます。オブジェクトの現在のバージョンが削除マーカーの場合は、「MethodNotAllowed」ステータスが返され、 `x-amz-delete-marker`応答ヘッダーがに設定され `true`ます。
GetObject	"GetObject"
GetObjectAcl	アカウントに必要なアクセスクレデンシャルがある場合、オブジェクトの所有者にオブジェクトに対するフルアクセスがあることを示す応答が返され、所有者の ID 、表示名、および権限が表示されます。
GetObjectLegalHold	"S3 REST APIを使用してS3オブジェクトロックを設定します"
GetObjectRetention	"S3 REST APIを使用してS3オブジェクトロックを設定します"
GetObjectTagging	サブリソースを使用して、 `tagging`オブジェクトのすべてのタグを返します。 バージョン管理 要求にクエリパラメータが指定されていない場合、 `versionId`バージョン管理されたバケット内のオブジェクトの最新バージョンのすべてのタグが返されます。オブジェクトの現在のバージョンが削除マーカーの場合は、「MethodNotAllowed」ステータスが返され、 `x-amz-delete-marker`応答ヘッダーがに設定され `true`ます。
ヘッドオブジェクト	"ヘッドオブジェクト"

操作	インプリメンテーション
RestoreObject	"RestoreObject"
PutObject	"PutObject"
CopyObject （以前の名前はPUT Object - Copy ）	"CopyObject"
PutObjectLegalHold	"S3 REST APIを使用してS3オブジェクトロックを設定します"
PutObjectRetention	"S3 REST APIを使用してS3オブジェクトロックを設定します"

操作	インプリメンテーション
PutObjectTagging	サブリソースを使用して、 `tagging`既存のオブジェクトに一連のタグを追加します。 オブジェクトタグの制限 タグは、新しいオブジェクトをアップロードするときに追加することも、既存のオブジェクトに追加することもできます。StorageGRID と Amazon S3 はどちらも、オブジェクトごとに最大 10 個のタグをサポートします。オブジェクトに関連付けられたタグには、一意のタグキーが必要です。タグキーには Unicode 文字を 128 文字まで、タグ値には Unicode 文字を 256 文字まで使用できます。キーと値では大文字と小文字が区別されます。 タグの更新と取り込み動作 PutObjectTaggingを使用してオブジェクトのタグを更新した場合、StorageGRIDはオブジェクトを再取り込みしません。これは、一致する ILM ルールで指定されている取り込み動作が使用されないことを意味します。更新によって発生したオブジェクト配置の変更は、通常のバックグラウンド ILM プロセスで ILM が再評価されるときに実施されます。 つまり、ILMルールの取り込み動作にStrictオプションが使用されている場合、必要なオブジェクト配置を実行できない場合（新たに必要な場所が使用できない場合など）は処理されません。更新されたオブジェクトは、必要な配置を実行可能になるまで現在の配置が維持されます。 競合の解決 同じキーに書き込む 2 つのクライアントなど、競合するクライアント要求は、「 latest-wins 」ベースで解決されます。「 latest-wins 」評価は、 S3 クライアントが処理を開始するタイミングではなく、StorageGRID システムが特定の要求を完了したタイミングで行われます。 バージョン管理 要求にクエリパラメータが指定されていない場合は `versionId`、バージョン管理されたバケット内のオブジェクトの最新バージョンにタグが追加されます。オブジェクトの現在のバージョンが削除マーカーの場合は、「MethodNotAllowed」ステータスが返され、 `x-amz-delete-marker`応答ヘッダーがに設定され `true`ます。
SelectObjectContent の順に選択します	"SelectObjectContent の順に選択します"

StorageGRID でサポートされている **Amazon S3 Select** 操作

StorageGRIDは、で次のAmazon S3 Select句、データ型、および演算子をサポートしています"SelectObjectContent コマンド"。

リストされていない項目はサポートされていません。

構文については、を参照してください"SelectObjectContent の順に選択します"。S3 Selectの詳細については、を参照して "S3 Select に関する AWS のドキュメント"ください。

問題 SelectObjectContent クエリを実行できるのは、 S3 Select が有効になっているテナントアカウントのみです。を参照してください"S3 Select を使用する際の考慮事項と要件"。

句

- リストを選択します
- FROM 句
- WHERE 句
- Limit 句

データ型

- ブール値
- 整数
- 文字列
- 浮動小数点数
- 10 進数、数値
- タイムスタンプ

運用者

論理演算子

- および
- ありません
- または

比較演算子

- <
- >
- ⇐
- >=
- =
- =
- <>
- !=

- 間（ Between ）
- インチ

パターンマッチング演算子

- いいね
- _
- %

単一の演算子

- は NULL です
- は NULL ではありません

数学演算子

- +
- -
- *
- /
- %

StorageGRID はAmazon S3 Selectオペレータの優先順位に従います。

集合関数

- 平均 ()
- カウント（ * ）
- 最大 ()
- 最小（）
- 合計 ()

条件付き関数

- ケース
- 集合体
- NULLIF

変換関数

- CAST （サポートされているデータタイプ用）

日付関数

- date_add

- DATE_DIFF
- 展開する
- 文字列まで（ _STRING ）
- 終了タイムスタンプ
- UTCNOW

文字列関数

- char_length 、 character_length
- 低い
- サブストリング
- トリム（ Trim ）
- 上限

StorageGRIDがサーバー側の暗号化を使用する方法

サーバ側の暗号化を使用して、保存中のオブジェクトデータを保護できます。StorageGRID は、オブジェクトを書き込む際にデータを暗号化し、ユーザがオブジェクトにアクセスする際にデータを復号化します。

サーバ側の暗号化を使用する場合は、暗号化キーの管理方法に基づいて、次の 2 つのオプションを同時に選択できます。

- * SSE （ StorageGRID で管理されるキーによるサーバ側の暗号化） * ：オブジェクトを格納する S3 要求を問題 で暗号化すると、 StorageGRID は一意のキーでオブジェクトを暗号化します。オブジェクトを読み出す S3 要求を問題 で実行すると、 StorageGRID は格納されているキーを使用してオブジェクトを復号化します。
- * SSE-C （ユーザ指定のキーによるサーバ側の暗号化） * ：オブジェクトを格納する S3 要求を問題 で処理するときに、独自の暗号化キーを指定します。オブジェクトを読み出すときは、同じ暗号化キーを要求に指定します。2 つの暗号化キーが一致すると、オブジェクトが復号化されてオブジェクトデータが返されます。

  オブジェクトの暗号化処理と復号化処理はすべて StorageGRID で管理されますが、指定する暗号化キーはユーザが管理する必要があります。

> 指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。

> SSE または SSE-C で暗号化されたオブジェクトは、バケットレベルまたはグリッドレベルの暗号化設定が無視されます。

SSEを使用

StorageGRID で管理される一意のキーでオブジェクトを暗号化する場合は、次の要求ヘッダーを使用します。

`x-amz-server-side-encryption`

SSE 要求ヘッダーは、次のオブジェクト処理でサポートされます。

- "PutObject"
- "CopyObject"
- "CreateMultipartUpload"

SSE-C を使用します

ユーザが管理する一意のキーでオブジェクトを暗号化する場合は、次の 3 つの要求ヘッダーを使用します。

要求ヘッダー	製品説明
`x-amz-server-side-encryption-customer-algorithm`	暗号化アルゴリズムを指定します。ヘッダー値はである必要があります `AES256`。
`x-amz-server-side-encryption-customer-key`	オブジェクトの暗号化と復号化に使用する暗号化キーを指定します。キーの値は、 Base64 でエンコードされた 256 ビットであることが必要です。
`x-amz-server-side-encryption-customer-key-MD5`	RFC 1321 に従って暗号化キーの MD5 ダイジェストを指定します。これは、暗号化キーがエラーなしで送信されたことを確認するために使用されます。MD5 ダイジェストの値は、 Base64 でエンコードされた 128 ビットであることが必要です。

SSE-C 要求ヘッダーは、次のオブジェクト処理でサポートされます。

- "GetObject"
- "ヘッドオブジェクト"
- "PutObject"
- "CopyObject"
- "CreateMultipartUpload"
- "パーツのアップロード"
- "パーツコピーをアップロード"

ユーザ指定のキーによるサーバ側の暗号化（ **SSE-C** ）を使用する場合の考慮事項

SSE-C を使用する場合は、次の考慮事項に注意してください。

- HTTPS を使用する必要があります。

> SSE-Cを使用している場合、StorageGRIDはhttp経由で行われた要求を拒否します。セキュリティ上の考慮事項として、httpを使用して誤って送信したキーは侵害されることを考慮する必要があります。キーを破棄し、必要に応じてローテーションします。

- 応答内の ETag は、オブジェクトデータの MD5 ではありません。
- 暗号化キーとオブジェクトの対応関係を管理する必要があります。StorageGRID では暗号化キーは格納されません。各オブジェクトに対して指定した暗号化キーを管理する責任はユーザにあります。
- バケットのバージョン管理が有効になっている場合は、オブジェクトのバージョンごとに固有の暗号化キーが必要です。各オブジェクトバージョンで使用される暗号化キーを管理する責任はユーザにあります。
- 暗号化キーはクライアント側で管理するため、キーローテーションなどの追加の防護策もクライアント側で管理する必要があります。

> 指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。

- バケットにクロスグリッドレプリケーションまたはCloudMirrorレプリケーションが設定されている場合は、SSE-Cオブジェクトを取り込むことはできません。取り込み処理は失敗します。

関連情報

"Amazon S3ユーザガイド：ユーザ指定のキーによるサーバ側の暗号化（SSE-C）の使用"

S3 CopyObjectリクエストを使用して**StorageGRID**でオブジェクトのコピーを作成する

S3 CopyObject要求を使用して、すでにS3に格納されているオブジェクトのコピーを作成できます。CopyObject操作は、GetObjectを実行してからPutObjectを実行する操作と同じです。

競合を解決します

同じキーに書き込む 2 つのクライアントなど、競合するクライアント要求は、「 latest-wins 」ベースで解決されます。「 latest-wins 」評価は、 S3 クライアントが処理を開始するタイミングではなく、 StorageGRID システムが特定の要求を完了したタイミングで行われます。

オブジェクトのサイズ

1回のPutObject処理の最大推奨サイズは5GiB（5、368、709、120バイト）です。5GiBを超えるオブジェクトがある場合は、代わりにを使用します"マルチパートアップロード"。

1回のPutObject処理のmaximum_supported_sizeは5TiB（5、497、558、138、880バイト）です。

> StorageGRID 11.6以前からアップグレードした場合、5GiBを超えるオブジェクトをアップロードしようとすると、S3 PUT Object size too largeアラートがトリガーされます。StorageGRID 11.7または11.8を新規にインストールした場合、この場合アラートはトリガーされません。ただし、AWS S3標準に準拠するため、StorageGRIDの今後のリリースでは5GiBを超えるオブジェクトのアップロードはサポートされません。

ユーザメタデータ内の **UTF-8** 文字

要求のユーザ定義メタデータのキー名または値に（エスケープされていない） UTF-8 文字が含まれている場合、 StorageGRID の動作は定義されていません。

StorageGRID は、ユーザー定義メタデータのキー名または値に含まれるエスケープされた UTF-8 文字を解析または解釈しません。エスケープされた UTF-8 文字は ASCII 文字として扱われます：

- ユーザ定義メタデータにエスケープされた UTF-8 文字が含まれている場合、要求は正常に実行されます。
- StorageGRID は、キー名または値の解釈された値に印刷不可能な文字が含まれている場合、 `x-amz-missing-meta` ヘッダーを返しません。

サポートされる要求ヘッダー

次の要求ヘッダーがサポートされています。

- `Content-Type`
- `x-amz-checksum-algorithm`： `CRC32`、 `CRC32C`、 `CRC64NVME`、または `SHA256`を指定します

  オブジェクトをコピーする場合、ソースオブジェクトに `checksum`が含まれているか、または `x-amz-checksum-algorithm`が含まれている場合、コピーされたオブジェクトにはFULL_OBJECTチェックサムが付与されます。

  ソースオブジェクトにチェックサムがあるが、リクエストに `x-amz-checksum-algorithm`が含まれていない場合、またはサポートされていないチェックサム値を使用している場合、コピーされたオブジェクトはソースオブジェクトと同じタイプのチェックサムを持ちます。StorageGRID は、無効またはサポートされていない `x-amz-checksum-algorithm`値を無視します。

  ソースオブジェクトにチェックサムがなく、 `x-amz-checksum-algorithm`が含まれていない場合、またはサポートされていないチェックサム値を使用している場合、コピーされたオブジェクトにはチェックサムがありません。

  > CopyObjectリクエストでチェックサムが指定されておらず、ソースオブジェクトにもチェックサムがない場合、StorageGRIDはオブジェクトのデフォルトのCRC-64/NVMEチェックサムを計算しません。

- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`
- `x-amz-meta-`に続けて、ユーザ定義のメタデータを含む名前と値のペアを指定します。
- `x-amz-metadata-directive`：デフォルト値はで `COPY`、オブジェクトと関連するメタデータをコピーできます。

  オブジェクトのコピー時に既存のメタデータを上書きするか、オブジェクトメタデータを更新するかを指定でき `REPLACE`ます。

- `x-amz-storage-class`
- `x-amz-tagging-directive`：デフォルト値はで `COPY`、オブジェクトとすべてのタグをコピーできます。

  オブジェクトのコピー時に既存のタグを上書きするか、タグを更新するかを指定でき `REPLACE`ます。

- S3 オブジェクトロック要求のヘッダー：
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

    これらのヘッダーを指定せずに要求を行うと、バケットのデフォルトの保持設定を使用してオブジェクトバージョンモードとretain-until-dateが計算されます。を参照して "S3 REST APIを使用してS3オブジェクトロックを設定します"
- SSE 要求ヘッダー：
  - `x-amz-copy-source-server-side-encryption-customer-algorithm`
  - `x-amz-copy-source-server-side-encryption-customer-key`
  - `x-amz-copy-source-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    を参照し [サーバ側の暗号化を行うための要求ヘッダー]

サポートされない要求ヘッダーです

次の要求ヘッダーはサポートされていません。

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `If-Match`

  > `If-Match`ヘッダーの動作は、StorageGRIDの構成によって異なります。このヘッダーを指定すると、エラーメッセージ（`501 Not Implemented`）が返される可能性があります。 `If-Match`ヘッダーが受け入れられたものの機能しない場合、より厳格な`501 Not Implemented`エラー動作を有効にするための手順を示すアラートが表示される可能性があります。

- `If-None-Match`

`If-None-Match`ヘッダーの動作は、StorageGRIDの構成によって異なります。このヘッダーを指定すると、エラーメッセージ（501 Not Implemented）が返される可能性があります。 `If-None-Match`ヘッダーが受け入れられたものの機能しない場合、より厳格な501 Not Implementedエラー動作を有効にするための手順を示すアラートが表示される可能性があります。

- x-amz-website-redirect-location

ストレージクラスのオプション

`x-amz-storage-class`要求ヘッダーはサポートされており、一致するILMルールでDual commitまたはBalancedが使用されている場合にStorageGRIDで作成されるオブジェクトコピーの数に影響しますlink:../ilm/data-protection-options-for-ingest.html["取り込みオプション"]。

- STANDARD

  （デフォルト） ILM ルールで Dual commit オプションが使用されている場合、または Balanced オプションによって中間コピーが作成される場合に、デュアルコミットの取り込み処理を指定します。

- REDUCED_REDUNDANCY

  ILM ルールで Dual commit オプションが使用されている場合、または Balanced オプションによって中間コピーが作成される場合に、シングルコミットの取り込み処理を指定します。

  S3 Object Lockが有効なバケットにオブジェクトを取り込む場合、この`REDUCED_REDUNDANCY`オプションは無視されます。従来の準拠バケットにオブジェクトを取り込む場合、オプションを指定すると `REDUCED_REDUNDANCY`エラーが返されます。StorageGRID では、常にデュアルコミットの取り込みが実行され、コンプライアンス要件が満たされます。

CopyObjectでの**x-amz-copy-source**の使用

ヘッダーで指定されたソースのバケットおよびキーがデスティネーションのバケットおよびキーと異なる場合は x-amz-copy-source、ソースのオブジェクトデータのコピーがデスティネーションに書き込まれます。

送信元と宛先が一致し、 `x-amz-metadata-directive`ヘッダーが `REPLACE`として指定されている場合、オブジェクトのメタデータはリクエストで指定されたメタデータ値で更新されます。この場合、StorageGRID はオブジェクトを再取り込みしません。これには2つの重要な結果があります。

- CopyObjectを使用して既存のオブジェクトを暗号化したり、既存のオブジェクトの暗号化を変更したりすることはできません。ヘッダーまたは x-amz-server-side-encryption-customer-algorithm`ヘッダーを指定すると `x-amz-server-side-encryption、StorageGRIDは要求を拒否してを返します XNotImplemented。
- 一致するILMルールで指定されている「取り込み動作」オプションは使用されません。アップデートによ

って発生するオブジェクト配置の変更は、通常のバックグラウンドILMプロセスによってILMが再評価された際に反映されます。

つまり、ILMルールの取り込み動作にStrictオプションが使用されている場合、必要なオブジェクト配置を実行できない場合（新たに必要な場所が使用できない場合など）は処理されません。更新されたオブジェクトは、必要な配置を実行可能になるまで現在の配置が維持されます。

サーバ側の暗号化を行うための要求ヘッダー

を使用する場合、"サーバ側の暗号化を使用する"指定する要求ヘッダーは、ソースオブジェクトが暗号化されているかどうか、およびターゲットオブジェクトを暗号化するかどうかによって異なります。

- ソースオブジェクトがユーザ指定のキーを使用して暗号化されている場合（SSE-C）は、オブジェクトを復号化してコピーできるように、CopyObject要求に次の3つのヘッダーを含める必要があります。
  - `x-amz-copy-source-server-side-encryption-customer-algorithm`:指定します `AES256`。
  - `x-amz-copy-source-server-side-encryption-customer-key`：ソースオブジェクトの作成時に指定した暗号化キーを指定します。
  - `x-amz-copy-source-server-side-encryption-customer-key-MD5`:ソースオブジェクトの作成時に指定したMD5ダイジェストを指定します。
- ユーザが指定および管理する一意のキーでターゲットオブジェクト（コピー）を暗号化する場合は、次の 3 つのヘッダーを含めます。
  - `x-amz-server-side-encryption-customer-algorithm`:指定します `AES256`。
  - `x-amz-server-side-encryption-customer-key`：ターゲットオブジェクトの新しい暗号化キーを指定します。
  - `x-amz-server-side-encryption-customer-key-MD5`：新しい暗号化キーのMD5ダイジェストを指定します。

> 指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。ユーザ指定のキーを使用してオブジェクトデータを保護する前に、の考慮事項を確認してください"サーバ側の暗号化を使用する"。

- ターゲットオブジェクト（コピー）をStorageGRID（SSE）で管理される一意のキーで暗号化する場合は、CopyObject要求に次のヘッダーを含めます。
  - `x-amz-server-side-encryption`

> `server-side-encryption`オブジェクトの値を更新できません。代わりに、：`REPLACE`を使用して新しい値 `x-amz-metadata-directive`でコピーを作成します `server-side-encryption`。

バージョン管理

ソースバケットがバージョン管理に対応している場合は、ヘッダーを使用してオブジェクトの最新バージョンをコピーできます `x-amz-copy-source`。オブジェクトの特定のバージョンをコピーするには'サブリソースを使用してコピーするバージョンを明示的に指定する必要があり `versionId`ますデスティネーションバケットがバージョン管理に対応している場合は、生成されたバージョンが応答ヘッダーで返され `x-amz-version-id`ます。ターゲットバケットでバージョン管理が一時停止されている場合は `x-amz-`

version-id、「null」の値が返されます。

StorageGRID のバケットから **GetObject** リクエストでオブジェクトを取得する

S3 GetObject要求を使用すると、S3バケットからオブジェクトを読み出すことができます。

GetObjectオブジェクトとマルチパートオブジェクト

要求パラメータを使用すると、マルチパートオブジェクトまたはセグメント化されたオブジェクトの特定の部分を読み出すことができます partNumber。 `x-amz-mp-parts-count`response要素は、オブジェクトに含まれるパーツの数を示します。

セグメント化されたオブジェクト/マルチパートオブジェクトとセグメント化されていないオブジェクト/マルチパート以外のオブジェクトの両方で1に設定できます partNumber。ただし、 `x-amz-mp-parts-count`応答要素はセグメント化されたオブジェクトまたはマルチパートオブジェクトの場合にのみ返されます。

ユーザメタデータ内の **UTF-8** 文字

StorageGRID は、ユーザ定義メタデータ内のエスケープされた UTF-8 文字を解析も解釈もしません。ユーザ定義メタデータにエスケープされたUTF-8文字が含まれているオブジェクトに対するGET要求で、キーの名前または値に印刷不能文字が含まれている場合にヘッダーが返されません x-amz-missing-meta。

サポートされる要求ヘッダー

次の要求ヘッダーがサポートされています。

- Accept-Encoding

  オブジェクトに保存された Content-Encoding`がない場合、 `Accept-Encoding: gzip`を使用したGETリクエストは、レスポンスにリアルタイムで圧縮を適用します。 `gzip`のみがGETレスポンスのエンコーディングに影響します。 `deflate、 br、および `identity`は影響しません。既に保存された`Content-Encoding`があるオブジェクトの場合、StorageGRIDは保存されたエンコーディングを返し、`Accept-Encoding`に基づくリアルタイム圧縮は追加で適用しません。StorageGRIDは、 `Accept-Encoding: gzip`を使用したGETリクエストに対する範囲読み取り操作をサポートしていません。

- x-amz-checksum-mode:指定 ENABLED

  > `Range`for GetObjectではヘッダーはサポートされていません `x-amz-checksum-mode`。enabledを指定して要求 `x-amz-checksum-mode`にを含める `Range` と、StorageGRIDは応答にチェックサム値を返しません。

サポートされない要求ヘッダーです

次の要求ヘッダーはサポートされておらず、が返されます。 XNotImplemented

- x-amz-website-redirect-location

バージョン管理

サブリソースを指定しない場合は `versionId`、バージョン管理されたバケット内のオブジェクトの最新バージョンが取得されます。オブジェクトの現在のバージョンが削除マーカーの場合は、「Not Found」ステータスが返され、 `x-amz-delete-marker`応答ヘッダーがに設定され `true`ます。

ユーザ指定の暗号化キーによるサーバ側の暗号化（ **SSE-C** ）の要求ヘッダー

指定した一意のキーでオブジェクトが暗号化されている場合は、 3 つのヘッダーをすべて使用します。

- `x-amz-server-side-encryption-customer-algorithm`:指定します `AES256`。
- `x-amz-server-side-encryption-customer-key`：オブジェクトの暗号化キーを指定します。
- `x-amz-server-side-encryption-customer-key-MD5`:オブジェクトの暗号化キーのMD5ダイジェストを指定します。

> 指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。ユーザ指定のキーを使用してオブジェクトデータを保護する前に、の考慮事項を確認してください"サーバ側の暗号化を使用します"。

クラウドストレージプールオブジェクトに対する**GetObject**の動作

オブジェクトがに格納されている場合"クラウドストレージプール"、GetObject要求の動作はオブジェクトの状態によって異なります。詳細については、を参照してください"ヘッドオブジェクト"。

> オブジェクトがクラウドストレージプールに格納されていて、そのオブジェクトのコピーがグリッドに1つ以上存在する場合、GetObject要求はクラウドストレージプールからデータを読み出す前にグリッドからデータを読み出そうとします。

オブジェクトの状態	**GetObject**の動作
StorageGRID に取り込まれているがまだ ILM によって評価されていないオブジェクト、または従来のストレージプールに格納されているオブジェクト、またはイレイジャーコーディングを使用しているオブジェクト	`200 OK` オブジェクトのコピーが読み出されます。
クラウドストレージプール内にあるが、まだ読み出し不可能な状態に移行していない	`200 OK` オブジェクトのコピーが読み出されます。
オブジェクトを読み出し不可能な状態に移行した	`403 Forbidden、 InvalidObjectState` 要求を使用し"RestoreObject"て、オブジェクトを読み出し可能な状態にリストアします。
読み出し不可能な状態からリストア中である	`403 Forbidden、 InvalidObjectState` RestoreObject要求が完了するまで待ちます。

オブジェクトの状態	**GetObject**の動作
クラウドストレージプールへのリストアが完了している	`200 OK` オブジェクトのコピーが読み出されます。

クラウドストレージプール内のマルチパートオブジェクトまたはセグメント化されたオブジェクト

マルチパートオブジェクトをアップロードした場合や StorageGRID が大きなオブジェクトをセグメントに分割した場合、 StorageGRID はオブジェクトのパーツまたはセグメントのサブセットをサンプリングすることでクラウドストレージプール内のオブジェクトが使用可能かどうかを判断します。オブジェクトの一部がすでに読み出し不可能な状態に移行されている場合や、オブジェクトの一部がまだリストアされていない場合に、GetObject要求が誤って返されることがあります `200 OK`。

このような場合は、次のよう

- GetObject要求から一部のデータが返される場合がありますが、転送の途中で停止することがあります。
- 後続のGetObject要求が返されることがあります `403 Forbidden`。

GetObjectとグリッド間レプリケーション

を使用していて"グリッド間レプリケーション"バケットで有効になっている場合"グリッドフェデレーション"、S3クライアントはGetObject要求を発行してオブジェクトのレプリケーションステータスを確認できます。応答には、次のいずれかの値を持つStorageGRID固有の応答ヘッダーが含まれ `x-ntap-sg-cgr-replication-status`ます。

グリッド	レプリケーションのステータス
ソース	• 完了:レプリケーションは成功しました。 • * pending*：オブジェクトはまだレプリケートされていません。 • **failure**:レプリケーションが永続的なエラーで失敗しました。ユーザーはエラーを解決する必要があります。
デスティネーション	**replica**:オブジェクトはソースグリッドからレプリケートされました。

StorageGRIDはヘッダーをサポートしていません `x-amz-replication-status`。

StorageGRID の **S3 HeadObject** リクエストを使用してオブジェクトからメタデータを取得する

S3 HeadObject要求を使用すると、オブジェクト自体を返さずにオブジェクトからメタデータを読み出すことができます。オブジェクトがクラウドストレージプールに格納されている場合は、HeadObjectを使用してオブジェクトの移行状態を確認できます。

HeadObjectオブジェクトとマルチパートオブジェクト

要求パラメータを使用すると、マルチパートオブジェクトまたはセグメント化されたオブジェクトの特定の部分のメタデータを読み出すことができます `partNumber`。 `x-amz-mp-parts-count`response要素は、オブジ

ェクトに含まれるパーツの数を示します。

セグメント化されたオブジェクト/マルチパートオブジェクトとセグメント化されていないオブジェクト/マルチパート以外のオブジェクトの両方で1に設定できます `partNumber`。ただし、 `x-amz-mp-parts-count`応答要素はセグメント化されたオブジェクトまたはマルチパートオブジェクトの場合にのみ返されます。

ユーザメタデータ内の **UTF-8** 文字

StorageGRID は、ユーザ定義メタデータ内のエスケープされた UTF-8 文字を解析も解釈もしません。ユーザ定義メタデータにエスケープされたUTF-8文字が含まれているオブジェクトに対するHEAD要求で、キーの名前または値に印刷不能文字が含まれている場合にヘッダーが返されません `x-amz-missing-meta`。

サポートされる要求ヘッダー

次の要求ヘッダーがサポートされます。

- `x-amz-checksum-mode`

> `partNumber`パラメータと `Range`ヘッダーは、for `HeadObject`ではサポートされていません `x-amz-checksum-mode`。 `enabled`を指定して要求に含める `x-amz-checksum-mode`と、 `StorageGRID`は応答でチェックサム値を返しません。

サポートされない要求ヘッダーです

次の要求ヘッダーはサポートされていないため、が返されます。 `XNotImplemented`

- `x-amz-website-redirect-location`

バージョン管理

サブリソースを指定しない場合は `versionId`、バージョン管理されたバケット内のオブジェクトの最新バージョンが取得されます。オブジェクトの現在のバージョンが削除マーカーの場合は、「Not Found」ステータスが返され、 `x-amz-delete-marker`応答ヘッダーがに設定され `true`ます。

ユーザ指定の暗号化キーによるサーバ側の暗号化（ **SSE-C** ）の要求ヘッダー

指定した一意のキーでオブジェクトが暗号化されている場合は、次の 3 つのヘッダーをすべて使用します。

- `x-amz-server-side-encryption-customer-algorithm`:指定します `AES256`。
- `x-amz-server-side-encryption-customer-key`：オブジェクトの暗号化キーを指定します。
- `x-amz-server-side-encryption-customer-key-MD5`:オブジェクトの暗号化キーのMD5ダイジェストを指定します。

> 指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。ユーザ指定のキーを使用してオブジェクトデータを保護する前に、の考慮事項を確認してください"サーバ側の暗号化を使用します"。

クラウドストレージプールオブジェクトに対する**HeadObject**応答

オブジェクトがに格納されている場合は"クラウドストレージプール"、次の応答ヘッダーが返されます。

- `x-amz-storage-class: GLACIER`
- `x-amz-restore`

応答ヘッダーは、オブジェクトがクラウドストレージプールに移動され、必要に応じて読み出し不可能な状態に移行されてリストアされるときの状態に関する情報を提供します。

オブジェクトの状態	**HeadObject**への応答
StorageGRID に取り込まれているがまだ ILM によって評価されていないオブジェクト、または従来のストレージプールに格納されているオブジェクト、またはイレイジャーコーディングを使用しているオブジェクト	`200 OK`（特別な応答ヘッダーは返されません）。

クラウドストレージプール内にあるが、まだ読み出し不可能な状態に移行していない	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	オブジェクトが読み出し不可能な状態に移行されるまでは、の値は `expiry-date`将来の任意の時刻に設定されます。移行の正確な時間は、 StorageGRID システムでは制御されません。

オブジェクトが読み出し不可能な状態に移行したが、少なくとも 1 つのコピーがグリッドに存在する	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	の値は、 `expiry-date`将来の遠い時刻に設定されています。
	
	注：グリッド上のコピーを使用できない場合（ストレージノードが停止している場合など）は、オブジェクトを正常に読み出す前に、クラウドストレージプールからコピーをリストアする要求を実行する必要があります"RestoreObject"。

オブジェクトの状態	**HeadObject**への応答

読み出し不可能な状態に移行しており、グリッドにコピーが存在しない	`200 OK`
	
	`x-amz-storage-class: GLACIER`

読み出し不可能な状態からリストア中である	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="true"`

クラウドストレージプールへのリストアが完了している	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2018 00:00:00 GMT"`
	
	には `expiry-date`、クラウドストレージプール内のオブジェクトが読み出し不可能な状態に戻るタイミングが示されます。

クラウドストレージプール内のマルチパートオブジェクトまたはセグメント化されたオブジェクト

マルチパートオブジェクトをアップロードした場合や StorageGRID が大きなオブジェクトをセグメントに分割した場合、 StorageGRID はオブジェクトのパーツまたはセグメントのサブセットをサンプリングすることでクラウドストレージプール内のオブジェクトが使用可能かどうかを判断します。オブジェクトの一部がすでに読み出し不可能な状態に移行されている場合や、オブジェクトの一部がまだリストアされていない場合に、HeadObject要求が誤って返されることがあります `x-amz-restore: ongoing-request="false"`。

HeadObjectとクロスグリッドレプリケーション

を使用していて"グリッド間レプリケーション"バケットで有効になっている場合"グリッドフェデレーション"、S3クライアントはHeadObject要求を発行してオブジェクトのレプリケーションステータスを確認できます。応答には、次のいずれかの値を持つStorageGRID固有の応答ヘッダーが含まれ `x-ntap-sg-cgr-replication-status`ます。

グリッド	レプリケーションのステータス
ソース	• 完了:レプリケーションは成功しました。 • * pending*：オブジェクトはまだレプリケートされていません。 • **failure**:レプリケーションが永続的なエラーで失敗しました。ユーザーはエラーを解決する必要があります。
デスティネーション	**replica**:オブジェクトはソースグリッドからレプリケートされました。

StorageGRIDはヘッダーをサポートしていません `x-amz-replication-status`。

S3 PutObjectリクエストを使用して**StorageGRID**のバケットにオブジェクトを追加する

S3 PutObject要求を使用して、バケットにオブジェクトを追加できます。

競合を解決します

同じキーに書き込む 2 つのクライアントなど、競合するクライアント要求は、「 latest-wins 」ベースで解決されます。「 latest-wins 」評価は、 S3 クライアントが処理を開始するタイミングではなく、 StorageGRID システムが特定の要求を完了したタイミングで行われます。

オブジェクトのサイズ

1回のPutObject処理の最大推奨サイズは5GiB（5、368、709、120バイト）です。5GiBを超えるオブジェクトがある場合は、代わりにを使用します"マルチパートアップロード"。

1回のPutObject処理のmaximum_supported_sizeは5TiB（5、497、558、138、880バイト）です。

StorageGRID 11.6以前からアップグレードした場合、5GiBを超えるオブジェクトをアップロードしようとすると、S3 PUT Object size too largeアラートがトリガーされます。StorageGRID 11.7または11.8を新規にインストールした場合、この場合アラートはトリガーされません。ただし、AWS S3標準に準拠するため、StorageGRIDの今後のリリースでは5GiBを超えるオブジェクトのアップロードはサポートされません。

ユーザメタデータのサイズ

Amazon S3 では、各 PUT 要求ヘッダー内のユーザ定義メタデータのサイズが 2KB に制限されます。StorageGRID では、ユーザメタデータが 24KiB に制限されます。ユーザ定義のメタデータのサイズは、各キーと値の UTF-8 エンコードでのバイト数の合計で測定されます。

ユーザメタデータ内の **UTF-8** 文字

要求のユーザ定義メタデータのキー名または値に（エスケープされていない） UTF-8 文字が含まれている場合、 StorageGRID の動作は定義されていません。

ユーザ定義メタデータのキー名または値に含まれているエスケープされた UTF-8 文字は、 StorageGRID で解析も解釈もされません。エスケープされた UTF-8 文字は ASCII 文字として扱われます。

- ユーザ定義メタデータにエスケープされたUTF-8文字が含まれている場合、PutObject、CopyObject 、GetObject、およびHeadObjectの各要求は成功します。
- キーの名前または値の解釈された値に印刷不能文字が含まれている場合、StorageGRIDはヘッダーを返しません `x-amz-missing-meta`。

オブジェクトタグの制限

タグは、新しいオブジェクトをアップロードするときに追加することも、既存のオブジェクトに追加することもできます。StorageGRID と Amazon S3 はどちらも、オブジェクトごとに最大 10 個のタグをサポートします。オブジェクトに関連付けられたタグには、一意のタグキーが必要です。タグキーには Unicode 文字を 128 文字まで、タグ値には Unicode 文字を 256 文字まで使用できます。キーと値では大文字と小文字が区別

されます。

オブジェクトの所有権

StorageGRID では、非所有者アカウントまたは匿名ユーザによって作成されたオブジェクトを含むすべてのオブジェクトが、バケット所有者アカウントによって所有されます。

サポートされる要求ヘッダー

次の要求ヘッダーがサポートされています。

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`

  > `aws-chunked`に `Content-Encoding`を指定した場合、StorageGRID は以下の項目を検証しません。

  - StorageGRID は、 `chunk-signature`をチャンクデータと照合して検証しません。
  - StorageGRIDは、 `x-amz-decoded-content-length`に指定した値をオブジェクトに対して検証しません。
- `Content-Language`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Expires`
- `Transfer-Encoding`

  ペイロード署名も使用されている場合は、チャンク転送エンコーディングがサポートされ `aws-chunked` ます。

- チェックサム要求ヘッダー：
  - `x-amz-checksum-crc32`
  - `x-amz-checksum-crc32c`
  - `x-amz-checksum-crc64nvme`
  - `x-amz-checksum-sha256`

  > PutObjectリクエストでチェックサムが指定されていない場合、StorageGRIDはオブジェクトのデフォルトのCRC-64/NVMEチェックサムを計算しません。

- `x-amz-meta-`に続けて、ユーザ定義のメタデータを含む名前と値のペアを指定します。

  ユーザ定義メタデータの名前と値のペアを指定する場合、一般的な形式は次のとおりです。

```
x-amz-meta-name: value
```

ILMルールの参照時間に*[ユーザ定義の作成時間]*オプションを使用する場合は、オブジェクトの作成日時を記録するメタデータの名前にを使用する必要があります `creation-time`。例：

```
x-amz-meta-creation-time: 1443399726
```

の値 `creation-time`は、1970年1月1日からの秒数として評価されます。

> ILMルールでは、参照時間に*ユーザ定義の作成時間*を使用し、取り込みオプションをBalancedまたはStrictの両方にすることはできません。ILM ルールの作成時にエラーが返されます。

- `x-amz-tagging`
- S3 Object Lock 要求のヘッダー
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

    これらのヘッダーを指定せずに要求を行うと、バケットのデフォルトの保持設定を使用してオブジェクトバージョンモードとretain-until-dateが計算されます。を参照して "S3 REST APIを使用してS3オブジェクトロックを設定します"
- SSE 要求ヘッダー：
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    を参照し [サーバ側の暗号化を行うための要求ヘッダー]

サポートされない要求ヘッダーです

次の要求ヘッダーはサポートされていません。

- `If-Match`

`If-Match`ヘッダーの動作は、StorageGRIDの構成によって異なります。このヘッダーを指定すると、エラーメッセージ（501 Not Implemented）が返される可能性があります。 `If-Match`ヘッダーが受け入れられたものの機能しない場合、より厳格な501 Not Implementedエラー動作を有効にするための手順を示すアラートが表示される可能性があります。

- If-None-Match

`If-None-Match`ヘッダーの動作は、StorageGRIDの構成によって異なります。このヘッダーを指定すると、エラーメッセージ（501 Not Implemented）が返される可能性があります。 `If-None-Match`ヘッダーが受け入れられたものの機能しない場合、より厳格な501 Not Implementedエラー動作を有効にするための手順を示すアラートが表示される可能性があります。

- x-amz-acl
- x-amz-checksum-md5
- x-amz-checksum-sha1
- x-amz-checksum-sha512
- x-amz-checksum-xxhash3
- x-amz-checksum-xxhash64
- x-amz-checksum-xxhash128
- x-amz-sdk-checksum-algorithm
- x-amz-trailer
- x-amz-website-redirect-location

`x-amz-website-redirect-location`ヘッダーが返され `XNotImplemented`ます。

ストレージクラスのオプション

`x-amz-storage-class`要求ヘッダーがサポートされます。で送信される値 `x-amz-storage-class`は、StorageGRIDによる取り込み時のオブジェクトデータの保護方法に影響し、StorageGRIDシステムに格納されるオブジェクトの永続的コピーの数（ILMで決定）には影響しません。

取り込まれたオブジェクトに一致するILMルールでStrict取り込みオプションが使用されている場合、`x-amz-storage-class`ヘッダーは効果がありません。

には次の値を使用でき `x-amz-storage-class`ます。

- `STANDARD`（デフォルト）
  - * Dual commit * ： ILM ルールの取り込み動作が Dual commit オプションに指定されている場合は、オブジェクトの取り込み直後にオブジェクトの 2 つ目のコピーが作成されて別のストレージノードに配置されます（デュアルコミット）。ILMが評価されると、StorageGRID はこれらの初期中間コピーがルールの配置手順を満たしているかどうかを判断します。作成されていない場合は、新しいオブジェクトコピーを別の場所に作成し、最初の中間コピーを削除しなければならないことがあります。
  - * Balanced *：ILMルールでBalancedオプションが指定されていて、ルールで指定されたすべてのコピーをStorageGRID がすぐに作成できない場合、StorageGRID は2つの中間コピーを別 々 のストレージノードに作成します。

    ILMルールで指定されたすべてのオブジェクトコピーをStorageGRIDでただちに作成できる場合（同期配置）、 `x-amz-storage-class`ヘッダーは効果がありません。

- `REDUCED_REDUNDANCY`
  - * Dual commit * ： ILM ルールの取り込み動作が Dual commit オプションに指定されている場合は、オブジェクトの取り込み時に StorageGRID が中間コピーを 1 つ作成します（シングルコミット）。
  - * Balanced *：ILMルールでBalancedオプションが指定されている場合、StorageGRID は、ルールで指定されたすべてのコピーをただちに作成できない場合にのみ中間コピーを1つ作成します。StorageGRID で同期配置を実行できる場合、このヘッダーは効果がありません。 `REDUCED_REDUNDANCY`オブジェクトに一致するILMルールで単一のレプリケートコピーが作成される場合は、オプションの使用を推奨します。この場合、を使用する `REDUCED_REDUNDANCY`と、取り込み処理のたびに余分なオブジェクトコピーを不要に作成および削除する必要がなくなります。

  それ以外の状況では、オプションの使用 `REDUCED_REDUNDANCY`は推奨されません。 `REDUCED_REDUNDANCY`取り込み中にオブジェクトデータが失われるリスクが高まります。たとえば、 ILM 評価の前にコピーが 1 つだけ格納されていたストレージノードに障害が発生すると、データが失われる可能性があります。

> レプリケートコピーを一定期間に 1 つだけ作成すると、データが永続的に失われるリスクがあります。オブジェクトのレプリケートコピーが 1 つしかない場合、ストレージノードに障害が発生したり、重大なエラーが発生すると、そのオブジェクトは失われます。また、アップグレードなどのメンテナンス作業中は、オブジェクトへのアクセスが一時的に失われます。

を指定する `REDUCED_REDUNDANCY`と、オブジェクトを最初に取り込んだときに作成されるコピー数にのみ影響します。オブジェクトがアクティブなILMポリシーで評価される際に作成されるオブジェクトのコピー数には影響せず、StorageGRIDシステムでデータが格納される際の冗長性レベルが低下することもありません。

> S3 Object Lockが有効なバケットにオブジェクトを取り込む場合、この `REDUCED_REDUNDANCY`オプションは無視されます。従来の準拠バケットにオブジェクトを取り込む場合、オプションを指定すると `REDUCED_REDUNDANCY`エラーが返されます。StorageGRID では、常にデュアルコミットの取り込みが実行され、コンプライアンス要件が満たされます。

サーバ側の暗号化を行うための要求ヘッダー

オブジェクトをサーバ側の暗号化で暗号化するには、次の要求ヘッダーを使用します。SSE オプションと

SSE-C オプションを同時に指定することはできません。

- * SSE * ： StorageGRID で管理される一意のキーでオブジェクトを暗号化するには、次のヘッダーを使用します。
  - `x-amz-server-side-encryption`

    ヘッダーがPutObject要求に含まれていない場合、 `x-amz-server-side-encryption`PutObject応答からグリッド全体が"格納オブジェクトの暗号化設定"省略されます。

- * SSE-C * ：ユーザが指定および管理する一意のキーでオブジェクトを暗号化する場合は、次の 3 つのヘッダーをすべて使用します。
  - `x-amz-server-side-encryption-customer-algorithm`:指定します `AES256`。
  - `x-amz-server-side-encryption-customer-key`：新しいオブジェクトの暗号化キーを指定します。
  - `x-amz-server-side-encryption-customer-key-MD5`：新しいオブジェクトの暗号化キーのMD5ダイジェストを指定します。

> 指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。ユーザ指定のキーを使用してオブジェクトデータを保護する前に、の考慮事項を確認してください"サーバ側の暗号化を使用する"。

> SSE または SSE-C で暗号化されたオブジェクトは、バケットレベルまたはグリッドレベルの暗号化設定が無視されます。

バージョン管理

バケットでバージョン管理が有効になっている場合は、格納されているオブジェクトのバージョンに対して一意のが `versionId`自動的に生成されます。これは `versionId`、応答ヘッダーを使用した応答でも返され`x-amz-version-id`ます。

バージョン管理が一時停止されている場合、オブジェクトのバージョンはnullで格納され `versionId`、nullのバージョンがすでに存在する場合は上書きされます。

Authorizationヘッダーのシグニチャ計算

ヘッダーを使用して要求を認証する場合 `Authorization`、StorageGRIDはAWSと次の点で異なります。

- StorageGRIDでは、ヘッダーをに含める `CanonicalHeaders`必要はありません `host`。
- StorageGRIDをに含める `CanonicalHeaders`必要はありません `Content-Type`。
- StorageGRIDでは、ヘッダーをに含める `CanonicalHeaders`必要はありません `x-amz-*`。

> 一般的なベストプラクティスとして、これらのヘッダーは必ずに含めて `CanonicalHeaders`検証してください。ただし、これらのヘッダーを除外しても、StorageGRIDはエラーを返しません。

詳細については、を参照してください "Authorizationヘッダーのシグニチャ計算：単一チャンクでのペイロードの転送（AWS Signature Version 4）"。

関連情報

- "ILM を使用してオブジェクトを管理する"
- "Amazon Simple Storage Service APIリファレンス：PutObject"

S3 RestoreObjectリクエストを使用して**StorageGRID**でオブジェクトを復元する

S3 RestoreObject要求を使用して、クラウドストレージプールに格納されているオブジェクトをリストアできます。

サポートされている要求タイプ

StorageGRIDでは、オブジェクトのリストアでRestoreObject要求のみがサポートされます。リストアのタイプはサポートされません `SELECT`。SELECT要求は戻ります `XNotImplemented`。

バージョン管理

必要に応じて、バージョン管理されたバケット内のオブジェクトの特定のバージョンをリストアするように指定します `versionId`。を指定しない場合、 `versionId`オブジェクトの最新バージョンがリストアされます。

クラウドストレージプールオブジェクトでの**RestoreObject**の動作

オブジェクトがに格納されている場合、"クラウドストレージプール"RestoreObject要求の動作はオブジェクトの状態に基づいて次のようになります。詳細については、を参照してください"ヘッドオブジェクト"。

> オブジェクトがクラウドストレージプールに格納されていて、そのオブジェクトのコピーがグリッドに1つ以上存在する場合は、RestoreObject要求を実行してオブジェクトをリストアする必要はありません。代わりに、GetObject要求を使用してローカルコピーを直接取得できます。

オブジェクトの状態	**RestoreObject**の動作
StorageGRID に取り込まれているがまだ ILM によって評価されていない、またはオブジェクトがクラウドストレージプールにない	`403 Forbidden、 InvalidObjectState`
クラウドストレージプール内にあるが、まだ読み出し不可能な状態に移行していない	`200 OK`変更は行われません。 注：オブジェクトが読み出し不可能な状態に移行されるまでは変更できません。 `expiry-date`

オブジェクトの状態	**RestoreObject**の動作
オブジェクトを読み出し不可能な状態に移行した	`202 Accepted`要求の本文に指定された日数だけ、オブジェクトの読み出し可能なコピーをクラウドストレージプールにリストアします。この期間が終了すると、オブジェクトは読み出し不可能な状態に戻ります。 必要に応じて、request要素を使用し `Tier`てリストアジョブの完了にかかる時間を指定します(`Expedited`、 `Standard`または `Bulk`)指定しない場合は `Tier Standard`、階層が使用されます。 重要：オブジェクトが S3 Glacier Deep Archive に移行されている場合、またはクラウドストレージプールが Azure Blob Storage を使用している場合、 `Expedited`階層を使用してオブジェクトを復元することはできません。以下のエラーが返されます `403 Forbidden`、`InvalidTier`：`Retrieval option is not supported by this storage class`。
読み出し不可能な状態からリストア中である	`409 Conflict`、 `RestoreAlreadyInProgress`
クラウドストレージプールへのリストアが完了している	`200 OK` *注：*オブジェクトが読み出し可能な状態にリストアされている場合は、RestoreObject要求をに新しい値を指定して再発行することで `Days`変更できます `expiry-date`。要求が実行された日時に基づいてリストア日が更新されます。

S3 SelectObjectContentリクエストを使用して**StorageGRID**でオブジェクトデータをフィルタリングする

S3 SelectObjectContent 要求を使用すると、シンプルな SQL ステートメントに基づいて S3 オブジェクトのコンテンツをフィルタリングできます。

詳細については、を参照してください "Amazon Simple Storage Service APIリファレンス：SelectObjectContent"。

開始する前に

- テナントアカウントには S3 Select 権限が割り当てられます。
- 照会するオブジェクトに対する権限が `s3:GetObject`必要です。
- 照会するオブジェクトは、次のいずれかの形式である必要があります。
  - * CSV *。そのまま使用することも、GZIPやbzip2のアーカイブに圧縮して使用することもできます。
  - 寄木細工。寄木細工オブジェクトの追加要件：
    - S3 Selectでは、GZIPまたはSnappyを使用したカラムナ圧縮のみがサポートされます。S3 Selectでは、寄木細工オブジェクトのオブジェクト全体の圧縮はサポートされません。
    - S3 Selectは寄木細工の出力をサポートしていません。出力形式はCSVまたはJSONで指定する必要があります。
    - 圧縮されていない行グループの最大サイズは512MBです。

    - オブジェクトのスキーマで指定されているデータ型を使用する必要があります。
    - interval、json、list、time、またはUUID論理型は使用できません。
- SQL 式の最大長は 256KB です。
- 入力または結果のすべてのレコードの最大長は 1MiB です。

CSV要求の構文例

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns="http://s3.amazonaws.com/doc/2006-03-
01/">
   <Expression>string</Expression>
   <ExpressionType>string</ExpressionType>
   <RequestProgress>
      <Enabled>boolean</Enabled>
   </RequestProgress>
   <InputSerialization>
      <CompressionType>GZIP</CompressionType>
      <CSV>
         <AllowQuotedRecordDelimiter>boolean</AllowQuotedRecordDelimiter>
         <Comments>#</Comments>
         <FieldDelimiter>\t</FieldDelimiter>
         <FileHeaderInfo>USE</FileHeaderInfo>
         <QuoteCharacter>'</QuoteCharacter>
         <QuoteEscapeCharacter>\\</QuoteEscapeCharacter>
         <RecordDelimiter>\n</RecordDelimiter>
      </CSV>
   </InputSerialization>
   <OutputSerialization>
      <CSV>
         <FieldDelimiter>string</FieldDelimiter>
         <QuoteCharacter>string</QuoteCharacter>
         <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
         <QuoteFields>string</QuoteFields>
         <RecordDelimiter>string</RecordDelimiter>
      </CSV>
   </OutputSerialization>
   <ScanRange>
      <End>long</End>
      <Start>long</Start>
   </ScanRange>
</SelectObjectContentRequest>
```

寄木リクエスト構文の例

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns=http://s3.amazonaws.com/doc/2006-03-01/>
   <Expression>string</Expression>
   <ExpressionType>string</ExpressionType>
   <RequestProgress>
      <Enabled>boolean</Enabled>
   </RequestProgress>
   <InputSerialization>
      <CompressionType>GZIP</CompressionType>
      <PARQUET>
      </PARQUET>
   </InputSerialization>
   <OutputSerialization>
      <CSV>
         <FieldDelimiter>string</FieldDelimiter>
         <QuoteCharacter>string</QuoteCharacter>
         <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
         <QuoteFields>string</QuoteFields>
         <RecordDelimiter>string</RecordDelimiter>
      </CSV>
   </OutputSerialization>
   <ScanRange>
      <End>long</End>
      <Start>long</Start>
   </ScanRange>
</SelectObjectContentRequest>
```

SQL クエリの例

このクエリは、州名、 2010 年人口、 2015 年推定人口、米国の人口調査データからの変化率を取得します。状態でないファイル内のレコードは無視されます。

```
SELECT STNAME, CENSUS2010POP, POPESTIMATE2015, CAST((POPESTIMATE2015 -
CENSUS2010POP) AS DECIMAL) / CENSUS2010POP * 100.0 FROM S3Object WHERE
NAME = STNAME
```

照会するファイルの最初の数行は `SUB-EST2020_ALL.csv`次のようになります。

```
SUMLEV,STATE,COUNTY,PLACE,COUSUB,CONCIT,PRIMGEO_FLAG,FUNCSTAT,NAME,STNAME,
CENSUS2010POP,
ESTIMATESBASE2010,POPESTIMATE2010,POPESTIMATE2011,POPESTIMATE2012,POPESTIM
ATE2013,POPESTIMATE2014,
POPESTIMATE2015,POPESTIMATE2016,POPESTIMATE2017,POPESTIMATE2018,POPESTIMAT
E2019,POPESTIMATE042020,
POPESTIMATE2020
040,01,000,00000,00000,00000,0,A,Alabama,Alabama,4779736,4780118,4785514,4
799642,4816632,4831586,
4843737,4854803,4866824,4877989,4891628,4907965,4920706,4921532
162,01,000,00124,00000,00000,0,A,Abbeville
city,Alabama,2688,2705,2699,2694,2645,2629,2610,2602,
2587,2578,2565,2555,2555,2553
162,01,000,00460,00000,00000,0,A,Adamsville
city,Alabama,4522,4487,4481,4474,4453,4430,4399,4371,
4335,4304,4285,4254,4224,4211
162,01,000,00484,00000,00000,0,A,Addison
town,Alabama,758,754,751,750,745,744,742,734,734,728,
725,723,719,717
```

AWS-CLIの使用例（CSV）

```
aws s3api select-object-content --endpoint-url https://10.224.7.44:10443
--no-verify-ssl  --bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.csv --expression-type SQL --input-serialization '{"CSV":
{"FileHeaderInfo": "USE", "Comments": "#", "QuoteEscapeCharacter": "\"",
"RecordDelimiter": "\n", "FieldDelimiter": ",", "QuoteCharacter": "\"",
"AllowQuotedRecordDelimiter": false}, "CompressionType": "NONE"}' --output
-serialization '{"CSV": {"QuoteFields": "ASNEEDED",
"QuoteEscapeCharacter": "#", "RecordDelimiter": "\n", "FieldDelimiter":
",", "QuoteCharacter": "\""}}' --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" changes.csv
```

出力ファイルの最初の数行は `changes.csv`次のようになります。

```
Alabama,4779736,4854803,1.570526070895965802295356898372629785 4
Alaska,710231,738430,3.970398363349389142405780654463125377 5
Arizona,6392017,6832810,6.895992297892824753125656580700583243 1
Arkansas,2915918,2979732,2.188470320495981025529524492801237894 9
California,37253956,38904296,4.429972483996062055798852610444914897 1
Colorado,5029196,5454328,8.453279609703022113276157859029554624 6
```

AWS-CLIの使用例（寄木細工）

```
aws s3api select-object-content  -endpoint-url https://10.224.7.44:10443
--bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.parquet --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" --expression-type
'SQL' --input-serialization '{"Parquet":{}}'  --output-serialization
'{"CSV": {}}' changes.csv
```

出力ファイルの最初のいくつかの行は、.csvを変更します。次のようになります。

```
Alabama,4779736,4854803,1.5705260708959658022953568983726297854
Alaska,710231,738430,3.9703983633493891424057806544631253775
Arizona,6392017,6832810,6.8959922978928247531256565807005832431
Arkansas,2915918,2979732,2.1884703204959810255295244928012378949
California,37253956,38904296,4.4299724839960620557988526104449148971
Colorado,5029196,5454328,8.4532796097030221132761578590295546246
```

マルチパートアップロードの処理

StorageGRIDでサポートされているマルチパートアップロード操作

このセクションでは、 StorageGRID でのマルチパートアップロードの処理のサポートについて説明します。

マルチパートアップロードのすべての処理に、次の条件と注意事項が適用されます。

- 1つのバケットに対して同時に実行するマルチパートアップロードの数が1、000を超えないようにしてください。そのバケットに対するListMultipartUploadsのクエリで不完全な結果が返されることがあります。
- StorageGRID は、マルチパートに AWS のサイズ制限を適用します。S3 クライアントは次のガイドラインに従う必要があります。
  - マルチパートアップロードの各パートのサイズは 5MiB （ 5 、 242 、 880 バイト）と 5GiB （ 5 、 368 、 709 、 120 バイト）の間にする必要があります。
  - 最後の部分は 5MiB （ 5,242,880 バイト）より小さくできます。
  - 一般に、パーツサイズはできるだけ大きくする必要があります。たとえば、 100GiB オブジェクトの場合、 5GB のパートサイズを使用します。各パートは固有のオブジェクトとみなされるため、大きなパートサイズを使用するとStorageGRID メタデータのオーバーヘッドが削減されます。
  - 5GB 未満のオブジェクトでは、マルチパートではないアップロードの使用を検討してください。
- ILMルールでBalancedまたはStrictが使用されている場合は、マルチパートオブジェクトの各パートの取り込み時にILMが評価され、マルチパートアップロードの完了時にオブジェクト全体に対してILMが評価され"取り込みオプション"ます。これがオブジェクトとパートの配置にどのように影響するかに注意する必要があります。
  - S3マルチパートアップロードの実行中にILMが変更されると、マルチパートアップロードの完了時に

オブジェクトの一部の部分が現在のILM要件を満たしていない可能性があります。正しく配置されていないパートはILMルールによる再評価の対象としてキューに登録され、あとで正しい場所に移動されます。

- パートに対して ILM を評価する際、 StorageGRID はオブジェクトのサイズではなくパートのサイズでフィルタリングします。つまり、オブジェクト全体のILM要件を満たしていない場所にオブジェクトの一部を格納できます。たとえば、10GB以上のオブジェクトをすべてDC1に格納し、それより小さいオブジェクトをすべてDC2に格納するルールの場合、10パートのマルチパートアップロードの1GBの各パートは取り込み時にDC2に格納されます。ただし、オブジェクト全体に対してILMが評価されると、オブジェクトのすべての部分がDC1に移動されます。

- すべてのマルチパートアップロード操作はStorageGRIDをサポートしています"整合性の値"。
- マルチパートアップロードを使用してオブジェクトを取り込んだ場合、は"オブジェクトのセグメント化しきい値（1GiB）"適用されません。
- 必要に応じて、マルチパートアップロードでを使用できます"サーバ側の暗号化"。SSE（StorageGRIDで管理されるキーによるサーバ側の暗号化）を使用するには、CreateMultipartUpload要求にのみ要求ヘッダーを含め `x-amz-server-side-encryption`ます。SSE-C（ユーザ指定のキーによるサーバ側の暗号化）を使用するには、CreateMultipartUpload要求と後続の各UploadPart要求に同じ3つの暗号化キー要求ヘッダーを指定します。
- マルチパートアップロードされたオブジェクトが"ブランチバケット"に含まれるかどうかは、取り込みが開始された時刻と、ブランチバケットのタイムフィルターによって異なります。
  - 前に。インジェストがブランチバケットの_Before_タイムスタンプより前に開始された場合、アップロードが完了した時期に関係なく、マルチパートアップロードオブジェクトが含まれます。
  - 後。ブランチバケットの_After_タイムスタンプ以降に取り込みが開始された場合、マルチパートアップロードされたオブジェクトが含まれます。
  - 間。ブランチバケットの_From_タイムスタンプと_To_タイムスタンプの間に取り込みが開始された場合、アップロードが完了したタイミングに関係なく、マルチパートアップロードオブジェクトが含まれます。
  - 除外する。取り込みがブランチバケットの「除外開始」時刻より前、または「除外終了」時刻より後に開始された場合、マルチパートアップロードオブジェクトが含まれます。

操作	インプリメンテーション
AbortMultipartUpload	Amazon S3 REST API のすべての動作が実装されています。予告なく変更される場合があります。
CompleteMultipartUpload	を参照し "CompleteMultipartUpload"
CreateMultipartUpload （以前の名前はInitiate Multipart Upload）	を参照し "CreateMultipartUpload"
ListMultipartUploads	を参照し "ListMultipartUploads"
ListParts	Amazon S3 REST API のすべての動作が実装されています。予告なく変更される場合があります。
パーツのアップロード	を参照し "パーツのアップロード"

操作	インプリメンテーション
パーツコピーをアップロード	を参照し "パーツコピーをアップロード"

StorageGRID S3 REST APIによるマルチパートアップロードの完了方法

CompleteMultipartUpload処理は、以前にアップロードされたパートをアセンブルして、オブジェクトのマルチパートアップロードを完了します。

StorageGRIDでは、CompleteMultipartUploadで要求パラメータの連続しない値が昇順でサポートされます `partNumber`。パラメータは任意の値から開始できます。

競合を解決します

同じキーに書き込む 2 つのクライアントなど、競合するクライアント要求は、「 latest-wins 」ベースで解決されます。「 latest-wins 」評価は、 S3 クライアントが処理を開始するタイミングではなく、 StorageGRID システムが特定の要求を完了したタイミングで行われます。

サポートされる要求ヘッダー

次の要求ヘッダーがサポートされています。

- チェックサム要求ヘッダー：
  - `x-amz-checksum-crc32`
  - `x-amz-checksum-crc32c`
  - `x-amz-checksum-crc64nvme`
  - `x-amz-checksum-sha256`
  - `x-amz-checksum-type`

  CreateMultipartUpload リクエストでチェックサムが指定されていない場合、StorageGRID はオブジェクトのデフォルトの CRC-64/NVME チェックサムを計算しません。

- `x-amz-storage-class`

  ヘッダーは `x-amz-storage-class`、一致するILMルールでが指定されている場合にStorageGRIDで作成されるオブジェクトコピーの数に影響します"デュアルコミットまたはBalanced取り込みオプション"。

- `STANDARD`

  （デフォルト） ILM ルールで Dual commit オプションが使用されている場合、または Balanced オプションによって中間コピーが作成される場合に、デュアルコミットの取り込み処理を指定します。

- `REDUCED_REDUNDANCY`

  ILM ルールで Dual commit オプションが使用されている場合、または Balanced オプションによって中間コピーが作成される場合に、シングルコミットの取り込み処理を指定します。

S3 Object Lockが有効なバケットにオブジェクトを取り込む場合、この `REDUCED_REDUNDANCY`オプションは無視されます。従来の準拠バケットにオブジェクトを取り込む場合、オプションを指定すると `REDUCED_REDUNDANCY`エラーが返されます。StorageGRID では、常にデュアルコミットの取り込みが実行され、コンプライアンス要件が満たされます。

マルチパートアップロードが 15 日以内に完了しないと、非アクティブな処理としてマークされ、関連するすべてのデータがシステムから削除されます。

`ETag`返される値はデータのMD5合計ではなく、Amazon S3 APIによるマルチパートオブジェクトの値の実装に従います `ETag。

サポートされない要求ヘッダーです

次の要求ヘッダーはサポートされていません。

- If-Match

  `If-Match`ヘッダーの動作は、StorageGRIDの構成によって異なります。このヘッダーを指定すると、エラーメッセージ（501 Not Implemented）が返される可能性があります。 `If-Match`ヘッダーが受け入れられたものの機能しない場合、より厳格な501 Not Implementedエラー動作を有効にするための手順を示すアラートが表示される可能性があります。

- If-None-Match

  `If-None-Match`ヘッダーの動作は、StorageGRIDの構成によって異なります。このヘッダーを指定すると、エラーメッセージ（501 Not Implemented）が返される可能性があります。 `If-None-Match`ヘッダーが受け入れられたものの機能しない場合、より厳格な501 Not Implementedエラー動作を有効にするための手順を示すアラートが表示される可能性があります。

- x-amz-checksum-md5
- x-amz-checksum-sha1
- x-amz-checksum-sha512
- x-amz-checksum-xxhash3
- x-amz-checksum-xxhash64
- x-amz-checksum-xxhash128

バージョン管理

マルチパートアップロードは、この処理で完了します。バケットでバージョン管理が有効になっている場合は、マルチパートアップロードの完了後にオブジェクトのバージョンが作成されます。

バケットでバージョン管理が有効になっている場合は、格納されているオブジェクトのバージョンに対して一意のが `versionId`自動的に生成されます。これは `versionId`、応答ヘッダーを使用した応答でも返され `x-amz-version-id`ます。

バージョン管理が一時停止されている場合、オブジェクトのバージョンはnullで格納され `versionId`、nullのバージョンがすでに存在する場合は上書きされます。

> バケットでバージョン管理が有効になっているときは、同じオブジェクトキーで同時に複数のマルチパートアップロードが実行されている場合でも、マルチパートアップロードが完了するたびに常に新しいバージョンが作成されます。バケットでバージョン管理が有効になっていないときは、マルチパートアップロードの開始後に、同じオブジェクトキーで別のマルチパートアップロードが開始されて先に完了することがあります。バージョン管理が有効になっていないバケットでは、最後に完了したマルチパートアップロードが優先されます。

レプリケーション、通知、またはメタデータ通知に失敗しました

マルチパートアップロードが行われるバケットでプラットフォームサービスが設定されている場合、関連するレプリケーション操作や通知操作が失敗してもマルチパートアップロードは正常に実行されます。

テナントでは、オブジェクトのメタデータまたはタグを更新することで、失敗したレプリケーションまたは通知をトリガーできます。テナントでは、既存の値を再送信し、不要な変更を回避できます。

を参照してください "プラットフォームサービスのトラブルシューティングを行う"。

StorageGRID での S3 CreateMultipartUpload リクエストヘッダーとオプション

CreateMultipartUpload（以前のInitiate Multipart Upload）処理は、オブジェクトのマルチパートアップロードを開始し、アップロードIDを返します。

`x-amz-storage-class`要求ヘッダーがサポートされます。で送信される値 `x-amz-storage-class`は、
StorageGRIDによる取り込み時のオブジェクトデータの保護方法に影響し、StorageGRIDシステムに格納されるオブジェクトの永続的コピーの数（ILMで決定）には影響しません。

取り込まれたオブジェクトに一致するILMルールでStrictが使用されている場合、"取り込みオプション" `x-amz-storage-class`ヘッダーは無効です。

には次の値を使用でき `x-amz-storage-class`ます。

- STANDARD（デフォルト）
  - * Dual commit *：ILMルールでDual commit取り込みオプションが指定されている場合は、オブジェクトが取り込まれるとすぐにそのオブジェクトの2つ目のコピーが作成されて別のストレージノードに分散されます（デュアルコミット）。ILMが評価されると、StorageGRID はこれらの初期中間コピーがルールの配置手順を満たしているかどうかを判断します。作成されていない場合は、新しいオブジェ

クトコピーを別の場所に作成し、最初の中間コピーを削除しなければならないことがあります。

- * Balanced *：ILMルールでBalancedオプションが指定されていて、ルールで指定されたすべてのコピーをStorageGRID がすぐに作成できない場合、StorageGRID は2つの中間コピーを別 々 のストレージノードに作成します。

  ILMルールで指定されたすべてのオブジェクトコピーをStorageGRIDでただちに作成できる場合（同期配置）、 `x-amz-storage-class`ヘッダーは効果がありません。

- `REDUCED_REDUNDANCY`

  - * Dual commit *：ILMルールでDual commitオプションが指定されている場合、StorageGRIDはオブジェクトの取り込み時に中間コピーを1つ作成します（シングルコミット）。
  - * Balanced *：ILMルールでBalancedオプションが指定されている場合、StorageGRID は、ルールで指定されたすべてのコピーをただちに作成できない場合にのみ中間コピーを1つ作成します。StorageGRID で同期配置を実行できる場合、このヘッダーは効果がありません。 `REDUCED_REDUNDANCY`オブジェクトに一致するILMルールで単一のレプリケートコピーが作成される場合は、オプションの使用を推奨します。この場合、を使用する `REDUCED_REDUNDANCY`と、取り込み処理のたびに余分なオブジェクトコピーを不要に作成および削除する必要がなくなります。

  それ以外の状況では、オプションの使用 `REDUCED_REDUNDANCY`は推奨されません。 `REDUCED_REDUNDANCY`取り込み中にオブジェクトデータが失われるリスクが高まります。たとえば、 ILM 評価の前にコピーが 1 つだけ格納されていたストレージノードに障害が発生すると、データが失われる可能性があります。

> レプリケートコピーを一定期間に 1 つだけ作成すると、データが永続的に失われるリスクがあります。オブジェクトのレプリケートコピーが 1 つしかない場合、ストレージノードに障害が発生したり、重大なエラーが発生すると、そのオブジェクトは失われます。また、アップグレードなどのメンテナンス作業中は、オブジェクトへのアクセスが一時的に失われます。

を指定する `REDUCED_REDUNDANCY`と、オブジェクトを最初に取り込んだときに作成されるコピー数にのみ影響します。オブジェクトがアクティブなILMポリシーで評価される際に作成されるオブジェクトのコピー数には影響せず、StorageGRIDシステムでデータが格納される際の冗長性レベルが低下することもありません。

> S3 Object Lockが有効なバケットにオブジェクトを取り込む場合、この `REDUCED_REDUNDANCY`オプションは無視されます。従来の準拠バケットにオブジェクトを取り込む場合、オプションを指定すると `REDUCED_REDUNDANCY`エラーが返されます。StorageGRID では、常にデュアルコミットの取り込みが実行され、コンプライアンス要件が満たされます。

サポートされる要求ヘッダー

次の要求ヘッダーがサポートされています。

- `Content-Type`
- `x-amz-checksum-algorithm`： `CRC32`、 `CRC32C`、 `CRC64NVME`、または `SHA256`を指定します

CreateMultipartUpload リクエストでチェックサムが指定されていない場合、StorageGRID はオブジェクトのデフォルトの CRC-64/NVME チェックサムを計算しません。StorageGRID は無効またはサポートされていない `x-amz-checksum-algorithm`値を無視します。

- `x-amz-checksum-type`
- `x-amz-meta-`に続けて、ユーザ定義のメタデータを含む名前と値のペアを指定します。

  ユーザ定義メタデータの名前と値のペアを指定する場合、一般的な形式は次のとおりです。

```
x-amz-meta-_name_: `value`
```

  ILMルールの参照時間に*[ユーザ定義の作成時間]*オプションを使用する場合は、オブジェクトの作成日時を記録するメタデータの名前にを使用する必要があります `creation-time`。例：

```
x-amz-meta-creation-time: 1443399726
```

  の値 `creation-time`は、1970年1月1日からの秒数として評価されます。

  従来の準拠が有効になっているバケットにオブジェクトを追加する場合、ユーザ定義のメタデータとして追加すること `creation-time`はできません。エラーが返されます。

- S3 オブジェクトロック要求のヘッダー：
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

    これらのヘッダーがない状態で要求を送信した場合、バケットのデフォルトの保持設定を使用して、オブジェクトバージョンの retain-date が計算されます。

  "S3 REST APIを使用してS3オブジェクトロックを設定します"

- SSE 要求ヘッダー：
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    [サーバ側の暗号化を行うための要求ヘッダー]

    StorageGRIDでのUTF-8文字の処理方法については、を参照してください"PutObject"。

サーバ側の暗号化を行うための要求ヘッダー

マルチパートオブジェクトをサーバ側の暗号化で暗号化するには、次の要求ヘッダーを使用します。SSE オプションと SSE-C オプションを同時に指定することはできません。

- **SSE**: StorageGRIDによって管理される一意のキーでオブジェクトを暗号化する場合は、CreateMultipartUpload要求で次のヘッダーを使用します。UploadPart要求でこのヘッダーを指定しないでください。
  - `x-amz-server-side-encryption`
- * SSE-C *：指定および管理する一意のキーでオブジェクトを暗号化する場合は、CreateMultipartUpload要求（および後続の各UploadPart要求）でこれら3つのヘッダーをすべて使用します。
  - `x-amz-server-side-encryption-customer-algorithm`:指定します `AES256`。
  - `x-amz-server-side-encryption-customer-key`：新しいオブジェクトの暗号化キーを指定します。
  - `x-amz-server-side-encryption-customer-key-MD5`：新しいオブジェクトの暗号化キーのMD5ダイジェストを指定します。

> 指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。ユーザ指定のキーを使用してオブジェクトデータを保護する前に、の考慮事項を確認してください"サーバ側の暗号化を使用する"。

サポートされない要求ヘッダーです

次の要求ヘッダーはサポートされていません。

- `x-amz-website-redirect-location`

> `x-amz-website-redirect-location`ヘッダーが返され `XNotImplemented`ます。

バージョン管理

マルチパートアップロードは、アップロードの開始、アップロードのリストの表示、パートのアップロード、アップロードしたパートのアセンブル、およびアップロードの完了の個別の処理に分けられます。CompleteMultipartUpload処理が実行されると、オブジェクトが作成されます（該当する場合はバージョン管理されます）。

S3 ListMultipartUploads 操作と StorageGRID でサポートされているパラメータ

ListMultipartUploads処理を実行すると、バケットで実行中のマルチパートアップロードがリストされます。

次の要求パラメータがサポートされています。

- `encoding-type`
- `key-marker`
- `max-uploads`

- `prefix`
- `upload-id-marker`
- `Host`
- `Date`
- `Authorization`

バージョン管理

マルチパートアップロードは、アップロードの開始、アップロードのリストの表示、パートのアップロード、アップロードしたパートのアセンブル、およびアップロードの完了の個別の処理に分けられます。CompleteMultipartUpload処理が実行されると、オブジェクトが作成されます（該当する場合はバージョン管理されます）。

StorageGRID の **S3 UploadPart** 処理でサポートされているリクエストヘッダーとサポートされていないリクエストヘッダー

UploadPart処理は、オブジェクトのマルチパートアップロード内のパートをアップロードします。

サポートされる要求ヘッダー

次の要求ヘッダーがサポートされています。

- チェックサム要求ヘッダー：
  - `x-amz-checksum-crc32`
  - `x-amz-checksum-crc32c`
  - `x-amz-checksum-crc64nvme`
  - `x-amz-checksum-sha256`

  CreateMultipartUploadリクエスト時にCRC-32、CRC-32C、CRC-64/NVME、またはSHA-256チェックサムを指定した場合は、各UploadPartリクエストにもチェックサムリクエストヘッダーを含める必要があります。

  > CreateMultipartUpload リクエストでチェックサムが指定されていない場合、StorageGRID はオブジェクトのデフォルトの CRC-64/NVME チェックサムを計算しません。

- `Content-Length`
- `Content-MD5`

サーバ側の暗号化を行うための要求ヘッダー

CreateMultipartUpload要求にSSE-C暗号化を指定した場合は、各UploadPart要求に次の要求ヘッダーも含める必要があります。

- `x-amz-server-side-encryption-customer-algorithm`:指定します `AES256`。
- `x-amz-server-side-encryption-customer-key`：CreateMultipartUpload要求で指定したものと同

じ暗号化キーを指定します。

- `x-amz-server-side-encryption-customer-key-MD5`：CreateMultipartUpload要求で指定したMD5ダイジェストと同じMD5ダイジェストを指定します。

> 指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。ユーザ指定のキーを使用してオブジェクトデータを保護する前に、の考慮事項を確認してください"サーバ側の暗号化を使用します"。

サポートされない要求ヘッダーです

次の要求ヘッダーはサポートされていません。

- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`
- `x-amz-checksum-md5`
- `x-amz-checksum-sha1`
- `x-amz-checksum-sha512`
- `x-amz-checksum-xxhash3`
- `x-amz-checksum-xxhash64`
- `x-amz-checksum-xxhash128`

バージョン管理

マルチパートアップロードは、アップロードの開始、アップロードのリストの表示、パートのアップロード、アップロードしたパートのアセンブル、およびアップロードの完了の個別の処理に分けられます。CompleteMultipartUpload処理が実行されると、オブジェクトが作成されます（該当する場合はバージョン管理されます）。

S3 UploadPartCopy 操作を使用して StorageGRID にオブジェクトの一部をアップロードする

UploadPartCopy操作は、データソースとして既存のオブジェクトからデータをコピーすることによって、オブジェクトの一部をアップロードします。

UploadPartCopy処理は、Amazon S3 REST APIのすべての動作で実装されます。予告なく変更される場合があります。

この要求は、StorageGRIDシステム内でで指定されたオブジェクトデータの読み取りと書き込みを行い `x-amz-copy-source-range`ます。

サポートされる要求ヘッダー

次の要求ヘッダーがサポートされています。

- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`

- `x-amz-copy-source-if-modified-since`

サーバ側の暗号化を行うための要求ヘッダー

CreateMultipartUpload要求にSSE-C暗号化を指定した場合は、各UploadPartCopy要求に次の要求ヘッダーも含める必要があります。

- `x-amz-server-side-encryption-customer-algorithm`:指定します `AES256`。
- `x-amz-server-side-encryption-customer-key`：CreateMultipartUpload要求で指定したものと同じ暗号化キーを指定します。
- `x-amz-server-side-encryption-customer-key-MD5`：CreateMultipartUpload要求で指定したMD5ダイジェストと同じMD5ダイジェストを指定します。

ソースオブジェクトがユーザ指定のキー（SSE-C）を使用して暗号化されている場合は、オブジェクトを復号化してコピーできるように、UploadPartCopy要求に次の3つのヘッダーを含める必要があります。

- `x-amz-copy-source-server-side-encryption-customer-algorithm`:指定します `AES256`。
- `x-amz-copy-source-server-side-encryption-customer-key`：ソースオブジェクトの作成時に指定した暗号化キーを指定します。
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`:ソースオブジェクトの作成時に指定したMD5ダイジェストを指定します。

> 指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。ユーザ指定のキーを使用してオブジェクトデータを保護する前に、の考慮事項を確認してください"サーバ側の暗号化を使用します"。

バージョン管理

マルチパートアップロードは、アップロードの開始、アップロードのリストの表示、パートのアップロード、アップロードしたパートのアセンブル、およびアップロードの完了の個別の処理に分けられます。CompleteMultipartUpload処理が実行されると、オブジェクトが作成されます（該当する場合はバージョン管理されます）。

S3チェックサムサポート

StorageGRID は、CreateMultipartUpload リクエスト時にチェックサムが指定されていたかどうかを自動的に検出し、UploadPartCopy 操作でそのチェックサムを使用します。UploadPartCopy リクエストでチェックサムを指定する必要はありません。CreateMultipartUpload リクエストでチェックサムが指定されていない場合、StorageGRID はオブジェクトのデフォルトの CRC-64/NVME チェックサムを計算しません。CreateMultipartUpload でチェックサムが指定されていない場合、StorageGRID はコピーされたパートにチェックサムを含めません。

StorageGRID S3 REST API エラー応答

StorageGRID システムでは、該当する S3 REST API の標準のエラー応答をすべてサポートしています。また、 StorageGRID の実装では、カスタム応答もいくつか追加されています。

サポートされている **S3 API** のエラーコード

名前	**HTTP**ステータス
アクセスが拒否されました	403禁止
BadDigest の略	400不正な要求
BucketAlreadyExists のようになりました	409 競合
BucketNotEmpty のように入力します	409 競合
IncompleteBody	400不正な要求
内部エラー	500 Internal Server Error （内部サーバエラー）
InvalidAccessKeyId	403禁止
アンヴァリッドドキュメント	400不正な要求
InvalidBucketName の略	400不正な要求
InvalidBucketState の場合	409 競合
InvalidDigest の略	400不正な要求
InvalidEncryptionAlgorithmError	400不正な要求
InvalidPart	400不正な要求
InvalidPartOrder	400不正な要求
InvalidRange ：無効な範囲	416 リクエストされた範囲が適合しません
InvalidRequest	400不正な要求
InvalidStorageClass	400不正な要求
InvalidTag	400不正な要求
InvalidURI	400不正な要求
KeyTooLong の 2 つのグループがあります	400不正な要求

名前	**HTTP**ステータス
MalformedXML の場合	400不正な要求
MetadataTooLarge	400不正な要求
MethodNotAllowed のように入力します	405 メソッドは許可されていません
MissingContentLength （ MissingContentLength ）	411 長さが必要です
MissingRequestBodyError	400不正な要求
MissingSecurityHeader	400不正な要求
NoSuchBucket	404が見つかりません
NoSuchKey	404が見つかりません
NoSuchUpload	404が見つかりません
実装なし	501 は実装されていません
NoSuchBucketPolicy のようになります	404が見つかりません
ObjectLockConfigurationNotFoundError	404が見つかりません
PreconditionalFailed	412 事前条件が失敗しました
RequestTimeTooSkewed	403禁止
サービスを利用できません	503 Service Unavailable （ 503 サービスが利用でき
SignatureDoesNotMatch のように指定します	403禁止
TooManyBuckets	400不正な要求
UserKeyMustBeSpecified	400不正な要求

StorageGRID カスタムのエラーコード

名前	製品説明	HTTPステータス
XBucketLifecycleNotAllowed のようになりました	バケットライフサイクル設定は従来の準拠バケットには適用されません	400不正な要求
XBucketPolicyParseException	受信したバケットポリシー JSON を解析できませんでした。	400不正な要求
XCompliConflict	準拠設定が古いため、処理が拒否されました。	403禁止
XCompliReducedRedundancyForbidden	レガシー準拠バケットでは冗長性の低下は許可されません	400不正な要求
XMaxBucketPolicyLengthExceeded （ XMaxBucketLengthExceeded ）	ポリシーが許容される最大バケットポリシー長を超えています。	400不正な要求
XMissingInternalRequestHeader	内部要求のヘッダーがありません。	400不正な要求
XNoSuchBucketCompliance です	指定したバケットで従来の準拠が有効になっていません。	404が見つかりません
XNotAcceptable	要求に含まれている Accept ヘッダーの 1 つ以上を満たすことができませんでした。	406 は許容されません
XNotImplemented	指定した要求の処理には、実装されていない機能が含まれます。	501 は実装されていません

StorageGRIDのカスタム処理

StorageGRID でサポートされているカスタムバケット操作

StorageGRIDシステムでは、S3 REST APIに追加されるカスタム処理をサポートしています。

次の表に、StorageGRIDでサポートされるカスタム処理を示します。

操作	製品説明
"GET Bucket consistency"	特定のバケットに適用されている整合性を返します。
"PUT Bucket consistency"	特定のバケットに適用する整合性を設定します。
"GET Bucket last access time のように指定します"	特定のバケットで最終アクセス時間の更新が有効になっているか無効になっているかを返します。

操作	製品説明
"PUT Bucket last access time のように指定します"	特定のバケットの最終アクセス時間の更新を有効または無効にできます。
"バケットのメタデータ通知設定を削除します"	特定のバケットに関連付けられているメタデータ通知設定 XML を削除します。
"GET Bucket metadata notification configuration のコマンドです"	特定のバケットに関連付けられているメタデータ通知設定 XML を返します。
"PUT Bucket metadata notification configuration のコマンドです"	バケットのメタデータ通知サービスを設定します。
"GET Storage Usage の略"	アカウントおよびアカウントに関連付けられている各バケットで使用されているストレージの総容量が表示されます。
"廃止予定：準拠設定を使用してCreateBucket"	廃止およびサポート終了：準拠を有効にした新しいバケットを作成できなくなりました。
"廃止予定：バケット準拠を取得します"	廃止されましたがサポートされています：既存の古い準拠バケットに対して現在有効な準拠設定を返します。
"廃止予定：PUT Bucket compliance"	廃止されましたがサポートされています：既存の古い準拠バケットの準拠設定を変更できます。

StorageGRIDで**GET Bucket**整合性リクエストを使用してバケットの整合性レベルを取得する

GET Bucket consistency要求を使用すると、特定のバケットに適用されている整合性を確認できます。

デフォルトの整合性は、新規作成されたオブジェクトのリードアフターライトを保証するように設定されます。

この処理を完了するには、s3：GetBucketConsistency権限またはrootアカウントが必要です。

要求例

```
GET /bucket?x-ntap-sg-consistency HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

応答

応答XMLでは、 `<Consistency>`次のいずれかの値が返されます。

整合性	製品説明
すべて	すべてのノードが即座にデータを受け取り、受け取れない場合は要求が失敗します。
strong-global	すべてのサイトのすべてのクライアント要求について、リードアフターライト整合性が保証されます。
strong-site	1 つのサイト内のすべてのクライアント要求について、リードアフターライト整合性が保証されます。
read-after-new-write の場合	（デフォルト）新規オブジェクトにはリードアフターライト整合性を、オブジェクトの更新には結果整合性を提供します。高可用性が確保され、データ保護が保証されます。ほとんどの場合に推奨されます。
利用可能	新規オブジェクトとオブジェクトの更新の両方について結果整合性を提供します。S3バケットの場合は、必要な場合にのみ使用します（読み取り頻度の低いログ値を含むバケットや、存在しないキーに対するHEAD処理やGET処理など）。S3 FabricPool バケットではサポートされません。

応答例

```
HTTP/1.1 200 OK
Date: Fri, 18 Sep 2020 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/11.5.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<Consistency xmlns="http://s3.storagegrid.com/doc/2015-02-01/">read-after-
new-write</Consistency>
```

関連情報

"整合性"

PUT Bucket整合性リクエストを使用して**StorageGRID**で整合性レベルを指定する

PUT Bucket consistency要求では、バケットで実行される処理に適用する整合性を指定できます。

デフォルトの整合性は、新規作成されたオブジェクトのリードアフターライトを保証するように設定されます。

開始する前に

この処理を完了するには、s3：PutBucketConsistency権限またはrootアカウントが必要です。

リクエスト

`x-ntap-sg-consistency`パラメータには、次のいずれかの値を指定する必要があります。

整合性	製品説明
すべて	すべてのノードが即座にデータを受け取り、受け取れない場合は要求が失敗します。
strong-global	すべてのサイトのすべてのクライアント要求について、リードアフターライト整合性が保証されます。
strong-site	1 つのサイト内のすべてのクライアント要求について、リードアフターライト整合性が保証されます。
read-after-new-write の場合	（デフォルト）新規オブジェクトにはリードアフターライト整合性を、オブジェクトの更新には結果整合性を提供します。高可用性が確保され、データ保護が保証されます。ほとんどの場合に推奨されます。
利用可能	新規オブジェクトとオブジェクトの更新の両方について結果整合性を提供します。S3バケットの場合は、必要な場合にのみ使用します（読み取り頻度の低いログ値を含むバケットや、存在しないキーに対するHEAD処理やGET処理など）。S3 FabricPool バケットではサポートされません。

*注：*一般に、「Read-after-new-write」整合性を使用する必要があります。要求が正しく動作しない場合は、可能であればアプリケーションクライアントの動作を変更します。または、API要求ごとに整合性を指定するようにクライアントを設定します。バケットレベルの整合性は最後の手段として設定してください。

要求例

```
PUT /bucket?x-ntap-sg-consistency=strong-global HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

関連情報

"整合性"

GET Bucket last access timeリクエストを使用して**StorageGRID**でバケットの最終アクセス時間ステータスを取得する

GET Bucket last access time 要求を使用すると、最終アクセス時間の更新が個々のバケットで有効になっているか無効になっているかを確認できます。

この処理を完了するには、s3：GetBucketLastAccessTime権限またはrootアカウントが必要です。

要求例

```
GET /bucket?x-ntap-sg-lastaccesstime HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

応答例

次の例では、バケットの最終アクセス時間の更新が有効になっています。

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/10.3.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<LastAccessTime xmlns="http://s3.storagegrid.com/doc/2015-02-01/">enabled
</LastAccessTime>
```

StorageGRID で **PUT Bucket** 最終アクセス時刻リクエストを使用して最終アクセス時刻の更新を有効または無効にする

PUT Bucket last access time 要求を使用すると、最終アクセス時間の更新を個々のバケットで有効または無効にできます。最終アクセス時間の更新を無効にするとパフォーマンスが向上します。バージョン 10.3.0 以降で作成されたバケットに対しては、いずれもデフォルトで無効になります。

この処理を完了するには、バケットのs3：PutBucketLastAccessTime権限またはrootアカウントが必要です。

> StorageGRID バージョン 10.3 以降では、すべての新規バケットで最終アクセス時間の更新がデフォルトで無効になります。以前のバージョンの StorageGRID で作成されたバケットにこの新たなデフォルトの動作を適用する場合は、対象となるバケットごとに最終アクセス時間の更新を無効にする必要があります。最終アクセス時間の更新を有効または無効にするには、PUT Bucket last access time要求を使用するか、Tenant Managerのバケットの詳細ページを使用します。を参照して "最終アクセス日時の更新を有効または無効にします"

バケットで最終アクセス時間の更新が無効になっている場合、バケットの処理の動作は次のようになります。

- GetObject、GetObjectAcl、GetObjectTagging、HeadObjectの各要求では、最終アクセス時間は更新されません。オブジェクトは、情報ライフサイクル管理（ ILM ）評価のキューに追加されません。

- メタデータのみを更新するCopyObject要求とPutObjectTagging要求では、最終アクセス時間も更新されます。オブジェクトは ILM 評価のキューに追加されます。
- ソースバケットで最終アクセス時間の更新が無効になっている場合、CopyObject要求でソースバケットの最終アクセス時間が更新されません。コピーされたオブジェクトは、ソースバケットの ILM 評価のキューに追加されません。ただし、デスティネーションについては、CopyObject要求で常に最終アクセス時間が更新されます。オブジェクトのコピーは、 ILM 評価のキューに追加されます。
- CompleteMultipartUpload要求で最終アクセス時間が更新されます。完了したオブジェクトは、 ILM 評価のキューに追加されます。

例をリクエストする

この例では、バケットの最終アクセス時間を有効にしています。

```
PUT /bucket?x-ntap-sg-lastaccesstime=enabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

この例では、バケットの最終アクセス時間を無効にしています。

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

StorageGRIDのDELETE Bucket**メタデータ通知設定リクエストで検索統合サービスを無効にします**

DELETE Bucket metadata notification configuration 要求では、設定 XML を削除することで、個々のバケットで検索統合サービスを無効化できます。

この処理を完了するには、バケットのs3：DeleteBucketMetadataNotification権限またはrootアカウントが必要です。

要求例

次の例は、バケットの検索統合サービスを無効にする方法を示しています。

```
DELETE /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

GET Bucketメタデータ通知設定リクエストを使用して**StorageGRID**で検索統合を設定する

GET Bucket metadata notification configuration 要求では、個々のバケットで検索統合を設定するために使用する設定 XML を読み出すことができます。

この処理を完了するには、s3：GetBucketMetadataNotification権限またはrootアカウントが必要です。

要求例

この要求は、というバケットのメタデータ通知設定を読み出します `bucket`。

```
GET /bucket?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

応答

応答の本文には、バケットのメタデータ通知設定が含まれます。メタデータ通知設定では、バケットでの検索統合の設定を確認できます。つまり、どのオブジェクトにインデックスが付けられ、そのオブジェクトメタデータがどのエンドポイントに送信されるかを確認できます。

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:_region:account-
ID_:domain/_mydomain/myindex/mytype_</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

各メタデータ通知設定には、 1 つ以上のルールが含まれています。各ルールは、環境 がオブジェクトを指定し、 StorageGRID がオブジェクトメタデータを送信するデスティネーションを指定します。デスティネーションは、 StorageGRID エンドポイントの URN を使用して指定する必要があります。

名前	製品説明	必須
MetadataNotificationConfiguration のページです	メタデータ通知でオブジェクトとデスティネーションの指定に使用されるルール用のコンテナタグ。 1 つ以上の Rule 要素を含みます。	はい
ルール	指定したインデックスにメタデータを追加する必要があるオブジェクトを特定するルール用のコンテナタグ。 プレフィックスが重複しているルールは拒否されます。 MetadataNotificationConfiguration 要素に含まれています。	はい
ID	ルールの一意の識別子。 Rule 要素に含まれています。	いいえ
ステータス	Status には「 Enabled 」または「 Disabled 」を指定できます。無効になっているルールについては操作が実行されません。 Rule 要素に含まれています。	はい
プレフィックス	プレフィックスと一致するオブジェクトにルールが適用され、そのメタデータが指定したデスティネーションに送信されます。 すべてのオブジェクトを照合するには、空のプレフィックスを指定します。 Rule 要素に含まれています。	はい
デスティネーション	ルールのデスティネーションのコンテナタグ。 Rule 要素に含まれています。	はい

名前	製品説明	必須
URN	オブジェクトメタデータが送信されるデスティネーションの URN 。次のプロパティを持つ StorageGRID エンドポイントの URN を指定する必要があります。 • `es`3番目の要素である必要があります。 • URNは、メタデータが格納されるインデックスとタイプ（の形式）で終わる必要があります `domain-name/myindex/mytype`。 エンドポイントは、 Tenant Manager またはテナント管理 API を使用して設定します。形式は次のとおりです。 • `arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` エンドポイントは設定 XML を送信する前に設定する必要があります。そうしないと、 404 エラーで設定が失敗します。 Urn は Destination 要素に含まれています。	はい

応答例

タグの間に含まれるXMLは `<MetadataNotificationConfiguration></MetadataNotificationConfiguration>`、バケットに対して検索統合エンドポイントとの統合がどのように設定されているかを示します。この例では、という名前のAWSドメインでホストされている `records`という名前およびタイプの `2017`Elasticsearchインデックスにオブジェクトメタデータが送信され `current`ます。

```
HTTP/1.1 200 OK
Date: Thu, 20 Jul 2017 18:24:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/11.0.0
x-amz-request-id: 3832973499
Content-Length: 264
Content-Type: application/xml

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix>2017</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-
1:3333333:domain/records/current/2017</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

関連情報

"テナントアカウントを使用する"

PUT Bucketメタデータ通知設定リクエストを使用して**StorageGRID**で検索統合サービスを有効にします

PUT Bucket metadata notification configuration 要求を使用すると、個々のバケットで検索統合サービスを有効化できます。要求の本文に含めるメタデータ通知設定 XML では、デスティネーション検索インデックスにメタデータを送信するオブジェクトを指定します。

この処理を完了するには、バケットのs3：PutBucketMetadataNotification権限またはrootアカウントが必要です。

リクエスト

要求の本文にメタデータ通知設定が含まれている必要があります。各メタデータ通知設定には、 1 つ以上のルールが含まれています。各ルールは、環境 がオブジェクトを指定し、 StorageGRID がオブジェクトメタデータを送信するデスティネーションを指定します。

オブジェクトはオブジェクト名のプレフィックスでフィルタリングできます。たとえば、プレフィックスがであるオブジェクトのメタデータをあるデスティネーションに送信し、プレフィックスがであるオブジェクトのメタデータを別のデスティネーション `/videos`に送信 `/images`できます。

プレフィックスが重複している設定は有効ではなく、送信時に拒否されます。たとえば、プレフィックスがのオブジェクト用のルールとプレフィックスがのオブジェクト用 `test2`のルールを含む設定は `test`許可されません。

デスティネーションは、 StorageGRID エンドポイントの URN を使用して指定する必要があります。エンド

ポイントは、メタデータ通知設定が送信された時点で存在している必要があります。存在していない場合、要求はとして失敗します `400 Bad Request`。次のエラーメッセージが表示されます。 `Unable to save the metadata notification (search) policy. The specified endpoint URN does not exist: URN`.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:region:account-
ID:domain/mydomain/myindex/mytype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

次の表に、メタデータ通知設定 XML の要素を示します。

名前	製品説明	必須
MetadataNotificationConfiguration のページです	メタデータ通知でオブジェクトとデスティネーションの指定に使用されるルール用のコンテナタグ。 1 つ以上の Rule 要素を含みます。	はい
ルール	指定したインデックスにメタデータを追加する必要があるオブジェクトを特定するルール用のコンテナタグ。 プレフィックスが重複しているルールは拒否されます。 MetadataNotificationConfiguration 要素に含まれています。	はい
ID	ルールの一意の識別子。 Rule 要素に含まれています。	いいえ

名前	製品説明	必須
ステータス	Status には「 Enabled 」または「 Disabled 」を指定できます。無効になっているルールについては操作が実行されません。 Rule 要素に含まれています。	はい
プレフィックス	プレフィックスと一致するオブジェクトにルールが適用され、そのメタデータが指定したデスティネーションに送信されます。 すべてのオブジェクトを照合するには、空のプレフィックスを指定します。 Rule 要素に含まれています。	はい
デスティネーション	ルールのデスティネーションのコンテナタグ。 Rule 要素に含まれています。	はい
URN	オブジェクトメタデータが送信されるデスティネーションの URN 。次のプロパティを持つ StorageGRID エンドポイントの URN を指定する必要があります。 • `es`3番目の要素である必要があります。 • URNは、メタデータが格納されるインデックスとタイプ（の形式）で終わる必要があります `domain-name/myindex/mytype`。 エンドポイントは、 Tenant Manager またはテナント管理 API を使用して設定します。形式は次のとおりです。 • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` エンドポイントは設定 XML を送信する前に設定する必要があります。そうしないと、 404 エラーで設定が失敗します。 Urn は Destination 要素に含まれています。	はい

例をリクエストする

次の例は、バケットの検索統合を有効にする方法を示しています。この例では、すべてのオブジェクトのオブジェクトメタデータが同じデスティネーションに送信されます。

```
PUT /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
           <Urn>urn:sgws:es:::sgws-notifications/test1/all</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

この例では、プレフィックスに一致するオブジェクトのオブジェクトメタデータが `/images`1つ目のデスティネーションに送信され、プレフィックスに一致するオブジェクトのオブジェクトメタデータが `/videos`2つ目のデスティネーションに送信されます。

```
PUT /graphics?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Images-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/images</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Videos-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/videos</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

検索統合サービスで生成される **JSON**

バケットで検索統合サービスを有効にすると、オブジェクトのメタデータまたはタグの追加、更新、削除が行われるたびに、 JSON ドキュメントが生成されてデスティネーションエンドポイントに送信されます。

次の例は、という名前のバケットにキーを持つオブジェクトが作成され `test`たときに生成されるJSONの例を示しています。 `SGWS/Tagging.txt` `test`バケットはバージョン管理されていないため `versionId`、タグは空です。

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region":"us-east-1",
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

メタデータ通知に含まれているオブジェクトメタデータ

次の表に、検索統合が有効になっている場合にデスティネーションエンドポイントに送信される JSON ドキュメント内のすべてのフィールドを示します。

ドキュメント名には、バケット名、オブジェクト名、バージョン ID （存在する場合）が含まれます。

タイプ	項目名	製品説明
バケットとオブジェクトの情報	バケット	バケットの名前
バケットとオブジェクトの情報	キー	オブジェクトキーの名前
バケットとオブジェクトの情報	versionId	バージョン管理されたバケット内のオブジェクトのオブジェクトバージョン
バケットとオブジェクトの情報	リージョン	バケットのリージョン（例： `us-east-1`
システムメタデータ	サイズ	HTTP クライアントから認識できるオブジェクトのサイズ（バイト）
システムメタデータ	MD5	オブジェクトのハッシュ
ユーザメタデータ	メタデータ *`key:value`*	オブジェクトのすべてのユーザメタデータをキーと値のペアとして格納

タイプ	項目名	製品説明
タグ	タグ *key:value*	オブジェクトに対して定義されたすべてのオブジェクトタグをキーと値のペアとして使用します

タグとユーザメタデータの場合、 StorageGRID は文字列または S3 イベント通知として Elasticsearch に日付と番号を渡します。これらの文字列を日付または数値として解釈するように Elasticsearch を設定するには、動的フィールドマッピングおよびマッピング日付形式に関する Elasticsearch の手順に従ってください。検索統合サービスを設定する前に、インデックスの動的フィールドマッピングを有効にする必要があります。ドキュメントのインデックス作成後は、インデックス内のドキュメントのフィールドタイプを編集することはできません。

関連情報

"テナントアカウントを使用する"

StorageGRIDで**GET Storage Usage**リクエストを使用してアカウントとバケットのストレージ使用量を取得

GET Storage Usage 要求を使用すると、アカウントで使用しているストレージの総容量とアカウントに関連付けられているバケットごとの使用容量を確認できます。

アカウントとそのバケットで使用されているストレージ容量は、クエリパラメータを指定してListBuckets要求を変更することで取得できます `x-ntap-sg-usage`。バケットによるストレージの使用量は、システムで処理される PUT 要求や DELETE 要求とは別に追跡されます。特にシステムの負荷が高い場合などは、使用量の値が要求の処理に基づく想定値と同じになるまでに少し時間がかかることがあります。

デフォルトでは、 StorageGRID は strong-global 整合性を使用して、使用状況の情報を取得します。strong-global整合性を達成できない場合、StorageGRID はstrong-site整合性で使用状況情報を取得しようとします。

この処理を完了するには、s3：ListAllMyBuckets権限またはrootアカウントが必要です。

要求例

```
GET /?x-ntap-sg-usage HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

応答例

次の例は、 2 つのバケットに 4 つのオブジェクトと 12 バイトのデータが格納されたアカウントです。各バケットには、 2 つのオブジェクトと 6 バイトのデータが格納されています。

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 00:49:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/10.2.0
x-amz-request-id: 727237123
Content-Length: 427
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<UsageResult xmlns="http://s3.storagegrid.com/doc/2015-02-01">
<CalculationTime>2014-11-19T05:30:11.000000Z</CalculationTime>
<ObjectCount>4</ObjectCount>
<DataBytes>12</DataBytes>
<Buckets>
<Bucket>
<Name>bucket1</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
<Bucket>
<Name>bucket2</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
</Buckets>
</UsageResult>
```

バージョン管理

応答では、格納されているすべてのオブジェクトバージョンがとの `DataBytes`値に加算され `ObjectCount`ます。削除マーカーは合計に追加されません `ObjectCount`。

関連情報

"整合性"

従来の準拠のためのバケット要求が廃止されました

レガシー **StorageGRID** コンプライアンス向けの非推奨のバケットリクエスト

従来の準拠機能で作成されたバケットの管理には、 StorageGRID S3 REST API の使用が必要になる場合があります。

コンプライアンス機能は廃止されました

以前のバージョンの StorageGRID で提供されていた StorageGRID 準拠機能は廃止され、 S3 オブジェクトロックに置き換えられました。

グローバル準拠設定を有効にしている場合は、 StorageGRID 11.6 でグローバル S3 オブジェクトロック設定が有効になっています。準拠を有効にした新しいバケットは作成できなくなりました。ただし、必要に応じて、 StorageGRID S3 REST API を使用して、従来の準拠バケットを管理できます。

- "S3 REST APIを使用してS3オブジェクトロックを設定します"
- "ILM を使用してオブジェクトを管理する"
- "ネットアップのナレッジベース： StorageGRID 11.5 でレガシー準拠バケットを管理する方法"

廃止された準拠要求：

- "DEPRECATED - PUT Bucket request modifications for compliance"

  SGCompliance XML 要素は廃止されました。これまでは、この StorageGRID カスタム要素を PUT Bucket 要求のオプションの XML 要求の本文に含めて準拠バケットを作成できました。

- "廃止されました。GET Bucket compliance"

  GET Bucket compliance要求は廃止されました。ただし、既存のレガシー準拠バケットに対して現在有効な準拠設定を引き続き確認することができます。

- "廃止されました。PUT Bucket compliance"

  PUT Bucket compliance要求は廃止されました。ただし、この要求を引き続き使用して、既存のレガシー準拠バケットの準拠設定を変更できます。たとえば、既存のバケットをリーガルホールドの対象にしたり、バケットの保持期間を長くしたりできます。

StorageGRIDのSGCompliance要素は廃止されました

SGCompliance XML 要素は廃止されました。以前は、このStorageGRIDカスタム要素をCreateBucket要求のオプションのXML要求本文に含めて、準拠バケットを作成できました。

以前のバージョンの StorageGRID で提供されていた StorageGRID 準拠機能は廃止され、 S3 オブジェクトロックに置き換えられました。詳細については、次を参照してください。

- "S3 REST APIを使用してS3オブジェクトロックを設定します"
- "ネットアップのナレッジベース： StorageGRID 11.5 でレガシー準拠バケットを管理する方法"

準拠を有効にした新しいバケットを作成することはできなくなりました。準拠のためにCreateBucket要求の変更を使用して新しい準拠バケットを作成しようとすると、次のエラーメッセージが返されます。

```
The Compliance feature is deprecated.
Contact your StorageGRID administrator if you need to create new Compliant
buckets.
```

GET Bucket compliance要求は廃止されました。ただし、既存のレガシー準拠バケットに対して現在有効な準拠設定を引き続き確認することができます。

以前のバージョンの StorageGRID で提供されていた StorageGRID 準拠機能は廃止され、 S3 オブジェクトロックに置き換えられました。詳細については、次を参照してください。

- "S3 REST APIを使用してS3オブジェクトロックを設定します"
- "ネットアップのナレッジベース： StorageGRID 11.5 でレガシー準拠バケットを管理する方法"

この処理を完了するには、s3：GetBucketCompliance権限またはrootアカウントが必要です。

要求例

次の要求例では、という名前のバケットの準拠設定を確認でき `mybucket`ます。

```
GET /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

応答例

応答XMLに、 `<SGCompliance>`バケットに有効な準拠設定が表示されます。次の応答例では、バケットの準拠設定が示されており、各オブジェクトはグリッドに取り込まれてから 1 年間（ 525 、 600 分）保持されます。このバケットには現在リーガルホールドはありません。各オブジェクトは 1 年後に自動的に削除されます。

```
HTTP/1.1 200 OK
Date: date
Connection: connection
Server: StorageGRID/11.1.0
x-amz-request-id: request ID
Content-Length: length
Content-Type: application/xml

<SGCompliance>
  <RetentionPeriodMinutes>525600</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

名前	製品説明
RetentionPeriodMinutes です	このバケットに追加されたオブジェクトの保持期間を分で指定します。保持期間は、オブジェクトがグリッドに取り込まれたときからの期間です。
LegalHold のようになります	• True ：このバケットは、現在リーガルホールドの対象です。このバケット内のオブジェクトは、保持期間が過ぎても、リーガルホールドが解除されるまで削除できません。 • False ：このバケットは、現在リーガルホールドの対象ではありません。このバケット内のオブジェクトは、保持期間が過ぎたら削除できます。
自動削除	• True ：このバケット内のオブジェクトは、バケットがリーガルホールドの対象である場合を除き、保持期間が過ぎると自動的に削除されます。 • false ：このバケット内のオブジェクトは、保持期間が過ぎても自動的には削除されません。これらのオブジェクトを削除する必要がある場合は、手動で削除する必要があります。

エラー応答

バケットが準拠バケットとして作成されていない場合、応答のHTTPステータスコードはになり、S3エラーコードはに `XNoSuchBucketCompliance`なります `404 Not Found`。

StorageGRID で廃止された **PUT Bucket compliance** リクエスト

PUT Bucket compliance要求は廃止されました。ただし、この要求を引き続き使用して、既存のレガシー準拠バケットの準拠設定を変更できます。たとえば、既存のバケットをリーガルホールドの対象にしたり、バケットの保持期間を長くしたりできます。

以前のバージョンの StorageGRID で提供されていた StorageGRID 準拠機能は廃止され、 S3 オブジェクトロックに置き換えられました。詳細については、次を参照してください。

- "S3 REST APIを使用してS3オブジェクトロックを設定します"
- "ネットアップのナレッジベース： StorageGRID 11.5 でレガシー準拠バケットを管理する方法"

この処理を完了するには、s3：PutBucketCompliance権限またはrootアカウントが必要です。

PUT Bucket compliance 要求を発行する際は、準拠設定のすべてのフィールドに値を指定する必要があります。

要求例

次の要求例では、という名前のバケットの準拠設定を変更し `mybucket`ます。この例では、のオブジェクト `mybucket`がグリッドに取り込まれてから1年ではなく2年間（1、051、200分）保持されます。このバケットにリーガルホールドはありません。各オブジェクトは 2 年後に自動的に削除されます。

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Content-Length: 152

<SGCompliance>
  <RetentionPeriodMinutes>1051200</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

名前	製品説明
RetentionPeriodMinutes です	このバケットに追加されたオブジェクトの保持期間を分で指定します。保持期間は、オブジェクトがグリッドに取り込まれたときからの期間です。 重要 RetentionPeriodMinutesに新しい値を指定する場合は、バケットの現在の保持期間以上の値を指定する必要があります。バケットの保持期間の設定後は、その値を減らすことはできず、増やすことしかできません。
LegalHold のようになります	• True ：このバケットは、現在リーガルホールドの対象です。このバケット内のオブジェクトは、保持期間が過ぎても、リーガルホールドが解除されるまで削除できません。 • False ：このバケットは、現在リーガルホールドの対象ではありません。このバケット内のオブジェクトは、保持期間が過ぎたら削除できます。
自動削除	• True ：このバケット内のオブジェクトは、バケットがリーガルホールドの対象である場合を除き、保持期間が過ぎると自動的に削除されます。 • false ：このバケット内のオブジェクトは、保持期間が過ぎても自動的には削除されません。これらのオブジェクトを削除する必要がある場合は、手動で削除する必要があります。

準拠設定の整合性

PUT Bucket compliance 要求によって S3 バケットの準拠設定を更新すると、 StorageGRID は、グリッド全体のバケットのメタデータを更新しようとします。デフォルトでは、StorageGRIDは* strong-global *整合性を使用して、バケットのメタデータを含むすべてのデータセンターサイトとストレージノードで、変更された準拠設定のリードアフターライト整合性を保証します。

データセンターサイトまたはサイトの複数のストレージノードが利用できないために、StorageGRIDが* strong-global *整合性を達成できない場合、応答のHTTPステータスコードは次のようになります。 `503 Service Unavailable.`

この応答を受け取った場合は、必要なストレージサービスをできるだけ早く利用可能にするために、グリッド管理者に問い合わせる必要があります。グリッド管理者が各サイトで十分な数のストレージノードを利用可能にできない場合、テクニカルサポートから* strong-site *整合性を強制的に適用して、失敗した要求を再試行するよう指示されることがあります。

> テクニカルサポートから指示され、このレベルを使用した場合の潜在的な影響を理解している場合を除き、PUT bucket complianceで* strong-site *整合性を強制的に実行しないでください。

整合性を* strong-site *に減らすと、StorageGRIDは、サイト内のクライアント要求についてのみ、更新された準拠設定のリードアフターライト整合性を保証します。そのため、すべてのサイトおよびストレージノードが利用可能になるまでの間、 StorageGRID システムにはこのバケットに対して複数の異なる設定が一時的に存在することになる場合があります。整合性のない設定を使用すると、予期せぬ望ましくない動作が生じる可能性がありますたとえば、バケットをリーガルホールドの対象にする場合に、より低い整合性を強制的に適用すると、一部のデータセンターサイトでバケットの以前の準拠設定（リーガルホールドのオフ）が引き続き有効になることがあります。したがって、リーガルホールドの対象と思われるオブジェクトは、保持期間が経過すると、ユーザによって削除される場合と、 AutoDelete によって削除される場合があります。

強制的に* strong-site *整合性を使用するには、次のようにPUT Bucket compliance要求を再発行し、HTTP要求ヘッダーを含めます `Consistency-Control`。

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Consistency-Control: strong-site
```

エラー応答

- バケットが準拠バケットとして作成されていない場合、応答のHTTPステータスコードはになります `404 Not Found`。
- 要求がバケットの現在の保持期間よりも短い場合 `RetentionPeriodMinutes`、HTTPステータスコードはになります `400 Bad Request`。

関連情報

"廃止：準拠のための PUT Bucket 要求の変更"

アクセスポリシーを管理する

StorageGRID が **AWS** ポリシーを使用して **S3** バケットとオブジェクトへのアクセスを制御する方法

StorageGRID では、 Amazon Web Services （ AWS ）ポリシー言語を使用して、 S3 テナントによるバケットおよびバケット内のオブジェクトへのアクセスを制御できます。StorageGRID システムには、 S3 REST API ポリシー言語のサブセットが実装されています。S3 API のアクセスポリシーは JSON 形式で記述されます。

アクセスポリシーの概要

StorageGRID は、次の 3 種類のアクセス ポリシーをサポートしています。

- バケットポリシー。S3 APIのGetBucketPolicy、PutBucketPolicy、DeleteBucketPolicyの各処理、またはTenant Managerまたはテナント管理APIを使用して管理されます。バケットポリシーはバケットに関連

付けられ、バケットとそのオブジェクトへのバケット所有者アカウントやその他のアカウントのユーザによるアクセスを制御するために使用されます。バケットポリシー環境 は 1 つのバケットのみで、場合によっては複数のグループに分かれています。

- * グループポリシー * 。 Tenant Manager またはテナント管理 API を使用して設定します。グループポリシーはアカウントのグループに関連付けられ、そのアカウントが所有する特定のリソースにそのグループがアクセスできるように設定されます。グループポリシー環境 は 1 つのグループに限定され、場合によっては複数のバケットに適用されます。
- セッション ポリシー。AssumeRole リクエストの一部として含まれます。セッション ポリシーは特定のセッションにのみ適用され、グループ ポリシーとバケット ポリシーによって付与される権限に加えて、ユーザーが持つ権限をさらに定義します。

グループ、バケット、セッション ポリシー間の優先順位に違いはありません。

StorageGRID のバケットとグループのポリシーは、 Amazon が定義している特定の文法に従って記述されます。各ポリシーは一連のステートメントからなり、各ステートメントは次の要素で構成されます。

- ステートメント ID （ SID ）（オプション）
- 効果
- プリンシパル / NotPrincipal
- リソース / メモリソース
- アクション / NotAction
- Condition （オプション）

次の構造を使用して、権限を指定するポリシーステートメントが構築されます。 <Effect> を付与して、<Condition> に該当する場合に <Principal> に <Resource> に対する <Action> の実行を許可または拒否します。

各ポリシー要素は、特定の機能に使用されます。

要素	製品説明
SID	Sid 要素はオプションです。SID は、ユーザの概要 としてのみ使用されます。StorageGRID システムに格納はされますが、システムで解釈されません。
効果	Effect 要素では、指定した処理を許可するか拒否するかを指定します。Action 要素でサポートされるキーワードを使用して、バケットやオブジェクトで許可（または拒否）する処理を指定する必要があります。

要素	製品説明
プリンシパル / NotPrincipal	ユーザ、グループ、およびアカウントに特定のリソースへのアクセスと特定の操作の実行を許可できます。要求に S3 の署名が含まれていない場合は、ワイルドカード文字（ * ）をプリンシパルとして指定することで匿名アクセスが許可されます。デフォルトでは、アカウントが所有するリソースへのアクセスは root アカウントにのみ許可されます。 プリンシパル： • `"Principal": "*"` 匿名（署名なし）リクエストを含む、すべてのユーザーに一致します • `"Principal": { "AWS": "*" }`認証済みのIDまたはユーザーに一致する（匿名リクエストには一致しない） • バケットポリシーにのみ適用されます • プリンシパルとは、権限が付与または拒否されるアカウント/ユーザーのことです。 Principal 要素を指定する必要があるのはバケットポリシーだけです。グループポリシーの場合は、ポリシーが関連付けられたグループが暗黙的にプリンシパルになります。
リソース / メモリソース	Resource 要素では、バケットとオブジェクトを指定します。Amazon リソースネーム（ ARN ）を使用してリソースを指定し、バケットやオブジェクトに対する権限を許可または拒否することができます。
アクション / NotAction	権限は Action 要素と Effect 要素の 2 つで構成されます。グループがリソースを要求すると、リソースへのアクセスが許可または拒否されます。権限を明示的に割り当てていないかぎりアクセスは拒否されますが、明示的な拒否を使用して別のポリシーで付与された権限を上書きすることもできます。
条件	Condition 要素はオプションです。条件を使用すると、ポリシーを適用する条件を示す式を作成できます。

Action 要素では、ワイルドカード文字（ * ）を使用してすべての処理または処理のサブセットを指定できます。たとえば、次の Action の値は、 s3 ： GetObject 、 s3 ： PutObject 、 s3 ： DeleteObject などの権限に一致します。

```
s3:*Object
```

Resource 要素では、ワイルドカード文字（ * ）および（？）を使用できます。アスタリスク（ * ）は 0 文字以上の文字に一致し、疑問符（？）は 0 文字以上の文字に一致します。 任意の 1 文字に一致します。

Principal要素では、匿名アクセスを設定してすべてのユーザに権限を付与する場合を除き、ワイルドカード文字はサポートされません。たとえば、 Principal の値としてワイルドカード（ * ）を設定します。

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

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

次の例では、 Effect 、 Principal 、 Action 、および Resource の各要素を使用して記述します。この例は、完全なバケットポリシーのステートメントで、「allow」という効果を使用して、Principals、adminグループ、およびfinanceグループ `federated-group/finance`に、というバケット `mybucket`に対して`Action`を実行する権限 `s3:ListBucket`、およびそのバケット内のすべてのオブジェクトに対してActionを`s3:GetObject`付与して `federated-group/admin`います。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::27233906934684427525:federated-group/admin",
          "arn:aws:iam::27233906934684427525:federated-group/finance"
        ]
      },
      "Action": [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::mybucket",
        "arn:aws:s3:::mybucket/*"
      ]
    }
  ]
}
```

バケットポリシーのサイズの上限は 20 、 480 バイトで、グループポリシーのサイズの上限は 5 、 120 バイトです。

ポリシーノセイコウセイ

デフォルトでは、グループポリシーに対するすべての更新の整合性レベルは結果整合性です。グループポリシーの整合性が取れた場合、ポリシーキャッシュのために変更が有効になるまでにさらに15分かかることがあります。デフォルトでは、バケットポリシーに対する更新の整合性は非常に高くなります。

バケットポリシーの更新の整合性保証は必要に応じて変更できます。たとえば、サイトが停止しているときにバケットポリシーを変更できるようにすることができます。

この場合は、PutBucketPolicy要求でヘッダーを設定する `Consistency-Control`か、PUT Bucket consistency要

求を使用します。バケットポリシーの整合性が確保されると、ポリシーキャッシュのために変更が有効になるまでにさらに8秒かかることがあります。

> 一時的な状況を回避するために整合性の値を別の値に設定する場合は、完了後にバケットレベルの設定を元の値に戻してください。そうしないと、以降のすべてのバケット要求で変更後の設定が使用されます。

セッションポリシーとは何ですか?

セッション ポリシーは、ユーザーがグループを引き受ける場合など、特定のセッション中に利用可能な権限を一時的に制限するアクセス ポリシーです。セッション ポリシーでは権限のサブセットのみを許可でき、追加の権限を付与することはできません。グループ自体にはより広範な権限がある可能性があります。

ポリシーステートメントでは **ARN** を使用します

ポリシーステートメントでは、 Principal 要素と Resource 要素で ARN を使用します。

- S3 リソースの ARN の指定には次の構文を使用します。

```
arn:aws:s3:::bucket-name
arn:aws:s3:::bucket-name/object_key
```

- アイデンティティリソースの ARN （ユーザおよびグループ）の指定には次の構文を使用します。

```
arn:aws:iam::account_id:root
arn:aws:iam::account_id:user/user_name
arn:aws:iam::account_id:group/group_name
arn:aws:iam::account_id:federated-user/user_name
arn:aws:iam::account_id:federated-group/group_name
```

その他の考慮事項：

- オブジェクトキーの一部にワイルドカードとしてアスタリスク（ * ）を使用すると、 0 文字以上の文字に一致します。
- オブジェクトキーで指定できる国際文字は、JSON UTF-8 または JSON \u エスケープシーケンスを使用してエンコードする必要があります。パーセントエンコーディングはサポートされていません。

  "RFC 2141 の URN 構文"

  PutBucketPolicy処理のHTTP要求の本文は、charset=UTF-8でエンコードする必要があります。

ポリシー内のリソースを指定します

ポリシーステートメントでは、 Resource 要素を使用して、権限を許可または拒否するバケットやオブジェクトを指定できます。

- Resource 要素はポリシーの各ステートメントに必要です。ポリシーでは、リソースは要素で指定されま

す。または、 `NotResource`除外する場合は要素でも指定され `Resource`ます。

- リソースは S3 リソースの ARN で指定します。例：

```
"Resource": "arn:aws:s3:::mybucket/*"
```

- オブジェクトキーの内部でポリシー変数を使用することもできます。例：

```
"Resource": "arn:aws:s3:::mybucket/home/${aws:username}/*"
```

- リソース値には、グループポリシー作成時にまだ存在しないバケットを指定できます。

ポリシーでプリンシパルを指定します

ポリシーステートメントでリソースへのアクセスを許可または拒否するユーザ、グループ、またはテナントアカウントを指定するには、 Principal 要素を使用します。

- バケットポリシーの各ポリシーステートメントには、 Principal 要素を含める必要があります。グループはプリンシパルとみなされるため、グループポリシーのポリシーステートメントではPrincipal要素は必要ありません。
- ポリシーでは、「Principal」要素または「NotPrincipal」要素（除外の場合）でプリンシパルを指定します。
- ID または ARN を使用してアカウントベースのアイデンティティを指定する必要があります。

```
"Principal": { "AWS": "account_id"}
"Principal": { "AWS": "identity_arn" }
```

- 次の例では、テナントアカウント ID 27233906934684427525 を使用しています。この場合、 root アカウントとそのすべてのユーザが含まれます。

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

- root アカウントのみを指定する場合は次のようになります。

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:root" }
```

- 特定のフェデレーテッドユーザ（「 Alex 」）を指定する場合は次のようになります。

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

- 特定のフェデレーテッドグループ（「 Managers 」）のみを指定する場合は次のようになります。

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

- 匿名プリンシパルを指定する場合は次のようになります。

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

- あいまいさを排除するために、ユーザ名の代わりに UUID を使用できます。

```
arn:aws:iam::27233906934684427525:user-uuid/de305d54-75b4-431b-adb2-
eb6b9e546013
```

  たとえば、Alexが組織を離れ、ユーザ名が削除されたとし `Alex` ます。新しい`Alex`が組織に参加し、同じユーザー名が割り当てられている場合 `Alex`、新しいユーザーは元のユーザーに付与された権限を意図せず継承する可能性があります。

- プリンシパル値には、バケットポリシー作成時にまだ存在しないグループ名またはユーザー名を指定できます。

ポリシーで権限を指定します

ポリシーでは、 Action 要素を使用してリソースに対する権限を許可または拒否します。ポリシーには、「 Action 」要素で示される一連の権限、または除外する「 NotAction 」要素で指定できる一連の権限があります。それぞれが特定の S3 REST API 処理に対応しています。

次の表に、バケットに適用される権限とオブジェクトに適用される権限を示します。

Amazon S3では、PutBucketReplicationとDeleteBucketReplicationの両方のアクションにs3：PutReplicationConfiguration権限が使用されるようになりました。StorageGRID では、元の Amazon S3 仕様に一致する個別の権限が各アクションに使用されます。

DELETEは、PUTを使用して既存の値を上書きした場合に実行されます。

バケットに適用される権限

権限	**S3 REST API** の処理	**StorageGRID** のカスタム
S3 ： CreateBucket を指定します	CreateBucket	はい。 注：グループポリシーでのみ使用します。
S3 ： DeleteBucket	DeleteBucket	

権限	**S3 REST API** の処理	**StorageGRID** のカスタム
S3 ： DeleteBucketMetadataNotification	バケットのメタデータ通知設定を削除します	はい
S3 ： DeleteBucketPolicy	DeleteBucketPolicy	
S3 ： DeleteReplicationConfiguration	DeleteBucketReplication	○（PUTとDELETEに別 々 の権限を設定）
S3 ： GetBucketAcl	GetBucketAcl	
S3 ： GetBucketCompliance	GET Bucket compliance（廃止）	はい
S3 ： GetBucketConsistency	GET Bucket consistency	はい
S3 ： GetBucketCORS	GetBucketCors	
S3 ： GetEncryptionConfiguration	GetBucketEncryptionの略	
S3 ： GetBucketLastAccessTime	GET Bucket last access time のように指定します	はい
S3 ： GetBucketLocation	GetBucketLocation	
S3 ： GetBucketMetadataNotification	GET Bucket metadata notification configuration のコマンドです	はい
S3 ： GetBucketNotification	GetBucketNotificationConfigurationを参照してください	
S3 ： GetBucketObjectLockConfiguration	GetObjectLockConfigurationの略	
S3 ： GetBucketPolicy	GetBucketPolicy	
S3 ： GetBucketTagging	GetBucketTagging	
S3 ： GetBucketVersioning	GetBucketVersioning	
S3 ： GetLifecycleConfiguration	GetBucketLifecycleConfiguration	
S3 ： GetReplicationConfiguration	GetBucketReplicationの略	

権限	**S3 REST API** の処理	**StorageGRID** のカスタム
S3 ： ListAllMyBuckets	• ListBuckets • GET Storage Usage の略	○（GET Storage Usage）。 注：グループポリシーでのみ使用します。
S3 ： ListBucket	• GetObject • ヘッドバケット • ヘッドオブジェクト • ListObjects	
S3 ： ListBucketMultipartUploads	• ListMultipartUploads	
S3 ： ListBucketVersions	GET Bucket versions （バケットバージョンの取得	
S3 ： PutBucketCompliance	PUT Bucket compliance（廃止）	はい
S3 ： PutBucketConsistency	PUT Bucket consistency	はい
S3 ： PutBucketCORS	• DeleteBucketCors† • PutBucketCorsの略	
S3 ： PutEncryptionConfiguration	• DeleteBucketEncryption • PutBucketEncryptionの略	
S3 ： PutBucketLastAccessTime	PUT Bucket last access time のように指定します	はい
S3 ： PutBucketMetadataNotification	PUT Bucket metadata notification configuration のコマンドです	はい
S3 ： PutBucketNotification	PutBucketNotificationConfigurationの略	
S3 ： PutBucketObjectLockConfiguration	• 要求ヘッダーが指定されたCreateBucket `x-amz-bucket-object-lock-enabled: true`（s3：CreateBucket権限も必要） • PutObjectLockConfiguration	

権限	**S3 REST API** の処理	**StorageGRID** のカスタム
S3 ： PutBucketPolicy	PutBucketPolicy	
S3 ： PutBucketTagging	• DeleteBucketTagging† • PutBucketTaggingの略	
S3 ： PutBucketVersioning	PutBucketVersioning	
S3 ： PutLifecycleConfiguration	• DeleteBucketLifecycle† • PutBucketLifecycleConfiguration	
S3 ： PutReplicationConfiguration	PutBucketReplicationの略	○（PUTとDELETEに別 々 の権限を設定）

オブジェクトに適用される権限

権限	**S3 REST API** の処理	**StorageGRID** のカスタム
S3 ： AbortMultipartUpload	• AbortMultipartUpload	
S3：Bypassガバナー 保持	• deleteObject • オブジェクトの削除 • PutObjectRetention	
S3 ： DeleteObject	• deleteObject • オブジェクトの削除	
S3 ： DeleteObjectTagging	DeleteObjectTagging	
S3 ： DeleteObjectVersionTagging	DeleteObjectTagging（オブジェクトの特定のバージョン）	
S3 ： DeleteObjectVersion	deleteObject（オブジェクトの特定のバージョン）	
S3 ： GetObject	• GetObject • ヘッドオブジェクト • SelectObjectContent の順に選択します	

権限	**S3 REST API** の処理	**StorageGRID** のカスタム
S3 ： GetObjectAcl	GetObjectAcl	
S3 ： GetObjectLegalHold	GetObjectLegalHold	
S3 ： GetObjectRetention	GetObjectRetention	
S3 ： GetObjectTagging	GetObjectTagging	
S3 ： GetObjectVersionTagging	GetObjectTagging（オブジェクトの特定のバージョン）	
S3：GetObjectVersion	GetObject（オブジェクトの特定のバージョン）	
S3 ： ListMultipartUploadParts	ListParts	
S3 ： PutObject	• CopyObject • CompleteMultipartUpload • CreateMultipartUpload • PutObject • パーツのアップロード • パーツコピーをアップロード	
S3 ： PutObjectLegalHold	PutObjectLegalHold	
S3 ： PutObjectRetention	PutObjectRetention	
S3 ： PutObjectTagging	PutObjectTagging	
S3 ： PutObjectVersionTagging	PutObjectTagging（オブジェクトの特定のバージョン）	
S3 ： PutOverwriteObject	• CompleteMultipartUpload • CopyObject • DeleteObjectTagging • PutObject • PutObjectTagging	はい
S3 ： RestoreObject	RestoreObject	

PutOverwriteObject 権限を使用する

s3 ： PutOverwriteObject 権限は、オブジェクトの作成または更新を行う環境 処理のカスタムの StorageGRID 権限です。この権限の設定により、オブジェクトのデータ、ユーザ定義メタデータ、または S3 オブジェクトのタグをクライアントが上書きできるかどうかが決まります。

この権限で可能な設定は次のとおりです。

- * allow * ：クライアントはオブジェクトを上書きできます。これがデフォルト設定です。
- **Deny**:クライアントはオブジェクトを上書きできません。PutOverwriteObject 権限が Deny に設定されている場合の動作は次のとおりです。
  - 同じパスで既存のオブジェクトが見つかった場合は、次の手順を実行します。
    - オブジェクトのデータ、ユーザ定義メタデータ、またはS3オブジェクトのタグを上書きすることはできません。
    - 実行中の取り込み処理はすべてキャンセルされ、エラーが返されます。
    - S3のバージョン管理が有効になっている場合は、Denyに設定すると、PutObjectTagging処理またはDeleteObjectTagging処理によってオブジェクトとその最新でないバージョンのTagSetが変更されなくなります。
  - 既存のオブジェクトが見つからない場合、この権限は無効です。
- この権限が存在しない場合、効果は「許可」が設定されている場合と同じです。

> 現在の S3 ポリシーで上書きが許可されていて、PutOverwriteObject 権限が Deny に設定されている場合、クライアントはオブジェクトのデータ、ユーザー定義のメタデータ、またはオブジェクトのタグ付けを上書きできません。さらに、クライアントによる変更を禁止する チェックボックスが選択されている場合 (**[構成] > [セキュリティ設定] > [ネットワークとオブジェクト]**)、その設定は PutOverwriteObject 権限の設定よりも優先されます。

ポリシーの条件を指定します

条件は、ポリシーが有効になるタイミングを定義します。条件は演算子とキーと値のペアで構成されます。

条件はキーと値のペアを使用して評価されます。Condition 要素には複数の条件を指定でき、各条件には複数のキーと値のペアを含めることができます。条件ブロックの形式は次のとおりです。

```
Condition: {
     condition_type: {
          condition_key: condition_values
```

次の例では、 IpAddress 条件で SourceIp 条件キーを使用しています。

```
"Condition": {
    "IpAddress": {
      "aws:SourceIp": "54.240.143.0/24"
        ...
},
        ...
```

サポートされる条件演算子は次の

条件演算子は次のように分類されます。

- 文字列
- 数値
- ブーリアン
- IPアドレス
- Null チェック

条件演算子	製品説明
StringEquals	キーを文字列値と比較し、完全一致であるかを確認します（大文字と小文字の区別あり）。
StringNotEquals	キーを文字列値と比較し、不一致であるかを確認します（大文字と小文字の区別あり）。
StringEqualsIgnoreCase	キーを文字列値と比較し、完全一致であるかを確認します（大文字と小文字の区別なし）。
StringNotEqualsIgnoreCase	キーを文字列値と比較し、不一致であるかを確認します（大文字と小文字の区別なし）。
StringLike	キーを文字列値と比較し、完全一致であるかを確認します（大文字と小文字の区別あり）。ワイルドカード文字「*」と「?」を使用できます。
StringNotLike	キーを文字列値と比較し、不一致であるかを確認します（大文字と小文字の区別あり）。ワイルドカード文字「*」と「?」を使用できます。
NumericEquals （数値機器）	キーを数値と比較し、完全一致であるかを確認します。
NumericNotEquals	キーを数値と比較し、不一致であるかを確認します。
NumericGreaterThan	キーを数値と比較し、「より大きい」の一致であるかどうかを確認します。

条件演算子	製品説明
NumericGreaterThanEquals	キーを数値と比較し、「以上」の一致であるかどうかを確認します。
NumericLessThan	キーを数値と比較し、「より小さい」一致であるかを確認します。
NumericLessThanEquals	キーを数値と比較し、「小なり」の一致であるかを確認します。
ブール値	キーをブール値と比較し、「trueまたはfalse」の一致であるかを確認します。
IP アドレス	キーを IP アドレスまたは IP アドレスの範囲と比較します。
NotIpAddress	キーを IP アドレスまたは IP アドレスの範囲と比較し、不一致であるかを確認します。
ヌル	現在の要求コンテキストに条件キーが存在するかどうかを確認します。
存在する場合	Null条件を除く、任意の条件演算子に追加して、その条件キーが存在しないかどうかを確認します。条件キーが存在しない場合はTRUEを返します。

サポートされている条件キー

Conditionキー	アクション	製品説明
AWS ： sourceIP	IP 演算子	リクエストが送信されたIPアドレスと比較します。バケット操作またはオブジェクト操作に使用できます。 注**:** S3 リクエストが管理ノードおよびゲートウェイノードのロードバランサーサービスを経由して送信された場合、これはロードバランサーサービスの上流の IP アドレスと比較されます。 注: サードパーティ製の非透過型ロードバランサーを使用する場合は、そのロードバランサーのIPアドレスと比較します。 `X-Forwarded-For`ヘッダーは有効性を確認できないため、無視されます。
AWS ：ユーザ名	リソース / ID	リクエストが送信された送信者のユーザー名と比較します。バケット操作またはオブジェクト操作に使用できます。

Conditionキー	アクション	製品説明
S3 ：デリミタ	S3 ： ListBucket と S3 ： ListBucketVersions 権限	ListObjects または ListObjectVersions リクエストで指定された区切り文字パラメータと比較します。
S3：ExistingObjectTag /<tag-key>	S3 ： DeleteObjectTagging S3 ： DeleteObjectVersionTagging S3 ： GetObject S3 ： GetObjectAcl 3：GetObjectTagging S3：GetObjectVersion S3：GetObjectVersionAcl S3 ： GetObjectVersionTagging S3：PutObjectAcl S3 ： PutObjectTagging S3：PutObjectVersionAcl S3 ： PutObjectVersionTagging	既存のオブジェクトに、特定のタグキーと値が存在する必要があります。
S3 ： max-keys	S3 ： ListBucket と S3 ： ListBucketVersions 権限	ListObjectsまたはListObjectVersionsリクエストで指定された max-keys パラメータと比較します。
s3:オブジェクトロックモード	S3 ： PutObject	と比較すると `object-lock-mode`PutObject 、CopyObject、および CreateMultipartUpload リクエストのリクエスト ヘッダーから展開されます。
s3:オブジェクトロックモード	S3 ： PutObjectRetention	と比較すると `object-lock-mode`PutObjectRetention リクエストの XML 本文から展開されます。

Conditionキー	アクション	製品説明
S3 ： object-lock-remaining-retention-days	S3 ： PutObject	要求ヘッダーで指定されたretain-until-dateと比較される `x-amz-object-lock-retain-until-date`か、バケットのデフォルト保持期間から計算され、次の要求でこれらの値が許容範囲内であることが確認されます。 • PutObject • CopyObject • CreateMultipartUpload
S3 ： object-lock-remaining-retention-days	S3 ： PutObjectRetention	は、PutObjectRetention要求で指定されたretain-until-dateと比較して、許容範囲内であることを確認します。
S3 ：プレフィックス	S3 ： ListBucket と S3 ： ListBucketVersions 権限	ListObjectsまたはListObjectVersionsリクエストで指定されたプレフィックスパラメータ、あるいはGetObjectまたはHeadObjectに指定されたキーと比較します。
S3：RequestObjectTag /<tag-key>	S3 ： PutObject S3 ： PutObjectTagging S3 ： PutObjectVersionTagging	オブジェクト要求にタグ付けが含まれる場合、特定のタグキーと値が必要です。
s3:x-amz-copy-source	S3 ： PutObject	リクエストヘッダーから展開された x-amz-copy-source を PutObject および UploadPartCopy リクエストと比較します。
s3:x-amz-サーバー側暗号化-カスタマーアルゴリズム	S3 ： PutObject	と比較すると `sse-customer-algorithm`または `copy-source-sse-customer-algorithm`PutObject 、CopyObject、CreateMultipartUpload、UploadPart 、UploadPartCopy、および CompleteMultipartUpload リクエストのリクエスト ヘッダーから展開されます。

ポリシーで変数を指定します

ポリシーで変数を使用すると、該当するポリシーの情報を設定できます。ポリシー変数は、要素内および要素内の文字列比較で `Condition`使用できます `Resource`。

この例では、変数は `${aws:username}`Resource要素の一部です。

```
"Resource": "arn:aws:s3:::bucket-name/home/${aws:username}/*"
```

この例では、変数は `${aws:username}`ConditionブロックのCondition値の一部です。

```
"Condition": {
    "StringLike": {
      "s3:prefix": "${aws:username}/*"
        ...
},
        ...
```

変数	製品説明
`${aws:SourceIp}`	SourceIp キーを指定の変数として使用します。
`${aws:username}`	username キーを指定の変数として使用します。
`${s3:prefix}`	サービス固有のプレフィックスキーを指定の変数として使用します。
`${s3:max-keys}`	サービス固有の max-keys キーを指定の変数として使用します。
`${*}`	特殊文字です。文字をリテラル * 文字として使用します。
`${?}`	特殊文字です。文字をリテラル?文字として使用します。
`${$}`	特殊文字です。文字「 $ 」をリテラル文字として使用します。

特別な処理を必要とするポリシーを作成します

ポリシーで付与される権限によって、アカウントの root ユーザがロックアウトされるなど、セキュリティや継続的な運用に支障が生じることがあります。StorageGRID の S3 REST API の実装では、ポリシーの検証時の制限は Amazon よりも厳しくありませんが、評価時は同等の制限が適用されます。

ポリシーの説明	ポリシータイプ	**Amazon** の動作	**StorageGRID** の動作
自身に対し、 root アカウントに対するすべての権限を拒否する	バケット	有効で適用されるが、 S3 バケットのすべてのポリシー処理に対する権限は引き続き root ユーザアカウントに付与される	同じ
自身に対しユーザ / グループに対するすべての権限を拒否する	グループ	有効で適用されます	同じ

ポリシーの説明	ポリシータイプ	**Amazon** の動作	**StorageGRID** の動作
外部アカウントグループに対し任意の権限を許可します	バケット	無効なプリンシパルです	有効だが、 S3 バケットのすべてのポリシー処理に対する権限をポリシーで許可すると 405 Method Not Allowed エラーが返されます
外部アカウントの root またはユーザに任意の権限を許可します	バケット	有効だが、 S3 バケットのすべてのポリシー処理に対する権限をポリシーで許可すると 405 Method Not Allowed エラーが返されます	同じ
すべてのユーザにすべての処理に対する権限を許可します	バケット	有効だが、外部アカウントの root およびユーザについては、 S3 バケットのすべてのポリシー処理に対する権限で 405 Method Not Allowed エラーが返されます	同じ
すべてのユーザに対してすべての処理に対する権限を拒否する	バケット	有効で適用されるが、 S3 バケットのすべてのポリシー処理に対する権限は引き続き root ユーザアカウントに付与される	同じ
プリンシパルとして新規のユーザまたはグループを指定します	バケット	無効なプリンシパルです	有効
リソースとして新規の S3 バケットを指定する必要があります	グループ	有効	同じ
プリンシパルとしてローカルグループを指定します	バケット	無効なプリンシパルです	有効
ポリシーは、オブジェクトをPUTするための非所有者アカウント（匿名アカウントを含む）権限を付与します。	バケット	有効。オブジェクトの所有権は作成者アカウントにあり、バケットポリシーは適用されません。作成者アカウントは、オブジェクトACLを使用してオブジェクトへのアクセス権限を付与する必要があります。	有効。オブジェクトはバケット所有者アカウントによって所有され、バケットポリシーが適用される。

Write-Once-Read-Many （ WORM ）による保護

データ、ユーザ定義オブジェクトのメタデータ、 S3 オブジェクトのタグを保護するために、 Write-Once-Read-Many （ WORM ）バケットを作成することができます。新しいオブジェクトの作成を許可し、既存のコンテンツの上書きや削除を防止するように WORM バケットを設定します。ここで説明するいずれかの方法を使用します。

上書きを常に拒否するには、次の操作を実行します。

- グリッド マネージャーから、構成 > セキュリティ > セキュリティ設定 > ネットワークとオブジェクト に移動し、クライアントの変更を禁止する チェックボックスをオンにします。
- 次のルールと S3 ポリシーを適用します。
  - S3 ポリシーに PutOverwriteObject DENY 処理を追加します。
  - S3 ポリシーに DeleteObject DENY 処理を追加します。
  - S3ポリシーにPutObject Allow処理を追加します。

> DeleteObject を S3 ポリシーで DENY に設定しても、「30日後にコピーをゼロにする」などのルールが存在する場合、ILM がオブジェクトを削除するのを防ぐことはできません。

> これらのルールとポリシーがすべて適用されても、同時書き込みからは保護されません（状況Aを参照）。保護の対象になるのはシーケンシャルな上書きです（状況 B を参照）。

- 状況 A * ：同時書き込み（保護対象外）

```
/mybucket/important.doc
PUT#1 ---> OK
PUT#2 -------> OK
```

- 状況 B * ：シーケンシャルな上書き（保護対象）

```
/mybucket/important.doc
PUT#1 -------> PUT#2 ---X (denied)
```

関連情報

- "StorageGRID の ILM ルールによるオブジェクトの管理"
- "バケットポリシーの例"
- "グループポリシーの例"
- "セッションポリシーの例"
- "ILM を使用してオブジェクトを管理する"
- "テナントアカウントを使用する"

StorageGRID S3 REST API セッションポリシーの例

次の例を使用して、 StorageGRIDセッション ポリシーを構築します。

例: オブジェクトの取得を許可するセッションポリシーを設定する

この例では、セッションのプリンシパルはbucket1からオブジェクトを取得することのみが許可されています。その他のアクションはすべて暗黙的に拒否されますが、"S3 ： PutOverwriteObject"権限の使用などのStorageGRID固有のアクションは除きます。セッションポリシーは、AssumeRole APIの呼び出し時にJSONファイルとして提供できます。

```
{
  "Statement": [
    {
      "Action": "s3:GetObject",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::bucket1/*"
    }
  ]
}
```

StorageGRID S3 REST API バケットポリシーの例

このセクションの例を使用して、バケットのStorageGRID アクセスポリシーを作成します。

バケットポリシーでは、そのポリシーが関連付けられたバケットに対するアクセス権限を指定します。バケットポリシーを設定するには、次のいずれかのツールを使用してS3 PutBucketPolicy APIを使用します。

- "テナントマネージャ"です。
- AWS CLIで次のコマンドを使用（を参照"バケットの処理"）：

```
> aws s3api put-bucket-policy --bucket examplebucket --policy
file://policy.json
```

StorageGRID では、プリンシパル：

- `"Principal": "*"` 匿名（署名なし）リクエストを含む、すべてのユーザーに一致します
- `"Principal": { "AWS": "*" }`認証済みのIDまたはユーザーに一致する（匿名リクエストには一致しない）
- バケットポリシーにのみ適用されます
- プリンシパルとは、権限が付与または拒否されるアカウント/ユーザーのことです。

例：すべてのユーザにバケットへの読み取り専用アクセスを許可する

この例では、匿名ユーザを含むすべてのユーザにバケット内のオブジェクトのリストとバケット内のすべての

オブジェクトのGetObject処理を許可しています。それ以外の処理はすべて拒否されます。バケットへの書き込み権限がrootアカウント以外に付与されていないため、このポリシーは特に有用ではない場合があります。

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadOnlyAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:GetObject", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"]
    }
  ]
}
```

例：あるアカウントのすべてのユーザにフルアクセスを許可し、別のアカウントのすべてのユーザにバケットへの読み取り専用アクセスを許可する

この例では、指定したアカウントのすべてのユーザにバケットへのフルアクセスを許可し、別のアカウントのすべてのユーザには、バケットのList処理とオブジェクトキープレフィックスで始まるバケット内のオブジェクトのGetObject処理のみを許可して `shared/`います。

> StorageGRID では、非所有者アカウント（匿名アカウントを含む）によって作成されたオブジェクトが、バケット所有者アカウントによって所有されます。バケットポリシーで、これらのオブジェクトの環境 を設定します。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "95390887230002558202"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::examplebucket/shared/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::examplebucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "shared/*"
        }
      }
    }
  ]
}
```

例：すべてのユーザにバケットへの読み取り専用アクセスを許可し、指定したグループにフルアクセスを許可する

この例では、匿名ユーザを含むすべてのユーザにバケットのList処理とバケット内のすべてのオブジェクトのGetObject処理を許可し、指定したアカウントのグループに属するユーザにのみ `Marketing`フルアクセスを許可しています。

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

例：クライアントの **IP** 範囲を限定して、すべてのユーザにバケットへの読み取り **/** 書き込みアクセスを許可する

この例では、指定した IP 範囲（ 54.240.143.0~54.240.143.255 で 54.240.143.188 を除く）からの要求についてのみ、匿名ユーザを含むすべてのユーザにバケットの List 処理とバケット内のすべてのオブジェクトの全処理を許可しています。それ以外の処理はすべて拒否され、 IP 範囲外の要求はすべて拒否されます。

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadWriteAccessIfInSourceIpRange",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:*Object", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"],
      "Condition": {
        "IpAddress": {"aws:SourceIp": "54.240.143.0/24"},
        "NotIpAddress": {"aws:SourceIp": "54.240.143.188"}
      }
    }
  ]
}
```

例：指定したフェデレーテッドユーザにのみバケットへのフルアクセスを許可します

この例では、フェデレーテッドユーザAlexにバケットとそのオブジェクトへのフルアクセスが許可され `examplebucket`ています。'root' を含む他のすべてのユーザは ' すべての操作を明示的に拒否されますただし、「 root 」による Put/Get/DeleteBucketPolicy は拒否されません。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Deny",
      "NotPrincipal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

例： **PutOverwriteObject** 権限

この例では、PutOverwriteObjectとDeleteObjectの効果により、 `Deny`オブジェクトのデータ、ユーザ定義メタデータ、S3オブジェクトのタグを誰も上書きまたは削除できなくなります。

```
{
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3:PutOverwriteObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": "arn:aws:s3:::wormbucket/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::wormbucket"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::wormbucket/*"
    }
  ]
}
```

StorageGRID S3 REST API グループポリシーの例

このセクションの例を使用して、グループのStorageGRID アクセスポリシーを作成します。

グループポリシーは、そのポリシーが関連付けられたグループに対するアクセス権限を指定します。ポリシーには暗黙的な要素が含まれていない `Principal`ため、要素はありません。グループポリシーは Tenant Manager または API を使用して設定します。

例： **Tenant Manager** を使用してグループポリシーを設定します

Tenant Managerでグループを追加または編集するときに、グループポリシーを選択して、このグループのメンバーに付与するS3アクセス権限を決定できます。を参照して "S3 テナント用のグループを作成します"

- * No S3 Access * ：デフォルトオプション。バケットポリシーでアクセスが許可されていないかぎり、このグループのユーザはS3リソースにアクセスできません。このオプションを選択すると、デフォルトでは root ユーザにのみ S3 リソースへのアクセスが許可されます。
- * 読み取り専用アクセス * ：このグループのユーザには、 S3 リソースへの読み取り専用アクセスが許可されます。たとえば、オブジェクトをリストして、オブジェクトデータ、メタデータ、タグを読み取ることができます。このオプションを選択すると、テキストボックスに読み取り専用グループポリシーの JSON 文字列が表示されます。この文字列は編集できません。
- * フルアクセス * ：このグループのユーザには、バケットを含む S3 リソースへのフルアクセスが許可されます。このオプションを選択すると、テキストボックスにフルアクセスグループポリシーの JSON 文字列が表示されます。この文字列は編集できません。
- ランサムウェアの軽減：このサンプルポリシーは、このテナントのすべてのバケットを環境 します。このグループのユーザは共通の操作を実行できますが、オブジェクトのバージョン管理が有効になっているバケットからオブジェクトを完全に削除することはできません。

  Manage All Buckets権限を持つTenant Managerユーザは、このグループポリシーよりも優先できます。[すべてのバケットを管理]権限を信頼できるユーザに制限し、可能な場合は多要素認証（MFA）を使用します。

- * カスタム * ：グループ内のユーザーには、テキストボックスで指定した権限が付与されます。

例：グループにすべてのバケットへのフルアクセスを許可する

この例では、バケットポリシーで明示的に拒否されている場合を除き、グループのすべてのメンバーにテナントアカウントが所有するすべてのバケットへのフルアクセスが許可されます。

