監視とトラブルシューティング
StorageGRID software

NetApp
December 03, 2025

This PDF was generated from https://docs.netapp.com/ja-jp/storagegrid-119/monitor/index.html on December 03, 2025. Always check docs.netapp.com for the latest.

目次

StorageGRIDシステムの監視とトラブルシューティング

StorageGRIDシステムを監視する

StorageGRIDシステムを監視する

StorageGRIDシステムを定期的に監視して、期待どおりに動作していることを確認します。

開始する前に

- グリッドマネージャにサインインするには、"サポートされているウェブブラウザ" 。
- あなたが持っている"特定のアクセス権限"。

> グリッド マネージャーに表示されるストレージ値の単位を変更するには、グリッド マネージャーの右上にあるユーザー ドロップダウンを選択し、*ユーザー設定*を選択します。

タスク概要

以下の手順では、次の方法について説明します。

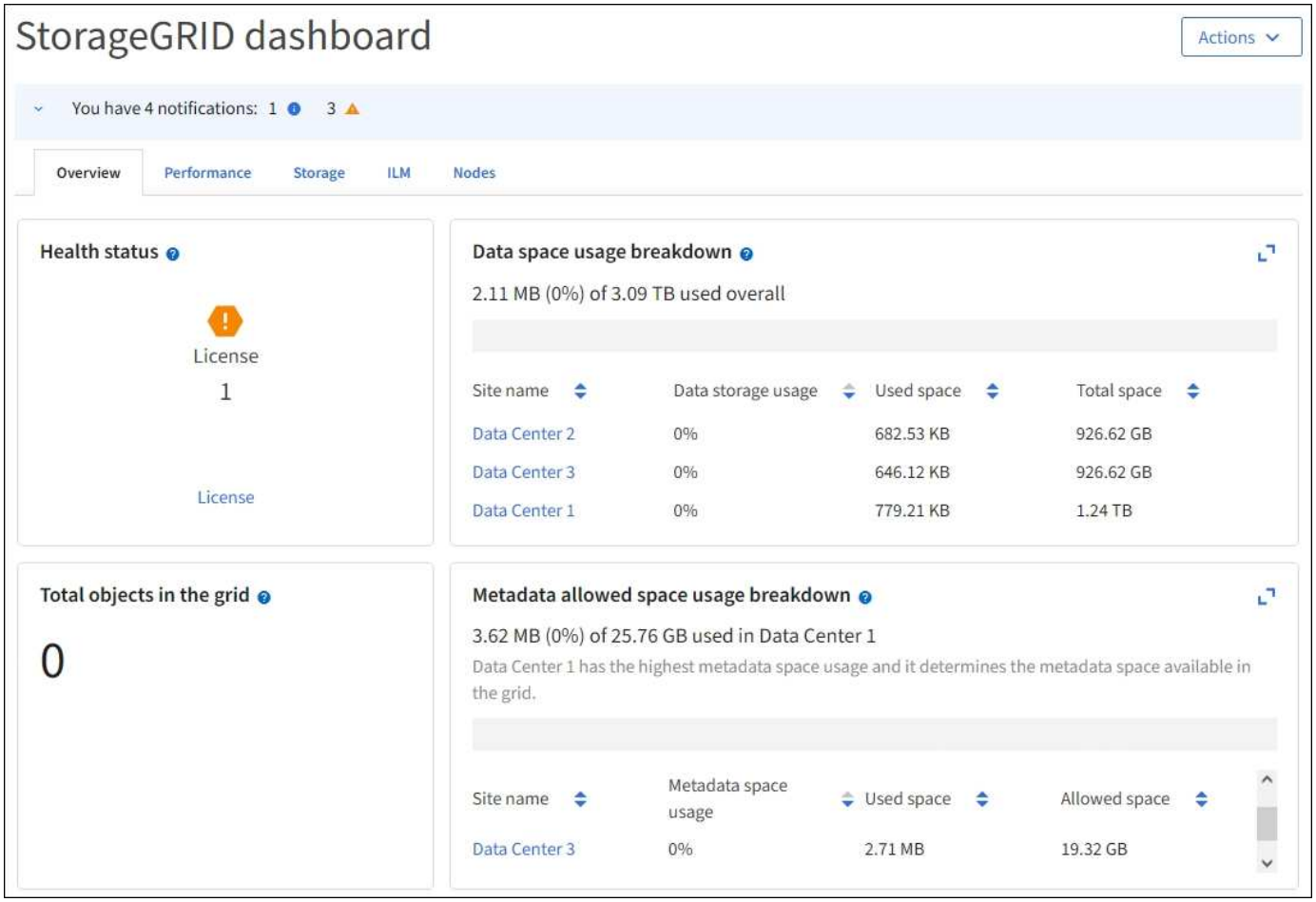
- "ダッシュボードの表示と管理"
- "ノードページを表示する"
- "システムの次の側面を定期的に監視します。"
  - "システム ヘルス"
  - "ストレージ容量"
  - "情報ライフサイクル管理"
  - "ネットワークとシステムリソース"
  - "テナント活動"
  - "負荷分散操作"
  - "グリッドフェデレーション接続"
- "アラートを管理する"
- "ログファイルを表示する"
- "監査メッセージとログの保存先を構成する"
- "外部のSyslogサーバーを使用する"監査情報を収集する
- "監視にはSNMPを使用する"
- "追加のStorageGRIDデータを取得する"指標と診断を含む

ダッシュボードの表示と管理

ダッシュボードを使用すると、システムアクティビティを一目で監視できます。カスタム ダッシュボードを作成して、 StorageGRIDの実装を監視できます。

> グリッド マネージャーに表示されるストレージ値の単位を変更するには、グリッド マネージャーの右上にあるユーザー ドロップダウンを選択し、*ユーザー設定*を選択します。

ダッシュボードはシステム構成によって異なる場合があります。



ダッシュボードを見る

ダッシュボードは、 StorageGRIDシステムに関する特定の情報が含まれるタブで構成されています。各タブには、カードに表示される情報のカテゴリが含まれています。

システム提供のダッシュボードをそのままご利用いただけます。さらに、 StorageGRIDの実装の監視に関連するタブとカードのみを含むカスタム ダッシュボードを作成することもできます。

システムが提供するダッシュボード タブには、次の種類の情報を含むカードが含まれています。

システム提供のダッシュボードのタブ	含む
概要	アクティブなアラート、スペースの使用状況、グリッド内のオブジェクトの合計数など、グリッドに関する一般情報。
パフォーマンス	スペース使用量、時間の経過に伴うストレージ使用量、S3 操作、リクエスト期間、エラー率。
ストレージ	テナントのクォータ使用量と論理スペース使用量。ユーザーデータとメタデータのスペース使用量の予測。
ILM	情報ライフサイクル管理キューと評価率。
ノード	ノード別の CPU、データ、およびメモリの使用量。ノードごとの S3 操作。ノードからサイトへの配布。

一部のカードは最大化して見やすくすることができます。最大化アイコンを選択カードの右上隅にあります。最大化されたカードを閉じるには、最小化アイコンを選択しますまたは、[閉じる] を選択します。

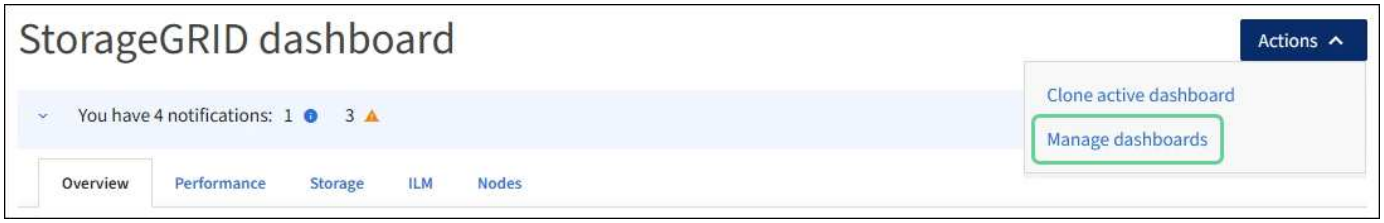
ダッシュボードを管理する

ルートアクセス権がある場合（"管理者グループの権限") では、ダッシュボードに対して次の管理タスクを実行できます。

- カスタムダッシュボードを最初から作成します。カスタム ダッシュボードを使用すると、表示されるStorageGRID情報とその情報の構成方法を制御できます。
- ダッシュボードを複製してカスタム ダッシュボードを作成します。
- ユーザーにアクティブなダッシュボードを設定します。アクティブなダッシュボードは、システム提供のダッシュボードまたはカスタム ダッシュボードにすることができます。
- デフォルトのダッシュボードを設定します。これは、ユーザーが独自のダッシュボードをアクティブ化しない限り、すべてのユーザーに表示されるものです。
- ダッシュボード名を編集します。
- ダッシュボードを編集して、タブやカードを追加または削除します。最小 1 個、最大 20 個のタブを作成できます。
- ダッシュボードを削除します。

ルート アクセス以外の権限がある場合は、アクティブなダッシュボードのみを設定できます。

ダッシュボードを管理するには、[アクション] > [ダッシュボードの管理] を選択します。



ダッシュボードを構成する

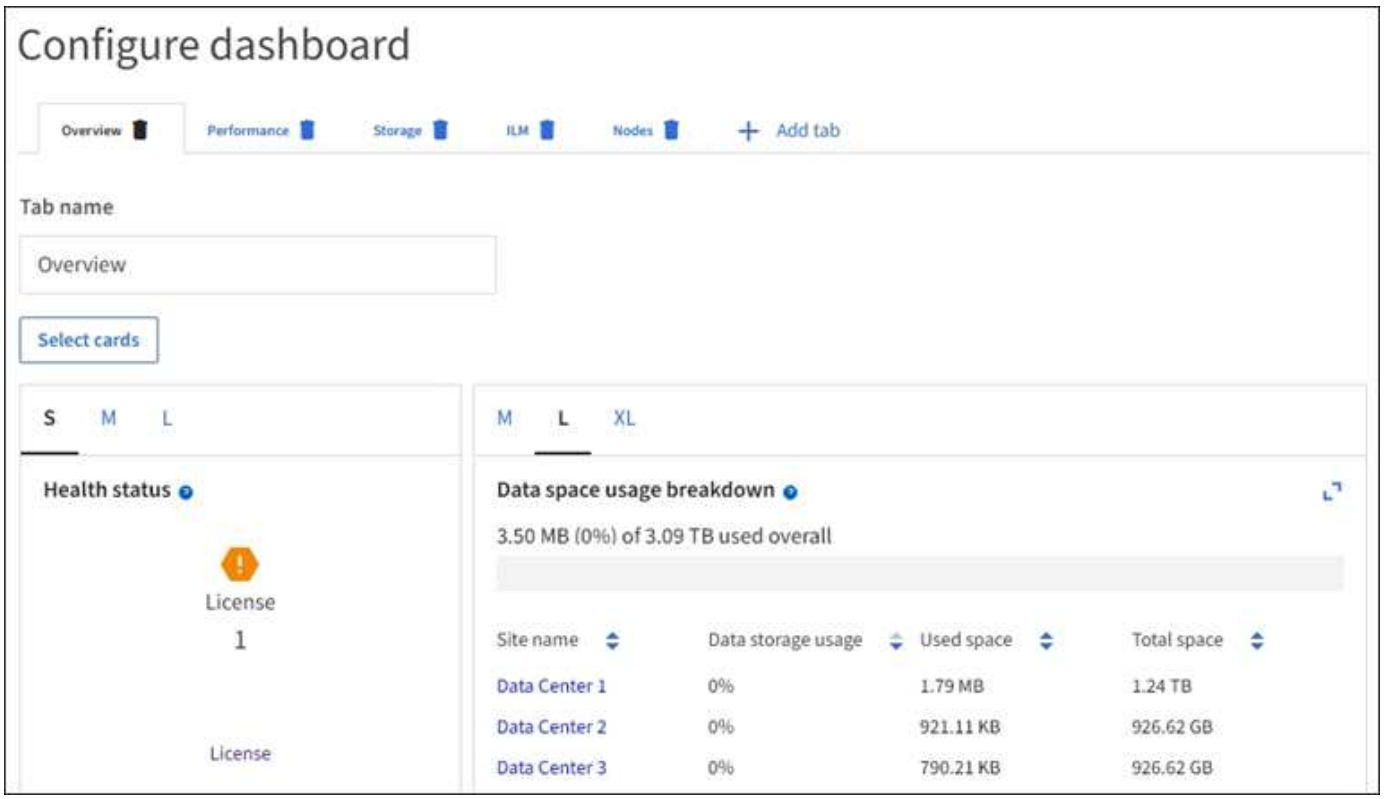
アクティブなダッシュボードを複製して新しいダッシュボードを作成するには、[アクション] > [アクティブなダッシュボードの複製*] を選択します。

既存のダッシュボードを編集または複製するには、[アクション] > [ダッシュボードの管理] を選択します。

システム提供のダッシュボードは編集または削除できません。

ダッシュボードを構成するときには、次のことが可能です。

- タブを追加または削除する
- タブの名前を変更し、新しいタブに一意の名前を付けます
- 各タブのカードを追加、削除、または並べ替え（ドラッグ）します
- カードの上部にある*S*、**M**、**L**、*XL*を選択して、個々のカードのサイズを選択します。



ノードページを表示する

ノードページを表示する

ダッシュボードで提供される情報よりも詳細なStorageGRIDシステム情報が必要な場合は、[ノード] ページを使用して、グリッド全体、グリッド内の各サイト、およびサイトの各ノードのメトリックを表示できます。

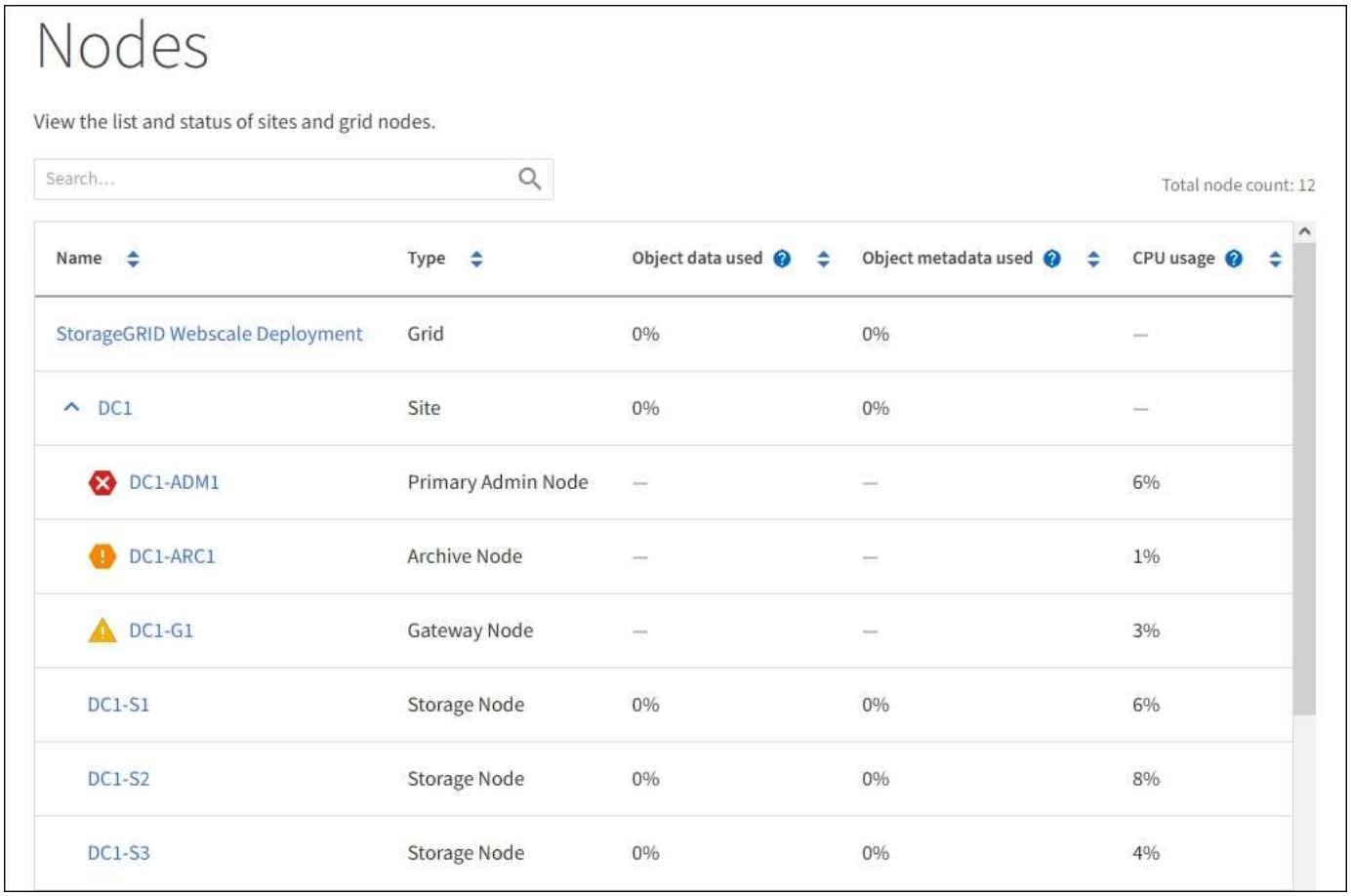
ノード テーブルには、グリッド全体、各サイト、および各ノードの概要情報がリストされます。ノードが切断されているか、アクティブなアラートがある場合は、ノード名の横にアイコンが表示されます。ノードが接

続されていてアクティブなアラートがない場合は、アイコンは表示されません。

アップグレード中や切断状態など、ノードがグリッドに接続されていない場合、特定のメトリックは利用できなくなるか、サイトとグリッドの合計から除外される可能性があります。ノードがグリッドに再接続した後、値が安定するまで数分間待ちます。

グリッド マネージャーに表示されるストレージ値の単位を変更するには、グリッド マネージャーの右上にあるユーザー ドロップダウンを選択し、*ユーザー設定*を選択します。

表示されているスクリーンショットは例です。結果はStorageGRID のバージョンによって異なる場合があります。



接続状態アイコン

ノードがグリッドから切断されている場合、ノード名の横に次のいずれかのアイコンが表示されます。

アイコン	説明	必要なアクション
	接続されていません - 不明 不明な理由により、ノードが切断されたか、ノード上のサービスが予期せず停止しました。たとえば、ノード上のサービスが停止したり、停電や予期しない停止のためにノードのネットワーク接続が失われたりする可能性があります。 ノードと通信できません というアラートもトリガーされる可能性があります。他のアラートもアクティブになっている可能性があります。	すぐに対処する必要があります。"各アラートを選択"推奨されるアクションに従ってください。 たとえば、停止したサービスを再起動したり、ノードのホストを再起動したりする必要がある場合があります。 注意: 管理されたシャットダウン操作中に、ノードが「不明」と表示される場合があります。このような場合には、不明状態を無視できます。
	接続されていません - 管理上ダウンしています 予想された理由により、ノードはグリッドに接続されていません。 たとえば、ノードまたはノード上のサービスが正常にシャットダウンされた、ノードが再起動中、またはソフトウェアがアップグレード中などです。 1 つ以上のアラートがアクティブになっている可能性もあります。 根本的な問題によっては、これらのノードは介入なしにオンラインに戻ることがよくあります。	このノードに影響するアラートがあるかどうかを判断します。 1つ以上のアラートがアクティブになっている場合、"各アラートを選択"推奨されるアクションに従ってください。

ノードがグリッドから切断されている場合、根本的なアラートが発生している可能性がありますが、「接続されていません」アイコンのみが表示されます。ノードのアクティブなアラートを表示するには、ノードを選択します。

アラートアイコン

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

重大: StorageGRIDノードまたはサービスの通常の操作を停止させる異常な状態が発生しています。根本的な問題に直ちに対処する必要があります。問題が解決されない場合、サービスが中断され、データが失われる可能性があります。

重大: 現在の操作に影響を及ぼしているか、重大なアラートのしきい値に近づいている異常な状態が存在します。異常な状態によってStorageGRIDノードまたはサービスの通常の動作が停止しないように、主要なアラートを調査して根本的な問題に対処する必要があります。

軽微: システムは正常に動作していますが、継続するとシステムの動作能力に影響を及ぼす可能性のある異常な状態が存在します。より深刻な問題を引き起こさないように、自然に消えない軽微なアラートを監視して解決する必要があります。

システム、サイト、またはノードの詳細を表示する

ノード テーブルに表示される情報をフィルターするには、[検索] フィールドに検索文字列を入力します。システム名、表示名、またはタイプで検索できます (たとえば、すべてのゲートウェイ ノードをすばやく見つけるには、**gat** と入力します)。

グリッド、サイト、またはノードの情報を表示するには:

- グリッド名を選択すると、 StorageGRIDシステム全体の統計の集計概要が表示されます。
- 特定のデータセンター サイトを選択すると、そのサイトのすべてのノードの統計の集計概要が表示されます。
- 特定のノードを選択すると、そのノードの詳細情報が表示されます。

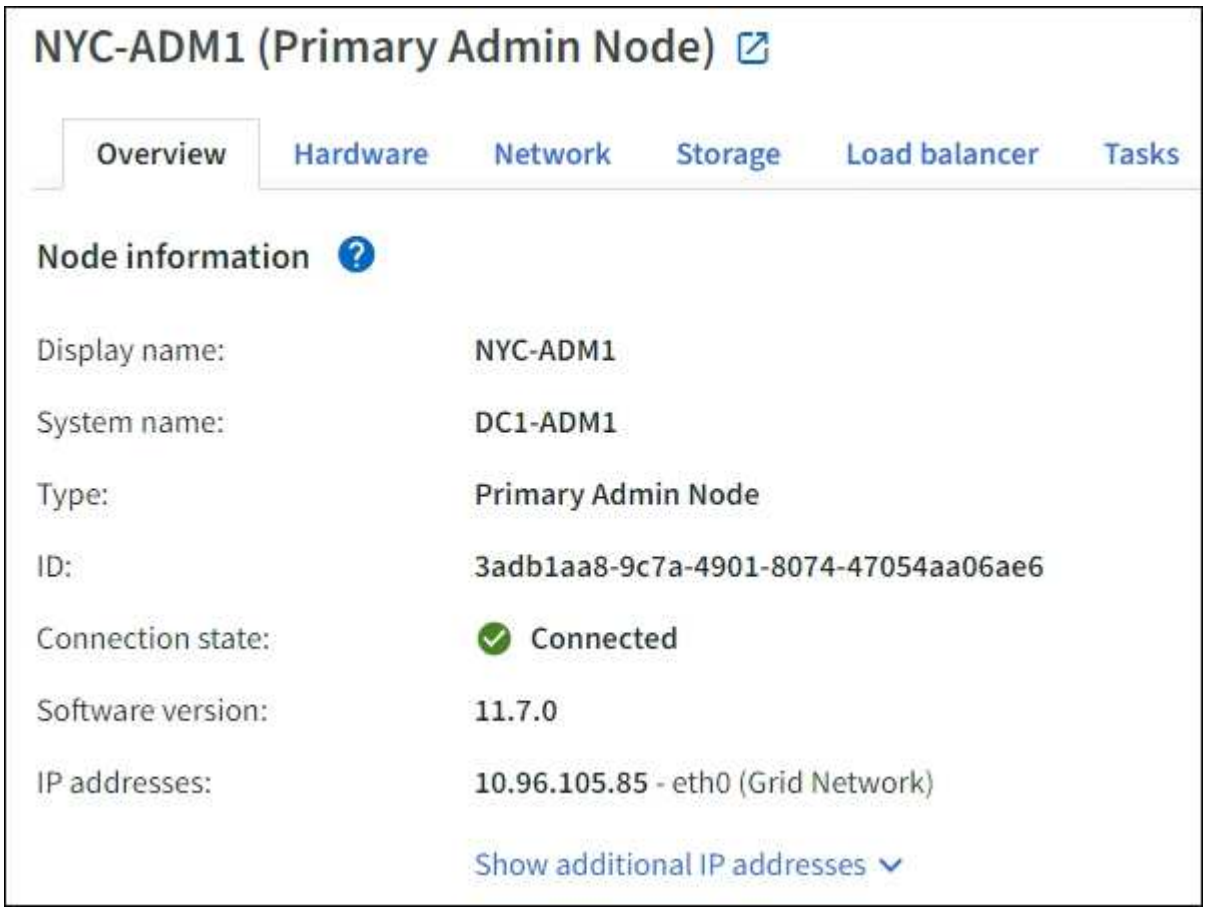
概要タブを表示する

「概要」タブには、各ノードに関する基本情報が表示されます。また、現在ノードに影響を与えているアラートも表示されます。

すべてのノードに対して概要タブが表示されます。

ノード情報

[概要] タブの [ノード情報] セクションには、ノードに関する基本情報が一覧表示されます。



ノードの概要情報には次のものが含まれます。

- 表示名 (ノードの名前が変更された場合にのみ表示されます): ノードの現在の表示名。使用"グリッド、サイト、ノードの名前を変更する"この値を更新する手順。
- システム名: インストール時にノードに入力した名前。システム名はStorageGRID の内部操作に使用され、変更できません。
- タイプ: ノードのタイプ (管理ノード、プライマリ管理ノード、ストレージ ノード、またはゲートウェイ ノード)。
- **ID**: ノードの一意の識別子。UUID とも呼ばれます。
- 接続状態: 3 つの状態のうちの 1 つ。最も深刻な状態のアイコンが表示されます。
  - 未知*  **:** 不明な理由により、ノードがグリッドに接続されていないか、**1** つ以上のサービスが予期せず停止しています。たとえば、ノード間のネットワーク接続が失われたり、電源が落ちたり、サービスが停止したりした場合などです。 *ノードと通信できません というアラートもトリガーされる可能性があります。他のアラートもアクティブになっている可能性があります。この状況には即時の対処が必要です。

    > 管理されたシャットダウン操作中に、ノードが「不明」として表示される場合があります。このような場合には、不明状態を無視できます。

  - *管理上ダウン*  : 予期された理由により、ノードはグリッドに接続されていません。たとえば、ノードまたはノード上のサービスが正常にシャットダウンされた、ノードが再起動中、またはソフトウェアがアップグレード中などです。 1 つ以上のアラートがアクティブになっている可能性もあります。
  - *接続済み*  : ノードはグリッドに接続されています。
- 使用ストレージ: ストレージノードのみ。
  - オブジェクト データ: ストレージ ノードで使用されているオブジェクト データの合計使用可能スペースの割合。
  - オブジェクト メタデータ: ストレージ ノードで使用されているオブジェクト メタデータに許可されている合計スペースの割合。
- ソフトウェア バージョン: ノードにインストールされているStorageGRIDのバージョン。
- **HA** グループ: 管理ノードとゲートウェイ ノードのみ。ノード上のネットワーク インターフェイスが高可用性グループに含まれているかどうか、およびそのインターフェイスがプライマリ インターフェイスであるかどうかが表示されます。
- **IP** アドレス: ノードの IP アドレス。ノードの IPv4 および IPv6 アドレスとインターフェース マッピングを表示するには、[追加の **IP** アドレスを表示] をクリックします。

アラート

「概要」タブの「アラート」セクションには、"現在このノードに影響を与えているが、サイレント化されていないアラート" 。アラート名を選択すると、追加の詳細と推奨されるアクションが表示されます。