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

例：グループにすべてのバケットへの読み取り専用アクセスを許可する

この例では、バケットポリシーで明示的に拒否されている場合を除き、グループのすべてのメンバーに S3 リソースへの読み取り専用アクセスが許可されます。たとえば、オブジェクトをリストして、オブジェクトデータ、メタデータ、タグを読み取ることができます。

```
{
  "Statement": [
    {
      "Sid": "AllowGroupReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

例：グループメンバーにバケット内の「フォルダ」へのフルアクセスのみを許可する

この例では、指定したバケット内の特定のフォルダ（キープレフィックス）のリストおよびアクセスのみがグループのメンバーに許可されます。これらのフォルダのプライバシー設定を決めるときは、他のグループポリシーやバケットポリシーのアクセス権限を考慮する必要があります。

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

StorageGRID監査ログで追跡されるS3操作

監査メッセージは StorageGRID サービスによって生成され、テキスト形式のログファイルに保存されます。監査ログのS3固有の監査メッセージを確認して、バケットとオブジェクトの処理に関する詳細を確認できます。

監査ログで追跡されるバケットの処理

- CreateBucket
- DeleteBucket
- DeleteBucketPolicy
- DeleteBucketTagging
- オブジェクトの削除
- GetBucketLifecycleConfiguration
- GetBucketPolicy
- GetBucketTagging
- ヘッドバケット
- ListObjects
- ListObjectVersions
- PUT Bucket compliance で確認してください

- PutBucketLifecycleConfiguration
- PutBucketPolicy
- PutBucketTaggingの略
- PutBucketVersioning

監査ログで追跡されるオブジェクトの処理

- CompleteMultipartUpload
- CopyObject
- deleteObject
- GetObject
- ヘッドオブジェクト
- PutObject
- RestoreObject
- SelectObject
- UploadPart（ILMルールの取り込みがBalancedまたはStrictの場合）
- UploadPartCopy（ILMルールの取り込みがBalancedまたはStrictの場合）

関連情報

- "監査ログファイルにアクセスします"
- "クライアント書き込み監査メッセージ"
- "クライアント読み取り監査メッセージ"

Swift REST APIの使用（サポート終了）

StorageGRID での Swift REST API サポート

Swift APIのサポートはすでに終了しており、今後のリリースで削除される予定です。



このバージョンのドキュメントサイトからSwiftの詳細が削除されました。を参照してください "StorageGRID 11.8：Swift REST APIの使用"

StorageGRIDシステムの監視とトラブルシューティング

StorageGRID システムを監視します

AutoSupport を使用します

StorageGRIDのAutoSupportについて学ぶ

AutoSupport機能を使用すると、StorageGRIDからNetAppテクニカルサポートに健全性パッケージとステータスパッケージを送信できます。

AutoSupportを使用すると、問題をより早く解決できます。テクニカル サポートでは、システムのストレージのニーズを監視し、新しいノードまたはサイトを追加する必要があるかどうかを判断するのに役立ちます。オプションで、 AutoSupport はパッケージを 1 つの追加の送信先に送信できます。

StorageGRIDには、次の2種類のAutoSupportがあります。

- * StorageGRID AutoSupport *はStorageGRIDソフトウェアの問題を報告します。StorageGRIDの初回インストール時にデフォルトで有効になっています。必要に応じてできます"デフォルトのAutoSupport設定の変更"。

> StorageGRID AutoSupportが有効になっていない場合、Grid Manager ダッシュボードにメッセージが表示されます。メッセージには、 AutoSupport構成ページへのリンクが含まれています。メッセージを閉じると、 AutoSupport が無効のままであっても、ブラウザのキャッシュがクリアされるまでメッセージは再び表示されません。

- *アプライアンス・ハードウェアAutoSupport *はStorageGRIDアプライアンスの問題を報告します。そうしなければならない"各アプライアンスでのハードウェアAutoSupportの設定"

Digital Advisorとは何ですか？

Active IQ Digital Advisor（Digital Advisor とも呼ばれます）はクラウドベースであり、NetAppのインストールベースから予測分析とコミュニティの知見を活用します。継続的なリスク評価、予測アラート、処方的ガイダンス、および自動化されたアクションにより、問題が発生する前に防止し、システムの健全性の向上とシステム可用性の向上を実現します。

NetApp Support SiteでDigital Advisorのダッシュボードと機能を使用するには、AutoSupportを有効にする必要があります。

"Digital Advisorドキュメント"

AutoSupportパッケージに含まれる情報

AutoSupportパッケージには、次のファイルと詳細が含まれています。

ファイル名	フィールド	製品説明
autosupport-history.xml	AutoSupportシーケンス番号+このAutoSupportのデスティネーション+配信ステータス+配信試行+ AutoSupport件名+配信URI 最終エラーAutoSupport PUTファイル名+生成時刻+ AutoSupport圧縮サイズ+ AutoSupport解凍後のサイズ+総収集時間（ミリ秒）	AutoSupport履歴ファイル。
AutoSupport .xml	ノード+サポートに連絡するプロトコル+ HTTP / HTTPSのサポートURL サポートアドレス AutoSupport OnDemand状態+ AutoSupport OnDemandサーバURL + AutoSupport OnDemandポーリング間隔	AutoSupportステータスファイル。使用するプロトコル、テクニカルサポートのURLとアドレス、ポーリング間隔、OnDemand AutoSupport（有効または無効）の詳細が表示されます。
buckets.xml	バケットID アカウントID +ビルドバージョン+ロケーションの制約設定+準拠設定 S3オブジェクトロック有効+ S3オブジェクトロック設定+整合性設定+ CORS設定+最終アクセス時間有効+ポリシー設定+通知有効+通知設定+通知設定+ Cloud Mirror設定+検索有効+バケットタグ付け設定+バケットタグ付け設定	設定の詳細と統計がバケットレベルで表示されます。バケット設定の例には、プラットフォームサービス、準拠、バケット整合性などがあります。
grid-configurations.xml	属性ID +属性名+値+インデックス+テーブルID +テーブル名	グリッド全体の設定情報ファイル。グリッド証明書、メタデータリザーブスペース、グリッド全体の設定（準拠、S3オブジェクトロック、オブジェクト圧縮、アラート、syslog、ILMの設定）、イレイジャーコーディングプロファイルの詳細、DNS名、およびに関する情報が格納されます"NMS名"。
GRID-SPEC.xml	グリッド仕様、raw XML	StorageGRIDの設定と導入に使用します。ノードのグリッド仕様、NTPサーバIP、DNSサーバIP、ネットワークトポロジ、およびハードウェアプロファイルが含まれます。
grid-tasks.xml	ノード+サービスパス+属性ID +属性名+値+インデックス+テーブルID +テーブル名	グリッドタスク（メンテナンス手順）のステータスファイル。グリッドのアクティブなタスク、終了したタスク、完了したタスク、失敗したタスク、および保留中のタスクの詳細が表示されます。

ファイル名	フィールド	製品説明
grid.json	Grid リビジョン+ソフトウェアバージョン+説明+ライセンス+パスワード DNS + NTP + サイト+ノード	グリッド情報。
ilm-configuration.xml	属性ID +属性名+値+インデックス+テーブルID +テーブル名	ILM設定の属性のリスト。
ilm-status.xml	ノード+サービスパス+属性ID +属性名+値+インデックス+テーブルID +テーブル名	ILM指標情報ファイル。各ノードのILM評価速度とグリッド全体の指標が格納されます。
ilm.xml	ILM raw XML	ILMのアクティブポリシーファイル。ストレージプールID、取り込み動作、フィルタ、ルール、概要など、アクティブなILMポリシーの詳細が格納されます。
LOG.TGZ	*n/a*	ダウンロード可能なログファイル。各ノードのと `servermanager.log`を含みます `bycast-err.log`。
manifest.xml	収集順序+このデータのAutoSupportコンテンツファイル名+このデータ項目の説明+収集されたバイト数+収集に費やされた時間+このデータ項目のステータス+エラーの説明+このデータのAutoSupportコンテンツタイプ+	すべてのAutoSupportファイルのAutoSupportメタデータと簡単な説明が含まれています。
nms-entities.xml	属性インデックス+エンティティOID +ノードID +デバイスモデルID +デバイスモデルバージョン+エンティティ名	のグループエンティティとサービスエンティティ"NMSツリー"。グリッドトポロジの詳細が表示されます。ノードは、ノードで実行されているサービスに基づいて特定できます。
objects-status.xml	ノード+サービスパス+属性ID +属性名+値+インデックス+テーブルID +テーブル名	オブジェクトのステータス（バックグラウンドスキャンステータス、アクティブな転送、転送速度、合計転送回数、削除速度、破損したフラグメント、損失オブジェクト、欠落オブジェクト、修復試行回数、スキャン速度、推定スキャン期間、修復完了ステータスなど）。

ファイル名	フィールド	製品説明
server-status.xml	ノード+サービスパス+属性ID +属性名+値+インデックス+テーブルID +テーブル名	サーバ構成各ノードの詳細情報が含まれます。プラットフォームタイプ、オペレーティングシステム、取り付けられているメモリ、使用可能なメモリ、ストレージ接続、ストレージアプライアンスのシャーシのシリアル番号、ストレージコントローラの障害ドライブ数、コンピューティングコントローラシャーシの温度、コンピューティングハードウェア、コンピューティングコントローラのシリアル番号、電源装置、ドライブサイズ、ドライブタイプ。
service-status.xml	ノード+サービスパス+属性ID +属性名+値+インデックス+テーブルID +テーブル名	サービスノード情報ファイル。割り当てられたテーブル領域、空きテーブル領域、データベースのリーパーメトリック、セグメント修復期間、修復ジョブ期間、自動ジョブ再開、自動ジョブ終了などの詳細が含まれます。
storage-grades.xml	ストレージグレードID +ストレージグレード名+ストレージノードID +ストレージノードパス	ストレージノードごとのストレージグレード定義ファイル。
概要- attributes.xml	グループOID +グループパス+サマリー属性ID +サマリー属性名+値+インデックス+テーブルID +テーブル名	StorageGRIDの使用状況情報を要約するシステムステータスデータの概要。グリッドの名前、サイトの名前、グリッドあたりおよびサイトあたりのストレージノード数、ライセンスタイプ、ライセンスの容量と使用状況、ソフトウェアのサポート条件、S3処理の詳細などの詳細が表示されます。
system-alerts.xml	名前+重大度+ノード名+アラートステータス+サイト名+アラートトリガー日時+アラート解決時間+ルールID +ノードID +サイトID +サイレント化+その他のアノテーション+その他のラベル	StorageGRIDシステムの潜在的な問題を示す現在のシステムアラート。

ファイル名	フィールド	製品説明
USERAGENTS.xml	ユーザエージェント+日数+ HTTP要求の合計バイト数+取得した合計バイト数+ PUT要求+ GET要求+ DELETE要求+ POST要求+ POST要求+オプション要求+平均要求時間（ミリ秒）+平均GET要求時間（ミリ秒）+平均削除要求時間（ミリ秒）+平均HEAD要求時間（ミリ秒）+平均POST要求時間（ミリ秒）+平均オプション要求時間（ミリ秒）	アプリケーションユーザエージェントに基づく統計。たとえば、ユーザエージェントあたりのPUT / GET / DELETE / HEAD処理の数や、各処理の合計バイトサイズなどです。
Xヘッダーデータ	X - NetApp - asup-generated-on + X - NetApp - asup-hostname + X - NetApp - asup-os-version + X - NetApp - asup-serial-num + X - NetApp - asup-subject + X - NetApp - asup-system-id + X - NetApp - asup-model-name +	AutoSupportヘッダーデータ。

StorageGRIDで**AutoSupport**を設定する

AutoSupport 機能を使用すると、StorageGRID システムは定期的およびイベント駆動型の健全性とステータスメッセージをテクニカルサポートに送信し、プロアクティブな監視とトラブルシューティングを可能にします。StorageGRID AutoSupport では、予測に基づく推奨機能のために Digital Advisor を使用することもできます。

デフォルトでは、ソフトウェアベースの StorageGRID システムに StorageGRID を初めてインストールする際に、週次およびイベントトリガーの AutoSupport 機能が有効になっています。ただし、各アプライアンスでハードウェアAutoSupportの設定必要があります。必要に応じて、AutoSupport の設定を変更できます。

StorageGRID AutoSupport の設定を変更する場合は、プライマリ管理ノードでのみ変更を行ってください。

開始する前に

- プライマリ管理ノードのGrid Managerに"サポートされている Web ブラウザ"を使用してサインインしています。
- あなたはを持っています"rootアクセス権限"。
- HTTPSを使用してAutoSupportパッケージを送信する場合は、直接または"プロキシサーバを使用する"のいずれかの方法で、プライマリ Admin ノードへのアウトバウンドインターネットアクセスを提供しています（インバウンド接続は不要です）。
- StorageGRID の AutoSupport ページで HTTP を選択した場合、AutoSupport パッケージを HTTPS として転送するには "プロキシサーバを設定しました" が必要です。NetApp の AutoSupport サーバは、HTTP を使用して送信されたパッケージを拒否します。

- SMTPをAutoSupportパッケージのプロトコルとして使用する場合は、"メールサーバーを設定しました"。

タスクの内容

次のオプションを任意に組み合わせて、AutoSupportパッケージをテクニカルサポートに送信できます。

- 毎週：AutoSupportパッケージを週に1回自動的に送信します。デフォルト設定： Enabled （有効）。
- * Event-triggered *：1時間ごと、または重大なシステムイベントが発生したときに、AutoSupportパッケージを自動的に送信します。デフォルト設定： Enabled （有効）。
- オンデマンド：テクニカルサポートがStorageGRIDシステムにAutoSupportパッケージを自動的に送信するよう要求できるようにします。これは、問題をアクティブに使用している場合（HTTPS AutoSupport転送プロトコルが必要）に役立ちます。デフォルト設定： Disabled （無効）。
- **User-triggered**: AutoSupportパッケージをいつでも手動で送信します。
- ログ収集:"ログファイルとシステムデータを手動で収集し、 AutoSupportパッケージを送信します" 。

AutoSupport の設定AutoSupport

AutoSupport のインストールのデフォルト設定を変更するか、各 StorageGRID アプライアンスでハードウェア AutoSupport を設定するには：

手順

1. サポート > ツール > * AutoSupport* > 設定 を選択します。
2. AutoSupportパッケージの送信に使用するプロトコルを選択します。
   - * HTTPS * ：これはデフォルトで、新規インストールに推奨される設定です。このプロトコルはポート443を使用します。必要に応じてAutoSupport オンデマンド機能を有効にします、HTTPSを使用する必要があります。
   - **HTTP**：HTTPを選択する場合は、AutoSupportパッケージをHTTPSとして転送するために"プロキシサーバを設定する"する必要があります。NetAppのAutoSupportサーバは、HTTPを使用して送信されたパッケージを拒否します。このプロトコルはポート80を使用します。
   - **SMTP**: このオプションは、AutoSupport パッケージをメールで送信する場合に使用します。まず最初に "メールサーバーの設定" 必要があります。

   設定したプロトコルは、HTTPSプロトコルが必要な AutoSupport on Demand を除くすべての AutoSupport パッケージの送信に使用されます。
3. [HTTPS]*を選択した場合は、テクニカルサポートサーバへの接続を保護するためにNetAppサポート証明書（TLS証明書）を使用するかどうかを選択します。
   - 証明書の確認（デフォルト）：AutoSupportパッケージの送信が安全であることを確認します。ネットアップサポート証明書は、 StorageGRID ソフトウェアとともにすでにインストールされています。
   - * 証明書を検証しない * ：このオプションは、証明書に一時的な問題があるなど、証明書の検証を使用しない理由が十分な場合にのみ選択してください。
4. **SMTP** を選択した場合は、送信者 フィールドに、以前設定したメールサーバーのアドレスを入力してください。
5. [保存（ Save ）] を選択します。週次パッケージ、ユーザトリガーパッケージ、およびイベントトリガーパッケージはすべて、選択したプロトコルを使用して送信されます。

週次**AutoSupport**を無効にする

デフォルトでは、StorageGRIDシステムは週に1回テクニカルサポートにAutoSupportパッケージを送信するように設定されています。

週次AutoSupportパッケージが送信されるタイミングを確認するには、* AutoSupport **>** Results タブに移動します。**[**毎週のスケジュール（**Weekly AutoSupport**）**]**セクションで、[次のスケジュール時間（Next Scheduled Time）]*の値を確認します。

週次AutoSupportパッケージの自動送信はいつでも無効にすることができます。

手順

1. サポート > ツール > * AutoSupport* > 設定 を選択します。
2. [毎週のAutoSupport を有効にする]*チェックボックスをオフにします。
3. [保存（ Save ）] を選択します。

イベントトリガー型**AutoSupport**の無効化

デフォルトでは、StorageGRIDシステムはAutoSupportパッケージを1時間ごとにテクニカルサポートに送信するように設定されています。

イベントトリガー型AutoSupportはいつでも無効にすることができます。

手順

1. サポート > ツール > * AutoSupport* > 設定 を選択します。
2. [Enable Event-Triggered AutoSupport *]チェックボックスをオフにします。
3. [保存（ Save ）] を選択します。

AutoSupport On Demand を有効にする

AutoSupport On Demand は、テクニカルサポートが問題解決に積極的に取り組んでいる場合に役立ちます。

デフォルトでは、 AutoSupport On Demand は無効になっています。この機能を有効にすると、テクニカルサポートがStorageGRIDシステムからAutoSupportパッケージを自動的に送信するように要求できます。テクニカルサポートは、 AutoSupport On Demand クエリのポーリング間隔も設定できます。

テクニカルサポートは、AutoSupport On Demandを有効または無効にできません。

手順

1. サポート > ツール > * AutoSupport* > 設定 を選択します。
2. プロトコルの * HTTPS * を選択します。
3. [毎週のAutoSupport を有効にする]*チェックボックスをオンにします。
4. [Enable AutoSupport on Demand]*チェックボックスをオンにします。
5. [保存（ Save ）] を選択します。

   AutoSupport On Demand は有効になっており、テクニカルサポートは AutoSupport On Demand 要求を StorageGRID に送信できます。

ソフトウェアアップデートのチェックを無効にします

デフォルトでは、 StorageGRID はネットアップに連絡して、ご使用のシステムでソフトウェアの更新が利用可能かどうかを判断します。StorageGRID ホットフィックスまたは新しいバージョンが利用可能な場合は、StorageGRID のアップグレードページに新しいバージョンが表示されます。

必要に応じて、ソフトウェアアップデートのチェックを無効にすることもできます。たとえば、 WAN でアクセスできないシステムの場合は、ダウンロードエラーを回避するためにチェックを無効にする必要があります。

手順

1. サポート > ツール > * AutoSupport* > 設定 を選択します。
2. [Check for software updates]*チェックボックスをオフにします。
3. [保存（ Save ）] を選択します。

AutoSupport デスティネーションを追加します

AutoSupportを有効にすると、ヘルスパッケージとステータスパッケージがテクニカルサポートに送信されます。すべてのAutoSupportパッケージに対して、追加の送信先を1つ指定できます。

AutoSupportパッケージの送信に使用されるプロトコルを確認または変更するには、AutoSupportを設定するの手順を参照してください。

> SMTPプロトコルを使用してAutoSupportパッケージを追加の送信先に送信することはできません。

手順

1. サポート > ツール > * AutoSupport* > 設定 を選択します。
2. [Enable Additional AutoSupport Destination]*を選択します。
3. 次の情報を指定します。

ホスト名
: 追加のAutoSupport 宛先サーバのサーバホスト名またはIPアドレス。

  > 追加の送信先は 1 つだけ入力できます。

ポート
: 追加のAutoSupport 宛先サーバへの接続に使用するポート。デフォルトは、HTTPの場合はポート80、HTTPSの場合はポート443です。

証明書の検証
: TLS証明書を使用して追加の送信先への接続を保護するかどうか。

  - 証明書の検証を使用するには、*証明書の検証*を選択します。
  - 証明書の検証なしでAutoSupportパッケージを送信する場合は、[証明書を検証しない]*を選択します。

    このオプションは、証明書の検証を使用しない理由がある場合（証明書に一時的な問題がある場合

など）にのみ選択してください。

4. [Verify certificate]*を選択した場合は、次の手順を実行します。
   a. CA証明書の場所を参照します。
   b. CA証明書ファイルをアップロードします。

      CA証明書のメタデータが表示されます。

5. [保存（ Save ）] を選択します。

   今後、毎週、イベントトリガー型、およびユーザトリガー型のすべてのAutoSupportパッケージが追加の送信先に送信されます。

[[autosupport-for-appliances]]アプライアンスの**AutoSupport**の設定

アプライアンスのAutoSupportではStorageGRIDハードウェアの問題が報告され、StorageGRID AutoSupportではStorageGRIDソフトウェアの問題が報告されます。ただし、SGF6112の場合、StorageGRID AutoSupportではハードウェアとソフトウェアの両方の問題が報告されます。SGF6112を除く各アプライアンスでAutoSupportを設定する必要があります。SGF6112は追加の設定は必要ありません。AutoSupportの実装方法は、サービスアプライアンスとストレージアプライアンスで異なります。

SANtricityを使用して、各ストレージアプライアンスのAutoSupportを有効にします。SANtricity AutoSupportは、アプライアンスの初期セットアップ時またはアプライアンスの設置後に設定できます。

- SG6000およびSG5700アプライアンスの場合は、 "SANtricity システムマネージャでAutoSupport を設定します"

"SANtricityシステムマネージャ"でプロキシ経由のAutoSupport配信を設定すると、Eシリーズ アプライアンスからのAutoSupportパッケージをStorageGRID AutoSupportに含めることができます。

StorageGRID AutoSupport では、DIMMやホストインターフェイスカード（HIC）などのハードウェアの問題は報告されません。ただし、一部のコンポーネント障害がトリガーされる可能性があり"ハードウェアアラート"ます。ベースボード管理コントローラ（BMC）を搭載したStorageGRIDアプライアンスでは、ハードウェア障害を報告するようにEメールおよびSNMPトラップを設定できます。

- "BMCアラートのEメール通知を設定する"
- "BMCのSNMP設定を行います"

関連情報

- "外部との通信に使用するポート"
- "NetAppサポート"

StorageGRIDで**AutoSupport**パッケージを手動でトリガーする

テクニカルサポートによるStorageGRIDシステムの問題のトラブルシューティングを支援するために、送信するAutoSupportパッケージを手動でトリガーできます。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。

- ルート アクセスまたはその他のグリッド構成権限があります。

手順

1. サポート > ツール > * AutoSupport* を選択します。
2. [アクション]タブで、*[ユーザートリガー型AutoSupportの送信]*を選択します。

   StorageGRID は、 AutoSupportパッケージをNetAppサポート サイトに送信しようとします。試行が成功すると、[結果] タブの [最新の結果] と [前回の成功時刻] の値が更新されます。問題がある場合は、「最新の結果」の値が「失敗」に更新され、 StorageGRID はAutoSupportパッケージの再送信を試行しません。

3. 1 分後にブラウザでAutoSupportページを更新し、最新の結果にアクセスしてください。



さらに、"より広範なログファイルとシステムデータを収集する" NetAppサポート サイトに送信してください。

StorageGRID が **AutoSupport** パッケージの障害を処理する方法

AutoSupportパッケージの送信試行が失敗した場合にStorageGRIDが実行するアクションのリストを確認します。

StorageGRID は、AutoSupport パッケージの種類に応じて異なる処理を実行します。AutoSupport パッケージのステータスを確認するには、サポート > ツール > **AutoSupport** > 結果 を選択します。

AutoSupportパッケージの送信に失敗すると、* AutoSupport ページの Results *タブに「Failed」と表示されます。



プロキシ サーバを設定して AutoSupport パッケージを NetApp に転送するように構成した場合は、"プロキシサーバの設定が正しいことを確認します。"。

週次**AutoSupport**パッケージエラー

週次AutoSupportパッケージの送信に失敗した場合、StorageGRIDシステムは次の処理を実行します。

1. 最新の結果属性を更新して再試行します。
2. AutoSupportパッケージの再送信を4分ごとに15回、1時間試行します。
3. 送信エラーが 1 時間発生した後、最新の結果属性を失敗に更新します。
4. 次回のスケジュールされた時刻に、AutoSupportパッケージの送信を再試行します。
5. NMSサービスが使用できないためにパッケージが失敗した場合や、7日前にパッケージが送信された場合は、AutoSupportの通常のスケジュールを維持します。
6. 7日以上パッケージが送信されていない場合、NMSサービスが再び使用可能になると、はAutoSupportパッケージをすぐに送信します。

ユーザトリガー型またはイベントトリガー型の**AutoSupport**パッケージエラー

ユーザトリガー型またはイベントトリガー型のAutoSupportパッケージの送信に失敗した場合、StorageGRIDシステムは次の処理を実行します。

1. 既知のエラーの場合は、エラーメッセージが表示されます。たとえば、ユーザが正しいEメール設定を指

定せずにSMTPプロトコルを選択すると、次のエラーが表示されます。 `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

2. パッケージの再送信は試行されません。
3. にエラーを記録し `nms.log`ます。

障害が発生し、SMTPが選択されているプロトコルである場合、AutoSupportページに次のエラーメッセージが表示される場合があります： `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

方法をご確認ください"Eメールサーバを設定します"。

AutoSupportパッケージの障害を修正する

障害が発生し、SMTPが選択されているプロトコルである場合は、StorageGRIDシステムのメールサーバーが正しく設定されており、メールサーバーが稼働していることを確認してください。次のエラーメッセージがAutoSupportページに表示される場合があります：AutoSupportパッケージは、メールサーバーページの設定が正しくないため、SMTPプロトコルを使用して送信できません。

StorageGRID経由でEシリーズAutoSupportパッケージを送信

EシリーズSANtricity System Manager AutoSupportパッケージは、ストレージアプライアンスの管理ポートではなく、StorageGRID管理ノード経由でテクニカルサポートに送信できます。

EシリーズアプライアンスでのAutoSupportの使用の詳細については、を参照してください "EシリーズハードウェアAutoSupport"。

開始する前に

- を使用してGrid Managerにサインインしておき"サポートされている Web ブラウザ"ます。
- あなたは"ストレージアプライアンス管理者またはRoot Access権限"があります。
- SANtricity AutoSupport が設定されました。
  - SG6000およびSG5700アプライアンスの場合は、 "SANtricity システムマネージャでAutoSupport を設定します"

> Grid Manager を使用して SANtricity System Manager にアクセスするには、 SANtricity ファームウェア 8.70 以降が必要です。

タスクの内容

EシリーズAutoSupportパッケージには、ストレージハードウェアの詳細が含まれており、StorageGRIDシステムから送信される他のAutoSupportパッケージよりも具体的です。

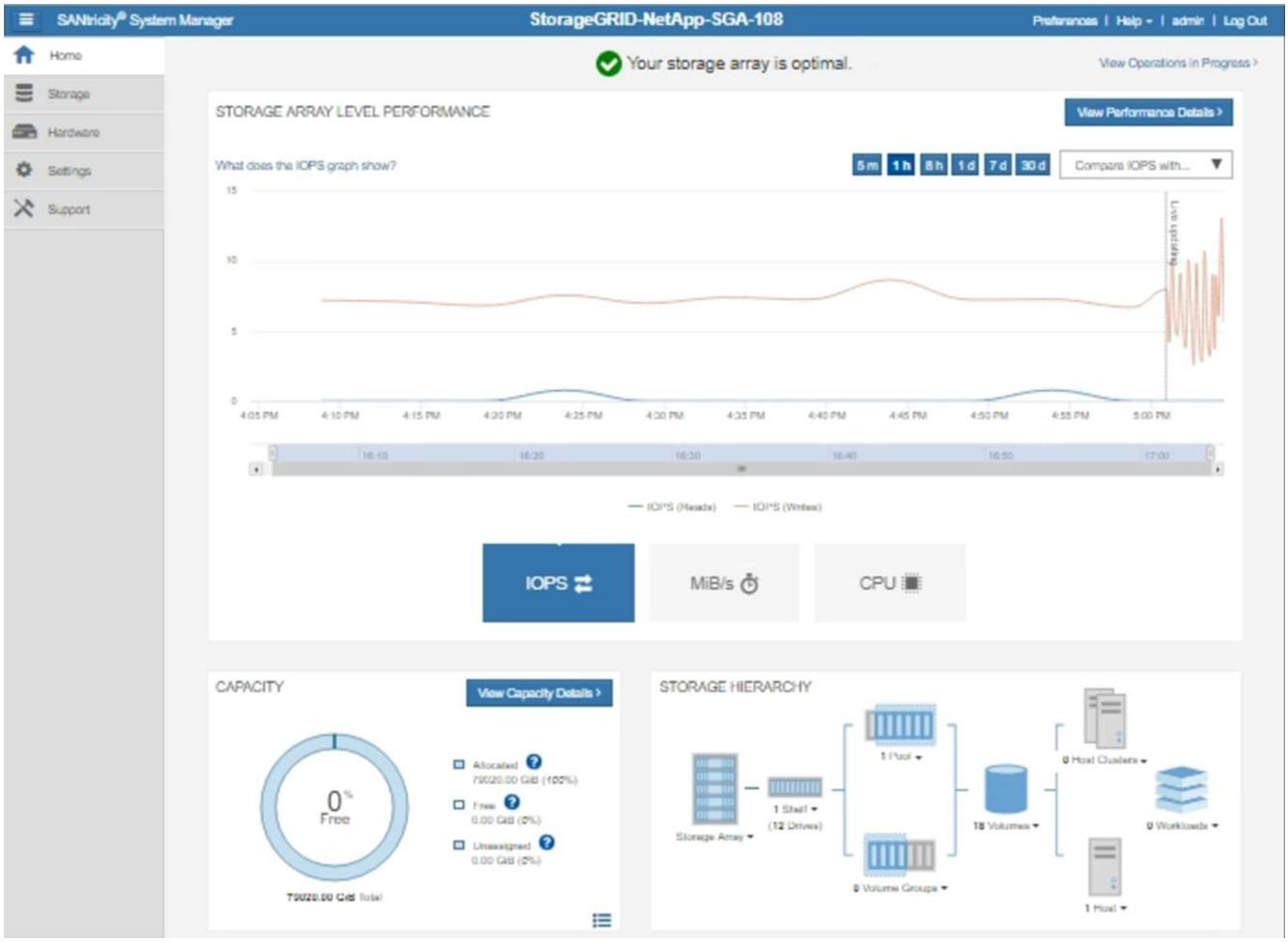
SANtricity System Managerでは、アプライアンスの管理ポートを使用せずにStorageGRID管理ノード経由でAutoSupportパッケージを送信するように特別なプロキシサーバアドレスを設定できます。この方法で送信されるAutoSupportパッケージはから送信され"優先送信者管理ノード"、グリッドマネージャで設定された任意のパッケージを使用し"管理プロキシの設定"ます。

この手順は、EシリーズAutoSupportパッケージ用にStorageGRIDプロキシサーバを設定するためだけに使用します。EシリーズのAutoSupport構成の詳細については、を参照してください "NetApp E シリーズおよび SANtricity に関するドキュメント"。

手順

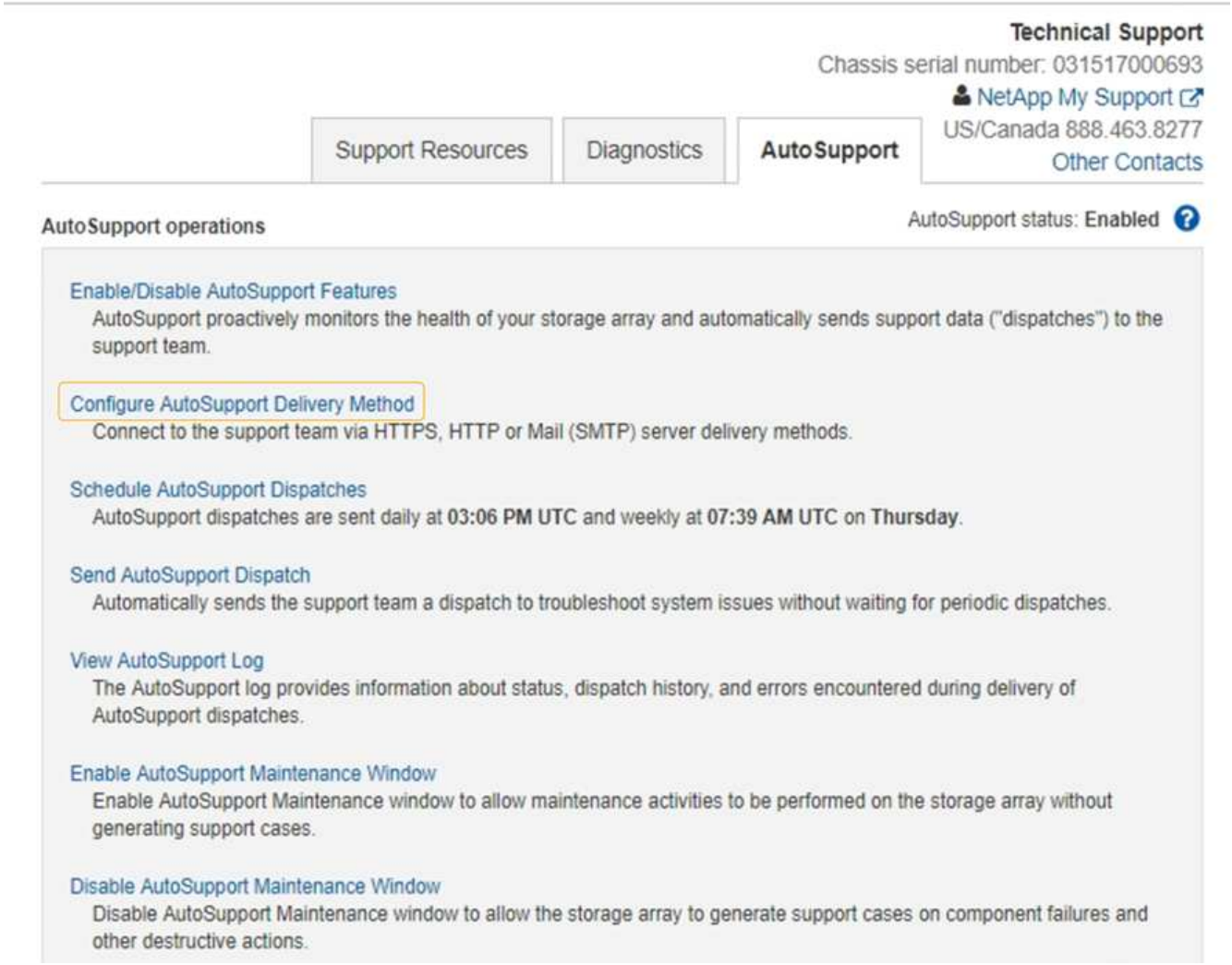
1. グリッド マネージャーで、[ノード] を選択します。
2. 左側のノードのリストから、設定するストレージアプライアンスノードを選択します。
3. SANtricity System Manager* を選択します。

   SANtricity の System Manager ホームページが表示されます。



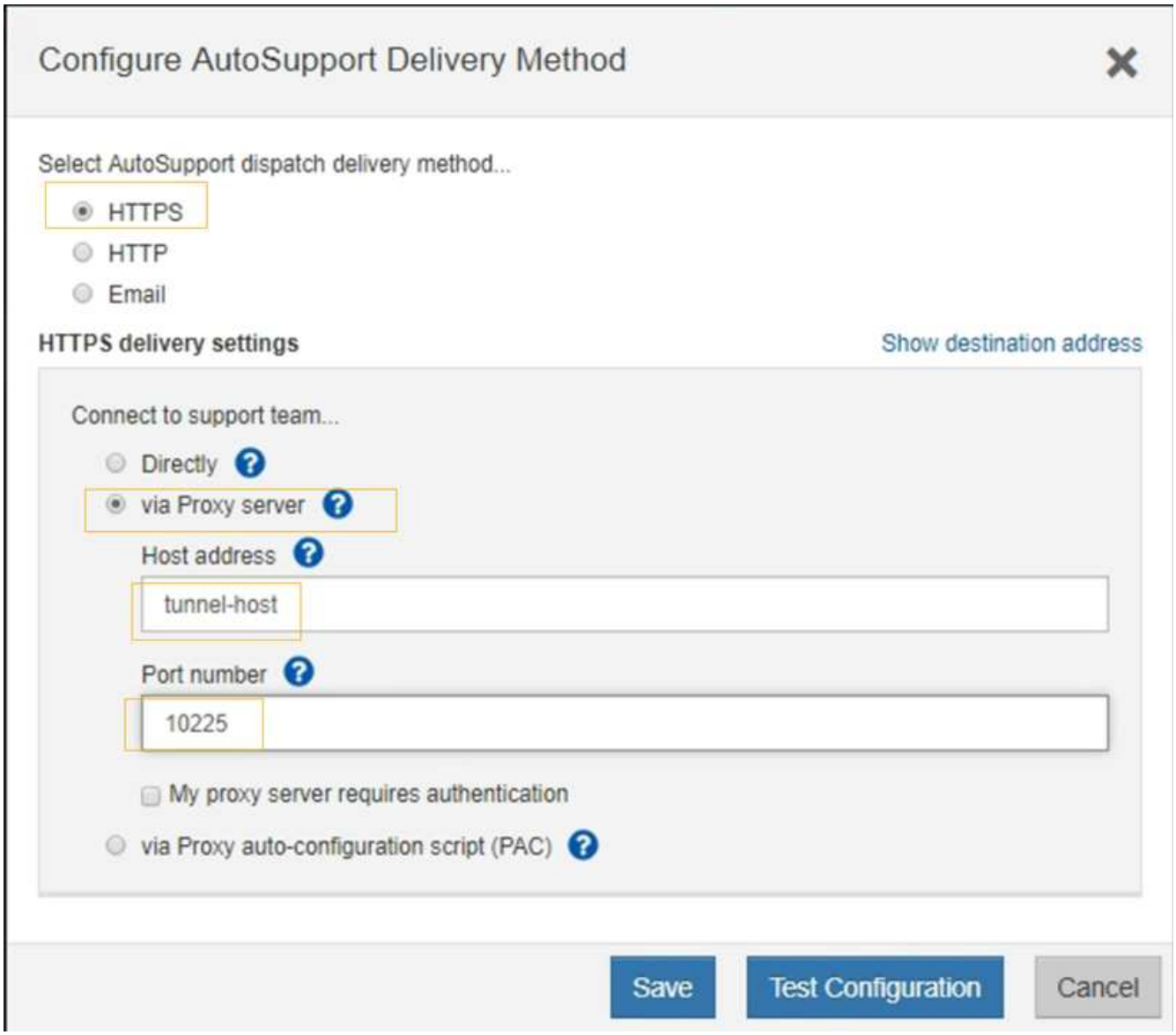
4. サポート > サポート センター > * AutoSupport* を選択します。

   AutoSupport operations ページが表示されます。



5. AutoSupport 配信方法の設定 * を選択します。

   AutoSupport 配信方法の設定ページが表示されます。



6. 配信方法として「 * HTTPS * 」を選択します。

   HTTPSを有効にする証明書が事前にインストールされています。

7. プロキシサーバー経由 * を選択します。
8. [Host address]にと入力します `tunnel-host`。

   `tunnel-host`は、管理ノードを使用してEシリーズAutoSupportパッケージを送信するための特別なアドレスです。

9. [Port Number]にと入力します `10225`。

   `10225`は、アプライアンスのEシリーズコントローラからAutoSupportパッケージを受け取るStorageGRIDプロキシサーバ上のポート番号です。

10. AutoSupport プロキシサーバーのルーティングと設定をテストするには、 * テスト構成 * を選択します。

    正しい場合は、緑色のバナーに「Your AutoSupport configuration has been verified」というメッセージが

表示されます。

テストに失敗した場合は、赤いバナーが表示されます。StorageGRID DNSの設定とネットワークを確認し、がNetAppサポートサイトに接続できることを確認してから、"優先送信者管理ノード"もう一度テストを実行してください。

11. [保存（ Save ）] を選択します。

設定が保存され、「AutoSupport配信方法が設定されました」という確認メッセージが表示されます。

StorageGRID システムを監視する

StorageGRIDシステムを定期的に監視して、想定どおりに動作していることを確認してください。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- そうだな "特定のアクセス権限"

> Grid Managerに表示されるストレージ値の単位を変更するには、Grid Managerの右上にあるユーザドロップダウンを選択し、*[ユーザ設定]*を選択します。

タスクの内容

ここでは、次の手順について説明します。

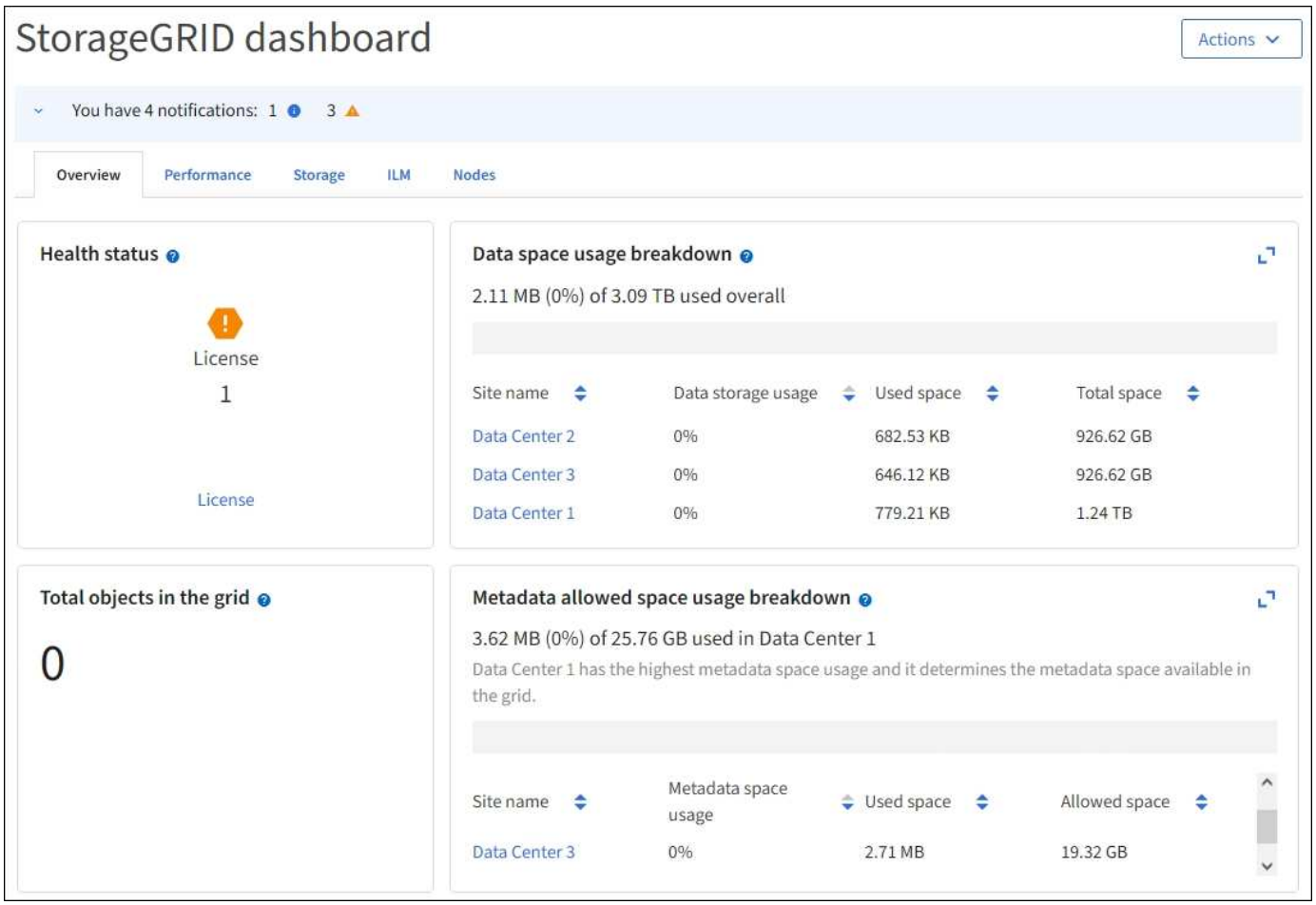
- "ダッシュボードを表示および管理します"
- "Nodes ページを表示します"
- "システムの次の側面を定期的に監視します。"
  - "システムヘルス"
  - "ストレージ容量"
  - "情報ライフサイクル管理"
  - "ネットワークおよびシステムリソース"
  - "テナントのアクティビティ"
  - "ロードバランシング操作"
  - "グリッドフェデレーション接続"
- "アラートの管理"
- "ログファイルの表示"
- "ログ管理と外部Syslogサーバーを構成する"
- "外部 syslog サーバを使用します"監査情報を収集するには
- "SNMPを使用した監視"
- "I/Oの優先順位を変更する"I/O操作の相対的な優先順位を変更する

StorageGRIDでダッシュボードを表示および管理する

ダッシュボードを使用すると、システムのアクティビティを一目で監視できます。StorageGRID の実装を監視するためのカスタムダッシュボードを作成できます。

Grid Managerに表示されるストレージ値の単位を変更するには、Grid Managerの右上にあるユーザドロップダウンを選択し、*[ユーザ設定]*を選択します。

ダッシュボードはシステム構成によって異なる場合があります。



ダッシュボードを表示します

ダッシュボードは、StorageGRID システムに関する特定の情報を表示するタブで構成されています。各タブには、カードに表示される情報のカテゴリが含まれています。

システム提供のダッシュボードはそのまま使用できます。また、StorageGRID の実装の監視に関連するタブとカードのみを含むカスタムダッシュボードを作成することもできます。

システム提供のダッシュボードタブには、次の種類の情報が記載されたカードが含まれています。

タブをクリックします	次を含む
概要	アクティブなアラート、スペース使用量、グリッド内のオブジェクトの合計など、グリッドに関する一般的な情報。
パフォーマンス	スペース使用量、一定期間のストレージ使用量、S3処理、要求期間、エラー率
ストレージ	テナントクォータ使用量および論理スペース使用量。ユーザデータとメタデータのスペース使用量を予測します。
ILM	情報ライフサイクル管理のキューと評価レート
ノード	ノード別のCPU、データ、メモリの使用率。ノード別のS3処理。ノードからサイトへの分散：

一部のカードは、見やすくするために最大化できます。カードの右上隅にある最大化アイコンを選択します。最大化されたカードを閉じるには、最小化アイコンを選択するか、**Close** を選択してください。

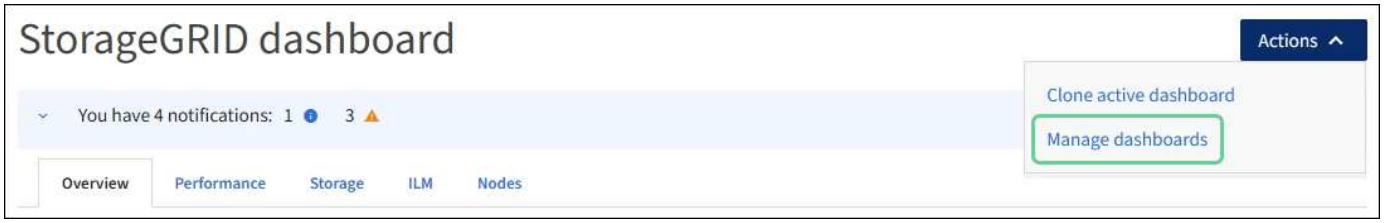
ダッシュボードを管理します

ルートアクセス（を参照"管理者グループの権限"）がある場合は、ダッシュボードに対して次の管理タスクを実行できます。

- カスタムダッシュボードを最初から作成します。カスタムダッシュボードを使用して、表示するStorageGRID 情報とその構成を制御できます。
- ダッシュボードをクローニングしてカスタムダッシュボードを作成する。
- ユーザーのアクティブなダッシュボードを設定します。アクティブなダッシュボードには、システムが提供するダッシュボードとカスタムダッシュボードがあります。
- デフォルトのダッシュボードを設定します。これは、ユーザーが独自のダッシュボードをアクティブ化しない限り、すべてのユーザーに表示されます。
- ダッシュボード名を編集します。
- ダッシュボードを編集して、タブやカードを追加または削除します。タブは1個以上20個以下にすることができます。
- ダッシュボードを削除します。

Root Access以外の権限がある場合は、アクティブなダッシュボードのみを設定できます。

ダッシュボードを管理するには、**[アクション]**>*[ダッシュボードの管理]*を選択します。



ダッシュボードを設定する

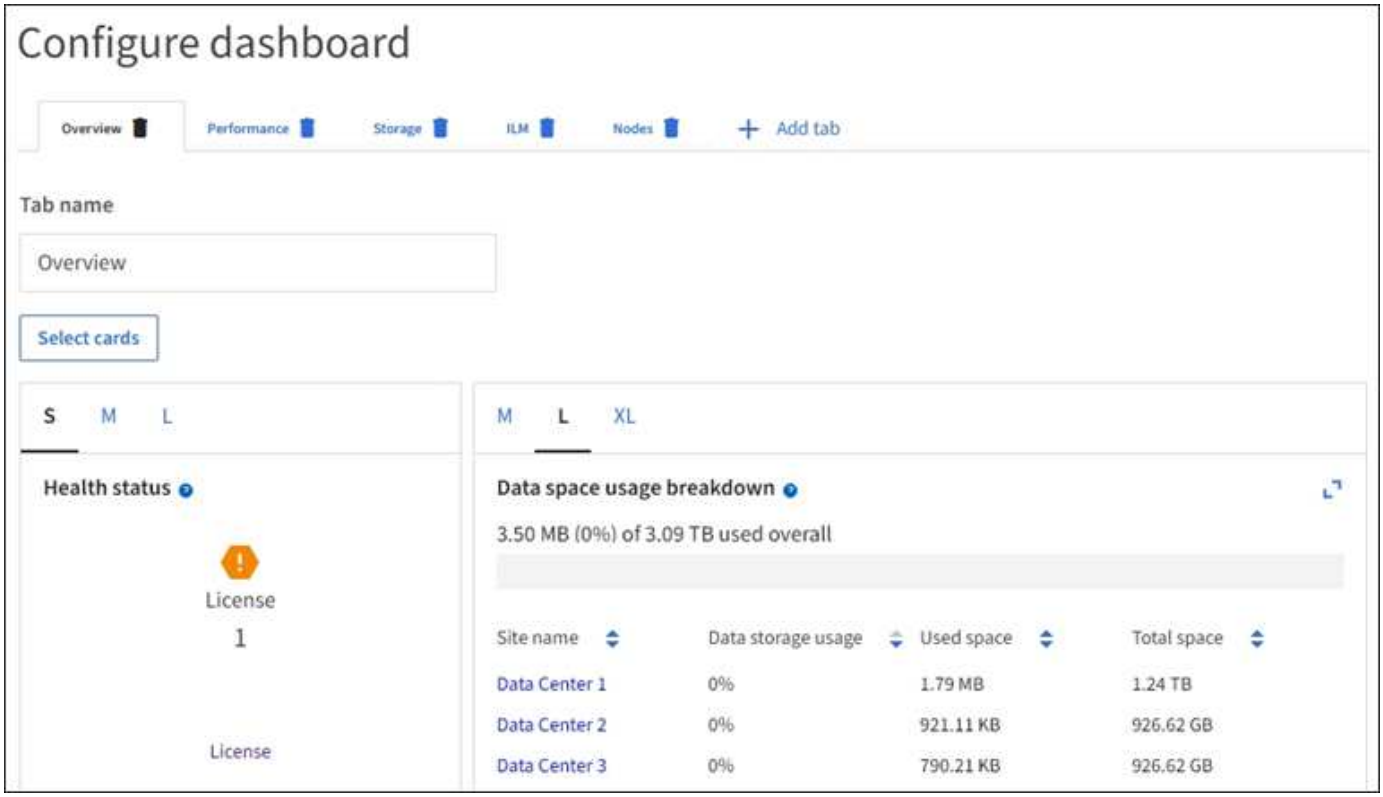
アクティブなダッシュボードをクローニングして新しいダッシュボードを作成するには、**[操作]**>*[アクティブなダッシュボードのクローニング]*を選択します。

既存のダッシュボードを編集またはクローンするには、**[アクション]**>*[ダッシュボードの管理]*を選択します。

システムが提供するダッシュボードは編集または削除できません。

ダッシュボードを設定する際には、次の操作を実行できます。

- タブを追加または削除します
- タブの名前を変更し、新しいタブに一意の名前を付けます
- 各タブのカードを追加、削除、または並べ替え（ドラッグ）します
- カード上部の* S 、 M 、 L 、または XL *を選択して、個 々 のカードのサイズを選択します



Nodes ページを表示します

StorageGRIDノードページを表示します

StorageGRID システムについて、ダッシュボードの情報よりも詳細な情報が必要な場合は、[Nodes]ページを使用してグリッド全体、グリッド内の各サイト、およびサイト内の各ノードの指標を表示できます。

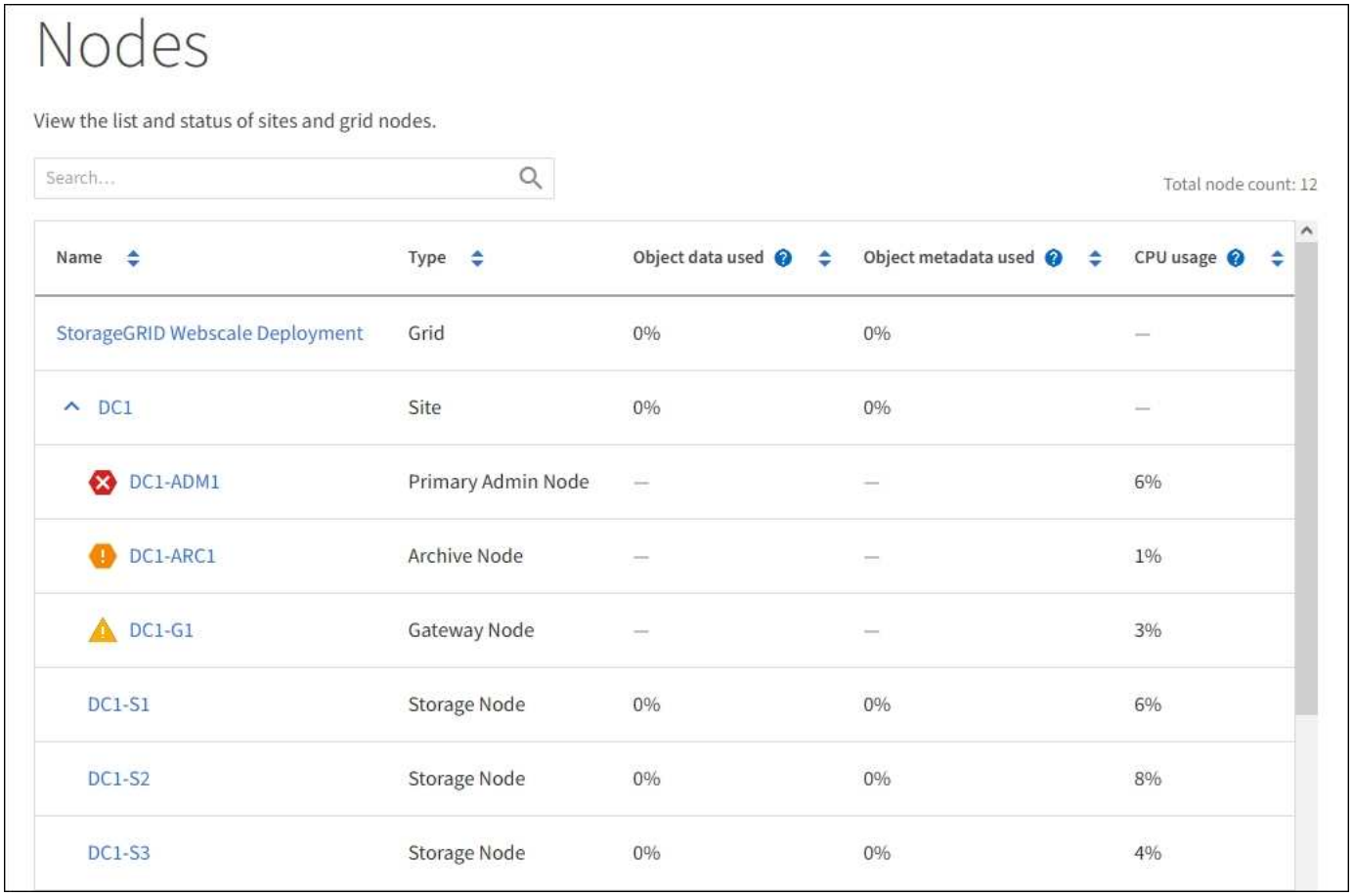
[Nodes]テーブルには、グリッド全体、各サイト、および各ノードの概要情報が表示されます。切断されてい

るノードやアクティブなアラートがあるノードは、ノード名の横にアイコンが表示されます。ノードが接続されていてアクティブなアラートがない場合は、アイコンは表示されません。

アップグレード中や切断状態など、ノードがグリッドに接続されていない場合は、特定の指標が使用できないか、サイトおよびグリッドの合計値から除外されることがあります。ノードがグリッドに再接続されたら、値が安定するまで数分待ちます。

Grid Managerに表示されるストレージ値の単位を変更するには、Grid Managerの右上にあるユーザドロップダウンを選択し、*[ユーザ設定]*を選択します。

ここに示されているスクリーンショットは一例です。StorageGRIDのバージョンによっては、結果が異なる場合があります。



接続状態アイコン

ノードがグリッドから切断されている場合は、ノード名の横に次のいずれかのアイコンが表示されます。

をクリックします。	製品説明	アクションが必要です
	• 接続されていません - 不明 * 理由が不明な場合、ノードが切断されているか、ノードのサービスが予期せず停止しています。たとえば、ノードのサービスが停止したり、電源障害や予期しない停止によってノードのネットワーク接続が失われたりする場合があります。 • Unable to communicate with node * アラートがトリガーされる場合もあります。他のアラートもアクティブになる可能性があります。	すぐに対処する必要があります。"各アラートを選択します"そして推奨される行動に従ってください。 たとえば、ノードのホストを停止または再起動したサービスの再起動が必要になることがあります。 注：管理されたシャットダウン処理の実行中は、ノードがUnknownと表示されることがあります。このような場合、 Unknown 状態は無視してかまいません。
	• 接続されていません - 管理上の理由により停止して 想定される理由により、ノードがグリッドに接続されていません。 たとえば、ノードまたはノード上のサービスが正常にシャットダウンされた、ノードがリブート中である、ソフトウェアのアップグレード中であるなどの原因が考えられます。1つ以上のアラートがアクティブになっている可能性もあります。 基盤となる問題 に基づいて、これらのノードは多くの場合、介入なしでオンラインに戻ります。	このノードに影響しているアラートがないかどうかを確認します。 アクティブなアラートがある場合は"各アラートを選択します"、推奨される対処方法に従います。

ノードがグリッドから切断されている場合、アラートが発生している可能性がありますが、表示されるのは「Not Connected」アイコンのみです。ノードのアクティブなアラートを表示するには、ノードを選択します。

警告アイコン

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

 重大：StorageGRID ノードまたはサービスの通常の動作を停止させる異常な状態が発生しています。根本的な問題に直ちに対処する必要があります。問題が解決されない場合、サービスの中断やデータ損失が発生する可能性があります。

 重大: 現在の運用に影響を与えている、または重大な警告の閾値に近づいている異常な状態が発生しています。重大なアラートを調査し、根本的な問題に対処して、異常な状態がStorageGRIDノードまたはサービスの正常な動作を妨げないようにする必要があります。

 軽微: システムは正常に動作していますが、異常な状態が発生しており、この状態が続くとシステムの動

作能力に影響を与える可能性があります。自然に解消されない軽微なアラートは監視して解決し、より深刻な問題に発展しないようにする必要があります。

システム、サイト、またはノードの詳細を表示します

[Nodes]テーブルに表示される情報をフィルタリングするには、**[Search]***フィールドに検索文字列を入力します。システム名、表示名、またはタイプで検索できます（たとえば、「 gat *」と入力すると、すべてのゲートウェイノードをすばやく特定できます）。

グリッド、サイト、またはノードの情報を表示するには、次の手順を実行します。

- グリッド名を選択すると、 StorageGRID システム全体の統計が要約して表示されます。
- 特定のデータセンターサイトを選択すると、そのサイトのすべてのノードの統計が要約して表示されます。
- 特定のノードを選択すると、そのノードの詳細情報が表示されます。

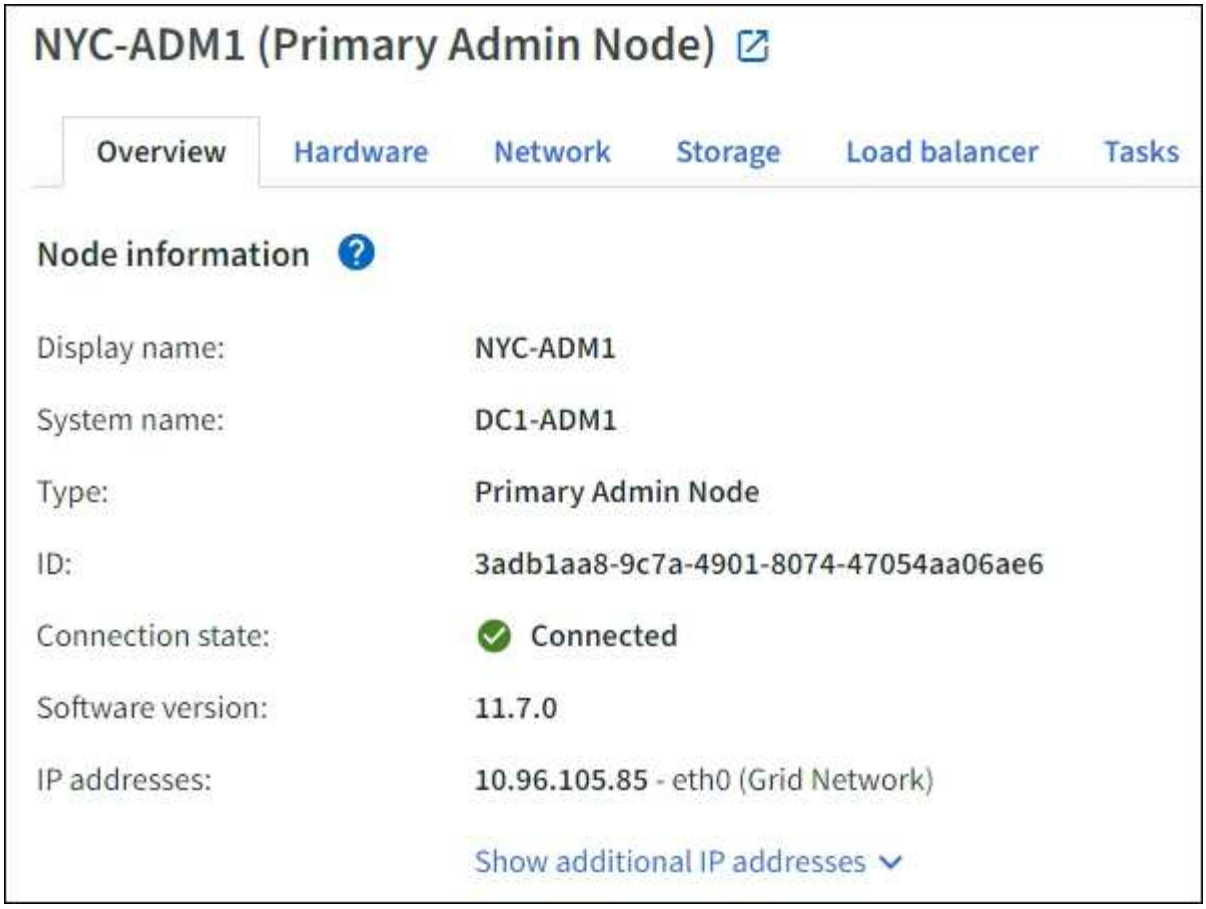
StorageGRID の概要タブを表示します

Overview タブには ' 各ノードに関する基本的な情報が表示されますまた、ノードに現在影響しているアラートも表示されます。

すべてのノードの Overview （概要）タブが表示されます。

ノード情報

[Overview]タブの[Node Information]セクションには、ノードに関する基本情報が表示されます。



ページの [概要] タブ"]

ノードの概要情報には次のものがあります。

- 表示名（ノードの名前が変更された場合にのみ表示）：ノードの現在の表示名。この値を更新するには、の手順を使用し"グリッド、サイト、ノードの名前を変更します"ます。
- システム名：インストール時に入力したノードの名前。システム名は内部StorageGRID 処理に使用され、変更することはできません。
- * Type *：ノードのタイプ（管理ノード、プライマリ管理ノード、ストレージノード、またはゲートウェイノード）。
- * ID *：ノードの一意の識別子。 UUID とも呼ばれます。
- * 接続状態 *： 3 つの状態のいずれか。最も重大な状態のアイコンが表示されます。
  - 不明：不明な理由により、ノードがグリッドに接続されていないか、1つ以上のサービスが予期せず停止しています。例えば、ノード間のネットワーク接続が失われた、電源が落ちた、またはサービスが停止した、といった場合が考えられます。*ノードと通信できません*アラートもトリガーされる場合があります。他のアラートもアクティブになっている可能性があります。この状況は早急な対応が必要です。

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

  - *管理上の問題で停止中*：ノードは想定される理由によりグリッドに接続されていません。例えば、ノード、またはノード上のサービスが正常にシャットダウンされた、ノードが再起動中である、

あるいはソフトウェアがアップグレード中である、といった場合です。1つ以上のアラートがアクティブになっている可能性もあります。

- 接続済み：ノードはグリッドに接続されています。

- * Storage Used * ：ストレージノードのみ。
  - * Object data * ：ストレージノードで使用されているオブジェクトデータに使用可能な合計スペースの割合。
  - * Object metadata * ：ストレージノードで使用されているオブジェクトメタデータに使用可能な合計スペースの割合。
- * ソフトウェアバージョン * ：ノードにインストールされている StorageGRID のバージョン。
- * HA グループ * ：管理ノードとゲートウェイノードのみ。ノードのネットワークインターフェイスがハイアベイラビリティグループに含まれている場合、およびそのインターフェイスがプライマリインターフェイスかどうかが表示されます。
- **IP**アドレス：ノードのIPアドレス。ノードのIPv4およびIPv6アドレスとインターフェイスマッピングを表示するには、*追加のIPアドレスを表示*を選択します。

アラート

[Overview]タブの[Alerts]セクションには、が表示されます"このノードに現在影響しているアラートで、サイレント化されていないアラート"。アラート名を選択すると、その他の詳細と推奨される対処方法が表示されます。



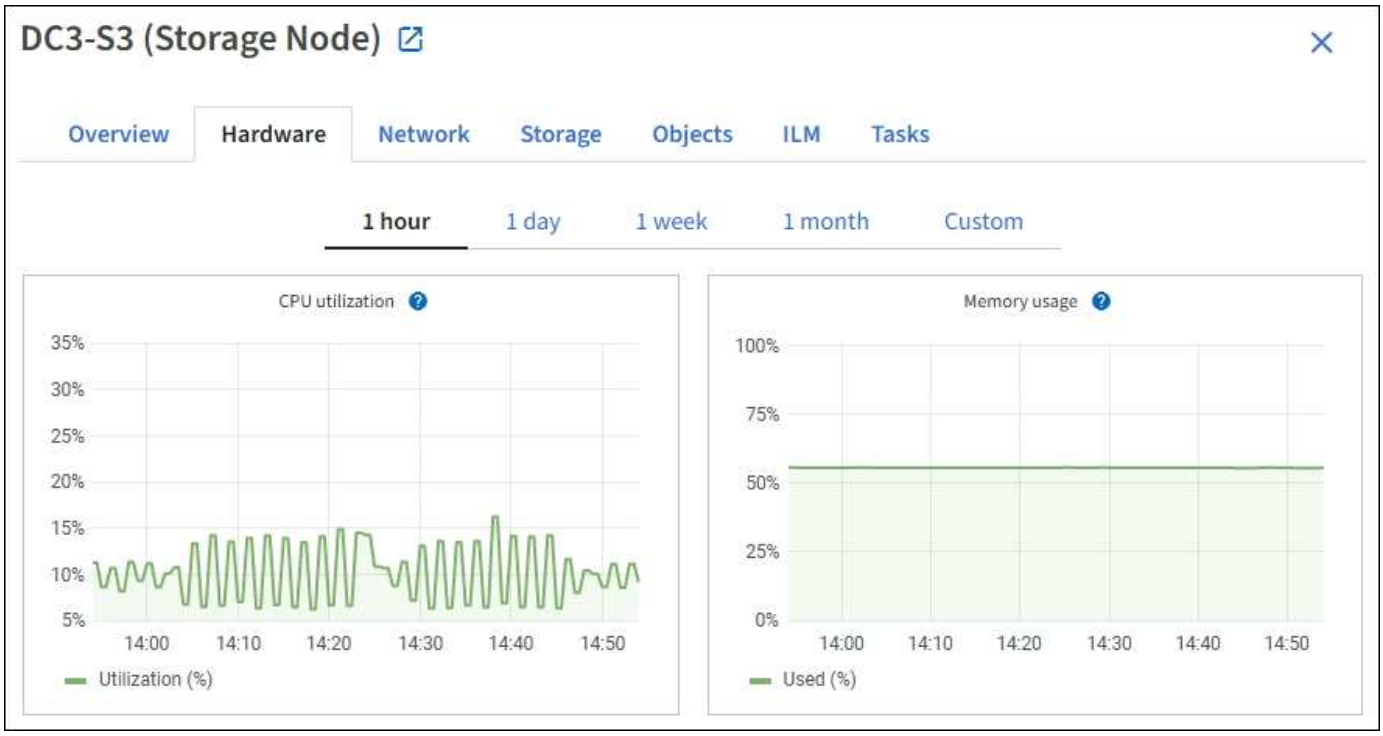
のアラートも含まれ"ノードの接続状態"ます。

StorageGRID ハードウェア タブを表示します

Hardware タブには、各ノードの CPU 利用率とメモリ使用量、およびアプライアンスに関する追加のハードウェア情報が表示されます。

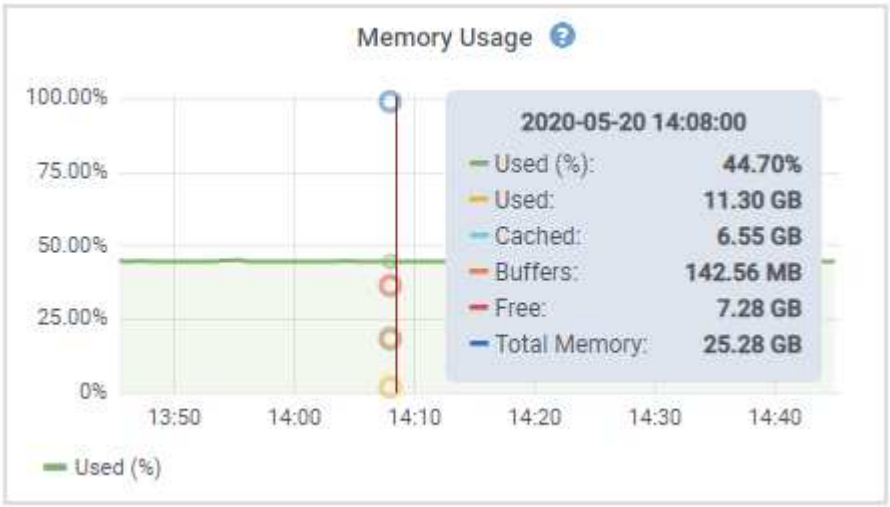
Grid Managerはリリースごとに更新され、このページのスクリーンショットの例とは異なる場合があります。

すべてのノードの Hardware （ハードウェア）タブが表示されます。



別の期間を表示するには、グラフまたはグラフの上にあるコントロールのいずれかを選択します。1 時間、 1 日、 1 週間、または 1 カ月の期間の情報を表示できます。また、カスタムの間隔を設定して、日時の範囲を指定することもできます。

CPU利用率とメモリ使用率の詳細を確認するには、各グラフにカーソルを合わせます。



ノードがアプライアンスノードの場合は、アプライアンスハードウェアに関する詳細情報を含むセクションも表示されます。

アプライアンスストレージノードに関する情報を表示します

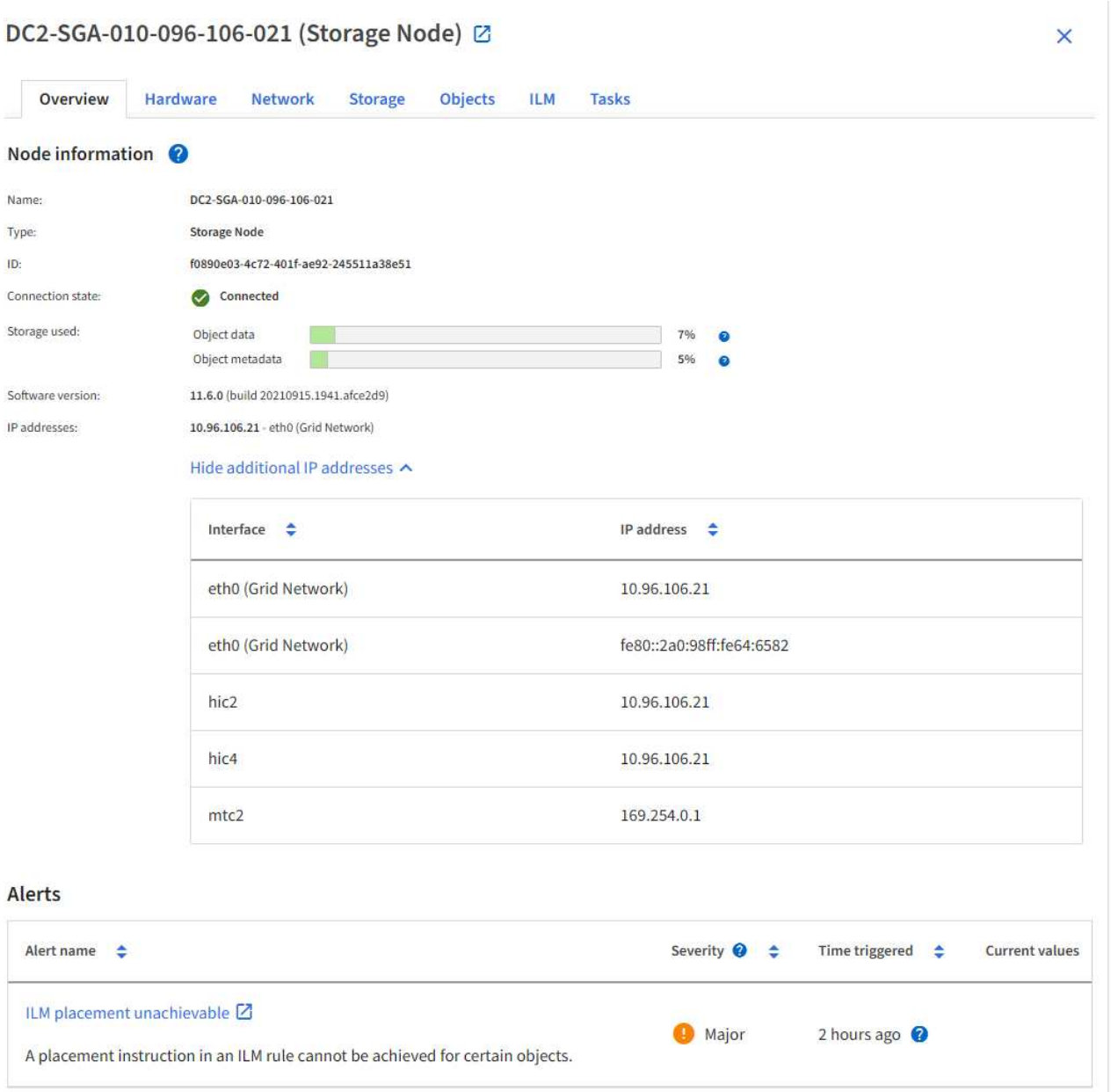
ノードページには、各アプライアンスストレージノードのサービスの健常性と、すべてのコンピューティング、ディスクデバイス、およびネットワークリソースに関する情報が表示されます。メモリ、ストレージハードウェア、コントローラファームウェアのバージョン、ネットワークリソース、ネットワークインターフェイスも表示されます。 ネットワークアドレス、およびデータの送受信。

手順

1. ノードページで、アプライアンスストレージノードを選択します。
2. 「 * 概要 * 」を選択します。

   Overview タブの Node information セクションには ' ノードの名前 ' タイプ 'ID' 接続状態など ' ノードの概要情報が表示されますIP アドレスのリストには、次のように各アドレスのインターフェイス名が含まれます。

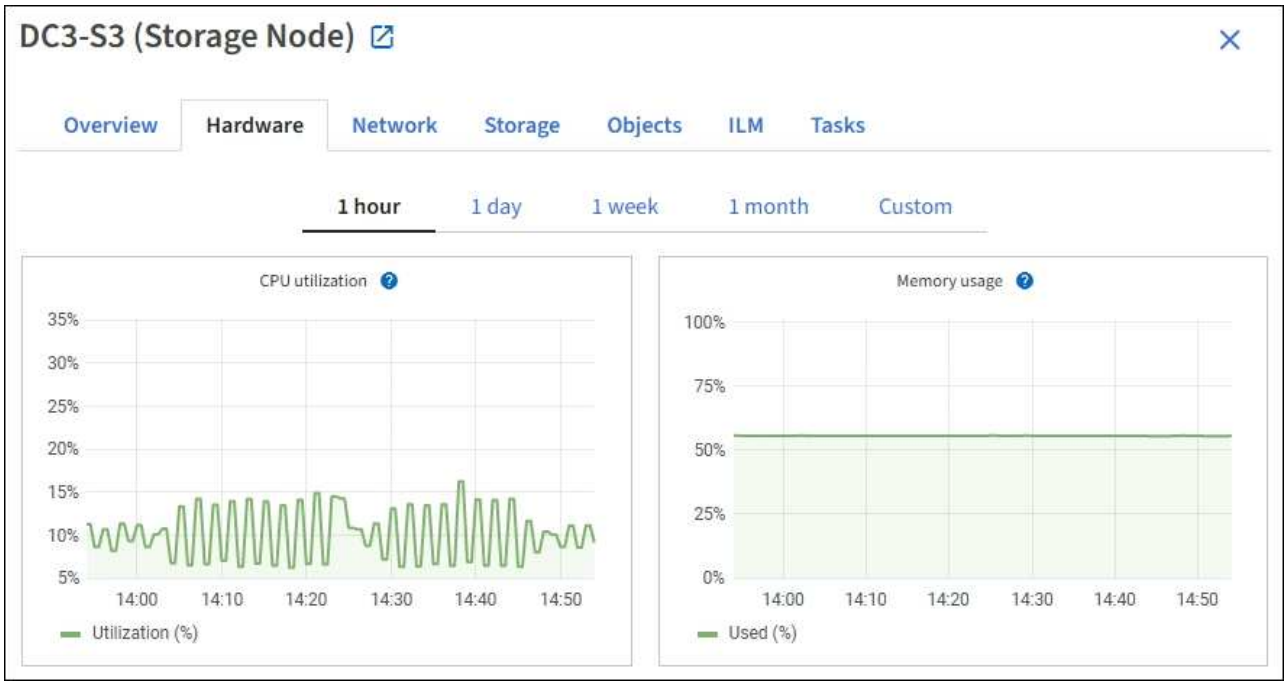
   - * eth * ：グリッドネットワーク、管理ネットワーク、またはクライアントネットワーク。
   - * HIC * ：アプライアンスの 10 、 25 、または 100GbE の物理ポートの 1 つ。これらのポートをボンディングして、 StorageGRID のグリッドネットワーク（ eth0 ）とクライアントネットワーク（ eth2 ）に接続できます。
   - * mtc * ：アプライアンス上の物理 1GbE ポートの 1 つ。1 つ以上の MTC インターフェイスがボンディングされて、 StorageGRID 管理ネットワークインターフェイス（ eth1 ）が形成されています。データセンターの技術者がローカルに接続するために、他の MTC インターフェイスを一時的に使用できます。



Overview （概要）タブの Alerts （アラート）セクションには、ノードのアクティブなアラートが表示されます。

3. アプライアンスの詳細情報を表示するには、「 * Hardware * 」を選択します。

   a. CPU使用率とメモリ使用率のグラフを表示して、時間の経過に伴うCPUとメモリの使用率の割合を確認してください。別の時間間隔を表示するには、チャートまたはグラフの上にあるコントロールのいずれかを選択してください。1時間、1日、1週間、または1ヶ月の間隔で利用可能な情報を表示できます。また、カスタム間隔を設定することもでき、日付と時間の範囲を指定できます。



b. 下にスクロールして、アプライアンスのコンポーネントの表を表示します。この表には、アプライアンスのモデル名、コントローラ名、シリアル番号、 IP アドレス、各コンポーネントのステータスなどの情報が含まれています。

> Compute Controller BMC IP 、 Compute hardware などの一部のフィールドは、その機能を持つアプライアンスに対してのみ表示されます。

ストレージシェルフのコンポーネントと拡張シェルフが設置に含まれている場合は、アプライアンステーブルの下の個別のテーブルに表示されます。

Appliance テーブルのフィールド	製品説明
アプライアンスのモデル	SANtricity OSに表示されるこのStorageGRID アプライアンスのモデル番号。
ストレージコントローラ名	SANtricity OSに表示されるこのStorageGRID アプライアンスの名前。
ストレージコントローラ A の管理 IP	ストレージコントローラAの管理ポート1のIPアドレス。このIPを使用してSANtricity OSにアクセスし、ストレージの問題をトラブルシューティングします。
ストレージコントローラ B の管理 IP	ストレージコントローラBの管理ポート1のIPアドレス。このIPを使用してSANtricity OSにアクセスし、ストレージの問題をトラブルシューティングします。 一部のアプライアンスモデルには、ストレージコントローラBが搭載されていません

Appliance テーブルのフィールド	製品説明
ストレージコントローラ WWID	SANtricity OSに表示されるストレージコントローラのWorld-Wide Identifier。
ストレージアプライアンスのシャーシのシリアル番号	アプライアンスのシャーシのシリアル番号。
ストレージコントローラのファームウェアバージョン	このアプライアンスのストレージコントローラ上のファームウェアのバージョン。
ストレージコントローラのSANtricity OSバージョン	ストレージコントローラAのSANtricity OSバージョン。
ストレージコントローラのNVSRAMバージョン	SANtricityシステムマネージャから報告されるストレージコントローラのNVSRAMバージョン。 SG6060とSG6160で、2台のコントローラでNVSRAMバージョンが一致していない場合は、コントローラAのバージョンが表示されます。コントローラAが取り付けられていないか動作していない場合は、コントローラBのバージョンが表示されます。
ストレージハードウェア	ストレージコントローラハードウェアの全体的なステータス。SANtricity System Manager からストレージハードウェアの要注意のステータスが報告された場合、 StorageGRID システムからも報告されます。 ステータスが「Needs Attention」の場合は、まずSANtricity OSを使用してストレージコントローラを確認します。次に、コンピューティングコントローラに適用されるアラートが他にないことを確認します。
ストレージコントローラの障害ドライブ数	最適な状態でないドライブの数。
ストレージコントローラ A	ストレージコントローラ A のステータス
ストレージコントローラ B	ストレージコントローラBのステータス。一部のアプライアンスモデルにはストレージコントローラBがありません。
ストレージコントローラの電源装置 A	ストレージコントローラの電源装置 A のステータス。
ストレージコントローラの電源装置 B	ストレージコントローラの電源装置 B のステータス。
ストレージデータドライブのタイプ	アプライアンス内のドライブのタイプ。HDD（ハードドライブ）やSSD（ソリッドステートドライブ）など。

Appliance テーブルのフィールド	製品説明
ストレージデータドライブのサイズ	1 つのデータドライブの実効サイズ。 SG6160の場合は、キャッシュドライブのサイズも表示されます。 注：拡張シェルフを搭載したノードの場合は、代わりにを使用して各シェルフのデータドライブのサイズください。有効なドライブサイズはシェルフによって異なる場合があります。
ストレージ RAID モード	アプライアンスに設定されている RAID モード。
ストレージ接続	ストレージ接続の状態。
電源装置全体	アプライアンスのすべての電源装置のステータス。
コンピューティングコントローラ BMC IP	コンピューティングコントローラ内の Baseboard Management Controller （ BMC ；ベースボード管理コントローラ）ポートの IP アドレス。この IP を使用して BMC インターフェイスに接続し、アプライアンスハードウェアを監視および診断します。 このフィールドは、BMCを搭載していないアプライアンスモデルに対しては表示されません。
コンピューティングコントローラのシリアル番号	コンピューティングコントローラのシリアル番号。
コンピューティングハードウェア	コンピューティングコントローラハードウェアのステータス。このフィールドは、コンピューティングハードウェアとストレージハードウェアが別途用意されていないアプライアンスモデルに対しては表示されません。
コントローラの CPU 温度を計算します	コンピューティングコントローラの CPU の温度ステータス。
コントローラシャーシの温度を計算します	コンピューティングコントローラの温度ステータス。
コンピュータコントローラ電源A	演算コントローラ用電源Aの状態。
コンピュータコントローラ電源B	演算コントローラ用電源Bの状態。

+

ストレージシェルフテーブルの列	製品説明
シェルフシャーシのシリアル番号	ストレージシェルフシャーシのシリアル番号。

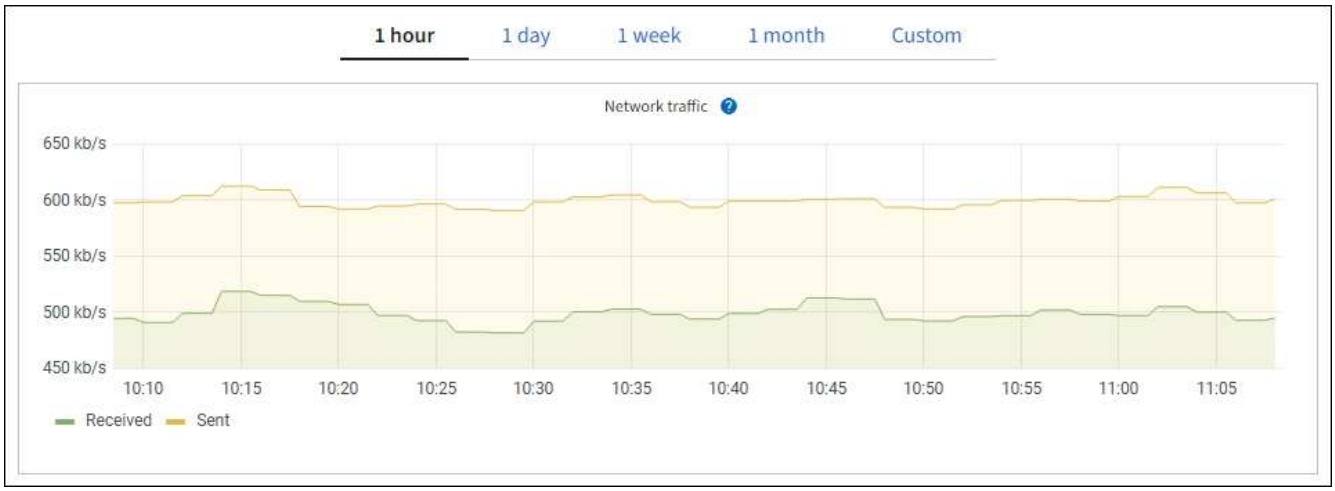
ストレージシェルフテーブルの列	製品説明
シェルフID	ストレージシェルフの数値識別子。 • 99 ：ストレージコントローラシェルフ • 0 ：最初の拡張シェルフ • 1 ： 2 台目の拡張シェルフ *注：*拡張シェルフはSG6060およびSG6160にのみ適用されます。
シェルフステータス	ストレージシェルフの全体的なステータス。
IOMのステータス	拡張シェルフの入出力モジュール（ IOM ）のステータス。拡張シェルフでない場合は N/A 。
電源装置ステータス	ストレージシェルフの電源装置の全体的なステータス。
ドロワーステータス	ストレージシェルフのドロワーのステータス。N/A は、シェルフにドロワーが搭載されていない場合。
ファンのステータス	ストレージシェルフの冷却ファンの全体的なステータス。
ドライブスロット	ストレージシェルフ内のドライブスロットの総数。
データドライブ	ストレージシェルフ内の、データストレージに使用されるドライブの数。
[[shelf_data_drive_size]] データドライブのサイズ	ストレージシェルフ内の 1 つのデータドライブの実効サイズ。
キャッシュドライブ	ストレージシェルフ内のキャッシュとして使用されるドライブの数。
キャッシュドライブサイズ	ストレージシェルフ内で最小のキャッシュドライブのサイズ。通常、キャッシュドライブのサイズはすべて同じです。
設定ステータス	ストレージシェルフの設定ステータス。

a. すべてのステータスが「Nominal」であることを確認します。

ステータスが「Nominal」でない場合は、現在のアラートを確認します。SANtricity System Manager を使用して、これらのハードウェアの値の一部を確認することもできます。アプライアンスの設置とメンテナンスの手順を参照してください。

4. 各ネットワークの情報を表示するには、「 * ネットワーク * 」を選択します。

Network Traffic グラフには、ネットワークトラフィック全体のサマリが表示されます。



a. ネットワークインターフェースのセクションを確認してください。

Network interfaces

Name	Hardware address	Speed	Duplex	Auto-negotiation	Link status
eth0	00:50:56:A7:66:75	10 Gigabit	Full	Off	Up

アプライアンス上の 10/25-GbE ネットワークポートがアクティブ/バックアップモードまたは LACP モードのどちらを使用するように構成されているかを判断するには、ネットワークインターフェイステーブルの **Speed** 列の値と以下の表を使用してください。

この表の値は、 4 つのリンクがすべて使用されていることを前提としています。

リンクモード	ボンディングモード	個々の **HIC** リンク速度（ **hic1** 、 **hic2** 、 **hic3** 、 **hic4** ）	想定されるグリッド / クライアントネットワーク速度（ **eth0** 、 **eth2** ）
アグリゲート	LACP	25	100
固定	LACP	25	50
固定	アクティブ / バックアップ	25	25
アグリゲート	LACP	10	40
固定	LACP	10	20
固定	アクティブ / バックアップ	10	10

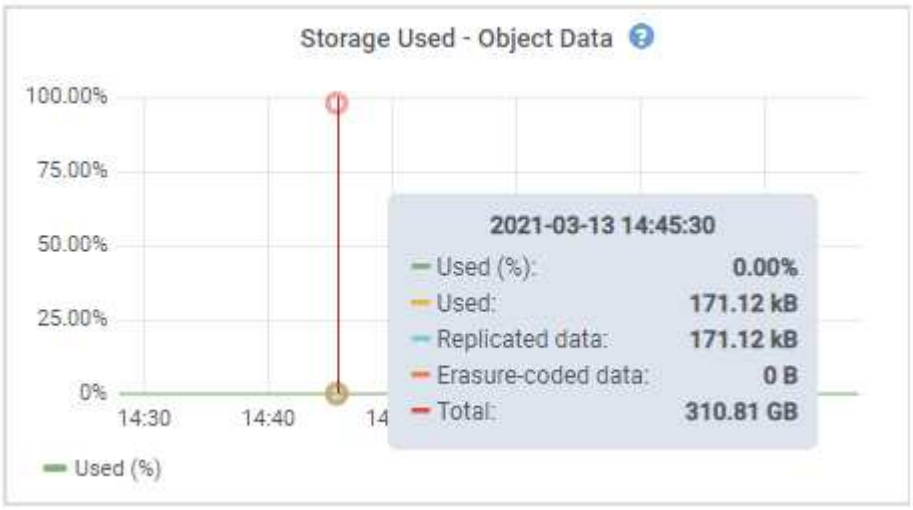
+

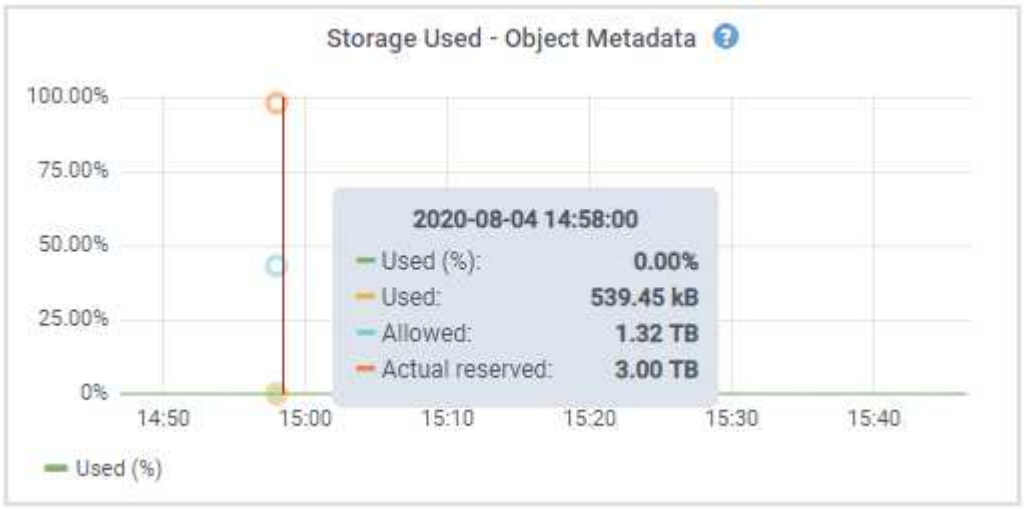
10 / 25GbEポートの設定の詳細については、を参照してください "ネットワークリンクを設定する"。

a. ネットワーク通信のセクションを確認してください。

   Receive テーブルと Transmit テーブルには、各ネットワークで送受信されたバイト数とパケット数、およびその他の送受信メトリックが表示されます。

5. 「 * Storage * 」を選択すると、オブジェクトデータとオブジェクトメタデータに使用されているストレージの割合、およびディスクデバイス、ボリューム、オブジェクトストアに関する情報がグラフに表示されます。





a. 下にスクロールして、各ボリュームとオブジェクトストアに使用可能なストレージ容量を表示します。

   各ディスクのWorldwide Nameは、SANtricity OS（アプライアンスのストレージコントローラに接続されている管理ソフトウェア）で標準のボリュームプロパティとして表示されるボリュームのWorld-Wide Identifier（WWID）と同じです。

ボリュームマウントポイントに関連するディスクの読み取りと書き込みの統計情報を解釈できるように、Disk Devices テーブルの * Name * 列に表示される名前の最初の部分（つまり、 *sdc_sd*,*sde* ）が Volumes テーブルの * Device * 列に表示される値と一致していることを確認します。

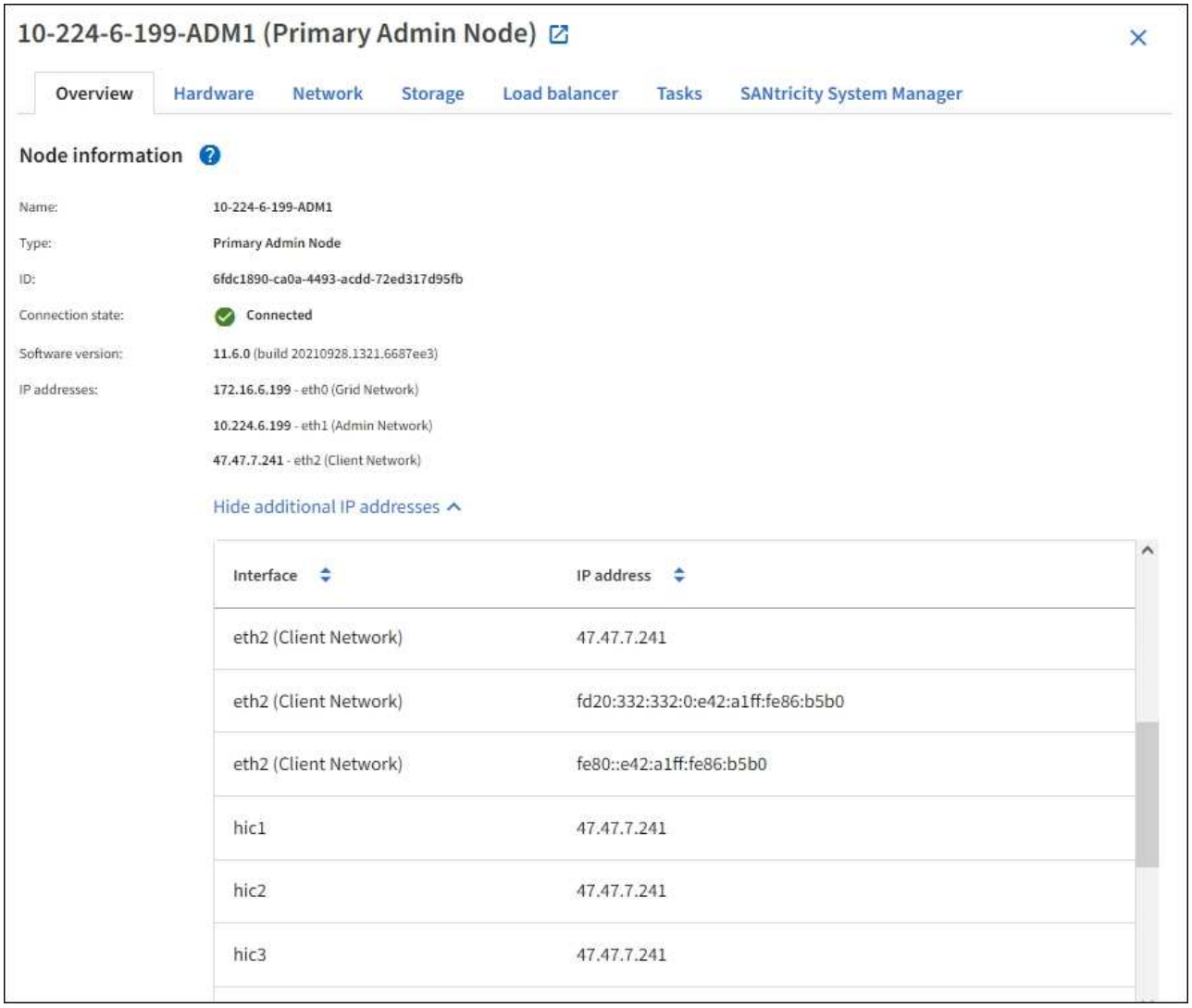
ノードページには、管理ノードまたはゲートウェイノードとして使用される各サービスアプライアンスのサービスの健常性とすべてのコンピューティング、ディスクデバイス、およびネットワークリソースに関する情報が表示されます。メモリ、ストレージハードウェア、ネットワークリソース、ネットワークインターフェイス、ネットワークアドレスも表示できます。 データを送受信します。

手順

1. Nodes ページで、アプライアンスの管理ノードまたはアプライアンスのゲートウェイノードを選択します。
2. [* Overview * （概要 * ）] タブを選択します。

   Overview タブの Node information セクションには ' ノードの名前 ' タイプ 'ID' 接続状態など ' ノードの概要情報が表示されますIP アドレスのリストには、次のように各アドレスのインターフェイス名が含まれます。

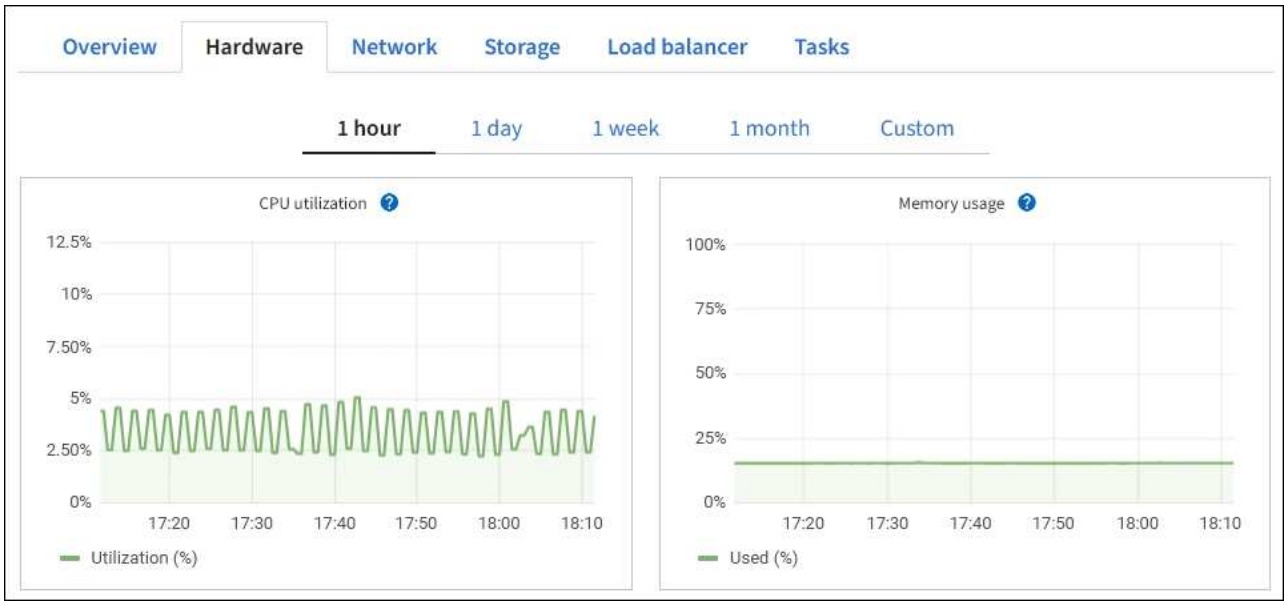
   - * adllb * および * adlli * ：管理ネットワーク・インターフェイスでアクティブ / バックアップ・ボンディングが使用されている場合に表示されます
   - * eth * ：グリッドネットワーク、管理ネットワーク、またはクライアントネットワーク。
   - * HIC * ：アプライアンスの 10 、 25 、または 100GbE の物理ポートの 1 つ。これらのポートをボンディングして、 StorageGRID のグリッドネットワーク（ eth0 ）とクライアントネットワーク（ eth2 ）に接続できます。
   - * mtc * ：アプライアンス上の物理 1GbE ポートの 1 つ。1 つ以上の MTC インターフェイスがボンディングされて、管理ネットワークインターフェイス（ eth1 ）が形成されています。データセンターの技術者がローカルに接続するために、他の MTC インターフェイスを一時的に使用できます。



Overview （概要）タブの Alerts （アラート）セクションには、ノードのアクティブなアラートが表示されます。

3. 機器に関する詳細情報を表示するには、*ハードウェア*タブを選択してください。

   a. CPU Utilization および Memory のグラフで、一定期間の CPU およびメモリ使用量の割合を確認します。別の期間を表示するには、グラフまたはグラフの上にあるコントロールのいずれかを選択します。1 時間、 1 日、 1 週間、または 1 カ月の期間の情報を表示できます。また、カスタムの間隔を設定して、日時の範囲を指定することもできます。



b. 機器のコンポーネント一覧表を表示するには、下にスクロールしてください。この表には、モデル名、シリアル番号、コントローラのファームウェアバージョン、各コンポーネントのステータスなどの情報が含まれています。

Appliance テーブルのフィールド	製品説明
アプライアンスのモデル	この StorageGRID アプライアンスのモデル番号。
ストレージコントローラの障害ドライブ数	最適な状態でないドライブの数。
ストレージデータドライブのタイプ	アプライアンス内のドライブのタイプ。HDD（ハードドライブ）やSSD（ソリッドステートドライブ）など。
ストレージデータドライブのサイズ	1 つのデータドライブの実効サイズ。
ストレージ RAID モード	アプライアンスの RAID モード。
電源装置全体	アプライアンスのすべての電源装置のステータス。
コンピューティングコントローラ BMC IP	コンピューティングコントローラ内の Baseboard Management Controller （ BMC ；ベースボード管理コントローラ）ポートの IP アドレス。この IP を使用して BMC インターフェイスに接続し、アプライアンスハードウェアを監視および診断することができます。 このフィールドは、BMCを搭載していないアプライアンスモデルに対しては表示されません。

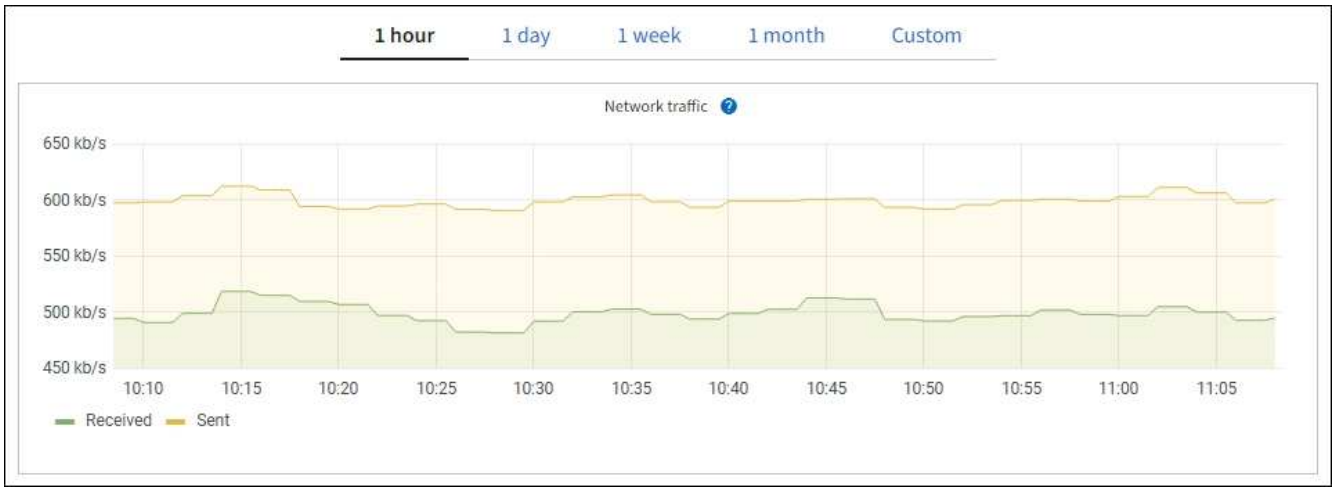
Appliance テーブルのフィールド	製品説明
コンピューティングコントローラのシリアル番号	コンピューティングコントローラのシリアル番号。
コンピューティングハードウェア	コンピューティングコントローラハードウェアのステータス。
コントローラの CPU 温度を計算します	コンピューティングコントローラの CPU の温度ステータス。
コントローラシャーシの温度を計算します	コンピューティングコントローラの温度ステータス。

c. すべてのステータスが「Nominal」であることを確認します。

ステータスが「Nominal」でない場合は、現在のアラートを確認します。

4. 各ネットワークの情報を表示するには、*ネットワーク*タブを選択してください。

Network Traffic グラフには、ネットワークトラフィック全体のサマリが表示されます。



a. ネットワークインターフェースのセクションを確認してください。

アプライアンス上の 4 つの 40/100-GbE ネットワークポートがアクティブ/バックアップモードまたは LACP モードのどちらを使用するように構成されているかを判断するには、ネットワークインターフェイステーブルの 速度 列の値と次の表を使用してください。

この表の値は、 4 つのリンクがすべて使用されていることを前提としています。

リンクモード	ボンディングモード	個々の **HIC** リンク速度（ **hic1** 、 **hic2** 、 **hic3** 、 **hic4** ）	想定されるグリッド / クライアントネットワーク速度（ **eth0** 、 **eth2** ）
アグリゲート	LACP	100	400
固定	LACP	100	200
固定	アクティブ / バックアップ	100	100
アグリゲート	LACP	40	160
固定	LACP	40	80
固定	アクティブ / バックアップ	40	40

a. ネットワーク通信のセクションを確認してください。

   受信および送信テーブルには、各ネットワークで送受信されたバイト数とパケット数、およびその他の受信および送信メトリックが表示されます。

5. サービスアプライアンス上のディスクデバイスとボリュームに関する情報を表示するには、*ストレージ* タブを選択してください。

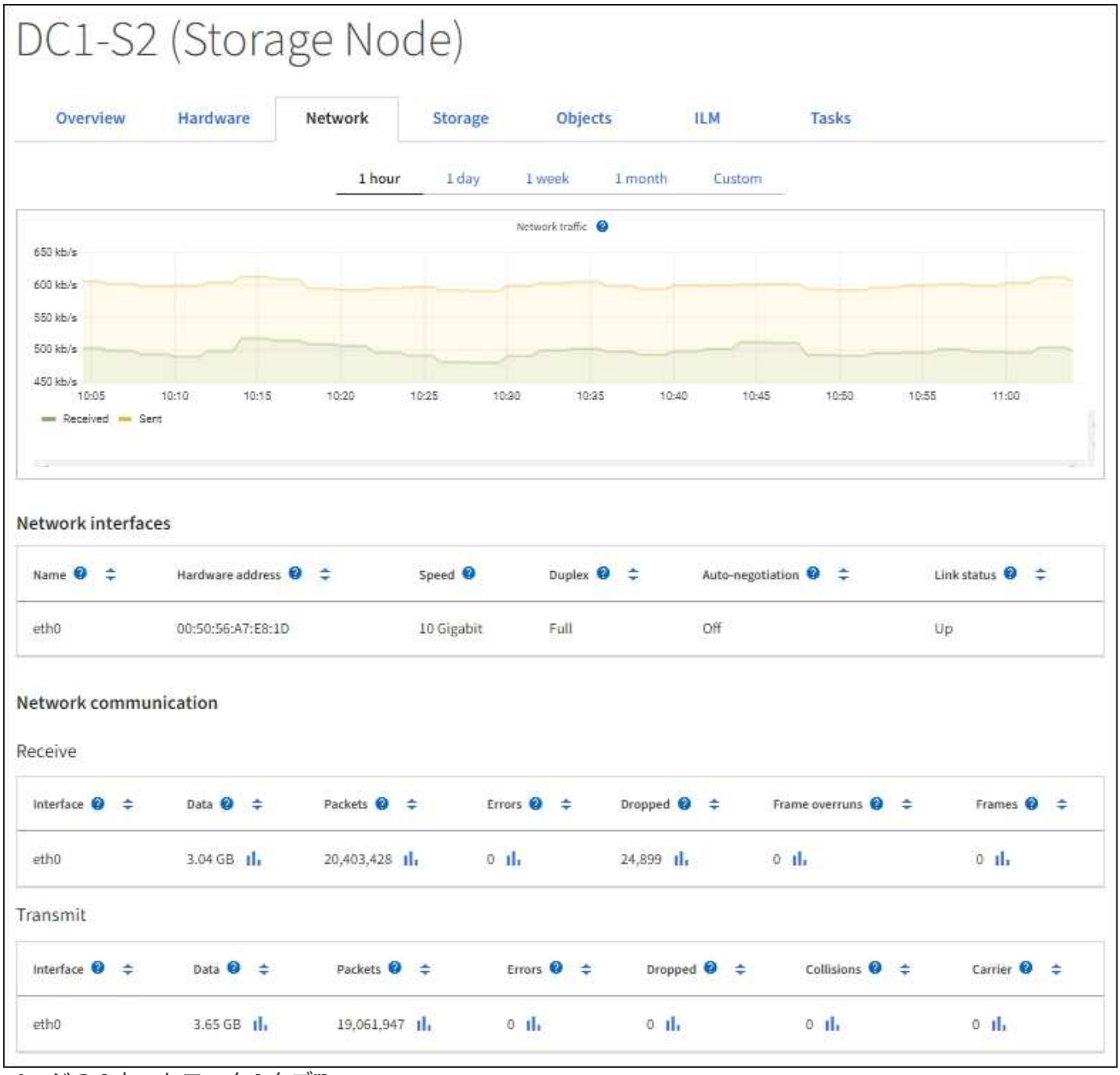
StorageGRID ネットワーク タブを表示します

Network タブには、ノード、サイト、またはグリッド上のすべてのネットワークインターフェイスで送受信されたネットワークトラフィックがグラフで表示されます。

ネットワークタブは、すべてのノード、各サイト、およびグリッド全体に対して表示されます。

別の期間を表示するには、グラフまたはグラフの上にあるコントロールのいずれかを選択します。1 時間、 1 日、 1 週間、または 1 カ月の期間の情報を表示できます。また、カスタムの間隔を設定して、日時の範囲を指定することもできます。

ノードの場合、各ノードの物理ネットワークポートに関する情報がネットワークインターフェイスの表に表示されます。ネットワーク通信テーブルには、各ノードの送受信処理の詳細と、ドライバから報告された障害カウンタが表示されます。



ページの [ネットワーク] タブ"]

関連情報

"ネットワーク接続とパフォーマンスを監視します"

StorageGRID ストレージタブを表示します

ストレージタブには、ストレージの可用性やその他のストレージ指標が表示されます。

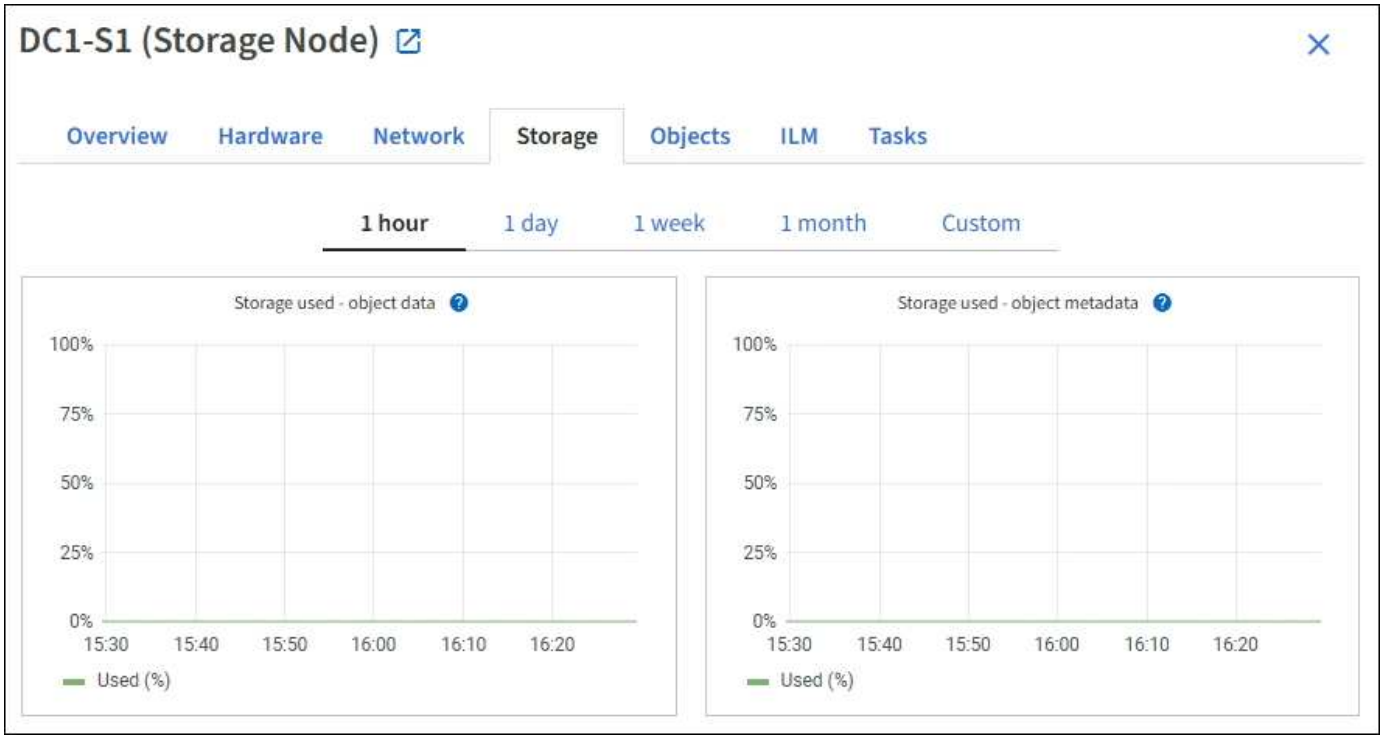
ストレージタブは、すべてのノード、各サイト、およびグリッド全体に対して表示されます。このタブには以下の情報が含まれています。

Storage Used グラフ

ストレージノード、各サイト、およびグリッド全体が対象である場合は、オブジェクトデータとオブジェクトメタデータで一定期間にわたって使用されているストレージの量を示すグラフがストレージタブに表

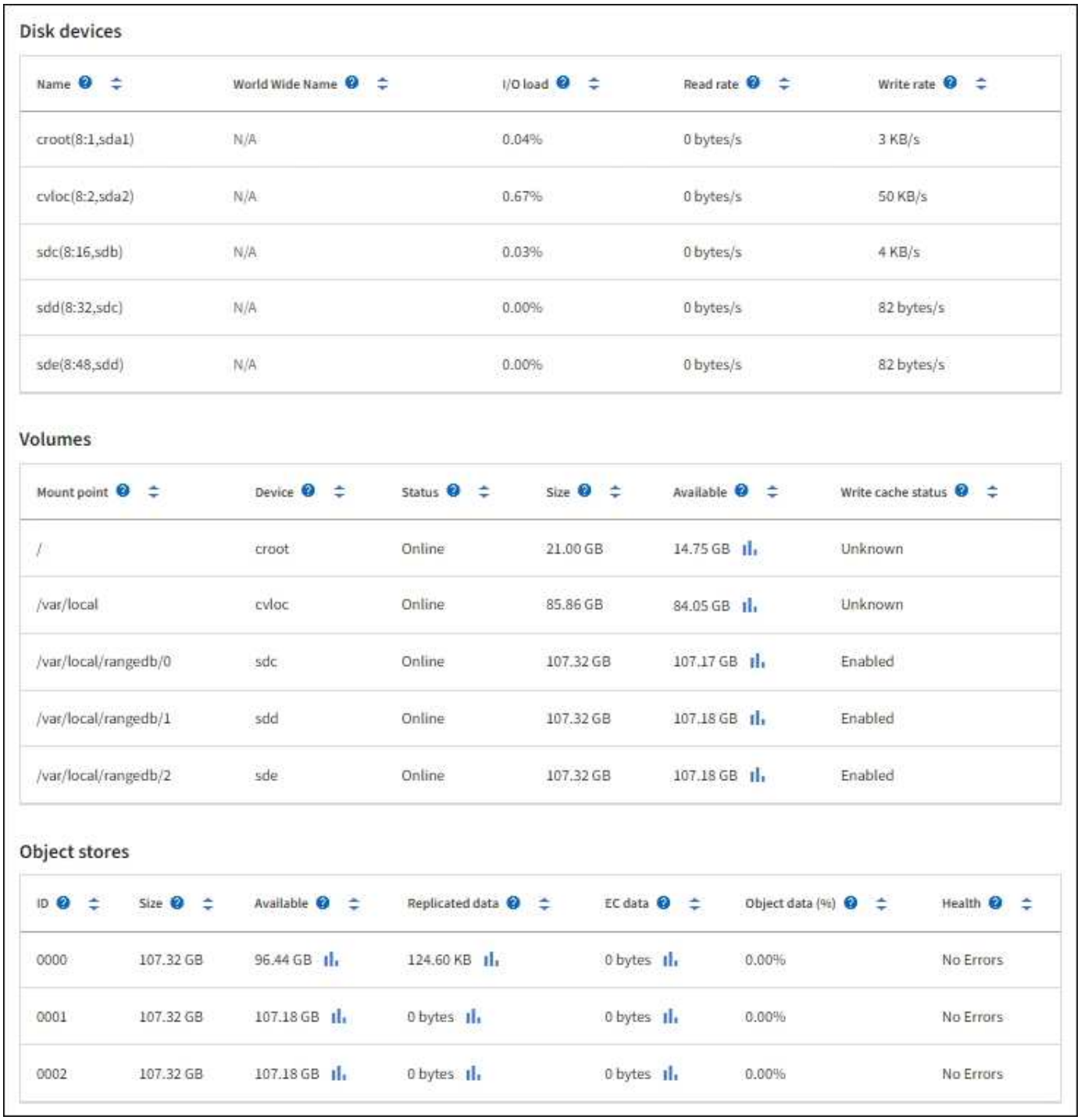
示されます。

アップグレード中や切断状態など、ノードがグリッドに接続されていない場合は、特定の指標が使用できないか、サイトおよびグリッドの合計値から除外されることがあります。ノードがグリッドに再接続されたら、値が安定するまで数分待ちます。



ディスクデバイス、ボリューム、およびオブジェクトはテーブルを格納します

すべてのノードが対象である場合は、ノード上のディスクデバイスとボリュームの詳細が表示されます。ストレージノードの場合、 Object Stores テーブルに各ストレージボリュームの情報が表示されます。



Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.67%	0 bytes/s	50 KB/s
sdc(8:16,sdb)	N/A	0.03%	0 bytes/s	4 KB/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s

Volumes

Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.75 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.05 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	124.60 KB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

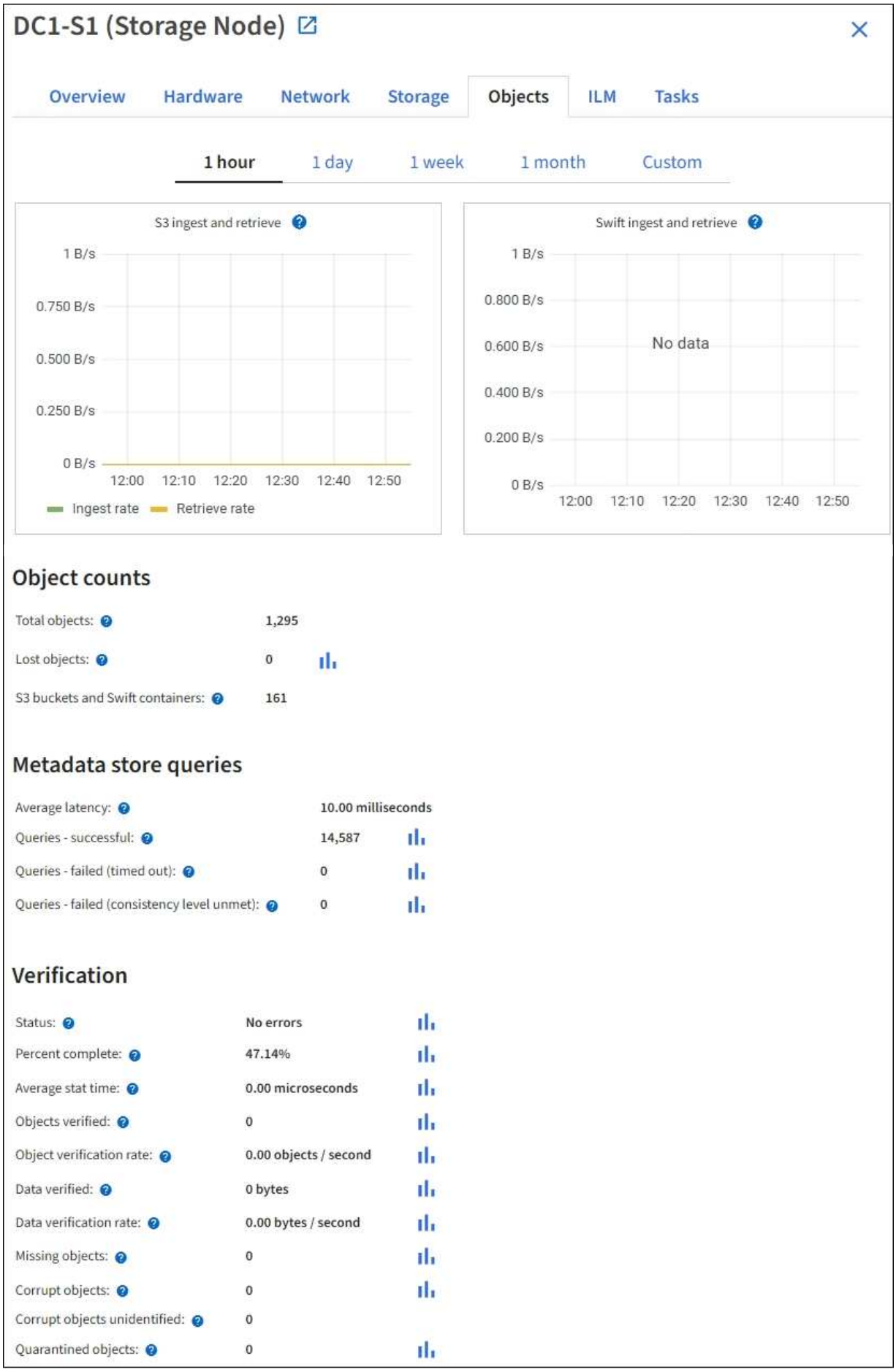
関連情報

"ストレージ容量を監視"

StorageGRID オブジェクトタブを表示します

[オブジェクト]タブには、に関する情報が表示されます"S3の取り込み速度と読み出し速度"。

各ストレージノード、各サイト、およびグリッド全体のオブジェクトタブが表示されます。ストレージノードが対象である場合は、オブジェクト数や、メタデータクエリやバックグラウンド検証に関する情報も表示されます。


DC1-S1 (Storage Node)
Overview
Hardware
Network
Storage
Objects
ILM
Tasks
1 hour
1 day
1 week
1 month
Custom
S3 ingest and retrieve
1 B/s
0.750 B/s
0.500 B/s
0.250 B/s
0 B/s
12:00
12:10
12:20
12:30
12:40
12:50
Ingest rate
Retrieve rate
Swift ingest and retrieve
1 B/s
0.800 B/s
0.600 B/s
0.400 B/s
0.200 B/s
0 B/s
No data
12:00
12:10
12:20
12:30
12:40
12:50
Object counts
Total objects: 1,295
Lost objects: 0
S3 buckets and Swift containers: 161
Metadata store queries
Average latency: 10.00 milliseconds
Queries - successful: 14,587
Queries - failed (timed out): 0
Queries - failed (consistency level unmet): 0
Verification
Status: No errors
Percent complete: 47.14%
Average stat time: 0.00 microseconds
Objects verified: 0
Object verification rate: 0.00 objects / second
Data verified: 0 bytes
Data verification rate: 0.00 bytes / second
Missing objects: 0
Corrupt objects: 0
Corrupt objects unidentified: 0
Quarantined objects: 0

ページの [

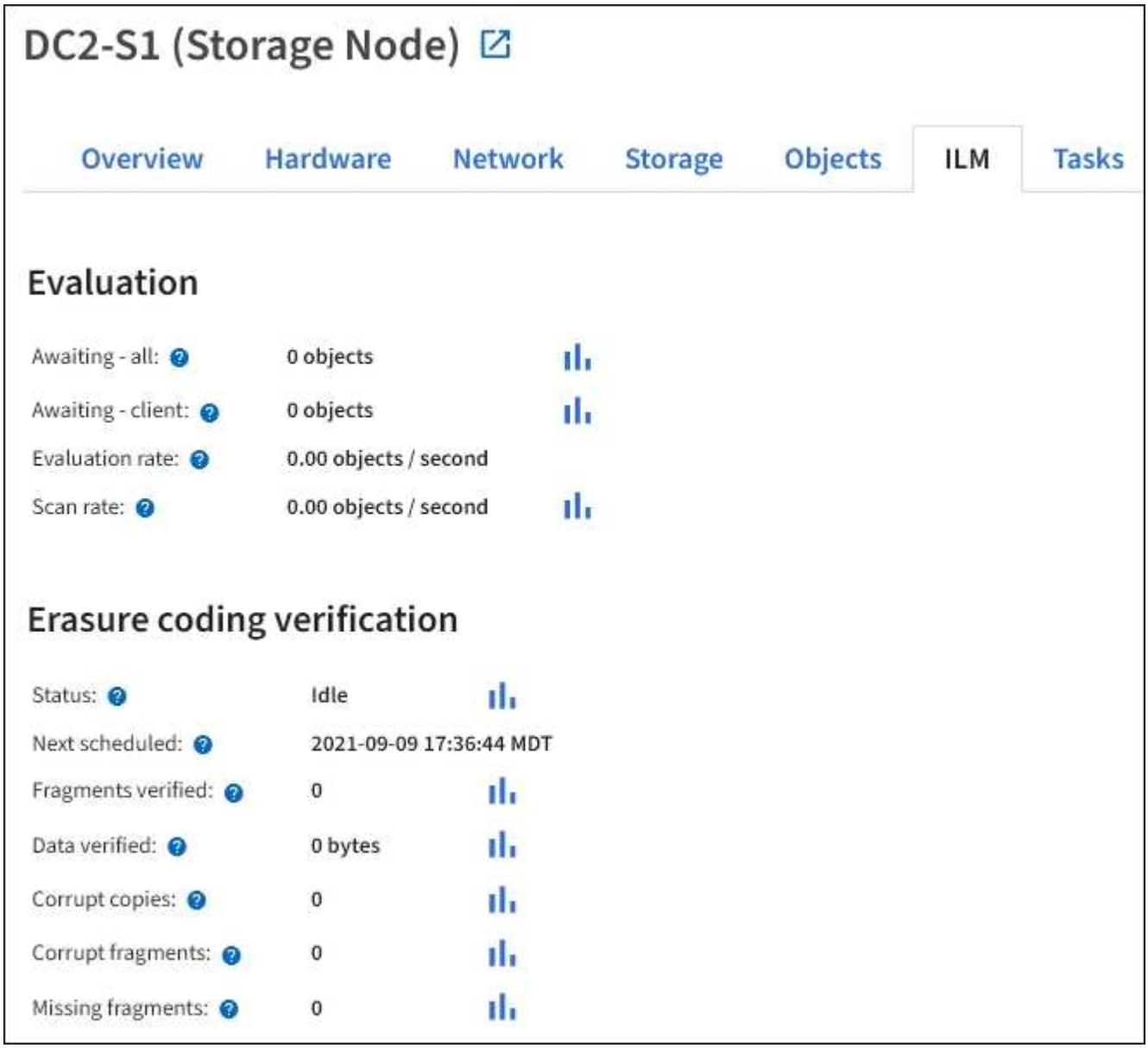
オブジェクト] タブ"]

StorageGRID ILM タブを表示します

[ILM]タブには、情報ライフサイクル管理（ILM）処理に関する情報が表示されます。

各ストレージノード、各サイト、およびグリッド全体に対して ILM タブが表示されます。各サイトおよびグリッドが対象である場合は、 ILM キューの状況の推移を示すグラフがこのタブに表示されます。グリッドが対象である場合は、 ILM によるすべてのオブジェクトのフルスキャンが完了するまでの推定時間も表示されます。

ストレージノードが対象である場合は、ILM評価とイレイジャーコーディングオブジェクトのバックグラウンド検証の詳細が表示されます。



関連情報

- "情報ライフサイクル管理を監視"

- "StorageGRID の管理"

StorageGRID タスク タブを使用します

すべてのノードに対して [タスク] タブが表示されます。このタブを使用して、ノードの名前を変更したり、ノードを再起動したり、アプライアンス ノードをメンテナンス モードにしたりできます。ストレージ ノードの場合、ストレージの状態を設定できます。

このタブの各オプションの完全な要件と手順については、次を参照してください。

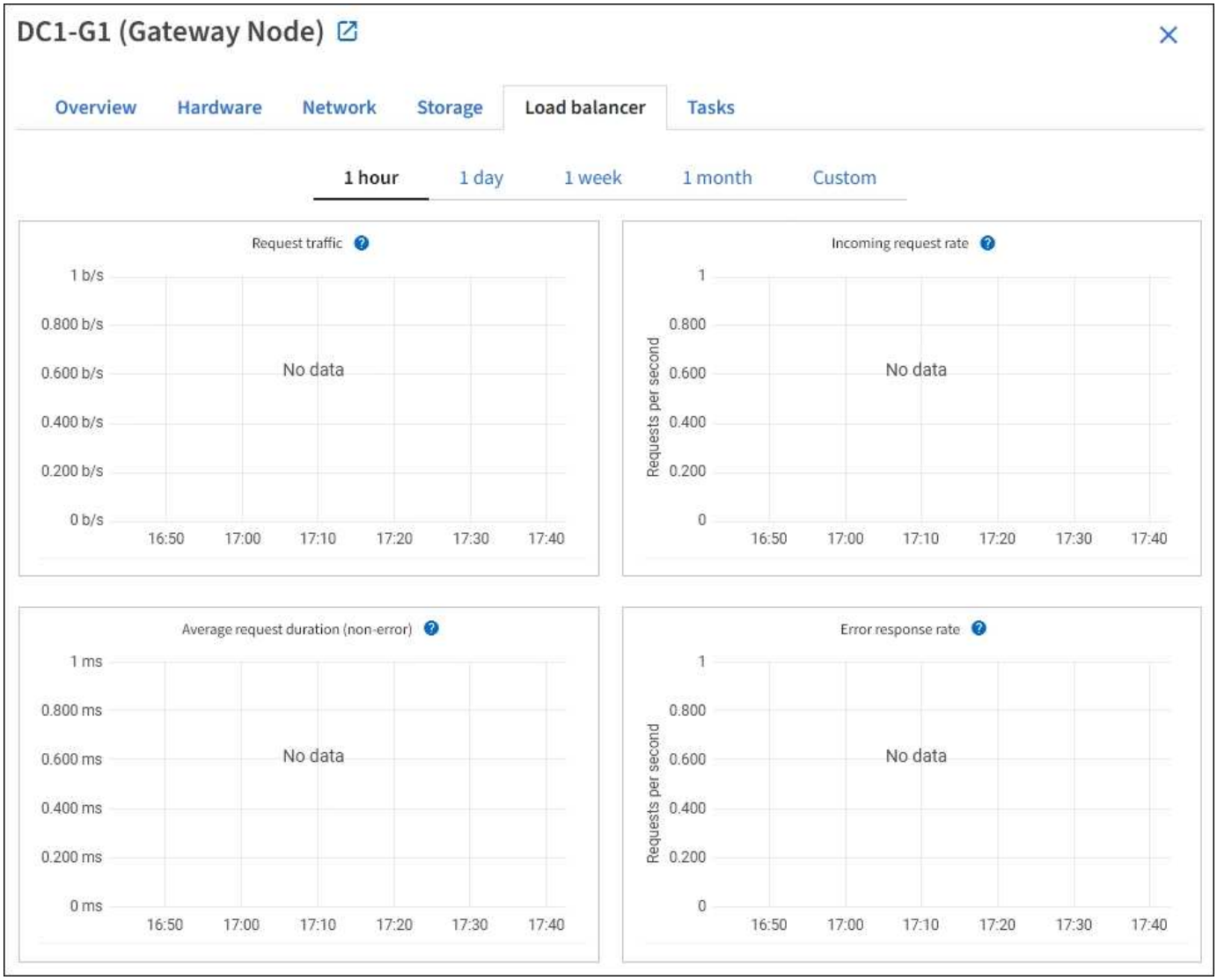
- "グリッド、サイト、ノードの名前を変更します"
- "グリッドノードをリブートします"
- "アプライアンスをメンテナンスモードにします"
- ストレージ ノードに直接接続されたボリュームまたは SAN ボリュームを追加した後、またはストレージ ノードを回復した後、ストレージ ノードのストレージ状態を確認または設定します。これらの手順は、これらのタスクを説明するトピックに記載されています。

StorageGRID ロード バランサタブを表示します

ロードバランサのタブには、ロードバランササービスの動作に関連するパフォーマンス グラフと診断グラフが表示されます。

管理ノードとゲートウェイノード、各サイト、およびグリッド全体が対象の場合は、ロードバランサのタブが表示されます。各サイトが対象である場合は、そのサイトのすべてのノードの統計が要約して表示されます。グリッド全体が対象である場合は、すべてのサイトの統計が要約して表示されます。

ロードバランササービスでI/Oが実行されていない場合やロードバランサが設定されていない場合は、グラフに「データなし」と表示されます。



ページ [ロードバランサ] タブ"]

トラフィックを要求します

このグラフには、ロードバランサエンドポイントと要求を行っているクライアントの間に送信されたデータのスループットの 3 分間の移動平均が、 1 秒あたりのビット数で示されます。

この値は、各要求が完了した時点で更新されます。そのため、要求数が少ない場合や要求の実行時間が非常に長い場合は、リアルタイムのスループットと異なる場合があります。[ネットワーク] タブを見ると、現在のネットワーク動作をよりリアルに表示できます。

受信要求レート

このグラフには、 1 秒あたりの新しい要求数の 3 分間の移動平均が、要求タイプ（ GET 、 PUT 、 HEAD 、 DELETE ）別に示されます。この値は、新しい要求のヘッダーが検証されると更新されます。

平均リクエスト時間（エラーなし）

このグラフには、要求期間の 3 分間の移動平均が、要求タイプ（ GET 、 PUT 、 HEAD 、 DELETE ）別に示されます。要求期間は、要求ヘッダーがロードバランササービスによって解析された時点から始まり、完全な応答本文がクライアントに返された時点で終了します。

エラー応答速度

このグラフには、 1 秒あたりにクライアントに返されたエラー応答数の 3 分間の移動平均が、エラー応答コード別に示されます。

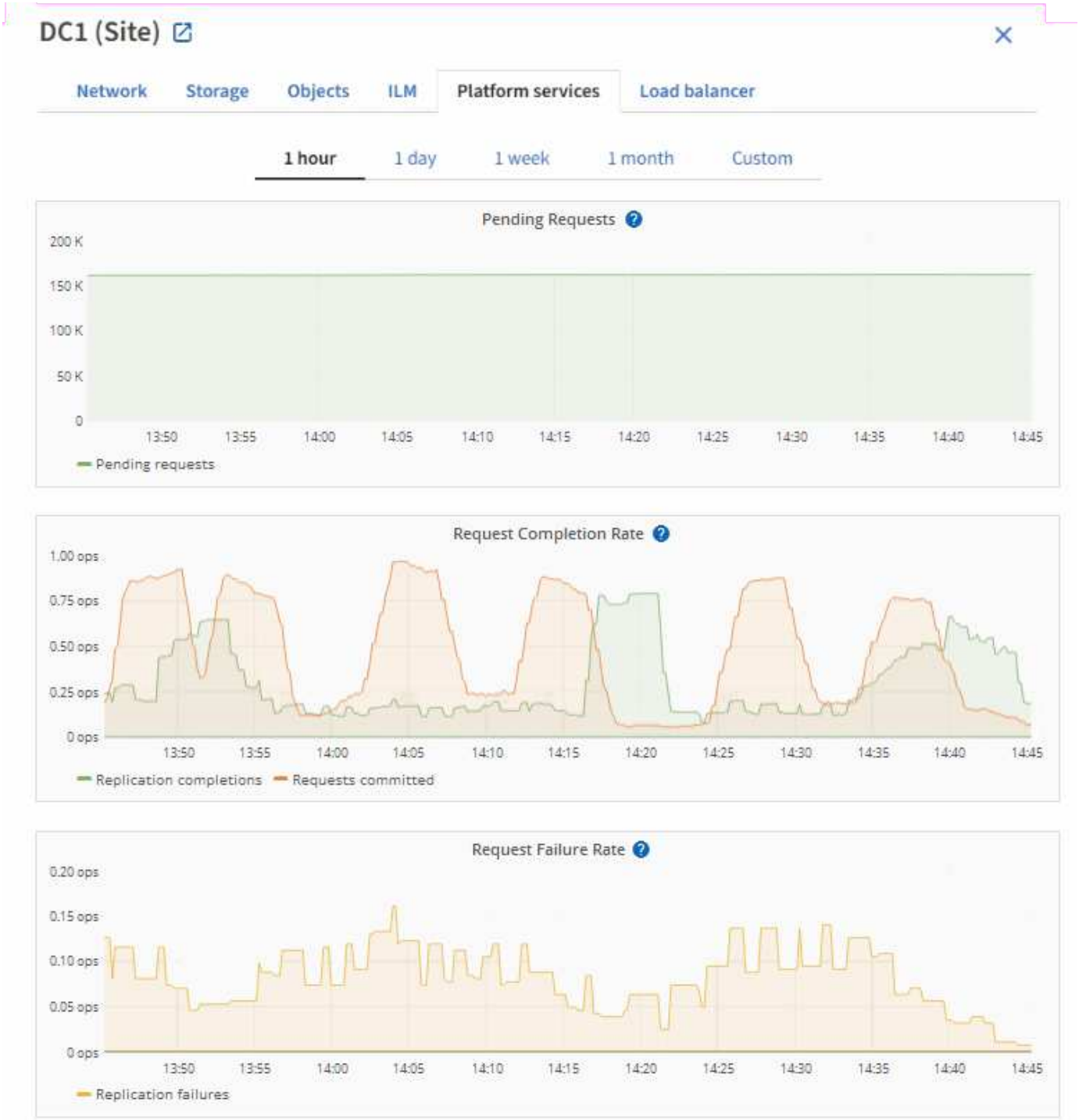
関連情報

- "ロードバランシング処理を監視する"
- "StorageGRID の管理"

StorageGRID プラットフォームサービスタブを表示します

プラットフォームサービスタブには、サイトでの S3 プラットフォームサービスの処理に関する情報が表示されます。

各サイトの [プラットフォームサービス] タブが表示されます。このタブには、 CloudMirror レプリケーションや検索統合サービスなどの S3 プラットフォームサービスに関する情報が表示されます。このタブのグラフには、保留中の要求数、要求の完了率、要求の失敗率などの指標が表示されます。



S3プラットフォームサービスの詳細（トラブルシューティングの詳細を含む）については、を参照してください"StorageGRID の管理手順"。

StorageGRID の **[** ドライブの管理 **]** タブを表示します

[Manage Drives]タブでは、この機能をサポートするアプライアンス内のドライブについて、詳細にアクセスし、トラブルシューティングとメンテナンスのタスクを実行できます。

[ドライブの管理]タブでは、次の操作を実行できます。

- アプライアンス内のデータストレージドライブのレイアウトを表示する
- ドライブの場所、タイプ、ステータス、ファームウェアバージョン、シリアル番号が一覧表示された表を表示する
- 各ドライブでトラブルシューティング機能とメンテナンス機能を実行する

[Manage Drives]タブにアクセスするには、が必要"ストレージアプライアンス管理者またはRoot Access権限"です。

ドライブの管理タブの使用方法については、を参照してください "[ドライブの管理タブを使用する"^]。

StorageGRID SANtricity System Manager タブを表示します

SANtricity の System Manager タブから、ストレージアプライアンスの管理ポートを設定したり接続したりしなくても、 SANtricity の System Manager にアクセスできます。このタブでは、ハードウェア診断と環境情報、およびドライブに関連する問題を確認できます。

> グリッドマネージャから SANtricity システムマネージャにアクセスする手順は、通常、アプライアンスのハードウェアを監視し、 E シリーズ AutoSupport を設定することだけを目的としています。ファームウェアのアップグレードなど、SANtricity System Managerの多くの機能や操作は、StorageGRID アプライアンスの監視には適用されません。問題を回避するために、必ずアプライアンスのハードウェアメンテナンス手順に従ってください。SANtricityファームウェアをアップグレードするには、ストレージアプライアンスのを参照してください "メンテナンス設定手順"。

> SANtricity の[System Manager]タブは、Eシリーズハードウェアを使用するストレージアプライアンスノードに対してのみ表示されます。

SANtricity システムマネージャを使用すると、次の操作を実行できます。

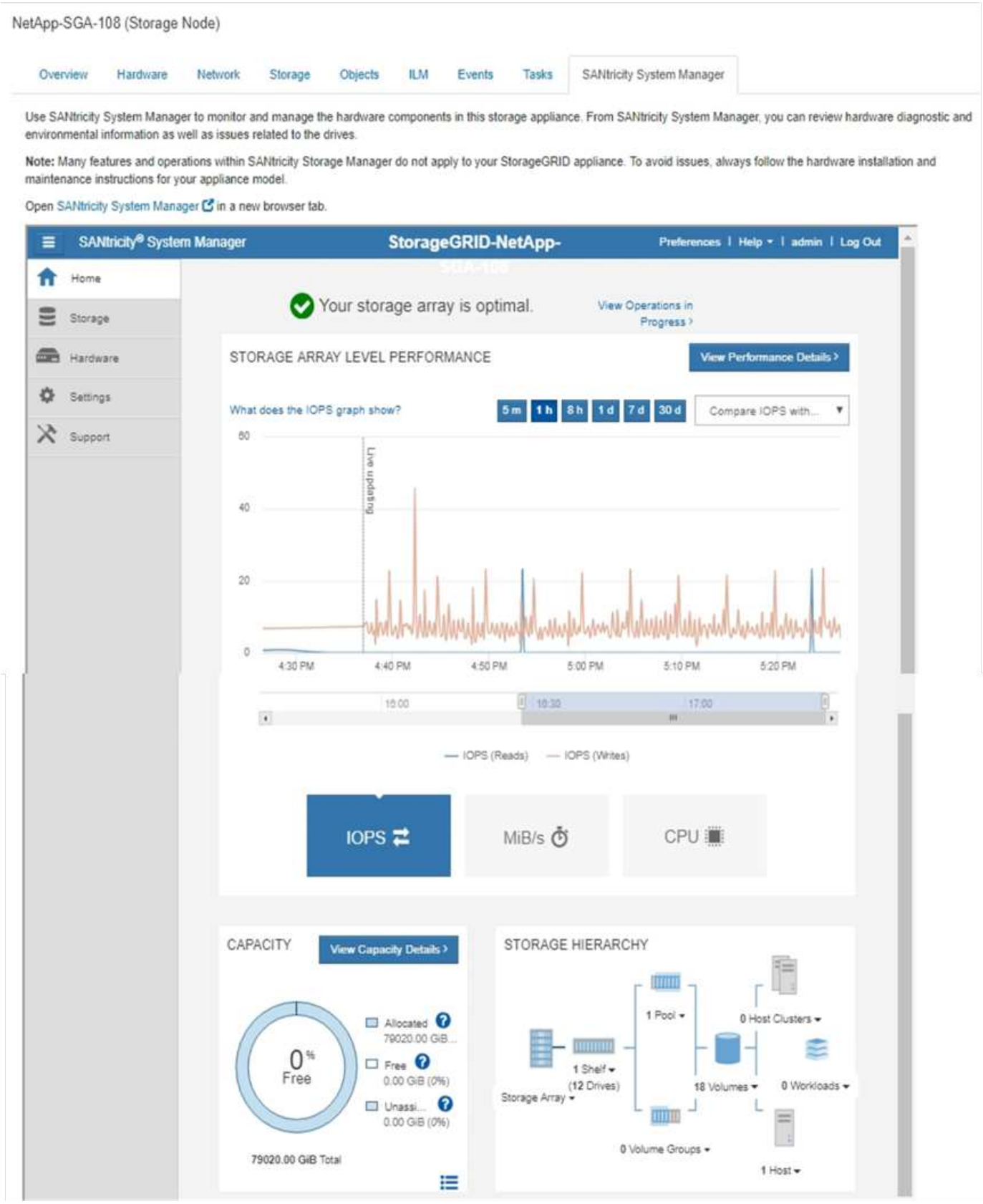
- ストレージアレイレベルのパフォーマンス、I/Oレイテンシ、ストレージコントローラのCPU利用率、スループットなどのパフォーマンスデータを表示します。
- ハードウェアコンポーネントのステータスを確認します。
- 診断データの表示、EシリーズAutoSupport の設定など、サポート機能を実行する。

> SANtricity System Manager を使用して E シリーズの AutoSupport のプロキシを設定するには、"StorageGRID経由でEシリーズAutoSupportパッケージを送信"を参照してください。

グリッドマネージャからSANtricity System Managerにアクセスするには、が必要です"ストレージアプライアンス管理者またはRoot Access権限"。

> Grid Manager を使用して SANtricity System Manager にアクセスするには、 SANtricity ファームウェア 8.70 以降が必要です。

このタブには、 SANtricity システムマネージャのホームページが表示されます。



SANtricity System Manager のリンクを使用すると、 SANtricity System Manager を新しいブラウザウィンドウで開いて確認しやすくなります。

ストレージアレイレベルのパフォーマンスと使用容量の詳細を確認するには、各グラフにカーソルを合わせま

す。

SANtricityの[System Manager]タブからアクセスできる情報の表示の詳細については、を参照してください "NetApp E シリーズおよび SANtricity に関するドキュメント"。

定期的に監視する情報

StorageGRIDで何をいつ監視するか

エラーが発生したりグリッドの一部が使用できなくなったりしてもStorageGRID システムは引き続き動作しますが、潜在的な問題がグリッドの効率や可用性に影響する前に監視して対処する必要があります。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- そうだな "特定のアクセス権限"

タスクの監視について

ビジーシステムでは大量の情報が生成されます。次のリストは、継続的に監視する必要がある最も重要な情報に関するガイダンスを示しています。

監視対象	頻度
"システムヘルスステータス"	毎日
の消費率"ストレージノードのオブジェクトとメタデータの容量"	毎週
"情報ライフサイクル管理のオペレーション"	毎週
"ネットワークおよびシステムリソース"	毎週
"テナントのアクティビティ"	毎週
"S3クライアント処理"	毎週
"ロードバランシング操作"	初期設定後と設定の変更後
"グリッドフェデレーション接続"	毎週

StorageGRIDでシステムの健全性を監視する

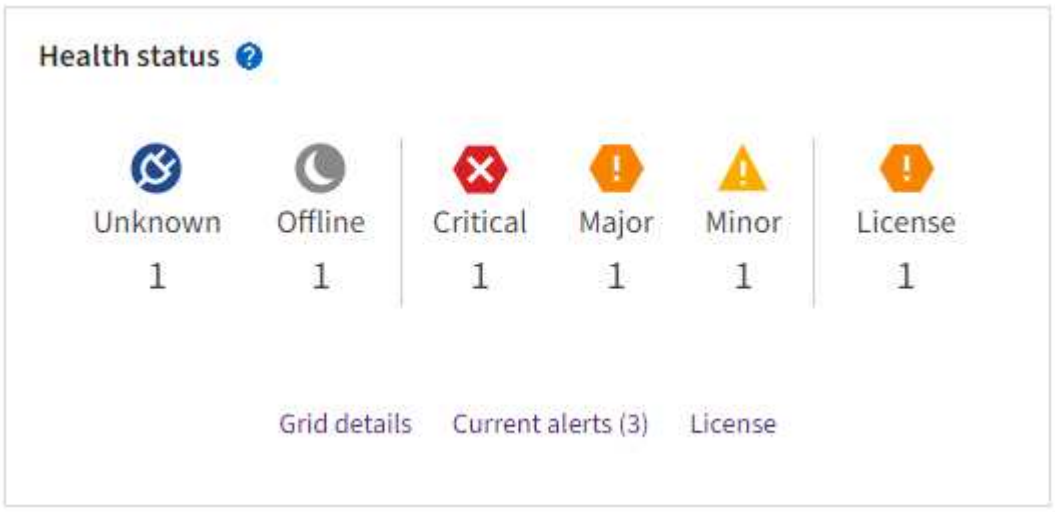
StorageGRID システム全体の健全性を毎日監視します。

タスクの内容

StorageGRID システムは、グリッドの一部が使用できない場合でも動作を継続できます。アラートによって

示される潜在的な問題は、必ずしもシステムの処理に問題があるとは限りません。Grid Managerのダッシュボードの[Health]ステータスカードにまとめられた問題を調査します。

アラートがトリガーされるとすぐに通知を受け取るには、またはを実行し "アラートのEメール通知を設定する""SNMPトラップを設定します"ます。



問題が発生している場合は、詳細を確認できるリンクが表示されます。

リンク	表示される状況
グリッドの詳細	すべてのノードが切断されています（接続状態がUnknownまたはAdministratively Down）。
現在のアラート（Critical、Major、Minor）	アラートは現在アクティブですです。
最近解決したアラート	過去1週間にトリガーされたアラート解決されました。
ライセンス	このStorageGRID システムには、ソフトウェアライセンスが付属した問題 があります。できます"必要に応じてライセンス情報を更新します"。

ノードの接続状態を監視します

1 つ以上のノードがグリッドから切断されると、重要な StorageGRID 処理に影響する可能性があります。ノードの接続状態を監視し、問題があれば迅速に対処します。

をクリックします。	製品説明	アクションが必要です
	• 接続されていません - 不明 * 理由が不明な場合、ノードが切断されているか、ノードのサービスが予期せず停止しています。たとえば、ノードのサービスが停止したり、電源障害や予期しない停止によってノードのネットワーク接続が失われたりする場合があります。 • Unable to communicate with node * アラートがトリガーされる場合もあります。他のアラートもアクティブになる可能性があります。	すぐに対処する必要があります。各アラートを選択しますそして推奨される行動に従ってください。 たとえば、ノードのホストを停止または再起動したサービスの再起動が必要になることがあります。 注：管理されたシャットダウン処理の実行中は、ノードがUnknownと表示されることがあります。このような場合、 Unknown 状態は無視してかまいません。
	• 接続されていません - 管理上の理由により停止して 想定される理由により、ノードがグリッドに接続されていません。 たとえば、ノードまたはノード上のサービスが正常にシャットダウンされた、ノードがリブート中である、ソフトウェアのアップグレード中であるなどの原因が考えられます。1つ以上のアラートがアクティブになっている可能性もあります。 基盤となる問題 に基づいて、これらのノードは多くの場合、介入なしでオンラインに戻ります。	このノードに影響しているアラートがないかどうかを確認します。 アクティブなアラートがある場合は各アラートを選択します、推奨される対処方法に従います。
	• 接続済み * ノードがグリッドに接続されます。	対処は不要です。

現在のアラートと解決済みのアラートを表示します

現在のアラート：アラートがトリガーされると、ダッシュボードにアラートアイコンが表示されます。ノードに関するアラートアイコンは、ノードページにも表示されます。の場合、"アラートEメール通知が設定されました"アラートをサイレント化していないかぎり、Eメール通知も送信されます。

解決済みのアラート：解決済みのアラートの履歴を検索して表示できます。

オプションとして、ビデオを視聴しました:

アラートの概要

次の表に、Grid Managerに表示される現在のアラートと解決済みのアラートの情報を示します。

列ヘッダー	製品説明
名前またはタイトル	アラートの名前と概要 。
重大度	アラートの重大度。現在のアラートで複数のアラートがグループ化されている場合は、各重大度で発生しているアラートのインスタンス数がタイトル行に表示されます。  重大：StorageGRID ノードまたはサービスの通常の動作を停止させる異常な状態が発生しています。根本的な問題に直ちに対処する必要があります。問題が解決されない場合、サービスの中断やデータ損失が発生する可能性があります。  重大: 現在の運用に影響を与えている、または重大な警告の閾値に近づいている異常な状態が発生しています。重大なアラートを調査し、根本的な問題に対処して、異常な状態がStorageGRIDノードまたはサービスの正常な動作を妨げないようにする必要があります。  軽微: システムは正常に動作していますが、異常な状態が発生しており、この状態が続くとシステムの動作能力に影響を与える可能性があります。自然に解消されない軽微なアラートは監視して解決し、より深刻な問題に発展しないようにする必要があります。
トリガーされた時刻	現在のアラート：アラートがトリガーされた日時（現地時間とUTC）。複数のアラートがグループ化されている場合は、タイトル行にアラートの最新のインスタンス（ _newnewest _ ）と最も古いインスタンス（ _oldest _ ）の時間が表示されます。 解決済みアラート：アラートがトリガーされてからの時間。
サイト / ノード	アラートが発生している、または発生しているサイトとノードの名前。
ステータス	アラートがアクティブか、サイレント化されているか、解決されているか。複数のアラートがグループ化され、ドロップダウンですべてのアラート * が選択されている場合、タイトル行には、そのアラートのアクティブなインスタンスの数と、サイレント化されたインスタンスの数が表示されます。
解決時間（解決済みアラートのみ）	アラートが解決されてからの時間。
現在の値または_data値_	アラートをトリガーした指標の値。一部のアラートでは、アラートの理解と調査に役立つ値が追加で表示されます。たとえば、 Low object data storage * アラートには、使用されているディスクスペースの割合、ディスクスペースの総容量、使用されているディスクスペースの容量の値が表示されます。 *注：*複数の現在のアラートがグループ化されている場合、現在の値はタイトル行に表示されません。

列ヘッダー	製品説明
トリガーされた値（解決済みのアラートのみ）	アラートをトリガーした指標の値。一部のアラートでは、アラートの理解と調査に役立つ値が追加で表示されます。たとえば、 Low object data storage * アラートには、使用されているディスクスペースの割合、ディスクスペースの総容量、使用されているディスクスペースの容量の値が表示されます。

手順

1. または[解決済みのアラート]のリンクを選択すると、それらのカテゴリのアラートのリストが表示されます。また、 Nodes **>*node*>*** Overview *を選択し、[Alerts]テーブルからアラートを選択して、アラートの詳細を表示することもできます。

   デフォルトでは、現在のアラートは次のように表示されます。

   - 最後にトリガーされたアラートが最初に表示されます。
   - 同じタイプの複数のアラートが 1 つのグループとして表示されます。
   - サイレント化されたアラートは表示されません。
   - 特定のノードの特定のアラートが複数の重大度のしきい値に達した場合は、最も重大度の高いアラートのみが表示されます。つまり、アラートが Minor 、 Major 、 Critical の各重大度のしきい値に達した場合は、 Critical アラートのみが表示されます。

     [Current alerts]ページは2分ごとに更新されます。

2. アラートのグループを展開するには、下向きキャレット を選択します。グループ内の個々のアラートを折りたたむには、上向きキャレット を選択するか、グループ名を選択します。
3. アラートのグループではなく個 々 のアラートを表示するには、*[Group alerts]*チェックボックスをオフにします。
4. 現在のアラートまたはアラートグループを並べ替えるには、各列ヘッダーの上/下矢印 を選択します。
   - グループアラート * を選択すると、アラートグループと各グループ内の個々のアラートの両方がソートされます。たとえば、グループ内のアラートを「時間トリガー」でソートして、特定のアラートの最新のインスタンスを確認できます。
   - [Group alerts]*をオフにすると、アラートのリスト全体がソートされます。たとえば、すべてのアラートを * Node/Site * でソートして、特定のノードに影響しているすべてのアラートを表示できます。
5. 現在のアラートをステータス（すべてのアラート、アクティブ、または*サイレント*）でフィルタリングするには、テーブルの上部にあるドロップダウンメニューを使用します。

   を参照して "アラート通知をサイレント化する"

6. 解決済みのアラートをソートするには：
   - [When triggered]*ドロップダウンメニューから期間を選択します。
   - 重大度*ドロップダウンメニューから1つ以上の重大度を選択します。
   - [* アラートルール * （ * Alert rule * ）] ドロップダウンメニューから 1 つ以上のデフォルトまたはカスタムのアラートルールを選択して、特定のアラートルールに関連する解決済みのアラートをフィルタリングします。
   - ノード * ドロップダウンメニューから 1 つ以上のノードを選択して、特定のノードに関連する解決済みアラートをフィルタします。

7. 特定のアラートの詳細を表示するには、アラートを選択します。選択したアラートの詳細と推奨される対処方法がダイアログボックスに表示されます。
8. （オプション）特定のアラートの[Silence this alert]を選択して、このアラートをトリガーしたアラートルールをサイレント化します。

   アラートルールをサイレント化するには、が必要です"アラートまたはRoot Access権限を管理します。"。

   > アラートルールをサイレント化する場合は注意が必要です。アラートルールがサイレント化されている場合、重大な処理が完了しないかぎり、根本的な問題が検出されないことがあります。

9. アラートルールの現在の条件を表示するには、次の手順を実行します。
   a. アラートの詳細から、*[条件の表示]*を選択します。

      定義されている各重大度の Prometheus 式がポップアップに表示されます。

   b. ポップアップを閉じるには、ポップアップの外側の任意の場所を選択してください。
10. 必要に応じて、*[ルールの編集]*を選択して、このアラートをトリガーしたアラートルールを編集します。

    アラートルールを編集するには、が必要です"アラートまたはRoot Access権限を管理します。"。

    > アラートルールを編集する場合は注意が必要です。トリガー値を変更した場合、重大な処理を完了できなくなるまで、根本的な問題が検出されないことがあります。

11. アラートの詳細を閉じるには、*[閉じる]*を選択します。

StorageGRIDでストレージ容量を監視する

使用可能な合計スペースを監視して、 StorageGRID システムのオブジェクトまたはオブジェクトメタデータのストレージスペースが不足しないようにします。

StorageGRID は、オブジェクトデータとオブジェクトメタデータを別々に格納し、オブジェクトメタデータを含む分散 Cassandra データベース用に一定量のスペースをリザーブします。オブジェクトとオブジェクトメタデータ用に消費されるスペースの合計量のほか、それぞれので消費されるスペースの傾向を監視します。これにより、ノードの追加を事前に計画し、サービスの停止を回避できます。

StorageGRIDシステムでは、グリッド全体、サイトごと、およびストレージノードごとに実行できます"ストレージ容量の情報を表示します"。

グリッド全体のストレージ容量を監視します

グリッドの全体的なストレージ容量を監視して、オブジェクトデータとオブジェクトメタデータ用に十分な空きスペースが残っていることを確認します。時間の経過に伴うストレージ容量の変化を理解しておくと、グリッドの使用可能なストレージ容量が消費される前にストレージノードまたはストレージボリュームを追加する際に役立ちます。

Grid Managerのダッシュボードでは、グリッド全体およびデータセンターごとに使用可能なストレージ容量を簡単に評価できます。ノードページには、オブジェクトデータとオブジェクトメタデータの詳細な値が表示されます。

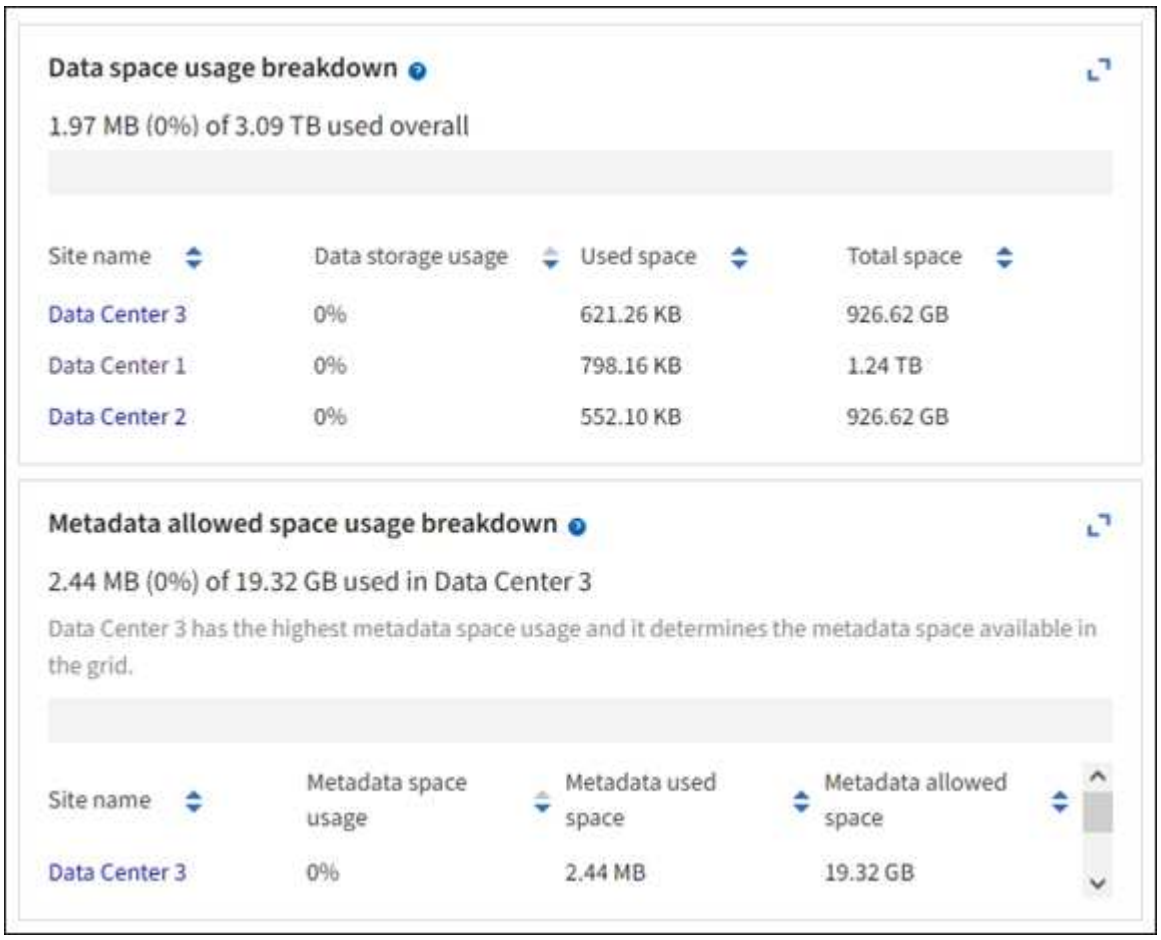
手順

1. グリッド全体および各データセンターで使用可能なストレージ容量を評価します。

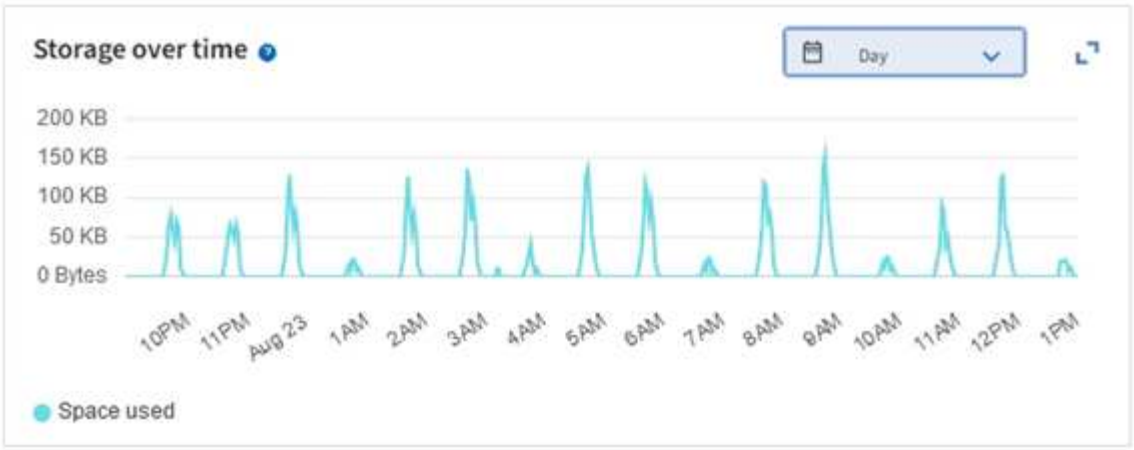
   a. [ダッシュボード]>[概要]*を選択します。

   b. [Data space usage]の内訳と[Metadata Allowed space usage]の内訳カードの値をメモします。各カードには、ストレージ使用率、使用済みスペースの容量、サイトで使用可能または許可されている合計スペースが表示されます。

      アーカイブメディアはこの概要に含まれません。



   a. [Storage Over Time]カードのグラフをメモします。期間のドロップダウンを使用すると、ストレージの消費速度を確認できます。



2. 使用済みのストレージ容量と、グリッドでオブジェクトデータとオブジェクトメタデータに使用できる残りのストレージ容量の詳細については、[Nodes]ページを使用してください。

   a. *ノード*を選択します。

   b. [***grid***>*Storage*] を選択します。



   c. と[Storage Used - object metadata]*のグラフにカーソルを合わせ、グリッド全体で使用可能なオブジェクトストレージとオブジェクトメタデータストレージの容量と使用済み容量の推移を確認します。

> サイトまたはグリッドの合計値には、オフラインのノードなど、指標が5分以上報告されていないノードは含まれません。

3. グリッドの使用可能なストレージ容量がすべて使用される前に、ストレージノードまたはストレージボリュームを追加する拡張を実行します。

   拡張のタイミングを計画する際には、追加のストレージを調達して設置するのにどれくらいの時間がかかるかを検討します。

ILM ポリシーでイレイジャーコーディングを使用している場合は、既存のストレージノードの使用率が約 70% のときに拡張して、追加する必要のあるノードの数を減らすことができます。

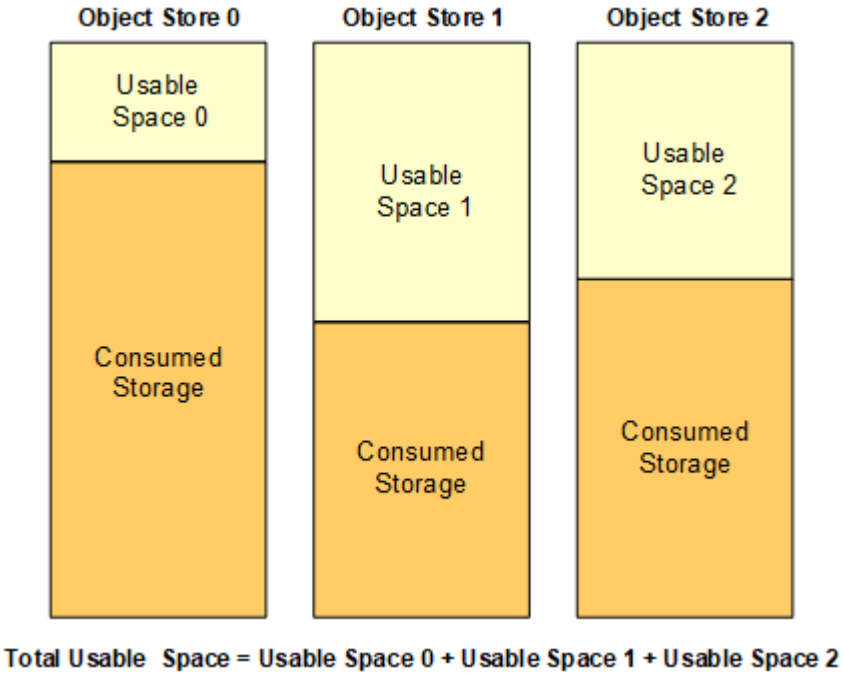
ストレージの拡張計画の詳細については、を参照して"StorageGRID の拡張手順"ください。

各ストレージノードのストレージ容量を監視します

各ストレージノードの使用可能な合計スペースを監視して、ノードに新しいオブジェクトデータ用の十分なスペースがあることを確認します。

タスクの内容

使用可能なスペースは、オブジェクトの格納に使用できるストレージスペースの量です。ストレージノードの使用可能な合計スペースは、ノード内のすべてのオブジェクトストアの使用可能なスペースの合計です。



手順

1. ノード > ストレージ ノード > ストレージ を選択します。

   ノードのグラフと表が表示されます。

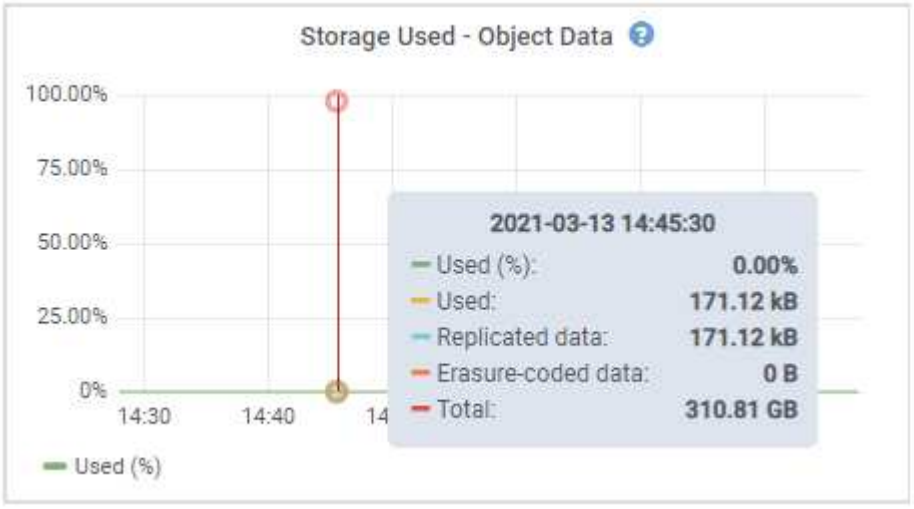
2. [Storage Used - object data]グラフにカーソルを合わせます。

   次の値が表示されます。

   - * Used （ % ） * ：オブジェクトデータに使用されている合計使用可能スペースの割合。
   - * Used * ：オブジェクトデータに使用されている合計使用可能スペースの量。
   - * Replicated data * ：このノード、サイト、またはグリッド上のレプリケートオブジェクトデータの推定量。
   - * イレイジャーコーディングデータ * ：このノード、サイト、またはグリッドにあるイレイジャーコー

ディングオブジェクトデータの推定量。

- * Total * ：このノード、サイト、またはグリッドで使用可能なスペースの総容量。[Used]の値はメトリックです `storagegrid_storage_utilization_data_bytes`。



3. グラフの下の Volumes テーブルと Object Stores テーブルで使用可能な値を確認します。

> これらの値のグラフを表示するには、「利用可能な列」のグラフアイコンを選択してください。

4. 一定期間の値を監視して、使用可能なストレージスペースが消費される速度を見積もります。
5. システムの正常な運用を維持するには、使用可能なスペースを使い切る前に、ストレージノードを追加するか、ストレージボリュームを追加するか、オブジェクトデータをアーカイブします。

   拡張のタイミングを計画する際には、追加のストレージを調達して設置するのにどれくらいの時間がかかるかを検討します。

> ILM ポリシーでイレイジャーコーディングを使用している場合は、既存のストレージノードの使用率が約 70% のときに拡張して、追加する必要のあるノードの数を減らすことができます。

   ストレージの拡張計画の詳細については、を参照して"StorageGRID の拡張手順"ください。

   "オブジェクトデータのストレージが少ない"ストレージノードにオブジェクトデータを格納するためのスペースが十分に残っていない場合にアラートがトリガーされます。

各ストレージノードのオブジェクトメタデータ容量を監視します

各ストレージノードのメタデータ使用量を監視して、重要なデータベース処理に使用できるスペースが十分に残っていることを確認します。オブジェクトメタデータが許容されるメタデータスペースの 100% を超える前に、各サイトに新しいストレージノードを追加する必要があります。

タスクの内容

StorageGRID は、冗長性を確保し、オブジェクトメタデータを損失から保護するために、各サイトでオブジェクトメタデータのコピーを 3 つ保持します。3 つのコピーは、各ストレージノードのストレージボリューム

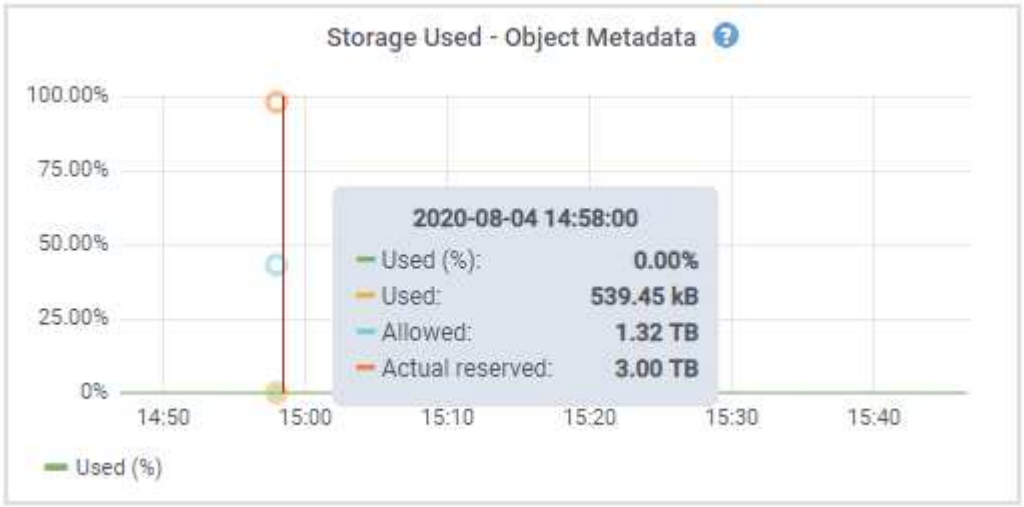
0 でメタデータ用にリザーブされたスペースを使用して、各サイトのすべてのストレージノードに均等に分散されます。

場合によっては、グリッドのオブジェクトメタデータ容量がオブジェクトのストレージ容量よりも早く消費されることがあります。たとえば、一般に大量の小さいオブジェクトを取り込む場合は、オブジェクトストレージの容量が十分に残っている場合でも、ストレージノードを追加してメタデータ容量を増やす必要があります。

メタデータの使用量を増やすことができる要因には、ユーザのメタデータとタグのサイズと数、マルチパートアップロードのパートの合計数、 ILM のストレージの場所に対する変更の頻度などがあります。

手順

1. ノード > ストレージ ノード > ストレージ を選択します。
2. [Storage Used - object metadata]グラフにカーソルを合わせると、その時点の値が表示されます。



使用済み（%）

このストレージノードで使用されている使用可能なメタデータスペースの割合。

Prometheus指標： `storagegrid_storage_utilization_metadata_bytes`および `storagegrid_storage_utilization_metadata_allowed_bytes`

使用済み

このストレージノードで使用されている使用可能なメタデータスペースのバイト数。

Prometheus指標： `storagegrid_storage_utilization_metadata_bytes`

許可

このストレージノードでオブジェクトメタデータに使用できるスペース。この値がストレージノードごとにどのように異なるかについては、を参照して"使用可能なメタデータスペースの完全な概要"ください。

Prometheus指標： `storagegrid_storage_utilization_metadata_allowed_bytes`

実際の予約

このストレージノードでメタデータ用にリザーブされている実際のスペース。使用可能なスペースと

重要なメタデータ処理に必要なスペースが含まれます。各ストレージノードのこの値の計算方法については、を参照してください"メタデータ用に実際にリザーブされているスペースのフル概要"。

*Prometheus*指標は今後のリリースで追加される予定です。

サイトまたはグリッドの合計値には、オフラインのノードなど、指標が5分以上報告されていないノードは含まれません。

3. Used （％） * 値が 70% 以上の場合は、各サイトにストレージノードを追加して StorageGRID システムを拡張します。

Low metadata storage * アラートは、「 Used （％）」の値が特定のしきい値に達するとトリガーされます。オブジェクトメタデータの使用スペースが使用可能なスペースの 100% を超えている場合、望ましくない結果が生じる可能性があります。

新しいノードを追加すると、サイト内のすべてのストレージノード間でオブジェクトメタデータが自動的にリバランシングされます。を参照してください"StorageGRID システムの拡張手順"。

スペース使用量の予測を監視します

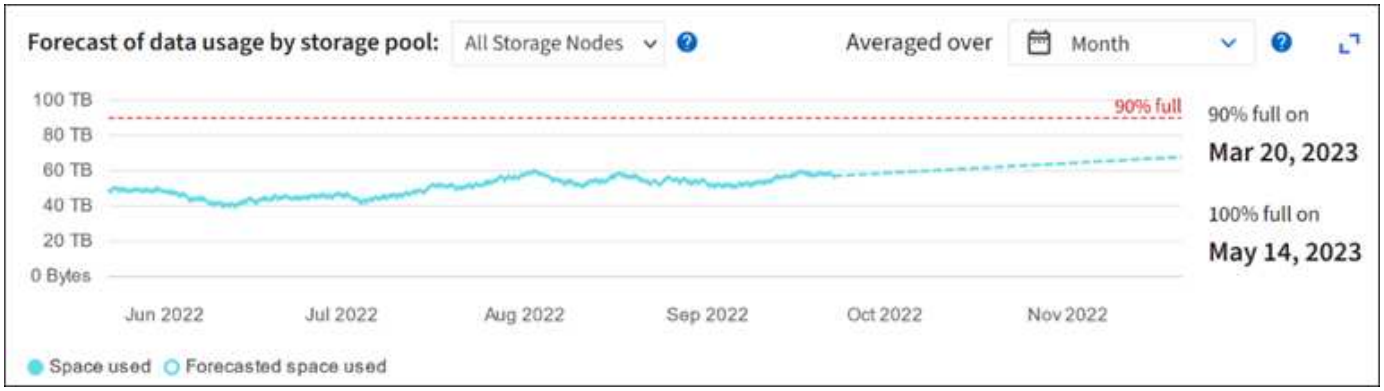
ユーザデータとメタデータのスペース使用量予測を監視して、必要なタイミングを予測し"グリッドを展開する"ます。

時間の経過とともに消費率が変化する場合は、[* Averaged Over *]プルダウンから短い範囲を選択して、最新の取り込みパターンのみを反映します。季節的なパターンに気付いた場合は、より長い範囲を選択してください。

StorageGRID を新規にインストールした場合は、スペース使用量の予測を評価する前に、データとメタデータが蓄積されていることを確認してください。

手順

1. ダッシュボードで、*[ストレージ]*を選択します。
2. ダッシュボードカード、ストレージプール別のデータ使用量の予測、サイト別のメタデータ使用量の予測を表示します。
3. 以下の値を使用して、データとメタデータのストレージ用に新しいストレージノードをいつ追加する必要があるかを見積もります。



StorageGRIDで情報ライフサイクル管理を監視

Information Lifecycle Management （ ILM ；情報ライフサイクル管理）システムは、グリッドに格納されているすべてのオブジェクトのデータ管理を提供します。グリッドが現在の負荷に対応できるかどうか、またはリソースの追加が必要かどうかを判断するには、ILM処理を監視する必要があります。

タスクの内容

StorageGRIDシステムは、アクティブなILMポリシーを適用することでオブジェクトを管理します。ILMポリシーと関連するILMルールによって、作成するコピーの数、作成するコピーのタイプ、配置場所、各コピーの保持期間が決まります。

オブジェクトの取り込みやその他のオブジェクト関連アクティビティは、StorageGRID によるILMの評価速度を超える可能性があります。そのため、ILMの配置手順をほぼリアルタイムで実行できないオブジェクトがキューに登録されます。StorageGRIDがクライアント操作に対応しているかどうかを監視する必要があります。

Grid Managerのダッシュボードタブを使用する

手順

Grid Managerのダッシュボードの[ILM]タブを使用して、ILMの処理を監視します。

1. Grid Manager にサインインします。
2. ダッシュボードで[ILM]タブを選択し、ILMキュー（オブジェクト）カードとILM評価レートカードの値をメモします。

   ダッシュボードのILMキュー（オブジェクト）カードが一時的に急増することが想定されます。ただし、キューが増え続けて減少することがない場合、グリッドが効率的に動作するには、ストレージノードを追加するか、ILMポリシーにオブジェクトがリモートサイトに配置されている場合はネットワーク帯域幅を増やす必要があります。

ノードページを使用する

手順

さらに、[ノード] ページを使用して ILM キューを調査します。

> ノード ページのチャートは、将来のStorageGRIDリリースで対応するダッシュボード カードに置き換えられます。

1. *ノード*を選択します。
2. ***grid name***>*ilm * を選択します。
3. ILMキューのグラフにカーソルを合わせると、ある時点における次の属性の値が表示されます。

   - * Objects queued （ from client operations ） * ：クライアント処理（取り込みなど）のために ILM による評価を待機しているオブジェクトの総数。
   - * Objects queued （ from all operations ） * ： ILM による評価を待機しているオブジェクトの総数。
   - * Scan rate （ objects/sec ） * ：グリッドのオブジェクトがスキャンされて ILM のキューに登録される速度。

- * 評価速度（オブジェクト数 / 秒） * ：グリッド内の ILM ポリシーに照らしてオブジェクトが評価されている現在の速度。

[ILM queue]セクションはグリッド専用です。この情報は、サイトまたはストレージノードの ILM タブには表示されません。

4. ILM キューセクションで、次の属性を確認します。
   - * Scan Period - Estimated *：ILMによるすべてのオブジェクトのフルスキャンが完了するまでの推定時間。

     フルスキャンが完了しても、 ILM がすべてのオブジェクトに適用されるとは限りません。

   - * Repairs Attempted *：レプリケートデータに対して試行されたオブジェクト修復処理の総数。この数は、ストレージノードがハイリスクオブジェクトの修復を試みるたびに増分します。グリッドがビジー状態になった場合は、リスクの高い ILM の修復が優先されます。

     修復後にレプリケーションが失敗した場合、同じオブジェクトの修復が再度増加する可能性があります。 + これらの属性は、ストレージ ノード ボリュームのリカバリの進行状況を監視するときに役立ちます。修復の試行回数の増加が止まり、完全スキャンが完了した場合、修復は完了したと考えられます。

5. あるいは、Prometheusクエリを送信して `storagegrid_ilm_scan_period_estimated_minutes`そして `storagegrid_ilm_repairs_attempted`。

StorageGRID でネットワークとシステムリソースを監視

効率的な運用には、ノードとサイト間のネットワークの整合性と帯域幅、および個 々 のグリッドノードによるリソース使用量が不可欠です。

ネットワーク接続とパフォーマンスを監視します

ネットワーク接続と帯域幅は、情報ライフサイクル管理（ ILM ）ポリシーでサイト間のレプリケートオブジェクトをコピーする場合や、サイト障害からの保護を提供するスキームを使用してイレイジャーコーディングオブジェクトを格納する場合に特に重要になります。サイト間のネットワークを使用できない場合、ネットワークレイテンシが高すぎる場合、またはネットワーク帯域幅が不十分な場合、一部の ILM ルールでオブジェクトが想定どおりに配置されない可能性があります。その結果、取り込みが失敗したり（ILMルールでStrict取り込みオプションが選択されている場合）、取り込みパフォーマンスの低下やILMバックログが発生する可能性があります。

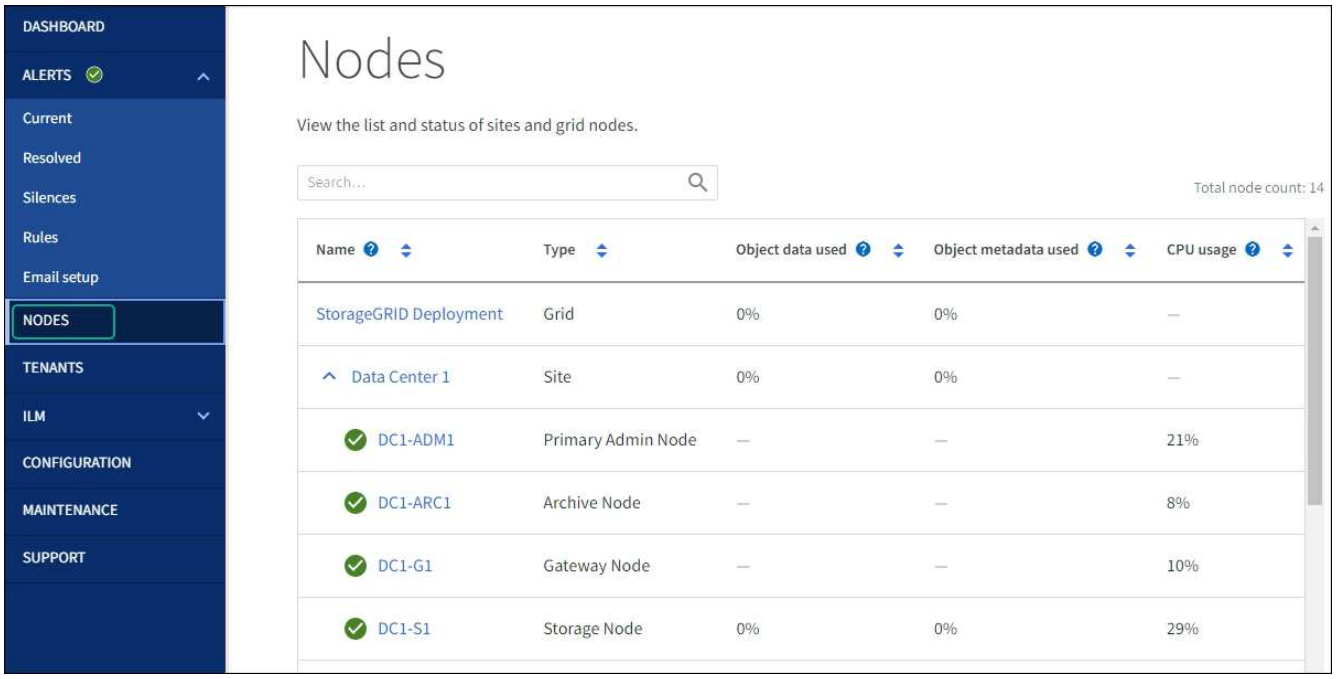
Grid Managerを使用して接続とネットワークのパフォーマンスを監視し、問題に迅速に対処できます。

また、特定のテナント、バケット、サブネット、またはロードバランサエンドポイントに関連するトラフィックを監視できるようにすることを検討してください"ネットワークトラフィック分類ポリシーの作成"。必要に応じて、トラフィック制限ポリシーを設定できます。

手順

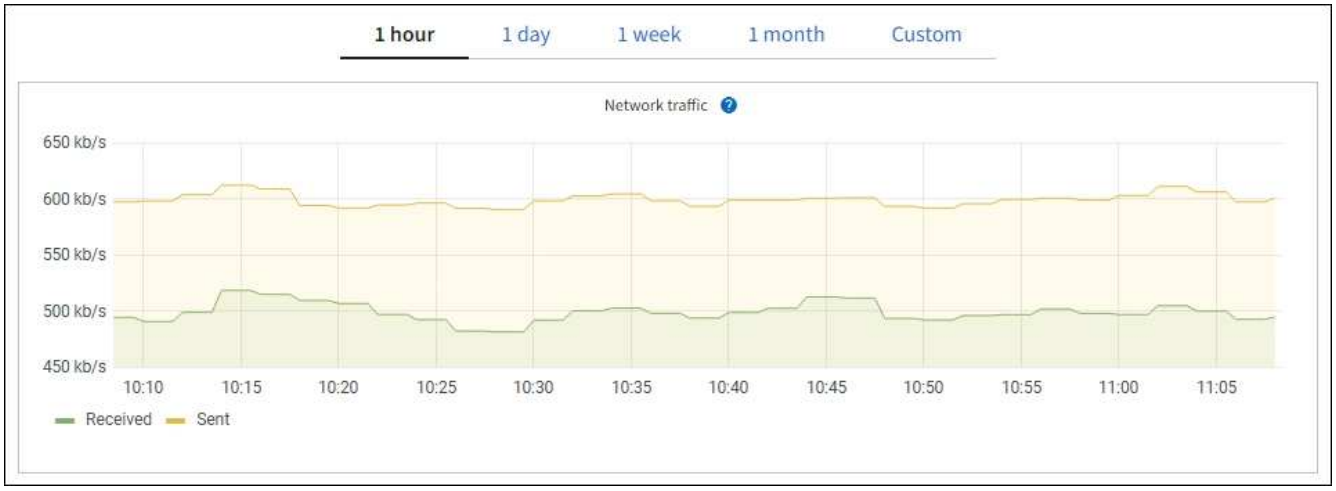
1. *ノード*を選択します。

   Nodes ページが表示されます。グリッド内の各ノードが表形式で表示されます。

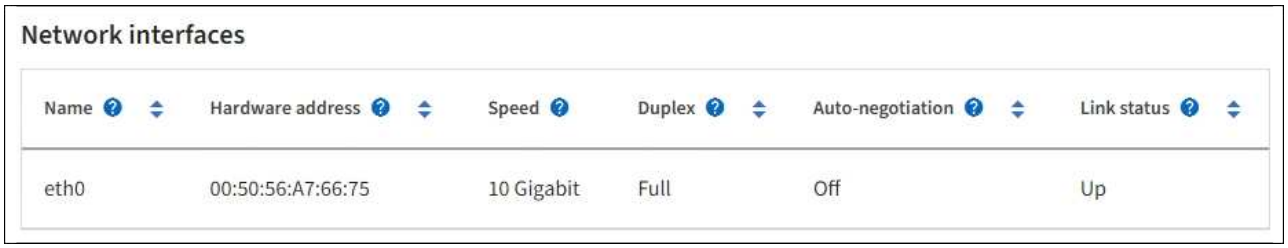


2. グリッド名、特定のデータセンターサイト、またはグリッドノードを選択し、 * ネットワーク * タブを選択します。

   このネットワークトラフィックのグラフには、グリッド全体、データセンターサイト、またはノードのネットワークトラフィックの概要が表示されます。



   a. グリッドノードを選択した場合は、ページの「 * ネットワークインターフェイス * 」セクションまでスクロールします。



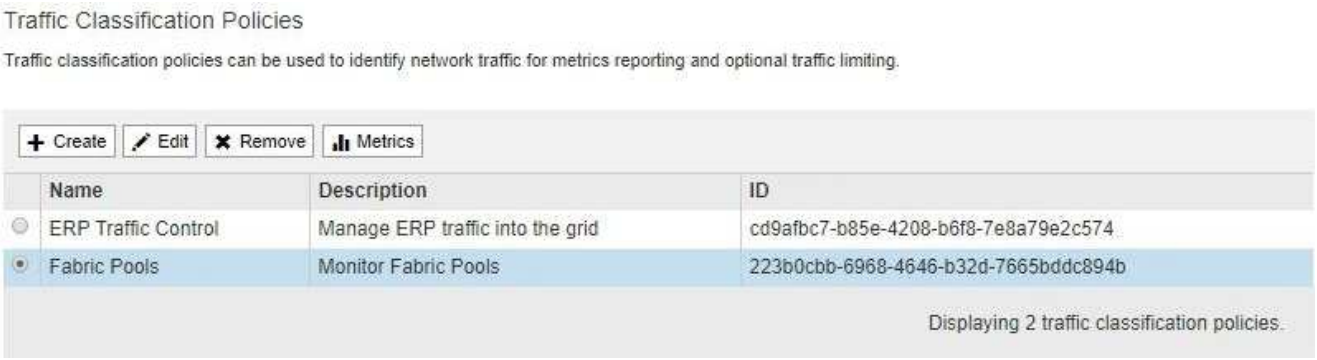
   b. グリッドノードがある場合は、下にスクロールしてページの「 * ネットワーク通信 * 」セクションを確認します。

受信および送信テーブルには、各ネットワークで送受信されたバイト数とパケット数、およびその他の受信および送信メトリックが表示されます。

3. トラフィック分類ポリシーに関連付けられたメトリックを使用して、ネットワークトラフィックを監視します。

   a. 構成 > ネットワーク > *トラフィック分類*を選択します。

      [Traffic Classification Policies] ページが表示され、既存のポリシーがテーブルにリストされます。



   a. ポリシーに関連付けられたネットワークメトリックを示すグラフを表示するには、ポリシーの左側にあるラジオボタンを選択し、次に*Metrics*を選択します。

   b. グラフを確認して、ポリシーに関連付けられているネットワークトラフィックを把握します。

      トラフィック分類ポリシーがネットワークトラフィックを制限するように設計されている場合は、トラフィックが制限される頻度を分析し、ポリシーがニーズを満たし続けるかどうかを判断します。時々、"必要に応じて、各トラフィック分類ポリシーを調整します"。

関連情報

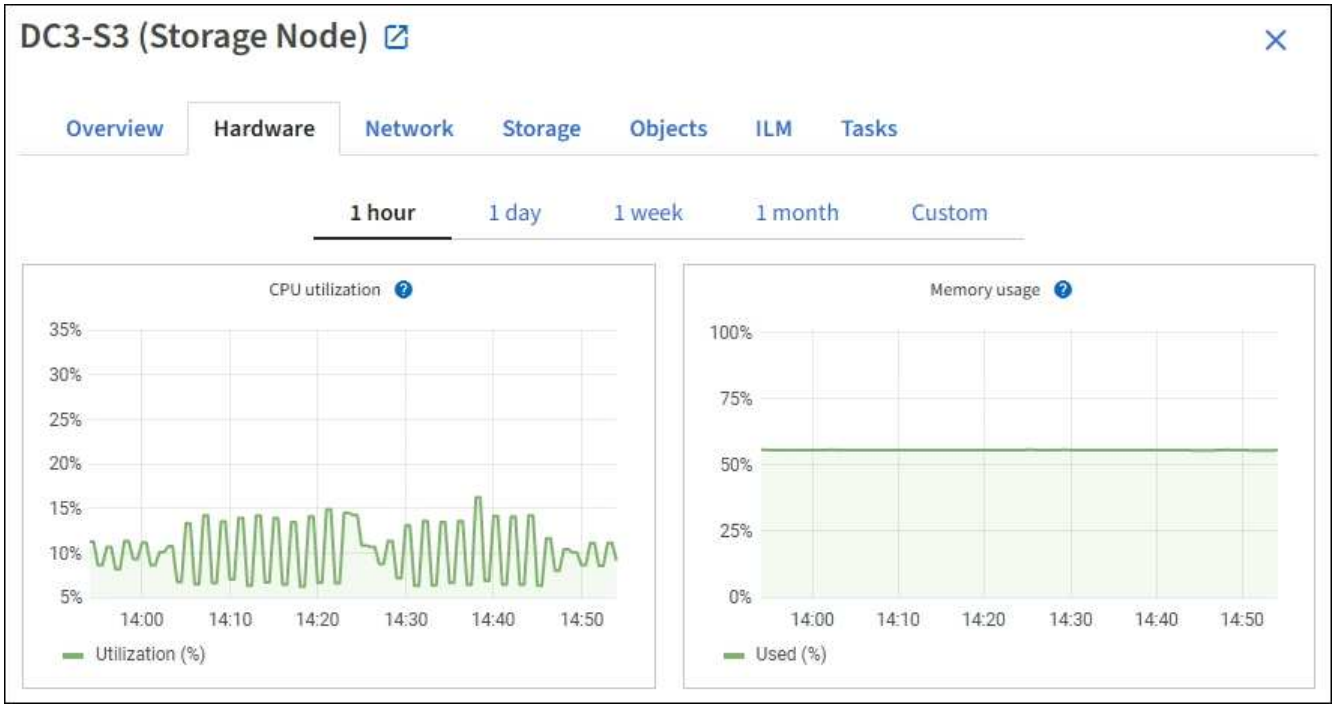
- "[ネットワーク タブを表示します"]
- "ノードの接続状態を監視します"

ノードレベルのリソースを監視

個 々 のグリッドノードを監視して、リソースの使用量レベルを確認します。ノードが常に過負荷状態になっていると、効率的な処理に必要なノードの数が増えます。

手順

1. ノード ページからノードを選択します。
2. [**Hardware**] タブを選択して、 CPU 使用率とメモリ使用率のグラフを表示します。



3. 別の期間を表示するには、グラフまたはグラフの上にあるコントロールのいずれかを選択します。1 時間、 1 日、 1 週間、または 1 カ月の期間の情報を表示できます。また、カスタムの間隔を設定して、日時の範囲を指定することもできます。
4. ノードがストレージアプライアンスまたはサービスアプライアンスでホストされている場合は、下にスクロールしてコンポーネントの表を表示します。すべてのコンポーネントのステータスが「Nominal（公称）」になっている必要があります。その他のステータスのコンポーネントを調査します。

関連情報

- "アプライアンスストレージノードに関する情報を表示します"
- "アプライアンスの管理ノードとゲートウェイノードに関する情報を表示します"

StorageGRID でテナントのアクティビティを監視する

S3クライアントアクティビティはすべてStorageGRIDテナントアカウントに関連付けられます。Grid Managerを使用して、すべてのテナントまたは特定のテナントのストレージ使用量またはネットワークトラフィックを監視できます。監査ログまたはGrafanaダッシュボードを使用して、テナントによるStorageGRID の使用状況に関する詳細情報を収集できます。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"rootアクセスまたはテナントアカウントの権限"。

すべてのテナントを表示します

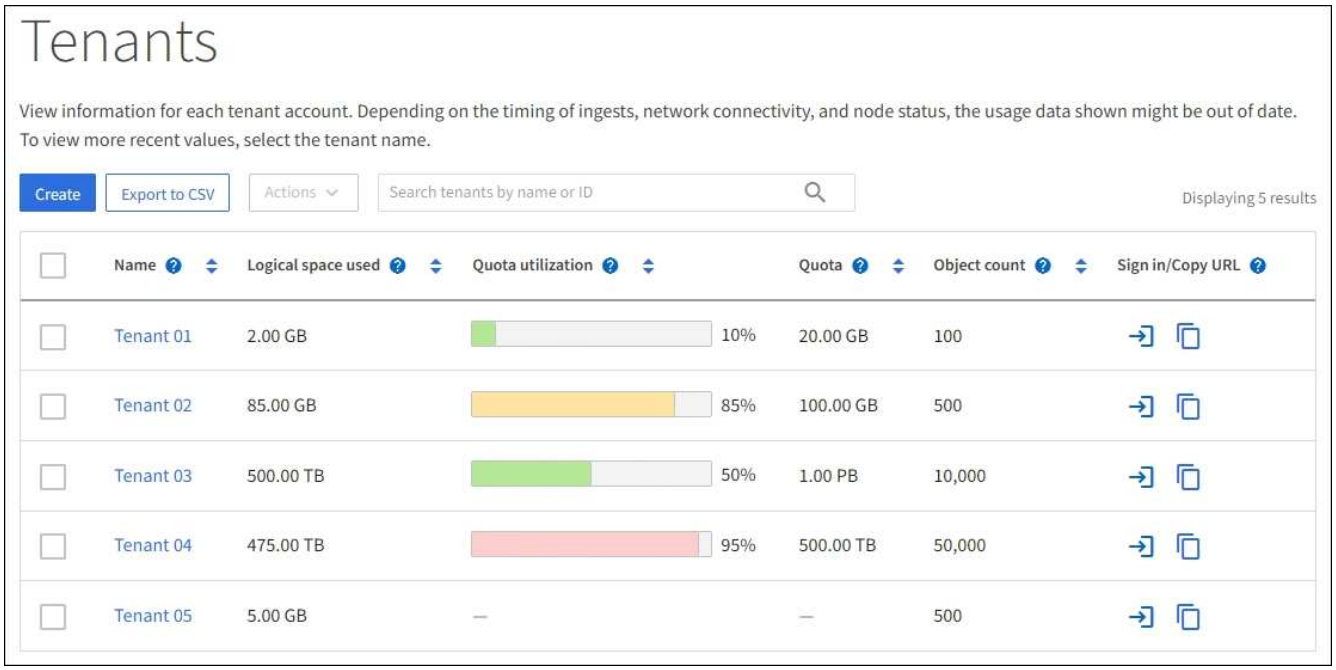
[Tenants]ページには、現在のすべてのテナントアカウントの基本情報が表示されます。

手順

1. *テナント*を選択します。
2. [Tenant]ページに表示される情報を確認します。

   テナントごとに、使用済みの論理スペース、クォータ使用量、クォータ、およびオブジェクト数が表示されます。テナントにクォータが設定されていない場合は、[クォータ使用量]フィールドと[クォータ]フィールドにダッシュ（—）が表示されます。

   > このテナントに属するすべてのオブジェクトの論理サイズには、未完了および進行中のマルチパートアップロードが含まれます。このサイズには、ILM ポリシーに使用される追加の物理スペースは含まれません。使用済みスペースの値は推定値です。これらの見積りは、取り込みのタイミング、ネットワーク接続、およびノードの状態によって影響を受けます。



3. 必要に応じて、**Sign in/Copy URL** 列のサインインリンク を選択して、テナントアカウントにサインインします。
4. 必要に応じて、**Sign in/Copy URL** 列のURLコピーリンク を選択して、テナントのサインインページのURLをコピーします。
5. 必要に応じて、*[CSVにエクスポート]*を選択して、すべてのテナントの使用状況の値を含むファイルを表示およびエクスポートし `.csv`ます。

   ファイルを開くか保存するかを確認するメッセージが表示されます `.csv`。

   ファイルの内容は `.csv`次の例のようになります。

Tenant ID	Display Name	Space Used (Bytes)	Quota utilization (%)	Quota (Bytes)	Object Count	Protocol
12659822378459233654	Tenant 01	2000000000	10	20000000000	100	S3
99658234112547853685	Tenant 02	85000000000	85	110000000	500	S3
03521145586975586321	Tenant 03	60500000000	50	150000	10000	S3
44251365987569885632	Tenant 04	4750000000	95	140000000	50000	S3
36521587546689565123	Tenant 05	5000000000	Infinity		500	S3

ファイルはスプレッドシートアプリケーションで開くことも、自動化で使用することもできます `.csv`。

6. オブジェクトが表示されない場合は、必要に応じて*>[削除]*を選択してテナントを削除します。を参照して "テナントアカウントを削除する"

   バケットまたはコンテナが含まれているテナントアカウントは削除できません。

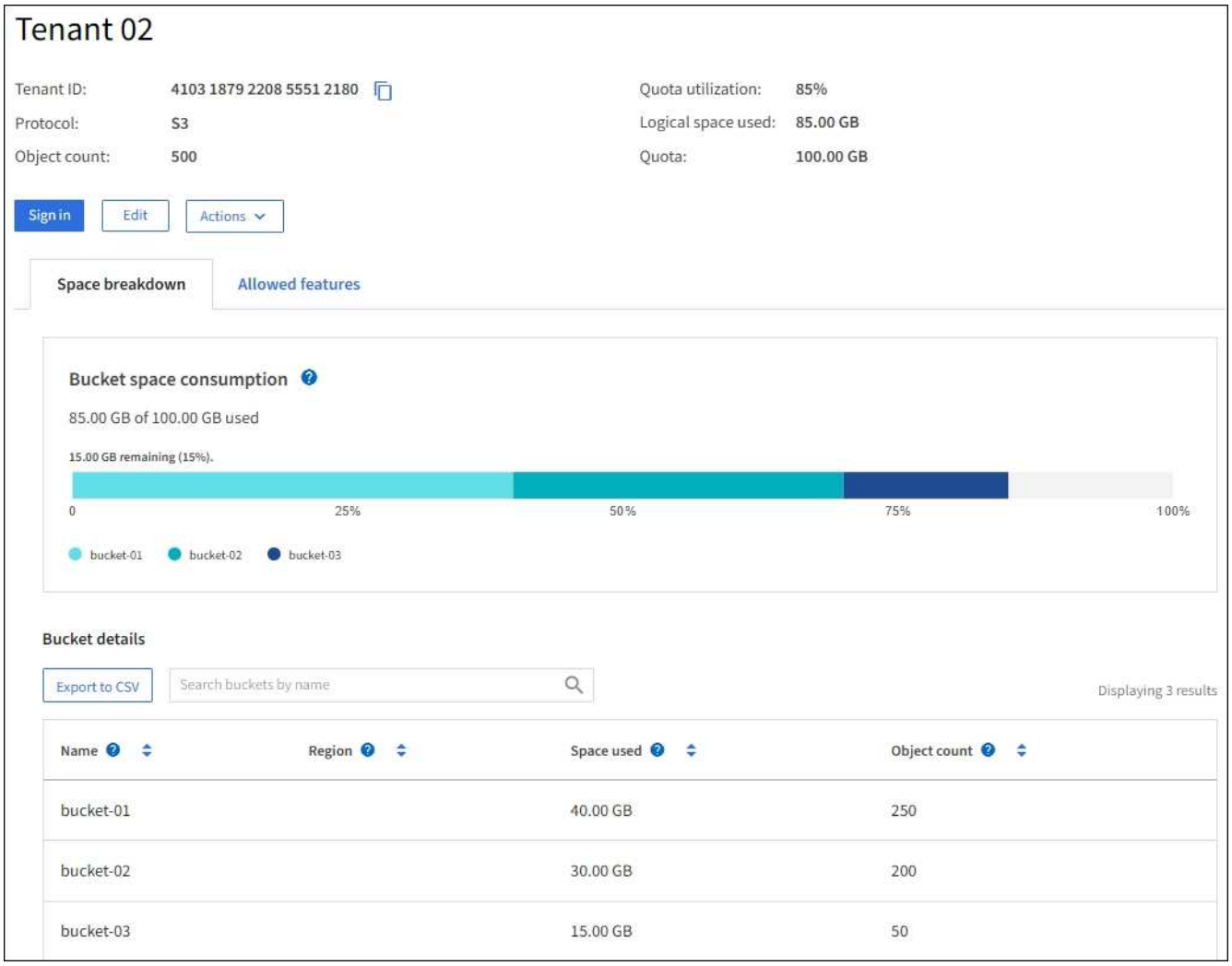
特定のテナントを表示します

特定のテナントの詳細を表示できます。

手順

1. [Tenants]ページでテナント名を選択します。

   テナントの詳細ページが表示されます。



2. ページ上部のテナントの概要を確認します。

   詳細ページのこのセクションには、テナントのオブジェクト数、クォータ使用量、使用済み論理スペース、クォータの設定など、テナントの概要情報が表示されます。

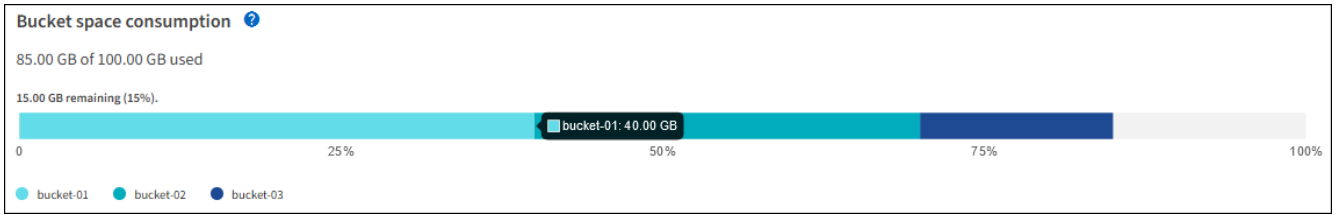
このテナントに属するすべてのオブジェクトの論理サイズには、未完了および進行中のマルチパートアップロードが含まれます。このサイズには、ILM ポリシーに使用される追加の物理スペースは含まれません。使用済みスペースの値は推定値です。これらの見積りは、取り込みのタイミング、ネットワーク接続、およびノードの状態によって影響を受けます。

3. [スペースの内訳]タブで、*[スペースの消費]*グラフを確認します。

   このグラフには、テナントのすべてのS3バケットの合計スペース消費量が表示されます。

   このテナントにクォータが設定されている場合は、クォータの使用済み容量と残り容量がテキストで表示されます（例： `85.00 GB of 100 GB used`）。クォータが設定されていない場合、テナントのクォータは無制限で、テキストには使用済みスペースの量（など）のみが含まれます `85.00 GB used`。棒グラフは、各バケットまたはコンテナのクォータの割合を示します。テナントがストレージクォータを 1% 以上かつ 1GB 以上超過した場合は、クォータの総容量と超過容量がグラフに表示されます。

   棒グラフにカーソルを合わせると、各バケットまたはコンテナで使用されるストレージを確認できます。空きスペースセグメントにカーソルを合わせると、残りのストレージクォータを確認できます。



クォータ使用量は内部の見積もりに基づいており、場合によっては超過する可能性があります。たとえば、テナントがクォータを超えた場合、 StorageGRID はテナントがオブジェクトのアップロードを開始したときにクォータをチェックし、新しい取り込みを拒否します。ただし、 StorageGRID では、クォータを超過したかどうかを判断する際に、現在のアップロードのサイズは考慮されません。オブジェクトが削除されると、クォータ使用量が再計算されるまでテナントが新しいオブジェクトを一時的にアップロードできなくなることがあります。クォータ使用量の計算には10分以上かかることがあります。

テナントのクォータ使用量は、テナントがStorageGRIDにアップロードしたオブジェクトデータの総容量（論理サイズ）を示します。クォータ使用量は、それらのオブジェクトのコピーとメタデータの格納に使用されているスペース（物理サイズ）ではありません。

「* Tenant quota usage high *」アラートルールを有効にすると、テナントがクォータを消費しているかどうかを確認できます。有効にすると、テナントのクォータの 90% が使用されたときにこのアラートがトリガーされます。手順については、を参照してください"アラートルールを編集"。

4. タブで、[Bucket details（バケットの詳細）]*を確認します。

   次の表に、テナントのS3バケットを示します。使用済みスペースは、バケットまたはコンテナ内のオブジェクトデータの総容量です。この値は、 ILM コピーとオブジェクトメタデータに必要なストレージスペースを表しているわけではありません。

5. 必要に応じて、「 * Export to CSV * 」を選択し、各バケットまたはコンテナの使用量の値を含む .csv ファイルを表示してエクスポートします。

個 々 のS3テナントのファイルの内容は `.csv`次の例のようになります。

Tenant ID	Bucket Name	Space Used (Bytes)	Number of Objects
64796966429038923647	bucket-01	88717711	14
64796966429038923647	bucket-02	21747507	11
64796966429038923647	bucket-03	15294070	3

ファイルはスプレッドシートアプリケーションで開くことも、自動化で使用することもできます `.csv`。

6. 必要に応じて、* Allowed features *タブを選択して、テナントに対して有効になっている権限と機能のリストを表示します。これらの設定のいずれかを変更する必要があるかどうかを確認します"テナントアカウントを編集します"。
7. テナントに* Use grid federation connection 権限がある場合は、必要に応じて Grid federation *タブを選択して接続の詳細を確認します。

   およびを参照してください"グリッドフェデレーションとは""グリッドフェデレーションに許可されたテナントを管理します"。

ネットワークトラフィックを表示します

テナントにトラフィック分類ポリシーが設定されている場合は、そのテナントのネットワークトラフィックを確認します。

手順

1. 構成 > ネットワーク > *トラフィック分類*を選択します。

   [Traffic Classification Policies] ページが表示され、既存のポリシーがテーブルにリストされます。

2. ポリシーのリストを確認して、特定のテナントに適用されるポリシーを特定します。
3. ポリシーに関連付けられている指標を表示するには、ポリシーの左側にあるラジオボタンを選択し、*[Metrics]*を選択します。
4. グラフを分析して、ポリシーがトラフィックを制限している頻度と、ポリシーを調整する必要があるかどうかを判断します。

詳細については、を参照してください "トラフィック分類ポリシーを管理します" 。

監査ログを使用します

必要に応じて、監査ログを使用してテナントのアクティビティをより詳細に監視できます。

たとえば、次の種類の情報を監視できます。

- PUT 、 GET 、 DELETE など、特定のクライアント処理
- オブジェクトサイズ
- オブジェクトに適用されている ILM ルール
- クライアント要求の送信元 IP

監査ログは、選択したログ分析ツールを使用して分析可能なテキストファイルに書き込まれます。これによ

り、クライアントアクティビティをよりよく理解したり、高度なチャージバックおよび課金モデルを実装したりできます。

詳細については、を参照してください "監査ログを確認します" 。

Prometheus指標を使用

必要に応じて、Prometheus指標を使用してテナントアクティビティをレポートします。

- グリッド マネージャーで、[サポート] > [ツール] > [メトリック] を選択します。 S3 概要などの既存のダッシュボードを使用して、クライアントのアクティビティを確認できます。

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

- Grid Managerの上部でヘルプアイコンを選択し、*[API documentation]*を選択します。グリッド管理 API の指標セクションの指標を使用して、テナントアクティビティ用のカスタムのアラートルールとダッシュボードを作成できます。

詳細については、を参照してください "サポート指標を確認" 。

StorageGRIDでS3クライアント操作を監視する

オブジェクトの取り込み速度と読み出し速度、およびオブジェクト数、クエリ、検証関連の指標を監視できます。StorageGRID システムのオブジェクトに対してクライアントアプリケーションが試みた読み取り、書き込み、変更の各処理について、成功した回数と失敗した回数を表示できます。

開始する前に

Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。

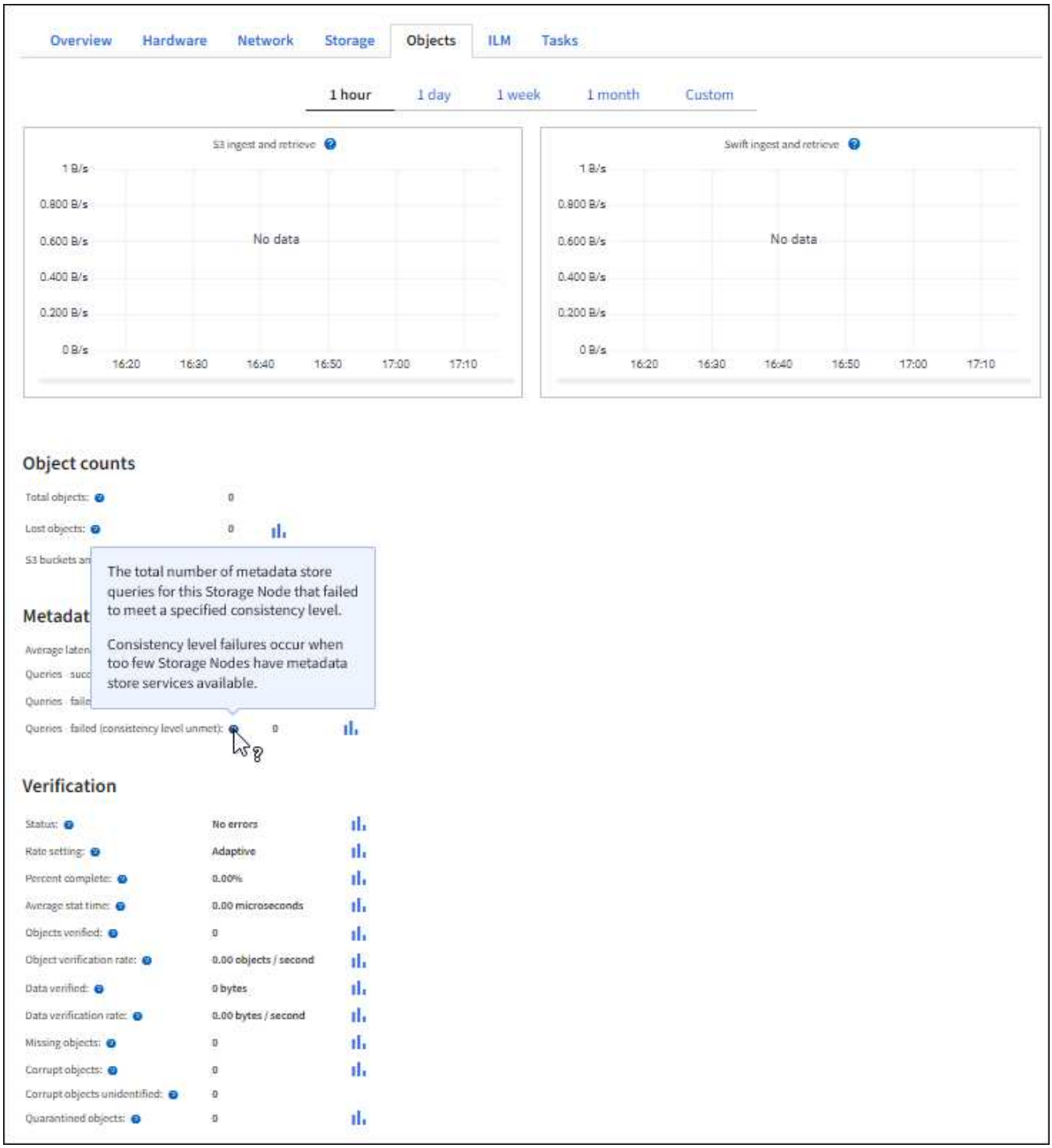
手順

1. ダッシュボードで、*[パフォーマンス]*タブを選択します。
2. S3のグラフを参照してください。このグラフには、選択した期間にストレージノードで実行されたクライアント処理の数と、ストレージノードが受信したAPI要求の数がまとめられています。
3. ノード を選択して、ノード ページにアクセスします。
4. [Nodes]ホームページ（グリッドレベル）で、*[Objects]*タブを選択します。

   グラフには、StorageGRIDシステム全体のS3の取り込み速度と読み出し速度（1秒あたりのバイト数）、および取り込みまたは読み出したデータの量が表示されます。時間間隔を選択するか、カスタムの間隔を適用できます。

5. 特定のストレージノードの情報を表示するには、左側のリストからノードを選択し、*[オブジェクト]*タブを選択します。

   グラフには、ノードの取り込み速度と読み出し速度が表示されます。このタブには、オブジェクト数、メタデータクエリ、および検証処理の指標も表示されます。



StorageGRID でロード バランシング操作を監視

ロードバランサを使用して StorageGRID へのクライアント接続を管理している場合は、システムを最初に設定したあとと、設定を変更したり拡張を行ったあとに、ロードバランシング処理を監視する必要があります。

タスクの内容

管理ノードまたはゲートウェイノード上のロードバランササービス、または外部の他社製ロードバランサを使用して、複数のストレージノードにクライアント要求を分散できます。

ロードバランシングを設定したら、オブジェクトの取り込みと読み出しの処理がストレージノード間で均等に分散されていることを確認する必要があります。要求が均等に分散されるため、 StorageGRID は負荷がかかっているクライアント要求への応答性を維持し、クライアントのパフォーマンスを維持できます。

ゲートウェイノードまたは管理ノードのハイアベイラビリティ（ HA ）グループをアクティブ / バックアップモードで設定した場合、グループ内の 1 つのノードだけがクライアント要求をアクティブに分散します。

詳細については、を参照してください "S3クライアント接続の設定"。

手順

1. S3クライアントがロードバランササービスを使用して接続する場合は、管理ノードまたはゲートウェイノードが想定どおりにトラフィックをアクティブに分散していることを確認します。
   a. *ノード*を選択します。
   b. ゲートウェイノードまたは管理ノードを選択します。
   c. [概要]*タブで、ノードインターフェイスがHAグループに含まれているかどうか、およびノードインターフェイスのロールがプライマリであるかどうかを確認します。

      プライマリの役割を持つノードとHAグループに属していないノードは、クライアントに要求をアクティブに分散している必要があります。

   d. クライアント要求をアクティブに分散する必要がある各ノードについて、を選択します"[Load Balancerタブ"]。
   e. 過去 1 週間のロードバランサ要求トラフィックのチャートを確認して、ノードが要求をアクティブに分散していることを確認します。

      アクティブ / バックアップ HA グループのノードでは、 Backup ロールが随時割り当てられる場合があります。この間、ノードはクライアント要求を分散しません。

   f. ノードのオブジェクトスループットを確認するには、過去 1 週間のロードバランサの受信要求速度のグラフを確認します。
   g. StorageGRID システムの管理ノードまたはゲートウェイノードごとに上記の手順を繰り返します。
   h. 必要に応じて、トラフィック分類ポリシーを使用して、ロードバランササービスで処理されているトラフィックのより詳細な分析を表示します。
2. これらの要求がストレージノードに均等に分散されていることを確認します。
   a. 「 * _ ストレージノード _ * > * LDR * > * HTTP * 」を選択します。
   b. 現在確立されている受信セッション数 * を確認します。
   c. グリッド内のストレージノードごとにこの手順を繰り返します。

      セッションの数はすべてのストレージノードでほぼ同じにします。

StorageGRID グリッド フェデレーション接続を監視

すべての基本情報"グリッドフェデレーション接続"、特定の接続に関する詳細情報、またはクロスグリッドレプリケーション処理に関するPrometheus指標を監視できます。接続はどちらのグリッドからも監視できます。

開始する前に

- いずれかのグリッドで、を使用してGrid Managerにサインインしておき"サポートされている Web ブラウザ"ます。
- サインインしているグリッドのが"rootアクセス権限"必要です。

すべての接続を表示します

[Grid Federation]ページには、すべてのグリッドフェデレーション接続と、グリッドフェデレーション接続の使用が許可されているすべてのテナントアカウントに関する基本的な情報が表示されます。

手順

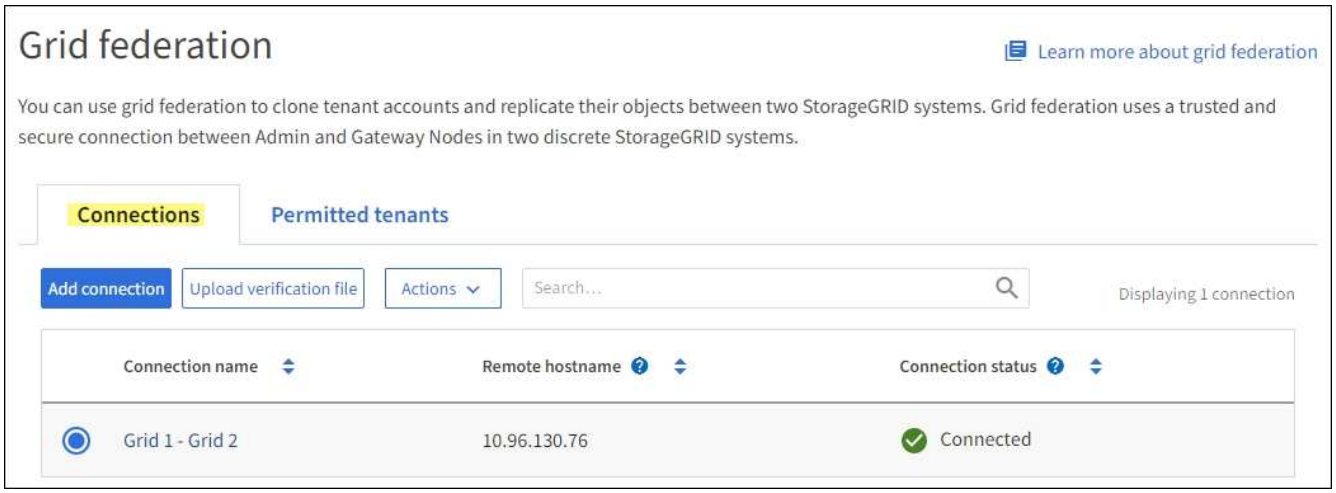
1. 構成 > システム > グリッド フェデレーション を選択します。

   [Grid Federation]ページが表示されます。

2. このグリッド上のすべての接続に関する基本情報を表示するには、*[接続]*タブを選択します。

   このタブでは、次の操作を実行できます。

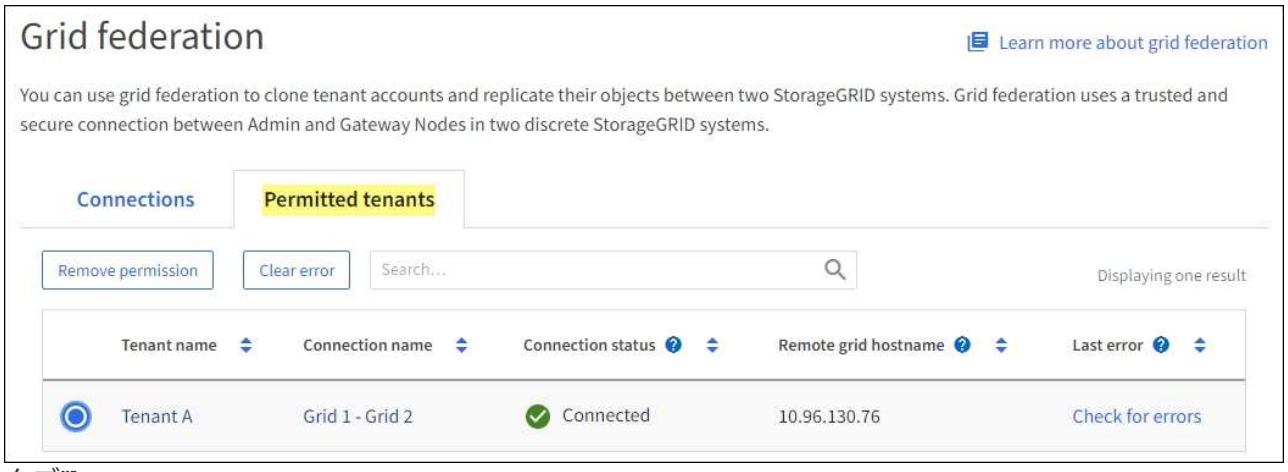
   - "新しい接続を作成します"です。
   - への既存の接続を選択し"編集またはテスト"ます。



3. 権限があるこのグリッド上のすべてのテナントアカウントに関する基本情報を表示するには、[Permitted tenants]*タブを選択します。

   このタブでは、次の操作を実行できます。

   - "許可されている各テナントの詳細ページを表示します"です。
   - 各接続の詳細ページを表示します。を参照して 特定の接続を表示します
   - 許可されているテナントとを選択します"権限を削除します"。
   - グリッド間レプリケーションにエラーがないかどうかを確認し、最後のエラーがある場合はクリアします。を参照して "グリッドフェデレーションエラーをトラブルシューティングする"



タブ"]

特定の接続を表示します

特定のグリッドフェデレーション接続の詳細を表示できます。

手順

1. [Grid Federation]ページでいずれかのタブを選択し、テーブルから接続名を選択します。

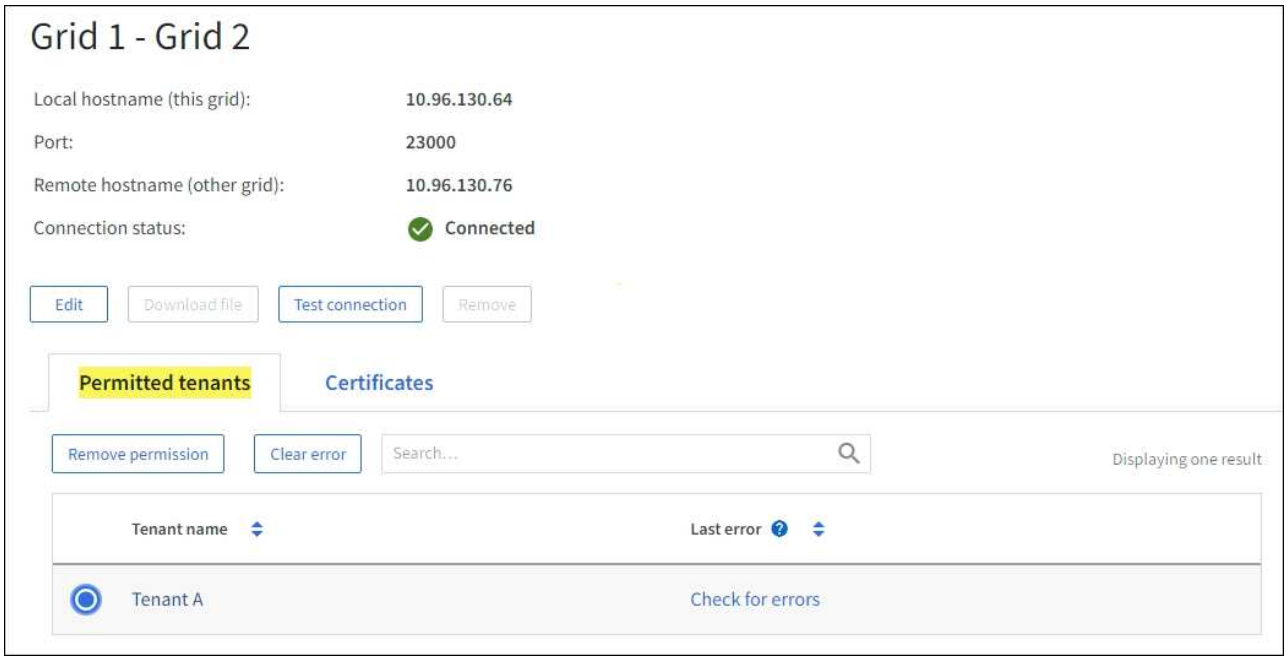
   接続の詳細ページでは、次の操作を実行できます。

   - ローカルおよびリモートのホスト名、ポート、接続ステータスなど、接続に関する基本的なステータス情報を表示します。
   - への接続を選択し"編集、テスト、または削除"ます。

2. 特定の接続を表示しているときに*[Permitted Tenants]*タブを選択すると、その接続で許可されているテナントに関する詳細が表示されます。

   このタブでは、次の操作を実行できます。

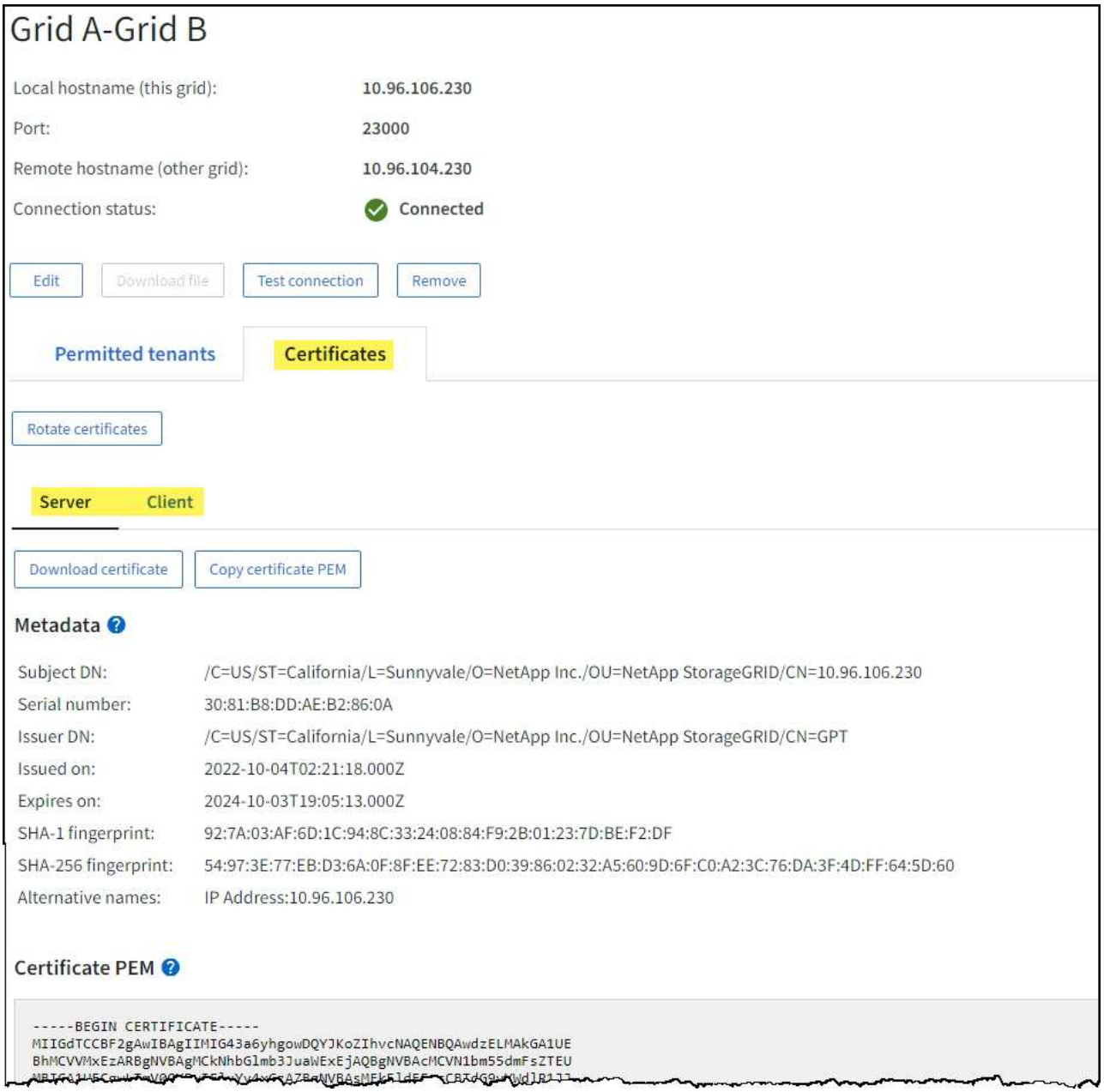
   - "許可されている各テナントの詳細ページを表示します"です。
   - "テナントの権限を削除します"接続を使用します。
   - クロスグリッドレプリケーションエラーがないかどうかを確認し、最後のエラーをクリアします。を参照して "グリッドフェデレーションエラーをトラブルシューティングする"



3. 特定の接続を表示している場合は、*[証明書]*タブを選択して、この接続でシステムによって生成されたサーバ証明書とクライアント証明書を表示します。

   このタブでは、次の操作を実行できます。

   - "接続証明書をローテーションします"です。
   - 関連する証明書を表示またはダウンロードするか、証明書PEMをコピーするには、* Server または Client *を選択します。



グリッド間レプリケーションの指標を確認します

Grafanaの[Cross-Grid Replication]ダッシュボードを使用して、グリッドでのクロスグリッドレプリケーション処理に関するPrometheus指標を表示できます。

手順

1. グリッド マネージャーから、[サポート] > [ツール] > [メトリック] を選択します。

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

2. ページの[Grafana]セクションで、*[Cross Grid Replication]*を選択します。

詳細については、を参照してください"サポート指標を確認"。

3. 複製に失敗したオブジェクトの複製を再試行するには、を参照してください"失敗したレプリケーション処理を特定して再試行します"。

アラートの管理

StorageGRID でアラートを管理する

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

アラートルールの条件が true と評価されると、特定の重大度レベルでアラートがトリガーされます。アラートがトリガーされると、次の処理が行われます。

- Grid Managerのダッシュボードにアラートの重大度アイコンが表示され、現在のアラートの数が増分されます。
- アラートは、ノード 概要ページと ノード > ***node*** > 概要 タブに表示されます。
- SMTP サーバを設定し、受信者に E メールアドレスを提供している場合は、 E メール通知が送信されます。
- StorageGRID SNMP エージェントが設定されている場合は、簡易ネットワーク管理プロトコル（ SNMP ）通知が送信されます。

カスタムアラートの作成、アラートの編集または無効化、アラート通知の管理を行うことができます。

詳細については、以下をご覧ください。

- ビデオをレビューします:

  アラートの概要

  カスタムアラート

- 参照"アラート一覧"。

StorageGRID アラートルールを表示

アラートルールでは、トリガーする条件を定義し"特定のアラート"ます。StorageGRID には一連のデフォルトアラートルールが用意されており、そのまま使用したり変更したりすることができます。また、カスタムのアラートルールを作成することもできます。

デフォルトとカスタムのアラートルールをすべて表示して、各アラートをトリガーする条件を確認したり、アラートが無効になっているかどうかを確認したりできます。

開始する前に

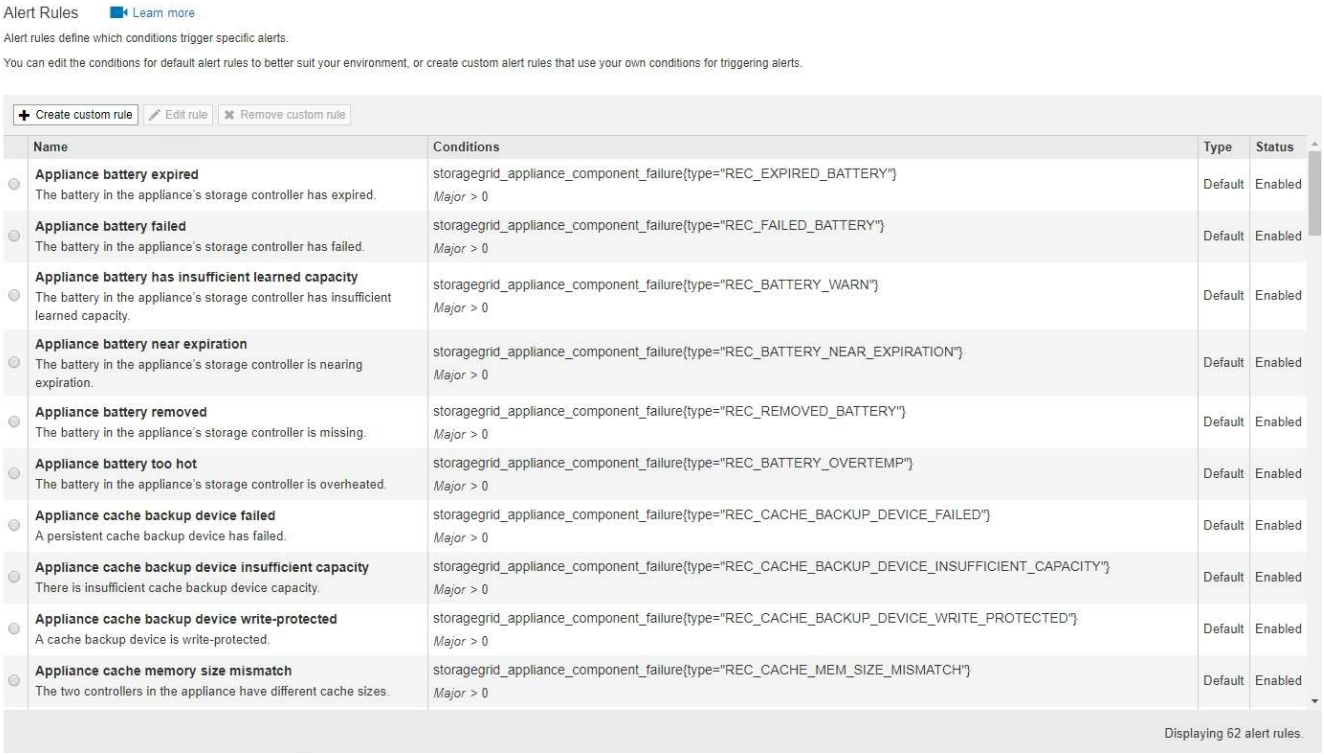
- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"アラートまたはRoot Access権限を管理します。"。
- オプションとして、ビデオを視聴しました:

  アラートの概要

手順

1. アラート > *ルール*を選択します。

   [Alert Rules] ページが表示されます。



2. アラートルールのテーブルの情報を確認します。

列ヘッダー	製品説明
名前	アラートルールの一意の名前と概要 。カスタムのアラートルールが最初に表示され、そのあとにデフォルトのアラートルールが表示されます。アラートルール名は E メール通知の件名となります。

列ヘッダー	製品説明
条件	このアラートがトリガーされるタイミングを決定する Prometheus 式。アラートは次の 1 つ以上の重大度レベルでトリガーできますが、重大度ごとの条件は不要です。 • *致命的*：StorageGRID ノードまたはサービスの通常の動作を停止させる異常な状態が発生しています。根本的な問題に直ちに対処する必要があります。問題が解決されない場合、サービスの中断やデータ損失が発生する可能性があります。 • **Major**：異常な状態が発生しており、現在の運用に影響を与えているか、または重大なアラートの閾値に近づいています。重大なアラートを調査し、根本的な問題に対処して、異常な状態が StorageGRID ノードまたはサービスの正常な動作を停止させないようにする必要があります。 • マイナー：システムは正常に動作していますが、異常な状態が発生しており、この状態が続くとシステムの動作能力に影響を与える可能性があります。自然に解消されない軽微なアラートは監視して解決し、より深刻な問題に発展しないようにする必要があります。
タイプ	アラートルールのタイプ。 • * デフォルト * ：システムに付属のアラートルール。デフォルトのアラートルールは、無効にするか、条件と期間を編集できます。デフォルトのアラートルールは削除できません。 • * デフォルト ** ：条件または期間が編集されたデフォルトのアラートルール。必要に応じて、変更した条件を元のデフォルトに戻すことができます。 • * Custom * ：ユーザが作成したアラートルール。カスタムのアラートルールは、無効化、編集、削除することができます。
ステータス	このアラートルールが現在有効になっているか無効になっているか。無効なアラートルールの条件は評価されないため、アラートはトリガーされません。

StorageGRIDでカスタムアラートルールを作成する

カスタムのアラートルールを作成して、アラートをトリガーする条件を独自に定義することができます。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"アラートまたはRoot Access権限を管理します。"。
- に精通している"よく使用される Prometheus 指標"必要があります。
- を理解する "Prometheus クエリの構文"必要があります。

- オプションとして、ビデオを視聴しました:

  カスタムアラート

タスクの内容

StorageGRID はカスタムアラートを検証しません。カスタムのアラートルールを作成する場合は、次の一般的なガイドラインに従ってください。

- デフォルトのアラートルールの条件を参考に、カスタムのアラートルールを作成します。
- アラートルールに複数の条件を定義する場合は、すべての条件に同じ式を使用します。その後、各条件のしきい値を変更します。
- 各条件に入力ミスやロジックエラーがないか、慎重にチェックしてください。
- Grid 管理 API にリストされている指標のみを使用してください。
- グリッド管理APIを使用して式をテストする場合、「successful」応答は空の応答本文（アラートがトリガーされない）である可能性があることに注意してください。アラートが実際にトリガーされるかどうかを確認するには、現在 true になるしきい値を一時的に設定します。

  たとえば、式をテストするには `node_memory_MemTotal_bytes < 24000000000`、まずを実行し `node_memory_MemTotal_bytes >= 0`、予期した結果が得られることを確認します（すべてのノードが値を返します）。次に、演算子としきい値を目的の値に戻して再実行します。結果がない場合は、この式に対するアラートが現在発生していません。

- アラートが想定どおりにトリガーされることを確認していないかぎり、カスタムアラートが機能しているとは思わないでください。

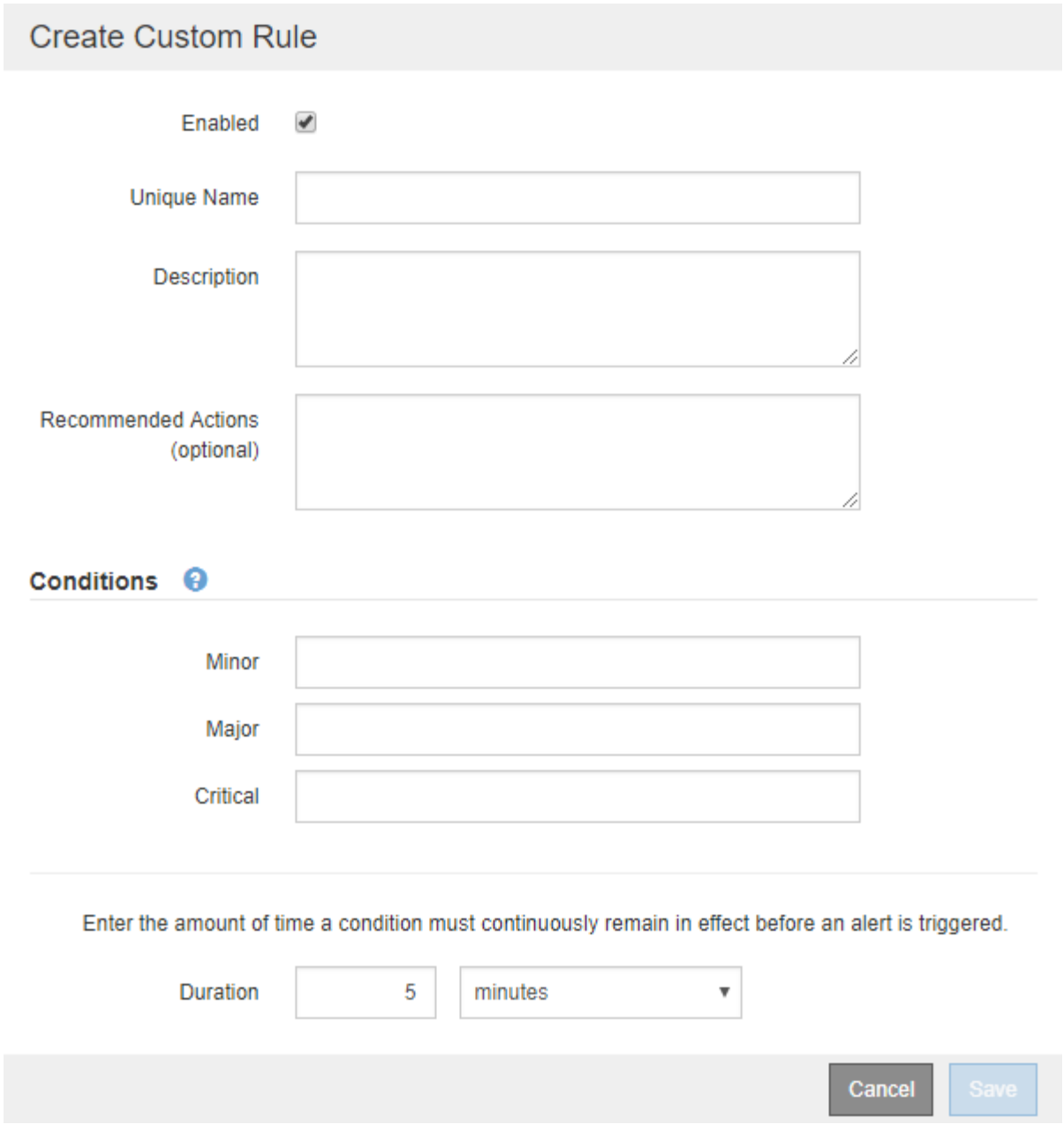
手順

1. アラート > *ルール*を選択します。

   [Alert Rules] ページが表示されます。

2. [* カスタムルールの作成 *] を選択します。

   [Create Custom Rule] ダイアログボックスが表示されます。



3. [有効]*チェックボックスをオンまたはオフにして、このアラートルールが現在有効になっているかどうかを確認します。

   アラートルールを無効にすると、ルールの式は評価されず、アラートはトリガーされません。

4. 次の情報を入力します。

フィールド	製品説明
一意の名前	このルールの一意の名前。アラートルール名は、 [Alerts] ページに表示され、電子メール通知の件名にもなります。アラートルールの名前は 1~64 文字で指定できます。

フィールド	製品説明
製品説明	発生している問題の概要 。概要 は、アラートページおよび E メール通知に表示されるアラートメッセージです。アラートルールの説明は、 1~128 文字で指定できます。
推奨される対処方法	必要に応じて、このアラートがトリガーされたときに実行する推奨される対処方法を指定します。推奨される対処方法をプレーンテキスト（書式コードなし）で入力します。アラートルールの推奨される対処方法は、 0~1 、 024 文字で指定できます。

5. Conditions セクションで、アラートの重大度レベルを 1 つ以上指定する Prometheus 式を入力します。

   基本式は、通常、次の形式で指定します。

   ```
   [metric] [operator] [value]
   ```

   式の文字数に制限はありませんが、ユーザインターフェイスでは 1 行で表示されます。少なくとも 1 つの式が必要です。

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

   ```
   node_memory_MemTotal_bytes < 24000000000
   ```

   利用可能なメトリクスを確認したり、Prometheus 式をテストしたりするには、ヘルプアイコン を選択し、Grid Management API のメトリクスセクションへのリンクをクリックしてください。

6. [* 期間 *] フィールドに、アラートがトリガーされるまでに条件を継続的に有効にしておく必要がある期間を入力し、時間の単位を選択します。

   条件が true になったときにすぐにアラートをトリガーするには、「 * 0 * 」と入力します。一時的な状況でアラートがトリガーされないようにするには、この値を大きくし

   デフォルトは5分です。

7. [保存（ Save ）] を選択します。

   ダイアログボックスが閉じ、新しいカスタムアラートルールがアラートルールテーブルに表示されます。

StorageGRID でアラートルールを編集する

アラートルールを編集してトリガー条件を変更したり、カスタムのアラートルールを使用してルール名、概要 、および推奨される対処方法を更新したりできます。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"アラートまたはRoot Access権限を管理します。"。

タスクの内容

デフォルトのアラートルールを編集する場合は、 Minor 、 Major 、 Critical の各アラートの条件と期間を変更できます。カスタムのアラートルールを編集する際に、ルールの名前、概要 、および推奨される対処方法を編集することもできます。

アラートルールを編集する場合は注意が必要です。トリガー値を変更した場合、重大な処理を完了できなくなるまで、根本的な問題が検出されないことがあります。

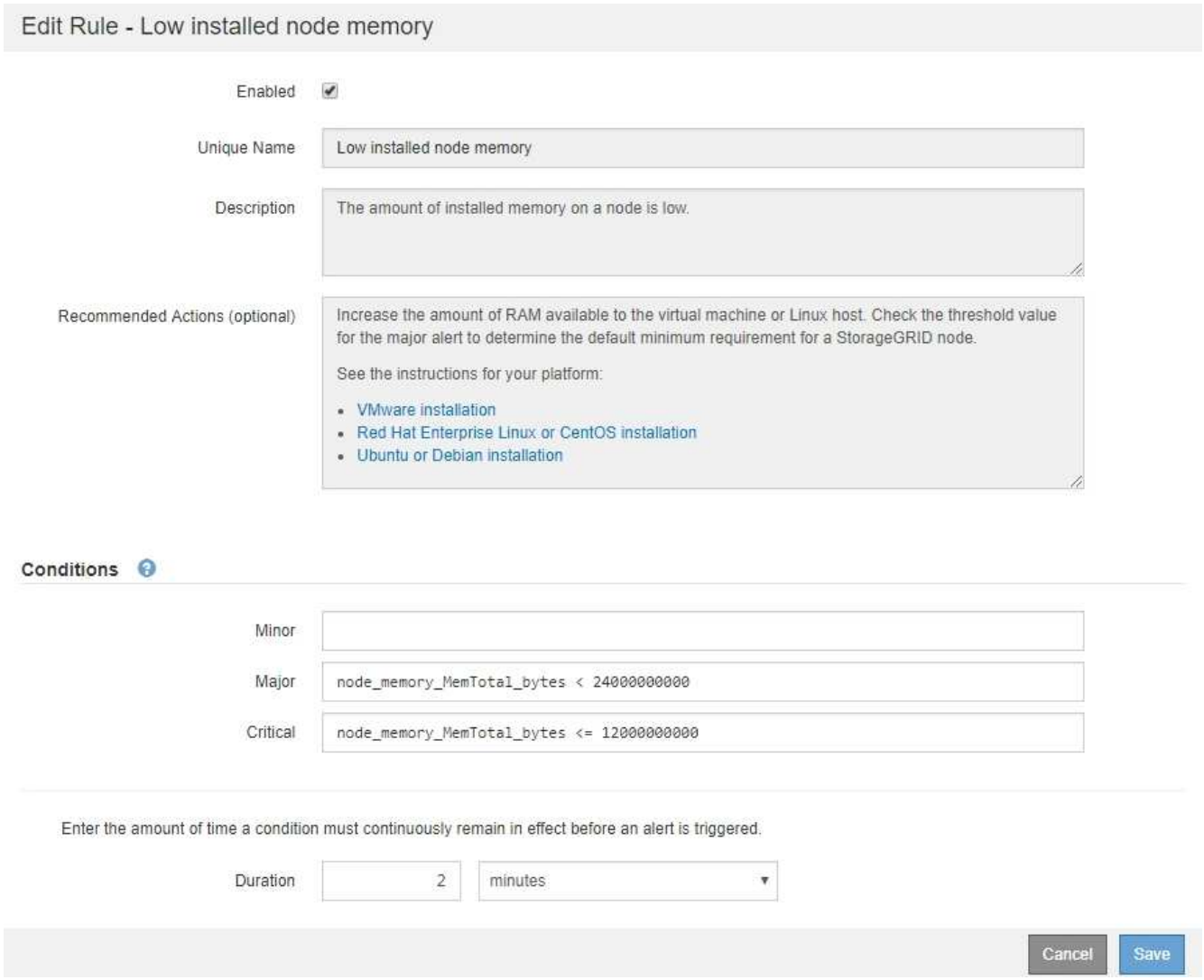
手順

1. アラート > *ルール*を選択します。

   [Alert Rules] ページが表示されます。

2. 編集するアラートルールのラジオボタンを選択します。
3. [* ルールの編集 *] を選択します。

   Edit Rule ダイアログボックスが表示されます。この例はデフォルトのアラートルールを示しています。[Unique Name]、概要]、および[Recommended Actions]のフィールドは無効になっており、編集することはできません。



4. [有効]*チェックボックスをオンまたはオフにして、このアラートルールが現在有効になっているかどうか

を確認します。

アラートルールを無効にすると、ルールの式は評価されず、アラートはトリガーされません。

現在のアラートのアラートルールを無効にした場合は、アラートがアクティブなアラートとして表示されなくなるまで数分待つ必要があります。

通常は、デフォルトのアラートルールを無効にすることは推奨されません。アラートルールが無効になっている場合は、重大な処理を完了できなくなるまで、根本的な問題が検出されない可能性があります。

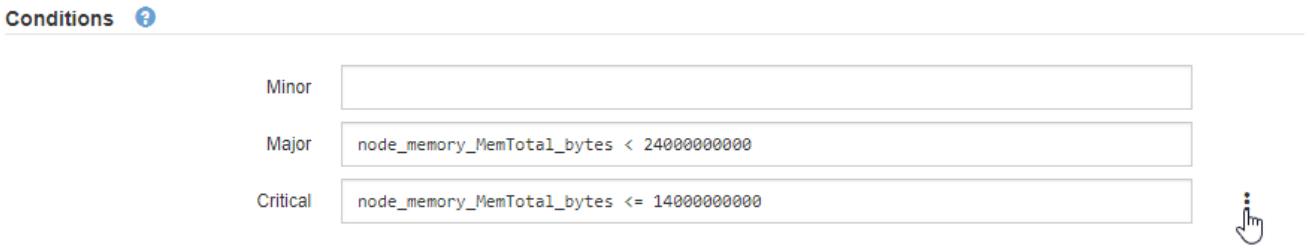
5. カスタムのアラートルールの場合は、次の情報を必要に応じて更新します。

この情報はデフォルトのアラートルールでは編集できません。

フィールド	製品説明
一意の名前	このルールの一意の名前。アラートルール名は、 [Alerts] ページに表示され、電子メール通知の件名にもなります。アラートルールの名前は 1~64 文字で指定できます。
製品説明	発生している問題の概要 。概要 は、アラートページおよび E メール通知に表示されるアラートメッセージです。アラートルールの説明は、 1~128 文字で指定できます。
推奨される対処方法	必要に応じて、このアラートがトリガーされたときに実行する推奨される対処方法を指定します。推奨される対処方法をプレーンテキスト（書式コードなし）で入力します。アラートルールの推奨される対処方法は、 0~1 、 024 文字で指定できます。

6. Conditions セクションで、 1 つ以上のアラート重大度レベルの Prometheus 式を入力または更新します。

編集したデフォルトのアラートルールの条件を元の値に戻す場合は、変更した条件の右側にある 3 つの点を選択します。



現在のアラートの条件を更新した場合は、更新前の条件が解決されるまで変更が適用されないことがあります。ルールのいずれかの条件が次回満たされた時点で、更新された値がアラートに反映されます。

基本式は、通常、次の形式で指定します。

```
[metric] [operator] [value]
```

式の文字数に制限はありませんが、ユーザインターフェイスでは 1 行で表示されます。少なくとも 1 つの式が必要です。

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

```
node_memory_MemTotal_bytes < 24000000000
```

7. [* Duration * （時間 * ）] フィールドに、アラートがトリガーされるまでに条件が継続的に有効である必要がある時間を入力し、時間の単位を選択します。

   条件が true になったときにすぐにアラートをトリガーするには、「 * 0 * 」と入力します。一時的な状況でアラートがトリガーされないようにするには、この値を大きくし

   デフォルトは5分です。

8. [保存（ Save ）] を選択します。

   デフォルトのアラート・ルールを編集した場合は ' ［ タイプ ］ カラムに **Default*** と表示されますデフォルトまたはカスタムのアラートルールを無効にした場合は、 * Status * 列に * Disabled * と表示されます。

StorageGRIDでアラートルールを無効にする

デフォルトまたはカスタムのアラートルールの有効 / 無効の状態を変更できます。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"アラートまたはRoot Access権限を管理します。"。

タスクの内容

アラートルールを無効にすると、ルールの式は評価されず、アラートはトリガーされません。

> 通常は、デフォルトのアラートルールを無効にすることは推奨されません。アラートルールが無効になっている場合は、重大な処理を完了できなくなるまで、根本的な問題が検出されない可能性があります。

手順

1. アラート > *ルール*を選択します。

   [Alert Rules] ページが表示されます。

2. 無効または有効にするアラートルールのラジオボタンを選択します。
3. [* ルールの編集 *] を選択します。

   Edit Rule ダイアログボックスが表示されます。

4. [有効]*チェックボックスをオンまたはオフにして、このアラートルールが現在有効になっているかどうかを確認します。

   アラートルールを無効にすると、ルールの式は評価されず、アラートはトリガーされません。

   現在のアラートのアラートルールを無効にした場合は、アラートがアクティブなアラートとして表示されなくなるまで数分待つ必要があります。

5. [保存（ Save ）] を選択します。
   - 無効 * は、 * ステータス * 列に表示されます。

StorageGRIDでカスタムアラートルールを削除する

不要となったカスタムのアラートルールは削除できます。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"アラートまたはRoot Access権限を管理します。"。

手順

1. アラート > *ルール*を選択します。

   [Alert Rules] ページが表示されます。

2. 削除するカスタムのアラートルールのラジオボタンを選択します。

   デフォルトのアラートルールは削除できません。

3. [* カスタムルールを削除 *] を選択します。

   確認のダイアログボックスが表示されます。

4. 「 * OK * 」を選択して、アラートルールを削除します。

   アラートのアクティブなインスタンスがあった場合、 10 分以内に解決されます。

アラート通知を管理します

StorageGRIDアラートの**SNMP**通知を設定する

アラート発生時に StorageGRID から SNMP 通知を送信するには、 StorageGRID SNMP エージェントを有効にし、 1 つ以上のトラップ送信先を設定する必要があります。

グリッド マネージャの 構成 > 監視 > **SNMP** エージェント オプションまたはグリッド管理 API の SNMP エンドポイントを使用して、 StorageGRID SNMP エージェントを有効にして構成できます。 SNMP エージェントは、SNMP プロトコルの 3 つのバージョンすべてをサポートします。

SNMPエージェントの設定方法については、を参照してください"SNMP による監視を使用する"。

StorageGRID SNMP エージェントの設定後に、次の 2 種類のイベントベースの通知を送信できます。

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

トラップ通知およびインフォーム通知は、デフォルトまたはカスタムアラートがいずれかの重大度レベルでトリガーされたときに送信されます。アラートの SNMP 通知を停止するには、アラートのサイレンスを設定する必要があります。を参照して "アラート通知をサイレント化する"

StorageGRID環境に複数の管理ノードが含まれている場合は、プライマリ管理ノードがアラート通知、AutoSupportパッケージ、SNMPトラップおよびインフォームの優先送信者となります。プライマリ管理ノードが使用できなくなると、他の管理ノードから一時的に通知が送信されます。を参照して "管理ノードとは"

StorageGRIDアラートのメール通知を設定する

アラート発生時に E メール通知が送信されるようにするには、 SMTP サーバに関する情報を指定する必要があります。また、アラート通知の受信者の E メールアドレスを入力する必要があります。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"アラートまたはRoot Access権限を管理します。"。
- "メールサーバーを設定しました"があります。

タスクの内容

StorageGRID環境に複数の管理ノードが含まれている場合は、プライマリ管理ノードがアラート通知、AutoSupportパッケージ、SNMPトラップおよびインフォームの優先送信者となります。プライマリ管理ノードが使用できなくなると、他の管理ノードから一時的に通知が送信されます。を参照して "管理ノードとは"

手順

1. アラート ＞ アラートメール を選択します。

   アラートメールのページが表示されます。

2. アラートが設定されたしきい値に達したときに通知メールを送信するには、アラートのメール通知を有効にする チェックボックスを選択してください。
3. 「重要度別にメールを受信する」セクションで、通知を受け取りたいアラートの種類を示すラジオボタンを選択します。
4. 「送信者」セクションで、アラート通知の送信元アドレスとして使用する有効なメールアドレスを指定してください。

   例： `storagegrid-alerts@example.com`

a. [受信者] セクションで、電子メールリストごとに電子メールアドレスを入力するか、アラートが発生したときに電子メールを受信する必要があるユーザーを入力します。

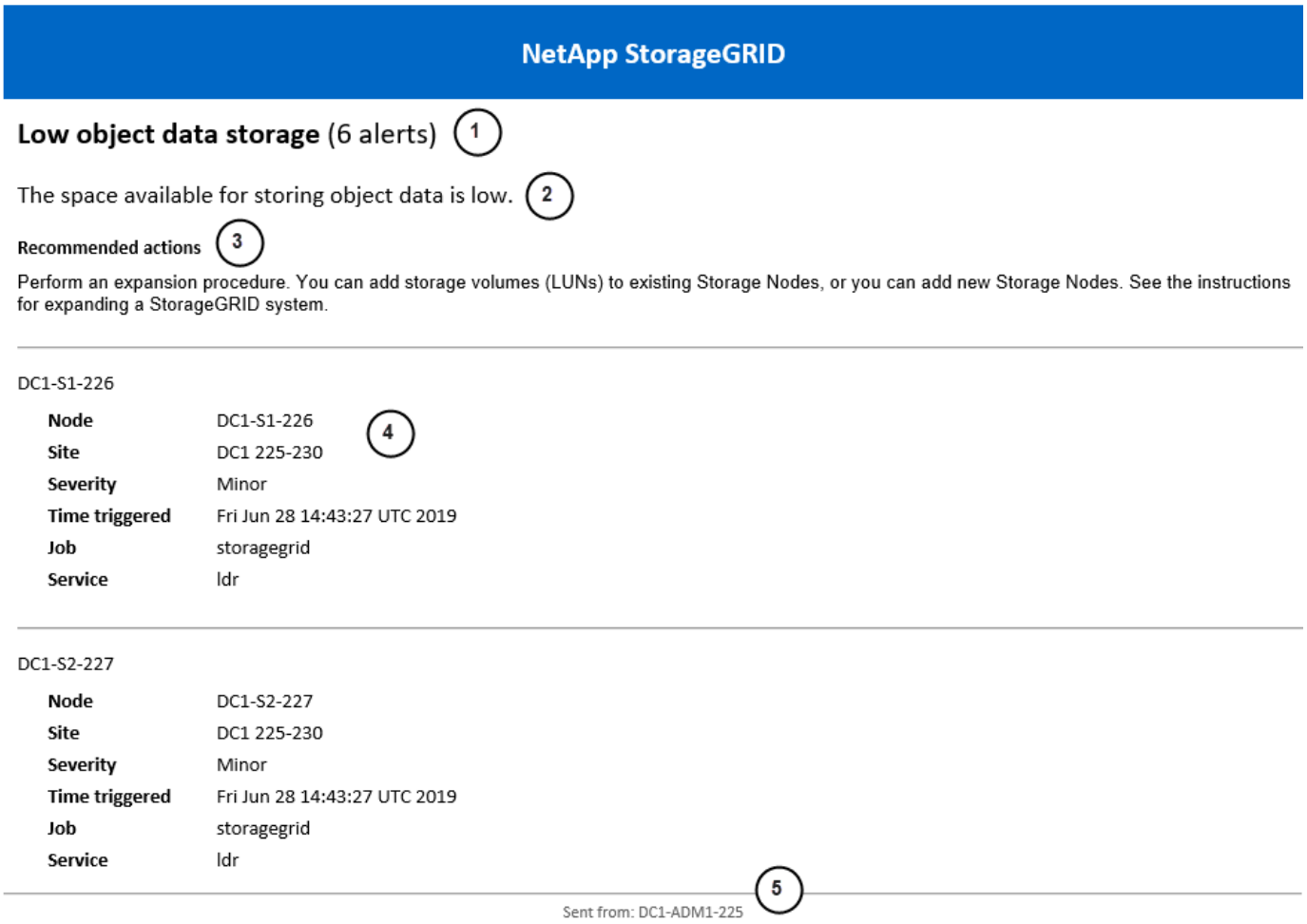
   受信者を追加するには、*受信者を追加*を選択してください。

5. [保存（ Save ）] を選択します。

アラート E メール通知に記載される情報

メールサーバーを設定し、アラート用のメールを有効にすると、アラートルールがサイレンス設定によって抑制されていない限り、アラートが発生した際に指定された受信者にメール通知が送信されます。"アラート通知をサイレント化する"を参照してください。

E メール通知には次の情報が含まれます。



コールアウト	製品説明
1	アラートの名前と、そのアラートのアクティブなインスタンスの数。
2	アラートの概要 。
3	アラートに対する推奨対応策。

コールアウト	製品説明
4	アラートのアクティブな各インスタンスに関する詳細情報。対象となるノードとサイト、アラートの重大度、アラートルールがトリガーされた UTC 時間、影響を受けるジョブとサービスの名前などが含まれます。
5	通知を送信した管理ノードのホスト名。

アラートのグループ化方法

StorageGRID は、アラートがトリガーされたときに大量の E メール通知が送信されないように、複数のアラートを同じ通知にまとめます。

StorageGRID で複数のアラートを E メール通知でグループ化する例については、次の表を参照してください。

動作	例
各アラート通知は、同じ名前のアラートにのみ適用されます。名前が異なる 2 つのアラートが同時にトリガーされると、 2 つの E メール通知が送信されます。	• アラート A は 2 つのノードで同時にトリガーされます。1 つの通知のみが送信されます。 • アラート A はノード 1 でトリガーされ、アラート B はノード 2 で同時にトリガーされます。2 つの通知が送信されます各アラートに 1 つずつ送信されます
特定のノードの特定のアラートが複数の重大度のしきい値に達した場合は、最も重大度の高いアラートに関してのみ通知が送信されます。	• アラート A がトリガーされ、 Minor 、 Major 、 Critical の各アラートしきい値に達した場合重大アラートに対して 1 つの通知が送信されます。
あるアラートが初めてトリガーされた場合、 StorageGRID は 2 分待ってから通知を送信します。この時間内に同じ名前のアラートがほかにもトリガーされた場合、 StorageGRID はすべてのアラートを最初の通知の最初のグループにまとめます	1. アラートAがノード1で8：00にトリガーされ、通知は送信されません。 2. アラートAがノード2で08：01にトリガーされ、通知は送信されません。 3. 08:02 で、アラートの両方のインスタンスを報告する通知が送信されます。
同じ名前の別のアラートがトリガーされた場合、 StorageGRID は 10 分待ってから新しい通知を送信します。新しい通知では、以前に報告されたものも含めて、アクティブなアラート（サイレント化されていない現在のアラート）がすべて報告されます。	1. アラートAがノード1で8：00にトリガーされ、通知が 08:02 に送信されます。 2. アラートAがノード2で08：05にトリガーされます。2回目の通知は8：15（10分後）に送信されます。両方のノードが報告されます。

動作	例
同じ名前の現在のアラートが複数あり、そのうちの 1 つのアラートが解決された場合、そのアラートが解決されたノードでアラートが再度発生しても新しい通知は送信されません。	1. アラート A がノード 1 に対してトリガーされます。通知が送信されます。 2. アラート A がノード 2 に対してトリガーされます。2 回目の通知が送信されます。 3. アラート A はノード 2 について解決されましたが、ノード 1 に対してはアクティブなままです。 4. アラート A がノード 2 に対して再度トリガーされます。ノード 1 のアラートがまだアクティブなため、新しい通知は送信されません。
StorageGRID は、アラートのすべてのインスタンスが解決されるか、アラートルールがサイレント化されるまで、 7 日ごとに E メール通知を送信します。	1. 3 月 8 日にノード 1 のアラート A がトリガーされます。通知が送信されます。 2. アラート A が解決されていないか、サイレント化されていその他の通知は 3 月 15 日、 3 月 22 日、 3 月 29 日などに送信されます。

アラート **E** メール通知のトラブルシューティング

メール通知失敗アラートがトリガーされ、メールが届かない場合は、以下の手順に従って問題を調査および解決してください。

- メールサーバー通知のテスト
- StorageGRIDアラートメール
- 複数管理者認証（MAV）メール

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたは"rootアクセス権限"を持っています。「アラートの管理」権限がある場合は、メールサーバーの設定を表示できますが、編集はできません。

手順

1. アラートメールの設定を確認してください。
   a. 受信者の有効な E メールアドレスが指定されていることを確認します。
   b. 設定 > *メールサーバー*を選択し、メール（SMTP）サーバーの設定が正しいことを確認してください。
2. スパムフィルタを確認し、 E メールが迷惑メールフォルダに送信されていないことを確認します。
3. メール管理者に問い合わせて、送信者アドレスからのメールがブロックされていないことを確認してください。
4. メール転送に関する以下の項目を確認してください。
   a. メールサーバーのログ監視：StorageGRID が使用するメールサーバーのログを表示します（設定 > メールサーバー）。StorageGRID がメールの送信を試みた時刻に一致するリレーエラー、認証エラー、およびその他の障害を検索します。

b. 配信不能レポート（バウンスバック）：メールが受信されず、StorageGRID が障害を報告しない場合、問題はバウンスバックである可能性があります。「送信元」アドレスに有効なメールアドレスを設定すると、これらのバウンスバック返信メールが表示されるようになります。

5. メール送信元の管理ノードのログファイルを収集してください。/var/local/log/prometheus.log ファイルと /var/local/log/nms.log ファイルを確認し、修正可能な明らかな問題がないか調べてください。問題が解決しない場合は、テクニカルサポートにお問い合わせください。

   テクニカルサポートは、ログの情報を参考に問題の原因を特定します。たとえば、指定したサーバに接続するときに、 prometheus.log ファイルにエラーが表示されることがあります。

   "ログファイルとシステムデータを収集"を参照してください。

StorageGRID でアラート通知をサイレンス

必要に応じて、サイレンスを設定してアラート通知を一時的に停止することができます。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"アラートまたはRoot Access権限を管理します。"。

タスクの内容

アラートルールは、グリッド全体、単一サイト、または単一ノードと、 1 つ以上の重大度に対してサイレント化できます。各サイレンスは、 1 つのアラートルールまたはすべてのアラートルールのすべての通知を停止します。

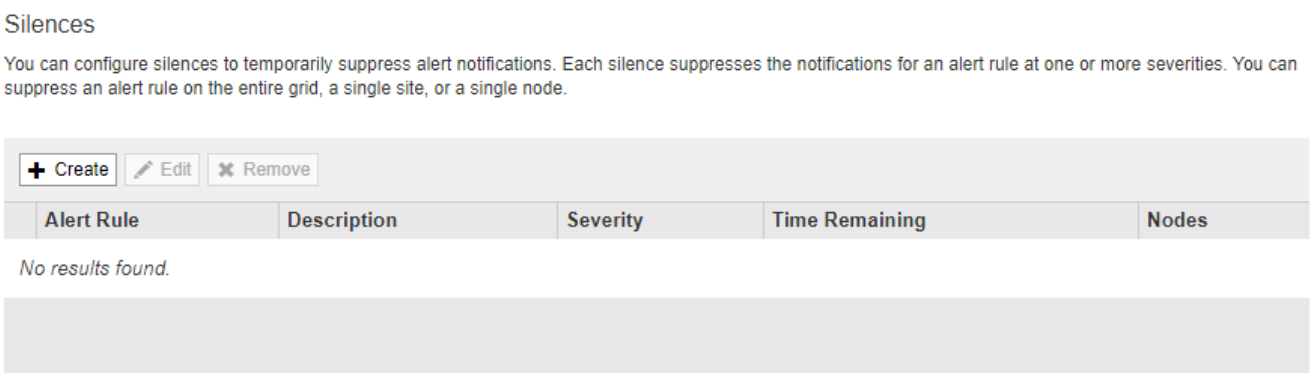
SNMP エージェントを有効にすると、サイレンスは SNMP トラップおよびインフォームも抑制します。

> アラートルールをサイレント化する場合は注意が必要です。アラートをサイレント化すると、重大な処理を完了できなくなるまで、原因となっている問題が検出されない可能性があります。

手順

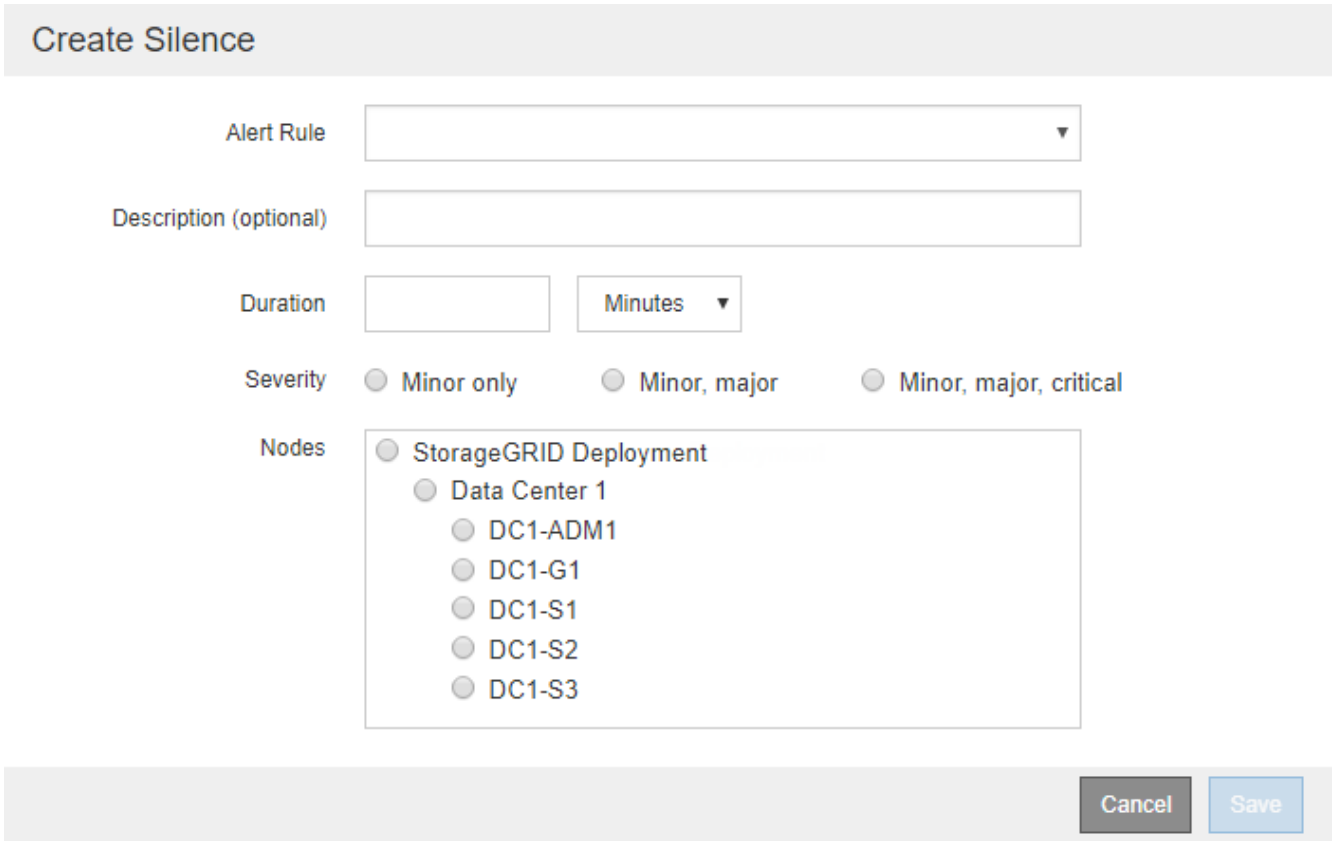
1. アラート > *サイレンス*を選択します。

   [Silences] ページが表示されます。



2. 「 * Create * 」を選択します。

[無音の作成] ダイアログボックスが表示されます。



3. 次の情報を選択または入力します。

フィールド	製品説明
アラートルール	サイレント化するアラートルールの名前。アラートルールが無効になっている場合でも、任意のデフォルトまたはカスタムのアラートルールを選択できます。 • 注：このダイアログボックスで指定した条件を使用してすべてのアラートルールをサイレント化する場合は、「 * すべてのルール * 」を選択します。
製品説明	必要に応じて、サイレンスの概要 。たとえば、このサイレンスの目的を入力します。
期間	このサイレンスを有効にしておく期間（分、時間、または日数）。サイレンスを有効にできる期間は、 5 分から 1 、 825 日（ 5 年）です。 • 注： * アラートルールを長時間サイレント化しないでください。アラートルールがサイレント化されている場合、重大な処理が完了しないかぎり、根本的な問題が検出されないことがあります。ただし、 * サービスアプライアンスリンク停止 * アラートや * ストレージアプライアンスリンク停止 * アラートなど、特定の意図的な設定によってアラートがトリガーされた場合は、拡張サイレンスを使用する必要があります。

フィールド	製品説明
重大度	サイレント化するアラートの重大度。選択した重大度のいずれかでアラートがトリガーされた場合、通知は送信されません。
ノード	このサイレンスを適用するノード。アラートルール、またはグリッド全体、単一サイト、または単一ノード上のすべてのルールを抑制することができます。グリッド全体を選択環境 する場合は、すべてのサイトとすべてのノードをサイレント化します。サイトを選択すると、そのサイトのノードにのみサイレンスが適用されます。 *注：*サイレンスごとに複数のノードまたは複数のサイトを選択することはできません。同じアラートルールを複数のノードまたは複数のサイトで一度に停止するには、追加のサイレンスを作成する必要があります。

4. [保存（ Save ）] を選択します。
5. 期限が切れる前に変更または終了するには、サイレンスを編集または削除できます。

オプション	製品説明
サイレンスを編集する	a. アラート > *サイレンス*を選択します。 b. テーブルで、編集するサイレンスのラジオボタンを選択します。 c. 「 * 編集 * 」を選択します。 d. 概要 、残り時間、選択した重大度、または対象となるノードを変更します。 e. [保存（ Save ）] を選択します。
サイレンスを削除する	a. アラート > *サイレンス*を選択します。 b. テーブルで、削除するサイレンスのラジオボタンを選択します。 c. 「 * 削除」を選択します。 d. このサイレンスを削除することを確認するには、「 * OK 」を選択します。 ◦ 注 * ：このアラートがトリガーされると（別のサイレンスで停止されていないかぎり）通知が送信されるようになりました。このアラートが現在トリガーされている場合は、 E メールまたは SNMP 通知の送信やアラートページの更新に数分かかることがあります。

関連情報

"SNMP エージェントを設定します"

StorageGRID のアラート

このリファレンスでは、Grid Managerに表示されるデフォルトアラートを示します。推奨される対処方法は、受信したアラートメッセージに記載されています。

必要に応じて、システムの管理方法に合わせてカスタムのアラートルールを作成できます。

一部のデフォルトアラートではが使用され"Prometheus 指標"ます。

アプライアンスのアラート

アラート名	製品説明
アプライアンスのバッテリの有効期間が終了し	アプライアンスのストレージコントローラのバッテリの有効期間が終了しました。
アプライアンスのバッテリに問題があります	アプライアンスのストレージコントローラのバッテリに障害が発生しました。
アプライアンスバッテリの学習容量が不足しています	アプライアンスのストレージコントローラのバッテリで学習容量が不足しています。
アプライアンスバッテリの有効期限が近づいています	アプライアンスのストレージコントローラのバッテリの有効期限が近づいています。
アプライアンスのバッテリが取り外されました	アプライアンスのストレージコントローラのバッテリがありません。
アプライアンスのバッテリが高温になっています	アプライアンスのストレージコントローラのバッテリが過熱しています。
アプライアンスの BMC 通信エラー	ベースボード管理コントローラ（ BMC ）との通信が失われました。
アプライアンスのブートデバイス障害が検出されました	アプライアンスのブートデバイスで問題が検出されました。
アプライアンスキャッシュバックアップデバイスに障害が発生しました	永続的キャッシュバックアップデバイスで障害が発生しました。
アプライアンスキャッシュバックアップデバイスに十分な容量がありません	キャッシュバックアップデバイスに十分な容量がありません。
アプライアンスのキャッシュ・バックアップ・デバイスの書き込み保護	キャッシュバックアップデバイスは書き込み保護されています。
アプライアンスのキャッシュメモリサイズが一致しません	アプライアンスの 2 台のコントローラは、キャッシュサイズが異なります。

アラート名	製品説明
アプライアンスCMOSバッテリ障害	機器内のCMOSバッテリーに問題が検出されました。
アプライアンスコンピューティングコントローラシャーシの温度が高すぎます	StorageGRID アプライアンスのコンピューティングコントローラの温度が公称のしきい値を超えました。
アプライアンスのコンピューティングコントローラの CPU 温度が高すぎます	StorageGRID アプライアンスのコンピューティングコントローラの CPU 温度が公称のしきい値を超えました。
アプライアンスのコンピューティングコントローラを確認する必要があります	StorageGRID アプライアンスのコンピューティングコントローラでハードウェア障害が検出されました。
アプライアンスコンピューティングコントローラの電源装置 A に問題があります	コンピューティングコントローラの電源装置Aに問題があります。
アプライアンスコンピューティングコントローラの電源装置 B に問題があります	コンピューティングコントローラの電源装置 B に問題があります。
アプライアンスコンピューティングハードウェアモニタのサービスが停止する	ストレージハードウェアのステータスを監視するサービスが停止しました。
アプライアンスのDASドライブが1日に書き込まれるデータの制限を超えています	ドライブに毎日大量のデータが書き込まれているため、保証が無効になる可能性があります。
アプライアンスのDASドライブ障害が検出されました	アプライアンスの直接接続型ストレージ（DAS）ドライブで問題が検出されました。
アプライアンスDASドライブが間違ったスロットまたはノードにあります	直接接続ストレージ (DAS) ドライブが間違ったスロットまたはノードに挿入されています
アプライアンスのDASドライブのロケーターライトが点灯	アプライアンスストレージノード内の1つ以上の直接接続型ストレージ（DAS）ドライブのドライブロケーターライトが点灯しています。
アプライアンスDASドライブのリビルド	直接接続型ストレージ（DAS）ドライブのリビルド中。これは、最近交換または取り外し/再挿入された場合に想定される現象です。

アラート名	製品説明
アプライアンスのファン障害が検出されました	アプライアンスのファンユニットに問題が検出されました。
アプライアンスのファイバ・チャネル障害が検出されました	アプライアンスストレージコントローラとコンピューティングコントローラの間でFibre Channelリンクの問題が検出されました
アプライアンスのファイバ・チャネル HBA ポート障害	Fibre Channel HBA ポートで障害が発生しているか、障害が発生しています。
アプライアンスのフラッシュキャッシュドライブが最適な状態でありません	SSD キャッシュに使用されているドライブが最適な状態でありません。
アプライアンスインターコネクト / バッテリキャニスターが取り外されました	インターコネクト / バッテリキャニスターがありません。
アプライアンスの LACP ポートがありません	StorageGRID アプライアンスのポートが LACP ボンドに参加していません。
アプライアンスNICの障害が検出されました	アプライアンスのネットワークインターフェイスカード（NIC）に問題が検出されました。
アプライアンス全体の電源装置がデグレード状態になりました	StorageGRID アプライアンスの電源が、推奨される動作電圧から逸脱しています。
アプライアンスSANtricity OSソフトウェアの更新が必要です	SANtricityソフトウェア バージョンは、 StorageGRIDのこのリリースに推奨される最小バージョンよりも低いです。
アプライアンスのSFP障害が検出されました	StorageGRID アプライアンスのコンピューティングコントローラで SFP 障害が検出されました。
アプライアンスSSDの重大な警告です	アプライアンスSSDから重大な警告が報告されています。
アプライアンスストレージコントローラ A の障害	StorageGRID アプライアンスのストレージコントローラ A で障害が発生した。
アプライアンスストレージコントローラ B の障害	StorageGRID アプライアンスのストレージコントローラ B で障害が発生した。
アプライアンスストレージコントローラのドライブ障害	StorageGRID アプライアンスの 1 つ以上のドライブで障害が発生しているか、または最適な状態でありません。

アラート名	製品説明
アプライアンスストレージコントローラハードウェア問題	SANtricity ソフトウェアから、 StorageGRID アプライアンスのコンポーネントについて「 Needs Attention 」が報告されます。
アプライアンスストレージコントローラの電源装置 A に障害が発生しました	StorageGRID アプライアンスの電源装置 A が、推奨される動作電圧から逸脱しています。
アプライアンスストレージコントローラの電源装置 B に障害が発生しました	StorageGRID アプライアンスの電源装置 B が、推奨される動作電圧から逸脱しています。
アプライアンスストレージハードウェアモニタのサービスが停止する	ストレージハードウェアのステータスを監視するサービスが停止しました。
アプライアンスストレージシェルフがデグレード状態になります	ストレージアプライアンスのストレージシェルフのいずれかのコンポーネントのステータスがデグレードになっています。
アプライアンスの温度が超過しました	アプライアンスのストレージコントローラの公称温度または最大温度を超えました。
アプライアンスの温度センサーが取り外されました	温度センサーが取り外されました。
アプライアンスUEFIセキュアブートエラー	アプライアンスが安全にブートされていません。
ディスク I/O が非常に遅い	ディスクI/Oが非常に遅い場合は、グリッドのパフォーマンスに影響する可能性があります。
ストレージアプライアンスのファンで障害が検出されました	アプライアンスのストレージコントローラのファンユニットで問題が検出されました。
ストレージアプライアンスストレージの接続がデグレードされました	コンピューティングコントローラとストレージコントローラの間の接続に問題があります。
ストレージデバイスにアクセスできません	ストレージデバイスにアクセスできません。

監査および**syslog**アラート

アラート名	製品説明
監査ログをメモリ内キューに追加しています	ノードからローカル syslog サーバにログを送信できず、メモリ内キューがいっぱいになっています。
外部 syslog サーバの転送エラーです	ノードから外部 syslog サーバにログを転送できません。
大規模な監査キュー	監査メッセージのディスク キューがいっぱいです。この状態に対処しないと、S3 操作が失敗する可能性があります。
ログをディスク上キューに追加しています	ノードから外部 syslog サーバにログを転送できず、ディスク上のキューがいっぱいになっています。

バケットアラート

アラート名	製品説明
FabricPool バケットにサポート対象外のバケット整合性設定があります	FabricPoolバケットでは、availableまたはstrong-siteの整合性レベルが使用されますが、この整合性レベルはサポートされていません。
FabricPoolバケットにサポートされていないバージョン管理設定があります	FabricPoolバケットでバージョン管理またはS3オブジェクトロックが有効になっているが、これはサポートされていない。
ListBucket Get/Head オブジェクトの権限チェックが無効になっています	ListBucket 存在しないキーに対する GetObject/HeadObject の権限チェックは無効になっています。

Cassandraアラート

アラート名	製品説明
Cassandra 自動コンパクターエラーです	Cassandra 自動コンパクターでエラーが発生しました。
Cassandra 自動コンパクターメトリックが古くなっています	Cassandra の自動圧縮機能を説明する指標が最新ではありません。
Cassandra 通信エラー	Cassandra サービスを実行するノード間の通信で問題が発生しています。
Cassandra の圧縮処理が過負荷です	Cassandra コンパクションプロセスが過負荷状態です。

アラート名	製品説明
Cassandraオーバーサイズ書き込みエラー	内部StorageGRID プロセスがCassandraに送信した書き込み要求が大きすぎます。
Cassandra 修復指標が最新ではありません	Cassandra 修復ジョブを説明する指標が最新ではありません。
Cassandra の修復の進捗が遅い	Cassandra データベースの修復の進捗状況が遅い。
Cassandra 修復サービスを使用できません	Cassandra 修復サービスは使用できません。
Cassandra テーブルが破損しています	Cassandra がテーブルの破損を検出しました。テーブルの破損が検出されると、 Cassandra が自動的に再起動します。

クラウドストレージプールのアラート

アラート名	製品説明
クラウドストレージプールの接続エラー	クラウドストレージプールの健全性チェックで、新たなエラーが 1 つ以上検出されました。
IAM Roles Anywhereエンドエンティティ証明書の有効期限	IAM Roles Anywhereエンドエンティティ証明書の有効期限が近づいています。

グリッド間レプリケーションのアラート

アラート名	製品説明
クロスグリッドレプリケーションの永続的な障害	ユーザの介入を必要とするグリッド間レプリケーションエラーが発生しました。
グリッド間レプリケーションリソースを使用できません	リソースを使用できないため、グリッド間レプリケーション要求が保留になっています。

DHCPアラート

アラート名	製品説明
DHCP リースの期限が切れました	ネットワークインターフェイスの DHCP リースが期限切れです。
DHCP リースがまもなく期限切れになります	ネットワークインターフェイスの DHCP リースがまもなく期限切れになります。
DHCP サーバが使用できません	DHCP サーバが使用できない。

デバッグおよびトレースアラート

アラート名	製品説明
パフォーマンスへの影響をデバッグします	デバッグモードを有効にすると、システムパフォーマンスに悪影響を及ぼす可能性があります。
トレース設定が有効になりました	トレース構成を有効にすると、システムパフォーマンスに悪影響を及ぼす可能性があります。

Eメールアラートと**AutoSupport** アラート

アラート名	製品説明
AutoSupport メッセージの送信に失敗しました	最新のAutoSupport メッセージの送信に失敗しました。
ドメイン名解決エラー	StorageGRIDノードがドメイン名を解決できませんでした。
E メール通知のエラーです	アラートの E メール通知を送信できませんでした。
ログアーカイブ先のバケットが見つかりません	ログのアーカイブ先バケットが見つからないため、ログを宛先バケットにアーカイブできません。
SNMPインフォームエラー	トラップ送信先へのSNMPインフォーム通知の送信時にエラーが発生しました。
SSH外部アクセスが有効	SSH 外部アクセスが 24 時間以上有効になっています。
SSHまたはコンソールログインが検出されました	過去24時間以内に、ユーザーがWebコンソールまたはSSHを使用してログインしました。

イレイジャーコーディング（**EC**）アラート

アラート名	製品説明
チャンクサービスにおける高ゴルーチン数	チャンクサービスで使用されているゴルーチンの数が異常に多く、デッドロックまたはリソースリークが発生している可能性があります。
EC のリバランシングに失敗しました	ECリバランシング手順 が失敗したか、停止しました。
EC の修復エラー	ECデータの修復ジョブが失敗したか停止しました。
EC の修復が停止した	ECデータの修復ジョブが停止しました。

アラート名	製品説明
イレイジャーコーディングフラグメント検証エラー	イレイジャーコーディングフラグメントは検証できなくなりました。破損したフラグメントは修復されない可能性があります。
修復が必要な状態の消去符号化グループ	消去符号化データの修復処理が行われていない場合、1つ以上の消去符号化グループが「修復が必要」状態になります。

証明書の有効期限に関するアラート

アラート名	製品説明
管理プロキシCA証明書の有効期限	管理プロキシサーバのCAバンドル内の1つ以上の証明書の有効期限が近づいています。
クライアント証明書の有効期限	1つ以上のクライアント証明書の有効期限が近づいています。
S3 のグローバル サーバー証明書の有効期限	S3 のグローバル サーバー証明書の有効期限が近づいています。
ロードバランサエンドポイント証明書の有効期限	1 つ以上のロードバランサエンドポイント証明書の有効期限が近づいています。
管理インターフェイスのサーバ証明書の有効期限	管理インターフェイスで使用されるサーバ証明書の有効期限が近づいています。
外部 syslog CA 証明書の有効期限	外部 syslog サーバ証明書への署名に使用される認証局（ CA ）証明書の有効期限が近づいています。
外部 syslog クライアント証明書の有効期限	外部 syslog サーバのクライアント証明書の有効期限が近づいています。
外部 syslog サーバ証明書の有効期限	外部 syslog サーバから提供されるサーバ証明書の有効期限が近づいています。

グリッドネットワークのアラート

アラート名	製品説明
Grid ネットワーク MTU が一致しません	グリッドネットワークインターフェイス（eth0）のMTU設定は、グリッド内のノード間で大きく異なります。

グリッドフェデレーションアラート

アラート名	製品説明
グリッドフェデレーション証明書の有効期限	1つ以上のグリッドフェデレーション証明書の有効期限が近づいています。
グリッドフェデレーション接続に失敗しました	ローカルグリッドとリモートグリッドの間のグリッドフェデレーション接続が機能していません。

高使用率または高レイテンシのアラート

アラート名	製品説明
メタデータクエリのレイテンシが高くなっています	Cassandra メタデータクエリの平均時間が長すぎます。

アイデンティティフェデレーションアラート

アラート名	製品説明
アイデンティティフェデレーションの同期に失敗する	アイデンティティソースからフェデレーテッドグループとフェデレーテッドユーザを同期できません。
テナントのアイデンティティフェデレーションの同期が失敗する	テナントで設定されたアイデンティティソースからフェデレーテッドグループとフェデレーテッドユーザを同期できない。

情報ライフサイクル管理（**ILM**）のアラート

アラート名	製品説明
ILM 配置を実現できません	特定のオブジェクトについては、 ILM ルールでの配置手順を実行できません。
ILM のスキャン速度が低下しています	ILM のスキャン速度は 100 オブジェクト / 秒未満に設定されます。

キー管理サーバ（**KMS**）のアラート

アラート名	製品説明
KMS CA 証明書の有効期限	キー管理サーバ（ KMS ）証明書への署名に使用する CA 証明書の有効期限が近づいています。
KMS クライアント証明書の有効期限	キー管理サーバのクライアント証明書の有効期限が近づいています
KMS の設定をロードできませんでした	キー管理サーバの設定は存在しますが、ロードできませんでした。

アラート名	製品説明
KMS 接続エラー	アプライアンスノードがサイトのキー管理サーバに接続できませんでした。
KMS 暗号化キー名が見つかりません	設定されているキー管理サーバに、指定した名前と一致する暗号化キーがありません。
KMS 暗号化キーのローテーションに失敗しました	アプライアンスのボリュームはすべて復号化されましたが、1つ以上のボリュームを最新のキーにローテーションできませんでした。
KMS は設定されていません	このサイトにはキー管理サーバがありません。
KMS キーでアプライアンスボリュームを復号化できませんでした	ノード暗号化が有効になっているアプライアンス上の 1 つ以上のボリュームを、現在の KMS キーで復号化できませんでした。
KMS サーバ証明書の有効期限	キー管理サーバ（ KMS ）で使用されるサーバ証明書の有効期限が近づいています。
KMSサーバの接続エラー	アプライアンスノードが、そのサイトのキー管理サーバクラスタ内の1つ以上のサーバに接続できませんでした。

ロードバランサのアラート

アラート名	製品説明
昇格したゼロリクエストロードバランサ接続	ロードバランサエンドポイントへの接続のうち、要求を実行せずに切断された接続の割合が高くなりました。

ローカルクロックオフセットアラート

アラート名	製品説明
ローカル・クロック・ラージ・タイム・オフセット	ローカルクロックとネットワークタイムプロトコル（NTP）時間のオフセットが大きすぎます。

メモリ不足またはスペース不足のアラート

アラート名	製品説明
監査ログのディスク容量が不足しています	監査ログに使用できるスペースが少なくなっています。この状態に対処しないと、S3 操作が失敗する可能性があります。
利用可能なノードメモリが少なくなっています	ノードの使用可能な RAM の容量が少なくなっています。

アラート名	製品説明
ストレージプールの空き容量が不足しています	ストレージノードにオブジェクトデータを格納できるスペースが少なくなっています。
ノードメモリが不足しています	ノードに搭載されているメモリの容量が少なくなっています。
メタデータストレージが不足しています	オブジェクトメタデータを格納できるスペースが少なくなっています。
ディスク容量不足です	指標データベースに使用できるスペースが少なくなっています。
オブジェクトデータのストレージが少ない	オブジェクトデータを格納できるスペースが少なくなっています。
読み取り専用のローウォーターマークの上書き	ストレージボリュームのソフト読み取り専用ウォーターマークの上書きが、ストレージノードで最適化された最小ウォーターマークを下回っています。
ルートディスク容量が不足しています	ルートディスクの使用可能なスペースが少なくなっています。
システムのデータ容量が不足しています	/var/local に使用可能なスペースが少なくなっています。この状態に対処しないと、S3 操作が失敗する可能性があります。
tmp ディレクトリの空きスペースが不足しています	/tmp ディレクトリのスペースが不足しています。

ノードまたはノードのネットワークアラート

アラート名	製品説明
ADC クォーラムが満たされていません	ADC サービスを備えたストレージ ノードがオフラインです。 ADC クォーラムが復元されるまで、拡張および廃止操作はブロックされます。
管理ネットワークの受信使用量	管理ネットワークで受信の使用率が高くなっています。
管理ネットワークの転送使用量	管理ネットワークでの転送使用率が高くなっています。
ファイアウォールの設定に失敗しました	ファイアウォール設定を適用できませんでした。
フォールバックモードの管理インターフェイスエンドポイント	すべての管理インターフェイスエンドポイントがデフォルトポートに長時間フォールバックしています。
ノードのネットワーク接続エラー	ノード間でデータを転送中にエラーが発生しました。

アラート名	製品説明
ノードネットワーク受信フレームエラー	ノードで受信したネットワークフレームの割合が高いとエラーが発生していました。
ノードが NTP サーバと同期されていません	ノードがネットワークタイムプロトコル（NTP）サーバと同期されていません。
NTP サーバでノードがロックされていません	ノードがネットワークタイムプロトコル（ NTP ）サーバにロックされていません。
非アプライアンスノードのネットワークが停止しています	1 つ以上のネットワークデバイスが停止しているか切断されています。
管理ネットワークでサービスアプライアンスのリンクが停止しています	アプライアンスの管理ネットワーク（eth1）へのインターフェイスが停止しているか切断されています。
管理ネットワークポート 1 のサービスアプライアンスリンクが停止しています	アプライアンスの管理ネットワークポート 1 が停止しているか切断されています。
クライアントネットワークでサービスアプライアンスのリンクが停止しています	アプライアンスのクライアントネットワーク（eth2）へのインターフェイスが停止しているか切断されています。
ネットワークポート1でサービスアプライアンスのリンクが停止しています	アプライアンスのネットワークポート1が停止しているか切断されています。
ネットワークポート2でサービスアプライアンスのリンクが停止しています	アプライアンスのネットワークポート2が停止しているか切断されています。
ネットワークポート3でサービスアプライアンスのリンクが停止しています	アプライアンスのネットワークポート3が停止しているか切断されています。
ネットワークポート4でサービスアプライアンスのリンクが停止しています	アプライアンスのネットワークポート4が停止しているか切断されています。
管理ネットワークでのストレージアプライアンスのリンクが停止しています	アプライアンスの管理ネットワーク（eth1）へのインターフェイスが停止しているか切断されています。

アラート名	製品説明
管理ネットワークポート 1 のストレージアプライアンスのリンクが停止しています	アプライアンスの管理ネットワークポート 1 が停止しているか切断されています。
クライアントネットワークでストレージアプライアンスのリンクが停止しています	アプライアンスのクライアントネットワーク（eth2）へのインターフェイスが停止しているか切断されています。
ネットワークポート1でストレージアプライアンスのリンクが停止しています	アプライアンスのネットワークポート1が停止しているか切断されています。
ネットワークポート2でストレージアプライアンスのリンクが停止しています	アプライアンスのネットワークポート2が停止しているか切断されています。
ネットワークポート3でストレージアプライアンスのリンクが停止しています	アプライアンスのネットワークポート3が停止しているか切断されています。
ネットワークポート4でストレージアプライアンスのリンクが停止しています	アプライアンスのネットワークポート4が停止しているか切断されています。
ストレージノードが目的のストレージ状態ではありません	内部エラーまたはボリューム関連の問題が原因で、ストレージノードのLDRサービスを目的の状態に移行できない
TCP接続の使用状況	このノードのTCP接続数が追跡可能な最大数に近づいています。
ノードと通信できません	1 つ以上のサービスが応答していないか、ノードに到達できません。
予期しないノードのリブートです	過去 24 時間以内にノードが予期せずリブートされました。

オブジェクトアラート

アラート名	製品説明
オブジェクトの存在チェックに失敗しました	オブジェクトの存在チェックジョブが失敗しました。
オブジェクトの存在チェックが停止しました	オブジェクトの存在チェックジョブが停止しました。
紛失の可能性があるオブジェクト	1 つ以上のオブジェクトがグリッドから失われる可能性があります。

アラート名	製品説明
孤立したオブジェクトが検出されました	孤立したオブジェクトが検出されました。
S3マルチパートアップロードのパートサイズが大きすぎます	クライアントが、パートサイズ制限を超えるマルチパートアップロード操作を試みています。
S3 PUTオブジェクトサイズが大きすぎます	クライアントがS3のサイズ制限を超えるPUT Object処理を試行しています。
サポートされていない条件付きヘッダーを使用したS3リクエスト	S3クライアントが、特定の操作においてサポートされていない条件付きヘッダー（If-MatchまたはIf-None-Match）を使用しています。
グローバル名前空間が有効な状態で誤ったリージョンを使用しているS3リクエスト	S3クライアントが、このグリッドのバケットにアクセスするために誤った署名リージョンを使用しています。
未識別の破損オブジェクトが検出されました	レプリケートオブジェクトストレージにファイルが見つかりましたが、レプリケートオブジェクトとして識別できませんでした。

オブジェクト破損アラート

アラート名	製品説明
オブジェクトサイズの不一致	オブジェクト存在チェック手順中に予期しないオブジェクト サイズが検出されました。

プラットフォームサービスのアラート

アラート名	製品説明
プラットフォームサービス保留中の要求容量が少なくなっています	保留中のPlatform Servicesリクエストの数が上限に近づいています。
プラットフォームサービスを利用できません	実行中または利用可能な状態の、 RSM サービスを搭載したストレージノードがサイトで不足しています。

ストレージボリュームのアラート

アラート名	製品説明
ストレージボリュームで対応が必要です	ストレージボリュームはオフラインで、対応が必要です。
ストレージボリュームをリストアする必要があります	ストレージボリュームがリカバリされたため、リストアが必要です。

アラート名	製品説明
ストレージボリュームはオフラインです	ストレージボリュームが5分以上オフラインになっている。
ストレージボリュームの再マウントが試行されました	ストレージボリュームがオフラインになり、自動再マウントがトリガーされました。ドライブの問題またはファイルシステムのエラーを示している可能性があります。
ボリュームのリストアでレプリケートデータの修復を開始できませんでした	修復されたボリュームのレプリケートデータの修復を自動的に開始できませんでした。

StorageGRID サービスのアラート

アラート名	製品説明
バックアップ構成を使用するnginxサービス	nginxサービスの設定が無効です。以前の設定が使用されています。
バックアップ設定を使用するnginx-gwサービス	nginx-gwサービスの設定が無効です。以前の設定が使用されています。
FIPSを無効にするにはリブートが必要です	セキュリティ ポリシーでは FIPS モードは必要ありませんが、FIPS モジュールが使用されています。
FIPSを有効にするにはリブートが必要です	セキュリティ ポリシーでは FIPS モードが必要ですが、FIPS モジュールは使用されていません。
バックアップ設定を使用したSSHサービス	SSHサービスの設定が無効です。以前の設定が使用されています。

テナントアラート

アラート名	製品説明
テナントクォータの使用率が高い	クォータスペースの使用率が高くなっています。通知の原因 が多すぎる可能性があるため、このルールはデフォルトで無効になっています。

StorageGRIDでよく使用される**Prometheus**メトリクス

デフォルトのアラートルールの条件を詳しく理解したり、カスタムのアラートルールの条件を作成したりするには、ここに示すPrometheus指標のよく使用されるリストを参照してください。

あなたもできますすべての指標の完全なリストを取得します。

Prometheusクエリの構文の詳細については、 "クエリの基本"を参照してください。

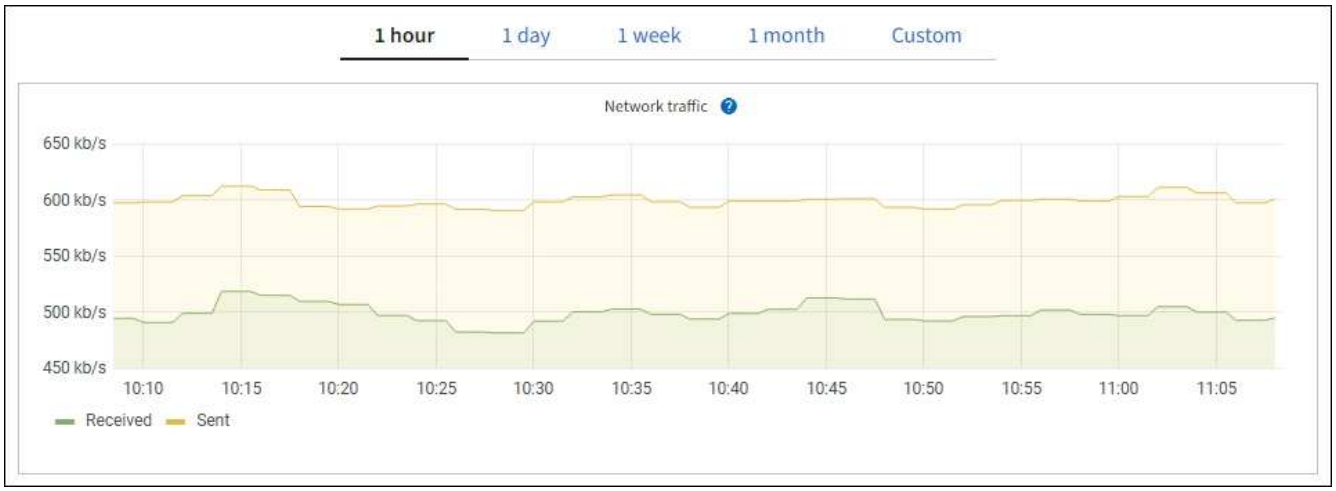
Prometheus指標とは

Prometheus指標は時系列の測定値です。管理ノードのPrometheusサービスは、すべてのノード上のサービスからこれらの指標を収集します。指標は、 Prometheus データ用にリザーブされたスペースがフルになるまで各管理ノードに保存されます。ボリュームの容量が上限に達すると、 `/var/local/mysql_ibdata/`最も古い指標から順に削除されます。

Prometheus指標はどこで使用されますか？

Prometheusで収集された指標は、Grid Managerのいくつかの場所で使用されます。

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



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

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

- サポート > ツール > 診断 ページと サポート > ツール > メトリック ページ: これらのページは主にテクニカル サポートによる使用を目的としており、Prometheus メトリックの値を使用するいくつかのツールとグラフを提供します。

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

次に、よく使用されるPrometheus指標を示します。

> 名前に_private_が含まれる指標は内部使用のみを目的としており、StorageGRID のリリース間で予告なく変更される場合があります。

alertmanager_notifications_failed_total

失敗したアラート通知の総数。

Node_filesystem_avail_bytes です

root以外のユーザが使用できるファイルシステムスペースの量（バイト）。

node_memory_MemAvailable_bytes

Memory information （メモリ情報）フィールド MemAvailable_bytes 。

Node_network_carrier

のキャリア値 `/sys/class/net/iface`。

Node_network_receate_errs_total

ネットワークデバイスの統計 `receive_errs`情報。

Node_network_transmit_errs_total

ネットワークデバイスの統計 `transmit_errs`情報。

storagegrid_administrative_down

想定内の理由でノードがグリッドに接続されていません。たとえば、ノードまたはノード上のサービスが正常にシャットダウンされた、ノードがリブート中である、ソフトウェアのアップグレード中であるなどの原因が考えられます。

storagegrid_apply_compute_controller_hardware_status

アプライアンスのコンピューティングコントローラハードウェアのステータス。

storagegrid_apply_failed_disks を指定します

アプライアンス内のストレージコントローラの場合、最適な状態でないドライブの数。

storagegrid_apply_storage_controller_hardware_status

アプライアンス内のストレージコントローラハードウェアの全体的なステータス。

storagegrid_content_bbuckets_or_containers

このストレージノードが認識している S3 バケットの合計数。

storagegrid_content_objects を参照してください

このストレージ ノードが認識している S3 データ オブジェクトの合計数。カウントは、S3 を介してシステムとインターフェースするクライアント アプリケーションによって作成されたデータ オブジェクトに対してのみ有効です。

storagegrid_content_objects_lost

StorageGRID システムに存在しないことが検出されたオブジェクトの合計数。損失の原因 を特定し、リカバリが可能かどうかを確認する必要があります。

"失われたオブジェクトデータと欠落しているオブジェクトデータのトラブルシューティング"

storagegrid_http_session_ining_attempted 」というメッセージが表示されます

ストレージノードに対して試行された HTTP セッションの総数。

storagegrid_http_session_ining_currently established

ストレージノード上で現在アクティブな（開いている） HTTP セッションの数。

storagegrid_http_session_ining_failed

不正な形式の HTTP 要求または処理中のエラーが原因で、正常に完了しなかった HTTP セッションの総数。

storagegrid_http_session_ining_successful

正常に完了した HTTP セッションの総数。

storagegrid_ilm_Awaiting _background_objects

スキャンによる ILM に評価を待機しているこのノード上のオブジェクトの合計数です。

storagegrid_ilm_Awaiting _client_evaluation_objects_per_second

このノードで ILM ポリシーに照らしてオブジェクトが評価されている現在の速度です。

storagegrid_ilm_Awaiting _client_objects

クライアント処理（取り込みなど）の ILM に評価を待機しているこのノード上のオブジェクトの合計数です。

storagegrid_ilm_Awaiting _total_objects

ILM 評価を待っているオブジェクトの合計数です。

storagegrid_ilm_scan_objects_per_second

このノードが所有するオブジェクトが ILM 用にスキャンされてキューに登録される速度です。

storagegrid_ilm_scan_periodEstimated _ minutes （ **StorageGRID _ ILM _** スキャン期間 _ 推定 _ 分）

このノードで ILM のフルスキャンが完了するまでの推定時間です。

- 注： * フルスキャンは、このノードが所有するすべてのオブジェクトに ILM が適用されたことを保証するものではありません。

storagegrid_load-balancer _endpoint_cert_expiry_time

エポックからのロードバランサエンドポイント証明書の有効期限（秒数）。

storagegrid_meta_query_average _latency _milliseconds

このサービスを使用してメタデータストアに対してクエリを実行するのに必要な平均時間。

storagegrid_network_received_bytes

インストール後に受信したデータの総容量。

storagegrid_network_transmitted _bytes

インストール後に送信されたデータの総容量。

storagegrid_node_name

使用可能な CPU 時間のうち、このサービスが現在使用している割合。サービスのビジー状態を示します。使用可能な CPU 時間は、サーバの CPU 数によって異なります。

storagegrid_ntp_Chosen_time_source_offset_milliseconds

選択した時間ソースによって提供される体系的な時間オフセット。オフセットは、時間ソースに到達するまでの遅延が、時間ソースが NTP クライアントに到達するために必要な時間と等しくない場合に適用されます。

storagegrid_ntp_locked

ノードがネットワークタイムプロトコル（NTP）サーバにロックされていません。

storagegrid_s3_data_transfers_bytes_ingested

属性の前回リセット後に S3 クライアントからこのストレージノードに取り込まれたデータの総容量。

storagegrid_s3_data_transfers_bytes_retrieved

属性の前回リセット後に S3 クライアントがこのストレージノードから読み出したデータの総容量。

storagegrid_s3_operations_failed

失敗した S3 処理（ HTTP ステータスコード 4xx と 5xx ）の総数。 S3 の認証エラーが原因のものは除きます。

storagegrid_s3_operations_successful

成功した S3 処理（ HTTP ステータスコード 2xx ）の総数。

storagegrid_s3_operations_unauthorized

認証エラーが原因で失敗した S3 処理の総数。

storagegrid_servercertificate_management_interface_cert_expiry_days のように指定します

管理インターフェイス証明書が期限切れになるまでの日数。

storagegrid_servercertificate_storage_api_endpoints_cert_expiry_days のように指定します

オブジェクトストレージ API 証明書が期限切れになるまでの日数。

storagegrid_service_cpu_seconds で指定します

インストール後にこのサービスが CPU を使用した時間の累計。

storagegrid_service_memory_usage_bytes

このサービスが現在使用しているメモリ（ RAM ）の容量。この値は、 Linux の top ユーティリティで RES として表示される値と同じです。

storagegrid_service_network_received_bytes

インストール後にこのサービスが受信したデータの総容量。

storagegrid_service_network_transmitted バイト数

このサービスから送信されたデータの総容量。

storagegrid_service_restarts

サービスが再起動された回数。

storagegrid_service_runtime_seconds

インストール後にサービスが実行されていた合計時間。

storagegrid_service_uptime</1> を指定します

前回のサービス再起動以降にサービスが実行されていた時間の合計。

storagegrid_storage_state_current

ストレージサービスの現在の状態。属性値は次のとおりです。

- 10 = オフライン
- 15 = メンテナンス
- 20 = 読み取り専用
- 30 = オンライン

storagegrid_storage_status のように指定します

ストレージサービスの現在のステータス。属性値は次のとおりです。

- 0 = エラーなし
- 10 = 移行中
- 20 = 空きスペースが不足しています
- 30 = ボリュームを使用できません
- 40= エラー

storagegrid_storage_utilization_data_bytes

ストレージノード上のレプリケートオブジェクトデータとイレイジャーコーディングオブジェクトデータの推定合計サイズ。

storagegrid_storage_utilization_meta_allowed_bytes

オブジェクトメタデータに使用できる各ストレージノードのボリューム 0 上の合計スペース。この値は、ノードでメタデータ用にリザーブされている実際のスペースよりも常に小さくなります。これは、重要なデータベース処理（コンパクションや修復など）や将来のハードウェアおよびソフトウェアのアップグレードに必要なリザーブスペースの一部が必要なためです。オブジェクトメタデータ用の許可スペースは、オブジェクトの全体的な容量を制御します。

storagegrid_storage_utilization_metadata_bytes

ストレージボリューム 0 上のオブジェクトメタデータのバイト数。

storagegrid_storage_utilization_total_space_bytes

すべてのオブジェクトストアに割り当てられているストレージスペースの総容量。

storagegrid_storage_utilization_usable_space_bytes

オブジェクトストレージスペースの残り容量。ストレージノード上のすべてのオブジェクトストアの使用可能スペースを合計して算出されます。

storagegrid_stenantUsagedata_bytes

テナントのすべてのオブジェクトの論理サイズ。

storagegrid_stenantUsageobject_count

テナントのオブジェクトの数。

storagegrid_tenant_dusation_QUOTA_bytes

テナントのオブジェクトに使用できる論理スペースの最大容量。クォータ指標を指定しない場合、使用可能なスペースは無制限です。

すべての指標のリストを取得します

すべての指標のリストを取得するには、グリッド管理APIを使用します。

手順

1. Grid Managerの上部でヘルプアイコンを選択し、*[API documentation]*を選択します。
2. 指標 * 処理を探します。
3. 操作を実行し `GET /grid/metric-names`ます。
4. 結果をダウンロードします。

ログファイル参照

StorageGRID ログファイル

StorageGRID には、イベント、診断メッセージ、およびエラー状態をキャプチャするために使用されるログが用意されています。テクニカルサポートにトラブルシューティングを依頼すると、ログファイルを収集して転送するように求められることがあります。

ログは次のように分類されます。

- "StorageGRID ソフトウェアのログ"
- "導入とメンテナンスのログ"
- "bycast.log について"

> 各ログタイプの詳細情報は参考用です。これらのログは、テクニカルサポートが高度なトラブルシューティングに使用することを目的としています。監査ログやアプリケーションログファイルを使用して問題の履歴を再構築する高度な手法については、この手順では説明していません。

ログにアクセスします

ログにアクセスするには、"ログファイルとシステムデータを収集します" 1 つ以上のノードから単一のログ ファイル アーカイブとして保存します。または、次のようにして各グリッド ノードの個別のログ ファイルにアクセスすることもできます。

手順

1. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
2. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。
3. 次のコマンドを入力してrootに切り替えます。 `su -`

4. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

syslogサーバへのログのエクスポート

ログをsyslogサーバにエクスポートすると、次の機能が提供されます。

- S3 リクエストに加えて、すべての Grid Manager および Tenant Manager リクエストのリストを受け取ります。
- 監査ログメソッドが原因でパフォーマンスに影響を与えることなく、エラーを返すS3要求の可視性が向上します。
- 解析が容易なHTTPレイヤ要求およびエラーコードへのアクセス。
- ロードバランサでトラフィック分類機能によってブロックされた要求の可視性が向上します。

ログをエクスポートするには、"ログ管理と外部Syslogサーバーを構成する" 。

ログファイルのカテゴリ

StorageGRID ログファイルアーカイブには、カテゴリごとに説明されているログ、およびメトリックと debug コマンドの出力が含まれている追加ファイルが含まれています。

アーカイブの場所	製品説明
acct-tunnel.log	ロードバランサーと連携するアカウントトンネルヘルパーのログ。
監査	通常のシステム動作中に生成される監査メッセージです。
base-os-logs	StorageGRID イメージのバージョンなど、ベースとなるオペレーティングシステムの情報。
バンドル	グローバル構成情報（バンドル）。
キャッシュサービス	サービス ログをキャッシュします (ゲートウェイ ノードのみ)。
Cassandra	Cassandra データベース情報と Reaper 修復ログ。
EC	現在のノードに関するVCS情報と、プロファイルIDによるECグループ情報。
グリッド（ Grid ）	一般的なグリッドログ（デバッグを含む(`bycast.log`）と `servermanager`ログ。
grid.json	グリッド構成ファイルをすべてのノードで共有また、 `node.json`は現在のノードに固有です。
シュラウド	ハイアベイラビリティグループの指標とログ。
インストール	`Gdu-server`インストールログを確認します。

アーカイブの場所	製品説明
internal-access.log	内部HTTPプロキシのトラフィックログ。
Lambda - アービトレータ	S3 Select プロキシ要求に関連するログです。
リークされた	leakd サービスからのログ。
lumberjack.log	ログ収集に関連するデバッグメッセージ。
manage-audit.log	`mgmt-api`監査ログにアクセスします。
指標	Grafana 、 Jaeger 、ノードエクスポータ、および Prometheus のサービスログ。
計算ミス	Miscd アクセスログとエラーログ。
MySQL	MariaDB データベースの設定と関連ログ。
ネット	ネットワーク関連のスクリプトおよび Dyip サービスによって生成されるログ。
nginx	ロードバランサとグリッドフェデレーションの設定ファイルとログ。Grid Manager と Tenant Manager のトラフィックログも含まれます。

アーカイブの場所	製品説明

nginx-gw と入力します	• `access.log`：Grid ManagerおよびTenant Manager要求のログメッセージ。
	◦ これらのメッセージは、syslogを使用してエクスポートする場合にプレフィックスとして付加されます `mgmt:`。
	◦ これらのログ・メッセージの形式は次のとおりです。
	`[$time_iso8601] $remote_addr $status $bytes_sent $request_length $request_time "$endpointId" "$request" "$http_host" "$http_user_agent" "$http_referer"`
	• `cgr-access.log.gz`：インバウンドのクロスグリッドレプリケーション要求。
	◦ これらのメッセージは、syslogを使用してエクスポートする場合にプレフィックスとして付加されます `cgr:`。
	◦ これらのログ・メッセージの形式は次のとおりです。
	`[$time_iso8601] $remote_addr $status $bytes_sent $request_length $request_time "$endpointId" "$upstream_addr" "$request" "$http_host"`
	• `endpoint-access.log.gz`: ロードバランサーエンドポイントへの S3 リクエスト。
	◦ これらのメッセージは、syslogを使用してエクスポートする場合にプレフィックスとして付加されます `endpoint:`。
	◦ これらのログ・メッセージの形式は次のとおりです。
	`[$time_iso8601] $remote_addr $status $bytes_sent $request_length $request_time "$endpointId" "$upstream_addr" "$request" "$http_host"`
	• `nginx-gw-dns-check.log`：新しいDNSチェックアラートに関連します。
	• stream-access.log：ストリームブロックの TCP/TLS ストリーム（レイヤー 4）プロキシセッション。
	注：これはHTTPリクエストログではありません。

NTP	NTP 構成ファイルとログ：
孤立オブジェクト	孤立したオブジェクトに関するログ。
OS	ノードとグリッドの状態ファイル（サービスを含む `pid`）。
その他	にあるログファイルは `/var/local/log`、他のフォルダに収集されません。
パフォーマンス	CPU 、ネットワーク、ディスク I/O のパフォーマンス情報
prometheus-data	ログ収集に Prometheus データが含まれている場合、現在の Prometheus 指標。

アーカイブの場所	製品説明
プロビジョニング	グリッドのプロビジョニングプロセスに関連するログです。
ラフト	プラットフォームサービスで使用される Raft クラスタのログ。
revision_history.json	改訂履歴。
routed-s3-access.log.gz	S3（グローバルネームスペース/フェデレーション URL）のようにルーティングされるグリッドフェデレーショントラフィックのアクセスログ。
SSH	SSHの設定およびサービスに関連するログ。
SNMP	SNMP通知の送信に使用するSNMPエージェントの設定。
ソケット - データ	ネットワークデバッグ用のソケットデータ。
system-bucket.log	`update-system-bucket-configuration.log`：システムバケットのログ。
system-commands.txt	StorageGRID コンテナコマンドの出力。ネットワークやディスクの使用状況などのシステム情報が含まれます。
synchronize-recovery-package	ADC サービスをホストするすべての管理ノードとストレージ ノード間で最新のリカバリ パッケージの一貫性を維持することに関連します。
update-cipher-configurations.log	`update-cors-configurations.log`：TLS/暗号化方式およびCORSの変更に関連するログをトレースします。
update-leakd-configurations.log	孤立検出設定ログ。

StorageGRID ソフトウェアのログ

StorageGRID のログを問題のトラブルシューティングに使用できます。

ログを外部のSyslogサーバーに送信したり、監査情報の送信先を変更したりする場合は、`bycast.log`そして `nms.log`、 見る"ログ管理を構成する"。

一般的な **StorageGRID** ログです

ファイル名	脚注	にあります
/var/local/log/bycast.log	主要なStorageGRIDトラブルシューティング ファイル。	すべてのノード

ファイル名	脚注	にあります
/var/local/log/bycast-err.log	のサブセットが含まれています `bycast.log`(重大度が ERROR および CRITICAL のメッセージ)。 CRITICAL メッセージもシステムに表示されます。	すべてのノード
/var/local/core/	プログラムが異常終了した場合に作成されるコアダンプファイルが格納されます。原因としては、アサーションエラー、違反、スレッドのタイムアウトなどが考えられます。 注：ファイル ``/var/local/core/kexec_cmd`は通常アプライアンスノードに存在し、エラーを示すものではありません。	すべてのノード

暗号関連のログ

ファイル名	脚注	にあります
/var/local/log/ssh-config-generation.log	SSH設定の生成およびSSHサービスのリロードに関連するログが記録されます。	すべてのノード
/var/local/log/nginx/config-generation.log	nginx構成の生成とnginxサービスのリロードに関連するログが記録されます。	すべてのノード
/var/local/log/nginx-gw/config-generation.log	nginx-gw構成の生成（およびnginx-gwサービスのリロード）に関連するログが記録されます。	管理ノードとゲートウェイノード
/var/local/log/update-cipher-configurations.log	TLSおよびSSHポリシーの設定に関連するログが記録されます。	すべてのノード

グリッドフェデレーションログ

ファイル名	脚注	にあります
/var/local/log/update（grid_federation_config.log）	グリッドフェデレーション接続用のnginx構成とnginx-gw構成の生成に関連するログが記録されます。	すべてのノード

NMS ログ

ファイル名	脚注	にあります
/var/local/log/nms.log	• Grid Manager と Tenant Manager からの通知が記録されます。 • NMSサービスの処理に関連するイベントが記録されます。たとえば、Eメール通知や設定の変更などです。 • システムで行われた設定の変更に伴う XML バンドルの更新が格納されます。 • 1 日に 1 回実行される属性のダウンサンプリングに関連するエラーメッセージが格納されます。 • ページ生成エラーや HTTP ステータス 500 エラーなど、 Java Web サーバのエラーメッセージが格納されます。 • AutoSupport に関連するログが含まれています。	管理ノード
/var/local/log/nms.errlog	MySQL データベースのアップグレードに関連するエラーメッセージが格納されます。 対応するサービスの標準エラー（ stderr ）ストリームが格納されます。サービスごとに 1 つのログファイルがあります。これらのファイルは、サービスに問題がなければ通常は空になります。	管理ノード
/var/local/log/nms.requestlog	管理 API から内部 StorageGRID サービスへの発信接続に関する情報が含まれます。	管理ノード

Server Manager のログです

ファイル名	脚注	にあります
/var/local/log/servermanager.log	サーバで実行されている Server Manager アプリケーションのログファイルです。	すべてのノード
/var/local/log/GridstatBackend.errlog	Server Manager GUI バックエンドアプリケーションのログファイルです。	すべてのノード

ファイル名	脚注	にあります
/var/local/log/gridstat.errlog	Server Manager GUI のログファイルです。	すべてのノード

StorageGRID サービスのログ

ファイル名	脚注	にあります
/var/local/log/acct.errlog		ADC サービスを実行しているストレージノード
/var/local/log/adc.errlog	対応するサービスの標準エラー（ stderr ）ストリームが格納されます。サービスごとに 1 つのログファイルがあります。これらのファイルは、サービスに問題がなければ通常は空になります。	ADC サービスを実行しているストレージノード
/var/local/log/ams.errlog		管理ノード
/var/local/log/cache-svc.log + /var/local/log/cache-svc.errlog	サービスのログをキャッシュします。	ゲートウェイノード
/var/local/log/cassandra/system.log	メタデータストア（ Cassandra データベース）の情報。新しいストレージノードの追加時に問題が発生した場合、または nodetool repair タスクが停止した場合に使用できます。	ストレージノード
/var/local/log/cassandra-reaper.log	Cassandra Reaper サービスの情報。 Cassandra データベース内のデータの修復を実行します。	ストレージノード
/var/local/log/cassandra-reaper.errlog	Cassandra Reaper サービスのエラー情報。	ストレージノード
/var/local/log/chunk.errlog		ストレージノード
/var/local/log/cmn.errlog		管理ノード
/var/local/log/cms.errlog	このログファイルは、古いバージョンの StorageGRID からアップグレードされたシステムに存在する場合があります。古い情報が含まれています。	ストレージノード
/var/local/log/dds.errlog		ストレージノード

ファイル名	脚注	にあります
/var/local/log/dmv.errlog		ストレージノード
/var/local/log/dynip *	グリッドで IP の動的な変更を監視してローカル設定を更新する dynip サービスに関連するログが記録されます。	すべてのノード
/var/local/log/grafana.log	Grid Manager で指標を視覚化するために使用される Grafana サービスに関連付けられたログ。	管理ノード
/var/local/log/hagroups.log	ハイアベイラビリティグループに関連付けられているログ。	管理ノードとゲートウェイノード
/var/local/log/hagroups（events.log）	バックアップからマスターまたは障害への移行など、状態の変化を追跡します。	管理ノードとゲートウェイノード
/var/local/log/idnt.errlog		ADC サービスを実行しているストレージノード
/var/local/log/jaeger.log	Jaeger サービスに関連付けられたログ。これは、トレース収集に使用されます。	すべてのノード
/var/local/log/kstn.errlog		ADC サービスを実行しているストレージノード
/var/local/log/lambda *	S3 Select サービスのログが記録されます。	管理ノードとゲートウェイノード このログは特定の管理ノードとゲートウェイノードにのみ記録されます。を参照してください"S3 Select の管理ノードとゲートウェイノードの要件と制限事項"。
/var/local/log/ldr.errlog		ストレージノード

ファイル名	脚注	にあります
/var/local/log/miscd/*。log	MISCd （ Information Service Control Daemon ）サービスのログが記録されます。このサービスは、他のノード上のサービスの照会と管理、およびノードの環境設定の管理（他のノードで実行されているサービスの状態の照会など）を行うためのインターフェイスを提供します。	すべてのノード
/var/local/log/nginx/*。log	nginx サービスのログが記録されます。このサービスは、各種のグリッドサービス（ Prometheus や dynip など）が HTTPS API を介して他のノード上のサービスと通信できるようにするための、認証とセキュアな通信のメカニズムとして機能します。	すべてのノード
/var/local/log/nginx-gw/*。log	nginx-gwサービスに関連する一般的なログ（エラーログ、管理ノード上の制限された管理ポートのログなど）が記録されます。	管理ノードとゲートウェイノード
/var/local/log/nginx-gw/cgr-access.log。gz	グリッド間レプリケーショントラフィックに関連するアクセスログが記録されます。	グリッドフェデレーション設定に応じて、管理ノード、ゲートウェイノード、またはその両方を選択します。グリッド間レプリケーションのデスティネーショングリッドでのみ検出されます。
/var/local/log/nginx-gw/endpoint-access.log。gz	クライアントからストレージノードへのS3トラフィックのロードバランシングを提供するロードバランササービスのアクセスログが記録されます。	管理ノードとゲートウェイノード
/var/local/log/persistence *	Persistence サービスのログが記録されます。このサービスは、リブート後も維持する必要があるルートディスク上のファイルを管理します。	すべてのノード

ファイル名	脚注	にあります
/var/local/log/prometheus.log	すべてのノードを対象に、 node exporter サービスのログと ade-exporter サービスのログが記録されます。 管理ノードについては、 Prometheus サービスと Alert Manager サービスのログも記録されます。	すべてのノード
/var/local/log/raft.log	RSM サービスで Rraft プロトコルに使用されるライブラリの出力が含まれます。	RSM サービスを搭載しているストレージノードです
/var/local/log/rms.errlog	S3 プラットフォームサービスで使用される Replicated State Machine （ RSM ）サービスのログが記録されます。	RSM サービスを搭載しているストレージノードです
/var/local/log/ssm.errlog		すべてのノード
/var/local/log/update-s3vs - domains.log	S3 仮想ホストドメイン名設定の更新の処理に関連するログが記録されます。 S3 クライアントアプリケーションを実装する手順を参照してください。	管理ノードとゲートウェイノード
/var/local/log/update-snmp-firewall *	SNMP 用に管理されているファイアウォールポートに関連するログが記録されます。	すべてのノード
/var/local/log/update-sysl.log	システムの syslog 設定に対する変更に関連するログが記録されます。	すべてのノード
/var/local/log/update-traffic-classes.log	トラフィック分類子設定の変更に関連するログが含まれます。	管理ノードとゲートウェイノード
/var/local/log/update-utcn.log	このノードでの「信頼されていないクライアントネットワーク」モードに関連するログが記録されます。	すべてのノード

関連情報

- "bycast.log について"
- "S3 REST APIを使用する"

StorageGRIDの導入とメンテナンスのログ

導入とメンテナンスのログを問題のトラブルシューティングに使用できます。

ファイル名	脚注	にあります
/var/local/log/install.log	ソフトウェアのインストール時に作成されます。インストールイベントが記録されます。	すべてのノード
/var/local/log/expansion-progress.log	拡張処理中に作成されます。拡張イベントが記録されます。	ストレージノード
/var/local/log/pa-move.log	スクリプトの実行中に作成され `pa-move.sh`ます。	プライマリ管理ノード
/var/local/log/pa-move-new（pa.log）	スクリプトの実行中に作成され `pa-move.sh`ます。	プライマリ管理ノード
/var/local/log/pa-move-old（pa.log）	スクリプトの実行中に作成され `pa-move.sh`ます。	プライマリ管理ノード
/var/local/log/gdu-server.log	GDU サービスによって作成されます。プライマリ管理ノードによって管理されるプロビジョニングとメンテナンスの手順に関連するイベントが記録されます。	管理ノード
/var/local/log/send（admin_hw.log）	インストール時に作成されます。プライマリ管理ノードとの通信に関連するデバッグ情報が記録されます。	すべてのノード
/var/local/log/upgrade.log	ソフトウェアのアップグレード中に作成されます。ソフトウェア更新イベントが記録されます。	すべてのノード

StorageGRID bycast.log について学ぶ

ファイル `/var/local/log/bycast.log`は、StorageGRIDソフトウェアのトラブルシューティングに使用する主要なファイルです。ファイルはグリッドノードごとに1つあり `bycast.log`ます。ファイルに、そのグリッドノードに固有のメッセージが含まれています。

ファイル `/var/local/log/bycast-err.log`はのサブセットです `bycast.log`。ERROR と CRITICAL の重大度のメッセージが含まれています。

必要に応じて、監査ログの送信先を変更し、監査情報を外部の syslog サーバーに送信することもできます。外部 Syslog サーバーが構成されている場合、監査レコードのローカル ログは引き続き生成され、保存されます。見る"ログ管理と外部Syslogサーバーを構成する" 。

bycast.log ファイルのローテーション

ファイルが1GBに達すると、 `bycast.log`既存のファイルが保存され、新しいログファイルが開始されます。

保存されたファイルの名前が変更され `bycast.log.1`、新しいファイルの名前がになり `bycast.log`ます。新しいが1GBに達すると `bycast.log`、 `bycast.log.1`が圧縮されてという名前に変更され、の名前がに変更さ `bycast.log.2.gz`れ `bycast.log.1`ます。 `bycast.log`

のローテーションの上限 `bycast.log`は21ファイルです。ファイルの22番目のバージョンが作成されると`bycast.log`、最も古いファイルが削除されます。

のローテーションの上限 `bycast-err.log`は7ファイルです。

> 圧縮されたログファイルは、ファイルが圧縮された同じ場所に解凍しないでください。ファイルを同じ場所で解凍すると、ログローテーションスクリプトの妨げになることがあります。

必要に応じて、監査ログの送信先を変更し、監査情報を外部の syslog サーバーに送信することもできます。外部 Syslog サーバーが構成されている場合、監査レコードのローカル ログは引き続き生成され、保存されます。見る"ログ管理と外部Syslogサーバーを構成する" 。

関連情報

"ログファイルとシステムデータを収集"

bycast.log のメッセージです

のメッセージ `bycast.log`は、Asynchronous Distributed Environment（ADE；非同期分散環境）によって書き込まれます。ADE は、グリッドノードの各サービスで使用されるランタイム環境です。

ADE のメッセージの例：

```
May 15 14:07:11 um-sec-rg1-agn3 ADE: |12455685    0357819531
SVMR EVHR 2019-05-05T27T17:10:29.784677| ERROR 0906 SVMR: Health
check on volume 3 has failed with reason 'TOUT'
```

ADE のメッセージには次の情報が含まれています。

メッセージセグメント	例の値
ノードID	12455685
ADEプロセスID	0357819531
モジュール名	SVMR
メッセージ ID	EVHR
UTC システム時間	2019-05-05T27T17：10：29.784677（YYY-MM-DDTHH：MM：SS.uuuuu）
重大度レベル	エラー
内部追跡番号	0906

メッセージセグメント	例の値
メッセージ	SVMR ：ボリューム 3 のヘルスチェックが失敗しました。理由：「 TOUT 」

bycast.log のメッセージの重大度

のメッセージ `bycast.log`には重大度レベルが割り当てられています。

例：

- *notice *-- 記録すべきイベントが発生しました。ほとんどのログメッセージはこのレベルです。
- * warning * — 予期しない状態が発生しました。
- * error * — 操作に影響を与える大きなエラーが発生しました。
- * critical * — 異常な状態が発生し、通常の動作が停止しました。原因となった状態にすぐに対処する必要があります。

のエラーコード `bycast.log`

のほとんどのエラーメッセージ `bycast.log`にはエラーコードが含まれています。

次の表に、の一般的な非数値コードを示し `bycast.log`ます。非数値コードの正確な意味は、レポートされるコンテキストによって異なります。

エラーコード	意味
SUCS	エラーはありません
GERR	不明
CANC	キャンセル済み
ABRT	中止
TOUT	タイムアウト
INVL	無効
NFND	見つかりません
vers	バージョン
会議	構成
失敗	失敗

エラーコード	意味
ICPL	不完全
完了しました	完了
SUNV	サービスを利用できません

次の表に、の数値エラーコードを示し `bycast.log`ます。

エラー番号	エラーコード	意味
001	EPERM	操作は許可されません
002	ENOENT	指定したファイルまたはディレクトリは存在しません
003	ESRCH	そのようなプロセスはありません
004	EINTR	システムコールが中断されました
005	EIO	I/Oエラー
006	ENXIO	該当するデバイスまたはアドレスはありません
007	E2BIG	引数リストが長すぎます
008	ENOEXEC	EXEC フォーマットエラー
009	EBADF	ファイル番号が正しくありません
010	ECHILD	子プロセスはありません
011	EAGAIN	再試行
012	ENOMEM	メモリ不足です
013	EACCES	権限が拒否されました
014	デフォルト	アドレスが無効です
015	ENOTBLK	ブロックデバイスが必要です
016	EBUSY	デバイスまたはリソースがビジー

エラー番号	エラーコード	意味
017	EEXIST	ファイルが存在します
018	EXDEV の場合	クロスデバイスリンク
019	ENODEV	該当するデバイスはありません
020	ENOTDIR	ディレクトリではありません
021	EISDIR	はディレクトリです
022	EINVAL	引数が無効です
023	ENFILE	ファイルテーブルオーバーフローです
024	EMFILE	開いているファイルが多すぎます
025	ENOTTY	タイプライターではありません
026	ETXTBSY	テキストファイルがビジーです
027	EFBIG	ファイルが大きすぎます
028	ENOSPC	デバイスにスペースが残っていません
029	ESPIPE	不正なシークです
030	EROFS	読み取り専用ファイルシステム
031	EMLINK	リンクが多すぎます
032	EPIPE	パイプ破損
033	エドム	関数のドメイン外の数学引数
034	エスランゲ	数学結果は表現できません
035	EDEADLK	リソースのデッドロックが発生する
036	ENAMETOOLONG	ファイル名が長すぎます
037	ENOLCK	使用可能なレコードロックがありません

エラー番号	エラーコード	意味
038	ENOSYS	関数が実装されていません
039	ENOTEMPTY	ディレクトリが空ではありません
040	ELOOP	シンボリックリンクが多すぎます
041		
042	ENOMSG	必要なタイプのメッセージがありません
043	EIDRM	識別子が削除されました
044	ECHRNG	チャネル番号が範囲外です
045	EL2NSYNC	レベル 2 が同期されていません
046	EL3HLT	レベル3停止
047	EL3RST	レベル 3 リセット
048	ELNRNG	リンク番号が範囲外です
049	EUNATCH	プロトコルドライバが接続されていません
050	ENOCSI	CSI 構造がありません
051	EL2HLT	レベル2停止
052	EBADE の実行	無効な交換です
053	EBADR	無効な要求記述子です
054	EXFULL （完全）	Exchange がいっぱいです
055	ENOANO	アノードなし
056	EBADRQC	無効な要求コードです
057	EBADSLT	無効なスロットです
058		

エラー番号	エラーコード	意味
059	EBFONT	フォントファイルの形式が正しくありません
060	ENOSTR	デバイスはストリームではありません
061	ENODATA	使用できるデータがありません
062	イータイム	タイマー期限切れ
063	ENOSR	Out of Streams のリソース
064	ENONET	マシンがネットワーク上にありません
065	ENOPKG	パッケージがインストールされていません
066	EREMOTE	オブジェクトがリモートです
067	ENOLINK	リンクが切断されました
068	EADV	アドバタイズエラー
069	ESRMNT	Srmount エラー
070	エコム	送信時の通信エラーです
071	EPROTO	プロトコルエラー
072	EMULTIHOP	マルチホップが試行されました
073	EDOTDOT	RFS 固有のエラー
074	EBADMSG と入力します	データメッセージではありません
075	EOVERFLOW	定義されたデータ型の値が大きすぎます
076	ENOTUNIQ	名前がネットワーク上で一意ではありません
077	EBADFD	ファイル記述子が無効な状態です
078	エルム変更	リモートアドレスが変更されました
079	ELIBACC	必要な共有ライブラリにアクセスできません

エラー番号	エラーコード	意味
080	ELIBBAD 社	破損した共有ライブラリにアクセスしています
081	ELIBSCN	
082	ELIBMAX	リンクしようとしている共有ライブラリが多すぎます
083	ELIBEXEC	共有ライブラリを直接実行することはできません
084	EILSEQ	不正なバイトシーケンスです
085	ERESTART	中断されたシステムコールを再開する必要があります
086	ESTRPIPE	ストリームパイプエラー
087	EUSERS	ユーザが多すぎます
088	ENOTSOCK	ソケット以外でのソケット操作
089	EDESTADDRREQ	送信先アドレスは必須です
090	エMSGSIZE	メッセージが長すぎます
091	EPROTOTYPE	ソケットのプロトコルタイプが正しくありません
092	ENOPROTOOPT	プロトコルを使用できません
093	EPROTONOSUPPORT	サポートされていないプロトコルです
094	ESOCKTNOSUPPORT の略	ソケットタイプはサポートされていません
095	EOPNOZ TSUPP	この処理は転送エンドポイントではサポートされません
096	EPFNOSUPPORT	サポートされていないプロトコルファミリーです
097	EAFNOSUPPORT	アドレスファミリーはプロトコルでサポートされていません
098	EADDRINUSE	アドレスはすでに使用されています

エラー番号	エラーコード	意味
099	EADDRNOTAVAIL	要求されたアドレスを割り当てることができません
100	ENETDOWN	ネットワークが停止しています
101	ENETUNREACH	ネットワークに到達できません
102	ENETRESET	リセットのためネットワークが接続を切断しました
103	ECONNABORTED	ソフトウェアが原因で接続が終了しました
104	ECONNRESET	ピアによって接続がリセットされました
105	ENOBUFS	使用可能なバッファスペースがありません
106	EISCONN	トランスポートエンドポイントはすでに接続されています
107	ENOTCONN	トランスポートエンドポイントが接続されていません
108	ESH ダウンタウン	トランスポートエンドポイントのシャットダウン後に送信できません
109	ETOOMANYREFS	参照が多すぎます：接続できません
110	ETIMEDOUT	接続がタイムアウトしました
111	ECONNREFUSED	接続が拒否されました
112	EHOSTDOWN	ホストが停止しています
113	EHOSTUNREACH	ホストへのルートがありません
114	エアルレーダド	処理をすでに実行中です
115	実行中	処理を実行中です
116		
117	EUCLEAN	構造はクリーニングが必要です
118	ENOTNAM	XENIX という名前のファイルではありません

エラー番号	エラーコード	意味
119	ENAVAIL	XENIX セマフォーがありません
120	EISNAM	は、名前付きタイプファイルです
121	EREMOTEIO	リモート I/O エラーです
122	EDQUOT	クォータを超過しました
123	ENOMEDIUM	メディアが見つかりません
124	EMEDIUMTYPE	メディアタイプが正しくありません
125	ECANCELED	処理がキャンセルされました
126	ENOKEY	必要なキーがありません
127	エクイメピ RED も含まれています	キーの有効期限が切れました
128	エーケヨヴォエド	キーが取り消されました
129	EKEYREJECTED	キーがサービスによって拒否されました
130	EOWNERDEAD の場合	堅牢な mutex のため : 所有者は死んだ
131	ENOTRECOVERABLE	堅牢な mutex の場合：状態は回復できません

ログ管理と外部**Syslog**サーバーを構成する

StorageGRIDの外部**syslog**サーバー

外部 syslog サーバは、 StorageGRID の外部にあるサーバであり、 1 箇所でシステム監査情報を収集できます。外部のsyslogサーバを使用すると、管理ノードのネットワークトラフィックを軽減し、情報をより効率的に管理できます。StorageGRIDの場合、発信syslogメッセージパケット形式はRFC 3164に準拠しています。

外部 syslog サーバに送信できる監査情報のタイプは次のとおりです。

- 通常のシステム運用中に生成された監査メッセージを含む監査ログ
- ログインやルートへのエスカレーションなど、セキュリティ関連のイベント
- アプリケーションログ：発生した問題 のトラブルシューティングのためにサポートケースをオープンする必要がある場合に要求されることがあります

外部**syslog**サーバを使用する状況

外部のsyslogサーバは、大規模なグリッドを使用する場合、複数のタイプのS3アプリケーションを使用する場合、またはすべての監査データを保持する場合に特に役立ちます。外部 syslog サーバに監査情報を送信すると、次のことが可能になります。

- 監査メッセージ、アプリケーションログ、セキュリティイベントなどの監査情報をより効率的に収集および管理します。
- 監査情報はさまざまなストレージノードから外部syslogサーバに直接転送されるため、管理ノードのネットワークトラフィックを削減します。管理ノードを経由する必要はありません。

> 外部syslogサーバにログを送信すると、8、192バイトを超える単一のログがメッセージの最後で切り捨てられ、外部syslogサーバの実装における一般的な制限事項に準拠します。

> 外部syslogサーバに障害が発生した場合にフルデータリカバリのオプションを最大限に活用するために、(`localaudit.log`各ノードに最大20GBのローカル監査レコードが保持されます。

外部**syslog**サーバの設定方法

外部Syslogサーバーの設定方法については、"ログ管理と外部Syslogサーバーを構成する" 。

TLSまたはRELP/TLSプロトコルを使用するように設定する場合は、次の証明書が必要です。

- サーバ**CA**証明書：PEMエンコードで外部syslogサーバを検証するための1つ以上の信頼されたCA証明書。省略すると、デフォルトの Grid CA 証明書が使用されます。
- クライアント証明書：PEMエンコードによる外部syslogサーバへの認証用のクライアント証明書。
- クライアント秘密鍵：PEMエンコードでのクライアント証明書の秘密鍵。

> クライアント証明書を使用する場合は、クライアント秘密鍵も使用する必要があります。暗号化された秘密鍵を指定する場合は、パスフレーズも指定する必要があります。暗号化された秘密鍵を使用した場合、セキュリティ上の大きなメリットはありません。これは、鍵とパスフレーズを格納する必要があるためです。暗号化されていない秘密鍵を使用することを推奨します（使用可能な場合）。

外部 **syslog** サーバのサイズを見積もる方法

通常、グリッドは、 1 秒あたりの S3 処理数または 1 秒あたりのバイト数で定義される、必要なスループットを達成するようにサイジングされます。たとえば、 1 秒あたりの S3 処理数が 1 、 000 件、つまり 1 秒あたり 2 、 000 MB のオブジェクトの取り込みと読み出しをグリッドで処理する必要があるとします。外部 syslog サーバのサイズは、グリッドのデータ要件に応じて決定する必要があります。

このセクションでは、外部 syslog サーバが処理可能である必要があるさまざまなタイプのログメッセージのレートと平均サイズを、グリッドの既知または望ましいパフォーマンス特性（ 1 秒あたりの S3 処理数）で見積もるためのヒューリスティック計算式をいくつか示します。

1 秒あたりの **S3** 処理数を推定式で使用します

グリッドをスループット用に 1 秒あたりのバイト数で表した場合、試算式を使用するには、このサイジング

を 1 秒あたりの S3 処理に変換する必要があります。グリッドのスループットを変換するには、最初に平均オブジェクトサイズを確認する必要があります。これには、既存の監査ログと指標の情報を使用するか（存在する場合）、 StorageGRID を使用するアプリケーションに関する知識が必要です。たとえば、グリッドのサイズが 2 、 000 MB/ 秒で、平均オブジェクトサイズが 2MB の場合、 1 秒あたり 1 、 000 S3 処理可能なサイズ（ 2 、 000 MB/ 秒）になるようにグリッドをサイジングしました。

以降のセクションで説明する外部 syslog サーバのサイジングの計算式は、一般的な推定値（ワーストケースの見積もり値ではありません）を示しています。設定やワークロードによっては、 syslog メッセージや syslog データの量が、式で予測される値よりも増減することがあります。式はガイドラインとしてのみ使用することを意図しています。

監査ログの推定式

グリッドでサポートされる 1 秒あたりの S3 処理数以外の S3 ワークロードに関する情報がない場合は、次の式を使用して、外部 syslog サーバで処理する必要がある監査ログのボリュームを推定できます。 監査レベルをデフォルト値のままにしておくという前提では、次のようになります（ [エラー] に設定されている [ストレージ] を除くすべてのカテゴリは [通常] に設定されています）。

```
Audit Log Rate = 2 x S3 Operations Rate
Audit Log Average Size = 800 bytes
```

たとえば、グリッドのサイズが 1 秒あたり 1 、 000 S3 処理の場合、 1 秒あたり 2 、 000 件の syslog メッセージをサポートするように外部 syslog サーバをサイジングし、 1 秒あたり 1.6 MB の割合で監査ログデータを受信（通常は格納）できるようにする必要があります。

ワークロードの詳細がわかっている場合は、より正確な概算が可能です。監査ログの場合、最も重要な追加変数は、PUT（GET）に対するS3処理の割合と、次のS3フィールドの平均サイズ（バイト）です（表で使用されている4文字の略語は監査ログのフィールド名です）。

コード	フィールド	製品説明
SACC	S3 テナントアカウント名（要求の送信者）	要求を送信したユーザのテナントアカウントの名前。匿名の要求の場合は空です。
SBAC	S3 テナントアカウント名（バケット所有者）	バケット所有者のテナントアカウント名。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。
S3BK	S3バケット	S3 バケット名。
S3KY	S3キー	バケット名を除く S3 キーの名前。バケットに対する処理では、このフィールドは指定されません。

P を使用して、 PUT の S3 処理の割合を表します。ここでは、 0 ≤ P ≤ 1 である（ 100% PUT ワークロードの場合は P = 1 、 100% GET ワークロードの場合は P = 0 ）。

ここでは、S3アカウント名、S3バケット、S3キーの合計の平均サイズをKで表します。S3 アカウント名が常に my-s3 アカウント（ 13 バイト）、バケット名が /my-application/bucket-12345 （ 28 バイト）のような固定長の名前、オブジェクト名が 5733a5d7-f069-41ef-8fbd-132474c69c （ 36 バイト）のような固定長のキーを持つとします。K の値は 90 （ 13+13+28+36 ）です。

P と K の値を決定できる場合は、次の式を使用して、外部 syslog サーバで処理する必要がある監査ログのボリュームを見積もることができます。これは、監査レベルをデフォルト（ Storage を除くすべてのカテゴリは Normal に設定されたまま）にしておくことを前提としています。 エラーに設定されているもの）：

```
Audit Log Rate = ((2 x P) + (1 - P)) x S3 Operations Rate
Audit Log Average Size = (570 + K) bytes
```

たとえば、グリッドのサイズが 1 秒あたり 1 、 000 S3 処理の場合、ワークロードの配置は 50% で、 S3 アカウント名やバケット名は オブジェクト名の平均値は 90 バイトで、 1 秒あたり 1 、 500 の syslog メッセージをサポートするように外部 syslog サーバをサイジングし、 1 秒あたり約 1MB の割合で監査ログデータを受信（通常は格納）できるようにする必要があります。

デフォルト以外の監査レベルの推定式

監査ログ用に提供される式では、デフォルトの監査レベル設定（「 Error 」に設定されているストレージを除く、すべてのカテゴリが「 Normal 」に設定されている）を使用するものとします。デフォルト以外の監査レベル設定に対する監査メッセージの割合と平均サイズを見積もるための詳細な式は使用できません。ただし、次の表を使用して料金を大まかに見積もることができます。 監査ログに提供されている平均サイズの式を使用することもできますが、「余分な」監査メッセージの平均サイズはデフォルトの監査メッセージよりも小さくなるため、見積もりが過剰になる可能性があることに注意してください。

条件	計算式
レプリケーション：すべての監査レベルをデバッグまたは通常に設定します	監査ログ速度= 8 x S3処理速度
イレイジャーコーディング：すべての監査レベルをデバッグまたは正常に設定	デフォルト設定と同じ式を使用します

セキュリティイベントの推定式

セキュリティイベントはS3処理とは関係なく、一般に生成されるログやデータの量はごくわずかです。そのため、計算式は提供されません。

アプリケーションログの推定式

グリッドでサポートされる 1 秒あたりの S3 処理数以外の情報が S3 ワークロードにない場合は、次の式を使用して、外部 syslog サーバで処理する必要があるアプリケーションログのボリュームを推定できます。

```
Application Log Rate = 3.3 x S3 Operations Rate
Application Log Average Size = 350 bytes
```

たとえば、グリッドの 1 秒あたりの S3 処理数が 1 、 000 の場合、 1 秒あたりのアプリケーションログ数が

3 、 300 になるように外部 syslog サーバをサイジングし、 1 秒あたり約 1.2 MB の割合でアプリケーションログデータを受信（格納）できるようにする必要があります。

ワークロードの詳細がわかっている場合は、より正確な概算が可能です。アプリケーションログの場合、最も重要な追加変数は、データ保護戦略（レプリケーションとイレイジャーコーディング）、S3処理の割合（GETとその他）、および次のS3フィールドの平均サイズ（バイト）です（表で使用されている4文字の略語は監査ログのフィールド名です）。

コード	フィールド	製品説明
SACC	S3 テナントアカウント名（要求の送信者）	要求を送信したユーザのテナントアカウントの名前。匿名の要求の場合は空です。
SBAC	S3 テナントアカウント名（バケット所有者）	バケット所有者のテナントアカウント名。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。
S3BK	S3バケット	S3 バケット名。
S3KY	S3キー	バケット名を除く S3 キーの名前。バケットに対する処理では、このフィールドは指定されません。

サイジング試算の例

このセクションでは、次のデータ保護方法でグリッドの推定式を使用する方法の例を説明します。

- レプリケーション
- イレイジャーコーディング

レプリケーションをデータ保護に使用する場合

P は、 PUT の S3 処理の割合を表します。ここでは、 0 ≤ P ≤ 1 である（ 100% PUT ワークロードの場合は P = 1 、 100% GET ワークロードの場合は P = 0 ）。

KをS3アカウント名、S3バケット、S3キーの合計の平均サイズとします。S3 アカウント名が常に my-s3 アカウント（ 13 バイト）、バケット名が /my-application/bucket-12345 （ 28 バイト）のような固定長の名前、オブジェクト名が 5733a5d7-f069-41ef-8fbd-132474c69c （ 36 バイト）のような固定長のキーを持つとします。K の値は 90 （ 13+13+28+36 ）です。

P と K の値を決定できる場合は、次の式を使用して、外部 syslog サーバで処理可能なアプリケーションログのボリュームを推定できます。

```
Application Log Rate = ((1.1 x P) + (2.5 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (220 + K)) + ((1 - P) x (240 + (0.2 x
K))) Bytes
```

たとえば、グリッドのサイズが 1 秒あたり 1 、 000 S3 処理の場合、ワークロードの配置が 50% で、 S3 アカウント名、バケット名、オブジェクト名の平均値が 90 バイトの場合、 1 秒あたりのアプリケーションログ数が 1800 になるように外部 syslog サーバをサイジングする必要があります。 そして、アプリケーションデータを 0.5 MB/ 秒のレートで受信（通常は保存）します。

イレイジャーコーディングをデータ保護に使用する場合

P は、 PUT の S3 処理の割合を表します。ここでは、 0 ≤ P ≤ 1 である（ 100% PUT ワークロードの場合は P = 1 、 100% GET ワークロードの場合は P = 0 ）。

KをS3アカウント名、S3バケット、S3キーの合計の平均サイズとします。S3 アカウント名が常に my-s3 アカウント（ 13 バイト）、バケット名が /my-application/bucket-12345 （ 28 バイト）のような固定長の名前、オブジェクト名が 5733a5d7-f069-41ef-8fbd-132474c69c （ 36 バイト）のような固定長のキーを持つとします。K の値は 90 （ 13+13+28+36 ）です。

P と K の値を決定できる場合は、次の式を使用して、外部 syslog サーバで処理可能なアプリケーションログのボリュームを推定できます。

```
Application Log Rate = ((3.2 x P) + (1.3 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (240 + (0.4 x K))) + ((1 - P) x (185 +
(0.9 x K))) Bytes
```

たとえば、グリッドのサイズが1秒あたり1、000 S3処理に対応している場合、ワークロードは50%のPUTになり、S3アカウント名、バケット名 オブジェクト名の平均は90バイトです。外部syslogサーバは、1秒あたり2、250個のアプリケーションログをサポートするようにサイズを設定し、1秒あたり0.6MBの速度でアプリケーションデータを受信（格納）できるようにする必要があります。

StorageGRIDでログ管理を構成する

必要に応じて、監査レベル、プロトコルヘッダー、監査メッセージとログの保存場所、およびログの保持期間を設定します。

すべてのStorageGRIDノードは、システム アクティビティとイベントを追跡するために監査メッセージとログを生成します。監査メッセージとログは、監視とトラブルシューティングに不可欠なツールです。

オプションで、"外部syslogサーバーを設定する"監査情報をリモートで保存できます。外部サーバーを使用することで、監査データの完全性を損なうことなく、監査メッセージのログ記録によるパフォーマンスへの影響を最小限に抑えることができます。外部 syslog サーバーは、大規模なグリッドを使用している場合、複数の種類の S3 アプリケーションを使用している場合、またはすべての監査データを保持したい場合に特に役立ちます。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"Maintenance権限またはRoot Access権限"。
- 外部Syslogサーバーを設定する予定の場合は、"外部syslogサーバを使用する場合の考慮事項" 。
- TLSまたはRELP/TLSプロトコルを使用して外部syslogサーバを設定する場合は、必要なサーバCAとクライアント証明書、およびクライアント秘密鍵が必要です。

監査ログでは、次のカテゴリのメッセージごとに異なる監査レベルを設定できます。

監査カテゴリ	デフォルト設定	詳細情報
システム	標準	"システム監査メッセージ"
ストレージ	エラー	"オブジェクトストレージ監査メッセージ"
管理	標準	"管理監査メッセージ"
クライアント読み取り	標準	"クライアント読み取り監査メッセージ"
クライアントからの書き込み	標準	"クライアント書き込み監査メッセージ"
ILM	標準	"ILM監査メッセージ"
グリッド間レプリケーション	エラー	"CGRR：クロスグリッドレプリケーション要求"

アップグレード中は、監査レベルの構成はすぐには有効になりません。

手順

1. 構成 > 監視 > *ログ管理*を選択します。
2. 監査メッセージのカテゴリごとに、ドロップダウンリストから監査レベルを選択します。

監査レベル	製品説明
オフ	このカテゴリの監査メッセージはログに記録されません。
エラー	エラー メッセージ (結果コードが「成功」(SUCS) ではなかった監査メッセージ) のみがログに記録されます。
標準	標準のトランザクション・メッセージはログに記録されますこのメッセージは ' カテゴリに関する次の手順に記載されています
デバッグ	非推奨です。このレベルの動作は Normal 監査レベルと同じです。

特定のレベルに含まれるメッセージには、上位レベルでロギングされるメッセージも含まれます。たとえば、 Normal レベルには Error レベルのメッセージがすべて含まれます。

S3 アプリケーションのクライアント読み取り操作の詳細な記録が必要ない場合は、オプションで クライアント読み取り 設定を エラー に変更して、監査ログに記録される監査メッセージの数を減らします。

3. [保存（ Save ）] を選択します。

HTTP要求ヘッダーの定義

オプションで、クライアントの読み取りおよび書き込み監査メッセージに含める HTTP 要求ヘッダーを定義できます。

手順

1. [Audit protocol headers]セクションで、クライアントの読み取り/書き込み監査メッセージに含めるHTTP要求ヘッダーを定義します。

   0 個以上の文字に一致させるには、ワイルドカードとしてアスタリスク（ * ）を使用します。リテラルアスタリスクに一致させるには、エスケープシーケンス（ \ * ）を使用します。

2. 必要に応じて、「 * 別のヘッダーを追加」を選択して追加のヘッダーを作成します。

   StorageGRID がリクエスト内の HTTP ヘッダーを検出すると、監査メッセージの HTRH フィールドにそれらを含めます。

   監査プロトコル要求ヘッダーは、*クライアント読み取り*または*クライアント書き込み*の監査レベルが*オフ*でない場合にのみログに記録されます。

3. [保存（ Save ）] を選択します

ログの場所を設定する

デフォルトでは、監査メッセージとログは、それらが生成されたノードに保存されます。StorageGRID は、監査メッセージとログを定期的にローテーションし、最終的には削除することで、過剰なディスク容量の消費を防ぎます。監査メッセージとログの一部を外部に保存するには、外部のsyslogサーバーを使用する。

ログ ファイルを内部に保存する場合は、ログ ストレージ用のテナントとバケットを選択し、ログ アーカイブを有効にします。

[use-external-syslog-server]]外部syslogサーバを使用する

必要に応じて、監査ログ、アプリケーションログ、およびセキュリティイベントログをグリッドの外部の場所に保存するように外部のsyslogサーバを設定できます。

外部のSyslogサーバーを使用しない場合は、この手順をスキップして、ログの場所を選択 。

この手順で使用できる構成オプションが要件を満たすほど柔軟性がない場合は、のプライベートAPIセクションにあるエンドポイントを使用して追加の構成オプションを適用できます `audit-destinations`。"Grid 管理 API"たとえば、ノードのグループごとに異なるsyslogサーバを使用する場合は、APIを使用できます。

syslog情報の入力

外部syslogサーバの設定ウィザードにアクセスし、StorageGRIDが外部syslogサーバにアクセスするために必要な情報を入力します。

手順

1. [ローカル ノードと外部サーバー] タブから、[外部 Syslog サーバーの構成] を選択します。または、以前に外部 Syslog サーバーを設定している場合は、[外部 **Syslog** サーバーの編集] を選択します。

   Configure external syslog serverウィザードが表示されます。

2. ウィザードの* syslog情報の入力*ステップで、* Host *フィールドに外部syslogサーバの有効な完全修飾ドメイン名またはIPv4またはIPv6アドレスを入力します。
3. 外部 syslog サーバのデスティネーションポートを入力します（ 1~65535 の整数で指定する必要があります）。デフォルトのポートは514です。
4. 外部 syslog サーバへの監査情報の送信に使用するプロトコルを選択します。

   TLS または RELP/TLS *を使用することを推奨します。これらのいずれかのオプションを使用するには、サーバ証明書をアップロードする必要があります。証明書を使用して、グリッドと外部 syslog サーバの間の接続を保護できます。詳細については、を参照してください "セキュリティ証明書を管理する"。

   すべてのプロトコルオプションで、外部 syslog サーバによるサポートおよび設定が必要です。外部 syslog サーバと互換性のあるオプションを選択する必要があります。

   > Reliable Event Logging Protocol (RELP) は、 syslog プロトコルの機能を拡張し、信頼性の高いイベントメッセージ配信を実現します。RELP を使用すると、外部 syslog サーバを再起動する必要がある場合に監査情報が失われないようにすることができます。

5. 「 * Continue * 」を選択します。
6. [[attach-certificate]* TLS または RELP/TLS *を選択した場合は、サーバCA証明書、クライアント証明書、およびクライアント秘密鍵をアップロードします。
   a. 使用する証明書またはキーの [* 参照] を選択します。
   b. 証明書またはキーファイルを選択します。
   c. ファイルをアップロードするには、 * 開く * を選択します。

      証明書またはキーファイル名の横に緑のチェックマークが表示され、正常にアップロードされたことを通知します。

7. 「 * Continue * 」を選択します。

syslog の内容を管理します

外部syslogサーバに送信する情報を選択できます。

手順

1. ウィザードの* syslogコンテンツの管理*ステップで、外部syslogサーバに送信する監査情報の種類をそれぞれ選択します。
   - 監査ログの送信：StorageGRID イベントとシステムアクティビティを送信します

- セキュリティイベントの送信:許可されていないユーザーがサインインしようとしたときや、ユーザーがrootとしてサインインしようとしたときなど、セキュリティイベントを送信します
- アプリケーションログを送信：次のようなトラブルシューティングに役立つ情報を送信します"StorageGRIDソフトウェアのログファイル"。
  - `bycast-err.log`
  - `bycast.log`
  - `jaeger.log`
  - `nms.log`（管理ノードのみ）
  - `prometheus.log`
  - `raft.log`
  - `hagroups.log`
- アクセスログを送信：外部要求に対するHTTPアクセスログをGrid Manager、Tenant Manger、設定されているロードバランサエンドポイント、およびリモートシステムからのグリッドフェデレーション要求に送信します。

2. ドロップダウンメニューを使用して、送信する監査情報のカテゴリごとに重大度とファシリティ（メッセージのタイプ）を選択します。

   重大度とファシリティの値を設定すると、ログをカスタマイズ可能な方法で集約して分析を容易にすることができます。

   a. では、[Passthrough]*を選択するか、重大度値を0~7で選択します。

      値を選択すると、StorageGRID は選択した値をこのタイプのすべてのメッセージに適用します。重要度を固定値で上書きすると、重要度ごとの詳細情報が失われます。

重大度	製品説明
パススルー	外部syslogに送信される各メッセージの重大度は、ノードにローカルにログインしたときと同じになります。 • 監査ログの場合、重大度は「info」です。 • セキュリティイベントの場合、重大度の値はノード上のLinuxディストリビューションによって生成されます。 • アプリケーションログの重大度は、問題の内容に応じて「info」と「notice」の間で異なります。たとえば、NTPサーバを追加してHAグループを設定すると値が「info」になり、SSMサービスまたはRSMサービスを意図的に停止すると値が「notice」になります。 • アクセスログの場合、重大度は「info」です。
0	EMERGENCY ：システムが使用できない
1	ALERT ：早急に対処が必要です
2	Critical ：クリティカルな状態です

重大度	製品説明
3	Error ：エラー状態
4	Warning ：警告状態です
5	通知：通常の状態だが重要な状態
6	INFORMATIONAL ：情報メッセージです
7	DEBUG ：デバッグレベルのメッセージ

b. *Facilty*では、*Passthrough*を選択するか、0～23のファシリティ値を選択します。

値を選択すると、このタイプのすべてのメッセージに適用されます。固定値でファシリティを上書きすると、さまざまなファシリティに関する情報が失われます。

ファシリティ	製品説明
パススルー	外部syslogに送信される各メッセージのファシリティ値は、ノードにローカルにログインしたときと同じです。 • 監査ログの場合、外部syslogサーバに送信されるファシリティは「local7」です。 • セキュリティイベントの場合、ファシリティ値はノード上のLinuxディストリビューションによって生成されます。 • アプリケーションログの場合、外部syslogサーバに送信されるアプリケーションログのファシリティ値は次のとおりです。 ◦ `bycast.log`:ユーザーまたはデーモン ◦ `bycast-err.log`：user、daemon、local3、またはlocal4 ◦ `jaeger.log`：local2 ◦ `nms.log`: local3 ◦ `prometheus.log`：local4 ◦ `raft.log`: local5 ◦ `hagroups.log`：local6 • アクセスログの場合、外部syslogサーバに送信されるファシリティは「local0」です。
0	kern （カーネルメッセージ）
1	ユーザ（ユーザレベルのメッセージ）

ファシリティ	製品説明
2	メール
3	デーモン（システムデーモン）
4	AUTH （セキュリティ / 認証メッセージ）
5	syslog （ syslogd で内部的に生成されるメッセージ）
6	LPR （ラインプリンタサブシステム）
7	News （ネットワークニュースサブシステム）
8	UUCP
9	cron クロックデーモン
10	セキュリティ（セキュリティ / 認可メッセージ）
11	FTP
12	NTP
13	logaudit （ログ監査）
14	logalert （ログアラート）
15	clock （ clock デーモン）
16	ローカル0
17	local1
18	local2
19	local3
20	local4
21	local5
22	local6

ファシリティ	製品説明
23	local7

3. 「 * Continue * 」を選択します。

テストメッセージを送信します

外部 syslog サーバを使用する前に、グリッド内のすべてのノードが外部 syslog サーバにテストメッセージを送信するよう要求してください。これらのテストメッセージは、外部 syslog サーバにデータを送信する前に、ログ収集インフラストラクチャ全体を検証するのに役立ちます。

外部syslogサーバがグリッド内の各ノードからテストメッセージを受信し、メッセージが想定どおりに処理されたことを確認するまでは、外部syslogサーバの設定を使用しないでください。

手順

1. 外部syslogサーバが適切に設定され、グリッド内のすべてのノードから監査情報を受信できることが確実であるためにテストメッセージを送信しない場合は、*[スキップして終了]*を選択します。

   緑色のバナーは、設定が保存されたことを示します。

2. それ以外の場合は、テストメッセージを送信（推奨）を選択します。

   テスト結果は、テストを停止するまでページに継続的に表示されます。テストの実行中も、以前に設定した送信先に監査メッセージが引き続き送信されます。

3. Syslog サーバーの構成中または実行時にエラーが発生した場合は、エラーを修正して、テスト メッセージの送信 を再度選択してください。

   エラーの解決方法については、を参照してください"外部 syslog サーバのトラブルシューティングを行います"。

4. すべてのノードがテストに合格したことを示す緑のバナーが表示されるまで待ちます。
5. syslog サーバを調べて、テストメッセージが正常に受信および処理されているかどうかを確認します。

   UDP を使用している場合は、ログ収集インフラストラクチャ全体を確認してください。UDP プロトコルでは、他のプロトコルほど厳密なエラー検出はできません。

6. 「 * ストップ & フィニッシュ * 」を選択します。

   監査および syslog サーバ * ページに戻ります。緑色のバナーは、syslogサーバの設定が保存されたことを示します。

   外部 Syslog サーバを含む宛先を選択するまで、 StorageGRID監査情報は外部 Syslog サーバに送信されません。

ログの場所を選択

監査ログ、セキュリティイベントログ、"StorageGRIDアプリケーション ログ" 、アクセスログが送信されます。

> StorageGRIDはデフォルトでローカルノードの監査先に設定され、監査情報をに格納します `/var/local/log/localaudit.log`。
>
> を使用する `/var/local/log/localaudit.log`と、Grid ManagerとTenant Managerの監査ログエントリがストレージノードに送信されることがあります。最新のエントリがあるノードを確認するには、コマンドを使用し `run-each-node --parallel "zgrep MGAU /var/local/log/localaudit.log | tail"`ます。
>
> 一部の送信先は、外部syslogサーバを設定した場合にのみ使用できます。

手順

1. ログの場所 > *ローカルノードと外部サーバー*を選択します。
2. ログ タイプに応じてログの場所を変更するには、別のオプションを選択します。

> *ローカルノードのみ*および*外部syslogサーバ*の方が一般的にパフォーマンスが向上します。

オプション	製品説明
ローカルノードのみ（デフォルト）	監査メッセージ、セキュリティ イベント ログ、アプリケーション ログは管理ノードに送信されません。代わりに、それらはそれを生成したノード (「ローカル ノード」) にのみ保存されます。各ローカルノードで生成された監査情報は、`/var/local/log/localaudit.log` 。 注: StorageGRID は、スペースを解放するために、定期的にローカル ログをローテーションで削除します。ノードのログ ファイルが 1 GB に達すると、既存のファイルが保存され、新しいログ ファイルが開始されます。ログのローテーション制限は 21 ファイルです。ログ ファイルの 22 番目のバージョンが作成されると、最も古いログ ファイルが削除されます。平均して、各ノードには約 20 GB のログ データが保存されます。ログを長期間保存するには、ログ保存にテナントとバケットを使用する 。
管理ノード/ローカルノード	監査メッセージは管理ノード上の監査ログに送信され、セキュリティ イベントログとアプリケーションログはそれらを生成したノードに格納されます。監査情報は次のファイルに格納されます。 • 管理ノード (プライマリおよび非プライマリ): `/var/local/audit/export/audit.log` • All nodes（すべてのノード）： `/var/local/log/localaudit.log`通常、ファイルが空であるか欠落しています。一部のメッセージの追加コピーなど、セカンダリ情報が含まれている場合があります。

オプション	製品説明
外部 syslog サーバ	監査情報は外部のSyslogサーバーに送信され、ローカルノードに保存されます。(`/var/local/log/localaudit.log` ）。送信される情報の種類は、外部 Syslog サーバーの設定方法によって異なります。このオプションは、外部syslogサーバーを設定しました 。
管理ノードと外部Syslogサーバー	監査メッセージは監査ログに送信されます (`/var/local/audit/export/audit.log`）が管理ノード上に作成され、監査情報は外部のSyslogサーバーに送信され、ローカルノードに保存されます。(`/var/local/log/localaudit.log` ）。送信される情報の種類は、外部 Syslog サーバーの設定方法によって異なります。このオプションは、外部syslogサーバーを設定しました 。

3. [保存（ Save ）] を選択します。

   警告メッセージが表示されます。

4. [OK]*を選択して、監査情報の保存先を変更することを確認します。

   選択した送信先に新しいログが送信されます。既存のログは現在の場所に残ります。

バケットを使用する

ログは定期的にローテーションされます。同じグリッド内の S3 バケットを使用して、ログを長期間保存します。

1. ログの場所 > *バケットの使用*を選択します。
2. アーカイブ ログを有効にする チェックボックスを選択します。
3. リストされているテナントとバケットが使用したいものでない場合は、[テナントとバケットの変更] を選択し、[テナントとバケットの作成] または [テナントとバケットの選択] を選択します。

   テナントとバケットを作成する

   a. 新しいテナント名を入力します。
   b. 新しいテナントのパスワードを入力して確認します。
   c. 新しいバケット名を入力します。
   d. *作成して有効化*を選択します。

   テナントとバケットを選択します

   a. プルダウンからテナント名を選択します。
   b. プルダウンからバケットを選択します。
   c. *選択して有効にする*を選択します。

4. [保存（ Save ）] を選択します。

ログは指定したテナントとバケットに保存されます。ログのオブジェクト キー名は次の形式になります。

```
system-logs/{node_hostname}/{absolute_path_to_log_file_on_node}--
{last_modified_time}.gz
```

例：

```
system-logs/DC1-SN1/var/local/log/localaudit.log--2025-05-12_13:41:44.gz
```

ログ保持期間の管理

ILMルールを作成するか、S3バケットのライフサイクルポリシーを設定することで、StorageGRID がログを保持する期間を管理できます。

ILMルール

バケット用のILMルールを作成し、このルールをアクティブなILMポリシーに追加します。

手順

1. [* ILM*>* Rules] を選択します。
2. 「作成」を選択します。"手順1（詳細を入力）" ILMルール作成ウィザードが表示されます。
   a. ルールに固有の名前を入力してください。例：アーカイブされたログのILMルール。
   b. ログアーカイブ用のS3テナントアカウントを選択します。
   c. ログアーカイブ用のS3バケットを指定してください。
3. 続けて"ステップ2（配置の定義）"、アーカイブされたログルールの配置場所を定義します。例えば、ILMルールでは、最初の1年間はサイト1に複製コピーを1つ、サイト2に複製コピーを1つ保存します。1年後、2+1のイレイジャーコーディングされたコピーが作成され、1か所のサイトのみに保存されます。
4. ルールを作成したら、それを有効なILMポリシーに追加します。

S3バケットのライフサイクル

ログアーカイブ用 S3 バケットに S3 バケットライフサイクルポリシーを設定します：