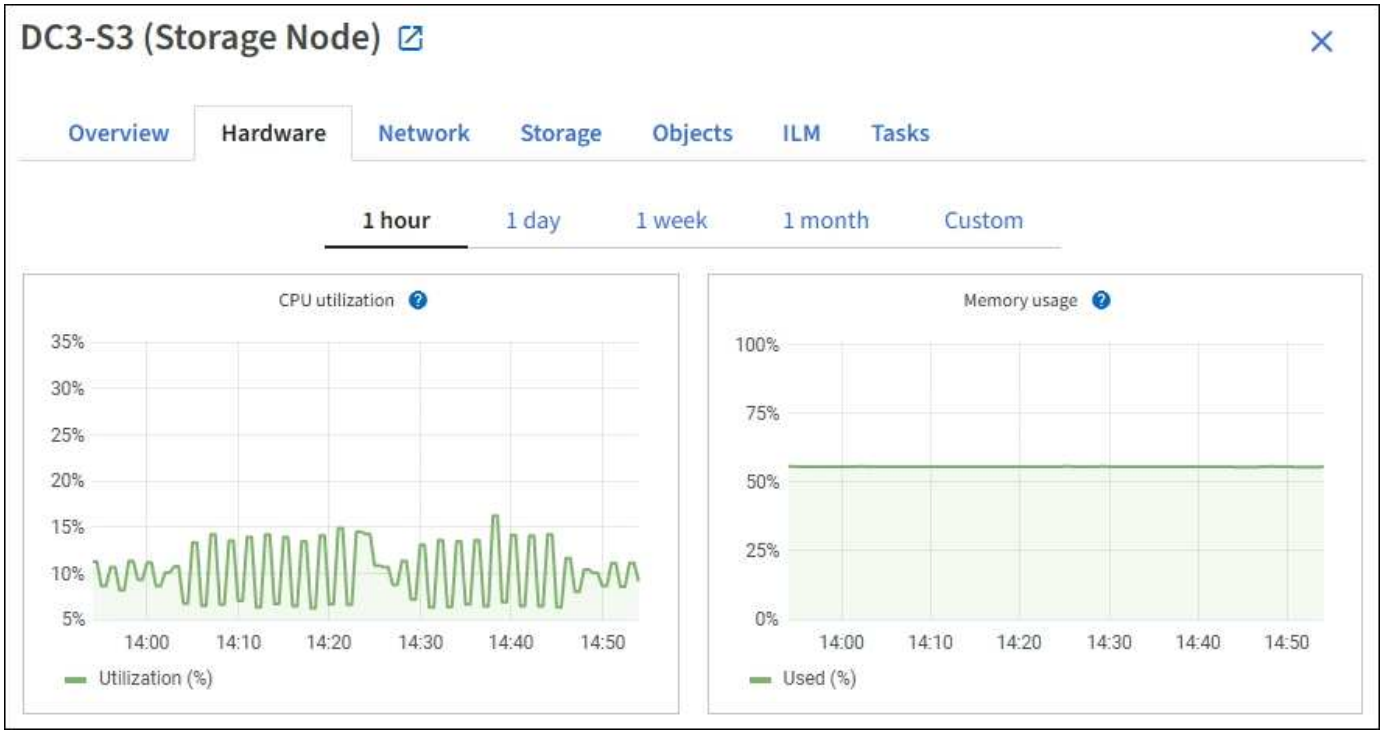
アラートには以下も含まれています"ノード接続状態"。

ハードウェアタブを表示する

[ハードウェア] タブには、各ノードの CPU 使用率とメモリ使用量、およびアプライアンスに関する追加のハードウェア情報が表示されます。

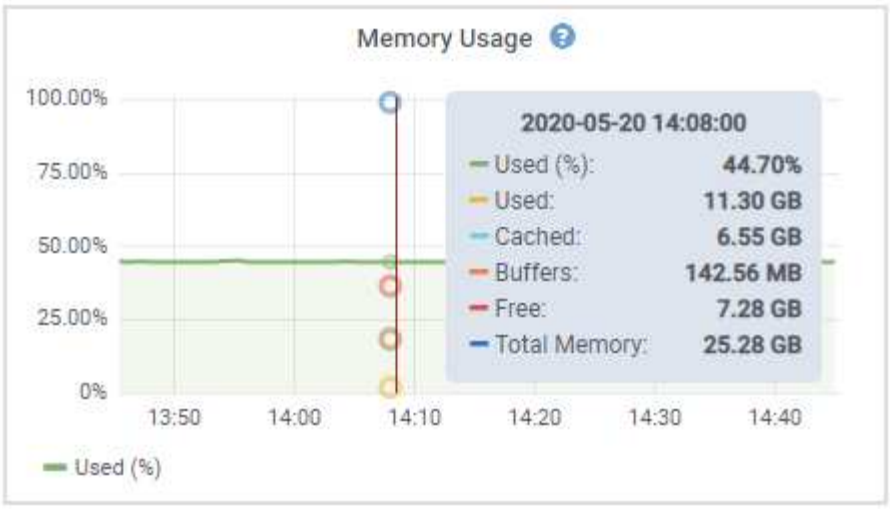
グリッド マネージャーはリリースごとに更新されるため、このページのサンプルのスクリーンショットと一致しない場合があります。

すべてのノードに対してハードウェア タブが表示されます。



異なる時間間隔を表示するには、チャートまたはグラフの上にあるコントロールのいずれかを選択します。 1 時間、1 日、1 週間、1 か月の間隔で情報を表示できます。カスタム間隔を設定して、日付と時刻の範囲を指定することもできます。

CPU 使用率とメモリ使用量の詳細を表示するには、各グラフの上にカーソルを置きます。



ノードがアプライアンス ノードの場合、このタブにはアプライアンス ハードウェアに関する詳細情報のセクションも含まれます。

アプライアンス ストレージ ノードに関する情報を表示する

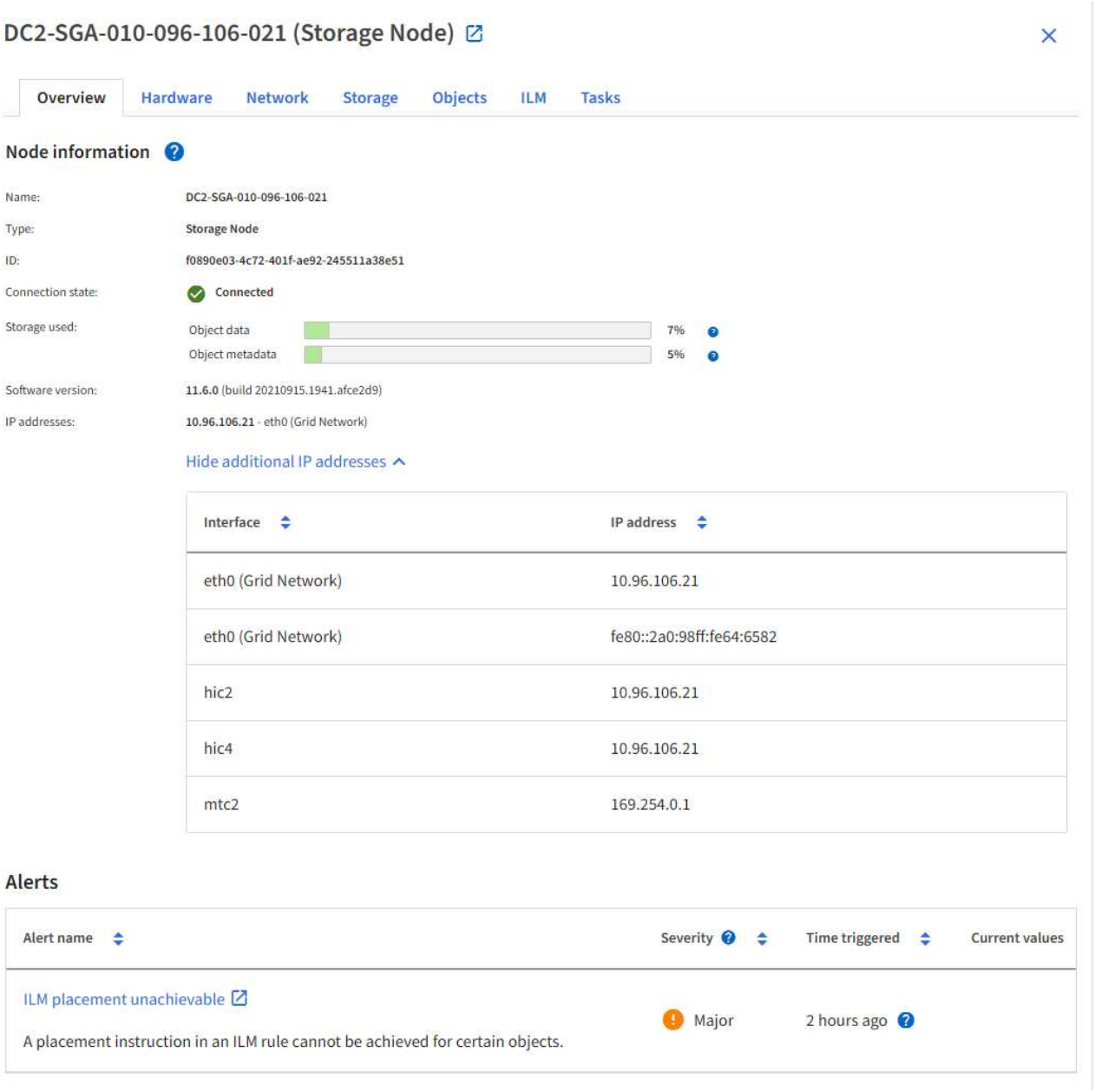
ノード ページには、各アプライアンス ストレージ ノードのサービス ヘルスとすべてのコンピューティング、ディスク デバイス、およびネットワーク リソースに関する情報が一覧表示されます。メモリ、ストレージ ハードウェア、コントローラー ファームウェア バージョン、ネットワーク リソース、ネットワーク インターフェイス、ネットワーク アドレスを確認したり、データの受信と送信を行ったりすることもできます。

手順

1. 「ノード」ページから、アプライアンス ストレージ ノードを選択します。
2. *概要*を選択します。

   [概要] タブの [ノード情報] セクションには、ノードの名前、タイプ、ID、接続状態など、ノードの概要情報が表示されます。 IP アドレスのリストには、次のように各アドレスのインターフェース名が含まれます。

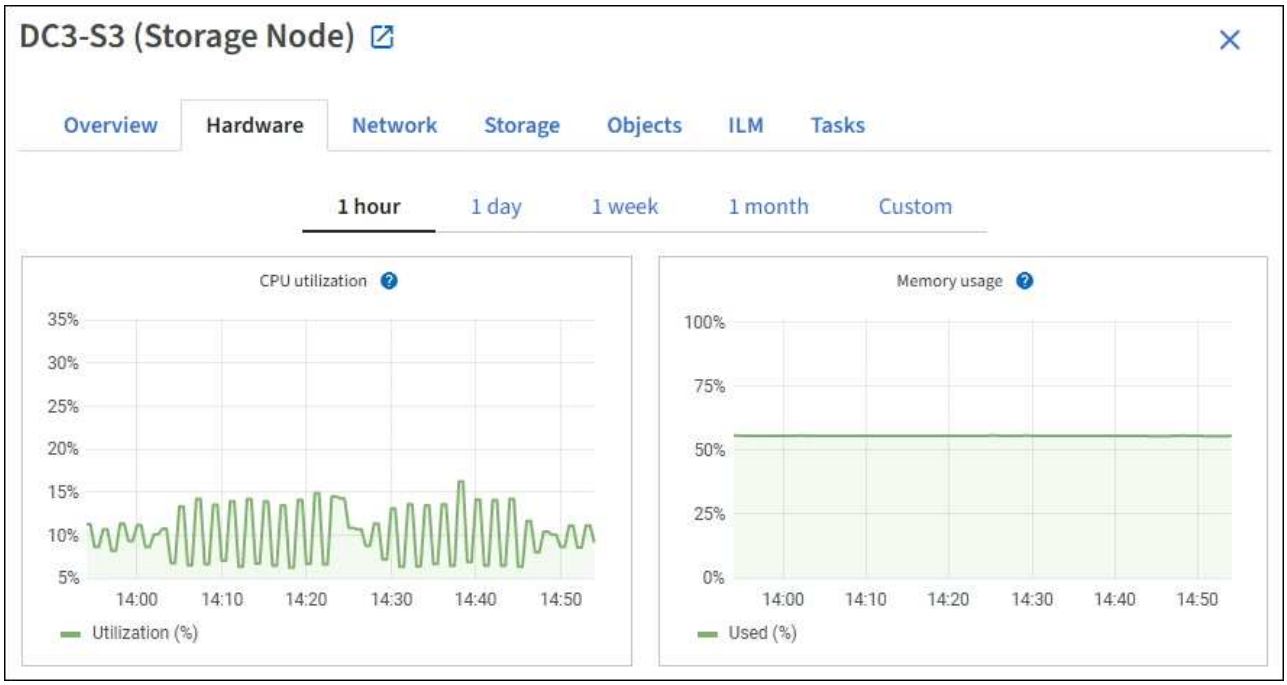
   - **eth**: グリッド ネットワーク、管理ネットワーク、またはクライアント ネットワーク。
   - **hic**: アプライアンス上の物理的な 10、25、または 100 GbE ポートの 1 つ。これらのポートは結合して、 StorageGRIDグリッド ネットワーク (eth0) およびクライアント ネットワーク (eth2) に接続できます。
   - **mtc**: アプライアンス上の物理 1 GbE ポートの 1 つ。 1 つ以上の mtc インターフェイスが結合されて、 StorageGRID管理ネットワーク インターフェイス (eth1) を形成します。他の mtc インターフェイスは、データ センターの技術者が一時的にローカル接続できるように残しておくことができます。



[概要] タブの [アラート] セクションには、ノードのアクティブなアラートが表示されます。

3. アプライアンスの詳細情報を表示するには、「ハードウェア」を選択します。

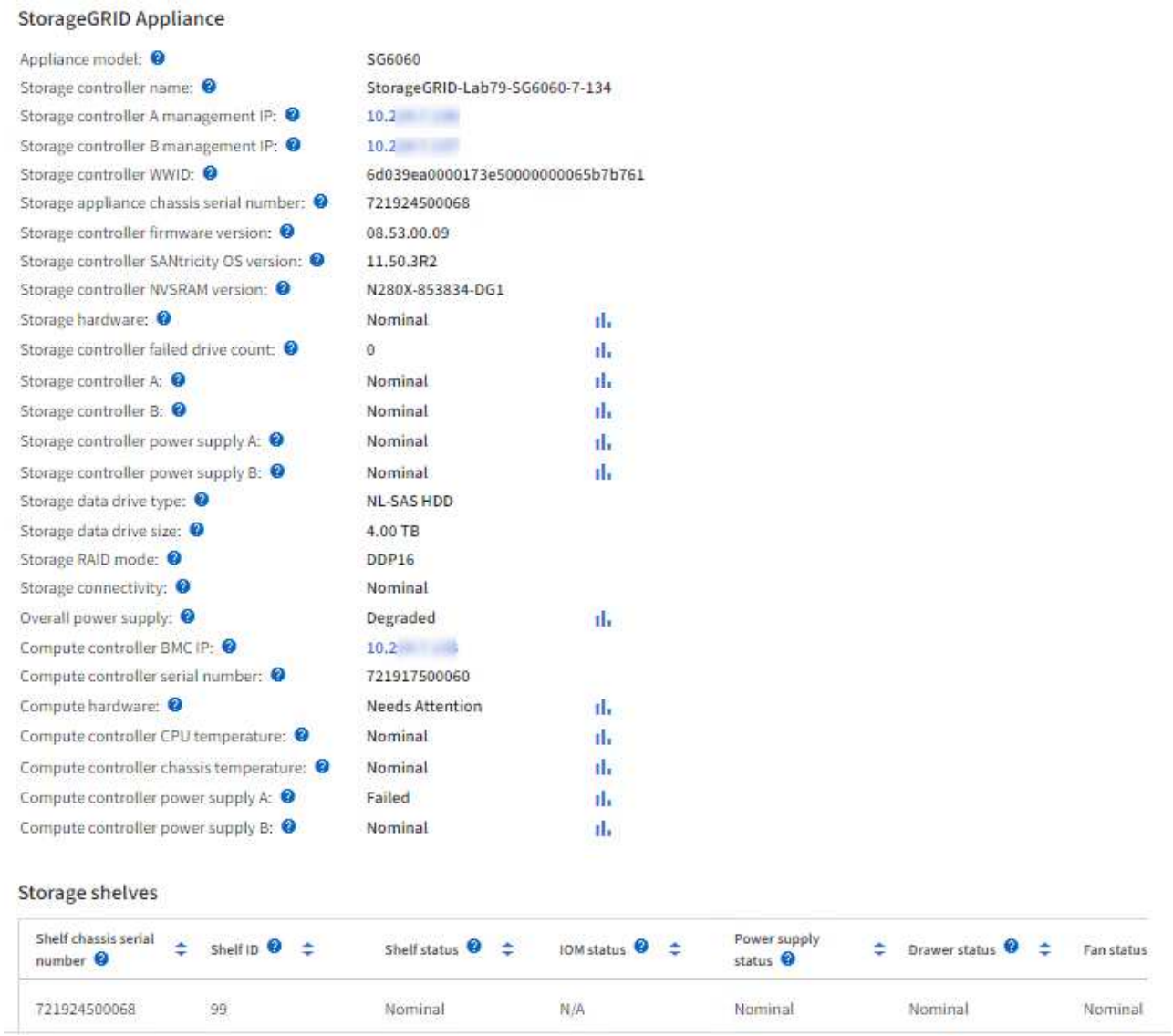
   a. CPU 使用率とメモリのグラフを表示して、時間の経過に伴う CPU とメモリの使用率の割合を確認します。異なる時間間隔を表示するには、チャートまたはグラフの上にあるコントロールのいずれかを選択します。 1 時間、1 日、1 週間、1 か月の間隔で情報を表示できます。カスタム間隔を設定して、日付と時刻の範囲を指定することもできます。



b. 下にスクロールして、アプライアンスのコンポーネント表を表示します。このテーブルには、アプライアンスのモデル名、コントローラ名、シリアル番号、IP アドレス、各コンポーネントのステータスなどの情報が含まれています。

> コンピューティング コントローラーBMC IP やコンピューティング ハードウェアなどの一部のフィールドは、その機能を備えたアプライアンスに対してのみ表示されます。

ストレージ シェルフのコンポーネント、およびインストールの一部である場合には拡張シェルフのコンポーネントは、アプライアンス テーブルの下の別のテーブルに表示されます。



アプライアンステーブルのフィールド	説明
アプライアンスモデル	SANtricity OS に表示されるこのStorageGRIDアプライアンスのモデル番号。
ストレージコントローラ名	SANtricity OS に表示されるこのStorageGRIDアプライアンスの名前。
ストレージコントローラA管理IP	ストレージ コントローラ A の管理ポート 1 の IP アドレス。この IP を使用してSANtricity OS にアクセスし、ストレージの問題をトラブルシューティングします。

アプライアンステーブルのフィールド	説明
ストレージコントローラB管理IP	ストレージ コントローラ B の管理ポート 1 の IP アドレス。この IP を使用してSANtricity OS にアクセスし、ストレージの問題をトラブルシューティングします。 一部のアプライアンス モデルにはストレージ コントローラ B がありません。
ストレージコントローラのWWID	SANtricity OS に表示されるストレージ コントローラのワールドワイド識別子。
ストレージアプライアンスシャーシのシリアル番号	アプライアンスのシャーシのシリアル番号。
ストレージコントローラのファームウェアバージョン	このアプライアンスのストレージ コントローラ上のファームウェアのバージョン。
ストレージコントローラSANtricity OSバージョン	ストレージ コントローラ A のSANtricity OS バージョン。
ストレージコントローラのNVSRAMバージョン	SANtricity System Manager によって報告されるストレージ コントローラの NVSRAM バージョン。 SG6060 および SG6160 の場合、2 つのコントローラ間で NVSRAM のバージョンが一致しない場合は、コントローラ A のバージョンが表示されます。コントローラ A がインストールされていないか動作していない場合は、コントローラ B のバージョンが表示されます。
ストレージハードウェア	ストレージ コントローラ ハードウェアの全体的なステータス。SANtricity System Manager がストレージ ハードウェアのステータスを「要注意」と報告した場合、 StorageGRIDシステムもこの値を報告します。 ステータスが「注意が必要」の場合は、まずSANtricity OS を使用してストレージ コントローラーを確認します。次に、コンピューティング コントローラーに適用される他のアラートが存在しないことを確認します。
ストレージコントローラの障害ドライブ数	最適ではないドライブの数。
ストレージコントローラA	ストレージ コントローラ A のステータス。
ストレージコントローラB	ストレージ コントローラ B のステータス。一部のアプライアンス モデルにはストレージ コントローラ B がありません。

アプライアンステーブルのフィールド	説明
ストレージコントローラ電源A	ストレージ コントローラの電源 A のステータス。
ストレージコントローラ電源B	ストレージ コントローラの電源 B のステータス。
ストレージデータドライブの種類	アプライアンス内のドライブの種類 (HDD (ハード ドライブ) や SSD (ソリッド ステート ドライブ) など)。
ストレージデータドライブのサイズ	1 つのデータ ドライブの有効サイズ。 SG6160 の場合、キャッシュ ドライブのサイズも表示されます。 注: 拡張シェルフを備えたノードの場合は、各シェルフのデータドライブサイズその代わり。有効なドライブ サイズはシェルフによって異なる場合があります。
ストレージRAIDモード	アプライアンスに設定されている RAID モード。
ストレージ接続	ストレージの接続状態。
全体的な電源供給	アプライアンスのすべての電源のステータス。
コンピューティングコントローラBMC IP	コンピューティング コントローラー内のベースボード管理コントローラー (BMC) ポートの IP アドレス。この IP を使用してBMCインターフェイスに接続し、アプライアンスのハードウェアを監視および診断します。 このフィールドは、 BMCが含まれていないアプライアンス モデルでは表示されません。
コンピューティングコントローラのシリアル番号	コンピューティング コントローラーのシリアル番号。
コンピューティングハードウェア	コンピューティング コントローラー ハードウェアのステータス。このフィールドは、コンピューティング ハードウェアとストレージ ハードウェアが別々になっていないアプライアンス モデルでは表示されません。
コンピューティングコントローラのCPU温度	コンピューティング コントローラーの CPU の温度状態。
コンピューティングコントローラシャーシの温度	コンピューティング コントローラーの温度状態。

+

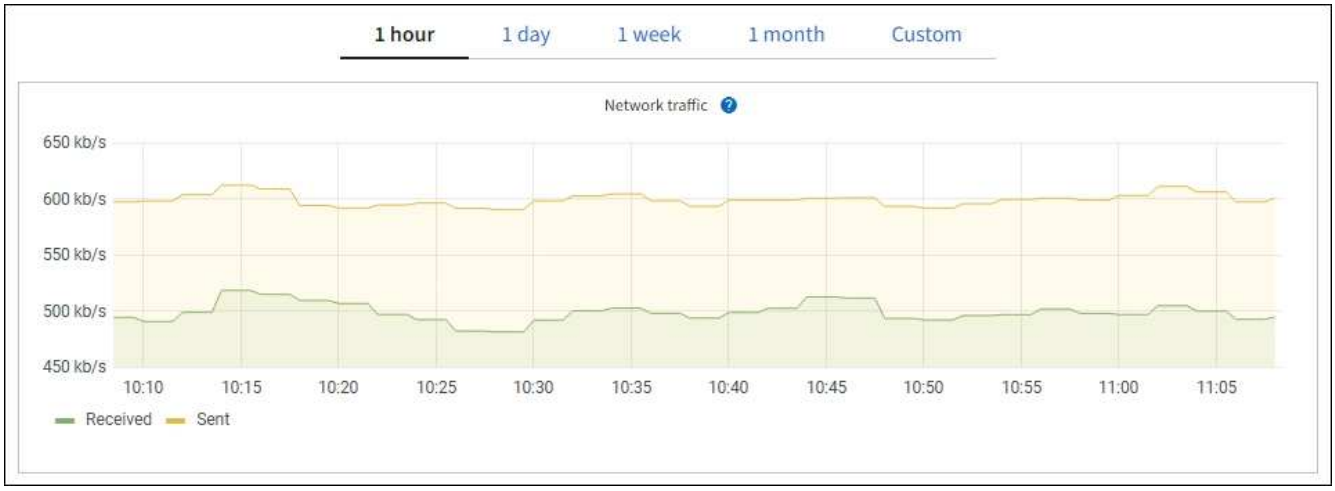
保管棚テーブルの列	説明
棚シャーシのシリアル番号	ストレージ シェルフ シャーシのシリアル番号。
Shelf ID	ストレージ シェルフの数値識別子。 • 99: ストレージコントローラシェルフ • 0: 最初の拡張棚 • 1: 2番目の拡張棚 注: 拡張シェルフは SG6060 および SG6160 にのみ適用されます。
棚の状態	保管棚の全体的な状態。
IOMのステータス	拡張シェルフ内の入出力モジュール (IOM) のステータス。拡張シェルフでない場合は N/A となります。
電源装置ステータス	ストレージ シェルフの電源の全体的な状態。
引き出しのステータス	収納棚の引き出しの状態。棚に引き出しがない場合は N/A となります。
ファンのステータス	ストレージ シェルフ内の冷却ファンの全体的な状態。
ドライブスロット	ストレージ シェルフ内のドライブ スロットの合計数。
データドライブ	ストレージ シェルフ内のデータ ストレージに使用されるドライブの数。
データドライブのサイズ	ストレージ シェルフ内の 1 つのデータ ドライブの有効サイズ。
キャッシュドライブ	ストレージ シェルフ内でキャッシュとして使用されるドライブの数。
キャッシュドライブサイズ	ストレージ シェルフ内の最小のキャッシュ ドライブのサイズ。通常、キャッシュ ドライブはすべて同じサイズです。
設定ステータス	ストレージ シェルフの構成ステータス。

a. すべてのステータスが「正常」であることを確認します。

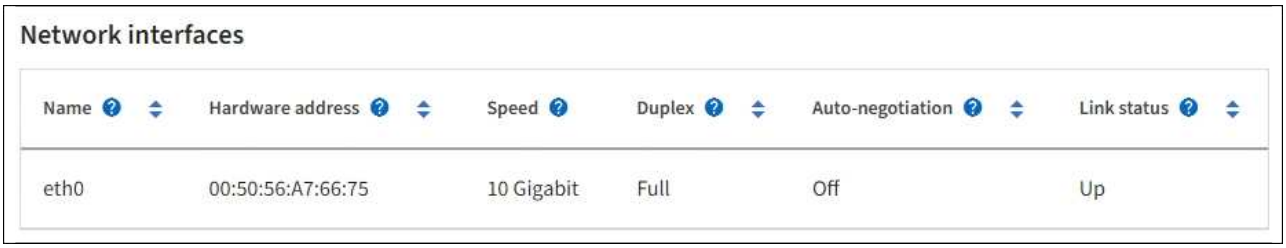
   ステータスが「正常」でない場合は、現在のアラートを確認してください。 SANtricity System Manager を使用して、これらのハードウェア値の一部について詳しく知ることもできます。アプライアンスのインストールとメンテナンスの手順を参照してください。

4. 各ネットワークの情報を表示するには、「ネットワーク」を選択します。

ネットワーク トラフィック グラフには、全体的なネットワーク トラフィックの概要が表示されます。



a. ネットワーク インターフェイス セクションを確認します。



次の表とネットワーク インターフェイス テーブルの 速度 列の値を使用して、アプライアンス上の 10/25 GbE ネットワーク ポートがアクティブ/バックアップ モードまたは LACP モードを使用するように構成されているかどうかを判断します。

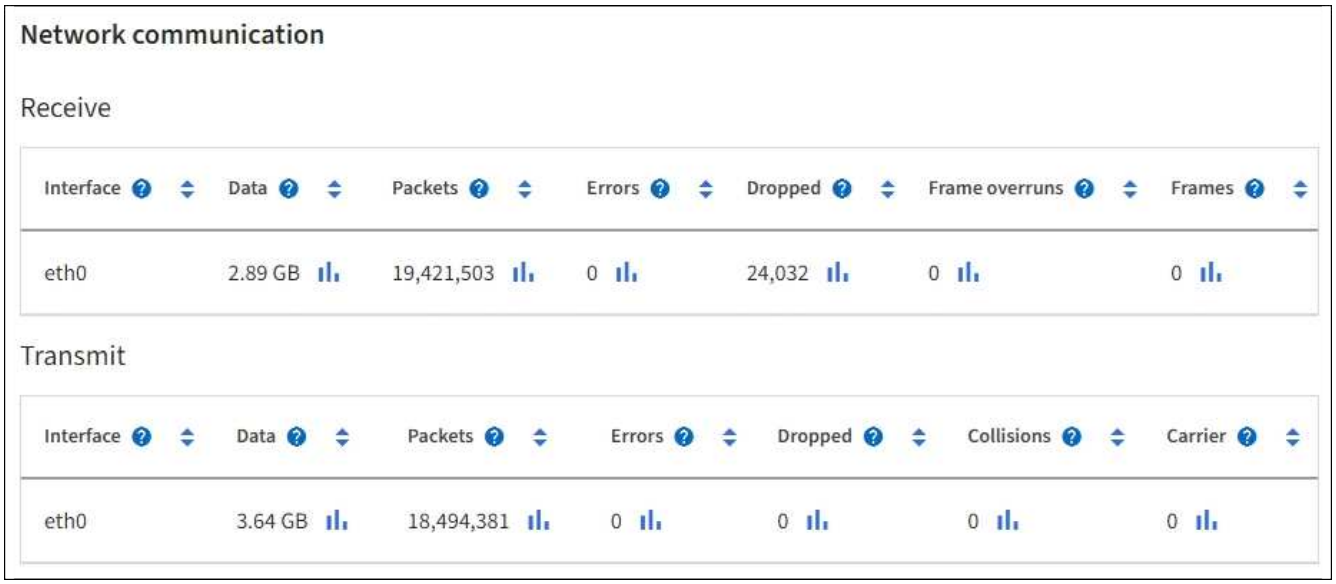
表に示されている値は、4 つのリンクすべてが使用されていることを前提としています。