```
{
      "Rules": [
        {
           "ID": "Retain logs forever",
           "Filter": {},
           "Status": "Enabled",
           "Expiration": {}
        }
      ]
}
```

ログアーカイブ用のS3バケットでS3バケットライフサイクルポリシーを設定すると、バケットライフサイクルフィルタに一致するオブジェクトに対して、ライフサイクル有効期限アクションがILMポリシーを上書きします。バケットライフサイクルフィルタに一致しないオブジェクトは、ILMポリシーの保持設定を使用します。オブジェクトがバケットライフサイクルフィルタに一致し、かつ有効期限アクションが明示的に指定されていない場合、ILMポリシーの保持設定は使用されず、オブジェクトのバージョンは永久に保持されるとみなされます。

メールサーバーの設定

StorageGRID 管理者として、システムイベントや問題についてご自身、他の管理者、およびテクニカルサポートに通知する StorageGRID のアラートおよび監視システムから通知を送信するために、メールサーバを設定する必要があります。

通知にメールサーバーを使用する StorageGRID の機能には、アラート、AutoSupport、および複数管理者認

証（MAV）があります。すべての通知に同じメールサーバーを使用できます。

開始する前に

- あなたはを持っています"rootアクセス権限"。
- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。

手順

1. 設定 > 監視 > メールサーバー を選択します。

   メールサーバーのページが表示されます。

2. プルダウンメニュー「メールサーバーが必要となる可能性のある機能を表示する」を選択します。機能のメール通知を設定するための詳細と必要な情報を確認するには、「表示」を選択します。

   グリッドマネージャー内の該当機能の設定ページに移動します。各機能の設定ページには、メール通知を送信するにはメールサーバーが必要であることを示す通知が表示されます。

3. メールサーバーページからメールサーバーを設定するには：

   a. メールサーバーのIPアドレスまたはFQDNを入力してください。

   b. メールサーバーが使用するポート番号を選択してください。デフォルト値は25です。

   c. 認証を必須にするには、*認証を使用する*を選択し、ユーザー名とパスワードを入力してください。

   d. SMTPサーバーのIDの確認を必須にするには、「トランスポート層セキュリティ（TLS）を使用する」を選択します。次に：

      i. CAバンドルを提供してください。

      ii. SMTPメールサーバーが、メール送信者に認証用のクライアント証明書の提供を要求する場合は、*クライアント証明書を送信*を選択してください。次に、クライアント証明書と秘密鍵を指定してください。

   e. メール設定が正しいことを確認するには、送信者と受信者を入力してテストメールを送信してください。「送信」を選択します。

      テスト用 E メールが送信されたことを示す確認メッセージが表示されます。

   f. すべての E メール受信者の受信ボックスを調べて、テスト用 E メールが受信されたことを確認します。

      数分以内に電子メールが受信されない場合、または * 電子メール通知エラー * アラートがトリガーされた場合は、設定を確認してから再試行してください。

   g. 他の管理ノードにサインインし、テスト用 E メールを送信してすべてのサイトからの接続を確認します。

      アラート通知をテストするときは、すべての管理ノードにサインインして接続を確認する必要があります。これは、すべての管理ノードがテストEメールを送信するAutoSupportパッケージのテストとは対照的です。

4. [保存（ Save ）] を選択します。

テストメールを送信しても、設定は保存されません。「保存」を選択してください。

E メール設定が保存されます。

5. メールサーバーを使用する機能の設定ページに移動し、メール通知の設定を完了してください。
   - "アラート"。アラートについては、"SNMP通知を設定する"。
   - "AutoSupport"。AutoSupport パッケージは、電子メール、HTTPS、または HTTP で送信できます（HTTP は推奨されません）。
   - "マルチ管理者認証（MAV）"。

SNMP による監視を使用する

StorageGRIDでSNMP監視を使用する

簡易ネットワーク管理プロトコル（ SNMP ）を使用して StorageGRID を監視する場合は、 StorageGRID に含まれる SNMP エージェントを設定する必要があります。

- "SNMP エージェントを設定します"
- "SNMP エージェントを更新します"

機能

各StorageGRID ノードは、MIBを提供するSNMPエージェント（デーモン）を実行します。StorageGRID MIBには、アラートのテーブルと通知の定義が含まれています。この MIB には、各ノードのプラットフォームやモデル番号など、システムの概要 情報も含まれています。各 StorageGRID ノードは MIB-II オブジェクトのサブセットもサポートしています。

グリッドノードにMIBファイルをダウンロードするかどうかを確認します"MIBファイルにアクセスします"。

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

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

トラップ

トラップはSNMPエージェントによって送信される通知で、管理システムによる確認応答は必要ありません。トラップは、アラートがトリガーされているなど、 StorageGRID 内で何らかの問題が発生したことを管理システムに通知するために使用されます。

トラップは、 SNMP の 3 つのバージョンすべてでサポートされています。

情報

通知はトラップと似ていますが、管理システムによる確認応答が必要です。SNMPエージェントは、一定の時間内に確認応答を受信しなかった場合、確認応答を受信するか、最大再試行値に達するまで、インフォームを再送信します。

インフォームは SNMPv2c および SNMPv3 でサポートされます。

トラップ通知およびインフォーム通知は、次の場合に送信されます。

- デフォルトまたはカスタムのアラートはいずれかの重大度レベルでトリガーされます。アラートのSNMP通知を停止するには、アラートを指定する必要があります"サイレンスの設定"。アラート通知はから送信されます"優先送信者管理ノード"。

  各アラートは、アラートの重大度レベルに基づいて、 activeMinorAlert 、 activeMagajorAlert 、および activeCriticalAlert の 3 つのトラップタイプのいずれかにマッピングされます。これらのトラップをトリガーできるアラートのリストについては、を参照してください"アラート一覧"。

SNMP バージョンサポート

次の表に、各 SNMP バージョンでサポートされる内容の概要を示します。

	SNMPv1	**SNMPv2c**	**SNMPv3**
クエリ （GETおよびGETNEXT）	読み取り専用 MIB クエリ	読み取り専用 MIB クエリ	読み取り専用 MIB クエリ
クエリ認証	コミュニティストリング	コミュニティストリング	ユーザベースのセキュリティモデル（ USM ）ユーザ
通知 （トラップと通知）	トラップのみ	トラップおよびインフォーム	トラップおよびインフォーム
通知認証	トラップの送信先ごとに、デフォルトのトラップコミュニティまたはカスタムのコミュニティストリングを指定します	トラップの送信先ごとに、デフォルトのトラップコミュニティまたはカスタムのコミュニティストリングを指定します	トラップの送信先ごとの USM ユーザ

制限事項

- StorageGRID は、読み取り専用 MIB アクセスをサポートしています。読み取り / 書き込みアクセスはサポートされていません。
- グリッド内のすべてのノードが同じ設定を受信します。
- SNMPv3 ： StorageGRID は TSM （ Transport Support Mode ）をサポートしていません。
- SNMPv3 ： SHA （ HMAC-SHA-96 ）だけがサポートされています。
- SNMPv3 ： AES のみがサポートされています。

読み取り専用のMIBアクセスと通知にサードパーティ製のSNMP管理システムを使用するように、StorageGRID SNMPエージェントを設定できます。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"rootアクセス権限"。

タスクの内容

StorageGRIDのSNMPエージェントは、SNMPv1、SNMPv2c、およびSNMPv3をサポートしています。エージェントは 1 つ以上のバージョンに設定できます。SNMPv3では、ユーザセキュリティモデル（USM）認証のみがサポートされます。

グリッド内のすべてのノードが同じSNMP設定を使用します。

基本設定の指定

最初の手順として、StorageGRID SMNPエージェントを有効にし、基本情報を提供します。

手順

1. 構成 > 監視 > **SNMP** エージェント を選択します。

   [SNMP agent]ページが表示されます。

2. すべてのグリッドノードでSNMPエージェントを有効にするには、*[SNMPを有効にする]*チェックボックスを選択します。
3. [Basic configuration]セクションに次の情報を入力します。

フィールド	製品説明
システムの連絡先	オプション。StorageGRIDシステムのプライマリ連絡先。SNMPメッセージでsysContactとして返されます。 システムの連絡先は通常、Eメールアドレスです。この値は、StorageGRIDシステム内のすべてのノードを環境に設定します。*システム連絡先*は最大255文字です。
システムの場所	オプション。StorageGRIDシステムの場所。SNMPメッセージでsysLocationとして返されます。 システムの場所には、StorageGRIDシステムの場所を特定するのに役立つ任意の情報を指定できます。たとえば、施設の住所を使用できます。この値は、StorageGRIDシステム内のすべてのノードを環境に設定します。*システムの場所*の最大文字数は255文字です。

フィールド	製品説明
SNMPエージェント通知の有効化	• 選択すると、StorageGRID SNMPエージェントはトラップおよびインフォーム通知を送信します。 • 選択しない場合、SNMPエージェントは読み取り専用MIBアクセスをサポートしますが、SNMP通知は送信しません。
認証トラップを有効にする	このオプションを選択すると、不適切に認証されたプロトコルメッセージを受信すると、StorageGRID SNMPエージェントは認証トラップを送信します。

コミュニティストリングの入力

SNMPv1またはSNMPv2cを使用する場合は、[Community Strings]セクションに情報を入力します。

管理システムが StorageGRID MIB を照会すると、コミュニティストリングが送信されます。コミュニティストリングがここで指定した値のいずれかと一致すると、 SNMP エージェントは管理システムに応答を送信します。

手順

1. 読み取り専用コミュニティ*には、必要に応じてコミュニティストリングを入力し、IPv4およびIPv6エージェントアドレスでの読み取り専用MIBアクセスを許可します。

   StorageGRIDシステムのセキュリティを確保するために、コミュニティストリングとして「public」を使用しないでください。このフィールドを空白のままにすると、StorageGRIDシステムのグリッドIDがコミュニティストリングとして使用されます。

   各コミュニティストリングの最大文字数は32文字で、空白文字は使用できません。

2. [別のコミュニティ文字列を追加する]*を選択して、文字列を追加します。

   最大 5 つの文字列を指定できます。

トラップ送信先の作成

[Other configurations]セクションの[Trap destinations]タブを使用して、StorageGRIDトラップまたはインフォーム通知の送信先を1つ以上定義します。SNMPエージェントを有効にして*[保存]*を選択すると、アラートがトリガーされたときにStorageGRIDから定義された各送信先に通知が送信されます。標準通知は、サポートされている MIB-II エンティティ（ ifdown や coldStart など）についても送信されます。

手順

1. [Default trap community]フィールドに、SNMPv1またはSNMPv2トラップの送信先に使用するデフォルトのコミュニティストリングをオプションで入力します。

   特定のトラップ送信先を定義するときは、必要に応じて別の（「カスタム」）コミュニティストリングを指定できます。

   *デフォルトのトラップコミュニティ*は最大32文字で、空白文字は使用できません。

2. トラップ送信先を追加するには、*[作成]*を選択します。
3. このトラップ送信先に使用するSNMPのバージョンを選択します。
4. [トラップ送信先の作成]フォームに、選択したバージョンの情報を入力します。

SNMPv1

バージョンとしてSNMPv1を選択した場合は、これらのフィールドに値を入力します。

フィールド	製品説明
タイプ	SNMPv1のトラップである必要があります。
ホスト	トラップを受信するIPv4またはIPv6アドレス、または完全修飾ドメイン名（FQDN）。
ポート	別の値を使用する必要がないかぎり、SNMPトラップの標準ポートである162を使用します。
プロトコル	TCPを使用する必要がないかぎり、標準のSNMPトラッププロトコルであるUDPを使用します。
コミュニティストリング	デフォルトのトラップコミュニティ（指定されている場合）を使用するか、このトラップ送信先のカスタムコミュニティストリングを入力します。 カスタムコミュニティストリングの最大文字数は32文字で、空白は使用できません。

SNMPv2c

バージョンとしてSNMPv2cを選択した場合は、これらのフィールドに値を入力します。

フィールド	製品説明
タイプ	送信先をトラップまたはインフォームのどちらに使用するか。
ホスト	トラップを受信するIPv4、IPv6アドレス、またはFQDN。
ポート	別の値を使用する必要がないかぎり、SNMPトラップの標準ポートである162を使用します。
プロトコル	TCPを使用する必要がないかぎり、標準のSNMPトラッププロトコルであるUDPを使用します。
コミュニティストリング	デフォルトのトラップコミュニティ（指定されている場合）を使用するか、このトラップ送信先のカスタムコミュニティストリングを入力します。 カスタムコミュニティストリングの最大文字数は32文字で、空白は使用できません。

SNMPv3

バージョンとしてSNMPv3を選択した場合は、これらのフィールドに値を入力します。

フィールド	製品説明
タイプ	送信先をトラップまたはインフォームのどちらに使用するか。
ホスト	トラップを受信するIPv4、IPv6アドレス、またはFQDN。
ポート	別の値を使用する必要がないかぎり、SNMPトラップの標準ポートである162を使用します。
プロトコル	TCPを使用する必要がないかぎり、標準のSNMPトラッププロトコルであるUDPを使用します。
USMユーザ	認証に使用するUSMユーザ。 • [*Trap] を選択した場合は、権限のあるエンジン ID を持たない USM ユーザだけが表示されます。 • *INFORM を選択した場合は、権限のあるエンジン ID を持つ USM ユーザのみが表示されます。 • ユーザが表示されない場合： i. トラップ送信先を作成して保存します。 ii. に移動USMユーザの作成してユーザを作成します。 iii. [トラップ送信先]タブに戻り、テーブルから保存先を選択して*[編集]*を選択します。 iv. ユーザを選択します。

5. 「 * Create * 」を選択します。

   トラップの送信先が作成され、テーブルに追加されます。

エージェントアドレスの作成

必要に応じて、[その他の設定]セクションの[エージェントアドレス]タブを使用して、1つ以上の「リスニングアドレス」を指定します。SNMPエージェントがクエリを受信できるStorageGRIDアドレスです。

エージェントアドレスを設定しない場合、デフォルトのリスニングアドレスはすべてのStorageGRID ネットワークのUDPポート161です。

手順

1. 「 * Create * 」を選択します。
2. 次の情報を入力します。

フィールド	製品説明
インターネットプロトコル	このアドレスでIPv4とIPv6のどちらを使用するか。 デフォルトでは、 SNMP は IPv4 を使用します。
転送プロトコル	このアドレスがUDPとTCPのどちらを使用するか。 デフォルトでは、 SNMP は UDP を使用します。
StorageGRIDネットワーク	エージェントがリッスンするStorageGRIDネットワーク。 • グリッドネットワーク、管理ネットワーク、クライアントネットワーク：SNMPエージェントは3つのネットワークすべてでクエリをリスンします。 • グリッドネットワーク • 管理ネットワーク • クライアントネットワーク 注：セキュアでないデータにクライアントネットワークを使用し、クライアントネットワークのエージェントアドレスを作成する場合は、SNMPトラフィックもセキュアではないことに注意してください。
ポート	必要に応じて、SNMPエージェントがリスンするポート番号。 SNMP エージェントのデフォルトの UDP ポートは 161 ですが、未使用のポート番号は任意に入力できます。 注：SNMPエージェントを保存すると、StorageGRIDは内部ファイアウォールのエージェントアドレスポートを自動的に開きます。これらのポートへのアクセスが外部ファイアウォールで許可されていることを確認してください。

3. 「 * Create * 」を選択します。

エージェントアドレスが作成され、テーブルに追加されます。

USMユーザの作成

SNMPv3を使用している場合は、[Other configurations]セクションの[USM Users]タブを使用して、MIBの照会やトラップとインフォームの受信を許可するUSMユーザを定義します。

SNMPv3 *trap* の宛先の場合は、管理ノードごとに USM ユーザーを作成することをお勧めします。各管理ノードに USM ユーザーが存在しない場合は、プライマリ管理ノードがダウンすると管理システムが通知の受信を停止する可能性があります。

SNMPv3_inform_destinationsには、エンジンIDを持つユーザが必要です。SNMPv3_trap_destinationには、エンジンIDを持つユーザを指定できません。

これらの手順は、SNMPv1またはSNMPv2cのみを使用している場合は適用されません。

手順

1. 「 * Create * 」を選択します。
2. 次の情報を入力します。

フィールド	製品説明
ユーザ名	このUSMユーザの一意の名前。 ユーザ名の最大文字数は32文字で、空白文字は使用できません。ユーザの作成後にユーザ名を変更することはできません。
読み取り専用MIBアクセス	選択した場合、このユーザにはMIBへの読み取り専用アクセス権が必要です。
信頼できるエンジンID	このユーザをインフォーム送信先で使用する場合は、このユーザの信頼できるエンジンID。 10～64の16進数（5～32バイト）をスペースなしで入力します。この値は、インフォームのトラップ送信先で選択されるUSMユーザに必要です。トラップのトラップ送信先で選択されるUSMユーザにはこの値を指定できません。 注：*読み取り専用MIBアクセス*を選択した場合、このフィールドは表示されません。これは、読み取り専用MIBアクセスを持つUSMユーザにはエンジンIDを設定できないためです。
セキュリティレベル	USMユーザのセキュリティレベル： • * authPriv * ：認証とプライバシー（暗号化）と通信します。認証プロトコルとパスワード、およびプライバシープロトコルとパスワードを指定する必要があります。 • * authNoPriv * ：このユーザは認証と通信し、プライバシーはありません（暗号化なし）。認証プロトコルとパスワードを指定する必要があります。
認証プロトコル	常に、サポートされている唯一のプロトコル（HMAC-SHA-96）であるSHAに設定します。
パスワード	このユーザが認証に使用するパスワード。
プライバシープロトコル	• authPriv *を選択し、常にAES（サポートされている唯一のプライバシープロトコル）に設定されている場合にのみ表示されます。

フィールド	製品説明
パスワード	「* authPriv *」を選択した場合にのみ表示されます。このユーザがプライバシーのために使用するパスワード。

3. 「 * Create * 」を選択します。

   USM ユーザが作成され、テーブルに追加されます。

4. SNMPエージェントの設定が完了したら、*[保存]*を選択します。

   新しい SNMP エージェント設定がアクティブになります。

関連情報

"外部との通信に使用するポート"

StorageGRID SNMPエージェントを更新する

SNMP通知を無効にしたり、コミュニティストリングを更新したり、エージェントアドレス、USMユーザ、トラップ送信先を追加または削除したりできます。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"rootアクセス権限"。

タスクの内容

SNMPエージェントページの各フィールドの詳細については、を参照してください"SNMP エージェントを設定します"。各タブで行った変更をコミットするには、ページの下部にある*[保存]*を選択する必要があります。

手順

1. 構成 > 監視 > **SNMP** エージェント を選択します。

   [SNMP agent]ページが表示されます。

2. すべてのグリッドノードでSNMPエージェントを無効にするには、**[Enable SNMP]***チェックボックスをオフにし、[Save]*を選択します。

   SNMPエージェントを再度有効にすると、以前のSNMP設定がすべて保持されます。

3. 必要に応じて、[Basic configuration]セクションの情報を更新します。
   a. 必要に応じて、*システムの連絡先*と*システムの場所*を更新します。
   b. 必要に応じて、[SNMPエージェント通知を有効にする]*チェックボックスをオンまたはオフにして、StorageGRID SNMPエージェントがトラップおよびインフォーム通知を送信するかどうかを制御します。

      このチェックボックスをオフにすると、SNMPエージェントは読み取り専用のMIBアクセスをサポートしますが、SNMP通知は送信しません。

c. 必要に応じて、*[認証トラップを有効にする]*チェックボックスをオンまたはオフにして、不適切に認証されたプロトコルメッセージを受信したときにStorageGRID SNMPエージェントが認証トラップを送信するかどうかを制御します。

4. SNMPv1またはSNMPv2cを使用する場合は、必要に応じて[コミュニティストリング]セクションで*読み取り専用コミュニティ*を更新または追加します。

5. トラップ送信先を更新するには、[Other configurations]セクションの[Trap destinations]タブを選択します。

   このタブを使用して、StorageGRIDトラップまたはインフォーム通知の送信先を定義します。SNMPエージェントを有効にして*[保存]*を選択すると、アラートがトリガーされたときにStorageGRIDから定義された各送信先に通知が送信されます。標準通知は、サポートされている MIB-II エンティティ（ ifdown や coldStart など）についても送信されます。

   入力する項目の詳細については、を参照してください"トラップ送信先の作成"。

   - 必要に応じて、デフォルトのトラップコミュニティを更新または削除します。

     デフォルトのトラップコミュニティを削除する場合は、既存のトラップ送信先でカスタムのコミュニティストリングが使用されていることを最初に確認する必要があります。

   - トラップ送信先を追加するには、*[作成]*を選択します。
   - トラップ送信先を編集するには、ラジオボタンを選択し、*[編集]*を選択します。
   - トラップ送信先を削除するには、ラジオボタンを選択して*[削除]*を選択します。
   - 変更をコミットするには、ページの下部にある*[保存]*を選択します。

6. エージェントアドレスを更新するには、[その他の設定]セクションの[エージェントアドレス]タブを選択します。

   このタブを使用して、1つまたは複数の「リスニングアドレス」を指定します。SNMPエージェントがクエリを受信できるStorageGRIDアドレスです。

   入力する項目の詳細については、を参照してください"エージェントアドレスの作成"。

   - エージェントアドレスを追加するには、*[作成]*を選択します。
   - エージェントアドレスを編集するには、ラジオボタンを選択し、*[編集]*を選択します。
   - エージェントアドレスを削除するには、ラジオボタンを選択し、*[削除]*を選択します。
   - 変更をコミットするには、ページの下部にある*[保存]*を選択します。

7. USMユーザを更新するには、[Other configurations]セクションで[USM Users]タブを選択します。

   このタブを使用して、 MIB の照会またはトラップおよびインフォームの受信を許可されている USM ユーザを定義します。

   入力する項目の詳細については、を参照してください"USMユーザの作成"。

   - USMユーザを追加するには、*[作成]*を選択します。
   - USMユーザを編集するには、ラジオボタンを選択し、*[編集]*を選択します。

     既存のUSMユーザのユーザ名は変更できません。ユーザ名を変更する必要がある場合は、ユーザを削

除して新しいユーザを作成する必要があります。

> ユーザーの権限のあるエンジンIDを追加または削除し、そのユーザーが宛先に対して現在選択されている場合は、宛先を編集または削除する必要があります。そうしないと、SNMP エージェント設定を保存したときに検証エラーが発生します。

- USMユーザを削除するには、ラジオボタンを選択し、*[削除]*を選択します。

> 削除したユーザがトラップ送信先として選択されている場合は、送信先を編集または削除する必要があります。そうしないと、 SNMP エージェント設定を保存したときに検証エラーが発生します。

- 変更をコミットするには、ページの下部にある*[保存]*を選択します。

8. SNMPエージェントの設定を更新したら、*[保存]*を選択します。

StorageGRID MIBファイルにアクセスする

MIBファイルには、グリッド内のノードの管理対象リソースとサービスのプロパティの定義と情報が含まれています。StorageGRID のオブジェクトと通知を定義するMIBファイルにアクセスできます。これらのファイルは、グリッドの監視に役立ちます。

SNMPおよびMIBファイルの詳細については、を参照してください"SNMP による監視を使用する"。

MIBファイルにアクセスします

MIBファイルにアクセスする手順は、次のとおりです。

手順

1. 構成 > 監視 > **SNMP** エージェント を選択します。
2. [SNMP agent]ページで、ダウンロードするファイルを選択します。
   - * NETAPP-STORAGEGRID-MIB.txt *：すべての管理ノードでアクセス可能なアラートテーブルと通知（トラップ）を定義します。
   - * ES-NetApp-06-MIB.mib *：Eシリーズベースのアプライアンスのオブジェクトと通知を定義します。
   - * mib_1_10.zip *：BMCインターフェイスを使用するアプライアンスのオブジェクトと通知を定義します。

> また、任意のStorageGRIDノードの次の場所にあるMIBファイルにアクセスすることもできます。 `/usr/share/snmp/mibs`

3. MIBファイルからStorageGRID OIDを抽出するには、次の手順を実行します。
   a. StorageGRID MIBのルートのOIDを取得します。

```
root@user-adm1:~ # snmptranslate -On -IR storagegrid
```

結果： `.1.3.6.1.4.1.789.28669` (`28669`は常にStorageGRIDのOID)

b. ツリー全体のStorageGRID OIDをgrepで指定します（を使用して `paste`行を結合）。

```
root@user-adm1:~ # snmptranslate -Tso | paste -d " " - - | grep 28669
```

この `snmptranslate`コマンドには、MIBの探索に役立つ多くのオプションがあります。このコマンドは、任意のStorageGRID ノードで使用できます。

MIBファイルの内容

すべてのオブジェクトはStorageGRID OIDの下にあります。

オブジェクト名	オブジェクト**ID**（**OID**）	製品説明
		NetApp StorageGRIDエンティティ用のMIBモジュール。

MIBオフシエクト

オブジェクト名	オブジェクト**ID**（**OID**）	タイプ	アクセス	**MIB**モジュール	製品説明
activeAlertCount	1.3.6.1.4.1.+789.28669.1.3	整数32	read-only	NETAPP-STORAGEGRID-MIB	activeAlertTable内のアクティブなアラートの数。
activeAlertTableの略	1.3.6.1.4.1.+789.28669.1.4	ActiveAlertEntryのシーケンス	アクセス不可	NETAPP-STORAGEGRID-MIB	StorageGRID のアクティブなアラートのテーブル。
アクティブアラートエントリ		順序	アクセス不可	NETAPP-STORAGEGRID-MIB	アラート ID でインデックス付けされた単一のStorageGRIDアラート。
activeAlertId	1.3.6.1.4.1.+789.28669.1.4.1.1	オクテット文字列	read-only	NETAPP-STORAGEGRID-MIB	アラートのID。現在アクティブなアラートのセット内でのみ一意です。
activeAlertNameの略	1.3.6.1.4.1.+789.28669.1.4.1.2	オクテット文字列	read-only	NETAPP-STORAGEGRID-MIB	アラートの名前。
activeAlertInstanceの略	1.3.6.1.4.1.+789.28669.1.4.1.3	オクテット文字列	read-only	NETAPP-STORAGEGRID-MIB	アラートを生成したエンティティの名前（通常はノード名）。
activeAlertSeverityの略	1.3.6.1.4.1.+789.28669.1.4.1.4	オクテット文字列	read-only	NETAPP-STORAGEGRID-MIB	アラートの重大度。

オブジェクト名	オブジェクトID（OID）	タイプ	アクセス	MIBモジュール	製品説明
activeAlertStartTimeの略	1.3.6.1.4.1.+789.28669.1.4.1.5	日時	read-only	NETAPP-STORAGEGRID-MIB	アラートがトリガーされた時刻。

追加の StorageGRID データを収集します

StorageGRIDでPUTおよびGETのパフォーマンスを監視

オブジェクトストアや読み出しなどの特定の処理のパフォーマンスを監視して、詳しい調査が必要な変更を特定することができます。

タスクの内容

PUTおよびGETのパフォーマンスを監視するには、S3コマンドをワークステーションから直接実行するか、オープンソースのS3testerアプリケーションを使用します。これらの方法を使用すると、クライアントアプリケーションの問題や外部ネットワークの問題など、 StorageGRID の外部にある要因とは関係なくパフォーマンスを評価できます。

PUT 処理と GET 処理のテストを実行するときは、次のガイドラインに従ってください。

- グリッドに通常取り込むオブジェクトと同等のサイズのオブジェクトを使用します。
- ローカルサイトとリモートサイトの両方に対して処理を実行します。

のメッセージには"監査ログ"、特定の処理の実行に必要な合計時間が示されます。たとえば、 S3 GET 要求に対する合計処理時間を確認するには、 SGET 監査メッセージの TIME 属性の値を確認します。また、DELETE、GET、HEAD、Metadata Updated、POST、PUTの各S3処理の監査メッセージでTIME属性を確認することもできます。

結果を分析する際には、要求を満たすために必要な平均時間と、達成可能な全体的なスループットを確認します。同じテストを定期的に繰り返し、結果を記録して、調査が必要な傾向を特定できるようにします。

- できます "github から S3tester をダウンロードします"。

StorageGRIDでオブジェクト検証操作を監視する

StorageGRID システムは、ストレージノード上のオブジェクトデータの整合性を検証して、オブジェクトの破損や欠落の有無を確認します。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"Maintenance権限またはRoot Access権限"。

タスクの内容

2つが"検証プロセス"連携してデータの整合性を確保します。

- * バックグラウンド検証 * は、オブジェクトデータの正確性を継続的にチェックするために自動的に実行されます。

バックグラウンド検証では、すべてのストレージノードが自動的かつ継続的にチェックされて、レプリケートオブジェクトデータとイレイジャーコーディングオブジェクトデータのコピーが破損していないかどうかが確認されます。問題が見つかった場合、 StorageGRID システムは、システム内の別の場所に格納されているコピーから、破損したオブジェクトデータを自動的に置き換えます。バックグラウンド検証は、クラウドストレージプール内のオブジェクトに対しては実行されません。

> 自動的に修正できない破損オブジェクトが検出されると、* Unidentified corrupt object detected *アラートがトリガーされます。

- * オブジェクトの存在チェック * は、オブジェクトデータの有無（正確性ではなく）をより迅速に確認するためにユーザによってトリガーされます。

  オブジェクトの存在チェックでは、オブジェクトとイレイジャーコーディングフラグメントの想定されるレプリケートコピーがすべてストレージノードに存在するかどうかが検証されます。オブジェクトの存在チェックは、ストレージデバイスの整合性を検証する手段を提供します。特に、最新のハードウェア問題がデータの整合性に影響を与える可能性がある場合に役立ちます。

バックグラウンド検証の結果を定期的に確認し、オブジェクトの存在をチェックする必要があります。オブジェクトデータの破損や欠落が見つかった場合は、すぐに調べてルート原因 を特定します。

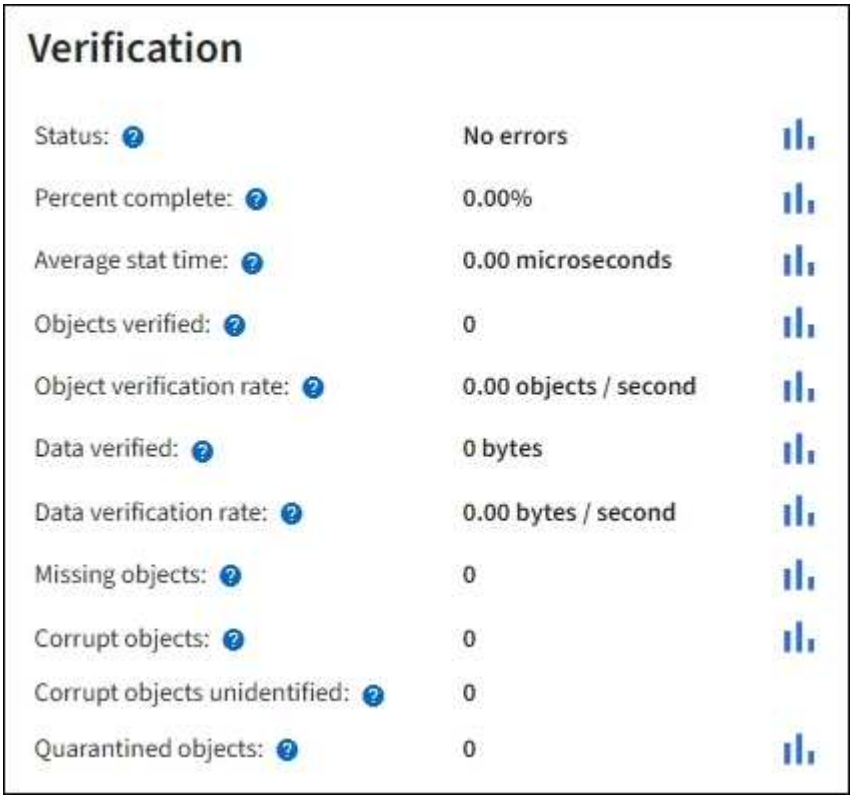
手順

1. バックグラウンド検証の結果を確認します。

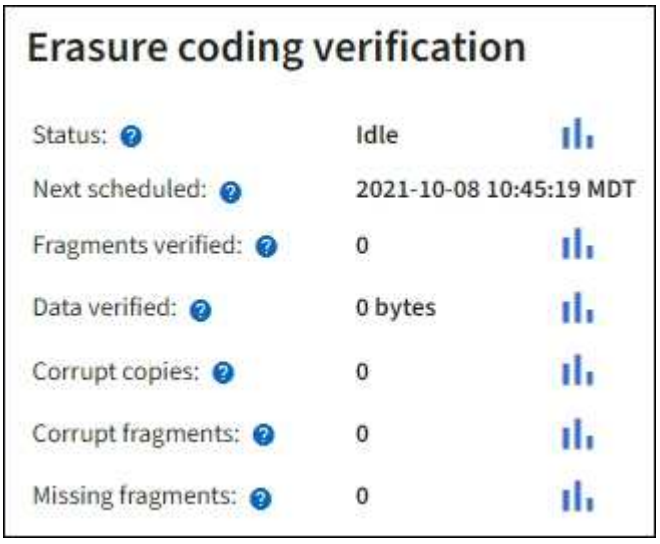
   a. ノード > ストレージ ノード > オブジェクト を選択します。

   b. 検証結果を確認します。

      - レプリケートされたオブジェクトデータの検証を確認するには、 Verification セクションの属性を確認します。

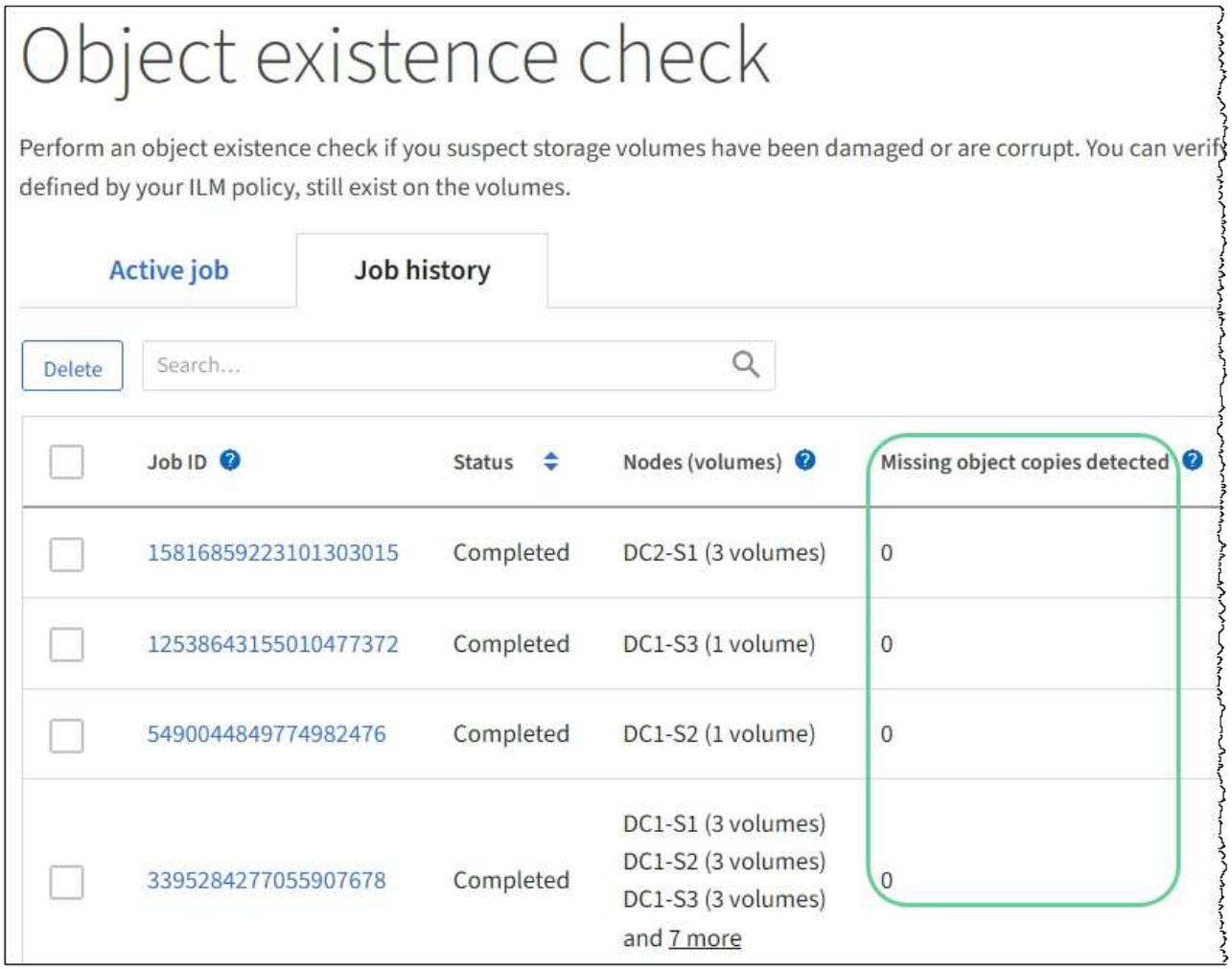


- イレイジャーコーディングフラグメントの検証を確認するには、「 * _ ストレージノード _ * > * ILM * 」を選択し、イレイジャーコーディングの検証セクションの属性を確認します。



属性名の横にある疑問符(?)を選択すると、ヘルプテキストが表示されます。

2. オブジェクト存在チェックジョブの結果を確認します。
   a. メンテナンス > オブジェクト存在チェック > *ジョブ履歴*を選択します。
   b. 不足しているオブジェクトのコピーが検出された列をスキャンします。いずれかのジョブで 100 個以上のオブジェクトのコピーが失われ、「オブジェクトが失われている可能性があります」というアラートがトリガーされた場合は、テクニカル サポートにお問い合わせください。



StorageGRID 監査メッセージを確認

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

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

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

各管理ノードで、監査メッセージがテキストファイルに保存されます。監査共有には、アクティブファイル（ audit.log ）と、圧縮された過去の監査ログが含まれています。グリッド内の各ノードには、ノードで生成された監査情報のコピーも格納されます。

監査ログファイルには、管理ノードのコマンドラインから直接アクセスできます。

StorageGRIDでは、デフォルトで監査情報を送信することも、送信先を変更することもできます。

- StorageGRIDはデフォルトでローカルノードの監査デスティネーションに設定されます。
- Grid ManagerおよびTenant Managerの監査ログエントリがストレージノードに送信されることがあります。
- 必要に応じて、監査ログのデスティネーションを変更したり、監査情報を外部 syslog サーバに送信したりできます。外部 syslog サーバが設定されても、監査レコードのローカルログは引き続き生成および格納されます。
- "ログ管理の構成について学ぶ" 。

監査ログファイル、監査メッセージの形式、監査メッセージのタイプ、および監査メッセージの分析に使用できるツールの詳細については、を参照してください"監査ログを確認します"。

StorageGRIDログファイルとシステムデータを収集

StorageGRIDログ ファイルとシステム データ (構成データを含む) を取得し、テクニカル サポートに送信できます。

開始する前に

- いずれかの管理ノードでグリッドマネージャにサインインしている。"サポートされている Web ブラウザ" 。
- そうだな "特定のアクセス権限"

タスクの内容

グリッドマネージャーを使用して収集する"ログファイル"選択した期間の任意のグリッド ノードからのシステム データおよび構成データを取得します。データは収集され、 `.tar.gz`このファイルは、ローカル コンピュータにダウンロードしたり、テクニカル サポートに送信したりできます。

必要に応じて、監査ログの送信先を変更し、監査情報を外部の syslog サーバーに送信することもできます。外部 Syslog サーバーが構成されている場合、監査レコードのローカル ログは引き続き生成され、保存されます。見る"ログ管理と外部Syslogサーバーを構成する" 。

ログ収集の開始に使用した管理ノードがログ収集中にオフラインになった場合、StorageGRID は結果を保持しません。ノードを再起動し、再起動完了後にログ収集を再開する必要があります。

手順

1. サポート > ツール > *ログ収集*を選択します。ノードのテーブルが表示されます。
2. ログファイルを収集するグリッドノードを選択します。

   ノード名、サイト、ノード タイプで並べ替えることができます。サイトとノードのタイプの列には、個々のサイトとノードのタイプで選択するためのフィルターが含まれています。

3. 「 * Continue * 」を選択します。
4. ログ ファイルに含めるデータの日付と時刻の範囲を選択します。

   非常に長い期間を選択した場合、または大規模なグリッド内のすべてのノードからログを収集した場合、ログ アーカイブが大きくなりすぎてノードに保存できなくなったり、管理ノードで収集してダウンロードできなくなったりする可能性があります。どちらかのシナリオが発生した場合は、より小さいデータ セッ

トでログ収集を再開します。

5. 収集するログのタイプを選択します。
   - アプリケーション ログ: テクニカル サポートがトラブルシューティングに最も頻繁に使用するアプリケーション固有のログ。収集されるログは、利用可能なアプリケーション ログのサブセットです。
   - 監査ログ: 通常のシステム操作中に生成された監査メッセージを含むログ。
   - ネットワーク トレース: ネットワークのデバッグに使用されるログ。
   - **Prometheus** データベース: すべてのノード上のサービスからの時系列メトリック。
6. オプションで、「**Notes**」テキスト ボックスを使用して、収集するログ ファイルに関するメモを入力します。

   このメモを使用して、ログファイルを収集する原因となった問題に関するテクニカルサポート情報を入力できます。メモは、ログファイルの収集に関するその他の情報とともにというファイルに追加され`info.txt`ます。 `info.txt`ファイルはログファイルのアーカイブパッケージに保存されます。
7. *ログを収集*を選択します。

   ログ収集ページを使用して、各グリッド ノードのログ ファイル収集の進行状況を監視できます。

   ログサイズに関するエラーメッセージが表示された場合は、ログを収集する期間を短縮するか、またはノードの数を減らしてください。
8. ログ収集に失敗した場合:
   - 「ログ収集に失敗しました」というメッセージが表示された場合は、ログ収集を再試行するか、再試行せずにセッションを終了することができます。
   - 「ログ収集が部分的に失敗しました」というメッセージが表示された場合は、ログ収集を再試行するか、セッションを終了するか、部分的なログ ファイルをダウンロードするか、部分的なログ ファイルをAutoSupportに送信することができます。

   > プロビジョニングパスフレーズ欄を空欄にして標準の再試行を行うか、パスフレーズを入力してSSHを使用して再試行するかを選択できます。
9. ログファイルの収集が完了したら:
   - ダウンロードするには*ダウンロード*を選択してください`.tar.gz`ファイル。
   - * AutoSupportに送信*を選択して送信します`.tar.gz`ファイルをテクニカル サポートに送信します。

     その`.tar.gz`ファイルには、ログ収集が成功したすべてのグリッド ノードからのすべてのログ ファイルが含まれます。組み合わせた`.tar.gz`ファイルには、グリッド ノードごとに 1 つのログ ファイル アーカイブが含まれます。

   AutoSupportパッケージの対象は `USER_TRIGGERED_SUPPORT_BUNDLE`。
10. [完了] を選択します。

    > その `.tar.gz`*完了*を選択するとファイルは削除されます。必ず最初にファイルをダウンロードまたは送信してください。

StorageGRID サポートメトリクスを確認

問題 のトラブルシューティングでは、テクニカルサポートと協力して StorageGRID システムの詳細な指標とグラフを確認することができます。

開始する前に

- Grid Managerにサインインする必要があります"サポートされている Web ブラウザ"。
- そうだな "特定のアクセス権限"

タスクの内容

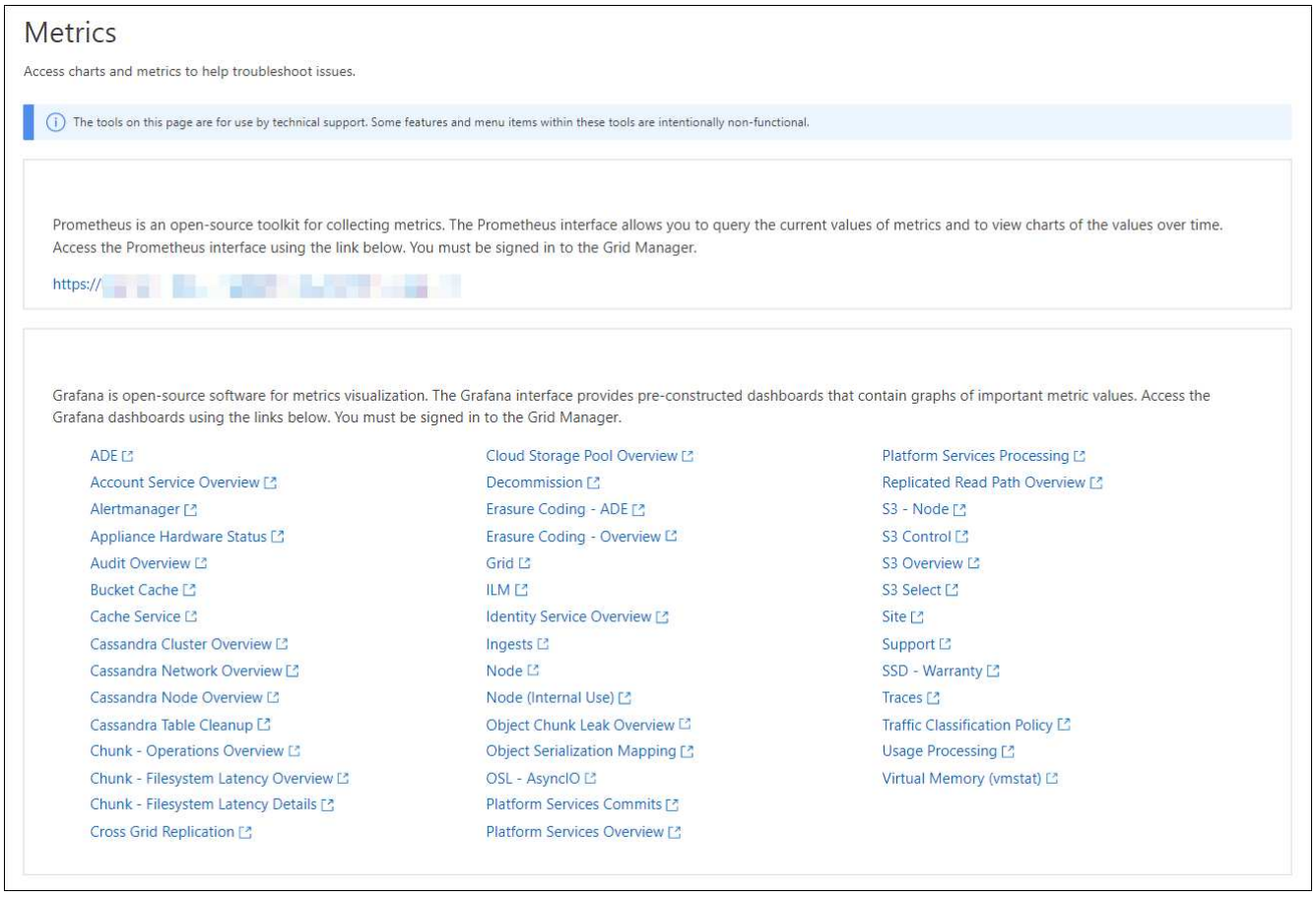
Metrics ページでは、 Prometheus と Grafana のユーザインターフェイスにアクセスできます。Prometheus は指標を収集するオープンソースソフトウェアです。Grafana は指標を視覚化するオープンソースソフトウェアです。

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

手順

1. テクニカル サポートの指示に従って、[サポート] > [ツール] > [メトリック] を選択します。

   ここでは、 [Metrics] ページの例を示します。



2. StorageGRID メトリクスの現在の値を照会したり、時間の経過に伴う値のグラフを表示したりするに

は、Prometheus セクションのリンクを選択してください。

Prometheus インターフェイスが表示されます。このインターフェイスでは、使用可能な StorageGRID 指標に対してクエリを実行したり、 StorageGRID 指標の推移をグラフ化したりできます。

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

3. 時間の経過に伴う StorageGRID メトリックのグラフを含む事前構築済みダッシュボードにアクセスするには、Grafana セクションのリンクを選択してください。

   選択したリンクに対応した Grafana インターフェイスが表示されます。



StorageGRIDで**I/O**の優先順位を変更する

入出力 (I/O) の優先順位付けにより、グリッド上の I/O 操作の相対的な優先順位を変更できます。

デフォルトでは、クライアントの PUT および GET I/O トラフィックには、消失訂正符号化 (EC) データの消去や EC 修復などのバックグラウンド アクティビティよりも最高の優先順位が与えられます。消失訂正符号化 (EC) データの消去と EC 修復アクティビティの優先度を上げると、これらのタスクをより早く完了できる可能性があります。 I/O 優先順位の変更の有効性は、クライアント要求のレート、ネットワーク トラフィックの変動、その他の進行中のネットワーク タスクによって影響を受けます。

開始する前に

- I/O 優先順位付けページを確認し、どのオプションがグリッドに影響を与える可能性があるかを判断します。
- 進行中のクライアント トラフィックが、より長い待機時間やクライアント タイムアウトを安全に処理できるかどうかを評価します。
- 優先順位の変更による影響を監視し、必要に応じて調整する準備をしてください。これらの変更はすぐに実装されますが、その効果が目に見えるようになるまでには数時間かかる場合があります。

手順

1. サポート > **I/O** 優先順位 を選択します。
2. (オプション) EC データを消去するバックグラウンド操作の EC パージおよび修復の優先度をデフォルト値から変更します。

   RAID ベースのノードを持つグリッドには、デフォルトの低い EC パージおよび修復優先度を使用します。

3. [保存（ Save ）] を選択します。
4. 監視する"指標"優先順位の変更による影響を評価するため。

StorageGRIDで診断を実行する

問題 のトラブルシューティングを行う場合、テクニカルサポートと協力して StorageGRID システムの診断を実行し、結果を確認します。

- "サポート指標を確認"
- "よく使用される Prometheus 指標"

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- そうだな "特定のアクセス権限"

タスクの内容

Diagnostics （診断）ページでは、グリッドの現在の状態に対して一連の診断チェックが実行されます。各診断点検には、次の 3 つのいずれかのステータスがあります。

- 正常：すべての値が正常範囲内です。
- 注意：1つ以上の値が正常範囲外です。
- 注意：1つ以上の値が正常範囲を大きく逸脱しています。

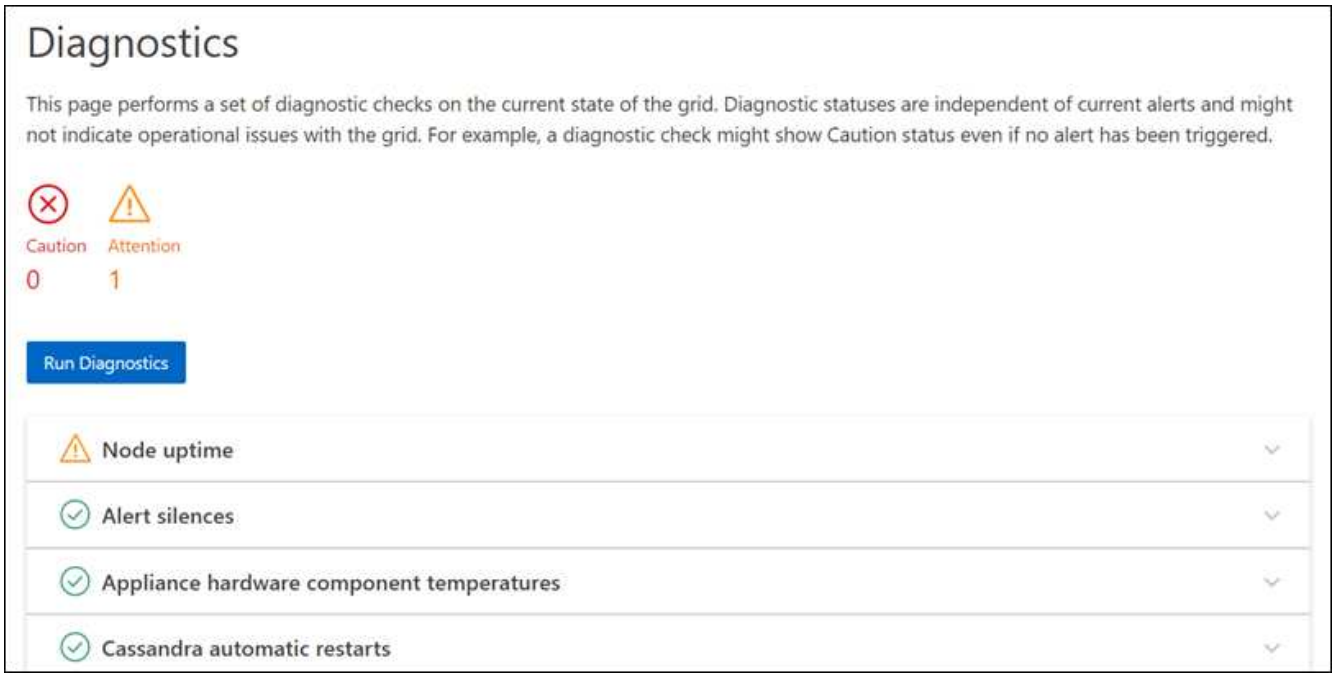
診断ステータスは現在のアラートとは関係なく、グリッドで発生している処理の問題を示しているとは限りません。たとえば、アラートがトリガーされていない場合でも、診断チェックで警告ステータスが表示されることがあります。

手順

1. サポート > ツール > *診断*を選択します。

   Diagnostics （診断）ページが表示され、診断チェックごとの結果がリストされます。結果は重大度（ [注意] 、 [注意] 、 [標準] ）でソートされます。それぞれの重大度の中で、結果はアルファベット順にソートされます。

   この例では、1 つの診断が「注意」ステータスになっており、3 つの診断が「正常」ステータスになっています。



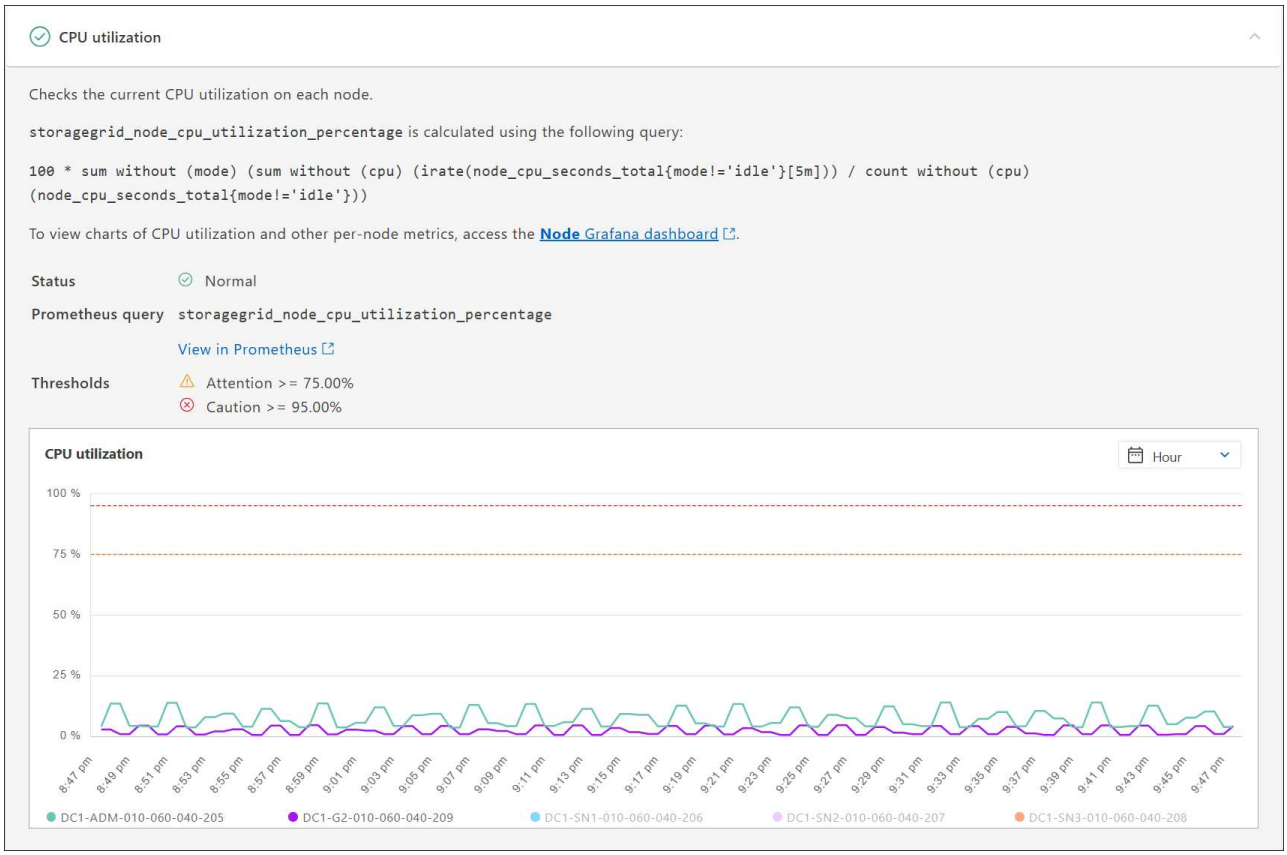
2. 特定の診断結果について詳しく知りたい場合は、該当する行を選択してください。

   診断とその現在の結果の詳細が表示されます。以下の詳細が表示されます。

   - * ステータス * ：この診断の現在のステータス。正常、注意、または注意。
   - * Prometheus クエリ * ：診断に使用した場合、ステータス値の生成に使用した Prometheus 式。（ Prometheus 式は一部の診断には使用されません）。
   - * しきい値 * ：診断に使用できる場合は、異常な診断ステータスごとにシステム定義のしきい値。（しきい値はすべての診断に使用されるわけではありません）。

     これらのしきい値は変更できません。

   - ステータス値: StorageGRIDシステム全体の診断のステータスと値を示すグラフと表 (スクリーンショットには表は表示されません)。この例では、 StorageGRIDシステム内の各ノードの現在の CPU 使用率が表示されます。すべてのノード値が「注意」および「警告」のしきい値を下回っているため、診断の全体的なステータスは「正常」です。



3. オプション: この診断に関連する Grafana チャートを表示するには、**Grafana** ダッシュボード を選択します。

   このリンクは、すべての診断で表示されるわけではありません。

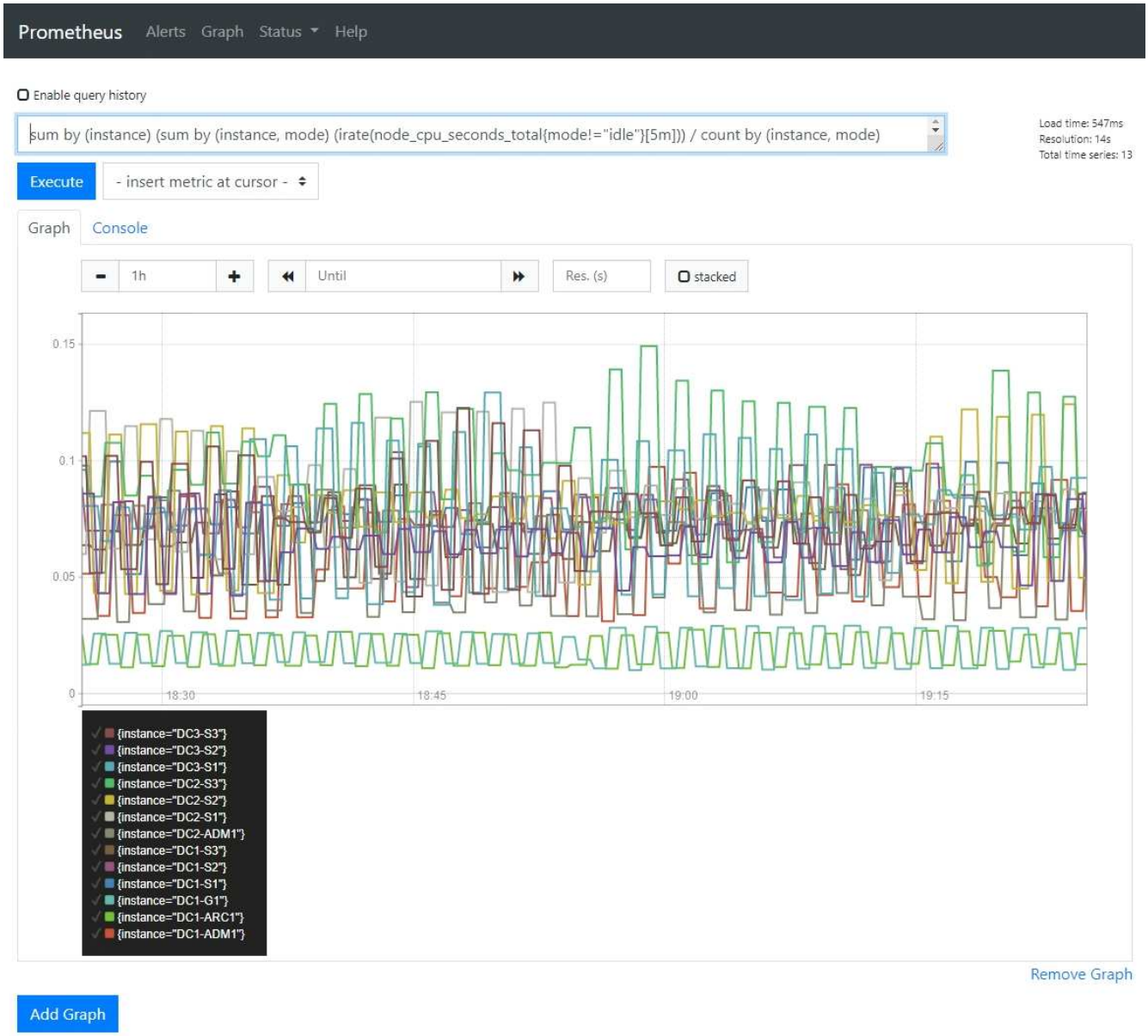
   関連する Grafana ダッシュボードが表示されます。この例では、ノード ダッシュボードが表示され、このノードの CPU 使用率の推移と、ノードのその他の Grafana チャートが表示されます。

   > サポート > ツール > メトリック ページの Grafana セクションから、事前に構築された Grafana ダッシュボードにアクセスすることもできます。



4. オプション：Prometheus の式の経時的なグラフを表示するには、*Prometheus で表示*を選択します。

   診断に使用された式の Prometheus グラフが表示されます。



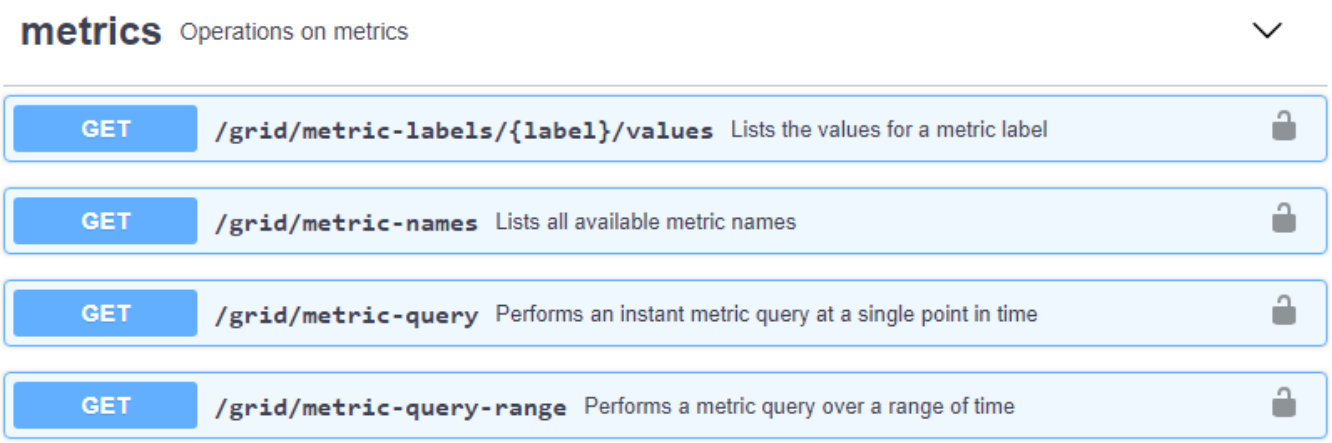
StorageGRID のカスタム監視アプリケーションを作成する

グリッド管理 API から取得される StorageGRID 指標を使用して、カスタムの監視アプリケーションやダッシュボードを構築できます。

グリッドマネージャの既存のページに表示されていない指標を監視する場合や、StorageGRID 用のカスタムダッシュボードを作成する場合は、グリッド管理APIを使用してStorageGRID 指標を照会できます。

また、 Grafana などの外部監視ツールを使用して、 Prometheus 指標に直接アクセスすることもできます。外部ツールを使用するには、管理用クライアント証明書をアップロードまたは生成して、 StorageGRID でセキュリティを確保するためにツールを認証する必要があります。を参照してください"StorageGRID の管理手順"。

利用可能なメトリクスの完全なリストを含む、メトリクスAPIの操作を表示するには、Grid Managerにアクセスしてください。ページ上部からヘルプアイコンを選択し、**API**ドキュメント > *メトリクス*を選択します。



[API documentation][Metrics]セクション"]

カスタム監視アプリケーションの実装方法の詳細については、このドキュメントでは説明していません。

StorageGRID システムのトラブルシューティングを行う

StorageGRID システムのトラブルシューティングを行う

StorageGRID システムの使用中に問題が発生した場合は、このセクションのヒントとガイドラインを参考に、問題 を特定し、解決してください。

多くの場合、問題は自分で解決できますが、一部の問題をテクニカルサポートにエスカレーションする必要があります。

問題を定義します

問題を解決するための最初のステップは、問題を明確に定義することです。

次の表に、問題を定義するために収集する情報の種類の例を示します。

質問	応答例
StorageGRID システムはどのような状況にあり、どのような症状があるか？	オブジェクトをStorageGRID に取り込めないことがクライアントアプリケーションから報告されている。
問題はいつ発生しましたか？	2020年1月8日14：50頃にオブジェクトの取り込みが最初に拒否されました。
最初にどのようにして問題に気付いたか。	クライアントアプリケーションから通知される。アラートの E メール通知も受け取った。
問題は一貫して発生しますか、または時々発生しますか？	問題は現在も続いています。

質問	応答例
問題が定期的に発生する場合は、原因 を実行する手順を確認してください	問題は、クライアントがオブジェクトの取り込みを試みるたびに発生します。
問題が断続的に発生する場合は、いつ発生しますか？各インシデントの発生時刻を記録します。	問題は間欠的ではありません。
この問題を以前に見たことがありますか？過去にこの問題が発生した頻度はどのくらいですか？	この問題 を初めて見たときです。

システムに対するリスクと影響を評価

問題を定義したら、 StorageGRID システムに対するリスクと影響を評価します。たとえば、クリティカルなアラートがあるからといって、システムがコアサービスを提供していないわけではありません。

次の表は、前述の問題の例について、システムの運用に対する影響をまとめたものです。

質問	応答例
StorageGRID システムでコンテンツを取り込むことはできますか。	いいえ。
クライアントアプリケーションでコンテンツを読み出せるかどうか	読み出すことができるオブジェクトと読み出すことができないオブジェクトがあります。
データがリスクにさらされているかどうか	いいえ。
業務を遂行する能力に重大な影響はありますか。	はい。クライアントアプリケーションからStorageGRID システムにオブジェクトを格納できず、データを一貫して読み出すことができないためです。

データを収集

問題を定義し、リスクと影響を評価したら、分析のためにデータを収集します。収集に最も役立つデータの種類は、問題の内容によって異なります。

収集するデータのタイプ	データを収集する理由	手順
最近の変更のタイムラインを作成します	StorageGRID システム、その設定、または環境を変更すると、原因 の新しい動作を開始できます。	• 最近の変更のタイムラインを作成します

収集するデータのタイプ	データを収集する理由	手順
アラートの確認	アラートは、原因となっている可能性のある根本的な問題に関する重要な手がかりを提供することで、問題の根本原因を迅速に特定するのに役立ちます。 現在のアラートのリストを確認して、StorageGRIDが問題の根本原因を特定したかどうかを確認します。 過去にトリガーされたアラートを確認して、詳細な分析情報を確認します。	• "現在のアラートと解決済みのアラートを表示します"
ベースラインを設定する	さまざまな運用値の通常レベルに関する情報を収集します。これらのベースライン値とこれらのベースラインからの偏差は、貴重な手がかりとなります。	• ベースラインを設定する
取り込みと読み出しのテストを実行する	取り込みと読み出しに関するパフォーマンスの問題のトラブルシューティングを行うには、ワークステーションを使用してオブジェクトの格納と読み出しを行います。クライアントアプリケーションを使用して確認した結果と比較します。	• "PUT / GET パフォーマンスを監視"
監査メッセージを確認します	StorageGRID の処理の詳細については、監査メッセージを確認してください。監査メッセージの詳細は、パフォーマンスの問題など、さまざまな種類の問題のトラブルシューティングに役立ちます。	• "監査メッセージを確認します"
オブジェクトの場所とストレージの整合性をチェックする	ストレージに問題がある場合は、オブジェクトが想定どおりに配置されていることを確認します。ストレージノード上のオブジェクトデータの整合性をチェックします。	• "オブジェクト検証処理を監視する" • "オブジェクトデータの場所を確認する" • "オブジェクトの整合性を検証"
テクニカルサポートに使用するデータを収集します	テクニカルサポートに問い合わせた際に、問題のトラブルシューティングに役立つデータの収集や特定の情報の確認を求められることがあります。	• "ログファイルとシステムデータを収集" • "AutoSupportパッケージを手動でトリガーする" • "サポート指標を確認"

最近の変更のタイムラインを作成します

問題が発生した場合は、最近の変更内容と、その変更がいつ行われたかを検討する必要があります。

- StorageGRID システム、その設定、または環境を変更すると、原因 の新しい動作を開始できます。
- 変更のスケジュールを確認することで、問題 の担当となる変更を特定し、各変更がその開発にどのような

影響を及ぼすかを特定できます。

システムに最近行われた変更の表を作成します。この表には、各変更がいつ行われたかに関する情報と、変更の進行中に他に何が行われたかに関する関連情報が含まれます。

変更時刻	変更のタイプ	詳細
例： • ノードのリカバリを開始したのはいつですか？ • ソフトウェアのアップグレードはいつ完了しましたか？ • プロセスを中断しましたか？	どうしましたか？何をしましたか？	変更に関連する詳細を文書化します。例： • ネットワークの詳細が変更されました。 • インストールされたホットフィックス。 • クライアントのワークロードの変化 同時に複数の変更が発生した場合は注意してください。たとえば、アップグレードの実行中にこの変更が行われたかどうかを確認します。

最近の重要な変更の例

重要な変更の例をいくつか示します。

- StorageGRID システムのインストール、拡張、リカバリを最近行ったかどうか
- システムは最近アップグレードされましたか？ホットフィックスが適用されましたか？
- ハードウェアの修理や交換を最近行ったかどうか
- ILM ポリシーは更新されているか。
- クライアントのワークロードは変化しましたか。
- クライアントアプリケーションまたはその動作に変化はありますか。
- ロードバランサを変更したか、管理ノードまたはゲートウェイノードのハイアベイラビリティグループを追加または削除したか。
- 開始されたタスクのうち、完了までに時間がかかるものはありますか？たとえば、次のようなもの
  - 障害が発生したストレージノードのリカバリ
  - ストレージノードの運用停止
- テナントの追加や LDAP 設定の変更など、ユーザ認証に変更がないかどうか
- データ移行を実行中かどうか
- プラットフォームサービスが最近有効化または変更されましたか？
- 最近、コンプライアンスを有効にしましたか？
- クラウドストレージプールは追加または削除されていますか？
- ストレージの圧縮や暗号化に変更がないかどうか
- ネットワークインフラに変更はありますか。たとえば、 VLAN 、ルータ、 DNS などです。
- NTP ソースに変更がないかどうか

- グリッド、管理、クライアントの各ネットワークインターフェイスに変更がないかどうか
- StorageGRID システムや環境にその他の変更がないかどうか

ベースラインを設定する

さまざまな運用値の通常レベルを記録することで、システムのベースラインを設定できます。将来的には、現在の値をこれらのベースラインと比較して、異常な値を検出して解決することができます。

プロパティ	値	取得方法
ストレージの平均消費量	1 日あたりの GB 消費量 1 日あたりの消費率	Grid Manager に移動します。ノードページで、グリッド全体またはサイトを選択し、ストレージタブに移動します。 Storage Used - Object Data チャートで、この線がかなり安定している期間を探します。グラフにカーソルを合わせて、各日のストレージ消費量を見積もります この情報は、システム全体または特定のデータセンターについて収集できます。
メタデータの平均消費量	1 日あたりの GB 消費量 1 日あたりの消費率	Grid Manager に移動します。ノードページで、グリッド全体またはサイトを選択し、ストレージタブに移動します。 Storage Used - Object Metadata チャートで、この線がかなり安定している期間を探します。グラフにカーソルを合わせて、各日のメタデータストレージ消費量を見積もります この情報は、システム全体または特定のデータセンターについて収集できます。
S3操作のレート	処理数 / 秒	グリッド マネージャー ダッシュボードで、パフォーマンス > ストレージ ノードの **S3** 操作 を選択します。 特定のサイトまたはノードの取り込みおよび取得レートと数を確認するには、[ノード] > [サイトまたはストレージ ノード] > [オブジェクト] を選択します。S3 の取り込みと取得チャートの上にカーソルを置きます。
ILM 評価の速度	オブジェクト数 / 秒	ノードページで、 * *GRID_NETWORK** > * ILM * を選択します。 ILM キューグラフで、この線がかなり安定している期間を探します。グラフにカーソルを合わせて、システムの*評価レート*のベースライン値を推定します。

プロパティ	値	取得方法
ILM のスキャン速度	オブジェクト数 / 秒	ノード > ***grid*** > **ILM** を選択します。 ILM キューグラフで、この線がかなり安定している期間を探します。グラフにカーソルを合わせて、システムの*スキャン速度*のベースライン値を推定します。
クライアント処理からキューに登録されたオブジェクト	オブジェクト数 / 秒	ノード > ***grid*** > **ILM** を選択します。 ILM キューグラフで、この線がかなり安定している期間を探します。グラフにカーソルを合わせて、システムの* Objects queued（クライアント処理からの）*のベースライン値を推定します。
クエリの平均レイテンシ	表示されます	ノード > ストレージ ノード > オブジェクト を選択します。クエリ テーブルで、平均待機時間の値を確認します。

データを分析する

収集した情報を使用して、問題の原因 と潜在的な解決策を特定します。

分析方法は問題の内容によって異なりますが、一般的には次の手順に従ってください。

- アラートを使用して、障害ポイントやボトルネックを特定します。
- アラートの履歴とチャートを使用して、問題の履歴を再構築します。
- チャートを使用して異常を特定し、問題の状況を通常の動作と比較します。

エスカレーション情報のチェックリスト

自分で問題を解決できない場合は、テクニカルサポートにお問い合わせください。テクニカルサポートに連絡する前に、次の表に記載された問題解決に必要な情報を収集してください。

✔	項目	脚注
	問題点	問題の症状は何ですか？問題はいつ発生しましたか？一貫して、または断続的に発生しますか？断続的に発生した場合、何回起きましたか？ 問題を定義します

✔	項目	脚注
	影響の評価	問題の重大度はどの程度ですか。クライアントアプリケーションにはどのような影響がありますか？ • クライアントは以前に正常に接続されていますか？ • クライアントはデータの取り込み、読み出し、削除を実行できますか。
	StorageGRID システム ID	メンテナンス > システム > *ライセンス*を選択します。StorageGRIDシステム ID は、現在のライセンスの一部として表示されます。
	ソフトウェアバージョン	グリッドマネージャの上部から、ヘルプアイコンを選択し、* バージョン情報 * を選択して StorageGRID のバージョンを確認します。
	カスタマイズ	StorageGRID システムの構成をまとめます。たとえば、次のように指定します。 • グリッドでストレージ圧縮、ストレージ暗号化、コンプライアンスを使用していますか？ • ILMによってレプリケートオブジェクトまたはイレイジャーコーディングオブジェクトが作成されるかILM によってサイトの冗長性が確保されるか、ILMルールでBalanced、Strict、Dual Commitの取り込み動作が使用されているか。
	ログファイルとシステムデータ	システムのログ ファイルとシステム データを収集します。サポート > ツール > *ログ収集*を選択します。 ログは、グリッド全体または選択したノードについて収集できます。 選択したノードのログのみを収集する場合は、ADC サービスを持つストレージ ノードを少なくとも 1 つ含めるようにしてください。サイトにインストールされる最初の 3 つのストレージ ノードには、ADC サービスが含まれます。
	ベースライン情報	取り込み処理、読み出し処理、およびストレージ消費量に関するベースライン情報を収集します。 ベースラインを設定する
	最近の変更のタイムライン	システムや環境に対する最近の変更をまとめたタイムラインを作成 最近の変更のタイムラインを作成します

✔	項目	脚注
	問題 を診断するための取り組みの歴史	問題 の診断またはトラブルシューティングの手順を自分で実行した場合は、実行した手順と結果を記録しておいてください。

オブジェクトやストレージの問題をトラブルシューティングする

StorageGRID でオブジェクトデータの場所を確認

問題によっては、実行することもでき"オブジェクトデータの格納先を確認"ます。たとえば、 ILM ポリシーが想定どおりに機能し、オブジェクトデータが意図した場所に格納されていることを確認できます。

開始する前に

- 次のいずれかのオブジェクト ID が必要です。
  - **UUID** ：オブジェクトの Universally Unique Identifier です。UUIDはすべて大文字で入力します。
  - * CBID * ： StorageGRID 内のオブジェクトの一意の識別子。監査ログからオブジェクトの CBID を取得できます。CBIDはすべて大文字で入力します。
  - * S3のバケットとオブジェクトキー*：オブジェクトがから取り込まれる"S3インターフェイス"と、クライアントアプリケーションはバケットとオブジェクトキーの組み合わせを使用してオブジェクトを格納および識別します。

手順

1. ILM * > * Object metadata lookup * を選択します。
2. [* 識別子 * （ * Identifier * ）] フィールドにオブジェクトの識別子を入力します。

   UUID、CBID、または S3 バケット/オブジェクト キーを入力できます。

3. オブジェクトの特定のバージョンを検索する場合は、バージョン ID を入力します（オプション）。



4. 「 * 検索 * 」を選択します。

   が"オブジェクトメタデータの検索結果"表示されます。このページには、次の種類の情報が表示されます。

- システムメタデータ（オブジェクト ID （ UUID ）、バージョン ID （オプション）、オブジェクト名、コンテナの名前、テナントアカウントの名前または ID 、オブジェクトの論理サイズ、オブジェクトの作成日時、オブジェクトの最終変更日時など）。
- オブジェクトに関連付けられているカスタムユーザメタデータのキーと値のペア。
- S3 オブジェクトの場合、オブジェクトに関連付けられているオブジェクトタグのキーと値のペア。
- レプリケートオブジェクトコピーの場合、各コピーの現在の格納場所。
- イレイジャーコーディングオブジェクトコピーの場合、各フラグメントの現在の格納場所。
- クラウドストレージプール内のオブジェクトコピーの場合、外部バケットの名前とオブジェクトの一意の識別子を含むオブジェクトの場所。
- セグメント化されたオブジェクトとマルチパートオブジェクトの場合、セグメント ID とデータサイズを含むオブジェクトセグメントのリスト。100 個を超えるセグメントを持つオブジェクトの場合は、最初の 100 個のセグメントだけが表示されます。
- 未処理の内部ストレージ形式のすべてのオブジェクトメタデータ。この未加工のメタデータには、リリース間で維持されるとはかぎらない内部のシステムメタデータが含まれます。

  次の例では、 2 つのレプリケートコピーとして格納された S3 テストオブジェクトのオブジェクトメタデータの検索結果が表示されています。

System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H$|TFbnQQ}|CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H$|TFboW28|CXG%

Raw Metadata


```
{
    "TYPE": "CTNT",
    "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
    "NAME": "testobject",
    "CBID": "0x8823DE7EC7C10416",
    "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
    "PPTH": "source",
    "META": {
        "BASE": {
            "PAWS": "2",
```


StorageGRID のストレージボリュームのオブジェクトストア障害について学ぶ

ストレージノードの基盤となるストレージは、複数のオブジェクトストアに分割されます。オブジェクトストアはストレージボリュームとも呼ばれます。

各ストレージ ノードのオブジェクト ストア情報を表示できます。 ノード > ストレージ ノード > ストレージを選択します。

Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
sdc(8:16,sdb)	N/A	0.05%	0 bytes/s	4 KB/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s
sdf(8:64,sde)	N/A	0.00%	0 bytes/s	82 bytes/s
sdg(8:80,sdf)	N/A	0.00%	0 bytes/s	82 bytes/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	4 KB/s
cvloc(8:2,sda2)	N/A	0.95%	0 bytes/s	52 KB/s

Volumes

Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.73 GB	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/3	sdf	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/4	sdg	Online	107.32 GB	107.18 GB	Enabled

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	1.55 MB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0003	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0004	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

障害の性質によっては、ストレージボリュームの障害がに反映されることがあります"ストレージボリュームのアラート"。ストレージボリュームに障害が発生した場合は、ストレージノードのすべての機能を復旧するために、障害が発生したストレージボリュームをできるだけ早く修復する必要があります。必要に応じて、*[設定]*タブに移動して、サーバの完全なリカバリの準備中にStorageGRIDシステムがこのタブを使用してデータを取得できるようにすることができ"ストレージノードを読み取り専用状態にします"ます。

StorageGRID でオブジェクトデータの整合性を検証する

StorageGRID システムは、ストレージノード上のオブジェクトデータの整合性を検証し、オブジェクトの破損や欠落の有無を確認します。

検証プロセスには、バックグラウンド検証とオブジェクトの存在チェック（旧称フォアグラウンド検証）の 2 つがあります。データの整合性を確保するために連携して機能します。バックグラウンド検証は、オブジェクトデータの正確性を継続的にチェックするために自動的に実行されます。オブジェクトの存在チェックは、オブジェクトの有無（正確性ではなく）をより迅速に確認するためにユーザによってトリガーされることがあります。

バックグラウンド検証とは何ですか？

バックグラウンド検証プロセスは、ストレージノードにオブジェクトデータの破損したコピーがないかどうかを自動的かつ継続的にチェックし、問題が見つかった場合は自動的に修復を試みます。

バックグラウンド検証は、レプリケートオブジェクトとイレイジャーコーディングオブジェクトの整合性を次の方法でチェックします。

- * レプリケートオブジェクト * ：バックグラウンド検証プロセスで破損したレプリケートオブジェクトが検出された場合、破損したコピーはその場所から削除され、ストレージノード上の他の場所に隔離されます。その後、アクティブなILMポリシーに従って新しい破損していないコピーが生成されて配置されます。新しいコピーは、元のコピーに使用されていたストレージノードに配置されるとはかぎりません。

  > ⓘ 破損したオブジェクトデータは、引き続きアクセスできるように、システムから削除されるのではなく隔離されます。隔離されたオブジェクトデータへのアクセスの詳細については、テクニカルサポートにお問い合わせください。

- * イレイジャーコーディングオブジェクト * ：バックグラウンド検証プロセスでイレイジャーコーディングオブジェクトのフラグメントの破損が検出された場合、 StorageGRID は自動的に残りのデータとパリティフラグメントを使用して同じストレージノード上に欠落フラグメントの再構築を試みます。破損したフラグメントを再構築できない場合は、オブジェクトの別のコピーを取得しようとします。読み出しに成功すると、 ILM 評価が実行されて、イレイジャーコーディングオブジェクトの置き換え用のコピーが作成されます。

  バックグラウンド検証プロセスでは、ストレージノード上のオブジェクトのみチェックされます。クラウドストレージプール内のオブジェクトはチェックされません。バックグラウンド検証を実行するには、 4 日以上経過したオブジェクトが必要です。

バックグラウンド検証は、通常のシステムアクティビティを妨げないように設定された間隔で継続的に実行されます。バックグラウンド検証を停止することはできません。ただし、問題があると疑われる場合は、バックグラウンド検証の回数を増やして、ストレージノードの内容をより迅速に検証することができます。

バックグラウンド検証に関連するアラート

破損したオブジェクトが検出され、自動的に修正できない場合（破損によってオブジェクトを特定できないため）は、* Unidentified corrupt object detected *アラートがトリガーされます。

バックグラウンド検証で別のコピーが見つからないために破損したオブジェクトを置き換えることができない場合は、「オブジェクトが失われている可能性があります」というアラートがトリガーされます。

オブジェクトの存在チェックとは何ですか？

オブジェクトの存在チェックでは、オブジェクトとイレイジャーコーディングフラグメントの想定されるレプリケートコピーがすべてストレージノードに存在するかどうかが検証されます。オブジェクトの存在チェックでは、オブジェクトデータ自体は検証されません（バックグラウンド検証で検証されます）。代わりに、ストレージデバイスの整合性を検証する方法が提供されます。特に、最新のハードウェア問題 がデータの整合性に影響を与える可能性がある場合に役立ちます。

自動的に実行されるバックグラウンド検証とは異なり、オブジェクト存在チェックジョブは手動で開始する必要があります。

オブジェクトの存在チェックでは、 StorageGRID に格納されているすべてのオブジェクトのメタデータが読み取られ、レプリケートされたオブジェクトコピーとイレイジャーコーディングされたオブジェクトフラグメントの両方の存在が検証されます。不足しているデータは次のように処理されます。

- * Replicated Copies * ：レプリケートオブジェクトデータのコピーが見つからない場合、 StorageGRID はシステム内の別の場所に格納されているコピーからコピーを自動的に置き換えます。ストレージノードは既存のコピーに対して ILM を評価します。これにより、別のコピーがないために、このオブジェクトに関して現在の ILM ポリシーは満たされていないという結果となります。システムのアクティブなILMポリシーに従って新しいコピーが生成されて配置されます。この新しいコピーは、欠落したコピーが格納されていた場所に配置されるとはかぎりません。
- * イレイジャーコーディングされたフラグメント * ：イレイジャーコーディングされたオブジェクトのフラグメントが欠落している場合、 StorageGRID は自動的に残りのフラグメントを使用して同じストレージノード上に欠落フラグメントの再構築を試みます。失われたフラグメントが多すぎるために欠落フラグメントを再構築できない場合、ILMはオブジェクトの別のコピーを探し、このコピーを使用して新しいイレイジャーコーディングフラグメントを生成します。

オブジェクトの存在チェックを実行します

オブジェクト存在チェックジョブは、一度に 1 つずつ作成して実行します。ジョブを作成するときに、検証するストレージノードとボリュームを選択します。また、ジョブの整合性も選択します。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"Maintenance権限またはRoot Access権限"。
- 確認するストレージ ノードがオンラインであることを確認しました。ノードのテーブルを表示するには、「ノード」を選択します。確認するノードのノード名の横にアラート アイコンが表示されていないことを確認します。
- チェックするノードで次の手順が * 実行されていないことを確認します。
  - Grid の拡張：ストレージノードを追加
  - ストレージノードの運用停止

- 障害ストレージボリュームのリカバリ
- 障害システムドライブがあるストレージノードのリカバリ
- EC のリバランシング
- アプライアンスノードのクローン

これらの手順の実行中は、オブジェクトの存在チェックで有用な情報が得られません。

タスクの内容

オブジェクトの存在確認ジョブは、グリッド内のオブジェクトの数、選択したストレージノードとボリューム、選択した整合性によって、完了するまでに数日から数週間かかることがあります。一度に実行できるジョブは 1 つだけですが、同時に複数のストレージノードとボリュームを選択することもできます。

手順

1. メンテナンス > タスク > *オブジェクト存在チェック*を選択します。
2. 「 * ジョブの作成 * 」を選択します。Create an object existence check job ウィザードが表示されます。
3. 検証するボリュームが含まれているノードを選択します。オンラインノードをすべて選択するには、列ヘッダーの*[ノード名]*チェックボックスをオンにします。

   ノード名またはサイトで検索できます。

   グリッドに接続されていないノードは選択できません。

4. 「 * Continue * 」を選択します。
5. リスト内のノードごとに 1 つ以上のボリュームを選択します。ストレージボリューム番号またはノード名を使用してボリュームを検索できます。

   選択した各ノードですべてのボリュームを選択するには、列ヘッダーの*[ストレージボリューム]*チェックボックスを選択します。

6. 「 * Continue * 」を選択します。
7. ジョブの整合性を選択します。

   整合性によって、オブジェクトの存在チェックに使用されるオブジェクトメタデータのコピーの数が決まります。

   - * strong-site * ：単一のサイトにおけるメタデータのコピーが 2 つ
   - * strong-global * ：各サイトにおけるメタデータのコピーが 2 つ
   - * all * （デフォルト）：各サイトに 3 つのメタデータのすべてのコピーを格納します。

     整合性の詳細については、ウィザードの説明を参照してください。

8. 「 * Continue * 」を選択します。
9. 選択内容を確認します。「 * Previous * 」を選択すると、ウィザードの前の手順に進み、選択内容を更新できます。

   オブジェクト存在チェックジョブが生成され、次のいずれかが実行されるまで実行されます。

- ジョブが完了します。
- ジョブを一時停止またはキャンセルした場合。一時停止したジョブは再開できますが、キャンセルしたジョブは再開できません。
- ジョブが停止します。Object existence check has ストール * アラートがトリガーされます。アラートに対して指定された対処方法に従います。
- ジョブが失敗します。* Object existence check has failed * というアラートがトリガーされます。アラートに対して指定された対処方法に従います。
- 「Service Unavailable」または「Internal server error」というメッセージが表示されます。1 分後にページを更新して、ジョブの監視を続行します。

> 必要に応じて、 [オブジェクトの有無] チェックページから移動して、ジョブの監視を続行することができます。

10. ジョブの実行中に、「 * Active job * 」タブを表示して、検出されたオブジェクトコピーが欠落していることを確認します。

    この値は、レプリケートオブジェクトとイレイジャーコーディングオブジェクトの欠落コピーのうち、 1 つ以上のフラグメントが欠落しているものの合計数を表します。

    検出された欠落オブジェクトのコピー数が 100 を超える場合、ストレージ ノードのストレージに問題がある可能性があります。

11. ジョブが完了したら、さらに必要なアクションを実行します。
    - 欠落オブジェクトコピーが 0 であることが検出された場合、問題は見つかりませんでした。対処は不要です。
    - 検出された欠落オブジェクトのコピー数がゼロより大きく、*潜在的に失われたオブジェクト*アラートがトリガーされていない場合、すべての欠落コピーはシステムによって修復されています。オブジェクトのコピーが将来損傷するのを防ぐために、ハードウェアの問題が修正されていることを確認します。
    - 検出されたオブジェクトのコピーの不足数がゼロより大きく、*オブジェクトが失われている可能性がある*アラートがトリガーされた場合、データの整合性が影響を受ける可能性があります。テクニカルサポートにお問い合わせください。
    - grep を使用して LLST 監査メッセージを抽出することで、潜在的に失われたオブジェクトのコピーを調査できます。 `grep LLST audit_file_name` 。

      この手順は、"紛失した可能性のある物品の調査"ただし、オブジェクトのコピーを検索する場合は、 `LLST` の代わりに `OLST` 。

12. ジョブでstrong-site整合性またはstrong-global整合性を選択した場合は、メタデータの整合性が確保されるまで約3週間待ってから、同じボリュームに対してジョブを再実行します。

    ジョブに含まれるノードとボリュームでメタデータの整合性を維持するための時間がかかっていた場合、誤って報告された欠落オブジェクトコピーまたは原因 を見逃していたオブジェクトコピーをジョブで再実行することで解決できます。 StorageGRID

    a. メンテナンス > オブジェクト存在チェック > *ジョブ履歴*を選択します。
    b. 再実行する準備ができているジョブを特定します。

i. 3 週間以上前に実行されたジョブを特定するには、「 * End time * 」列を参照してください。

ii. これらのジョブについては、コンシステンシコントロール列をスキャンして、強サイトまたは強グローバルを確認します。

c. 再実行する各ジョブのチェックボックスをオンにして、*再実行*を選択します。

d. ジョブの再実行ウィザードで、選択したノードとボリューム、および整合性を確認します。

e. ジョブを再実行する準備ができたら、 * 再実行 * を選択します。

[アクティブジョブ] タブが表示されます。選択したすべてのジョブは、strong-siteの一貫性のある1つのジョブとして再実行されます。[詳細] セクションの [関連ジョブ] フィールドには、元のジョブのジョブ ID が一覧表示されます。

StorageGRIDでS3 PUTオブジェクトサイズが大きすぎるというアラートを解決する

S3 PUT Object size too largeアラートは、S3サイズの上限である5GiBを超えるマルチパートでないPutObject処理をテナントが試行するとトリガーされます。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- そうだな "特定のアクセス権限"

5GiBを超えるオブジェクトを使用しているテナントを確認して、通知できるようにします。

手順

1. 構成 > 監視 > 監査および **syslog** サーバー に移動します。
2. クライアントからの書き込みがNormalの場合は、監査ログにアクセスします。

a. 入力 `ssh admin@primary_Admin_Node_IP`

b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

c. 次のコマンドを入力してrootに切り替えます。 `su -`

d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

rootとしてログインすると、プロンプトがからに `#`変わります `$`。

e. 監査ログが格納されているディレクトリに移動します。

監査ログディレクトリおよび該当するノードは、監査デスティネーションの設定によって異なります。

オプション	デスティネーション
ローカルノード（デフォルト）	`/var/local/log/localaudit.log`

オプション	デスティネーション
管理ノード/ローカルノード	• 管理ノード (プライマリおよび非プライマリ): `/var/local/audit/export/audit.log` • All nodes（すべてのノード）：`/var/local/log/localaudit.log`通常、このモードではファイルが空か欠落しています。
外部 syslog サーバ	`/var/local/log/localaudit.log`

監査先の設定に応じて、次のように入力します。 `cd /var/local/log`または `/var/local/audit/export/`

詳細については、"ログの場所を選択" 。

f. 5GiBを超えるオブジェクトを使用しているテナントを特定します。

i. 入力 `zgrep SPUT * | egrep "CSIZ\(UI64\):([5-9]|[1-9][0-9]+)[0-9]{9}"`

ii. 結果内の各監査メッセージについて、フィールドを確認してテナントアカウントIDを確認し`S3AI`ます。メッセージ内の他のフィールドを使用して、クライアント、バケット、およびオブジェクトによって使用されていたIPアドレスを確認します。

コード	製品説明
saip	送信元IP
S3AI	テナントID
S3BK	バケット
S3KY	オブジェクト
CSIZ	サイズ（バイト）

監査ログ結果の例

```
audit.log:2023-01-05T18:47:05.525999
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1672943621106262][TIME(UI64):804317333
3][SAIP(IPAD):"10.96.99.127"][S3AI(CSTR):"93390849266154004343"][SACC(CS
TR):"bhavna"][S3AK(CSTR):"06OX85M40Q90Y280B7YT"][SUSR(CSTR):"urn:sgws:id
entity::93390849266154004343:root"][SBAI(CSTR):"93390849266154004343"][S
BAC(CSTR):"bhavna"][S3BK(CSTR):"test"][S3KY(CSTR):"large-
object"][CBID(UI64):0x077EA25F3B36C69A][UUID(CSTR):"A80219A2-CD1E-466F-
9094-
B9C0FDE2FFA3"][CSIZ(UI64):6040000000][MTME(UI64):1672943621338958][AVER(
UI32):10][ATIM(UI64):1672944425525999][ATYP(FC32):SPUT][ANID(UI32):12220
829][AMID(FC32):S3RQ][ATID(UI64):4333283179807659119]]
```

3. [Client Writes]が[Normal]でない場合は、アラートのテナントIDを使用してテナントを特定します。

   a. サポート > ツール > ログ収集 に移動します。アラート内のストレージ ノードのアプリケーション ログを収集します。アラートの前後 15 分を指定します。。 "ログファイルとシステムデータを収集" 。

   b. ファイルを展開し、次の場所に移動し `bycast.log`ます。

      ```
      /GID<grid_id>_<time_stamp>/<site_node>/<time_stamp>/grid/bycast.log
      ```

   c. ログを検索し、フィールドで `method=PUT`クライアントを特定し `clientIP`ます。

      - bycast.logの例*

```
Jan  5 18:33:41 BHAVNAJ-DC1-S1-2-65 ADE: |12220829 1870864574 S3RQ %CEA
2023-01-05T18:33:41.208790| NOTICE   1404 af23cb66b7e3efa5 S3RQ:
EVENT_PROCESS_CREATE - connection=1672943621106262 method=PUT
name=</test/4MiB-0> auth=<V4> clientIP=<10.96.99.127>
```

4. テナントに、PutObjectの最大サイズが5GiBであり、5GiBを超えるオブジェクトにマルチパートアップロードを使用するように伝えます。
5. アプリケーションが変更されている場合は、警告を1週間無視します。

失われたオブジェクトデータと欠落しているオブジェクトデータのトラブルシューティング

StorageGRIDで紛失したオブジェクトデータと行方不明のオブジェクトデータについて学ぶ

オブジェクトはさまざまな理由で読み出されます。たとえば、クライアントアプリケーションからの読み取り要求、レプリケートされたオブジェクトデータのバックグラウンド検証、 ILM ルールによる再評価、ストレージノードのリカバリ時のオブジェクトデータのリストアなどの目的で行われます。

StorageGRIDシステムは、オブジェクトのメタデータ内の場所情報を使用して、オブジェクトを取得する場所を決定します。オブジェクトのコピーが予期された場所に見つからない場合、システムは、ILM ポリシーにオブジェクトのコピーを 2 つ以上作成するルールが含まれていると想定して、システム内の他の場所からオブジェクトの別のコピーを取得しようとします。

この取得が成功すると、 StorageGRIDシステムはオブジェクトの失われたコピーを置き換えます。それ以外の場合は、次のように「オブジェクトが失われる可能性がある」というアラートがトリガーされます。

- レプリケートコピーについては、別のコピーを読み出せない場合、オブジェクトが失われたとみなされてアラートがトリガーされます。
- イレイジャーコーディングコピーの場合、想定される場所からコピーを読み出せない場合は、別の場所からの読み出しが試行される前に、Corrupt Copies Detected（ECOR）属性の値が1つ増分されます。他のコピーが見つからない場合は、アラートがトリガーされます。

すべての「オブジェクトが失われる可能性がある」アラートをただちに調査し、損失の根本原因を特定し、オブジェクトがオフラインまたは現在利用できないストレージ ノードにまだ存在する可能性があるかどうかを判断する必要があります。見る"紛失した可能性のある物品を調査する" 。紛失物アラートは、注意を怠ると誤ってトリガーされる可能性があります。

コピーのないオブジェクト データが失われた場合、回復ソリューションはありません。しかし、あなたは"紛失の可能性のあるオブジェクトのカウンターをリセットする"既知の紛失オブジェクトが新たな紛失オブジェクトを覆い隠してしまうことを防ぐためです。

StorageGRID で紛失の可能性のあるオブジェクトアラートを解決する

*オブジェクトが失われる可能性がある*アラートがトリガーされた場合は、すぐに調査する必要があります。影響を受けるオブジェクトに関する情報を収集し、テクニカル サポートに連絡してください。

開始する前に

- Grid Managerにサインインする必要があります"サポートされている Web ブラウザ"。
- そうだな "特定のアクセス権限"
- ファイルが必要 `Passwords.txt`です。

タスクの内容

オブジェクトが失われている可能性がある アラートは、 StorageGRIDで利用可能な情報によると、グリッド内にオブジェクトのコピーが存在しないことを示します。データは永久に失われた可能性があります。

損失オブジェクトのアラートをただちに調査してください。これ以上のデータ損失を防ぐための対処が必要になる場合があります。迅速に対処すれば、損失オブジェクトをリストアできる場合があります。

> 10 個を超えるオブジェクトの損失が報告された場合は、テクニカル サポートにお問い合わせください。この手順を自分で実行しないでください。

手順

1. *ノード*を選択します。
2. [***Storage Node***>* Objects*] を選択します。
3. オブジェクト数の表に表示された損失オブジェクトの数を確認します。

   この数値は、 StorageGRID システム全体で欠落していることがグリッドノードで検出されたオブジェクトの合計数を示します。この値は、 LDR サービスと DDS サービスに含まれるデータストアコンポーネントの損失オブジェクトカウンタの合計です。

4. 管理ノードから、"監査ログにアクセスします" *オブジェクトが失われる可能性がある*アラートをトリガーしたオブジェクトの一意の識別子 (UUID) を決定します。

   a. グリッドノードにログインします。

      i. 次のコマンドを入力します。 `ssh admin@grid_node_IP`

      ii. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

      iii. 次のコマンドを入力してrootに切り替えます。 `su -`

      iv. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。`root`としてログインすると、プロンプトがからに `#`変わります `$`。

   b. 監査ログが格納されているディレクトリに移動します。

      監査ログディレクトリおよび該当するノードは、監査デスティネーションの設定によって異なります。

オプション	デスティネーション
ローカルノード（デフォルト）	`/var/local/log/localaudit.log`
管理ノード/ローカルノード	• 管理ノード (プライマリおよび非プライマリ): `/var/local/audit/export/audit.log` • All nodes（すべてのノード）：`/var/local/log/localaudit.log`通常、このモードではファイルが空か欠落しています。
外部 syslog サーバ	`/var/local/log/localaudit.log`

      監査先の設定に応じて、次のように入力します。 `cd /var/local/log`または `/var/local/audit/export/`

      詳細については、"ログの場所を選択" 。

   c. grep を使用して Object Lost （ OLST ）監査メッセージを抽出します。入力： `grep OLST audit_file_name`

   d. メッセージに含まれている UUID の値をメモします。

```
Admin: # grep OLST audit.log
2020-02-12T19:18:54.780426
[AUDT:[CBID(UI64):0x38186FE53E3C49A5][UUID(CSTR):"926026C4-00A4-449B-
AC72-BCCA72DD1311"]
[PATH(CSTR):"source/cats"][NOID(UI32):12288733][VOLI(UI64):3222345986
][RSLT(FC32):NONE][AVER(UI32):10]
[ATIM(UI64):1581535134780426][ATYP(FC32):OLST][ANID(UI32):12448208][A
MID(FC32):ILMX][ATID(UI64):7729403978647354233]]
```

5. UUIDを使用して損失オブジェクトのメタデータを検索します。

a. ILM * > * Object metadata lookup * を選択します。

b. UUIDを入力し、*[検索]*を選択します。

c. メタデータ内の場所を確認し、該当する処理を実行します。

メタデータ	まとめ
オブジェクト<object_identifier>が見つかりません	オブジェクトが見つからない場合は、メッセージ「ERROR":""」が返されます。 オブジェクトが見つからない場合は、紛失の可能性のあるオブジェクトのカウンターをリセットするアラートをクリアします。オブジェクトがない場合は、オブジェクトが意図的に削除されたことを示します。
場所が 0 より大きい	出力に場所がリストされている場合、「オブジェクトが失われる可能性がある」アラートは誤検知である可能性があります。 オブジェクトが存在することを確認します。出力に表示されたノード ID とファイルパスを使用して、オブジェクトファイルがリストされた場所にあることを確認します。 オブジェクトが存在する場合、紛失の可能性のあるオブジェクトのカウンターをリセットするアラートをクリアします。
場所 = 0	出力に場所がリストされていない場合は、オブジェクトが欠落している可能性があります。テクニカル サポートにお問い合わせください。 テクニカルサポートから、ストレージ復旧手順が進行中かどうかを確認するよう求められる場合があります。参照： • "アプライアンスのストレージボリュームにオブジェクトデータをリストアします" • "システムドライブに損傷がない場合は、オブジェクトデータをストレージボリュームにリストアします" • "オブジェクトデータをストレージボリュームにリストアする（システムドライブの障害）"

6. 紛失したオブジェクトの問題を解決した後、アラートが誤検知にならないように、紛失した可能性のあるオブジェクトのカウンターをリセットします。

a. *ノード*を選択します。

b. ストレージノード > *タスク*を選択します。

c. 潜在的に失われたオブジェクトのカウンターをリセットするセクションで、[リセット] を選択します。

Low object data storage * アラートは、オブジェクトデータを格納可能な各ストレージノードのスペースを監視します。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- そうだな "特定のアクセス権限"

タスクの内容

Low object data storage *アラートは、ストレージノード上のレプリケートオブジェクトデータとイレイジャーコーディングオブジェクトデータの合計量がアラートルールで設定されている条件のいずれかを満たすとトリガーされます。

デフォルトでは、次の条件が true と評価されると、 Major アラートがトリガーされます。

```
(storagegrid_storage_utilization_data_bytes/
(storagegrid_storage_utilization_data_bytes +
storagegrid_storage_utilization_usable_space_bytes)) >=0.90
```

この条件では、次のように

- `storagegrid_storage_utilization_data_bytes`は、ストレージノードのレプリケートオブジェクトデータとイレイジャーコーディングオブジェクトデータの推定合計サイズです。
- `storagegrid_storage_utilization_usable_space_bytes`は、ストレージノードに残っているオブジェクトストレージスペースの総容量です。

Major または Minor * Low object data storage * アラートがトリガーされた場合は、できるだけ早く拡張手順を実行する必要があります。

手順

1. アラート > *現在*を選択します。

   [Alerts] ページが表示されます。

2. アラートの表で、必要に応じて「 * Low object data storage * 」アラートグループを展開し、表示するアラートを選択します。

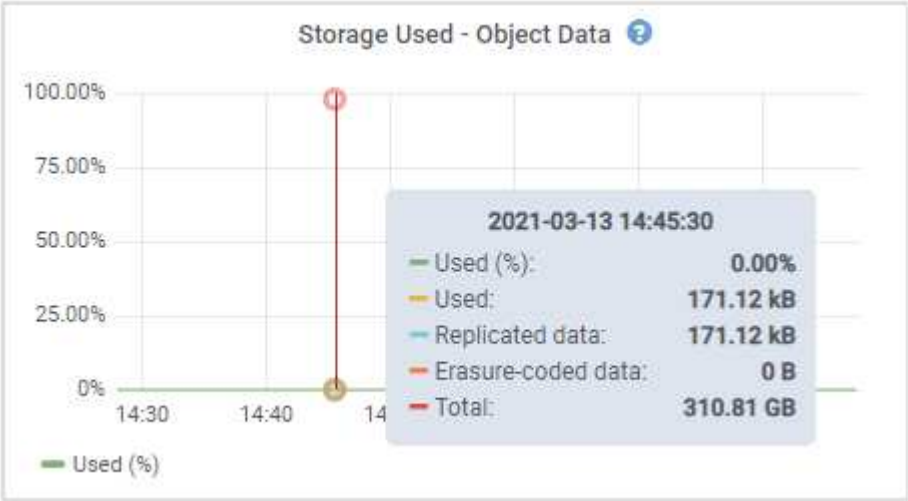
   アラートグループの見出しではなく、アラートを選択します。

3. ダイアログボックスで詳細を確認し、次の点に注意してください。
   - トリガーされた時刻
   - サイトとノードの名前
   - このアラートに関する指標の現在の値
4. ノード > ストレージ ノードまたはサイト > ストレージ を選択します。

5. [Storage Used - Object Data]グラフにカーソルを合わせます。

   次の値が表示されます。

   - * Used （％） * ：オブジェクトデータに使用されている合計使用可能スペースの割合。
   - * Used * ：オブジェクトデータに使用されている合計使用可能スペースの量。
   - * Replicated data * ：このノード、サイト、またはグリッド上のレプリケートオブジェクトデータの推定量。
   - * イレイジャーコーディングデータ * ：このノード、サイト、またはグリッドにあるイレイジャーコーディングオブジェクトデータの推定量。
   - * Total * ：このノード、サイト、またはグリッドで使用可能なスペースの総容量。[Used]の値はメトリックです `storagegrid_storage_utilization_data_bytes`。



6. グラフ上部の時間コントロールを選択して、期間を変えながらストレージの使用状況を確認します。

   ストレージの使用状況の推移を確認することで、アラートがトリガーされた前後のストレージの使用量がわかり、ノードの残りのスペースがいっぱいになるまでの時間を予測できます。

7. できるだけ早く、"ストレージ容量を追加"あなたのグリッドに。

   既存のストレージノードにストレージボリューム（ LUN ）を追加するか、または新しいストレージノードを追加することができます。

   詳細については、を参照してください "ストレージノードがいっぱいになったときの管理"。

StorageGRIDで透かしの上書きアラートを解決する

ストレージボリュームのウォーターマークにカスタム値を使用する場合は、「読み取り専用の低ウォーターマーク上書き * 」アラートを解決する必要があります。可能であれば、最適化された値の使用を開始するようにシステムを更新してください。

以前のリリースでは、3つ"ストレージボリュームのウォーターマーク"はグローバル設定でした。—すべての

ストレージノードのすべてのストレージボリュームに同じ値が適用されていました。StorageGRID 11.6 以降では、ストレージノードのサイズとボリュームの相対容量に基づいて、ストレージボリュームごとにこれらのウォーターマークを最適化できます。

StorageGRID 11.6以降にアップグレードすると、次のいずれかに該当する場合を除き、最適化された読み取り専用ウォーターマークと読み取り/書き込みウォーターマークがすべてのストレージボリュームに自動的に適用されます。

- システムは容量に近く、最適化されたウォーターマークが適用されている場合は新しいデータを受け入れられません。この場合、 StorageGRID はウォーターマーク設定を変更しません。
- 以前にストレージボリュームのウォーターマークをカスタム値に設定している。StorageGRID では、カスタムウォーターマーク設定を最適化された値で上書きしません。ただし、ストレージボリュームのソフト読み取り専用ウォーターマークのカスタム値が小さすぎると、StorageGRIDによって* Low read-only watermark override *アラートがトリガーされることがあります。

アラートを確認します

ストレージボリュームのウォーターマークにカスタム値を使用すると、 1 つ以上のストレージノードに対して * 読み取り専用の低ウォーターマーク上書き * アラートがトリガーされる可能性があります。

アラートの各インスタンスで、ストレージボリュームのソフト読み取り専用ウォーターマークのカスタム値が、そのストレージノードに対して最適化された最小値よりも小さいことが示されています。カスタム設定を引き続き使用すると、ストレージノードのスペースが非常に少なくなる可能性があります。この値を超えると、ストレージノードは読み取り専用状態に安全に移行できます。ノードの容量が上限に達すると、一部のストレージボリュームにアクセスできなくなる（自動的にアンマウントされる）ことがあります。

たとえば、ストレージボリュームのソフト読み取り専用ウォーターマークを5GBに設定したとします。次に、ストレージノード A の 4 つのストレージボリュームについて、 StorageGRID が次の最適化値を計算したとします。

ボリューム0	12GB
ボリューム1	12GB
巻2	11GB
巻三	15GB

カスタムのウォーターマーク（ 5GB ）がそのノード内のすべてのボリュームに対する最小最適値（ 11GB ）よりも小さいため、「 Low read-only watermark overrid* 」アラートがストレージノード A に対してトリガーされます。カスタム設定を引き続き使用すると、ノードが読み取り専用状態に安全に移行できるようになる前に、ノードのスペースが非常に少なくなる可能性があります。

アラートを解決します

1 つ以上の * 読み取り専用の低ウォーターマーク上書き * アラートがトリガーされた場合は、次の手順を実行します。また、現在カスタムのウォーターマーク設定を使用しており、アラートがトリガーされていない場合でも最適化された設定の使用を開始する場合にも、この手順を使用できます。

開始する前に

- StorageGRID 11.6以降へのアップグレードが完了している。
- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"rootアクセス権限"。

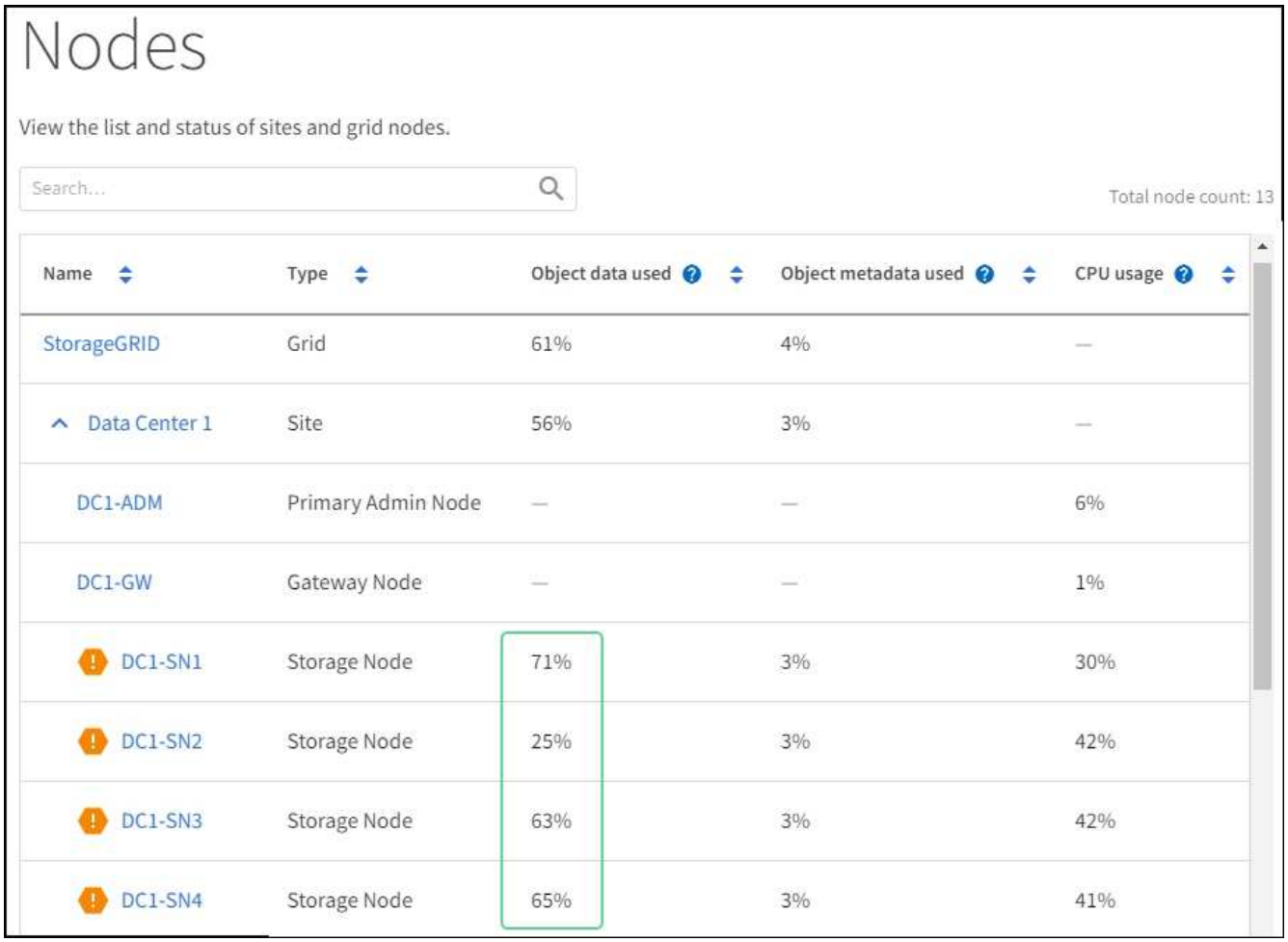
タスクの内容

カスタム・ウォーターマーク設定を新しいウォーターマークの上書きに更新することにより ' 読み取り専用のロー・ウォーターマーク・オーバーライド * アラートを解決できますただし、 1 つ以上のストレージノードがいっぱいに近づいている場合や特別な ILM 要件がある場合は、まず最適化されたストレージウォーターマークを表示して、そのノードを安全に使用できるかどうかを確認する必要があります。

グリッド全体のオブジェクトデータ使用量を評価します

手順

1. *ノード*を選択します。
2. グリッド内のサイトごとに、ノードのリストを展開します。
3. 各サイトの各ストレージノードについて、「 * Object Data Used * 」列に表示されている割合値を確認します。



4. 該当する手順を実行します。
   a. ほぼすべてのストレージノードが上限に近い場合（使用済みオブジェクトデータがすべて * されている値が 80% 未満の場合など）は、無視設定を使用できます。にアクセスします。

b. ILMルールの取り込み動作がStrictに設定されている場合や特定のストレージプールがフルに近い場合は、およびの手順を実行します。最適化されたストレージウォーターマークを表示する最適化されたウォーターマークを使用できるかどうかを確認します

最適化されたストレージのウォーターマークの表示

StorageGRIDでは、2つのPrometheus指標を使用して、ストレージボリュームのソフト読み取り専用ウォーターマークに対して計算された最適化された値が表示されます。グリッド内の各ストレージノードの最適化された最小値と最大値を表示できます。

手順

1. サポート > ツール > *メトリック*を選択します。
2. Prometheus セクションで、 Prometheus ユーザインターフェイスへのリンクを選択します。
3. 推奨されるソフト読み取り専用の最小ウォーターマークを確認するには、次の Prometheus 指標を入力し、 * Execute * を選択します。

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

   最後の列には、各ストレージノードのすべてのストレージボリュームについて、ソフト読み取り専用ウォーターマークの最適化された最小値が表示されます。この値がストレージボリュームのソフト読み取り専用ウォーターマークのカスタム設定よりも大きい場合は、ストレージノードに対して* Low read-only watermark override *アラートがトリガーされます。

4. 推奨されるソフト読み取り専用の最大ウォーターマークを確認するには、次の Prometheus 指標を入力し、 * Execute * を選択します。

   ```
   storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
   ```

   最後の列には、各ストレージノード上のすべてのストレージボリュームについて、ソフト読み取り専用ウォーターマークの最適化された最大値が表示されます。

5. [[maximum_optimized_value] 各ストレージノードの最適化された最大値をメモします。

最適化されたウォーターマークを使用できるかどうかを判断する

手順

1. *ノード*を選択します。
2. オンラインのストレージノードごとに上記の手順を繰り返します。
   a. [***Storage Node***>* Storage*] を選択します。
   b. オブジェクトストアの表までスクロールしてください。
   c. 各オブジェクトストア（ボリューム）の Available * 値を、そのストレージノード用にメモした最大最適ウォーターマークと比較します。
3. オンラインの各ストレージノード上の少なくとも1つのボリュームに、そのノードで最適化された最大ウォーターマークよりも多くのスペースがある場合は、に進み、最適化されたウォーターマークを使用最適化されたウォーターマークの使用を開始します。

   それ以外の場合は、できるだけ早くグリッドを拡張してください。"ストレージボリュームを追加します"既存のノードまたは"新しいストレージノードを追加します"。次に、に移動して最適化されたウォーター

マークを使用透かし設定を更新します。

4. ストレージボリュームのウォーターマークにカスタム値を引き続き使用する必要がある場合"無音"、または"無効化"* Low read-only watermark override *アラート。

> 各ストレージノード上の各ストレージボリュームには、同じカスタムのウォーターマーク値が適用されます。ストレージボリュームのウォーターマーク原因 に推奨よりも小さい値を使用すると、ノードの容量に達したときに一部のストレージボリュームにアクセスできなくなる（自動的にアンマウントされる）ことがあります。

最適化されたウォーターマークを使用する

手順

1. サポート > その他 > ストレージのウォーターマーク に移動します。
2. [最適化された値を使用する]チェックボックスをオンにします。
3. [保存（ Save ）] を選択します。

ストレージノードのサイズとボリュームの相対容量に基づいて、ストレージボリュームごとに最適化されたストレージボリュームのウォーターマーク設定が有効になりました。

StorageGRID でメタデータの問題のトラブルシューティング

メタデータに問題が発生した場合は、問題の原因と推奨される対処方法をアラートで通知します。特に、Low metadata storageアラートがトリガーされた場合は、新しいストレージノードを追加する必要があります。

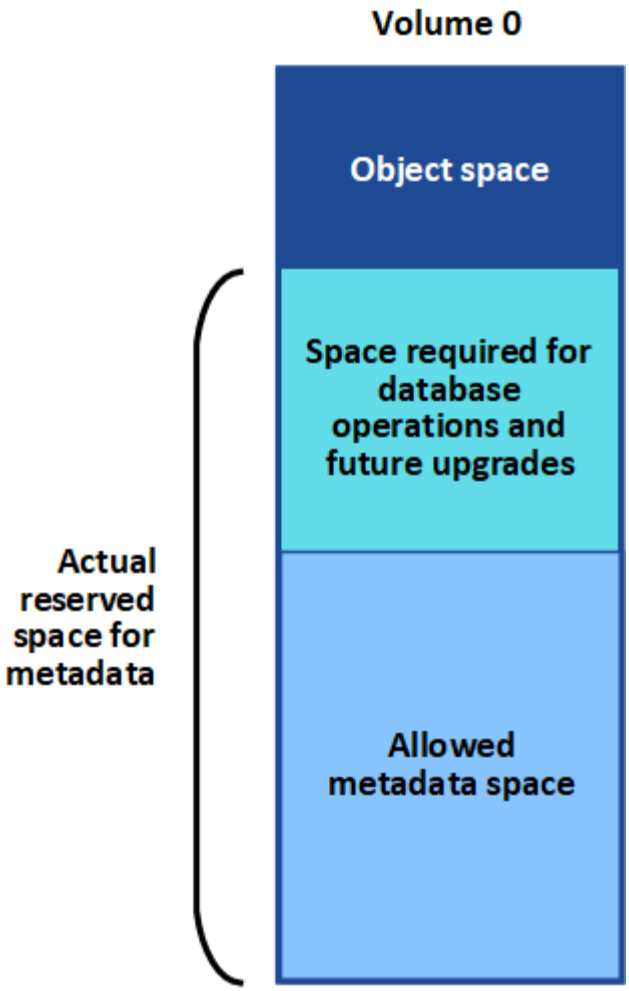
開始する前に

Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。

タスクの内容

メタデータ関連アラートがトリガーされたそれぞれの推奨される対処方法に従います。Low metadata storage * アラートがトリガーされた場合は、新しいストレージノードを追加する必要があります。

StorageGRID は、各ストレージノードのボリューム 0 上にオブジェクトメタデータ用に一定量のスペースをリザーブします。このスペースは_actualリザーブスペース_と呼ばれ、オブジェクトメタデータに使用できるスペース（使用できるメタデータスペース）と、コンパクションや修復などの重要なデータベース処理に必要なスペースに分割されます。許可されるメタデータスペースは、オブジェクトの全体的な容量を決定します。



オブジェクトメタデータがメタデータに使用できるスペースの100%を超えると、データベース処理を効率的に実行できず、エラーが発生します。

"各ストレージノードのオブジェクトメタデータ容量を監視します"エラーを予測し、発生する前に修正するのに役立ちます。

StorageGRID は、次の Prometheus 指標を使用して、許可されているメタデータスペースの使用状況を測定します。

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utiliza
tion_metadata_allowed_bytes
```

この Prometheus 式が特定のしきい値に達すると、 * Low metadata storage * アラートがトリガーされます。

- * Minor * ：オブジェクトメタデータが、許可されているメタデータスペースの 70% 以上を使用しています。できるだけ早く新しいストレージノードを追加する必要があります。
- * Major * ：オブジェクトメタデータが使用しているメタデータスペースが 90% 以上あります。すぐに新しいストレージノードを追加する必要があります。

オブジェクトメタデータが使用可能なメタデータスペースの90%以上を使用している場合は、ダッシュボードに警告が表示されます。この警告が表示された場合は、すぐに新しいストレージノードを追加する必要があります。オブジェクトメタデータの使用量は、使用できるスペースの 100% を超えないようにする必要があります。

- * クリティカル * ：オブジェクトメタデータが使用可能なメタデータスペースの 100% 以上を使用しており、重要なデータベース処理に必要なスペースを使い始めています。新しいオブジェクトの取り込みを停止し、すぐに新しいストレージノードを追加する必要があります。

ボリューム 0 のサイズが Metadata Reserved Space ストレージオプションより小さい場合（非本番環境など）は、「 Low metadata storage * 」アラートが正確に計算されないことがあります。

手順

1. アラート > *現在*を選択します。
2. アラートの表で、必要に応じて「 * Low metadata storage * 」アラートグループを展開し、表示する特定のアラートを選択します。
3. アラートダイアログボックスで詳細を確認します。
4. Major または Critical の * Low metadata storage * アラートがトリガーされた場合は、すぐに拡張を実行してストレージノードを追加します。

StorageGRID は各サイトですべてのオブジェクトメタデータの完全なコピーを保持するため、グリッド全体のメタデータ容量は最も小規模なサイトのメタデータ容量によって制限されます。1つのサイトにメタデータ容量を追加する必要がある場合は、同じ数のストレージノードも必要です"他のサイトを展開します"。

拡張の実行後、 StorageGRID によって既存のオブジェクトメタデータが新しいノードに再配分され、グリッドの全体的なメタデータ容量が増加します。ユーザによる操作は必要ありません。Low metadata storage * アラートがクリアされます。

StorageGRID の証明書エラーのトラブルシューティング

Webブラウザ、S3クライアント、または外部の監視ツールを使用してStorageGRIDに接続しようとしたときにセキュリティまたは証明書の問題が発生した場合は、証明書を確認する必要があります。

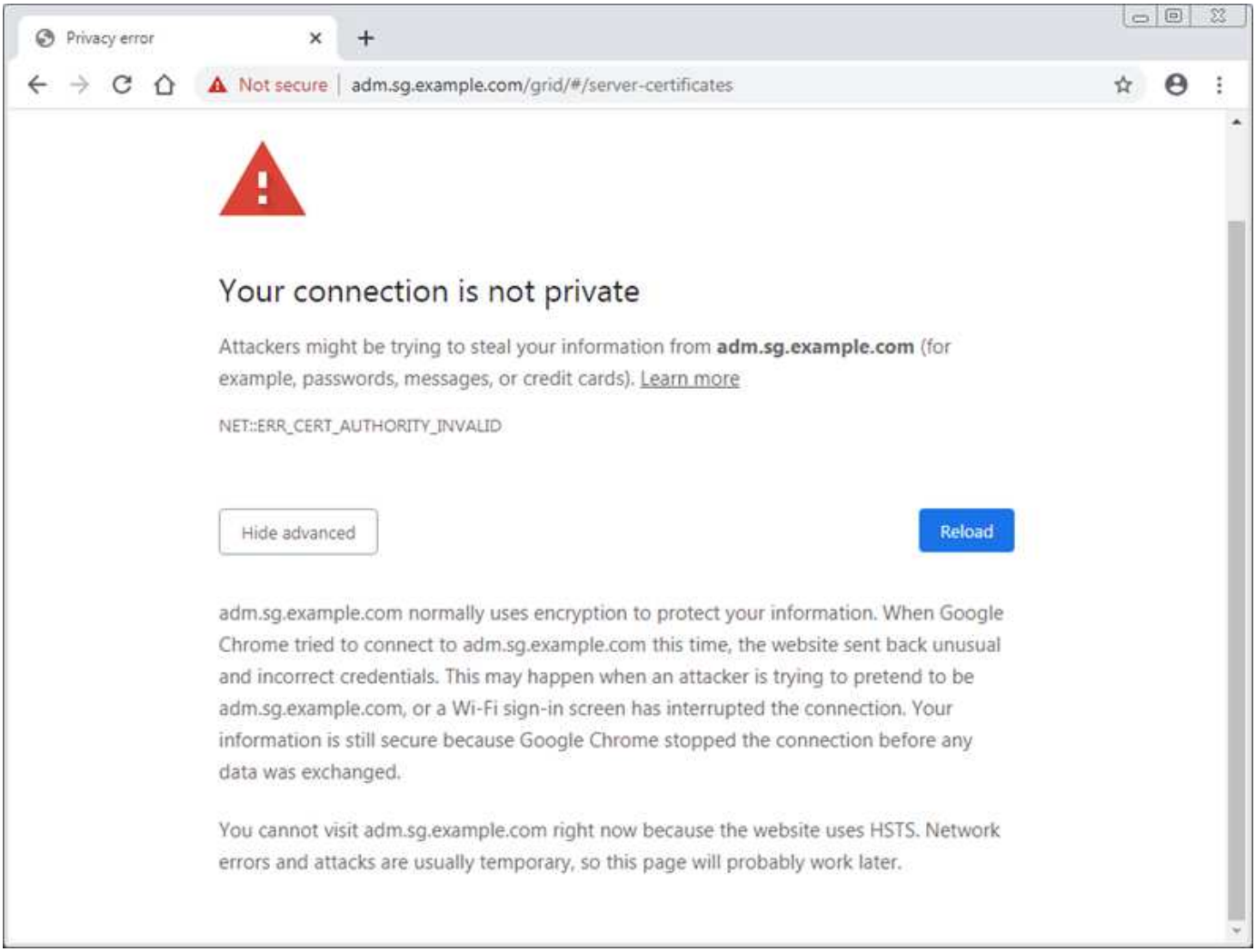
タスクの内容

証明書エラーは、グリッドマネージャ、グリッド管理 API 、テナントマネージャ、またはテナント管理 API を使用して StorageGRID に接続しようとしたときに、原因 で発生する可能性があります。証明書エラーは、S3クライアントまたは外部の監視ツールに接続しようとしたときにも発生することがあります。

IP アドレスではなくドメイン名を使用して Grid Manager または Tenant Manager にアクセスする場合は、次のいずれかの場合に証明書のエラーが表示され、バイパスするオプションはありません。

- カスタム管理インターフェイス証明書の有効期限が切れます。
- カスタムの管理インターフェイス証明書をデフォルトのサーバ証明書に戻した場合。

次の例は、カスタム管理インターフェイス証明書の有効期限が切れたときの証明書エラーを示しています。



サーバ証明書の問題によって処理が中断されないようにするために、サーバ証明書の有効期限が近づくと* Expiration of server certificate for Management Interface *アラートがトリガーされます。

外部 Prometheus 統合にクライアント証明書を使用している場合、証明書のエラーは、 StorageGRID 管理インターフェイス証明書またはクライアント証明書が原因で発生することがあります。クライアント証明書の有効期限が近づくと、 ［ 証明書 ］ ページ * アラートで設定されたクライアント証明書の有効期限がトリガーされます。

手順

期限切れの証明書に関するアラート通知を受け取った場合は、証明書の詳細にアクセスします。 構成 > セキュリティ > *証明書*を選択し、"適切な証明書タブを選択します" 。

1. 証明書の有効期間を確認します。+一部のWebブラウザおよびS3クライアントでは、有効期間が398日を超える証明書が受け入れられません。
2. 証明書の有効期限が切れているか、まもなく期限切れになる場合は、新しい証明書をアップロードまたは生成します。
   - サーバ証明書については、の手順を参照してください"Grid Manager および Tenant Manager 用のカスタムサーバ証明書を設定する"。
   - クライアント証明書については、の手順を参照してください"クライアント証明書を設定しています

"。

3. サーバ証明書エラーの場合は、次のいずれかまたは両方を実行してください。
   - 証明書の Subject Alternative Name （ SAN ）が設定されていること、および SAN が接続先のノードの IP アドレスまたはホスト名と一致していることを確認してください。
   - ドメイン名を使用して StorageGRID に接続しようとしている場合は、次の手順を実行します。
     i. 接続エラーをバイパスして Grid Manager にアクセスするために、ドメイン名ではなく管理ノードの IP アドレスを入力します。
     ii. グリッドマネージャから*構成* > セキュリティ > *証明書*を選択し、"適切な証明書タブを選択します"新しいカスタム証明書をインストールするか、デフォルトの証明書を続行します。
     iii. StorageGRIDの管理手順で、の手順を参照してください"Grid Manager および Tenant Manager 用のカスタムサーバ証明書を設定する"。

StorageGRIDの管理ノードとユーザーインターフェースの問題のトラブルシューティング

管理ノードとStorageGRIDユーザインターフェイスに関する問題の原因を特定するのに役立ついくつかのタスクを実行できます。

管理ノードのサインインエラー

StorageGRID管理ノードへのサインイン時にエラーが発生した場合は、またはの "ハードウェア"問題、"管理ノードサービス"または"問題 とCassandraデータベース"が接続されているストレージノードで問題が発生している可能性があります"ネットワーク"。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはファイルを持ってい `Passwords.txt`ます。
- そうだな "特定のアクセス権限"

タスクの内容

管理ノードにサインインしようとしたときに次のいずれかのエラーメッセージが表示された場合は、以下のトラブルシューティングのガイドラインに従ってください。

- `Your credentials for this account were invalid. Please try again.`
- `Waiting for services to start…`
- `Internal server error. The server encountered an error and could not complete your request. Please try again. If the problem persists, contact Technical Support.`
- `Unable to communicate with server. Reloading page…`

手順

1. 10 分待ってから、もう一度サインインしてください。

   エラーが自動的に解決されない場合は、次の手順に進みます。

2. StorageGRIDシステムに複数の管理ノードがある場合は、別の管理ノードからGrid Managerにサインインして、使用できない管理ノードのステータスを確認します。
   - サインインできる場合は、ダッシュボード、ノード、アラート、および*サポート*オプションを使用して、エラーの原因を特定できます。
   - 管理ノードが1つしかない場合やサインインできない場合は、次の手順に進みます。
3. ノードのハードウェアがオフラインかどうかを確認します。
4. StorageGRID システムでシングル サインオン（SSO）が有効になっている場合は、"OIDC"または"SAML"を使用した SSO の設定を参照してください。

   問題を解決するには、 1 つの管理ノードの SSO を一時的に無効にしてから再度有効にする必要があります。

5. 使用しているアカウントがフェデレーテッドユーザに属しているかどうかを確認します。

   フェデレーテッドユーザアカウントが機能していない場合は、 root などのローカルユーザとして Grid Manager にサインインしてみてください。

   - ローカルユーザがサインインできる場合は、次の手順を実行します。
     i. アラートを確認します。
     ii. 構成 > アクセス制御 > *ID連携*を選択します。
     iii. 「接続テスト」を選択して、LDAPサーバの接続設定を検証します。
     iv. テストに失敗した場合は、設定エラーを解決します。
   - ローカルユーザがサインインできず、クレデンシャルが正しいことが確実な場合は、次の手順に進みます。
6. セキュア シェル (SSH) を使用して管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@Admin_Node_IP`
   b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

      rootとしてログインすると、プロンプトがからに `#`変わります `$`。

7. グリッドノード上で実行されているすべてのサービスのステータスを表示します。 `storagegrid-status`

   NMS 、 mi 、 nginx 、 mgmt の各 API サービスがすべて実行されていることを確認します。

   出力は、サービスのステータスが変わるとすぐに更新されます。

```
$ storagegrid-status
Host Name                      99-211
IP Address                     10.96.99.211
Operating System Kernel        4.19.0          Verified
Operating System Environment   Debian 10.1     Verified
StorageGRID Webscale Release   11.4.0          Verified
Networking                                     Verified
Storage Subsystem                              Verified
Database Engine                5.5.9999+default Running
Network Monitoring             11.4.0          Running
Time Synchronization           1:4.2.8p10+dfsg Running
ams                            11.4.0          Running
cmn                            11.4.0          Running
nms                            11.4.0          Running
ssm                            11.4.0          Running
mi                             11.4.0          Running
dynip                          11.4.0          Running
nginx                          1.10.3          Running
tomcat                         9.0.27          Running
grafana                        6.4.3           Running
mgmt api                       11.4.0          Running
prometheus                     11.4.0          Running
persistence                    11.4.0          Running
ade exporter                   11.4.0          Running
alertmanager                   11.4.0          Running
attrDownPurge                  11.4.0          Running
attrDownSamp1                  11.4.0          Running
attrDownSamp2                  11.4.0          Running
node exporter                  0.17.0+ds       Running
sg snmp agent                  11.4.0          Running
```

8. nginx-gwサービスが実行されていることを確認します。 `# service nginx-gw status`
9. Lumberjackを使用してログを収集します。 `# /usr/local/sbin/lumberjack.rb`

   過去に認証に失敗したことがある場合は、 --start および --end Lumberjack スクリプトオプションを使用して適切な期間を指定します。これらのオプションの詳細については、 lumberjack -h を使用してください。

   ログアーカイブがコピーされた場所がターミナル画面に出力されます。

10. [[review_logs,start=10] 次のログを確認します。
    - `/var/local/log/bycast.log`
    - `/var/local/log/bycast-err.log`
    - `/var/local/log/nms.log`

◦ **/*commands.txt

11. 管理ノードで問題を特定できなかった場合は、次のいずれかのコマンドを問題 で実行し、サイトで ADC サービスを実行する 3 つのストレージノードの IP アドレスを確認します。通常はサイトにインストールされた最初の 3 つのストレージノードです。

```
# cat /etc/hosts
```

```
# gpt-list-services adc
```

管理ノードは認証プロセスで ADC サービスを使用します。

12. 管理ノードから、sshを使用して特定したIPアドレスを使用して各ADCストレージノードにログインします。
13. グリッドノード上で実行されているすべてのサービスのステータスを表示します。 `storagegrid-status`

idnt 、 acct 、 nginx 、および Cassandra のサービスがすべて実行されていることを確認します。

14. 手順とログを確認しますを繰り返しLumberjack を使用してログを収集しますて、ストレージノードのログを確認します。
15. 問題を解決できない場合は、テクニカルサポートにお問い合わせください。

収集したログをテクニカルサポートに送信します。も参照してください"ログファイル参照"。

ユーザインターフェイスに関する問題

StorageGRID ソフトウェアのアップグレード後に、Grid ManagerまたはTenant Managerのユーザインターフェイスが想定どおりに応答しないことがあります。

手順

1. を使用していることを確認し"サポートされている Web ブラウザ"ます。
2. Web ブラウザのキャッシュをクリアします。

キャッシュをクリアすると、以前のバージョンの StorageGRID ソフトウェアで使用されていた古いリソースが削除され、ユーザインターフェイスが再び正しく動作するようになります。手順については、 Web ブラウザのドキュメントを参照してください。

StorageGRID のネットワーク、ハードウェア、プラットフォームの問題のトラブルシューティング

ここでは、 StorageGRID ネットワーク、ハードウェア、およびプラットフォームの問題に関連する問題の原因を特定するのに役立ついくつかのタスクを紹介します。

[[422-unprocessable-entity-errors]]
== "422: Unprocessable Entity"エラー

エラー422: Unprocessable Entityは、さまざまな理由で発生する可能性があります。エラーメッセージを調べて、問題 の原因を特定します。

表示されたいずれかのエラーメッセージが表示された場合は、推奨される対処方法を実行してください。

エラーメッセージ	ルート原因 および対処方法

`422: Unprocessable Entity`
 	
`Validation failed. Please check`
`the values you entered for errors. Test connection failed.`
`Please verify your configuration. Unable to authenticate, please verify your username and password: LDAP Result Code 8 "Strong Auth Required": 00002028: LdapErr: DSID-0C090256, comment: The server requires`
`binds to turn on integrity checking if SSL\TLS are not already active on the connection, data 0, v3839`
	このメッセージは、 Windows Active Directory （ AD ）を使用してアイデンティティフェデレーションを設定するときに、 Transport Layer Security （ TLS ）で「 TLS を使用しない」オプションを選択した場合に表示されることがあります。
	
	LDAP 署名を強制する AD サーバでは、「 TLS を使用しない」オプションの使用はサポートされていません。STARTTLS を使用する * オプションまたは TLS に LDAPS * を使用するオプションのいずれかを選択する必要があります。

`422: Unprocessable Entity`
 	
`Validation failed. Please check`
`the values you entered for errors. Test connection failed.`
`Please verify your configuration.Unable to begin TLS, verify your certificate and TLS configuration: LDAP Result Code 200 "Network Error": TLS handshake failed (EOF)`
	このメッセージは、サポートされない暗号を使用して、 StorageGRID からフェデレーションまたはクラウドストレージプールの識別に使用する外部システムへの Transport Layer Security （ TLS ）接続を試みた場合に表示されます。
	
	外部システムで提供されている暗号を確認します。StorageGRIDの管理手順に従って、発信TLS接続にはのいずれかを使用する必要があります"StorageGRID でサポートされている暗号"。

グリッドネットワーク**MTU mismatch**アラート

グリッドネットワークインターフェイス（ eth0 ）の最大伝送ユニット（ MTU ）設定がグリッド内のノード間で大きく異なる場合に、 * Grid Network MTU mismatch * アラートがトリガーされます。

タスクの内容

MTU 設定の違いから、 eth0 ネットワークの一部がジャンボフレーム用に設定されているが、すべてではないことがわかります。MTU サイズが 1000 を超えると、原因 のネットワークパフォーマンスの問題が発生する可能性があります。

手順

1. デフォルトでは外部 SSH アクセスはブロックされます。必要に応じて、"一時的にアクセスを許可する" 。
2. すべてのノードの eth0 についての MTU 設定を表示します。
   - Grid Manager に用意されているクエリを使用する。
   - に移動し *primary Admin Node IP address*`/metrics/graph`て次のクエリを入力します。 `node_network_mtu_bytes{device="eth0"}`
3. "MTUの設定を変更します。"必要に応じて、すべてのノードのグリッドネットワークインターフェイス（eth0）で同じにする必要があります。
   - LinuxベースおよびVMwareベースのノードの場合は、次のコマンドを使用します。 `/usr/sbin/change-ip.py [-h] [-n node] mtu network [network...]`

     例： `change-ip.py -n node 1500 grid admin`

     注：Linuxベースのノードでは、コンテナ内のネットワークに必要なMTU値がホストインターフェイスにすでに設定されている値を超える場合は、まずホストインターフェイスのMTU値を適切なMTU値に設定してから、スクリプトを使用してコンテナ内のネットワークのMTU値を変更する必要があります `change-ip.py`。

     Linux または VMware ベースのノードで MTU を変更するには、次の引数を使用します。

位置指定引数	製品説明
`mtu`	設定する MTU 。1280 ～ 9216 の範囲内にある必要があります。
`network`	MTU を適用するネットワーク。次のネットワークタイプを 1 つ以上指定します。 • グリッド（ Grid ） • 管理者 • クライアント

+

オプションの引数	製品説明
`-h, - help`	ヘルプメッセージを表示して終了します。
`-n node, --node node`	ノード。デフォルトはローカルノードです。

4. 外部SSHアクセスを許可している場合は、"アクセスをブロックする"タスクが完了したら。

Node network reception frame errorアラート

*ノードネットワーク受信フレームエラー*アラートは、StorageGRIDとネットワークハードウェア間の接続の問題が原因で発生する場合があります。このアラートは、原因となっている問題に対処すると自動的にクリアされます。

タスクの内容

*ノードネットワーク受信フレームエラー*アラートは、StorageGRIDに接続するネットワークハードウェアの次の問題が原因で発生する可能性があります。

- Forward Error Correction （ FEC; 前方誤り訂正）が必要で、使用されていません
- スイッチポートと NIC の MTU が一致しません
- リンクエラー率が高くなっています
- NIC リングバッファオーバーラン

手順

1. ネットワーク構成に応じて、このアラートのすべての潜在的な原因についてトラブルシューティング手順を実行します。
2. エラーの原因 に応じて、次の手順を実行します。

FECが一致しません

これらの手順は、StorageGRIDアプライアンスでFECの不一致が原因の*ノードネットワーク受信フレームエラー*アラートにのみ該当します。

a. StorageGRID アプライアンスに接続されているスイッチのポートの FEC ステータスを確認します。

b. アプライアンスからスイッチへのケーブルの物理的な整合性をチェックしてください。

c. アラートを解決するためにFEC設定を変更する場合は、まずStorageGRIDアプライアンスインストーラの[Link Configuration]ページで、アプライアンスが* Auto *モードに設定されていることを確認します（使用しているアプライアンスの手順を参照してください。

   - "SG6160"
   - "SGF6112"
   - "SG6000"
   - "SG5800"
   - "SG5700"
   - "SG110およびSG1100"
   - "SG100およびSG1000"

d. スイッチポートのFEC設定を変更します。StorageGRID アプライアンスのポートは、可能であれば、 FEC 設定を調整して一致させます。

   StorageGRID アプライアンスではFECを設定できません。アプライアンスは、接続先のスイッチポートで FEC 設定を検出し、ミラーリングしようとします。リンクが 25GbE または 100GbE のネットワーク速度に強制的に設定されている場合、スイッチと NIC が共通の FEC 設定をネゴシエートできない可能性があります。共通のFEC設定がない場合、ネットワークは「no-FEC」モードに戻ります。FECが有効になっていない場合、接続は電気的ノイズによるエラーの影響を受けやすくなります。

   StorageGRID アプライアンスは、NO FECに加えて、Firecode（FC）FECとReed Solomon（RS）FECをサポートしています。

スイッチポートと **NIC** の **MTU** が一致しません

スイッチポートとNICのMTUの不一致がアラートの原因である場合は、ノードに設定されているMTUサイズがスイッチポートのMTU設定と同じであることを確認します。

ノードに設定されている MTU サイズは、そのノードが接続されているスイッチポートの設定よりも小さい場合があります。この構成で可能なStorageGRIDノードのMTUよりも大きいイーサネットフレームを受信すると、* Node network reception frame error *アラートが報告されることがあります。このような状況が発生していると思われる場合は、スイッチポートの MTU を StorageGRID ネットワークインターフェイスの MTU に一致するように変更するか、 StorageGRID ネットワークインターフェイスの MTU をスイッチポートに合わせて変更します。 MTU の目的または要件に応じて変更します。

ネットワークのパフォーマンスを最大限に高めるには、すべてのノードのグリッドネットワークインターフェイスで MTU 値がほぼ同じになるように設定する必要があります。個々のノードのグリッドネットワークの MTU 設定に大きな違いがある場合は、 * Grid Network MTU mismatch * アラートがトリガーされます。MTU値はすべてのネットワークタイプで同じである必要はありません。詳細については、を参照してください Grid Network MTU mismatch アラートのトラブルシューティングを行います 。

も参照してください "MTU 設定を変更します"。

リンクエラー率が高くなっています

a. まだイネーブルになっていない場合は、 FEC をイネーブル
b. ネットワークケーブルの品質が良好で、損傷や不適切な接続がないことを確認します。
c. ケーブルに問題がない場合は、テクニカルサポートにお問い合わせください。

電気的ノイズが大きい環境では、エラー率が高くなることがあります。

NIC リングバッファオーバーラン

エラーが NIC リングのバッファオーバーランである場合は、テクニカルサポートに連絡してください。

StorageGRID システムが過負荷になっていて、ネットワークイベントをタイムリーに処理できない場合、リングバッファがオーバーランする可能性があります。

3. 問題を監視し、アラートが解決しない場合はテクニカルサポートにお問い合わせください。

時刻同期エラー

グリッドで時刻の同期に関する問題が発生する可能性があります。

時刻の同期の問題が発生する場合は、少なくとも 4 つの外部 NTP ソースが指定されており、それぞれ Stratum 3 以上であることを確認します。それらのすべての外部 NTP ソースが正常に動作しており、StorageGRID のノードからアクセスできることを確認する必要があります。

本番レベルのStorageGRIDインストールの場合"外部NTPソースの指定"は、Windows Server 2016より前のバージョンのWindowsでWindows Time (W32Time)サービスを使用しないでください。以前のバージョンの Windows のタイムサービスは精度が十分でないため、StorageGRID などの高精度環境での使用は Microsoft でサポートされていません。

Linux ：ネットワーク接続の問題

Linuxホストでホストされ ているStorageGRIDノードのネットワーク接続に問題が発生する可能性があります。

MAC アドレスのクローニング

場合によっては、MAC アドレスの複製を使用することでネットワークの問題を解決できます。仮想ホストを使用している場合は、ノード構成ファイルで各ネットワークの MAC アドレス複製キーの値を「true」に設定

します。この設定により、 StorageGRIDコンテナの MAC アドレスはホストの MAC アドレスを使用するようになります。指示を参照してください"ノード構成ファイルを作成する"。

> Linuxホスト OS で使用する仮想ネットワークインターフェースを個別に作成してください。Linux ホスト OS と StorageGRID コンテナに同じネットワークインターフェースを使用すると、ホスト OS にアクセスできなくなる可能性があります。

詳細については、"MACクローニングを有効にする" 。

Linux：ノードのステータスが「**orphaned**」になっている

orphaned 状態の Linux ノードは、通常、 StorageGRID サービスまたはノードのコンテナを制御している StorageGRID ノードデーモンが予期せず停止したことを示しています。

タスクの内容

Linux ノードが orphaned 状態になった場合は、次のように対応策を実行してください。

- ログでエラーとメッセージを確認します。
- ノードを再起動してみます。
- 必要に応じて、コンテナエンジンのコマンドを使用して既存のノードコンテナを停止します。
- ノードを再起動します。

手順

1. サービスデーモンと orphaned 状態のノードの両方のログを調べ、明らかなエラーや予期しない終了に関するメッセージがないか確認します。
2. ホストに root としてログインするか、 sudo 権限を持つアカウントを使ってログインします。
3. 次のコマンドを実行して、ノードの再起動を試行します。 `$ sudo storagegrid node start node-name`

   ```
   $ sudo storagegrid node start DC1-S1-172-16-1-172
   ```

   ノードが孤立している場合、応答はになります

   ```
   Not starting ORPHANED node DC1-S1-172-16-1-172
   ```

4. Linux から、コンテナエンジンおよび StorageGRID ノードを制御しているすべてのプロセスを停止します。例：`sudo docker stop --time secondscontainer-name`

   に `seconds`、コンテナの停止を待機する秒数を入力します（通常は15分以内）。例：

   ```
   sudo docker stop --time 900 storagegrid-DC1-S1-172-16-1-172
   ```

5. ノードを再起動します。 `storagegrid node start node-name`

```
storagegrid node start DC1-S1-172-16-1-172
```

Linux ： IPv6 サポートのトラブルシューティングを行います

Linux ホストに StorageGRID ノードをインストールしていて、 IPv6 アドレスが想定どおりにノードコンテナに割り当てられていない場合は、カーネルでの IPv6 サポートの有効化が必要となることがあります。

タスクの内容

グリッドノードに割り当てられているIPv6アドレスを表示するには、次の手順を実行します。

1. *ノード*を選択し、ノードを選択します。
2. [概要]タブの*の横にある[追加のIPアドレスを表示]*を選択します。

IPv6 アドレスが表示されず、ノードが Linux ホストにインストールされている場合は、次の手順に従ってカーネルで IPv6 サポートを有効にします。

手順

1. ホストに root としてログインするか、 sudo 権限を持つアカウントを使ってログインします。
2. 次のコマンドを実行します。 `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@SG:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

結果は0になるはずです。

```
net.ipv6.conf.all.disable_ipv6 = 0
```

結果が0でない場合は、オペレーティングシステムのマニュアルで設定の変更方法を参照してください `sysctl`。次に進む前に、値を 0 に変更します。

3. StorageGRIDノードコンテナを入力します。 `storagegrid node enter node-name`
4. 次のコマンドを実行します。 `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@DC1-S1:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

結果は1になるはずです。

```
net.ipv6.conf.all.disable_ipv6 = 1
```

結果が 1 でない場合、この手順 は適用されません。テクニカルサポートにお問い合わせください。

5. コンテナを終了します。 `exit`

```
root@DC1-S1:~ # exit
```

6. rootとして、次のファイルを編集します。 `/var/lib/storagegrid/settings/sysctl.d/net.conf`

```
sudo vi /var/lib/storagegrid/settings/sysctl.d/net.conf
```

7. 次の 2 行を探して、コメントタグを削除します。次に、ファイルを保存して閉じます。

```
net.ipv6.conf.all.disable_ipv6 = 0
```

```
net.ipv6.conf.default.disable_ipv6 = 0
```

8. 次のコマンドを実行して、 StorageGRID コンテナを再起動します。

```
storagegrid node stop node-name
```

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

StorageGRID の外部 syslog サーバーエラーメッセージのトラブルシューティング

次の表に、を使用した外部syslogサーバに関するエラーメッセージと対処方法を示します。

外部 Syslog サーバーが正しく構成されていることを確認するためのテスト メッセージの送信で問題が発生した場合、外部 Syslog サーバーの構成ウィザードによってこれらのエラーが表示されます。

実行時に問題が発生する場合は、"外部 syslog サーバの転送エラーです"警告。このアラートを受け取った場合は、アラートの指示に従ってテスト メッセージを再送信し、詳細なエラー メッセージを取得してください。

外部syslogサーバへの監査情報の送信の詳細については、次の項を参照してください。

- "外部syslogサーバを使用する場合の考慮事項"
- "ログ管理と外部Syslogサーバーを構成する"

エラーメッセージ	概要 および推奨される対処方法
ホスト名を解決できません	syslog サーバに対して入力した FQDN を IP アドレスに解決できませんでした。 1. 入力したホスト名を確認します。IPアドレスを入力した場合は、W.X.Y.Z（ドット付き10進数）表記の有効なIPアドレスであることを確認してください。 2. DNS サーバが正しく設定されていることを確認します。 3. 各ノードから DNS サーバの IP アドレスにアクセスできることを確認します。
接続が拒否されました	syslog サーバへの TCP または TLS 接続が拒否されました。ホストの TCP ポートまたは TLS ポートをリスンしているサービスがないか、ファイアウォールがアクセスをブロックしている可能性があります。 1. 入力した syslog サーバの FQDN または IP アドレス、ポート、およびプロトコルが正しいことを確認してください。 2. syslog サービスのホストが、指定したポートをリスンしている syslog デーモンを実行していることを確認します。 3. ファイアウォールがノードから syslog サーバの IP およびポートへの TCP / TLS 接続へのアクセスをブロックしていないことを確認します。
ネットワークに到達できません	syslog サーバは直接接続されたサブネット上にはありません。ルータが、リストされたノードから syslog サーバにテストメッセージを転送できなかったことを示す ICMP 障害メッセージを返しました。 1. syslog サーバの正しい FQDN または IP アドレスが入力されていることを確認してください。 2. 表示された各ノードについて、グリッドネットワークサブネットリスト、管理ネットワークサブネットリスト、およびクライアントネットワークゲートウェイを確認します。想定されるネットワークインターフェイスとゲートウェイ（グリッド、管理、またはクライアント）を介してトラフィックが syslog サーバにルーティングされるように設定されていることを確認します。
ホストに到達できません	syslog サーバは直接接続されたサブネット上にあります（表示されたノードのグリッド IP 、管理 IP 、またはクライアント IP アドレスに使用されるサブネット）。ノードはテストメッセージを送信しようとしましたが、 syslog サーバの MAC アドレスに対する ARP 要求への応答を受信しませんでした。 1. syslog サーバの正しい FQDN または IP アドレスが入力されていることを確認してください。 2. syslog サービスを実行しているホストが稼働していることを確認します。

エラーメッセージ	概要 および推奨される対処方法
接続がタイムアウトしました	TCP / TLS 接続が試行されましたが、 syslog サーバからの応答が長時間受信されませんでした。ルーティングが正しく設定されていないか、ファイアウォールが応答を送信せずにトラフィックをドロップしている可能性があります（一般的な設定）。 1. syslog サーバの正しい FQDN または IP アドレスが入力されていることを確認してください。 2. 表示された各ノードについて、グリッドネットワークサブネットリスト、管理ネットワークサブネットリスト、およびクライアントネットワークゲートウェイを確認します。syslogサーバに到達する予定のネットワークインターフェイスおよびゲートウェイ（グリッド、管理、またはクライアント）を使用して、トラフィックがsyslogサーバにルーティングされるように設定されていることを確認します。 3. ファイアウォールによって syslog サーバの IP とポートにリストされているノードからの TCP / TLS 接続へのアクセスがブロックされていないことを確認します。
パートナーによる接続が切断されました	syslog サーバへの TCP 接続は正常に確立されましたが、その後閉じられました。これには次のような理由があります。 • syslog サーバが再起動またはリブートされた可能性があります。 • ノードと syslog サーバで TCP / TLS 設定が異なる場合があります。 • 中間ファイアウォールがアイドル状態の TCP 接続を閉じている可能性があります。 • syslog サーバのポートをリスンしている非 syslog サーバが接続を閉じた可能性があります。 この問題を解決するには： 1. 入力した syslog サーバの FQDN または IP アドレス、ポート、およびプロトコルが正しいことを確認してください。 2. TLS を使用している場合は、 syslog サーバも TLS を使用していることを確認します。TCP を使用している場合は、 syslog サーバも TCP を使用していることを確認します。 3. アイドル状態の TCP 接続を閉じるように中間ファイアウォールが設定されていないことを確認します。
TLS 証明書エラーです	syslog サーバから受信したサーバ証明書が、指定した CA 証明書バンドルおよびクライアント証明書と互換性がありませんでした。 1. CA 証明書バンドルおよびクライアント証明書（存在する場合）が syslog サーバ上のサーバ証明書と互換性があることを確認します。 2. syslog サーバのサーバ証明書に想定される IP 値または FQDN 値が含まれていることを確認します。

エラーメッセージ	概要 および推奨される対処方法
転送が中断されました	syslog レコードが syslog サーバに転送されなくなり、 StorageGRID が原因を検出できなくなりました。 このエラーが表示されたデバッグログを確認して、ルート原因 を特定します。
TLS セッションが終了しました	syslog サーバが TLS セッションを終了し、 StorageGRID が原因を検出できません。 1. このエラーが表示されたデバッグログを確認して、ルート原因 を特定します。 2. 入力した syslog サーバの FQDN または IP アドレス、ポート、およびプロトコルが正しいことを確認してください。 3. TLS を使用している場合は、 syslog サーバも TLS を使用していることを確認します。TCP を使用している場合は、 syslog サーバも TCP を使用していることを確認します。 4. CA 証明書バンドルおよびクライアント証明書（存在する場合）が syslog サーバのサーバ証明書と互換性があることを確認します。 5. syslog サーバのサーバ証明書に想定される IP 値または FQDN 値が含まれていることを確認します。
結果の照会に失敗しました	syslog サーバの設定およびテストに使用されている管理ノードが、表示されているノードにテスト結果を要求できません。1 つ以上のノードが停止している可能性があります。 1. 標準的なトラブルシューティング手順に従って、ノードがオンラインで、必要なすべてのサービスが実行されていることを確認します。 2. 表示されたノードで miscd サービスを再起動します。

StorageGRIDにおけるロードバランサのキャッシュの問題について学ぶ

ロードバランサーのキャッシュで発生する可能性のある問題とそのトラブルシューティング方法について説明します。

リクエストがキャッシュヒットであったかどうかを判断する

- X-Cache ヘッダーは、キャッシュ サービスによって処理される要求への応答に設定されます。可能なコード:
  - `HIT`: オブジェクトはキャッシュから提供されました
  - `PARTIAL-HIT`: バケット/キーのレコードはキャッシュ内にありましたが、要求された範囲のすべてをキャッシュから提供することはできませんでした
  - `STALE`: バケット/キーにはキャッシュ内にレコードがありましたが、オブジェクトは最後にキャッシュから提供されてから更新されました。
  - `MISS`: オブジェクトはキャッシュ内にありませんでした

- その `nginx-gw/endpoint-access.log.gz`リクエストのレコードには、キャッシュによって処理されるリクエストの「unix:/run/cache-svc/cache-svc.sock」が含まれます。
- その `cache-svc/cache-svc.log`「リクエスト 320390: 正常に完了しました (キャッシュ ヒット)」または「リクエスト 320375: 正常に完了しました (キャッシュ ミス)」などのメッセージを報告します。同じ「Request <*number*>」文字列を持つ他のレコードを検索して、要求されたパスを見つけます。

キャッシュヒット率が低い

- 新しいワークロードが追加されたり、ワークロードによってアクセスされるワーキング セットが変更されたりすると、キャッシュ ヒット率が低下することが予想されます。このような状況では、時間の経過とともにヒット率が増加すると予想されます。
- 複数のワークロードがキャッシュを使用している場合は、トラフィック分類ポリシーを追加して、キャッシュによって処理されるワークロードの一部を分離することを検討してください。キャッシュヒット率メトリックは、トラフィック分類ポリシーごとに利用できます。一部のワークロードでキャッシュ ヒット率が低下している場合は、そのワークロードをキャッシュが有効になっていない他のエンドポイントに移動することを検討してください。
- キャッシュ削除率を評価します。キャッシュが小さすぎてワーキング セットに収まらない場合は、高い削除率が発生し、ヒット率が低下する可能性があります。
- FPVR では、特定のワークロードのヒット率を向上させるオプションが利用できる場合があります。

パフォーマンスが低い

- キャッシュヒット率を評価します。キャッシュヒット率が低いと、全体的なパフォーマンスが低下する可能性があります。
- キャッシュ削除率を評価します。削除中、一部のストレージ リソースはディスクから既存のオブジェクトを削除するために使用されます。削除プロセスが新しいオブジェクトへのアクセスに対応できない場合、システムはハード ウォーターマークしきい値に達し、キャッシュのバイパスを開始する可能性があります。
- 「ネットワーク インターフェイスの受信使用量」および「ネットワーク インターフェイスの送信使用量」診断を使用して、ネットワーク制限を確認します。

監査ログを確認します

監査メッセージとログ

ここでは、 StorageGRID 監査メッセージおよび監査ログの構造と内容について説明します。この情報を使用して、システムアクティビティの監査証跡を判読し、分析できます。

ここに記載する手順は、システムのアクティビティおよび使用状況のレポート生成を担当する管理者を対象としています。このようなレポートの生成には、 StorageGRID システムの監査メッセージの分析が必要となります。

テキストログファイルを使用するには、管理ノード上に設定されている監査共有へのアクセスが必要です。

監査メッセージレベルの設定と外部Syslogサーバの使用については、以下を参照してください。"ログ管理と外部Syslogサーバーを構成する" 。

監査メッセージが**StorageGRID**システムを通じて保存用の**audit.log**ファイルにどのように移動するか

すべての StorageGRID サービスは通常のシステム運用中に監査メッセージを生成します。これらの監査メッセージがStorageGRIDシステムを経由してファイルにどのように移動するかを理解しておく必要があります `audit.log`。

監査メッセージと監査メッセージの保持に関する次のワークフローは、 StorageGRID が*管理ノード/ローカル ノード* または 管理ノードと外部 **Syslog** サーバー 用に設定されている場合にのみ適用されます。StorageGRIDが「ローカルノードのみ」（デフォルト）または「外部syslogサーバー」に設定されている場合、監査メッセージは各ノードにローカルに保存されます。 `/var/local/log/localaudit.log`ファイルであり、管理ノードまたはストレージ ノードでは処理できません。

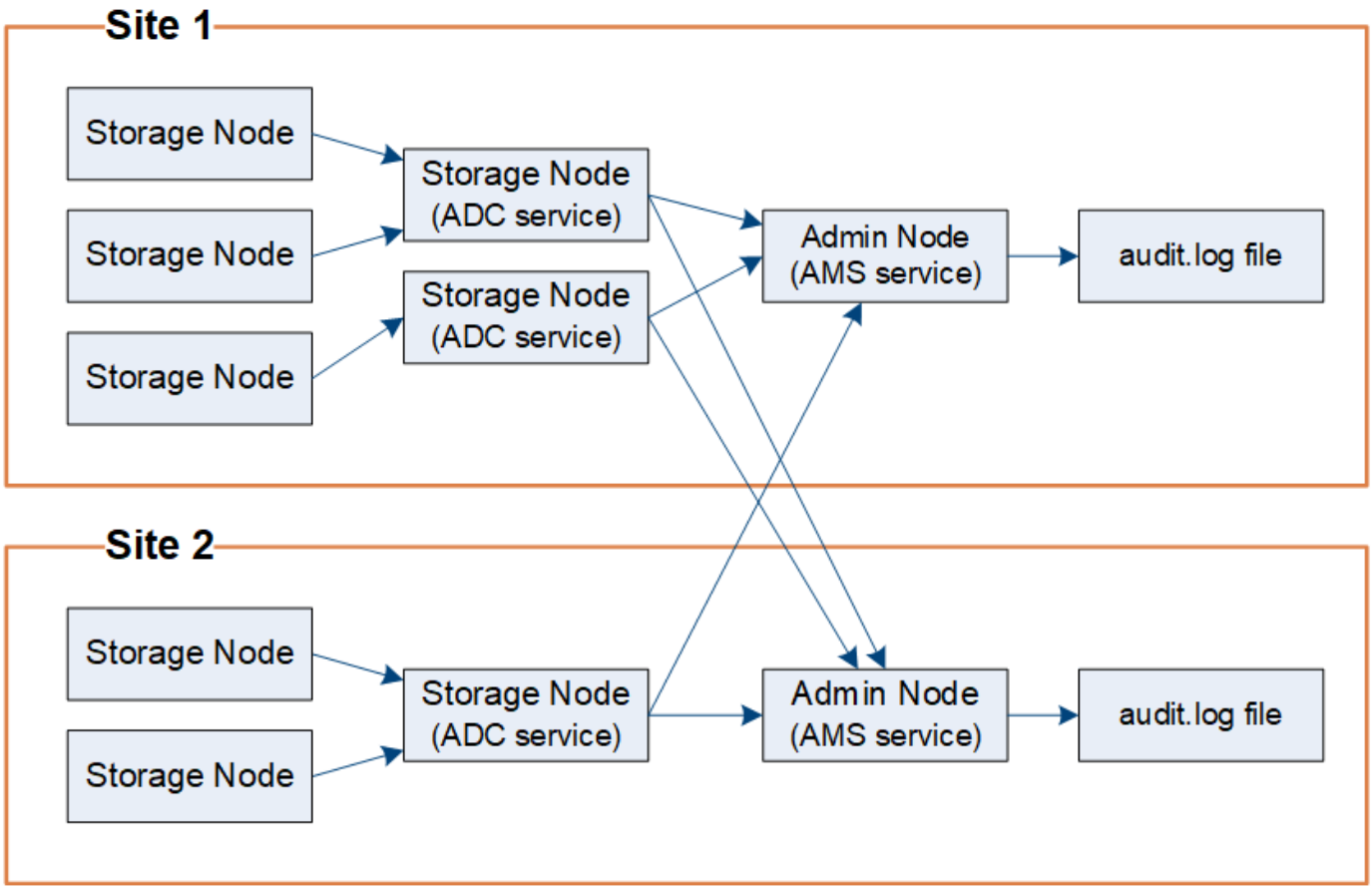
監査メッセージのフロー

監査メッセージは、 StorageGRID が*管理ノード/ローカル ノード* または 管理ノードと外部 **syslog** サーバー 用に構成されている場合、および管理ドメイン コントローラー (ADC) サービスを持つストレージ ノードによって処理されます。

監査メッセージのフロー図に示すように、各 StorageGRID ノードは監査メッセージをデータセンターサイトにあるいずれかの ADC サービスに送信します。ADC サービスは、各サイトに設置されている最初の 3 つのストレージノードで自動的に有効になります。

次に、各 ADC サービスはリレーとして機能し、監査メッセージの集合を StorageGRID システム内のすべての管理ノードに送信します。これにより、システムアクティビティの完全な記録が各管理ノードに提供されます。

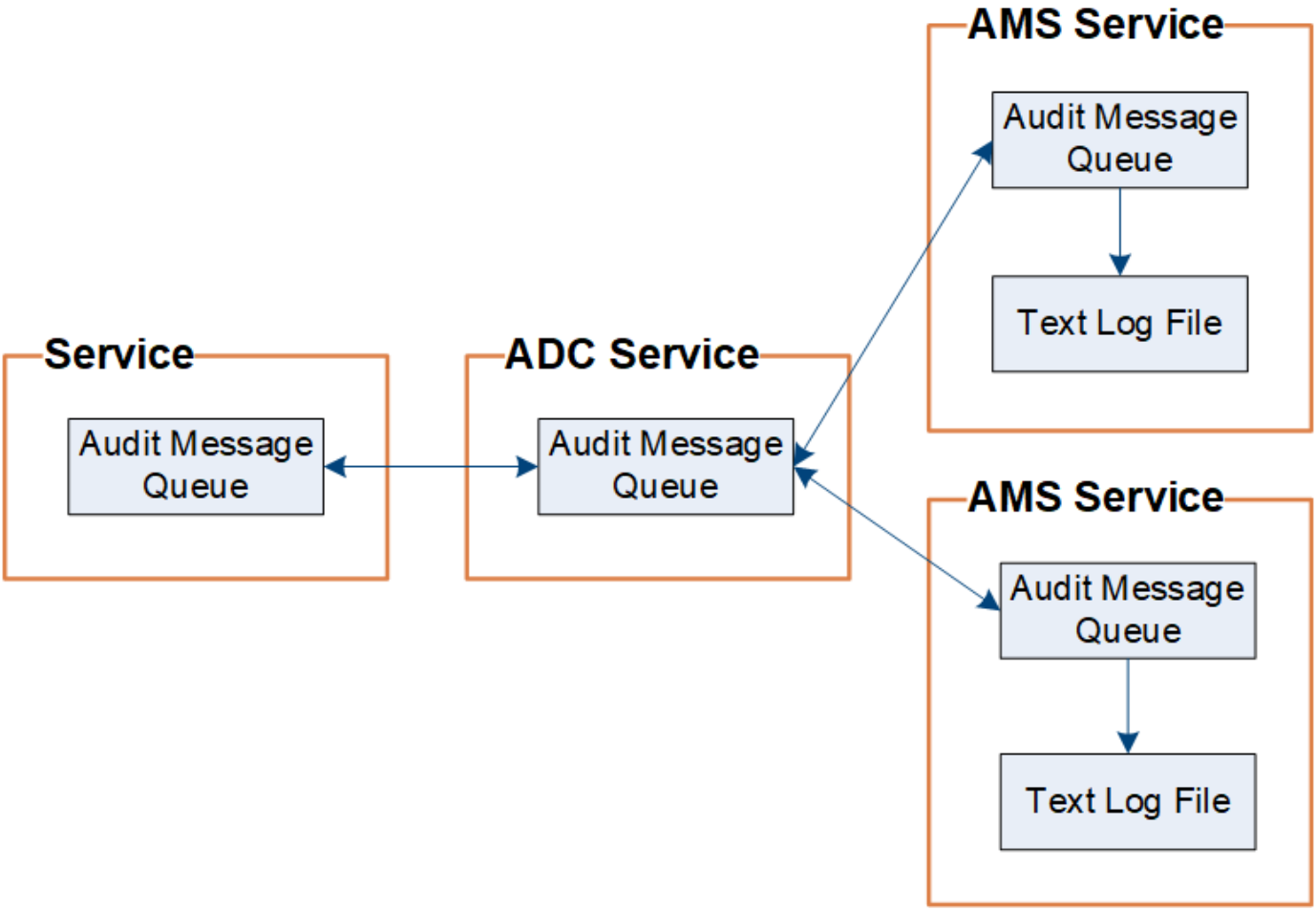
各管理ノードで監査メッセージがテキストログファイルに格納されます。アクティブなログファイルの名前はです `audit.log`。



監査メッセージの保持

StorageGRID では、コピー / 削除プロセスを使用して、監査ログに書き込まれる前に監査メッセージが失われないようにします。

ノードが監査メッセージを生成または中継すると、そのメッセージはグリッド ノードのシステム ディスク上の監査メッセージ キューに格納されます。メッセージのコピーは、管理ノードの監査ログファイルにメッセージが書き込まれるまで、常に監査メッセージキューに保持されます。 `/var/local/audit/export`ディレクトリ。これにより、転送中に監査メッセージが失われるのを防ぐことができます。



ネットワーク接続の問題や監査容量の不足により、監査メッセージ キューが一時的に増加する場合があります。キューが増加すると、各ノードの利用可能なスペースをより多く消費するようになります。 `/var/local/` ディレクトリ。問題が解決せず、ノードの監査メッセージ ディレクトリがいっぱいになると、個々のノードはバックログの処理を優先し、一時的に新しいメッセージを処理できなくなります。

具体的には、次のような動作が発生することがあります。

- もし `/var/local/audit/export`管理ノードが使用するディレクトリがいっぱいになると、ディレクトリがいっぱいでなくなるまで、管理ノードは新しい監査メッセージに使用できないというフラグが付けられます。 S3 クライアント要求は影響を受けません。監査リポジトリに到達できない場合、XAMS (到達不能監査リポジトリ) アラームがトリガーされます。
- もし `/var/local/`ADC サービスを使用するストレージ ノードによって使用されるディレクトリが 92% いっぱいになると、ディレクトリが 87% いっぱいになるまで、ノードは監査メッセージに使用できないというフラグが付けられます。他のノードへの S3 クライアント要求は影響を受けません。監査リレーに到達できない場合、NRLY (使用可能な監査リレー) アラームがトリガーされます。

> ADCサービスを使用する使用可能なストレージノードがない場合、ストレージノードは監査メッセージをローカルのファイルに格納します `/var/local/log/localaudit.log`。

- もし `/var/local/`ストレージノードが使用するディレクトリが`85%`いっぱいになると、ノードは`S3`クライアントのリクエストを拒否し始めます。 `503 Service Unavailable`。

原因 監査メッセージキューが大幅に増加すると、次のような問題が発生する可能性があります。

- 管理ノードまたは ADC サービスを採用するストレージノードの停止。システムのいずれかのノードが停止すると、残りのノードはバックログ状態になる可能性があります。
- システムの監査キャパシティを超えるアクティビティ率の継続。
- `/var/local/`監査メッセージとは関係のない理由でADCストレージノードのスペースがいっぱいになっている。この場合、ノードは新しい監査メッセージの受け入れを停止し、現在のバックログの優先順位を設定します。これにより、他のノードで原因 バックログが発生する可能性があります。

Large audit queue アラートと **Audit Messages Queued** （ **AMQS** ）アラーム

時間の経過に伴う監査メッセージキューのサイズを監視できるように、ストレージノードキューまたは管理ノードキュー内のメッセージの数が特定のしきい値に達すると、 * Large audit queue * アラートと従来の AMQS アラームがトリガーされます。

「 Large audit queue * 」アラートまたは従来の AMQS アラームがトリガーされた場合は、最初にシステムの負荷を確認します。最近のトランザクションの数が膨大であった場合は、アラートとアラームは時間が経過すると解決するため、無視してかまいません。