リンクモード	ボンドモード	個々の**HIC**リンク速度（**hic1**、**hic2**、**hic3**、**hic4**）	予想されるグリッド/クライアントネットワーク速度 **(eth0**、**eth2)**
Aggregate	LACP	25	100
固定	LACP	25	50
固定	アクティブ/バックアップ	25	25
Aggregate	LACP	10	40
固定	LACP	10	20
固定	アクティブ/バックアップ	10	10

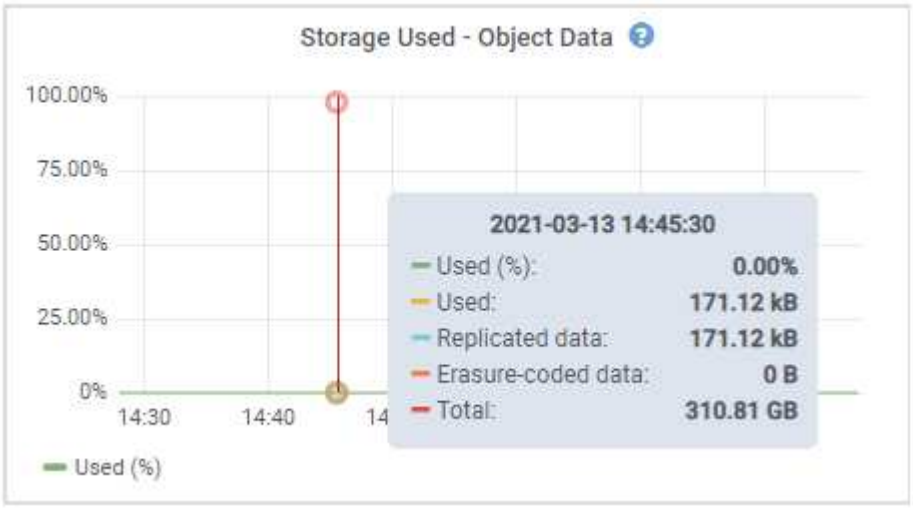
見る "ネットワークリンクを構成する"10/25 GbE ポートの設定の詳細については、こちらをご覧ください。

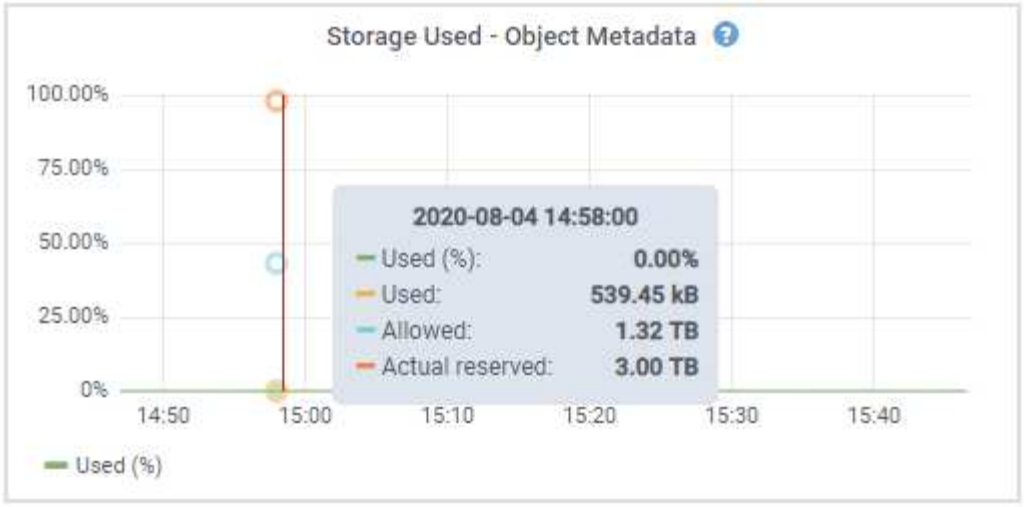
b. ネットワーク通信セクションを確認します。

受信テーブルと送信テーブルには、各ネットワークで受信および送信されたバイト数とパケット数、およびその他の受信および送信メトリックが表示されます。



5. ストレージ を選択すると、オブジェクト データとオブジェクト メタデータに時間の経過とともに使用されたストレージの割合、およびディスク デバイス、ボリューム、オブジェクト ストアに関する情報を示すグラフが表示されます。

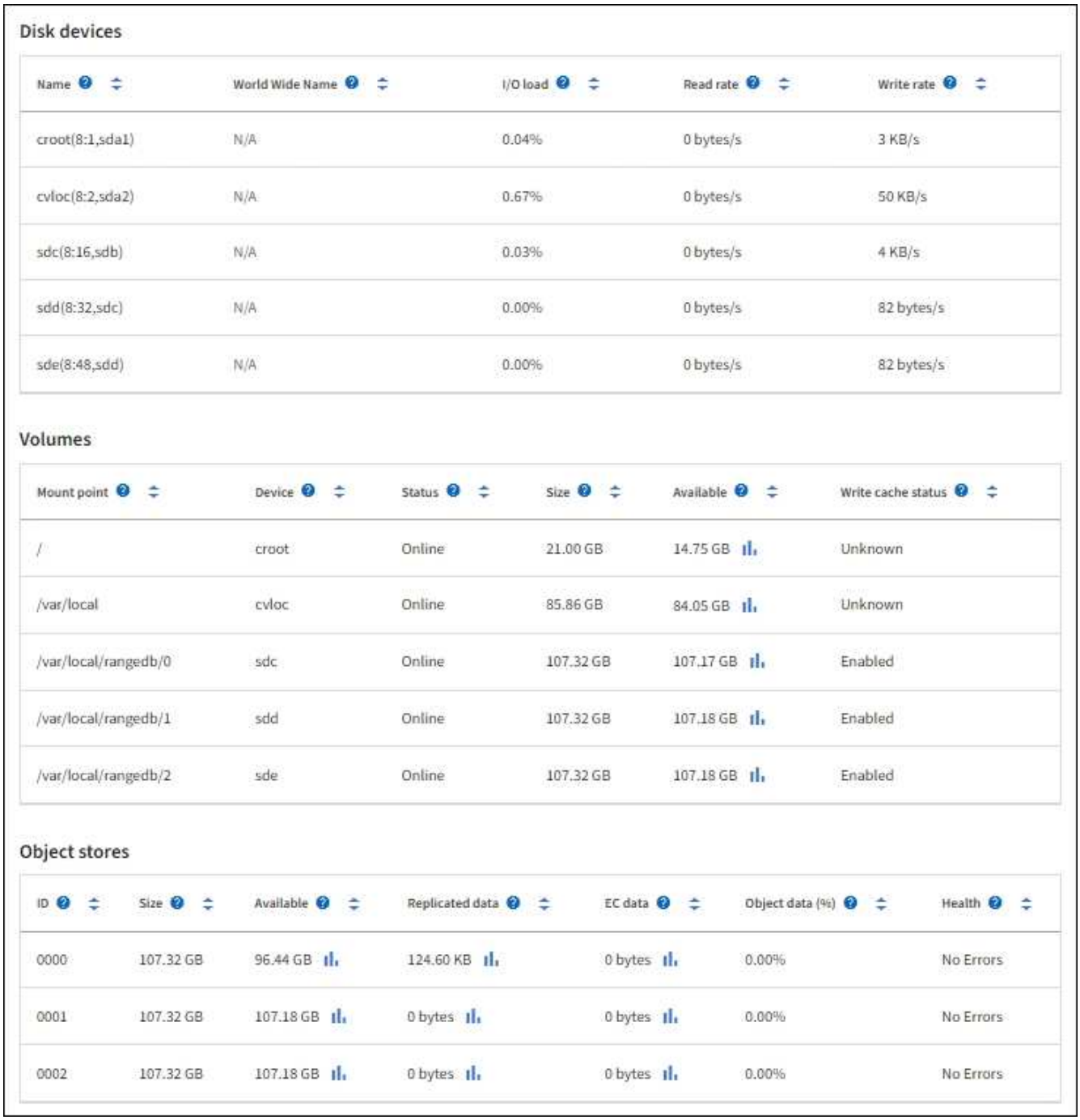




a. 下にスクロールすると、各ボリュームとオブジェクト ストアで使用可能なストレージの量が表示されます。

   各ディスクのワールドワイド名は、 SANtricity OS (アプライアンスのストレージ コントローラに接続された管理ソフトウェア) で標準ボリューム プロパティを表示したときに表示されるボリュームのワールドワイド識別子 (WWID) と一致します。

   ボリューム マウント ポイントに関連するディスクの読み取りおよび書き込みの統計を解釈できるように、ディスク デバイス テーブルの 名前 列に表示される名前の最初の部分 (つまり、*sdc*、*sdd*、*sde* など) は、ボリューム テーブルの デバイス 列に表示される値と一致します。



Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.67%	0 bytes/s	50 KB/s
sdc(8:16,sdb)	N/A	0.03%	0 bytes/s	4 KB/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s

Volumes

Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.75 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.05 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	124.60 KB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

アプライアンスの管理ノードとゲートウェイノードに関する情報を表示します

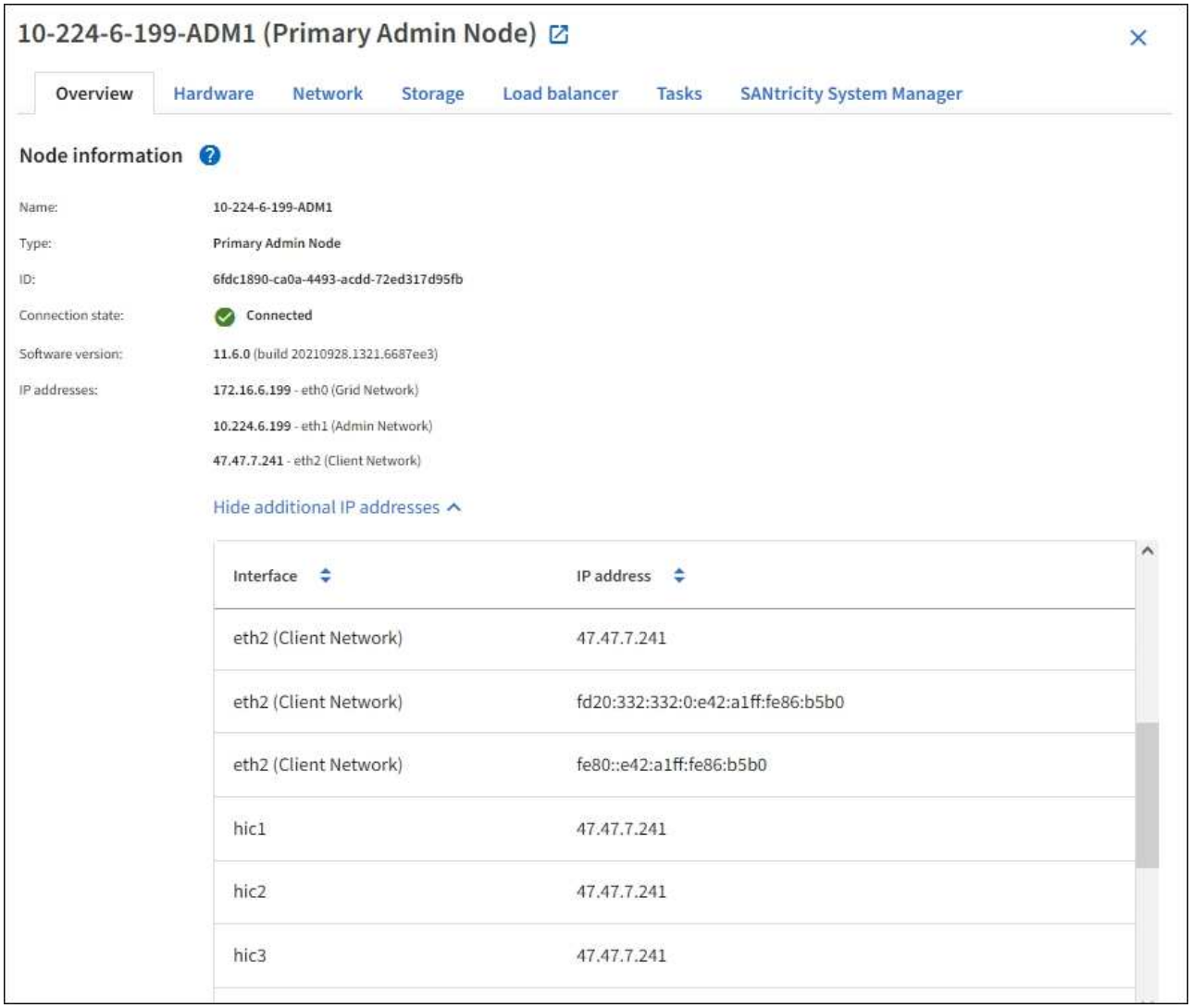
[ノード] ページには、管理ノードまたはゲートウェイ ノードとして使用される各サービス アプライアンスのサービス ヘルスとすべてのコンピューティング リソース、ディスク デバイス リソース、およびネットワーク リソースに関する情報が一覧表示されます。メモリ、ストレージ ハードウェア、ネットワーク リソース、ネットワーク インターフェイス、ネットワーク アドレスを確認したり、データの受信と送信を行ったりすることもできます。

手順

1. 「ノード」ページで、アプライアンス管理ノードまたはアプライアンス ゲートウェイ ノードを選択します。
2. *概要*を選択します。

[概要] タブの [ノード情報] セクションには、ノードの名前、タイプ、ID、接続状態など、ノードの概要情報が表示されます。 IP アドレスのリストには、次のように各アドレスのインターフェース名が含まれます。

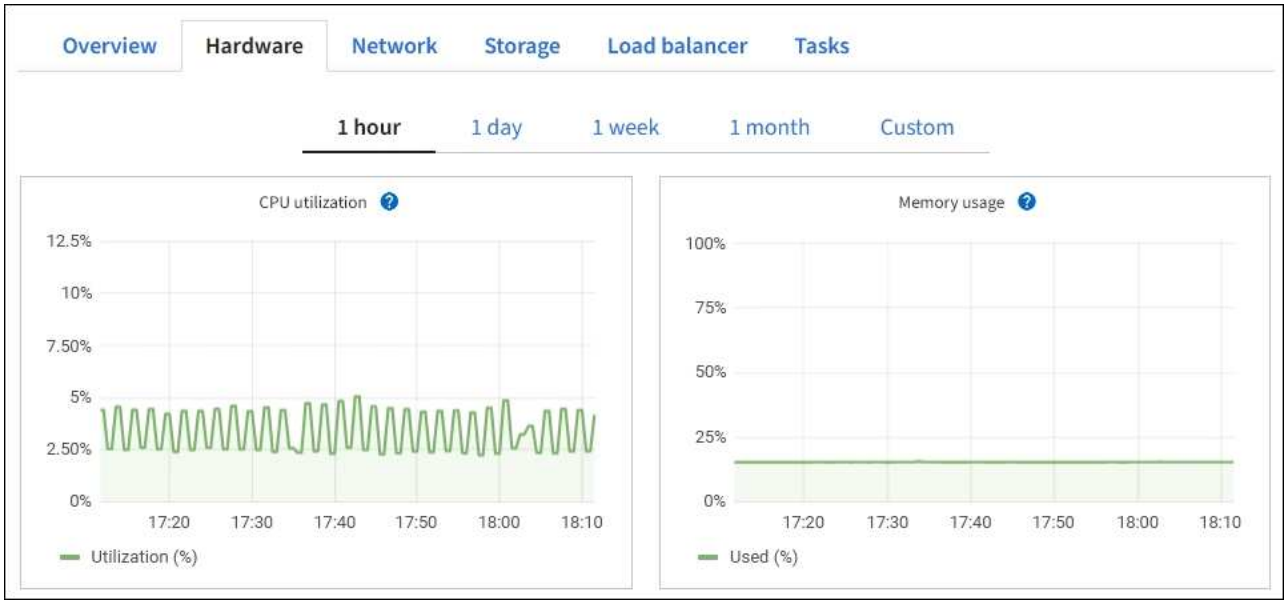
- **adllb** および **adlli**: 管理ネットワークインターフェースにアクティブ/バックアップボンディングが使用されている場合に表示されます。
- **eth**: グリッド ネットワーク、管理ネットワーク、またはクライアント ネットワーク。
- **hic**: アプライアンス上の物理的な 10、25、または 100 GbE ポートの 1 つ。これらのポートは結合して、 StorageGRIDグリッド ネットワーク (eth0) およびクライアント ネットワーク (eth2) に接続できます。
- **mtc**: アプライアンス上の物理 1 GbE ポートの 1 つ。 1 つ以上の mtc インターフェイスが結合されて、管理ネットワーク インターフェイス (eth1) を形成します。他の mtc インターフェイスは、データセンターの技術者が一時的にローカル接続できるように残しておくことができます。



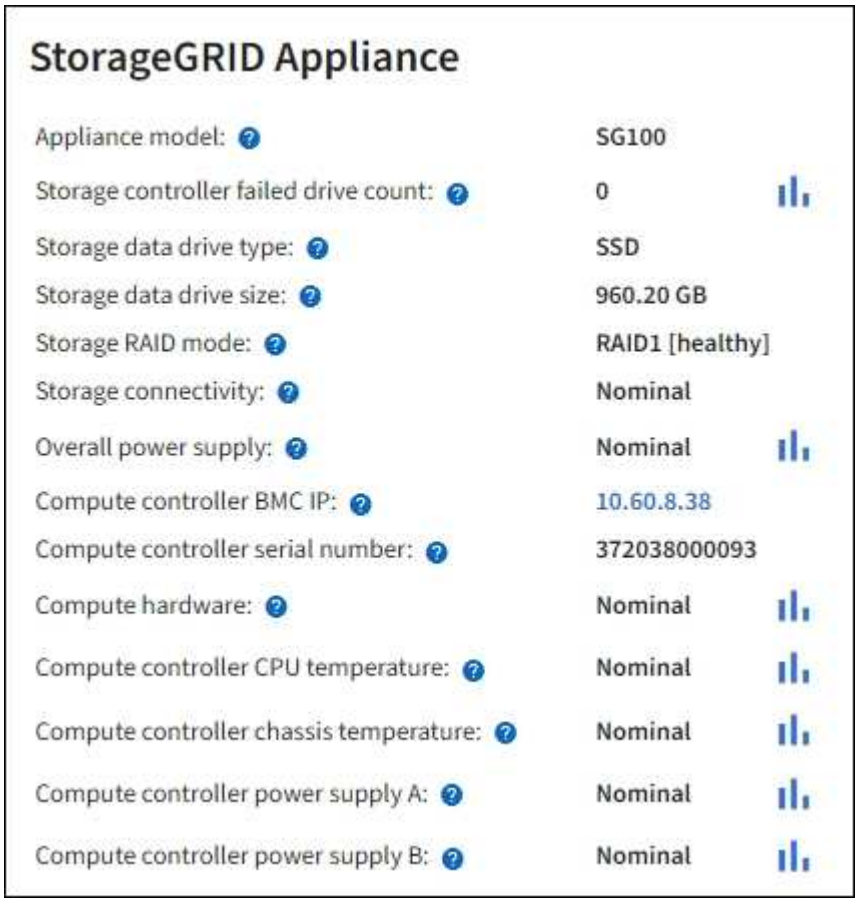
[概要] タブの [アラート] セクションには、ノードのアクティブなアラートが表示されます。

3. アプライアンスの詳細情報を表示するには、「ハードウェア」を選択します。
   a. CPU 使用率とメモリのグラフを表示して、時間の経過に伴う CPU とメモリの使用率の割合を確認します。異なる時間間隔を表示するには、チャートまたはグラフの上にあるコントロールのいずれかを

選択します。 1 時間、1 日、1 週間、1 か月の間隔で情報を表示できます。カスタム間隔を設定して、日付と時刻の範囲を指定することもできます。



b. 下にスクロールして、アプライアンスのコンポーネント表を表示します。このテーブルには、モデル名、シリアル番号、コントローラーのファームウェア バージョン、各コンポーネントのステータスなどの情報が含まれています。



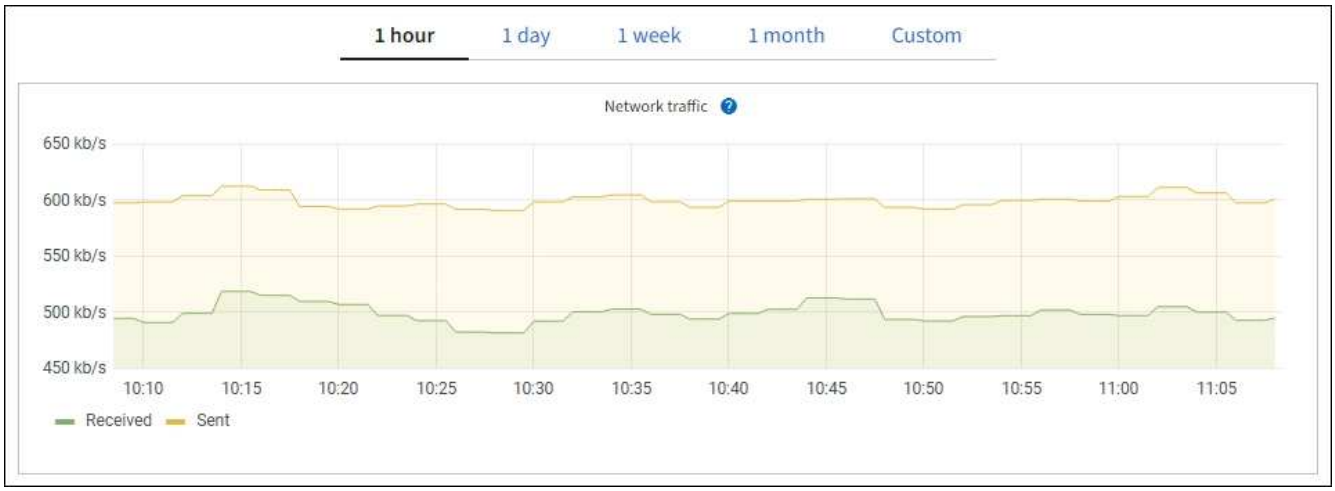
アプライアンステーブルのフィールド	説明
アプライアンスモデル	このStorageGRIDアプライアンスのモデル番号。
ストレージコントローラの障害ドライブ数	最適ではないドライブの数。
ストレージデータドライブの種類	アプライアンス内のドライブの種類 (HDD (ハード ドライブ) や SSD (ソリッド ステート ドライブ) など)。
ストレージデータドライブのサイズ	1 つのデータ ドライブの有効サイズ。
ストレージRAIDモード	アプライアンスの RAID モード。
全体的な電源供給	アプライアンス内のすべての電源のステータス。
コンピューティングコントローラBMC IP	コンピューティング コントローラー内のベースボード管理コントローラー (BMC) ポートの IP アドレス。この IP を使用してBMCインターフェイスに接続し、アプライアンスのハードウェアを監視および診断できます。 このフィールドは、 BMCが含まれていないアプライアンス モデルでは表示されません。
コンピューティングコントローラのシリアル番号	コンピューティング コントローラーのシリアル番号。
コンピューティングハードウェア	コンピューティング コントローラー ハードウェアのステータス。
コンピューティングコントローラのCPU温度	コンピューティング コントローラーの CPU の温度状態。
コンピューティングコントローラシャーシの温度	コンピューティング コントローラーの温度状態。

a. すべてのステータスが「正常」であることを確認します。

   ステータスが「正常」でない場合は、現在のアラートを確認してください。

4. 各ネットワークの情報を表示するには、「ネットワーク」を選択します。

ネットワーク トラフィック グラフには、全体的なネットワーク トラフィックの概要が表示されます。



a. ネットワーク インターフェイス セクションを確認します。

Network interfaces

Name	Hardware address	Speed	Duplex	Auto-negotiation	Link status
eth0	0C:42:A1:86:B5:B0	100 Gigabit	Full	Off	Up
eth1	B4:A9:FC:71:68:36	Gigabit	Full	Off	Up
eth2	0C:42:A1:86:B5:B0	100 Gigabit	Full	Off	Up
hic1	0C:42:A1:86:B5:B0	25 Gigabit	Full	On	Up
hic2	0C:42:A1:86:B5:B0	25 Gigabit	Full	On	Up
hic3	0C:42:A1:86:B5:B0	25 Gigabit	Full	On	Up
hic4	0C:42:A1:86:B5:B0	25 Gigabit	Full	On	Up
mtc1	B4:A9:FC:71:68:36	Gigabit	Full	On	Up
mtc2	B4:A9:FC:71:68:35	Gigabit	Full	On	Up

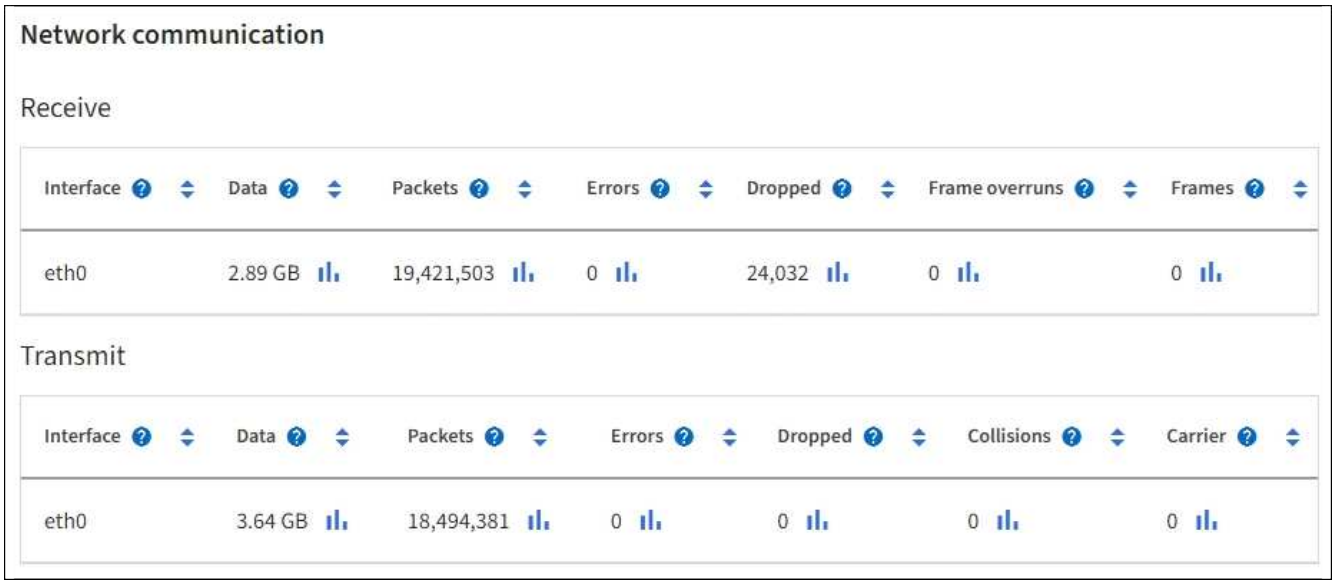
次の表とネットワーク インターフェイス テーブルの 速度 列の値を使用して、アプライアンス上の 4 つの 40/100 GbE ネットワーク ポートがアクティブ/バックアップ モードと LACP モードのどちらを使用するように構成されているかを確認します。

表に示されている値は、4 つのリンクすべてが使用されていることを前提としています。

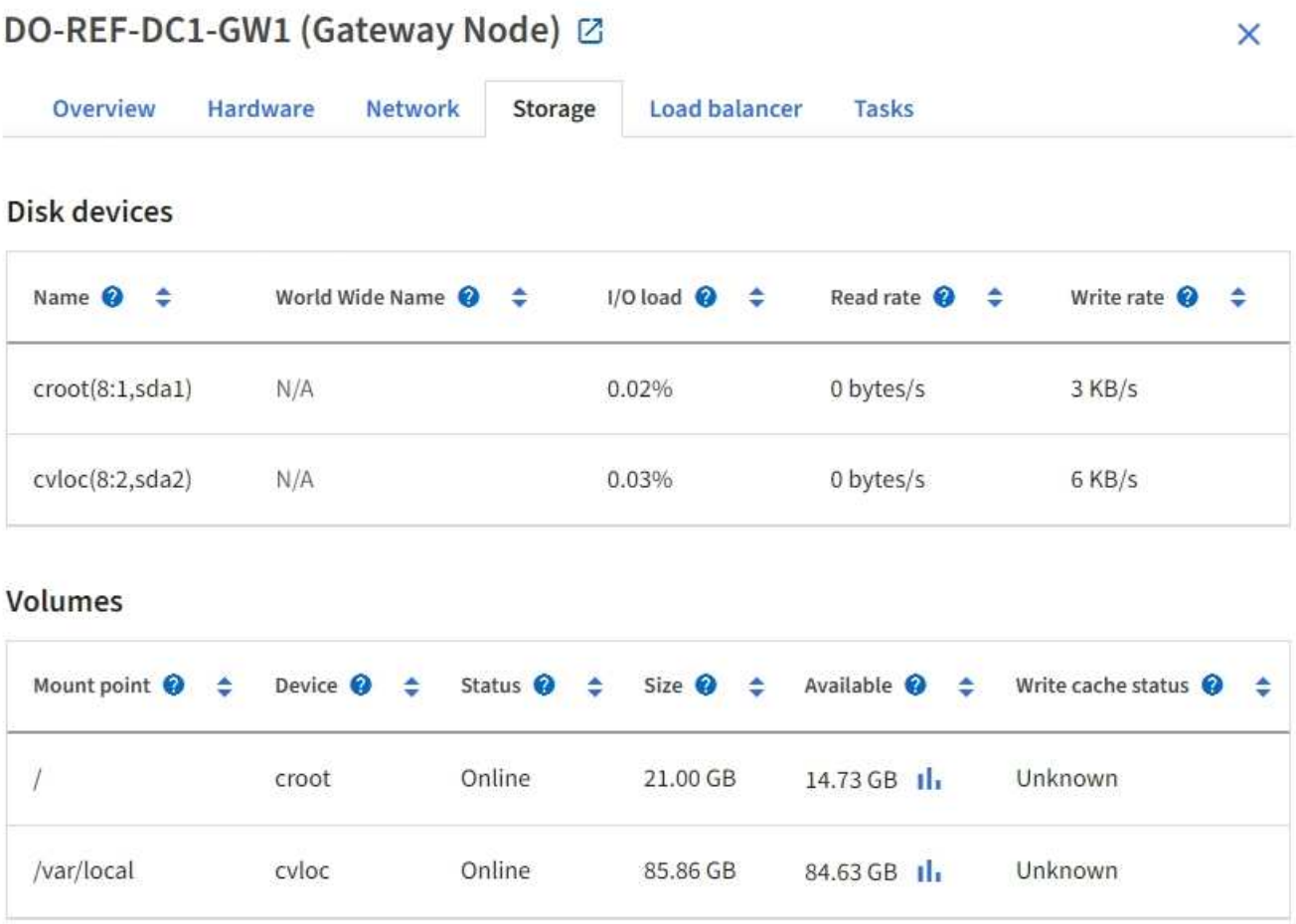
リンクモード	ボンドモード	個々のHICリンク速度（hic1、hic2、hic3、hic4）	予想されるグリッド/クライアントネットワーク速度 (eth0、eth2)
Aggregate	LACP	100	400
固定	LACP	100	200
固定	アクティブ/バックアップ	100	100
Aggregate	LACP	40	160
固定	LACP	40	80
固定	アクティブ/バックアップ	40	40

b. ネットワーク通信セクションを確認します。

受信テーブルと送信テーブルには、各ネットワークで受信および送信されたバイト数とパケット数、およびその他の受信および送信メトリックが表示されます。



5. サービス アプライアンス上のディスク デバイスとボリュームに関する情報を表示するには、[ストレージ]を選択します。



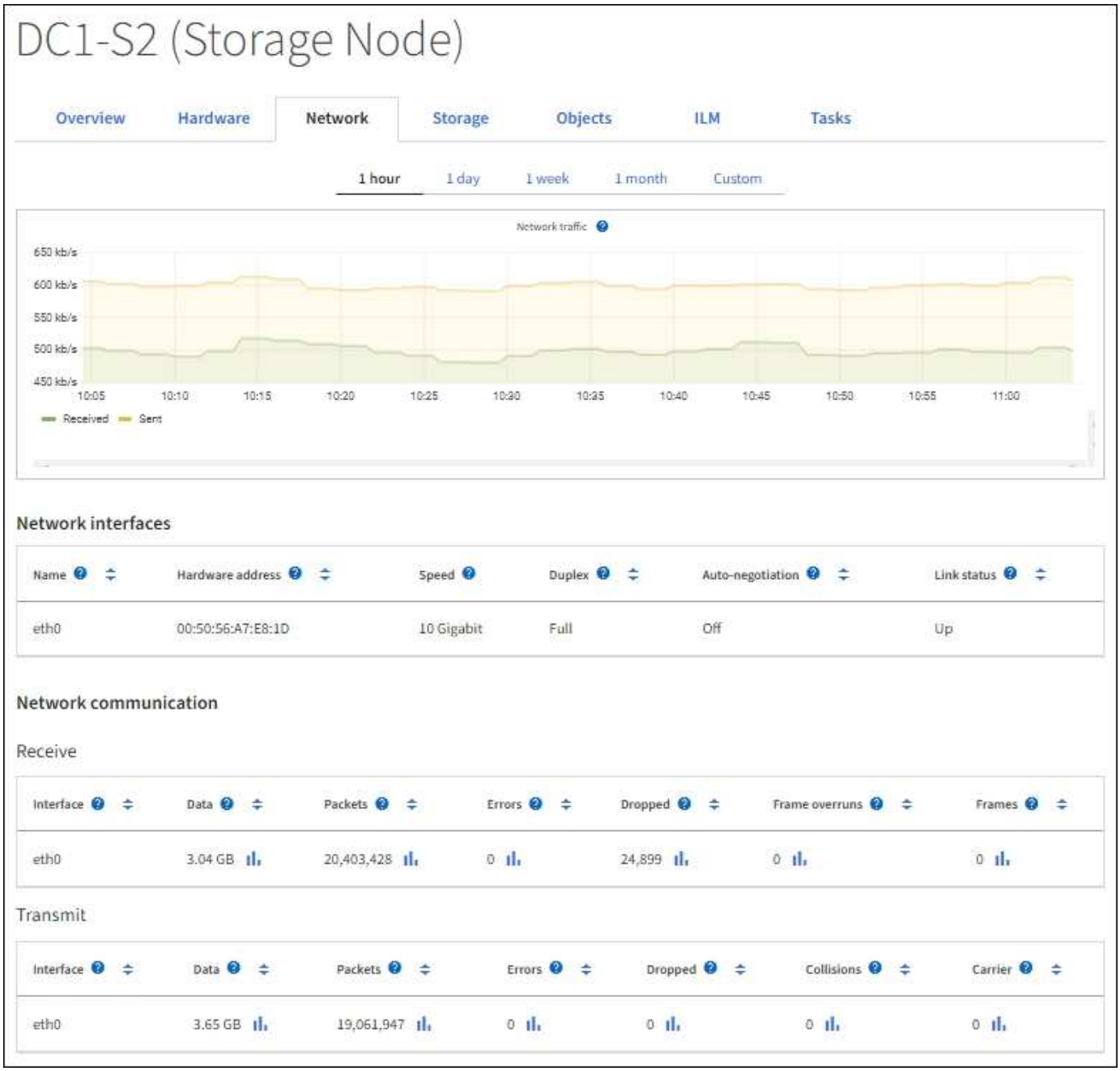
ネットワークタブを表示する

[ネットワーク] タブには、ノード、サイト、またはグリッド上のすべてのネットワーク インターフェイスで受信および送信されたネットワーク トラフィックを示すグラフが表示されます。

すべてのノード、各サイト、およびグリッド全体に対して [ネットワーク] タブが表示されます。

異なる時間間隔を表示するには、チャートまたはグラフの上にあるコントロールのいずれかを選択します。 1 時間、1 日、1 週間、1 か月の間隔で情報を表示できます。カスタム間隔を設定して、日付と時刻の範囲を指定することもできます。

ノードの場合、ネットワーク インターフェイス テーブルには、各ノードの物理ネットワーク ポートに関する情報が提供されます。ネットワーク通信テーブルには、各ノードの受信および送信操作と、ドライバーによって報告された障害カウンターの詳細が示されます。



関連情報

"ネットワーク接続とパフォーマンスを監視する"

ストレージタブを表示する

[ストレージ] タブには、ストレージの可用性やその他のストレージ メトリックの概要が表示されます。

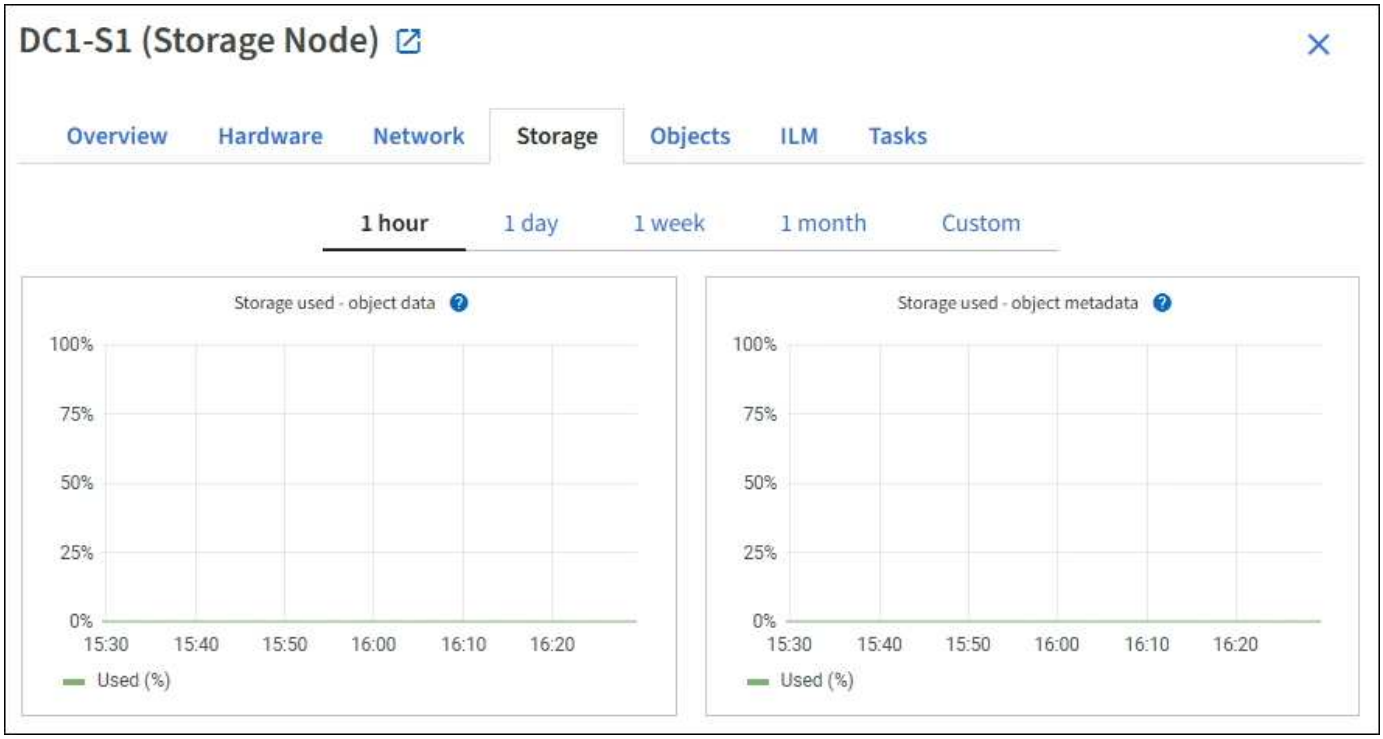
すべてのノード、各サイト、およびグリッド全体に対して [ストレージ] タブが表示されます。

ストレージ使用状況グラフ

ストレージ ノード、各サイト、およびグリッド全体について、ストレージ タブには、時間の経過に伴ってオブジェクト データとオブジェクト メタデータによって使用されたストレージの量を示すグラフが含まれま

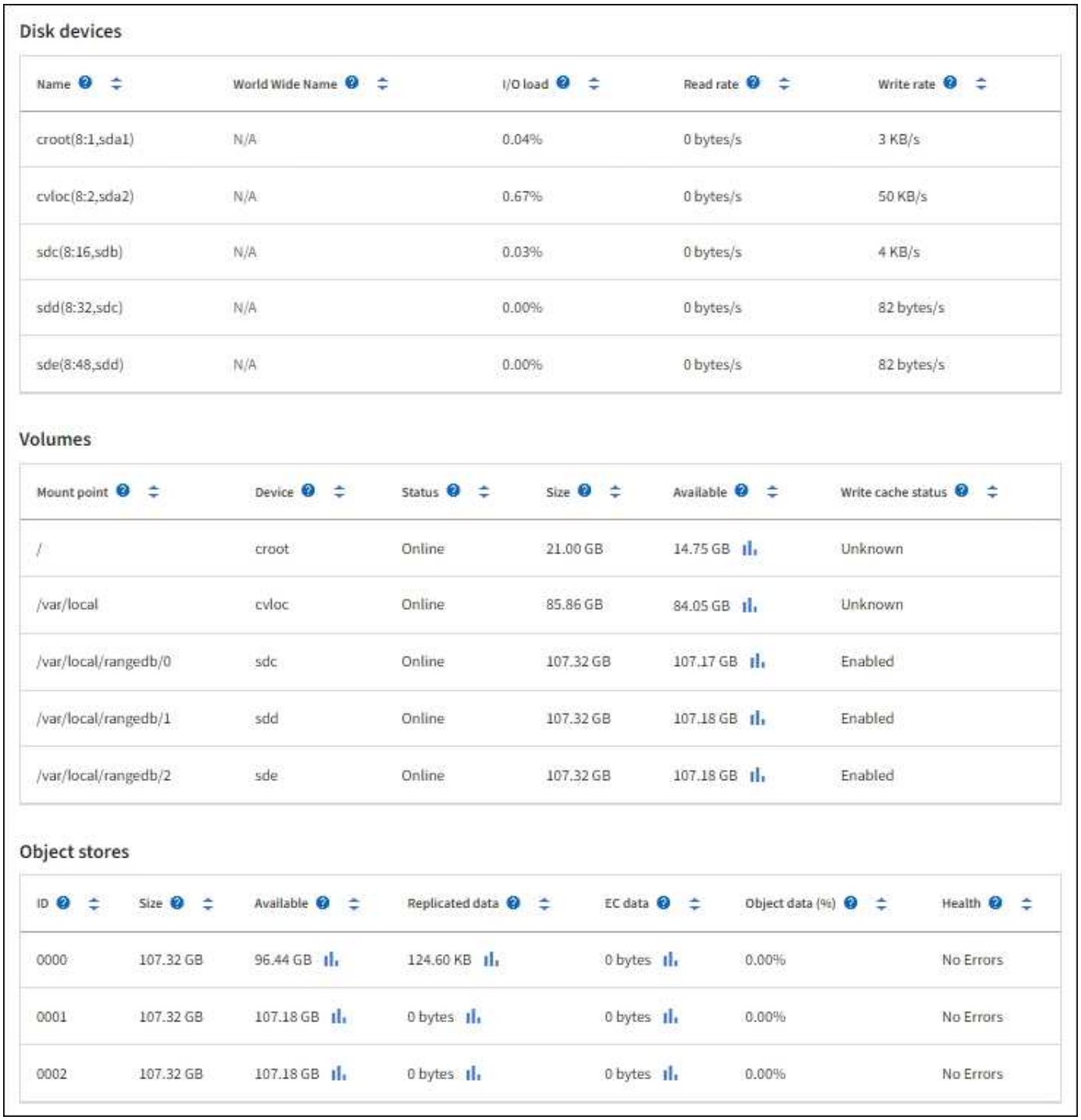
す。

アップグレード中や切断状態など、ノードがグリッドに接続されていない場合、特定のメトリックは利用できなくなるか、サイトとグリッドの合計から除外される可能性があります。ノードがグリッドに再接続した後、値が安定するまで数分間待ちます。



ディスクデバイス、ボリューム、オブジェクトストアテーブル

すべてのノードについて、[ストレージ] タブには、ノード上のディスク デバイスとボリュームの詳細が表示されます。ストレージ ノードの場合、オブジェクト ストア テーブルには各ストレージ ボリュームに関する情報が提供されます。



Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.67%	0 bytes/s	50 KB/s
sdc(8:16,sdb)	N/A	0.03%	0 bytes/s	4 KB/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s

Volumes

Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.75 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.05 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	124.60 KB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

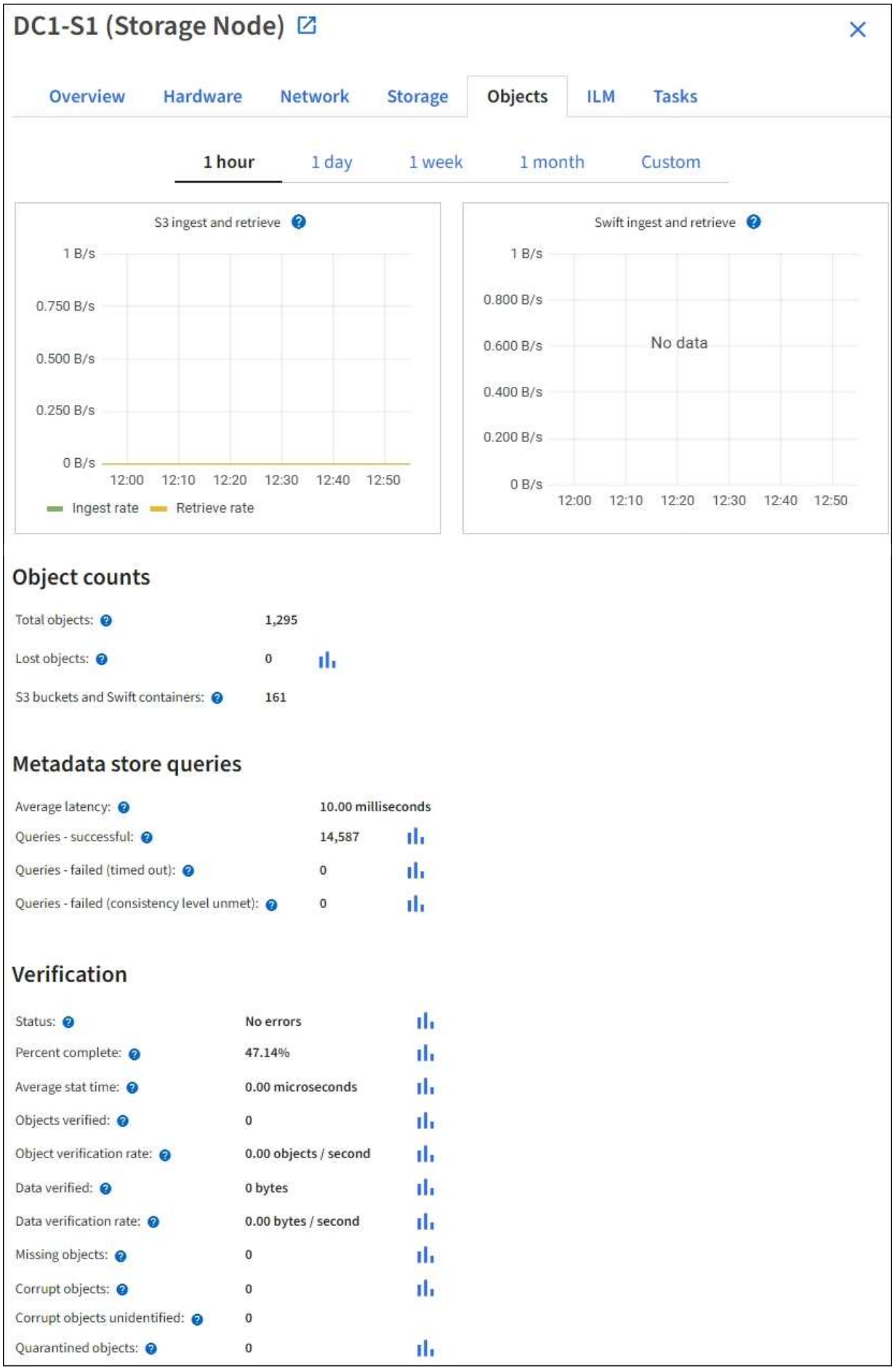
関連情報

"ストレージ容量を監視する"

オブジェクトタブを表示する

オブジェクトタブには以下の情報が表示されます。"S3 の取り込みと取得の速度" 。

オブジェクト タブは、各ストレージ ノード、各サイト、およびグリッド全体に対して表示されます。ストレージ ノードの場合、[オブジェクト] タブには、オブジェクト数、メタデータ クエリ、バックグラウンド検証に関する情報も表示されます。

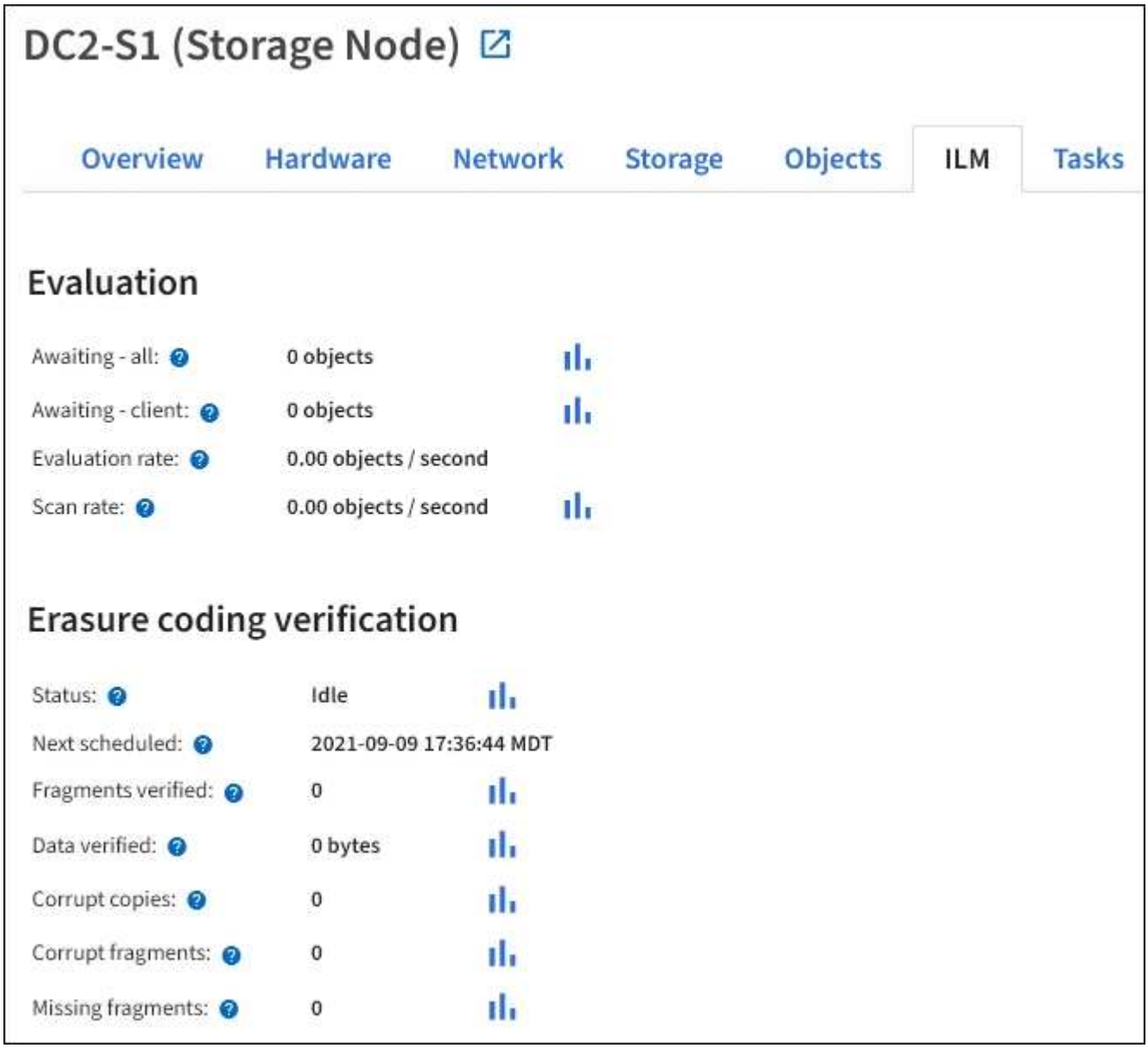

DC1-S1 (Storage Node)
Overview
Hardware
Network
Storage
Objects
ILM
Tasks
1 hour
1 day
1 week
1 month
Custom
S3 ingest and retrieve
1 B/s
0.750 B/s
0.500 B/s
0.250 B/s
0 B/s
12:00
12:10
12:20
12:30
12:40
12:50
Ingest rate
Retrieve rate
Swift ingest and retrieve
1 B/s
0.800 B/s
0.600 B/s
0.400 B/s
0.200 B/s
0 B/s
No data
12:00
12:10
12:20
12:30
12:40
12:50
Object counts
Total objects: 1,295
Lost objects: 0
S3 buckets and Swift containers: 161
Metadata store queries
Average latency: 10.00 milliseconds
Queries - successful: 14,587
Queries - failed (timed out): 0
Queries - failed (consistency level unmet): 0
Verification
Status: No errors
Percent complete: 47.14%
Average stat time: 0.00 microseconds
Objects verified: 0
Object verification rate: 0.00 objects / second
Data verified: 0 bytes
Data verification rate: 0.00 bytes / second
Missing objects: 0
Corrupt objects: 0
Corrupt objects unidentified: 0
Quarantined objects: 0

ILMタブを表示

ILM タブには、情報ライフサイクル管理 (ILM) 操作に関する情報が表示されます。

ILM タブは、各ストレージ ノード、各サイト、およびグリッド全体に対して表示されます。各サイトおよびグリッドについて、ILM タブには時間の経過に伴う ILM キューのグラフが表示されます。グリッドの場合、このタブには、すべてのオブジェクトの完全な ILM スキャンを完了するのにかかる推定時間も表示されます。

ストレージ ノードの場合、ILM タブには、消去コード化されたオブジェクトの ILM 評価とバックグラウンド検証に関する詳細が表示されます。



関連情報

- "情報ライフサイクル管理を監視する"
- "StorageGRIDの管理"

タスクタブを使用する

すべてのノードに対して [タスク] タブが表示されます。このタブを使用して、ノードの名前を変更したり、ノードを再起動したり、アプライアンス ノードをメンテナンス モードにしたりできます。