アラートまたはアラームが継続して発生し、重大度が増す場合は、キュー サイズのグラフを表示します。数時間または数日にわたってその数が着実に増加している場合は、監査負荷がシステムの監査能力を超えている可能性があります。クライアント書き込みとクライアント読み取りの監査レベルをエラーまたはオフに変更して、クライアント操作率を下げるか、ログに記録される監査メッセージの数を減らします。見る"ログ管理と外部Syslogサーバーを構成する" 。

重複メッセージです

StorageGRID システムは、ネットワークまたはノードの障害が発生した場合に保守的なアプローチを採用します。そのため、監査ログでメッセージが重複する可能性があります。

StorageGRID 管理ノードのコマンドラインから監査ログファイルにアクセスする

監査共有には、アクティブなファイルと圧縮された監査ログファイルが格納され`audit.log`ます。監査ログファイルには、管理ノードのコマンドラインから直接アクセスできます。

その `audit.log`管理ノード/ローカル ノード または 管理ノードと外部 **syslog** サーバー に対してStorageGRIDを構成しない限り、ファイルは空のままになります。詳細については、 "ログの場所を選択" 。

開始する前に

- そうだな "特定のアクセス権限"
- ファイルが必要 `Passwords.txt`です。
- 管理ノードの IP アドレスを確認しておく必要があります。

手順

1. 管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`
   b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`

d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

rootとしてログインすると、プロンプトがからに `#`変わります `$`。

2. 監査ログファイルが保存されているディレクトリに移動します。

```
cd /var/local/audit/export/
```

3. 必要に応じて、現在の監査ログファイルまたは保存された監査ログファイルを表示します。

StorageGRIDにおける監査ログファイルのローテーションについて学ぶ

StorageGRIDが*管理ノード/ローカルノード*または*管理ノードと外部Syslogサーバー*用に構成されている場合、監査ログファイルは管理ノードの `/var/local/audit/export/`ディレクトリ。アクティブな監査ログファイルの名前は `audit.log`。

> 必要に応じて、監査ログの送信先を変更し、監査情報を外部の syslog サーバーに送信することもできます。外部 Syslog サーバーが構成されている場合、監査レコードのローカル ログは引き続き生成され、保存されます。。 "監査メッセージと外部syslogサーバの設定" 。

アクティブなファイルが1日に1回 `audit.log`保存され、新しい `audit.log`ファイルが開始されます。保存されたファイルの名前は、の形式で保存された日時を示します `yyyy-mm-dd.txt`。1日に複数の監査ログが作成される場合は、ファイル名にファイルが保存された日付に番号が付加された形式でファイル名に使用され `yyyy-mm-dd.txt.n`ます。たとえば、 `2018-04-15.txt`2018年4月15日に作成されて保存された最初のログファイルと2番目のログファイルは、と `2018-04-15.txt.1`です。

1日後、保存されたファイルは圧縮され、名前が変更され、形式は次のようになります。 `yyyy-mm-dd.txt.gz`、元の日付が保持されます。時間が経つにつれて、監査ログに割り当てられた管理ノードのストレージが消費されます。スクリプトは監査ログのスペース消費を監視し、必要に応じてログファイルを削除して、 `/var/local/audit/export/`ディレクトリ。監査ログは作成日に基づいて削除されます。最も古いログが最初に削除されます。次のファイルでスクリプトのアクションを監視できます。 `/var/local/log/manage-audit.log`。

この例は、アクティブファイル、前日のファイル(`2018-04-15.txt`）、および前日の圧縮ファイルを示して `audit.log`(`2018-04-14.txt.gz`います。

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

監査ログファイルの形式

StorageGRIDの監査ログファイルの形式について学ぶ

監査ログファイルはすべての管理ノードに存在し、一連の監査メッセージが格納されています。

各監査メッセージには次の情報が含まれます。

- 監査メッセージ（ ATIM ）をトリガーしたイベントの協定世界時（ UTC ）を ISO 8601 形式で表した値と、末尾のスペース。

  YYYY-MM-DDTHH:MM:SS.UUUUUU`を指定します `*UUUUUU*。はマイクロ秒です。

- 監査メッセージ自体。で始まり、角かっこで囲まれます。 `AUDT`

次の例は、監査ログファイル内の 3 つの監査メッセージを示しています（読みやすくするために改行しています）。これらのメッセージは、テナントが S3 バケットを作成し、オブジェクトを 2 つバケットに追加したときに生成されました。

```
2019-08-07T18:43:30.247711
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991681][TIME(UI64):73520][SAI
P(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][AVER(UI32):10][ATIM(UI64):1565203410247711]
[ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):7074142
142472611085]]

2019-08-07T18:43:30.783597
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991696][TIME(UI64):120713][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-0"]
[CBID(UI64):0x779557A069B2C037][UUID(CSTR):"94BA6949-38E1-4B0C-BC80-
EB44FB4FCC7F"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410783597][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):84396067221084560 22]]

2019-08-07T18:43:30.784558
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991693][TIME(UI64):121666][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-2000"]
[CBID(UI64):0x180CBD8E678EED17][UUID(CSTR):"19CE06D0-D2CF-4B03-9C38-
E578D66F7ADD"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410784558][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):13489590586043706682]]
```

デフォルトの形式では、監査ログファイル内の監査メッセージの読みやすさや解釈が容易ではありません。を使用すると、監査ログ内の監査メッセージの簡単な概要を取得できます"audit-explainツール"。を使用すると、ログに記録された書き込み、読み取り、削除の各処理の所要時間を確認できます"audit-sumツール"。

audit-explainツールを使用して**StorageGRID**監査メッセージを翻訳する

ツールを使用すると、監査ログ内の監査メッセージを読みやすい形式に変換できます `audit-explain`。

開始する前に

- そうだな "特定のアクセス権限"
- ファイルが必要 `Passwords.txt`です。
- プライマリ管理ノードの IP アドレスを確認しておく必要があります。

タスクの内容

この `audit-explain`ツールはプライマリ管理ノードで使用でき、監査ログ内の監査メッセージの概要を簡単に確認できます。

> この `audit-explain`ツールは、主にトラブルシューティング処理中にテクニカルサポートが使用することを目的としています。クエリの処理には `audit-explain`大量のCPU電力が消費されることがあり、StorageGRIDの処理に影響を与える可能性があります。

この例は、ツールからの一般的な出力を示してい `audit-explain`ます。これらの4つの"SPUT"監査メッセージは、アカウントIDが92484777680322627870のS3テナントがS3 PUT要求を使用して「bucket1」という名前のバケットを作成し、そのバケットにオブジェクトを3つ追加したときに生成されました。

```
SPUT S3 PUT bucket bucket1 account:92484777680322627870 usec:124673
SPUT S3 PUT object bucket1/part1.txt tenant:92484777680322627870
cbid:9DCB157394F99FE5 usec:101485
SPUT S3 PUT object bucket1/part2.txt tenant:92484777680322627870
cbid:3CFBB07AB3D32CA9 usec:102804
SPUT S3 PUT object bucket1/part3.txt tenant:92484777680322627870
cbid:5373D73831ECC743 usec:93874
```

この `audit-explain`ツールでは、次の操作を実行できます。

- プレーンまたは圧縮された監査ログを処理します。例：

  ```
  audit-explain audit.log

  audit-explain 2019-08-12.txt.gz
  ```

- 複数のファイルを同時に処理します。例：

  ```
  audit-explain audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz

  audit-explain /var/local/audit/export/*
  ```

- パイプからの入力を受け入れます。これにより、コマンドまたはその他の方法を使用して入力をフィルタリングおよび前処理 `grep`できます。例：

  ```
  grep SPUT audit.log | audit-explain

  grep bucket-name audit.log | audit-explain
  ```

監査ログは非常に大きく、解析に時間がかかる可能性があるため、ファイル全体ではなく、対象の部分をフィ

ルタリングして実行することで、時間を節約でき `audit-explain`ます。

> この `audit-explain`ツールは、圧縮ファイルをパイプ付き入力として受け入れません。圧縮ファイルを処理するには、コマンドライン引数としてファイル名を指定するか、ツールを使用し `zcat`て最初にファイルを解凍します。例：
>
> ```
> zcat audit.log.gz | audit-explain
> ```

使用可能なオプションを表示するには、オプションを使用し `help (-h)`ます。例：

```
$ audit-explain -h
```

手順

1. プライマリ管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`
   b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

      rootとしてログインすると、プロンプトがからに `#`変わります `$`。
2. 次のコマンドを入力します。 `/var/local/audit/export/audit.log`分析するファイルの名前と場所を表します。

   ```
   $ audit-explain /var/local/audit/export/audit.log
   ```

   この `audit-explain`ツールは、指定されたファイル内のすべてのメッセージの判読可能な解釈を出力します。

   > 行の長さを短くし、読みやすくするために、タイムスタンプはデフォルトでは表示されません。タイムスタンプを表示する場合は、timestamp(`-t`）オプションを使用します。

audit-sumツールを使用して**StorageGRID**監査メッセージを要約する

ツールを使用して、書き込み、読み取り、HEAD、および削除の監査メッセージをカウントし、各処理タイプの最小、最大、平均時間（またはサイズ）を確認できます `audit-sum`。

開始する前に

- そうだな "特定のアクセス権限"
- あなたはファイルを持ってい `Passwords.txt`ます。
- プライマリ管理ノードのIPアドレスを確認しておきます。

タスクの内容

`audit-sum`ツールはプライマリ管理ノードで使用でき、ログに記録された書き込み、読み取り、削除の各処理の所要時間が表示されます。

この `audit-sum`ツールは、主にトラブルシューティング処理中にテクニカルサポートが使用することを目的としています。クエリの処理には `audit-sum`大量のCPU電力が消費されることがあり、StorageGRIDの処理に影響を与える可能性があります。

この例は、ツールからの一般的な出力を示してい `audit-sum`ます。この例は、プロトコル処理に要した時間を示しています。

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  IDEL                      274
  SDEL                   213371        0.004          20.934
0.352
  SGET                   201906        0.010        1740.290
1.132
  SHEA                    22716        0.005           2.349
0.272
  SPUT                 1771398        0.011        1770.563
0.487
```

その `audit-sum`このツールは、監査ログ内の次の S3 および ILM 監査メッセージの数と時間を提供します。

機能が廃止されると、監査コードは製品およびドキュメントから削除されます。ここに記載されていない監査コードが発生した場合は、このトピックの以前のバージョンで、古いStorageGRIDリリースを確認してください。例： "StorageGRID 11.8 監査合計ツールの使用" 。

コード	製品説明	を参照してください
IDEL	ILM Initiated Delete ： ILM がオブジェクトを削除する処理を開始すると記録されます。	"IDEL ： ILM Initiated Delete"
SDEL	S3 DELETE ：オブジェクトまたはバケットを削除するトランザクションの成功をログに記録します。	"SDEL ： S3 DELETE"
SGET	S3 GET ：バケット内のオブジェクトを読み出しまたはリストアップするトランザクションの成功をログに記録します。	"SGET ： S3 GET"

コード	製品説明	を参照してください
Shea	S3 HEAD ：オブジェクトまたはバケットの存在を確認するトランザクションの成功をログに記録します。	"Shea ： S3 ヘッド"
SPUT	S3 PUT ：オブジェクトまたはバケットを新規に作成するトランザクションの成功をログに記録します。	"SPUT ： S3 PUT"

この `audit-sum`ツールでは、次の操作を実行できます。

- プレーンまたは圧縮された監査ログを処理します。例：

```
audit-sum audit.log

audit-sum 2019-08-12.txt.gz
```

- 複数のファイルを同時に処理します。例：

```
audit-sum audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz

audit-sum /var/local/audit/export/*
```

- パイプからの入力を受け入れます。これにより、コマンドまたはその他の方法を使用して入力をフィルタリングおよび前処理 `grep`できます。例：

```
grep WGET audit.log | audit-sum

grep bucket1 audit.log | audit-sum

grep SPUT audit.log | grep bucket1 | audit-sum
```

> このツールは、パイプ入力として圧縮ファイルを受け入れません。圧縮ファイルを処理するには、コマンドライン引数としてファイル名を指定するか、 `zcat`まずファイルを解凍するツールです。例えば：
>
> ```
> audit-sum audit.log.gz
>
> zcat audit.log.gz | audit-sum
> ```

コマンドラインオプションを使用して、バケットに対する処理をオブジェクトに対する処理とは別にまとめたり、メッセージの概要をバケット名、期間、ターゲットタイプ別にグループ化したりできます。デフォルトでは、要約には最小処理時間、最大処理時間、平均処理時間が表示されますが、オプションを使用してオブジェクトサイズを確認することもできます `size (-s)`。

使用可能なオプションを表示するには、オプションを使用し `help (-h)`ます。例：

```
$ audit-sum -h
```

手順

1. プライマリ管理ノードにログインします。

a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`

b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

c. 次のコマンドを入力してrootに切り替えます。 `su -`

d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

rootとしてログインすると、プロンプトがからに `#`変わります `$`。

2. 書き込み、読み取り、 HEAD 、削除の処理に関連するすべてのメッセージを分析するには、次の手順を実行します。

a. 次のコマンドを入力します。 `/var/local/audit/export/audit.log`分析するファイルの名前と場所を表します。

```
$ audit-sum /var/local/audit/export/audit.log
```

この例は、ツールからの一般的な出力を示してい `audit-sum`ます。この例は、プロトコル処理に要した時間を示しています。

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
=============
  IDEL                      274
  SDEL                   213371        0.004          20.934
0.352
  SGET                   201906        0.010        1740.290
1.132
  SHEA                    22716        0.005           2.349
0.272
  SPUT                 1771398        0.011        1770.563
0.487
```

この例では、平均処理時間では SGET （ S3 GET ）処理が 1.13 秒と最も長い一方で、最大処理時間では SGET 処理と SPUT （ S3 PUT ）処理がどちらも約 1 、 770 秒と一番長くなっています。

b. 最も時間がかかった読み出し処理を10件表示するには、grepコマンドを使用してSGETメッセージのみを選択し、long出力オプションを追加し(`-l`ます）、オブジェクトパスを含めます。

```
grep SGET audit.log | audit-sum -l
```

結果にはタイプ（オブジェクトまたはバケット）とパスが含まれます。この情報を使用して、監査ログを grep してこれらのオブジェクトに関連する他のメッセージを出力できます。

```
Total:          201906 operations
    Slowest:      1740.290 sec
    Average:         1.132 sec
    Fastest:         0.010 sec
    Slowest operations:
        time(usec)       source ip         type      size(B) path
        ========== ============== ============ ============ ====
        1740289662   10.96.101.125       object   5663711385
backup/r9O1OaQ8JB-1566861764-4519.iso
        1624414429   10.96.101.125       object   5375001556
backup/r9O1OaQ8JB-1566861764-6618.iso
        1533143793   10.96.101.125       object   5183661466
backup/r9O1OaQ8JB-1566861764-4518.iso
             70839   10.96.101.125       object        28338
bucket3/dat.1566861764-6619
             68487   10.96.101.125       object        27890
bucket3/dat.1566861764-6615
             67798   10.96.101.125       object        27671
bucket5/dat.1566861764-6617
             67027   10.96.101.125       object        27230
bucket5/dat.1566861764-4517
             60922   10.96.101.125       object        26118
bucket3/dat.1566861764-4520
             35588   10.96.101.125       object        11311
bucket3/dat.1566861764-6616
             23897   10.96.101.125       object        10692
bucket3/dat.1566861764-4516
```

+
この出力例からは、最も時間がかかった 3 個の S3 GET 要求が、他のオブジェクトよりもはるかに大きい約 5GB のオブジェクトに対して実行されたことがわかります。サイズが大きいと、最悪の場合の読み出し時間が長くなります。

3. グリッドに取り込まれているオブジェクトとグリッドから読み出されているオブジェクトのサイズを確認する場合は、sizeオプションを使用し(`-s`ます）。

```
audit-sum -s audit.log
```

```
  message group            count       min(MB)          max(MB)
average(MB)
  =============            =====     ========        ========
============
  IDEL                       274        0.004        5000.000
1654.502
  SDEL                    213371        0.000          10.504
1.695
  SGET                    201906        0.000        5000.000
14.920
  SHEA                     22716        0.001          10.504
2.967
  SPUT                   1771398        0.000        5000.000
2.495
```

この例では、 SPUT の平均オブジェクトサイズは 2.5MB 未満ですが、 SGET の平均サイズははるかに大きいことがわかります。SPUT メッセージの数は SGET メッセージの数よりもはるかに多く、ほとんどのオブジェクトが読み出されていないことを示しています。

4. 昨日の読み出しに時間がかかっていないかどうかを確認するには、次の手順を実行

   a. 該当する監査ログでコマンドを実行し、group-by-timeオプションを使用し(`-gt`ます。そのあとに期間（15M、1H、10Sなど）を指定します。

      ```
      grep SGET audit.log | audit-sum -gt 1H
      ```

```
  message group           count    min(sec)       max(sec)
average(sec)
  =============           =====     ========        ========
============
  2019-09-05T00            7591        0.010        1481.867
1.254
  2019-09-05T01            4173        0.011        1740.290
1.115
  2019-09-05T02           20142        0.011        1274.961
1.562
  2019-09-05T03           57591        0.010        1383.867
1.254
  2019-09-05T04          124171        0.013        1740.290
1.405
  2019-09-05T05          420182        0.021        1274.511
1.562
  2019-09-05T06         1220371        0.015        6274.961
5.562
  2019-09-05T07          527142        0.011        1974.228
2.002
  2019-09-05T08          384173        0.012        1740.290
1.105
  2019-09-05T09           27591        0.010        1481.867
1.354
```

これらの結果は、S3 GET トラフィックが 06:00 から 07:00 の間に急増したことを示しています。この期間中、最大時間と平均時間はどちらもかなり長くなっており、カウントが増加しても徐々に増加することはありません。これらのメトリックは、ネットワークまたはグリッドの要求処理能力の容量が超過した可能性を示唆しています。

b. 昨日読み出されたオブジェクトのサイズを1時間ごとに確認するには、sizeオプションを追加し(`-s`ます）。

```
grep SGET audit.log | audit-sum -gt 1H -s
```

```
  message group           count       min(B)          max(B)
average(B)
  =============           =====     ========        ========
============
  2019-09-05T00            7591        0.040        1481.867
1.976
  2019-09-05T01            4173        0.043        1740.290
2.062
  2019-09-05T02           20142        0.083        1274.961
2.303
  2019-09-05T03           57591        0.912        1383.867
1.182
  2019-09-05T04          124171        0.730        1740.290
1.528
  2019-09-05T05          420182        0.875        4274.511
2.398
  2019-09-05T06         1220371        0.691  5663711385.961
51.328
  2019-09-05T07          527142        0.130        1974.228
2.147
  2019-09-05T08          384173        0.625        1740.290
1.878
  2019-09-05T09           27591        0.689        1481.867
1.354
```

この結果から、読み出しトラフィックの量が最大に達したときに、非常に大容量の読み出しが発生したことがわかります。

c. 詳細を確認するには、を使用し"audit-explainツール"て、その時間内のすべてのSGET処理を確認します。

```
grep 2019-09-05T06 audit.log | grep SGET | audit-explain | less
```

grepコマンドの出力に多数の行が表示される場合は、コマンドを追加して `less`監査ログファイルの内容を1ページ（1画面）ずつ表示します。

5. バケットに対する SPUT 処理にオブジェクトに対する SPUT 処理よりも時間がかかっているかどうかを確認するには、次の手順を実行します。

a. 最初に、オプションを使用し `-go`ます。このオプションは、オブジェクト処理とバケット処理でメッセージを個別にグループ化します。

```
grep SPUT sample.log | audit-sum -go
```

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  SPUT.bucket                 1        0.125           0.125
0.125
  SPUT.object                12        0.025           1.019
0.236
```

上記の結果から、バケットに対する SPUT 処理とオブジェクトに対する SPUT 処理でパフォーマンス特性が異なることがわかります。

b. SPUT処理に最も時間がかかっているバケットを特定するには、オプションを使用し `-gb`ます。このオプションはバケットごとにメッセージをグループ化します。

```
grep SPUT audit.log | audit-sum -gb
```

```
  message group                  count     min(sec)        max(sec)
average(sec)
  =============                  =====     ========        ========
============
  SPUT.cho-non-versioning        71943        0.046        1770.563
1.571
  SPUT.cho-versioning            54277        0.047        1736.633
1.415
  SPUT.cho-west-region           80615        0.040          55.557
1.329
  SPUT.ldt002                  1564563        0.011          51.569
0.361
```

c. SPUTオブジェクトサイズが最も大きいバケットを確認するには、オプションと `-s`オプションの両方を使用し `-gb`ます。

```
grep SPUT audit.log | audit-sum -gb -s
```

```
  message group                    count       min(B)          max(B)
average(B)
  =============                    =====     ========        ========
============
  SPUT.cho-non-versioning          71943        2.097        5000.000
21.672
  SPUT.cho-versioning              54277        2.097        5000.000
21.120
  SPUT.cho-west-region             80615        2.097         800.000
14.433
  SPUT.ldt002                    1564563        0.000         999.972
0.352
```

監査メッセージの形式

StorageGRID監査メッセージの構造について学ぶ

StorageGRID システム内でやり取りされる監査メッセージには、すべてのメッセージに共通の標準情報と、報告対象のイベントまたはアクティビティを説明する固有のコンテンツが含まれます。

ツールと"audit-sumの略"ツールから提供される概要情報では不十分な場合は"監査-説明する"、このセクションを参照して、すべての監査メッセージの一般的な形式を理解してください。

以下は、監査ログファイルに記録されている監査メッセージの例です。

```
2014-07-17T03:50:47.484627
[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP(F
C32):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265006
03516]]
```

各監査メッセージには、一連の属性要素で構成されます。文字列全体は角かっこで囲まれてい(`[]`ます）。文字列内の各属性要素には次のような特徴があります。

- 角かっこで囲まれている `[ ]`
- 監査メッセージを示す文字列で始まる `AUDT`
- 前後に区切り記号（カンマやスペース）がない
- 改行文字で終了 `\n`

各要素には、次の形式で報告される属性コード、データ型、および値が含まれます。

```
[ATTR(type):value][ATTR(type):value]...
[ATTR(type):value]\n
```

メッセージ内の属性要素の数は、メッセージのイベントタイプによって異なります。属性要素は特定の順序でリストされません。

次に、属性要素について説明します。

- `ATTR`は、レポートされる属性の4文字のコードです。すべての監査メッセージに共通する属性とイベント固有の属性があります。
- `type`は、UI64、FC32など、値のプログラミングデータタイプの4文字の識別子です。タイプはかっこで囲まれてい`( )`ます。
- `value`は属性の内容で、通常は数値またはテキスト値です。値は常にコロンの後に続き (:`ます）。データ型CStrの値は二重引用符で囲まれます。

StorageGRID監査メッセージのデータ型

監査メッセージ内の情報の格納にはさまざまなデータタイプが使用されます。

タイプ	製品説明
UI32	符号なし長整数（ 32 ビット）。 0~4 、 294 、 967 、 295 の数値を格納できます。
UI64	符号なし倍精度長整数（ 64 ビット）。 0~18 、 446 、 744 、 073 、 709 、 551 、 615 の数値を格納できます。
FC32	4文字の定数。"ABCD"などの4つのASCII文字で表される32ビットの符号なし整数値です。
iPad	IP アドレスに使用されます。
CSTR	UTF-8文字の可変長配列。文字は次の方法でエスケープできます。 • バックスラッシュは \\ 。 • 復帰文字は \r です • 二重引用符は \" 。 • 改行（新しい行）は \n です • 文字は、それぞれに相当する 16 進数に置き換えることができます（ \xHH の形式、 HH は該当する文字を表す 16 進値）。

StorageGRID監査メッセージ内のイベント固有のデータ

監査ログ内の各監査メッセージはシステムイベントに固有のデータを記録します。

メッセージ自体を識別する開いているコンテナに続く一連の属性は、 `[AUDT:`監査メッセージで説明されて

いるイベントまたはアクションに関する情報を提供します。以下の例では、これらの属性を強調表示しています。

```
2018-12-05T08:24:45.921845 [AUDT: \[RSLT\(FC32\):SUCS\]
\[TIME\(UI64\):11454\]\[SAIP\(IPAD\):"10.224.0.100"\]\[S3AI\(CSTR\):"60025
621595611246499"\]
\[SACC\(CSTR\):"account"\]\[S3AK\(CSTR\):"SGKH4_Nc8SO1H6w3w0nCOFCGgk__E6dY
zKlumRsKJA=="\]
\[SUSR\(CSTR\):"urn:sgws:identity::60025621595611246499:root"\]
\[SBAI\(CSTR\):"60025621595611246499"\]\[SBAC\(CSTR\):"account"\]\[S3BK\(C
STR\):"bucket"\]
\[S3KY\(CSTR\):"object"\]\[CBID\(UI64\):0xCC128B9B9E428347\]
\[UUID\(CSTR\):"B975D2CE-E4DA-4D14-8A23-
1CB4B83F2CD8"\]\[CSIZ\(UI64\):30720\][AVER(UI32):10]
\[ATIM(UI64):1543998285921845]\[ATYP\(FC32\):SHEA\][ANID(UI32):12281045][A
MID(FC32):S3RQ]
\[ATID(UI64):15552417629170647261]]
```

エレメント（この例では下線付き）は、 `ATYP`メッセージを生成したイベントを識別します。この例のメッセージには、S3 HEAD要求が成功して生成されたことを示すメッセージコード（[ATYP（FC32）：Shea]）が含まれてい"Shea"ます。

StorageGRID監査メッセージの共通要素

すべての監査メッセージには、共通の要素が含まれています。

コード	タイプ	製品説明
AMid	FC32	Module ID：メッセージを生成したモジュールIDの4文字の識別子。これは、監査メッセージが生成されたコードセグメントを示します。
ANID	UI32	Node ID ：メッセージを生成したサービスに割り当てられたグリッドノード ID 。各サービスには、 StorageGRID システムの設定およびインストール時に一意の識別子が割り当てられます。このIDは変更できません。
ASES	UI64	Audit Session Identifier ：以前のリリースでは、この要素はサービスの開始後に監査システムが初期化された時間を示していました。この時間値は、オペレーティングシステムのエポック（1970年1月1日00：00：00 UTC）からのマイクロ秒数で測定されました。 • 注： * この要素は廃止され、監査メッセージには表示されなくなりました。

コード	タイプ	製品説明
ASQN	UI64	Sequence Count ：以前のリリースでは、このカウンタはグリッドノード（ ANID ）上で監査メッセージが生成されるたびに増分し、サービスの再起動時にゼロにリセットされていました。 • 注： * この要素は廃止され、監査メッセージには表示されなくなりました。
ATID	UI64	Trace ID ： 1 つのイベントによってトリガーされた一連のメッセージで共有される識別子。
ATIM	UI64	Timestamp：監査メッセージをトリガーしたイベントが生成された時刻。オペレーティングシステムのエポック（1970年1月1日00：00：00 UTC）からのマイクロ秒数で測定されます。タイムスタンプをローカルの日時に変換するためのツールは、ほとんどがミリ秒に基づいています。 ログに記録されたタイムスタンプの丸めや切り捨てが必要な場合があります。ファイル内の監査メッセージの先頭に表示される判読可能な時刻`audit.log`は、ISO 8601形式のATIM属性です。日付と時刻は、で表され`*YYYY-MMDDTHH:MM:SS.UUUUUU*`ます。 `T`は、日付の時間セグメントの先頭を示すリテラル文字列です。 `*UUUUUU*`はマイクロ秒です。
ATYP	FC32	Event Type：ログに記録されるイベントの4文字の識別子。これは、メッセージの「ペイロード」コンテンツ、つまり含まれる属性を管理します。
ビーバー	UI32	Version ：監査メッセージのバージョン。StorageGRID ソフトウェアのバージョンアップに伴い、新しいバージョンのサービスによって新しい機能が監査レポートに組み込まれる可能性があります。このフィールドは、旧バージョンのサービスのメッセージを処理できるよう、 AMS サービスにおける下位互換性を可能にします。
RSLT	FC32	Result ：イベント、プロセス、またはトランザクションの結果。該当しないメッセージの場合は、誤ってフィルタリングされないように SUCS ではなく NONE が使用されます。

StorageGRID監査メッセージの形式と例

各監査メッセージには詳細な情報が含まれています。監査メッセージはすべて同じ形式です。

次に、ファイルに記録されている監査メッセージの例を示し`audit.log`ます。

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPUT
][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224144
102530435]]
```

監査メッセージには、記録されたイベントに関する情報と、監査メッセージ自体に関する情報が含まれています。

監査メッセージによって記録されているイベントは、 ATYP 属性（以下で強調表示されている部分）で識別します。

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224
144102530435]]
```

ATYP 属性の値は SPUT です。"SPUT"S3 PUTトランザクションを表し、バケットへのオブジェクトの取り込みをログに記録します。

次の監査メッセージは、オブジェクトが関連付けられているバケットも示しています。

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK\(CSTR\):"s3small1"][S3
KY(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):
0][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPU
T][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):157922414
4102530435]]
```

PUT イベントがいつ発生したかを調べるには、監査メッセージの先頭の世界標準時（ UTC ）のタイムスタンプを確認します。この値は、監査メッセージ自体のATIM属性を判読できる形式です。

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM\(UI64\):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):15792241
44102530435]]
```

ATIM は、 UNIX エポックの開始時点からの時間をマイクロ秒数で記録します。この例では、値は `1405631878959669`2014年7月17日木曜日21:17:59 UTCに変換されます。

監査メッセージとオブジェクトライフサイクル

StorageGRIDで監査メッセージが生成される場合

監査メッセージは、オブジェクトの取り込み、読み出し、または削除が行われるたびに生成されます。監査ログでこれらのトランザクションを特定するには、S3 API固有の監査メッセージを検索します。

監査メッセージは各プロトコルに固有な識別子によってリンクされます。

プロトコル	コード
S3 処理をリンクしています	S3BK（バケット）、S3KY（キー）、またはその両方
内部処理をリンクしています	CBID（オブジェクトの内部識別子）

監査メッセージのタイミング

グリッドノード間のタイミングの違い、オブジェクトサイズ、ネットワーク遅延などの要因により、各サービスによって生成される監査メッセージの順序はこのセクションに記載する例とは異なる場合があります。

StorageGRID でのオブジェクト取り込みトランザクションの監査メッセージ

監査ログでクライアントの取り込みトランザクションを特定するには、S3 API固有の監査メッセージを検索します。

取り込みトランザクション中に生成されるすべての監査メッセージが次の表に記載されているわけではありません。取り込みトランザクションのトレースに必要なメッセージのみが含まれます。

S3 の取り込み監査メッセージ

コード	名前	製品説明	トレース	を参照してください
SPUT	S3 PUT トランザクション	S3 PUT 取り込みトランザクションが正常に完了しました。	CBID 、 S3BK 、 S3KY	"SPUT ： S3 PUT"
ORLM の場合	オブジェクトルールを満たしました	このオブジェクトが ILM ポリシーを満たしました。	CBID	"ORLM ：オブジェクトルールが満たされています"

例： **S3** オブジェクトの取り込み

以下の一連の監査メッセージは、 S3 クライアントがストレージノード（ LDR サービス）にオブジェクトを取り込んだときに生成され、監査ログに保存された監査メッセージの例です。

この例では、アクティブなILMポリシーにMake 2 Copies ILMルールが含まれています。

以下の例には、トランザクション中に生成されたすべての監査メッセージが含まれているわけではなく、S3 取り込みトランザクション（ SPUT ）に関連するメッセージだけが示されています。

この例では、 S3 バケットは以前に作成済みであることを前提としています。

SPUT ： S3 PUT

SPUT メッセージは、特定のバケットにオブジェクトを作成する S3 PUT トランザクションが実行されたことを示します。

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):25771][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"][S3BK(CSTR):"example"][S3KY(CSTR):"testobject-0-
3"][CBID\(UI64\):0x8EF52DF8025E63A8][CSIZ(UI64):30720][AVER(UI32):10][ATIM
(UI64):150032627859669][ATYP\(FC32\):SPUT][ANID(UI32):12086324][AMID(FC32)
:S3RQ][ATID(UI64):14399932238768197038]]
```

ORLM ：オブジェクトルールが満たされています

ORLM メッセージは、このオブジェクトが ILM ポリシーに準拠していることを示します。メッセージには、オブジェクトの CBID と適用された ILM ルールの名前が含まれています。

レプリケートオブジェクトの場合、 LOCS フィールドにはオブジェクトの場所の LDR ノード ID とボリューム ID が記録されます。

```
2019-07-
17T21:18:31.230669[AUDT:[CBID\(UI64\):0x50C4F7AC2BC8EDF7][RULE(CSTR):"Make
2 Copies"][STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"0B344E18-98ED-4F22-
A6C8-A93ED68F8D3F"][LOCS(CSTR):"CLDI 12828634 2148730112, CLDI 12745543
2147552014"][RSLT(FC32):SUCS][AVER(UI32):10][ATYP\(FC32\):ORLM][ATIM(UI64)
:1563398230669][ATID(UI64):15494889725796157557][ANID(UI32):13100453][AMID
(FC32):BCMS]]
```

イレイジャーコーディングオブジェクトの場合は、LOCSフィールドにイレイジャーコーディングプロファイルIDとイレイジャーコーディンググループIDが表示されます。

```
2019-02-23T01:52:54.647537
[AUDT:[CBID(UI64):0xFA8ABE5B5001F7E2][RULE(CSTR):"EC_2_plus_1"][STAT(FC32)
:DONE][CSIZ(UI64):10000][UUID(CSTR):"E291E456-D11A-4701-8F51-
D2F7CC9AFECA"][LOCS(CSTR):"CLEC 1 A471E45D-A400-47C7-86AC-
12E77F229831"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1550929974537]\[
ATYP\(FC32\):ORLM\][ANID(UI32):12355278][AMID(FC32):ILMX][ATID(UI64):41685
59046473725560]]
```

PATH フィールドには、S3 バケットとキー情報が含まれます。

```
2019-09-15.txt:2018-01-24T13:52:54.131559
[AUDT:[CBID(UI64):0x82704DFA4C9674F4][RULE(CSTR):"Make 2
Copies"][STAT(FC32):DONE][CSIZ(UI64):3145729][UUID(CSTR):"8C1C9CAC-22BB-
4880-9115-
CE604F8CE687"][PATH(CSTR):"frisbee_Bucket1/GridDataTests151683676324774_1_
1vf9d"][LOCS(CSTR):"CLDI 12525468, CLDI
12222978"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1568555574559][ATYP(
FC32):ORLM][ANID(UI32):12525468][AMID(FC32):OBDI][ATID(UI64):3448338865383
69336]]
```

StorageGRIDにおけるオブジェクト削除トランザクションの監査メッセージ

監査ログでオブジェクトの削除トランザクションを特定するには、S3 API固有の監査メッセージを検索します。

以下の表には、削除トランザクション中に生成されたすべての監査メッセージが含まれているわけではなく、削除トランザクションをトレースするために必要なメッセージのみが含まれています。

S3 の削除監査メッセージ

コード	名前	製品説明	トレース	を参照してください
SDEL	S3 削除	バケットからのオブジェクトの削除が要求されました。	CBID 、 S3KY	"SDEL ： S3 DELETE"

例： **S3** オブジェクトの削除

S3 クライアントがストレージノード（ LDR サービス）からオブジェクトを削除すると、監査メッセージが生成されて監査ログに保存されます。

以下の例には、削除トランザクション中に生成されたすべての監査メッセージが含まれているわけではなく、S3 の削除トランザクション（ SDEL ）に関連するメッセージだけが示されています。

SDEL ： S3 削除

オブジェクトの削除は、クライアントがLDRサービスにDeleteObject要求を送信した時点で開始されます。メッセージには、オブジェクトの削除元のバケットと、オブジェクトの識別に使用される S3 キーが含まれています。

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):14316][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"]\[S3BK\(CSTR\):"example"\]\[S3KY\(CSTR\):"testobject-0-
7"\][CBID\(UI64\):0x339F21C5A6964D89][CSIZ(UI64):30720][AVER(UI32):10][ATI
M(UI64):150032627859669][ATYP\(FC32\):SDEL][ANID(UI32):12086324][AMID(FC32
):S3RQ][ATID(UI64):4727861330952970593]]
```

StorageGRID のオブジェクト取得トランザクションの監査メッセージ

監査ログでオブジェクトの読み出しトランザクションを特定するには、S3 API固有の監査メッセージを検索します。

取得トランザクション中に生成されるすべての監査メッセージが次の表に記載されているわけではありません。取得トランザクションのトレースに必要なメッセージのみが含まれます。

S3 の読み出し監査メッセージ

コード	名前	製品説明	トレース	を参照してください
SGET	S3 GET	バケットからのオブジェクトの読み出しが要求されました。	CBID 、 S3BK 、 S3KY	"SGET ： S3 GET"

例： **S3** オブジェクトの読み出し

S3 クライアントがストレージノード（ LDR サービス）からオブジェクトを読み出すと、監査メッセージが生成されて監査ログに保存されます。

以下の例には、トランザクション中に生成されたすべての監査メッセージが含まれているわけではなく、S3 読み出しトランザクション（ SGET ）に関連するメッセージだけが示されています。

SGET ： S3 GET

オブジェクトの読み出しは、クライアントがLDRサービスにGetObject要求を送信したときに開始されます。メッセージには、オブジェクトの読み出し元のバケットと、オブジェクトの識別に使用される S3 キーが含まれています。

```
2017-09-20T22:53:08.782605
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):47807][SAIP(IPAD):"10.96.112.26"][S3AI(
CSTR):"43979298178977966408"][SACC(CSTR):"s3-account-
a"][S3AK(CSTR):"SGKHt7GzEcu0yXhFhT_rL5mep4nJt1w75GBh-
O_FEw=="][SUSR(CSTR):"urn:sgws:identity::43979298178977966408:root"][SBAI(
CSTR):"43979298178977966408"][SBAC(CSTR):"s3-account-
a"]\[S3BK\(CSTR\):"bucket-
anonymous"\]\[S3KY\(CSTR\):"Hello.txt"\][CBID(UI64):0x83D70C6F1F662B02][CS
IZ(UI64):12][AVER(UI32):10][ATIM(UI64):1505947988782605]\[ATYP\(FC32\):SGE
T\][ANID(UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):17742374343649889669]
]
```

バケットポリシーで許可されている場合、クライアントはオブジェクトを匿名で読み出したり、別のテナントアカウントが所有しているバケットからオブジェクトを読み出すことができます。監査メッセージには、このような匿名要求およびクロスアカウント要求を追跡できるように、バケット所有者のテナントアカウントに関する情報が含まれています。

次のメッセージ例では、クライアントが所有していないバケットに格納されているオブジェクトに対するGetObject要求を送信しています。SBAI と SBAC の値にはバケット所有者のテナントアカウント ID と名前が記録されますが、これは S3AI および SACC に記録されているクライアントのテナントアカウント ID および名前とは異なります。

```
2017-09-20T22:53:15.876415
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):53244][SAIP(IPAD):"10.96.112.26"]\[S3AI
\(CSTR\):"17915054115450519830"\]\[SACC\(CSTR\):"s3-account-
b"\][S3AK(CSTR):"SGKHpoblWlP_kBkqSCbTi754Ls8lBUog67I2LlSiUg=="][SUSR(CSTR)
:"urn:sgws:identity::17915054115450519830:root"]\[SBAI\(CSTR\):"4397929817
8977966408"\]\[SBAC\(CSTR\):"s3-account-a"\][S3BK(CSTR):"bucket-
anonymous"][S3KY(CSTR):"Hello.txt"][CBID(UI64):0x83D70C6F1F662B02][CSIZ(UI
64):12][AVER(UI32):10][ATIM(UI64):1505947995876415][ATYP(FC32):SGET][ANID(
UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):6888780247515624902]]
```

例：オブジェクトの **S3 Select**

S3 クライアントがオブジェクトに対して S3 Select クエリを実行すると、監査メッセージが生成されて監査ログに保存されます。

以下の例には、トランザクション中に生成されたすべての監査メッセージが含まれているわけではなく、S3 Select トランザクション（ SelectObjectContent ）に関連するトランザクションのみが表示されます。

各クエリには2つの監査メッセージが生成されます。1つはS3 Select要求の承認を実行するメッセージ（S3SR フィールドが「select」に設定されている）で、もう1つは処理中にストレージからデータを取得する標準のGET処理です。

```
2021-11-08T15:35:30.750038
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636385730715700][TIME(UI64):29173][SAI
P(IPAD):"192.168.7.44"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Ten
ant1636027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:id
entity::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBA
C(CSTR):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"][S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):0][S3SR(CSTR):"select"][AVER(UI32):10][ATIM(UI64
):1636385730750038][ATYP(FC32):SPOS][ANID(UI32):12601166][AMID(FC32):S3RQ]
[ATID(UI64):1363009709396895985]]
```

```
2021-11-08T15:35:32.604886
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636383069486504][TIME(UI64):430690][SA
IP(IPAD):"192.168.7.44"][HTRH(CSTR):"{\"x-forwarded-
for\":\"unix:\"}"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Tenant16
36027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:identit
y::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBAC(CST
R):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"][S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):10185581][MTME(UI64):1636380348695262][AVER(UI32
):10][ATIM(UI64):1636385732604886][ATYP(FC32):SGET][ANID(UI32):12733063][A
MID(FC32):S3RQ][ATID(UI64):16562288121152341130]]
```

StorageGRIDにおける**S3**オブジェクトのメタデータ更新に関する監査メッセージ

S3 クライアントがオブジェクトのメタデータを更新すると、監査メッセージが生成されます。

S3 メタデータの更新監査メッセージ

コード	名前	製品説明	トレース	を参照してください
SUPD	S3 メタデータが更新されました	S3 クライアントが取り込まれたオブジェクトのメタデータを更新すると生成されます。	CBID 、 S3KY 、 HTRH	"SUPD ： S3 メタデータが更新されました"

例： **S3** メタデータの更新

次の例は、既存の S3 オブジェクトのメタデータを更新するトランザクションの成功を示しています。

SUPD ： S3 メタデータの更新

S3クライアントは、S3オブジェクト（S3KY）の指定されたメタデータ（(`x-amz-meta-*`）を更新するリクエスト（SUPD）を行います。

この例では、リクエスト ヘッダーがフィールド HTRH に含まれています。これは、監査プロトコル ヘッダーとして設定されているためです （設定 > 監視 > 監査と **syslog** サーバ）。"ログ管理と外部Syslogサーバーを構成する"を参照してください。

```
2017-07-11T21:54:03.157462
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):17631][SAIP(IPAD):"10.96.100.254"]
[HTRH(CSTR):"{\"accept-encoding\":\"identity\",\"authorization\":\"AWS
LIUF17FGJARQHPY2E761:jul/hnZs/uNY+aVvV0lTSYhEGts=\",
\"content-length\":\"0\",\"date\":\"Tue, 11 Jul 2017 21:54:03
GMT\",\"host\":\"10.96.99.163:18082\",
\"user-agent\":\"aws-cli/1.9.20 Python/2.7.6 Linux/3.13.0-119-generic
botocore/1.3.20\",
\"x-amz-copy-source\":\"/testbkt1/testobj1\",\"x-amz-metadata-
directive\":\"REPLACE\",\"x-amz-meta-city\":\"Vancouver\"}"]
[S3AI(CSTR):"20956855414285633225"][SACC(CSTR):"acct1"][S3AK(CSTR):"SGKHyy
v9ZQqWRbJSQc5vI7mgioJwrdplShE02AUaww=="]
[SUSR(CSTR):"urn:sgws:identity::20956855414285633225:root"]
[SBAI(CSTR):"20956855414285633225"][SBAC(CSTR):"acct1"][S3BK(CSTR):"testbk
t1"]
[S3KY(CSTR):"testobj1"][CBID(UI64):0xCB1D5C213434DD48][CSIZ(UI64):10][AVER
(UI32):10]
[ATIM(UI64):1499810043157462][ATYP(FC32):SUPD][ANID(UI32):12258396][AMID(F
C32):S3RQ]
[ATID(UI64):8987436599021955788]]
```

監査メッセージ

StorageGRIDの監査メッセージの種類とコードについて学ぶ

システムから返される監査メッセージの詳細について、次のセクションで説明します。各監査メッセージをメッセージが表すアクティビティのクラスでグループ化して、表に記載します。これらの分類は、監査対象のアクティビティのタイプを理解し、必要な監査メッセージフィルタリングのタイプを選択する場合に役立ちます。

監査メッセージは、 4 文字のコードでアルファベット順に一覧表示されます。このアルファベット順のリストでは、特定のメッセージに関する情報を検索できます。

この章で使用する4文字のコードは、次のメッセージ例に示すように、監査メッセージ内のATYP値です。

```
2014-07-17T03:50:47.484627
\[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP\
(FC32\):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265
00603516]]
```

監査メッセージのレベルの設定、ログの保存先の変更、監査情報用の外部Syslogサーバーの使用については、以下を参照してください。"ログ管理と外部Syslogサーバーを構成する"

監査メッセージのカテゴリ

StorageGRID のシステムイベントの監査メッセージ

システム監査カテゴリに属する監査メッセージは、監査システム自体、グリッドノードの状態、システム全体のタスクアクティビティ（グリッドタスク）、およびサービスバックアップ処理に関連するイベントに使用されます。

コード	メッセージのタイトルと概要	を参照してください
ECMC	Missing Erasure-Coded Data Fragment：イレイジャーコーディングされたデータフラグメントの欠落が検出されたことを示します。	"ECMC：イレイジャーコーディングされたデータフラグメントの欠落"
ECOC	Corrupt Erasure-Coded Data Fragment：イレイジャーコーディングデータフラグメントの破損が検出されたことを示します。	"ECOC：イレイジャーコーディングされたデータフラグメントの破損"
ETAF	Security Authentication Failed ： Transport Layer Security （ TLS ）を使用した接続試行が失敗しました。	"ETAF ：セキュリティ認証に失敗しました"
GNRG	GNDS Registration ：サービスが StorageGRID システムに自身に関する情報を更新または登録しました。	"GNRG ： GNDS 登録"

コード	メッセージのタイトルと概要	を参照してください
GNUR	GNDS Unregistration ：サービスが StorageGRID システムから自身の登録を解除しました。	"GNUR ： GNDS 登録解除"
GTED	Grid Task Ended ： CMN サービスがグリッドタスクの処理を完了しました。	"GTED ： Grid タスクが終了しました"
GTSt	Grid Task Started ： CMN サービスがグリッドタスクの処理を開始しました。	"GTSt ： Grid タスクが開始されました"
GTSU	Grid Task Submitted ：グリッドタスクが CMN サービスに送信されました。	"GTSU ： Grid タスクが送信されました"
LLST	Location Lost ：この監査メッセージは、場所が失われたときに生成されます。	"LLST ：ロケーションが失われました"
OLST	Object Lost ：要求されたオブジェクトが StorageGRID システム内に見つかりません。	"OLST: システムが損失オブジェクトを検出しました"
サッド	Security Audit Disable ：監査メッセージのロギングがオフになりました。	"SADD ：セキュリティ監査無効"
Sade 社	Security Audit Enable ：監査メッセージのロギングが再開されました。	"Sade ：セキュリティ監査を有効にします"
SVRF	Object Store Verify Fail ：コンテンツブロックが検証チェックに失敗しました。	"SVRF ：オブジェクトストアの検証に失敗しました"
SVRU の場合	Object Store Verify Unknown ：オブジェクトストアで想定外のオブジェクトデータが検出されました。	"SVRU ：オブジェクトストア検証が不明です"
SYSD	Node Stop ：シャットダウンが要求されました。	"SYSD ：ノード停止"
SYST	Node Stopping ：サービスが正常な停止を開始しました。	"SYST ：ノードを停止しています"
SYSU	Node Start ：サービスが開始されました。前回のシャットダウンのタイプがメッセージに示されます。	"SYSU ：ノードが開始されました"

StorageGRID のオブジェクトストレージイベントの監査メッセージ

オブジェクトストレージ監査カテゴリに属する監査メッセージは、StorageGRID システム内のオブジェクトの格納と管理に関連するイベントに使用されます。オブジェクトの

格納と読み出し、グリッドノードからグリッドノードへの転送、および検証が含まれます。

機能が廃止されたため、製品やドキュメントから監査コードが削除されました。ここに記載されていない監査コードが発生した場合は、古いSGリリースについてこのトピックの以前のバージョンを確認してください。たとえば、 "StorageGRID 11.8オブジェクトストレージ監査メッセージ"です。

コード	製品説明	を参照してください
ブロア	Bucket Read Only Request：バケットが読み取り専用モードになったか、または終了しました。	"BROR：バケット読み取り専用要求"
CBSE	Object Send End ：ソースエンティティが、グリッドノードからグリッドノードへのデータ転送処理を完了しました。	"CBSE ：オブジェクト送信終了"
CBRE	Object Receive End ：デスティネーションエンティティが、グリッドノードからグリッドノードへのデータ転送処理を完了しました。	"CBRE ：オブジェクト受信終了"
CGRR	Cross-Grid Replication Request：StorageGRID が、グリッドフェデレーション接続内のバケット間でオブジェクトをレプリケートするために、グリッド間レプリケーション処理を試行しました。	"CGRR：クロスグリッドレプリケーション要求"
EBDL	Empty Bucket Delete：ILMスキャナが、すべてのオブジェクトを削除中のバケット内のオブジェクトを削除しました（空のバケット処理を実行中）。	"EBDL：空のバケット削除"
EBKR	Empty Bucket Request：ユーザが、空のバケットをオンまたはオフにする（バケットオブジェクトを削除する、またはオブジェクトの削除を停止する）要求を送信しました。	"EBKR：バケット要求が空です"
SCMT	Object Store Commit ：コンテンツブロックの格納と検証がすべて完了し、要求可能な状態になりました。	"SCMT：オブジェクトストアコミット要求"
SREM	Object Store Remove ：コンテンツブロックがグリッドノードから削除され、直接要求できなくなりました。	"SREM ：オブジェクトストアの削除"

StorageGRID におけるクライアントの読み取り操作の監査メッセージ

クライアント読み取り監査メッセージは、S3クライアントアプリケーションがオブジェクトの読み出しを要求するときに記録されます。

コード	製品説明	によって使用されます	を参照してください
S3SL	S3 Select要求：S3 Select要求がクライアントに返されたあとに完了をログに記録します。S3SLメッセージには、エラーメッセージとエラーコードの詳細を含めることができます。要求は成功しなかった可能性があります。	S3 クライアント	"S3SL：S3 Select要求"
SGET	S3 GET ：バケット内のオブジェクトを読み出しまたはリストアップするトランザクションの成功をログに記録します。 • 注：トランザクションがサブリソースで動作している場合、監査メッセージには S3SR フィールドが含まれます。	S3 クライアント	"SGET ： S3 GET"
Shea	S3 HEAD ：オブジェクトまたはバケットの存在を確認するトランザクションの成功をログに記録します。	S3 クライアント	"Shea ： S3 ヘッド"

StorageGRID におけるクライアント書き込み操作の監査メッセージ

クライアント書き込み監査メッセージは、S3クライアントアプリケーションがオブジェクトを作成または変更する要求を行うと記録されます。

コード	製品説明	によって使用されます	を参照してください
OWR	Object Overwrite ：あるオブジェクトを別のオブジェクトで上書きするトランザクションをログに記録します。	S3 クライアント	"OVWR ：オブジェクトを上書き"
SDEL	S3 DELETE ：オブジェクトまたはバケットを削除するトランザクションの成功をログに記録します。 • 注：トランザクションがサブリソースで動作している場合、監査メッセージには S3SR フィールドが含まれます。	S3 クライアント	"SDEL ： S3 DELETE"
SPO	S3 POST ：オブジェクトを AWS Glacier ストレージからクラウドストレージプールにリストアするトランザクションの成功をログに記録します。	S3 クライアント	"SPO ： S3 POST"

コード	製品説明	によって使用されます	を参照してください
SPUT	S3 PUT ：オブジェクトまたはバケットを新規に作成するトランザクションの成功をログに記録します。 • 注：トランザクションがサブリソースで動作している場合、監査メッセージには S3SR フィールドが含まれます。	S3 クライアント	"SPUT ： S3 PUT"
SUPD	S3 Metadata Updated ：既存のオブジェクトまたはバケットのメタデータを更新するトランザクションの成功をログに記録します。	S3 クライアント	"SUPD ： S3 メタデータが更新されました"

StorageGRID管理監査メッセージ

管理カテゴリでは、管理 API に対するユーザ要求がログに記録されます。

コード	メッセージのタイトルと概要	を参照してください
MGAU	管理 API 監査メッセージ：ユーザ要求のログ。	"MGAU ：管理監査メッセージ"

StorageGRID ILM監査メッセージ

ILM監査カテゴリに属する監査メッセージは、情報ライフサイクル管理（ILM）処理に関連するイベントに使用されます。

コード	メッセージのタイトルと概要	を参照してください
IDEL	ILM Initiated Delete ：この監査メッセージは、 ILM がオブジェクトを削除する処理を開始すると生成されます。	"IDEL ： ILM Initiated Delete"
LCU	上書きされたオブジェクトのクリーンアップ。この監査メッセージは、ストレージスペースを解放するために上書きされたオブジェクトが自動的に削除されたときに生成されます。	"LKCU: 上書きされたオブジェクトのクリーンアップ"
ORLM の場合	Object Rules Met：この監査メッセージは、ILMルールの指定に従ってオブジェクトデータが格納された場合に生成されます。	"ORLM ：オブジェクトルールが満たされています"

監査メッセージリファレンス

StorageGRIDのバケット読み取り専用リクエストのBROR監査メッセージ

この監査メッセージは、バケットが読み取り専用モードになったときまたは終了したときにLDRサービスによって生成されます。たとえば、すべてのオブジェクトが削除されている間にバケットが読み取り専用モードになったとします。

コード	フィールド	製品説明
BKHD	バケットUUID	バケットID。
ブローブ	バケットの読み取り専用要求値	バケットが読み取り専用になっているか、または読み取り専用のままになっているか（1=読み取り専用、0=読み取り専用ではない）。
ブラザーズ	バケット読み取り専用の理由	バケットが読み取り専用になっている理由、または読み取り専用状態のままになっている理由。たとえば、emptyBucketなどです。
S3AI	S3テナントアカウントID	要求を送信したテナントアカウントのID。空の値は匿名アクセスであることを示します。
S3BK	S3バケット	S3 バケット名。

StorageGRIDにおけるオブジェクト受信開始の**CBRB**監査メッセージ

通常のシステム運用中は、データへのアクセスおよびデータのレプリケートと保持が行われる際に、異なるノード間でコンテンツブロックが継続的に転送されます。このメッセージは、あるノードから別のノードへのコンテンツブロックの転送が開始したときに転送先のエンティティによって生成されます。

コード	フィールド	製品説明
CNID	接続識別子	ノード間のセッション / 接続の一意の識別子。
CBID	Content Block Identifier の略	転送されるコンテンツブロックの一意の識別子。
CTDR	転送方向（ Transfer Direction ）	CBID 転送がプッシュで開始されたかプルで開始されたかを示します。 PUSH ：転送処理は送信側エンティティによって要求されました。 PULL ：転送処理は受信側エンティティによって要求されました。
CTSR	ソースエンティティ	CBID 転送のソース（送信側）のノード ID 。
CTD	デスティネーションエンティティ	CBID 転送のデスティネーション（受信側）のノード ID 。
CTSS	開始シーケンスカウント（ Start Sequence Count ）	最初のシーケンスカウントが要求されたことを示します。成功すると、このシーケンスカウントから転送が開始されます。

コード	フィールド	製品説明
CTES	想定される終了シーケンス数	最後に要求されたシーケンスカウントを示します。成功すると、このシーケンスカウントを受信したときに転送が完了したとみなされます。
RSLT	転送開始ステータス	転送が開始された時点のステータス： SUCS ：転送が開始されました。

この監査メッセージは、 Content Block Identifier で識別されたとおりに単一のコンテンツでノード間のデータ転送処理が開始されたことを意味します。この処理では、「 Start Sequence Count 」から「 Expected End Sequence Count 」までのデータが要求されます。送信側と受信側のノードは、ノード ID によって識別されます。この情報を使用すると、システムのデータフローを追跡できます。ストレージ監査メッセージと組み合わせて使用すると、レプリカ数を検証できます。

StorageGRIDにおけるオブジェクト受信終了の**CBRE**監査メッセージ

このメッセージは、あるノードから別のノードへのコンテンツブロックの転送が完了したときに転送先のエンティティによって生成されます。

コード	フィールド	製品説明
CNID	接続識別子	ノード間のセッション / 接続の一意の識別子。
CBID	Content Block Identifier の略	転送されるコンテンツブロックの一意の識別子。
CTDR	転送方向（ Transfer Direction ）	CBID 転送がプッシュで開始されたかプルで開始されたかを示します。 PUSH ：転送処理は送信側エンティティによって要求されました。 PULL ：転送処理は受信側エンティティによって要求されました。
CTSR	ソースエンティティ	CBID 転送のソース（送信側）のノード ID 。
CTD	デスティネーションエンティティ	CBID 転送のデスティネーション（受信側）のノード ID 。
CTSS	開始シーケンスカウント（ Start Sequence Count ）	転送が開始されたシーケンスカウントを示します。
CTA	実際の終了シーケンス数	転送に成功した最後のシーケンスカウントを示します。実際の終了シーケンスカウントが開始シーケンスカウントと同じで、転送結果が成功しなかった場合、データは交換されませんでした。

コード	フィールド	製品説明
RSLT	転送結果	（送信側エンティティから見た）転送処理の結果： SUCS ：転送が正常に完了しました。要求されたすべてのシーケンスカウントが送信されました。 CONL ：転送中に接続が失われました CTMO ：接続の確立中または転送中に接続がタイムアウトしました UNRE ：デスティネーションノード ID に到達できません CRPT：破損したデータまたは無効なデータの受信が原因で転送が終了しました

この監査メッセージは、ノード間のデータ転送処理が完了したことを意味します。転送結果が成功した場合は、「 Start Sequence Count 」から「 Actual End Sequence Count 」にデータが転送されます。送信側と受信側のノードは、ノード ID によって識別されます。この情報を使用すると、システムのデータフローを追跡し、エラーを検出、集計、分析できます。ストレージ監査メッセージと組み合わせれば、レプリカ数の検証にも使用できます。

StorageGRIDでのオブジェクト送信開始の**CBSB**監査メッセージ

通常のシステム運用中は、データへのアクセスおよびデータのレプリケートと保持が行われる際に、異なるノード間でコンテンツブロックが継続的に転送されます。このメッセージは、あるノードから別のノードへのコンテンツブロックの転送が開始したときにソースエンティティによって生成されます。

コード	フィールド	製品説明
CNID	接続識別子	ノード間のセッション / 接続の一意の識別子。
CBID	Content Block Identifier の略	転送されるコンテンツブロックの一意の識別子。
CTDR	転送方向（ Transfer Direction ）	CBID 転送がプッシュで開始されたかプルで開始されたかを示します。 PUSH ：転送処理は送信側エンティティによって要求されました。 PULL ：転送処理は受信側エンティティによって要求されました。
CTSR	ソースエンティティ	CBID 転送のソース（送信側）のノード ID 。
CTD	デスティネーションエンティティ	CBID 転送のデスティネーション（受信側）のノード ID 。

コード	フィールド	製品説明
CTSS	開始シーケンスカウント（ Start Sequence Count ）	最初のシーケンスカウントが要求されたことを示します。成功すると、このシーケンスカウントから転送が開始されます。
CTES	想定される終了シーケンス数	最後に要求されたシーケンスカウントを示します。成功すると、このシーケンスカウントを受信したときに転送が完了したとみなされます。
RSLT	転送開始ステータス	転送が開始された時点のステータス： SUCS ：転送が開始されました。

この監査メッセージは、 Content Block Identifier で識別されたとおりに単一のコンテンツでノード間のデータ転送処理が開始されたことを意味します。この処理では、「 Start Sequence Count 」から「 Expected End Sequence Count 」までのデータが要求されます。送信側と受信側のノードは、ノード ID によって識別されます。この情報を使用すると、システムのデータフローを追跡できます。ストレージ監査メッセージと組み合わせて使用すると、レプリカ数を検証できます。

StorageGRIDにおけるオブジェクト送信終了の**CBSE**監査メッセージ

このメッセージは、あるノードから別のノードへのコンテンツブロックの転送が完了したときに転送元のエンティティによって生成されます。

コード	フィールド	製品説明
CNID	接続識別子	ノード間のセッション / 接続の一意の識別子。
CBID	Content Block Identifier の略	転送されるコンテンツブロックの一意の識別子。
CTDR	転送方向（ Transfer Direction ）	CBID 転送がプッシュで開始されたかプルで開始されたかを示します。 PUSH ：転送処理は送信側エンティティによって要求されました。 PULL ：転送処理は受信側エンティティによって要求されました。
CTSR	ソースエンティティ	CBID 転送のソース（送信側）のノード ID 。
CTD	デスティネーションエンティティ	CBID 転送のデスティネーション（受信側）のノード ID 。

コード	フィールド	製品説明
CTSS	開始シーケンスカウント（ Start Sequence Count ）	転送が開始されたシーケンスカウントを示します。
CTA	実際の終了シーケンス数	転送に成功した最後のシーケンスカウントを示します。実際の終了シーケンスカウントが開始シーケンスカウントと同じで、転送結果が成功しなかった場合、データは交換されませんでした。
RSLT	転送結果	（送信側エンティティから見た）転送処理の結果： SUCS ：転送が正常に完了しました。要求されたすべてのシーケンスカウントが送信されました。 CONL ：転送中に接続が失われました CTMO ：接続の確立中または転送中に接続がタイムアウトしました UNRE ：デスティネーションノード ID に到達できません CRPT：破損したデータまたは無効なデータの受信が原因で転送が終了しました

この監査メッセージは、ノード間のデータ転送処理が完了したことを意味します。転送結果が成功した場合は、「 Start Sequence Count 」から「 Actual End Sequence Count 」にデータが転送されます。送信側と受信側のノードは、ノード ID によって識別されます。この情報を使用すると、システムのデータフローを追跡し、エラーを検出、集計、分析できます。ストレージ監査メッセージと組み合わせれば、レプリカ数の検証にも使用できます。

StorageGRIDのクロスグリッドレプリケーション要求の**CGRR**監査メッセージ

このメッセージは、StorageGRID がグリッドフェデレーション接続内のバケット間でオブジェクトをレプリケートするためにグリッド間レプリケーション処理を試行したときに生成されます。

コード	フィールド	製品説明
CSIZ	オブジェクトサイズ	オブジェクトのサイズ（バイト）。 CSIZ属性はStorageGRID 11.8で導入されました。そのため、StorageGRID 11.7から11.8へのアップグレードにまたがるグリッド間レプリケーション要求で、オブジェクトの合計サイズが不正確になることがあります。
S3AI	S3テナントアカウントID	オブジェクトのレプリケート元のバケットを所有するテナントアカウントのID。

コード	フィールド	製品説明
GFID	グリッドフェデレーション接続ID	グリッド間レプリケーションに使用されているグリッドフェデレーション接続のID。
オペー	CGR操作	クロスグリッドレプリケーション処理が試行されたタイプ。 • 0 =オブジェクトをレプリケートします • 1 =マルチパートオブジェクトをレプリケートします • 2 =削除マーカーを複製します
S3BK	S3バケット	S3 バケット名。
S3KY	S3 キー	バケット名を除く S3 キーの名前。
VSID	バージョン ID	レプリケートされていたオブジェクトの特定のバージョンのバージョンID。
RSLT	結果コード	成功（SUCS）または一般エラー（GERR）を返します。

StorageGRIDにおける空のバケットオブジェクトの削除に関する**EBDL**監査メッセージ

すべてのオブジェクトを削除中のバケット内のオブジェクトがILMスキャナによって削除されました（空のバケット処理を実行中）。

コード	フィールド	製品説明
CSIZ	オブジェクトサイズ	オブジェクトのサイズ（バイト）。
パス	S3バケット/キー	S3バケット名とS3キー名。
SEGC	コンテナUUID	セグメント化されたオブジェクトのコンテナのUUID。この値は、オブジェクトがセグメント化されている場合にのみ使用できます。
UUID	Universally Unique Identifier の略	StorageGRID システム内でのオブジェクトの識別子。
RSLT	削除処理の結果	イベント、プロセス、またはトランザクションの結果。該当しないメッセージの場合は、誤ってフィルタリングされないように SUCS ではなく NONE が使用されます。

StorageGRIDにおける空のバケットリクエストに対するEBKR監査メッセージ

このメッセージは、ユーザが、空のバケットをオンまたはオフにする（バケットオブジェクトを削除する、またはオブジェクトの削除を停止する）要求を送信したことを示しています。

コード	フィールド	製品説明
bUID	バケットUUID	バケットID。
EBJS	空のバケットJSON設定	現在の空のバケットの設定を表すJSONが格納されます。
S3AI	S3テナントアカウントID	要求を送信したユーザのテナントアカウント ID 。空の値は匿名アクセスであることを示します。
S3BK	S3 バケット	S3 バケット名。

StorageGRIDにおける消失訂正符号化データの欠落に関するECMC監査メッセージ

この監査メッセージは、イレイジャーコーディングされたデータフラグメントの欠落がシステムで検出されたことを示します。

コード	フィールド	製品説明
VCMC	VCS ID を入力します	欠落しているチャンクが含まれている VCS の名前。
MCID	チャンク ID	欠落しているイレイジャーコーディングフラグメントの識別子。
RSLT	結果	このフィールドの値は「 NONE 」です。RSLT は必須のメッセージフィールドですが、このメッセージには該当しません。このメッセージがフィルタリングされないように、「 UCS 」ではなく「 none 」が使用されます。

StorageGRIDの破損した消去符号化データに関するECOC監査メッセージ

この監査メッセージは、イレイジャーコーディングされたデータフラグメントの破損がシステムで検出されたことを示します。

コード	フィールド	製品説明
Vcco	VCS ID を入力します	破損したチャンクが含まれている VCS の名前。

コード	フィールド	製品説明
VLID	ボリュームID	破損したイレイジャーコーディングフラグメントが含まれている RangeDB ボリューム。
CCID	チャンク ID	破損したイレイジャーコーディングフラグメントの識別子。
RSLT	結果	このフィールドの値は「 NONE 」です。RSLT は必須のメッセージフィールドですが、このメッセージには該当しません。このメッセージがフィルタリングされないように、「 UCS 」ではなく「 none 」が使用されます。

StorageGRIDにおけるセキュリティ認証失敗に関する**ETAF**監査メッセージ

このメッセージは、 Transport Layer Security （ TLS ）を使用した接続試行が失敗した場合に生成されます。

コード	フィールド	製品説明
CNID	接続識別子	認証が失敗した TCP / IP 接続の一意のシステム識別子。
RUID	ユーザ ID	リモートユーザの ID を表すサービスに依存する識別子。
RSLT	理由コード	失敗の理由： SCNI ：セキュアな接続を確立できませんでした。 CERM ：証明書がありません。 CERT ：証明書が無効です。 CERE ：証明書が期限切れです。 CERR ：証明書が取り消されています。 CSGN ：証明書の署名が無効です。 CSGU ：証明書の署名者が不明です。 UCRM ：ユーザクレデンシャルがありません。 UCRI ：ユーザクレデンシャルが無効です。 UCRU ：ユーザのクレデンシャルが拒否されました。 TOUT ：認証がタイムアウトしました。

TLS を使用するセキュアなサービスへの接続が確立されると、サービスに組み込まれている TLS プロファイルおよびその他のロジックを使用してリモートエンティティのクレデンシャルが検証されます。無効、想定

外、許可されていない証明書またはクレデンシャルが原因でこの認証が失敗すると、監査メッセージがログに記録されます。これにより、不正アクセスやその他のセキュリティ関連の接続問題を照会できます。

このメッセージは、リモートエンティティの設定が正しくない場合や、無効または許可されていないクレデンシャルをシステムに提示しようとした場合に生成されることがあります。この監査メッセージを監視して、システムへの不正なアクセス試行を検出する必要があります。

StorageGRIDにおけるGNDS登録のGNRG監査メッセージ

CMN サービスは、 StorageGRID システムで CMN サービスに関する情報を更新または登録したときにこの監査メッセージを生成します。

コード	フィールド	製品説明
RSLT	結果	更新リクエストの結果： • SUCS ：成功しました • SUNV ：サービスを使用できません • GERR ：その他の失敗
GNID	ノードID	更新要求を開始したサービスのノード ID 。
GNTP	デバイスタイプ	グリッドノードのデバイスタイプ（ LDR サービスの場合は BLDR など）。
GNDV	デバイスモデルのバージョン	DMDL バンドル内のグリッドノードのデバイスモデルバージョンを識別する文字列。
GNGP	グループ	グリッドノードが属するグループ（リンクコストとサービス - クエリランキングのコンテキストで）。
GNIA	IP アドレス	グリッドノードの IP アドレス。

このメッセージは、グリッドノードがグリッドノードバンドル内の自身のエントリを更新するたびに生成されます。

StorageGRIDにおけるGNDS登録解除に関するGNUR監査メッセージ

CMN サービスは、 StorageGRID システムから CMN サービスに関する情報の登録を解除したときにこの監査メッセージを生成します。

コード	フィールド	製品説明
RSLT	結果	更新リクエストの結果： • SUCS ：成功しました • SUNV ：サービスを使用できません • GERR ：その他の失敗
GNID	ノードID	更新要求を開始したサービスのノード ID 。

StorageGRIDで終了したグリッドタスクの**GTED**監査メッセージ

この監査メッセージは、 CMN サービスが指定されたグリッドタスクの処理を完了し、タスクを Historical テーブルに移動したことを示します。結果が SUCS 、 ABRT 、 ROLF のいずれかである場合は、対応する Grid Task Started 監査メッセージも生成されます。それ以外の結果は、このグリッドタスクの処理が開始されなかったことを示します。

コード	フィールド	製品説明
TSID	タスクID	このフィールドは、生成されたグリッドタスクを一意に識別します。また、グリッドタスクをライフサイクル全体にわたって管理できます。 • 注： * タスク ID は、グリッドタスクが送信された時点ではなく、生成された時点で割り当てられます。特定のグリッドタスクを複数回送信することができます。この場合、送信済み、開始、および終了の監査メッセージを一意にリンクするためのタスク ID フィールドでは不十分です。
RSLT	結果	グリッドタスクの最終ステータス： • SUCS ：グリッドタスクが正常に完了しました。 • ABRT：グリッドタスクはロールバックエラーなしで終了しました。 • Rolf：グリッドタスクは終了し、ロールバックプロセスを完了できませんでした。 • CANC ：グリッドタスクは開始前にユーザによってキャンセルされました。 • EXPR ：グリッドタスクは開始前に期限切れとなりました。 • IVLD ：グリッドタスクは無効でした。 • AUTH ：グリッドタスクは許可されていませんでした。 • DUPL ：グリッドタスクは重複として拒否されました。

StorageGRIDで開始されたグリッドタスクのGTST監査メッセージ

この監査メッセージは、 CMN サービスが指定されたグリッドタスクの処理を開始したことを示します。この監査メッセージは、内部の Grid Task Submission サービスによって開始されて自動アクティブ化用に選択されているグリッドタスクの Grid Task Submitted メッセージの直後に生成されます。Pending テーブルに送信されるグリッドタスクの場合、このメッセージはユーザがグリッドタスクを開始するときに生成されます。

コード	フィールド	製品説明
TSID	タスクID	このフィールドは、生成されたグリッドタスクを一意に識別します。また、タスクをライフサイクル全体にわたって管理できます。 • 注： * タスク ID は、グリッドタスクが送信された時点ではなく、生成された時点で割り当てられます。特定のグリッドタスクを複数回送信することができます。この場合、送信済み、開始、および終了の監査メッセージを一意にリンクするためのタスク ID フィールドでは不十分です。
RSLT	結果	結果。このフィールドの値は 1 つだけです。 • SUCS ：グリッドタスクが正常に開始されました。

StorageGRIDで送信されたグリッドタスクのGTSU監査メッセージ

この監査メッセージは、グリッドタスクが CMN サービスに送信されたことを示します。

コード	フィールド	製品説明
TSID	タスクID	生成されたグリッドタスクを一意に識別し、タスクをライフサイクル全体にわたって管理できるようにします。 • 注： * タスク ID は、グリッドタスクが送信された時点ではなく、生成された時点で割り当てられます。特定のグリッドタスクを複数回送信することができます。この場合、送信済み、開始、および終了の監査メッセージを一意にリンクするためのタスク ID フィールドでは不十分です。
ttyp	タスクタイプ（ Task Type ）	グリッドタスクのタイプ。
Tver	タスクバージョン	グリッドタスクのバージョンを示す番号。
TDSC	タスクの説明	グリッドタスクの判読可能な概要 。

コード	フィールド	製品説明
付加価値を提供します	タイムスタンプ後の有効な値	グリッドタスクの有効期間の開始時間（ UNIX 時間 1970 年 1 月 1 日からの UINT64 マイクロ秒数）。
VBTS	タイムスタンプの前に有効です	グリッドタスクの有効期間の終了時間（ UNIX 時間 1970 年 1 月 1 日からの UINT64 マイクロ秒数）。
TsRC	ソース	タスクのソース： • TXTB ：グリッドタスクは、 StorageGRID システム経由で署名付きテキストブロックとして送信されました。 • GRID ：グリッドタスクは、内部の Grid Task Submission サービス経由で送信されました。
ACTV	アクティベーションタイプ	アクティブ化のタイプ： • Auto ：グリッドタスクは自動でアクティブ化されます。 • PEND ：グリッドタスクは Pending テーブルに追加されました。TXTB ソースの場合はこのタイプのみです。
RSLT	結果	送信結果： • SUCS ：グリッドタスクは正常に送信されました。 • FAIL ：タスクは Historical テーブルに直接移動されました。

StorageGRIDにおける**ILM**開始削除の**IDEL**監査メッセージ

このメッセージは、 ILM によってオブジェクトを削除する処理が開始された場合に生成されます。

IDEL メッセージは、次のいずれかの状況で生成されます。

- * 準拠 S3 バケット内のオブジェクト * ：このメッセージは、保持期間が経過したために ILM によってオブジェクトの自動削除処理が開始された場合に生成されます（自動削除設定が有効になっていて、リーガルホールドがオフの場合）。
- 非準拠**S3**バケット内のオブジェクトの場合。このメッセージは、現在オブジェクトに適用されている配置手順がアクティブなILMポリシーにないためにオブジェクトを削除する処理がILMによって開始された場合に生成されます。

コード	フィールド	製品説明
CBID	Content Block Identifier の略	オブジェクトの CBID 。

コード	フィールド	製品説明
CMPA	準拠：自動削除	準拠 S3 バケット内のオブジェクトのみが対象。0 （ false ）または 1 （ true ）。バケットがリーガルホールドの対象である場合を除き、保持期間の終了時に準拠オブジェクトを自動的に削除するかどうかを示します。
テンプレート	コンプライアンス：リーガルホールド	準拠 S3 バケット内のオブジェクトのみが対象。0 （ false ）または 1 （ true ）。バケットが現在リーガルホールドの対象であるかどうかを示します。
CMPR	準拠：保持期間	準拠 S3 バケット内のオブジェクトのみが対象。オブジェクトの保持期間の長さ（分）。
CTME	準拠：取り込み時間	準拠 S3 バケット内のオブジェクトのみが対象。オブジェクトの取り込み時間。この値に保持期間を分単位で追加することで、オブジェクトをバケットから削除できるタイミングを判断できます。
dmrk	マーカーバージョン ID を削除します	バージョン管理されたバケットからオブジェクトを削除するときに作成された削除マーカーのバージョン ID 。バケットに対する処理では、このフィールドは指定されません。
CSIZ	コンテンツのサイズ	オブジェクトのサイズ（バイト）。
LOCS	場所	StorageGRID システム内のオブジェクトデータの格納場所。オブジェクトに場所がない場合（削除されている場合など）、 LOCS の値は "" です。 CLEC：イレイジャーコーディングオブジェクトの場合、オブジェクトのデータに適用されているイレイジャーコーディングプロファイルIDとイレイジャーコーディンググループID。 CLDI ：レプリケートされたオブジェクトの場合、オブジェクトの場所の LDR ノード ID とボリューム ID 。 CLNL ：オブジェクトデータがアーカイブされている場合は、オブジェクトの場所の ARC ノード ID 。
パス	S3バケット/キー	S3バケット名とS3キー名。
RSLT	結果	ILM 処理の結果。 SUCS ： ILM 処理が成功しました。

コード	フィールド	製品説明
ルール	ルールラベル（ Rules Label ）	• 保持期間が経過したために準拠 S3 バケット内のオブジェクトが自動的に削除されている場合、このフィールドは空白になります。 • 現在オブジェクトに適用される配置手順がないためにオブジェクトが削除されている場合、このフィールドには、オブジェクトに適用された最後の ILM ルールの判読可能なラベルが表示されます。
SgRP	サイト（グループ）	オブジェクトが存在する場合は、指定したサイトで削除されています。このサイトは、オブジェクトが取り込まれたサイトではありません。
UUID	Universally Unique Identifier の略	StorageGRID システム内でのオブジェクトの識別子。
VSID	バージョン ID	削除されたオブジェクトの特定のバージョンのバージョン ID 。バージョン管理に対応していないバケット内のバケットおよびオブジェクトに対する処理には、このフィールドは含まれません。

StorageGRIDで上書きされたオブジェクトのクリーンアップに関する**LKCU**監査メッセージ

このメッセージは、ストレージスペースを解放するためにクリーンアップが必要な上書きされたオブジェクトを StorageGRID が削除した場合に生成されます。オブジェクトがすでに含まれているパスにS3クライアントがオブジェクトを書き込むと、オブジェクトが上書きされます。削除処理は自動的にバックグラウンドで実行されます。

コード	フィールド	製品説明
CSIZ	コンテンツのサイズ	オブジェクトのサイズ（バイト）。
LTYP	クリーンアップのタイプ	_ 内部使用のみ。 _
LUID （ LUID ）	オブジェクト UUID が削除されました	削除されたオブジェクトの識別子。
パス	S3バケット/キー	S3バケット名とS3キー名。
SEGC	コンテナUUID	セグメント化されたオブジェクトのコンテナのUUID。この値は、オブジェクトがセグメント化されている場合にのみ使用できます。
UUID	Universally Unique Identifier の略	まだ存在するオブジェクトの ID 。この値は、オブジェクトが削除されていない場合にのみ使用できます。

StorageGRIDでリークされたオブジェクトのクリーンアップに関するLKDM監査メッセージ

このメッセージは、リークしたチャンクがクリーンアップまたは削除された場合に生成されます。チャンクは、レプリケートオブジェクトまたはイレイジャーコーディングオブジェクトの一部です。

コード	フィールド	製品説明
CLOC	チャンクの場所	削除されたリークされたチャンクのファイルパス。

CTYP	チャンクタイプ	チャンクのタイプ：
		
		`ec: Erasure-coded object chunk`
		
		`repl: Replicated object chunk`

LTYP	リークタイプ	次の5種類の漏れが検出されます。
		
		`object_leaked: Object doesn’t exist in the grid`
		
		`location_leaked: Object exists in the grid, but found location doesn’t belong to object`
		
		`mup_seg_leaked: Multipart upload was stopped or not completed, and the segment/part was left out`
		
		`segment_leaked: Parent UUID/CBID (associated container object) is valid but doesn’t contain this segment`
		
		`no_parent: Container object is deleted, but object segment was left out and not deleted`

CTIM	チャンクの作成時間	リークされたチャンクが作成された時刻。
UUID	Universally Unique Identifier の略	チャンクが属するオブジェクトの識別子。
CBID	Content Block Identifier の略	リークされたチャンクが属するオブジェクトのCBID。
CSIZ	コンテンツのサイズ	チャンクのサイズ（バイト）。

StorageGRIDで失われたオブジェクトのコピー場所に関するLLST監査メッセージ

このメッセージは、オブジェクトコピー（レプリケートまたはイレイジャーコーディン

グ）の場所が見つからない場合に生成されます。

コード	フィールド	製品説明
CBIL	CBID	影響を受ける CBID 。
ECPR	イレイジャーコーディングプロファイル	イレイジャーコーディングされたオブジェクトデータ用。使用されているイレイジャーコーディングプロファイルのID。
LTYP	保管場所タイプ	CLDI （ Online ）：レプリケートされたオブジェクトデータ用 CLEC （ Online ）：イレイジャーコーディングされたオブジェクトデータ用 CLNL （ Nearline ）：アーカイブされたレプリケートオブジェクトデータ用
NOID	ソースノード ID	場所が失われたノード ID 。
PCLD	レプリケートオブジェクトへのパス	損失オブジェクトデータのディスクの場所への完全なパス。LTYP の値が CLDI （つまりレプリケートオブジェクトの場合）の場合にのみ返されます。 形式は次のとおりです。 `/var/local/rangedb/2/p/13/13/00oJs6X%{h{U)SeUFxE@`
RSLT	結果	常に NONE 。RSLT は必須のメッセージフィールドですが、このメッセージには該当しません。このメッセージがフィルタリングされないように、 SUCS ではなく NONE が使用されます。
TsRC	トリガ元	USER ：ユーザがトリガーしました SYST ：システムがトリガーされました
UUID	Universally Unique ID の略	StorageGRID システムでの該当オブジェクトの識別子。

StorageGRIDの管理APIリクエストのMGAU監査メッセージ

管理カテゴリでは、管理 API に対するユーザ要求がログに記録されます。有効なAPI URIに対するGET要求またはHEAD要求ではないすべてのHTTP要求で、ユーザ名、IP、および要求タイプを含む応答がAPIに対して記録されます。無効なAPI URI（/api/v3-authorizeなど）や有効なAPI URIへの無効な要求はログに記録されません。

コード	フィールド	製品説明
MDIP	宛先 IP アドレス	サーバ（デスティネーション）の IP アドレス。
MDNA	ドメイン名	ホストのドメイン名。
MPAT	要求パス	要求のパス。
MPQP	要求クエリパラメータ	要求のクエリパラメータ。
MRBD の略	リクエストの本文	要求の本文の内容。応答の本文はデフォルトでログに記録されますが、要求の本文は応答の本文が空の特定のケースでログに記録されます。応答の本文には次の情報が含まれていないため、それぞれの POST メソッドの要求本文から取り込まれます。 • ユーザ名とアカウント ID ： * POST authorize * • 新しいサブネット設定： * POST /grid/grid-networks/update * • 新しい NTP サーバ： * POST /grid/ntp-servers /update * に含まれています • 運用停止されたサーバ ID は、 * POST /grid/servers/decommission * に記載されています • 注： * 機密情報は、削除（ S3 アクセスキーなど）またはアスタリスクでマスク（パスワードなど）されます。
検査	要求メソッド	HTTP 要求メソッド： • 投稿 • PUT • 削除 • パッチ
MRSC	応答コード	応答コード。
MRSP	応答の本文	デフォルトでは、応答の内容（応答の本文）がログに記録されます。 • 注： * 機密情報は、削除（ S3 アクセスキーなど）またはアスタリスクでマスク（パスワードなど）されます。
MSIP	送信元 IP アドレス	クライアント（送信元）の IP アドレス。
MUUN	ユーザのURN	要求を送信したユーザの URN （ Uniform Resource Name ）。

コード	フィールド	製品説明
RSLT	結果	成功（ SUCS ）、またはバックエンドによって報告されたエラーが返されます。

StorageGRIDでシステムが検出した紛失オブジェクトに関する**OLST**監査メッセージ

このメッセージは、DDSサービスがStorageGRID システム内でオブジェクトのコピーを見つけることができない場合に生成されます。

コード	フィールド	製品説明
CBID	Content Block Identifier の略	損失オブジェクトの CBID 。
NOID	ノードID	損失オブジェクトが最後に確認された直接またはニアラインの場所（該当する場合）。ボリューム情報がない場合は、ノード ID だけでボリューム ID がないケースもあります。
パス	S3バケット/キー	S3バケット名とS3キー名（該当する場合）。
RSLT	結果	このフィールドの値は NONE です。RSLT は必須のメッセージフィールドですが、このメッセージには該当しません。このメッセージがフィルタリングされないように、 SUCS ではなく NONE が使用されます。
UUID	Universally Unique ID の略	StorageGRID システム内の損失オブジェクトの識別子。
ヴォル	ボリュームID	損失オブジェクトが最後に確認された場所のストレージノードのボリュームID（該当する場合）。

StorageGRIDで**ILM**ルールが満たされた場合の**ORLM**監査メッセージ

このメッセージは、 ILM ルールで指定されたとおりにオブジェクトが格納およびコピーされた場合に生成されます。

ORLM メッセージは、ポリシー内の別のルールで高度なフィルタ「オブジェクトサイズ」が使用されている場合に、オブジェクトがデフォルトの Make 2 Copies ルールによって格納されたときには生成されません。

コード	フィールド	製品説明
bUID	バケットヘッダー	バケット ID フィールド。内部処理に使用されます。STAT が PRGD の場合にのみ表示されます。
CBID	Content Block Identifier の略	オブジェクトの CBID 。

コード	フィールド	製品説明
CSIZ	コンテンツのサイズ	オブジェクトのサイズ（バイト）。
LOCS	場所	StorageGRID システム内のオブジェクトデータの格納場所。オブジェクトに場所がない場合（削除されている場合など）、 LOCS の値は "" です。 CLEC：イレイジャーコーディングオブジェクトの場合、オブジェクトのデータに適用されているイレイジャーコーディングプロファイルIDとイレイジャーコーディンググループID。 CLDI ：レプリケートされたオブジェクトの場合、オブジェクトの場所の LDR ノード ID とボリューム ID 。 CLNL ：オブジェクトデータがアーカイブされている場合は、オブジェクトの場所の ARC ノード ID 。
パス	S3バケット/キー	S3バケット名とS3キー名。
RSLT	結果	ILM 処理の結果。 SUCS ： ILM 処理が成功しました。
ルール	ルールラベル（ Rules Label ）	このオブジェクトに適用されている ILM ルールの判読可能なラベル。
SEGC	コンテナUUID	セグメント化されたオブジェクトのコンテナのUUID。この値は、オブジェクトがセグメント化されている場合にのみ使用できます。
SGCB	コンテナCBID	セグメント化されたオブジェクトのコンテナのCBID。この値はセグメント化されたオブジェクトとマルチパートオブジェクトに対してのみ使用できます。
統計	ステータス	ILM 処理のステータス。 DONE ：オブジェクトに対する ILM 処理が完了しました。 DFER ： ILM によって再評価されるようオブジェクトがマークされました。 PRGD ：オブジェクトが StorageGRID システムから削除されました。 NLOC ：オブジェクトデータを StorageGRID システムで検出できなくなります。このステータスは、オブジェクトデータのすべてのコピーが欠落または破損していることを示している可能性があります。

コード	フィールド	製品説明
UUID	Universally Unique Identifier の略	StorageGRID システム内でのオブジェクトの識別子。
VSID	バージョン ID	バージョン管理されたバケットで作成された新しいオブジェクトのバージョン ID 。バージョン管理に対応していないバケット内のバケットおよびオブジェクトに対する処理には、このフィールドは含まれません。

ORLM監査メッセージは、1つのオブジェクトに対して複数回発行できます。たとえば、次のいずれかのイベントが発生するたびに発行されます。

- オブジェクトが対応する ILM ルールを無期限に満たしたとき。
- オブジェクトが対応する ILM ルールを一時的に満たしたとき。
- オブジェクトが ILM ルールによって削除されたとき。
- バックグラウンド検証プロセスにより、レプリケートされたオブジェクトデータのコピーが破損していることが検出されたとき。StorageGRID システムは、破損したオブジェクトを交換するために ILM 評価を実行します。

関連情報

- "オブジェクトの取り込みトランザクション"
- "オブジェクトの削除トランザクション"

StorageGRIDにおけるオブジェクトの上書きに関する**OVWR**監査メッセージ

このメッセージは、外部（クライアントが要求した）処理によって、あるオブジェクトが別のオブジェクトで上書きされた場合に生成されます。

コード	フィールド	製品説明
CBID	Content Block Identifier （新規）	新しいオブジェクトの CBID 。
CSIZ	前のオブジェクトサイズ	上書きされるオブジェクトのサイズ（バイト単位）。
OCBD	コンテンツブロック識別子（前のもの）	既存のオブジェクトの CBID 。
UUID	Universally Unique ID （新規）	StorageGRID システム内での新しいオブジェクトの識別子。

コード	フィールド	製品説明
OUID	Universally Unique ID （旧）	StorageGRID システム内での以前のオブジェクトの識別子。
パス	S3オブジェクトパス	前のオブジェクトと新しいオブジェクトの両方に使用されるS3オブジェクトのパス
RSLT	結果コード	Object Overwrite トランザクションの結果。常に次の結果になります。 SUCS ：成功しました
SgRP	サイト（グループ）	上書きされたオブジェクトがある場合は指定したサイトで削除されています。このサイトは、上書きされたオブジェクトが取り込まれたサイトではありません。

StorageGRIDにおける**S3 Select**リクエストの**S3SL**監査メッセージ

このメッセージは、S3 Select要求がクライアントに返されたあとに完了を記録します。S3SLメッセージには、エラーメッセージとエラーコードの詳細を含めることができます。要求は成功しなかった可能性があります。

コード	フィールド	製品説明
BYSC	スキャンされたバイト数	ストレージノードからスキャン（受信）されたバイト数。 オブジェクトが圧縮されている場合、BYSCとBYPRは異なる可能性があります。オブジェクトが圧縮されている場合、BYSCは圧縮されたバイト数を持ち、BYPRは解凍後のバイト数になります。
BYPR	処理されたバイト数	処理されたバイト数。S3 Selectジョブで実際に処理または処理された「スキャンされたバイト数」のバイト数を示します。
BYRT	返されたバイト数	S3 Selectジョブがクライアントに返されたバイト数。
レポート	処理されたレコード	S3 Selectジョブがストレージノードから受信したレコードまたは行の数。
RERT	レコードが返されました	S3 Selectジョブがクライアントに返されたレコードまたは行の数。
JOFI	ジョブは終了しました	S3 Selectジョブの処理が完了したかどうかを示します。これがfalseの場合、ジョブは完了しませんでした。エラーフィールドにはデータが含まれている可能性があります。クライアントに結果が一部しか表示されていない場合や、結果がまったく表示されない場合があります。

コード	フィールド	製品説明
リード	Request ID	S3 Select要求の識別子。
EXTM	実行時間	S3 Selectジョブが完了するまでにかかった時間（秒）。
ERMG	エラーメッセージ	S3 Selectジョブが生成されたことを示すエラーメッセージ。
アーティ	エラータイプ	S3 Selectジョブが生成したエラータイプ。
エルスト	スタックトレースエラー	S3 Selectジョブが生成したエラーStacktrace。
S3BK	S3バケット	S3 バケット名。
S3AK	S3 アクセスキー ID （要求の送信者）	要求を送信したユーザのS3アクセスキーID。
S3AI	S3 テナントアカウント ID （要求の送信者）	要求を送信したユーザのテナントアカウント ID 。
S3KY	S3 キー	バケット名を除く S3 キーの名前。

StorageGRIDにおけるセキュリティ監査の無効化に関する**SADD**監査メッセージ

このメッセージは、発信元のサービス（ノードID）が監査メッセージのログ記録を無効にしたことを示しています。StorageGRID は監査メッセージの収集および配信を停止しました。

コード	フィールド	製品説明
AETM	enable メソッド	監査を無効にするために使用されたメソッド。
EUN	ユーザー名	監査ログを無効にするコマンドを実行したユーザ名。
RSLT	結果	このフィールドの値は NONE です。RSLT は必須のメッセージフィールドですが、このメッセージには該当しません。このメッセージがフィルタリングされないように、 SUCS ではなく NONE が使用されます。

このメッセージは、以前は有効だったロギングが現在は無効になっていることを示します。一般には、システムのパフォーマンスを向上させるために一括取り込み時にのみ実行される処理です。一括アクティビティ後に監査がリストアされ（ SADE ）、監査を無効にする機能は永続的にブロックされます。

StorageGRIDにおけるセキュリティ監査有効化のためのSADE監査メッセージ

このメッセージは、発信元のサービス（ノードID）が監査メッセージのログ記録を復元したことを示しています。StorageGRID は監査メッセージの収集と配信を再開しました。

コード	フィールド	製品説明
AETM	enable メソッド	監査を有効にするために使用されたメソッド。
EUN	ユーザー名	監査ログを有効にするコマンドを実行したユーザ名。
RSLT	結果	このフィールドの値は NONE です。RSLT は必須のメッセージフィールドですが、このメッセージには該当しません。このメッセージがフィルタリングされないように、 SUCS ではなく NONE が使用されます。

このメッセージは、以前は無効（ SADD ）だったロギングが現在は有効になっていることを示します。一般には、システムのパフォーマンスを向上させるために一括取り込み時にのみ実行される処理です。一括アクティビティ後に監査がリストアされ、監査を無効にする機能は永続的にブロックされます。

StorageGRIDのオブジェクトストアコミットのSCMT監査メッセージ

グリッドコンテンツは、コミット（永続的に格納）されるまでは、使用可能にならず、格納済みとして認識されません。永続的に格納されたコンテンツは、ディスクに完全に書き込まれ、関連する整合性チェックに合格したコンテンツです。このメッセージは、コンテンツブロックがストレージにコミットされたときに生成されます。

コード	フィールド	製品説明
CBID	Content Block Identifier の略	永続的ストレージにコミットされたコンテンツブロックの一意の識別子。
RSLT	結果コード	オブジェクトがディスクに格納された時点のステータス： SUCS ：オブジェクトが正常に格納されました。

このメッセージは、コンテンツブロックの格納と検証がすべて完了し、要求可能な状態になったことを意味します。この機能を使用すると、システム内のデータフローを追跡できます。

StorageGRIDのS3 DELETEトランザクションのSDEL監査メッセージ

S3クライアントがDELETEトランザクションを実行すると、指定したオブジェクトまたはバケットを削除する要求、またはバケット/オブジェクトサブリソースを削除する要求が送信されます。このメッセージは、トランザクションが成功した場合にサーバによって出力されます。

コード	フィールド	製品説明
ASRS	引き受けたロールセッションURN	引き受けたロールセッションの一意の識別子。 S3 リクエストが AssumeRole リクエストからの一時的なセキュリティ認証情報を使用している場合にのみ存在します。
ASRU	引き受けたロール URN	引き受けたロールの一意の識別子。 S3 リクエストが AssumeRole リクエストからの一時的なセキュリティ認証情報を使用している場合にのみ存在します。
CBID	Content Block Identifier の略	要求されたコンテンツブロックの一意の識別子。CBID が不明な場合、このフィールドは 0 に設定されます。バケットに対する処理では、このフィールドは指定されません。
CNCH	整合性制御ヘッダー	要求に Consistency-Control HTTP 要求ヘッダーが存在する場合は、その値。
CNID	接続識別子	TCP / IP 接続の一意のシステム識別子。
CSIZ	コンテンツサイズ（ Content Size ）	削除されたオブジェクトのサイズ（バイト単位）。バケットに対する処理では、このフィールドは指定されません。
dmrk	マーカーバージョン ID を削除します	バージョン管理されたバケットからオブジェクトを削除するときに作成された削除マーカーのバージョン ID 。バケットに対する処理では、このフィールドは指定されません。
GFID	グリッドフェデレーション接続ID	グリッド間レプリケーションの削除要求に関連付けられたグリッドフェデレーション接続の接続ID。デスティネーショングリッドの監査ログにのみ含まれます。
gfsaだ	GridフェデレーションのソースアカウントID	グリッド間レプリケーションの削除要求を行うソースグリッド上のテナントのアカウントID。デスティネーショングリッドの監査ログにのみ含まれます。

コード	フィールド	製品説明
HTRH	HTTP 要求ヘッダー	設定時に選択した、ログに記録される HTTP 要求ヘッダーの名前と値のリスト。 `X-Forwarded-For`は、要求に含まれていて、値が要求の送信元IPアドレス（SAIP監査フィールド）と異なる場合に自動的に追加されます`X-Forwarded-For`。 `x-amz-bypass-governance-retention`は、要求に含まれている場合は自動的に追加されます。
MTME	最終変更時刻	オブジェクトが最後に変更された日時を示す Unix タイムスタンプ（マイクロ秒）。
RSLT	結果コード	DELETEトランザクションの結果。常に次の結果になります。 SUCS ：成功しました
S3AI	S3 テナントアカウント ID （要求の送信者）	要求を送信したユーザのテナントアカウント ID 。空の値は匿名アクセスであることを示します。
S3AK	S3 アクセスキー ID （要求の送信者）	要求を送信したユーザのハッシュ済み S3 アクセスキー ID 。空の値は匿名アクセスであることを示します。
S3BK	S3 バケット	S3 バケット名。
S3KY	S3 キー	バケット名を除く S3 キーの名前。バケットに対する処理では、このフィールドは指定されません。
S3SR	S3 サブリソース	必要に応じて、処理対象のバケットまたはオブジェクトサブリソース。
SACC	S3 テナントアカウント名（要求の送信者）	要求を送信したユーザのテナントアカウントの名前。匿名の要求の場合は空です。
saip	IP アドレス（要求送信者）	要求を送信したクライアントアプリケーションの IP アドレス。
SBAC	S3 テナントアカウント名（バケット所有者）	バケット所有者のテナントアカウント名。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。

コード	フィールド	製品説明
SBAI	S3 テナントアカウント ID （バケット所有者）	ターゲットバケットの所有者のテナントアカウント ID 。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。
SgRP	サイト（グループ）	オブジェクトが存在する場合は、指定したサイトで削除されています。このサイトは、オブジェクトが取り込まれたサイトではありません。
サスペンション	S3 ユーザの URN （要求の送信者）	要求を送信しているユーザのテナントアカウント ID とユーザ名。ローカルユーザまたは LDAP ユーザです。例： `urn:sgws:identity::03393893651506583485:root` 匿名の要求の場合は空です。
時間	時間	要求の合計処理時間（マイクロ秒）。
TLIP	信頼できるロードバランサの IP アドレス	要求が信頼できるレイヤ 7 ロードバランサによってルーティングされた場合は、ロードバランサの IP アドレス。
UUDM	削除マーカーのUniversally Unique Identifier（汎用一意識別子）	削除マーカーの識別子。監査ログメッセージでは、UUDMまたはUUIDのいずれかを指定します。UUDMはオブジェクトの削除要求によって作成された削除マーカー、UUIDはオブジェクトを示します。
UUID	Universally Unique Identifier の略	StorageGRID システム内でのオブジェクトの識別子。
VSID	バージョン ID	削除されたオブジェクトの特定のバージョンのバージョン ID 。バージョン管理に対応していないバケット内のバケットおよびオブジェクトに対する処理には、このフィールドは含まれません。

StorageGRIDのS3 GETトランザクションのSGET監査メッセージ

S3クライアントがGETトランザクションを実行すると、オブジェクトを読み出したりバケット内のオブジェクトをリストしたり、バケット/オブジェクトサブリソースを削除したりする要求が送信されます。このメッセージは、トランザクションが成功した場合にサーバによって出力されます。

コード	フィールド	製品説明
ASRS	引き受けたロールセッションURN	引き受けたロールセッションの一意の識別子。 S3 リクエストが AssumeRole リクエストからの一時的なセキュリティ認証情報を使用している場合にのみ存在します。
ASRU	引き受けたロール URN	引き受けたロールの一意の識別子。 S3 リクエストが AssumeRole リクエストからの一時的なセキュリティ認証情報を使用している場合にのみ存在します。
CBID	Content Block Identifier の略	要求されたコンテンツブロックの一意の識別子。CBID が不明な場合、このフィールドは 0 に設定されます。バケットに対する処理では、このフィールドは指定されません。
CNCH	整合性制御ヘッダー	要求に Consistency-Control HTTP 要求ヘッダーが存在する場合は、その値。
CNID	接続識別子	TCP / IP 接続の一意のシステム識別子。
CSIZ	コンテンツサイズ（ Content Size ）	読み出されたオブジェクトのサイズ（バイト単位）。バケットに対する処理では、このフィールドは指定されません。
HTRH	HTTP 要求ヘッダー	設定時に選択した、ログに記録される HTTP 要求ヘッダーの名前と値のリスト。 `X-Forwarded-For`は、要求に含まれていて、値が要求の送信元IPアドレス（SAIP監査フィールド）と異なる場合に自動的に追加されます`X-Forwarded-For`。
能力	ListObjectsV2	_v2 format_responseが要求されました。詳細については、を参照してください "AWS ListObjectsV2"。GET Bucket処理の場合のみ。
NCHD	子の数	キーと共通のプレフィックスが含まれます。GET Bucket処理の場合のみ。
rang	範囲の読み取り	範囲読み取り処理の場合のみ。この要求によって読み取られたバイトの範囲を示します。スラッシュ（ / ）の後の値は、オブジェクト全体のサイズを示します。
RSLT	結果コード	GETトランザクションの結果。常に次の結果になります。 SUCS ：成功しました

コード	フィールド	製品説明
S3AI	S3 テナントアカウント ID （要求の送信者）	要求を送信したユーザのテナントアカウント ID 。空の値は匿名アクセスであることを示します。
S3AK	S3 アクセスキー ID （要求の送信者）	要求を送信したユーザのハッシュ済み S3 アクセスキー ID 。空の値は匿名アクセスであることを示します。
S3BK	S3 バケット	S3 バケット名。
S3KY	S3 キー	バケット名を除く S3 キーの名前。バケットに対する処理では、このフィールドは指定されません。
S3SR	S3 サブリソース	必要に応じて、処理対象のバケットまたはオブジェクトサブリソース。
SACC	S3 テナントアカウント名（要求の送信者）	要求を送信したユーザのテナントアカウントの名前。匿名の要求の場合は空です。
saip	IP アドレス（要求送信者）	要求を送信したクライアントアプリケーションの IP アドレス。
SBAC	S3 テナントアカウント名（バケット所有者）	バケット所有者のテナントアカウント名。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。
SBAI	S3 テナントアカウント ID （バケット所有者）	ターゲットバケットの所有者のテナントアカウント ID 。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。
サスペンション	S3 ユーザの URN （要求の送信者）	要求を送信しているユーザのテナントアカウント ID とユーザ名。ローカルユーザまたは LDAP ユーザです。例： `urn:sgws:identity::03393893651506583485:root` 匿名の要求の場合は空です。
時間	時間	要求の合計処理時間（マイクロ秒）。
TLIP	信頼できるロードバランサの IP アドレス	要求が信頼できるレイヤ 7 ロードバランサによってルーティングされた場合は、ロードバランサの IP アドレス。
TRNC	切り捨てられる、または切り捨てられない	すべての結果が返された場合はfalseに設定されます。より多くの結果が返される場合はtrueに設定します。GET Bucket処理の場合のみ。

コード	フィールド	製品説明
UUID	Universally Unique Identifier の略	StorageGRID システム内でのオブジェクトの識別子。
VSID	バージョン ID	要求されたオブジェクトの特定のバージョンのバージョン ID 。バージョン管理に対応していないバケット内のバケットおよびオブジェクトに対する処理には、このフィールドは含まれません。

StorageGRIDにおける**S3 HEAD**操作の**SHEA**監査メッセージ

S3 クライアントが HEAD 操作を発行すると、オブジェクトまたはバケットの存在を確認し、オブジェクトに関するメタデータを取得する要求が行われます。操作が成功した場合、このメッセージはサーバーによって発行されます。

コード	フィールド	製品説明
ASRS	引き受けたロールセッションURN	引き受けたロールセッションの一意の識別子。 S3 リクエストが AssumeRole リクエストからの一時的なセキュリティ認証情報を使用している場合にのみ存在します。
ASRU	引き受けたロール URN	引き受けたロールの一意の識別子。 S3 リクエストが AssumeRole リクエストからの一時的なセキュリティ認証情報を使用している場合にのみ存在します。
CBID	Content Block Identifier の略	要求されたコンテンツブロックの一意の識別子。CBID が不明な場合、このフィールドは 0 に設定されます。バケットに対する処理では、このフィールドは指定されません。
CNID	接続識別子	TCP / IP 接続の一意のシステム識別子。
CSIZ	コンテンツサイズ（ Content Size ）	チェックしたオブジェクトのサイズ（バイト単位）。バケットに対する処理では、このフィールドは指定されません。
HTRH	HTTP 要求ヘッダー	設定時に選択した、ログに記録される HTTP 要求ヘッダーの名前と値のリスト。 `X-Forwarded-For`は、要求に含まれていて、値が要求の送信元IPアドレス（SAIP監査フィールド）と異なる場合に自動的に追加されます`X-Forwarded-For`。

コード	フィールド	製品説明
RSLT	結果コード	GETトランザクションの結果。常に次の結果になります。 SUCS ：成功しました
S3AI	S3 テナントアカウント ID （要求の送信者）	要求を送信したユーザのテナントアカウント ID 。空の値は匿名アクセスであることを示します。
S3AK	S3 アクセスキー ID （要求の送信者）	要求を送信したユーザのハッシュ済み S3 アクセスキー ID 。空の値は匿名アクセスであることを示します。
S3BK	S3 バケット	S3 バケット名。
S3KY	S3 キー	バケット名を除く S3 キーの名前。バケットに対する処理では、このフィールドは指定されません。
SACC	S3 テナントアカウント名（要求の送信者）	要求を送信したユーザのテナントアカウントの名前。匿名の要求の場合は空です。
saip	IP アドレス（要求送信者）	要求を送信したクライアントアプリケーションの IP アドレス。
SBAC	S3 テナントアカウント名（バケット所有者）	バケット所有者のテナントアカウント名。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。
SBAI	S3 テナントアカウント ID （バケット所有者）	ターゲットバケットの所有者のテナントアカウント ID 。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。
サスペンション	S3 ユーザの URN （要求の送信者）	要求を送信しているユーザのテナントアカウント ID とユーザ名。ローカルユーザまたは LDAP ユーザです。例： `urn:sgws:identity::03393893651506583485:root` 匿名の要求の場合は空です。
時間	時間	要求の合計処理時間（マイクロ秒）。
TLIP	信頼できるロードバランサの IP アドレス	要求が信頼できるレイヤ 7 ロードバランサによってルーティングされた場合は、ロードバランサの IP アドレス。

コード	フィールド	製品説明
UUID	Universally Unique Identifier の略	StorageGRID システム内でのオブジェクトの識別子。
VSID	バージョン ID	要求されたオブジェクトの特定のバージョンのバージョン ID 。バージョン管理に対応していないバケット内のバケットおよびオブジェクトに対する処理には、このフィールドは含まれません。

StorageGRID における **S3 POST** トランザクションの **SPOS** 監査メッセージ

S3 クライアントが POST Object 要求を実行すると、トランザクションが成功した場合にサーバによってこのメッセージが生成されます。

コード	フィールド	製品説明
ASRS	引き受けたロールセッションURN	引き受けたロールセッションの一意の識別子。 S3 リクエストが AssumeRole リクエストからの一時的なセキュリティ認証情報を使用している場合にのみ存在します。
ASRU	引き受けたロール URN	引き受けたロールの一意の識別子。 S3 リクエストが AssumeRole リクエストからの一時的なセキュリティ認証情報を使用している場合にのみ存在します。
CBID	Content Block Identifier の略	要求されたコンテンツブロックの一意の識別子。CBID が不明な場合、このフィールドは 0 に設定されます。
CNCH	整合性制御ヘッダー	要求に Consistency-Control HTTP 要求ヘッダーが存在する場合は、その値。
CNID	接続識別子	TCP / IP 接続の一意のシステム識別子。
CSIZ	コンテンツサイズ（ Content Size ）	読み出されたオブジェクトのサイズ（バイト単位）。

コード	フィールド	製品説明
HTRH	HTTP 要求ヘッダー	設定時に選択した、ログに記録される HTTP 要求ヘッダーの名前と値のリスト。 `X-Forwarded-For`は、要求に含まれていて、値が要求の送信元IPアドレス（SAIP監査フィールド）と異なる場合に自動的に追加されます`X-Forwarded-For`。 （SPOSでは想定されません）。
RSLT	結果コード	RestoreObject要求の結果。常に次の結果になります。 SUCS ：成功しました
S3AI	S3 テナントアカウント ID （要求の送信者）	要求を送信したユーザのテナントアカウント ID 。空の値は匿名アクセスであることを示します。
S3AK	S3 アクセスキー ID （要求の送信者）	要求を送信したユーザのハッシュ済み S3 アクセスキー ID 。空の値は匿名アクセスであることを示します。
S3BK	S3 バケット	S3 バケット名。
S3KY	S3 キー	バケット名を除く S3 キーの名前。バケットに対する処理では、このフィールドは指定されません。
S3SR	S3 サブリソース	必要に応じて、処理対象のバケットまたはオブジェクトサブリソース。 S3 Select処理の場合は、を「select」に設定します。
SACC	S3 テナントアカウント名（要求の送信者）	要求を送信したユーザのテナントアカウントの名前。匿名の要求の場合は空です。
saip	IP アドレス（要求送信者）	要求を送信したクライアントアプリケーションの IP アドレス。
SBAC	S3 テナントアカウント名（バケット所有者）	バケット所有者のテナントアカウント名。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。

コード	フィールド	製品説明
SBAI	S3 テナントアカウント ID （バケット所有者）	ターゲットバケットの所有者のテナントアカウント ID 。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。
SRCF	サブリソースの設定	リストア情報。
サスペンション	S3 ユーザの URN （要求の送信者）	要求を送信しているユーザのテナントアカウント ID とユーザ名。ローカルユーザまたは LDAP ユーザです。例： `urn:sgws:identity::03393893651506583485:root` 匿名の要求の場合は空です。
時間	時間	要求の合計処理時間（マイクロ秒）。
TLIP	信頼できるロードバランサの IP アドレス	要求が信頼できるレイヤ 7 ロードバランサによってルーティングされた場合は、ロードバランサの IP アドレス。
UUID	Universally Unique Identifier の略	StorageGRID システム内でのオブジェクトの識別子。
VSID	バージョン ID	要求されたオブジェクトの特定のバージョンのバージョン ID 。バージョン管理に対応していないバケット内のバケットおよびオブジェクトに対する処理には、このフィールドは含まれません。

StorageGRIDにおける**S3 PUT**トランザクションの**SPUT**監査メッセージ

S3クライアントがPUTトランザクションを実行すると、新しいオブジェクトまたはバケットを作成する要求、またはバケット/オブジェクトサブリソースを削除する要求が送信されます。このメッセージは、トランザクションが成功した場合にサーバによって出力されます。

コード	フィールド	製品説明
ASRS	引き受けたロールセッションURN	引き受けたロールセッションの一意の識別子。 S3 リクエストが AssumeRole リクエストからの一時的なセキュリティ認証情報を使用している場合にのみ存在します。
ASRU	引き受けたロール URN	引き受けたロールの一意の識別子。 S3 リクエストが AssumeRole リクエストからの一時的なセキュリティ認証情報を使用している場合にのみ存在します。

コード	フィールド	製品説明
CBID	Content Block Identifier の略	要求されたコンテンツブロックの一意の識別子。CBID が不明な場合、このフィールドは 0 に設定されます。バケットに対する処理では、このフィールドは指定されません。
CMP	コンプライアンス設定	バケットの作成時に使用された準拠設定（要求に存在する場合）（最初の1024文字に切り詰められます）。
CNCH	整合性制御ヘッダー	要求に Consistency-Control HTTP 要求ヘッダーが存在する場合は、その値。
CNID	接続識別子	TCP / IP 接続の一意のシステム識別子。
CSIZ	コンテンツサイズ（ Content Size ）	読み出されたオブジェクトのサイズ（バイト単位）。バケットに対する処理では、このフィールドは指定されません。
GFID	グリッドフェデレーション接続ID	グリッド間レプリケーションPUT要求に関連付けられたグリッドフェデレーション接続の接続ID。デスティネーショングリッドの監査ログにのみ含まれます。
gfsaだ	Gridフェデレーションのソースアカウント ID	グリッド間レプリケーションPUT要求を行うソースグリッド上のテナントのアカウントID。デスティネーショングリッドの監査ログにのみ含まれます。
HTRH	HTTP 要求ヘッダー	設定時に選択した、ログに記録される HTTP 要求ヘッダーの名前と値のリスト。 `X-Forwarded-For`は、要求に含まれていて、値が要求の送信元IPアドレス（SAIP監査フィールド）と異なる場合に自動的に追加されます`X-Forwarded-For`。 `x-amz-bypass-governance-retention`は、要求に含まれている場合は自動的に追加されます。
LKEN	オブジェクトロックが有効になりました	要求ヘッダーの値 `x-amz-bucket-object-lock-enabled`（要求に含まれている場合）。
LKLH	オブジェクトロックリーガルホールド	要求ヘッダーの値 `x-amz-object-lock-legal-hold`（PutObject要求に存在する場合）。

コード	フィールド	製品説明
LKMD	オブジェクトロック保持モード	要求ヘッダーの値 `x-amz-object-lock-mode`（PutObject要求に存在する場合）。
LKRU	オブジェクトロック終了日まで保持	要求ヘッダーの値 `x-amz-object-lock-retain-until-date`（PutObject要求に存在する場合）。値は、オブジェクトが取り込まれた日から100年以内に制限されます。
MTME	最終変更時刻	オブジェクトが最後に変更された日時を示す Unix タイムスタンプ（マイクロ秒）。
RSLT	結果コード	PUTトランザクションの結果。常に次の結果になります。 SUCS ：成功しました
S3AI	S3 テナントアカウント ID （要求の送信者）	要求を送信したユーザのテナントアカウント ID 。空の値は匿名アクセスであることを示します。
S3AK	S3 アクセスキー ID （要求の送信者）	要求を送信したユーザのハッシュ済み S3 アクセスキー ID 。空の値は匿名アクセスであることを示します。
S3BK	S3 バケット	S3 バケット名。
S3KY	S3 キー	バケット名を除く S3 キーの名前。バケットに対する処理では、このフィールドは指定されません。
S3SR	S3 サブリソース	必要に応じて、処理対象のバケットまたはオブジェクトサブリソース。
SACC	S3 テナントアカウント名（要求の送信者）	要求を送信したユーザのテナントアカウントの名前。匿名の要求の場合は空です。
saip	IP アドレス（要求送信者）	要求を送信したクライアントアプリケーションの IP アドレス。
SBAC	S3 テナントアカウント名（バケット所有者）	バケット所有者のテナントアカウント名。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。
SBAI	S3 テナントアカウント ID （バケット所有者）	ターゲットバケットの所有者のテナントアカウント ID 。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。

コード	フィールド	製品説明
SRCF	サブリソースの設定	新しいサブリソース設定（最初の 1024 文字に切り詰められます）。
サスペンション	S3 ユーザの URN （要求の送信者）	要求を送信しているユーザのテナントアカウント ID とユーザ名。ローカルユーザまたは LDAP ユーザです。例： `urn:sgws:identity::03393893651506583485:root` 匿名の要求の場合は空です。
時間	時間	要求の合計処理時間（マイクロ秒）。
TLIP	信頼できるロードバランサの IP アドレス	要求が信頼できるレイヤ 7 ロードバランサによってルーティングされた場合は、ロードバランサの IP アドレス。
ULID	ID をアップロードします	CompleteMultipartUpload処理のSPUTメッセージにのみ含まれます。すべてのパーツがアップロードされ、アセンブルされたことを示します。
UUID	Universally Unique Identifier の略	StorageGRID システム内でのオブジェクトの識別子。
VSID	バージョン ID	バージョン管理されたバケットで作成された新しいオブジェクトのバージョン ID 。バージョン管理に対応していないバケット内のバケットおよびオブジェクトに対する処理には、このフィールドは含まれません。
VSST	バージョン管理の状態	バケットの新しいバージョン管理状態。「enabled」または「suspended」の2つの状態が使用されます。オブジェクトに対する処理には、このフィールドは含まれません。

StorageGRIDにおけるオブジェクトストア削除の**SREM**監査メッセージ

このメッセージは、コンテンツが永続的ストレージから削除され、通常の API でアクセスできなくなった場合に表示されます。

コード	フィールド	製品説明
CBID	Content Block Identifier の略	永続的ストレージから削除されたコンテンツブロックの一意の識別子。
RSLT	結果コード	コンテンツ削除処理の結果を示します。次の値のみが定義されています。 SUCS ：コンテンツが永続的ストレージから削除されました

この監査メッセージは、指定されたコンテンツブロックがノードから削除され、直接要求できなくなったこと

を意味します。このメッセージを使用して、システム内の削除されたコンテンツのフローを追跡できます。

StorageGRIDのS3メタデータ更新のSUPD監査メッセージ

このメッセージは、 S3 クライアントが取り込まれたオブジェクトのメタデータを更新したときに S3 API によって生成されます。このメッセージは、メタデータの更新が成功した場合にサーバによって出力されます。

コード	フィールド	製品説明
CBID	Content Block Identifier の略	要求されたコンテンツブロックの一意の識別子。CBID が不明な場合、このフィールドは 0 に設定されます。バケットに対する処理では、このフィールドは指定されません。
CNCH	整合性制御ヘッダー	バケットの準拠設定の更新時に要求に Consistency-Control HTTP 要求ヘッダーが存在する場合は、その値。
CNID	接続識別子	TCP / IP 接続の一意のシステム識別子。
CSIZ	コンテンツサイズ（ Content Size ）	読み出されたオブジェクトのサイズ（バイト単位）。バケットに対する処理では、このフィールドは指定されません。
HTRH	HTTP 要求ヘッダー	設定時に選択した、ログに記録される HTTP 要求ヘッダーの名前と値のリスト。 `X-Forwarded-For`は、要求に含まれていて、値が要求の送信元IPアドレス（SAIP監査フィールド）と異なる場合に自動的に追加されます`X-Forwarded-For`。
RSLT	結果コード	GETトランザクションの結果。常に次の結果になります。 SUCS ：成功しました
S3AI	S3 テナントアカウント ID （要求の送信者）	要求を送信したユーザのテナントアカウント ID 。空の値は匿名アクセスであることを示します。
S3AK	S3 アクセスキー ID （要求の送信者）	要求を送信したユーザのハッシュ済み S3 アクセスキー ID 。空の値は匿名アクセスであることを示します。
S3BK	S3 バケット	S3 バケット名。

コード	フィールド	製品説明
S3KY	S3 キー	バケット名を除く S3 キーの名前。バケットに対する処理では、このフィールドは指定されません。
SACC	S3 テナントアカウント名（要求の送信者）	要求を送信したユーザのテナントアカウントの名前。匿名の要求の場合は空です。
saip	IP アドレス（要求送信者）	要求を送信したクライアントアプリケーションの IP アドレス。
SBAC	S3 テナントアカウント名（バケット所有者）	バケット所有者のテナントアカウント名。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。
SBAI	S3 テナントアカウント ID （バケット所有者）	ターゲットバケットの所有者のテナントアカウント ID 。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。
サスペンション	S3 ユーザの URN （要求の送信者）	要求を送信しているユーザのテナントアカウント ID とユーザ名。ローカルユーザまたは LDAP ユーザです。例： `urn:sgws:identity::03393893651506583485:root` 匿名の要求の場合は空です。
時間	時間	要求の合計処理時間（マイクロ秒）。
TLIP	信頼できるロードバランサの IP アドレス	要求が信頼できるレイヤ 7 ロードバランサによってルーティングされた場合は、ロードバランサの IP アドレス。
UUID	Universally Unique Identifier の略	StorageGRID システム内でのオブジェクトの識別子。
VSID	バージョン ID	メタデータが更新されたオブジェクトの特定のバージョンのバージョン ID 。バージョン管理に対応していないバケット内のバケットおよびオブジェクトに対する処理には、このフィールドは含まれません。

StorageGRIDにおけるオブジェクトストア検証失敗の**SVRF**監査メッセージ

このメッセージは、コンテンツブロックが検証プロセスに失敗したときに生成されます。レプリケートされたオブジェクトデータがディスクに対して読み書きされるたびに、要求元ユーザに送信されるデータがシステムにもともと取り込まれたデータと同一であることを確認するために複数の検証チェックと整合性チェックが実行されます。これらのチェックのいずれかが失敗した場合、破損したレプリケートオブジェクトデータ

は再び読み出されないように自動的に隔離されます。

コード	フィールド	製品説明
CBID	Content Block Identifier の略	検証に失敗したコンテンツブロックの一意の識別子。
RSLT	結果コード	検証失敗のタイプ： CRCF ：巡回冗長検査（ CRC ）が失敗しました。 HMAC ：ハッシュベースのメッセージ認証コード（ HMAC ）チェックが失敗しました。 EHSH ：暗号化されたコンテンツハッシュが想定外です。 PHSH ：元のコンテンツハッシュが想定外です。 SEQC ：ディスク上のデータシーケンスが正しくありません。 PERR ：ディスクファイルの構造が無効です。 DERR ：ディスクエラーです。 FNAM ：ファイル名が無効です。

このメッセージは注意深く監視する必要があります。コンテンツ検証の失敗は、ハードウェア障害の兆候を示している可能性があります。

メッセージをトリガーした処理を確認するには、 AMID （ Module ID ）フィールドの値を参照してください。たとえば、 SVFY はバックグラウンド検証である Storage Verifier モジュールによってメッセージが生成されたことを示し、 STOR はコンテンツの読み出しによってメッセージがトリガーされたことを示します。

StorageGRID の不明なオブジェクトストアコンテンツに関する **SVRU** 監査メッセージ

LDR サービスのストレージコンポーネントは、オブジェクトストア内のレプリケートされたオブジェクトデータのすべてのコピーを継続的にスキャンします。このメッセージは、レプリケートされたオブジェクトデータの不明または想定外のコピーがオブジェクトストアで検出されて隔離ディレクトリに移動されたときに生成されます。

コード	フィールド	製品説明
FPTH	ファイルパス	想定外のオブジェクトコピーのファイルパス。
RSLT	結果	このフィールドの値は「 NONE 」です。RSLT は必須のメッセージフィールドですが、このメッセージには該当しません。このメッセージがフィルタリングされないように、「 UCS 」ではなく「 none 」が使用されます。

SVRU：Object Store Verify Unknown監査メッセージは注意深く監視する必要があります。オブジェクトストアでオブジェクトデータの想定外のコピーが検出されたことを意味します。ハードウェア障害の兆候を示している可能性があるため、この状況をすぐに調査してこれらのコピーが作成された方法を特定する必要があります。

StorageGRIDにおける正常なノード停止のSYSD監査メッセージ

サービスが正常に停止されると、シャットダウンが要求されたことを示すためにこのメッセージが生成されます。監査メッセージキューはシャットダウン前にクリアされないため、通常、このメッセージは次回の再起動後にのみ送信されます。サービスが再起動していない場合は、シャットダウンシーケンスの最初に送信された SYST メッセージを確認します。

コード	フィールド	製品説明
RSLT	シャットダウンをクリーニングします	シャットダウンのタイプ： SUCS ：システムはクリーンシャットダウンされました。

このメッセージが示すのはレポート元のサービスの停止のみで、ホストサーバの停止については示されません。SYSDのRSLTは、「クリーン」シャットダウンによってのみ生成されるため、「ダーティー」シャットダウンを示すことはできません。

StorageGRIDでノードが停止する際のSYST監査メッセージ

サービスが正常に停止された場合、シャットダウンが要求され、サービスがシャットダウンシーケンスを開始したことを示すために、このメッセージが生成されます。SYSTは、サービスが再起動される前にシャットダウンが要求されたかどうかを判断するために使用できます（通常、サービスが再起動された後に送信されるSYSDとは異なります）。

コード	フィールド	製品説明
RSLT	シャットダウンをクリーニングします	シャットダウンのタイプ： SUCS ：システムはクリーンシャットダウンされました。

このメッセージが示すのはレポート元のサービスの停止のみで、ホストサーバの停止については示されません。SYSTメッセージのRSLTコードは、「クリーン」シャットダウンによってのみ生成されるため、「ダーティー」シャットダウンを示すことはできません。

StorageGRIDでノードのSYSU監査メッセージが開始されます

サービスが再起動されると、前回のシャットダウンがクリーン（コマンドによるもの）か不規則（想定外）かを示すためにこのメッセージが生成されます。

コード	フィールド	製品説明
RSLT	シャットダウンをクリーニングします	シャットダウンのタイプ： SUCS ：システムはクリーンシャットダウンされました。 DSDN ：システムはクリーンシャットダウンされませんでした。 VRGN ：サーバインストール（または再インストール）後の初めての起動です。

このメッセージが示すのはレポート元のサービスの起動のみで、ホストサーバの起動については示されません。このメッセージは、次の場合に使用できます。

- 監査証跡における不連続を検出します。
- サービスが処理中に失敗していないかどうかを確認します（ StorageGRID システムの分散によってこれらのエラーが隠されることがあります）。失敗したサービスは、 Server Manager によって自動的に再開されます。

StorageGRIDシステムの容量または機能を拡張します

StorageGRIDシステムの拡張について学ぶ

運用を中断することなく、 StorageGRIDシステムを拡張して容量や機能を増やす方法について説明します。既存のストレージ ノードにストレージ ボリュームを追加したり、既存のサイトに新しいグリッド ノードを追加したり、新しいサイトを追加したりできます。

グリッド ノードを展開する前に、アクティブなデータ修復ジョブがないことを確認する必要があります。修復に失敗した場合は、修復を再起動して完了させてから、廃止または拡張手順を実行する必要があります。。"データ修復ジョブを確認します" 。

StorageGRIDを拡張すると、次の項目を追加できます。

- ストレージボリュームからストレージノードへ
- キソンノサイトヘノアタラシイクリツトノオト
- まったく新しいサイト

拡張を実施する理由によって、追加する必要がある各タイプの新しいノードの数と、追加する新しいノードの場所が決まります。たとえば、ストレージ容量の拡張、メタデータ容量の追加、冗長性や新機能の追加を行う場合、ノード要件は異なります。

実行している拡張のタイプに応じた手順に従います。

グリッドノードの追加

1. の手順に従います"既存のサイトへのグリッドノードの追加"。
2. "サブネットの更新"です。
3. グリッドノードの導入：
   - "アプライアンス"
   - "VMware"
   - "Linux"

> 「Linux」は、RHEL、Ubuntu、または Debian のデプロイメントを指します。サポートされているバージョンのリストについては、 "NetApp Interoperability Matrix Tool（IMT）" 。

1. "拡張の実行"です。
2. "拡張したシステムの設定"です。

ストレージボリュームを追加します

の手順に従います"ストレージノードへのストレージボリュームの追加"。

新しいサイトを追加します

1. の手順に従います"新しいサイトを追加しています"。
2. "サブネットの更新"です。
3. グリッドノードの導入：
   - "アプライアンス"
   - "VMware"
   - "Linux"

> 「Linux」は、RHEL、Ubuntu、または Debian のデプロイメントを指します。サポートされているバージョンのリストについては、 "NetApp Interoperability Matrix Tool（IMT）" 。

1. "拡張の実行"です。
2. "拡張したシステムの設定"です。

拡張計画

StorageGRIDにおける複製データの拡張計画

環境の情報ライフサイクル管理（ ILM ）ポリシーに、オブジェクトのレプリケートコピーを作成するルールが含まれている場合は、追加するストレージの量と、新しいストレージボリュームまたはストレージノードの追加先を検討する必要があります。

ストレージを追加する場所については、レプリケートコピーを作成する ILM ルールを確認してください。ILM ルールで複数のオブジェクトコピーが作成される場合は、オブジェクトコピーが作成されるそれぞれの場所に

ストレージを追加することを検討してください。簡単な例として、2サイトのグリッドがあり、各サイトにオブジェクトコピーを1つ作成するILMルールがある場合は、各サイトに移動してグリッドの全体的なオブジェクト容量を増やす必要があります"ストレージを追加します"。オブジェクトレプリケーションの詳細については、を参照してください"レプリケーションとは"。

パフォーマンス上の理由から、サイト間でストレージ容量と処理能力のバランスを維持することをお勧めします。そのため、この例では、各サイトに同じ数のストレージノードを追加するか、各サイトにストレージボリュームを追加する必要があります。

より複雑な ILM ポリシーで、バケット名などの条件に基づいてオブジェクトを別々の場所に配置するルールや、オブジェクトの場所を一定期間変更するルールが含まれている場合は、拡張に必要なストレージについての分析も似ていますが、より複雑です。

全体的なストレージ容量がどれだけ早く消費されるかを記録しておくと、拡張に必要なストレージ容量や、追加のストレージ容量が必要になる時期を把握するのに役立ちます。Grid Managerを使用して、次"ストレージ容量を監視してグラフ化"の操作を実行できます。

拡張のタイミングを計画するときは、追加のストレージの調達とインストールにどれくらいの時間がかかるかを考慮する必要があります。拡張計画を簡素化するには、既存のストレージ ノードの容量が 70% に達したときにストレージ ノードを追加することを検討してください。

StorageGRIDにおける消失訂正符号化（EC）データの拡張計画

イレイジャーコーディングコピーを作成するルールが ILM ポリシーに含まれている場合は、新しいストレージの追加場所と新しいストレージを追加するタイミングを計画する必要があります。追加するストレージの量や追加のタイミングによって、グリッドの使用可能なストレージ容量が左右される場合があります。

ストレージ拡張を計画するための最初の手順は、イレイジャーコーディングオブジェクトを作成する ILM ポリシーのルールを調べることです。StorageGRID はイレイジャーコーディングされた各オブジェクト用に _k+m_fragments を作成して各フラグメントを別のストレージノードに格納するため、拡張後にイレイジャーコーディングされた新しいデータ用のスペースを少なくとも -k +m_Storage ノードに確保する必要があります。イレイジャーコーディングプロファイルでサイト障害から保護されている場合は、各サイトにストレージを追加する必要があります。イレイジャーコーディングプロファイルの詳細については、を参照してください"イレイジャーコーディングスキームとは"。

追加する必要があるノードの数は、拡張を実施する時点での既存のノードの使用状況によっても異なります。

イレイジャーコーディングオブジェクト用のストレージ容量の追加に関する一般的な推奨事項

詳細な計算を行わない場合は、既存のストレージノードの容量が 70% に達した時点で各サイトに 2 つのストレージノードを追加できます。

この一般的な推奨事項は、単一サイトのグリッドとイレイジャーコーディングによってサイト障害から保護されるグリッドの両方で、広範なイレイジャーコーディングスキームに渡って合理的な結果を提供します。

この推奨事項につながった要因をよりよく理解したり、サイトのより正確な計画を作成したりするには、を参照してください"イレイジャーコーディングデータのリバランシングに関する考慮事項"。お客様の状況に合わせてカスタマイズした推奨事項については、ネットアッププロフェッショナルサービスのコンサルタントにお問い合わせください。

StorageGRIDの拡張後の EC 再バランス調整について学ぶ

拡張を実行してストレージノードを追加し、ILMルールを使用してデータをイレイジャーコーディングする場合、使用しているイレイジャーコーディングスキームに対応する十分な数のストレージノードを追加できない場合は、イレイジャーコーディング（EC）のリバランシング手順の実行が必要になることがあります。

これらの考慮事項を確認したら、拡張を実行し、に移動して"ストレージノードの追加後にイレイジャーコーディングデータをリバランシングします"手順を実行します。

EC のリバランシングとは何ですか？

EC のリバランシングは、ストレージノードの拡張後に必要になる可能性がある StorageGRID 手順 です。手順 は、プライマリ管理ノードからコマンドラインスクリプトとして実行されます。ECのリバランシング手順を実行すると、StorageGRID はサイトの既存のストレージノードと新しく追加したストレージノードにイレイジャーコーディングフラグメントを再配分します。

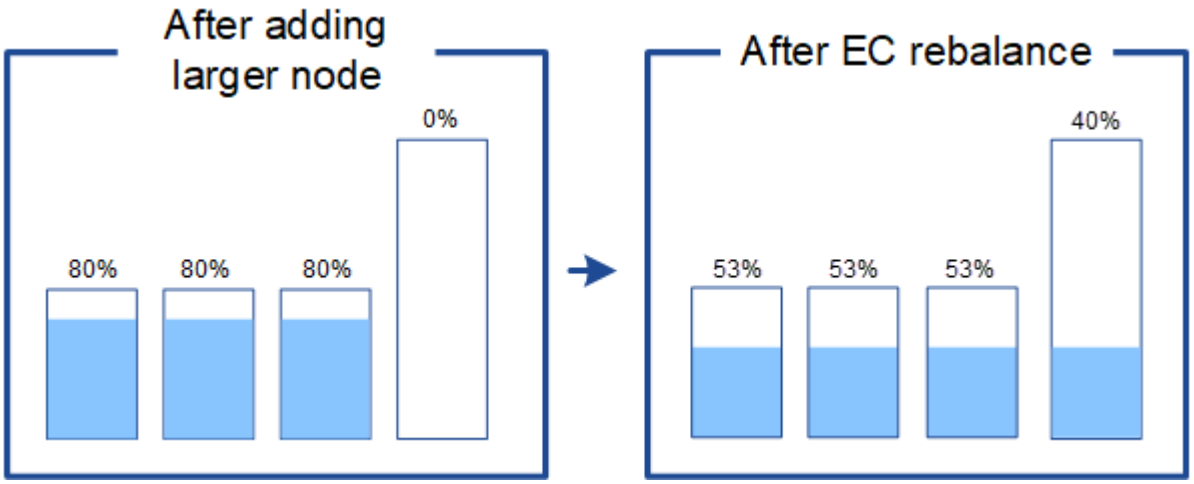
EC のリバランシング手順 ：

- イレイジャーコーディングされたオブジェクトデータのみを移動します。レプリケートされたオブジェクトデータは移動されません。
- サイト内のデータを再配布します。サイト間でデータを移動することはありません。
- サイトのすべてのストレージノードにデータを再配分します。ストレージボリューム内でデータが再配置されることはありません。
- 各ノードが同じ使用可能なスペースを持つように、データのバイトを分散させます。レプリケートされたデータが多いノードは、リバランス完了後にイレイジャーコーディングされたデータの保存量が少なくなる可能性があります。
- 各ノードの相対的な容量を考慮せずに、使用可能なスペースをストレージノード間で均等に再分配します。複製データも計算に含まれます。
- リバランス処理は、使用可能な領域がまだ均等に分配されていない場合でも、それ以上消去符号化されたデータを移動できなくなった時点で完了したとみなされます。
- 容量が80%以上使用されているストレージノード、またはメタデータ専用のストレージノードには、イレイジャーコーディングされたデータを配布しません。
- イレイジャーコーディングフラグメントの再配置に追加リソースが必要になると、ILM処理とS3クライアント処理のパフォーマンスが低下する可能性があります。

EC Rebalance 手順 が完了すると、次のようになります。

- イレイジャーコーディングデータは、利用可能なスペースが少ないストレージノードから利用可能なスペースが多いストレージノードに移動されます。
- イレイジャーコーディングオブジェクトのデータ保護は変更されません。
- 次の2つの理由により、ストレージノード間で使用済み（%）の値が異なる可能性があります。
  - レプリケートオブジェクトコピーは既存のノードのスペースを引き続き消費します。ECのリバランシング手順 では、レプリケートデータは移動されません。
  - 最終的にすべてのノードがほぼ同じ量の使用可能なスペースを持つことになるとしても、容量の大きいノードは容量の小さいノードに比べて相対的に使用率が低い可能性があります。

例えば、2+1 イレイジャーコーディング方式の場合、200 TB のノードが 3 つあり、それぞれが 80% まで使用されているとします（各ノードに 200 × 0.8 = 160 TB、サイト全体では 480 TB）。400 TB のノードを追加してリバランス手順を実行すると、すべての古いノードのイレイジャーコーディングされたデータ量はほぼ同じになります（106.66 TB、つまり 53% の使用率）。新しいノードには（160 TB のデータ、つまり 40% が使用される）データが格納されます。この場合、大きいノードの Used (%) は、小さいノードの Used (%) よりも低くなります。再バランス処理は、使用可能な領域のバランスが取れる前に完了します。これは、イレイジャーコーディング方式の制約を破ることなく、これ以上イレイジャーコーディングされたデータを移動できないためです。



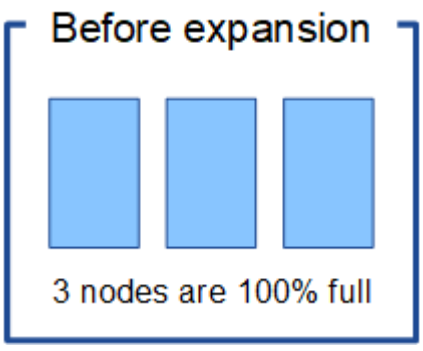
イレイジャーコーディングデータをリバランシングするタイミング

EC 再バランス手順では、既存の消去符号化データを再分配して、ノードがいっぱいになったり、いっぱいになったままにならないようにします。この手順により、サイト上で EC エンコーディングを続行できるようになります。

サイト上のデータ分布に懸念される偏りがあり、サイトに主に EC データが格納されている場合は、再バランス手順を実行します (複製されたデータは再バランスによって移動できないため)。

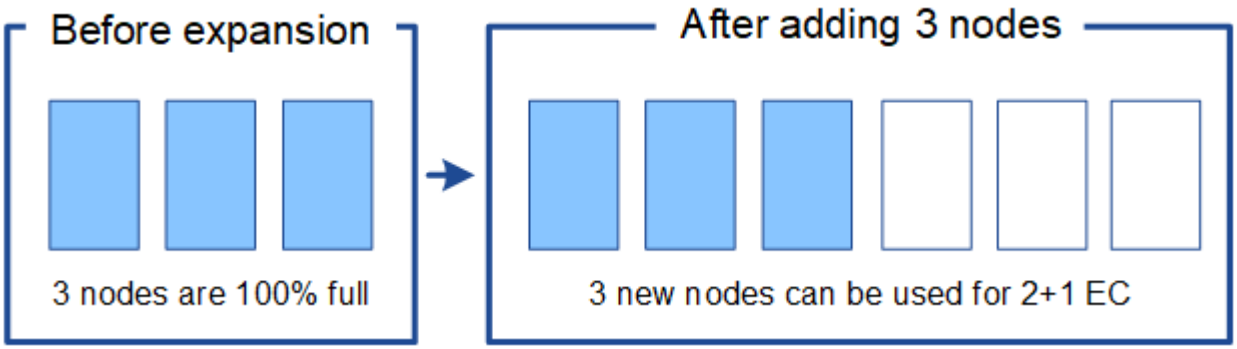
次のシナリオを考えてみましょう。

- StorageGRID は、 3 つのストレージノードで構成される単一サイトで実行されています。
- ILMポリシーでは、1.0MBを超えるすべてのオブジェクトに2+1のイレイジャーコーディングルールを使用し、サイズの小さいオブジェクトには2-copyレプリケーションルールを使用します。
- すべてのストレージノードが完全にいっぱいになりました。Low Object Storage *アラートがMajor重大度レベルでトリガーされました。



十分な数のノードを追加すれば、リバランスは不要です。

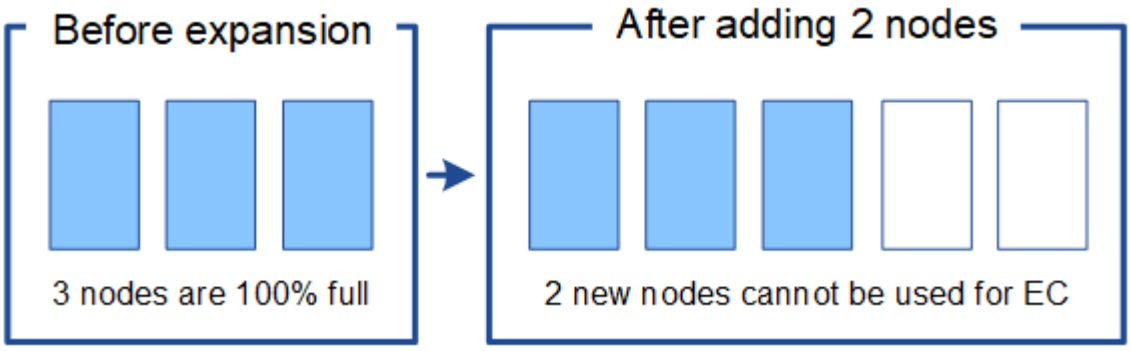
ECのリバランシングが不要な状況を把握するために、新しいストレージノードを3つ以上追加したとします。この場合、ECリバランシングを実行する必要はありません。元のストレージノードはフルのままですが、新しいオブジェクトは3つの新しいノードを2+1のイレイジャーコーディングに使用します。2つのデータフラグメントと1つのパリティフラグメントを別 々 のノードに格納できます。



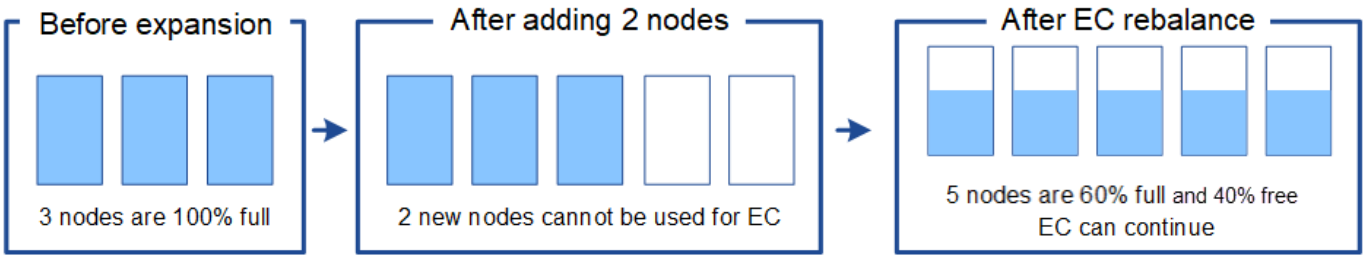
この場合、ECのリバランシング手順 は実行できますが、既存のイレイジャーコーディングデータを移動するとグリッドのパフォーマンスが一時的に低下し、クライアント処理に影響する可能性があります。

十分な数のノードを追加できない場合は、リバランシングが必要です

ECのリバランシングが必要な状況を把握するために、ストレージノードを3つではなく2つしか追加できないとします。2+1スキームでは、利用可能なスペースを確保するために少なくとも3つのストレージノードが必要であるため、空のノードを新しいイレイジャーコーディングデータに使用することはできません。



新しいストレージノードを利用するには、ECリバランス手順を実行する必要があります。この手順が実行されると、StorageGRID は既存の消去符号化データとパリティフラグメントを再分配し、サイト内のすべてのストレージノード間で使用可能な領域が均等に分配されるようにします。この例では、ECリバランス手順が完了すると、5つのノードすべてが60%使用済みとなり、使用可能な容量は40%になります。そして、すべてのストレージノードで2+1イレイジャーコーディング方式へのオブジェクトの取り込みを継続できます。



ECのリバランシングに関する推奨事項

次のステートメントの_all_が当てはまる場合、ECのリバランシングが必要になります。

- オブジェクトデータにイレイジャーコーディングを使用します。
- Low Object Storage * アラートがトリガーされました。このアラートは、ノードが 80% 以上フルであることを示します。
- 使用中のイレイジャーコーディングスキームに使用する十分な数の新しいストレージノードを追加できません。を参照して "イレイジャーコーディングオブジェクトのストレージ容量を追加します"
- ECのリバランシング手順の実行中は、S3クライアントの書き込み処理と読み取り処理のパフォーマンスが低下しても問題ありません。

ストレージノードをほぼ同じレベルに配置し、S3クライアントがECのリバランシング手順の実行中に書き込み処理と読み取り処理のパフォーマンス低下を許容できる場合は、必要に応じてECのリバランシング手順を実行できます。

EC のリバランシングが手順 と他のメンテナンスタスクと連携する仕組み

ECリバランシング手順 を実行するときに一部のメンテナンス手順を実行することはできません。

手順	**EC** のリバランシングで許可される手順 ？
追加の EC リバランシング手順	いいえ。 一度に実行できる EC のリバランシング手順 は 1 つだけです。
手順 の運用を停止 EC データの修復ジョブ	いいえ。 • EC Rebalance 手順 が実行されている間は、手順 または EC データの修復の運用を停止することはできません。 • ストレージノードが手順 を運用停止したり、 EC データの修復が実行されている間は、 EC のリバランシング手順 を開始できません。
Expansion 手順 の略	いいえ。 拡張時に新しいストレージノードを追加する必要がある場合は、すべての新しいノードを追加したあとにECリバランシング手順 を実行します。

手順	**EC** のリバランシングで許可される手順 ？
アップグレード手順	いいえ。 StorageGRID ソフトウェアをアップグレードする必要がある場合は、EC rebalance手順 の実行前または実行後にアップグレード手順 を実行します。必要に応じて、ソフトウェアアップグレードを実行するために EC Rebalance 手順 を終了できます。
アプライアンスノードのクローン手順	いいえ。 アプライアンスストレージノードをクローニングする必要がある場合は、新しいノードの追加後にECリバランシング手順 を実行します。
Hotfix 手順 の略	はい。 StorageGRID ホットフィックスは、 EC Rebalance 手順 の実行中に適用できます。
その他のメンテナンス手順	いいえ。 他のメンテナンス手順を実行する前に、 EC Rebalance 手順 を終了する必要があります。

EC のリバランシングが行われる手順 と **ILM** の相互作用

EC のリバランシング手順 を実行している間は、 ILM を変更して既存のイレイジャーコーディングオブジェクトの場所が変更されないようにしてください。たとえば、イレイジャーコーディングプロファイルが異なるILMルールは使用しないでください。このようなILMの変更が必要な場合は、ECのリバランシング手順 を終了する必要があります。

拡張ガイドライン

StorageGRIDでオブジェクト容量を追加するためのガイドライン

StorageGRID システムのオブジェクトストレージ容量を拡張するには、既存のストレージノードにストレージボリュームを追加するか、または既存のサイトに新しいストレージノードを追加します。情報ライフサイクル管理（ ILM ）ポリシーの要件を満たす方法でストレージ容量を追加する必要があります。

ストレージボリュームの追加に関するガイドラインを次に示します

既存のストレージノードにストレージボリュームを追加する前に、次のガイドラインと制限事項を確認してください。

- 現在のILMルールを調べて、またはで使用可能なストレージを拡張する"レプリケートされたオブジェクト"場所とタイミングを決定する必要があります"ストレージボリュームを追加します""イレイジャーコーディングオブジェクト"。

- オブジェクトメタデータはボリューム0にのみ格納されるため、ストレージボリュームを追加してもシステムのメタデータ容量を増やすことはできません。
- 各ソフトウェアベースのストレージノードでサポートされるストレージボリュームは最大 48 個です。それよりも多くの容量が必要な場合は、新しいストレージノードを追加する必要があります。
- 各SG6060アプライアンスには、1台または2台の拡張シェルフを追加できます。各拡張シェルフに16個のストレージボリュームが追加されます。両方の拡張シェルフを設置した場合、SG6060では合計48個のストレージボリュームをサポートできます。
- 各SG6160アプライアンスには、1台または2台の拡張シェルフを追加できます。各拡張シェルフに60個のストレージボリュームが追加されます。両方の拡張シェルフを設置した場合、SG6160では合計180個のストレージボリュームをサポートできます。
- 他のストレージアプライアンスにストレージボリュームを追加することはできません。
- 既存のストレージボリュームのサイズは拡張できません。
- ストレージノードへのストレージボリュームの追加は、システムのアップグレード、リカバリ処理、またはその他の拡張と同時に実行することはできません。

ストレージボリュームを追加することにし、 ILM ポリシーを満たすために拡張する必要があるストレージノードを決めたら、該当するタイプのストレージノードの手順に従います。

- SG6060ストレージアプライアンスに拡張シェルフを1台または2台追加する場合は、に進みます "導入したSG6060に拡張シェルフを追加"。
- SG6160ストレージアプライアンスに拡張シェルフを1台または2台追加する場合は、に進みます。 "導入したSG6160に拡張シェルフを追加"
- ソフトウェアベースのノードの場合は、の手順に従います"ストレージノードへのストレージボリュームの追加"。

ストレージノードの追加に関するガイドラインを次に示します

既存のサイトにストレージノードを追加する前に、次のガイドラインと制限事項を確認してください。

- 現在のILMルールを確認して、またはで使用可能なストレージを増やすためにストレージノードをいつどこに追加するかを決定する必要があります"レプリケートされたオブジェクト""イレイジャーコーディングオブジェクト"。
- 1 つの拡張手順 に追加できるストレージノードは 10 個までです。
- 単一の拡張手順 で複数のサイトにストレージノードを追加することができます。
- 1 つの拡張手順 で、ストレージノードとその他のタイプのノードを追加できます。
- 拡張手順 を開始する前に、リカバリの一環として実行されるデータ修復処理がすべて完了したことを確認する必要があります。を参照して "データ修復ジョブを確認します"
- 拡張の実行前または実行後にストレージノードを削除する必要がある場合は、 1 つの運用停止ノード手順の 10 個を超えるストレージノードの運用を停止しないでください。
- 基盤となるストレージの I/O パフォーマンスを維持するために十分なストレージ ノードを追加します。書き込み操作は、使用可能なストレージ容量に基づいてストレージ ノード間で分散されます。拡張されたストレージ ノードに使用可能なストレージ容量が大幅に増えると、それらのノードは大幅に多くの書き込みを受け取ることになります。特に、既存のストレージ ノードがほぼいっぱいになると、新しい書き込みは拡張されたストレージ ノードのみに依存します。読み取りおよび削除操作は、特定のワークロードに応じて処理されます。

ストレージノード上の **ADC** サービスに関するガイドライン

拡張を設定する場合は、新しい各ストレージノードに Administrative Domain Controller （ ADC ）サービスを含めるかどうかを選択する必要があります。ADC サービスは、グリッドサービスの場所と可用性を追跡します。

- あなたは "ADC サービスを同じサイト内の 1 つのストレージ ノードから別のストレージ ノードに移動する"。
- StorageGRIDシステムでは、各サイトで常にを使用できる必要があり"ADC サービスのクォーラム"ます。
- 各サイトで少なくとも 3 つのストレージノードに ADC サービスが含まれている必要があります。
- すべてのストレージノードに ADC サービスを追加することは推奨されません。ノード間の通信量が増加しているため、 ADC サービスが多すぎると原因 の速度が低下する可能性があります。
- 1 つのグリッドに ADC サービスがあるストレージノードが 48 個を超えないようにします。各サイトに ADC サービスが 3 つある 16 のサイトに相当します。
- 通常、新しいノードに対して **ADC** サービス 設定を選択する場合は、 自動 を選択する必要があります。新しいノードが ADC サービスを含む別のストレージ ノードを置き換える場合にのみ、[はい] を選択します。残っている ADC サービスが少なすぎる場合はストレージ ノードを廃止できないため、[はい] を選択すると、古いサービスが削除される前に新しい ADC サービスが利用可能になります。

StorageGRIDでメタデータ容量を追加するためのガイドライン

オブジェクトメタデータ用のスペースを十分に確保するために、各サイトに新しいストレージノードを追加する拡張手順 の実行が必要になる場合があります。

StorageGRID は、各ストレージノードのボリューム 0 にオブジェクトメタデータ用のスペースをリザーブします。すべてのオブジェクトメタデータのコピーが各サイトに 3 つ保持され、すべてのストレージノードに均等に分散されます。

Grid Manager を使用してストレージノードのメタデータ容量を監視し、メタデータ容量がどれくらいの速さで消費されているかを見積もることができます。また、使用済みメタデータスペースが特定のしきい値に達すると、ストレージノードに対して * Low metadata storage * アラートがトリガーされます。

グリッドの使用方法によっては、グリッドのオブジェクトメタデータ容量がオブジェクトのストレージ容量よりも早く消費される場合があります。たとえば、一般に大量の小さいオブジェクトを取り込みたり、大量のユーザメタデータやタグをオブジェクトに追加したりする場合、オブジェクトストレージの容量が十分に残っていても、メタデータ容量を増やすためにストレージノードの追加が必要になることがあります。

詳細については、次を参照してください。

- "オブジェクトメタデータストレージを管理する"
- "各ストレージノードのオブジェクトメタデータ容量を監視します"

メタデータ容量を増やす場合のガイドライン

ストレージノードを追加してメタデータ容量を増やす前に、次のガイドラインと制限事項を確認してください。

- 十分なオブジェクトストレージ容量がある場合は、オブジェクトメタデータ用の使用可能なスペースが増えると、 StorageGRID システムに格納できるオブジェクトの数も増えます。

- 各サイトにストレージノードを 1 つ以上追加して、グリッドのメタデータ容量を増やすことができます。
- 特定のストレージノードでオブジェクトメタデータ用にリザーブされている実際のスペースは、Metadata Reserved Space ストレージオプション（システム全体の設定）、ノードに割り当てられている RAM の容量、ノードのボリューム 0 のサイズによって異なります。
- メタデータはボリューム0にのみ格納されるため、既存のストレージノードにストレージボリュームを追加してもメタデータ容量を増やすことはできません。
- 新しいサイトを追加してメタデータ容量を増やすことはできません。
- StorageGRID は、すべてのオブジェクトメタデータのコピーを各サイトで 3 つ保持します。このため、システムのメタデータ容量は最小のサイトのメタデータ容量によって制限されます。
- メタデータ容量を追加するときは、各サイトに同じ数のストレージノードを追加する必要があります。

メタデータのみのストレージノードには、次の特定のハードウェア要件があります。

- StorageGRIDアプライアンスを使用している場合、メタデータのみのノードを設定できるのは、1.9TBまたは3.8TBのドライブを12本搭載したSGF6112アプライアンスだけです。
- ソフトウェアベースのノードを使用する場合は、メタデータのみのノードリソースが既存のストレージノードリソースと一致している必要があります。例：
  - 既存のStorageGRIDサイトでSG6000またはSG6100アプライアンスを使用している場合は、ソフトウェアベースのメタデータのみのノードが次の最小要件を満たしている必要があります。
    - 128GBのRAM
    - 8コアCPU
    - 8TB SSDまたはCassandraデータベース用同等のストレージ（rangedb/0）
  - 既存のStorageGRIDサイトが 24 GB RAM、8 コア CPU、3 TB または 4 TB のメタデータ ストレージを備えた仮想ストレージ ノードを使用している場合、ソフトウェア ベースのメタデータ専用ノードでは同様のリソース (24 GB RAM、8 コア CPU、4 TB のメタデータ ストレージ (rangedb/0)) を使用する必要があります。
- 新しいStorageGRIDサイトを追加するときは、新しいサイトの総メタデータ容量が少なくとも既存のStorageGRIDサイトと一致し、新しいサイトのリソースが既存のStorageGRIDサイトのストレージノードと一致している必要があります。

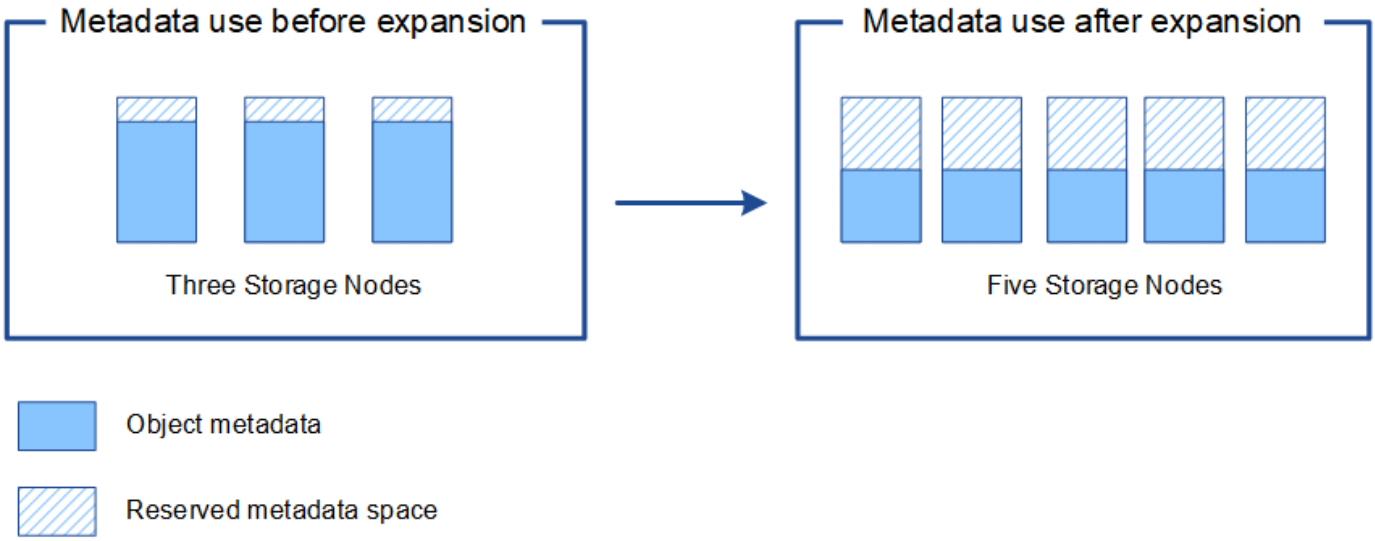
を参照してください"Metadata Reserved Spaceとは何かの概要"。

ストレージノードを追加したときにメタデータが再配分される仕組み

拡張時にストレージノードを追加すると、 StorageGRID によって、既存のオブジェクトメタデータが各サイトの新しいノードに再配分され、グリッドの全体的なメタデータ容量が増加します。ユーザによる操作は必要ありません。

次の図は、拡張でストレージノードを追加した場合に StorageGRID によってオブジェクトメタデータがどのように再配分されるかを示しています。図の左側は、拡張前の 3 つのストレージノードのボリューム 0 を表しています。メタデータが各ノードの使用可能なメタデータスペースの大部分を消費しており、「 Low metadata storage * 」アラートがトリガーされています。

図の右側は、サイトへの 2 つのストレージノードの追加後に既存のメタデータがどのように再配置されるかを示しています。各ノードのメタデータの量が減少し、「 Low metadata storage * 」アラートがトリガーされなくなり、メタデータに使用できるスペースが増えました。



StorageGRIDにグリッドノードを追加するためのガイドライン

既存のサイトに新しいグリッドノードを追加することで、 StorageGRID システムに冗長性を追加したり機能を追加したりできます。

たとえば、ハイアベイラビリティ（HA）グループで使用するゲートウェイノードを追加したり、リモートサイトに管理ノードを追加してローカルノードを使用した監視を許可したりできます。

次のタイプの 1 つ以上のノードを、 1 回の拡張処理で 1 つ以上の既存のサイトに追加することができます。

- 非プライマリ管理ノード
- ストレージノード
- ゲートウェイノード

グリッドノードを追加する場合は、次の制限事項に注意してください。

- プライマリ管理ノードは最初のインストール時に導入されます。拡張時にプライマリ管理ノードを追加することはできません。
- 同じ拡張内でストレージノードとその他のタイプのノードを追加できます。
- ストレージノードを追加するときは、新しいノードの数と場所を慎重に計画する必要があります。を参照して "オブジェクト容量を追加する場合のガイドラインを次に示します"
- ファイアウォール制御ページの信頼されていないクライアント ネットワーク タブで 新しいノードのデフォルトの設定 オプションが 信頼されていない の場合、クライアント ネットワークを使用して拡張ノードに接続するクライアント アプリケーションは、ロード バランサーのエンドポイント ポートを使用して接続する必要があります (*[構成] > [セキュリティ] > [ファイアウォール制御])。指示を参照してください"新しいノードのセキュリティ設定を変更します"そして"ロードバランサエンドポイントを設定する"。

StorageGRIDに新しいサイトを追加するためのガイドライン

新しいサイトを追加して StorageGRID システムを拡張することができます。

サイトの追加に関するガイドライン

サイトを追加する前に、次の要件および制限事項を確認してください。

- 拡張処理で追加できるサイトは 1 つだけです。
- 拡張時に既存のサイトにグリッドノードを追加することはできません。
- すべてのサイトには、少なくとも3つのストレージノードが含まれている必要があります。これらは、複合型ストレージノードとメタデータ専用ストレージノードの任意の組み合わせで構成できます。ストレージノードが3つを超える場合、3つのADCサービスが利用可能であれば、複合型、メタデータ専用、データ専用ストレージノードの任意の組み合わせを使用できます。詳細については、"グリッドごとおよびサイトごとの必要なストレージノード"を参照してください。
- 新しいサイトを追加しても、保存できるオブジェクトの数は自動的に増えるわけではありません。グリッド全体のオブジェクト容量は、利用可能なストレージ容量、ILMポリシー、および各サイトのメタデータ容量によって決まります。
- 新しいサイトのサイジングを行うときは、十分なメタデータ容量が確保されている必要があります。

  StorageGRID は、すべてのオブジェクトのメタデータのコピーを各サイトに保持します。新しいサイトを追加する際は、既存のオブジェクトメタデータに必要なメタデータ容量と、将来の拡張に対応できるメタデータ容量の両方が確保されていることを確認してください。

  詳細については、次の資料を参照してください。

  - "オブジェクトメタデータストレージを管理する"
  - "各ストレージノードのオブジェクトメタデータ容量を監視します"
- サイト間の使用可能なネットワーク帯域幅およびネットワークレイテンシのレベルを考慮する必要があります。すべてのオブジェクトが取り込まれたサイトにのみ格納されている場合でも、メタデータの更新はサイト間で継続的にレプリケートされます。

  遅延によるパフォーマンス低下を回避するために：

  - 遅延時間が100ミリ秒を超えるサイト間では、イレイジャーコーディングは推奨されません。
  - StorageGRID システムのサイトは、複数の大陸にまたがるような広範囲な地理的距離に及ぶべきではありません。
- StorageGRID システムは拡張時も動作し続けるため、拡張手順 を開始する前に ILM ルールを確認し、拡張手順 が完了するまで、オブジェクトコピーが新しいサイトに格納されないようにする必要があります。

  例えば、拡張を開始する前に、デフォルトのストレージプール（すべてのストレージノード）を使用するルールがないか確認してください。該当するルールがある場合は、既存のストレージノードを使用して新しいストレージプールを作成し、ILMルールを更新して新しいストレージプールを使用するようにしてください。それ以外の場合は、そのサイトの最初のノードがアクティブになるとすぐに、オブジェクトが新しいサイトにコピーされます。

  新しいサイトを追加する際に ILM ポリシーを変更する方法の詳細については、"ILMポリシーの変更例"を参照してください。

StorageGRIDシステムの拡張準備

拡張処理を実行する前に、機器を揃え、新しいハードウェアとネットワークの設置と設定を行ってください。

項目	脚注
StorageGRID インストールアーカイブ	新しいグリッドノードや新しいサイトを追加する場合は、StorageGRID インストールアーカイブをダウンロードして展開する必要があります。グリッドで現在実行されているバージョンと同じバージョンを使用する必要があります。 詳細については、の手順を参照してくださいStorageGRID インストールファイルのダウンロードと展開。 *注：*既存のストレージノードに新しいストレージボリュームを追加する場合や新しいStorageGRID アプライアンスをインストールする場合は、ファイルをダウンロードする必要はありません。
サービスラップトップ	サービスラップトップには次のものがあります。 • ネットワークポート • SSH クライアント（ PuTTY など） • "サポートされている Web ブラウザ"
`Passwords.txt`ファイル	コマンド ラインでグリッド ノードにアクセスするために必要なパスワードが含まれます。リカバリパッケージに含まれています。
プロビジョニングパスフレーズ	このパスフレーズは、 StorageGRID システムが最初にインストールされるときに作成されて文書化されます。プロビジョニングパスフレーズがファイルに含まれていません `Passwords.txt`。
StorageGRID のドキュメント	• "StorageGRID の管理" • "リリースノート"。NetAppアカウントでサインインするか、アカウントを作成してリリースノートにアクセスする必要があります。 • "使用しているプラットフォームに対応したインストール手順"
ご使用のプラットフォームの最新ドキュメント	サポートされているバージョンについては、を参照してください "Interoperability Matrix Tool（IMT）"。

StorageGRID インストールファイルをダウンロードして展開します

新しいグリッドノードや新しいサイトを追加する前に、適切な StorageGRID インストールアーカイブをダウンロードし、ファイルを展開する必要があります。

タスクの内容

拡張処理は、グリッドで現在実行されているバージョンの StorageGRID を使用して実行する必要があります。

手順

1. に進みます "NetAppのダウンロード：StorageGRID"。
2. グリッドで現在実行されている StorageGRID のバージョンを選択します。
3. ネットアップアカウントのユーザ名とパスワードを使用してサインインします。
4. [End User License Agreement]を読み、チェックボックスをオンにして、*[Accept & Continue]*を選択します。
5. ダウンロードページの* Install StorageGRID *列で、使用しているプラットフォームに対応するファイルまたは `.zip`ファイルを選択し `.tgz`ます。

   インストールアーカイブファイルに表示されるバージョンは、現在インストールされているソフトウェアのバージョンと一致している必要があります。

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

プラットフォーム	インストールアーカイブ
RHEL	`StorageGRID-Webscale-version-RPM-uniqueID.zip` `StorageGRID-Webscale-version-RPM-uniqueID.tgz`
Ubuntu 、 Debian 、 またはアプライアンス	`StorageGRID-Webscale-version-DEB-uniqueID.zip` `StorageGRID-Webscale-version-DEB-uniqueID.tgz`
VMware	`StorageGRID-Webscale-version-VMware-uniqueID.zip` `StorageGRID-Webscale-version-VMware-uniqueID.tgz`
OpenStack / その他のハイパーバイザー	OpenStack の既存の環境を拡張する場合は、上記のサポートされている Linux ディストリビューションのいずれかを実行する仮想マシンを導入し、 Linux に関する適切な手順に従う必要があります。

6. アーカイブファイルをダウンロードして展開します。
7. プラットフォームに応じた手順に従って、プラットフォーム、計画したグリッドトポロジ、および StorageGRID システムの拡張方法に基づいて、必要なファイルを選択します。

   各プラットフォームの手順に記載されているパスは、アーカイブファイルによってインストールされた最上位ディレクトリに対する相対パスです。

8. RHEL システムを拡張する場合は、適切なファイルを選択します。

パスとファイル名	製品説明
	StorageGRID ダウンロードファイルに含まれているすべてのファイルについて説明するテキストファイル。

パスとファイル名	製品説明
	製品サポートのない無償ライセンス。
	RHELホストにStorageGRIDノードイメージをインストールするためのRPMパッケージ。
	RHELホストにStorageGRIDホストサービスをインストールするためのRPMパッケージ。
導入スクリプトツール	製品説明
	StorageGRID システムの設定を自動化するための Python スクリプト。
	StorageGRID アプライアンスの設定を自動化するための Python スクリプト。
	スクリプトで使用する構成ファイルの例 `configure-storagegrid.py`。
	シングルサインオンが有効な場合にグリッド管理 API にサインインするために使用できる Python スクリプトの例。このスクリプトは、Pingフェデレーション統合にも使用できます。
	スクリプトで使用する空の構成ファイル `configure-storagegrid.py`。
	StorageGRIDコンテナ導入用のRHELホストを設定するためのサンプルのAnsibleのロールとプレイブック。必要に応じて、ロールまたはプレイブックをカスタマイズできます。
	Active DirectoryまたはPingフェデレーションを使用してシングルサインオン（SSO）が有効になっている場合にグリッド管理APIにサインインするために使用できるPythonスクリプトの例。
	関連するPythonスクリプトによって呼び出され、AzureとのSSO対話を実行するヘルパースクリプト `storagegrid-ssoauth-azure.py`。

パスとファイル名	製品説明
	StorageGRID の API スキーマ 注：アップグレードを実行する前に、これらのスキーマを使用して、アップグレード互換性テスト用の非本番環境のStorageGRID 環境がない場合、StorageGRID 管理APIを使用するように記述したコードが新しいStorageGRID リリースと互換性があることを確認できます。

1. Ubuntu または Debian システムを拡張する場合は、適切なファイルを選択します。

パスとファイル名	製品説明
	StorageGRID ダウンロードファイルに含まれているすべてのファイルについて説明するテキストファイル。
	テスト環境やコンセプトの実証環境に使用できる、非本番環境のNetAppライセンスファイル。
	Ubuntu ホストまたは Debian ホストに StorageGRID ノードイメージをインストールするための DEB パッケージ。
	ファイルのMD5チェックサム `/debs/storagegrid-webscale-images-version-SHA.deb`。
	Ubuntu ホストまたは Debian ホストに StorageGRID ホストサービスをインストールするための DEB パッケージ。
導入スクリプトツール	製品説明
	StorageGRID システムの設定を自動化するための Python スクリプト。
	StorageGRID アプライアンスの設定を自動化するための Python スクリプト。
	シングルサインオンが有効な場合にグリッド管理 API にサインインするために使用できる Python スクリプトの例。このスクリプトは、Pingフェデレーション統合にも使用できます。

パスとファイル名	製品説明
	スクリプトで使用する構成ファイルの例 `configure-storagegrid.py`。
	スクリプトで使用する空の構成ファイル `configure-storagegrid.py`。
	StorageGRID コンテナ導入用の Ubuntu ホストまたは Debian ホストを設定するためのサンプルの Ansible のロールとプレイブック。必要に応じて、ロールまたはプレイブックをカスタマイズできます。
	Active DirectoryまたはPingフェデレーションを使用してシングルサインオン（SSO）が有効になっている場合にグリッド管理APIにサインインするために使用できるPythonスクリプトの例。
	関連するPythonスクリプトによって呼び出され、AzureとのSSO対話を実行するヘルパースクリプト `storagegrid-ssoauth-azure.py`。
	StorageGRID の API スキーマ 注：アップグレードを実行する前に、これらのスキーマを使用して、アップグレード互換性テスト用の非本番環境のStorageGRID 環境がない場合、StorageGRID 管理APIを使用するように記述したコードが新しいStorageGRID リリースと互換性があることを確認できます。

1. VMware システムを拡張する場合は、適切なファイルを選択します。

パスとファイル名	製品説明
	StorageGRID ダウンロードファイルに含まれているすべてのファイルについて説明するテキストファイル。
	製品サポートのない無償ライセンス。
	グリッドノード仮想マシンを作成するためのテンプレートとして使用される仮想マシンディスクファイル。
	(`.mf`プライマリ管理ノードを導入するための`Open Virtualization Format`テンプレートファイル）（.ovf とマニフェストファイル

パスとファイル名	製品説明
	テンプレートファイル(.ovf）とマニフェストファイル(.mf）。非プライマリ管理ノードを導入するためのものです。
	テンプレートファイル(.ovf）とマニフェストファイル(.mf）を使用してゲートウェイノードを導入します。
	(.mf`仮想マシンベースのストレージノードを導入するためのテンプレートファイル(.ovf`とマニフェストファイル）
導入スクリプトツール	製品説明
	仮想グリッドノードの導入を自動化するための Bash シェルスクリプト。
	スクリプトで使用する構成ファイルの例 `deploy-vsphere-ovftool.sh`。
	StorageGRID システムの設定を自動化するための Python スクリプト。
	StorageGRID アプライアンスの設定を自動化するための Python スクリプト。
	シングルサインオン（SSO）が有効な場合にグリッド管理APIにサインインするために使用できるPythonスクリプトの例。このスクリプトは、Pingフェデレーション統合にも使用できます。
	スクリプトで使用する構成ファイルの例 `configure-storagegrid.py`。
	スクリプトで使用する空の構成ファイル `configure-storagegrid.py`。
	Active DirectoryまたはPingフェデレーションを使用してシングルサインオン（SSO）が有効になっている場合にグリッド管理APIにサインインするために使用できるPythonスクリプトの例。
	関連するPythonスクリプトによって呼び出され、AzureとのSSO対話を実行するヘルパースクリプト `storagegrid-ssoauth-azure.py`。

パスとファイル名	製品説明
	StorageGRID の API スキーマ 注：アップグレードを実行する前に、これらのスキーマを使用して、アップグレード互換性テスト用の非本番環境のStorageGRID 環境がない場合、StorageGRID 管理APIを使用するように記述したコードが新しいStorageGRID リリースと互換性があることを確認できます。

1. StorageGRID アプライアンスベースのシステムを拡張する場合は、該当するファイルを選択してください。

> アプライアンスのインストールでは、ネットワーク トラフィックを回避する必要がある場合にのみこれらのファイルが必要です。アプライアンスは、リカバリ手順を実行する管理ノードから必要なファイルをダウンロードできます。

パスとファイル名	製品説明
	アプライアンスに StorageGRID ノードイメージをインストールするための DEB パッケージ。
	ファイルのMD5チェックサム `/debs/storagegridwebscale-images-version-SHA.deb`。

ハードウェアとネットワークの確認

StorageGRID システムの拡張を開始する前に、次の点を確認してください。

- 新しいグリッドノードまたは新しいサイトをサポートするために必要なハードウェアを設置して設定しておきます。
- すべての新しいノードに、既存および新規のすべてのノードへの双方向通信パスがある（グリッドネットワークの要件）。特に、拡張で追加する新しいノードとプライマリ管理ノードの間で次のTCPポートが開いていることを確認します。
  - 1055
  - 7443
  - 8011
  - 10342

  を参照して "内部でのグリッドノードの通信"
- プライマリ管理ノードは、 StorageGRID システムをホストするすべての拡張サーバと通信できます。
- 新しいノードのいずれかに、以前に使用していないサブネットのグリッドネットワークIPアドレスが設定されている場合は、グリッドネットワークサブネットリストがすでに設定されて"新しいサブネットが追加されました"います。それ以外の場合は、拡張をキャンセルし、新しいサブネットを追加してから、手順

をもう一度開始する必要があります。

- グリッドノード間またはStorageGRID サイト間のグリッドネットワークでNetwork Address Translation（NAT；ネットワークアドレス変換）を使用していない。グリッドネットワークにプライベート IPv4 アドレスを使用する場合は、使用するアドレスに各サイトのすべてのグリッドノードから直接ルーティングできる必要があります。NAT を使用してパブリックネットワークセグメント全体にグリッドネットワークをブリッジする方法は、グリッド内のすべてのノードに対して透過的なトンネリングアプリケーションを使用する場合、つまりグリッドノードがパブリック IP アドレスを認識する必要がない場合にのみサポートされます。

  この NAT の制限は、グリッドノードとグリッドネットワークに固有のものです。必要に応じて、ゲートウェイノードにパブリック IP アドレスを指定する場合など、外部クライアントとグリッドノードの間で NAT を使用できます。

Grid ノードまたはサイトを追加

StorageGRIDにグリッド ノードまたは新しいサイトを追加するためのワークフローの概要

既存のサイトにグリッドノードを追加する場合や新しいサイトを追加する場合は、次の手順に従ってください。一度に実行できる拡張のタイプは1つだけです。

開始する前に

- あなたはを持っています"rootアクセスまたはMaintenance権限"。
- グリッドのすべての既存ノードがすべてのサイトで動作している。
- これで、前の拡張、アップグレード、運用停止、またはリカバリの手順が完了しました。

> 拡張は、別の拡張、アップグレード、リカバリ、またはアクティブな運用停止の手順 を実行中のときは開始できません。ただし、必要に応じて、運用停止手順 を一時停止して拡張を開始できます。

手順

1. "グリッドネットワークのサブネットを更新する"。
2. "新しいグリッドノードを展開する"。
3. "拡張の実行"です。

StorageGRIDの拡張のためにグリッド ネットワークにサブネットを追加または更新します

グリッドノードまたは新しいサイトを追加した場合は、サブネットの更新、またはグリッドネットワークへのサブネットの追加が必要になることがあります。

StorageGRID は、グリッドネットワーク（ eth0 ）上のグリッドノード間の通信に使用されるネットワークサブネットのリストを管理します。このエントリには、 StorageGRID システムの各サイトでグリッドネットワークに使用されているサブネット、およびグリッドネットワークゲートウェイ経由でアクセスされる NTP 、 DNS 、 LDAP 、またはその他の外部サーバに使用されるサブネットが含まれます。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"Maintenance権限またはRoot Access権限"。
- プロビジョニングパスフレーズを用意します。
- 設定するサブネットのネットワークアドレスを CIDR 表記で指定しておきます。

タスクの内容

グリッドネットワークの IP アドレスが使用されていないサブネットに新しいノードがある場合は、拡張を開始する前にグリッドネットワークのサブネットリストに新しいサブネットを追加する必要があります。それ以外の場合は、拡張をキャンセルし、新しいサブネットを追加してから、手順 をもう一度開始する必要があります。

いずれのノードのグリッドネットワーク、管理ネットワーク、またはクライアントネットワークにおいても、以下の IPv4 アドレスを含むサブネットを使用しないでください。

- 192,168,130,101
- 192,168,130,121
- 192,168,131,101
- 192,168,131,121
- 192,168,130,102
- 192,168,130,122
- 192,168,131,102
- 192,168,131,122
- 198.51.100.2
- 198.51.100.4

例えば、どのノードのグリッドネットワーク、管理ネットワーク、またはクライアントネットワークにも、以下のサブネット範囲を使用しないでください。

- 192.168.130.0/24 は、このサブネット範囲に IP アドレス 192.168.130.101 と 192.168.130.102 が含まれているためです。
- 192.168.131.0/24 は、このサブネット範囲に IP アドレス 192.168.131.101 と 192.168.131.102 が含まれているためです。
- 198.51.100.0/24 は、このサブネット範囲に IP アドレス 198.51.100.2 と 198.51.100.4 が含まれているためです。

手順

1. メンテナンス > ネットワーク > グリッド ネットワーク を選択します。
2. CIDR表記で新しいサブネットを追加する場合は、*[別のサブネットを追加]*を選択します。

   たとえば、と入力し `10.96.104.0/22`ます。

3. プロビジョニングパスフレーズを入力し、 * Save * を選択します。
4. 変更が適用されるまで待ってから、新しい回復パッケージをダウンロードしてください。

a. メンテナンス > システム > *回復パッケージ*を選択します。

b. **Provisioning passphrase** を入力してください。

> リカバリ パッケージ ファイルには、 StorageGRIDシステムからデータを取得するために使用できる暗号化キーとパスワードが含まれているため、セキュリティで保護する必要があります。プライマリ管理ノードを回復するためにも使用されます。

指定したサブネットが、 StorageGRID システムに対して自動的に設定されます。

StorageGRIDに新しいグリッドノードを展開する

拡張時に新しいグリッドノードを導入する手順は、グリッドを最初にインストールしたときに使用した手順と同じです。拡張を実行する前に、すべての新しいグリッドノードの導入が完了している必要があります。

グリッドを拡張する場合、追加するノードが既存のノードタイプと一致している必要はありません。VMware ノード、 Linux コンテナベースのノード、またはアプライアンスノードを追加できます。

VMware ：グリッドノードを導入する

拡張で追加する VMware ノードごとに、 VMware vSphere で仮想マシンを導入する必要があります。

手順

1. "新しいノードを仮想マシンとして導入"1 つ以上のStorageGRIDネットワークに接続します。

   ノードを導入する際には、必要に応じてノードポートを再マッピングしたり、 CPU やメモリの設定を増やしたりできます。

2. 新しいVMwareノードをすべて導入したら、を"拡張手順 を実行します"参照してください。

Linux ：グリッドノードを導入します

グリッドノードは、新規の Linux ホストにも既存の Linux ホストにも導入できます。グリッドに追加する StorageGRID ノードの CPU 、 RAM 、およびストレージの要件に対応するために追加の Linux ホストが必要な場合は、最初にインストールしたときと同じ方法で準備します。その後、インストール時のグリッドノードと同じ方法で拡張ノードを導入します。

開始する前に

- Linuxのバージョンに応じてStorageGRIDをインストールするための手順があり、"ハードウェアとストレージの要件" 。
- 既存のホストに新しいグリッドノードを導入する場合は、既存のホストが追加のノードに対応する十分な CPU 、 RAM 、ストレージ容量を備えていることを確認しておきます。
- 障害ドメインを最小限に抑えるための計画が必要です。たとえば、すべてのゲートウェイノードを 1 つの物理ホストに導入することは避けてください。

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

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

手順

1. ホストを新規に追加する場合は、 StorageGRID ノードの導入に関するインストール手順を参照します。
2. 新しいホストを導入するには、ホストの準備手順に従います。
3. ノード構成ファイルを作成し、 StorageGRID の設定を検証するには、グリッドノードの導入手順に従います。
4. 新しい Linux ホストにノードを追加する場合は、 StorageGRID ホストサービスを開始します。
5. 既存のLinuxホストにノードを追加する場合は、StorageGRIDホストサービスCLIを使用して新しいノードを起動します。`sudo storagegrid node start [<node name\>]`

終了後

すべての新しいグリッドノードの導入が完了したら、実行できます"拡張を実行"。

アプライアンス：ストレージノード、ゲートウェイノード、または非プライマリ管理ノードの導入

アプライアンスノードに StorageGRID ソフトウェアをインストールするには、アプライアンスに含まれている StorageGRID アプライアンスインストーラを使用します。拡張時、各ストレージアプライアンスは単一のストレージノードとして機能し、各サービスアプライアンスは単一のゲートウェイノードまたは非プライマリ管理ノードとして機能します。すべてのアプライアンスは、グリッドネットワーク、管理ネットワーク、およびクライアントネットワークに接続できます。

開始する前に

- アプライアンスをラックまたはキャビネットに設置し、ネットワークに接続し、電源を投入しておきます。
- これで手順は完了 "ハードウェアをセットアップする"です。

  アプライアンスハードウェアのセットアップには、StorageGRID 接続（ネットワークリンクとIPアドレス）の設定に必要な手順のほか、ノード暗号化の有効化、RAIDモードの変更、ネットワークポートの再マッピングのオプションの手順が含まれます。

- StorageGRID アプライアンスインストーラの IP 設定ページに表示されるすべてのグリッドネットワークサブネットが、プライマリ管理ノードのグリッドネットワークサブネットリストで定義されている。
- 交換用アプライアンスの StorageGRID アプライアンスインストーラファームウェアは、グリッドで現在実行されている StorageGRID ソフトウェアのバージョンと互換性があります。互換性がない場合は、StorageGRID アプライアンスインストーラのファームウェアをアップグレードする必要があります。
- を搭載したサービスラップトップを用意しておき"サポートされている Web ブラウザ"ます。
- アプライアンスのコンピューティングコントローラに割り当てられている IP アドレスのいずれかを確認しておきます。接続されているどの StorageGRID ネットワークの IP アドレスでも使用できます。

タスクの内容

アプライアンスノードに StorageGRID をインストールするプロセスには、次のフェーズがあります。

- プライマリ管理ノードの IP アドレスおよびアプライアンスノードの名前を指定または確認します。

- インストールを開始し、ボリュームの設定とソフトウェアのインストールが行われている間待機します。

  アプライアンスインストールタスクの途中で、インストールが一時停止します。インストールを再開するには、 Grid Manager にサインインし、グリッドノードをすべて承認し、 StorageGRID のインストールプロセスを完了します。

  > 一度に複数のアプライアンスノードを導入する必要がある場合は、アプライアンスインストールスクリプトを使用してインストールプロセスを自動化できます `configure-sga.py`。

手順

1. ブラウザを開き、アプライアンスのコンピューティングコントローラの IP アドレスのいずれかを入力します。

   `https://Controller_IP:8443`

   StorageGRID アプライアンスインストーラのホームページが表示されます。

2. 「 * プライマリ管理ノード * 接続」セクションで、プライマリ管理ノードの IP アドレスを指定する必要があるかどうかを確認します。

   このデータセンターに他のノードがすでにインストールされている場合は、プライマリ管理ノードまたは ADMIN_IP が設定された少なくとも 1 つのグリッドノードが同じサブネットにあるという想定で、 StorageGRID アプライアンスインストーラがこの IP アドレスを自動的に検出します。

3. この IP アドレスが表示されない場合や変更する必要がある場合は、アドレスを指定します。

オプション	製品説明
IP を手動で入力します	a. [管理ノードの検出を有効にする]*チェックボックスをオフにします。 b. IPアドレスを手動で入力します。 c. [保存（ Save ）] を選択します。 d. 新しい IP アドレスの接続状態が READY になるまで待ちます。
接続されたすべてのプライマリ管理ノードの自動検出	a. [管理ノードの検出を有効にする]*チェックボックスを選択します。 b. 検出された IP アドレスのリストが表示されるまで待ちます。 c. このアプライアンスストレージノードを導入するグリッドのプライマリ管理ノードを選択します。 d. [保存（ Save ）] を選択します。 e. 新しい IP アドレスの接続状態が READY になるまで待ちます。

4. [* ノード名 *] フィールドに、このアプライアンス・ノードに使用する名前を入力し、 [* 保存 *] を選択します。

   このノード名は、 StorageGRID システムでこのアプライアンスノードに割り当てられ、このタブは、

Grid Manager のノードページ（概要タブ）に表示されます。ノードを承認するときに、必要に応じて、この名前を変更できます。

5. [Installation]セクションで、現在の状態が「**Ready to start installation of *node name* into grid with primary Admin Node_admin_IP_**」であり、[Start Installation]*ボタンが有効になっていることを確認します。

   [Start Installation* （インストールの開始）] ボタンが有効になっていない場合は、ネットワーク設定またはポート設定の変更が必要になることがあります。手順については、アプライアンスのメンテナンス手順を参照してください。

6. StorageGRID アプライアンスインストーラのホームページで、「インストールの開始」を選択します。

   現在の状態が「インストール中です」に変わり、モニターのインストールページが表示されます。

7. 拡張に複数のアプライアンスノードが含まれている場合は、アプライアンスごとに上記の手順を繰り返します。

   > 一度に複数のアプライアンスストレージノードを導入する必要がある場合は、 configure-sga.py アプライアンスインストールスクリプトを使用してインストールプロセスを自動化できます。

8. モニターのインストールページに手動でアクセスする必要がある場合は、メニューバーから「Monitor Installation」を選択してください。

   モニターのインストールページには、インストールの進行状況が表示されます。

   青色のステータスバーは、現在進行中のタスクを示します。緑のステータスバーは、正常に完了したタスクを示します。

   > インストーラは、以前のインストールで完了したタスクが再実行されないようにします。インストールを再実行している場合、再実行する必要のないタスクはすべて緑色のステータスバーと「スキップ済み」のステータスで表示されます。

9. インストールの最初の 2 つのステージの進行状況を確認します。

   *1.アプライアンスを設定 *

   この段階では、次のいずれかのプロセスが実行されます。

   - ストレージアプライアンスの場合、インストーラはストレージコントローラに接続し、既存の設定があれば消去し、SANtricity OSと通信してボリュームを設定し、ホストを設定します。
   - サービスアプライアンスの場合、既存の設定があればインストーラがコンピューティングコントローラのドライブから消去し、ホストを設定します。

     *2.OS * をインストールします

   インストーラが StorageGRID のベースとなるオペレーティングシステムイメージをアプライアンスにコピーします。

10. コンソールウィンドウにメッセージが表示され、 Grid Manager を使用してノードを承認するように求めるメッセージが表示されるまで、インストールの進行状況の監視を続けます。

この拡張で追加したすべてのノードが承認できる状態になるまでは、 Grid Manager でノードを承認しないでください。

StorageGRID拡張を実行する

拡張を行うと、新しいグリッドノードが既存の StorageGRID 環境に追加されます。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- プロビジョニングパスフレーズを用意します。
- この拡張で追加するすべてのグリッドノードの導入が完了している。
- あなたはを持っています"Maintenance権限またはRoot Access権限"。
- ストレージノードを追加する場合は、リカバリの一環として実行されるデータ修復処理がすべて完了したことを確認しておきます。を参照して "データ修復ジョブを確認します"
- ストレージノードを追加していて、それらのノードにカスタムのストレージグレードを割り当てる場合は、が完了している必要"カスタムのストレージグレードを作成しました"があります。また、Root access権限、またはMaintenance権限とILM権限の両方が必要です。
- 新しいサイトを追加する場合は、ILMルールの確認と更新を完了しておきます。拡張が完了するまでオブジェクトコピーが新しいサイトに格納されないようにする必要があります。たとえば、ルールでデフォルトのストレージプール（* All Storage Nodes *）が使用されている場合は、既存のストレージノードとその新しいストレージプールを使用するILMポリシーのみを含む"ILMルールを更新"必要があります"新しいストレージプールを作成します"。そうしないと、そのサイトの最初のノードがアクティブになるとすぐに新しいサイトにオブジェクトがコピーされます。

タスクの内容

拡張の実行には、次の主なユーザタスクが含まれます。

1. 拡張を設定します。
2. 拡張を開始します。
3. 新しいリカバリ パッケージ ファイルをダウンロードします。
4. すべての新しいノードのインストールと設定が完了し、すべてのサービスが開始されるまで、拡張の手順と段階を監視します。

大規模なグリッドでは、拡張の手順や段階によっては実行にかなりの時間がかかることがあります。たとえば、新しいストレージノードへの Cassandra のストリーミングは、Cassandra データベースが空の場合は数分程度で完了します。ただし、 Cassandra データベースに大量のオブジェクトメタデータが含まれている場合は、数時間以上かかることがあります。「Cassandraクラスタの拡張」または「Starting Cassandra and streaming data」のステージの間は、ストレージノードをリブートしないでください。

手順

1. **Maintenance** > **Tasks** > **Grid expansion** を選択します。

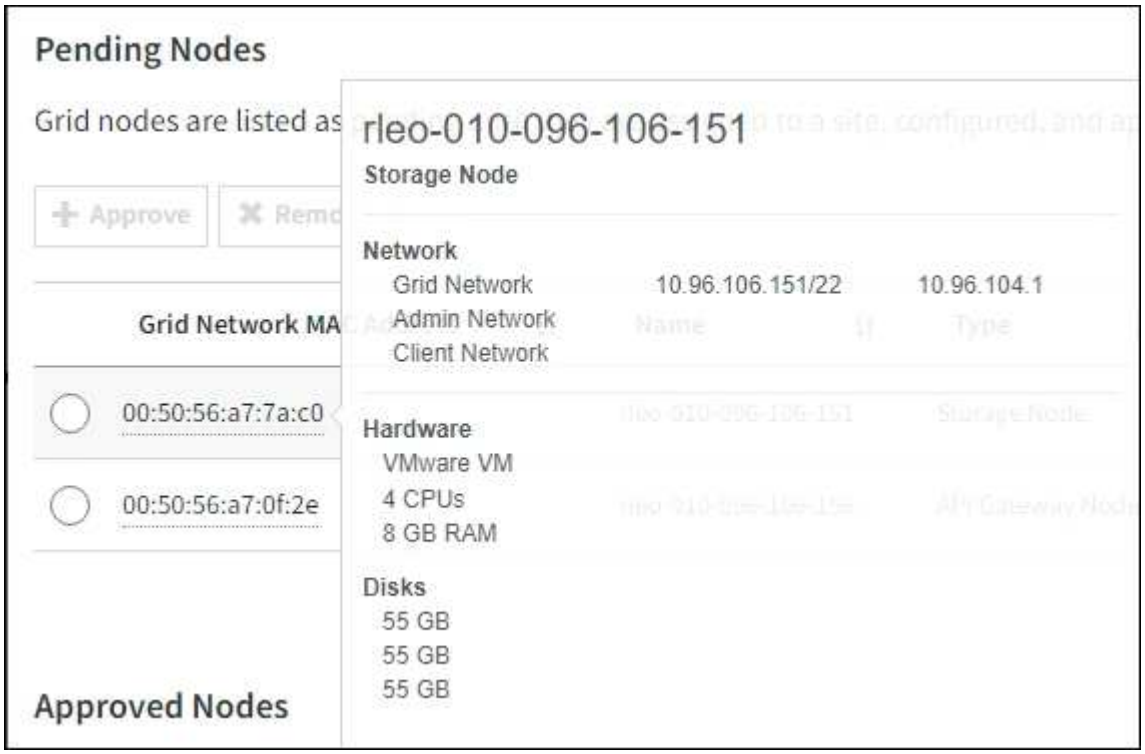
   グリッド展開ページが表示されます。「保留中のノード」セクションには、追加準備が整ったノードが表示されます。

2. [拡張の構成] を選択します。

   [サイトの選択] ダイアログボックスが表示されます。

3. 開始する拡張のタイプを選択します。
   - 新しいサイトを追加する場合は、「 * 新規」を選択し、新しいサイトの名前を入力します。
   - 既存のサイトにノードを追加する場合は、* Existing *を選択します。
4. [保存（ Save ）] を選択します。
5. 「 * Pending Nodes * 」のリストを確認し、導入したすべてのグリッドノードが表示されていることを確認します。

   必要に応じて、ノードの*[Grid Network MAC Address]*にカーソルを合わせると、そのノードに関する詳細を確認できます。



   ノードが見つからない場合は、ノードが正常に導入されたことを確認します。

6. 保留状態のノードのリストで、この拡張で追加するノードを承認します。
   a. 承認する最初の保留中のグリッドノードの横にあるラジオボタンを選択します。
   b. [* 承認（ Approve ）] を選択し

      グリッドノードの設定フォームが表示されます。

   c. 必要に応じて、一般設定を変更します。

フィールド	製品説明
サイト	グリッドノードを関連付けるサイトの名前。複数のノードを追加する場合は、各ノードに適したサイトを選択してください。新しいサイトを追加する場合は、すべてのノードが新しいサイトに追加されます。
名前	ノードのシステム名。システム名は内部StorageGRID 処理に必要であり、変更することはできません。
ストレージタイプ（ストレージノードのみ）	• データとメタデータ（「組み合わせ」）：オブジェクトデータとメタデータのストレージノード • データ専用：オブジェクトデータのみ（メタデータなし）を含むストレージノード • メタデータのみ：メタデータのみを含むストレージノード（オブジェクトデータは含まれない）
NTP ロール	グリッドノードのNetwork Time Protocol（NTP；ネットワークタイムプロトコル）ロール。 • ノードにNTPロールを自動的に割り当てる場合は、* Automatic *（デフォルト）を選択します。Primaryロールは、管理ノード、ADCサービスを使用するストレージノード、ゲートウェイノード、および非静的IPアドレスが設定されたグリッドノードに割り当てられます。Clientロールは他のすべてのグリッドノードに割り当てられます。 • プライマリNTPロールを手動でノードに割り当てるには、*[プライマリ]*を選択します。外部タイミングソースへの冗長システムアクセスを提供するには、各サイトの少なくとも2つのノードにPrimaryロールが必要です。 • クライアントNTPロールをノードに手動で割り当てるには、*[クライアント]*を選択します。

フィールド	製品説明
ADCサービス（統合ストレージノードまたはメタデータ専用ストレージノード）	このストレージ ノードが管理ドメイン コントローラ (ADC) サービスを実行するかどうか。 ADC サービスは、グリッド サービスの場所と可用性を追跡します。各サイトの少なくとも 3 つのストレージ ノードに ADC サービスが含まれている必要があります。 • 交換するストレージ ノードに ADC サービスが含まれている場合は、[はい] を選択します。残っている ADC サービスが少なすぎる場合はストレージ ノードを廃止できないため、この設定により、古いサービスが削除される前に新しい ADC サービスが利用可能になります。 • あなたはできる"ADC サービスを同じサイト内の別のストレージノードに移動する"ADC サービスのクォーラムが満たされていることを確認します。 • このノードにADCサービスが必要かどうかをシステムで自動的に判断するには、*[Automatic]*を選択します。 については、を参照して"ADCクォーラム"ください。
ストレージグレード（組み合わせたストレージノードまたはデータ専用ストレージノード）	デフォルト*のストレージグレードを使用するか、この新しいノードに割り当てるカスタムのストレージグレードを選択します。 ストレージグレードはILMストレージプールで使用されるため、選択内容がストレージノードに配置されるオブジェクトに影響する可能性があります。

d. 必要に応じて、グリッドネットワーク、管理ネットワーク、およびクライアントネットワークの設定を変更します。

   - * IPv4 Address （ CIDR ） * ：ネットワークインターフェイスの CIDR ネットワークアドレス。例： 172.16.10.100/24

     ノードの承認中にグリッドネットワークでノードのIPアドレスが重複していることがわかった場合は、拡張をキャンセルし、重複しないIPで仮想マシンまたはアプライアンスを再導入してから、拡張を再開する必要があります。

   - * Gateway * ：グリッドノードのデフォルトゲートウェイ。例： 172.16.10.1
   - * Subnets （ CIDR ） * ：管理ネットワーク用の 1 つ以上のサブネットワーク。

e. [保存（ Save ）] を選択します。

   承認済みグリッドノードが [承認済みノード] リストに移動します。

   - 承認済みグリッドノードのプロパティを変更するには、そのラジオボタンを選択し、 * 編集 * を選択します。
   - 承認済みのグリッドノードを保留中のノードのリストに戻すには、該当するオプションボタンを選択し、 * リセット * を選択します。
   - 承認済みのグリッドノードを完全に削除するには、ノードの電源をオフにします。次に、そのラジオボタンを選択し、 * 削除 * を選択します。

f. 承認する保留中のグリッドノードごとに、上記の手順を繰り返します。

> 可能であれば、保留中のグリッドノードをすべて承認し、 1 回の拡張を実施してください。小規模な拡張を複数回実施すると、さらに時間がかかります。

7. すべてのグリッドノードを承認したら、*プロビジョニングパスフレーズ*を入力し、*展開*を選択します。

   数分後にページが更新され、拡張手順 のステータスが表示されます。個 々 のグリッドノードに影響するタスクが進行中の場合、[Grid Node Status]セクションに各グリッドノードの現在のステータスが表示されます。

> 新しいアプライアンスの「グリッドノードのインストール」の手順で、StorageGRIDアプライアンスインストーラのインストールがステージ3からステージ4の「インストールの完了」に移動します。ステージ 4 が完了すると、コントローラがリブートします。

> サイトの拡張には、新しいサイト用の Cassandra を設定するための追加タスクが含まれます。

8. リカバリ パッケージのダウンロード リンクが表示されたらすぐに、リカバリ パッケージ ファイルをダウンロードします。

   StorageGRIDシステムのグリッド トポロジを変更した後は、できるだけ早くリカバリ パッケージ ファイルの更新されたコピーをダウンロードする必要があります。リカバリ パッケージ ファイルを使用すると、障害が発生した場合にシステムを復元できます。

   a. ダウンロードリンクを選択します。
   b. プロビジョニングパスフレーズを入力し、 * ダウンロードの開始 * を選択します。
   c. ダウンロードが完了したら、ファイルを開き `.zip`、ファイルを含むコンテンツにアクセスできることを確認し `Passwords.txt`ます。
   d. ダウンロードしたリカバリパッケージファイルをコピーします(`.zip`) を 2 つの安全でセキュリティ保護された別の場所に保管します。

> リカバリ パッケージ ファイルには、 StorageGRIDシステムからデータを取得するために使用できる暗号化キーとパスワードが含まれているため、セキュリティで保護する必要があります。

9. 既存のサイトにストレージノードを追加する場合やサイトを追加する場合は、新しいグリッドノードでサービスが開始されたときにCassandraステージを監視します。

> 「Cassandraクラスタの拡張」または「Starting Cassandra and streaming data」段階の間は、ストレージノードをリブートしないでください。特に既存のストレージノードに大量のオブジェクトメタデータが含まれている場合、これらのステージは新しいストレージノードごとに完了するまでに数時間かかることがあります。

ストレージノードの追加

既存のサイトにストレージノードを追加する場合は、「Starting Cassandra and streaming data」ステータスメッセージに表示される割合を確認します。

この割合は、使用可能な Cassandra データの合計量と、新しいノードに書き込み済みの量に基づいて、 Cassandra のストリーミング処理の進捗状況から概算したものです。

サイトを追加しています

新しいサイトを追加する場合は、を使用して `nodetool status`Cassandraストリーミングの進捗状況を監視し、「Cassandraクラスタの拡張」段階で新しいサイトにコピーされたメタデータの量を確認します。新しいサイトの総データ負荷は、現在のサイトの合計の約 20% 以内である必要があります。

10. すべてのタスクが完了し、 * 拡張の設定 * ボタンが再表示されるまで、拡張の監視を続けます。

終了後

追加したグリッドノードのタイプに応じて、統合と設定に関する追加の手順を実行します。を参照して "拡張後の設定手順"

ストレージボリュームを追加します

StorageGRIDシステムにストレージボリュームを追加する

サポートされている最大ボリューム数を下回るストレージ ノードのストレージ容量を拡張できます。複製されたコピーまたは消去コード化されたコピーの ILM 要件を満たすには、複数のストレージ ノードにストレージ ボリュームを追加する必要がある場合があります。

開始する前に

ストレージボリュームを追加する前に、を参照し"オブジェクト容量を追加する場合のガイドラインを次に示します"て、ILMポリシーの要件を満たすためにボリュームを追加する場所を確認しておく必要があります。

> この手順はソフトウェアベースのストレージノードにのみ該当します。拡張シェルフを設置してSG6060またはSG6160にストレージボリュームを追加する方法については、または "導入したSG6160に拡張シェルフを追加"を参照してください "導入したSG6060に拡張シェルフを追加"。他のアプライアンスストレージノードは拡張できません。

タスクの内容

ストレージノードの基盤となるストレージは、複数のストレージボリュームに分割されます。ストレージボリュームは、 StorageGRID システムでフォーマットされてオブジェクトの格納用にマウントされたブロックベースのストレージデバイスです。各ストレージノードでサポートされるストレージボリュームは、 Grid Manager では _ オブジェクトストア _ と呼ばれ、最大 48 個です。

> オブジェクトメタデータは常にオブジェクトストア 0 に格納されます。

各オブジェクトストアは、 ID に対応するボリュームにマウントされます。たとえば、IDが0000のオブジェクトストアはマウントポイントに対応して `/var/local/rangedb/0`います。

新しいストレージボリュームを追加する前に、 Grid Manager を使用して、各ストレージノードの現在のオブジェクトストアと対応するマウントポイントを表示します。この情報は、ストレージボリュームを追加するときに役立ちます。

手順

1. ノード > ***site*** > ストレージ ノード > ストレージ を選択します。
2. 下にスクロールして、各ボリュームとオブジェクトストアに使用可能なストレージ容量を表示します。

   アプライアンスストレージノードの場合、各ディスクのWorldwide Nameは、SANtricity OS（アプライアンスのストレージコントローラに接続されている管理ソフトウェア）で標準のボリュームプロパティとして表示されるボリュームのWorld-Wide Identifier（WWID）と同じです。

   ボリュームマウントポイントに関連するディスクの読み取りと書き込みの統計情報を解釈できるように、 Disk Devices テーブルの * Name * 列に表示される名前の最初の部分（つまり、 *sdc_sd*,*sde* ）が Volumes テーブルの * Device * 列に表示される値と一致していることを確認します。

Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
sdc(8:16,sdb)	N/A	0.05%	0 bytes/s	4 KB/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s
sdf(8:64,sde)	N/A	0.00%	0 bytes/s	82 bytes/s
sdg(8:80,sdf)	N/A	0.00%	0 bytes/s	82 bytes/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	4 KB/s
cvloc(8:2,sda2)	N/A	0.95%	0 bytes/s	52 KB/s

Volumes

Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.73 GB	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/3	sdf	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/4	sdg	Online	107.32 GB	107.18 GB	Enabled

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	1.55 MB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0003	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0004	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

3. プラットフォームに応じた手順に従って、ストレージノードに新しいストレージボリュームを追加します。
   - "VMware ：ストレージノードにストレージボリュームを追加"
   - "Linux ：ストレージノードに直接接続型ボリュームまたは SAN ボリュームを追加"

StorageGRIDのVMwareストレージノードにストレージボリュームを追加する

ストレージ ノードに含まれるストレージ ボリュームが 16 個未満の場合は、VMware vSphere を使用してボリュームを追加することで容量を増やすことができます。

開始する前に

- あなたは、"VMware環境向けStorageGRIDのインストール手順" 。
- あなたはファイルを持ってい `Passwords.txt`ます。
- そうだな "特定のアクセス権限"

> ソフトウェアのアップグレード、リカバリ手順 、または別の拡張手順 がアクティブな間は、ストレージノードにストレージボリュームを追加しないでください。

タスクの内容

ストレージボリュームを追加するときは、ストレージノードが一時的に使用できない状態になっています。クライアント向けのグリッドサービスへの影響を回避するために、この手順 は一度に 1 つのストレージノードでのみ実行してください。

手順

1. 必要に応じて、新しいストレージハードウェアを設置し、新しい VMware データストアを作成します。
2. ストレージとして使用する仮想マシン（オブジェクトストア）に 1 つ以上のハードディスクを追加します。
   a. VMware vSphere Client を開きます。
   b. 仮想マシンの設定を編集して、 1 つ以上のハードディスクを追加します。

   通常、ハードディスクは仮想マシンディスク（ VMDK ）として設定されます。VMDKは一般的に使用され、管理も簡単です。一方、RDMは、より大きなオブジェクトサイズ（100MBを超えるなど）を使用するワークロードのパフォーマンスに優れている場合があります。仮想マシンへのハードディスクの追加の詳細については、VMware vSphereのドキュメントを参照してください。
3. VMware vSphere Clientで* Restart Guest OS *オプションを使用するか、仮想マシンへのsshセッションで次のコマンドを入力して、仮想マシンを再起動します。`sudo reboot`

   > 仮想マシンの再起動に*パワーオフ*または*リセット*を使用しないでください。
4. ストレージノードで使用する新しいストレージを設定します。
   a. グリッドノードにログインします。
      i. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
      ii. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

iii. 次のコマンドを入力してrootに切り替えます。 `su -`

iv. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。`root`としてログインすると、プロンプトがからに `#`変わります `$`。

b. 新しいストレージボリュームを設定します。