このタブの各オプションの完全な要件と手順については、以下を参照してください。

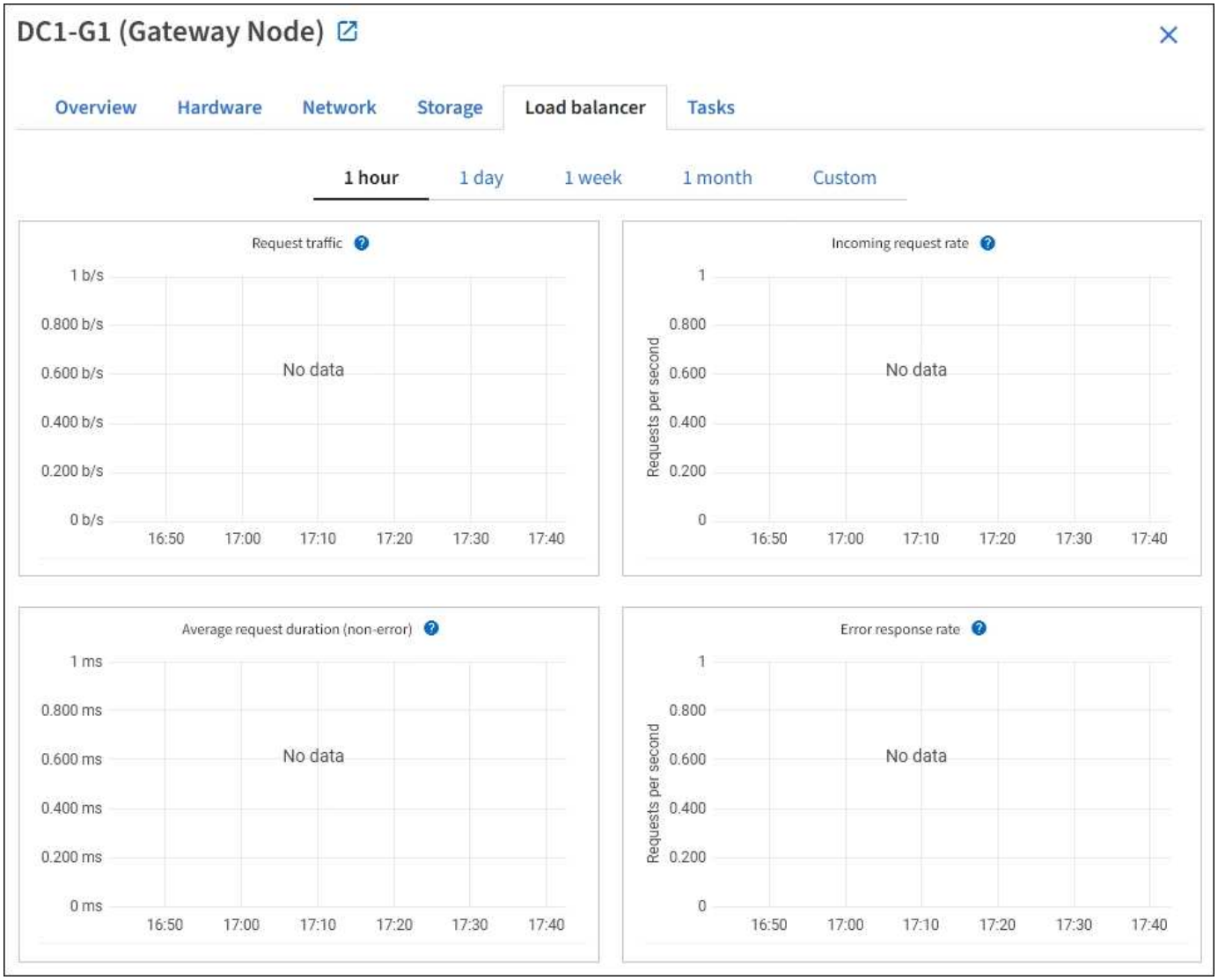
- "グリッド、サイト、ノードの名前を変更する"
- "グリッドノードを再起動する"
- "アプライアンスをメンテナンスモードにする"

ロードバランサータブを表示する

ロード バランサ タブには、ロード バランサ サービスの動作に関連するパフォーマンス グラフと診断グラフが含まれています。

ロード バランサ タブは、管理ノードとゲートウェイ ノード、各サイト、およびグリッド全体に対して表示されます。各サイトの「ロード バランサ」タブには、そのサイトのすべてのノードの統計の集計概要が表示されます。グリッド全体については、[ロード バランサ] タブにすべてのサイトの統計の集計概要が表示されます。

ロード バランサ サービスを通じて I/O が実行されていない場合、またはロード バランサが構成されていない場合は、グラフに「データなし」と表示されます。



リクエストトラフィック

このグラフは、ロード バランサーのエンドポイントとリクエストを行っているクライアント間で送信されるデータのスループットの 3 分間の移動平均 (ビット/秒) を示します。

> この値は各リクエストの完了時に更新されます。その結果、この値は、要求レートが低い場合や要求の存続期間が非常に長い場合には、リアルタイムのスループットと異なる可能性があります。現在のネットワークの動作をより現実的に把握するには、[ネットワーク] タブを確認します。

受信リクエスト率

このグラフには、リクエストの種類 (GET、PUT、HEAD、DELETE) 別に分類された、1 秒あたりの新規リクエスト数の 3 分間の移動平均が表示されます。この値は、新しいリクエストのヘッダーが検証されたときに更新されます。

平均リクエスト時間（エラーなし）

このグラフには、リクエストの種類 (GET、PUT、HEAD、DELETE) 別に分類された、リクエスト継続時間の 3 分間の移動平均が表示されます。各リクエストの期間は、リクエスト ヘッダーがロード バランサ サービス

によって解析されたときに開始され、完全なレスポンス本文がクライアントに返されたときに終了します。

エラー応答率

このグラフには、エラー応答コード別に分類された、1 秒あたりにクライアントに返されたエラー応答の数の 3 分間の移動平均が表示されます。

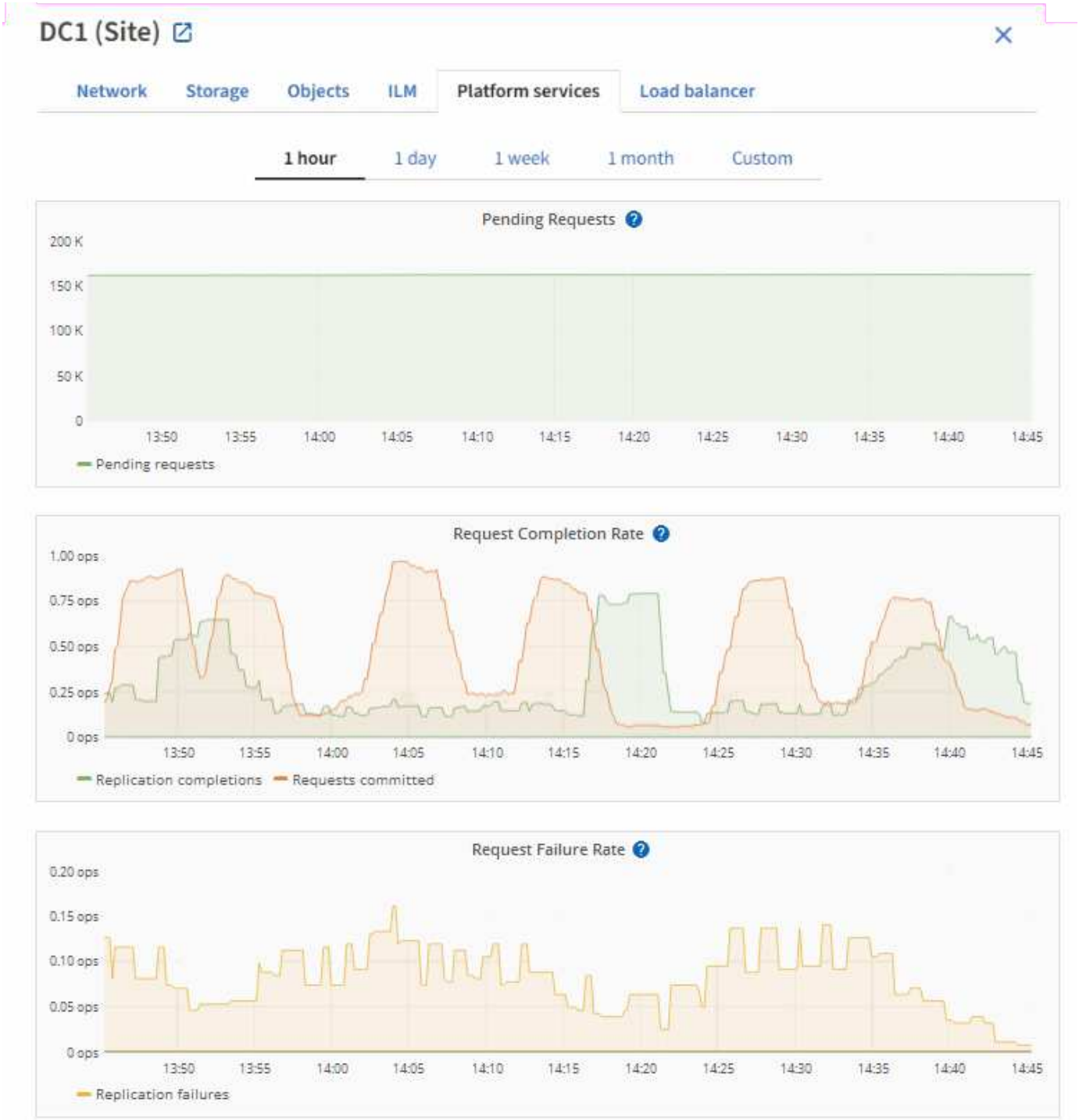
関連情報

- "負荷分散操作を監視する"
- "StorageGRIDの管理"

プラットフォームサービスタブを表示する

プラットフォーム サービス タブには、サイト上の S3 プラットフォーム サービス操作に関する情報が表示されます。

各サイトのプラットフォーム サービス タブが表示されます。このタブには、CloudMirror レプリケーションや検索統合サービスなどの S3 プラットフォーム サービスに関する情報が表示されます。このタブのグラフには、保留中のリクエストの数、リクエストの完了率、リクエストの失敗率などのメトリックが表示されます。



S3プラットフォームサービスの詳細（トラブルシューティングの詳細を含む）については、"StorageGRIDの管理手順" 。

ドライブの管理タブを表示する

「ドライブの管理」タブでは、この機能をサポートするアプライアンス内のドライブの詳細にアクセスし、トラブルシューティングやメンテナンスのタスクを実行できます。

「ドライブの管理」タブを使用すると、次の操作を実行できます。

- アプライアンス内のデータストレージドライブのレイアウトを表示します
- 各ドライブの場所、タイプ、ステータス、ファームウェア バージョン、シリアル番号をリストした表を表示します。
- 各ドライブのトラブルシューティングとメンテナンス機能を実行します

ドライブの管理タブにアクセスするには、"ストレージアプライアンス管理者またはルートアクセス権限" 。

ドライブの管理タブの使用方法については、以下を参照してください。 "ドライブの管理タブを使用する" 。

SANtricity System Manager タブを表示する (E シリーズのみ)

SANtricity System Manager タブを使用すると、ストレージ アプライアンスの管理ポートを構成または接続しなくても、 SANtricity System Manager にアクセスできます。このタブを使用すると、ハードウェア診断および環境情報や、ドライブに関連する問題を確認できます。

Grid Manager からSANtricity System Manager にアクセスするのは、通常、アプライアンスのハードウェアを監視し、E シリーズAutoSupportを構成するためだけに行われます。ファームウェアのアップグレードなど、 SANtricity System Manager 内の多くの機能と操作は、StorageGRIDアプライアンスの監視には適用されません。問題を回避するには、必ずアプライアンスのハードウェア メンテナンス手順に従ってください。 SANtricityファームウェアをアップグレードするには、 "メンテナンス構成手順"ストレージアプライアンス用。

SANtricity System Manager タブは、E シリーズ ハードウェアを使用するストレージ アプライアンス ノードに対してのみ表示されます。

SANtricity System Manager を使用すると、次のことができます。

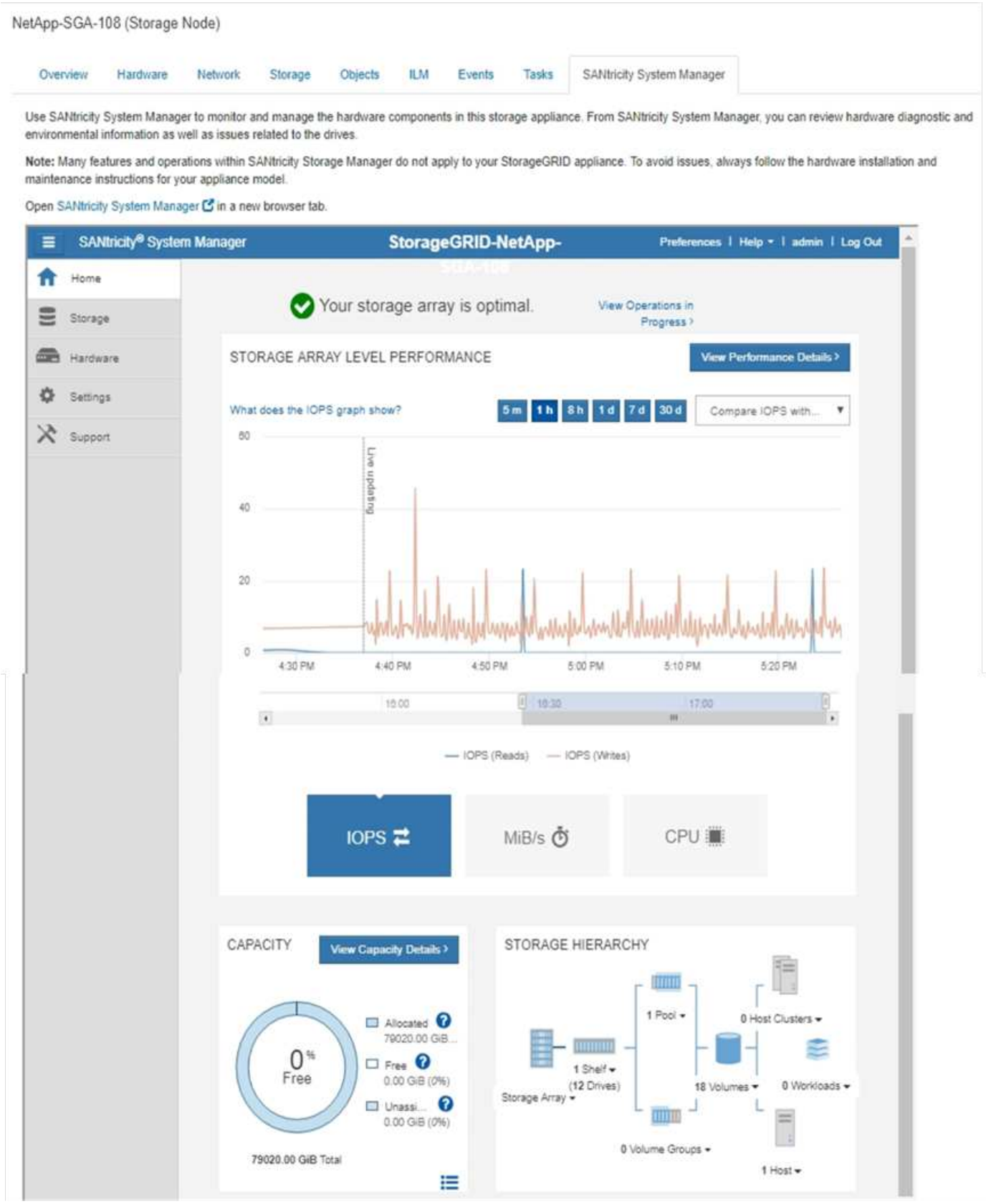
- ストレージ アレイ レベルのパフォーマンス、I/O レイテンシ、ストレージ コントローラーの CPU 使用率、スループットなどのパフォーマンス データを表示します。
- ハードウェア コンポーネントのステータスを確認します。
- 診断データの表示や E シリーズAutoSupportの構成などのサポート機能を実行します。

SANtricity System Managerを使用してEシリーズAutoSupportのプロキシを設定するには、"EシリーズAutoSupportパッケージをStorageGRID経由で送信する" 。

グリッドマネージャを通じてSANtricity System Managerにアクセスするには、"ストレージアプライアンス管理者またはルートアクセス権限" 。

Grid Manager を使用してSANtricity System Manager にアクセスするには、 SANtricityファームウェア 8.70 以上が必要です。

タブには、 SANtricity System Manager のホームページが表示されます。



SANtricity System Manager リンクを使用すると、 SANtricity System Manager を新しいブラウザ ウィンドウで開き、簡単に表示することができます。

ストレージ アレイ レベルのパフォーマンスと容量使用率の詳細を表示するには、各グラフの上にカーソルを

置きます。

SANtricity System Managerタブからアクセスできる情報の表示の詳細については、以下を参照してください。 "NetApp EシリーズおよびSANtricityのドキュメント" 。

定期的に監視する情報

何をいつ監視するか

エラーが発生したり、グリッドの一部が使用できなくなったりしても、 StorageGRIDシステムは動作を継続できますが、グリッドの効率や可用性に影響が出る前に、潜在的な問題を監視して対処する必要があります。

開始する前に

- グリッドマネージャにサインインするには、"サポートされているウェブブラウザ" 。
- あなたが持っている"特定のアクセス権限"。

監視タスクについて

ビジーなシステムは大量の情報を生成します。次のリストは、継続的に監視する必要がある最も重要な情報についてのガイダンスを提供します。

監視対象	頻度
"システムの健全性状態"	日次
割合"ストレージノードオブジェクトとメタデータ容量"消費されている	週次
"情報ライフサイクル管理業務"	週次
"ネットワークとシステムリソース"	週次
"テナント活動"	週次
"S3クライアント操作"	週次
"負荷分散操作"	初期設定後および設定変更後
"グリッドフェデレーション接続"	週次

システムの健全性を監視する

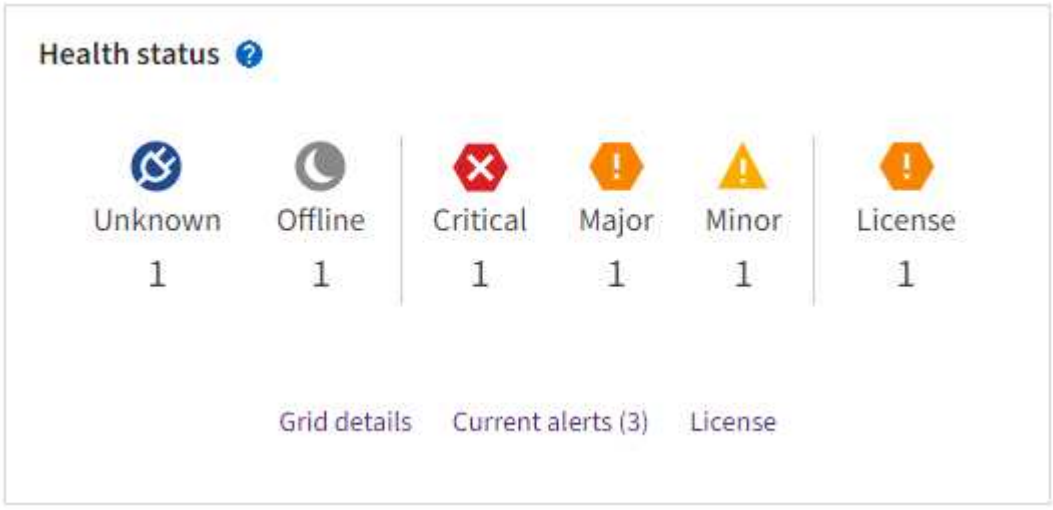
StorageGRIDシステムの全体的な健全性を毎日監視します。

タスク概要

StorageGRIDシステムは、グリッドの一部が利用できなくなった場合でも動作を継続できます。アラートによ

って示される潜在的な問題は、必ずしもシステム操作の問題ではありません。グリッド マネージャー ダッシュボードのヘルス ステータス カードにまとめられた問題を調査します。

アラートが発生したらすぐに通知を受け取るには、 "アラートのメール通知を設定する"または"SNMPトラップを設定する"。



問題がある場合は、追加の詳細を表示できるリンクが表示されます。

リンク	...のときに表示されます。
グリッドの詳細	すべてのノードが切断されています (接続状態が不明または管理上ダウンしています)。
現在のアラート（重大、重大、軽微）	アラートは現在アクティブ。
最近解決されたアラート	過去1週間に発生したアラート解決されました。
ライセンス	このStorageGRIDシステムのソフトウェア ライセンスに問題があります。あなたは "必要に応じてライセンス情報を更新する"。

ノード接続状態を監視する

1 つ以上のノードがグリッドから切断されると、重要なStorageGRID操作に影響が出る可能性があります。ノードの接続状態を監視し、問題があればすぐに対処します。

アイコン	説明	必要なアクション
	接続されていません - 不明 不明な理由により、ノードが切断されたか、ノード上のサービスが予期せず停止しました。たとえば、ノード上のサービスが停止したり、停電や予期しない停止のためにノードのネットワーク接続が失われたりする可能性があります。 ノードと通信できません というアラートもトリガーされる可能性があります。他のアラートもアクティブになっている可能性があります。	すぐに対処する必要があります。各アラートを選択推奨されるアクションに従ってください。 たとえば、停止したサービスを再起動したり、ノードのホストを再起動したりする必要がある場合があります。 注意: 管理されたシャットダウン操作中に、ノードが「不明」と表示される場合があります。このような場合には、不明状態を無視できます。
	接続されていません - 管理上ダウンしています 予想された理由により、ノードはグリッドに接続されていません。 たとえば、ノードまたはノード上のサービスが正常にシャットダウンされた、ノードが再起動中、またはソフトウェアがアップグレード中などです。 1 つ以上のアラートがアクティブになっている可能性もあります。 根本的な問題によっては、これらのノードは介入なしにオンラインに戻ることがよくあります。	このノードに影響するアラートがあるかどうかを判断します。 1つ以上のアラートがアクティブになっている場合、各アラートを選択推奨されるアクションに従ってください。
	接続済み ノードはグリッドに接続されています。	対処は必要ありません。

現在のアラートと解決済みのアラートを表示する

現在のアラート: アラートがトリガーされると、ダッシュボードにアラート アイコンが表示されます。ノードページのノードに対してアラート アイコンも表示されます。もし"アラートメール通知が設定されている"アラートが消音されていない限り、電子メール通知も送信されます。

解決済みのアラート: 解決済みのアラートの履歴を検索して表示できます。

オプションとして、ビデオを視聴しました: "ビデオ: アラートの概要"

次の表は、グリッド マネージャーに表示される現在のアラートと解決済みのアラートの情報について説明しています。

列ヘッダー	説明
名前または役職	アラートの名前と説明。
重大度	アラートの重大度。現在のアラートの場合、複数のアラートがグループ化されていると、タイトル行に各重大度で発生しているアラートのインスタンスの数が表示されます。 重大: StorageGRIDノードまたはサービスの通常の操作を停止させる異常な状態が発生しています。根本的な問題に直ちに対処する必要があります。問題が解決されない場合、サービスが中断され、データが失われる可能性があります。 重大: 現在の操作に影響を及ぼしているか、重大なアラートのしきい値に近づいている異常な状態が存在します。異常な状態によってStorageGRIDノードまたはサービスの通常の動作が停止しないように、主要なアラートを調査して根本的な問題に対処する必要があります。 軽微: システムは正常に動作していますが、継続するとシステムの動作能力に影響を及ぼす可能性のある異常な状態が存在します。より深刻な問題を引き起こさないように、自然に消えない軽微なアラートを監視して解決する必要があります。
トリガー時間	現在のアラート: アラートがトリガーされた日時（現地時間と UTC）。複数のアラートがグループ化されている場合、タイトル行には、アラートの最新のインスタンス (*newest*) とアラートの最も古いインスタンス (*oldest*) の時間が表示されます。 解決済みのアラート: アラートがトリガーされてからどのくらいの時間が経過したか。
サイト/ノード	アラートが発生している、または発生したサイトとノードの名前。
ステータス	アラートがアクティブ、サイレント、または解決済みかどうか。複数のアラートがグループ化され、ドロップダウンで すべてのアラート が選択されている場合、タイトル行には、そのアラートのアクティブなインスタンスの数と、サイレントになっているインスタンスの数が表示されます。

列ヘッダー	説明
解決時間（解決されたアラートのみ）	アラートが解決されてからどれくらい経ったか。
現在の値または_データ値_	アラートをトリガーする原因となったメトリックの値。一部のアラートでは、アラートを理解して調査するのに役立つ追加の値が表示されます。たとえば、「オブジェクト データ ストレージ不足」アラートに表示される値には、使用されているディスク領域の割合、ディスク領域の合計量、使用されているディスク領域の量が含まれます。 注: 複数の現在のアラートがグループ化されている場合、現在の値はタイトル行に表示されません。
トリガーされた値（解決されたアラートのみ）	アラートをトリガーする原因となったメトリックの値。一部のアラートでは、アラートを理解して調査するのに役立つ追加の値が表示されます。たとえば、「オブジェクト データ ストレージ不足」アラートに表示される値には、使用されているディスク領域の割合、ディスク領域の合計量、使用されているディスク領域の量が含まれます。

手順

1. 現在のアラート または 解決済みのアラート リンクを選択すると、それらのカテゴリのアラートのリストが表示されます。 ノード > ***node*** > 概要 を選択し、アラート テーブルからアラートを選択して、アラートの詳細を表示することもできます。

   デフォルトでは、現在のアラートは次のように表示されます。

   - 最近トリガーされたアラートが最初に表示されます。
   - 同じタイプの複数のアラートはグループとして表示されます。
   - 消音されたアラートは表示されません。
   - 特定のノード上の特定のアラートについては、複数の重大度のしきい値に達した場合、最も重大度のアラートのみが表示されます。つまり、マイナー、メジャー、およびクリティカルの重大度のアラートしきい値に達した場合は、クリティカルなアラートのみが表示されます。

     「現在のアラート」ページは 2 分ごとに更新されます。

2. アラートのグループを展開するには、下向き矢印を選択します。グループ内の個々のアラートを折りたたむには、上向きのキャレットを選択します、またはグループの名前を選択します。
3. アラートのグループではなく個々のアラートを表示するには、[アラートのグループ] チェックボックスをオフにします。
4. 現在のアラートまたはアラートグループを並べ替えるには、上/下矢印を選択します各列ヘッダーに。
   - グループアラート*を選択すると、アラートグループと各グループ内の個々のアラートの両方が並べ替えられます。たとえば、特定のアラートの最新のインスタンスを探すために、グループ内のアラートを「*トリガーされた時間」で並べ替えることができます。
   - グループアラート をクリアすると、アラートのリスト全体が並べ替えられます。たとえば、特定のノードに影響するすべてのアラートを表示するには、すべてのアラートを ノード/サイト で並べ替えることができます。

5. 現在のアラートをステータス（すべてのアラート、アクティブ、または*サイレンス*）別にフィルタリングするには、表の上部にあるドロップダウン メニューを使用します。

   見る"サイレントアラート通知" 。

6. 解決済みのアラートを並べ替えるには:
   - *トリガー時*ドロップダウン メニューから期間を選択します。
   - *重大度*ドロップダウン メニューから 1 つ以上の重大度を選択します。
   - 特定のアラート ルールに関連する解決済みのアラートをフィルターするには、[アラート ルール] ドロップダウン メニューから 1 つ以上のデフォルトまたはカスタムのアラート ルールを選択します。
   - 特定のノードに関連する解決済みのアラートをフィルタリングするには、「ノード」ドロップダウン メニューから 1 つ以上のノードを選択します。
7. 特定のアラートの詳細を表示するには、アラートを選択します。ダイアログ ボックスには、選択したアラートの詳細と推奨されるアクションが表示されます。
8. (オプション) 特定のアラートに対して、「このアラートを無音にする」を選択して、このアラートをトリガーしたアラート ルールを無音にします。

   あなたは"アラートまたはルートアクセス権限を管理する"アラートルールを無音にします。

   > アラート ルールを無音にする場合は注意してください。アラート ルールが無効になっている場合、重要な操作の完了が妨げられるまで、根本的な問題を検出できない可能性があります。

9. アラート ルールの現在の条件を表示するには:
   a. アラートの詳細から、[条件の表示] を選択します。

      定義された重大度ごとに Prometheus 式をリストしたポップアップが表示されます。

   b. ポップアップを閉じるには、ポップアップの外側の任意の場所をクリックします。
10. 必要に応じて、[ルールの編集] を選択して、このアラートをトリガーしたアラート ルールを編集します。

    あなたは"アラートまたはルートアクセス権限を管理する"アラートルールを編集します。

    > アラート ルールを編集する場合は注意してください。トリガー値を変更すると、重要な操作が完了できなくなるまで、根本的な問題を検出できない可能性があります。

11. アラートの詳細を閉じるには、[閉じる] を選択します。

ストレージ容量を監視する

使用可能な合計スペースを監視して、 StorageGRIDシステムのオブジェクトまたはオブジェクト メタデータのストレージ スペースが不足しないことを確認します。

StorageGRID はオブジェクト データとオブジェクト メタデータを個別に保存し、オブジェクト メタデータを含む分散 Cassandra データベース用に特定の量のスペースを予約します。オブジェクトとオブジェクト メタデータに消費されるスペースの合計量と、それぞれの消費されるスペース量の傾向を監視します。これにより、ノードの追加を事前に計画し、サービスの停止を回避することができます。