```
sudo add_rangedbs.rb
```

新しいストレージボリュームがすべて検出され、それらをフォーマットするように求められます。

c. 「 * y * 」と入力して、フォーマットを確定します。

d. 以前にフォーマットされたボリュームがある場合は、それらを再フォーマットするかどうかを決めます。

- 再フォーマットするには「 * y * 」と入力します。
- 再フォーマットをスキップするには「 * n * 」と入力します。

`setup_rangedbs.sh`スクリプトが自動的に実行されます。

5. サービスが正しく開始されることを確認します。

a. サーバ上のすべてのサービスのステータスのリストを表示します。

```
sudo storagegrid-status
```

ステータスは自動的に更新されます。

a. すべてのサービスが「 Running 」または「 Verified 」になるまで待ちます。

b. ステータス画面を終了します。

```
Ctrl+C
```

6. ストレージノードがオンラインであることを確認します。

a. を使用してGrid Managerにサインインし"サポートされている Web ブラウザ"ます。

b. ノード > ストレージノード > *タスク*を選択します。

c. *ストレージ状態*ドロップダウンリストが読み取り専用またはオフラインに設定されている場合は、*オンライン*を選択します。

d. [保存（ Save ）] を選択します。

7. 新しいオブジェクト ストアを表示するには、[ストレージ] を選択します。

8. ボリューム テーブルで詳細を表示します。

結果

拡張したストレージノードの容量をオブジェクトデータの保存に使用できます。

StorageGRIDのLinuxストレージノードに直接接続またはSANボリュームを追加する

ストレージノードのストレージボリュームが 48 個より少ない場合は、新しいブロックストレージデバイスを追加して Linux ホストから認識されるようにし、ストレージノードで使用される StorageGRID 構成ファイルに新しいブロックデバイスマッピングを追加することで、ストレージノードの容量を増やすことができます。

開始する前に

- あなたは、"StorageGRIDのインストール手順" Linux プラットフォーム用。
- あなたはファイルを持ってい `Passwords.txt`ます。
- そうだな "特定のアクセス権限"

> ソフトウェアのアップグレード、リカバリ手順 、または別の拡張手順 がアクティブな間は、ストレージノードにストレージボリュームを追加しないでください。

タスクの内容

ストレージボリュームを追加するときは、ストレージノードが一時的に使用できない状態になっています。クライアント向けのグリッドサービスへの影響を回避するために、この手順 は一度に 1 つのストレージノードでのみ実行してください。

手順

1. 新しいストレージハードウェアを設置します。

   詳細については、ハードウェアベンダーが提供しているドキュメントを参照してください。

2. 必要なサイズの新しいブロックストレージボリュームを作成します。
   - 新しいドライブを接続してRAIDコントローラ構成を必要に応じて更新するか、共有ストレージアレイに新しいSAN LUNを割り当ててLinuxホストからアクセスできるようにします。
   - 既存のストレージノード上のストレージボリュームと同じ永続的な命名規則を使用します。
   - StorageGRID のノード移行機能を使用する場合は、このストレージノードの移行のターゲットとなる他の Linux ホストから新しいボリュームが認識されるようにします。詳細については、使用している Linux プラットフォーム用の StorageGRID のインストール手順を参照してください。
3. ストレージノードをサポートするLinuxホストに、rootとして、またはsudo権限を持つアカウントでログインします。
4. 新しいストレージボリュームが Linux ホストで認識されていることを確認します。

   デバイスを再スキャンしなければならない場合があります。

5. 次のコマンドを実行して、ストレージノードを一時的に無効にします。

   ```
   sudo storagegrid node stop <node-name>
   ```

6. vimやpicoなどのテキストエディタを使用して、ストレージノードのノード構成ファイルを編集します。このファイルは、にあります `/etc/storagegrid/nodes/<node-name>.conf`。
7. ノード構成ファイルで、既存のオブジェクトストレージのブロックデバイスマッピングが含まれているセクションを探します。

この例では、 `BLOCK_DEVICE_RANGEDB_00`からは `BLOCK_DEVICE_RANGEDB_03`既存のオブジェクトストレージのブロックデバイスマッピングです。

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/sgws-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/sgws-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/sgws-sn1-rangedb-3
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

8. このストレージノード用に追加したブロックストレージボリュームに対応する新しいオブジェクトストレージのブロックデバイスマッピングを追加します。

   次から始めるようにし `BLOCK_DEVICE_RANGEDB_nn`てください。隙間を空けてはいけません。

   - 上記の例に基づいて、から開始し `BLOCK_DEVICE_RANGEDB_04`ます。
   - 次の例では、4つの新しいブロックストレージボリュームがノードに追加されています。
     BLOCK_DEVICE_RANGEDB_04 BLOCK_DEVICE_RANGEDB_07

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/sgws-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/sgws-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/sgws-sn1-rangedb-3
BLOCK_DEVICE_RANGEDB_04 = /dev/mapper/sgws-sn1-rangedb-4
BLOCK_DEVICE_RANGEDB_05 = /dev/mapper/sgws-sn1-rangedb-5
BLOCK_DEVICE_RANGEDB_06 = /dev/mapper/sgws-sn1-rangedb-6
BLOCK_DEVICE_RANGEDB_07 = /dev/mapper/sgws-sn1-rangedb-7
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

9. 次のコマンドを実行して、ストレージノードのノード構成ファイルに対する変更を検証します。

```
sudo storagegrid node validate <node-name>
```

エラーや警告がある場合は、次の手順に進む前に対処してください。

次のようなエラーが表示された場合は、ノード構成ファイルがで使用されているブロックデバイス `<PURPOSE>`をLinuxファイルシステム内のに `<path-name>`マッピングしようとしてい `<node-name>`ますが、その場所に有効なブロックデバイススペシャルファイル（またはブロックデバイススペシャルファイルへのソフトリンク）がありません。

```
Checking configuration file for node <node-name>…
ERROR: BLOCK_DEVICE_<PURPOSE> = <path-name>
<path-name> is not a valid block device
```

正しいが入力されていることを確認します `<path-name>`。

10. 次のコマンドを実行して、新しいブロックデバイスマッピングを設定したノードを再起動します。

```
sudo storagegrid node start <node-name>
```

11. ファイルに記載されているパスワードを使用して、ストレージノードにadminとしてログインし `Passwords.txt`ます。
12. サービスが正しく開始されることを確認します。
    a. サーバ上のすべてのサービスのステータスのリストを表示します。+
    ```
    sudo storagegrid-status
    ```
    ステータスは自動的に更新されます。
    b. すべてのサービスが「 Running 」または「 Verified 」になるまで待ちます。
    c. ステータス画面を終了します。
    ```
    Ctrl+C
    ```
13. ストレージノードで使用する新しいストレージを設定します。
    a. 新しいストレージボリュームを設定します。
    ```
    sudo add_rangedbs.rb
    ```
    新しいストレージボリュームがすべて検出され、それらをフォーマットするように求められます。
    b. 「 * y * 」と入力して、ストレージボリュームをフォーマットします。
    c. 以前にフォーマットされたボリュームがある場合は、それらを再フォーマットするかどうかを決めます。
    - 再フォーマットするには「 * y * 」と入力します。
    - 再フォーマットをスキップするには「 * n * 」と入力します。

`setup_rangedbs.sh`スクリプトが自動的に実行されます。

14. ストレージノードのストレージの状態がオンラインであることを確認します。
    a. を使用してGrid Managerにサインインし"サポートされている Web ブラウザ"ます。
    b. ノード > ストレージノード > *タスク*を選択します。
    c. *ストレージ状態*ドロップダウンリストが読み取り専用またはオフラインに設定されている場合は、*オンライン*を選択します。
    d. [保存（ Save ）] を選択します。
15. 新しいオブジェクト ストアを表示するには、[ストレージ] を選択します。
16. ボリューム テーブルで詳細を表示します。

結果

拡張したストレージノードの容量をオブジェクトデータの保存に使用できるようになりました。

拡張したシステムを設定します

StorageGRIDで新しく追加されたノードとサイトを構成する

拡張が完了したら、統合と設定のための追加の手順を実行する必要があります。

タスクの内容

拡張で追加するグリッドノードまたはサイトに応じて、以下の設定タスクを実行する必要があります。システムのインストールおよび管理時に選択したオプション、および拡張時に追加したノードとサイトの設定方法によっては、一部のタスクはオプションです。

手順

1. サイトを追加した場合：
    - "ストレージプールを作成します"（サイト）と、新しいストレージノード用に選択した各ストレージグレード。
    - ILMポリシーが新しい要件を満たしていることを確認します。ルールの変更が必要な場合、"新しいルールを作成します"および"ILMポリシーを更新します"。ルールがすでに正しい場合は、"新しいポリシーをアクティブ化します"StorageGRIDで新しいノードが使用されるようにルールを変更する必要はありません。
    - そのサイトからネットワークタイムプロトコル（NTP）サーバにアクセスできることを確認します。を参照して "NTPサーバを管理します。"

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

2. 既存のサイトにストレージノードを追加した場合は、次の手順を実行します。

- "ストレージプールの詳細を表示します"追加した各ノードが想定されるストレージプールに含まれ、想定されるILMルールで使用されていることを確認するため。
- ILMポリシーが新しい要件を満たしていることを確認します。ルールの変更が必要な場合、"新しいルールを作成します"および"ILMポリシーを更新します"。ルールがすでに正しい場合は、"新しいポリシーをアクティブ化します"StorageGRIDで新しいノードが使用されるようにルールを変更する必要はありません。
- "ストレージノードがアクティブであることを確認します"オブジェクトを取り込むことができます。
- 推奨される数のストレージノードを追加できなかった場合は、イレイジャーコーディングデータをリバランシングします。を参照して "ストレージノードの追加後にイレイジャーコーディングデータをリバランシングします"

3. ゲートウェイノードを追加した場合：
   - クライアント接続に高可用性 (HA) グループを使用する場合は、オプションでゲートウェイ ノードを HA グループに追加します。既存の HA グループのリストを確認し、新しいノードを追加するには、[構成] > [ネットワーク] > [高可用性グループ] を選択します。見る"ハイアベイラビリティグループを設定する" 。
4. 管理ノードを追加した場合の手順は次のとおりです。
   a. StorageGRID システムでシングル サインオン（SSO）が有効になっている場合は、新しい管理ノードの証明書利用者信頼を作成してください。この証明書利用者信頼を作成するまで、ノードにサインインすることはできません。SSO の設定については、"OIDC" または "SAML" を参照してください。
   b. 管理ノードでロード バランサ サービスを使用する予定の場合は、オプションで新しい管理ノードを HA グループに追加します。既存の HA グループのリストを確認し、新しいノードを追加するには、[構成] > [ネットワーク] > [高可用性グループ] を選択します。見る"ハイアベイラビリティグループを設定する" 。
   c. 必要に応じて、 Prometheus データベースをプライマリ管理ノードから拡張管理ノードにコピーします。これは、各管理ノードで指標の履歴の整合性を維持する場合に行います。を参照して "Prometheus 指標をコピーする"
   d. 必要に応じて、既存の監査ログをプライマリ管理ノードから拡張管理ノードにコピーします。これは、各管理ノードでログの履歴情報の整合性を維持する場合に行います。を参照して "監査ログをコピーする"
5. 拡張ノードが信頼できないクライアント ネットワークで追加されたかどうかを確認するか、ノードのクライアント ネットワークが信頼できないか信頼できるかを変更するには、[構成] > [セキュリティ] > [ファイアウォール制御] に移動します。

   拡張ノードのクライアントネットワークが信頼されていない場合は、ロードバランサエンドポイントを使用してクライアントネットワークのノードへの接続を確立する必要があります。およびを参照してください"ロードバランサエンドポイントを設定する""ファイアウォールコントロールを管理します"。
6. DNSを設定します。

   DNS 設定をグリッドノードごとに個別に指定していた場合は、新しいノード用のノード単位のカスタム DNS 設定を追加する必要があります。を参照して "単一のグリッドノードの DNS 設定を変更します"

適切に動作するように、2つまたは3つのDNSサーバを指定します。3つ以上を指定すると、一部のプラットフォームではOSに制限があるため、3つだけが使用される可能性があります。ルーティングが制限されている環境では、個 々 のノード（通常はサイトのすべてのノード）で、最大3つのDNSサーバの異なるセットを使用できます"DNSサーバリストをカスタマイズします"。

可能であれば、各サイトがローカルにアクセスできるDNSサーバを使用して、孤立したサイトが外部の宛先のFQDNを解決できるようにします。

StorageGRID拡張後にストレージノードがアクティブであることを確認する

新しいストレージノードを追加する拡張処理が完了すると、 StorageGRID システムは新しいストレージノードの使用を自動的に開始します。StorageGRID システムを使用して、新しいストレージノードがアクティブになっていることを確認する必要があります。

手順

1. を使用してGrid Managerにサインインし"サポートされている Web ブラウザ"ます。
2. ノード > 拡張ストレージノード > *ストレージ*を選択します。
3. [Storage Used - Object Data]グラフにカーソルを合わせて、* Used *の値を確認します。これは、オブジェクトデータに使用されている使用可能な合計スペースの量です。
4. グラフ上でカーソルを右に移動して、「使用済み」の値が増加していることを確認します。

Prometheus メトリックをStorageGRIDの新しい管理ノードにコピーする

新しい管理ノードを追加したら、 Prometheus で管理されている指標の履歴を必要に応じてプライマリ管理ノードから新しい管理ノードにコピーできます。指標をコピーすると、管理ノード間で指標の履歴の整合性が確保されます。

開始する前に

- 新しい管理ノードがインストールされて実行されている必要があります。
- あなたはファイルを持ってい `Passwords.txt`ます。
- プロビジョニングパスフレーズを用意します。

タスクの内容

管理ノードを追加すると、ソフトウェアのインストールプロセスによって新しい Prometheus データベースが作成されます。Prometheus データベースをプライマリ管理ノード（ *source Admin Node*） から新しい管理ノードにコピーすることで、ノード間で指標の履歴の整合性を維持できます。

> Prometheus データベースのコピーには 1 時間以上かかる場合があります。ソース管理ノードでサービスが停止している間は、グリッドマネージャの一部の機能が使用できなくなります。

手順

1. ソース管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
   b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。
2. ソース管理ノードからPrometheusサービスを停止します。 `service prometheus stop`

3. 新しい管理ノードで次の手順を実行します。

   a. 新しい管理ノードにログインします。

      i. 次のコマンドを入力します。 `ssh admin@grid_node_IP`

      ii. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

      iii. 次のコマンドを入力してrootに切り替えます。 `su -`

      iv. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

   b. Prometheusサービスを停止します。 `service prometheus stop`

   c. SSH エージェントに SSH 秘密鍵を追加します。入力：`ssh-add`

   d. ファイルに記載されているSSHアクセスパスワードを入力し `Passwords.txt`ます。

   e. ソース管理ノードのPrometheusデータベースを新しい管理ノードにコピーします。
   `/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`

   f. プロンプトが表示されたら、 * Enter * を押して、新しい管理ノード上の新しい Prometheus データベースを破棄することを確認します。

      元の Prometheus データベースとその履歴データが新しい管理ノードにコピーされます。コピー処理が完了すると、新しい管理ノードがスクリプトによって起動されます。次のステータスが表示されます。

```
Database cloned, starting services
```

   a. 他のサーバにパスワードなしでアクセスする必要がなくなった場合は、 SSH エージェントから秘密鍵を削除します。入力：

      ```
      ssh-add -D
      ```

4. ソース管理ノードで Prometheus サービスを再起動します。

   ```
   service prometheus start
   ```

監査ログを**StorageGRID**の新しい管理ノードにコピーする

拡張手順を通じて新しい管理ノードを追加すると、その AMS サービスは、その管理ノードがシステムに参加した後に発生するイベントとアクションのみをログに記録します。必要に応じて、以前にインストールした管理ノードから新しい拡張管理ノードに監査ログをコピーして、 StorageGRIDシステムの残りの部分と同期させることができます。

開始する前に

- 管理ノードを追加する拡張手順が完了している必要があります。
- あなたはファイルを持ってい `Passwords.txt`ます。

タスクの内容

新しい管理ノードで監査メッセージの履歴を確認できるようにするには、既存の管理ノードから拡張管理ノードに監査ログファイルを手動でコピーする必要があります。

デフォルトでは、監査情報は `localaudit`各ノードにログオンします。この手順を使用するには、管理ノードを監査先として次のように設定しておく必要があります。

- ログの送信先として*管理ノード/ローカル ノード*を設定しました。
- ログの保存先として*管理ノードと外部 syslog サーバー*を設定しました。

参照"監査メッセージと外部syslogサーバの設定"詳細については。

手順

1. プライマリ管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@_primary_Admin_Node_IP`
   b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

   rootとしてログインすると、プロンプトがからに `#`変わります `$`。
2. AMSサービスを停止して新しいファイルが作成されないようにします。 `service ams stop`
3. 監査エクスポートディレクトリに移動します。

   ```
   cd /var/local/audit/export/
   ```
4. ソースの名前を変更する `audit.log`ファイルをコピーして、コピー先の拡張管理ノード上のファイルを上書きしないようにします。

   ```
   ls -l
   mv audit.log _new_name_.txt
   ```
5. すべての監査ログファイルを拡張管理ノードのデスティネーションの場所にコピーします。

   ```
   scp -p * IP_address:/var/local/audit/export/
   ```
6. のパスフレーズの入力を求められたら `/root/.ssh/id_rsa`、ファイルに含まれているプライマリ管理ノードのSSHアクセスパスワードを入力し `Passwords.txt`ます。
7. 元のファイルを復元し `audit.log`ます。

   ```
   mv new_name.txt audit.log
   ```
8. AMS サービスを開始します。

   ```
   service ams start
   ```
9. サーバからログアウトします。

   ```
   exit
   ```

10. 拡張管理ノードにログインします。
    a. 次のコマンドを入力します。 `ssh admin@expansion_Admin_Node_IP`
    b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。
    c. 次のコマンドを入力してrootに切り替えます。 `su -`
    d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

       rootとしてログインすると、プロンプトがからに `#`変わります `$`。

11. 監査ログファイルのユーザとグループの設定を更新します。

```
cd /var/local/audit/export/

chown ams-user:bycast *
```

12. サーバからログアウトします。

```
exit
```

StorageGRIDシステムにノードを追加した後、消失訂正符号化データを再バランスします。

ストレージノードを追加したら、イレイジャーコーディング（EC）のリバランシング手順を使用して、既存のストレージノードと新しいストレージノードにイレイジャーコーディングフラグメントを再配置できます。

開始する前に

- 新しいストレージノードを追加する拡張手順が完了している。
- を確認しておきます"イレイジャーコーディングデータのリバランシングに関する考慮事項"。
- この手順では複製されたオブジェクト データは移動されず、EC 再バランス手順では複製されたデータは移動されないことを理解します。ただし、EC データを移動する場所を決定する際には、複製されたデータが考慮されます。
- あなたはファイルを持ってい `Passwords.txt`ます。

この手順 が実行されたときの動作

手順 を起動する前に、次の点に注意してください。

- 1つ以上のボリュームがオフラインの（アンマウントされた）場合、またはオンラインの（マウントされた）ボリュームがエラー状態の場合、ECリバランシング手順 は開始されません。
- EC のリバランシングによって、手順 が一時的に大量のストレージをリザーブします。ストレージアラートがトリガーされる場合がありますが、リバランシングが完了すると解決します。予約に十分なストレージがない場合、 EC のリバランシング手順 は失敗します。ストレージ予約は、手順 が失敗したか成功したかに関係なく、 EC のリバランシング手順 が完了したときに解放されます。
- ECのリバランシング手順の処理中にボリュームがオフラインになると、リバランシング手順は終了します。移動済みのデータフラグメントは新しい場所に残り、データが失われることはありません。

  すべてのボリュームがオンラインに戻ったら、手順を再実行できます。

- ECリバランシング手順の実行中は、ILM処理とS3クライアント処理のパフォーマンスに影響する可能性があります。

> オブジェクト（またはオブジェクトパーツ）をアップロードするS3 API処理は、ECのリバランシング手順の実行中に24時間以上かかると失敗することがあります。該当するILMルールで取り込み時にBalanced配置またはStrict配置が使用されている場合、長時間のPUT処理は失敗します。次のエラーが報告されます。 `500 Internal Server Error`

- ジョブ完了条件。ECのリバランシング手順は、次のいずれかに該当する場合は完了したとみなされます。
  - イレイジャーコーディングされたデータをこれ以上移動することはできません。
  - すべてのノードのデータは、目標とする使用可能領域パーティションの5%以内の偏差に収まっています。
  - 手順は30日間実行されています。

手順

1. [[review_object_storage]] リバランシングするサイトの現在のオブジェクトストレージの詳細を確認します。
   a. *ノード*を選択します。
   b. サイトで最初のストレージノードを選択します。
   c. [* ストレージ *] タブを選択します。
   d. [Storage Used - Object Data]グラフにカーソルを合わせ、ストレージノード上のレプリケートデータとイレイジャーコーディングデータの現在の量を確認します。
   e. 同じ手順を繰り返して、サイトの他のストレージノードを表示します。
2. プライマリ管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`
   b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

      rootとしてログインすると、プロンプトがからに `#`変わります `$`。
3. 手順 を起動します。

   `rebalance-data start — site "*site-name*"

   「*site-name*」には、新しいストレージノードを最初に追加したサイトを指定します。引用符で囲み `site-name`ます。

   EC Rebalance 手順 が開始され、ジョブ ID が返されます。
4. ジョブ ID をコピーします。
5. EC再バランス手順のステータスを監視します。
   - 単一の EC Rebalance 手順 のステータスを表示するには、次の手順を実行します

```
rebalance-data status --job-id job-id
```

には *job-id*、手順の開始時に返されたIDを指定します。

- 現在の EC Rebalance 手順 と、以前に完了した手順のステータスを表示するには、次の手順を実行します。

```
rebalance-data status
```

> rebalance -dataコマンド のヘルプを表示するには、次の手順を実行します。
>
> ```
> rebalance-data --help
> ```

6. 返されたステータスに基づいて、追加の手順を実行します。

   - がの `In progress`場合、 `State`ECリバランシング処理は引き続き実行されています。手順 は、完了するまで定期的に監視する必要があります。

     サイト内のストレージ ノード間のデータ分散を評価するには、[ノード] ページに移動します。

   ECリバランス処理は、すべてのノードの使用可能容量が目標とする使用可能容量パーティションの5%以内の偏差になった時点で完了とみなされ、停止します。

   - がの `Success`場合は `State`、必要に応じてオブジェクトストレージを確認するサイトの更新された詳細を表示します。

     サイトのストレージノード間で、使用可能な容量がより均等に配分されるはずです。

   - が `Failure`次の場合 `State`：

     i. サイトのすべてのストレージノードがグリッドに接続されていることを確認します。

     ii. これらのストレージノードに影響している可能性があるアラートがないかどうかを確認し、解決してください。

     iii. ECリバランシング手順 を再起動します。

     ```
     rebalance-data start --job-id job-id
     ```

     iv. ステータスの表示新しい手順の。がまだの `Failure`場合は `State`、テクニカルサポートにお問い合わせください。

7. EC Rebalance 手順 によって大量の負荷が生成されている（取り込み処理に影響があるなど）場合は、手順 を一時停止します。

   ```
   rebalance-data pause --job-id job-id
   ```

8. EC のリバランシング手順 を終了する必要がある場合（ StorageGRID ソフトウェアのアップグレードを実行できるようにする場合など）は、次のように入力します。

   ```
   rebalance-data terminate --job-id job-id
   ```

ECのリバランシング手順を終了すると、移動済みのデータフラグメントは新しい場所に残ります。データは元の場所に戻されません。

9. 複数のサイトでイレイジャーコーディングを使用している場合は、影響を受ける他のすべてのサイトに対してこの手順 を実行します。

StorageGRIDの拡張エラーのトラブルシューティング

グリッド拡張プロセス中に解決できないエラーが発生した場合やグリッドタスクが失敗した場合は、ログファイルを収集してテクニカルサポートにお問い合わせください。

テクニカルサポートに連絡する前に、トラブルシューティングに役立つ必要なログファイルを収集してください。

手順

1. デフォルトでは外部 SSH アクセスはブロックされます。必要に応じて、"一時的にアクセスを許可する" 。
2. 障害が発生した拡張ノードに接続します。
   a. 次のコマンドを入力します： `ssh -p 8022 admin@grid_node_IP`

      ポート 8022 はベース OS の SSH ポートで、ポート 22 は StorageGRID を実行しているコンテナエンジンの SSH ポートです。

   b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

   rootとしてログインすると、プロンプトがからに `#`変わります `$`。
3. インストールの段階に応じて、グリッドノードから次のいずれかのログを取得します。

プラットフォーム	ログ
VMware	• `/var/log/daemon.log` • `/var/log/storagegrid/daemon.log` • `/var/log/storagegrid/nodes/<node-name>.log`
Linux	• `/var/log/storagegrid/daemon.log` • `/etc/storagegrid/nodes/<node-name>.conf`（障害が発生した各ノード） • `/var/log/storagegrid/nodes/<node-name>.log`（障害が発生した各ノード。存在しない場合もあります）

4. 外部SSHアクセスを許可している場合は、"アクセスをブロックする"タスクが完了したら。

StorageGRIDシステムの保守

StorageGRIDグリッドのメンテナンス

グリッドのメンテナンスタスクには、ノードまたはサイトの運用停止、グリッド、ノードまたはサイトの名前変更、ネットワークのメンテナンスが含まれます。ホストとミドルウェアの手順やグリッドノードの手順を実行することもできます。

これらの手順では、「Linux」は Red Hat® Enterprise Linux® (RHEL)、Ubuntu®、または Debian® のデプロイメントを指します。サポートされているバージョンのリストについては、"NetApp Interoperability Matrix Tool" 。

開始する前に

- StorageGRID システムを幅広く理解している。
- StorageGRID システムのトポロジを確認し、グリッドの設定を把握しておきます。
- すべての指示に厳密に従い、すべての警告に注意する必要があります。
- ここで説明していないメンテナンス手順がサポートされていないか、サービス契約が必要であることを理解しておきます。

アプライアンスのメンテナンス手順

ハードウェアの手順については、を参照して "StorageGRIDアプライアンスのメンテナンス手順"ください。

StorageGRID 復旧パッケージをダウンロードします

リカバリ パッケージ ファイルを使用すると、障害が発生した場合にStorageGRIDシステムを復元できます。

開始する前に

- どの管理ノードからでも、グリッドマネージャにサインインするには、"サポートされている Web ブラウザ" 。
- プロビジョニングパスフレーズを用意します。
- そうだな "特定のアクセス権限"

StorageGRIDシステムのグリッド トポロジを変更する前、またはソフトウェアをアップグレードする前に、現在のリカバリ パッケージ ファイルをダウンロードしてください。次に、グリッド トポロジを変更した後、またはソフトウェアをアップグレードした後、リカバリ パッケージの新しいコピーをダウンロードします。

手順

1. メンテナンス > システム > *回復パッケージ*を選択します。
2. プロビジョニングパスフレーズを入力し、*[ダウンロードの開始]*を選択します。

   ダウンロードがすぐに開始されます。

3. ダウンロードが完了したら、ファイルを開き `.zip`、ファイルを含むコンテンツにアクセスできることを確認し `Passwords.txt`ます。
4. ダウンロードしたリカバリパッケージファイルをコピーします(`.zip`) を 2 つの安全でセキュリティ保護された別の場所に保管します。

> リカバリ パッケージ ファイルには、 StorageGRIDシステムからデータを取得するために使用できる暗号化キーとパスワードが含まれているため、セキュリティで保護する必要があります。

ノードまたはサイトの運用を停止

StorageGRIDノードまたはサイトの運用停止

手順 の運用停止を実行して、グリッドノードまたはサイト全体を StorageGRID システムから完全に削除できます。

グリッドノードまたはサイトを削除するには、次のいずれかの運用停止手順を実行します。

- を実行"グリッドノードの運用停止"して、1つ以上のノードを削除します。ノードは1つ以上のサイトに配置できます。削除するノードは、オンラインで StorageGRID システムに接続されている場合とオフラインで切断されている場合があります。
- を実行し"サイトの運用停止"てサイトを削除します。すべてのノードがStorageGRID に接続されている場合は、*接続サイトの運用停止*を実行します。すべてのノードがStorageGRID から切断されている場合は、*切断されたサイトの運用停止*を実行します。接続されているノードと切断されているノードがサイトに混在している場合は、オフラインのすべてのノードをオンラインに戻す必要があります。

> 切断されているサイトの運用停止を実行する前に、NetAppの営業担当者にお問い合わせください。運用停止サイトのウィザードですべての手順を有効にする前に、要件を確認してください。切断されているサイトの運用停止は、サイトをリカバリしたり、サイトからオブジェクトデータをリカバリしたりできる可能性がある場合は、試行しないでください。

グリッド ノードを廃止する前に、アクティブなデータ修復ジョブがないことを確認する必要があります。修復に失敗した場合は、修復を再起動して完了させてから廃止手順を実行する必要があります。。 "データ修復ジョブを確認します" 。

ノードの運用停止

StorageGRIDグリッドノードの運用停止

ノードの運用停止手順を使用して、1つ以上のサイトにある1つ以上のグリッドノードを削除できます。プライマリ管理ノードは運用停止できません。

ノードの運用を停止するタイミング

次のいずれかに該当する場合は、ノードの運用停止手順 を使用します。

- 拡張時に大容量のストレージノードを追加し、オブジェクトを保持したまま小さなストレージノードを1

つ以上削除する場合。

古いアプライアンスを新しいアプライアンスに交換する場合は、拡張の際に新しいアプライアンスを追加してから古いアプライアンスの運用を停止するのではなく、検討して "アプライアンスノードのクローニング"ください。

- 総ストレージ容量を減らす必要がある場合。
- ゲートウェイノードが不要になった場合。
- 非プライマリ管理ノードが不要になった場合。
- 切断されているノードがグリッドに含まれており、リカバリまたはオンラインに戻すことはできません。
- グリッドにアーカイブノードがあります。

ノードの運用を停止する方法

接続されているグリッドノードまたは切断されているグリッドノードの運用を停止できます。

接続されているノードの運用停止

一般的に、グリッド ノードを廃止する場合は、それらがStorageGRIDシステムに接続されており、すべてのノードの状態が正常である ([ノード] ページと [ノードの廃止] ページに緑色のアイコンが表示される) 場合にのみ行う必要があります。

手順については、を参照してください"接続されているグリッドノードの運用を停止"。

切断されているノードの運用停止

場合によっては、グリッドに現在接続されていないノード（[Health]が[Unknown]または[Administratively Down]のノード）の運用停止が必要になることがあります。

手順については、を参照してください"切断されているグリッドノードの運用を停止"。

ノードの運用を停止する前の考慮事項

いずれかの手順を実行する前に、各タイプのノードに関する考慮事項を確認してください。

- "管理ノードまたはゲートウェイノードの運用停止に関する考慮事項"
- "ストレージノードの運用停止に関する考慮事項"

StorageGRID Adminノードまたは**Gateway**ノードの運用停止に関する考慮事項

管理ノードまたはゲートウェイノードの運用停止に関する考慮事項を確認します。

管理ノードに関する考慮事項

- プライマリ管理ノードは運用停止できません。
- いずれかのネットワークインターフェイスがハイアベイラビリティ（HA）グループに属している管理ノードの運用を停止することはできません。最初に、 HA グループからネットワークインターフェイスを削除する必要があります。の手順を参照してください"HAグループの管理"。
- 必要に応じて、管理ノードの運用停止中にILMポリシーを安全に変更できます。

- シングルサインオン（ SSO ）が有効な StorageGRID システムで管理ノードの運用を停止した場合は、ノードの証明書利用者信頼を Active Directory フェデレーションサービス（ AD FS ）から削除する必要があります。
- を使用する場合は"グリッドフェデレーション"、運用停止するノードのIPアドレスがグリッドフェデレーション接続用に指定されていないことを確認してください。
- 切断されている管理ノードの運用を停止すると、そのノードの監査ログが失われますが、これらのログはプライマリ管理ノードにも存在している必要があります。

ゲートウェイノードに関する考慮事項

- いずれかのネットワークインターフェイスがハイアベイラビリティ（HA）グループに属しているゲートウェイノードの運用を停止することはできません。最初に、 HA グループからネットワークインターフェイスを削除する必要があります。の手順を参照してください"HAグループの管理"。
- 必要に応じて、ゲートウェイノードの運用停止中にILMポリシーを安全に変更できます。
- を使用する場合は"グリッドフェデレーション"、運用停止するノードのIPアドレスがグリッドフェデレーション接続用に指定されていないことを確認してください。
- 切断されているゲートウェイノードは安全に運用停止できます。

ストレージノードに関する考慮事項

StorageGRIDにおけるストレージノードの廃止に関する考慮事項

ストレージノードの運用を停止する前に、ノードをクローニングできるかどうかを検討してください。その後、ノードの運用を停止する場合は、手順の運用停止時にStorageGRIDがオブジェクトとメタデータをどのように管理するかを確認します。

ノードの運用停止ではなくクローンを作成するタイミング

古いアプライアンスストレージノードを新しいアプライアンス以上のアプライアンスに交換する場合は、拡張で新しいアプライアンスを追加してから古いアプライアンスの運用を停止するのではなく、アプライアンスノードをクローニングすることを検討してください。

アプライアンスノードのクローニングを使用すると、同じStorageGRIDサイトにある既存のアプライアンスノードを互換性のあるアプライアンスと簡単に交換できます。クローニングプロセスでは、すべてのデータが新しいアプライアンスに転送され、新しいアプライアンスが稼働状態になり、古いアプライアンスはインストール前の状態のままになります。

アプライアンスノードは、次の処理が必要な場合にクローニングできます。

- 寿命に達しているアプライアンスを交換します。
- 既存のノードをアップグレードして、強化されたアプライアンステクノロジを活用します。
- StorageGRID システム内のストレージノードの数を変更することなく、グリッドのストレージ容量を拡張できます。
- RAIDモードの変更などにより、ストレージ効率が向上します。

詳細は、を参照してください "アプライアンスノードのクローニング"。

接続されているストレージノードに関する考慮事項

接続されているストレージノードの運用停止に関する考慮事項を確認します。

- 1 つのノードの運用停止手順 では、 10 個を超えるストレージノードの運用を停止しないでください。
- システムは常に、運用要件（"ADCクォーラム"およびアクティブな"ILMポリシー"を含む）を満たすのに十分なストレージノードを備えている必要があります。廃止によってサイトのADC数がクォーラムを下回る場合、StorageGRID は ADC サービスを同じサイト内の利用可能な非ADCストレージノードに自動的に移動し、ADCクォーラムを維持します。ADCサービスを自動的に移動できない場合は、既存のストレージノードを廃止する前に"拡張操作で新しいストレージノードを追加する"が必要になることがあります。

  ソフトウェアベースのメタデータのみのノードを含むグリッド内のストレージノードの運用を停止する場合は注意が必要です。store_both_objectsとmetadataに設定されているすべてのノードの運用を停止すると、オブジェクトを格納する機能がグリッドから削除されます。メタデータ専用ストレージノードの詳細については、を参照してください"ストレージノードのタイプ"。

- ストレージノードを削除すると、大量のオブジェクトデータがネットワーク経由で転送されます。この転送が通常のシステム処理に影響することはありませんが、StorageGRIDシステムが消費するネットワーク帯域幅の総量に影響する可能性があります。
- ストレージノードの運用停止に関連するタスクは、通常のシステム処理に関連するタスクよりも優先度が低くなっています。つまり、運用停止処理が StorageGRID の通常のシステム処理を妨げることはなく、システムがアクティブでない期間に運用停止処理をスケジュールする必要もありません。運用停止処理はバックグラウンドで実行されるため、プロセスの所要時間を見積もることは困難です。一般に、システムがビジー状態でないとき、または一度に 1 つのストレージノードのみを削除するときは、運用停止処理が迅速に終了します。
- ストレージノードの運用停止には、数日から数週間かかることがあります。それに応じてこの手順 を計画してください運用停止プロセスはシステム処理に影響しないように設計されていますが、他の手順が制限される可能性があります。一般に、システムのアップグレードや拡張を計画している場合は、グリッドノードを削除する前に実行する必要があります。
- ストレージノードの削除中に別のメンテナンス手順を実行する必要がある場合は、別の手順の完了後に再開できます"運用停止手順を一時停止します。"。

> * Pause * ボタンは、 ILM 評価またはイレイジャーコーディングデータの運用停止ステージに達したときにのみ有効になります。ただし、 ILM 評価（データ移行）はバックグラウンドで継続して実行されます。

- 運用停止タスクの実行中は、どのグリッドノードでもデータ修復処理を実行できません。
- ストレージノードの運用停止中は、ILMポリシーに変更を加えないでください。
- データを完全かつ安全に削除するには、運用停止手順の完了後にストレージノードのドライブを消去する必要があります。

切断されているストレージノードに関する考慮事項

切断されているストレージノードの運用停止に関する考慮事項を確認してください。

- 切断されているノードは、オンラインにしたりリカバリしたりできないことが確実である場合を除き、運用停止しないでください。

ノードからオブジェクトデータをリカバリできる可能性がある場合は、この手順 を実行しないでください。代わりに、テクニカルサポートに問い合わせて、ノードのリカバリが可能かどうかを確認してください。

- 切断されているストレージノードの運用を停止すると、StorageGRIDは他のストレージノードのデータを使用して、切断されているノード上にあったオブジェクトデータとメタデータを再構築します。
- 切断されている複数のストレージノードの運用を停止すると、データが失われる可能性があります。十分な数のオブジェクトコピー、イレイジャーコーディングフラグメント、またはオブジェクトメタデータが残っていると、システムがデータを再構築できない場合があります。ソフトウェアベースのメタデータ専用ノードがあるグリッド内のストレージノードの運用を停止する場合は、オブジェクトとメタデータの両方を格納するように設定されたすべてのノードの運用を停止すると、グリッドからすべてのオブジェクトストレージが削除されます。メタデータ専用ストレージノードの詳細については、を参照してください"ストレージノードのタイプ"。

切断されていてリカバリできないストレージノードが複数ある場合は、テクニカルサポートに連絡して、最適な対処方法を確認してください。

- 切断されているストレージノードの運用を停止すると、 StorageGRID は運用停止手順の終了時にデータ修復ジョブを開始します。これらのジョブは、切断されているノードに格納されていたオブジェクトデータとメタデータの再構築を試みます。
- 切断されているストレージノードの運用を停止する場合、手順 の運用停止は比較的短時間で完了します。ただし、データ修復ジョブは実行に数日から数週間かかることがあり、運用停止手順 によって監視されません。これらのジョブは手動で監視し、必要に応じて再開してください。を参照して "データ修復ジョブを確認します"
- オブジェクトの唯一のコピーを含む切断されているストレージノードの運用を停止すると、そのオブジェクトは失われます。データ修復ジョブは、現在接続されているストレージノードに、 1 つ以上のレプリケートコピーまたは十分なイレイジャーコーディングフラグメントが含まれている場合のみ、オブジェクトを再構築してリカバリできます。

StorageGRID ADC定足数とは何ですか？

ADCクォーラムは、各サイトで最低限の数の管理ドメインコントローラー（ADC）サービスが利用可能であることを保証します。StorageGRIDは、必要に応じて廃止措置時にADCサービスを自動的に移動します。

一部のストレージノードにあるADCサービスは、グリッドトポロジ情報を管理し、設定サービスをグリッドに提供します。StorageGRID システムでは、各サイトで ADC サービスのクォーラムが常に利用可能である必要があります。

ノードを削除すると原因 ADCクォーラムが満たされなくなる場合は、ストレージノードの運用を停止できません。運用停止中にADCクォーラムを満たすには、各サイトで少なくとも3つのストレージノードにADCサービスが必要です。ADCサービスを使用するストレージノードがサイトに3つ以上ある場合は、運用停止後もそれらのノードの過半数が利用可能な状態のままである必要があります。 `((0.5 * Storage Nodes with ADC) + 1)`

ソフトウェアベースのメタデータのみのノードを含むグリッド内のストレージノードの運用を停止する場合は注意が必要です。store_both_objectsとmetadataに設定されているすべてのノードの運用を停止すると、オブジェクトを格納する機能がグリッドから削除されます。メタデータ専用ストレージノードの詳細については、を参照してください"ストレージノードのタイプ"。

たとえば、ADCサービスがあるストレージノードが6つあるサイトにあり、3つのストレージノードの運用を停止するとします。ADC クォーラムの要件により、次の 2 つの運用停止手順を実行する必要があります。

- 最初の運用停止手順では、ADCサービスを使用する4つのストレージノードを引き続き使用できるようにする必要があります。 `((0.5 * 6) + 1)`そのため、最初に運用停止できるのは、 2 つのストレージノードのみです。
- 2 番目の廃止手順では、ADC クォーラムで使用可能な状態を保つために必要な ADC サービスが 3 つだけになったため、3 番目のストレージ ノードを削除できます。 `((0.5 * 4) + 1)`。

ADCサービスを持つストレージノードを廃止する場合、廃止によってサイトのADC数がクォーラムを下回るときは、StorageGRIDはADCサービスを同じサイト内の別のストレージノードに自動的に移動します。自動移動を実行するには、グリッド内のすべてのノードが接続されていること、およびサービスを受信するために同じサイトにADC以外のストレージノードが利用可能であることが必要です。廃止手順では、サイトごとに最低3台のADCストレージノードを維持します。例えば、あるサイトで4つまたは6つのADCノードを廃止した場合、同じサイトに利用可能な非ADCノードが存在すると仮定すると、手順完了後には3つのADCストレージノードが残ります。

ADCサービスを自動的に移動できない場合は、"ADCサービスを手動で移動する"同じサイト内の別のストレージノードへ移動するか、または"拡張時に新しいストレージノードを追加する"ADCサービスを備えるように指定することができます。そうすれば、クォーラムに影響を与えることなく、既存のストレージノードを廃止できます。

StorageGRID ILM ポリシーとストレージ構成を確認する

ストレージノードの運用を停止する場合は、運用停止プロセスを開始する前に StorageGRID システムの ILM ポリシーを確認してください。

運用停止時に、運用停止されたストレージノードのすべてのオブジェクトデータが他のストレージノードに移行されます。

運用停止中の ILM ポリシーは、運用停止後のポリシーとして使用されます。運用停止を開始する前と運用停止の完了後に、このポリシーがデータの要件を満たしていることを確認する必要があります。

各のルールを確認して、ストレージノードの運用停止に対応できるように、StorageGRIDシステムの容量が適切な場所に適切なタイプの十分な容量を引き続き確保する必要があり"アクティブなILMポリシー"ます。

次の点を考慮してください。

- ILM 評価サービスで ILM ルールを満たすようにオブジェクトデータをコピーすることは可能か。
- 運用停止処理の進行中にサイトが一時的に使用不能になった場合は、どうなりますか？追加のコピーを別の場所に作成できるか。
- 運用停止プロセスは、コンテンツの最終的な配信にどのように影響しますか。で説明されているように"ストレージノードを統合します"、古いシステムの運用を停止する前に実行する必要があります"新しいスト

レージノードを追加します"。小さいストレージノードの運用を停止してから、交換用に大きいストレージノードを追加すると、以前からあるストレージノードが容量の限界に近づき、新しいストレージノードにはほとんどコンテンツが存在しない状態になる可能性があります。新しいオブジェクトデータの書き込み処理のほとんどは新しいストレージノードに送信されるため、システム処理の全体的な効率が低下します。

- アクティブなILMポリシーを満たす十分な数のストレージノードが常にシステムに含まれているか。

> ILMポリシーを満たすことができないと、バックログやアラートが発生し、StorageGRIDシステムの運用が停止する可能性があります。

次の表に示す領域を評価して、運用停止プロセスの結果として提示される推奨トポロジがILMポリシーを満たしていることを確認します。

評価する領域	考慮事項
使用可能容量	StorageGRIDシステムに格納されているすべてのオブジェクトデータ（運用を停止するストレージノードに現在格納されているオブジェクトデータの永続的なコピーを含む）を格納できるだけの十分なストレージ容量を確保できるか。 運用停止処理が完了してから妥当な期間にわたって格納されるオブジェクトデータの予測される増加に対応できるだけの十分な容量を確保できるか。
ストレージの場所	StorageGRID システム全体に十分な容量が残っている場合、StorageGRID システムのビジネスルールを満たす適切な場所に容量が配置されているか。
ストレージタイプ	運用停止処理が完了したあとに、適切なタイプのストレージを十分に確保できるか。 たとえば、コンテンツが古くなったときに、ILMルールによってあるタイプのストレージから別のタイプのストレージにコンテンツが移動されることがあります。この場合、StorageGRIDシステムの最終構成で、適切なタイプのストレージが十分に確保されていることを確認する必要があります。

StorageGRIDストレージノードの統合

ストレージノードを統合すると、サイトや環境のストレージノード数を減らしながら、ストレージ容量を増やすことができます。

ストレージノードを統合する場合は"StorageGRIDシステムを拡張する"、容量の大きい新しいストレージノードを追加してから、容量の小さい古いストレージノードの運用を停止します。手順 の運用を停止すると、オブジェクトが古いストレージノードから新しいストレージノードに移行されます。

古いアプライアンスと小規模なアプライアンスを新しいモデルまたは大容量のアプライアンスに統合する場合は、検討して "アプライアンスノードのクローニング"ください（1対1の交換を行わない場合は、アプライアンスノードのクローニングと運用停止手順を使用してください）。

たとえば、 3 つの古いストレージノードを 2 つの新しい大容量のストレージノードで置き換えます。最初に拡張手順 を使用して 2 つの新しい大容量のストレージノードを追加し、そのあとに運用停止手順 を使用して 3 つの古い小容量のストレージノードを削除します。

既存のストレージノードを削除する前に新たな容量を追加することで、 StorageGRID システム全体でバランスよくデータを分散できます。また、既存のストレージノードがストレージのウォーターマークレベルを超える可能性が低くなります。

複数のStorageGRIDストレージノードを廃止する

複数のストレージノードを削除する必要がある場合は、運用停止処理を順次実行することも並列に実行することもできます。

ソフトウェアベースのメタデータのみのノードを含むグリッド内のストレージノードの運用を停止する場合は注意が必要です。store_both_objectsとmetadataに設定されているすべてのノードの運用を停止すると、オブジェクトを格納する機能がグリッドから削除されます。メタデータ専用ストレージノードの詳細については、を参照してください"ストレージノードのタイプ"。

- 複数のストレージノードの運用を順次停止する場合は、最初のストレージノードの運用停止が完了するのを待ってから、次のストレージノードの運用停止を開始する必要があります。
- 複数のストレージノードの運用を並列に停止する場合は、対象となるすべてのストレージノードで同時に運用停止タスクが処理されます。その結果、ファイルの永続的なコピーがすべて「読み取り専用」とマークされ、この機能が有効になっているグリッドでの削除が一時的に無効になる可能性があります。

StorageGRID でデータ修復ジョブを確認する

グリッド ノードを廃止または拡張する前に、アクティブなデータ修復ジョブがないことを確認する必要があります。修復に失敗した場合は、修復を再起動して完了させてから廃止手順を実行する必要があります。

- 参照"カクチヨウタイフ"グリッド ノードを展開する方法の詳細については、こちらをご覧ください。
- グリッドマネージャーを使用して、進行中の復元プロセスを監視し、復元履歴を表示します。以下の手順を参照してください。
  - "アプライアンスのストレージボリュームにオブジェクトデータをリストアします"
  - "システムドライブに損傷がない場合は、オブジェクトデータをストレージボリュームにリストアします"
  - "オブジェクトデータをストレージボリュームにリストアする（システムドライブの障害）"

StorageGRIDノードの運用停止に必要な資料を収集

グリッドノードの運用停止を実行する前に、次の情報を取得する必要があります。

項目	脚注
回復パッケージ `.zip`ファイル	絶対です"最新のリカバリパッケージをダウンロードする" `.zip`ファイル（`sgws-recovery-package-id-revision.zip`）。障害が発生した場合、リカバリ パッケージ ファイルを使用してシステムを復元できます。
`Passwords.txt`ファイル	このファイルには、コマンド ラインでグリッド ノードにアクセスするために必要なパスワードが含まれており、リカバリ パッケージに含まれています。
プロビジョニングパスフレーズ	このパスフレーズは、 StorageGRID システムが最初にインストールされるときに作成されて文書化されます。プロビジョニングパスフレーズがファイルに含まれていません `Passwords.txt`。
運用停止前の StorageGRID システムのトポロジの概要	システムの現在のトポロジを記載したドキュメントがあれば、すべて入手します。

関連情報

"Web ブラウザの要件"

StorageGRID のノード廃止ページにアクセスする

Grid Manager の Decommission Nodes ページにアクセスすると、運用停止できるノードが一目でわかります。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"Maintenance権限またはRoot Access権限"。

> ソフトウェアベースのメタデータのみのノードを含むグリッド内のストレージノードの運用を停止する場合は注意が必要です。store_both_objectsとmetadataに設定されているすべてのノードの運用を停止すると、オブジェクトを格納する機能がグリッドから削除されます。メタデータ専用ストレージノードの詳細については、を参照してください"ストレージノードのタイプ"。

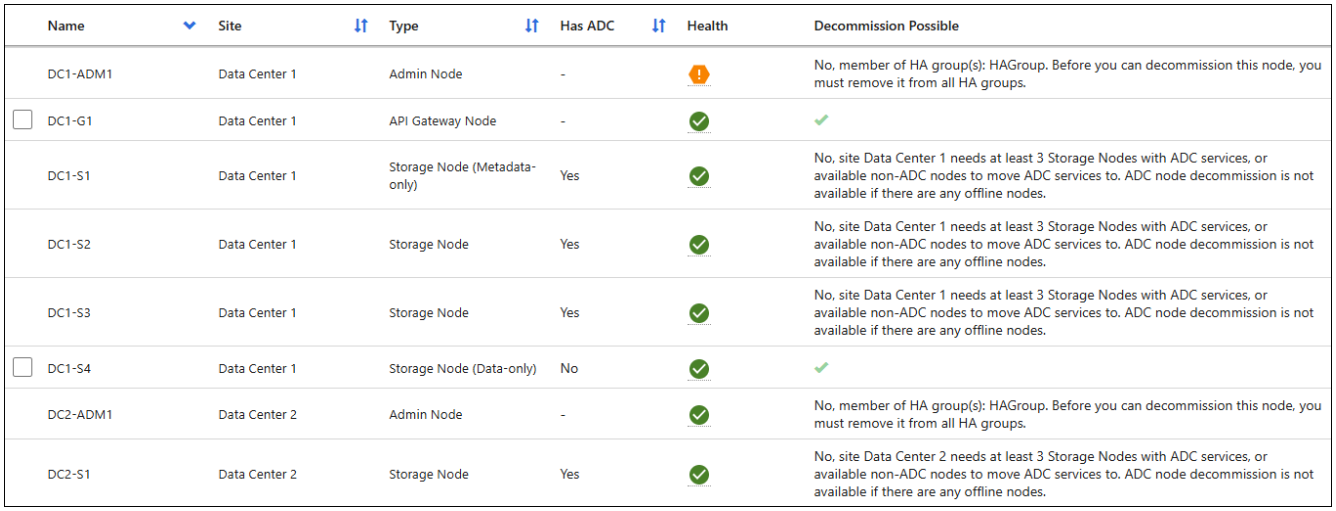
手順

1. メンテナンス > タスク > *廃止*を選択します。
2. [Decommission Nodes] を選択します。

   Decommission Nodes ページが表示されます。このページでは、次の操作を実行できます。

   - 現時点で運用停止できるグリッドノードを確認できます。
   - すべてのグリッドノードの健全性を確認できます
   - リストを * Name * 、 * Site * 、 * Type * 、または * has ADC* で昇順または降順にソートします。
   - 検索キーワードを入力すると、特定のノードをすばやく検索できます。

この例では、「廃止可能」列に緑色のチェックマークが表示されている場合、API ゲートウェイノードとデータ専用ストレージノードを廃止できることを示しています。他のノードは、さまざまな理由により廃止することができません。例えば、プライマリ管理ノードは、このノードタイプの廃止がサポートされていないため、廃止できません。メタデータ専用のストレージノードは、サイトが "ADC クォーラム" を満たさなくなるため、廃止することはできません。



Name	Site	Type	Has ADC	Health	Decommission Possible
DC1-ADM1	Data Center 1	Admin Node	-		No, member of HA group(s): HAGroup. Before you can decommission this node, you must remove it from all HA groups.
DC1-G1	Data Center 1	API Gateway Node	-		✔
DC1-S1	Data Center 1	Storage Node (Metadata-only)	Yes		No, site Data Center 1 needs at least 3 Storage Nodes with ADC services, or available non-ADC nodes to move ADC services to. ADC node decommission is not available if there are any offline nodes.
DC1-S2	Data Center 1	Storage Node	Yes		No, site Data Center 1 needs at least 3 Storage Nodes with ADC services, or available non-ADC nodes to move ADC services to. ADC node decommission is not available if there are any offline nodes.
DC1-S3	Data Center 1	Storage Node	Yes		No, site Data Center 1 needs at least 3 Storage Nodes with ADC services, or available non-ADC nodes to move ADC services to. ADC node decommission is not available if there are any offline nodes.
DC1-S4	Data Center 1	Storage Node (Data-only)	No		✔
DC2-ADM1	Data Center 2	Admin Node	-		No, member of HA group(s): HAGroup. Before you can decommission this node, you must remove it from all HA groups.
DC2-S1	Data Center 2	Storage Node	Yes		No, site Data Center 2 needs at least 3 Storage Nodes with ADC services, or available non-ADC nodes to move ADC services to. ADC node decommission is not available if there are any offline nodes.

3. 運用停止するノードごとに「 * Decommission possible * 」列を確認します。

運用停止できるグリッドノードの場合は、この列に緑のチェックマークが表示され、左側の列にチェックボックスが表示されます。運用停止できないノードの場合、この列には問題 が表示されます。ノードを運用停止できない理由が複数ある場合は、最も重大な理由が表示されます。

運用停止の可能性がある理由	製品説明	解決する手順
NO、_node type_decommissioningはサポートされていません。	プライマリ管理ノードは運用停止できません。	ありません。
いいえ。少なくとも 1 つのグリッドノードが切断されています。 注意: このメッセージは、接続されたグリッド ノードに対してのみ表示されます。	切断されているグリッドノードがあると、接続されているグリッドノードの運用を停止できません。 • Health * 列には、切断されているグリッドノード用の次のアイコンが表示されます。 ◦ （灰色）：管理上の停止 ◦ （青）：不明	切断されているすべてのノードをオンラインに戻すか、接続されているノードを削除する必要があります"切断されているすべてのノードの運用停止"。 注：グリッドに切断されているノードが複数ある場合は、それらをすべて同時に運用停止する必要があるため、予期しない結果が生じる可能性があります。

運用停止の可能性がある理由	製品説明	解決する手順
いいえ。必要なノードが現在切断されており、リカバリが必要です。 注意: このメッセージは、切断されたグリッド ノードに対してのみ表示されます。	必要なノード（ADCクォーラムに必要なストレージノードなど）も切断されている場合は、切断されているグリッドノードの運用を停止できません。	a. 切断されているすべてのノードについて、運用停止の可能性があるメッセージを確認します。 b. 必要なノードであるため運用停止できないノードを特定します。 ◦ 必要なノードのヘルスが「 Administratively Down 」の場合は、ノードをオンラインに戻します。 ◦ 必要なノードの健全性が「 Unknown 」の場合は、ノードリカバリ手順を実行して必要なノードをリカバリします。
いいえ、HA グループのメンバーです: グループ名。このノードを廃止する前に、すべての HA グループから削除する必要があります。	ノードインターフェイスがハイアベイラビリティ（HA）グループに属している管理ノードまたはゲートウェイノードの運用を停止することはできません。	HA グループを編集して、ノードのインターフェイスを削除するか、 HA グループ全体を削除します。を参照して "ハイアベイラビリティグループを設定する"
いいえ、サイト *x* には、ADC サービスを備えたストレージノードが少なくとも 3 つ、または ADC サービスを移動するための利用可能な非 ADC ノードが必要です。いずれかのノードがオフラインになっている場合、ADC ノードの廃止は利用できません。	ストレージノードのみ（統合ストレージノードまたはメタデータ専用ストレージノード）。サイトに十分な数のノードが残らず、ADCクォーラム要件を満たせない場合、またはADCサービスを自動的に移動できない場合は、ストレージノードを廃止することはできません。自動移動には、グリッド全体で2つ以上のADCストレージノードがオンラインであること、および同じサイト上に利用可能な非ADCストレージノードがあることが必要です。	自動ADCサービス移動の条件が満たされていることを確認してください（"ADCクォーラム"を参照）。または、同一サイト内の別のストレージノードへ"ADCサービスを手動で移動する"してください。また、サイトに新しいストレージノードを追加し、そのノードにADCサービスを持たせるように指定することで、拡張を行うこともできます。"StorageGRID にグリッドノードを追加するワークフローの概要"を参照してください。

運用停止の可能性がある理由	製品説明	解決する手順
いいえ。イレイジャーコーディングプロファイルには少なくとも_n_ストレージノードが必要です。プロファイルが ILM ルールで使用されていない場合は、非アクティブ化できます。	ストレージ ノードのみ。既存の消去コーディング プロファイルに十分なノードが残っていない限り、ストレージ ノードを廃止することはできません。 たとえば、4+2のイレイジャーコーディング用のイレイジャーコーディングプロファイルがある場合は、少なくとも6個のストレージノードを残す必要があります。	影響を受けるイレイジャーコーディングプロファイルごとに、プロファイルの使用方法に応じて次のいずれかの手順を実行します。 • アクティブな**ILM**ポリシーで使用：拡張を実行します。イレイジャーコーディングを続行できるように十分な数の新しいストレージノードを追加してください。の手順を参照してください"グリッドを拡張します"。 • * ILMルールで使用されているが、アクティブなILMポリシーでは使用されていない*：ルールを編集または削除し、イレイジャーコーディングプロファイルを非アクティブ化します。 • どの**ILM**ルールでも使用されていない：イレイジャーコーディングプロファイルを非アクティブ化します。 *注：*イレイジャーコーディングプロファイルを非アクティブ化しようとしたときに、オブジェクトデータがまだプロファイルに関連付けられている場合は、エラーメッセージが表示されます。無効化プロセスを再度実行する前に、数週間待つ必要がある場合があります。 詳細はこちらをご覧ください "イレイジャーコーディングプロファイルの非アクティブ化"。
いいえ。ノードが切断されていないかぎり、アーカイブノードの運用を停止することはできません。	アーカイブノードが接続されている場合は削除できません。	注：アーカイブノードのサポートは削除されました。アーカイブノードの運用を停止する必要がある場合は、を参照してください。 "グリッドノードの運用停止（StorageGRID 11.8ドキュメントサイト）"

グリッドに現在接続されていないノード（「 Health 」が「 Unknown 」または「 Administratively Down 」のノード）の運用を停止することが必要になる場合があります。

開始する前に

- 運用停止に関する考慮事項と運用停止に関する考慮事項について理解しておく"管理ノードとゲートウェイノード""ストレージノード"必要があります。
- 前提条件となる項目をすべて用意しておきます。
- アクティブなデータ修復ジョブがないことを確認しておきます。を参照して "データ修復ジョブを確認します"
- グリッド内でストレージノードのリカバリが実行中でないことを確認します。実行中の場合は、リカバリの一環として実行される Cassandra の再構築が完了するまで待機する必要があります。そのあとで運用停止を続行できます。
- ノード運用停止手順 が一時停止されていないかぎり、ノード手順 の運用停止中に他のメンテナンス手順が実行されないようにしておきます。
- 運用停止するノードの * 運用停止可能な * 列には、緑のチェックマークが表示されます。
- プロビジョニングパスフレーズを用意します。

タスクの内容

Health 列で青色の「不明」アイコン または灰色の「管理上ダウン」アイコン を探すことで、切断されたノードを特定できます。

切断されているノードの運用を停止する前に、次の点に注意して

- この手順 は、主に切断されている 1 つのノードを削除することを目的としています。グリッド内に切断されているノードが複数ある場合は、それらのノードをすべて同時に運用停止する必要があるため、予期しない結果になる可能性があります。

> 切断されている複数のストレージノードを一度に運用停止すると、データが失われる可能性があります。を参照して "切断されているストレージノードに関する考慮事項"

> ソフトウェアベースのメタデータのみのノードを含むグリッド内のストレージノードの運用を停止する場合は注意が必要です。store_both_objectsとmetadataに設定されているすべてのノードの運用を停止すると、オブジェクトを格納する機能がグリッドから削除されます。メタデータ専用ストレージノードの詳細については、を参照してください"ストレージノードのタイプ"。

- 切断されているノードを削除できない場合（ADCクォーラムに必要なストレージノードなど）は、切断されている他のノードを削除できません。

手順

1. アーカイブノードの運用を停止する場合（切断する必要があります）を除き、切断されているグリッドノードをオンラインに戻すか、リカバリします。

   手順については'を参照して "グリッドノードのリカバリ手順" ください

2. 切断されているグリッドノードをリカバリできず、切断されている間に運用を停止する場合は、そのノードのチェックボックスを選択します。

   グリッド内に切断されているノードが複数ある場合は、それらのノードをすべて同時に運用停止する必要があるため、予期しない結果になる可能性があります。

   切断されている複数のグリッドノードの運用を一度に停止する場合、特に複数のストレージノードを選択する場合は注意が必要です。切断されていてリカバリできないストレージノードが複数ある場合は、テクニカルサポートに連絡して、最適な対処方法を確認してください。

3. プロビジョニングパスフレーズを入力します。

   [* 分解を開始 * （ Start Decommission * ）] ボタンが有効になります。

4. 「廃止措置の開始」を選択します。

   切断されているノードが選択されていることと、そのノードにオブジェクトの唯一のコピーが含まれている場合はオブジェクトデータが失われることを示す警告が表示されます。

5. ノードの一覧を確認し、**OK** を選択してください。

   廃止手順が開始され、各ノードの進行状況が表示されます。手順中に、グリッド構成の変更を含む新しいリカバリ パッケージが生成されます。

6. 新しいリカバリパッケージが利用可能になったら、リンクを選択するか、メンテナンス > システム > リカバリパッケージ を選択してリカバリパッケージページにアクセスしてください。次に、 `.zip`ファイルをダウンロードします。

   説明書をご覧ください"リカバリパッケージのダウンロード"。

   廃止手順中に問題が発生した場合にグリッドを回復できるように、できるだけ早く回復パッケージをダウンロードしてください。

   リカバリ パッケージ ファイルには、 StorageGRIDシステムからデータを取得するために使用できる暗号化キーとパスワードが含まれているため、セキュリティで保護する必要があります。

7. 運用停止ページを定期的に監視して、選択したすべてのノードの運用が正常に停止されることを確認してください。

   ストレージノードの運用停止には、数日から数週間かかることがあります。すべてのタスクが完了すると、成功メッセージとともにノード選択リストが再表示されます。切断されているストレージノードの運用を停止した場合は、修復ジョブが開始されたことを示す情報メッセージが表示されます。

8. 運用停止手順 の一環としてノードが自動的にシャットダウンされたら、運用停止したノードに関連付けられている残りの仮想マシンやその他のリソースをすべて削除します。

   ノードが自動的にシャットダウンされるまで、この手順を実行しないでください。

9. ストレージノードを廃止する場合は、廃止プロセス中に自動的に開始される*レプリケートデータ*および*イレイジャーコーディング（EC）データ*の修復ジョブのステータスを監視してください。

レプリケートデータ

- 修理が完了しているかどうかを確認するには、次
  i. ノード > 修復中のストレージノード > **ILM** を選択します。
  ii. 「評価」セクションの属性を確認します。修理が完了すると、 *Awaiting - All * 属性は 0 個のオブジェクトを示します。
- 修理を詳細に監視するには、次の手順を実行します。
  i. *ノード*を選択します。
  ii. ***grid name***>*ilm * を選択します。
  iii. ILM キュー グラフの上にカーソルを置くと、スキャン レート **(**オブジェクト**/**秒**)** 属性の値が表示されます。これは、グリッド内のオブジェクトがスキャンされ、ILM のキューに入れられるレートです。
  iv. ILM キュー セクションで、次の属性を確認します。
    - * Scan Period - Estimated *：ILMによるすべてのオブジェクトのフルスキャンが完了するまでの推定時間。

      完全スキャンでは、すべてのオブジェクトに ILM が適用されていることが保証されません。

    - 試行された修復: 高リスクと見なされる複製されたデータに対して試行されたオブジェクト修復操作の合計数。高リスク オブジェクトとは、ILM ポリシーによって指定されているか、コピーの損失の結果として、コピーが 1 つ残っているオブジェクトのことです。このカウントは、ストレージ ノードが高リスクのオブジェクトの修復を試みるたびに増加します。グリッドが混雑している場合は、リスクの高い ILM 修復が優先されます。

      修復後にレプリケーションが失敗した場合、同じオブジェクトの修復が再度増加する可能性があります。 + これらの属性は、ストレージ ノード ボリュームのリカバリの進行状況を監視するときに役立ちます。修復の試行回数の増加が止まり、完全スキャンが完了した場合、修復は完了したと考えられます。

  v. あるいは、Prometheusクエリを送信して `storagegrid_ilm_scan_period_estimated_minutes`そして `storagegrid_ilm_repairs_attempted`。

イレイジャーコーディング（**EC**）データ

消去符号化データの修復を監視し、失敗した可能性のあるリクエストを再試行するには、サポート > ツール > メトリクス を選択して、現在のジョブの完了までの推定時間と完了率を表示します。次に、Grafana セクションで **EC** 概要 を選択します。**Grid EC Job Estimated Time to Completion** と **Grid EC Job Percentage Completed** のダッシュボードを確認します。

終了後

切断されているノードが運用停止され、すべてのデータ修復ジョブが完了したら、必要に応じて、接続されているグリッドノードの運用を停止できます。

その後、手順 の運用停止が完了したら、次の手順を実行します。

- 運用停止したグリッドノードのドライブを確実に消去します。市販のデータ消去ツールまたはデータ消去サービスを使用して、ドライブからデータを完全かつ安全に削除します。
- アプライアンスノードの運用を停止し、ノード暗号化を使用してアプライアンスのデータが保護されていた場合は、 StorageGRID アプライアンスインストーラを使用してキー管理サーバ設定（ Clear KMS ）をクリアします。アプライアンスを別のグリッドに追加する場合は、 KMS の設定をクリアする必要があります。手順については、を参照してください "メンテナンスモードでノード暗号化を監視します"。

接続された**StorageGRID**ノードの運用停止

グリッドに接続されているノードは、運用停止して完全に削除できます。

開始する前に

- 運用停止に関する考慮事項と運用停止に関する考慮事項について理解しておく"管理ノードとゲートウェイノード""ストレージノード"必要があります。
- 必要な情報やデータ、機器をすべて揃えておきます。
- アクティブなデータ修復ジョブがないことを確認しておきます。
- グリッド内でストレージノードのリカバリが実行中でないことを確認します。停止している場合は、リカバリの一環として実行されたCassandraの再構築が完了するまで待ちます。そのあとで運用停止を続行できます。
- ノード運用停止手順 が一時停止されていないかぎり、ノード手順 の運用停止中に他のメンテナンス手順が実行されないようにしておきます。
- プロビジョニングパスフレーズを用意します。
- Grid ノードが接続されています。
- 運用を停止するノードの*[Decommission Possible]*列に緑のチェックマークが表示されている。

> 1つ以上のボリュームがオフライン（アンマウント済み）の場合、またはオンライン（マウント済み）でエラー状態の場合、運用停止は開始されません。

> 運用停止の実行中に1つ以上のボリュームがオフラインになると、それらのボリュームがオンラインに戻ったあとに運用停止プロセスが完了します。

- すべてのグリッドノードは正常（緑色）の状態です。**Health** 列にこれらのアイコンのいずれかが表示されている場合は、問題を解決する必要があります：

をクリックします。	色	重大度
	黄	通知
	薄いオレンジ	マイナー
	濃いオレンジ	メジャー

をクリックします。	色	重大度
	赤	重大

- 以前に切断されているストレージノードの運用を停止した場合は、データ修復ジョブがすべて正常に完了している。を参照して "データ修復ジョブを確認します"



この手順 で指示されるまでは、グリッドノードの仮想マシンやその他のリソースを削除しないでください。



ソフトウェアベースのメタデータのみのノードを含むグリッド内のストレージノードの運用を停止する場合は注意が必要です。store_both_objectsとmetadataに設定されているすべてのノードの運用を停止すると、オブジェクトを格納する機能がグリッドから削除されます。メタデータ専用ストレージノードの詳細については、を参照してください"ストレージノードのタイプ"。

タスクの内容

運用を停止すると、ノードのサービスは無効になり、ノードは自動的にシャットダウンされます。

手順

1. [Decommission Nodes]ページで、運用を停止する各グリッドノードのチェックボックスを選択します。
2. プロビジョニングパスフレーズを入力します。

   [* 分解を開始 * （ Start Decommission * ）] ボタンが有効になります。

3. [Start Decommission]*を選択します。
4. 確認ダイアログでノードのリストを確認し、*[OK]*を選択します。

   ノードの運用停止手順 が開始され、各ノードの進捗状況が表示されます。

   運用停止手順 の開始後にストレージノードをオフラインにしないでください。状態を変更すると、一部のコンテンツが他の場所にコピーされなくなる可能性があります。

5. 新しいリカバリ パッケージが利用可能になったらすぐに、バナーのリカバリ パッケージ リンクを選択するか、[メンテナンス] > [システム] > [リカバリ パッケージ] を選択してリカバリ パッケージ ページにアクセスします。次に、 `.zip`ファイル。

   見る"リカバリパッケージのダウンロード" 。

   廃止手順中に問題が発生した場合にグリッドを回復できるように、できるだけ早く回復パッケージをダウンロードしてください。

6. Decommission Nodes ページを定期的に監視して、選択したすべてのノードの運用が正常に停止されることを確認します。

   ストレージノードの運用停止には、数日から数週間かかることがあります。

すべてのタスクが完了すると、成功メッセージとともにノード選択リストが再表示されます。

終了後

ノードの運用停止手順 が完了したら、次の手順を実行します。

1. プラットフォームに応じた手順に従います。例：
   - **Linux**: ボリュームをデタッチし、インストール中に作成したノード構成ファイルを削除する必要がある場合があります。見る"ソフトウェアベースのノードにStorageGRIDをインストールする" 。
   - * VMware *：vCenterの[ディスクから削除]オプションを使用して仮想マシンを削除できます。また、仮想マシンに依存しないデータディスクを削除しなければならない場合もあります。
   - * StorageGRID アプライアンス * ：アプライアンスノードは自動的に導入されていない状態に戻り、StorageGRID アプライアンスインストーラにアクセスできます。アプライアンスの電源をオフにするか、別の StorageGRID システムに追加できます。
2. 運用停止したグリッドノードのドライブを確実に消去します。市販のデータ消去ツールまたはデータ消去サービスを使用して、ドライブからデータを完全かつ安全に削除します。
3. アプライアンスノードの運用を停止し、ノード暗号化を使用してアプライアンスのデータが保護されていた場合は、 StorageGRID アプライアンスインストーラを使用してキー管理サーバ設定（ Clear KMS ）をクリアします。アプライアンスを別のグリッドに追加する場合は、 KMS の設定をクリアする必要があります。手順については、を参照してください "メンテナンスモードでノード暗号化を監視します"。

StorageGRID ストレージノードの廃止プロセスを一時停止して再開します

2 回目のメンテナンス手順 を実行する必要がある場合は、ストレージノードの運用停止手順 を特定の段階で一時停止できます。もう一方の手順 の運用停止が完了したら、運用停止手順を再開できます。

> * Pause * ボタンは、 ILM 評価またはイレイジャーコーディングデータの運用停止ステージに達したときにのみ有効になります。ただし、 ILM 評価（データ移行）はバックグラウンドで継続して実行されます。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"Maintenance権限またはRoot Access権限"。

手順

1. メンテナンス > タスク > *廃止*を選択します。

   Decommission ページが表示されます。

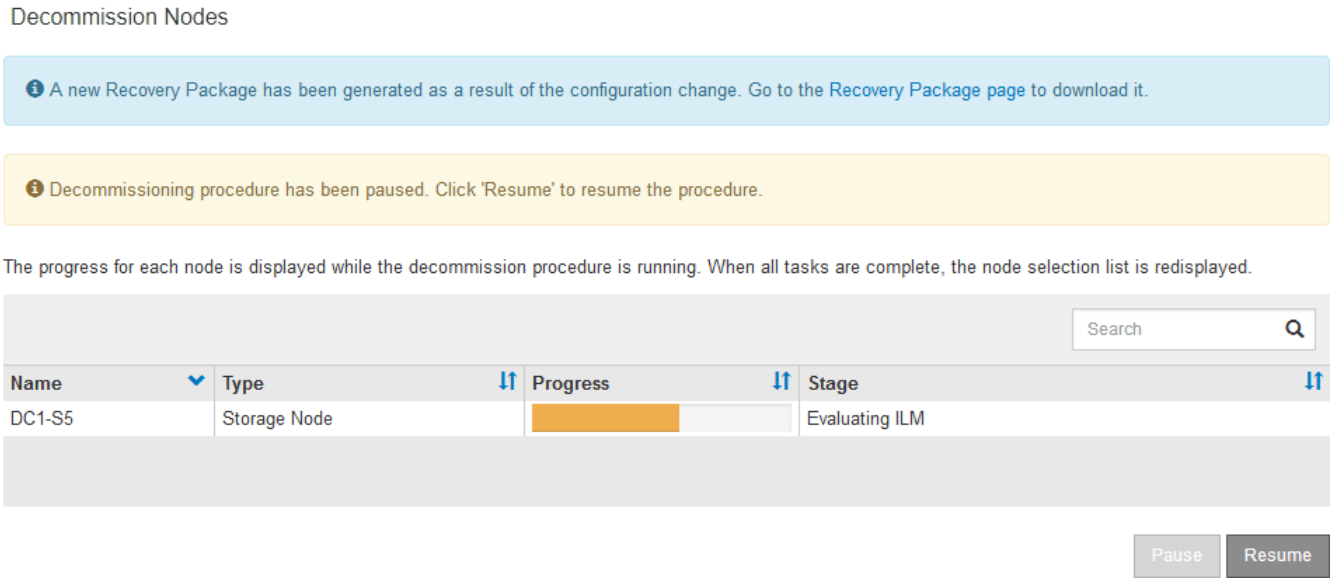
2. [Decommission Nodes] を選択します。

   Decommission Nodes ページが表示されます。手順 の運用停止が次のいずれかの段階に達すると、 * 一時停止 * ボタンが有効になります。

   - ILM を評価中です
   - イレイジャーコーディングデータの運用停止

3. 手順 を一時停止するには、 * 一時停止 * を選択します。

   現在のステージが一時停止され、 * Resume * （続行）ボタンが有効になります。



4. もう一方のメンテナンス手順 が終了したら、 [* Resume （続行）] を選択して運用停止を続行します。

運用停止サイト

StorageGRIDにおけるサイトの運用停止に関する考慮事項

サイトの運用停止手順 を使用してサイトを削除する前に、考慮事項を確認しておく必要があります。

サイトの運用を停止した場合の動作

サイトの運用を停止すると、 StorageGRID はサイトのすべてのノードとサイト自体を StorageGRID システムから完全に削除します。

サイトの運用停止手順 が完了したら、次の手順を実行します

- StorageGRID を使用してサイトやサイトの任意のノードを表示したり、アクセスしたりすることはできなくなります。
- サイトを参照していたストレージプールやイレイジャーコーディングプロファイルは使用できなくなります。StorageGRIDでサイトの運用を停止すると、ストレージプールが自動的に削除され、イレイジャーコーディングプロファイルが非アクティブ化されます。

接続されているサイトと切断されているサイトの運用停止手順の違い

サイト運用停止手順 を使用すると、すべてのノードが StorageGRID に接続されているサイト（接続されていないサイトの運用停止と呼ばれる）を削除したり、すべてのノードが StorageGRID から切断されているサイト（切断されたサイトの運用停止と呼ばれる）を削除したりできます。作業を開始する前に、これらの手順の違いを理解しておく必要があります。

サイトに接続されたノード（）と切断されたノード（または）が混在している場合は、オフラインのノードをすべてオンラインに戻す必要があります。

- 接続されたサイトの運用停止機能を使用すると、 StorageGRID システムから運用サイトを削除できます。たとえば、接続されたサイトの運用停止を実行して、機能しているが不要になったサイトを削除できます。
- StorageGRID は、接続されているサイトを削除する際、 ILM を使用してサイトのオブジェクトデータを管理します。接続されたサイトの運用停止を開始するには、すべての ILM ルールからサイトを削除し、新しい ILM ポリシーをアクティブ化する必要があります。オブジェクトデータを移行するための ILM プロセスとサイトを削除するための内部プロセスは同時に発生する可能性がありますが、実際の運用停止手順を開始する前に ILM の手順を完了しておくことを推奨します。
- 切断されたサイトの運用停止機能を使用すると、障害が発生したサイトを StorageGRID システムから削除できます。たとえば、切断されたサイトの運用停止を実行して、火災や洪水によって破壊されたサイトを削除できます。

  切断されているサイトを削除すると、 StorageGRID はすべてのノードをリカバリ不能とみなし、データの保持を試みません。ただし、切断されたサイトの運用停止を開始する前に、サイトをすべての ILM ルールから削除して、新しい ILM ポリシーをアクティブ化する必要があります。

切断されたサイトの運用停止手順 を実行する前に、ネットアップのアカウント担当者にお問い合わせください。運用停止サイトのウィザードですべての手順を有効にする前に、要件を確認してください。切断されているサイトの運用停止は、サイトをリカバリしたり、サイトからオブジェクトデータをリカバリしたりできる可能性がある場合は、試行しないでください。

接続されているサイトまたは切断されているサイトを削除するための一般的な要件

接続されているサイトや切断されているサイトを削除する前に、次の要件について確認しておく必要があります。

- プライマリ管理ノードを含むサイトは運用停止できません。
- いずれかのノードのインターフェイスがハイアベイラビリティ（HA）グループに属している場合は、サイトの運用を停止できません。HA グループを編集してノードのインターフェイスを削除するか、 HA グループ全体を削除する必要があります。
- 接続済み（）と切断済み（または）ノードが混在しているサイトは廃止できません。
- 他のサイトのいずれかのノードが切断されている場合、サイトを廃止することはできません（または）。
- ec-node-repair処理が実行中の場合は、サイトの運用停止手順 を開始できません。イレイジャーコーディングデータの修復の追跡については、を参照してください"データ修復ジョブを確認します"。
- サイトの運用停止中は、手順 は次の処理を実行します。
  - 運用停止するサイトを参照するILMルールを作成することはできません。また、既存のILMルールを編集してサイトを参照することもできません。
  - 拡張やアップグレードなど、その他のメンテナンス手順は実行できません。

接続されているサイトの運用停止中に別のメンテナンス手順を実行する必要がある場合は、実行できます"ストレージノードを削除している間に手順 を一時停止します"。* Pause * ボタンは、 ILM 評価またはイレイジャーコーディングデータの運用停止ステージに達したときにのみ有効になります。ただし、 ILM 評価（データ移行）はバックグラウンドで継続して実行されます。2 つ目のメンテナンス手順 が完了したら、運用停止手順を再開できます。

    - サイトの運用停止手順 の開始後にノードをリカバリする必要がある場合は、サポートにお問い合わせください。

- 一度に複数のサイトを運用停止することはできません。
- サイトに 1 つ以上の管理ノードが含まれており、 StorageGRID システムでシングルサインオン（ SSO ）が有効になっている場合は、そのサイトに対する証明書利用者信頼をすべて Active Directory フェデレーションサービス（ AD FS ）から削除する必要があります。

情報ライフサイクル管理（ **ILM** ）の要件

サイトを削除する場合は、 ILM 設定を更新する必要があります。Decommission Site ウィザードでは、次のことを確認するために、いくつかの前提条件となる手順を実行できます。

- このサイトはILMポリシーでは参照されていません。該当する場合は、ポリシーを編集するか、新しいILMルールを使用してポリシーを作成してアクティブ化する必要があります。
- サイトを参照するILMルールはありません。ルールがどのポリシーでも使用されていない場合でも同様です。サイトを参照するすべてのルールを削除または編集する必要があります。

StorageGRIDはサイトの運用を停止すると、サイトを参照している未使用のイレイジャーコーディングプロファイルを自動的に非アクティブ化し、サイトを参照している未使用のストレージプールを自動的に削除します。All Storage Nodesストレージプール（StorageGRID 11.6以前）が存在する場合は、すべてのサイトを使用するため削除されます。

サイトを削除する前に、新しい ILM ルールを作成して新しい ILM ポリシーをアクティブ化する必要がある場合があります。以下の手順は、ILMの仕組みを十分に理解していること、およびストレージプール、イレイジャーコーディングプロファイル、ILMルールの作成、およびILMポリシーのシミュレートとアクティブ化に精通していることを前提としています。を参照して"ILM を使用してオブジェクトを管理する"

接続されているサイトでのオブジェクトデータに関する考慮事項

接続されたサイトの運用停止を実行する場合は、新しい ILM ルールと新しい ILM ポリシーを作成するときに、サイトの既存のオブジェクトデータで実行する処理を決定する必要があります。次のいずれか、または両方を実行できます。

- 選択したサイトからグリッド内の 1 つ以上の他のサイトにオブジェクトデータを移動します。
- データ移動の例 * ：サニーベールで新しいサイトを追加したために、ローリーでサイトの運用を停止するとします。この例では、すべてのオブジェクトデータを古いサイトから新しいサイトに移動します。ILMルールとILMポリシーを更新する前に、両方のサイトの容量を確認する必要があります。サニーベールサイトにローリーサイトのオブジェクトデータを保存できるだけの十分な容量があり、将来の成長に備えてサニーベールに十分な容量が残っていることを確認する必要があります。

十分な容量を確保するには、この手順を実行する前に、既存のサイトにストレージボリュームまたはストレージノードを追加するか、新しいサイトを追加しなければならない場合があり"グリッドを展開する"ます。

- 選択したサイトからオブジェクトコピーを削除します。
- データの削除の例 * ：現在、 3 コピーの ILM ルールを使用して 3 つのサイト間でオブジェクトデータをレプリケートしているとします。サイトの運用を停止する前に、同等の 2-copy ILM ルールを作成して、 2 つのサイトにのみデータを格納することができます。2-copy ルールを使用する新しい ILM ポリシーをアクティブ化すると、 ILM 要件を満たさなくなるため、 StorageGRID は 3 番目のサイトからコピーを削除します。ただし、オブジェクトデータは引き続き保護され、残りの 2 つのサイトの容量は同じになります。

サイトの削除に対応するためにシングルコピーの ILM ルールを作成しないでください。ある期間にレプリケートコピーを 1 つしか作成しない ILM ルールには、データが永続的に失われるリスクがあります。オブジェクトのレプリケートコピーが 1 つしかない場合、ストレージノードに障害が発生したり、重大なエラーが発生すると、そのオブジェクトは失われます。また、アップグレードなどのメンテナンス作業中は、オブジェクトへのアクセスが一時的に失われます。

接続されたサイトの運用停止に関する追加要件

StorageGRID で接続されているサイトを削除する前に、次の点を確認してください。

- StorageGRID システム内のすべてのノードの接続状態が「接続済み」（）である必要があります。ただし、ノードにはアクティブなアラートが存在する可能性があります。

1 つ以上のノードが切断されている場合は、 Decommission Site ウィザードの手順 1~4 を完了できます。ただし、すべてのノードが接続されていないかぎり、運用停止プロセスを開始するウィザードの手順5を完了することはできません。

- 削除するサイトにロードバランシングに使用されるゲートウェイノードまたは管理ノードが含まれている場合は、同等の新しいノードを別のサイトに追加しなければならないことがあります"グリッドを展開する"。サイトの運用停止手順 を開始する前に、クライアントが交換用ノードに接続できることを確認してください。
- 削除するサイトにハイアベイラビリティ（ HA ）グループ内のゲートウェイノードまたは管理ノードがある場合は、運用停止サイトウィザードの手順 1~4 を完了できます。ただし、運用停止プロセスを開始するウィザードの手順5を完了するには、これらのノードをすべてのHAグループから削除する必要があります。既存のクライアントがサイトのノードを含む HA グループに接続している場合は、サイトの削除後も引き続き StorageGRID に接続できることを確認する必要があります。
- 削除するサイトのストレージノードにクライアントが直接接続している場合は、サイトの運用停止手順 を開始する前に、それらのクライアントが他のサイトのストレージノードに接続できることを確認する必要があります。
- アクティブなILMポリシーの変更によって移動されるオブジェクトデータを格納できる十分なスペースを残りのサイトに確保する必要があります。場合によっては、接続されているサイトの運用停止を完了する前に、ストレージノード、ストレージボリューム、または新しいサイトの追加が必要になる"グリッドを展開する"ことがあります。
- 手順 の運用停止が完了するまでに、十分な時間を確保する必要があります。StorageGRID の ILM プロセスの運用が停止されるまでに、サイトからオブジェクトデータを移動または削除するのに数日、数週間、

場合によっては数カ月かかることがあります。

> サイトからオブジェクトデータを移動または削除するには、サイトのデータ量、システムの負荷、ネットワークのレイテンシ、および ILM に求められる変更の性質に応じて、数日、数週間、場合によっては数カ月かかることがあります。

- Decommission Site ウィザードの手順 1~4 をできるだけ早く完了する必要があります。実際の運用停止手順 を開始する前にサイトからデータを移動できるようにすると（ウィザードの手順 5 で「運用停止 * を開始」を選択して）、運用停止手順 の処理がより迅速になり、システム停止やパフォーマンスへの影響も少なくなります。

切断されたサイトの運用停止に関する追加要件

StorageGRID で切断されているサイトを削除する前に、次の点を確認してください。

- ネットアップのアカウント担当者に連絡しておきます。運用停止サイトのウィザードですべての手順を有効にする前に、要件を確認してください。

> 切断されているサイトの運用停止は、サイトをリカバリしたり、サイトからオブジェクトデータをリカバリしたりできる可能性がある場合は、試行しないでください。を参照して "テクニカルサポートによるサイトのリカバリ方法"

- サイトのすべてのノードの接続状態が次のいずれかである必要があります。
  - 不明 （） ： 不明な理由により、ノードが切断されたか、ノード上のサービスが予期せず停止しました。例えば、ノード上のサービスが停止したり、停電や予期せぬ障害によってノードのネットワーク接続が失われたりする可能性があります。
  - 管理上のダウン (): ノードは想定される理由によりグリッドに接続されていません。例えば、ノードまたはノード上のサービスが正常にシャットダウンされた場合などです。
- 他のすべてのサイトのすべてのノードは、接続状態が*接続済み*（）である必要があります。ただし、これらの他のノードにはアクティブなアラートが存在する可能性があります。
- StorageGRID を使用してサイトに格納されているオブジェクトデータを表示したり読み出したりすることができなくなることを理解しておく必要があります。StorageGRID はこの手順 を実行する際、切断されているサイトのデータを一切保持しません。

> ILM ルールとポリシーが単一サイトの損失を防ぐように設計されている場合は、オブジェクトのコピーが残りのサイトに存在します。

- あるオブジェクトの唯一のコピーがサイトに格納されていた場合、オブジェクトは失われて読み出せないことを理解しておく必要があります。

サイトを削除した場合の整合性に関する考慮事項

S3バケットの整合性によって、StorageGRIDがオブジェクトメタデータをすべてのノードとサイトに完全にレプリケートしてから、オブジェクトの取り込みが成功したことをクライアントに通知するかどうかが決まります。整合性では、オブジェクトの可用性と、異なるストレージノードおよびサイト間でのオブジェクトの整合性のバランスが維持されます。

StorageGRID でサイトを削除するときは、削除するサイトにデータが書き込まれていないことを確認する必

要があります。そのため、各バケットまたはコンテナの整合性が一時的に上書きされます。サイトの運用停止プロセスの開始後、 StorageGRID は一時的に strong-site 整合性を使用し、オブジェクトのメタデータがサイトに書き込まれないようにします。

この一時的な上書きの結果、残りのサイトで複数のノードが使用できなくなった場合、サイトの運用停止中に発生するクライアントの書き込み、更新、および削除の処理が失敗する可能性があることに注意してください。

StorageGRIDサイトの運用停止に必要な資料を収集

サイトの運用を停止する前に、以下を準備しておく必要があります。

項目	脚注
回復パッケージ `.zip`ファイル	最新のリカバリパッケージをダウンロードする必要があります `.zip`ファイル（`sgws-recovery-package-id-revision.zip`）。障害が発生した場合、リカバリ パッケージ ファイルを使用してシステムを復元できます。 "リカバリパッケージをダウンロードする"
`Passwords.txt`ファイル	このファイルには、コマンド ラインでグリッド ノードにアクセスするために必要なパスワードが含まれており、リカバリ パッケージに含まれています。
プロビジョニングパスフレーズ	このパスフレーズは、 StorageGRID システムが最初にインストールされるときに作成されて文書化されます。プロビジョニングパスフレーズがファイルに含まれていません `Passwords.txt`。
運用停止前の StorageGRID システムのトポロジの概要	システムの現在のトポロジを記載したドキュメントがあれば、すべて入手します。

関連情報

"Web ブラウザの要件"

StorageGRIDで廃止措置を行うサイトを選択してください

サイトの運用を停止できるかどうかを判断するには、まず Decommission Site ウィザードにアクセスします。

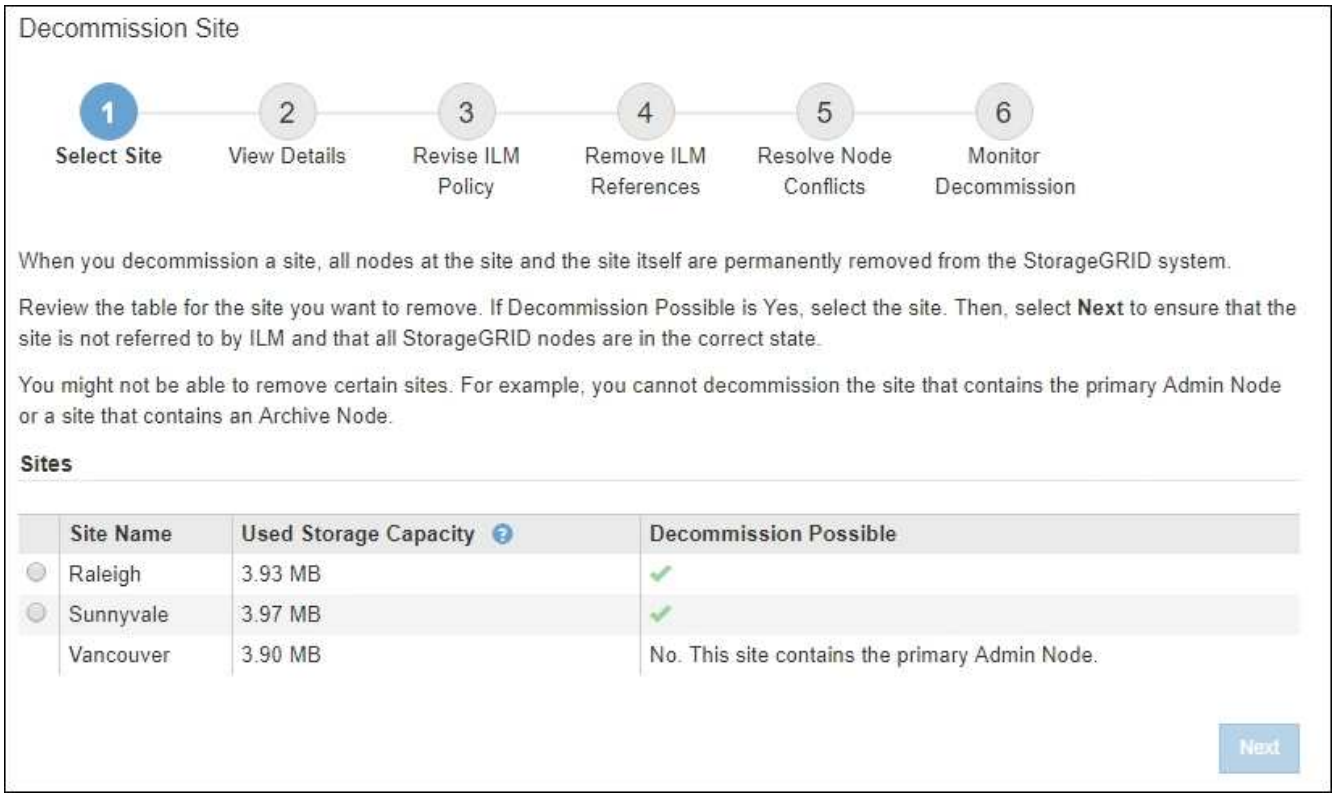
開始する前に

- 必要な情報や資料をすべて入手しておきます。
- サイトの削除に関する考慮事項を確認しておきます。
- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"rootアクセス権限またはMaintenance権限とILM権限"。

手順

1. メンテナンス > タスク > *廃止*を選択します。
2. [Decommission Site] を選択します。

   Decommission Site ウィザードの Step 1 （ Select Site ）が表示されます。この手順には、 StorageGRID システムのサイトのアルファベット順に記載されています。



3. 「使用済みストレージ容量」列の値を確認し、各サイトのオブジェクトデータに現在使用されているストレージの容量を特定します。

   使用済みストレージ容量は概算値です。ノードがオフラインの場合は、ストレージの使用容量が最後に確認されたサイトの値になります。

   - 接続されたサイトの運用停止の場合、この値は、このサイトを安全に運用停止するために、他のサイトに移動したり、 ILM によって削除したりする必要があるオブジェクトデータの量を表します。
   - 切断されているサイトの運用停止の場合、この値は、このサイトの運用を停止するとシステムのデータストレージにアクセスできなくなる容量を表します。

     単一サイトの損失を防ぐように ILM ポリシーを設定した場合、オブジェクトデータのコピーが残りのサイトに残っている必要があります。

4. 「 * Decommission possible * 」列の理由を確認して、現在運用停止できるサイトを特定します。

   サイトを運用停止できない理由が複数ある場合は、最も重大な理由が表示されます。

運用停止の可能性がある理由	製品説明	次の手順に進みます
緑色のチェックマーク（）	このサイトは運用停止できます。	にアクセスします。
いいえ。このサイトにはプライマリ管理ノードが含まれています。	プライマリ管理ノードを含むサイトは運用停止できません。	ありません。この手順 は実行できません。
いいえ。このサイトには1つ以上のアーカイブノードが含まれています。	アーカイブノードを含むサイトは運用停止できません。	ありません。この手順 は実行できません。
いいえ。このサイトのすべてのノードが切断されています。ネットアップの担当者にお問い合わせください。	サイト内のすべてのノードが接続されていない限り、接続済みサイトの廃止を実行することはできません（）。	切断されたサイトの運用停止を実行する場合は、ネットアップのアカウント担当者にお問い合わせください。この担当者が要件を確認し、残りの運用停止サイトウィザードを有効にします。 • 重要 * ：サイトを削除できるように、オンラインノードをオフラインにしないでください。データが失われます。

この例では、3つの拠点を持つStorageGRIDシステムを示しています。RaleighサイトとSunnyvaleサイトの緑色のチェックマーク（）は、これらのサイトを運用停止できることを示しています。ただし、Vancouverサイトにはプライマリ管理ノードが含まれているため、Vancouverサイトを運用停止することはできません。

1. 運用停止が可能な場合は、サイトのオプションボタンを選択します。

   「 * 次へ * 」ボタンが有効になっています。

2. 「 * 次へ * 」を選択します。

   手順 2 （詳細を表示）が表示されます。

StorageGRID で運用停止前にサイトの詳細を確認してください

運用停止サイトウィザードの手順 2 （詳細を表示）では、サイトに含まれているノード、各ストレージノードで使用されているスペースの量、およびグリッド内の他のサイトで利用可能な空きスペースの量を確認できます。

開始する前に

サイトの運用を停止する前に、サイトに格納されているオブジェクトデータの量を確認する必要があります。

- 接続されたサイトの運用停止処理を実行する場合は、 ILM を更新する前にサイトに現在存在しているオブジェクトデータの量を把握しておく必要があります。サイトの容量とデータ保護のニーズに基づいて、新しい ILM ルールを作成して、データを他のサイトに移動したり、サイトからオブジェクトデータを削除し

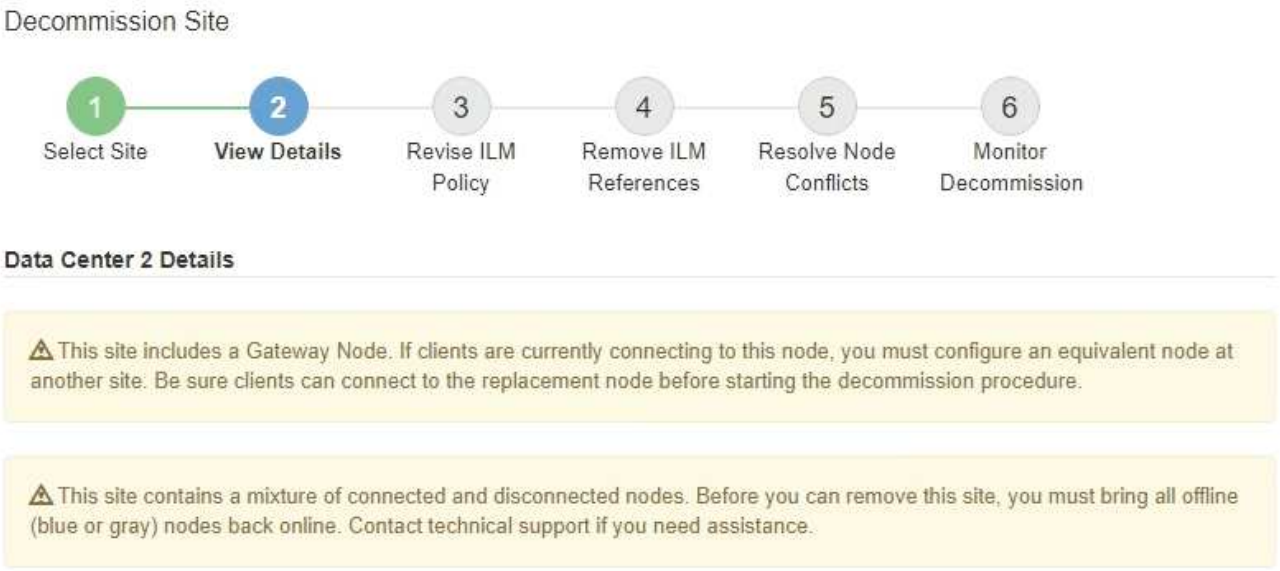
たりできます。

- 可能であれば、運用停止手順 を開始する前にストレージノードを拡張する必要があります。
- 切断されたサイトの運用停止処理を実行する場合は、サイトを削除した時点で永続的にアクセスできなくなるオブジェクトデータの量を把握しておく必要があります。

> 切断されているサイトの運用停止を実行する場合、ILMでオブジェクトデータを移動または削除することはできません。サイトに残っているデータはすべて失われます。ただし、単一サイトの損失を防ぐように ILM ポリシーが設計されている場合、オブジェクトデータのコピーは残りのサイトに残ります。を参照して "サイト障害からの保護を有効にします"

手順

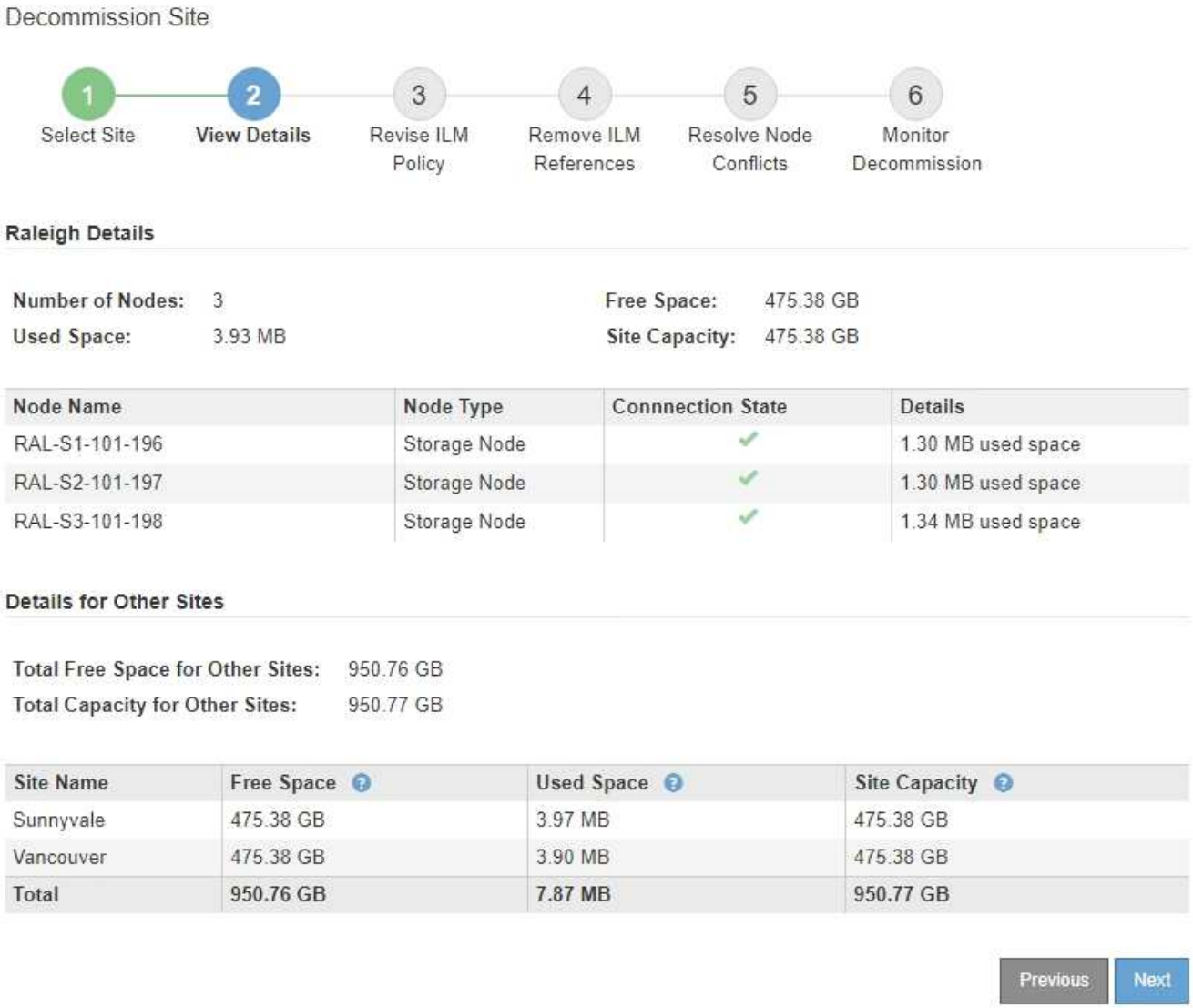
1. 手順 2 （詳細の表示）で、削除するように選択したサイトに関連する警告を確認します。



次の場合は警告が表示されます。

  - サイトにゲートウェイノードが含まれている。S3クライアントが現在このノードに接続している場合は、別のサイトに対応するノードを設定する必要があります。手順 の運用停止を続行する前に、クライアントが交換用ノードに接続できることを確認してください。
  - このサイトには、接続されたノード（）と切断されたノード（または）が混在しています。このサイトを削除する前に、オフラインになっているすべてのノードをオンラインに戻す必要があります。

2. 削除するように選択したサイトの詳細を確認します。



選択したサイトについては、次の情報が表示されます。

- ノード数
- サイト内のすべてのストレージノードの使用済みスペース、空きスペース、および容量の合計。
  - 接続されているサイトの運用停止の場合、「使用済みスペース」の値は、 ILM を使用して他のサイトに移動または削除する必要があるオブジェクトデータの量を表します。
  - 切断されたサイトの運用停止処理の場合、サイトを削除したときにアクセスできなくなるオブジェクトデータの量は「 * Used Space * 」の値で示されます。
- ノード名、タイプ、および接続状態：
  - （接続済み）
  - （Administratively Down）
  - （不明）
- 各ノードの詳細：
  - 各ストレージノードについて、オブジェクトデータに使用されているスペースの量。

- 管理ノードとゲートウェイノードの場合、ノードが現在ハイアベイラビリティ（HA）グループで使用されているかどうか。HAグループで使用されている管理ノードまたはゲートウェイノードは運用停止できません。運用停止を開始する前に、HAグループを編集してサイトのすべてのノードを削除するか、HAグループにこのサイトのノードのみが含まれている場合はHAグループを削除します。手順については、を参照してください"ハイアベイラビリティ（HA）グループを管理します"。

3. ページの詳細セクションで、グリッド内の他のサイトで利用可能なスペースを評価します。

Details for Other Sites

Total Free Space for Other Sites:	950.76 GB
Total Capacity for Other Sites:	950.77 GB

Site Name	Free Space	Used Space	Site Capacity
Sunnyvale	475.38 GB	3.97 MB	475.38 GB
Vancouver	475.38 GB	3.90 MB	475.38 GB
Total	950.76 GB	7.87 MB	950.77 GB

接続されたサイトの運用停止処理を実行していて、 ILM を使用して（削除するだけでなく）選択したサイトからオブジェクトデータを移動する場合は、移動されたデータに対応できる十分な容量を他のサイトに確保し、将来の拡張に備えて十分な容量を確保する必要があります。

削除するサイトの * 使用済みスペース * が、他のサイトの * 合計空きスペース * より大きい場合、警告が表示されます。サイトの削除後に十分なストレージ容量が確保されるようにするために、この手順 を実行する前に拡張の実行が必要になる場合があります。

4. 「 * 次へ * 」を選択します。

手順 3 （ ILM ポリシーの改訂）が表示されます。

StorageGRIDでサイトの廃止に関する**ILM**ポリシーを改訂する

[Decommission Site]ウィザードの[Step 3（Revise ILM Policies]）では、サイトがILMポリシーで参照されているかどうかを確認できます。

開始する前に

あなたは方法を十分に理解している"ILMによるオブジェクトの管理"ます。ストレージプールとILMルールの作成、およびILMポリシーのシミュレートとアクティブ化について十分に理解している。

タスクの内容

ポリシー（アクティブまたは非アクティブ）に含まれるILMルールがそのサイトを参照している場合、StorageGRIDはサイトの運用を停止できません。

運用を停止するサイトを参照しているILMポリシーがある場合は、それらのポリシーを削除するか、次の要件を満たすように編集する必要があります。

- すべてのオブジェクトデータを完全に保護
- 廃止するサイトを参照しないでください。

- サイトを参照するストレージプールを使用したり、[すべてのサイト]オプションを使用したりしないでください。
- サイトを参照するイレイジャーコーディングプロファイルは使用しないでください。
- StorageGRID 11.6以前のインストールでは、Make 2 Copiesルールは使用しないでください。

> サイトの削除に対応するためにシングルコピーの ILM ルールを作成しないでください。ある期間にレプリケートコピーを 1 つしか作成しない ILM ルールには、データが永続的に失われるリスクがあります。オブジェクトのレプリケートコピーが 1 つしかない場合、ストレージノードに障害が発生したり、重大なエラーが発生すると、そのオブジェクトは失われます。また、アップグレードなどのメンテナンス作業中は、オブジェクトへのアクセスが一時的に失われます。

> _connectedサイトの運用停止_を実行する場合は、削除するサイトの現在のオブジェクトデータをStorageGRIDがどのように管理するかを検討する必要があります。データ保護の要件に応じて、新しいルールで既存のオブジェクトデータを別のサイトに移動したり、不要になった余分なオブジェクトコピーを削除したりできます。

新しいポリシーの設計についてサポートが必要な場合は、テクニカルサポートにお問い合わせください。

手順

1. 手順3（[Revise ILM Policies]）で、運用停止対象として選択したサイトを参照するILMポリシーがないかどうかを確認します。
2. ポリシーが表示されない場合は、*[次へ]*を選択してに進みます"手順 4 ： ILM 参照を削除する"。
3. 1つ以上の_active_ILMポリシーが表示された場合は、既存の各ポリシーをクローニングするか、運用停止するサイトを参照しない新しいポリシーを作成します。

   a. [Policy Name]列でポリシーのリンクを選択します。

      ブラウザの新しいタブに、ポリシーのILMポリシーの詳細ページが表示されます。[Decommission Site] ページは、 [other] タブに表示されたままになります。

   b. 必要に応じて、次のガイドラインと手順に従ってください。

      - ILMルールの操作：
        - "1つ以上のストレージプールを作成する"サイトを参照していません
        - "ルールの編集または置換"サイトを参照しています。

          > このルールでは* All Storage Nodes ストレージプールを使用しているため、Make 2 Copies *ルールは選択しないでください。このルールは許可されていません。

      - ILMポリシーの操作：
        - "既存のILMポリシーをクローニングする" または "新しいILMポリシーを作成します"。
        - デフォルトのルールやその他のルールがサイトを参照していないことを確認します。

ILM ルールの順序が正しいことを確認してください。ポリシーをアクティブ化すると、新規および既存のオブジェクトがリスト内の順にルールによって評価されます。

c. テストオブジェクトを取り込み、ポリシーをシミュレートして、正しいルールが適用されることを確認します。

原因 ポリシーにエラーがあると、回復不能なデータ損失が発生する可能性があります。ポリシーをアクティブ化する前によく確認およびシミュレートし、想定どおりに機能することを確認してください。

新しい ILM ポリシーをアクティブ化すると、 StorageGRID は、そのポリシーを使用して、既存のオブジェクトと新たに取り込まれたオブジェクトを含むすべてのオブジェクトを管理します。新しい ILM ポリシーをアクティブ化する前に、既存のレプリケートオブジェクトとイレイジャーコーディングオブジェクトの配置に対する変更を確認してください。既存のオブジェクトの場所を変更すると、新しい配置が評価されて実装される際に一時的なリソースの問題が発生する可能性があります。

d. 新しいポリシーをアクティブ化し、古いポリシーが非アクティブになったことを確認します。

複数のポリシーをアクティブ化する場合は、"手順に従ってILMポリシータグを作成します。"を参照してください。

接続さ StorageGRID れたサイトの運用停止手順を実行すると、新しい ILM ポリシーをアクティブ化した時点で、選択したサイトからオブジェクトデータの削除が開始されます。すべてのオブジェクトコピーの移動または削除には数週間かかることがあります。サイトにオブジェクトデータが残っている間もサイトの運用停止を安全に開始できますが、実際の運用停止手順 を開始する前にデータをサイトから移動することが許可されている場合は、運用停止手順 の処理がより迅速になり、システム停止やパフォーマンスへの影響も少なくなります （ウィザードの手順 5 で「 * 分解を開始」を選択）。

4. EACH_INACTIVE_POLICYについては、前の手順で説明したように、最初に各ポリシーのリンクを選択して編集または削除します。
   - "ポリシーを編集します。"そのため、廃棄されるサイトを参照していません。
   - "ポリシーを削除します。"です。
5. ILMルールとポリシーの変更が完了したら、手順3（[Revise ILM Policies]）に記載されたポリシーは削除されます。「 * 次へ * 」を選択します。

   手順 4 （ Remove ILM References ）が表示されます。

StorageGRID のサイトへの **ILM** 参照を削除します

[Decommission Site]ウィザードの手順4（Remove ILM References）では、ILMポリシーで使用されていないルールも含め、サイトを参照している未使用のILMルールを削除または編集する必要があります。

手順

1. 未使用の ILM ルールがサイトを参照しているかどうかを確認します。

ILMルールが表示されても、それらのルールはサイトを参照していますが、どのポリシーでも使用されていません。

> StorageGRIDはサイトの運用を停止すると、サイトを参照している未使用のイレイジャーコーディングプロファイルを自動的に非アクティブ化し、サイトを参照している未使用のストレージプールを自動的に削除します。All Storage Nodesストレージプール（StorageGRID 11.6以前）は、All Sitesサイトを使用しているため削除されています。

2. 使用されていない各ルールを編集または削除します。
   - ルールを編集するには、ILMルールページに移動して、サイトを参照するイレイジャーコーディングプロファイルまたはストレージプールを使用するすべての配置を更新します。次に、 * 手順 4 （ ILM 参照の削除） * に戻ります。
   - ルールを削除するには、ゴミ箱アイコン を選択し、**OK** を選択します。

     > サイトの運用を停止する前に、* Make 2 Copies *ルールを削除する必要があります。

3. サイトを参照している未使用のILMルールがないこと、および*[Next]*ボタンが有効になっていることを確認します。
4. 「 * 次へ * 」を選択します。

> サイトを参照している残りのストレージプールとイレイジャーコーディングプロファイルは、サイトを削除すると無効になります。StorageGRIDはサイトの運用を停止すると、サイトを参照している未使用のイレイジャーコーディングプロファイルを自動的に非アクティブ化し、サイトを参照している未使用のストレージプールを自動的に削除します。All Storage Nodesストレージプール（StorageGRID 11.6以前）は、All Sitesサイトを使用しているため削除されています。

ステップ 5 （ノードの競合を解決）が表示されます。

ノードの競合を解決し、**StorageGRID**でサイトの廃止を開始します

Decommission Site ウィザードの Step 5 （ Resolve Node Conflicts ）から、StorageGRID システム内のノードが切断されているか、選択したサイトのノードが High Availability （ HA ）グループに属しているかを確認できます。いずれかのノードの競合が解決されたら、このページから運用停止手順 を開始します。

開始する前に

StorageGRID システムのすべてのノードが次のように正しい状態であることを確認する必要があります。

- StorageGRIDシステムのすべてのノードが接続されている必要があります（）。

> 切断されたサイトの運用停止を実行する場合は、削除するサイトのすべてのノードを切断し、他のすべてのサイトのすべてのノードを接続する必要があります。

> 1つ以上のボリュームがオフライン（アンマウント済み）の場合、またはオンライン（マウント済み）でエラー状態の場合、運用停止は開始されません。

運用停止の実行中に1つ以上のボリュームがオフラインになると、それらのボリュームがオンラインに戻ったあとに運用停止プロセスが完了します。

- 削除するサイトにハイアベイラビリティ（ HA ）グループに属するインターフェイスを持つことはできません。

タスクの内容

手順 5 （ノードの競合を解決）用に表示されたノードがある場合は、運用停止を開始する前に問題 を修正する必要があります。

このページからサイトの手順 の運用停止を開始する前に、次の考慮事項を確認してください。

- 手順 の運用停止が完了するまでに、十分な時間を確保する必要があります。

サイトからオブジェクトデータを移動または削除するには、サイトのデータ量、システムの負荷、ネットワークのレイテンシ、および ILM に求められる変更の性質に応じて、数日、数週間、場合によっては数カ月かかることがあります。

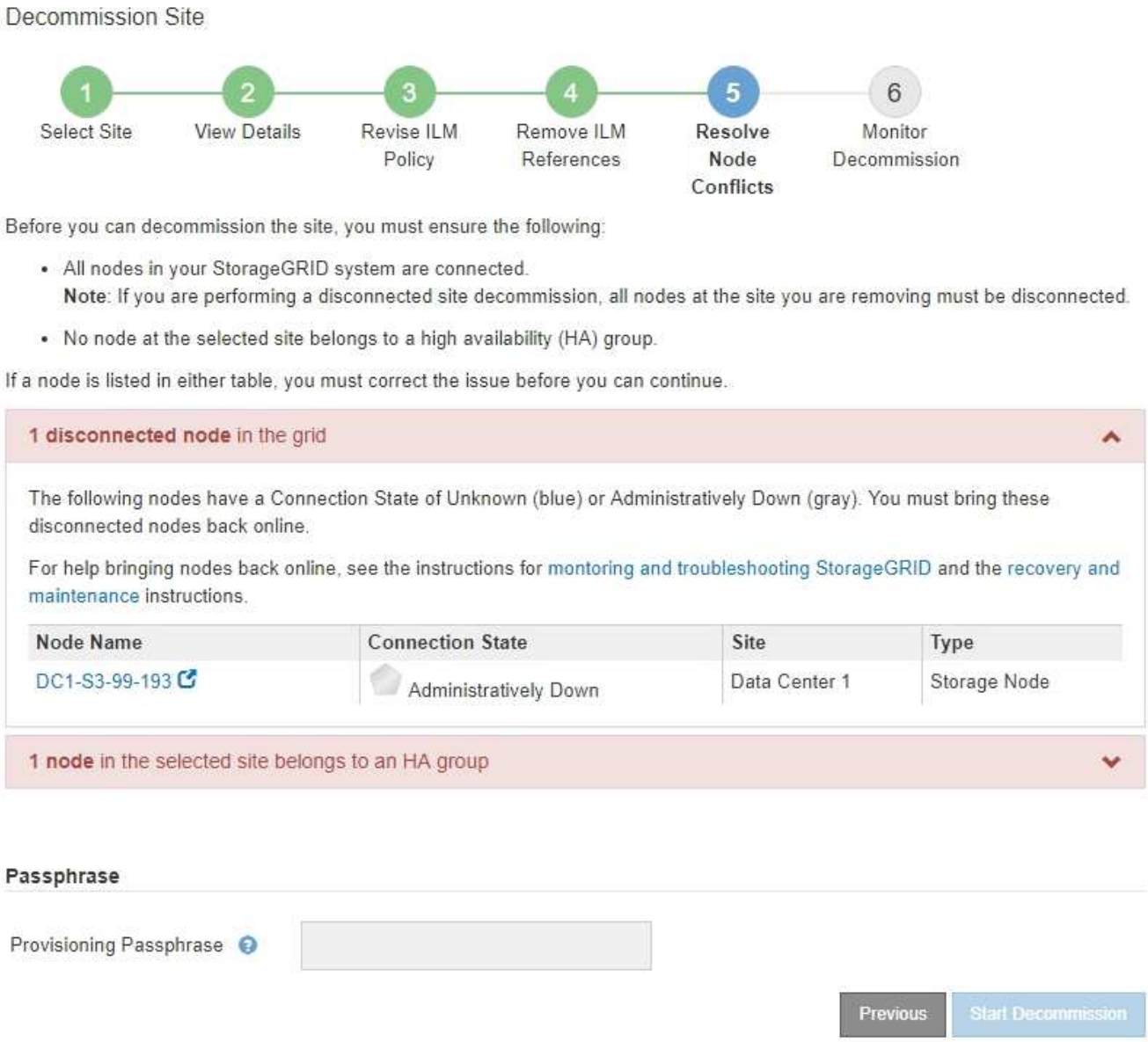
- サイトの運用停止中は、手順 は次の処理を実行します。
  - 運用停止するサイトを参照するILMルールを作成することはできません。また、既存のILMルールを編集してサイトを参照することもできません。
  - 拡張やアップグレードなど、その他のメンテナンス手順は実行できません。

接続されているサイトの運用停止中に別のメンテナンス手順 を実行する必要がある場合は、ストレージノードを削除している間に手順 を一時停止できます。[Pause]*ボタンは、「レプリケートデータとイレイジャーコーディングデータの運用停止」ステージで有効になります。

  - サイトの運用停止手順 の開始後にノードをリカバリする必要がある場合は、サポートにお問い合わせください。

手順

1. ステップ 5 （ノードの競合の解決） の切断されたノードのセクションを確認して、StorageGRID システム内のノードに接続状態が不明 （ ） または管理上のダウン （ ） のものがあるかどうかを確認してください。

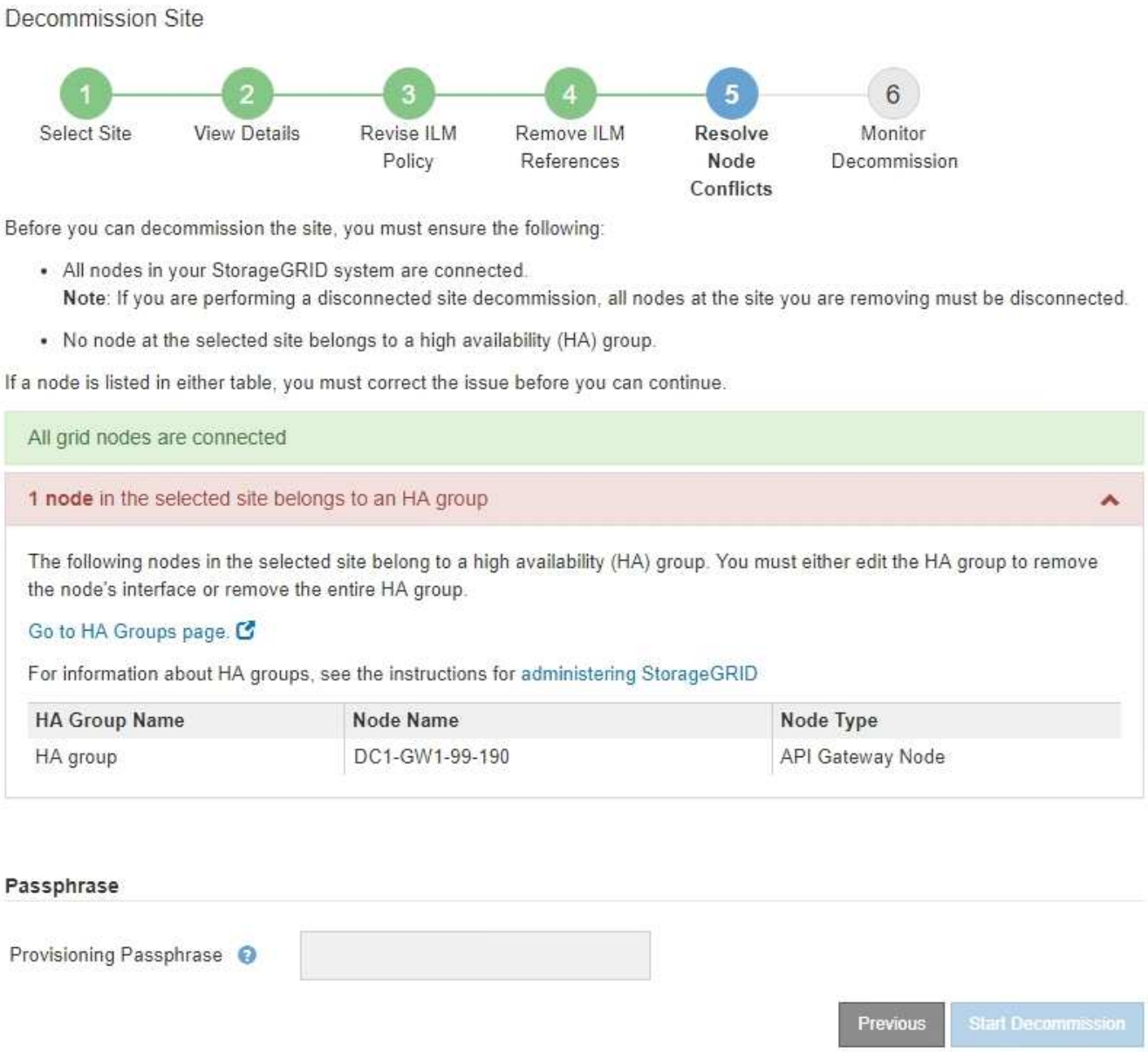


2. 切断されているノードがある場合は、オンラインに戻します。

   を参照してください"ノードの手順"。サポートが必要な場合は、テクニカルサポートにお問い合わせください。

3. 切断されているすべてのノードがオンラインに戻ったら、手順 5 （ノードの競合を解決）の HA グループに関するセクションを確認します。

   このテーブルには、選択したサイトにあるハイアベイラビリティ（ HA ）グループに属するノードがすべて表示されます。



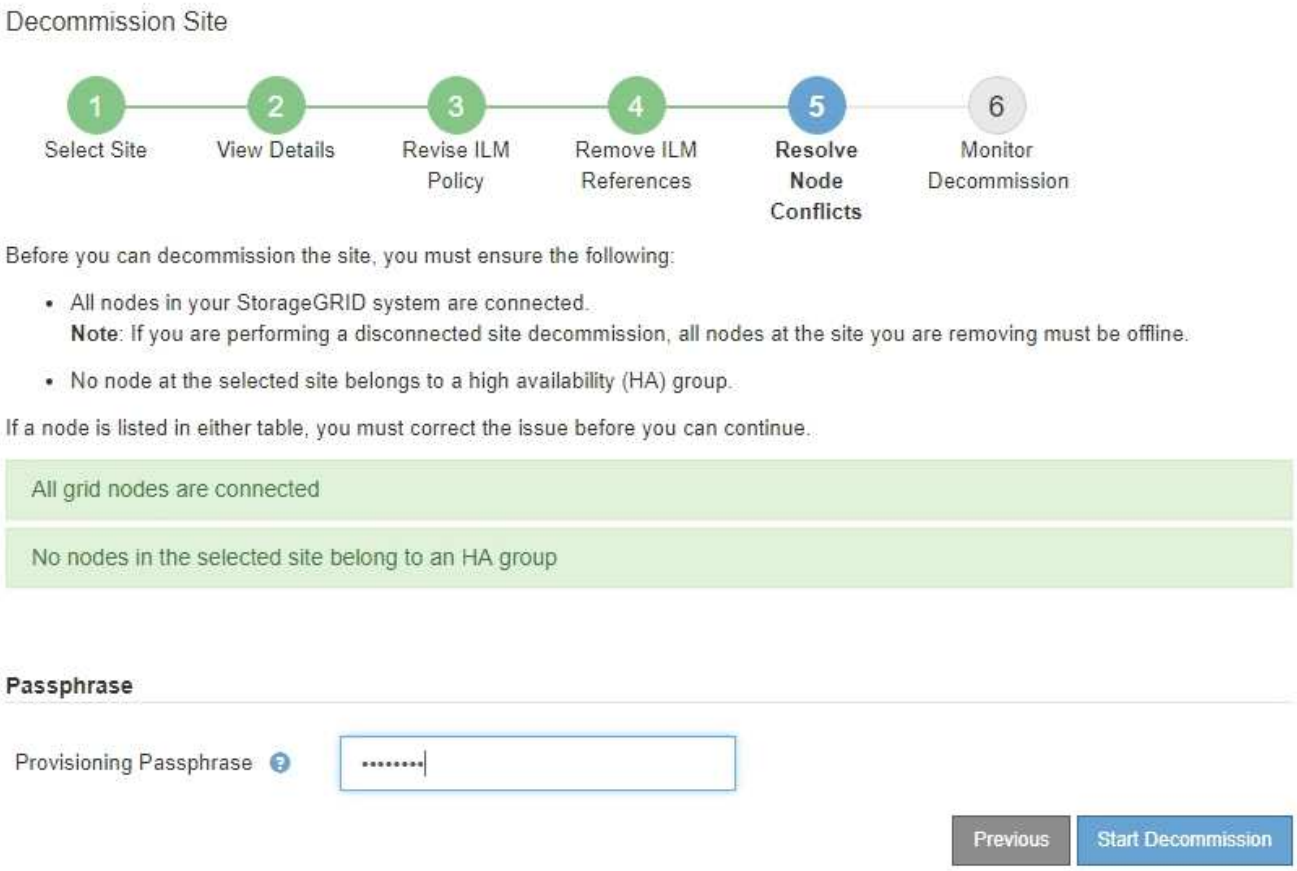
4. 表示されたノードがある場合は、次のいずれかを実行します。

   - 該当する各 HA グループを編集してノードインターフェイスを削除します。
   - このサイトからノードのみを含む HA グループを削除します。StorageGRID の管理手順を参照してください。

   すべてのノードが接続されており、選択したサイト内のノードがHAグループで使用されていない場合、*プロビジョニングパスフレーズ*フィールドが有効になります。

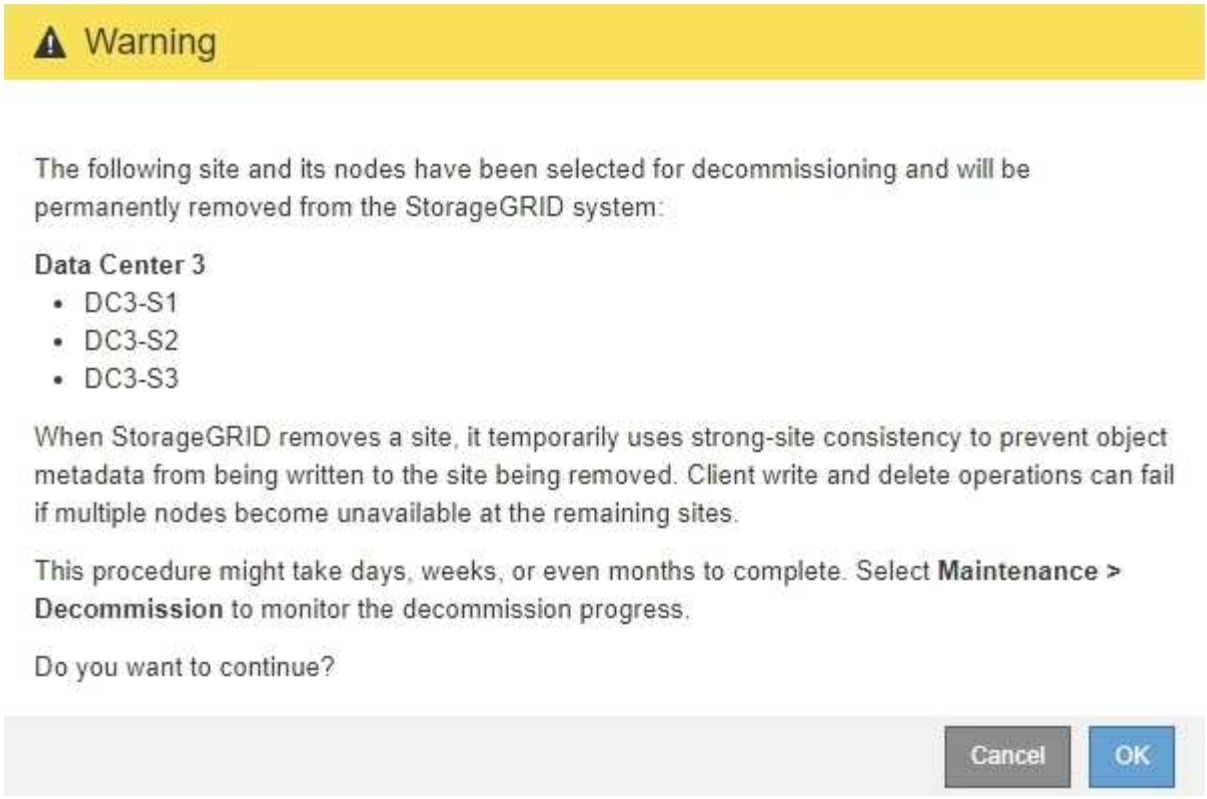
5. プロビジョニングパスフレーズを入力します。

   [* 分解を開始 * （ Start Decommission * ）] ボタンが有効になります。



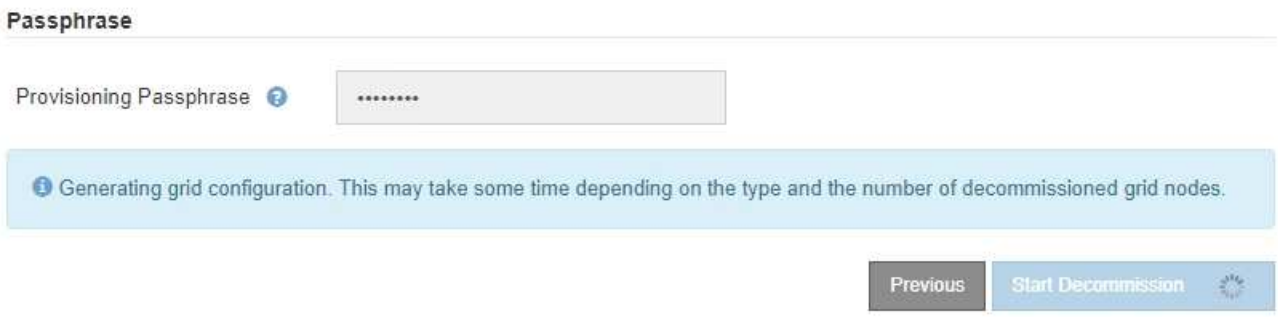
6. サイトの運用停止手順 を開始する準備ができたら、 * 運用停止を開始 * を選択します。

   削除するサイトとノードが警告として表示されます。サイトを完全に削除するには、数日、数週間、場合によっては数か月かかることがあります。



7. 警告を確認します。開始する準備ができたら、「 * OK * 」を選択します。

   新しいグリッド設定が生成されるときにメッセージが表示されます。運用停止するグリッドノードのタイプと数によっては、このプロセスには時間がかかることがあります。



   新しいグリッド設定が生成されると、ステップ 6 （ Monitor Decommission ）が表示されます。

   [前へ *] ボタンは、運用停止が完了するまで無効のままです。

StorageGRIDでサイトの廃止措置の進捗状況を監視する

Decommission Site ページウィザードの Step 6 （ Monitor Decommission ）では、サイトが削除されるまで進行状況を監視できます。

タスクの内容

StorageGRID は、接続されているサイトを削除するときに、次の順序でノードを削除します。

1. ゲートウェイノード
2. 管理ノード
3. ストレージノード

StorageGRID は切断されているサイトを削除するときに、次の順序でノードを削除します。

1. ゲートウェイノード
2. ストレージノード
3. 管理ノード

各ゲートウェイノードまたは管理ノードの削除には数分から 1 時間程度しかかかる場合がありますが、ストレージノードには数日から数週間かかる場合があります。

手順

1. 新しいリカバリ パッケージが生成されたらすぐに、ファイルをダウンロードしてください。



廃止手順中に問題が発生した場合にグリッドを回復できるように、できるだけ早く回復パッケージをダウンロードしてください。

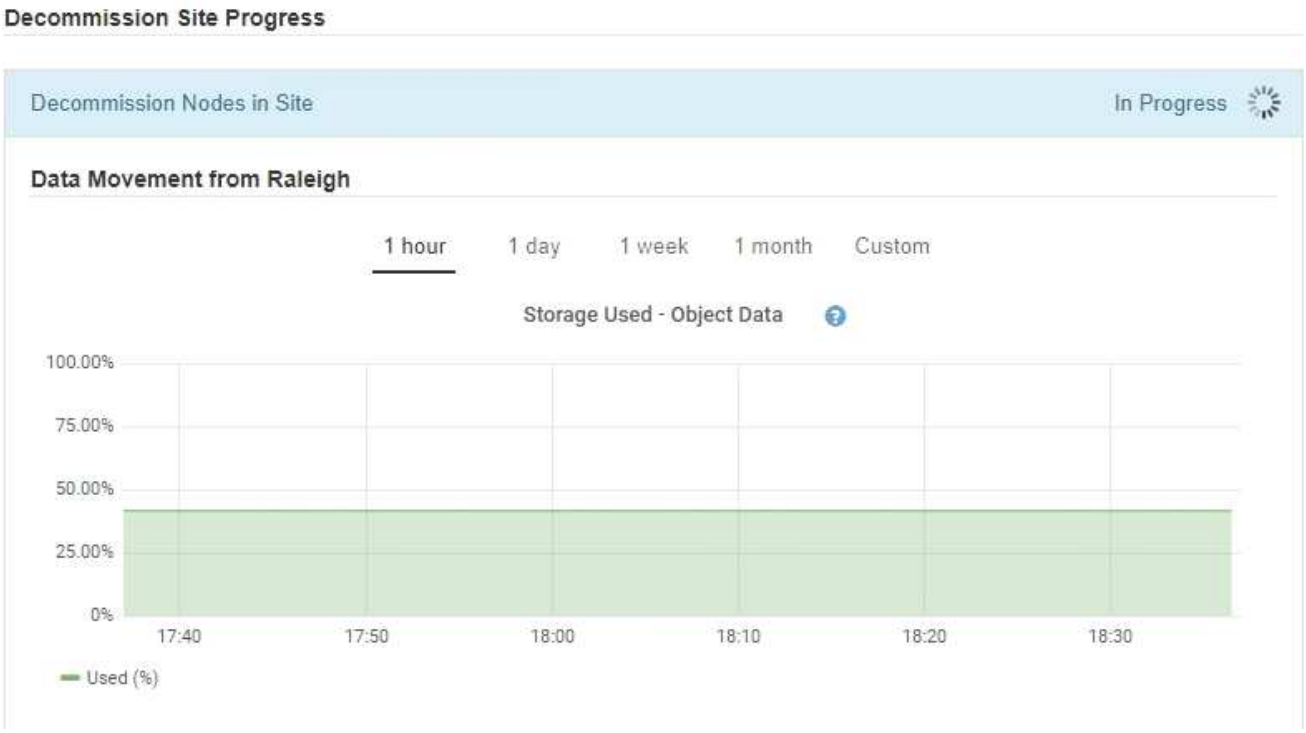
a. メッセージ内のリンクを選択するか、メンテナンス > システム > *回復パッケージ*を選択します。
b. ファイルをダウンロードし `.zip`ます。

説明書をご覧ください"リカバリパッケージのダウンロード"。

リカバリ パッケージ ファイルには、 StorageGRIDシステムからデータを取得するために使用できる暗号化キーとパスワードが含まれているため、セキュリティで保護する必要があります。

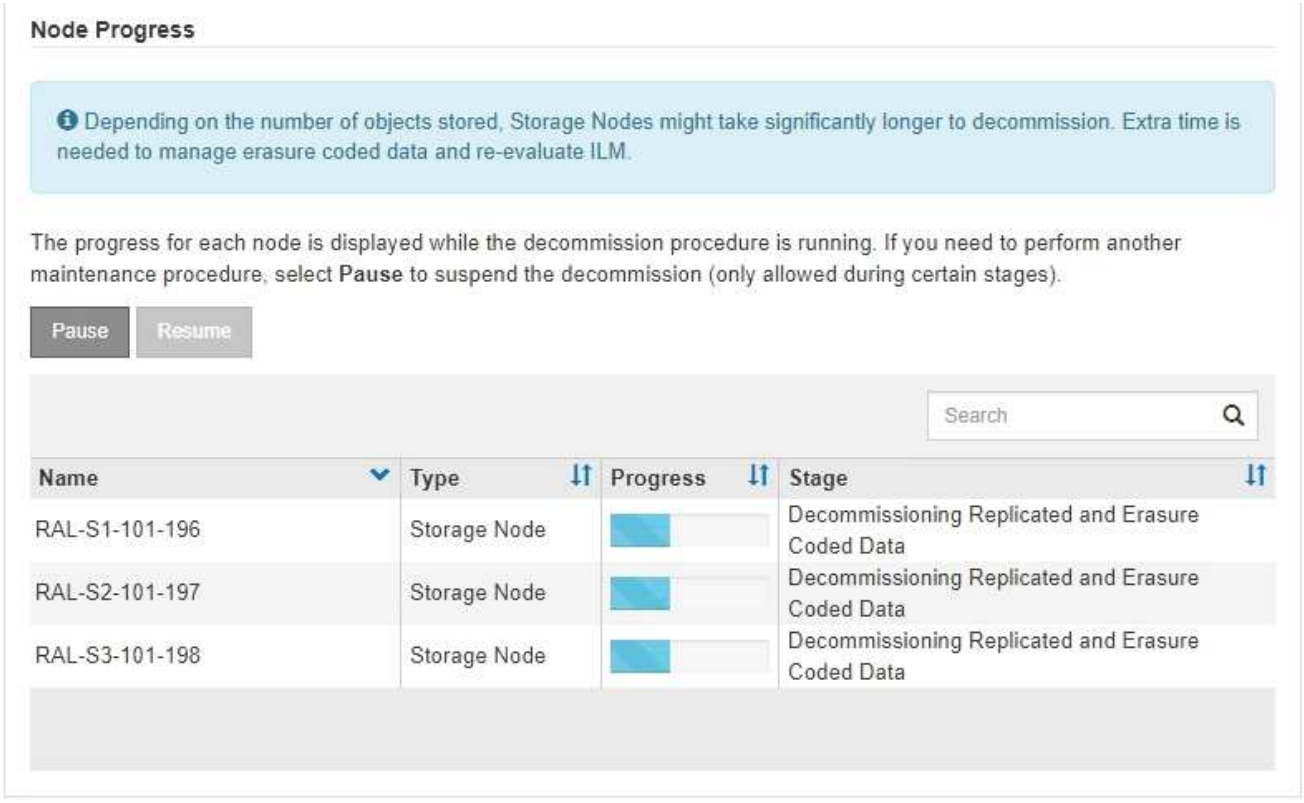
2. データ移動グラフを使用して、このサイトから他のサイトへのオブジェクトデータの移動を監視します。

データの移動は、手順 3 （ ILM ポリシーの改訂）で新しい ILM ポリシーをアクティブ化すると開始されます。データの移動は、手順 の運用停止処理の間に行われます。



3. ページの Node Progress セクションで、ノードが削除される場合の運用停止手順 の進行状況を監視します。

   ストレージノードを削除すると、各ノードで一連のステージが実行されます。これらのステージのほとんどは迅速または不透過的に行われますが、移動が必要なデータの量に応じて、他のステージが完了するまでに数日から数週間かかることがあります。イレイジャーコーディングデータを管理して ILM を再評価するために追加の時間が必要です。



接続されているサイトの運用停止の進行状況を監視している場合は、次の表を参照して、ストレージノードの運用停止ステージを確認してください。

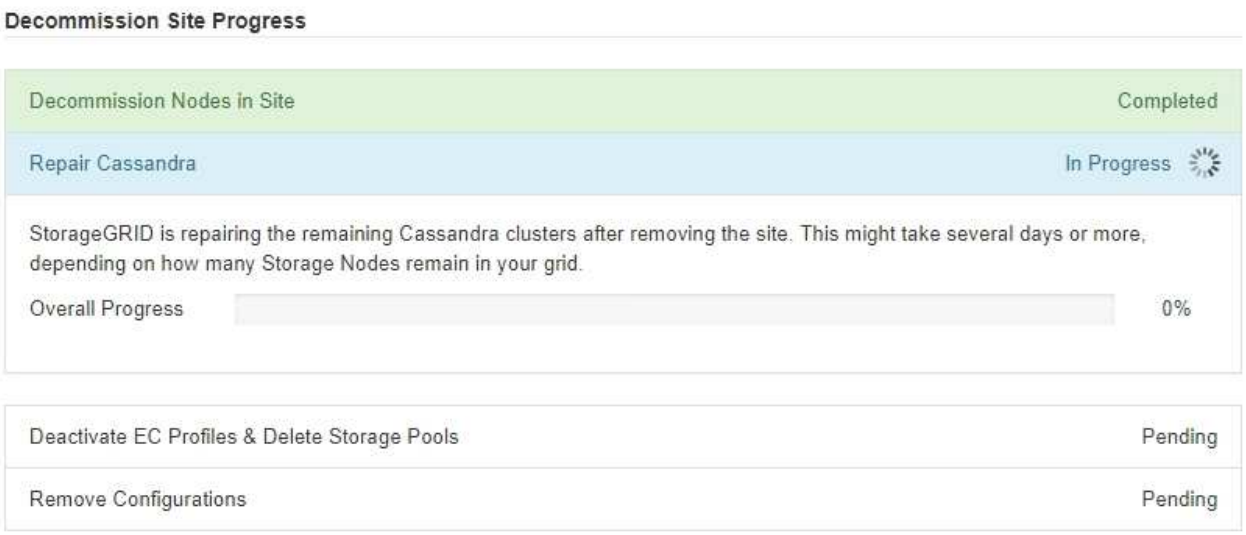
段階	推定時間
保留中	分以下
ロックされるまで待ちます	分
タスクの準備	分以下
LDR を運用停止にする	分
レプリケートデータとイレイジャーコーディングデータの運用停止	データ量に基づく数時間、数日、または数週間 • 注：その他のメンテナンス作業が必要な場合は、この段階でサイトの運用停止を一時停止できます。
LDR が状態を設定	分
監査キューをフラッシュします	メッセージ数とネットワーク遅延に基づいて、数分から数時間に短縮されます。
完了	分

切断されているサイトの運用停止の進行状況を監視する場合は、次の表を参照して、ストレージノードの運用停止ステージを確認してください。

段階	推定時間
保留中	分以下
ロックされるまで待ちます	分
タスクの準備	分以下
外部サービスを無効にします	分
証明書の取り消し	分
ノードの登録解除	分
ストレージグレードの登録解除	分
ストレージグループの削除	分

段階	推定時間
エンティティの削除	分
完了	分

4. すべてのノードが完了ステージになったら、残りのサイトの運用停止処理が完了するまで待ちます。
   - StorageGRID は、 * Repair Cassandra * ステップ中に、グリッドに残っている Cassandra クラスタに対して必要な修復を実行します。グリッドに残っているストレージノードの数によっては、この修復に数日以上かかることがあります。



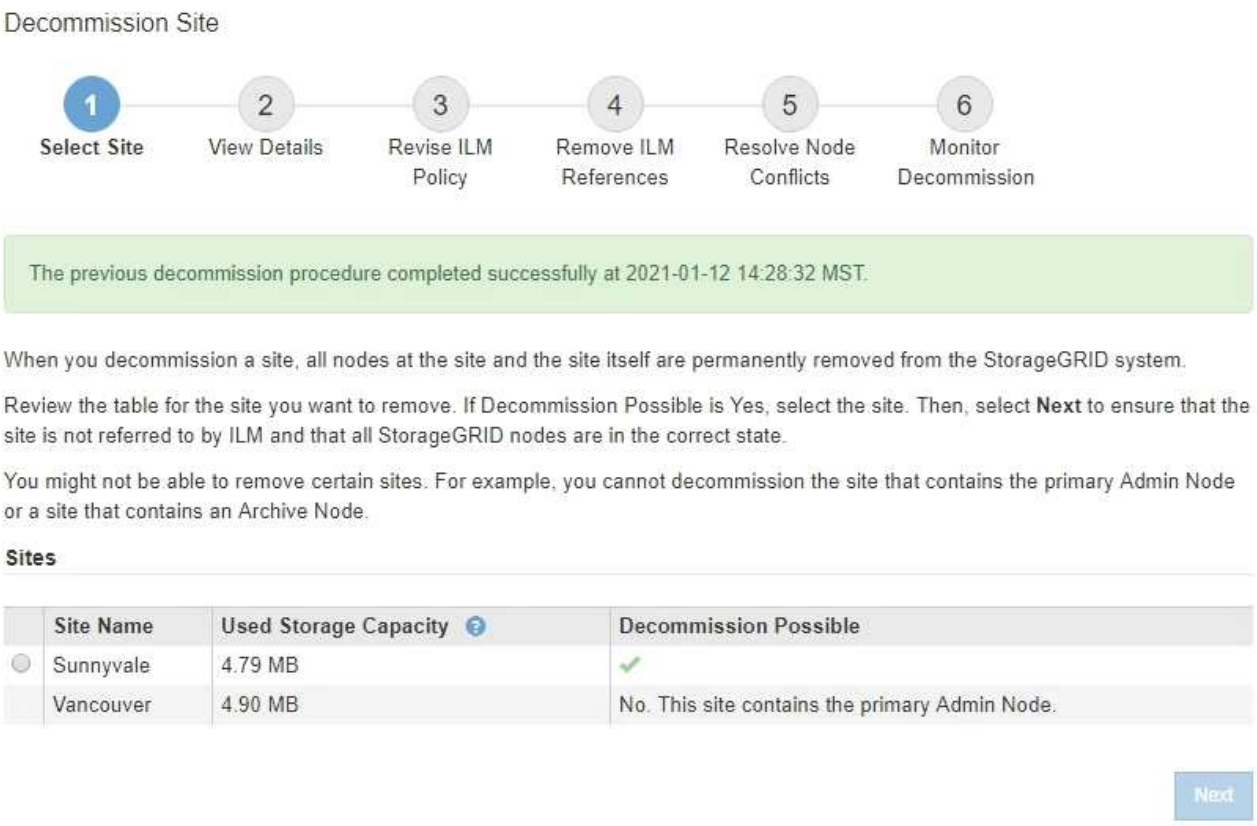
   - [EC プロファイルの非アクティブ化とストレージプールの削除 * （ Deactivate EC Profiles & Delete Storage Pools * ）] ステップでは、次の ILM の変更が行われます。
     - サイトを参照していたイレイジャーコーディングプロファイルはすべて非アクティブ化されます。
     - サイトを参照していたストレージプールがすべて削除されます。

> All Storage Nodesストレージプール（StorageGRID 11.6以前）も、All Sitesサイトを使用しているため削除されています。

   - 最後に、 * 構成の削除 * ステップで、サイトとそのノードへの残りの参照がグリッドの残りの部分から削除されます。



5. 運用停止手順 が完了すると、運用停止サイトのページに成功のメッセージが表示され、削除したサイトは表示されなくなります。



終了後

サイトの運用停止手順 が完了したら、次の作業を実行します。

- 運用停止したサイトのすべてのストレージノードのドライブを確実に消去します。市販のデータ消去ツールまたはデータ消去サービスを使用して、ドライブからデータを完全かつ安全に削除します。
- サイトに 1 つ以上の管理ノードが含まれていて、 StorageGRID システムでシングルサインオン（ SSO ）が有効になっている場合は、そのサイトに対する証明書利用者信頼をすべて Active Directory フェデレーションサービス（ AD FS ）から削除します。
- 接続されているサイトの運用停止手順 でノードの電源が自動的にオフになったら、関連する仮想マシンを

削除します。

グリッド、サイト、またはノードの名前変更

StorageGRID の名前変更手順を使用する

必要に応じて、グリッド全体、各サイト、および各ノードについて、Grid Managerで表示される表示名を変更できます。表示名は、必要なときに安全に更新できます。

手順 の名前変更とは何ですか。

StorageGRID を最初にインストールするときは、グリッド、各サイト、および各ノードの名前を指定します。これらの初期名は_システム名_と呼ばれ、StorageGRID 全体で最初に表示される名前です。

システム名は内部StorageGRID 処理に必要であり、変更することはできません。ただし、名前変更手順 を使用して、グリッド、各サイト、および各ノードのnew_display names_を定義できます。これらの表示名は、基になるシステム名の代わりに（場合によっては、それに加えて）StorageGRID のさまざまな場所に表示されます。

入力ミスを修正する場合、別の命名規則を実装する場合、またはサイトとそのすべてのノードが再配置されたことを示す場合は、名前変更手順 を使用します。システム名とは異なり、表示名は必要に応じていつでも更新でき、StorageGRID の処理には影響しません。

システム名と表示名はどこに表示されますか？

次の表は、StorageGRID ユーザー・インターフェイスおよびStorageGRID ファイルでシステム名と表示名が表示される場所をまとめたものです。

場所	システム名	表示名
Grid Managerのページ	項目の名前が変更されない限り表示されます	項目の名前が変更された場合は、システム名の代わりに次の場所に表示されます。 • ダッシュボード • [Nodes]ページ • ハイアベイラビリティグループ、ロードバランサエンドポイント、VLANインターフェイス、キー管理サーバ、グリッドパスワード、 ファイアウォール制御 • アラート • ストレージプールの定義 • オブジェクトメタデータの検索ページ • メンテナンス手順に関するページ（アップグレード、ホットフィックス、SANtricity OSのアップグレード、運用停止、拡張、リカバリ、およびオブジェクトの存在のチェック • サポートページ（ログと診断） • シングルサインオンページ。テーブルで管理ノードのホスト名の横に表示され、管理ノードの詳細を確認できます
ノード > ノードの概要 タブ	常に表示されます	項目の名前が変更された場合にのみ表示されます
• node-health * API	常に返されます	項目の名前が変更された場合にのみ返されます

SSHを使用してノードにアクセスするときにプロンプトを表示します	項目の名前が変更されていない場合は、プライマリ名として表示されます。
	`admin@SYSTEM-NAME: ~ $`
	項目の名前が変更されたときにかっこで囲まれます。
	`admin@DISPLAY-NAME(SYSTEM-NAME):~ $`
		項目の名前が変更されたときにプライマリ名として表示されます。
		`admin@DISPLAY-NAME(SYSTEM-NAME):~ $`

`Passwords.txt`リカバリパッケージ内のファイル	表示形式 `Server Name`	表示形式 `Display Name`

場所	システム名	表示名
`/etc/hosts`すべてのノード上のファイル 例： `10.96.99.128 SYSTEM-NAME 28989c59-a2c3-4d30-bb09-6879adf2437f DISPLAY-NAME localhost-grid # storagegrid-gen-host`	常に2番目の列に表示されます	項目の名前が変更されると、4番目の列に表示されます
`topology-display-names.json`、Auto Supportデータに付属	含まれません	項目の名前が変更されていない場合は空です。名前が変更されていない場合は、グリッド、サイト、およびノードのIDが表示名にマッピングされます。

表示名の要件

この手順 を使用する前に、表示名の要件を確認してください。

ノードの表示名

ノードの表示名は次のルールに従う必要があります。

- StorageGRID システム全体で一意である必要があります。
- StorageGRID システム内の他の項目のシステム名と同じにすることはできません。
- 1文字以上32文字以下にする必要があります。
- 数字、ハイフン（-）、大文字と小文字を含めることができます。
- 先頭または末尾にはアルファベットまたは数字を使用できますが、先頭または末尾にハイフンを使用することはできません。
- すべての数字を指定することはできません。
- 大文字と小文字は区別されません。たとえば `DC1-ADM`、と `dc1-adm`は重複しているとみなされます。

以前に別のノードで使用されていた表示名を使用してノードの名前を変更できます。ただし、表示名やシステム名が重複しないようにする必要があります。

グリッドとサイトの表示名

グリッドとサイトの表示名は同じルールに従いますが、次の例外があります。

- スペースを含めることができます。

- 次の特殊文字を含めることができます。 `= - _ : , . @ !`
- 先頭と末尾にハイフンを含む特殊文字を使用できます。
- すべての数字または特殊文字を使用できます。

表示名のベストプラクティス

複数の項目の名前を変更する場合は、この手順 を使用する前に一般的な命名規則を文書化してください。名前が一目で一意で一貫性があり、わかりやすいシステムを考えてみましょう。

組織の要件に合わせて任意の命名規則を使用できます。次のような基本的な提案を検討してください。

- サイトインジケータ：複数のサイトがある場合は、各ノード名にサイトコードを追加します。
- ノードタイプ：通常、ノード名はノードのタイプを示します。、 `adm`、 `gw`などの省略形を使用できます（`s`ストレージノード、管理ノード、ゲートウェイノード）。
- ノード番号：サイトに特定のタイプのノードが複数含まれている場合は、各ノードの名前に一意の番号を追加します。

時間の経過とともに変更される可能性のある名前に特定の詳細を追加する前に、よく考えてください。たとえば、ノード名にIPアドレスを含めないでください。これらのアドレスは変更可能です。同様に、機器を移動したりハードウェアをアップグレードしたりすると、ラックの場所やアプライアンスのモデル番号が変わることがあります。

表示名の例

StorageGRID システムに3つのデータセンターがあり、各データセンターに異なるタイプのノードがあるとします。表示名は次のように簡単になります。

- グリッド： `StorageGRID Deployment`
- 最初のサイト： `Data Center 1`
  - `dc1-adm1`
  - `dc1-s1`
  - `dc1-s2`
  - `dc1-s3`
  - `dc1-gw1`
- セカンドサイト： `Data Center 2`
  - `dc2-adm2`
  - `dc2-s1`
  - `dc2-s2`
  - `dc2-s3`
- * 3番目のサイト*： `Data Center 3`
  - `dc3-s1`
  - `dc3-s2`

- dc3-s3

StorageGRID表示名の追加または更新

この手順 を使用して、グリッド、サイト、およびノードに使用される表示名を追加または更新できます。1つのアイテム、複数のアイテム、またはすべてのアイテムの名前を同時に変更できます。表示名を定義または更新しても、StorageGRID の処理には影響しません。

開始する前に

- どの管理ノードからでも、グリッドマネージャにサインインするには、"サポートされている Web ブラウザ" 。
- あなたはを持っています"Maintenance権限またはRoot Access権限"。
- プロビジョニングパスフレーズを用意します。
- 表示名の要件とベストプラクティスを理解している。を参照して "グリッド、サイト、ノードの名前を変更します"

グリッド、サイト、またはノードの名前を変更する方法

StorageGRID システム、1つ以上のサイト、または1つ以上のノードの名前を変更できます。

以前別のノードで使用されていた表示名を使用することもできます。ただし、この名前を変更しても表示名やシステム名が重複しないようにする必要があります。

名前を変更する項目を選択します

開始するには、名前を変更する項目を選択します。

手順

1. メンテナンス > タスク > *グリッド、サイト、ノードの名前変更*を選択します。
2. [名前の選択]ステップで、名前を変更する項目を選択します。

変更する項目	指示
システム内のすべて（またはほとんどすべて）の名前	a. [すべて選択]*を選択します。 b. 必要に応じて、名前を変更しない項目をクリアします。
グリッドの名前	グリッドのチェックボックスを選択します。
サイトとその一部またはすべてのノードの名前	a. サイトのテーブルヘッダーのチェックボックスをオンにします。 b. 必要に応じて、名前を変更しないノードを選択解除します。
サイトの名前	サイトのチェックボックスをオンにします。
ノードの名前	ノードのチェックボックスを選択します。

3. 「 * Continue * 」を選択します。
4. 選択した項目を含むテーブルを確認します。
    - [表示名]列には、各項目の現在の名前が表示されます。項目の名前が一度も変更されていない場合、表示名はシステム名と同じになります。
    - [システム名]列には、インストール時に各項目に入力した名前が表示されます。システム名は内部StorageGRID 処理に使用され、変更することはできません。たとえば、ノードのシステム名をホスト名にすることができます。
    - 「* Type *」列は、項目のタイプ（グリッド、サイト、または特定のタイプのノード）を示します。

新しい名前を提案します

[新しい名前を提案する]ステップでは、各項目の表示名を個別に入力することも、項目の名前を一括して変更することもできます。

項目名を個別に変更します

名前を変更する各項目の表示名を入力するには、次の手順に従います。

手順

1. [表示名（Display name *）]フィールドに、リスト内の各項目の表示名を入力します。

   命名要件については、を参照してください"グリッド、サイト、ノードの名前を変更します"。

2. 名前を変更したくないアイテムを削除するには、*リストから削除*列の✕を選択します。

   項目に新しい名前を提案しない場合は、その名前をテーブルから削除する必要があります。

3. テーブル内のすべての項目に新しい名前を指定したら、*名前の変更*を選択します。

   成功を示すメッセージが表示されます。新しい表示名がGrid Manager全体で使用されるようになりました。

項目の名前を一括して変更します

アイテム名が共通の文字列を共有していて、別の文字列に置き換える場合は、一括名前変更ツールを使用します。

手順

1. [新しい名前を提案する]ステップで、*[一括名称変更ツールを使用する]*を選択します。

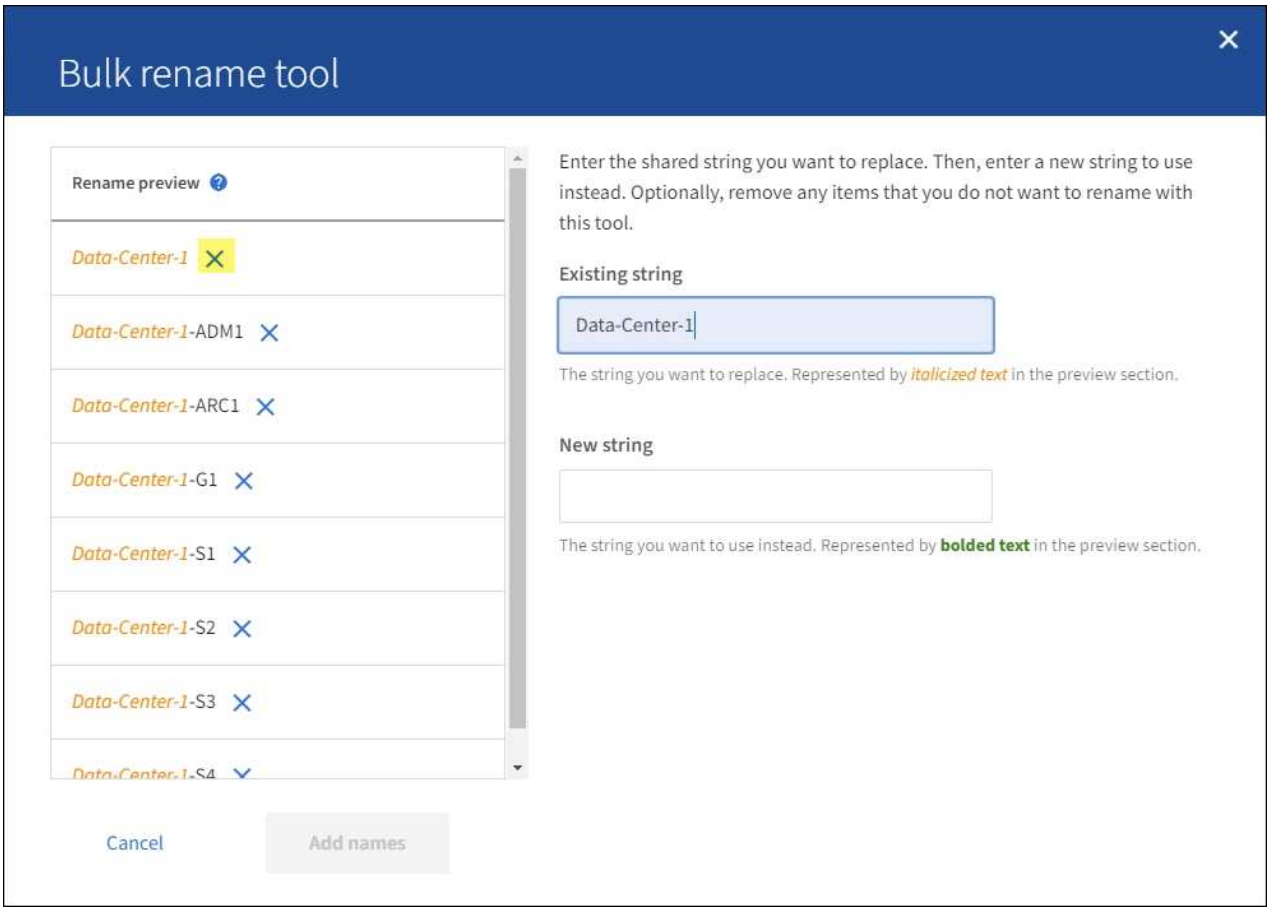
   プレビューの名前変更*には、*新しい名前を提案*ステップで表示されたすべての項目が含まれています。プレビューを使用して、共有文字列を置換した後に表示名がどのように表示されるかを確認できます。

2. [**existing string**]フィールドに、置き換える共有文字列を入力します。たとえば、置換する文字列がである場合は `Data-Center-1`、* Data-Center-1 *と入力します。

   入力すると、テキストが左側の名前のどこにあるかが強調表示されます。

3. ✕を選択して、このツールで名前を変更したくない項目を削除します。

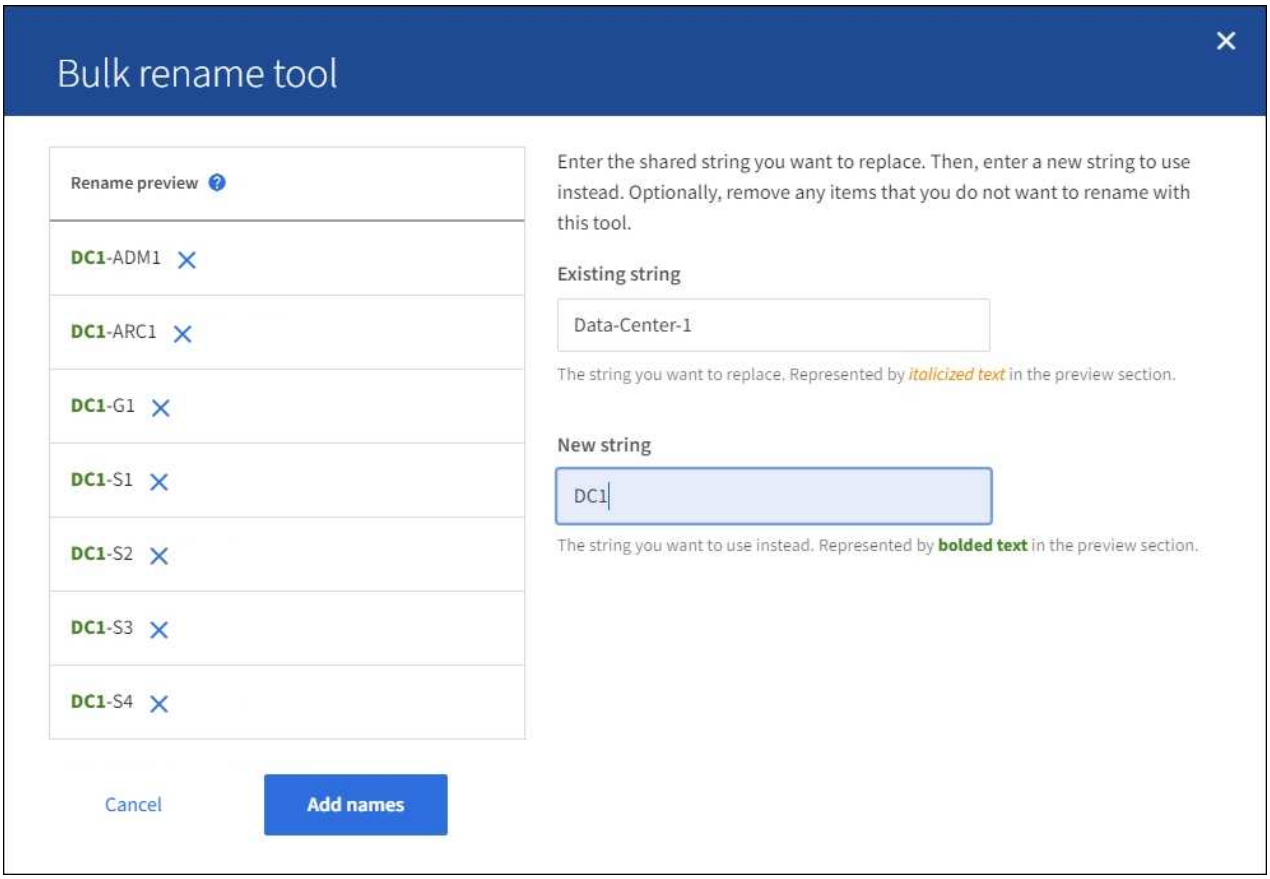
   例えば、文字列 `Data-Center-1`を含むすべてのノードの名前を変更したいが、 `Data-Center-1`サイト自体の名前は変更したくない場合を考えます。✕を選択して、名前変更プレビューからサイトを削除します。



4. [新しい文字列*]フィールドに、代わりに使用する置換文字列を入力します。たとえば、「* DC1 *」と入力します。

   命名要件については、を参照してください"グリッド、サイト、ノードの名前を変更します"。

   置換文字列を入力すると、左側の名前が更新されるため、新しい名前が正しいことを確認できます。



5. プレビューに表示された名前に問題がなければ、*名前を追加*を選択して、*新しい名前を提案*ステップのテーブルに名前を追加します。
6. 必要に応じて追加の変更を行うか、✕を選択して、名前を変更したくない項目を削除してください。
7. テーブル内のすべての項目の名前を変更する準備ができたら、*名前の変更*を選択します。

   成功メッセージが表示されます。新しい表示名がGrid Manager全体で使用されるようになりました。

リカバリパッケージをダウンロードする

アイテムの名前変更が完了したら、新しい回復パッケージをダウンロードして保存します。名前を変更したアイテムの新しい表示名は、 `Passwords.txt`ファイル。

手順

1. プロビジョニングパスフレーズを入力します。
2. [リカバリパッケージのダウンロード] を選択します。

   ダウンロードがすぐに開始されます。

3. ダウンロードが完了したら、ファイルを開い `Passwords.txt`てすべてのノードのサーバ名と名前を変更したノードの表示名を確認します。
4. ファイルを2つの安全な場所、安全な場所、および別 々 の場所にコピーし `sgws-recovery-package-*id-revision*.zip`ます。

リカバリ パッケージ ファイルには、 StorageGRIDシステムからデータを取得するために使用できる暗号化キーとパスワードが含まれているため、セキュリティで保護する必要があります。

5. [完了]*を選択して、最初のステップに戻ります。

表示名をシステム名に戻します

名前を変更したグリッド、サイト、またはノードを元のシステム名に戻すことができます。アイテムをシステム名に戻すと、Grid Managerページやその他のStorageGRID ロケーションにそのアイテムの*表示名*が表示されなくなります。項目のシステム名のみが表示されます。

手順

1. メンテナンス > タスク > *グリッド、サイト、ノードの名前変更*を選択します。
2. [名前の選択]ステップで、システム名に戻す項目を選択します。
3. 「 * Continue * 」を選択します。
4. [新しい名前を提案する]ステップでは、表示名を個別に、または一括してシステム名に戻します。

   システム名に個別にリバートします

   a. 各項目の元のシステム名をコピーして*表示名*フィールドに貼り付けるか、✕を選択して元に戻したくない項目を削除してください。

      表示名を元に戻すには、システム名を*表示名*フィールドに表示する必要がありますが、名前の大文字と小文字は区別されません。

   b. [名前の変更 *] を選択します。

      成功を示すメッセージが表示されます。これらの項目の表示名は使用されなくなります。

   一括してシステム名に戻します

   a. [新しい名前を提案する]ステップで、*[一括名称変更ツールを使用する]*を選択します。
   b. [**existing string**]フィールドに、置換する表示名の文字列を入力します。
   c. [新しい文字列*]フィールドに、代わりに使用するシステム名文字列を入力します。
   d. を選択して、[新しい名前の提案]*ステップのテーブルに名前を追加します。
   e. 「表示名」フィールドの各項目が、「システム名」フィールドの名前と一致していることを確認してください。変更を加えるか、✕を選択して、元に戻したくない項目を削除してください。

      表示名を元に戻すには、システム名を*表示名*フィールドに表示する必要がありますが、名前の大文字と小文字は区別されません。

   f. [名前の変更 *] を選択します。

      成功メッセージが表示されます。これらの項目の表示名は使用されなくなります。

5. 新しいリカバリパッケージをダウンロードして保存する 。

復元した項目の表示名は、ファイルに含まれなくなり `Passwords.txt`ます。

ノードの手順

StorageGRIDノードのメンテナンス手順

特定のグリッドノードまたはノードサービスに関連したメンテナンス手順の実行が必要になる場合があります。

ADC の移動

その"ADCサービス"一部のストレージ ノード上に存在します。特定の廃止およびノード変換の状況では、ADC サービスを同じサイト上の別のストレージ ノードに移動する必要があります。

ストレージノードをデータ専用ノードに変換する

ADC サービスが含まれていないストレージ ノードをデータ専用のストレージ ノードに変換できます。

ノードの再起動、シャットダウン、電源

次の手順を使用して、1つ以上のノードをリブートしたり、ノードをシャットダウンして再起動したり、ノードの電源をオフにして再度オンにしたりします。

ポートの再マップ

ポートの再マッピング手順を使用して、ノードからポートの再マッピングを削除できます。たとえば、以前に再マッピングされたポートを使用してロードバランサエンドポイントを設定する場合などです。

サーバーマネージャー

Server Manager はすべてのグリッドノード上で実行されてサービスの開始と停止を管理し、StorageGRID システムでサービスが正常に開始および終了するようにします。また、すべてのグリッドノードのサービスを監視し、エラーが報告された場合は自動的に再開を試みます。

サーバー マネージャーの手順を実行するには、通常、ノードのコマンド ラインにアクセスする必要があります。

> Server Manager には、テクニカルサポートから指示があった場合にのみアクセスしてください。

StorageGRIDでADCサービスを移動します

ADC サービスを同じサイト上の別のストレージ ノードに移動できます。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたが持っている"Maintenance権限またはRoot Access権限"。
- ソース ノードには ADC サービスが含まれています。
- ターゲット ノードに ADC サービスが含まれていません。
- ターゲット ノードは、メタデータのみのノード、または結合された (メタデータとオブジェクト データ) ノードのいずれかです。

- ソース ノードとターゲット ノードは同じサイトにあります。

タスクの内容

ADCサービスをストレージノード間で手動で移動するには、「ADCの移動」手順を使用します。例えば、ADCサービスをノード間で再分配したり、ADCサービスをより高性能なノードに移動したりする場合があります。

この手順では、ADC、IDNT、ACCT、および RSM サービスを、同じサイト上の 1 つのストレージ ノードから別のストレージ ノードに移動します。 RSM、IDNT、および ACCT サービスは ADC サービスに依存しているため、ADC サービスが移動すると自動的に移動します。

- ストレージノードの"ストレージノードをデータ専用ノードに変換する"または廃止の前に、ADC サービスを手動で移動する必要はありません。これらの手順では、必要に応じて ADC サービスが自動的に移動されます。要件の詳細については、"ADCの定足数とは何ですか？"を参照してください。
- StorageGRID は、ADC サービスを、サービスのホスティング要件を満たす最新のストレージノードに移行します。

手順

1. ソース ノードとターゲット ノードのノード ID を記録します。

   グリッド管理APIでは、ソースノードIDは次のように呼ばれます。 `sourceNodeId` 。ターゲットノードIDは `targetNodeId`。

2. Grid Managerの上部でヘルプアイコンを選択し、*[API documentation]*を選択します。
3. [Go to private API documentation]*を選択します。
4. 選択してください `POST /private/move-adc/start`手術。参照"問題 API 要求"詳細についてはこちらをご覧ください。

   手順中、2 つのノードが順番に再起動します。最初にソース ノードが再起動し、次にターゲット ノードが再起動します。

5. 使用できます `GET /private/move-adc`手順を監視します。エラーが発生した場合は、 `POST /private/move-adc/retry`手順を再試行します。
6. "リカバリパッケージをダウンロードする"この手順を完了した後。

StorageGRIDストレージノードをデータ専用ノードに変換する

パフォーマンスを向上させるには、低速の非 ADC ストレージ ノードをデータ専用のストレージ ノードに変換できます。

ストレージノードのパフォーマンス特性が異なる場合は、データ専用のストレージノードを使用するのが理にかなっています。たとえば、パフォーマンスを潜在的に向上させるために、データ専用で大容量の回転式ディスクストレージノードと、メタデータ専用のハイパフォーマンスストレージノードを組み合わせることができます。

さらに、Cassandra から RAM の少ないノードを削除することで、ノードごとのメタデータ容量制限が増加し、メタデータ容量を増やすことができます。。 "オブジェクトメタデータストレージを管理する" 。

データのみのノードを変換する場合、グリッドにはサイトごとに少なくとも 3 つの結合されたストレージ ノードまたはメタデータのみのストレージ ノードが含まれている必要があります。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"Maintenance権限またはRoot Access権限"。
- ストレージ ノードは、メタデータのみのノードでもデータのみのノードでもありません。
- ストレージノードにADCサービスが含まれており、グリッド全体で2つ以上のADCストレージノードがオンラインであり、かつ同じサイト上にADCサービスをホストできる非ADCストレージノードが存在する場合。
- サイト内の他のノードに十分なメタデータスペースがある（または"グリッドを拡張しました") を追加して、変換するストレージ ノードから移行されるメタデータを収容します。



  - 同じサイト上の他のノードに移行するメタデータが、"メタデータ予約領域" 、グリッドが不安定になります。
  - 変換を開始すると、グリッドを拡張できなくなります。

タスクの内容

この手順を使用して、1つまたは複数の複合ストレージノードをデータ専用ノードに変換します。ストレージノードにADCサービスが含まれている場合、変換中にそのサービスは自動的に同じサイト内の別のストレージノードに移動されます。

この手順では、ストレージ ノードの変換に加えて、ノードから Cassandra を廃止します。すべてのメタデータは、結合されたストレージ ノードまたはメタデータのみのストレージ ノードに移行されます。移行する必要があるメタデータの量に応じて、この手順が完了するまでにノードごとに最大数日かかる場合があります。



通常、ノードあたりのメタデータ使用量が 1 TB 未満の場合、一度に最大 10 個のノードを変換できます。ノードあたりのメタデータ使用量が 1 TB を超える場合は、代わりに手順ごとに最大 5 つのノードを変換します。



StorageGRID は、ADC サービスを、サービスのホスティング要件を満たす最新のストレージ ノードに移行します。

手順

1. 変換する ADC 以外のストレージ ノードのノード ID を記録します。
2. Grid Managerの上部でヘルプアイコンを選択し、*[API documentation]*を選択します。
3. [Go to private API documentation]*を選択します。
4. 選択してください `POST /private/convert-to-data-only-node/start`手術。参照"問題 API 要求"詳細についてはこちらをご覧ください。

   手順の実行中に各ノードが再起動します。

5. 使用できます `GET /private/convert-to-data-only-node`手順を監視します。エラーが発生した場合は、`POST /private/convert-to-data-only-node/retry`手順を再試行します。
6. "リカバリパッケージをダウンロードする"この手順を完了した後。

リブート、シャットダウン、および電源の手順

StorageGRIDローリングリブートを実行する

ローリングリブートを実行すると、サービスを停止することなく複数のグリッドノードをリブートできます。

開始する前に

- プライマリ管理ノードでGrid Managerにサインインし、を使用している"サポートされている Web ブラウザ"。

  この手順を実行するには、プライマリ管理ノードにサインインする必要があります。

- あなたはを持っています"Maintenance権限またはRoot Access権限"。

タスクの内容

複数のノードを同時にリブートする必要がある場合は、この手順を使用します。たとえば、この手順は、グリッドのFIPSモードを変更したあとに使用できます"TLSおよびSSHセキュリティポリシー"。FIPSモードが変更された場合は、すべてのノードをリブートして変更を有効にする必要があります。

1つのノードだけをリブートする必要がある場合は、リブートできます"[Tasksタブからノードをリブートする"]。

StorageGRIDでグリッドノードをリブートすると、各ノードでコマンドが実行される `reboot`ため、ノードがシャットダウンされて再起動されます。すべてのサービスが自動的に再開されます。

- VMwareノードをリブートすると、仮想マシンがリブートされます。
- Linuxノードをリブートすると、コンテナがリブートされます。
- StorageGRIDアプライアンスノードをリブートすると、コンピューティングコントローラがリブートされます。

ローリングリブート手順では、次の例外を除き、複数のノードを同時にリブートできます。

- 同じタイプの2つのノードが同時にリブートされることはありません。
- ゲートウェイノードと管理ノードは同時にリブートされません。

代わりに、HAグループ、オブジェクトデータ、重要なノードサービスを常に使用できるようにするために、これらのノードが順番にリブートされます。

プライマリ管理ノードをリブートすると、ブラウザからグリッドマネージャに一時的にアクセスできなくなるため、手順を監視できなくなります。このため、プライマリ管理ノードは最後にリブートされます。

ローリングリブートの実行

リブートするノードを選択し、選択内容を確認し、リブート手順を開始して、進行状況を監視します。

ノードを選択

最初の手順として、[Rolling reboot]ページにアクセスし、リブートするノードを選択します。

手順

1. メンテナンス > タスク > *ローリング再起動*を選択します。
2. [ノード名]列の接続状態とアラートのアイコンを確認します。

> ノードがグリッドから切断されている場合、ノードを再起動することはできません。これらのアイコンが付いているノードでは、チェックボックスが無効になります：または

3. アクティブなアラートがあるノードがある場合は、*[アラートの概要]*列でアラートのリストを確認します。

> ノードの現在のアラートをすべて表示するには、を選択することもできます"[Nodes> Overviewタブ"]。

4. 必要に応じて、推奨される対処方法を実行して現在のアラートを解決します。
5. 必要に応じて、すべてのノードが接続されていてすべてのノードをリブートする場合は、テーブルヘッダーのチェックボックスを選択して*[すべて選択]*を選択します。それ以外の場合は、リブートする各ノードを選択します。

   テーブルのフィルタオプションを使用して、ノードのサブセットを表示できます。たとえば、特定のサイトのストレージノードのみまたはすべてのノードを表示および選択できます。

6. [Review selection]*を選択します。

選択内容の確認

この手順では、手順全体のリブートにかかる時間を確認し、正しいノードを選択したことを確認できます。

1. [Review]選択ページで[Summary]を確認します。リブートされるノード数と、すべてのノードがリブートする推定合計時間が表示されます。
2. 必要に応じて、リブートリストから特定のノードを削除するには、*[削除]*を選択します。
3. 必要に応じて、ノードを追加するには、**[前の手順]***を選択し、追加のノードを選択して[選択内容の確認]*を選択します。
4. 選択したすべてのノードでローリングリブート手順を開始する準備ができたら、*[ノードのリブート]*を選択します。
5. プライマリ管理ノードのリブートを選択した場合は、情報メッセージを読んで*[はい]*を選択します。

> プライマリ管理ノードが最後にリブートするノードになります。このノードのリブート中は、ブラウザの接続が失われます。プライマリ管理ノードが再び使用可能になったら、[Rolling reboot]ページをリロードする必要があります。

ローリングリブートの監視

ローリングリブート手順の実行中は、プライマリ管理ノードから監視できます。

手順

1. 処理の全体的な進捗状況を確認します。これには次の情報が含まれます。
   - リブートされたノードの数
   - リブート中のノードの数
   - リブートが必要なノードの数
2. 各タイプのノードの表を確認します。

   表には、各ノードでの処理の進捗状況バーが表示され、そのノードのリブートステージが表示されます。リブートステージは次のいずれかになります。

   - リブートの待機中
   - サービスを停止しています
   - システムノリフウト
   - サービスを開始しています
   - リブート完了

ローリングリブートの手順を停止する

プライマリ管理ノードからローリングリブート手順を停止できます。手順を停止すると、ステータスが「Stopping services」、「rebooting system」、または「Starting services」のノードのリブート処理が完了します。ただし、これらのノードは手順の一部として追跡されなくなります。

手順

1. メンテナンス > タスク > *ローリング再起動*を選択します。
2. [Monitor reboot]ステップで、[Stop reboot procedure]*を選択します。

タスクタブから**StorageGRID**ノードをリブートします

グリッドノードは、[Nodes]ページの[Tasks]タブで個別にリブートできます。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"Maintenance権限またはRoot Access権限"。
- プロビジョニングパスフレーズを用意します。
- プライマリ管理ノードまたはストレージノードをリブートする場合は、次の考慮事項を確認しておく必要があります。
  - プライマリ管理ノードをリブートすると、ブラウザからGrid Managerに一時的にアクセスできなくなります。
  - 特定のサイトで複数のストレージノードをリブートすると、リブート中は特定のオブジェクトにアクセスできない場合があります。この問題は、いずれかのILMルールで* Dual commit 取り込みオプショ

ンが使用されている（またはルールで Balanced *が指定されており、必要なすべてのコピーをただちに作成できない）場合に発生する可能性があります。この場合StorageGRID、新しく取り込まれたオブジェクトは同じサイト上の2つのストレージノードにコミットされ、あとでILMが評価されます。

◦ ストレージノードのリブート中もすべてのオブジェクトにアクセスできるようにするには、ノードをリブートする前に、サイトでのオブジェクトの取り込みを約 1 時間停止します。

タスクの内容

StorageGRIDがグリッドノードをリブートすると、そのノードでコマンドが実行され `reboot`、ノードがシャットダウンされて再起動されます。すべてのサービスが自動的に再開されます。

- VMwareノードをリブートすると、仮想マシンがリブートされます。
- Linuxノードをリブートすると、コンテナがリブートされます。
- StorageGRIDアプライアンスノードをリブートすると、コンピューティングコントローラがリブートされます。

複数のノードをリブートする必要がある場合は、を使用できます"ローリングリブート手順"。

手順

1. *ノード*を選択します。
2. リブートするグリッドノードを選択します。
3. [* タスク * （ Tasks * ）] タブを選択します。
4. [Reboot] を選択します。

   確認のダイアログボックスが表示されます。プライマリ管理ノードをリブートすると、サービスの停止中はブラウザと Grid Manager の接続が一時的に失われることを知らせる確認ダイアログボックスが表示されます。

5. プロビジョニングパスフレーズを入力し、「 * OK 」を選択します。
6. ノードがリブートするまで待ちます。

   サービスがシャットダウンするまでに時間がかかる場合があります。

   ノードのリブート中は、[Nodes]ページにそのノードのグレーの（Administratively Down）アイコンが表示されます。すべてのサービスが再開され、ノードがグリッドに正常に接続されると、[Nodes]ページに通常ステータス（ノード名の左側にアイコンはありません）が表示され、アクティブなアラートがなく、ノードがグリッドに接続されていることが示されます。

コマンドシェルから**StorageGRID**ノードをリブート

リブート処理を詳細に監視する必要がある場合や、Grid Managerにアクセスできない場合は、グリッドノードにログインし、コマンドシェルからServer Manager rebootコマンドを実行します。

開始する前に

あなたはファイルを持ってい `Passwords.txt`ます。

手順

1. グリッドノードにログインします。

   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`

   b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

   c. 次のコマンドを入力してrootに切り替えます。 `su -`

   d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

   rootとしてログインすると、プロンプトがからに `#`変わります `$`。

2. 必要に応じて、サービスを停止します。 `service servermanager stop`

   サービスの停止は任意ですが、実行することを推奨します。サービスのシャットダウンには最大 15 分かかる場合があります。次の手順でノードをリブートする前に、リモートからシステムにログインしてシャットダウンプロセスを監視することもできます。

3. グリッドノードをリブートします。 `reboot`

4. コマンドシェルからログアウトします。 `exit`

StorageGRIDノードをシャットダウンする

グリッドノードは、ノードのコマンドシェルからシャットダウンできます。

開始する前に

- あなたはファイルを持ってい `Passwords.txt`ます。

タスクの内容

この手順 を実行する前に、次の考慮事項を確認してください。

- 通常は、業務の中断を避けるために、一度に複数のノードをシャットダウンすることは避けてください。
- ドキュメントまたはテクニカルサポートから明示的に指示がないかぎり、メンテナンス手順 の実行中はノードをシャットダウンしないでください。
- シャットダウンプロセスは、ノードがインストールされている場所によって次のように異なります。
  - VMware ノードをシャットダウンすると、仮想マシンがシャットダウンされます。
  - Linux ノードをシャットダウンすると、コンテナがシャットダウンされます。
  - StorageGRID アプライアンスノードをシャットダウンすると、コンピューティングコントローラがシャットダウンされます。
- サイトで複数のストレージノードをシャットダウンする場合は、ノードをシャットダウンする前に、そのサイトでのオブジェクトの取り込みを約1時間停止します。

  いずれかのILMルールで* Dual commit 取り込みオプションが使用されている場合（またはルールで Balanced *オプションが使用されていて必要なすべてのコピーをすぐに作成できない場合 ）、StorageGRID は新たに取り込まれたオブジェクトを同じサイトの2つのストレージノードにただちにコミットし、あとでILMを評価します。サイトで複数のストレージノードがシャットダウンされている場合は、シャットダウン中に新たに取り込んだオブジェクトにアクセスできない可能性があります。使用可能なストレージノードがサイトで少なすぎる場合も、書き込み処理が失敗する可能性があります。を参照して "ILM を使用してオブジェクトを管理する"

手順

1. グリッドノードにログインします。

   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`

   b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

   c. 次のコマンドを入力してrootに切り替えます。 `su -`

   d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

   rootとしてログインすると、プロンプトがからに `#`変わります `$`。

2. すべてのサービスを停止します。 `service servermanager stop`

   サービスのシャットダウンには最大 15 分かかる場合があります。リモートからシステムにログインしてシャットダウンプロセスを監視することもできます。

3. VMware仮想マシンで実行されているノードまたはアプライアンスノードの場合は、shutdownコマンドを実行します。 `shutdown -h now`

   この手順は、コマンドの結果に関係なく実行し `service servermanager stop`ます。

   > アプライアンスノードでコマンドを実行したら、 `shutdown -h now`アプライアンスの電源を再投入してノードを再起動する必要があります。

   アプライアンスの場合、このコマンドはコントローラをシャットダウンしますが、アプライアンスの電源はオンになったままです。次の手順を実行する必要があります。

4. アプライアンスノードの電源をオフにする場合は、アプライアンスの手順に従います。

SG6160

a. SG6100-CNストレージコントローラの電源をオフにします。

b. SG6100-CNストレージコントローラの青色の電源LEDが消灯するまで待ちます。

SGF6112

a. アプライアンスの電源をオフにします。

b. 青色の電源 LED が消灯するまで待ちます。

SG6000

a. ストレージコントローラの背面にある緑のキャッシュアクティブ LED が消灯するまで待ちます。

   この LED は、キャッシュデータをドライブに書き込む必要があるときに点灯します。この LED が消灯するのを待ってから、電源をオフにする必要があります。

b. アプライアンスの電源をオフにし、青色の電源 LED が消灯するまで待ちます。

SG5800

a. ストレージコントローラの背面にある緑のキャッシュアクティブ LED が消灯するまで待ちます。

   この LED は、キャッシュデータをドライブに書き込む必要があるときに点灯します。この LED が消灯するのを待ってから、電源をオフにする必要があります。

b. SANtricity システムマネージャのホームページで、「 * 進行中の処理を表示」を選択します。

c. すべての処理が完了したことを確認してから、次の手順に進みます。

d. コントローラシェルフの両方の電源スイッチをオフにし、コントローラシェルフのすべてのLEDが消灯するまで待ちます。

SG5700

a. ストレージコントローラの背面にある緑のキャッシュアクティブ LED が消灯するまで待ちます。

   この LED は、キャッシュデータをドライブに書き込む必要があるときに点灯します。この LED が消灯するのを待ってから、電源をオフにする必要があります。

b. アプライアンスの電源をオフにし、すべての LED とデジタル表示ディスプレイの動作が停止するまで待ちます。

SG100または**SG1000**

a. アプライアンスの電源をオフにします。

b. 青色の電源 LED が消灯するまで待ちます。

StorageGRIDホストの電源を切る

ホストの電源をオフにする前に、そのホスト上のすべてのグリッドノードのサービスを

停止する必要があります。

手順

1. グリッドノードにログインします。

   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`

   b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

   c. 次のコマンドを入力してrootに切り替えます。 `su -`

   d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

   rootとしてログインすると、プロンプトがからに `#`変わります `$`。

2. ノードで実行されているすべてのサービスを停止します。 `service servermanager stop`

   サービスのシャットダウンには最大 15 分かかる場合があります。リモートからシステムにログインしてシャットダウンプロセスを監視することもできます。

3. ホストの各ノードについて、手順 1 と 2 を繰り返します。

4. Linux ホストの場合：

   a. ホストオペレーティングシステムにログインします。

   b. ノードを停止します。 `storagegrid node stop`

   c. ホストオペレーティングシステムをシャットダウンします。

5. VMware仮想マシンで実行されているノードまたはアプライアンスノードの場合は、shutdownコマンドを実行します。 `shutdown -h now`

   この手順は、コマンドの結果に関係なく実行し `service servermanager stop`ます。

   > アプライアンスノードでコマンドを実行したら、 `shutdown -h now`アプライアンスの電源を再投入してノードを再起動する必要があります。

   アプライアンスの場合、このコマンドはコントローラをシャットダウンしますが、アプライアンスの電源はオンになったままです。次の手順を実行する必要があります。

6. アプライアンスノードの電源をオフにする場合は、アプライアンスの手順に従います。

SG6160

a. SG6100-CNストレージコントローラの電源をオフにします。

b. SG6100-CNストレージコントローラの青色の電源LEDが消灯するまで待ちます。

SGF6112

a. アプライアンスの電源をオフにします。

b. 青色の電源 LED が消灯するまで待ちます。

SG6000

a. ストレージコントローラの背面にある緑のキャッシュアクティブ LED が消灯するまで待ちます。

   この LED は、キャッシュデータをドライブに書き込む必要があるときに点灯します。この LED が消灯するのを待ってから、電源をオフにする必要があります。

b. アプライアンスの電源をオフにし、青色の電源 LED が消灯するまで待ちます。

SG5800

a. ストレージコントローラの背面にある緑のキャッシュアクティブ LED が消灯するまで待ちます。

   この LED は、キャッシュデータをドライブに書き込む必要があるときに点灯します。この LED が消灯するのを待ってから、電源をオフにする必要があります。

b. SANtricity システムマネージャのホームページで、「 * 進行中の処理を表示」を選択します。

c. すべての処理が完了したことを確認してから、次の手順に進みます。

d. コントローラシェルフの両方の電源スイッチをオフにし、コントローラシェルフのすべてのLEDが消灯するまで待ちます。

SG5700

a. ストレージコントローラの背面にある緑のキャッシュアクティブ LED が消灯するまで待ちます。

   この LED は、キャッシュデータをドライブに書き込む必要があるときに点灯します。この LED が消灯するのを待ってから、電源をオフにする必要があります。

b. アプライアンスの電源をオフにし、すべての LED とデジタル表示ディスプレイの動作が停止するまで待ちます。

SG110または**SG1100**

a. アプライアンスの電源をオフにします。

b. 青色の電源 LED が消灯するまで待ちます。

SG100または**SG1000**

a. アプライアンスの電源をオフにします。

b. 青色の電源 LED が消灯するまで待ちます。

7. コマンドシェルからログアウトします。 `exit`

関連情報

- "SGF6112およびSG6160ストレージアプライアンス"
- "SG6000ストレージアプライアンス"
- "SG5700ストレージアプライアンス"
- "SG5800ストレージアプライアンス"
- "SG110およびSG1100サービスアプライアンス"
- "SG100およびSG1000サービス アプライアンス"

すべての**StorageGRID**ノードの電源をオフにしてオンにする

データセンターの移行などで、 StorageGRID システム全体のシャットダウンが必要になる場合があります。ここでは、通常の方法でシャットダウンと起動を実行する場合の推奨手順について、その概要を記載します。

サイトまたはグリッド内のすべてのノードの電源をオフにすると、ストレージノードがオフラインの間は、取り込まれたオブジェクトにアクセスできなくなります。

サービスを停止し、グリッドノードをシャットダウンします

StorageGRID システムの電源をオフにするには、各グリッドノードで実行されているすべてのサービスを停止してから、すべての VMware 仮想マシン、コンテナエンジン、および StorageGRID アプライアンスをシャットダウンする必要があります。

タスクの内容

まず管理ノードとゲートウェイノードのサービスを停止し、次にストレージノードのサービスを停止してください。

この方法なら、プライマリ管理ノードを使用して他のグリッドノードのステータスをできるだけ長く監視できます。

> 単一のホストに複数のグリッドノードが含まれている場合は、そのホスト上のすべてのノードを停止するまでホストをシャットダウンしないでください。ホストにプライマリ管理ノードが含まれている場合は、そのホストを最後にシャットダウンします。

> 必要に応じて、グリッドの機能や可用性に影響を与えることなくホストのメンテナンスを実行できます"Linux ホスト間でのノードの移行"。

手順

1. デフォルトでは外部 SSH アクセスはブロックされます。必要に応じて、"一時的にアクセスを許可する"。
2. すべてのクライアントアプリケーションからグリッドへのアクセスを停止します。
3. [[log_in_on_gn]][各ゲートウェイノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`

b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

c. 次のコマンドを入力してrootに切り替えます。 `su -`

d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

rootとしてログインすると、プロンプトがからに `#`変わります `$`。

4. ノードで実行されているすべてのサービスを停止します。 `service servermanager stop`

サービスのシャットダウンには最大 15 分かかる場合があります。リモートからシステムにログインしてシャットダウンプロセスを監視することもできます。

5. 前の2つの手順を繰り返して、すべてのストレージノードと非プライマリ管理ノードのサービスを停止します。

これらのノードのサービスは、どの順序で停止してもかまいません。

> コマンドを実行してアプライアンスストレージノードのサービスを停止する場合 `service servermanager stop`は、アプライアンスの電源を再投入してノードを再起動する必要があります。

6. プライマリ管理ノードに対して、およびについての手順を繰り返しますノードにログインしますノードのすべてのサービスを停止しています。

7. Linux ホストで実行されているノードの場合：

a. ホストオペレーティングシステムにログインします。

b. ノードを停止します。 `storagegrid node stop`

c. ホストオペレーティングシステムをシャットダウンします。

8. VMware仮想マシンで実行されているノードとアプライアンスストレージノードの場合は、shutdownコマンドを実行します。 `shutdown -h now`

この手順は、コマンドの結果に関係なく実行し `service servermanager stop`ます。

アプライアンスの場合、このコマンドはコンピューティングコントローラをシャットダウンしますが、アプライアンスの電源はオンになったままです。次の手順を実行する必要があります。

9. アプライアンスノードがある場合は、アプライアンスに応じた手順を実行します。

SG110または**SG1100**

a. アプライアンスの電源をオフにします。

b. 青色の電源 LED が消灯するまで待ちます。

SG100または**SG1000**

a. アプライアンスの電源をオフにします。

b. 青色の電源 LED が消灯するまで待ちます。

SG6160

a. SG6100-CNストレージコントローラの電源をオフにします。

b. SG6100-CNストレージコントローラの青色の電源LEDが消灯するまで待ちます。

SGF6112

a. アプライアンスの電源をオフにします。

b. 青色の電源 LED が消灯するまで待ちます。

SG6000

a. ストレージコントローラの背面にある緑のキャッシュアクティブ LED が消灯するまで待ちます。

   この LED は、キャッシュデータをドライブに書き込む必要があるときに点灯します。この LED が消灯するのを待ってから、電源をオフにする必要があります。

b. アプライアンスの電源をオフにし、青色の電源 LED が消灯するまで待ちます。

SG5800

a. ストレージコントローラの背面にある緑のキャッシュアクティブ LED が消灯するまで待ちます。

   この LED は、キャッシュデータをドライブに書き込む必要があるときに点灯します。この LED が消灯するのを待ってから、電源をオフにする必要があります。

b. SANtricity システムマネージャのホームページで、「 * 進行中の処理を表示」を選択します。

c. すべての処理が完了したことを確認してから、次の手順に進みます。

d. コントローラシェルフの両方の電源スイッチをオフにし、コントローラシェルフのすべてのLEDが消灯するまで待ちます。

SG5700

a. ストレージコントローラの背面にある緑のキャッシュアクティブ LED が消灯するまで待ちます。

   この LED は、キャッシュデータをドライブに書き込む必要があるときに点灯します。この LED が消灯するのを待ってから、電源をオフにする必要があります。

b. アプライアンスの電源をオフにし、すべての LED とデジタル表示ディスプレイの動作が停止するまで待ちます。

10. 必要に応じて、コマンドシェルからログアウトします。 `exit`

    これで、 StorageGRID グリッドのシャットダウンは完了です。

11. 外部SSHアクセスを許可している場合は、"アクセスをブロックする"ノードのシャットダウンが完了したら。

グリッドノードを起動します

可能であれば、次の順序でグリッドノードの電源をオンにします。

- 最初に管理ノードの電源をオンにします。
- 最後にゲートウェイノードの電源をオンにします。

> ホストに複数のグリッドノードが含まれている場合、ホストの電源を入れると、ノードは自動的にオンラインに戻ります。

手順

1. プライマリ管理ノードと非プライマリ管理ノードのホストの電源をオンにします。

   > ストレージノードが再起動されるまで、管理ノードにログインすることはできません。

2. すべてのストレージノードのホストの電源をオンにします。

   これらのノードは、どの順序で電源をオンにしてもかまいません。

3. すべてのゲートウェイノードのホストの電源をオンにします。
4. Grid Manager にサインインします。
5. *ノード*を選択し、グリッド ノードのステータスを監視します。ノード名の横に警告アイコンがないことを確認します。

関連情報

- "SGF6112およびSG6160ストレージアプライアンス"
- "SG110およびSG1100サービスアプライアンス"
- "SG100およびSG1000サービス アプライアンス"
- "SG6000ストレージアプライアンス"
- "SG5800ストレージアプライアンス"
- "SG5700ストレージアプライアンス"

ポートの再マッピング手順

StorageGRIDアプライアンスのポート再マップを削除します

ロードバランササービスのエンドポイントを設定する場合、ポートの再マッピングのマッピング先ポートとしてすでに設定されているポートを使用するには、まず既存のポートの再マッピングを削除する必要があります。そうしないと、エンドポイントが有効に

なりません。ノードのすべてのポートの再マッピングを削除するには、再マッピングされたポートが競合している各管理ノードおよびゲートウェイノードでスクリプトを実行する必要があります。

タスクの内容

この手順 は、ポートの再マッピングをすべて削除します。一部の再マッピングを保持する必要がある場合は、テクニカルサポートにお問い合わせください。

ロードバランサエンドポイントの設定については、を参照してください"ロードバランサエンドポイントの設定"。

> ポートの再マッピングでクライアントアクセスが可能な場合は、サービスの中断を回避するために、別のポートをロードバランサエンドポイントとして使用するようにクライアントを再設定します。そうしないと、ポートマッピングを削除するとクライアントアクセスが失われるため、適切にスケジュールを設定する必要があります。

> この手順 は、ベアメタルホスト上のコンテナとして導入した StorageGRID システムでは機能しません。の手順を参照してください"ベアメタルホストでのポートの再マッピングの削除"。

手順

1. デフォルトでは外部 SSH アクセスはブロックされます。必要に応じて、"一時的にアクセスを許可する"。
2. ノードにログインします。
   a. 次のコマンドを入力します。 `ssh -p 8022 admin@node_IP`

      ポート 8022 はベース OS の SSH ポートで、ポート 22 は StorageGRID を実行しているコンテナエンジンの SSH ポートです。

   b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

      rootとしてログインすると、プロンプトがからに `#`変わります `$`。
3. 次のスクリプトを実行します。 `remove-port-remap.sh`
4. ノードをリブートします。 `reboot`
5. コマンドシェルからログアウトします。 `exit`
6. 再マッピングされたポートが競合している管理ノードおよびゲートウェイノードごとに上記の手順を繰り返します。
7. 外部SSHアクセスを許可している場合は、"アクセスをブロックする"ポートの再マップの削除が完了したら。

関連情報

- "外部との通信に使用するポート"

ロードバランササービスのエンドポイントを設定する場合、ポートの再マッピングのマッピング先ポートとしてすでに設定されているポートを使用するには、まず既存のポートの再マッピングを削除する必要があります。そうしないと、エンドポイントが有効になりません。

タスクの内容

ベアメタルホストで StorageGRID を実行している場合は、ポートの再マッピングを削除する一般的な手順 ではなく、この手順 に従ってください。ノードのすべてのポートの再マッピングを削除してノードを再起動するには、再マッピングされたポートが競合している各管理ノードおよびゲートウェイノードのノード構成ファイルを編集する必要があります。

> この手順 は、ポートの再マッピングをすべて削除します。一部の再マッピングを保持する必要がある場合は、テクニカルサポートにお問い合わせください。

ロードバランサエンドポイントの設定については、 StorageGRID の管理手順を参照してください。

> この手順 では、ノードの再起動時にサービスが一時的に失われる可能性があります。

手順

1. ノードをサポートしているホストにログインします。root として、または sudo 権限を持つアカウントでログインします。
2. 次のコマンドを実行して、ノードを一時的に無効にします。 `sudo storagegrid node stop node-name`
3. vim や pico などのテキストエディタを使用して、ノードのノード構成ファイルを編集します。

   ノード構成ファイルはにあります `/etc/storagegrid/nodes/node-name.conf`。
4. ノード構成ファイルで、ポートの再マッピングが含まれているセクションを探します。

   次の例の最後の 2 行を参照してください。

```
ADMIN_NETWORK_CONFIG = STATIC
ADMIN_NETWORK_ESL = 10.0.0.0/8, 172.19.0.0/16, 172.21.0.0/16
ADMIN_NETWORK_GATEWAY = 10.224.0.1
ADMIN_NETWORK_IP = 10.224.5.140
ADMIN_NETWORK_MASK = 255.255.248.0
ADMIN_NETWORK_MTU = 1400
ADMIN_NETWORK_TARGET = eth1
ADMIN_NETWORK_TARGET_TYPE = DedicatedInterface
BLOCK_DEVICE_VAR_LOCAL = /dev/sda2
CLIENT_NETWORK_CONFIG = STATIC
CLIENT_NETWORK_GATEWAY = 47.47.0.1
CLIENT_NETWORK_IP = 47.47.5.140
CLIENT_NETWORK_MASK = 255.255.248.0
CLIENT_NETWORK_MTU = 1400
CLIENT_NETWORK_TARGET = eth2
CLIENT_NETWORK_TARGET_TYPE = DedicatedInterface
GRID_NETWORK_CONFIG = STATIC
GRID_NETWORK_GATEWAY = 192.168.0.1
GRID_NETWORK_IP = 192.168.5.140
GRID_NETWORK_MASK = 255.255.248.0
GRID_NETWORK_MTU = 1400
GRID_NETWORK_TARGET = eth0
GRID_NETWORK_TARGET_TYPE = DedicatedInterface
NODE_TYPE = VM_API_Gateway
PORT_REMAP = client/tcp/8082/443
PORT_REMAP_INBOUND = client/tcp/8082/443
```

5. PORT_REMAP エントリと PORT_REMAP_INBOUND エントリを編集して、ポートの再マッピングを削除します。

```
PORT_REMAP =
PORT_REMAP_INBOUND =
```

6. 次のコマンドを実行して、ノードのノード構成ファイルに対する変更を検証します。`sudo storagegrid node validate node-name`

   エラーや警告がある場合は、次の手順に進む前に対処してください。

7. 次のコマンドを実行して、ポートの再マッピングを行わずにノードを再起動します。 `sudo storagegrid node start node-name`
8. ファイルに記載されているパスワードを使用して、ノードにadminとしてログインし `Passwords.txt`ます。
9. サービスが正しく開始されることを確認します。
   a. サーバ上のすべてのサービスのステータスのリストを表示します。`sudo storagegrid-status`

ステータスは自動的に更新されます。

b. すべてのサービスのステータスが「 Running 」または「 Verified 」になるまで待ちます。

c. ステータス画面を終了します。`Ctrl+C`

10. 再マッピングされたポートが競合している管理ノードおよびゲートウェイノードごとに上記の手順を繰り返します。

Server Managerの手順

StorageGRIDサーバーマネージャーのステータスとバージョンを表示

グリッドノードごとに、そのグリッドノード上で実行されている Server Manager の現在のステータスとバージョンを表示できます。そのグリッドノード上で実行されているすべてのサービスの現在のステータスも取得できます。

開始する前に

あなたはファイルを持ってい `Passwords.txt`ます。

手順

1. グリッドノードにログインします。

   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`

   b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

   c. 次のコマンドを入力してrootに切り替えます。 `su -`

   d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

   rootとしてログインすると、プロンプトがからに `#`変わります `$`。

2. グリッドノード上で実行されているServer Managerの現在のステータスを表示します。 **`service servermanager status`**

   グリッドノード上で実行されている Server Manager の現在のステータスが（実行中かどうかに関係なく）報告されます。Server Managerのステータスがの場合は `running`、最後に起動されてから実行されていた時間が表示されます。例：

   ```
   servermanager running for 1d, 13h, 0m, 30s
   ```

3. グリッドノードで実行されているServer Managerの現在のバージョンを表示します。 **`service servermanager version`**

   現在のバージョンが表示されます。例：

   ```
   11.1.0-20180425.1905.39c9493
   ```

4. コマンドシェルからログアウトします。 **`exit`**

すべての**StorageGRID**サービスの現在のステータスを表示する

グリッドノード上で実行されているすべてのサービスの現在のステータスはいつでも表示できます。

開始する前に

あなたはファイルを持ってい `Passwords.txt`ます。

手順

1. グリッドノードにログインします。

   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`

   b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

   c. 次のコマンドを入力してrootに切り替えます。 `su -`

   d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

   rootとしてログインすると、プロンプトがからに `#`変わります `$`。

2. グリッドノード上で実行されているすべてのサービスのステータスを表示します。 `storagegrid-status`

   たとえば、プライマリ管理ノードの出力には、 AMS 、 CMN 、および NMS の各サービスの現在のステータスが実行中と表示されます。この出力は、サービスのステータスが変わるとすぐに更新されます。

```
Host Name                      190-ADM1
IP Address
Operating System Kernel        4.9.0          Verified
Operating System Environment   Debian 9.4     Verified
StorageGRID Webscale Release   11.1.0         Verified
Networking                                    Verified
Storage Subsystem                             Verified
Database Engine                5.5.9999+default Running
Network Monitoring             11.1.0         Running
Time Synchronization           1:4.2.8p10+dfsg Running
ams                            11.1.0         Running
cmn                            11.1.0         Running
nms                            11.1.0         Running
ssm                            11.1.0         Running
mi                             11.1.0         Running
dynip                          11.1.0         Running
nginx                          1.10.3         Running
tomcat                         8.5.14         Running
grafana                        4.2.0          Running
mgmt api                       11.1.0         Running
prometheus                     1.5.2+ds       Running
persistence                    11.1.0         Running
ade exporter                   11.1.0         Running
attrDownPurge                  11.1.0         Running
attrDownSamp1                  11.1.0         Running
attrDownSamp2                  11.1.0         Running
node exporter                  0.13.0+ds      Running
```

3. コマンドラインに戻り、 * Ctrl * + * C * を押します。

4. 必要に応じて、グリッドノードで実行されているすべてのサービスに関する静的レポートを表示します。 `/usr/local/servermanager/reader.rb`

このレポートには、継続的に更新されるレポートと同じ情報が含まれますが、サービスのステータスが変わっても更新されません。

5. コマンドシェルからログアウトします。 `exit`

StorageGRIDサーバーマネージャーとすべてのサービスを開始する

Server Manager の起動が必要な場合があります。 Server Manager を起動すると、グリッドノード上のすべてのサービスも開始されます。

開始する前に

あなたはファイルを持ってい `Passwords.txt`ます。

タスクの内容

Server Manager がすでに実行されているグリッドノードで Server Manager を起動すると、 Server Manager が再起動し、グリッドノード上のすべてのサービスが再開されます。

手順

1. グリッドノードにログインします。

   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`

   b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

   c. 次のコマンドを入力してrootに切り替えます。 `su -`

   d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

   rootとしてログインすると、プロンプトがからに `#`変わります `$`。

2. Server Managerを起動します。 `service servermanager start`

3. コマンドシェルからログアウトします。 `exit`

StorageGRIDサーバーマネージャーとすべてのサービスを再起動

Server Managerと、グリッドノード上で実行されているすべてのサービスを再起動する必要がある場合があります。

開始する前に

あなたはファイルを持ってい `Passwords.txt`ます。

手順

1. グリッドノードにログインします。

   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`

   b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

   c. 次のコマンドを入力してrootに切り替えます。 `su -`

   d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

rootとしてログインすると、プロンプトがからに `#`変わります `$`。

2. グリッドノード上のServer Managerおよびすべてのサービスを再起動します。 `service servermanager restart`

   グリッドノード上の Server Manager およびすべてのサービスが停止され、その後再開されます。

   > コマンドを使用する `restart`ことは、コマンドに続けてコマンドを `start`使用することと同じ `stop`です。

3. コマンドシェルからログアウトします。 `exit`

StorageGRIDサーバーマネージャーとすべてのサービスを停止します

Server Manager は常時実行中であることが前提ですが、あるグリッドノードで実行されている Server Manager およびすべてのサービスの停止が必要になる場合もあります。

開始する前に

あなたはファイルを持ってい `Passwords.txt`ます。

手順

1. グリッドノードにログインします。

   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`

   b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

   c. 次のコマンドを入力してrootに切り替えます。 `su -`

   d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

   rootとしてログインすると、プロンプトがからに `#`変わります `$`。

2. グリッドノードで実行されているServer Managerおよびすべてのサービスを停止します。 `service servermanager stop`

   グリッドノードで実行されている Server Manager およびすべてのサービスが正常に終了します。サービスのシャットダウンには最大 15 分かかる場合があります。

3. コマンドシェルからログアウトします。 `exit`

StorageGRIDサービスの現在のステータスを表示する

グリッドノード上で実行されているサービスの現在のステータスは、いつでも確認できます。

開始する前に

あなたはファイルを持ってい `Passwords.txt`ます。

手順

1. グリッドノードにログインします。

a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`

b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

c. 次のコマンドを入力してrootに切り替えます。 `su -`

d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

rootとしてログインすると、プロンプトがからに `#`変わります `$`。

2. グリッドノード上で実行されているサービスの現在のステータスを表示します。「 * SERVICE_SERVICE_STATUS * 」グリッドノード上で実行されている要求されたサービスの現在のステータスが報告されます（実行中かどうかは関係ありません）。例：

```
cmn running for 1d, 14h, 21m, 2s
```

3. コマンドシェルからログアウトします。 **`exit`**

StorageGRIDサービスを停止する

一部のメンテナンス手順では、グリッドノード上の他のサービスを実行したまま、単一のサービスを停止する必要があります。個々のサービスの停止は、メンテナンス手順 から指示があった場合にのみ実行してください。

開始する前に

あなたはファイルを持ってい `Passwords.txt`ます。

タスクの内容

これらの手順を使用してサービスを「管理上停止」した場合、Server Managerはサービスを自動的に再開しません。サービスを手動で開始するか、 Server Manager を再起動する必要があります。

ストレージノード上の LDR サービスを停止する必要がある場合は、アクティブな接続があると、サービスの停止に時間がかかることがあります。

手順

1. グリッドノードにログインします。

a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`

b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

c. 次のコマンドを入力してrootに切り替えます。 `su -`

d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

rootとしてログインすると、プロンプトがからに `#`変わります `$`。

2. 個 々 のサービスを停止します。 `service servicename stop`

例：

```
service ldr stop
```

サービスの停止には最大 11 分かかる場合があります。

3. コマンドシェルからログアウトします。 `exit`

関連情報

"サービスを強制終了します"

StorageGRIDサービスを強制終了する

サービスをすぐに停止する必要がある場合は、コマンドを使用し `force-stop`ます。

開始する前に

あなたはファイルを持ってい `Passwords.txt`ます。

手順

1. グリッドノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
   b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

   rootとしてログインすると、プロンプトがからに `#`変わります `$`。

2. サービスを手動で強制終了します。 `service servicename force-stop`

   例：

   ```
   service ldr force-stop
   ```

   システムは 30 秒待機してからサービスを終了します。

3. コマンドシェルからログアウトします。 `exit`

StorageGRIDサービスを開始または再起動する

停止されたサービスの開始や、サービスの停止と再開が必要になる場合があります。

開始する前に

あなたはファイルを持ってい `Passwords.txt`ます。

手順

1. グリッドノードにログインします。

a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。
c. 次のコマンドを入力してrootに切り替えます。 `su -`
d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

rootとしてログインすると、プロンプトがからに `#`変わります `$`。

2. サービスが現在実行されているか停止されているかに基づいて、問題 に対するコマンドを決定します。

   ◦ サービスが現在停止している場合は、コマンドを使用し `start`てサービスを手動で開始します。 `service servicename start`

   例：

   ```
   service ldr start
   ```

   ◦ サービスが現在実行中の場合は、コマンドを使用し `restart`てサービスを停止し、再開します。 `service servicename restart`

   例：

```
service ldr restart
```

+

> コマンドを使用する `restart`ことは、コマンドに続けてコマンドを `start`使用することと同じ `stop`です。サービスが現在停止している場合でも、を実行できます `restart`。

3. コマンドシェルからログアウトします。 `exit`

StorageGRID DoNotStart ファイルを使用する

テクニカルサポートの指示の下でメンテナンスや設定の手順を実行している場合は、Server Manager の起動時または再起動時にサービスが開始されないように、DoNotStart ファイルを使用するよう求められることがあります。

> DoNotStart ファイルは、テクニカルサポートから指示があった場合のみ追加または削除してください。

サービスが開始されないようにするには、そのサービスのディレクトリに DoNotStart ファイルを配置します。Server Manager は起動時に DoNotStart ファイルを検索し、ファイルが存在する場合、サービス（およびそれに依存するサービス）は開始されません。DoNotStart ファイルを削除すると、停止されていたサービスは、 Server Manager が次回起動または再起動したときに開始されます。DoNotStartファイルが削除されても、サービスは自動的に開始されません。

すべてのサービスを再開しないようにする最も効率的な方法は、 NTP サービスを開始しないようにすることです。すべてのサービスはNTPサービスに依存しており、NTPサービスが実行されていないと実行できません。

サービスの **DoNotStart** ファイルを追加します

個別のサービスが開始しないようにするには、グリッドノードのそのサービスのディレクトリに DoNotStart ファイルを追加します。

開始する前に

あなたはファイルを持ってい `Passwords.txt`ます。

手順

1. グリッドノードにログインします。

   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`

   b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

   c. 次のコマンドを入力してrootに切り替えます。 `su -`

   d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

   rootとしてログインすると、プロンプトがからに `#`変わります `$`。

2. DoNotStartファイルを追加します。 `touch /etc/sv/service/DoNotStart`

   `service`は、開始できないようにするサービスの名前です。例えば、

   ```
   touch /etc/sv/ldr/DoNotStart
   ```

   DoNotStart ファイルが作成されます。ファイルの内容は不要です。

   Server Manager またはグリッドノードが再起動されたときに Server Manager は再起動しますが、サービスは再開されません。

3. コマンドシェルからログアウトします。 `exit`

サービスの **DoNotStart** ファイルを削除します

サービスを開始できないようにする DoNotStart ファイルを削除するには、そのサービスを開始する必要があります。

開始する前に

あなたはファイルを持ってい `Passwords.txt`ます。

手順

1. グリッドノードにログインします。

   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`

b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

c. 次のコマンドを入力してrootに切り替えます。 `su -`

d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

rootとしてログインすると、プロンプトがからに `#`変わります `$`。

2. serviceディレクトリからDoNotStartファイルを削除します。 `rm /etc/sv/service/DoNotStart`

ここで、 `service`はサービスの名前です。例えば、

```
rm /etc/sv/ldr/DoNotStart
```

3. サービスを開始します。 `service servicename start`

4. コマンドシェルからログアウトします。 `exit`

StorageGRID でのサーバーマネージャーのトラブルシューティング

Server Manager の使用時に問題が発生した場合は、そのログファイルを確認します。

Server Managerに関連するエラーメッセージは、Server Managerログファイルに記録されます。このファイルは次の場所にあります。 `/var/local/log/servermanager.log`

このファイルでエラーに関するエラーメッセージを確認してください。必要に応じて、問題 をテクニカルサポートにエスカレーションします。テクニカルサポートにログファイルを転送するよう求められる場合があります。

エラー状態のサービス

サービスがエラー状態になったことが検出された場合は、サービスの再開を試みてください。

開始する前に

あなたはファイルを持ってい `Passwords.txt`ます。

タスクの内容

Server Manager は、サービスを監視し、予期せず停止したサービスがあれば再起動します。サービスで障害が発生すると、 Server Manager はそのサービスの再起動を試行します。5 分以内にサービスの開始が 3 回失敗すると、サービスはエラー状態になります。Server Manager は再起動を試行しません。

手順

1. グリッドノードにログインします。

a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`

b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

c. 次のコマンドを入力してrootに切り替えます。 `su -`

d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

rootとしてログインすると、プロンプトがからに `#`変わります `$`。

2. サービスのエラー状態を確認します。 `service servicename status`

   例：

   ```
   service ldr status
   ```

   サービスがエラー状態の場合は、次のメッセージが返されます。 `servicename in error state`例：

   ```
   ldr in error state
   ```

   > サービスステータスがの場合は `disabled`、の手順を参照してください"サービスのDoNotStart ファイルを削除しています"。

3. サービスを再起動してエラー状態の解消を試みます。 `service servicename restart`

   サービスを再開できない場合は、テクニカルサポートにお問い合わせください。

4. コマンドシェルからログアウトします。 `exit`

ネットワーク手順

StorageGRIDグリッドネットワークのサブネットを更新します

StorageGRID は、グリッドネットワーク（ eth0 ）上のグリッドノード間の通信に使用されるネットワークサブネットのリストを管理します。このエントリには、StorageGRID システムの各サイトでグリッドネットワークに使用されているサブネット、およびグリッドネットワークゲートウェイ経由でアクセスされる NTP 、 DNS 、 LDAP 、またはその他の外部サーバに使用されるサブネットが含まれます。グリッドノードまたは新しいサイトを追加した場合は、サブネットの更新、またはグリッドネットワークへのサブネットの追加が必要になることがあります。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"Maintenance権限またはRoot Access権限"。
- プロビジョニングパスフレーズを用意します。
- 設定するサブネットのネットワークアドレスを CIDR 表記で指定しておきます。

タスクの内容

新しいサブネットの追加を含む拡張アクティビティを実行する場合は、拡張手順 を開始する前に、グリッドネットワークサブネットリストに新しいサブネットを追加する必要があります。それ以外の場合は、拡張をキャンセルして新しいサブネットを追加し、もう一度拡張を開始する必要があります。

どのノードのグリッド ネットワーク、管理ネットワーク、またはクライアント ネットワークにも、次の IPv4 アドレスを含むサブネットを使用しないでください。

- 192,168,130,101
- 192,168,130,121
- 192,168,131,101
- 192,168,131,121
- 192,168,130,102
- 192,168,130,122
- 192,168,131,102
- 192,168,131,122
- 198.51.100.2
- 198.51.100.4

たとえば、どのノードのグリッド ネットワーク、管理ネットワーク、またはクライアント ネットワークにも次のサブネット範囲を使用しないでください。

- 192.168.130.0/24 は、このサブネット範囲に IP アドレス 192.168.130.101 と 192.168.130.102 が含まれているためです。
- 192.168.131.0/24 は、このサブネット範囲に IP アドレス 192.168.131.101 と 192.168.131.102 が含まれているためです。
- 198.51.100.0/24 は、このサブネット範囲に IP アドレス 198.51.100.2 と 198.51.100.4 が含まれているためです。

サブネットを追加します

手順

1. メンテナンス > ネットワーク > グリッド ネットワーク を選択します。
2. CIDR表記で新しいサブネットを追加する場合は、*[別のサブネットを追加]*を選択します。

   たとえば、と入力し `10.96.104.0/22`ます。

3. プロビジョニングパスフレーズを入力し、 * Save * を選択します。
4. 変更が適用されるまで待ってから、新しい回復パッケージをダウンロードしてください。
   a. メンテナンス > システム > *回復パッケージ*を選択します。
   b. **Provisioning passphrase** を入力してください。

リカバリ パッケージ ファイルには、 StorageGRIDシステムからデータを取得するために使用できる暗号化キーとパスワードが含まれているため、セキュリティで保護する必要があります。プライマリ管理ノードを回復するためにも使用されます。

指定したサブネットが、 StorageGRID システムに対して自動的に設定されます。

サブネットを編集します

手順

1. メンテナンス > ネットワーク > グリッド ネットワーク を選択します。
2. 編集するサブネットを選択し、必要な変更を行います。
3. プロビジョニングパスフレーズを入力し、 * Save * を選択します。
4. 確認ダイアログボックスで「 * はい * 」を選択します。
5. 変更が適用されるまで待ってから、新しい回復パッケージをダウンロードしてください。
   a. メンテナンス > システム > *回復パッケージ*を選択します。
   b. **Provisioning passphrase** を入力してください。

サブネットを削除します。

手順

1. メンテナンス > ネットワーク > グリッド ネットワーク を選択します。
2. サブネットの横にある削除アイコン を選択します。
3. プロビジョニングパスフレーズを入力し、*[保存]*を選択します。
4. 確認ダイアログボックスで「 * はい * 」を選択します。
5. 変更が適用されるまで待ってから、新しい回復パッケージをダウンロードしてください。
   a. メンテナンス > システム > *回復パッケージ*を選択します。
   b. **Provisioning passphrase** を入力してください。

IP アドレスを設定する

StorageGRID IP アドレスに関するガイドライン

IP 変更ツールを使用してグリッドノードの IP アドレスを設定することで、ネットワーク設定を実行できます。

グリッドの導入時に設定されたネットワーク設定を変更するには、ほとんどの場合、 IP 変更ツールを使用する必要があります。標準の Linux ネットワークコマンドおよびファイルを使用して手動で変更すると、すべての StorageGRID サービスに変更が反映されなかったり、アップグレード、リブート、ノードリカバリ手順の実行後に変更が失われたりすることがあります。

IP 変更手順 は、停止を伴う手順 の可能性があります。グリッドの一部は、新しい設定が適用されるまで使用できない場合があります。

グリッドネットワークサブネットリストのみを変更する場合は、グリッドマネージャを使用してネットワーク設定の追加または変更を行います。グリッドネットワーク設定問題 が原因でグリッドマネージャにアクセスできない場合、またはグリッドネットワークルーティングの変更とその他のネットワーク変更を同時に実行する場合は、 IP 変更ツールを使用します。

グリッド内のすべてのノードのグリッドネットワークIPアドレスを変更する場合は、を使用し"グリッド全体で変更される特殊な手順"ます。

イーサネットインターフェイス

eth0 に割り当てられる IP アドレスは、常にグリッドノードのグリッドネットワーク IP アドレスになります。eth1 に割り当てられている IP アドレスは、常にグリッドノードの管理ネットワーク IP アドレスです。eth2 に割り当てられている IP アドレスは、常にグリッドノードのクライアントネットワーク IP アドレスです。

StorageGRID アプライアンスなどの一部のプラットフォームでは、 eth0 、 eth1 、 eth2 が、下位のブリッジで構成されるアグリゲートインターフェイスや物理 / VLAN インターフェイスのボンドである場合があります。これらのプラットフォームでは、 * ssm* > * Resources * タブに、 eth0 、 eth1 、 eth2 に加えて、他のインターフェイスに割り当てられているグリッドネットワーク、管理ネットワーク、およびクライアントネットワークの IP アドレスが表示されることがあります。

DHCP

DHCP は導入フェーズでのみ設定できます。設定中にDHCPを設定することはできません。グリッドノードの IP アドレス、サブネットマスク、およびデフォルトゲートウェイを変更する場合は、 IP アドレス変更手順を使用する必要があります。IP 変更ツールを使用すると、原因 の DHCP アドレスが静的アドレスになります。

ハイアベイラビリティ（**HA**）グループ

- クライアントネットワークインターフェイスがHAグループに含まれている場合、そのインターフェイスのクライアントネットワークIPアドレスを、HAグループに設定されているサブネット外のアドレスに変更することはできません。
- クライアントネットワークのIPアドレスを、クライアントネットワークインターフェイスで設定されたHAグループに割り当てられている既存の仮想IPアドレスの値に変更することはできません。
- グリッドネットワークインターフェイスがHAグループに含まれている場合、そのインターフェイスのグリッドネットワークIPアドレスをHAグループに設定されているサブネット外のアドレスに変更することはできません。
- グリッドネットワークのIPアドレスを、グリッドネットワークインターフェイスに設定されたHAグループに割り当てられている既存の仮想IPアドレスの値に変更することはできません。

StorageGRIDでノードネットワーク構成を変更する

IPアドレス変更ツールを使用すると、1つまたは複数のノードのネットワーク構成を変更できます。グリッドネットワークの設定を変更したり、管理者ネットワークやクライアントネットワークを追加、変更、または削除したりできます。アプライアンスノードの BMC の LAN IP 設定を変更することもできます。

開始する前に

あなたはファイルを持ってい `Passwords.txt`ます。

タスクの内容

Linux: グリッド ノードを管理ネットワークまたはクライアント ネットワークに初めて追加する場合、以前にノード構成ファイルで ADMIN_NETWORK_TARGET または CLIENT_NETWORK_TARGET を構成していなかったときは、ここで構成する必要があります。 StorageGRIDをご覧ください"インストール手順"Linux オペ

レーティング システム用。

アプライアンス： StorageGRID アプライアンスでは、初期インストール時にStorageGRID アプライアンスインストーラでクライアントネットワークまたは管理ネットワークを設定しなかった場合、IP変更ツールのみを使用してネットワークを追加することはできません。まず、リンクを設定し、アプライアンスを通常の動作モードに戻してから、IP変更ツールを使用してネットワーク設定を変更する必要があります "アプライアンスをメンテナンスモードにします"。を参照してください "ネットワークリンクを設定するための手順"。

任意のネットワーク上の 1 つ以上のノードの IP アドレス、サブネットマスク、ゲートウェイ、または MTU 値を変更できます。

クライアントネットワークまたは管理ネットワークからノードを追加または削除することもできます。

- クライアントネットワークまたは管理ネットワークにノードを追加するには、そのネットワーク上の IP アドレス / サブネットマスクをノードに追加します。
- クライアントネットワークまたは管理ネットワークからノードを削除するには、そのネットワーク上のノードの IP アドレス / サブネットマスクを削除します。

  グリッドネットワークからノードを削除できません。

> IPアドレスの交換は許可されていません。グリッドノード間で IP アドレスを交換する必要がある場合は、一時的な中間 IP アドレスを使用する必要があります。

> StorageGRID システムでシングル サインオン（SSO）が有効になっており、管理ノードの IP アドレスを変更する場合、管理ノードの IP アドレスを使用して構成された証明書利用者信頼（推奨されている完全修飾ドメイン名ではなく）はすべて無効になることに注意してください。今後は、そのノードにサインインできなくなります。IP アドレスを変更した直後に、Active Directory Federation Services (AD FS) 内のノードの証明書利用者信頼を新しい IP アドレスで更新または再構成する必要があります。"OIDC" または "SAML" を使用した SSO の設定手順を参照してください。

> IP 変更ツールを使用してネットワークに加えた変更は、 StorageGRID アプライアンスのインストーラファームウェアに反映されます。そのため、アプライアンスに StorageGRID ソフトウェアを再インストールした場合や、アプライアンスをメンテナンスモードにした場合も、正しいネットワーク設定が適用されます。

手順

1. デフォルトでは外部 SSH アクセスはブロックされます。必要に応じて、"一時的にアクセスを許可する"。
2. プライマリ管理ノードにログインします。

   a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`

   b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

   c. 次のコマンドを入力してrootに切り替えます。 `su -`

   d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

   rootとしてログインすると、プロンプトがからに `#`変わります `$`。

3. 次のコマンドを入力して、IP変更ツールを起動します。 `change-ip`
4. プロンプトでプロビジョニングパスフレーズを入力します。

   メインメニューが表示されます。

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

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

Selection:
```

5. オプションで * 1 * を選択して、更新するノードを選択します。次に、次のいずれかのオプションを選択します。

   - *1 * ：シングルノード — 名前で選択
   - * 2 * ：単一ノード — サイトで選択してから名前で選択します
   - *3: シングルノード — 現在の IP で選択
   - * 4 * ：サイト内のすべてのノード
   - * 5 * ：グリッド内のすべてのノード
     - 注： * すべてのノードを更新する場合は、「 all 」が選択されたままにしておきます。

   選択を行うと、メインメニューが表示され、 [選択したノード * （ Selected nodes * ）] フィールドが更新されて選択内容が反映されます。以降のすべての操作は、表示されているノードでのみ実行されます。

6. メインメニューでオプション * 2 * を選択し、選択したノードの IP / マスク、ゲートウェイ、および MTU 情報を編集します。
   a. 変更するネットワークを選択します。
      - * 1 * ：グリッドネットワーク
      - * 2 * ：管理ネットワーク
      - *3 *: クライアントネットワーク
      - **4**:すべてのネットワーク

      選択すると、ノード名、ネットワーク名（グリッド、管理、またはクライアント）、データタイプ（IP /マスク、 ゲートウェイ（MTU）、および現在の値。

      DHCP によって設定されたインターフェイスの IP アドレス、プレフィックス長、ゲートウェイ、または MTU を編集すると、インターフェイスが static に変更されます。DHCP によって設定されたインターフェイスを変更するように選択すると、インターフェイスが static に変更されることを通知する警告が表示されます。

として設定されたインターフェイスは `fixed`編集できません。

b. 新しい値を設定するには、現在の値の形式で入力します。

c. 現在の値を変更しない場合は、 **Enter** キーを押します。

d. データタイプがの場合は `IP/mask`、* d または 0.0.0.0/0 *と入力して、ノードから管理ネットワークまたはクライアントネットワークを削除できます。

e. 変更するすべてのノードを編集したら、「 * q * 」と入力してメインメニューに戻ります。

変更内容は、クリアまたは適用されるまで保持されます。

7. 次のいずれかのオプションを選択して、変更内容を確認します。

◦ **5**: 変更された項目のみを表示するために分離された出力の編集を表示します。変更は、次の出力例に示すように、緑（追加）または赤（削除）で強調表示されます。

```
================================================================================
Site: RTP
================================================================================
username-x Grid    IP      [    172.16.0.239/21 ]: 172.16.0.240/21
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Admin   IP      [    10.224.0.244/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.245/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.240/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.241/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.242/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.243/21 ]: 0.0.0.0/0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   MTU     [               1400 ]: 0
username-x Admin   MTU     [               1400 ]: 0
username-x Admin   MTU     [               1400 ]: 0
username-x Admin   MTU     [               1400 ]: 0
username-x Admin   MTU     [               1400 ]: 0
username-x Admin   MTU     [               1400 ]: 0
Press Enter to continue
```

◦ **6**: 編集内容を出力に表示し、設定全体を表示します。変更は、緑（追加）または赤（削除）で強調表示されます。

> 一部のコマンドラインインターフェイスでは、追加と削除が取り消し線で示される場合があります。正しく表示されるためには、使用するターミナルクライアントが必要な VT100 エスケープシーケンスをサポートしている必要があります。

8. オプション * 7 * を選択して、すべての変更を検証します。

この検証により、グリッド、管理、クライアントの各ネットワークに関するルール（重複するサブネットの使用の禁止など）に違反していないことが確認されます。

この例では、検証でエラーが返されています。

```
Validating new networking configuration... FAILED.

  DK-10-224-5-20-G1: The admin subnet 172.18.0.0/16 overlaps the 172.18.0.0/21 grid network.
  DK-10-224-5-22-S1: Duplicate Grid IP 172.16.5.18 (also in use by DK-10-224-5-21-ADM1)

You must correct these errors before you can apply any changes.
Checking for Grid Network IP address swaps... PASSED.

Press Enter to continue
```

この例では、検証に合格しています。

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

Press Enter to continue
```

9. 検証に合格したら、次のいずれかのオプションを選択します。
   - **8**: 適用されていない変更を保存します。

     このオプションを使用すると、適用されていない変更を失うことなく、 IP 変更ツールを終了してあとで再起動できます。

   - **10**: 新しいネットワーク設定を適用します。
10. オプション * 10 * を選択した場合は、次のいずれかのオプションを選択します。
    - * apply * ：必要に応じて、変更をただちに適用し、各ノードを自動的に再起動します。

      新しいネットワーク設定で物理的な変更が不要な場合は、 *apply * を選択して、変更をすぐに適用できます。必要に応じて、ノードが自動的に再起動されます。再起動が必要なノードが表示されます。

    - * stage * ：ノードが次回手動で再起動されるときに変更を適用します。

      新しいネットワーク構成を機能させるためにネットワーク構成を物理的または仮想的に変更する必要がある場合は、 * stage * オプションを使用して影響を受けるノードをシャットダウンし、必要な物理ネットワーク変更を行って、影響を受けるノードを再起動する必要があります。これらのネットワーク変更を行わずに [*apple] を選択すると、通常、変更は失敗します。

      > stage * オプションを使用する場合は、システムの停止を最小限に抑えるためにステージング後すぐにノードを再起動する必要があります。

    - **cancel**:この時点ではネットワークを変更しないでください。

      提案した変更がノードの再起動を必要とするかどうかが不明である場合は、ユーザへの影響を最小限に抑えるために変更を延期できます。「 * CANCEL * 」を選択すると、メインメニューに戻り、変更内容が保持されるので、後で適用できます。

      apply * または * stage * を選択すると、新しいネットワーク構成ファイルが生成され、プロビジョニングが実行され、ノードが新しい作業情報で更新されます。

      プロビジョニング中に、更新が適用されたときのステータスが出力に表示されます。

```
Generating new grid networking description file...

Running provisioning...

Updating grid network configuration on Name
```

変更を適用またはステージングすると、グリッド構成の変更の結果として新しいリカバリ パッケージが生成されます。

11. 「 * stage * 」を選択した場合は、プロビジョニングが完了したあとに次の手順を実行します。
    a. ネットワークに対して必要な物理的または仮想的な変更を行います。
        - 物理ネットワークの変更 * ：必要に応じて、物理ネットワークに変更を加え、ノードを安全にシャットダウンします。
        - Linux *：ノードを管理ネットワークまたはクライアントネットワークに初めて追加する場合は、の説明に従ってインターフェイスが追加されていることを確認します。"Linux ：既存のノードにインターフェイスを追加"
    b. 影響を受けたノードを再起動します。
12. 変更が完了したら、「 *0 」を選択して IP 変更ツールを終了します。
13. グリッド マネージャーから新しいリカバリ パッケージをダウンロードします。
    a. メンテナンス > システム > *回復パッケージ*を選択します。
    b. プロビジョニングパスフレーズを入力します。
14. 外部SSHアクセスを許可している場合は、"アクセスをブロックする"ノードネットワーク構成の変更が完了したら。

LACP PDUレートを一時的に変更する

NIC ファームウェアのアップグレードなど、アプライアンスにインストールされているネットワーク コンポーネントに対してメンテナンス操作を実行するには、現在の LACP PDU レート設定が NIC 通信タイミング要件を満たしていることを確認できます。必要に応じて、LACP PDU レートを高速 (1 秒待機) と低速 (30 秒待機) の間で非永続的に切り替えることができます。

> LACP PDUレートを永続的に変更するには、 "ネットワークリンクを設定する" 。

開始する前に

- 管理ノードがインストールされ、実行されています。
- あなたはファイルを持ってい `Passwords.txt`ます。

手順

1. プライマリ管理ノードにログインします。
    a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`
    b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。
    c. 次のコマンドを入力してrootに切り替えます。 `su -`

d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

rootとしてログインすると、プロンプトがからに `#`変わります `$`。

2. 現在の LACP PDU レート設定を確認するには、次のコマンドを入力します。

```
run-each-node --parallel --port 8022 '/usr/sbin/set-lacp-rate.sh'
```

3. LACP PDU レートを一時的に変更するには、次のコマンドを入力します。

```
run-each-node --parallel --port 8022 '/usr/sbin/set-lacp-rate.sh <speed>'
```

どこ `<speed>`は `fast`または `slow`。

LACP PDU レートは、アプライアンスの次回の再起動時に以前の設定に戻ります。

アプライアンスノードの**BMC LAN IP**設定を変更する

アプライアンスノードの BMC の LAN IP 設定を変更できます。

1. グリッドマネージャで、ノード > グリッドノード > **BMC**設定 に移動します。
2. LAN IP設定セクションで、IP割り当てタイプとして **Static** または **DHCP** を選択します。
3. BMC の MAC アドレス、IPv4 アドレス （CIDR）、およびデフォルト ゲートウェイを入力してください。
4. [保存（ Save ）] を選択します。

BMC LAN IP設定は、 `PUT /bmc-configuration/root-password`または `GET /bmc-configuration/root-password` APIを使用して変更または表示することもできます。

StorageGRID の管理ネットワークのサブネットリストを追加または変更します

ノードの管理ネットワークサブネットリストで、サブネットの追加、削除、または変更を行うことができます。

開始する前に

- あなたはファイルを持ってい `Passwords.txt`ます。

管理ネットワークサブネットリストで、すべてのノードに対してサブネットの追加、削除、または変更を行うことができます。

どのノードのグリッド ネットワーク、管理ネットワーク、またはクライアント ネットワークにも、次の IPv4 アドレスを含むサブネットを使用しないでください。

- 192,168,130,101
- 192,168,130,121
- 192,168,131,101
- 192,168,131,121
- 192,168,130,102
- 192,168,130,122
- 192,168,131,102
- 192,168,131,122
- 198.51.100.2
- 198.51.100.4

たとえば、どのノードのグリッド ネットワーク、管理ネットワーク、またはクライアント ネットワークにも次のサブネット範囲を使用しないでください。

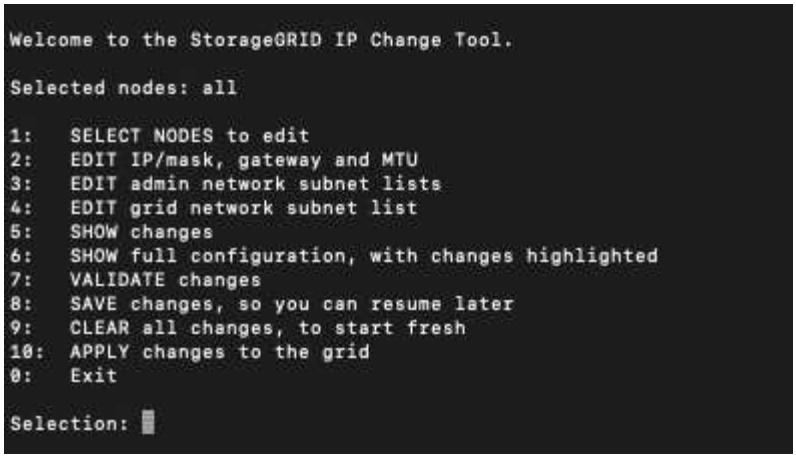
- 192.168.130.0/24 は、このサブネット範囲に IP アドレス 192.168.130.101 と 192.168.130.102 が含まれているためです。
- 192.168.131.0/24 は、このサブネット範囲に IP アドレス 192.168.131.101 と 192.168.131.102 が含まれているためです。
- 198.51.100.0/24 は、このサブネット範囲に IP アドレス 198.51.100.2 と 198.51.100.4 が含まれているためです。

手順

1. デフォルトでは外部 SSH アクセスはブロックされます。必要に応じて、"一時的にアクセスを許可する"。
2. プライマリ管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`
   b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

   rootとしてログインすると、プロンプトがからに `#`変わります `$`。
3. 次のコマンドを入力して、IP変更ツールを起動します。 `change-ip`
4. プロンプトでプロビジョニングパスフレーズを入力します。

   メインメニューが表示されます。



5. 必要に応じて、処理を実行するネットワークまたはノードを制限します。次のいずれかを選択します。
   - 操作を実行する特定のノードでフィルターを適用する場合は、 * 1 * を選択して、編集するノードを選択します。次のいずれかのオプションを選択します。
     - * 1 * ：シングルノード（名前で選択）
     - * 2 * ：シングルノード（サイトで選択したあとに名前で選択）
     - * 3 * ：シングルノード（現在の IP で選択）
     - * 4 * ：サイト内のすべてのノード
     - * 5 * ：グリッド内のすべてのノード
     - * 0 * ：戻ります
   - 「すべて」を選択したままにします。選択が完了すると、メインメニュー画面が表示されます。[選択したノード] フィールドに新しい選択内容が反映され、選択したすべての操作がこの項目に対してのみ実行されます。
6. メインメニューで、管理ネットワークのサブネットを編集するオプションを選択します（オプション * 3 * ）。
7. 次のいずれかを選択します。
   - サブネットを追加するには、次のコマンドを入力します。 `add CIDR`
   - サブネットを削除するには、次のコマンドを入力します。 `del CIDR`
   - 次のコマンドを入力して、サブネットのリストを設定します。 `set CIDR`

   すべてのコマンドで、次の形式で複数のアドレスを入力できます。 `add CIDR, CIDR`

   例： `add 172.14.0.0/16, 172.15.0.0/16, 172.16.0.0/16`

   「上矢印」を使用して以前に入力した値を現在の入力プロンプトに呼び出し、必要に応じて編集することで、入力に必要な量を減らすことができます。

   次の入力例では、管理ネットワークサブネットリストにサブネットを追加しています。

```
Editing: Admin Network Subnet List for node DK-10-224-5-20-G1

Press <enter> to use the list as shown
Use up arrow to recall a previously typed value, which you can then edit
Use 'add <CIDR> [, <CIDR>]' to add subnets <CIDR> [, <CIDR>] to the list
Use 'del <CIDR> [, <CIDR>]' to delete subnets <CIDR> [, <CIDR>] from the list
Use 'set <CIDR> [, <CIDR>]' to set the list to the given list
Use q to complete the editing session early and return to the previous menu

DK-10-224-5-20-G1
  10.0.0.0/8
  172.19.0.0/16
  172.21.0.0/16
  172.20.0.0/16

[add/del/set/quit <CIDR>, ...]: add 172.14.0.0/16, 172.15.0.0/16
```

8. 準備ができたら、「 * q * 」と入力してメインメニュー画面に戻ります。変更内容は、クリアまたは適用されるまで保持されます。

> 手順 3 で「すべての」ノード選択モードのいずれかを選択した場合は、**Enter** (q* なし) を押して、リスト内の次のノードに移動します。

9. 次のいずれかを選択します。

   - オプション * 5 * を選択すると、変更された項目のみを表示するために分離された出力に編集内容が表示されます。次の出力例に示すように、変更は緑（追加）または赤（削除）で強調表示されます。

```
================================================================================
Site: Data Center 1
================================================================================
DC1-ADM1-105-154 Admin  Subnets                          add 172.17.0.0/16
                                                         del 172.16.0.0/16
                                [       172.14.0.0/16 ]
                                [       172.15.0.0/16 ]
                                [       172.17.0.0/16 ]
                                [       172.19.0.0/16 ]
                                [       172.20.0.0/16 ]
                                [       172.21.0.0/16 ]
Press Enter to continue
```

   - オプション * 6 * を選択すると、設定全体を表示する出力に編集内容が表示されます。変更は、緑（追加）または赤（削除）で強調表示されます。* 注：一部のターミナルエミュレータでは、取り消し線の形式で追加と削除が表示される場合があります。

     サブネットリストを変更しようとすると、次のメッセージが表示されます。

```
CAUTION: The Admin Network subnet list on the node might contain /32
subnets derived from automatically applied routes that aren't
persistent. Host routes (/32 subnets) are applied automatically if
the IP addresses provided for external services such as NTP or DNS
aren't reachable using default StorageGRID routing, but are reachable
using a different interface and gateway. Making and applying changes
to the subnet list will make all automatically applied subnets
persistent. If you don't want that to happen, delete the unwanted
subnets before applying changes. If you know that all /32 subnets in
the list were added intentionally, you can ignore this caution.
```

NTP および DNS サーバのサブネットをネットワークに明確に割り当てなかった場合、 StorageGRID は接続のホストルート（ /32 ）を自動的に作成します。たとえば、 DNS サーバまたは NTP サーバへのアウトバウンド接続に /16 または /24 ルートを使用する場合は、自動的に作成された /32 ルートを削除し、必要なルートを追加する必要があります。自動で作成されたホストルートを削除しなかった場合は、サブネットリストに変更を適用したあともそのルートが保持されます。

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

10. オプション * 7 * を選択して、すべての段階的な変更を検証します。

    この検証により、重複するサブネットを使用するなど、グリッドネットワーク、管理ネットワーク、クライアントネットワークのルールが確実に実行されます。

11. 必要に応じて、オプション * 8 を選択してステージングされたすべての変更を保存し、後で戻って変更を続行します。

    このオプションを使用すると、適用されていない変更を失うことなく、 IP 変更ツールを終了してあとで再起動できます。

12. 次のいずれかを実行します。

    - 新しいネットワーク設定を保存または適用せずにすべての変更をクリアする場合は、オプション * 9 * を選択します。
    - 変更を適用し、新しいネットワーク設定をプロビジョニングする準備ができたら、オプション * 10 を選択します。プロビジョニング中に更新が適用されると、次の出力例に示すようにステータスが出力に表示されます。

      ```
      Generating new grid networking description file...

      Running provisioning...

      Updating grid network configuration on Name
      ```

13. グリッド マネージャーから新しいリカバリ パッケージをダウンロードします。

a. メンテナンス > システム > *回復パッケージ*を選択します。

b. プロビジョニングパスフレーズを入力します。

14. 外部SSHアクセスを許可している場合は、"アクセスをブロックする"サブネット リストへの追加または変更が完了したら。

StorageGRID のグリッドネットワークのサブネットリストを追加または変更します

IP 変更ツールを使用して、グリッドネットワークのサブネットを追加または変更することができます。

開始する前に

- あなたはファイルを持ってい `Passwords.txt`ます。

グリッドネットワークサブネットリストで、サブネットの追加、削除、または変更を行うことができます。変更を行うと、グリッド内のすべてのノードでのルーティングに影響します。

グリッドネットワークサブネットリストのみを変更する場合は、グリッドマネージャを使用してネットワーク設定の追加または変更を行います。グリッドネットワーク設定問題 が原因でグリッドマネージャにアクセスできない場合、またはグリッドネットワークルーティングの変更とその他のネットワーク変更を同時に実行する場合は、 IP 変更ツールを使用します。

どのノードのグリッド ネットワーク、管理ネットワーク、またはクライアント ネットワークにも、次の IPv4 アドレスを含むサブネットを使用しないでください。

- 192,168,130,101
- 192,168,130,121
- 192,168,131,101
- 192,168,131,121
- 192,168,130,102
- 192,168,130,122
- 192,168,131,102
- 192,168,131,122
- 198.51.100.2
- 198.51.100.4

たとえば、どのノードのグリッド ネットワーク、管理ネットワーク、またはクライアント ネットワークにも次のサブネット範囲を使用しないでください。

- 192.168.130.0/24 は、このサブネット範囲に IP アドレス 192.168.130.101 と 192.168.130.102 が含まれているためです。
- 192.168.131.0/24 は、このサブネット範囲に IP アドレス 192.168.131.101 と 192.168.131.102 が含まれているためです。
- 198.51.100.0/24 は、このサブネット範囲に IP アドレス 198.51.100.2 と 198.51.100.4 が含まれているためです。

手順

1. デフォルトでは外部 SSH アクセスはブロックされます。必要に応じて、"一時的にアクセスを許可する"。
2. プライマリ管理ノードにログインします。

   a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`

   b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

   c. 次のコマンドを入力してrootに切り替えます。 `su -`

   d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

   rootとしてログインすると、プロンプトがからに `#`変わります `$`。

3. 次のコマンドを入力して、IP変更ツールを起動します。 `change-ip`
4. プロンプトでプロビジョニングパスフレーズを入力します。

   メインメニューが表示されます。

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

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

Selection:
```

5. メインメニューで、グリッドネットワークのサブネットを編集するオプションを選択します（オプション * 4 * ）。

   グリッドネットワークサブネットリストに対する変更は、グリッド全体に反映されます。

6. 次のいずれかを選択します。

   - サブネットを追加するには、次のコマンドを入力します。 `add CIDR`
   - サブネットを削除するには、次のコマンドを入力します。 `del CIDR`
   - 次のコマンドを入力して、サブネットのリストを設定します。 `set CIDR`

   すべてのコマンドで、次の形式で複数のアドレスを入力できます。 `add CIDR, CIDR`

   例： `add 172.14.0.0/16, 172.15.0.0/16, 172.16.0.0/16`

「上矢印」を使用して以前に入力した値を現在の入力プロンプトに呼び出し、必要に応じて編集することで、入力に必要な量を減らすことができます。

次の入力例では、グリッドネットワークサブネットリストのサブネットを設定しています。

```
Editing: Grid Network Subnet List

Press <enter> to use the list as shown
Use up arrow to recall a previously typed value, which you can then edit
Use 'add <CIDR> [, <CIDR>]' to add subnets <CIDR> [, <CIDR>] to the list
Use 'del <CIDR> [, <CIDR>]' to delete subnets <CIDR> [, <CIDR>] from the list
Use 'set <CIDR> [, <CIDR>]' to set the list to the given list
Use q to complete the editing session early and return to the previous menu

Grid Network Subnet List
  172.16.0.0/21
  172.17.0.0/21
  172.18.0.0/21
  192.168.0.0/21

[add/del/set/quit <CIDR>, ...]: set 172.30.0.0/21, 172.31.0.0/21, 192.168.0.0/21
```

7. 準備ができたら、「 * q * 」と入力してメインメニュー画面に戻ります。変更内容は、クリアまたは適用されるまで保持されます。
8. 次のいずれかを選択します。
   - オプション * 5 * を選択すると、変更された項目のみを表示するために分離された出力に編集内容が表示されます。次の出力例に示すように、変更は緑（追加）または赤（削除）で強調表示されます。

```
================================================================================
Grid Network Subnet List (GNSL)
================================================================================
                                                        add 172.30.0.0/21
                                                        add 172.31.0.0/21
                                                        del 172.16.0.0/21
                                                        del 172.17.0.0/21
                                                        del 172.18.0.0/21
                                [       172.30.0.0/21 ]
                                [       172.31.0.0/21 ]
                                [      192.168.0.0/21 ]
Press Enter to continue
```

   - オプション * 6 * を選択すると、設定全体を表示する出力に編集内容が表示されます。変更は、緑（追加）または赤（削除）で強調表示されます。

一部のコマンドラインインターフェイスでは、追加と削除が取り消し線で示される場合があります。

9. オプション * 7 * を選択して、すべての段階的な変更を検証します。

   この検証により、重複するサブネットを使用するなど、グリッドネットワーク、管理ネットワーク、クライアントネットワークのルールが確実に実行されます。

10. 必要に応じて、オプション * 8 を選択してステージングされたすべての変更を保存し、後で戻って変更を

続行します。

このオプションを使用すると、適用されていない変更を失うことなく、 IP 変更ツールを終了してあとで再起動できます。

11. 次のいずれかを実行します。
    - 新しいネットワーク設定を保存または適用せずにすべての変更をクリアする場合は、オプション * 9 * を選択します。
    - 変更を適用し、新しいネットワーク設定をプロビジョニングする準備ができたら、オプション * 10 を選択します。プロビジョニング中に更新が適用されると、次の出力例に示すようにステータスが出力に表示されます。

```
Generating new grid networking description file...

Running provisioning...

Updating grid network configuration on Name
```

12. グリッドネットワークの変更時にオプション * 10 を選択した場合は、次のいずれかのオプションを選択します。
    - * apply * ：必要に応じて、変更をただちに適用し、各ノードを自動的に再起動します。

      外部的な変更なしで新しいネットワーク設定が古いネットワーク設定と同時に機能する場合は、 * apply * オプションを使用して、設定の変更を完全に自動化することができます。

    - * stage * ：ノードが次回再起動されるときに変更を適用します。

      新しいネットワーク構成を機能させるためにネットワーク構成を物理的または仮想的に変更する必要がある場合は、 * stage * オプションを使用して影響を受けるノードをシャットダウンし、必要な物理ネットワーク変更を行って、影響を受けるノードを再起動する必要があります。

      stage *オプションを使用する場合は、中断を最小限に抑えるために、ステージング後できるだけ早くノードを再起動してください。

    - **cancel**:この時点ではネットワークを変更しないでください。

      提案した変更がノードの再起動を必要とするかどうかが不明である場合は、ユーザへの影響を最小限に抑えるために変更を延期できます。「 * CANCEL * 」を選択すると、メインメニューに戻り、変更内容が保持されるので、後で適用できます。

    変更を適用またはステージングすると、グリッド構成の変更の結果として新しいリカバリ パッケージが生成されます。

13. エラーが原因で設定が停止した場合は、次のオプションを使用できます。
    - IP変更手順 を終了してメインメニューに戻るには、「* a *」と入力します。
    - 失敗した処理を再試行するには、「 * r * 」と入力します。
    - 次の処理に進むには、 * c * と入力します。

失敗した処理は、メインメニューからオプション * 10 * （変更の適用）を選択することで後で再試行できます。すべての処理が正常に完了するまで、 IP 変更手順 は完了しません。

- 手動での介入（ノードのリブートなど）が必要なときに、ツールでは失敗と判断された操作が実際には正常に完了したことがわかった場合は、「 * f * 」と入力してその操作を成功とマークし、次の処理に進みます。

14. グリッド マネージャーから新しいリカバリ パッケージをダウンロードします。
    a. メンテナンス > システム > *回復パッケージ*を選択します。
    b. プロビジョニングパスフレーズを入力します。

> リカバリ パッケージ ファイルには、 StorageGRIDシステムからデータを取得するために使用できる暗号化キーとパスワードが含まれているため、セキュリティで保護する必要があります。

15. 外部SSHアクセスを許可している場合は、"アクセスをブロックする"サブネット リストへの追加または変更が完了したら。

StorageGRIDグリッド内のすべてのノードの**IP**アドレスを変更します

グリッド内のすべてのノードのグリッドネットワーク IP アドレスを変更する必要がある場合は、次の特別な手順 に従う必要があります。手順 を使用してグリッドネットワークのIPをグリッド全体で変更し、個 々 のノードを変更することはできません。

開始する前に

- あなたはファイルを持ってい `Passwords.txt`ます。

グリッドを正常に起動するには、すべての変更を同時に行う必要があります。

> この 手順 環境 はグリッドネットワークのみです。この手順 を使用して管理ネットワークまたはクライアントネットワークのIPアドレスを変更することはできません。

一方のサイトでのみノードのIPアドレスとMTUを変更する場合は、手順に従います"ノードのネットワーク設定の変更"。

手順

1. DNS や NTP の変更、シングルサインオン（ SSO ）設定の変更（使用している場合）など、 IP 変更ツールを使用しない変更については、事前に計画を立てる必要があります。

> 既存手順 の NTP サーバが新しい IP アドレスでグリッドにアクセスできなくなる場合は、IP の変更を行う前に新しい NTP サーバを追加します。

> 既存手順 の DNS サーバが新しい IP アドレスでグリッドにアクセスできなくなる場合は、IP の変更を行う前に新しい DNS サーバを追加します。

StorageGRID システムで SSO が有効になっており、証明書利用者信頼が（推奨されている完全修飾ドメイン名ではなく）管理ノードの IP アドレスを使用して構成されている場合は、IP アドレスを変更した直後に、Active Directory フェデレーション サービス（AD FS）でこれらの証明書利用者信頼を更新または再構成する準備をしてください。"OIDC" または "SAML" を使用した SSO の設定については、該当するドキュメントを参照してください。

必要に応じて、新しい IP アドレス用の新しいサブネットを追加します。

2. デフォルトでは外部 SSH アクセスはブロックされます。必要に応じて、"一時的にアクセスを許可する"。
3. プライマリ管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`
   b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

   rootとしてログインすると、プロンプトがからに `#`変わります `$`。
4. 次のコマンドを入力して、IP変更ツールを起動します。 `change-ip`
5. プロンプトでプロビジョニングパスフレーズを入力します。

   メインメニューが表示されます。デフォルトでは、この `Selected nodes`フィールドはに設定されて `all`います。

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

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

Selection:
```

6. メインメニューで「 * 2 * 」を選択して、すべてのノードの IP / サブネットマスク、ゲートウェイ、 MTU 情報を編集します。
   a. 1 * を選択してグリッドネットワークを変更します。

      選択が完了すると、ノード名、グリッドネットワーク名、データタイプ（ IP / マスク、ゲートウェイ、または MTU ）がプロンプトに表示されます。 および現在の値。

      DHCP によって設定されたインターフェイスの IP アドレス、プレフィックス長、ゲートウェイ、または MTU を編集すると、インターフェイスが static に変更されます。DHCP によって設定された各インターフェイスの前に、警告が表示されます。

として設定されたインターフェイスは `fixed`編集できません。

a. 新しい値を設定するには、現在の値の形式で入力します。

b. 変更するすべてのノードを編集したら、「 * q * 」と入力してメインメニューに戻ります。

変更内容は、クリアまたは適用されるまで保持されます。

7. 次のいずれかのオプションを選択して、変更内容を確認します。

- **5**: 変更された項目のみを表示するために分離された出力の編集を表示します。変更は、次の出力例に示すように、緑（追加）または赤（削除）で強調表示されます。

```
================================================================================
Site: RTP
================================================================================
username-x Grid    IP      [    172.16.0.239/21 ]: 172.16.0.240/21
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Admin   IP      [    10.224.0.244/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.245/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.240/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.241/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.242/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.243/21 ]: 0.0.0.0/0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   MTU     [               1400 ]: 0
username-x Admin   MTU     [               1400 ]: 0
username-x Admin   MTU     [               1400 ]: 0
username-x Admin   MTU     [               1400 ]: 0
username-x Admin   MTU     [               1400 ]: 0
username-x Admin   MTU     [               1400 ]: 0
Press Enter to continue
```

- **6**: 編集内容を出力に表示し、設定全体を表示します。変更は、緑（追加）または赤（削除）で強調表示されます。

> 一部のコマンドラインインターフェイスでは、追加と削除が取り消し線で示される場合があります。正しく表示されるためには、使用するターミナルクライアントが必要な VT100 エスケープシーケンスをサポートしている必要があります。

8. オプション * 7 * を選択して、すべての変更を検証します。

この検証により、グリッドネットワークに関するルール（重複するサブネットの不使用など）に違反していないことが確認されます。

この例では、検証でエラーが返されています。

```
Validating new networking configuration... FAILED.

  DK-10-224-5-20-G1: The admin subnet 172.18.0.0/16 overlaps the 172.18.0.0/21 grid network.
  DK-10-224-5-22-S1: Duplicate Grid IP 172.16.5.18 (also in use by DK-10-224-5-21-ADM1)

You must correct these errors before you can apply any changes.
Checking for Grid Network IP address swaps... PASSED.

Press Enter to continue
```

この例では、検証に合格しています。

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

Press Enter to continue
```

9. 検証に合格したら、* 10 *を選択して新しいネットワーク構成を適用します。
10. 次にノードを再起動したときに変更を適用するには、 * stage * を選択します。

> 「 * stage * 」を選択する必要があります。手動または* stage ではなく apply *を選択してローリングリスタートを実行しないでください。グリッドは正常に起動しません。

11. 変更が完了したら、 **0** を選択して IP 変更ツールを終了します。
12. すべてのノードを同時にシャットダウンします。

> すべてのノードが同時に停止するように、グリッド全体をシャットダウンする必要があります。

13. ネットワークに対して必要な物理的または仮想的な変更を行います。
14. すべてのグリッドノードが停止していることを確認します。
15. すべてのノードの電源をオンにします。
16. グリッドが正常に起動したら、次の操作を行います。
    a. 新しいNTPサーバを追加した場合は、古いNTPサーバの値を削除します。
    b. 新しいDNSサーバを追加した場合は、古いDNSサーバの値を削除します。
17. グリッド マネージャーから新しいリカバリ パッケージをダウンロードします。
    a. メンテナンス > システム > *回復パッケージ*を選択します。
    b. プロビジョニングパスフレーズを入力します。
18. 外部SSHアクセスを許可している場合は、"アクセスをブロックする" IP アドレスの変更が完了したら。

関連情報

- "グリッドネットワークのサブネットリストに対する追加または変更"
- "グリッドノードをシャットダウンします"

既存のノードにインターフェイスを追加

StorageGRIDの**Linux**ノードに管理者またはクライアントインターフェースを追加する

管理ネットワークまたはクライアントネットワーク上のインターフェイスをインストールしたあとに Linux ノードに追加するには、次の手順を実行します。

インストール中に Linux ホストのノード構成ファイルで ADMIN_NETWORK_TARGET または CLIENT_NETWORK_TARGET を構成しなかった場合は、この手順を使用してインターフェイスを追加します。ノード構成ファイルの詳細については、以下を参照してください。"ソフトウェアベースのノードにStorageGRIDをインストールする" 。

この手順 は、ノード内ではなく、新しいネットワーク割り当てが必要なノードをホストしている Linux サーバ上で実行します。この手順 で追加されるのはノードだけです。他のネットワークパラメータを指定しようとすると、検証エラーが発生します。

アドレス情報を指定するには、 IP 変更ツールを使用する必要があります。を参照して "ノードのネットワーク設定の変更"

手順

1. ノードをホストしている Linux サーバにログインします。
2. ノード構成ファイルを編集します `/etc/storagegrid/nodes/node-name.conf`。

   他のネットワークパラメータは指定しないでください。指定しないと、検証エラーが発生します。

   a. 新しいネットワークターゲットのエントリを追加します。例：

      ```
      CLIENT_NETWORK_TARGET = bond0.3206
      ```

   b. オプション： MAC アドレスのエントリを追加します。例：

      ```
      CLIENT_NETWORK_MAC = aa:57:61:07:ea:5c
      ```

3. node validate コマンドを実行します。

   ```
   sudo storagegrid node validate node-name
   ```

4. 検証エラーをすべて解決します。
5. node reload コマンドを実行します。

   ```
   sudo storagegrid node reload node-name
   ```

StorageGRIDの**Linux**ノードにトランクまたはアクセスインターフェースを追加する

Linux ノードをインストールしたあとで、そのノードにトランクインターフェイスまたはアクセスインターフェイスを追加できます。追加したインターフェイスは、 VLAN インターフェイスのページと HA グループのページに表示されます。

開始する前に

- あなたは、"StorageGRIDのインストール手順" Linux プラットフォーム上で。
- あなたはファイルを持ってい `Passwords.txt`ます。
- そうだな "特定のアクセス権限"

> ソフトウェアのアップグレード、リカバリ手順 、または拡張手順 がアクティブなときは、ノードにインターフェイスを追加しないでください。

タスクの内容

ノードのインストール後に Linux ノードに 1 つ以上のインターフェイスを追加するには、次の手順を実行します。たとえば、管理ノードまたはゲートウェイノードにトランクインターフェイスを追加して、 VLAN インターフェイスを使用して複数のアプリケーションまたはテナントに属するトラフィックを分離できます。または、ハイアベイラビリティ（ HA ）グループで使用するアクセスインターフェイスを追加することもできます。

トランクインターフェイスを追加する場合は、 StorageGRID で VLAN インターフェイスを設定する必要があります。アクセスインターフェイスを追加する場合は、そのインターフェイスをHAグループに直接追加できます。VLANインターフェイスを設定する必要はありません。

インターフェイスを追加するときは、ノードを一時的に使用できなくなります。この手順 は一度に 1 つのノードで実行する必要があります。

手順

1. ノードをホストしている Linux サーバにログインします。
2. vim や pico などのテキストエディタを使用して、ノード構成ファイルを編集します。

   ```
   /etc/storagegrid/nodes/node-name.conf
   ```

3. ファイルにエントリを追加して名前を指定し、必要に応じて、ノードに追加する各インターフェイスの概要 を指定します。次の形式を使用します。

   ```
   INTERFACE_TARGET_nnnn=value
   ```

   _nnnn_には、追加するエントリごとに一意の番号を指定します `INTERFACE_TARGET`。

   value _ には、ベアメタルホスト上の物理インターフェイスの名前を指定します。その後、必要に応じて、カンマを追加してインターフェイスの概要 を指定します。このインターフェイスは、 VLAN インターフェイスのページと HA グループのページに表示されます。

   例：

   ```
   INTERFACE_TARGET_0001=ens256, Trunk
   ```

   > 他のネットワークパラメータは指定しないでください。指定しないと、検証エラーが発生します。

4. 次のコマンドを実行して、ノード構成ファイルに対する変更を検証します。

   ```
   sudo storagegrid node validate node-name
   ```

エラーや警告がある場合は、次の手順に進む前に対処してください。

5. 次のコマンドを実行して、ノードの設定を更新します。

```
sudo storagegrid node reload node-name
```

終了後

- 1つ以上のトランクインターフェイスを追加した場合は、に進み、"VLAN インターフェイスを設定します" 新しい親インターフェイスごとに1つ以上のVLANインターフェイスを設定します。
- アクセスインターフェイスを追加した場合は、に進み、"ハイアベイラビリティグループを設定する"新しいインターフェイスをHAグループに直接追加します。

StorageGRIDの**VMware**ノードにトランクインターフェイスまたはアクセスインターフェイスを追加する

ノードのインストールが完了したら、 VM ノードにトランクインターフェイスまたはアクセスインターフェイスを追加できます。追加したインターフェイスは、 VLAN インターフェイスのページと HA グループのページに表示されます。

開始する前に

- 以下の手順にアクセスできます"VMwareプラットフォームへのStorageGRID のインストール"。
- 管理ノードとゲートウェイノードの VMware 仮想マシンが必要です。
- グリッドネットワーク、管理ネットワーク、またはクライアントネットワークとして使用されていないネットワークサブネットを用意しておきます。
- あなたはファイルを持ってい `Passwords.txt`ます。
- そうだな "特定のアクセス権限"

> ソフトウェアのアップグレード、リカバリ手順 、または拡張手順 がアクティブなときは、ノードにインターフェイスを追加しないでください。

タスクの内容

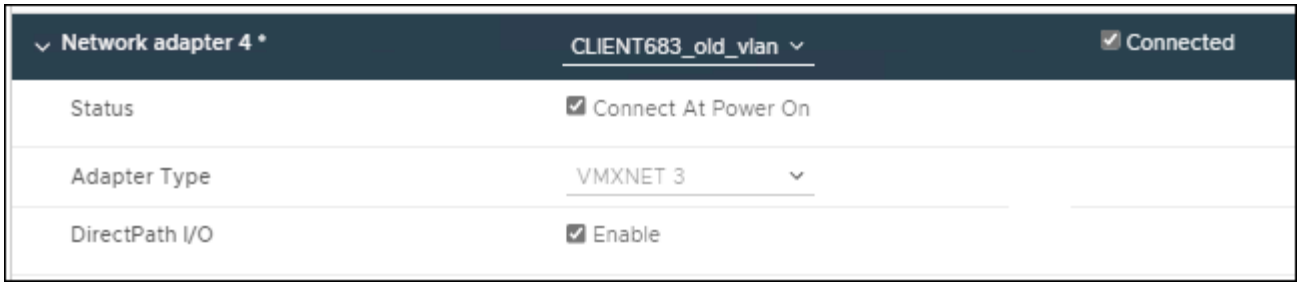
ノードのインストール後に VMware ノードに 1 つ以上のインターフェイスを追加するには、次の手順を実行します。たとえば、管理ノードまたはゲートウェイノードにトランクインターフェイスを追加して、 VLAN インターフェイスを使用して複数のアプリケーションまたはテナントに属するトラフィックを分離できます。ハイアベイラビリティ（ HA ）グループで使用するアクセスインターフェイスを追加することもできます。

トランクインターフェイスを追加する場合は、 StorageGRID で VLAN インターフェイスを設定する必要があります。アクセスインターフェイスを追加する場合は、そのインターフェイスをHAグループに直接追加できます。VLANインターフェイスを設定する必要はありません。

インターフェイスを追加するときに、ノードを一時的に使用できなくなることがあります。

手順

1. vCenter で、新しいネットワークアダプタ（ VMXNET3 タイプ）を管理ノードとゲートウェイノード VM に追加します。[接続済み]チェックボックスと[電源オン時に接続]チェックボックスをオンにします。



2. SSH を使用して管理ノードまたはゲートウェイノードにログインします。
3. を使用し `ip link show`て、新しいネットワークインターフェイスens256が検出されたことを確認します。

```
ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode
DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1400 qdisc mq state UP
mode DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:4e:5b brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN mode
DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:fa:ce brd ff:ff:ff:ff:ff:ff
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1400 qdisc mq state UP
mode DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:d6:87 brd ff:ff:ff:ff:ff:ff
5: ens256: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq master
ens256vrf state UP mode DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:ea:88 brd ff:ff:ff:ff:ff:ff
```

終了後

- 1つ以上のトランクインターフェイスを追加した場合は、に進み、"VLAN インターフェイスを設定します" 新しい親インターフェイスごとに1つ以上のVLANインターフェイスを設定します。
- アクセスインターフェイスを追加した場合は、に進み、"ハイアベイラビリティグループを設定する"新しいインターフェイスをHAグループに直接追加します。

StorageGRIDでDNSサーバーを設定する

IPアドレスではなく完全修飾ドメイン名（FQDN）ホスト名を使用できるように、DNSサーバを追加、更新、および削除できます。

外部の宛先のホスト名を指定するときに、IPアドレスの代わりに完全修飾ドメイン名（FQDN）を使用するには、使用する各DNSサーバのIPアドレスを指定します。これらのエントリは、AutoSupport 、アラートEメール、SNMP通知、プラットフォームサービスエンドポイント、クラウドストレージプール、 その他多数。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"Maintenance権限またはRoot Access権限"。
- 設定するDNSサーバのIPアドレスを確認しておきます。

タスクの内容

適切に動作するように、2つまたは3つのDNSサーバを指定します。3つ以上を指定すると、一部のプラットフォームではOSに制限があるため、3つだけが使用される可能性があります。ルーティングが制限されている環境では、個 々 のノード（通常はサイトのすべてのノード）で、最大3つのDNSサーバの異なるセットを使用できます"DNSサーバリストをカスタマイズします"。

可能であれば、各サイトがローカルにアクセスできるDNSサーバを使用して、孤立したサイトが外部の宛先のFQDNを解決できるようにします。

DNSサーバを追加します

DNSサーバを追加する手順は、次のとおりです。

手順

1. メンテナンス > ネットワーク > **DNS** サーバー を選択します。
2. DNSサーバを追加するには、*[別のサーバを追加]*を選択します。
3. [保存（ Save ）] を選択します。

DNSサーバを変更します

DNSサーバを変更する手順は、次のとおりです。

手順

1. メンテナンス > ネットワーク > **DNS** サーバー を選択します。
2. 編集するサーバ名のIPアドレスを選択し、必要な変更を行います。
3. [保存（ Save ）] を選択します。

DNSサーバを削除します

DNSサーバのIPアドレスを削除する手順は、次のとおりです。

手順

1. メンテナンス > ネットワーク > **DNS** サーバー を選択します。
2. IPアドレスの横にある削除アイコン✕を選択します。
3. [保存（ Save ）] を選択します。

単一の**StorageGRID**ノードの**DNS**構成を変更する

導入環境全体でDNSをグローバルに設定する代わりに、スクリプトを実行してDNSをグリッドノードごとに設定することができます。

通常、DNS サーバーを構成するには、グリッド マネージャーの メンテナンス > ネットワーク > **DNS** サーバ

ー オプションを使用する必要があります。異なるグリッド ノードに異なる DNS サーバーを使用する必要がある場合のみ、次のスクリプトを使用してください。

手順

1. デフォルトでは外部 SSH アクセスはブロックされます。必要に応じて、"一時的にアクセスを許可する"。
2. プライマリ管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`
   b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

      rootとしてログインすると、プロンプトがからに `#`変わります `$`。

   e. SSH エージェントに SSH 秘密鍵を追加します。入力： `ssh-add`
   f. ファイルに記載されているSSHアクセスパスワードを入力し `Passwords.txt`ます。
3. カスタムDNS設定で更新するノードにログインします。 `ssh node_IP_address`
4. DNSセットアップスクリプトを実行します。 `setup_resolv.rb.`

   スクリプトから、サポートされるコマンドの一覧が返されます。

```
Tool to modify external name servers

available commands:
  add search <domain>
               add a specified domain to search list
               e.g.> add search netapp.com
  remove search <domain>
               remove a specified domain from list
               e.g.> remove search netapp.com
  add nameserver <ip>
               add a specified IP address to the name server list
               e.g.> add nameserver 192.0.2.65
  remove nameserver <ip>
               remove a specified IP address from list
               e.g.> remove nameserver 192.0.2.65
  remove nameserver all
               remove all nameservers from list
  save         write configuration to disk and quit
  abort        quit without saving changes
  help         display this help message


Current list of name servers:
    192.0.2.64
Name servers inherited from global DNS configuration:
    192.0.2.126
    192.0.2.127
Current list of search entries:
    netapp.com

Enter command [`add search <domain>|remove search <domain>|add
nameserver <ip>`]
              [`remove nameserver <ip>|remove nameserver
all|save|abort|help`]
```

5. ネットワークにドメインネームサービスを提供するサーバのIPv4アドレスを追加します。 `add <nameserver IP_address>`
6. このコマンドを繰り返して `add nameserver`ネームサーバを追加します。
7. 他のコマンドについてはプロンプトが表示されたら、その指示に従います。
8. 変更を保存してアプリケーションを終了します。 `save`
9. サーバ上のコマンドシェルを閉じます。 `exit`
10. グリッドノードごとに、～の手順を繰り返しますノードにログインしますコマンドシェルを閉じています。

11. 他のサーバにパスワードなしでアクセスする必要がなくなった場合は、 SSH エージェントから秘密鍵を削除します。入力： `ssh-add -D`
12. 外部SSHアクセスを許可している場合は、"アクセスをブロックする" DNS 構成の変更が完了したら。

StorageGRIDでNTPサーバーを管理する

ネットワークタイムプロトコル（NTP）サーバを追加、更新、または削除して、StorageGRID システムのグリッドノード間でデータが正確に同期されるようにすることができます。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"Maintenance権限またはRoot Access権限"。
- プロビジョニングパスフレーズを用意します。
- 設定するNTPサーバのIPv4アドレスを確認しておきます。

StorageGRID でのNTPの使用方法

StorageGRID システムは、ネットワークタイムプロトコル（NTP）を使用して、グリッド内のすべてのグリッドノード間で時間を同期します。

各サイトでは、 StorageGRID システムの少なくとも 2 つのノードにプライマリ NTP ロールが割り当てられます。推奨される最低 4 つ、最大 6 つの外部時間ソース、および相互に同期します。StorageGRID システムのプライマリ NTP ノード以外のノードは、すべて NTP クライアントとして機能し、プライマリ NTP ノードと同期されます。

外部NTPサーバは、以前にプライマリNTPロールを割り当てたノードに接続します。このため、プライマリNTPロールを持つノードを少なくとも2つ指定することを推奨します。

NTPサーバのガイドライン

タイミングの問題から保護するには、次の注意事項に従ってください。

- 外部NTPサーバは、以前にプライマリNTPロールを割り当てたノードに接続します。このため、プライマリNTPロールを持つノードを少なくとも2つ指定することを推奨します。
- 各サイトの少なくとも2つのノードが、少なくとも4つの外部NTPソースにアクセスできることを確認します。NTP ソースにアクセスできるノードがサイトに 1 つしかないと、そのノードがダウンした場合にタイミングの問題が生じます。また、各サイトで 2 つのノードをプライマリ NTP ソースとして指定することにより、サイトがグリッドの他の部分から分離されても、正確なタイミングが保証されます。
- 指定する外部 NTP サーバは、 NTP プロトコルを使用している必要があります。時間のずれに伴う問題を防ぐには、 Stratum 3 以上の NTP サーバ参照を指定する必要があります。

> 運用レベルの StorageGRID インストールに外部 NTP ソースを指定する場合、Windows Server 2016 より前のバージョンの Windows では Windows 時刻 （W32Time） サービスを使用しないでください。以前のバージョンの Windows のタイム サービスは十分な精度を備えておらず、StorageGRID を含む高精度環境での使用は Microsoft によってサポートされていません。詳細については、 "高精度時間のサポート境界"を参照してください。

NTPサーバの設定

NTPサーバを追加、更新、または削除する手順は、次のとおりです。

手順

1. メンテナンス > ネットワーク > **NTP** サーバー を選択します。
2. [Servers]セクションで、必要に応じてNTPサーバエントリを追加、更新、または削除します。

   NTPサーバは少なくとも4つ含める必要があり、最大6つまで指定できます。

3. StorageGRID システムのプロビジョニングパスフレーズを入力し、*[保存]*を選択します。

   設定の更新が完了するまで、ページは無効になります。

> 新しいNTPサーバを保存した後に、すべてのNTPサーバが接続テストに失敗した場合は、続行しないでください。テクニカルサポートにお問い合わせください。

NTPサーバの問題を解決します

インストール時に指定した最初の NTP サーバの安定性や可用性に問題が生じた場合は、サーバの追加や既存のサーバの更新や削除を行って、 StorageGRID システムが使用する外部 NTP ソースのリストを更新できます。

隔離されたStorageGRIDノードのネットワーク接続を復元します

状況によっては、1つ以上のノードグループがグリッドの残りの部分にアクセスできない場合があります。たとえば、サイト全体またはグリッド全体でIPアドレスを変更すると、ノードが分離される可能性があります。

タスクの内容

ノードの分離は次のように表示されます。

- などのアラート：ノードと通信できません（アラート>*現在の*）
- 接続関連の診断（サポート > ツール > 診断）

分離されているノードがあると、次のような影響があります。

- 複数のノードが分離されていると、 Grid Manager へのサインインやアクセスができなくなる可能性があります。
- 複数のノードが分離されている場合は、Tenant Managerのダッシュボードに表示されるストレージ使用量とクォータの値が最新でない可能性があります。合計はネットワーク接続が回復すると更新されます。

分離問題 を解決するには、グリッドから分離されている各分離ノードまたはグループ内の 1 つ（プライマリ管理ノードを含まないサブネット内のすべてのノード）で、コマンドラインユーティリティを実行します。このユーティリティは、グリッド内の分離されていないノードの IP アドレスをノードに提供します。これにより、分離されているノードまたはノードのグループがグリッド全体に再びアクセスできるようになります。

ネットワークでマルチキャストドメインネームシステム（mDNS）が無効になっている場合は、分離された各ノードでコマンドラインユーティリティを実行する必要があります。

手順

この手順は、一部のサービスのみがオフラインである場合、または通信エラーが報告されている場合は適用されません。

1. ノードにアクセスして分離に関するメッセージを確認します `/var/local/log/dynip.log`。

   例：

   ```
   [2018-01-09T19:11:00.545] UpdateQueue - WARNING -- Possible isolation,
   no contact with other nodes.
   If this warning persists, manual action might be required.
   ```

   VMware コンソールを使用している場合は、ノードが分離された可能性があることを示すメッセージが含まれます。

   Linux環境では、分離メッセージがファイルに表示されます `/var/log/storagegrid/node/<nodename>.log`。

2. 分離に関するメッセージが繰り返し表示され、保持されている場合は、次のコマンドを実行します。

   `add_node_ip.py <address>`

   `<address>`は、グリッドに接続されているリモートノードのIPアドレスです。

   ```
   # /usr/sbin/add_node_ip.py  10.224.4.210

   Retrieving local host information
   Validating remote node at address 10.224.4.210
   Sending node IP hint for 10.224.4.210 to local node
   Local node found on remote node. Update complete.
   ```

3. 分離されていた各ノードについて、次の点を確認します。
   - ノードのサービスが開始されている。
   - コマンドの実行後、動的IPサービスのステータスは「Running」になります `storagegrid-status`。
   - [Nodes]ページで、ノードがグリッドの残りの部分から切断されていると表示されなくなります。

コマンドを実行しても問題が解決しない場合 `add_node_ip.py`は、解決が必要な他のネットワークの問題がある可能性があります。

ホストとミドルウェアの手順

StorageGRIDノードを新しいLinuxホストに移行する

グリッドの機能や可用性に影響を与えることなく、ホストのメンテナンスを実行するために、1つのLinuxホスト（*source host*）から別のLinuxホスト（*target host*）に1つ以上のStorageGRID ノードを移行できます。

たとえば、ノードを移行してOSのパッチ適用を実行し、リブートすることができます。

開始する前に

- 移行サポートを含めるようにStorageGRID の展開を計画しました。見る"ノードコンテナの移行要件" 。
- ターゲットホストはStorageGRID で使用する準備が完了しています。
- 共有ストレージは、すべてのノード単位のストレージボリュームに使用されます
- ネットワークインターフェイスの名前は、ホスト間で一貫しています。

> ⓘ 本番環境では、1つのホストで複数のストレージノードを実行しないでください。各ストレージノードに専用のホストを使用すると、分離された障害ドメインが提供されます。
>
> 管理ノードやゲートウェイノードなど、他のタイプのノードは、同じホストに導入することができます。ただし、同じタイプのノードが複数ある場合（たとえば2つのゲートウェイノード）は、すべてのインスタンスを同じホストにインストールしないでください。

ソースホストからノードをエクスポートします

最初の手順として、グリッドノードをシャットダウンし、ソースLinuxホストからエクスポートします。

次のコマンドを_source host_で実行します。

手順

1. ソースホストで現在実行されているすべてのノードのステータスを取得します。

   ```
   sudo storagegrid node status all
   ```

   出力例：

   ```
   Name Config-State Run-State
   DC1-ADM1 Configured Running
   DC1-ARC1 Configured Running
   DC1-GW1 Configured Running
   DC1-S1 Configured Running
   DC1-S2 Configured Running
   DC1-S3 Configured Running
   ```

2. 移行するノードの名前を特定し、Run-StateがRunningの場合は停止します。

```
sudo storagegrid node stop DC1-S3
```

出力例：

```
Stopping node DC1-S3
Waiting up to 630 seconds for node shutdown
```

3. ソースホストからノードをエクスポートします。

```
sudo storagegrid node export DC1-S3
```

出力例：

```
Finished exporting node DC1-S3 to /dev/mapper/sgws-dc1-s3-var-local.
Use 'storagegrid node import /dev/mapper/sgws-dc1-s3-var-local' if you
want to import it again.
```

4. 出力に表示されたコマンドを書き留めます `import`。

次の手順で、このコマンドをターゲットホストで実行します。

ターゲットホストにノードをインポートします

ソースホストからノードをエクスポートしたら、ターゲットホストにノードをインポートして検証します。検証では、ソースホストと同じブロックストレージおよびネットワークインターフェイスデバイスにノードがアクセスできるかどうかを確認します。

次のコマンドを_target host_で実行します。

手順

1. ターゲットホストにノードをインポートします。

```
sudo storagegrid node import /dev/mapper/sgws-dc1-s3-var-local
```

出力例：

```
Finished importing node DC1-S3 from /dev/mapper/sgws-dc1-s3-var-local.
You should run 'storagegrid node validate DC1-S3'
```

2. 新しいホストでノード構成を検証します。

```
sudo storagegrid node validate DC1-S3
```

出力例：

```
Confirming existence of node DC1-S3... PASSED
Checking configuration file /etc/storagegrid/nodes/DC1-S3.conf for node
DC1-S3... PASSED
Checking for duplication of unique values... PASSED
```

3. 検証エラーが発生した場合は、移行したノードを開始する前に対処してください。

   トラブルシューティング情報については、 StorageGRID"インストール手順" Linux オペレーティング システム用。

移行済みノードを起動します

移行済みノードの検証が完了したら、_target host_でコマンドを実行してノードを起動します。

手順

1. 新しいホストでノードを開始します。

   ```
   sudo storagegrid node start DC1-S3
   ```

2. Grid Managerにサインインし、ノードのステータスが緑でアラートがないことを確認します。

   ノードのステータスが緑色の場合、移行済みノードは完全に再起動してグリッドに再参加しています。ステータスが緑色でない場合は、複数のノードがアウトオブサービス状態にならないように、追加のノードを移行しないでください。

3. Grid Manager にアクセスできない場合は、 10 分待ってから次のコマンドを実行します。

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

   移行済みノードのRun-StateがRunningになっていることを確認します。

StorageGRIDでVMware仮想マシンを自動再起動するように構成します

VMware vSphere ハイパーバイザーの再起動後に仮想マシンが再起動しない場合は、仮想マシンが自動で再起動するように設定する必要があります。

グリッドノードのリカバリ中または別のメンテナンス手順 の実行中に仮想マシンが再起動しない場合は、この手順 を実行する必要があります。

手順

1. VMware vSphere Client ツリーで、起動されていない仮想マシンを選択します。
2. 仮想マシンを右クリックし、 * 電源オン * を選択します。
3. 仮想マシンが自動的に再起動されるように、 VMware vSphere ハイパーバイザーを設定します。

ノードをリカバリまたは交換

StorageGRIDノードリカバリに関する警告と考慮事項

グリッドノードに障害が発生した場合は、できるだけ早くリカバリする必要があります。ノードのリカバリを開始する前に、ノードのリカバリに関する警告と考慮事項をすべて確認しておく必要があります。

> StorageGRID は、複数のノードが相互に連携する分散システムです。グリッドノードのリストアにディスクSnapshotを使用しないでください。各タイプのノードのリカバリとメンテナンスの手順を参照してください。

> StorageGRIDサイト全体に障害が発生した場合は、テクニカル サポートにお問い合わせください。テクニカル サポートはお客様と協力し、回復されるデータの量を最大化し、ビジネス目標を満たすサイト回復計画を策定し、実行します。。 "テクニカルサポートによるサイトのリカバリ方法" 。

障害グリッドノードをできるだけ早くリカバリする理由には、次のものがあります。

- グリッドノードで障害が発生すると、システムデータとオブジェクトデータの冗長性が低下して、別のノードで障害が発生した場合にデータが永続的に失われるリスクが高まります。
- グリッドノードで障害が発生すると、日常業務の効率に影響する可能性があります。
- グリッドノードで障害が発生すると、システム処理の監視を減らすことができます。
- 厳格な ILM ルールが適用されている場合、障害が発生したグリッドノードで原因 500 Internal Server エラーが発生する可能性があります。
- グリッドノードがすぐにリカバリされないと、リカバリ時間が長くなる可能性があります。たとえば、リカバリが完了する前にキューをクリアする必要が生じる場合があります。

リカバリするグリッドノードのタイプに応じて、必ずリカバリ手順 に従ってください。リカバリ手順は、プライマリまたは非プライマリ管理ノード、ゲートウェイノード、アプライアンスノード、およびストレージノードで異なります。

グリッドノードをリカバリするための前提条件

グリッドノードをリカバリする際の前提条件は次のとおりです。

- 障害が発生した物理または仮想ハードウェアの交換と設定が完了している。
- 交換用アプライアンスのStorageGRIDアプライアンスインストーラのバージョンは、StorageGRIDシステムのソフトウェアバージョンと同じです（を参照） "StorageGRID アプライアンスインストーラのバージョンを確認してアップグレードします"。
- プライマリ管理ノード以外のグリッドノードを復旧する場合、復旧対象のグリッドノードと復旧手順を管理する管理ノードとの間に接続が確立されている必要があります。
- アプライアンス ストレージ ノードをリカバリする場合は、アプライアンスのインストール時に、元のアプライアンスと同じストレージ タイプ (結合、メタデータのみ、またはデータのみ) を指定する必要があります。異なるストレージ タイプを指定した場合、リカバリは失敗し、正しいストレージ タイプを指定

してアプライアンスを再インストールする必要があります。

複数のグリッドノードをホストしているサーバで障害が発生した場合のノードリカバリの順序

複数のグリッドノードをホストしているサーバーが故障した場合、ノードは任意の順序で復旧できます。ただし、障害が発生したサーバーがプライマリ管理ノードをホストしており、プライマリ以外の管理ノードが存在しない場合は、まずプライマリ管理ノードを復旧する必要があります。

リカバリしたノードの **IP** アドレス

現在他のノードに割り当てられているIPアドレスを使用してノードをリカバリしないでください。新しいノードを導入するときは、障害が発生したノードの現在の IP アドレスまたは未使用の IP アドレスを使用します。

新しい IP アドレスを使用して新しいノードを導入し、そのノードをリカバリする場合は、リカバリしたノードでも新しい IP アドレスが使用されます。元の IP アドレスに戻す場合は、リカバリ完了後に IP 変更ツールを使用します。

StorageGRIDグリッドノードのリカバリに必要な資料を収集する

メンテナンス手順を実行する前に、障害グリッドノードのリカバリに必要な情報、ファイル、機器などが揃っていることを確認する必要があります。

項目	脚注
StorageGRID インストールアーカイブ	グリッドノードのリカバリが必要な場合は、プラットフォームに応じてを実行する必要がありStorageGRID インストールファイルをダウンロードしますます。 *注：*ストレージノードで障害ストレージボリュームをリカバリする場合は、ファイルをダウンロードする必要はありません。
サービスラップトップ	サービスラップトップには次のものが必要です。 • ネットワークポート • SSH クライアント（ PuTTY など） • "サポートされている Web ブラウザ"

項目	脚注
回復パッケージ `.zip`ファイル	最新のリカバリパッケージのコピーを入手する `.zip`ファイル：`sgws-recovery-package-*id-revision*.zip` の内容は `.zip`システムが変更されるたびにファイルが更新されます。このような変更を行った後は、最新バージョンのリカバリ パッケージを安全な場所に保存するように指示されます。グリッド障害から回復するには、最新のコピーを使用します。 任意の管理ノードにログインしたら、グリッド マネージャーを使用してリカバリ パッケージをダウンロードします。 メンテナンス > システム > *回復パッケージ*を選択します。 グリッド マネージャーにアクセスできない場合は、ADC サービスを含む一部のストレージ ノードに、暗号化されたリカバリ パッケージのコピーが保存されています。各ストレージ ノードで、リカバリ パッケージの次の場所を調べます。 `/var/local/install/sgws-recovery-package-*grid-id-revision*.zip.gpg`最も高いリビジョン番号のリカバリ パッケージを使用します。
`Passwords.txt`ファイル	コマンド ラインでグリッド ノードにアクセスするために必要なパスワードが含まれます。リカバリパッケージに含まれています。
プロビジョニングパスフレーズ	このパスフレーズは、 StorageGRID システムが最初にインストールされるときに作成されて文書化されます。プロビジョニングパスフレーズがファイルに含まれていません `Passwords.txt`。
ご使用のプラットフォームの最新ドキュメント	ドキュメントについては、プラットフォームのベンダーの Web サイトを参照してください。 現在サポートされているプラットフォームのバージョンについては、を参照してください "NetApp Interoperability Matrix Tool"。

StorageGRID インストールファイルをダウンロードして展開します

ソフトウェアをダウンロードし、ファイルを展開し"ストレージノード上の障害ストレージボリュームのリカバリ"ます。

グリッドで現在実行されているバージョンの StorageGRID を使用する必要があります。

手順

1. 現在インストールされているソフトウェアのバージョンを確認します。Grid Manager の上部からヘルプアイコンを選択し、 * バージョン情報 * を選択します。
2. に進みます "ネットアップの StorageGRID ダウンロードページ"。
3. グリッドで現在実行されている StorageGRID のバージョンを選択します。

   StorageGRIDソフトウェアのバージョンの形式は次のとおりです。 `11.x.y`

4. ネットアップアカウントのユーザ名とパスワードを使用してサインインします。
5. [End User License Agreement]を読み、チェックボックスをオンにして、*[Accept & Continue]*を選択します。
6. ダウンロードページの* Install StorageGRID *列で、使用しているプラットフォームに対応するファイルまたは `.zip`ファイルを選択し `.tgz`ます。

   インストールアーカイブファイルに表示されるバージョンは、現在インストールされているソフトウェアのバージョンと一致している必要があります。

   Windowsを実行している場合は、ファイルを使用し `.zip`ます。

プラットフォーム	インストールアーカイブ
RHEL	`StorageGRID-Webscale-version-RPM-uniqueID.zip` `StorageGRID-Webscale-version-RPM-uniqueID.tgz`
Ubuntu 、 Debian 、またはアプライアンス	`StorageGRID-Webscale-version-DEB-uniqueID.zip` `StorageGRID-Webscale-version-DEB-uniqueID.tgz`
VMware	`StorageGRID-Webscale-version-VMware-uniqueID.zip` `StorageGRID-Webscale-version-VMware-uniqueID.tgz`

7. アーカイブファイルをダウンロードして展開します。
8. プラットフォームと回復する必要があるグリッド ノードに基づいて、プラットフォームに適切なセクションに進み、必要なファイルを選択します。

   各プラットフォームの手順に記載されているパスは、アーカイブファイルによってインストールされた最上位ディレクトリに対する相対パスです。

9. 回復中の場合"ソフトウェアベースのノード"適切なファイルを選択します。

RHEL

パスとファイル名	製品説明
	StorageGRID ダウンロードファイルに含まれているすべてのファイルについて説明するテキストファイル。
	製品サポートのない無償ライセンス。
	RHELホストにStorageGRIDノードイメージをインストールするためのRPMパッケージ。
	RHELホストにStorageGRIDホストサービスをインストールするためのRPMパッケージ。
導入スクリプトツール	製品説明
	StorageGRID システムの設定を自動化するための Python スクリプト。
	StorageGRID アプライアンスの設定を自動化するための Python スクリプト。
	スクリプトで使用する構成ファイルの例 `configure-storagegrid.py`。
	シングルサインオンが有効な場合にグリッド管理 API にサインインするために使用できる Python スクリプトの例。このスクリプトは、Pingフェデレーション統合にも使用できます。
	スクリプトで使用する空の構成ファイル `configure-storagegrid.py`。
	StorageGRIDコンテナ導入用のRHELホストを設定するためのサンプルのAnsibleのロールとプレイブック。必要に応じて、ロールまたはプレイブックをカスタマイズできます。
	Active DirectoryまたはPingフェデレーションを使用してシングルサインオン（SSO）が有効になっている場合にグリッド管理APIにサインインするために使用できるPythonスクリプトの例。

パスとファイル名	製品説明
	関連するPythonスクリプトによって呼び出され、AzureとのSSO対話を実行するヘルパースクリプト `storagegrid-ssoauth-azure.py`。
	StorageGRID の API スキーマ 注：アップグレードを実行する前に、これらのスキーマを使用して、アップグレード互換性テスト用の非本番環境のStorageGRID 環境がない場合、StorageGRID 管理APIを使用するように記述したコードが新しいStorageGRID リリースと互換性があることを確認できます。

Ubuntu または **Debian**

パスとファイル名	製品説明
	StorageGRID ダウンロードファイルに含まれているすべてのファイルについて説明するテキストファイル。
	テスト環境やコンセプトの実証環境に使用できる、非本番環境のNetAppライセンスファイル。
	Ubuntu ホストまたは Debian ホストに StorageGRID ノードイメージをインストールするための DEB パッケージ。
	ファイルのMD5チェックサム `/debs/storagegrid-webscale-images-version-SHA.deb`。
	Ubuntu ホストまたは Debian ホストに StorageGRID ホストサービスをインストールするための DEB パッケージ。
導入スクリプトツール	製品説明
	StorageGRID システムの設定を自動化するための Python スクリプト。
	StorageGRID アプライアンスの設定を自動化するための Python スクリプト。

パスとファイル名	製品説明
	シングルサインオンが有効な場合にグリッド管理 API にサインインするために使用できる Python スクリプトの例。このスクリプトは、Pingフェデレーション統合にも使用できます。
	スクリプトで使用する構成ファイルの例 `configure-storagegrid.py`。
	スクリプトで使用する空の構成ファイル `configure-storagegrid.py`。
	StorageGRID コンテナ導入用の Ubuntu ホストまたは Debian ホストを設定するためのサンプルの Ansible のロールとプレイブック。必要に応じて、ロールまたはプレイブックをカスタマイズできます。
	Active DirectoryまたはPingフェデレーションを使用してシングルサインオン（SSO）が有効になっている場合にグリッド管理APIにサインインするために使用できるPythonスクリプトの例。
	関連するPythonスクリプトによって呼び出され、AzureとのSSO対話を実行するヘルパースクリプト `storagegrid-ssoauth-azure.py`。
	StorageGRID の API スキーマ 注：アップグレードを実行する前に、これらのスキーマを使用して、アップグレード互換性テスト用の非本番環境のStorageGRID 環境がない場合、StorageGRID 管理APIを使用するように記述したコードが新しいStorageGRID リリースと互換性があることを確認できます。

VMware

パスとファイル名	製品説明
	StorageGRID ダウンロードファイルに含まれているすべてのファイルについて説明するテキストファイル。
	製品サポートのない無償ライセンス。

パスとファイル名	製品説明
	グリッドノード仮想マシンを作成するためのテンプレートとして使用される仮想マシンディスクファイル。
	(`.mf`プライマリ管理ノードを導入するためのOpen Virtualization Formatテンプレートファイル）(`.ovf`とマニフェストファイル
	テンプレートファイル(`.ovf`）とマニフェストファイル(`.mf`）。非プライマリ管理ノードを導入するためのものです。
	テンプレートファイル(`.ovf`）とマニフェストファイル(`.mf`）を使用してゲートウェイノードを導入します。
	(`.mf`仮想マシンベースのストレージノードを導入するためのテンプレートファイル(`.ovf`とマニフェストファイル）
導入スクリプトツール	製品説明
	仮想グリッドノードの導入を自動化するためのBash シェルスクリプト。
	スクリプトで使用する構成ファイルの例`deploy-vsphere-ovftool.sh`。
	StorageGRID システムの設定を自動化するための Python スクリプト。
	StorageGRID アプライアンスの設定を自動化するための Python スクリプト。
	シングルサインオン（SSO）が有効な場合にグリッド管理APIにサインインするために使用できるPythonスクリプトの例。このスクリプトは、Pingフェデレーション統合にも使用できます。
	スクリプトで使用する構成ファイルの例`configure-storagegrid.py`。
	スクリプトで使用する空の構成ファイル`configure-storagegrid.py`。

パスとファイル名	製品説明
	Active DirectoryまたはPingフェデレーションを使用してシングルサインオン（SSO）が有効になっている場合にグリッド管理APIにサインインするために使用できるPythonスクリプトの例。
	関連するPythonスクリプトによって呼び出され、AzureとのSSO対話を実行するヘルパースクリプト `storagegrid-ssoauth-azure.py`。
	StorageGRID の API スキーマ 注：アップグレードを実行する前に、これらのスキーマを使用して、アップグレード互換性テスト用の非本番環境のStorageGRID 環境がない場合、StorageGRID 管理APIを使用するように記述したコードが新しいStorageGRID リリースと互換性があることを確認できます。

10. StorageGRID アプライアンスベースのシステムをリカバリする場合は、該当するファイルを選択してください。

アプライアンスのインストールでは、ネットワーク トラフィックを回避する必要がある場合にのみこれらのファイルが必要です。アプライアンスは、リカバリ手順を実行する管理ノードから必要なファイルをダウンロードできます。

パスとファイル名	製品説明
	アプライアンスに StorageGRID ノードイメージをインストールするための DEB パッケージ。
	ファイルのMD5チェックサム `/debs/storagegridwebscale-images-version-SHA.deb`。

StorageGRIDノード復旧手順を選択

障害が発生したノードの種類に応じて、適切な復旧手順を選択してください。

Grid ノード	**Recovery** 手順 の略
ストレージノード	ストレージノードの復旧手順は、障害の種類によって異なります。 "ストレージノードの障害からリカバリします"

Grid ノード	Recovery 手順 の略
管理ノード	管理ノードの手順 は、プライマリ管理ノードと非プライマリ管理ノードのどちらをリカバリする必要があるかによって異なります。 "管理ノードの障害からリカバリ"
ゲートウェイノード	"ゲートウェイノードの障害からリカバリします"
アーカイブノード	"アーカイブノードの障害からのリカバリ（StorageGRID 11.8ドキュメントサイト）"

複数のグリッドノードをホストしているサーバーが故障した場合、ノードは任意の順序で復旧できます。ただし、障害が発生したサーバーがプライマリ管理ノードをホストしており、プライマリ以外の管理ノードが存在しない場合は、まずプライマリ管理ノードを復旧する必要があります。プライマリ管理ノードを最初に復旧することで、他のノードの復旧がプライマリ管理ノードへの接続を試みる際に停止するのを防ぐことができます。プライマリ以外の管理ノードが利用可能な場合は、それを使用して他のノードを復旧することもできます。これにより、プライマリ管理ノードに接続することなく復旧処理を進めることができます。

ストレージノードの障害からリカバリします

StorageGRIDストレージノードの障害から回復する

障害ストレージノードをリカバリする手順 は、障害のタイプおよび障害が発生したストレージノードのタイプによって異なります。

次の表を参照して、障害が発生したストレージノードのリカバリ手順 を選択してください。

問題	アクション	脚注
複数のストレージノードで障害が発生した。	テクニカルサポートにお問い合わせください。	複数のストレージノードが故障した場合、データ損失につながる可能性のある Cassandra データベースの不整合を防ぐため、技術サポートによる復旧支援が必要です。サイト復旧手順が必要になる場合があります。 テクニカルサポートは、2つ目のストレージノードの復旧を開始しても安全な時期を判断できます。 注：1つのサイトでADCサービスを含むストレージノードが複数障害を起こした場合、そのサイトに対する保留中のプラットフォームサービスリクエストはすべて失われます。
サイトの複数のストレージノードで障害が発生したか、サイト全体で障害が発生した。	テクニカルサポートにお問い合わせください。サイトリカバリ手順の実行が必要になる場合があります。	テクニカルサポートは、お客様の状況を評価し、リカバリプランを作成します。を参照して "テクニカルサポートによるサイトのリカバリ方法"
アプライアンスストレージノードで障害が発生した。	"アプライアンスストレージノードをリカバリします"	アプライアンスストレージノードのリカバリ手順 は、すべての障害で同じです。
ストレージボリュームで障害が発生したが、システムドライブには損傷がない	"システムドライブに損傷がない場合は、ストレージボリューム障害からリカバリします"	この手順 はソフトウェアベースのストレージノードに使用されます。
システムドライブで障害が発生した。	"システムドライブ障害からリカバリします"	ノード交換用手順 は、導入プラットフォーム、およびストレージボリュームに障害が発生しているかどうかによって異なります。

一部の StorageGRID リカバリ手順では、 Reaper を使用して Cassandra の修復を処理します。関連サービスまたは必要なサービスが開始されるとすぐに修理が自動的に行われます。スクリプトの出力に「reaper」または「cassandra repair」と記載されていることがあります。修復が失敗したことを示すエラーメッセージが表示された場合は、エラーメッセージに示されているコマンドを実行します。

アプライアンスストレージノードをリカバリします

StorageGRIDアプライアンスストレージノードのリカバリに関する警告

障害が発生した StorageGRID アプライアンスストレージノードのリカバリ用手順 は、システムドライブの損失からリカバリする場合も、ストレージボリュームのみの損失からリカバリする場合も同じです。

複数のストレージ ノードに障害が発生した場合 (またはオフラインの場合) は、テクニカル サポートにお問い合わせください。次の回復手順は実行しないでください。データが失われる可能性があります。詳細については、 "テクニカルサポートによるサイトのリカバリ方法" 。

レプリケートコピーを 1 つだけ保存するように ILM ルールを設定している場合に、そのコピーがあるストレージボリュームで障害が発生すると、オブジェクトをリカバリできません。

コントローラの交換やSANtricity OSの再インストールなど、ハードウェアのメンテナンス手順については、を参照してください "ストレージアプライアンスのメンテナンス手順"。

StorageGRIDアプライアンスストレージノードの再インストールの準備

アプライアンスストレージノードをリカバリする場合は、最初に StorageGRID ソフトウェアを再インストールするアプライアンスを準備する必要があります。

手順

1. 障害が発生したストレージノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
   b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

   rootとしてログインすると、プロンプトがからに `#`変わります `$`。
2. StorageGRIDソフトウェアをインストールするためのアプライアンスストレージノードを準備します。 `sgareinstall`
3. 続行するかどうかを確認するメッセージが表示されたら、 `y`

   アプライアンスがリブートされ、 SSH セッションが終了します。通常は 5 分程度で StorageGRID アプライアンスインストーラが使用可能になりますが、場合によっては最大で 30 分待つ必要があります。

   電源を再投入したり、アプライアンスをリセットしたりして、リブートを高速化しようとしないでください。BIOS、BMC、またはその他のファームウェアの自動アップグレードを中断することがあります。

   StorageGRID アプライアンスストレージノードがリセットされ、ストレージノード上のデータにアクセスできなくなります。元のインストールプロセスで設定した IP アドレスはそのまま使用する必要がありますが、手順 の完了時に確認しておくことを推奨します。

   コマンドの実行後、 `sgareinstall`StorageGRIDでプロビジョニングされたアカウント、パスワード、およ

びSSHキーがすべて削除され、新しいホストキーが生成されます。

StorageGRID アプライアンスのインストールを開始します

StorageGRID をアプライアンスストレージノードにインストールするには、アプライアンスに含まれている StorageGRID アプライアンスインストーラを使用します。

開始する前に

- アプライアンスをラックに設置し、ネットワークに接続し、電源を投入しておきます。
- StorageGRID アプライアンスインストーラを使用してアプライアンスのネットワークリンクと IP アドレスを設定しておきます。
- 以下のいずれかの管理ノードの IP アドレスを把握しています。
  - StorageGRID グリッドのプライマリ管理ノード
  - プライマリ以外の管理ノード（利用可能な場合）
- StorageGRID アプライアンスインストーラの IP 設定ページに表示されるすべてのグリッドネットワークサブネットが、プライマリ管理ノードのグリッドネットワークサブネットリストで定義されている。
- これらの必要な準備作業を完了しておくには、ストレージアプライアンスのインストール手順に従ってください。を参照してください "ハードウェア設置のクイックスタート"
- を使用している"サポートされている Web ブラウザ"。
- アプライアンスのコンピューティングコントローラに割り当てられている IP アドレスのいずれかを確認しておきます。管理ネットワーク（コントローラの管理ポート 1 ）、グリッドネットワーク、またはクライアントネットワークの IP アドレスを使用できます。

タスクの内容

StorageGRID をアプライアンスストレージノードにインストールするには、次の手順を実行します。

- プライマリ管理ノードのIPアドレスを指定します。プライマリ管理ノードが利用できない場合は、利用可能であれば、プライマリ以外の管理ノードのIPアドレスを指定します。また、ノードのホスト名（システム名）を確認します。
- インストールを開始し、ボリュームの設定とソフトウェアのインストールが行われている間待機します。

> アプライアンス ストレージ ノードを回復する場合は、元のアプライアンスと同じストレージ タイプ (結合、メタデータのみ、またはデータのみ) で再インストールします。異なるストレージ タイプを指定した場合、リカバリは失敗し、正しいストレージ タイプを指定してアプライアンスを再インストールする必要があります。

- プロセスの途中でインストールが一時停止します。インストールを再開するには、 Grid Manager にサインインして、保留状態のストレージノードを障害ノードの代わりとして設定する必要があります。
- ノードを設定すると、アプライアンスのインストールプロセスが完了してアプライアンスがリブートされます。

手順

1. ブラウザを開き、コンピューティングコントローラの IP アドレスのいずれかを入力します。

   ```
   https://Controller_IP:8443
   ```

StorageGRID アプライアンスインストーラのホームページが表示されます。

2. プライマリ管理ノードの接続セクションで、プライマリ管理ノードの IP アドレスを指定する必要があるかどうかを確認します。

   プライマリ管理ノードまたは ADMIN_IP が設定された少なくとも 1 つのグリッドノードが同じサブネットにある場合は、 StorageGRID アプライアンスインストーラがこの IP アドレスを自動的に検出します。

3. この IP アドレスが表示されない場合や変更する必要がある場合は、アドレスを指定します。

オプション	手順
IP を手動で入力します	a. [管理ノードの検出を有効にする]*チェックボックスをオフにします。 b. IP アドレスを手動で入力します。 注: インストールの場合、ノードのインストールに使用する管理ノードの IP アドレスを手動で入力します。リカバリの場合、プライマリ管理ノードの IP が使用可能な場合はそれを使用し、そうでない場合は非プライマリ管理ノードの IP を使用します。 a. [保存（ Save ）] を選択します。 b. 新しいIPアドレスの接続状態が「READY」になるまで待ちます。
接続されたすべてのプライマリ管理ノードの自動検出	a. [管理ノードの検出を有効にする]*チェックボックスを選択します。 b. 検出された IP アドレスのリストから、このアプライアンス ストレージ ノードがデプロイされるグリッドの管理ノードを選択します。 注: リカバリの場合、プライマリ管理ノードの IP が使用可能な場合はそれを使用し、そうでない場合は非プライマリ管理ノードの IP を使用します。 a. [保存（ Save ）] を選択します。 b. 新しいIPアドレスの接続状態が「READY」になるまで待ちます。

4. 「ノード名」フィールドに、復旧対象のノードで使用されていたホスト名（システム名）と同じものを入力し、「保存」を選択します。

5. 「インストール」セクションで、現在の状態が「 `node name` をプライマリ管理ノード `admin_ip` を持つグリッドにインストールする準備ができています」であることと、*インストールの開始*ボタンが有効になっていることを確認します。

   [Start Installation* （インストールの開始）] ボタンが有効になっていない場合は、ネットワーク設定またはポート設定の変更が必要になることがあります。手順については、アプライアンスのメンテナンス手順を参照してください。

6. StorageGRID アプライアンスインストーラーのホームページで、「インストールの開始」を選択します。

現在の状態が「インストール中です」に変わり、モニターのインストールページが表示されます。

> モニターのインストールページに手動でアクセスする必要がある場合は、メニューバーから「モニターのインストール」を選択してください。参照してください "アプライアンスの設置を監視する"。

StorageGRID アプライアンスの設置を監視する

StorageGRID アプライアンスインストーラでは、インストールが完了するまでステータスが提供されます。ソフトウェアのインストールが完了すると、アプライアンスがリブートされます。

手順

1. インストールの進行状況を監視するには、メニューバーから*Monitor installation*を選択してください。

   モニターのインストールページには、インストールの進行状況が表示されます。

   青色のステータスバーは、現在進行中のタスクを示します。緑のステータスバーは、正常に完了したタスクを示します。

   > インストーラは、以前のインストールで完了したタスクが再実行されないようにします。インストールを再実行している場合、再実行する必要のないタスクはすべて緑色のステータスバーと「スキップ済み」のステータスで表示されます。

2. インストールの最初の 2 つのステージの進行状況を確認します。
   - *1.ストレージの構成 *

     インストーラがストレージコントローラに接続し、既存の設定があれば消去し、SANtricity OSと通信してボリュームを設定し、ホストを設定します。

   - *2.OS * をインストールします

     インストーラが StorageGRID のベースとなるオペレーティングシステムイメージをアプライアンスにコピーします。

3. インストールの進行状況の監視を続けて、組み込みのコンソールに「 Install StorageGRID * 」ステージが一時停止し、グリッドマネージャを使用して管理ノード上でこのノードを承認するように求めるメッセージが表示されるまで待ちます。
4. にアクセスします。

リカバリの開始を選択して**StorageGRID**アプライアンスストレージノードを構成します

障害が発生したノードの代わりとしてアプライアンスストレージノードを設定するには、 Grid Manager で [Start Recovery] を選択する必要があります。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。

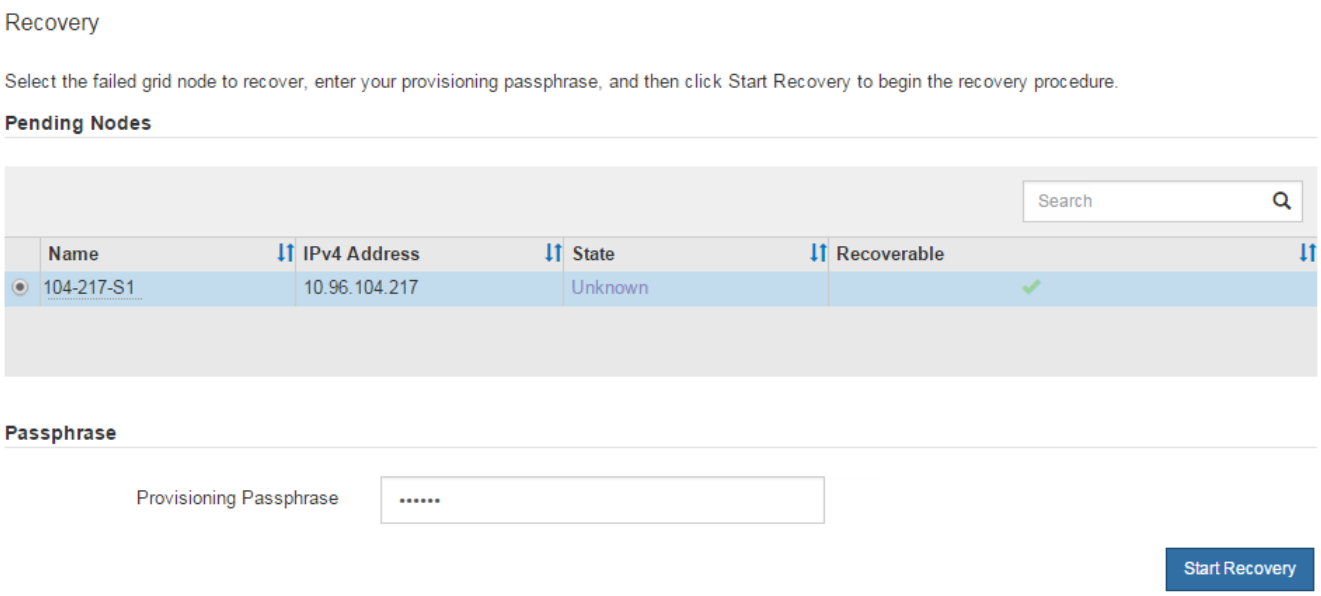
- あなたはを持っています"Maintenance権限またはRoot Access権限"。
- プロビジョニングパスフレーズを用意します。
- リカバリ用アプライアンスストレージノードを導入しておきます。
- イレイジャーコーディングデータの修復ジョブの開始日を確認しておきます。

手順

1. グリッドマネージャから、メンテナンス > タスク > *ノード復旧*を選択します。
2. リカバリするグリッドノードを Pending Nodes リストで選択します。

   ノードに障害が発生するとリストに表示されますが、ノードを再インストールしてリカバリの準備ができるまでは選択できません。

3. **Provisioning passphrase** を入力してください。
4. 「リカバリを開始」を選択します。



5. リカバリ中のグリッドノードテーブルで、リカバリの進行状況を監視します。
   - グリッドノードが「手動ステップ待ち」段階に達した場合は、"アプライアンスのストレージボリュームを手動で再マウントおよび再フォーマットする"。
   - 「手動の手順を待っています」というメッセージが表示されない場合は、ストレージボリュームが自動的に再マウントおよび再フォーマットされたことを意味し、"オブジェクトデータをボリュームに復元する"ことができます。

> 復旧処理のどの段階でも、*リセット*を選択して新しい復旧を開始できます。手順をリセットするとノードが不確定な状態になることを示すダイアログボックスが表示されます。
>
> 手順をリセットしたあとにリカバリを再試行する場合は、ノードでを実行して、アプライアンスノードをインストール前の状態にリストアする必要があります `sgareinstall`。

自動手順による保存済みストレージボリュームの再マウントおよび障害が発生したストレージボリュームの再フォーマットが失敗した場合は、これらの操作を完了するために2つのスクリプトを手動で実行する必要があります。最初のスクリプトは、StorageGRIDストレージボリュームとして適切にフォーマットされたボリュームを再マウントします。2番目のスクリプトは、マウントされていないボリュームを再フォーマットし、必要に応じて Cassandra データベースを再構築して、サービスを開始します。

ストレージノードの復旧中に、Grid Managerに「Waiting for manual steps」というメッセージが表示された場合は、次の手順に従ってストレージボリュームを再マウントおよび再フォーマットしてください。このメッセージが表示されない場合は、再マウントおよび再フォーマット操作は自動的に完了しているため、この手順をスキップして"オブジェクトデータを復元する"に進むことができます。

開始する前に

- 障害が発生したストレージボリュームのうち、必要と判断した場合はハードウェアを交換しておく必要があります。

  スクリプトを実行 `sn-remount-volumes`すると、障害ストレージボリュームを追加で特定できる場合があります。

- ストレージ ノードの廃止が進行中でないことを確認したか、ノードの廃止手順を一時停止しました。 (グリッド マネージャーで、メンテナンス > タスク > 廃止 を選択します。)
- 拡張が進行中ではないことを確認しました。 (グリッド マネージャーで、メンテナンス > タスク > 拡張 を選択します。)

> 複数のストレージ ノードがオフラインの場合は、テクニカル サポートにお問い合わせください。実行しないでください `sn-recovery-postinstall.sh`スクリプト。