あなたはできる"ストレージ容量情報を表示する"グリッド全体、各サイト、およびStorageGRIDシステム内の各ストレージ ノードに対して。

グリッド全体のストレージ容量を監視する

グリッドの全体的なストレージ容量を監視して、オブジェクト データとオブジェクト メタデータに十分な空き領域が残っていることを確認します。ストレージ容量が時間の経過とともにどのように変化するかを理解しておくと、グリッドの使用可能なストレージ容量が消費される前に、ストレージ ノードまたはストレージ ボリュームを追加する計画を立てるのに役立ちます。

グリッド マネージャー ダッシュボードを使用すると、グリッド全体および各データ センターで使用可能なストレージの容量を簡単に評価できます。ノード ページには、オブジェクト データとオブジェクト メタデータのより詳細な値が提供されます。

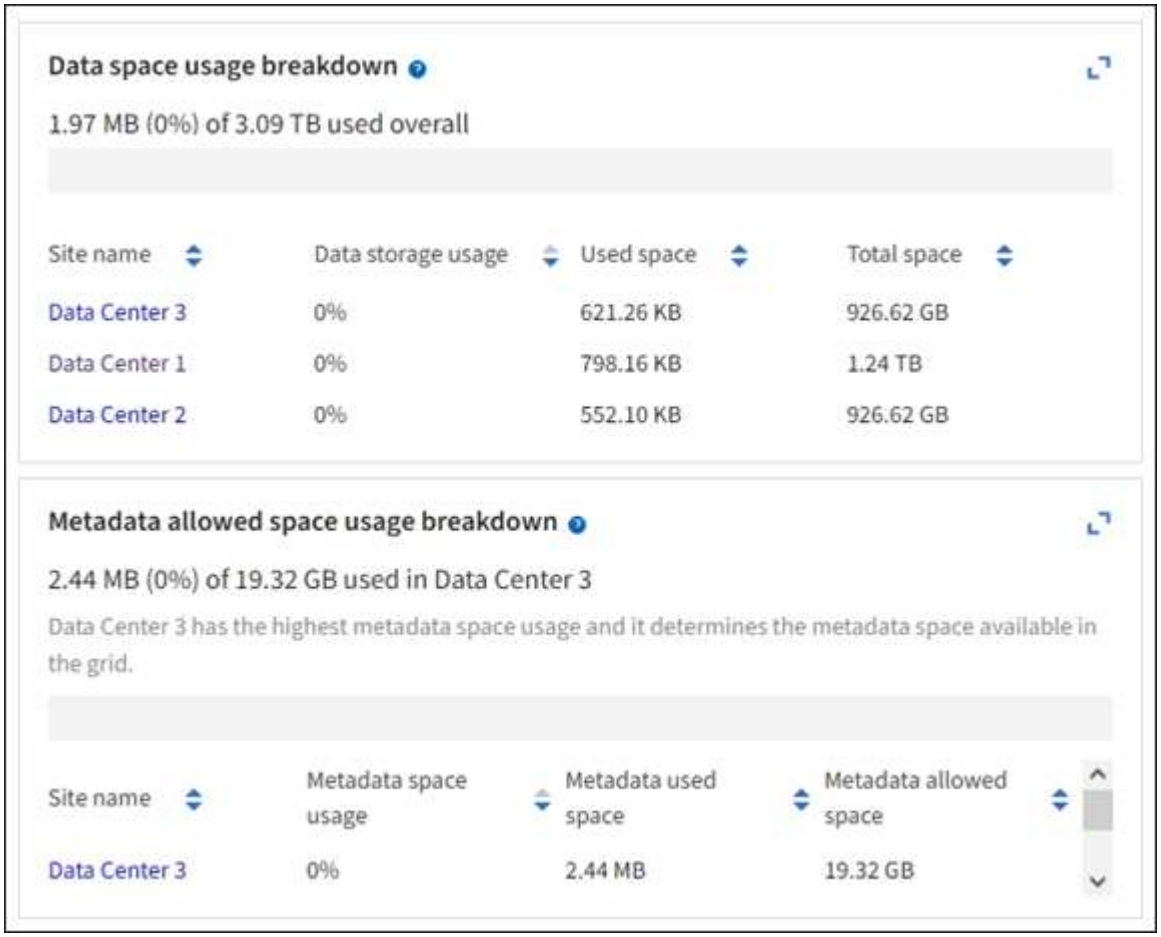
手順

1. グリッド全体および各データセンターで使用可能なストレージの量を評価します。

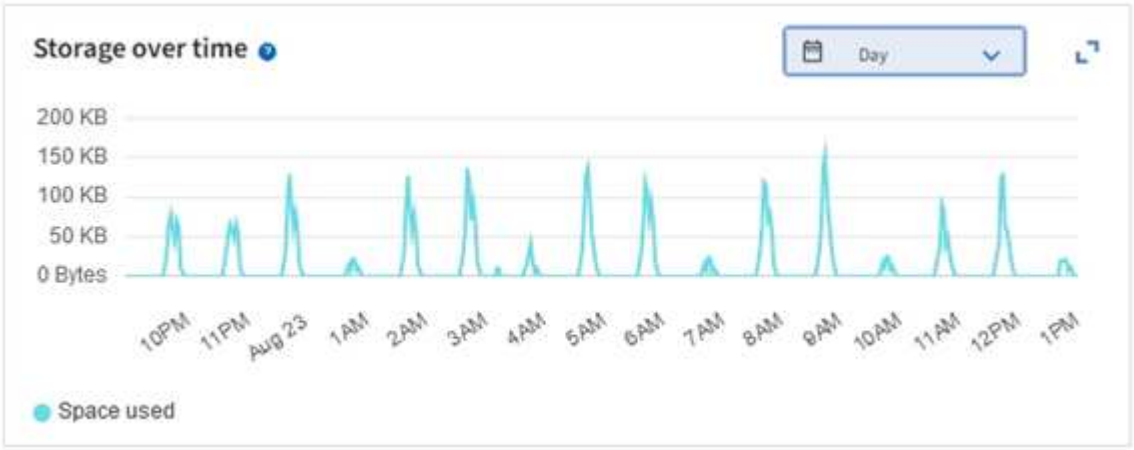
   a. *ダッシュボード > 概要*を選択します。

   b. データ領域使用量の内訳カードとメタデータ許容領域使用量の内訳カードの値をメモします。各カードには、ストレージの使用率、使用済みスペースの容量、およびサイトごとに使用可能または許可されている合計スペースがリストされます。

      概要にはアーカイブ メディアは含まれません。



a. ストレージの経時変化カードのグラフに注目してください。期間ドロップダウンを使用すると、ストレージが消費される速度を判断するのに役立ちます。



2. 使用されたストレージの量と、オブジェクト データおよびオブジェクト メタデータ用にグリッド上で使用可能なストレージの量に関する詳細情報を確認するには、[ノード] ページを使用します。

a. 「NODES」を選択します。

b. ***grid*** > *ストレージ*を選択します。

c. 使用済みストレージ - オブジェクト データ と 使用済みストレージ - オブジェクト メタデータ のチャートの上にカーソルを置くと、グリッド全体で使用可能なオブジェクト ストレージとオブジェクト メタデータ ストレージの量、および時間の経過に伴う使用量が表示されます。

> サイトまたはグリッドの合計値には、オフライン ノードなど、少なくとも 5 分間メトリックを報告していないノードは含まれません。

3. グリッドの使用可能なストレージ容量が消費される前に、ストレージ ノードまたはストレージ ボリュー

ムを追加する拡張を実行することを計画します。

拡張のタイミングを計画するときは、追加のストレージの調達とインストールにどれくらいの時間がかかるかを考慮してください。

> ILM ポリシーで消去コーディングを使用する場合は、既存のストレージ ノードが約 70% 使用されたときに拡張して、追加する必要があるノードの数を減らすことをお勧めします。

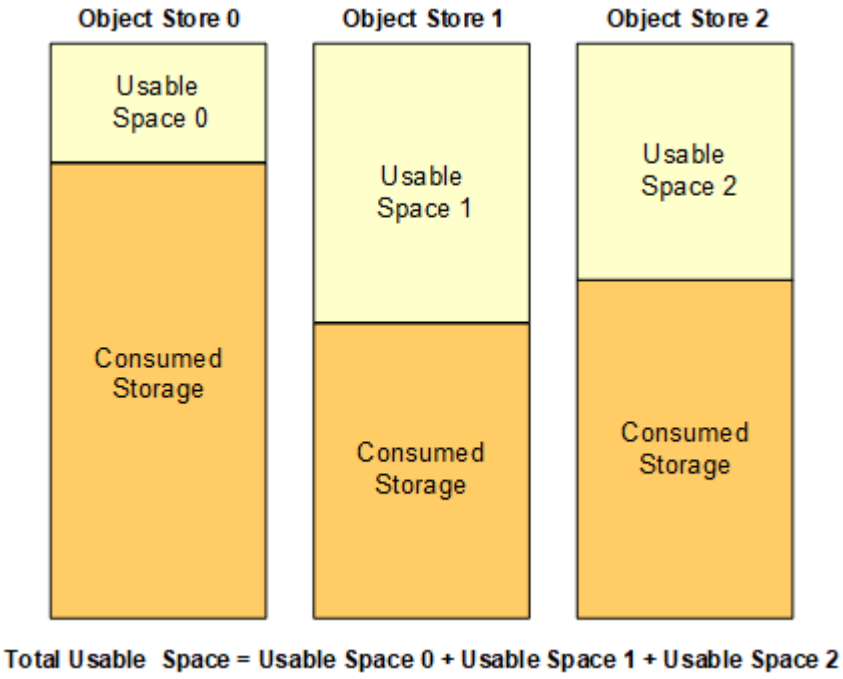
ストレージ拡張の計画の詳細については、"StorageGRIDの拡張手順" 。

各ストレージノードのストレージ容量を監視する

各ストレージ ノードの合計使用可能スペースを監視して、ノードに新しいオブジェクト データ用の十分なスペースがあることを確認します。

タスク概要

使用可能スペースとは、オブジェクトを保存するために使用できるストレージスペースの量です。ストレージ ノードの合計使用可能スペースは、ノード内のすべてのオブジェクト ストアの使用可能スペースを合計して計算されます。



手順

1. **NODES** > ***Storage Node*** > **Storage** を選択します。

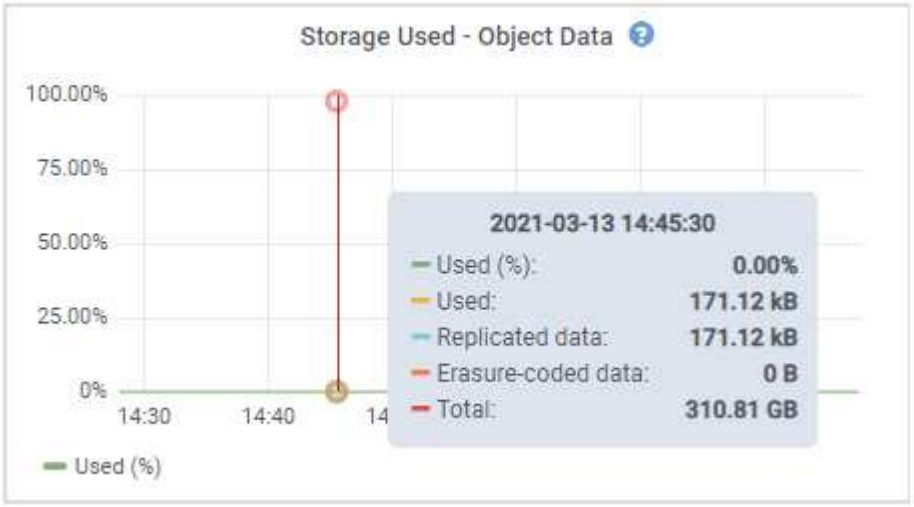
   ノードのグラフと表が表示されます。

2. 使用済みストレージ - オブジェクト データ グラフの上にカーソルを置きます。

   次の値が表示されます。

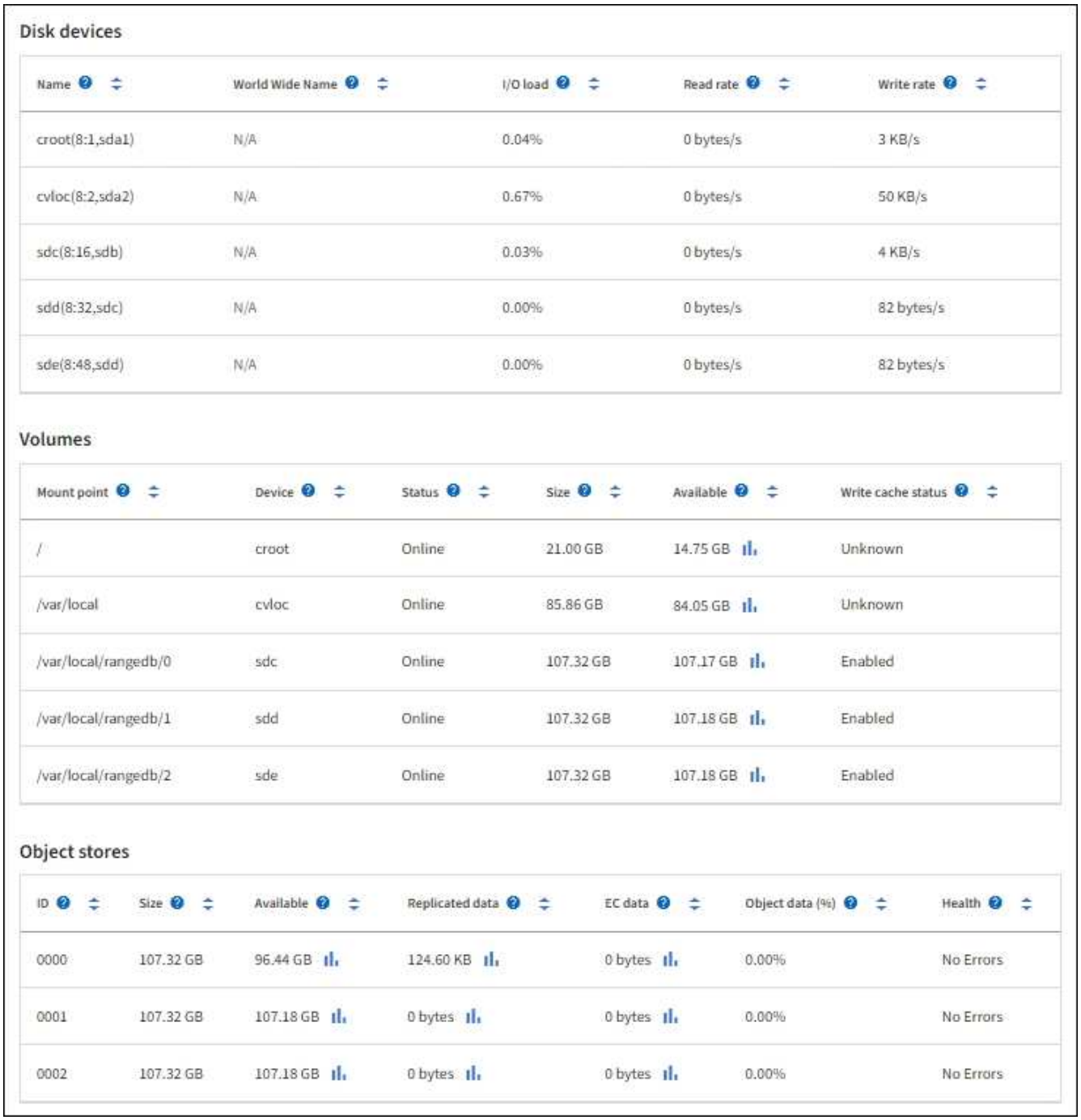
   - 使用済み **(%)**: オブジェクト データに使用されている合計使用可能スペースの割合。

- 使用済み: オブジェクト データに使用されている合計使用可能スペースの量。
- 複製されたデータ: このノード、サイト、またはグリッド上の複製されたオブジェクト データの量の推定値。
- 消去コード化データ: このノード、サイト、またはグリッド上の消去コード化オブジェクト データの量の推定値。
- 合計: このノード、サイト、またはグリッド上の使用可能なスペースの合計量。使用価値は `storagegrid_storage_utilization_data_bytes`メトリック。



3. グラフの下のボリュームとオブジェクト ストアのテーブルで利用可能な値を確認します。

これらの値のグラフを表示するには、グラフアイコンをクリックします。 [利用可能] 列に表示されます。



Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.67%	0 bytes/s	50 KB/s
sdc(8:16,sdb)	N/A	0.03%	0 bytes/s	4 KB/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s

Volumes

Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.75 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.05 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	124.60 KB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

4. 時間の経過に伴う値を監視して、使用可能なストレージ領域の消費率を推定します。
5. 正常なシステム操作を維持するには、使用可能なスペースが消費される前に、ストレージ ノードを追加したり、ストレージ ボリュームを追加したり、オブジェクト データをアーカイブしたりします。

   拡張のタイミングを計画するときは、追加のストレージの調達とインストールにどれくらいの時間がかかるかを考慮してください。

   > ILM ポリシーで消去コーディングを使用する場合は、既存のストレージ ノードが約 70% 使用されたときに拡張して、追加する必要があるノードの数を減らすことをお勧めします。

   ストレージ拡張の計画の詳細については、"StorageGRIDの拡張手順" 。

その"低オブジェクトデータストレージ"ストレージ ノードにオブジェクト データを保存するのに十分なスペースが残っていない場合にアラートがトリガーされます。

各ストレージノードのオブジェクトメタデータ容量を監視する

各ストレージ ノードのメタデータの使用状況を監視し、重要なデータベース操作に十分なスペースが確保されていることを確認します。オブジェクト メタデータが許可されたメタデータ領域の 100% を超える前に、各サイトに新しいストレージ ノードを追加する必要があります。

タスク概要

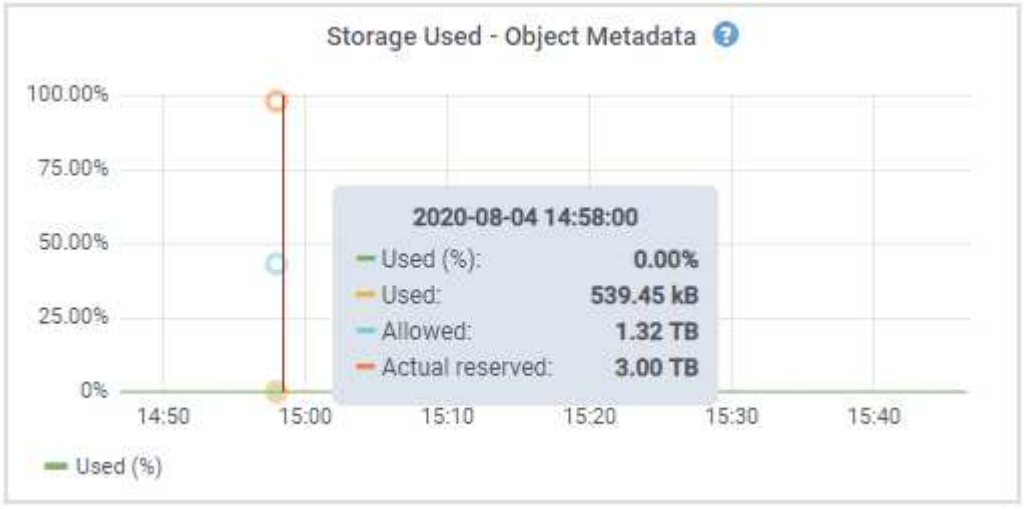
StorageGRID は、冗長性を提供し、オブジェクト メタデータの損失を防ぐために、各サイトでオブジェクト メタデータのコピーを 3 つ保持します。 3 つのコピーは、各ストレージ ノードのストレージ ボリューム 0 上のメタデータ用に予約されているスペースを使用して、各サイトのすべてのストレージ ノードに均等に分散されます。

場合によっては、グリッドのオブジェクト メタデータ容量がオブジェクト ストレージ容量よりも早く消費されることがあります。たとえば、通常、多数の小さなオブジェクトを取り込む場合、十分なオブジェクト ストレージ容量が残っていても、メタデータ容量を増やすためにストレージ ノードを追加する必要がある場合があります。

メタデータの使用量を増やす要因としては、ユーザー メタデータとタグのサイズと量、マルチパート アップロードのパートの合計数、ILM ストレージの場所の変更頻度などが挙げられます。

手順

1. **NODES** > ***Storage Node*** > **Storage** を選択します。
2. 特定の時間の値を表示するには、「使用済みストレージ - オブジェクト メタデータ」グラフの上にカーソルを置きます。



使用済み（**%**）

このストレージ ノードで使用されている、許可されたメタデータ領域の割合。

Prometheus メトリック: `storagegrid_storage_utilization_metadata_bytes`そして `storagegrid_storage_utilization_metadata_allowed_bytes`

使用済み

このストレージ ノードで使用されている許可されたメタデータ領域のバイト数。

Prometheus メトリック: `storagegrid_storage_utilization_metadata_bytes`

許容

このストレージ ノード上のオブジェクト メタデータに許可されるスペース。各ストレージノードでこの値がどのように決定されるかについては、"許可されたメタデータスペースの完全な説明" 。

Prometheus メトリック: `storagegrid_storage_utilization_metadata_allowed_bytes`

実際の予約

このストレージ ノード上のメタデータ用に予約されている実際のスペース。必須のメタデータ操作に許可されたスペースと必要なスペースが含まれます。各ストレージノードのこの値がどのように計算されるかについては、"メタデータ用に実際に予約されているスペースの完全な説明" 。

Prometheus メトリックは将来のリリースで追加される予定です。

> ⓘ サイトまたはグリッドの合計値には、オフライン ノードなど、少なくとも 5 分間メトリックを報告していないノードは含まれません。

3. 使用率 **(%)** の値が 70% 以上の場合は、各サイトにストレージ ノードを追加してStorageGRIDシステムを拡張します。

> ⓘ メタデータ ストレージ不足 アラートは、使用済み **(%)** 値が特定のしきい値に達するとトリガーされます。オブジェクト メタデータが許可されたスペースの 100% を超えるスペースを使用すると、望ましくない結果が発生する可能性があります。

新しいノードを追加すると、システムはサイト内のすべてのストレージ ノード間でオブジェクト メタデータを自動的に再調整します。参照"StorageGRIDシステムを拡張するための手順"。

スペース使用予測を監視する

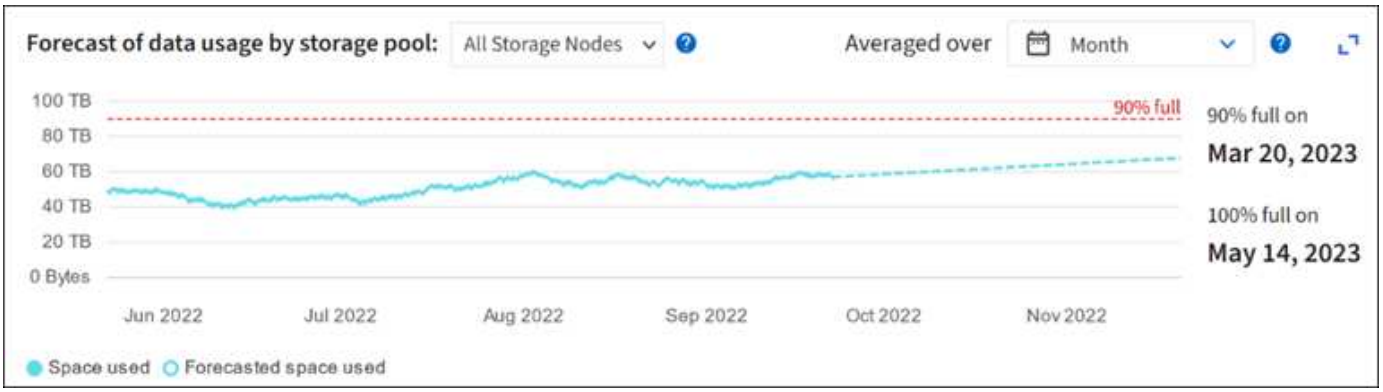
ユーザーデータとメタデータのスペース使用量予測を監視して、いつ必要になるかを予測します。"グリッドを展開する" 。

消費率が時間の経過とともに変化することに気付いた場合は、[平均期間] プルダウンからより短い範囲を選択して、最新の取り込みパターンのみを反映させます。季節的なパターンに気付いた場合は、より長い範囲を選択します。

新しいStorageGRIDをインストールしている場合は、スペース使用量の予測を評価する前に、データとメタデータを蓄積してください。

手順

1. ダッシュボードで、[ストレージ]を選択します。
2. ダッシュボード カード、ストレージ プール別のデータ使用量の予測、サイト別のメタデータ使用量の予測を表示します。
3. これらの値を使用して、データおよびメタデータのストレージ用に新しいストレージ ノードを追加する必要がある時期を見積もってください。



情報ライフサイクル管理を監視する

情報ライフサイクル管理 (ILM) システムは、グリッドに保存されているすべてのオブジェクトのデータ管理を提供します。グリッドが現在の負荷を処理できるかどうか、またはさらにリソースが必要かどうかを把握するには、ILM 操作を監視する必要があります。

タスク概要

StorageGRIDシステムは、アクティブな ILM ポリシーを適用してオブジェクトを管理します。 ILM ポリシーと関連する ILM ルールによって、作成されるコピーの数、作成されるコピーの種類、コピーの配置場所、および各コピーが保持される期間が決まります。

オブジェクトの取り込みやその他のオブジェクト関連のアクティビティによって、 StorageGRID がILM を評価できる速度が超過する可能性があり、その結果、ILM 配置指示をほぼリアルタイムで実行できないオブジェクトがシステムによってキューに入れられることになります。 StorageGRID がクライアントのアクションに対応しているかどうかを監視する必要があります。

グリッドマネージャーダッシュボードタブを使用する

手順

Grid Manager ダッシュボードの ILM タブを使用して、ILM 操作を監視します。

1. グリッド マネージャーにSign in。
2. ダッシュボードから ILM タブを選択し、ILM キュー (オブジェクト) カードと ILM 評価レート カードの値をメモします。

   ダッシュボードの ILM キュー (オブジェクト) カードに一時的な急増が発生することが予想されます。しかし、キューが増加し続け、減少しない場合は、グリッドが効率的に動作するために、より多くのリソース（ストレージ ノードを増やすか、ILM ポリシーによってオブジェクトがリモートの場所に配置されている場合はより多くのネットワーク帯域幅）が必要になります。

NODESページを使用する

手順

さらに、**NODES** ページを使用して ILM キューを調査します。

> **NODES** ページのチャートは、将来のStorageGRIDリリースで対応するダッシュボード カードに置き換えられます。

1. 「NODES」を選択します。
2. グリッド名 > **ILM** を選択します。
3. ILM キュー グラフの上にカーソルを置くと、特定の時点での次の属性の値が表示されます。
   - キューに入れられたオブジェクト **(**クライアント操作から**)**: クライアント操作 (取り込みなど) により ILM 評価を待機しているオブジェクトの合計数。
   - キューに入れられたオブジェクト **(**すべての操作から**)**: ILM 評価を待機しているオブジェクトの合計数。
   - スキャン レート **(**オブジェクト**/**秒**)**: グリッド内のオブジェクトがスキャンされ、ILM のキューに追加されるレート。
   - 評価レート **(**オブジェクト**/**秒**)**: グリッド内の ILM ポリシーに対してオブジェクトが評価される現在のレート。
4. ILM キュー セクションで、次の属性を確認します。

   ILM キュー セクションはグリッドのみに含まれます。この情報は、サイトまたはストレージ ノードの ILM タブには表示されません。

   - スキャン期間 **-** 推定: すべてのオブジェクトの完全な ILM スキャンを完了するのにかかる推定時間。

     完全スキャンでは、すべてのオブジェクトに ILM が適用されていることが保証されるわけではありません。

   - 試行された修復: 複製されたデータに対して試行されたオブジェクト修復操作の合計数。このカウントは、ストレージ ノードが高リスクのオブジェクトの修復を試みるたびに増加します。グリッドが混雑している場合は、リスクの高い ILM 修復が優先されます。

     修復後にレプリケーションが失敗した場合、同じオブジェクトの修復が再度増加する可能性があります。

これらの属性は、ストレージ ノード ボリュームのリカバリの進行状況を監視するときに役立ちます。修復の試行回数の増加が止まり、完全スキャンが完了した場合、修復は完了したと考えられます。

ネットワークとシステムリソースを監視する

ノードとサイト間のネットワークの整合性と帯域幅、および個々のグリッド ノードによるリソースの使用は、効率的な運用に重要です。

ネットワーク接続とパフォーマンスを監視する

情報ライフサイクル管理 (ILM) ポリシーによって、複製されたオブジェクトがサイト間でコピーされるか、サイト損失保護を提供するスキームを使用して消去コード化されたオブジェクトが保存される場合、ネットワーク接続と帯域幅は特に重要です。サイト間のネットワークが利用できない場合、ネットワークの遅延が大きすぎる場合、またはネットワーク帯域幅が不十分な場合、一部の ILM ルールではオブジェクトを期待どおりに配置できない可能性があります。これにより、取り込みの失敗 (ILM ルールに [厳密な取り込み] オプションが選択されている場合) が発生したり、取り込みのパフォーマンスが低下して ILM バックログが発生したりする可能性があります。

グリッド マネージャーを使用して接続とネットワーク パフォーマンスを監視し、問題があればすぐに対処で

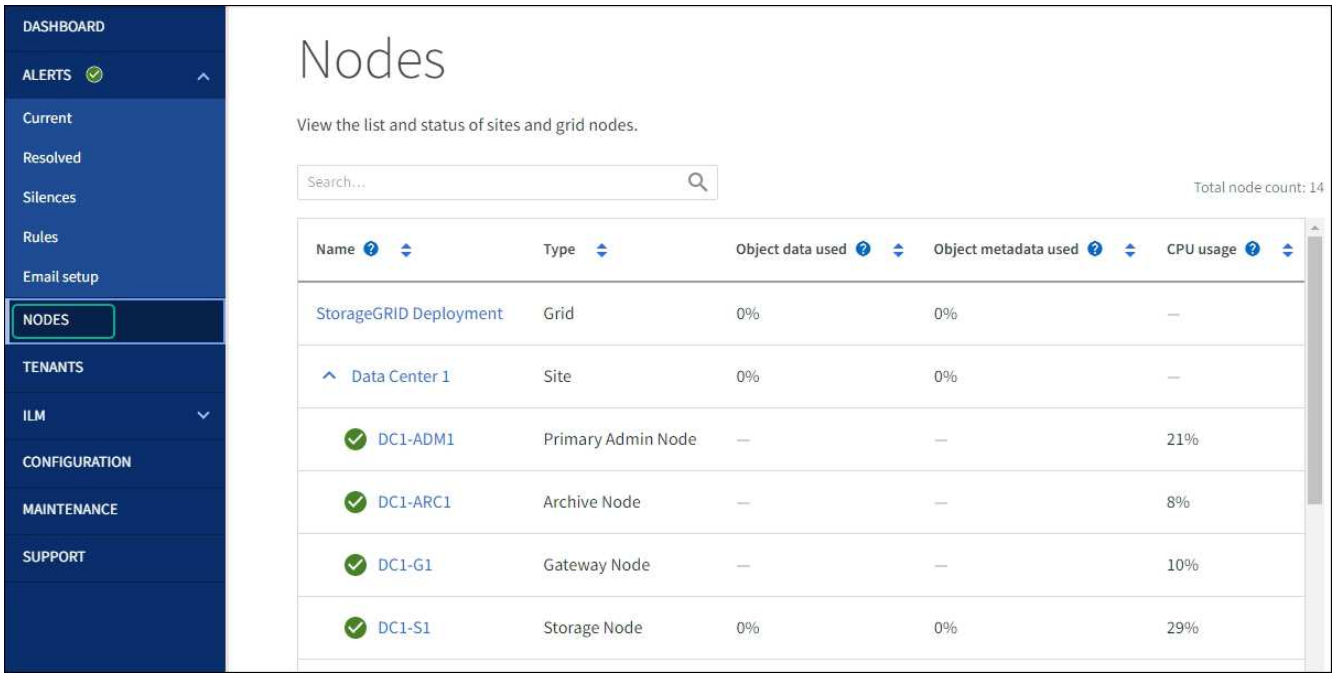
きるようにします。

さらに、考慮する"ネットワークトラフィック分類ポリシーの作成"特定のテナント、バケット、サブネット、またはロードバランサエンドポイントに関連するトラフィックを監視できるようになります。必要に応じてトラフィック制限ポリシーを設定できます。

手順

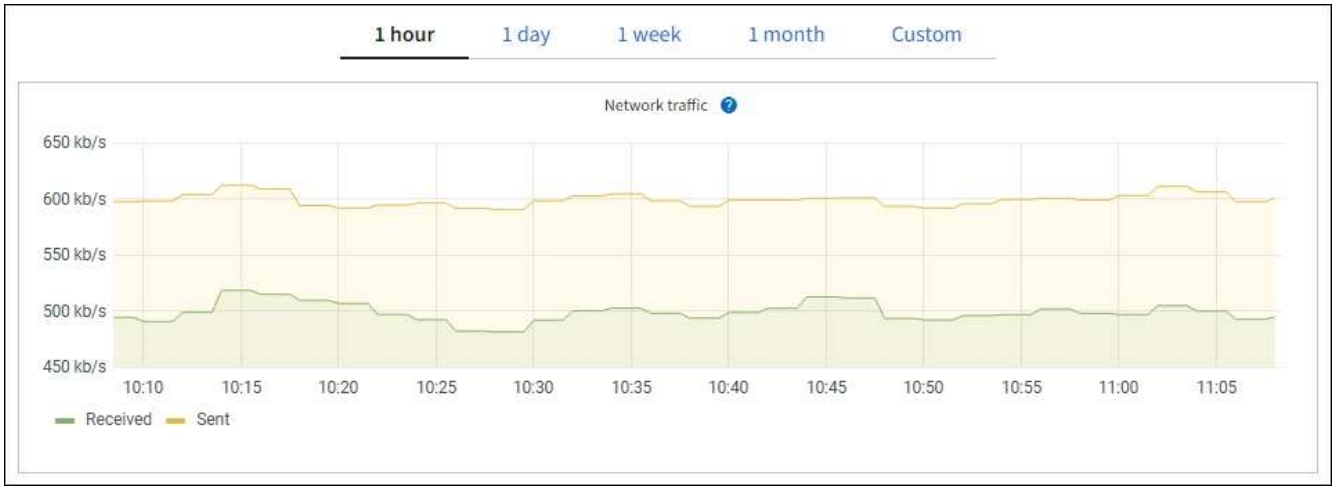
1. 「NODES」を選択します。

   ノード ページが表示されます。グリッド内の各ノードは表形式でリストされます。

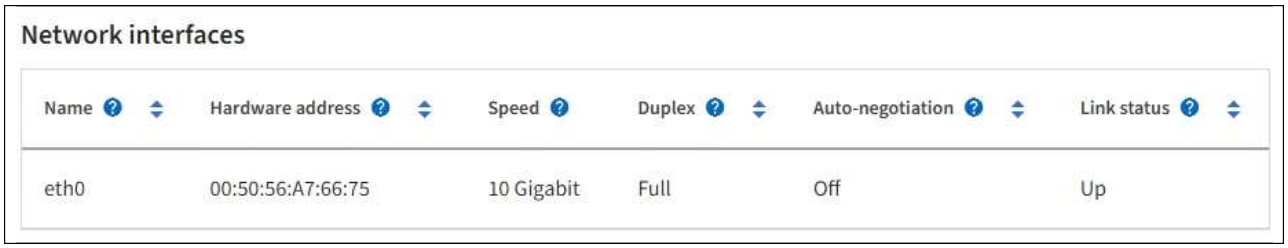


2. グリッド名、特定のデータセンター サイト、またはグリッド ノードを選択し、[ネットワーク] タブを選択します。

   ネットワーク トラフィック グラフには、グリッド全体、データ センター サイト、またはノードの全体的なネットワーク トラフィックの概要が表示されます。

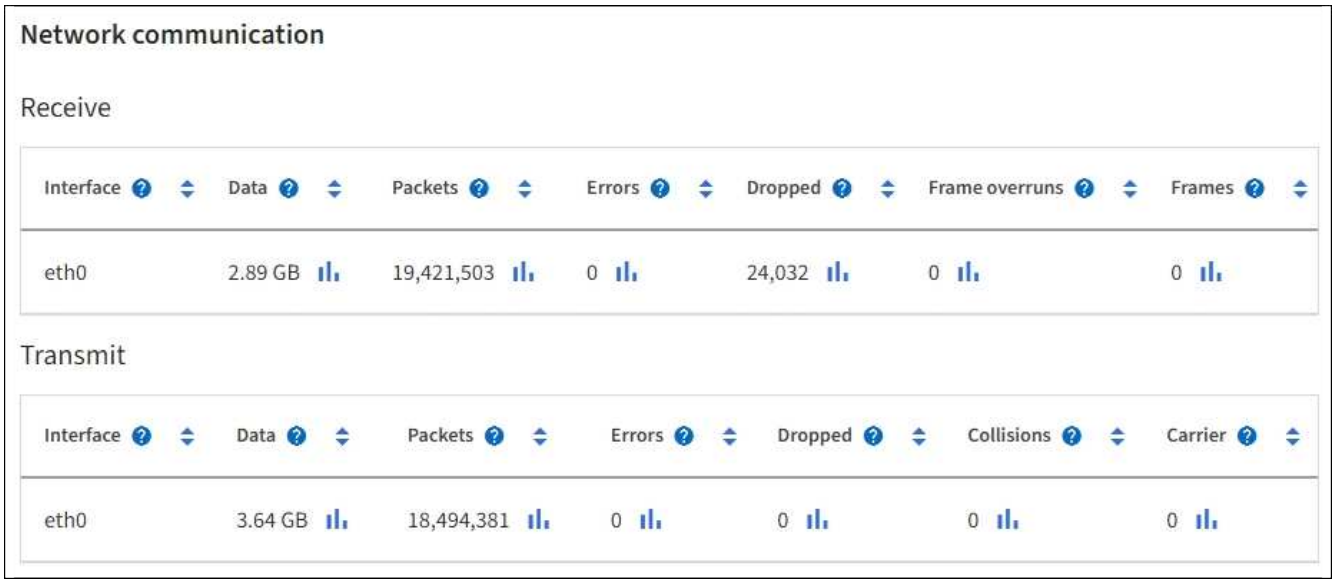


   a. グリッド ノードを選択した場合は、下にスクロールしてページの ネットワーク インターフェイス セクションを確認します。



b. グリッド ノードの場合は、下にスクロールしてページの ネットワーク通信 セクションを確認します。

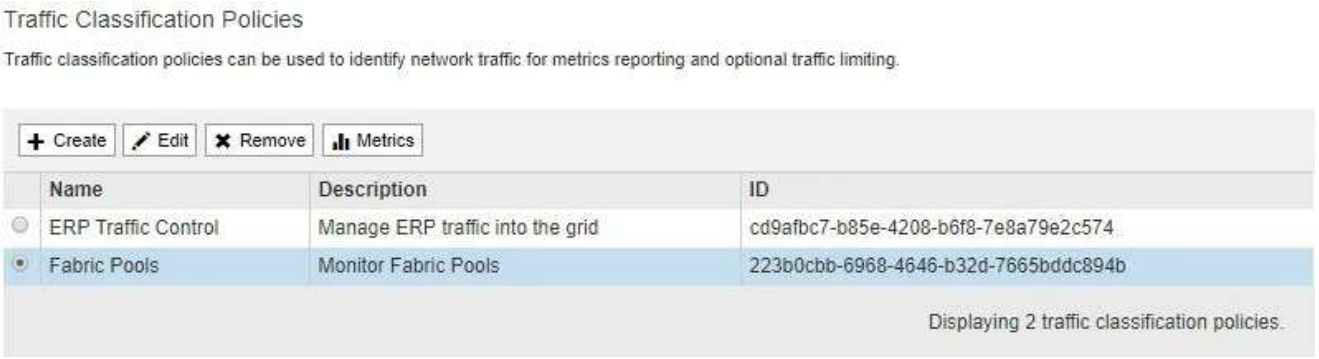
受信テーブルと送信テーブルには、各ネットワークで受信および送信されたバイト数とパケット数、およびその他の受信および送信メトリックが表示されます。



3. トラフィック分類ポリシーに関連付けられたメトリックを使用して、ネットワーク トラフィックを監視します。

a. 構成 > ネットワーク > *トラフィック分類*を選択します。

「トラフィック分類ポリシー」ページが表示され、既存のポリシーが表にリストされます。



a. ポリシーに関連付けられたネットワーク メトリックを示すグラフを表示するには、ポリシーの左側にあるラジオ ボタンを選択し、[メトリック] をクリックします。

b. グラフを確認して、ポリシーに関連付けられたネットワーク トラフィックを理解します。

トラフィック分類ポリシーがネットワーク トラフィックを制限するように設計されている場合は、トラフィックが制限される頻度を分析し、ポリシーが引き続きニーズを満たしているかどうかを判断します。時々、"必要に応じて各トラフィック分類ポリシーを調整する" 。

関連情報

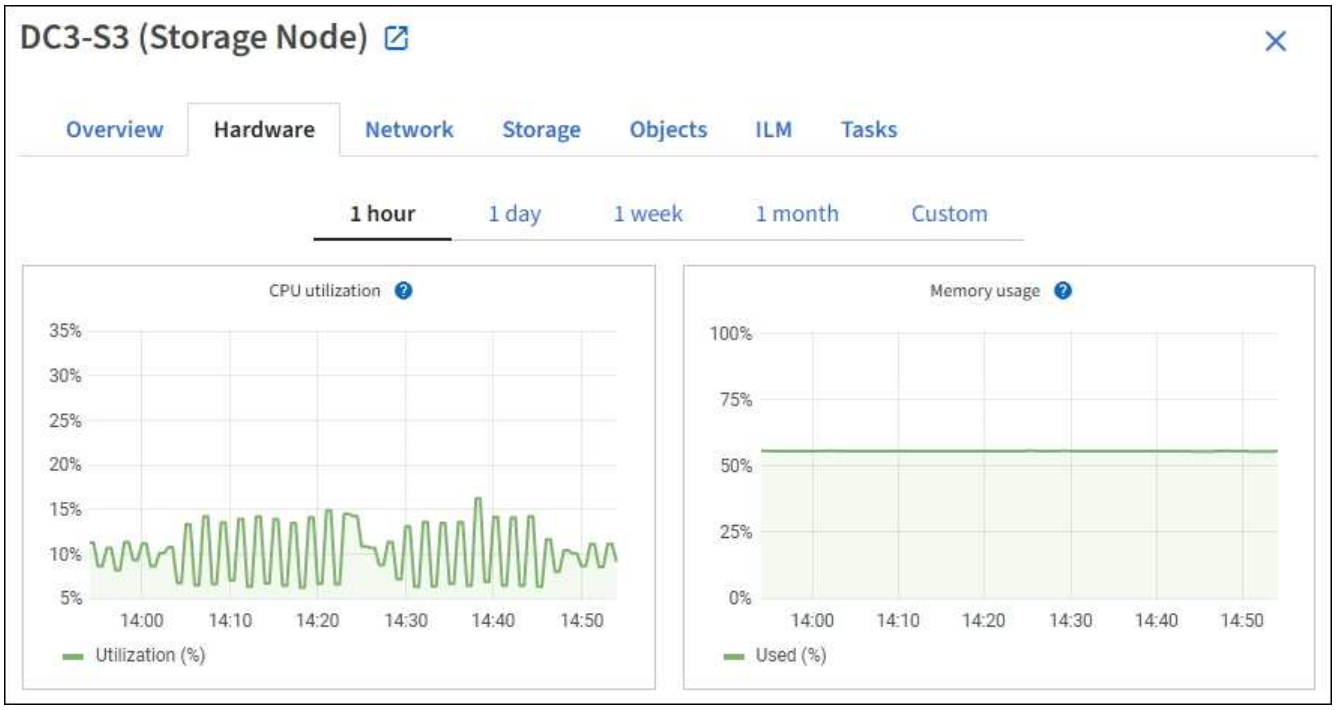
- "ネットワークタブを表示する"
- "ノード接続状態を監視する"

ノードレベルのリソースを監視する

個々のグリッド ノードを監視して、リソースの使用レベルを確認します。ノードが継続的に過負荷になっている場合、効率的な操作のためにさらに多くのノードが必要になる可能性があります。

手順

1. **NODES** ページからノードを選択します。
2. ハードウェア タブを選択すると、CPU 使用率とメモリ使用量のグラフが表示されます。



3. 異なる時間間隔を表示するには、チャートまたはグラフの上にあるコントロールのいずれかを選択します。 1 時間、1 日、1 週間、1 か月の間隔で情報を表示できます。カスタム間隔を設定して、日付と時刻の範囲を指定することもできます。
4. ノードがストレージ アプライアンスまたはサービス アプライアンス上でホストされている場合は、下にスクロールしてコンポーネントのテーブルを表示します。すべてのコンポーネントのステータスは「正常」である必要があります。その他のステータスを持つコンポーネントを調査します。

関連情報

- "アプライアンス ストレージ ノードに関する情報を表示する"
- "アプライアンスの管理ノードとゲートウェイノードに関する情報を表示します"

すべての S3 クライアント アクティビティは、 StorageGRIDテナント アカウントに関連付けられています。グリッド マネージャーを使用すると、すべてのテナントまたは特定のテナントのストレージ使用量やネットワーク トラフィックを監視できます。監査ログまたは Grafana ダッシュボードを使用して、テナントがStorageGRID をどのように使用しているかについてのより詳細な情報を収集できます。

開始する前に

- グリッドマネージャにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは"ルートアクセスまたはテナントアカウントの権限"。

すべてのテナントを表示

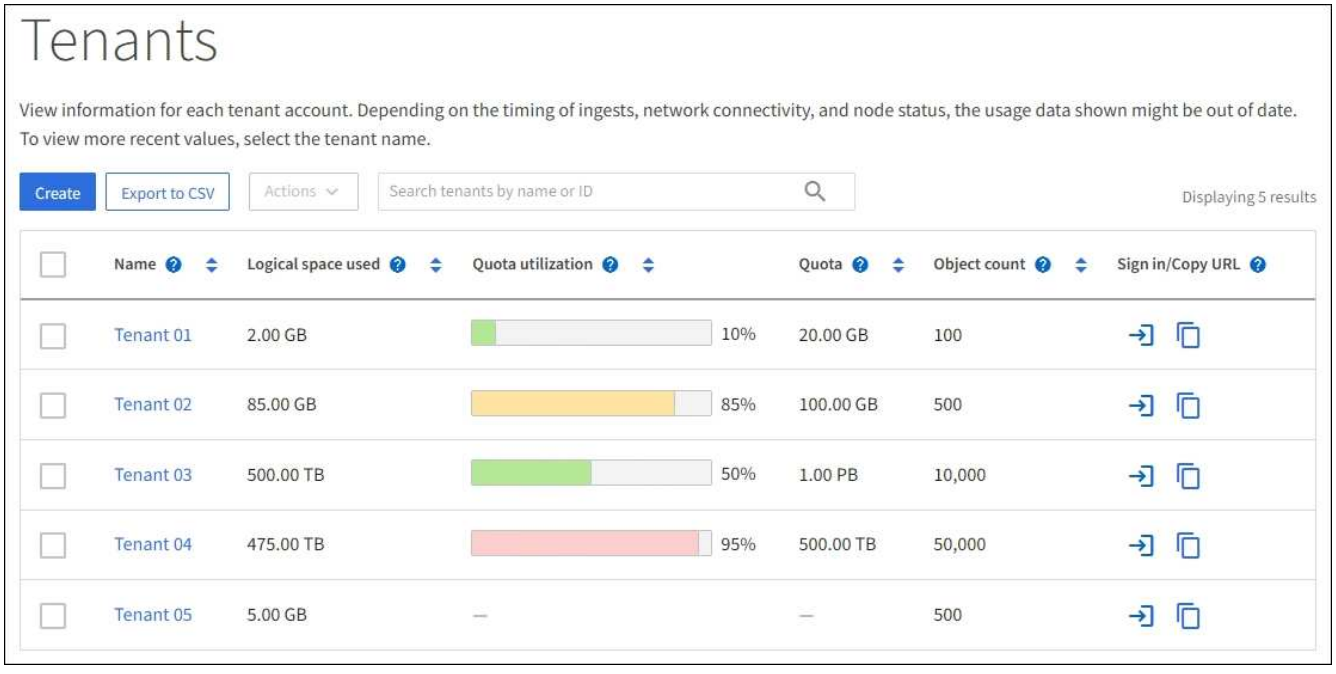
「テナント」ページには、現在のすべてのテナント アカウントの基本情報が表示されます。

手順

1. *TENANTS*を選択します。
2. テナント ページに表示される情報を確認します。

   各テナントの使用済み論理スペース、クォータ使用量、クォータ、およびオブジェクト数がリストされます。テナントにクォータが設定されていない場合、クォータ使用量フィールドとクォータフィールドにダッシュ (—) が含まれます。

   使用済みスペースの値は推定値です。これらの見積りは、取り込みのタイミング、ネットワーク接続、およびノードの状態によって影響を受けます。



3. 必要に応じて、サインインリンクを選択してテナントアカウントにサインインします。 *Sign in/URL をコピー*列に表示されます。

4. 必要に応じて、[URL のコピー] リンクを選択して、テナントのサインイン ページの URL をコピーします。 *Sign in/URLをコピー*列に表示されます。
5. 必要に応じて、*CSVにエクスポート*を選択して、 `.csv`すべてのテナントの使用状況値を含むファイル。

   開くか保存するかを選択するメッセージが表示されます。 `.csv`ファイル。

   の内容は `.csv`ファイルは次の例のようになります。

Tenant ID	Display Name	Space Used (Bytes)	Quota utilization (%)	Quota (Bytes)	Object Count	Protocol
12659822378459233654	Tenant 01	2000000000	10	20000000000	100	S3
99658234112547853685	Tenant 02	85000000000	85	110000000	500	S3
03521145586975586321	Tenant 03	60500000000	50	150000	10000	S3
44251365987569885632	Tenant 04	4750000000	95	140000000	50000	S3
36521587546689565123	Tenant 05	5000000000	Infinity		500	S3

   開くことができます `.csv`スプレッドシート アプリケーションでファイルを保存するか、自動化で使用します。

6. オブジェクトがリストされていない場合は、オプションで [アクション] > [削除] を選択して、1 つ以上のテナントを削除します。見る"テナントアカウントを削除する" 。

   アカウントにバケットまたはコンテナが含まれている場合、テナント アカウントを削除することはできません。

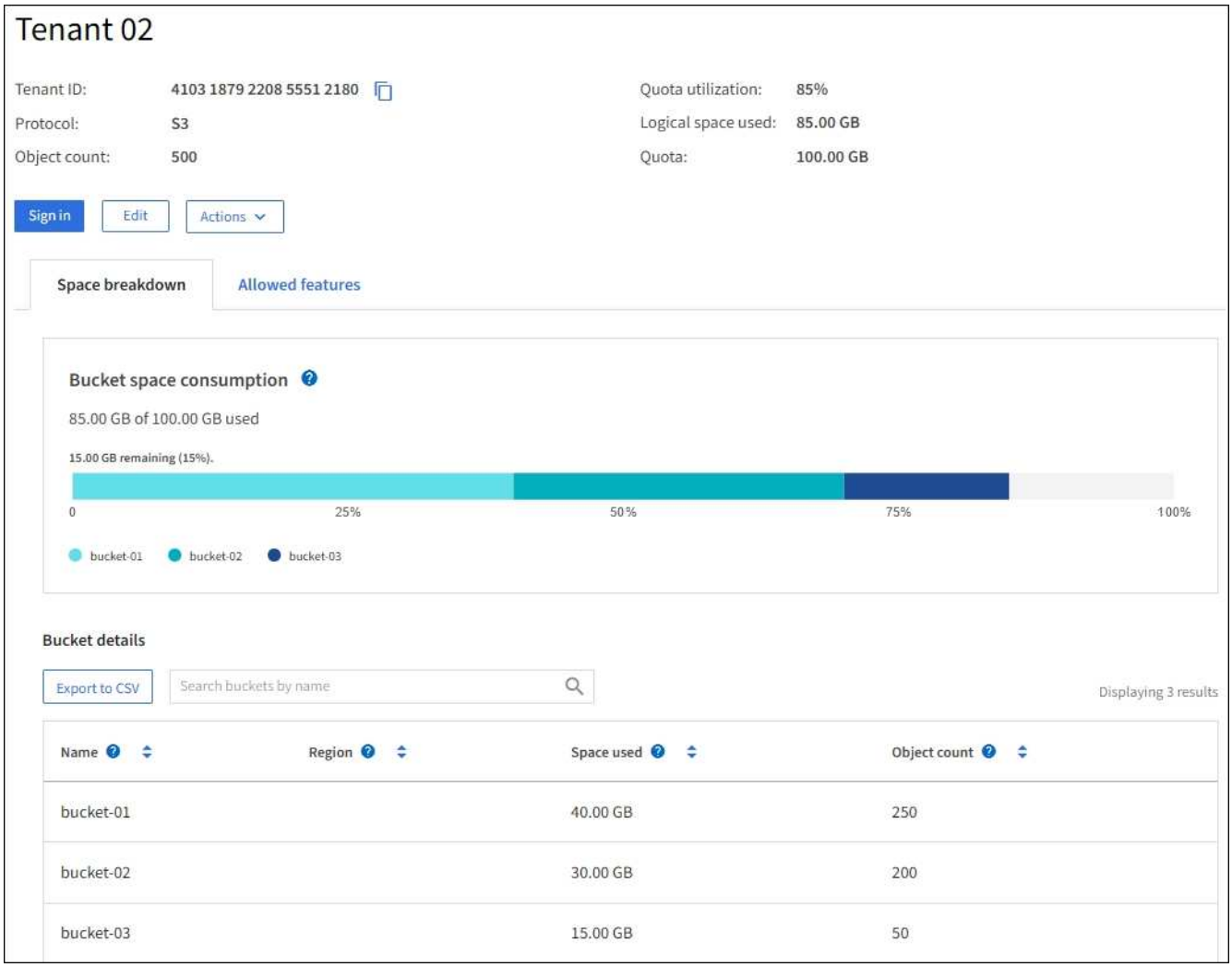
特定のテナントを表示する

特定のテナントの詳細を表示できます。

手順

1. 「テナント」ページからテナント名を選択します。

   テナントの詳細ページが表示されます。



2. ページ上部のテナントの概要を確認します。

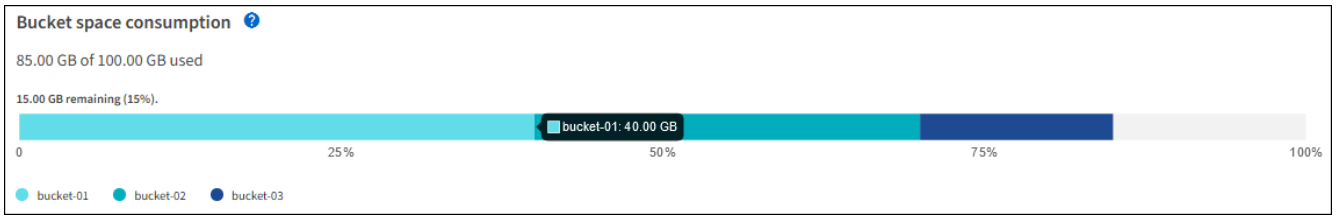
   詳細ページのこのセクションでは、テナントのオブジェクト数、クォータ使用量、使用されている論理スペース、クォータ設定など、テナントの概要情報が提供されます。

3. *スペースの内訳*タブから、*スペース消費量*グラフを確認します。

   このグラフには、テナントのすべての S3 バケットの合計スペース消費量が表示されます。

   このテナントにクォータが設定されている場合は、使用済みおよび残りのクォータの量がテキストで表示されます（例： `85.00 GB of 100 GB used` ）。クォータが設定されていない場合、テナントのクォータは無制限となり、テキストには使用されているスペースの量のみが含まれます（例： `85.00 GB used` ）。棒グラフには、各バケットまたはコンテナの割り当ての割合が表示されます。テナントがストレージ クォータを 1% 以上超過し、少なくとも 1 GB 超過している場合、チャートには合計クォータと超過量が表示されます。

   棒グラフの上にカーソルを置くと、各バケットまたはコンテナで使用されているストレージが表示されます。空き領域セグメントの上にカーソルを置くと、残っているストレージ クォータの量を確認できます。