タスクの内容

この手順 を完了するには、次の作業を行います。

- リカバリされたストレージノードにログインします。
- スクリプトを実行し `sn-remount-volumes`て、適切にフォーマットされたストレージボリュームを再マウントします。このスクリプトを実行すると、次の処理が行われます。
  - 各ストレージボリュームをマウントしてアンマウントし、 XFS ジャーナルをリプレイします。
  - XFS ファイルの整合性チェックを実行します。
  - ファイルシステムに整合性がある場合は、ストレージボリュームが適切にフォーマットされた StorageGRID ストレージボリュームであるかどうかを確認します。
  - ストレージボリュームが適切にフォーマットされている場合は、ストレージボリュームを再マウントします。ボリューム上の既存のデータはそのまま維持されます。
- スクリプトの出力を確認し、問題を解決します。
- スクリプトを実行し `sn-recovery-postinstall.sh`ます。このスクリプトを実行すると、次の処理が実行されます。

リカバリ中に（手順4）を実行して障害ストレージボリュームを再フォーマットし、オブジェクトメタデータをリストアする前にストレージノードをリブートしないでください `sn-recovery-postinstall.sh`。完了前にストレージノードをリブート `sn-recovery-postinstall.sh`すると、サービスが開始しようとするときにエラーが発生し、StorageGRIDアプライアンスノードがメンテナンスモードを終了します。

- スクリプトでマウントできなかったストレージボリューム、または適切にフォーマットされていないストレージボリュームを再フォーマットし `sn-remount-volumes`ます。

ストレージボリュームを再フォーマットすると、そのボリューム上のデータはすべて失われます。複数のオブジェクトコピーを格納するように ILM ルールが設定されている場合は、グリッド内の他の場所からオブジェクトデータをリストアするために追加の手順 を実行する必要があります。

- 必要に応じて、ノードの Cassandra データベースを再構築します。
- ストレージノードのサービスを開始します。

手順

1. リカバリしたストレージノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
   b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

   rootとしてログインすると、プロンプトがからに `#`変わります `$`。

2. 最初のスクリプトを実行し、適切にフォーマットされたストレージボリュームを再マウントします。

   すべてのストレージボリュームが新規でフォーマットが必要な場合、またはすべてのストレージボリュームで障害が発生した場合は、この手順を省略して 2 つ目のスクリプトを実行し、マウントされていないストレージボリュームをすべて再フォーマットします。

   a. スクリプトを実行します。 `sn-remount-volumes`

      データが格納されたストレージボリュームでこのスクリプトを実行すると、数時間かかることがあります。

   b. スクリプトの実行時に、出力と回答 のプロンプトを確認します。

      必要に応じて、コマンドを使用してスクリプトのログファイルの内容を監視でき `tail -f`(`/var/local/log/sn-remount-volumes.log`ます）。ログファイルには、コマンドラインの出力よりも詳細な情報が含まれています。

```
root@SG:~ # sn-remount-volumes
The configured LDR noid is 12632740
```

```
====== Device /dev/sdb ======
Mount and unmount device /dev/sdb and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sdb:
Mount device /dev/sdb to /tmp/sdb-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12632740, volume number 0 in the volID file
Attempting to remount /dev/sdb
Device /dev/sdb remounted successfully

====== Device /dev/sdc ======
Mount and unmount device /dev/sdc and checking file system
consistency:
Error: File system consistency check retry failed on device /dev/sdc.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh, this volume and any data on this volume will be
deleted. If you only had two copies of object data, you will
temporarily have only a single copy.
StorageGRID will attempt to restore data redundancy by making
additional replicated copies or EC fragments, according to the rules
in the active ILM policies.

Don't continue to the next step if you believe that the data
remaining on this volume can't be rebuilt from elsewhere in the grid
(for example, if your ILM policy uses a rule that makes only one copy
or if volumes have failed on multiple nodes). Instead, contact
support to determine how to recover your data.

====== Device /dev/sdd ======
Mount and unmount device /dev/sdd and checking file system
consistency:
Failed to mount device /dev/sdd
This device could be an uninitialized disk or has corrupted
superblock.
File system check might take a long time. Do you want to continue? (y
or n) [y/N]? y

Error: File system consistency check retry failed on device /dev/sdd.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
```

```
postinstall.sh, this volume and any data on this volume will be
deleted. If you only had two copies of object data, you will
temporarily have only a single copy.
StorageGRID will attempt to restore data redundancy by making
additional replicated copies or EC fragments, according to the rules
in the active ILM policies.

Don't continue to the next step if you believe that the data
remaining on this volume can't be rebuilt from elsewhere in the grid
(for example, if your ILM policy uses a rule that makes only one copy
or if volumes have failed on multiple nodes). Instead, contact
support to determine how to recover your data.

====== Device /dev/sde ======
Mount and unmount device /dev/sde and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sde:
Mount device /dev/sde to /tmp/sde-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12000078, volume number 9 in the volID file
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

この出力例では、 1 つのストレージボリュームが正常に再マウントされ、 3 つのストレージボリュームでエラーが発生しています。

- `/dev/sdb`XFSファイルシステムの整合性チェックに合格し、ボリューム構造が有効であったため、正常に再マウントされました。スクリプトによって再マウントされたデバイスのデータは保持されています。
- `/dev/sdc`ストレージボリュームが新規または破損しているため、XFSファイルシステムの整合性チェックに失敗しました。
- `/dev/sdd`ディスクが初期化されていないか、ディスクのスーパーブロックが破損しているため、マウントできませんでした。スクリプトがストレージボリュームをマウントできない場合は、ファイルシステムの整合性チェックを実行するかどうかを確認するメッセージが表示されます。
  - ストレージ・ボリュームが新しいディスクに接続されている場合は、回答 * N * をプロンプトに表示します。新しいディスク上のファイルシステムをチェックする必要はありません。
  - ストレージ・ボリュームが既存のディスクに接続されている場合は、回答 * Y * がプロンプトに表示されます。ファイルシステムのチェックの結果を使用して、破損の原因を特定できます。結果はログファイルに保存され `/var/local/log/sn-remount-volumes.log`ます。
- `/dev/sde`XFSファイルシステムの整合性チェックに合格し、ボリューム構造が有効でしたが、ファイル内のLDRノードID `volID`がこのストレージノードのID（上部に表示）と一致しませんでした `configured LDR noid`。このメッセージは、このボリュームが別のストレージノードに属していることを示しています。

3. スクリプトの出力を確認し、問題を解決します。

ストレージボリュームが XFS ファイルシステムの整合性チェックに合格できなかった場合、またはストレージボリュームをマウントできなかった場合は、出力のエラーメッセージをよく確認してください。これらのボリュームでスクリプトを実行した場合の影響を理解しておく必要があります `sn-recovery-postinstall.sh`。

a. 想定しているすべてのボリュームのエントリが結果に含まれていることを確認します。ボリュームが表示されない場合は、スクリプトを再実行します。

b. マウントされたすべてのデバイスのメッセージを確認します。ストレージボリュームがこのストレージノードに属していないことを示すエラーがないことを確認します。

この例では、 /dev/sde の出力に、次のエラーメッセージが含まれています。

```
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

あるストレージボリュームが別のストレージノードに属していると報告される場合は、テクニカルサポートにお問い合わせください。スクリプトを実行すると `sn-recovery-postinstall.sh`ストレージボリュームが再フォーマットされ、データが失われる可能性があります。

c. マウントできなかったストレージデバイスがある場合は、デバイス名をメモし、デバイスを修理または交換します。

マウントできなかったストレージデバイスはすべて修理または交換する必要があります。

d. マウントできないデバイスをすべて修復または交換したら、スクリプトをもう一度実行して、 `sn-remount-volumes`再マウント可能なすべてのストレージボリュームが再マウントされたことを確認します。

ストレージボリュームをマウントできない場合、またはストレージボリュームが適切にフォーマットされていない場合に次の手順に進むと、ボリュームとそのボリューム上のデータが削除されます。オブジェクトデータのコピーが 2 つあった場合、次の手順 （オブジェクトデータのリストア）が完了するまでコピーは 1 つだけになります。

障害ストレージボリュームに残っているデータをグリッド内の他の場所から再構築できないと考えられる場合は、スクリプトを実行しないでください（ILMポリシーでコピーを1つだけ作成するルールが使用されている場合や、複数のノードでボリュームで障害が発生した場合 `sn-recovery-postinstall.sh`など）。代わりに、テクニカルサポートに問い合わせてデータのリカバリ方法を確認してください。

4. スクリプトを実行し `sn-recovery-postinstall.sh`ます。 `sn-recovery-postinstall.sh`

このスクリプトは、マウントできなかったストレージボリューム、または適切にフォーマットされていないストレージボリュームを再フォーマットし、必要に応じてノードの Cassandra データベースを再構築して、ストレージノードのサービスを開始します。

次の点に注意してください。

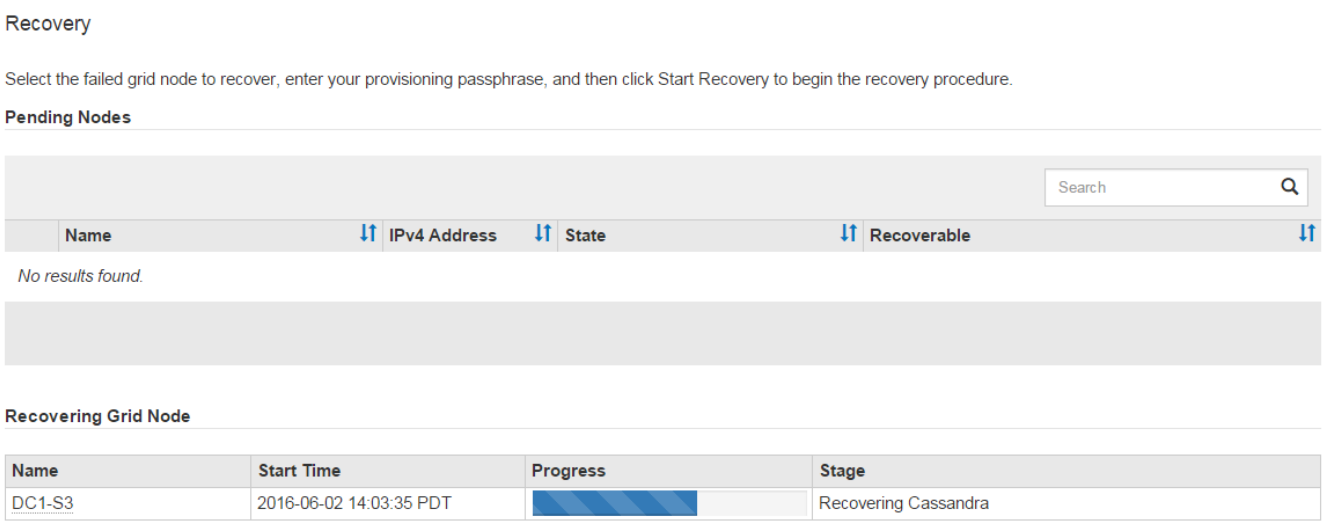
- スクリプトの実行には数時間かかることがあります。
- 一般に、スクリプトの実行中は、 SSH セッションは単独で行う必要があります。
- SSHセッションがアクティブな間は、*Ctrl+C*を押さないでください。
- このスクリプトは、ネットワークの中断が発生して SSH セッションが終了した場合にバックグラウンドで実行されますが、進行状況はリカバリページで確認できます。
- ストレージノードで RSM サービスを使用している場合は、ノードサービスの再起動時にスクリプトが 5 分間停止しているように見えることがあります。この 5 分間の遅延は、 RSM サービスが初めて起動するときに発生します。

RSM サービスは、 ADC サービスが含まれるストレージノードにあります。

一部の StorageGRID リカバリ手順では、 Reaper を使用して Cassandra の修復を処理します。関連サービスまたは必要なサービスが開始されるとすぐに修理が自動的に行われます。スクリプトの出力に「reaper」または「cassandra repair」と記載されていることがあります。修復が失敗したことを示すエラーメッセージが表示された場合は、エラーメッセージに示されているコマンドを実行します。

5. スクリプトの実行中に `sn-recovery-postinstall.sh`、Grid Managerの[Recovery]ページを監視します。

   [Recovery]ページの[Progress]バーと[Stage]列には、スクリプトのステータスの概要が表示され `sn-recovery-postinstall.sh`ます。



6. スクリプトでノードのサービスが開始されたら、 `sn-recovery-postinstall.sh`スクリプトでフォーマットされたストレージボリュームにオブジェクトデータをリストアできます。

   スクリプトは、オブジェクトデータを復元するためにGrid Managerボリューム復元プロセスを使用するかどうかを確認します。

   - ほとんどの場合、"Grid Managerを使用してオブジェクトデータをリストアする"。回答 `y` Grid Manager を使用します。
   - まれなケースとして、交換用ノードのオブジェクトストレージに使用できるボリュームが元のノードよりも少ないことがわかっている場合は、テクニカルサポートに連絡してオブジェクトデータを手動

で復元してください。これらのケースのいずれかに該当する場合は、 `n`と回答し、任意のキーを押してコマンドラインに戻ってください。

StorageGRIDアプライアンスのストレージボリュームにオブジェクトデータを復元します

アプライアンスストレージノードのストレージボリュームをリカバリしたら、ストレージノードの障害で失われたレプリケートオブジェクトデータまたはイレイジャーコーディングオブジェクトデータをリストアできます。

開始する前に

- 自動手順による保存済みストレージボリュームの再マウントおよび障害が発生したストレージボリュームの再フォーマットが失敗した場合は、次のいずれかの手順を実行してください。
  - "アプライアンスストレージボリュームの再マウントと再フォーマット（手動手順）"
  - "ストレージボリュームの再マウントと再フォーマット（手動手順）"
- オブジェクトを復元するストレージノードの接続状態が、Grid Manager の ノード > 概要 タブで 接続済み であることを確認しました。
- 以下の内容を確認しました：
  - ストレージノードを追加するためのグリッド拡張は現在進行中ではありません。
  - ストレージノードの廃止処理は実行中でないか、失敗しています。
  - 障害が発生したストレージボリュームの復旧処理は実行されていません。
  - システムドライブに障害が発生したストレージノードの復旧処理は実行されていません。
  - ECリバランス処理は実行されていません。
  - アプライアンスノードのクローン作成は実行されていません。

タスクの内容

ドライブを交換し、ボリュームをフォーマットした後、Grid Manager は メンテナンス > ボリュームの復元 > 復元するノード タブに、復元候補としてボリュームを表示します。

可能なかぎり、Grid Managerの[Volume restoration]ページを使用してオブジェクトデータをリストアします。ボリュームのリストア準備ができたときにボリュームのリストアを自動的に開始するか、またはをボリュームのリストアを手動で実行する選択できる自動リストアモードを有効にします。次のガイドラインに従ってください。

- ボリュームが メンテナンス > ボリュームの復元 > 復元するノード にリストされている場合は、以下の手順に従ってオブジェクト データを復元します。次の場合、ボリュームがリストされます。
  - ノード内の一部の（すべてではない）ストレージボリュームで障害が発生した
  - ノード内のすべてのストレージボリュームで障害が発生し、同じ数以上のボリュームに交換中です

    Grid Managerの[Volume restore]ページでは、とを実行することもできますボリュームのリストアプロセスを監視復元履歴を表示します。

  復旧したストレージノードに含まれるボリューム数が、交換前のノードに含まれるボリューム数より少ない場合は、テクニカルサポートにお問い合わせください。

次の2種類のオブジェクトデータをリストアできます。

- グリッドのILMルールがオブジェクトコピーを使用できるように設定されている場合、レプリケートデータオブジェクトは別の場所からリストアされます。
  - ILMルールが複製コピーを1つだけ保存するように設定されており、そのコピーが障害の発生したストレージボリューム上に存在していた場合、オブジェクトを復旧することはできません。
  - オブジェクトのコピーがクラウドストレージプールにしか残っていない場合、 StorageGRID は、オブジェクトデータをリストアするために複数の要求をクラウドストレージプールエンドポイントに問題する必要があります。
- イレイジャーコーディング（EC）データオブジェクトは、格納されているフラグメントを再編成してリストアされます。破損または損失したフラグメントは、イレイジャーコーディングアルゴリズムによって、残りのデータフラグメントとパリティフラグメントから再作成されます。

  イレイジャーコーディングデータの修復は、一部のストレージノードがオフライン状態で開始できます。ただし、すべてのイレイジャーコーディングデータを把握できない場合は、修復を完了できません。修復はすべてのノードが使用可能になったあとに完了します。

ボリュームのリストアは、オブジェクトコピーが格納されているリソースが使用可能かどうかに依存します。ボリュームのリストアは非線形であり、完了までに数日から数週間かかることがあります。

自動復元モードを有効にする

自動リストアモードを有効にすると、ボリュームのリストア準備が整うと、ボリュームのリストアが自動的に開始されます。

手順

1. Grid Manager で、[メンテナンス] > [ボリュームの復元] に移動します。
2. タブを選択し、[自動復元モード]*の切り替えをスライドさせて有効な位置にします。
3. 確認のダイアログボックスが表示されたら、詳細を確認します。

   - どのノードでも、ボリューム復元ジョブを手動で開始することはできません。
   - ボリュームのリストアは、他のメンテナンス手順が実行されていない場合にのみ自動的に開始されます。
   - 進捗状況監視ページでジョブのステータスを監視できます。
   - StorageGRIDは、開始に失敗したボリュームのリストアを自動的に再試行します。
4. 自動リストアモードを有効にした結果がわかったら、確認ダイアログボックスで*[はい]*を選択します。

   自動復元モードはいつでも無効にできます。

障害が発生したボリュームまたはノードを手動でリストアする

障害が発生したボリュームまたはノードをリストアする手順は、次のとおりです。

手順

1. Grid Manager で、[メンテナンス] > [ボリュームの復元] に移動します。
2. タブを選択し、[自動復元モード]*の切り替えを無効な位置にスライドさせます。

   タブの数は、リストアが必要なボリュームを含むノードの数を示します。

3. 各ノードを展開して、リストアが必要なボリュームとそのステータスを確認します。
4. 各ボリュームのリストアを妨げる問題を修正します。ボリュームステータスとして「Waiting for manual steps」（手動手順を待機しています）を選択すると、問題が表示されます。
5. リストアするノードを選択します。すべてのボリュームのステータスが[Ready to restore]になっています。

   ボリュームは一度に1つのノードに対してのみリストアできます。

   ノード内の各ボリュームは、復元準備が完了したことを示す必要があります。

6. [リストアの開始]*を選択します。
7. 表示される可能性のある警告に対処するか、*[とにかく開始]*を選択して警告を無視し、リストアを開始します。

リストアの開始時に、ノードは*タブから[リストアの進捗状況]*タブに移動します。

ボリュームのリストアを開始できない場合は、*[リストアするノード]*タブに戻ります。

リストアの進捗状況を表示します

[リストアの進捗状況]*タブには、ボリュームリストアプロセスのステータスと、リストア対象のノードのボリュームに関する情報が表示されます。

すべてのボリュームにおける複製オブジェクトおよび消去符号化オブジェクトのデータ修復率は、処理中のすべての修復作業をまとめた平均値です。それらのボリューム内のオブジェクトのうち、損傷がなく修復を必要としないものの割合も示されています。

> レプリケートされたデータのリストアは、レプリケートされたコピーが格納されているリソースの可用性に依存します。レプリケートされたデータのリストアはノンリニアで、完了までに数日から数週間かかることがあります。

[Restoration jobs]セクションには、Grid Managerから開始されたボリュームリストアに関する情報が表示されます。

- [Restoration jobs]セクションの数値は、リストア中またはリストア用にキューに登録されているボリュームの数を示します。
- このテーブルには、リストア対象のノード内の各ボリュームに関する情報とその進捗状況が表示されます。
  - 各ノードの進捗状況には、各ジョブの割合が表示されます。
  - [Details]列を展開して、リストアの開始時刻とジョブIDを表示します。
- ボリュームのリストアに失敗した場合：
  - [Status]列にと表示され `failed (attempting retry)`、自動的に再試行されます。

- 複数のリストアジョブが失敗した場合は、最新のジョブが最初に自動的に再試行されます。
- 再試行が失敗し続けると、* EC repair failure *アラートがトリガーされます。アラートに記載されている手順に従って、問題を解決します。

リストア履歴を表示します

[リストア履歴]*タブには、正常に完了したすべてのボリュームリストアに関する情報が表示されます。

サイズはレプリケートオブジェクトには適用されず、イレイジャーコーディング（EC）データオブジェクトを含むリストアの場合にのみ表示されます。

StorageGRID アプライアンスストレージノードの復元後にストレージの状態を確認する

アプライアンスストレージノードをリカバリしたら、アプライアンスストレージノードに必要とされる状態が「 Online 」に設定されていることを確認し、ストレージノードサーバが再起動するたびにオンライン状態になるようにする必要があります。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- ストレージノードがリカバリされ、データリカバリが完了している必要があります。

手順

1. ノード > ストレージノード > *タスク*を選択します。
2. *ストレージ状態*ドロップダウンリストが読み取り専用またはオフラインに設定されている場合は、*オンライン*を選択します。
3. [保存（ Save ）] を選択します。

システムドライブに損傷がない場合は、ストレージボリューム障害からリカバリします

StorageGRIDストレージボリュームのリカバリに関する警告

ストレージノードの障害ストレージボリュームをリカバリする前に、次の警告を確認してください。

ストレージノード内のストレージボリューム（ rangedb ）は、ボリューム ID と呼ばれる 16 進数で識別されます。たとえば、 0000 は最初のボリューム、 000F は 16 番目のボリュームです。各ストレージノードの最初のオブジェクトストア（ボリューム 0 ）は、オブジェクトメタデータと Cassandra データベースの処理に最大 4TB のスペースを使用します。このボリュームの残りのスペースはオブジェクトデータに使用されます。他のすべてのストレージボリュームは、オブジェクトデータ専用のボリュームです。

次の場合、ボリューム回復手順の一環として Cassandra データベースが再構築される可能性があります。

- ボリューム 0 に障害が発生し、回復されました。
- システムドライブと 1 つ以上のストレージボリュームで障害が発生し、リカバリされた。

Cassandra が再構築されると、システムは他のストレージ ノードからの情報を使用します。 Cassandra が最近再構築された場合、Cassandra データはグリッド全体でまだ一貫していない可能性があります。オフライ

ンのストレージノードが多すぎる場合:

- 一部の Cassandra データは利用できない可能性があります。
- データが失われる可能性があります。

> 複数のストレージ ノードに障害が発生した場合 (またはオフラインの場合) は、テクニカル サポートにお問い合わせください。次の回復手順は実行しないでください。データが失われる可能性があります。詳細については、 "テクニカルサポートによるサイトのリカバリ方法" 。

> ILM ルールが複製されたコピーを 1 つだけ保存するように構成されていて、そのコピーが障害が発生したストレージ ボリューム上に存在する場合、オブジェクトを回復することはできません。

関連情報

"グリッドノードのリカバリに関する警告と考慮事項"

StorageGRIDで障害が発生したストレージボリュームを特定してアンマウントします

ストレージボリュームに障害が発生したストレージノードをリカバリする場合は、障害ボリュームを特定し、アンマウントする必要があります。障害ストレージボリュームのみがリカバリ手順 で再フォーマットされることを確認する必要があります。

開始する前に

Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。

タスクの内容

障害が発生したストレージボリュームはできるだけ早くリカバリする必要があります。

まず最初に、接続解除されたボリューム、アンマウントが必要なボリューム、または I/O エラーが発生しているボリュームを検出します。障害ボリュームがランダムに破損したファイルシステムを含んでいる状態で接続されている場合は、ディスクの未使用部分または未割り当て部分の破損をシステムが検出できないことがあります。

> ディスクの追加や再接続、ノードの停止、ノードの開始、リブートなど、ボリュームをリカバリするための手動手順を実行する前に、この手順 を完了しておく必要があります。そうしないと、スクリプトの実行時に `reformat_storage_block_devices.rb`ファイルシステムエラーが発生し、スクリプトがハングしたり失敗したりする可能性があります。

> コマンドを実行する前に、ハードウェアを修理してディスクを適切に接続して `reboot`ください。

> 障害ストレージボリュームは慎重に特定してください。この情報を使用して、再フォーマットが必要なボリュームを確認します。ボリュームの再フォーマット後は、ボリューム上のデータをリカバリできません。

障害が発生したストレージ ボリュームを回復するには、障害が発生したストレージ ボリュームのデバイス名とボリューム ID の両方を知っておく必要があります。

インストール時に、各ストレージ デバイスにファイル システムのユニバーサル ユニーク ID (UUID) が割り当てられ、割り当てられたファイル システム UUID を使用してストレージ ノード上の rangedb ディレクトリにマウントされます。ファイルシステムUUIDとrangedbディレクトリは、 `/etc/fstab`ファイル。マウント ポイント、デバイス名、ボリュームのサイズがグリッド マネージャーに表示されます。

手順

1. 次の手順を実行して、障害ストレージボリュームとそのデバイス名を記録します。
   a. ノード > ***site*** > ***failed Storage Node*** > ストレージ を選択します。
   b. 下にスクロールしてボリューム テーブルとオブジェクト ストア テーブルを見つけ、ステータスが不明またはオフラインの各ボリュームについて次の情報を記録します。
      - ボリューム テーブルから、マウント ポイント、デバイス、サイズを記録します。
      - オブジェクトストアテーブルから、 `object_store_ID` 。

      `object_store_ID`は、障害ストレージボリュームのIDです。たとえば、IDが0000のオブジェクトストアのコマンドでと指定します `0`。

2. 障害が発生したストレージノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
   b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

      rootとしてログインすると、プロンプトがからに `#`変わります `$`。

3. 次のスクリプトを実行して、障害ストレージボリュームをアンマウントします。

   ```
   sn-unmount-volume object_store_ID
   ```

4. プロンプトが表示されたら、* y *を押して、ストレージボリューム0に応じてCassandraサービスを停止します。

   Cassandraサービスがすでに停止している場合は、プロンプトは表示されません。Cassandra サービスは、ボリューム 0 に対してのみ停止します。

   ```
   root@Storage-180:~/var/local/tmp/storage~ # sn-unmount-volume 0
   Services depending on storage volume 0 (cassandra) aren't down.
   Services depending on storage volume 0 must be stopped before running
   this script.
   Stop services that require storage volume 0 [y/N]? y
   Shutting down services that require storage volume 0.
   Services requiring storage volume 0 stopped.
   Unmounting /var/local/rangedb/0
   /var/local/rangedb/0 is unmounted.
   ```

数秒後にボリュームがアンマウントされます。プロセスの各ステップを示すメッセージが表示されます。最後のメッセージは、ボリュームがアンマウントされたことを示しています。

5. ボリュームがビジー状態であるためにアンマウントに失敗した場合は、オプションを使用して強制的にアンマウントできます `--use-umountof`。

> オプションを使用して強制的にアンマウントする `--use-umountof` と、ボリュームを使用しているプロセスやサービスが予期せずに動作したり、クラッシュしたりする可能性があります。

```
root@Storage-180:~ # sn-unmount-volume --use-umountof
/var/local/rangedb/2
Unmounting /var/local/rangedb/2 using umountof
/var/local/rangedb/2 is unmounted.
Informing LDR service of changes to storage volumes
```

障害が発生したストレージボリュームを復旧し、**StorageGRID** で **Cassandra** データベースを再構築します

障害が発生したストレージボリュームでストレージを再フォーマットして再マウントするスクリプトを実行し、システムが必要であると判断した場合にはストレージノードの Cassandra データベースを再構築する必要があります。

開始する前に

- あなたはファイルを持ってい `Passwords.txt`ます。
- サーバ上のシステムドライブに損傷はありません。
- 障害の原因 が特定され、必要に応じて交換用ストレージハードウェアがすでに入手されている。
- 交換用ストレージの合計サイズは、元のストレージと同じです。
- ストレージ ノードの廃止が進行中でないことを確認したか、ノードの廃止手順を一時停止しました。 (グリッド マネージャーで、メンテナンス > タスク > 廃止 を選択します。)
- 拡張が進行中ではないことを確認しました。 (グリッド マネージャーで、メンテナンス > タスク > 拡張 を選択します。)
- そうだな "ストレージボリュームのリカバリに関する警告を確認"

手順

1. 必要に応じて、前述の手順で特定してアンマウントした障害ストレージボリュームに関連付けられた、障害が発生した物理または仮想ストレージを交換します。

   この手順ではボリュームを再マウントしないでください。ストレージは、あとの手順で再マウントしてに追加し `/etc/fstab`ます。

2. グリッドマネージャで*ノード*に移動> **`appliance Storage Node`** > ハードウェア。ページのStorageGRIDアプライアンス セクションで、ストレージ RAID モードが正常であることを確認します。
3. 障害が発生したストレージノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@`*`grid_node_IP`*

b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

c. 次のコマンドを入力してrootに切り替えます。 `su -`

d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

rootとしてログインすると、プロンプトがからに `#`変わります `$`。

4. テキストエディタ（viまたはvim）を使用してファイルから障害ボリュームを削除し `/etc/fstab`、ファイルを保存します。

ファイルで障害ボリュームをコメントアウトする `/etc/fstab`だけでは不十分です。リカバリプロセスでは、ファイル内のすべての行がマウントされたファイルシステムと一致することが検証されるため、 `fstab`ボリュームをから削除する必要があります `fstab`。

5. 障害ストレージボリュームを再フォーマットし、必要に応じて Cassandra データベースを再構築します。入力： `reformat_storage_block_devices.rb`

- ストレージボリューム0がアンマウントされると、Cassandraサービスが停止していることを示すプロンプトとメッセージが表示されます。
- 必要に応じて Cassandra データベースを再構築するよう求められます。
  - 警告を確認します。いずれの状況も該当しない場合は、 Cassandra データベースを再構築します。「 * y * 」と入力します
  - 複数のストレージノードがオフラインの場合。入力してください: **n**

    スクリプトは Cassandra を再構築せずに終了します。テクニカルサポートにお問い合わせください。
- ストレージノード上の各rangedbドライブについて、のプロンプトが表示されたら `Reformat the rangedb drive <name> (device <major number>:<minor number>)? [y/n]?`、次のいずれかの応答を入力します。
  - * y * ：エラーが発生したドライブを再フォーマットします。これにより、ストレージボリュームが再フォーマットされ、再フォーマットされたストレージボリュームがファイルに追加され `/etc/fstab`ます。
  - *n*ドライブにエラーがなく、ドライブを再フォーマットしない場合。

*n * を選択すると、スクリプトが終了します。ドライブをマウントするか（ドライブ上のデータを保持する必要があり、ドライブが誤ってアンマウントされた場合）、ドライブを取り外します。次に、コマンドをもう一度実行し `reformat_storage_block_devices.rb`ます。

一部の StorageGRID リカバリ手順では、 Reaper を使用して Cassandra の修復を処理します。関連サービスまたは必要なサービスが開始されるとすぐに修理が自動的に行われます。スクリプトの出力に「reaper」または「cassandra repair」と記載されていることがあります。修復が失敗したことを示すエラーメッセージが表示された場合は、エラーメッセージに示されているコマンドを実行します。

次の出力例では、ドライブを `/dev/sdf`再フォーマットする必要がありますが、Cassandraを再構築す

る必要はありませんでした。

```
root@DC1-S1:~ # reformat_storage_block_devices.rb
Formatting devices that are not in use...
Skipping in use device /dev/sdc
Skipping in use device /dev/sdd
Skipping in use device /dev/sde
Reformat the rangedb drive /dev/sdf (device 8:64)? [Y/n]? y
Successfully formatted /dev/sdf with UUID b951bfcb-4804-41ad-b490-
805dfd8df16c
All devices processed
Running: /usr/local/ldr/setup_rangedb.sh 12368435
Cassandra does not need rebuilding.
Starting services.
Informing storage services of new volume

Reformatting done.  Now do manual steps to
restore copies of data.
```

次の手順

ストレージボリュームの再フォーマットと再マウントが完了し、必要な Cassandra 操作が完了したら、"Grid Managerを使用してオブジェクトデータをリストアする"。

システムドライブが損傷していない**StorageGRID**ストレージボリュームにオブジェクトデータを復元します

システムドライブに損傷がないストレージノードでストレージボリュームをリカバリしたら、ストレージボリュームの障害で失われたレプリケートオブジェクトデータまたはイレイジャーコーディングオブジェクトデータをリストアできます。

開始する前に

- 自動手順による保存済みストレージボリュームの再マウントおよび障害が発生したストレージボリュームの再フォーマットが失敗した場合は、次のいずれかの手順を実行してください。
  - "アプライアンスストレージボリュームの再マウントと再フォーマット（手動手順）"
  - "ストレージボリュームの再マウントと再フォーマット（手動手順）"
- オブジェクトを復元するストレージノードの接続状態が、Grid Manager の ノード > 概要 タブで 接続済み であることを確認しました。
- 以下の内容を確認しました：
  - ストレージノードを追加するためのグリッド拡張は現在進行中ではありません。
  - ストレージノードの廃止処理は実行中でないか、失敗しています。
  - 障害が発生したストレージボリュームの復旧処理は実行されていません。
  - システムドライブに障害が発生したストレージノードの復旧処理は実行されていません。
  - ECリバランス処理は実行されていません。

- アプライアンスノードのクローン作成は実行されていません。

タスクの内容

ドライブを交換し、ボリュームをフォーマットした後、Grid Manager は メンテナンス > ボリュームの復元 > 復元するノード タブに、復元候補としてボリュームを表示します。

可能なかぎり、Grid Managerの[Volume restoration]ページを使用してオブジェクトデータをリストアします。ボリュームのリストア準備ができたときにボリュームのリストアを自動的に開始するか、またはをボリュームのリストアを手動で実行する選択できます。次のガイドラインに従ってください。

- ボリュームが メンテナンス > ボリュームの復元 > 復元するノード にリストされている場合は、以下の手順に従ってオブジェクト データを復元します。次の場合、ボリュームがリストされます。
  - ノード内の一部の（すべてではない）ストレージボリュームで障害が発生した
  - ノード内のすべてのストレージボリュームで障害が発生し、同じ数以上のボリュームに交換中です

    Grid Managerの[Volume restore]ページでは、とを実行することもできますボリュームのリストアプロセスを監視復元履歴を表示します。

  復旧したストレージノードに含まれるボリューム数が、交換前のノードに含まれるボリューム数より少ない場合は、テクニカルサポートにお問い合わせください。

次の2種類のオブジェクトデータをリストアできます。

- グリッドのILMルールがオブジェクトコピーを使用できるように設定されている場合、レプリケートデータオブジェクトは別の場所からリストアされます。
  - ILMルールが複製コピーを1つだけ保存するように設定されており、そのコピーが障害の発生したストレージボリューム上に存在していた場合、オブジェクトを復旧することはできません。
  - オブジェクトのコピーがクラウドストレージプールにしか残っていない場合、 StorageGRID は、オブジェクトデータをリストアするために複数の要求をクラウドストレージプールエンドポイントに問題する必要があります。
- イレイジャーコーディング（EC）データオブジェクトは、格納されているフラグメントを再編成してリストアされます。破損または損失したフラグメントは、イレイジャーコーディングアルゴリズムによって、残りのデータフラグメントとパリティフラグメントから再作成されます。

  イレイジャーコーディングデータの修復は、一部のストレージノードがオフライン状態で開始できます。ただし、すべてのイレイジャーコーディングデータを把握できない場合は、修復を完了できません。修復はすべてのノードが使用可能になったあとに完了します。

> ボリュームのリストアは、オブジェクトコピーが格納されているリソースが使用可能かどうかに依存します。ボリュームのリストアは非線形であり、完了までに数日から数週間かかることがあります。

自動復元モードを有効にする

自動リストアモードを有効にすると、ボリュームのリストア準備が整うと、ボリュームのリストアが自動的に開始されます。

手順

1. Grid Manager で、[メンテナンス] > [ボリュームの復元] に移動します。
2. タブを選択し、[自動復元モード]*の切り替えをスライドさせて有効な位置にします。
3. 確認のダイアログボックスが表示されたら、詳細を確認します。

   - どのノードでも、ボリューム復元ジョブを手動で開始することはできません。
   - ボリュームのリストアは、他のメンテナンス手順が実行されていない場合にのみ自動的に開始されます。
   - 進捗状況監視ページでジョブのステータスを監視できます。
   - StorageGRIDは、開始に失敗したボリュームのリストアを自動的に再試行します。

4. 自動リストアモードを有効にした結果がわかったら、確認ダイアログボックスで*[はい]*を選択します。

   自動復元モードはいつでも無効にできます。

障害が発生したボリュームまたはノードを手動でリストアする

障害が発生したボリュームまたはノードをリストアする手順は、次のとおりです。

手順

1. Grid Manager で、[メンテナンス] > [ボリュームの復元] に移動します。
2. タブを選択し、[自動復元モード]*の切り替えを無効な位置にスライドさせます。

   タブの数は、リストアが必要なボリュームを含むノードの数を示します。

3. 各ノードを展開して、リストアが必要なボリュームとそのステータスを確認します。
4. 各ボリュームのリストアを妨げる問題を修正します。ボリュームステータスとして「Waiting for manual steps」（手動手順を待機しています）を選択すると、問題が表示されます。
5. リストアするノードを選択します。すべてのボリュームのステータスが[Ready to restore]になっています。

   ボリュームは一度に1つのノードに対してのみリストアできます。

   ノード内の各ボリュームは、復元準備が完了したことを示す必要があります。

6. [リストアの開始]*を選択します。
7. 表示される可能性のある警告に対処するか、*[とにかく開始]*を選択して警告を無視し、リストアを開始します。

リストアの開始時に、ノードは*タブから[リストアの進捗状況]*タブに移動します。

ボリュームのリストアを開始できない場合は、*[リストアするノード]*タブに戻ります。

リストアの進捗状況を表示します

[リストアの進捗状況]*タブには、ボリュームリストアプロセスのステータスと、リストア対象のノードのボリュームに関する情報が表示されます。

すべてのボリュームにおける複製オブジェクトおよび消去符号化オブジェクトのデータ修復率は、処理中のすべての修復作業をまとめた平均値です。それらのボリューム内のオブジェクトのうち、損傷がなく修復を必要としないものの割合も示されています。

> レプリケートされたデータのリストアは、レプリケートされたコピーが格納されているリソースの可用性に依存します。レプリケートされたデータのリストアはノンリニアで、完了までに数日から数週間かかることがあります。

[Restoration jobs]セクションには、Grid Managerから開始されたボリュームリストアに関する情報が表示されます。

- [Restoration jobs]セクションの数値は、リストア中またはリストア用にキューに登録されているボリュームの数を示します。
- このテーブルには、リストア対象のノード内の各ボリュームに関する情報とその進捗状況が表示されます。
  - 各ノードの進捗状況には、各ジョブの割合が表示されます。
  - [Details]列を展開して、リストアの開始時刻とジョブIDを表示します。
- ボリュームのリストアに失敗した場合：
  - [Status]列にと表示され `failed (attempting retry)`、自動的に再試行されます。
  - 複数のリストアジョブが失敗した場合は、最新のジョブが最初に自動的に再試行されます。
  - 再試行が失敗し続けると、* EC repair failure *アラートがトリガーされます。アラートに記載されている手順に従って、問題を解決します。

リストア履歴を表示します

[リストア履歴]*タブには、正常に完了したすべてのボリュームリストアに関する情報が表示されます。

> サイズはレプリケートオブジェクトには適用されず、イレイジャーコーディング（EC）データオブジェクトを含むリストアの場合にのみ表示されます。

StorageGRIDストレージボリュームの復旧後にストレージの状態を確認する

ストレージボリュームをリカバリしたら、ストレージノードに必要とされる状態が「 Online 」に設定されていることを確認し、ストレージノードサーバが再起動するたびにオンライン状態になるようにする必要があります。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- ストレージノードがリカバリされ、データリカバリが完了している必要があります。

手順

1. ノード > ストレージノード > *タスク*を選択します。
2. *ストレージ状態*ドロップダウンリストが読み取り専用またはオフラインに設定されている場合は、*オンライン*を選択します。
3. [保存（ Save ）] を選択します。

システムドライブ障害からリカバリします

StorageGRIDストレージノードのシステムドライブ復旧に関する警告

ストレージノードの障害システムドライブをリカバリする前に、一般的な警告と以下の固有の警告を確認してください"グリッドノードのリカバリに関する警告と考慮事項"。

ストレージ ノードには、オブジェクト メタデータを含む Cassandra データベースがあります。次の場合には、Cassandra データベースが再構築される可能性があります。

- ストレージ ボリュームに障害が発生し、回復しました。
- システムドライブと 1 つ以上のストレージボリュームで障害が発生し、リカバリされた。

Cassandra が再構築されると、システムは他のストレージ ノードからの情報を使用します。 Cassandra が最近再構築された場合、Cassandra データはグリッド全体でまだ一貫していない可能性があります。オフラインのストレージノードが多すぎる場合:

- 一部の Cassandra データは利用できない可能性があります。
- データが失われる可能性があります。

> 複数のストレージ ノードに障害が発生した場合 (またはオフラインの場合) は、テクニカル サポートにお問い合わせください。次の回復手順を実行しないでください。データが失われる可能性があります。詳細については、 "テクニカルサポートによるサイトのリカバリ方法" 。

> このストレージノードが、障害が発生したストレージボリュームを持つ別のストレージノードによるオブジェクトの取得を可能にするために読み取り専用メンテナンスモードになっている場合は、この障害が発生したストレージノードを復旧する前に、障害が発生したストレージボリュームを持つストレージノード上のボリュームを復旧してください。"システムドライブに損傷がない場合は、ストレージボリューム障害からリカバリします"の手順を参照してください。

> レプリケートコピーを 1 つだけ保存するように ILM ルールを設定している場合に、そのコピーがあるストレージボリュームで障害が発生すると、オブジェクトをリカバリできません。

StorageGRIDストレージノードを交換する

システムドライブで障害が発生した場合は、最初にストレージノードを交換する必要があります。

使用しているプラットフォームに対応するノード交換用手順 を選択する必要があります。ノードの交換手順は、すべてのタイプのグリッドノードで同じです。

> この 手順 環境 ソフトウェアベースのストレージノードのみ。別の手順に従って、を実行する必要があり"アプライアンスストレージノードをリカバリします"ます。

- Linux：*システムドライブで障害が発生したかどうかが不明な場合は、手順に従ってノードを交換し、必要なリカバリ手順を確認してください。

プラットフォーム	手順
VMware	"VMware ノードを交換"
Linux	"Linux ノードを交換"
OpenStack	リカバリ処理を対象とした OpenStack 用の仮想マシンディスクファイルおよびスクリプトは、現在は提供されていません。OpenStack 環境で実行されているノードのリカバリが必要な場合は、使用している Linux オペレーティングシステム用のファイルをダウンロードしてください。次に、の手順に従います"Linuxノードの交換"。

リカバリの開始を選択して **StorageGRID** ストレージノードを構成します

ストレージノードを交換したら、 Grid Manager で Start Recovery を選択して、障害が発生したノードの代わりとして新しいノードを設定する必要があります。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"Maintenance権限またはRoot Access権限"。
- プロビジョニングパスフレーズを用意します。
- 交換用ノードの導入と設定を完了しておきます。
- イレイジャーコーディングデータの修復ジョブの開始日を確認しておきます。

タスクの内容

ストレージノードが Linux ホストにコンテナとしてインストールされている場合は、次のいずれかに該当する場合にのみこの手順を実行する必要があります。

- フラグを使用し `--force`てノードをインポートするか、または `storagegrid node force-recovery *node-name*`
- ノードの完全な再インストールを実行するか、 /var/local をリストアする必要がありました。

手順

1. プライマリ管理ノードにログインします。プライマリ管理ノードが利用できない場合は、プライマリ以外の管理ノードが存在すればそちらを使用してください。
2. グリッドマネージャから、メンテナンス > タスク > *ノード復旧*を選択します。
3. リカバリするグリッドノードを Pending Nodes リストで選択します。

   ノードに障害が発生するとリストに表示されますが、ノードを再インストールしてリカバリの準備ができるまでは選択できません。

4. **Provisioning passphrase** を入力してください。
5. 「リカバリを開始」をクリックします。
6. **Maintenance** > **Tasks** > **Node recovery** を選択し、復旧の進捗状況を確認することで、復旧の進行状況を監視します。

- グリッドノードが「手動ステップ待ち」段階に達した場合は、"ストレージボリュームを手動で再マウントおよび再フォーマットする"。手動手順が完了したら、"オブジェクトデータをボリュームに復元する"に進みます。
- グリッドノードの復旧が「手動手順待ち」の段階を経ずに「進行中」から「復旧済み」に移行した場合、それ以上の操作は必要ありません。

> 復旧処理のどの段階でも、*リセット*を選択して新しい復旧を開始できます。手順をリセットするとノードが不確定な状態になることを示すダイアログボックスが表示されます。
>
> 手順をリセットした後に復旧を再試行する場合は、アプライアンスノードを次のようにプリインストール状態に復元する必要があります。
>
> - * vmware * ：導入した仮想グリッドノードを削除します。その後、リカバリを再開する準備ができたら、ノードを再導入します。
> - * Linux *：Linuxホストで次のコマンドを実行してノードを再起動します。
>
> `storagegrid node force-recovery node-name`

StorageGRIDストレージボリュームの再マウントと再フォーマット（手動手順）

自動手順による保存済みストレージボリュームの再マウントおよび障害が発生したストレージボリュームの再フォーマットが失敗した場合は、これらの操作を完了するために2つのスクリプトを手動で実行する必要があります。最初のスクリプトは、StorageGRIDストレージボリュームとして適切にフォーマットされたボリュームを再マウントします。2番目のスクリプトは、マウントされていないボリュームを再フォーマットし、必要に応じて Cassandra データベースを再構築して、サービスを開始します。

ストレージノードの復旧中に、Grid Manager に「Waiting for manual steps」というメッセージが表示された場合は、次の手順に従ってストレージボリュームを再マウントおよび再フォーマットしてください。このメッセージが表示されない場合は、再マウントおよび再フォーマット操作は自動的に完了しているため、この手順をスキップして"オブジェクトデータを復元する"に進むことができます。

開始する前に

- 障害が発生したストレージボリュームのうち、必要と判断した場合はハードウェアを交換しておく必要があります。

  スクリプトを実行 `sn-remount-volumes`すると、障害ストレージボリュームを追加で特定できる場合があります。

- ストレージ ノードの廃止が進行中でないことを確認したか、ノードの廃止手順を一時停止しました。 (グリッド マネージャーで、メンテナンス > タスク > 廃止 を選択します。)
- 拡張が進行中ではないことを確認しました。 (グリッド マネージャーで、メンテナンス > タスク > 拡張 を選択します。)
- そうだな "ストレージノードのシステムドライブのリカバリに関する警告を確認しました"

> 複数のストレージ ノードがオフラインの場合は、テクニカル サポートにお問い合わせください。実行しないでください `sn-recovery-postinstall.sh`スクリプト。

タスクの内容

この手順 を完了するには、次の作業を行います。

- リカバリされたストレージノードにログインします。
- スクリプトを実行し `sn-remount-volumes`て、適切にフォーマットされたストレージボリュームを再マウントします。このスクリプトを実行すると、次の処理が行われます。
  - 各ストレージボリュームをマウントしてアンマウントし、 XFS ジャーナルをリプレイします。
  - XFS ファイルの整合性チェックを実行します。
  - ファイルシステムに整合性がある場合は、ストレージボリュームが適切にフォーマットされた StorageGRID ストレージボリュームであるかどうかを確認します。
  - ストレージボリュームが適切にフォーマットされている場合は、ストレージボリュームを再マウントします。ボリューム上の既存のデータはそのまま維持されます。
- スクリプトの出力を確認し、問題を解決します。
- スクリプトを実行し `sn-recovery-postinstall.sh`ます。このスクリプトを実行すると、次の処理が実行されます。

  を実行して障害ストレージボリュームを再フォーマットし、オブジェクトメタデータをリストアする前に、リカバリ中にストレージノードをリブートしないで `sn-recovery-postinstall.sh`ください。完了前にストレージノードをリブート `sn-recovery-postinstall.sh`すると、サービスが開始しようとするときにエラーが発生し、StorageGRIDアプライアンスノードがメンテナンスモードを終了します。の手順を参照してくださいインストール後のスクリプト。

  - スクリプトでマウントできなかったストレージボリューム、または適切にフォーマットされていないストレージボリュームを再フォーマットし `sn-remount-volumes`ます。

    ストレージボリュームを再フォーマットすると、そのボリューム上のデータはすべて失われます。複数のオブジェクトコピーを格納するように ILM ルールが設定されている場合は、グリッド内の他の場所からオブジェクトデータをリストアするために追加の手順 を実行する必要があります。

  - 必要に応じて、ノードの Cassandra データベースを再構築します。
  - ストレージノードのサービスを開始します。

手順

1. リカバリしたストレージノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
   b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

   rootとしてログインすると、プロンプトがからに `#`変わります `$`。
2. 最初のスクリプトを実行し、適切にフォーマットされたストレージボリュームを再マウントします。

すべてのストレージボリュームが新規でフォーマットが必要な場合、またはすべてのストレージボリュームで障害が発生した場合は、この手順を省略して 2 つ目のスクリプトを実行し、マウントされていないストレージボリュームをすべて再フォーマットします。

a. スクリプトを実行します。 `sn-remount-volumes`

データが格納されたストレージボリュームでこのスクリプトを実行すると、数時間かかることがあります。

b. スクリプトの実行時に、出力と回答 のプロンプトを確認します。

必要に応じて、コマンドを使用してスクリプトのログファイルの内容を監視でき `tail -f(`/var/local/log/sn-remount-volumes.log`ます）。ログファイルには、コマンドラインの出力よりも詳細な情報が含まれています。

```
root@SG:~ # sn-remount-volumes
The configured LDR noid is 12632740

====== Device /dev/sdb ======
Mount and unmount device /dev/sdb and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sdb:
Mount device /dev/sdb to /tmp/sdb-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12632740, volume number 0 in the volID file
Attempting to remount /dev/sdb
Device /dev/sdb remounted successfully

====== Device /dev/sdc ======
Mount and unmount device /dev/sdc and checking file system
consistency:
Error: File system consistency check retry failed on device /dev/sdc.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh,
this volume and any data on this volume will be deleted. If you only
had two
copies of object data, you will temporarily have only a single copy.
StorageGRID will attempt to restore data redundancy by making
additional replicated copies or EC fragments, according to the rules
in
the active ILM policies.
```

```
Don't continue to the next step if you believe that the data
remaining on
this volume can't be rebuilt from elsewhere in the grid (for example,
if
your ILM policy uses a rule that makes only one copy or if volumes
have
failed on multiple nodes). Instead, contact support to determine how
to
recover your data.

====== Device /dev/sdd ======
Mount and unmount device /dev/sdd and checking file system
consistency:
Failed to mount device /dev/sdd
This device could be an uninitialized disk or has corrupted
superblock.
File system check might take a long time. Do you want to continue? (y
or n) [y/N]? y

Error: File system consistency check retry failed on device /dev/sdd.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh,
this volume and any data on this volume will be deleted. If you only
had two
copies of object data, you will temporarily have only a single copy.
StorageGRID will attempt to restore data redundancy by making
additional replicated copies or EC fragments, according to the rules
in
the active ILM policies.

Don't continue to the next step if you believe that the data
remaining on
this volume can't be rebuilt from elsewhere in the grid (for example,
if
your ILM policy uses a rule that makes only one copy or if volumes
have
failed on multiple nodes). Instead, contact support to determine how
to
recover your data.

====== Device /dev/sde ======
Mount and unmount device /dev/sde and checking file system
consistency:
```

```
The device is consistent.
Check rangedb structure on device /dev/sde:
Mount device /dev/sde to /tmp/sde-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12000078, volume number 9 in the volID file
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

この出力例では、 1 つのストレージボリュームが正常に再マウントされ、 3 つのストレージボリュームでエラーが発生しています。

- `/dev/sdb`XFSファイルシステムの整合性チェックに合格し、ボリューム構造が有効であったため、正常に再マウントされました。スクリプトによって再マウントされたデバイスのデータは保持されています。
- `/dev/sdc`ストレージボリュームが新規または破損しているため、XFSファイルシステムの整合性チェックに失敗しました。
- `/dev/sdd`ディスクが初期化されていないか、ディスクのスーパーブロックが破損しているため、マウントできませんでした。スクリプトがストレージボリュームをマウントできない場合は、ファイルシステムの整合性チェックを実行するかどうかを確認するメッセージが表示されます。
  - ストレージ・ボリュームが新しいディスクに接続されている場合は、回答 * N * をプロンプトに表示します。新しいディスク上のファイルシステムをチェックする必要はありません。
  - ストレージ・ボリュームが既存のディスクに接続されている場合は、回答 * Y * がプロンプトに表示されます。ファイルシステムのチェックの結果を使用して、破損の原因を特定できます。結果はログファイルに保存され `/var/local/log/sn-remount-volumes.log`ます。
- `/dev/sde`XFSファイルシステムの整合性チェックに合格し、ボリューム構造が有効でしたが、volIDファイル内のLDRノードIDがこのストレージノードのID（上部に表示）と一致しませんでした `configured LDR noid。このメッセージは、このボリュームが別のストレージノードに属していることを示しています。

3. スクリプトの出力を確認し、問題を解決します。

> ストレージボリュームが XFS ファイルシステムの整合性チェックに合格できなかった場合、またはストレージボリュームをマウントできなかった場合は、出力のエラーメッセージをよく確認してください。これらのボリュームでスクリプトを実行した場合の影響を理解しておく必要があります `sn-recovery-postinstall.sh`。

a. 想定しているすべてのボリュームのエントリが結果に含まれていることを確認します。ボリュームが表示されない場合は、スクリプトを再実行します。

b. マウントされたすべてのデバイスのメッセージを確認します。ストレージボリュームがこのストレージノードに属していないことを示すエラーがないことを確認します。

この例では、の出力 `/dev/sde`に次のエラーメッセージが含まれています。

```
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

あるストレージボリュームが別のストレージノードに属していると報告される場合は、テクニカルサポートにお問い合わせください。スクリプトを実行すると `sn-recovery-postinstall.sh`ストレージボリュームが再フォーマットされ、データが失われる可能性があります。

c. マウントできなかったストレージデバイスがある場合は、デバイス名をメモし、デバイスを修理または交換します。

マウントできなかったストレージデバイスはすべて修理または交換する必要があります。

d. マウントできないデバイスをすべて修復または交換したら、スクリプトをもう一度実行して、 `sn-remount-volumes`再マウント可能なすべてのストレージボリュームが再マウントされたことを確認します。

ストレージボリュームをマウントできない場合、またはストレージボリュームが適切にフォーマットされていない場合に次の手順に進むと、ボリュームとそのボリューム上のデータが削除されます。オブジェクトデータのコピーが 2 つあった場合、次の手順 （オブジェクトデータのリストア）が完了するまでコピーは 1 つだけになります。

障害ストレージボリュームに残っているデータをグリッド内の他の場所から再構築できないと考えられる場合は、スクリプトを実行しないでください（ILMポリシーでコピーを1つだけ作成するルールが使用されている場合や、複数のノードでボリュームで障害が発生した場合 `sn-recovery-postinstall.sh`など）。代わりに、テクニカルサポートに問い合わせてデータのリカバリ方法を確認してください。

4. スクリプトを実行し `sn-recovery-postinstall.sh`ます。 `sn-recovery-postinstall.sh`

このスクリプトは、マウントできなかったストレージボリューム、または適切にフォーマットされていないストレージボリュームを再フォーマットし、必要に応じてノードの Cassandra データベースを再構築して、ストレージノードのサービスを開始します。

次の点に注意してください。

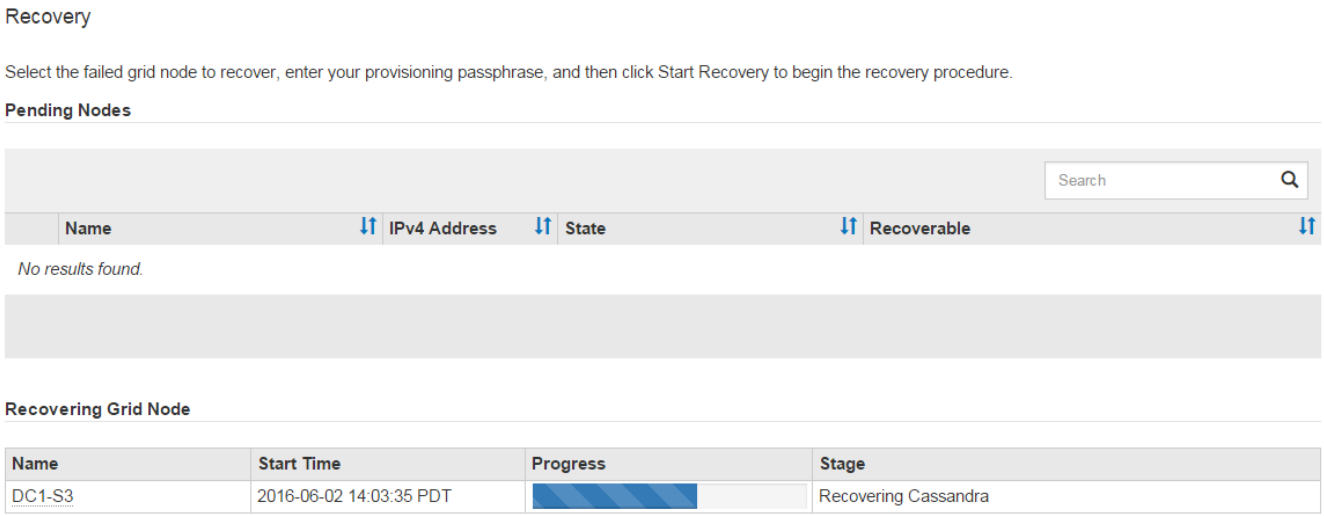
- スクリプトの実行には数時間かかることがあります。
- 一般に、スクリプトの実行中は、 SSH セッションは単独で行う必要があります。
- SSHセッションがアクティブな間は、*Ctrl+C*を押さないでください。
- このスクリプトは、ネットワークの中断が発生して SSH セッションが終了した場合にバックグラウンドで実行されますが、進行状況はリカバリページで確認できます。
- ストレージノードで RSM サービスを使用している場合は、ノードサービスの再起動時にスクリプトが 5 分間停止しているように見えることがあります。この 5 分間の遅延は、 RSM サービスが初めて起動するときに発生します。

RSM サービスは、 ADC サービスが含まれるストレージノードにあります。

一部の StorageGRID リカバリ手順では、 Reaper を使用して Cassandra の修復を処理します。関連サービスまたは必要なサービスが開始されるとすぐに修理が自動的に行われます。スクリプトの出力に「reaper」または「cassandra repair」と記載されていることがあります。修復が失敗したことを示すエラーメッセージが表示された場合は、エラーメッセージに示されているコマンドを実行します。

5. スクリプトの実行中は `sn-recovery-postinstall.sh`、Grid Managerの[Recovery]ページを監視してください。

   [Recovery]ページの[Progress]バーと[Stage]列には、スクリプトのステータスの概要が表示され `sn-recovery-postinstall.sh`ます。



6. スクリプトでノードのサービスが開始されたら、 `sn-recovery-postinstall.sh`スクリプトでフォーマットされたストレージボリュームにオブジェクトデータをリストアできます。

   Grid Managerのボリュームリストアプロセスを使用するかどうかを確認するメッセージが表示されます。

   - ほとんどの場合、"Grid Managerを使用してオブジェクトデータをリストアする"。回答 `y` Grid Manager を使用します。
   - まれなケースとして、交換用ノードのオブジェクトストレージに使用できるボリュームが元のノードよりも少ないことがわかっている場合は、テクニカルサポートに連絡してオブジェクトデータを手動で復元してください。これらのケースのいずれかに該当する場合は、 `n`と回答し、任意のキーを押してコマンドラインに戻ってください。

オブジェクトデータを**StorageGRID**ストレージボリュームに復元（システムドライブ障害）

非アプライアンスストレージノードのストレージボリュームをリカバリしたら、ストレージノードの障害で失われたレプリケートオブジェクトデータまたはイレイジャーコーディングオブジェクトデータをリストアできます。

開始する前に

- 自動手順による保存済みストレージボリュームの再マウントおよび障害が発生したストレージボリュームの再フォーマットが失敗した場合は、次のいずれかの手順を実行してください。
  - "アプライアンスストレージボリュームの再マウントと再フォーマット（手動手順）"

- "ストレージボリュームの再マウントと再フォーマット（手動手順）"

- オブジェクトを復元するストレージノードの接続状態が、Grid Manager の ノード > 概要 タブで 接続済み であることを確認しました。
- 以下の内容を確認しました：
  - ストレージノードを追加するためのグリッド拡張は現在進行中ではありません。
  - ストレージノードの廃止処理は実行中でないか、失敗しています。
  - 障害が発生したストレージボリュームの復旧処理は実行されていません。
  - システムドライブに障害が発生したストレージノードの復旧処理は実行されていません。
  - ECリバランス処理は実行されていません。
  - アプライアンスノードのクローン作成は実行されていません。

タスクの内容

ドライブを交換し、ボリュームをフォーマットした後、Grid Manager は メンテナンス > ボリュームの復元 > 復元するノード タブに、復元候補としてボリュームを表示します。

可能なかぎり、Grid Managerの[Volume restoration]ページを使用してオブジェクトデータをリストアします。ボリュームのリストア準備ができたときにボリュームのリストアを自動的に開始するか、またはをボリュームのリストアを手動で実行する選択でき自動リストアモードを有効にするます。次のガイドラインに従ってください。

- ボリュームが メンテナンス > ボリュームの復元 > 復元するノード にリストされている場合は、以下の手順に従ってオブジェクト データを復元します。次の場合、ボリュームがリストされます。
  - ノード内の一部の（すべてではない）ストレージボリュームで障害が発生した
  - ノード内のすべてのストレージボリュームで障害が発生し、同じ数以上のボリュームに交換中です

    Grid Managerの[Volume restore]ページでは、とを実行することもできますボリュームのリストアプロセスを監視復元履歴を表示します。

  復旧したストレージノードに含まれるボリューム数が、交換前のノードに含まれるボリューム数より少ない場合は、テクニカルサポートにお問い合わせください。

次の2種類のオブジェクトデータをリストアできます。

- グリッドのILMルールがオブジェクトコピーを使用できるように設定されている場合、レプリケートデータオブジェクトは別の場所からリストアされます。
  - ILMルールが複製コピーを1つだけ保存するように設定されており、そのコピーが障害の発生したストレージボリューム上に存在していた場合、オブジェクトを復旧することはできません。
  - オブジェクトのコピーがクラウドストレージプールにしか残っていない場合、 StorageGRID は、オブジェクトデータをリストアするために複数の要求をクラウドストレージプールエンドポイントに問題する必要があります。
- イレイジャーコーディング（EC）データオブジェクトは、格納されているフラグメントを再編成してリストアされます。破損または損失したフラグメントは、イレイジャーコーディングアルゴリズムによって、残りのデータフラグメントとパリティフラグメントから再作成されます。

イレイジャーコーディングデータの修復は、一部のストレージノードがオフライン状態で開始できます。ただし、すべてのイレイジャーコーディングデータを把握できない場合は、修復を完了できません。修復はすべてのノードが使用可能になったあとに完了します。

ボリュームのリストアは、オブジェクトコピーが格納されているリソースが使用可能かどうかに依存します。ボリュームのリストアは非線形であり、完了までに数日から数週間かかることがあります。

自動復元モードを有効にする

自動リストアモードを有効にすると、ボリュームのリストア準備が整うと、ボリュームのリストアが自動的に開始されます。

手順

1. Grid Manager で、[メンテナンス] > [ボリュームの復元] に移動します。
2. タブを選択し、[自動復元モード]*の切り替えをスライドさせて有効な位置にします。
3. 確認のダイアログボックスが表示されたら、詳細を確認します。

   - どのノードでも、ボリューム復元ジョブを手動で開始することはできません。
   - ボリュームのリストアは、他のメンテナンス手順が実行されていない場合にのみ自動的に開始されます。
   - 進捗状況監視ページでジョブのステータスを監視できます。
   - StorageGRIDは、開始に失敗したボリュームのリストアを自動的に再試行します。

4. 自動リストアモードを有効にした結果がわかったら、確認ダイアログボックスで*[はい]*を選択します。

   自動復元モードはいつでも無効にできます。

障害が発生したボリュームまたはノードを手動でリストアする

障害が発生したボリュームまたはノードをリストアする手順は、次のとおりです。

手順

1. Grid Manager で、[メンテナンス] > [ボリュームの復元] に移動します。
2. タブを選択し、[自動復元モード]*の切り替えを無効な位置にスライドさせます。

   タブの数は、リストアが必要なボリュームを含むノードの数を示します。

3. 各ノードを展開して、リストアが必要なボリュームとそのステータスを確認します。
4. 各ボリュームのリストアを妨げる問題を修正します。ボリュームステータスとして「Waiting for manual steps」（手動手順を待機しています）を選択すると、問題が表示されます。
5. リストアするノードを選択します。すべてのボリュームのステータスが[Ready to restore]になっています。

   ボリュームは一度に1つのノードに対してのみリストアできます。

ノード内の各ボリュームは、復元準備が完了したことを示す必要があります。

6. [リストアの開始]*を選択します。
7. 表示される可能性のある警告に対処するか、*[とにかく開始]*を選択して警告を無視し、リストアを開始します。

リストアの開始時に、ノードは*タブから[リストアの進捗状況]*タブに移動します。

ボリュームのリストアを開始できない場合は、*[リストアするノード]*タブに戻ります。

リストアの進捗状況を表示します

[リストアの進捗状況]*タブには、ボリュームリストアプロセスのステータスと、リストア対象のノードのボリュームに関する情報が表示されます。

すべてのボリュームにおける複製オブジェクトおよび消去符号化オブジェクトのデータ修復率は、処理中のすべての修復作業をまとめた平均値です。それらのボリューム内のオブジェクトのうち、損傷がなく修復を必要としないものの割合も示されています。

> レプリケートされたデータのリストアは、レプリケートされたコピーが格納されているリソースの可用性に依存します。レプリケートされたデータのリストアはノンリニアで、完了までに数日から数週間かかることがあります。

[Restoration jobs]セクションには、Grid Managerから開始されたボリュームリストアに関する情報が表示されます。

- [Restoration jobs]セクションの数値は、リストア中またはリストア用にキューに登録されているボリュームの数を示します。
- このテーブルには、リストア対象のノード内の各ボリュームに関する情報とその進捗状況が表示されます。
  - 各ノードの進捗状況には、各ジョブの割合が表示されます。
  - [Details]列を展開して、リストアの開始時刻とジョブIDを表示します。
- ボリュームのリストアに失敗した場合：
  - [Status]列にと表示され `failed (attempting retry)`、自動的に再試行されます。
  - 複数のリストアジョブが失敗した場合は、最新のジョブが最初に自動的に再試行されます。
  - 再試行が失敗し続けると、* EC repair failure *アラートがトリガーされます。アラートに記載されている手順に従って、問題を解決します。

リストア履歴を表示します

[リストア履歴]*タブには、正常に完了したすべてのボリュームリストアに関する情報が表示されます。

> サイズはレプリケートオブジェクトには適用されず、イレイジャーコーディング（EC）データオブジェクトを含むリストアの場合にのみ表示されます。

StorageGRIDストレージノードシステムドライブの復元後にストレージの状態を確認する

ストレージノードのシステムドライブをリカバリしたら、ストレージノードに必要とされる状態が「 Online 」に設定されていることを確認し、ストレージノードサーバが再起動するたびにオンライン状態になるようにする必要があります。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- ストレージノードがリカバリされ、データリカバリが完了している必要があります。

手順

1. ノード > ストレージノード > *タスク*を選択します。
2. *ストレージ状態*ドロップダウンリストが読み取り専用またはオフラインに設定されている場合は、*オンライン*を選択します。
3. [保存（ Save ）] を選択します。

管理ノードの障害からリカバリ

StorageGRIDにおけるプライマリまたは非プライマリ管理ノードの復旧

管理ノードのリカバリプロセスは、プライマリ管理ノードと非プライマリ管理ノードで異なります。

プライマリまたは非プライマリ管理ノードのおおまかなリカバリ手順は同じですが、詳細は異なります。

リカバリ対象の管理ノードの正しいリカバリ手順 に必ず従ってください。手順の概要は同じように見えますが、詳細な手順は異なります。

選択肢

- "同じプライマリ管理ノードを使用してプライマリ管理ノードを復旧する"
- "プライマリ管理ノードの障害から非プライマリ管理ノードを使用して復旧する"
- "非プライマリ管理ノードの障害からリカバリします"

同じプライマリ管理ノードを使用してプライマリ管理ノードの障害から復旧する

同じプライマリ管理ノードを使用して StorageGRID プライマリ管理ノードをリカバリする

プライマリ管理ノードの障害からリカバリするには、特定のタスクを実行する必要があります。プライマリ管理ノードは、グリッドの Configuration Management Node （ CMN ）サービスをホストします。

> プライマリ管理ノードに障害が発生した場合は、速やかに修理または交換する必要があります。そうしないと、特定のメンテナンス手順を実行できなくなる可能性があります。

プライマリ管理ノードをリカバリするには、次の手順を実行します。

1. "障害が発生したプライマリ管理ノードから監査ログをコピーする"
2. "プライマリ管理ノードを交換"
3. "交換用プライマリ管理ノードの設定"
4. "リカバリされたプライマリ管理ノードにホットフィックスの要件があるかどうかを確認します。"
5. "リカバリされたプライマリ管理ノードで監査ログをリストアする"
6. "プライマリ管理ノードをリカバリする際の管理ノードデータベースのリストア"
7. "プライマリ管理ノードをリカバリする際にPrometheus指標をリストアする"

障害が発生した **StorageGRID** プライマリ管理ノードから監査ログをコピーする

障害が発生したプライマリ管理ノードから監査ログをコピーできる場合は、グリッドのシステムアクティビティと使用状況のレコードを維持するために監査ログを保存します。リカバリしたプライマリ管理ノードが起動したら、保存しておいた監査ログをそのノードにリストアします。

タスクの内容

この手順 は、障害が発生した管理ノードの監査ログファイルを別のグリッドノードの一時的な場所にコピーします。保存した監査ログは、交換用管理ノードにコピーできます。新しい管理ノードには監査ログが自動的にコピーされません。

障害の種類によっては、障害が発生した管理ノードから監査ログをコピーできない場合があります。管理ノードが 1 つしかない環境の場合、リカバリした管理ノードで新しい空のファイルの監査ログへのイベントの記録が開始され、以前に記録されたデータは失われます。管理ノードが複数ある環境の場合は、別の管理ノードから監査ログをリカバリできます。

> 現時点では障害管理ノードで監査ログにアクセスできない場合は、あとから（ホストのリカバリ後などに）アクセスできる可能性があります。

手順

1. 可能であれば、障害が発生したプライマリ管理ノードにログインします。それ以外の場合は、利用可能な管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
   b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

      rootとしてログインすると、プロンプトがからに `#`変わります `$`。
2. AMSサービスを停止して新しいログファイルが作成されないようにします。`service ams stop`
3. 監査エクスポートディレクトリに移動します。

   ```
   cd /var/local/audit/export
   ```

   （または `cd /var/local/log`以前のシステムの場合

4. ソース ログ ファイルの名前を一意の番号付きファイル名に変更します。

   - ログファイルが `/var/local/audit/export`ディレクトリの名前は `audit.log`。
   - ログファイルが `/var/local/log`ディレクトリの名前は `localaudit.log`。

   たとえば、 `localaudit.log`ファイルへ `2025-10-22.txt.1`。

   ```
   ls -l
   mv localaudit.log 2025-10-22.txt.1
   ```

5. AMSサービスを再起動します。 `service ams start`
6. すべての監査ログファイルを別のグリッドノードの一時的な場所にコピーするためのディレクトリを作成します。 `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

   プロンプトが表示されたら、 admin のパスワードを入力します。

7. すべての監査ログファイルを一時的な場所にコピーします。 `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

   プロンプトが表示されたら、 admin のパスワードを入力します。

8. rootとしてログアウトします。 `exit`

同じプライマリ管理ノードを使用して**StorageGRID**プライマリ管理ノードを交換する

プライマリ管理ノードをリカバリするには、まず物理または仮想ハードウェアの交換が必要です。

プライマリ管理ノードをリカバリするには、まず物理または仮想ハードウェアの交換が必要です。

- 障害が発生したプライマリ管理ノードは、同じプラットフォーム上で稼働しているプライマリ管理ノードに置き換えることができます。
- VMware または Linux ホスト上で実行されているプライマリ管理ノードを、StorageGRID サービスアプライアンスでホストされているプライマリ管理ノードに置き換えることができます。
- VMwareホスト上で稼働しているプライマリ管理ノードを、SG1000またはSG100サービスアプライアンスに置き換えることができます。

ノードに対して選択した交換用プラットフォームに一致する手順 を使用します。（すべてのノードタイプに適した）ノード交換手順 を完了すると、プライマリ管理ノードのリカバリに関する次のステップが手順 から表示されます。

交換用プラットフォーム	手順
VMware	"VMwareノードをリカバリノードに置き換える" "VMwareノードをSG1000またはSG100に交換する"
Linux	"Linux ノードを交換"
サービスアプライアンス	"サービスアプライアンスを交換します"
OpenStack	リカバリ処理を対象とした OpenStack 用の仮想マシンディスクファイルおよびスクリプトは、現在は提供されていません。OpenStack 環境で実行されているノードのリカバリが必要な場合は、使用している Linux オペレーティングシステム用のファイルをダウンロードしてください。次に、の手順に従います"Linuxノードの交換"。

StorageGRID で代替プライマリ管理ノードを構成します

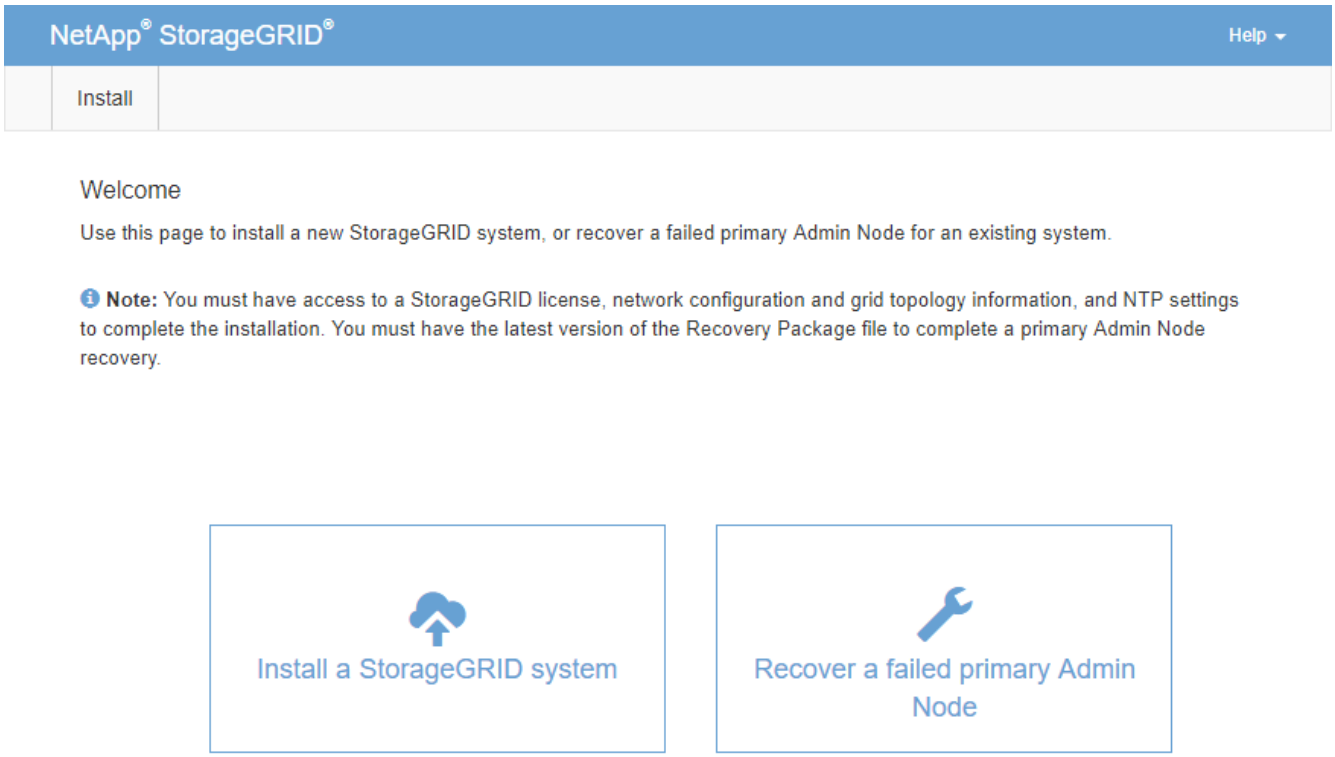
交換用ノードは、 StorageGRID システムのプライマリ管理ノードとして設定する必要があります。

開始する前に

- 仮想マシンでホストされているプライマリ管理ノードについて、仮想マシンを導入し、電源をオンにして初期化しておきます。
- サービスアプライアンスでホストされるプライマリ管理ノードの場合は、アプライアンスを交換し、ソフトウェアをインストールしておく必要があります。を参照してください "使用しているアプライアンスのインストール手順"。
- リカバリパッケージファイルの最新のバックアップがあります(`sgws-recovery-package-id-revision.zip`) 。
- プロビジョニングパスフレーズを用意します。

手順

1. Webブラウザを開き、に移動します `https://primary_admin_node_ip`。
2. 必要に応じて一時インストーラパスワードを管理します。
   - いずれかの方法ですでにパスワードが設定されている場合は、パスワードを入力して続行します。
     - ユーザが以前にインストーラにアクセスしているときにパスワードを設定した
     - ベアメタルシステムの場合、パスワードは次の場所にあるノード構成ファイルから自動的にインポートされます。 `/etc/storagegrid/nodes/<node_name>.conf`
     - VMの場合、OVFプロパティからSSH /コンソールパスワードが自動的にインポートされました。
   - パスワードが設定されていない場合は、必要に応じてStorageGRIDインストーラを保護するためのパスワードを設定します。
3. 障害が発生したプライマリ管理ノードを復旧する を選択します。



4. リカバリ パッケージの最新のバックアップをアップロードします。
   a. [* 参照 *] を選択します。
   b. お使いの StorageGRID システムの最新のリカバリパッケージファイルを見つけ、「開く」を選択します。
5. プロビジョニングパスフレーズを入力します。
6. 「リカバリを開始」を選択します。

   リカバリプロセスが開始されます。必要なサービスが開始されるまでの数分間、 Grid Manager を使用できなくなることがあります。リカバリが完了すると、サインインページが表示されます。

7. StorageGRID システムでシングルサインオン（ SSO ）が有効になっており、リカバリした管理ノードの証明書利用者信頼がデフォルトの管理インターフェイス証明書を使用するように設定されている場合は、ノードの証明書利用者信頼を Active Directory フェデレーションサービス（ AD FS ）で更新（削除および再作成）します。管理ノードのリカバリプロセス中に生成された新しいデフォルトサーバ証明書を使用します。

証明書利用者信頼を構成するには、"OIDC"または"SAML"を使用した SSO の設定を参照してください。デフォルトのサーバー証明書にアクセスするには、管理ノードのコマンドシェルにログインしてください。 `/var/local/mgmt-api`ディレクトリに移動し、 `server.crt`ファイルを選択します。

プライマリ管理ノードをリカバリしたら、"ホットフィックスの適用が必要かどうかを判断する"を実行します。

StorageGRIDのプライマリ管理ノードのホットフィックス要件を決定します

プライマリ管理ノードをリカバリしたら、ホットフィックスを適用する必要があるかどうかを確認します。

開始する前に

プライマリ管理ノードのリカバリが完了しました。

手順

1. を使用してGrid Managerにサインインし"サポートされている Web ブラウザ"ます。
2. *ノード*を選択します。
3. 左側のリストで、プライマリ管理ノードを選択します。
4. [概要] タブの [ソフトウェアバージョン] フィールドに表示されているバージョンを確認します。
5. 他のグリッドノードを選択します。
6. [概要] タブの [ソフトウェアバージョン] フィールドに表示されているバージョンを確認します。
   - [ソフトウェアバージョン]フィールドに表示されているバージョンが同じ場合は、ホットフィックスを適用する必要はありません。
   - [ソフトウェアバージョン]フィールドに表示されたバージョンが異なる場合は、リカバリしたプライマリ管理ノードを同じバージョンに更新する必要があり"ホットフィックスを適用します"ます。

復元された **StorageGRID** プライマリ管理ノードの監査ログを復元する

障害が発生したプライマリ管理ノードから監査ログを保存できた場合は、リカバリするプライマリ管理ノードにそのログをコピーできます。

開始する前に

- リカバリした管理ノードがインストールされて実行されている。
- 元の管理ノードで障害が発生したあとに、監査ログを別の場所にコピーしておきます。

タスクの内容

管理ノードで障害が発生すると、その管理ノードに保存された監査ログが失われる可能性があります。障害が発生した管理ノードから監査ログをコピーし、リカバリされた管理ノードにリストアすることで、データを損失から守ることができる場合があります。障害によっては、障害が発生した管理ノードから監査ログをコピーできない場合があります。その場合、管理ノードが複数ある環境ではすべての管理ノードに監査ログがレプリケートされるため、別の管理ノードから監査ログをリカバリできます。

管理ノードが1つしかなく、障害ノードから監査ログをコピーできない場合は、リカバリされた管理ノードで、新規インストールの場合と同様に監査ログへのイベントの記録が開始されます。

ロギング機能を復旧させるために、管理ノードはできるだけ早くリカバリする必要があります。

デフォルトでは、監査情報は管理ノードの監査ログに送信されます。次のいずれかに該当する場合は、これらの手順をスキップしてかまいません。

- 外部 syslog サーバを設定し、管理ノードではなく syslog サーバに監査ログを送信するようになりました。
- 監査メッセージを生成したローカルノードにのみ保存するように明示的に指定します。

見る"ログ管理と外部Syslogサーバーを構成する"詳細については。

手順

1. リカバリした管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@recovery_Admin_Node_IP`
   b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

   rootとしてログインすると、プロンプトがからに `#`変わります `$`。
2. 保存された監査ファイルを確認します。 `cd /var/local/audit/export`
3. 保持されている監査ログファイルをリカバリした管理ノードにコピーします。 `scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY* .`

   プロンプトが表示されたら、 admin のパスワードを入力します。
4. セキュリティ上の理由により、監査ログがリカバリされた管理ノードにコピーされたことを確認したら、監査ログを障害グリッドノードから削除します。
5. 回復された管理ノード上の監査ログ ファイルのユーザーとグループの設定を更新します。 `chown ams-user:bycast *`
6. rootとしてログアウトします。 `exit`

プライマリ管理ノードの復旧時に**StorageGRID**管理ノードデータベースをリストアする

障害が発生したプライマリ管理ノード上の属性とアラートの履歴情報を保持するには、管理ノードデータベースをリストアします。このデータベースをリストアできるのは、StorageGRID システムに別の管理ノードがある場合のみです。

開始する前に

- リカバリした管理ノードがインストールされて実行されている。
- StorageGRID システムには少なくとも2つの管理ノードが含まれています。
- あなたはファイルを持ってい `Passwords.txt`ます。
- プロビジョニングパスフレーズを用意します。

タスクの内容

管理ノードで障害が発生すると、その管理ノードデータベースに格納されていた履歴情報が失われます。この

データベースには次の情報が含まれています。

- アラートの履歴
- 属性データの履歴（[Nodes]ページの従来のグラフで使用）

管理ノードをリカバリする際に、ソフトウェアのインストールプロセスによって、リカバリしたノードに空の管理ノードデータベースが作成されます。ただし、新しいデータベースには、現在システムに含まれているサーバとサービス、またはあとで追加されたサーバの情報だけが含まれます。

プライマリ管理ノードをリストアした StorageGRID システムに別の管理ノードがある場合は、プライマリでない管理ノード（ *source Admin Nod* ）の管理ノードデータベースをリカバリしたプライマリ管理ノードにコピーすることで、履歴情報をリストアできます。システムにプライマリ管理ノードしかない場合は、管理ノードデータベースをリストアできません。

管理ノードデータベースのコピーには数時間かかることがあります。ソース管理ノードでサービスが停止している間は、グリッドマネージャの一部の機能が使用できなくなります。

手順

1. ソース管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
   b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。
2. ソース管理ノードから、MIサービスを停止します。 `service mi stop`
3. ソース管理ノードから、管理アプリケーションプログラムインターフェイス（mgmt-api）サービスを停止します。 `service mgmt-api stop`
4. リカバリした管理ノードで次の手順を実行します。
   a. リカバリした管理ノードにログインします。
      i. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
      ii. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。
      iii. 次のコマンドを入力してrootに切り替えます。 `su -`
      iv. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。
   b. MIサービスを停止します。 `service mi stop`
   c. mgmt-apiサービスを停止します。 `service mgmt-api stop`
   d. SSH エージェントに SSH 秘密鍵を追加します。入力：`ssh-add`
   e. ファイルに記載されているSSHアクセスパスワードを入力し `Passwords.txt`ます。
   f. プロンプトが表示されたら、リカバリした管理ノードで MI データベースを上書きすることを確定します。

      データベースとその履歴データが、リカバリした管理ノードにコピーされます。コピー処理が完了すると、リカバリした管理ノードがスクリプトによって起動されます。

g. 他のサーバにパスワードなしでアクセスする必要がなくなった場合は、 SSH エージェントから秘密鍵を削除します。入力：`ssh-add -D`

5. ソース管理ノードでサービスを再起動します。 `service servermanager start`

StorageGRID プライマリ管理ノードのリカバリ時に Prometheus メトリクスを復元する

プライマリ管理ノードで障害が発生した場合、そのノード上の Prometheus で管理されていた過去の指標を必要に応じてリストアすることができます。Prometheus 指標をリストアできるのは、 StorageGRID システムに別の管理ノードがある場合のみです。

開始する前に

- リカバリした管理ノードがインストールされて実行されている。
- StorageGRID システムには少なくとも2つの管理ノードが含まれています。
- あなたはファイルを持ってい `Passwords.txt`ます。
- プロビジョニングパスフレーズを用意します。

タスクの内容

管理ノードで障害が発生すると、 Prometheus データベースで管理されていた管理ノード上の指標は失われます。管理ノードをリカバリする際に、ソフトウェアのインストールプロセスによって新しい Prometheus データベースが作成されます。リカバリした管理ノードを起動すると、 StorageGRID システムを新規にインストールした場合と同様に指標が記録されます。

プライマリ管理ノードをリストアした StorageGRID システムに別の管理ノードがある場合は、プライマリでない管理ノード（ _SOURCE 管理ノード）の Prometheus データベースをリカバリしたプライマリ管理ノードにコピーすることで、過去の指標をリストアできます。システムにプライマリ管理ノードしかない場合は、Prometheusデータベースをリストアできません。

> Prometheus データベースのコピーには 1 時間以上かかる場合があります。ソース管理ノードでサービスが停止している間は、グリッドマネージャの一部の機能が使用できなくなります。

手順

1. ソース管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
   b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。
2. ソース管理ノードからPrometheusサービスを停止します。 `service prometheus stop`
3. リカバリした管理ノードで次の手順を実行します。
   a. リカバリした管理ノードにログインします。
      i. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
      ii. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。
      iii. 次のコマンドを入力してrootに切り替えます。 `su -`

iv. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

b. Prometheusサービスを停止します。 `service prometheus stop`

c. SSH エージェントに SSH 秘密鍵を追加します。入力：`ssh-add`

d. ファイルに記載されているSSHアクセスパスワードを入力し `Passwords.txt`ます。

e. ソース管理ノードのPrometheusデータベースをリカバリした管理ノードにコピーします。
`/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`

f. プロンプトが表示されたら、 * Enter * を押して、リカバリした管理ノード上の新しい Prometheus データベースを破棄することを確認します。

元の Prometheus データベースとその履歴データが、リカバリした管理ノードにコピーされます。コピー処理が完了すると、リカバリした管理ノードがスクリプトによって起動されます。次のステータスが表示されます。

データベースのクローニング、サービスの開始

a. 他のサーバにパスワードなしでアクセスする必要がなくなった場合は、 SSH エージェントから秘密鍵を削除します。入力：`ssh-add -D`

4. ソース管理ノードでPrometheusサービスを再起動します。`.service prometheus start`

プライマリ管理ノードの障害から非プライマリ管理ノードを使用して復旧する

プライマリ以外の管理ノードを使用して **StorageGRID** プライマリ管理ノードの障害から回復する

プライマリ管理ノードの障害から非プライマリ管理ノードを使用して復旧するには、特定の一連のタスクを完了する必要があります。プライマリ管理ノードは、グリッドの構成管理ノード（CMN）サービスをホストします。

非プライマリ管理ノードを使用してプライマリ管理ノードを復旧するための概要手順は次のとおりです：

1. "障害が発生したプライマリ管理ノードから監査ログをコピーする"
2. "プライマリ管理ノードを交換"
3. "プライマリ管理ノードを構成するには、「リカバリの開始」を選択してください。"
4. "プライマリ管理ノードのホットフィックスの要件を確認"
5. "リカバリされたプライマリ管理ノードで監査ログをリストアする"
6. "プライマリ管理ノードをリカバリする際の Prometheus 指標のリストア"

障害が発生したプライマリ管理ノードから**StorageGRID**監査ログをコピーする

障害が発生したプライマリ管理ノードから監査ログをコピーできる場合は、グリッドのシステムアクティビティと使用状況のレコードを維持するために監査ログを保存します。リカバリしたプライマリ管理ノードが起動したら、保存しておいた監査ログをそのノードにリストアします。

タスクの内容

この手順 は、障害が発生した管理ノードの監査ログファイルを別のグリッドノードの一時的な場所にコピーします。保存した監査ログは、交換用管理ノードにコピーできます。新しい管理ノードには監査ログが自動的にコピーされません。

障害の種類によっては、障害が発生した管理ノードから監査ログをコピーできない場合があります。管理ノードが 1 つしかない環境の場合、リカバリした管理ノードで新しい空のファイルの監査ログへのイベントの記録が開始され、以前に記録されたデータは失われます。管理ノードが複数ある環境の場合は、別の管理ノードから監査ログをリカバリできます。

> ⓘ 現時点では障害管理ノードで監査ログにアクセスできない場合は、あとから（ホストのリカバリ後などに）アクセスできる可能性があります。

手順

1. 可能であれば、障害が発生したプライマリ管理ノードにログインします。それ以外の場合は、利用可能な管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
   b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。
   c. ルートユーザーアカウントに切り替えるには、次のコマンドを入力してください： `su -`
   d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

      rootとしてログインすると、プロンプトがからに `#`変わります `$`。
2. AMSサービスを停止して新しいログファイルが作成されないようにします。`service ams stop`
3. 監査エクスポートディレクトリに移動します。

   ```
   cd /var/local/audit/export
   ```

   （または `cd /var/local/log`以前のシステムの場合
4. ソース ログ ファイルの名前を一意の番号付きファイル名に変更します。

   > ⓘ
   > - ログファイルが `/var/local/audit/export`ディレクトリの名前は `audit.log`。
   > - ログファイルが `/var/local/log`ディレクトリの名前は `localaudit.log`。

   たとえば、 `localaudit.log`ファイルへ `2025-10-22.txt.1`。

   ```
   ls -l
   mv localaudit.log 2025-10-22.txt.1
   ```
5. AMSサービスを再起動します。 `service ams start`
6. すべての監査ログファイルを別のグリッドノードの一時的な場所にコピーするためのディレクトリを作成します。 `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

   プロンプトが表示されたら、管理者ユーザーアカウントのパスワードを入力してください。

7. すべての監査ログファイルを一時的な場所にコピーします。 `scp -p * admin@ grid_node_IP:/var/local/tmp/saved-audit-logs`

   プロンプトが表示されたら、管理者ユーザーアカウントのパスワードを入力してください。

8. rootユーザーとしてログアウトします： `exit`。

非プライマリ管理ノードを使用して**StorageGRID**プライマリ管理ノードを交換する

プライマリ管理ノードをリカバリするには、まず物理または仮想ハードウェアの交換が必要です。

- 障害が発生したプライマリ管理ノードは、同じプラットフォーム上で稼働しているプライマリ管理ノードに置き換えることができます。
- VMware または Linux ホスト上で実行されているプライマリ管理ノードを、StorageGRID サービスアプライアンスでホストされているプライマリ管理ノードに置き換えることができます。
- VMwareホスト上で稼働しているプライマリ管理ノードを、SG1000またはSG100サービスアプライアンスに置き換えることができます。

ノードに対して選択した交換用プラットフォームに一致する手順 を使用します。（すべてのノードタイプに適した）ノード交換手順 を完了すると、プライマリ管理ノードのリカバリに関する次のステップが手順 から表示されます。

交換用プラットフォーム	手順
VMware	"VMwareノードをリカバリノードに置き換える" "VMwareノードをSG1000またはSG100サービスアプライアンスに置き換える"
Linux	"Linux ノードを交換"
サービスアプライアンス	"サービスアプライアンスを交換します"
OpenStack	リカバリ処理を対象とした OpenStack 用の仮想マシンディスクファイルおよびスクリプトは、現在は提供されていません。OpenStack 環境で実行されているノードのリカバリが必要な場合は、使用している Linux オペレーティングシステム用のファイルをダウンロードしてください。次に、の手順に従います"Linuxノードの交換"。

プライマリ管理ノードを設定するには、「リカバリの開始」を選択します。

プライマリ管理ノードを交換した後は、Grid Manager で「Start Recovery」を選択し、新しいノードを障害が発生したノードの代替として構成する必要があります。

開始する前に

- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。

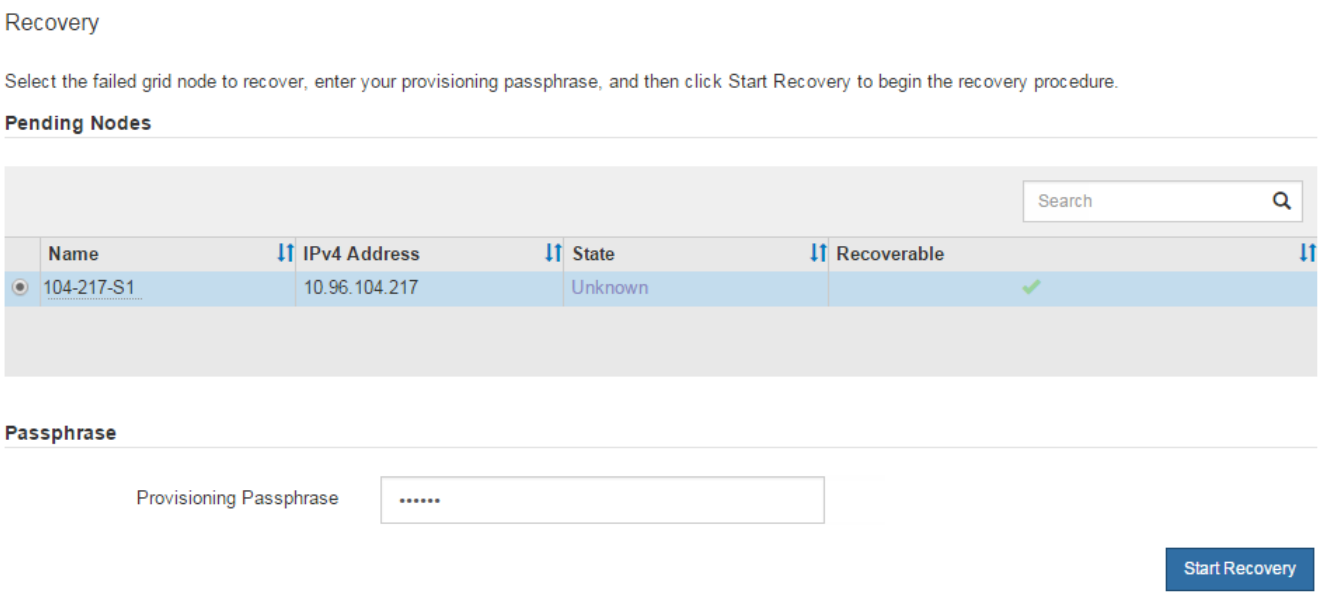
- あなたはを持っています"Maintenance権限またはRoot Access権限"。
- プロビジョニングパスフレーズを用意します。
- 交換用ノードの導入と設定を完了しておきます。

手順

1. グリッドマネージャから、メンテナンス > タスク > *ノード復旧*を選択します。
2. リカバリするグリッドノードを Pending Nodes リストで選択します。

   ノードに障害が発生するとリストに表示されますが、ノードを再インストールしてリカバリの準備ができるまでは選択できません。

3. **Provisioning passphrase** を入力してください。
4. 「リカバリを開始」を選択します。



5. リカバリ中のグリッドノードテーブルで、リカバリの進行状況を監視します。

   復旧処理の実行中に、*リセット*を選択すると、新しい復旧処理を開始できます。手順をリセットするとノードが不確定な状態になることを示すダイアログボックスが表示されます。

   手順 をリセットしたあとにリカバリを再試行する場合は、次の手順でノードをインストール前の状態にリストアする必要があります。

   - * vmware * ：導入した仮想グリッドノードを削除します。その後、リカバリを再開する準備ができたら、ノードを再導入します。
   - * Linux *：Linuxホストで次のコマンドを実行してノードを再起動します。 `storagegrid node force-recovery node-name`
   - アプライアンス：手順をリセットしたあとにリカバリを再試行する場合は、ノードでを実行してアプライアンスノードをインストール前の状態にリストアする必要があります `sgareinstall`。を参照して "再インストールのためのアプライアンスの準備（プラットフォームの交換のみ）"

6. StorageGRID システムでシングルサインオン（ SSO ）が有効になっており、リカバリした管理ノードの証明書利用者信頼がデフォルトの管理インターフェイス証明書を使用するように設定されている場合は、ノードの証明書利用者信頼を Active Directory フェデレーションサービス（ AD FS ）で更新（削除および再作成）します。管理ノードのリカバリプロセス中に生成された新しいデフォルトサーバ証明書を使用します。

> 証明書利用者信頼を構成するには、"シングルサインオンを設定します" 。デフォルトのサーバー証明書にアクセスするには、管理ノードのコマンド シェルにログインします。に行く `/var/local/mgmt-api`ディレクトリを選択し、 `server.crt`ファイル。

プライマリ管理ノードの **StorageGRID** ホットフィックス要件の確認

プライマリ管理ノードを復旧した後、ホットフィックスを適用する必要があるかどうかを判断してください。

開始する前に

プライマリ管理ノードの復旧が完了しました。

手順

1. を使用してGrid Managerにサインインし"サポートされている Web ブラウザ"ます。
2. *ノード*を選択します。
3. 左側のリストで、プライマリ管理ノードを選択します。
4. [概要] タブの [ソフトウェアバージョン] フィールドに表示されているバージョンを確認します。
5. 他のグリッドノードを選択します。
6. 概要タブで、*ソフトウェアバージョン*フィールドに表示されているバージョンを確認してください。
   - [ソフトウェアバージョン]フィールドに表示されているバージョンが同じ場合は、ホットフィックスを適用する必要はありません。
   - [ソフトウェアバージョン]フィールドに表示されたバージョンが異なる場合は、リカバリしたプライマリ管理ノードを同じバージョンに更新する必要があり"ホットフィックスを適用します"ます。

復旧したプライマリ管理ノードの**StorageGRID**監査ログを復元する

障害が発生したプライマリ管理ノードから監査ログを保存できた場合は、リカバリするプライマリ管理ノードにそのログをコピーできます。

開始する前に

- リカバリした管理ノードがインストールされて実行されている。
- 元の管理ノードで障害が発生したあとに、監査ログを別の場所にコピーしておきます。

タスクの内容

管理ノードで障害が発生すると、その管理ノードに保存された監査ログが失われる可能性があります。障害が発生した管理ノードから監査ログをコピーし、リカバリされた管理ノードにリストアすることで、データを損失から守ることができる場合があります。障害によっては、障害が発生した管理ノードから監査ログをコピーできない場合があります。その場合、管理ノードが複数ある環境ではすべての管理ノードに監査ログがレプリケートされるため、別の管理ノードから監査ログをリカバリできます。

管理ノードが1つしかなく、障害ノードから監査ログをコピーできない場合は、リカバリされた管理ノードで、新規インストールの場合と同様に監査ログへのイベントの記録が開始されます。

ロギング機能を復旧させるために、管理ノードはできるだけ早くリカバリする必要があります。

> デフォルトでは、監査情報は管理ノードの監査ログに送信されます。次のいずれかに該当する場合は、これらの手順をスキップしてかまいません。
>
> - 外部 syslog サーバを設定し、管理ノードではなく syslog サーバに監査ログを送信するようになりました。
> - 監査メッセージを生成したローカルノードにのみ保存するように明示的に指定します。
>
> 見る"ログ管理と外部Syslogサーバーを構成する"詳細については。

手順

1. リカバリした管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@recovery_Admin_Node_IP`
   b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

   rootとしてログインすると、プロンプトがからに `#`変わります `$`。
2. 保存された監査ファイルを確認します。 `cd /var/local/audit/export`
3. 保持されている監査ログファイルをリカバリした管理ノードにコピーします。 `scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY* .`

   プロンプトが表示されたら、 admin のパスワードを入力します。
4. セキュリティ上の理由により、監査ログがリカバリされた管理ノードにコピーされたことを確認したら、監査ログを障害グリッドノードから削除します。
5. 回復された管理ノード上の監査ログ ファイルのユーザーとグループの設定を更新します。 `chown ams-user:bycast *`
6. rootとしてログアウトします。 `exit`

StorageGRID プライマリ管理ノードの復旧時に **Prometheus** メトリクスを復元する

プライマリ管理ノードで障害が発生した場合、そのノード上の Prometheus で管理されていた過去の指標を必要に応じてリストアすることができます。Prometheus 指標をリストアできるのは、 StorageGRID システムに別の管理ノードがある場合のみです。

開始する前に

- リカバリした管理ノードがインストールされて実行されている。
- StorageGRID システムには少なくとも2つの管理ノードが含まれています。
- あなたはファイルを持ってい `Passwords.txt`ます。

- プロビジョニングパスフレーズを用意します。

タスクの内容

管理ノードで障害が発生すると、 Prometheus データベースで管理されていた管理ノード上の指標は失われます。管理ノードをリカバリする際に、ソフトウェアのインストールプロセスによって新しい Prometheus データベースが作成されます。リカバリした管理ノードを起動すると、 StorageGRID システムを新規にインストールした場合と同様に指標が記録されます。

プライマリ管理ノードをリストアした StorageGRID システムに別の管理ノードがある場合は、プライマリでない管理ノード（ _SOURCE 管理ノード）の Prometheus データベースをリカバリしたプライマリ管理ノードにコピーすることで、過去の指標をリストアできます。システムにプライマリ管理ノードしかない場合は、Prometheusデータベースをリストアできません。

> Prometheus データベースのコピーには 1 時間以上かかる場合があります。ソース管理ノードでサービスが停止している間は、グリッドマネージャの一部の機能が使用できなくなります。

手順

1. ソース管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
   b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。
2. ソース管理ノードからPrometheusサービスを停止します。 `service prometheus stop`
3. リカバリした管理ノードで次の手順を実行します。
   a. リカバリした管理ノードにログインします。
      i. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
      ii. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。
      iii. 次のコマンドを入力してrootに切り替えます。 `su -`
      iv. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。
   b. Prometheusサービスを停止します。 `service prometheus stop`
   c. SSH エージェントに SSH 秘密鍵を追加します。入力：`ssh-add`
   d. ファイルに記載されているSSHアクセスパスワードを入力し `Passwords.txt`ます。
   e. ソース管理ノードのPrometheusデータベースをリカバリした管理ノードにコピーします。
      `/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`
   f. プロンプトが表示されたら、 * Enter * を押して、リカバリした管理ノード上の新しい Prometheus データベースを破棄することを確認します。

      元の Prometheus データベースとその履歴データが、リカバリした管理ノードにコピーされます。コピー処理が完了すると、リカバリした管理ノードがスクリプトによって起動されます。次のステータスが表示されます。

   データベースのクローニング、サービスの開始

a. 他のサーバにパスワードなしでアクセスする必要がなくなった場合は、 SSH エージェントから秘密鍵を削除します。入力：`ssh-add -D`

4. ソース管理ノードでPrometheusサービスを再起動します。`.service prometheus start`

非プライマリ管理ノードの障害からリカバリします

StorageGRID 非プライマリ管理ノードの障害からの回復

非プライマリ管理ノードの障害からリカバリするには、次のタスクを実行する必要があります。1 つの管理ノードが Configuration Management Node （ CMN ）サービスをホストしており、これをプライマリ管理ノードと呼びます。管理ノードを複数使用することはできますが、 StorageGRID システムごとに配置できるプライマリ管理ノードは 1 つだけです。それ以外の管理ノードはすべて非プライマリ管理ノードです。

非プライマリ管理ノードをリカバリするには、次の手順を実行します。

1. "障害が発生した非プライマリ管理ノードから監査ログをコピーする"
2. "非プライマリ管理ノードの交換"
3. "[Start Recoveryを選択して非プライマリ管理ノードを設定"]
4. "リカバリされた非プライマリ管理ノードで監査ログをリストアする"
5. "非プライマリ管理ノードをリカバリする際の管理ノードデータベースのリストア"
6. "非プライマリ管理ノードをリカバリする際のPrometheus指標のリストア"

障害が発生した **StorageGRID** 非プライマリ管理ノードから監査ログをコピーする

障害が発生した管理ノードから監査ログをコピーできる場合は、グリッドのシステムアクティビティと使用状況のレコードを維持するために監査ログを保存します。リカバリした非プライマリ管理ノードが起動したら、保存しておいた監査ログをそのノードにリストアします。

この手順 は、障害が発生した管理ノードの監査ログファイルを別のグリッドノードの一時的な場所にコピーします。保存した監査ログは、交換用管理ノードにコピーできます。新しい管理ノードには監査ログが自動的にコピーされません。

障害の種類によっては、障害が発生した管理ノードから監査ログをコピーできない場合があります。管理ノードが 1 つしかない環境の場合、リカバリした管理ノードで新しい空のファイルの監査ログへのイベントの記録が開始され、以前に記録されたデータは失われます。管理ノードが複数ある環境の場合は、別の管理ノードから監査ログをリカバリできます。

> 現時点では障害管理ノードで監査ログにアクセスできない場合は、あとから（ホストのリカバリ後などに）アクセスできる可能性があります。

1. 可能であれば、障害管理ノードにログインします。できない場合は、プライマリ管理ノードまたは別の管理ノードにログインします。

   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`

b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

c. 次のコマンドを入力してrootに切り替えます。 `su -`

d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

rootとしてログインすると、プロンプトがからに `#`変わります `$`。

2. AMSサービスを停止して新しいログファイルが作成されないようにします。`service ams stop`
3. 監査エクスポートディレクトリに移動します。

   ```
   cd /var/local/audit/export/
   ```

4. ソースaudit.logファイルの名前を一意の番号付きファイル名に変更します。たとえば、audit.logファイルの名前をに変更し `2023-10-25.txt.1`ます。

   ```
   ls -l
   mv audit.log 2023-10-25.txt.1
   ```

5. AMSサービスを再起動します。 `service ams start`
6. すべての監査ログファイルを別のグリッドノードの一時的な場所にコピーするためのディレクトリを作成します。 `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

   プロンプトが表示されたら、 admin のパスワードを入力します。

7. すべての監査ログファイルを一時的な場所にコピーします。 `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

   プロンプトが表示されたら、 admin のパスワードを入力します。

8. rootとしてログアウトします。 `exit`

StorageGRID 非プライマリ管理ノードの交換

非プライマリ管理ノードをリカバリするには、まず物理または仮想ハードウェアの交換が必要です。

障害が発生した非プライマリ管理ノードを同じプラットフォームで実行されている非プライマリ管理ノードと交換することも、 VMware または Linux ホストで実行されている非プライマリ管理ノードをサービスアプライアンスでホストされている非プライマリ管理ノードと交換することもできます。

ノードに対して選択した交換用プラットフォームに一致する手順 を使用します。（すべてのノードタイプに適した）ノード交換手順 を完了すると、非プライマリ管理ノードのリカバリに関する次の手順がその手順 から指示されます。

交換用プラットフォーム	手順
VMware	"VMware ノードを交換"

交換用プラットフォーム	手順
Linux	"Linux ノードを交換"
サービスアプライアンス	"サービスアプライアンスを交換します"
OpenStack	リカバリ処理を対象とした OpenStack 用の仮想マシンディスクファイルおよびスクリプトは、現在は提供されていません。OpenStack 環境で実行されているノードのリカバリが必要な場合は、使用している Linux オペレーティングシステム用のファイルをダウンロードしてください。次に、の手順に従いますLinuxノードの交換"。

「**Start Recovery**」を選択して、**StorageGRID** 非プライマリ管理ノードを設定します

非プライマリ管理ノードを交換したら、 Grid Manager で Start Recovery を選択して、新しいノードを障害ノードの代わりとして設定する必要があります。

開始する前に

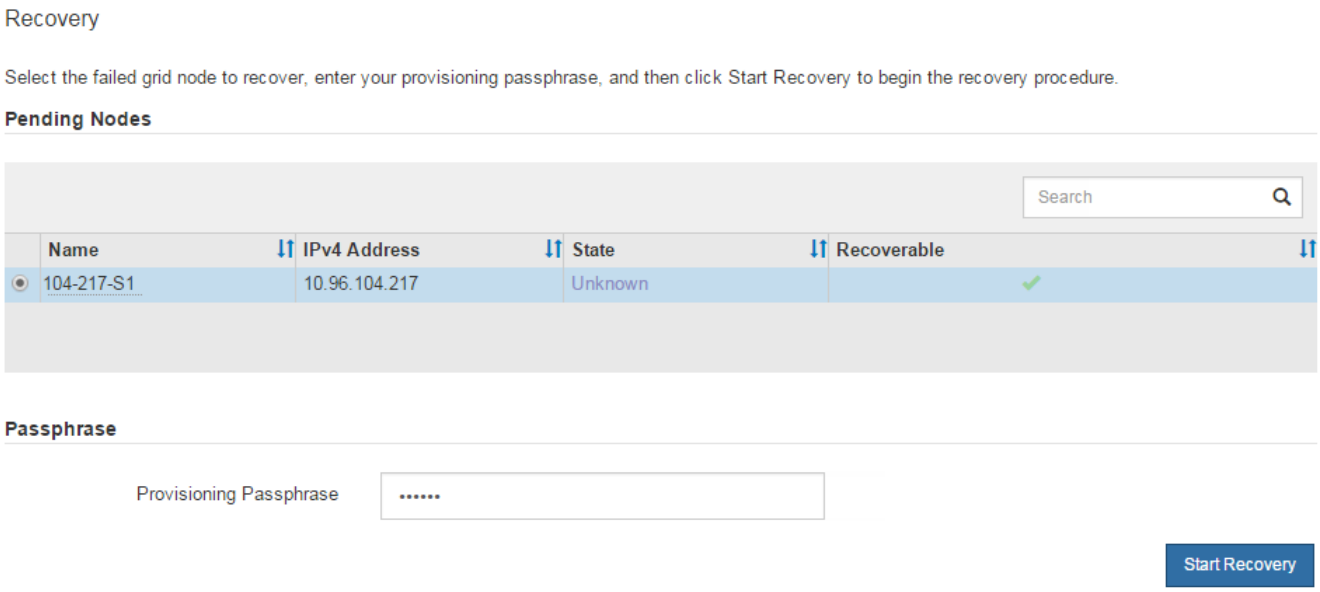
- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"Maintenance権限またはRoot Access権限"。
- プロビジョニングパスフレーズを用意します。
- 交換用ノードの導入と設定を完了しておきます。

手順

1. グリッドマネージャから、メンテナンス > タスク > *ノード復旧*を選択します。
2. リカバリするグリッドノードを Pending Nodes リストで選択します。

   ノードに障害が発生するとリストに表示されますが、ノードを再インストールしてリカバリの準備ができるまでは選択できません。

3. **Provisioning passphrase** を入力してください。
4. 「リカバリを開始」を選択します。



5. リカバリ中のグリッドノードテーブルで、リカバリの進行状況を監視します。

   復旧処理の実行中に、*リセット*を選択すると、新しい復旧処理を開始できます。手順をリセットするとノードが不確定な状態になることを示すダイアログボックスが表示されます。

   手順 をリセットしたあとにリカバリを再試行する場合は、次の手順でノードをインストール前の状態にリストアする必要があります。

   - * vmware * ：導入した仮想グリッドノードを削除します。その後、リカバリを再開する準備ができたら、ノードを再導入します。
   - * Linux *：Linuxホストで次のコマンドを実行してノードを再起動します。 `storagegrid node force-recovery node-name`
   - アプライアンス：手順をリセットしたあとにリカバリを再試行する場合は、ノードでを実行してアプライアンスノードをインストール前の状態にリストアする必要があります `sgareinstall`。を参照して "再インストールのためのアプライアンスの準備（プラットフォームの交換のみ）"

6. StorageGRID システムでシングルサインオン（ SSO ）が有効になっており、リカバリした管理ノードの証明書利用者信頼がデフォルトの管理インターフェイス証明書を使用するように設定されている場合は、ノードの証明書利用者信頼を Active Directory フェデレーションサービス（ AD FS ）で更新（削除および再作成）します。管理ノードのリカバリプロセス中に生成された新しいデフォルトサーバ証明書を使用します。

   証明書利用者信頼を構成するには、"シングルサインオンを設定します" 。デフォルトのサーバー証明書にアクセスするには、管理ノードのコマンド シェルにログインします。に行く `/var/local/mgmt-api`ディレクトリを選択し、 `server.crt`ファイル。

復元された **StorageGRID** 非プライマリ管理ノードの監査ログを復元する

障害が発生した非プライマリ管理ノードから監査ログを保存できたために監査ログの履歴情報が保持されている場合は、リカバリする非プライマリ管理ノードにその情報をコピーできます。

開始する前に

- リカバリした管理ノードがインストールされて実行されている。
- 元の管理ノードで障害が発生したあとに、監査ログを別の場所にコピーしておきます。

タスクの内容

管理ノードで障害が発生すると、その管理ノードに保存された監査ログが失われる可能性があります。障害が発生した管理ノードから監査ログをコピーし、リカバリされた管理ノードにリストアすることで、データを損失から守ることができる場合があります。障害によっては、障害が発生した管理ノードから監査ログをコピーできない場合があります。その場合、管理ノードが複数ある環境ではすべての管理ノードに監査ログがレプリケートされるため、別の管理ノードから監査ログをリカバリできます。

管理ノードが1つしかなく、障害ノードから監査ログをコピーできない場合は、リカバリされた管理ノードで、新規インストールの場合と同様に監査ログへのイベントの記録が開始されます。

ロギング機能を復旧させるために、管理ノードはできるだけ早くリカバリする必要があります。

> デフォルトでは、監査情報は管理ノードの監査ログに送信されます。次のいずれかに該当する場合は、これらの手順をスキップしてかまいません。
>
> - 外部 syslog サーバを設定し、管理ノードではなく syslog サーバに監査ログを送信するようになりました。
> - 監査メッセージを生成したローカルノードにのみ保存するように明示的に指定します。
>
> 見る"ログ管理と外部Syslogサーバーを構成する"詳細については。

手順

1. リカバリした管理ノードにログインします。

   a. 次のコマンドを入力します。+
   `ssh admin@recovery_Admin_Node_IP`

   b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

   c. 次のコマンドを入力してrootに切り替えます。 `su -`

   d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

   rootとしてログインすると、プロンプトがからに `#`変わります `$`。

2. 保持されている監査ファイルを確認します。

   ```
   cd /var/local/log
   ```

3. 保持されている監査ログファイルをリカバリされた管理ノードにコピーします。

   ```
   scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY*
   ```

   プロンプトが表示されたら、 admin のパスワードを入力します。

4. セキュリティ上の理由により、監査ログがリカバリされた管理ノードにコピーされたことを確認したら、監査ログを障害グリッドノードから削除します。

5. リカバリされた管理ノードで、監査ログファイルのユーザとグループの設定を更新します。

```
chown ams-user:bycast *
```

6. rootとしてログアウトします。 `exit`

プライマリ以外の管理ノードを復旧する際に**StorageGRID**管理ノードデータベースをリストアする

障害が発生した非プライマリ管理ノード上の属性とアラートの履歴情報を保持するには、プライマリ管理ノードから管理ノードデータベースをリストアします。

開始する前に

- リカバリした管理ノードがインストールされて実行されている。
- StorageGRID システムには少なくとも2つの管理ノードが含まれています。
- あなたはファイルを持ってい `Passwords.txt`ます。
- プロビジョニングパスフレーズを用意します。

タスクの内容

管理ノードで障害が発生すると、その管理ノードデータベースに格納されていた履歴情報が失われます。このデータベースには次の情報が含まれています。

- アラートの履歴
- ノードページのグラフで使用される履歴属性データ

管理ノードをリカバリする際に、ソフトウェアのインストールプロセスによって、リカバリしたノードに空の管理ノードデータベースが作成されます。ただし、新しいデータベースには、現在システムに含まれているサーバとサービス、またはあとで追加されたサーバの情報だけが含まれます。

非プライマリ管理ノードをリストアした場合は、プライマリ管理ノード（ *source Admin Node*） の管理ノードデータベースをリカバリしたノードにコピーすることで、履歴情報をリストアできます。

> 管理ノードデータベースのコピーには数時間かかることがあります。ソースノードでサービスが停止している間は、 Grid Manager の一部の機能が使用できなくなります。

手順

1. ソース管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
   b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。
2. ソース管理ノードから次のコマンドを実行します。プロンプトが表示されたら、プロビジョニングパスフレーズを入力します。 `recover-access-points`
3. ソース管理ノードから、MIサービスを停止します。 `service mi stop`
4. ソース管理ノードから、管理アプリケーションプログラムインターフェイス（mgmt-api）サービスを停止

します。 `service mgmt-api stop`

5. リカバリした管理ノードで次の手順を実行します。
   a. リカバリした管理ノードにログインします。
      i. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
      ii. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。
      iii. 次のコマンドを入力してrootに切り替えます。 `su -`
      iv. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。
   b. MIサービスを停止します。 `service mi stop`
   c. mgmt-apiサービスを停止します。 `service mgmt-api stop`
   d. SSH エージェントに SSH 秘密鍵を追加します。入力：`ssh-add`
   e. ファイルに記載されているSSHアクセスパスワードを入力し `Passwords.txt`ます。
   f. 他のサーバにパスワードなしでアクセスする必要がなくなった場合は、 SSH エージェントから秘密鍵を削除します。入力：`ssh-add -D`
6. ソース管理ノードでサービスを再起動します。 `service servermanager start`

StorageGRID 非プライマリ管理ノードのリカバリ時に **Prometheus** メトリクスを復元する

非プライマリ管理ノードで障害が発生した場合、そのノード上の Prometheus で管理されていた過去の指標を必要に応じてリストアすることができます。

開始する前に

- リカバリした管理ノードがインストールされて実行されている。
- StorageGRID システムには少なくとも2つの管理ノードが含まれています。
- あなたはファイルを持ってい `Passwords.txt`ます。
- プロビジョニングパスフレーズを用意します。

タスクの内容

管理ノードで障害が発生すると、 Prometheus データベースで管理されていた管理ノード上の指標は失われます。管理ノードをリカバリする際に、ソフトウェアのインストールプロセスによって新しい Prometheus データベースが作成されます。リカバリした管理ノードを起動すると、 StorageGRID システムを新規にインストールした場合と同様に指標が記録されます。

非プライマリ管理ノードをリストアした場合は、プライマリ管理ノード（ *source Admin Node*） の Prometheus データベースをリカバリした管理ノードにコピーすることで、過去の指標をリストアできます。

> Prometheus データベースのコピーには 1 時間以上かかる場合があります。ソース管理ノードでサービスが停止している間は、グリッドマネージャの一部の機能が使用できなくなります。

手順

1. ソース管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`

b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

c. 次のコマンドを入力してrootに切り替えます。 `su -`

d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

2. ソース管理ノードからPrometheusサービスを停止します。 `service prometheus stop`

3. リカバリした管理ノードで次の手順を実行します。

a. リカバリした管理ノードにログインします。

i. 次のコマンドを入力します。 `ssh admin@grid_node_IP`

ii. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

iii. 次のコマンドを入力してrootに切り替えます。 `su -`

iv. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

b. Prometheusサービスを停止します。 `service prometheus stop`

c. SSH エージェントに SSH 秘密鍵を追加します。入力：`ssh-add`

d. ファイルに記載されているSSHアクセスパスワードを入力し `Passwords.txt`ます。

e. ソース管理ノードのPrometheusデータベースをリカバリした管理ノードにコピーします。 `/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`

f. プロンプトが表示されたら、 * Enter * を押して、リカバリした管理ノード上の新しい Prometheus データベースを破棄することを確認します。

元の Prometheus データベースとその履歴データが、リカバリした管理ノードにコピーされます。コピー処理が完了すると、リカバリした管理ノードがスクリプトによって起動されます。次のステータスが表示されます。

データベースのクローニング、サービスの開始

a. 他のサーバにパスワードなしでアクセスする必要がなくなった場合は、 SSH エージェントから秘密鍵を削除します。入力：`ssh-add -D`

4. ソース管理ノードでPrometheusサービスを再起動します。.`service prometheus start`

ゲートウェイノードの障害からリカバリします

StorageGRIDゲートウェイノードの交換

障害が発生したゲートウェイノードを同じ物理または仮想ハードウェアで実行されているゲートウェイノードと交換することも、 VMware または Linux ホストで実行されているゲートウェイノードをサービスアプライアンスでホストされているゲートウェイノードと交換することもできます。

ノードの交換用手順 を確認する必要があるのは、交換用ノードで使用するプラットフォームによって異なります。（すべてのノードタイプに適した）ノードの交換手順 が完了すると、手順 からゲートウェイノードのリカバリに関する次の手順が表示されます。

交換用プラットフォーム	手順
VMware	"VMware ノードを交換"
Linux	"Linux ノードを交換"
サービスアプライアンス	"サービスアプライアンスを交換します"
OpenStack	リカバリ処理を対象とした OpenStack 用の仮想マシンディスクファイルおよびスクリプトは、現在は提供されていません。OpenStack 環境で実行されているノードのリカバリが必要な場合は、使用している Linux オペレーティングシステム用のファイルをダウンロードしてください。次に、の手順に従います"Linuxノードの交換"。

リカバリの開始を選択して**StorageGRID**ゲートウェイノードを構成します

ゲートウェイノードを交換したら、 Grid Manager で Start Recovery を選択して、障害が発生したノードの代わりとして新しいノードを設定する必要があります。

開始する前に

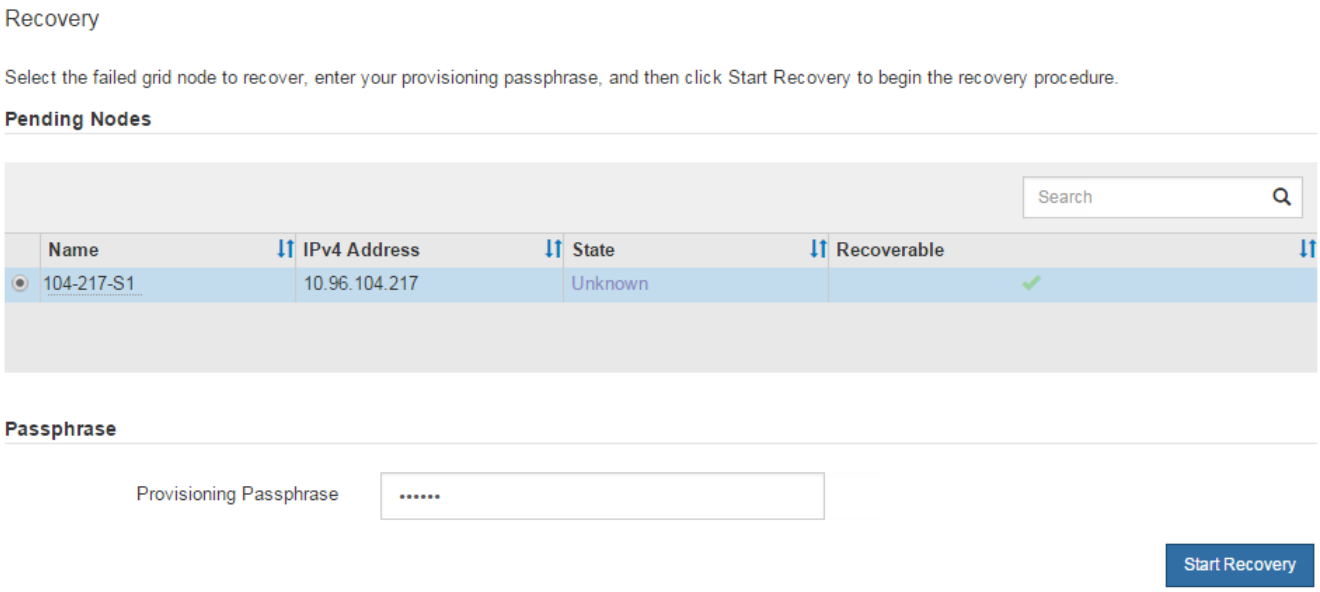
- Grid Managerにサインインしておきます"サポートされている Web ブラウザ"。
- あなたはを持っています"Maintenance権限またはRoot Access権限"。
- プロビジョニングパスフレーズを用意します。
- 交換用ノードの導入と設定を完了しておきます。

手順

1. グリッドマネージャから、メンテナンス > タスク > *ノード復旧*を選択します。
2. リカバリするグリッドノードを Pending Nodes リストで選択します。

   ノードに障害が発生するとリストに表示されますが、ノードを再インストールしてリカバリの準備ができるまでは選択できません。

3. **Provisioning passphrase** を入力してください。
4. 「リカバリを開始」を選択します。



5. リカバリ中のグリッドノードテーブルで、リカバリの進行状況を監視します。

> 復旧処理の実行中に、*リセット*を選択すると、新しい復旧処理を開始できます。手順をリセットするとノードが不確定な状態になることを示すダイアログボックスが表示されます。

手順 をリセットしたあとにリカバリを再試行する場合は、次の手順でノードをインストール前の状態にリストアする必要があります。

- * vmware * ：導入した仮想グリッドノードを削除します。その後、リカバリを再開する準備ができたら、ノードを再導入します。
- * Linux *：Linuxホストで次のコマンドを実行してノードを再起動します。 `storagegrid node force-recovery node-name`
- アプライアンス：手順をリセットしたあとにリカバリを再試行する場合は、ノードでを実行してアプライアンスノードをインストール前の状態にリストアする必要があります `sgareinstall`。を参照して "再インストールのためのアプライアンスの準備（プラットフォームの交換のみ）"

アーカイブノードの障害からリカバリします

StorageGRIDアーカイブノードの障害から回復する

アーカイブノードのサポートが廃止されました。

アーカイブノードのリカバリについては、を参照してください "アーカイブノードの障害からのリカバリ（StorageGRID 11.8ドキュメントサイト）"。

Linuxノードの交換

StorageGRIDのLinuxノードを置き換える

障害発生時に新しい物理ホストまたは仮想ホストを導入するか、既存のホストにLinuxを再インストールする必要がある場合は、グリッドノードをリカバリする前に交換ホストを導入して設定します。この手順 は、すべてのタイプのグリッドノードのリカバリプロセスの 1 つのステップです。

「Linux」は、Red Hat® Enterprise Linux® (RHEL)、Ubuntu®、または Debian® のデプロイメントを指します。サポートされているバージョンのリストについては、 "NetApp Interoperability Matrix Tool（IMT）" 。

この手順は、ソフトウェアベースのストレージノード、プライマリまたは非プライマリ管理ノード、またはゲートウェイノードのリカバリプロセスの一部としてのみ実行します。リカバリするグリッドノードのタイプに関係なく、手順は同じです。

物理または仮想のLinuxホスト上に複数のグリッドノードがホストされている場合、グリッドノードは任意の順序で復旧できます。ただし、プライマリ管理ノードが存在する場合は、他のグリッドノードがプライマリ管理ノードに接続しようとして復旧が遅延するのを防ぐため、まずプライマリ管理ノードを復旧する必要があります。プライマリ管理ノードを最初に復旧できない場合で、プライマリ以外の管理ノードが利用可能な場合は、プライマリ以外の管理ノードを使用して、任意の順序でノードを復旧できます。

StorageGRID用の新しいLinuxホストをデプロイします

いくつかの例外を除き、最初のインストールプロセス時と同じ方法で新しいホストを準備します。

新規または再インストールされた物理または仮想 Linux ホストを展開するには、Linux オペレーティング システムのStorageGRIDインストール手順にあるホストの準備手順に従います。見る"Linux をインストールします" 。

> 「Linux」は、RHEL、Ubuntu、または Debian のデプロイメントを指します。サポートされているバージョンのリストについては、 "NetApp Interoperability Matrix Tool（IMT）" 。

この手順 には、次のタスクが含まれています。

1. Linux をインストールします。
2. ホストネットワークを設定する。
3. ホストストレージを設定する。
4. コンテナエンジンを取り付ける。
5. StorageGRID ホストサービスをインストールする。

> インストール手順の「StorageGRIDホストサービスのインストール」タスクが完了したら停止します。「グリッドノードの導入」タスクを開始しないでください。

これらの手順を実行する際は、次の重要なガイドラインに注意してください。

- 元のホストと同じホストインターフェイス名を使用してください。
- 共有ストレージを使用してStorageGRID ノードをサポートする場合、または障害ノードから一部またはす

べてのドライブまたはSSDを交換用ノードに移動した場合は、元のホストと同じストレージマッピングを再確立する必要があります。たとえば、インストール手順の推奨に従ってでWWIDとエイリアスを使用していた場合 `/etc/multipath.conf`は、交換用ホストのでも同じエイリアスとWWIDのペアを使用して `/etc/multipath.conf`ください。

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

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

StorageGRIDノードをホストにリストアします

障害グリッドノードを新しいLinuxホストにリストアするには、次の手順を実行してノード構成ファイルをリストアします。

1. ノードをリストアして検証ノード構成ファイルをリストアする。新規インストールの場合は、ホストにインストールするグリッドノードごとにノード構成ファイルを作成します。交換ホストにグリッドノードをリストアするときは、障害グリッドノードのノード構成ファイルをリストアまたは交換します。
2. StorageGRID ホストサービスを開始しますです。
3. 必要に応じて、起動しないノードをリカバリ。

以前のホストのブロックストレージボリュームが保持されている場合は、追加のリカバリ手順の実行が必要になることがあります。このセクションのコマンドを使用して、必要な追加手順を特定できます。

グリッドノードをリストアして検証する

プライマリ以外の管理ノードからノードを復旧する場合は、復旧したノードがプライマリ管理ノードではなく、プライマリ以外の管理ノードに登録されるように、ADMIN_IP をプライマリ以外の管理ノードのグリッドネットワーク IP アドレスに設定してください。管理ネットワークキーのルールを確認するには、"Linux デプロイメント用の StorageGRID ノード構成ファイルを作成する"を参照してください。

障害グリッドノードのグリッド構成ファイルをリストアして検証し、エラーをすべて解決する必要があります。

タスクの内容

前のホストの障害によってボリュームが失われていないかぎり、ホストに必要なグリッドノードをインポートできます。 `/var/local`たとえば、使用しているLinuxオペレーティングシステムでのStorageGRIDのインストール手順に従って、StorageGRIDシステムのデータボリュームに共有ストレージを使用していた場合は、`/var/local`ボリュームが残っている可能性があります。ノードをインポートすると、ノード構成ファイルがホストにリストアされます。

欠落しているノードをインポートできない場合は、ノードのグリッド構成ファイルを再作成する必要があります。

次に、 StorageGRID の再起動に進む前に、グリッド構成ファイルを検証し、予想されるネットワークまたはストレージの問題を解決する必要があります。ノードの構成ファイルを再作成する場合は、リカバリするノードに使用されていたのと同じ名前を交換用ノードに使用する必要があります。

参照"Linuxのインストール手順"場所の詳細については、 `/var/local`ノードのボリューム。

手順

1. リカバリしたホストのコマンドラインで、現在設定されているすべてのStorageGRIDノードを一覧表示します。`sudo storagegrid node list`

   グリッドノードが設定されていない場合、出力は表示されません。グリッドノードが設定されている場合は、次の形式で出力が表示されます。

```
Name               Metadata-Volume
=============================================================
dc1-adm1           /dev/mapper/sgws-adm1-var-local
dc1-gw1            /dev/mapper/sgws-gw1-var-local
dc1-sn1            /dev/mapper/sgws-sn1-var-local
dc1-arc1           /dev/mapper/sgws-arc1-var-local
```

   ホストで設定する必要があるグリッドノードの一部またはすべてが表示されない場合は、表示されないグリッドノードをリストアする必要があります。

2. ボリュームを含むグリッドノードをインポートするには `/var/local`：

   a. インポートする各ノードに対して次のコマンドを実行します。`sudo storagegrid node import node-var-local-volume-path`

      `storagegrid node import`コマンドが成功するのは、ターゲットノードが最後に実行されたホストでクリーンシャットダウンされている場合だけです。そうでない場合は、次のようなエラーが表示されます。

```
This node (node-name) appears to be owned by another host (UUID host-uuid).

Use the --force flag if you are sure import is safe.
```

   a. 別のホストが所有しているノードに関するエラーが表示された場合は、フラグを指定してコマンドをもう一度実行し `--force`、インポートを完了します。`sudo storagegrid --force node import node-var-local-volume-path`

      フラグを指定してインポートされたノードが `--force`グリッドに再参加できるようにするには、追加のリカバリ手順が必要です（を参照）"次の手順：必要に応じて追加のリカバリ手順を実行します"。

3. グリッドノードに `/var/local`ボリュームの場合は、ノードの構成ファイルを再作成してホストに復元します。手順については、"ノード構成ファイルを作成" 。

ノードの構成ファイルを再作成する場合は、リカバリするノードに使用されていたのと同じ名前を交換用ノードに使用する必要があります。Linux 環境の場合は、構成ファイルの名前にノード名が含まれていることを確認します。可能な場合は、同じネットワークインターフェイス、ブロックデバイスマッピング、および IP アドレスを使用してください。これにより、リカバリ時にノードにコピーしなければならないデータ量を最小限に抑えることができるため、リカバリにかかる時間を大幅に（場合によっては、数週間から数分に）短縮できます。

ノードの構成ファイルを再作成するときに、で始まる構成変数の値として新しいブロックデバイス（StorageGRIDノードで以前に使用していなかったデバイス）を使用する場合 `BLOCK_DEVICE_`は、のガイドラインに従ってくださいブロックデバイスが見つからないエラーを修正します。

4. リカバリしたホストで次のコマンドを実行して、すべての StorageGRID ノードを一覧表示します。

   ```
   sudo storagegrid node list
   ```

5. StorageGRID のノードリストの出力に表示されている各グリッドノードのノード構成ファイルを検証します。

   ```
   sudo storagegrid node validate node-name
   ```

   StorageGRID ホストサービスを開始する前に、すべてのエラーまたは警告に対処する必要があります。以下のセクションでは、リカバリ時に特に問題となるエラーについて詳しく説明します。

ネットワークインターフェイスが見つからないエラーを修正

ホストネットワークが正しく設定されていない場合や名前のスペルが間違っている場合は、StorageGRIDがファイルに指定されているマッピングをチェックするときにエラーが発生し `/etc/storagegrid/nodes/*node-name*.conf`ます。

次のエラーまたは警告が表示されることがあります。

```
Checking configuration file /etc/storagegrid/nodes/<node-name>.conf for
node <node-name>...
ERROR: <node-name>: GRID_NETWORK_TARGET = <host-interface-name>
       <node-name>: Interface <host-interface-name>' does not exist
```

エラーは、グリッドネットワーク、管理ネットワーク、またはクライアントネットワークについて報告される場合があります。このエラーは、ファイルが指定されたStorageGRIDネットワークをという名前のホストインターフェイスにマッピングしている *host-interface-name*`が、現在のホストにその名前のインターフェイスがないことを意味します `/etc/storagegrid/nodes/*node-name*.conf。

このエラーが表示された場合は、の手順を完了していることを確認してください"新しい Linux ホストを導入する"。すべてのホストインターフェイスに、元のホストで使用されていた名前と同じ名前を使用します。

ノード構成ファイルに指定されている名前をホストインターフェイスに付けることができない場合は、ノード構成ファイルを編集して、 GRID_NETWORK_TARGET 、 ADMIN_NETWORK_TARGET 、または CLIENT_network_target の値を既存のホストインターフェイスに一致するように変更できます。

ホストインターフェイスが適切な物理ネットワークポートまたは VLAN へのアクセスを提供し、インターフェイスがボンドデバイスまたはブリッジデバイスを直接参照していないことを確認してください。ホストのボンドデバイスの上に VLAN （または他の仮想インターフェイス）を設定するか、ブリッジと仮想イーサネット（ veth ）のペアを使用する必要があります。

ブロックデバイスが見つからないエラーを修正します

システムは、リカバリされた各ノードが有効なブロックデバイススペシャルファイル、またはブロックデバイススペシャルファイルへの有効なソフトリンクにマッピングされていることを確認します。StorageGRIDがファイル内で無効なマッピングを検出すると、 `/etc/storagegrid/nodes/*node-name*.conf`ブロックデバイスが見つからないというエラーが表示されます。

次のエラーが発生することがあります。

```
Checking configuration file /etc/storagegrid/nodes/<node-name>.conf for
node <node-name>...
ERROR: <node-name>: BLOCK_DEVICE_PURPOSE = <path-name>
       <node-name>: <path-name> does not exist
```

つまり、*node-name_for*で使用されるブロックデバイスが*Linux*ファイルシステム内の指定されたパス名にマッピングされ *PURPOSE*`ますが、その場所に有効なブロックデバイススペシャルファイルまたはブロックデバイススペシャルファイルへのソフトリンクがないことを意味します *`/etc/storagegrid/nodes/_node-name.conf*。

の手順が完了していることを確認します"新しい Linux ホストを導入する"。すべてのブロックデバイスに、元のホストで使用されていたのと同じ永続的なデバイス名を使用します。

見つからないブロックデバイススペシャルファイルをリストアまたは再作成できない場合は、適切なサイズとストレージカテゴリの新しいブロックデバイスを割り当て、ノード構成ファイルを編集して、新しいブロックデバイススペシャルファイルを参照するようにの値を変更します `BLOCK_DEVICE_PURPOSE`。

Linux オペレーティング システムの表を使用して、適切なサイズとストレージ カテゴリを決定します。見る"ストレージとパフォーマンスの要件" 。

推奨事項を確認する"ホストストレージの構成"ブロック デバイスの交換に進む前に。

> 障害が発生したホストで元のブロックデバイスが失われたために、で始まる構成ファイルの変数に新しいブロックストレージデバイスを指定する必要がある場合は `BLOCK_DEVICE_`、リカバリ手順を実行する前に新しいブロックデバイスがフォーマットされていないことを確認してください。共有ストレージを使用していて新しいボリュームを作成済みの場合、新しいブロックデバイスはアンフォーマットされます。状況がわからない場合は、新しいブロックストレージデバイスのスペシャルファイルに対して次のコマンドを実行します。

> 次のコマンドは、新しいブロックストレージデバイスに対してのみ実行してください。デバイス上のデータはすべて失われるため、リカバリ対象のノードの有効なデータがブロックストレージに残っていると思われる場合は、このコマンドを実行しないでください。
>
> ```
> sudo dd if=/dev/zero of=/dev/mapper/my-block-device-name bs=1G count=1
> ```

StorageGRID ホストサービスを開始する

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

手順

1. 各ホストで次のコマンドを実行します。

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

2. 次のコマンドを実行して、導入の進行状況を確認します。

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

3. いずれかのノードのステータスが「Not Running」または「Stopped」になった場合は、次のコマンドを実行します。

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

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

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

正常に開始しないノードをリカバリします

StorageGRID ノードがグリッドに正常に再参加できずリカバリ可能と表示されない場合は、ノードが破損している可能性があります。ノードを強制的にリカバリモードに設定することができます。

手順

1. ノードのネットワーク設定が正しいことを確認します。

   ネットワークインターフェイスのマッピングまたはグリッドネットワークのIPアドレス/ゲートウェイが正しくないため、ノードがグリッドに再参加できなかった可能性があります。

2. ネットワーク設定が正しい場合は、次のコマンドを実行し `force-recovery`ます。

   ```
   sudo storagegrid node force-recovery node-name
   ```

3. ノードに対して追加のリカバリ手順を実行します。を参照して "次の手順：必要に応じて追加のリカバリ手順を実行します"

追加のStorageGRIDノードリカバリ手順を実行する

交換ホストで実行されている StorageGRID ノードをリカバリした方法によっては、ノードごとに追加のリカバリ手順を実行する必要があります。

Linux ホストを交換、または障害グリッドノードを新しいホストにリストアした際に対応処置が不要であった場合は、ノードのリカバリはこれで完了です。

対処方法と次の手順

ノードの交換時に、次のいずれかの対処が必要になった場合があります。

- フラグを使用してノードをインポートする必要があり `--force`ました。
- 構成ファイルの値が `BLOCK_DEVICE_<PURPOSE>`（の場合） `<PURPOSE>`参照するブロックデバイスに、ホストの障害前と同じデータが格納されていません。
- ノードに対してを実行し `storagegrid node force-recovery *node-name*`ます。
- 新しいブロックデバイスを追加した。

これらの対処方法のいずれかを実行した場合は、追加のリカバリ手順を実行する必要があります。

リカバリのタイプ	次の手順に進みます
プライマリ管理ノード	• "プライマリ管理ノードを設定するには、「リカバリの開始」を選択します。" • "プライマリ管理ノードを非プライマリ管理ノードを使用して復旧する"
非プライマリ管理ノード	"[リカバリの開始 を選択して、非プライマリ管理ノードを設定します"]
ゲートウェイノード	"Start Recovery を選択して、ゲートウェイノードを設定します"
ストレージノード（ソフトウェアベース）： • フラグを使用してノードをインポートした場合 `--force`、または `storagegrid node force-recovery *node-name*` • ノードの完全な再インストールを実行する必要があった場合や、/var/local をリストアする必要があった場合	"Start Recovery を選択して、ストレージノードを設定します"

リカバリのタイプ	次の手順に進みます
ストレージノード（ソフトウェアベース）： • 新しいブロックデバイスを追加した場合。 • 構成ファイル変数の値が `BLOCK_DEVICE_<PURPOSE>`（の場合）`<PURPOSE>`参照するブロックデバイスに、ホスト障害前と同じデータが格納されていない。	"システムドライブに損傷がない場合は、ストレージボリューム障害からリカバリします"

StorageGRID の VMware ノードをリカバリノードに交換する

VMwareでホストされていた障害StorageGRID ノードをリカバリする場合は、障害ノードを削除してリカバリノードを導入します。

開始する前に

仮想マシンをリストアできないため、交換する必要があることを確認しました。

タスクの内容

VMware vSphere Web Client を使用して、最初に障害グリッドノードに関連付けられた仮想マシンを削除します。その後、新しい仮想マシンを導入できます。

この手順 は、グリッドノードのリカバリプロセスの一部です。ノードの削除と導入の手順は、管理ノード、ストレージノード、ゲートウェイノードを含むすべてのVMwareノードで同じです。

手順

1. VMware vSphere Web Clientにログインします。
2. 障害が発生したグリッドノード仮想マシンに移動します。
3. リカバリノードを導入するために必要なすべての情報をメモしておきます。
   a. 仮想マシンを右クリックし、 * 設定の編集 * タブを選択して、使用中の設定を確認します。
   b. [* vApp Options*] タブを選択して、グリッドノードのネットワーク設定を表示し、記録します。
4. 障害グリッドノードがストレージノードである場合は、データストレージに使用されている仮想ハードディスクが破損していないかどうかを確認し、リカバリされたグリッドノードへの再接続に備えて保持しておきます。
5. 仮想マシンの電源をオフにします。
6. 仮想マシンを削除するには、 * Actions * > * All vCenter Actions * > * Delete from Disk * を選択します。
7. 交換ノードとなる新しい仮想マシンを展開し、1 つ以上のStorageGRIDネットワークに接続します。手順については、"仮想マシンとしてのStorageGRID ノードの導入" 。

   ノードを導入する際には、必要に応じてノードポートを再マッピングしたり、 CPU やメモリの設定を増やしたりできます。

   新しいノードを導入したら、ストレージ要件に従って新しい仮想ディスクを追加し、以前に削除した障害グリッドノードから保存した仮想ハードディスクを再接続するか、またはその両方を実行します。

8. リカバリするノードのタイプに応じて、ノードのリカバリ手順 を実行します。

ノードのタイプ	に移動
管理ノード	"StorageGRIDにおけるプライマリまたは非プライマリ管理ノードの復旧"
ゲートウェイノード	"Start Recovery を選択して、ゲートウェイノードを設定します"
ストレージノード	"Start Recovery を選択して、ストレージノードを設定します"

StorageGRID の VMware ノードを SG1000 または SG100 に交換する

プライマリ管理ノードがVMwareノードとして動作している場合、それをSG1000またはSG100サービスアプライアンスに置き換えることができます。

> ノードの交換が完了し、検証が済んだら、元のVMwareノードを削除する必要があります。古いノードをそのまま放置しておくと、再びオンラインになった場合にグリッドに重大な障害を引き起こす危険性があります。

開始する前に

- 仮想マシンをリストアできないため、交換する必要があることを確認しました。
- グリッドの保守作業が進行中ではないことを確認しました。
- SG1000またはSG100サービスアプライアンスのStorageGRIDアプライアンスインストーラーのバージョンが、StorageGRIDシステムのソフトウェアバージョンと一致していることを確認しました。
- 既存のプライマリ管理ノードに関する以下の情報があります。

  ノード名：サービスアプライアンスをインストールする際は、既存のプライマリ管理ノードと同じノード名を使用する必要があります。ノード名はホスト名（システム名）です。

  IPアドレス：サービスアプライアンスには、既存のプライマリ管理ノードと同じIPアドレスを割り当てることができます（推奨）。または、各ネットワークで新しい未使用のIPアドレスを選択することもできます。

- プロビジョニングパスフレーズを用意します。

ステップ1：VMwareノードを交換する

まず、グリッドマネージャーで既存のプライマリ管理ノードを削除します。次に、StorageGRID アプライアンスインストーラーを使用して、SG1000 または SG100 サービスアプライアンスを新しいプライマリ管理ノードとしてインストールし、ノードを復旧します。新しい IP アドレスを使用する場合は、既存のプライマリ管理ノードを削除する前にサービスアプライアンスをインストールできます。

既存のIPアドレスを使用する

既存のプライマリ管理ノードのIPアドレスを使用して、プライマリ管理ノードを置き換えます。

手順

1. Grid Manager からリカバリパッケージをダウンロードします：
   a. **Maintenance** > **Recovery package** を選択します。
   b. プロビジョニングパスフレーズを入力して、パッケージをダウンロードしてください。
2. 既存のプライマリ管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
   b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。
   c. root に切り替えます： `su -`
   d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

   rootとしてログインすると、プロンプトがからに `#`変わります `$`。
3. "既存のプライマリ管理ノードから監査ログをコピーする"。
4. グリッドノード上のサーバーマネージャーとすべてのサービスを停止します。

   ```
   shutdown -h now
   ```

   サービス停止まで最大15分かかる場合があります。
5. "SG1000またはSG100サービスアプライアンスのインストール"。
6. "SG1000またはSG100サービスアプライアンスのデプロイ"。
7. 「インストールの開始」を選択後、インストールが「StorageGRID インストーラーのロード」の手順に達するまで約 10 分お待ちください。

   6～7分後、ブラウザはリダイレクトされ、リカバリが開始されます。
8. アプライアンスの時計が正しいことを確認してください。
   a. SSHを使用してポート8022に接続します：
      i. コマンドを入力してください： `ssh -p 8022 admin@grid_node_IP`。
      ii. root に切り替えます： `su -`
      iii. と入力します `netapp1!`。
   b. 機器の時計が現在のUTC時刻から数分以内の誤差に収まっていることを確認してください。必要に応じて、正しい日付と時刻を設定してください：

      ```
      date -s "DD Mon YYYY HH:MM:SS"
      ```

9. ウェブブラウザに戻り、*障害が発生したプライマリ管理ノードを復旧する*を選択してください。
10. ダウンロードしたリカバリーパッケージをアップロードします。
11. プロビジョニングパスフレーズを入力し、*リカバリの開始*を選択します。

    復旧の進行状況を示すバーが表示されます。復旧プロセスが完了し、サービスが開始されるまで、6分から10分ほどかかります。

12. 指示が表示されたら、グリッドマネージャーにログインしてください。

新しいIPアドレスを使用する

プライマリ管理ノードを新しいIPアドレスに置き換えます。

手順

1. "SG1000またはSG100サービスアプライアンスのインストール"。
2. 復旧時にNTPエラーが発生しないよう、機器の時計が正しいことを確認してください。
   a. SSHを使用してポート8022に接続します：
      i. コマンドを入力してください： `ssh -p 8022 admin@grid_node_IP`。
      ii. root に切り替えます： `su -`
      iii. と入力します `netapp1!`。
   b. 機器の時計が現在の協定世界時（UTC）から数分以内の誤差に収まっていることを確認してください。必要に応じて、正しい日付と時刻を設定してください。

      ```
      date -s "DD Mon YYYY HH:MM:SS"
      ```

3. StorageGRID アプライアンスインストーラーの **StorageGRID** ソフトウェアのアップロード に移動し、アプライアンスにプリロードされているソフトウェアバージョンが、グリッドで実行されているStorageGRID のバージョンと一致していることを確認してください。バージョンが一致しない場合：
   a. "NetAppサポート サイト"から、正しい StorageGRID Debian インストールパッケージをダウンロードしてください。
   b. インストールソフトウェアを削除するには、「削除」を選択します。
   c. `storagegrid-webscale-images-<sg-version>.deb`と `storagegrid-webscale-images-<sgversion>.deb.md5`ファイルをアップロードします。
4. StorageGRID アプライアンスインストーラーの「ホーム」タブで、ノードタイプとして「Primary Admin (with Load Balancer)」を選択します。
5. ノード名を入力してください。ノード名は、既存のプライマリ管理ノード名と一致している必要があります。

   インストールの開始 を選択しないでください。

6. 新しいIPアドレスのサブネットがグリッドネットワーク内にあるかどうかを確認してください。新しいIPサブネットが存在しない場合は、グリッドネットワークに追加します。

a. Grid Managerで、**Maintenance** > *Grid Network*を選択します。

b. サブネットリストを更新するには、プロビジョニングパスフレーズを入力してください。

7. GRID Managerからリカバリパッケージをダウンロードします。

a. **Maintenance** > **Recovery package** を選択します。

b. プロビジョニングパスフレーズを入力し、パッケージをダウンロードしてください。

8. 既存のプライマリ管理ノードにログインします。

a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`

b. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

c. 次のコマンドを入力してrootに切り替えます。 `su -`

d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

rootとしてログインすると、プロンプトがからに `#`変わります `$`。

9. "既存のプライマリ管理ノードから監査ログをコピーする"。

10. グリッドノード上のサーバーマネージャーとすべてのサービスを停止します。

```
service servermanager stop
```

サービス停止まで最大15分かかる場合があります。

11. StorageGRID アプライアンスインストーラの「ホーム」タブで、次の操作を行います：

a. 以下の設定を確認してください：

- ノードタイプは **Primary Admin (with Load Balancer)** に設定されています。
- ノード名が既存のプライマリ管理ノード名と一致します

b. 新しいIPアドレスを記録してください。

12. 「インストール開始」を選択します。

インストールが **StorageGRID** インストーラーのロード ステップに達するまで、約 10 分かかります。

6～7分後、ブラウザはリダイレクトされ、リカバリ手順が開始されます。

13. アプライアンスの時計が正しいことを確認してください。

a. SSHを使用してポート8022に接続します：

i. コマンドを入力してください： `ssh -p 8022 admin@grid_node_IP`。

ii. root に切り替えます： `su -`

iii. と入力します `netapp1!`。

b. 機器の時計が現在のUTC時刻から数分以内の誤差に収まっていることを確認してください。必要に応じて、正しい日付と時刻を設定してください：

```
date -s "DD Mon YYYY HH:MM:SS"
```

14. ウェブブラウザに戻り、*障害が発生したプライマリ管理ノードを復旧する*を選択します。
15. ダウンロードしたリカバリーパッケージをアップロードします。
16. プロビジョニングパスフレーズを入力し、*リカバリの開始*を選択します。

    プライマリ管理ノードの復旧ページが消え、その後再び表示されます。もう一度 **Start Recovery** を選択すると、 `500: Internal Server Error`が表示されます。これは、復旧が開始されたものの、新しい IP アドレスを使用している Grid Manager に更新情報を送信できないためです。この問題を解決するには、 `/etc/hosts`ファイルでプライマリ管理ノードの IP アドレスを更新してください：

    a. SSHを使用してポート8022に接続します：
        i. コマンドを入力してください： `ssh -p 8022 admin@grid_node_IP`。
        ii. root に切り替えます： `su -`
        iii. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。
    b. ログにアクセスする：

    ```
    tail /var/local/log/install.log
    ```

    以下のエラーが繰り返し表示されます： `curl: (7) Failed to connect to <primary_Admin_Node_name> port9999: No route to host`

    これは想定される動作です。StorageGRID は、既存のプライマリ管理ノードの IP アドレスを使用して、プライマリ管理ノードにアップデートを送信しようとしています。

    c. コンテナが実行されていることを確認します。

    ```
    storagegrid node status
    ```

```
storagegrid node enter <primary_Admin_Node_name>
```

    a. コンテナ内の `/etc/hosts`ファイルで、既存のプライマリ管理ノードのIPアドレスを新しいIPアドレスに置き換えます。
    b. ファイルを保存します。
    c. ウェブブラウザに戻ります。数秒後、復旧の進行状況を示すバーが表示されます。

    復旧プロセスが完了し、サービスが開始されるまで、6分から10分ほどかかります。

17. 指示が表示されたら、グリッドマネージャーにログインしてください。
18. リカバリパッケージを更新します。

    a. プライマリ管理ノードにログインします。
        i. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`

ii. root に切り替えます： `su -`

iii. 次のコマンドを入力します： `change-ip`

b. オプション **3 – Edit admin network subnet lists** を選択し、新しいサブネットを追加します。

StorageGRID は、新しいプライマリ管理ノードの IP アドレスを使用して、新しいリカバリパッケージを自動的に生成します。

19. Grid Managerから最新のリカバリパッケージをダウンロードしてください。

ステップ2：ノードの完全復旧

復元手順（監査ログ、管理ノードデータベース、およびPrometheusメトリクス）のソース管理ノードとして、既存のプライマリ以外の管理ノードを使用します。グリッドにプライマリ以外の管理ノードがない場合、復旧したプライマリ管理ノードとは異なるIPアドレスで実行されている、交換対象の元のVMwareノードを使用できます。

手順

1. "監査ログを復元する"。
2. "管理ノードデータベースを復元する"。
3. "Prometheusメトリクスを復元する"。
4. 新しいプライマリ管理ノードが正しく機能していることを確認してください。次に、元の VM ノードまたはベアメタルコンテナをすぐに削除してください。

障害が発生したノードをサービスアプライアンスと交換します

障害が発生した**StorageGRID**ノードをサービスアプライアンスと交換

サービスアプライアンスを使用して、障害が発生したゲートウェイノード、障害が発生した非プライマリ管理ノード、またはVMware、Linuxホスト、またはサービスアプライアンスでホストされていた障害が発生したプライマリ管理ノードをリカバリできます。この手順 は、グリッドノードのリカバリ手順 の 1 つのステップです。

開始する前に

- 次のいずれかの状況に該当することを確認しておきます。
  - ノードをホストしている仮想マシンをリストアできません。
  - グリッドノードの物理 / 仮想 Linux ホストに障害が発生したため、交換する必要がある。
  - グリッドノードをホストしているサービスアプライアンスを交換する必要があります。
- サービスアプライアンスのStorageGRID アプライアンスインストーラのバージョンがStorageGRID システムのソフトウェアバージョンと一致していることを確認しておきます。を参照してください "StorageGRID アプライアンスインストーラのバージョンを確認してアップグレードします"

> SG110とSG1100サービスアプライアンス、またはSG100とSG1000サービスアプライアンスの両方を同じサイトに導入しないでください。パフォーマンスが予測不能になる可能性があります。

タスクの内容

次の場合、サービスアプライアンスを使用して障害グリッドノードをリカバリできます。

- 障害ノードはVMwareまたはLinuxでホストされていました（"プラットフォームの変更"）
- 障害ノードはサービスアプライアンスでホストされていました（"プラットフォームの交換"）

StorageGRIDサービスアプライアンスのインストール（プラットフォーム変更のみ）

交換用ノードにサービスアプライアンスを使用してVMwareまたはLinuxホストでホストされていた障害グリッドノードをリカバリする場合は、最初に障害ノードと同じノード名（システム名）を使用して新しいアプライアンスハードウェアを設置する必要があります。

開始する前に

障害ノードに関する次の情報を確認しておきます。

- * ノード名 * ：障害が発生したノードと同じノード名を使用してサービスアプライアンスをインストールする必要があります。ノード名はホスト名（システム名）です。
- * IP アドレス * ：障害が発生したノードと同じ IP アドレスをサービスアプライアンスに割り当てることができます。これは推奨されるオプションであり、各ネットワークで新しい未使用の IP アドレスを選択することもできます。

タスクの内容

この手順 は、 VMware または Linux でホストされていた障害ノードをサービスアプライアンスでホストされているノードと交換してリカバリする場合にのみ実行してください。

手順

1. 新しいサービスアプライアンスの設置手順に従います。を参照してください "ハードウェア設置のクイックスタート"
2. ノード名の入力を求められたら、障害ノードのノード名を使用します。

StorageGRID アプライアンスの再設置の準備（プラットフォーム交換のみ）

サービスアプライアンスでホストされていたグリッドノードをリカバリする場合は、最初に StorageGRID ソフトウェアを再インストールするアプライアンスを準備する必要があります。

この手順 は、サービスアプライアンスでホストされていた障害ノードを交換する場合にのみ実行してください。障害ノードが元 々 VMwareまたはLinuxホストでホストされていた場合は、次の手順を実行しないでください。

手順

1. 障害が発生したグリッドノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
   b. ファイルに記載されているパスワードを入力し `Passwords.txt` ます。

c. 次のコマンドを入力してrootに切り替えます。 `su -`

d. ファイルに記載されているパスワードを入力し `Passwords.txt`ます。

rootとしてログインすると、プロンプトがからに `#`変わります `$`。

2. StorageGRID ソフトウェアをアプライアンスにインストールする準備をします。入力： `sgareinstall`

3. 続行するかどうかを確認するメッセージが表示されたら、 `y`

アプライアンスがリブートされ、 SSH セッションが終了します。通常は 5 分程度で StorageGRID アプライアンスインストーラが使用可能になりますが、場合によっては最大で 30 分待つ必要があります。

サービスアプライアンスがリセットされ、グリッドノード上のデータにアクセスできなくなります。元のインストールプロセスで設定した IP アドレスはそのまま使用する必要がありますが、手順 の完了時に確認しておくことを推奨します。

コマンドの実行後、 `sgareinstall`StorageGRIDでプロビジョニングされたアカウント、パスワード、およびSSHキーがすべて削除され、新しいホストキーが生成されます。

サービスアプライアンスで**StorageGRID**ソフトウェアのインストールを開始する

ゲートウェイノードまたは管理ノードをサービスアプライアンスにインストールするには、アプライアンスに含まれているStorageGRIDアプライアンスインストーラを使用します。

開始する前に

- アプライアンスをラックに設置し、ネットワークに接続して電源をオンにします。
- StorageGRID アプライアンスインストーラを使用して、アプライアンスのネットワークリンクとIPアドレスを設定します。
- ゲートウェイノードまたはプライマリ以外の管理ノードをインストールする場合は、以下のいずれかの管理ノードの IP アドレスを把握している必要があります。
  - StorageGRID グリッドのプライマリ管理ノード
  - プライマリ以外の管理ノードが利用可能で、ノードの復旧に使用されている場合
- プライマリ管理ノード以外の管理ノードを使用してノード（プライマリ管理ノードを含む）を復旧する場合、その管理ノードのIPアドレスを指定できます。
- StorageGRID アプライアンスインストーラの[IP Configuration]ページにリストされているすべてのグリッドネットワークサブネットは、プライマリ管理ノードのグリッドネットワークサブネットリストで定義されます。

  を参照してください "ハードウェア設置のクイックスタート"

- を使用している"サポートされている Web ブラウザ"。
- アプライアンスに割り当てられたIPアドレスのいずれかを確認しておきます。管理ネットワーク、グリッドネットワーク、またはクライアントネットワークの IP アドレスを使用できます。
- プライマリ管理ノードをインストールする場合は、このバージョンの StorageGRID 用の Ubuntu または Debian のインストールファイルが必要です。

最新バージョンの StorageGRID ソフトウェアは、製造時にサービスアプライアンスにプリロードされています。プリロードされたソフトウェアのバージョンがStorageGRID 環境で使用されているバージョンと一致する場合は、インストールファイルは必要ありません。

タスクの内容

サービスアプライアンスにStorageGRIDソフトウェアをインストールするには、次の手順を実行します。

- プライマリ管理ノードの場合、ノード名を指定し、必要に応じて適切なソフトウェアパッケージをアップロードします。プライマリ管理ノードを復旧する場合で、グリッド内にプライマリ以外の管理ノードが存在する場合は、プライマリ以外の管理ノードを使用してノードを復旧し、その管理ノードのIPアドレスを指定するか、現在の構成を使用してノードをインストールまたは復旧するかのいずれかを選択できます。
- 非プライマリ管理ノードまたはゲートウェイノードの場合は、プライマリ管理ノードの IP アドレスとノードの名前を指定または確認します。
- インストールを開始し、ボリュームの設定とソフトウェアのインストールが行われている間待機します。
- プロセスの途中でインストールが一時停止します。インストールを再開するには、 Grid Manager にサインインして、保留状態のノードを障害ノードの代わりとして設定する必要があります。
- ノードを設定すると、アプライアンスのインストールプロセスが完了してアプライアンスがリブートされます。

手順

1. ブラウザを開き、サービスアプライアンスのいずれかのIPアドレスを入力します。

   `https://Controller_IP:8443`

   StorageGRID アプライアンスインストーラのホームページが表示されます。

2. プライマリ管理ノードをインストールするには:
   a. このノードセクションで、 * ノードタイプ * に * プライマリ管理者 * を選択します。
   b. *ノード名*フィールドに、復旧対象のノードに使用されていた名前と同じ名前を入力し、*保存*を選択します。
   c. インストールモードのセクションで利用可能な2つのモードから、適切なモードを選択してください。「ノードをインストールするか、現在の構成を使用してこのノードを復旧する」方法、または「プライマリ以外の管理ノードを使用してこのノードを復旧する」方法のいずれかを選択できます。

現在の構成方法

現在の構成を使用して、ノードをインストールするか、このノードを復旧してください。

i. インストールセクションで、「現在の状態」に表示されているソフトウェアのバージョンを確認してください。インストール準備が整ったソフトウェアのバージョンが正しい場合は、インストール手順に進んでください。

ii. 別のバージョンのソフトウェアをアップロードする必要がある場合は、*詳細設定*メニューで*StorageGRID ソフトウェアのアップロード*を選択してください。「StorageGRID ソフトウェアのアップロード」ページが表示されます。

iii. 「参照」を選択して、StorageGRID ソフトウェアの「ソフトウェアパッケージ」と「チェックサムファイル」をアップロードします。ファイルを選択すると、自動的にアップロードされます。

iv. 「ホーム」を選択して、StorageGRID アプライアンスインストーラのホームページに戻ります。

非プライマリ管理者ノード方式

プライマリ以外の管理ノードを使用して、このノードを復旧してください。

i. 「非プライマリ管理ノードIP」フィールドに、復旧に使用する非プライマリ管理ノードのグリッドネットワークIPアドレスを入力し、*保存*を選択します。

ii. インストールする準備ができたソフトウェアのバージョンが正しい場合は、に進みますインストール手順。

3. ゲートウェイ ノードまたは非プライマリ管理ノードをインストールするには:

a. このノードセクションで、 * ノードタイプ * には、リストアするノードのタイプに応じて * ゲートウェイ * または * 非プライマリ管理 * を選択します。

b. *ノード名*フィールドに、復旧対象のノードに使用されていた名前と同じ名前を入力し、*保存*を選択します。

c. プライマリ管理ノードの接続セクションで、プライマリ管理ノードの IP アドレスを指定する必要があるかどうかを確認します。

プライマリ管理ノードまたは ADMIN_IP が設定された少なくとも 1 つのグリッドノードが同じサブネットにある場合は、 StorageGRID アプライアンスインストーラがこの IP アドレスを自動的に検出します。

d. この IP アドレスが表示されない場合、または変更する必要がある場合は、アドレスを指定します。

オプション	製品説明
IP を手動で入力します	a. [管理ノードの検出を有効にする]*チェックボックスをオフにします。 b. IPアドレスを手動で入力します。 c. [保存（ Save ）] を選択します。 d. 新しいIPアドレスの接続状態が「READY」になるまで待ちます。

オプション	製品説明
接続されたすべてのプライマリ管理ノードの自動検出	a. [管理ノードの検出を有効にする]*チェックボックスを選択します。 b. 検出された IP アドレスのリストから、このサービスアプライアンスを導入するグリッドのプライマリ管理ノードを選択します。 c. [保存（ Save ）] を選択します。 d. 新しいIPアドレスの接続状態が「READY」になるまで待ちます。

4. インストールセクションで、現在の状態がノード名のインストールを開始する準備ができていること、および * インストールの開始 * ボタンが有効になっていることを確認します。

   *インストールの開始*ボタンが有効になっていない場合は、ネットワーク構成またはポート設定を変更する必要がある可能性があります。アプライアンスのメンテナンス手順を参照してください。

5. StorageGRID アプライアンスインストーラーのホームページで、「インストールの開始」を選択します。

   現在の状態が「インストール中です」に変わり、モニターのインストールページが表示されます。

   モニターのインストールページに手動でアクセスする必要がある場合は、メニューバーから「Monitor installation」を選択してください。

StorageGRIDサービスアプライアンスのインストールの監視

StorageGRID アプライアンスインストーラでは、インストールが完了するまでステータスが提供されます。ソフトウェアのインストールが完了すると、アプライアンスがリブートされます。

手順

1. インストールの進行状況を監視するには、メニューバーから*Monitor installation*を選択してください。

   モニターのインストールページには、インストールの進行状況が表示されます。

   青色のステータスバーは、現在進行中のタスクを示します。緑のステータスバーは、正常に完了したタスクを示します。

   インストーラは、以前のインストールで完了したタスクが再実行されないようにします。インストールを再実行している場合、再実行する必要のないタスクはすべて緑色のステータスバーと「スキップ済み」のステータスで表示されます。

2. インストールの最初の 2 つのステージの進行状況を確認します。

   - *1.ストレージの構成 *

     インストーラが既存の設定をすべてドライブから消去し、ホストを設定します。

   - *2.OS * をインストールします

インストーラが StorageGRID のベースとなるオペレーティングシステムイメージをプライマリ管理ノードからアプライアンスにコピーするか、ベースとなるオペレーティングシステムイメージをプライマリ管理ノードのインストールパッケージからインストールします。

3. 次のいずれかが実行されるまで、インストールの進行状況を監視します。
   - アプライアンスゲートウェイノードまたは非プライマリアプライアンス管理ノードの場合、 * Install StorageGRID * ステージが一時停止し、組み込みのコンソールにメッセージが表示されて、グリッドマネージャを使用して管理ノードでこのノードを承認するように求められます。
   - アプライアンスプライマリ管理ノードの場合、第 5 フェーズ（ Load StorageGRID Installer ）が表示されます。5 つ目のフェーズが 10 分以上たっても完了しない場合は、ページを手動で更新してください。
4. リカバリするアプライアンスグリッドノードのタイプに対応するリカバリプロセスの次の手順に進みます。

リカバリのタイプ	参考文献
ゲートウェイノード	"Start Recovery を選択して、ゲートウェイノードを設定します"
非プライマリ管理ノード	"[リカバリの開始 を選択して、非プライマリ管理ノードを設定します"]
プライマリ管理ノード	"交換用プライマリ管理ノードを設定"

テクニカルサポートによるStorageGRIDサイトの復旧方法

StorageGRID サイト全体に障害が発生した場合、または複数のストレージノードで障害が発生した場合は、テクニカルサポートにお問い合わせください。テクニカルサポートは、お客様の状況を評価し、リカバリプランを作成してから、障害が発生したノードまたはサイトをビジネス目標に沿った方法でリカバリし、リカバリ時間を最適化して、不要なデータ損失を防ぎます。

サイトリカバリは、テクニカルサポートのみが実行できます。

StorageGRID システムは、さまざまな障害に対する耐障害性を備えており、多くのリカバリ手順やメンテナンス手順を自分で実行できます。ただし、一般化された単純なサイトリカバリ手順 は作成が困難です。詳細な手順は、状況に固有の要因によって異なるためです。例：

- * あなたのビジネス目標 *: StorageGRID の場所の完全な損失の後、あなたのビジネス目的を満たす最もよい方法を評価するべきである。たとえば、失われたサイトをインプレースで再構築しますか？失われた StorageGRID サイトを新しい場所に交換しますか？お客様の状況はそれぞれ異なり、優先事項に対応するようにリカバリプランを設計する必要があります。
- 障害の正確な内容：サイトリカバリを開始する前に、障害が発生したサイトに損傷がないノードがないか、リカバリ可能なオブジェクトが含まれているストレージノードがないかを確認します。有効なデータが含まれているノードまたはストレージボリュームを再構築すると、不要なデータ損失が発生する可能性があります。
- アクティブな**ILM**ポリシー：グリッド内のオブジェクトコピーの数、タイプ、場所は、アクティブなILM

ポリシーによって制御されます。ILMポリシーの詳細は、リカバリ可能なデータの量やリカバリに必要な特定の手法に影響する可能性があります。

> サイトにオブジェクトの唯一のコピーが含まれていてサイトが失われると、そのオブジェクトは失われます。

- バケット（またはコンテナ）の整合性：バケット（またはコンテナ）に適用される整合性は、StorageGRIDがオブジェクトメタデータをすべてのノードとサイトに完全にレプリケートしてから、オブジェクトの取り込みが成功したことをクライアントに通知するかどうかに影響します。整合性の値で結果整合性が確保されている場合は、サイト障害時に一部のオブジェクトメタデータが失われている可能性があります。リカバリ可能なデータの量や、リカバリ手順 の詳細に影響する可能性があります。
- 最近の変更履歴：リカバリ手順の詳細は、障害発生時にメンテナンス手順を実行中かどうか、またはILMポリシーに最近変更が加えられたかどうかによって影響を受ける可能性があります。テクニカルサポートは、サイトのリカバリを開始する前に、グリッドの最新の履歴と現在の状況を評価する必要があります。

> サイトリカバリは、テクニカルサポートのみが実行できます。

次に、テクニカルサポートが障害が発生したサイトのリカバリに使用するプロセスの概要を示します。

1. テクニカルサポート：
   a. 障害の詳細な評価を行います。
   b. お客様と協力して、ビジネス目標を確認します。
   c. お客様の状況に合わせてリカバリプランを作成します。
2. プライマリ管理ノードで障害が発生した場合は、テクニカルサポートがそのノードをリカバリします。
3. テクニカルサポートは、以下の概要に従って、すべてのストレージノードをリカバリします。
   a. 必要に応じて、ストレージノードのハードウェアまたは仮想マシンを交換します。
   b. 障害が発生したサイトにオブジェクトメタデータをリストアする。
   c. リカバリしたストレージノードにオブジェクトデータをリストアします。

      > 単一の障害ストレージノードのリカバリ手順を使用すると、データが失われます。

   > サイト全体で障害が発生した場合、テクニカルサポートは専用のコマンドを使用してオブジェクトとオブジェクトメタデータをリストアします。

4. テクニカルサポートは障害が発生した他のノードをリカバリします

   オブジェクトメタデータとデータのリカバリが完了したら、テクニカルサポートは標準の手順に従って、障害が発生したゲートウェイノードまたは非プライマリ管理ノードをリカバリします。

関連情報

"サイトの運用停止"

StorageGRIDソリューションとリソース

へ移動 "StorageGRIDソリューションとリソース"StorageGRID環境でアプリケーションをテストおよび有効化する方法を学習します。

NetAppコンソールを使用してStorageGRIDを管理する方法

へ移動 "NetAppコンソールを使用したStorageGRID管理"Grid Manager を使用してNetAppコンソールからStorageGRIDシステムを管理する方法と、バックアップ、データ階層化などにNetAppコンソールのデータ サービスを使用する方法を学習します。

- BlueXPはNetAppコンソールになりました*

NetAppコンソールは、強化され再構築されたBlueXP基盤上に構築され、オンプレミスとクラウド環境全体にわたるエンタープライズ グレードのNetAppストレージとNetAppデータ サービスの集中管理を提供し、リアルタイムの分析情報、ワークフローの高速化、および高度なセキュリティとコンプライアンスを備えた簡素化された管理を実現します。

変更内容の詳細については、 "NetAppコンソールのリリースノート"。

法的通知

法的通知では、著作権に関する声明、商標、特許などにアクセスできます。

著作権

"https://www.netapp.com/company/legal/copyright/"

商標

NetApp、NetAppのロゴ、およびNetAppの商標ページに記載されているマークは、NetApp、Inc.の商標です。その他の会社名および製品名は、それを所有する各社の商標である場合があります。

"https://www.netapp.com/company/legal/trademarks/"

特許

NetAppが所有する特許の最新リストは、次のサイトで参照できます。

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

プライバシーポリシー

"https://www.netapp.com/company/legal/privacy-policy/"

APIライセンス

このドキュメントは、 StorageGRID S3 REST API に対するライセンスまたはその他の権利を付与するものではありません。StorageGRID S3 REST API の使用またはアクセスには、 NetAppとの個別のライセンス契約が必要であり、その契約に従います。

オープンソース

通知ファイルには、ネットアップソフトウェアで使用されるサードパーティの著作権およびライセンスに関する情報が記載されています。

https://library.netapp.com/ecm/ecm_download_file/ECMLP3351268

https://library.netapp.com/ecm/ecm_download_file/ECMLP3373066

著作権に関する情報

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

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

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

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

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

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

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

商標に関する情報

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