クォータ使用量は内部推定に基づいており、場合によっては超過する可能性があります。たとえば、 StorageGRID は、テナントがオブジェクトのアップロードを開始するとクォータをチェックし、テナントがクォータを超過している場合は新しい取り込みを拒否します。ただし、 StorageGRID は、クォータを超過したかどうかを判断する際に、現在のアップロードのサイズを考慮しません。オブジェクトが削除されると、クォータ使用量が再計算されるまで、テナントは一時的に新しいオブジェクトのアップロードができなくなる可能性があります。クォータ使用量の計算には 10 分以上かかる場合があります。

テナントのクォータ使用量は、テナントがStorageGRIDにアップロードしたオブジェクトデータの合計量 (論理サイズ) を示します。クォータ使用量は、それらのオブジェクトとそのメタデータのコピーを保存するために使用されるスペース (物理サイズ) を表すものではありません。

テナント クォータ使用量高 アラート ルールを有効にして、テナントがクォータを消費しているかどうかを判断できます。有効にすると、テナントがクォータの 90% を使用したときにこのアラートがトリガーされます。手順については、"アラートルールを編集する" 。

4. *スペースの内訳*タブから、*バケットの詳細*を確認します。

   この表には、テナントの S3 バケットがリストされます。使用済みスペースは、バケットまたはコンテナ内のオブジェクト データの合計量です。この値は、ILM コピーおよびオブジェクト メタデータに必要なストレージ スペースを表すものではありません。

5. 必要に応じて、[CSV にエクスポート] を選択して、各バケットまたはコンテナの使用状況値を含む .csv ファイルを表示およびエクスポートします。

   個々のS3テナントの `.csv`ファイルは次の例のようになります。

Tenant ID	Bucket Name	Space Used (Bytes)	Number of Objects
64796966429038923647	bucket-01	88717711	14
64796966429038923647	bucket-02	21747507	11
64796966429038923647	bucket-03	15294070	3

   開くことができます `.csv`スプレッドシート アプリケーションでファイルを保存するか、自動化で使用します。

6. 必要に応じて、[許可された機能] タブを選択して、テナントに対して有効になっている権限と機能のリストを表示します。見る"テナントアカウントの編集"これらの設定を変更する必要がある場合。
7. テナントに グリッド フェデレーション接続の使用 権限がある場合は、オプションで グリッド フェデレーション タブを選択して、接続の詳細を確認します。

   見る"グリッドフェデレーションとは何ですか?"そして"グリッドフェデレーションの許可されたテナントを管理する"。

ネットワークトラフィックを表示する

テナントにトラフィック分類ポリシーが設定されている場合は、そのテナントのネットワーク トラフィックを確認します。

手順

1. 構成 > ネットワーク > *トラフィック分類*を選択します。

   「トラフィック分類ポリシー」ページが表示され、既存のポリシーが表にリストされます。

2. ポリシーのリストを確認し、特定のテナントに適用されるポリシーを特定します。
3. ポリシーに関連付けられているメトリックを表示するには、ポリシーの左側にあるラジオ ボタンを選択し、メトリック を選択します。
4. グラフを分析して、ポリシーがトラフィックを制限している頻度と、ポリシーを調整する必要があるかどうかを判断します。

見る"トラフィック分類ポリシーを管理する"詳細についてはこちらをご覧ください。

監査ログを使用する

オプションで、監査ログを使用して、テナントのアクティビティをより詳細に監視できます。

たとえば、次の種類の情報を監視できます。

- PUT、GET、DELETEなどの特定のクライアント操作
- オブジェクトのサイズ
- オブジェクトに適用されるILMルール
- クライアントリクエストの送信元IP

監査ログはテキスト ファイルに書き込まれ、任意のログ分析ツールを使用して分析できます。これにより、クライアントのアクティビティをより深く理解したり、高度なチャージバックおよび課金モデルを実装したりできるようになります。

見る"監査ログを確認する"詳細についてはこちらをご覧ください。

Prometheusメトリクスを使用する

必要に応じて、Prometheus メトリックを使用してテナントのアクティビティをレポートします。

- グリッド マネージャーで、サポート > ツール > メトリック を選択します。S3 概要などの既存のダッシュボードを使用して、クライアントのアクティビティを確認できます。

  > メトリクス ページで利用できるツールは、主にテクニカル サポートが使用することを目的としています。これらのツール内の一部の機能とメニュー項目は意図的に機能しないようになっています。

- グリッド マネージャーの上部から、ヘルプ アイコンを選択し、**API** ドキュメント を選択します。グリッド管理 API のメトリック セクションのメトリックを使用して、テナント アクティビティのカスタム アラート ルールとダッシュボードを作成できます。

見る"サポート指標を確認する"詳細についてはこちらをご覧ください。

S3 クライアント操作を監視する

オブジェクトの取り込みと取得の速度、およびオブジェクト数、クエリ、検証のメトリクスを監視できます。クライアント アプリケーションによるStorageGRIDシステム内のオブジェクトの読み取り、書き込み、および変更の成功および失敗の試行回数を表示できます。

開始する前に

- グリッドマネージャにサインインするには、"サポートされているウェブブラウザ" 。

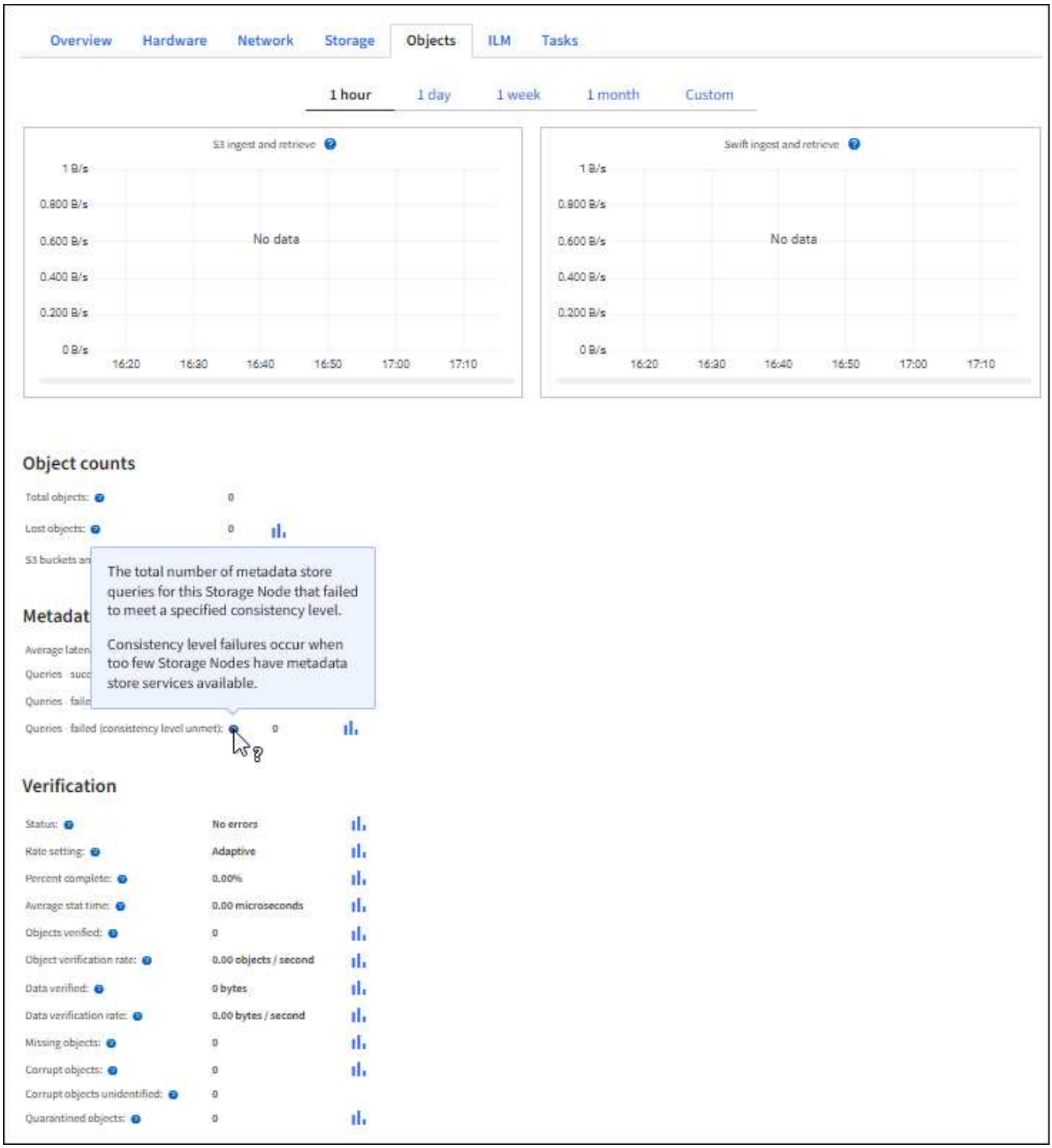
手順

1. ダッシュボードから、[パフォーマンス] タブを選択します。
2. 選択した期間中にストレージノードによって実行されたクライアント操作の数とストレージノードによって受信された API 要求の数をまとめた S3 チャートを参照してください。
3. ノード ページにアクセスするには、**NODES** を選択します。
4. ノードのホームページ (グリッド レベル) から、[オブジェクト] タブを選択します。

   このグラフには、 StorageGRIDシステム全体の S3 取り込みおよび取得速度 (バイト/秒) と、取り込みまたは取得されたデータの量が表示されます。時間間隔を選択するか、カスタム間隔を適用できます。

5. 特定のストレージ ノードの情報を表示するには、左側のリストからノードを選択し、[オブジェクト] タブを選択します。

   グラフには、ノードの取り込み速度と取得速度が表示されます。このタブには、オブジェクト数、メタデータ クエリ、検証操作のメトリックも含まれます。



負荷分散操作を監視する

ロード バランサを使用してStorageGRIDへのクライアント接続を管理している場合は、システムを最初に構成した後、および構成の変更や拡張を実行した後に、ロード バランシング操作を監視する必要があります。

タスク概要

管理ノードまたはゲートウェイ ノード上のロード バランサ サービス、または外部のサードパーティ ロード バランサを使用して、クライアント要求を複数のストレージ ノードに分散できます。

負荷分散を構成した後、オブジェクトの取り込みおよび取得操作がストレージ ノード間で均等に分散されていることを確認する必要があります。要求が均等に分散されるため、 StorageGRID は負荷がかかってもクライアントの要求に応答し続け、クライアントのパフォーマンスを維持することができます。

ゲートウェイ ノードまたは管理ノードの高可用性 (HA) グループをアクティブ バックアップ モードで構成した場合、グループ内の 1 つのノードのみがクライアント要求をアクティブに分散します。

詳細については、以下を参照してください。 "S3クライアント接続を構成する" 。

手順

1. S3 クライアントがロード バランサ サービスを使用して接続する場合は、管理ノードまたはゲートウェイ ノードが期待どおりにトラフィックをアクティブに分散していることを確認します。
   a. 「NODES」を選択します。
   b. ゲートウェイ ノードまたは管理ノードを選択します。
   c. 概要 タブで、ノード インターフェイスが HA グループに属しているかどうか、およびノード インターフェイスにプライマリの役割があるかどうかを確認します。

      プライマリの役割を持つノードと HA グループに属していないノードは、クライアントへのリクエストをアクティブに分散する必要があります。

   d. クライアントリクエストをアクティブに分散する各ノードに対して、"ロードバランサタブ" 。
   e. 過去 1 週間のロード バランサ要求トラフィックのグラフを確認して、ノードが要求をアクティブに分散していることを確認します。

      アクティブ バックアップ HA グループ内のノードは、随時バックアップ ロールを引き受ける場合があります。その間、ノードはクライアントの要求を分散しません。

   f. 過去 1 週間のロード バランサの受信要求率のグラフを確認して、ノードのオブジェクト スループットを確認します。
   g. StorageGRIDシステム内の各管理ノードまたはゲートウェイ ノードに対してこれらの手順を繰り返します。
   h. 必要に応じて、トラフィック分類ポリシーを使用して、ロード バランサ サービスによって処理されるトラフィックのより詳細な分析を表示します。
2. これらの要求がストレージ ノードに均等に分散されていることを確認します。
   a. ***Storage Node*** > **LDR** > **HTTP** を選択します。
   b. *現在確立されている着信セッション*の数を確認します。
   c. グリッド内の各ストレージ ノードに対して繰り返します。

      セッション数は、すべてのストレージ ノード間でほぼ等しくなる必要があります。

グリッドフェデレーション接続を監視する

すべての基本情報を監視できます"グリッドフェデレーション接続"、特定の接続に関する詳細情報、またはクロスグリッドレプリケーション操作に関する Prometheus メトリック。どちらのグリッドからでも接続を監視できます。

開始する前に

- いずれかのグリッドのグリッドマネージャにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは"ルートアクセス権限"サインインしているグリッドの。

すべての接続を表示

グリッド フェデレーション ページには、すべてのグリッド フェデレーション接続と、グリッド フェデレーション接続の使用が許可されているすべてのテナント アカウントに関する基本情報が表示されます。

手順

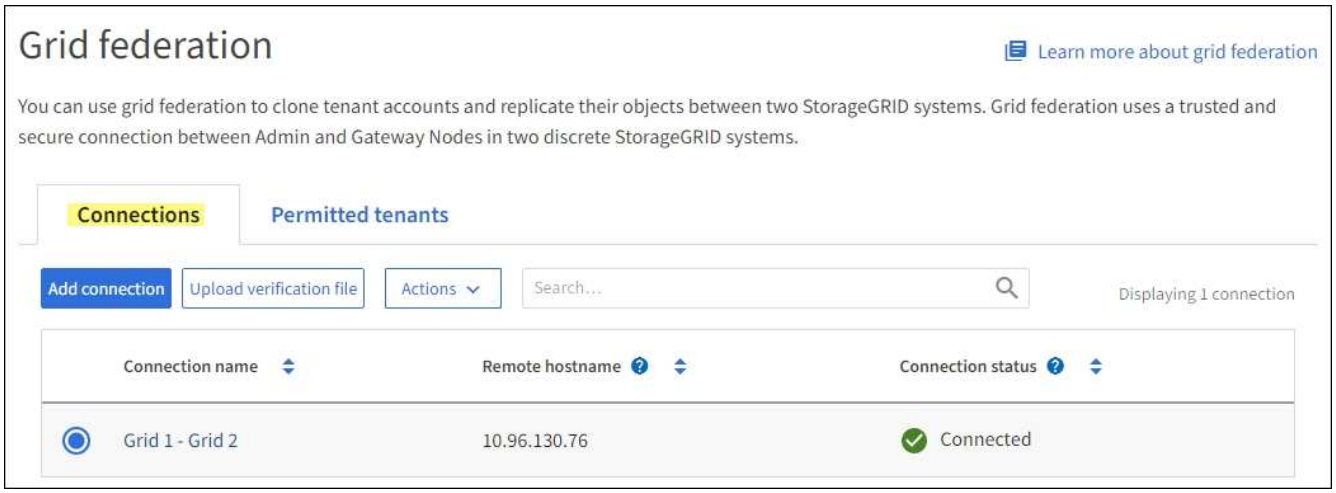
1. 構成 > システム > グリッド フェデレーション を選択します。

   グリッド フェデレーション ページが表示されます。

2. このグリッド上のすべての接続の基本情報を表示するには、[接続] タブを選択します。

   このタブから、次の操作を実行できます。

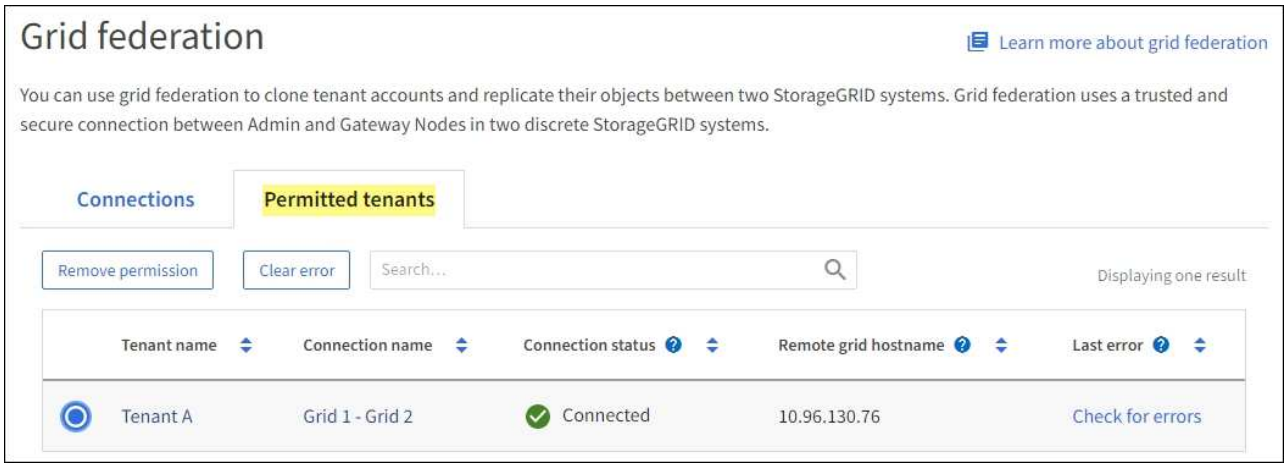
   - "新しい接続を作成する" 。
   - 既存の接続を選択して"編集またはテスト"。



3. このグリッド上で グリッド フェデレーション接続の使用 権限を持つすべてのテナント アカウントの基本情報を表示するには、許可されたテナント タブを選択します。

   このタブから、次の操作を実行できます。

   - "許可された各テナントの詳細ページを表示する" 。
   - 各接続の詳細ページを表示します。見る特定の接続を表示する 。
   - 許可されたテナントを選択し、"権限を削除する" 。
   - グリッド間のレプリケーション エラーを確認し、最後のエラーがあればクリアします。見る"グリッド フェデレーションエラーのトラブルシューティング" 。



特定の接続を表示する

特定のグリッド フェデレーション接続の詳細を表示できます。

手順

1. グリッド フェデレーション ページからいずれかのタブを選択し、テーブルから接続名を選択します。

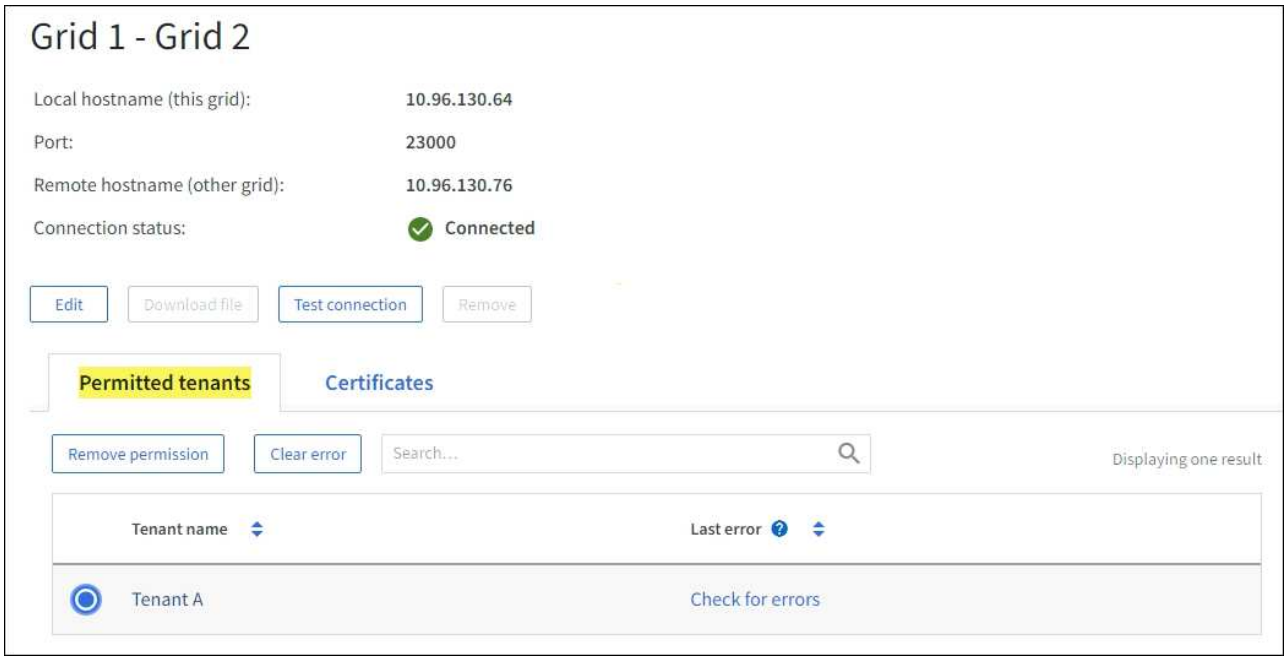
   接続の詳細ページから、次の操作を実行できます。

   - ローカルおよびリモートのホスト名、ポート、接続ステータスなど、接続に関する基本的なステータス情報を表示します。
   - 接続を選択して"編集、テスト、削除"。

2. 特定の接続を表示する場合は、[許可されたテナント] タブを選択して、その接続に許可されたテナントの詳細を表示します。

   このタブから、次の操作を実行できます。

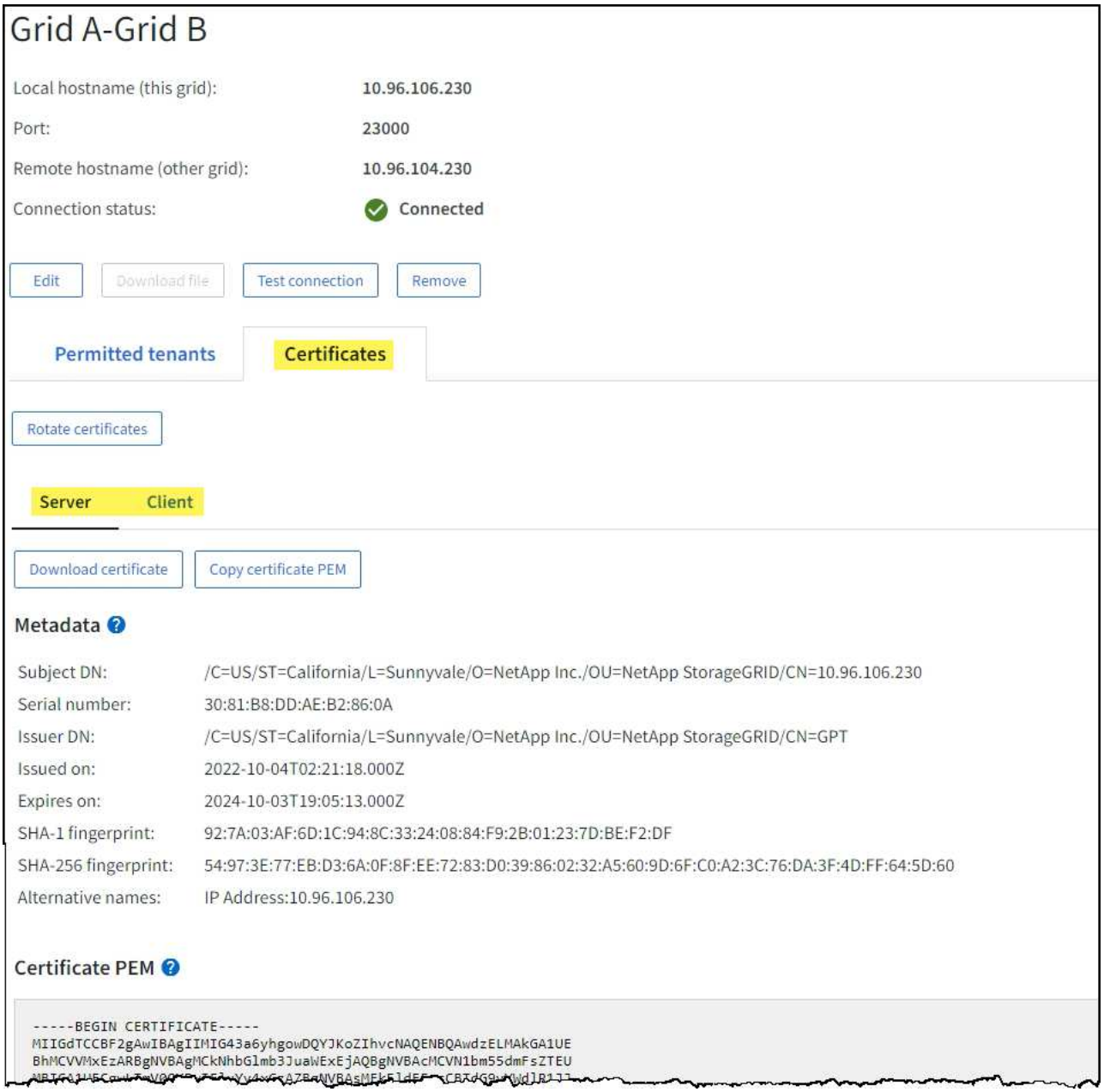
   - "許可された各テナントの詳細ページを表示する" 。
   - "テナントの権限を削除する"接続を使用します。
   - グリッド間のレプリケーション エラーを確認し、最後のエラーをクリアします。見る"グリッドフェデレーションエラーのトラブルシューティング" 。



3. 特定の接続を表示する場合は、[証明書] タブを選択して、この接続のシステム生成サーバー証明書とクライアント証明書を表示します。

   このタブから、次の操作を実行できます。

   - "接続証明書をローテーションする" 。
   - 関連する証明書を表示またはダウンロードするか、証明書 PEM をコピーするには、「サーバー」または「クライアント」を選択します。



クロスグリッドレプリケーションメトリックを確認する

Grafana のクロスグリッド レプリケーション ダッシュボードを使用して、グリッド上のクロスグリッド レプリケーション操作に関する Prometheus メトリックを表示できます。

手順

1. グリッド マネージャーから、サポート > ツール > メトリック を選択します。

> メトリクス ページで利用できるツールは、テクニカル サポートが使用することを目的としています。これらのツール内の一部の機能とメニュー項目は意図的に機能せず、変更される可能性があります。リストを見る"よく使われるPrometheusメトリクス"。

2. ページの Grafana セクションで、**Cross Grid Replication** を選択します。

詳しい手順については、"サポート指標を確認する" 。

3. 複製に失敗したオブジェクトの複製を再試行するには、"失敗したレプリケーション操作を識別して再試行する" 。

アラートを管理する

アラートを管理する

アラート システムは、 StorageGRID の操作中に発生する可能性のある問題を検出、評価、解決するための使いやすいインターフェイスを提供します。

アラート ルールの条件が true と評価されると、特定の重大度レベルでアラートがトリガーされます。アラートがトリガーされると、次のアクションが発生します。

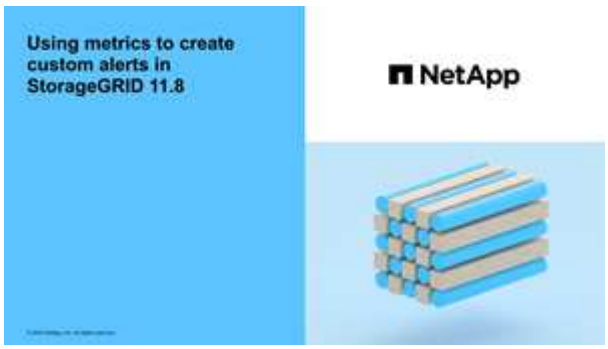
- グリッド マネージャーのダッシュボードにアラートの重大度アイコンが表示され、現在のアラートの数が増加します。
- アラートは、**NODES** 概要ページと **NODES** > ***node*** > 概要 タブに表示されます。
- SMTP サーバーを設定し、受信者の電子メール アドレスを指定している場合、電子メール通知が送信されます。
- StorageGRID SNMP エージェントが設定されていると、簡易ネットワーク管理プロトコル (SNMP) 通知が送信されます。

カスタム アラートを作成したり、アラートを編集または無効化したり、アラート通知を管理したりできます。

詳細については、以下をご覧ください。

- ビデオをレビューします: "ビデオ: アラートの概要"

- ビデオをレビューします: "ビデオ: カスタムアラート"



- 参照"アラート一覧"。

アラートルールを表示

アラートルールは、トリガーとなる条件を定義します。"特定のアラート" 。StorageGRID にはデフォルトのアラート ルールのセットが含まれており、そのまま使用することも、変更することも、カスタム アラート ルールを作成することもできます。

すべてのデフォルトおよびカスタムのアラート ルールのリストを表示して、各アラートをトリガーする条件を確認し、無効になっているアラートがあるかどうかを確認できます。

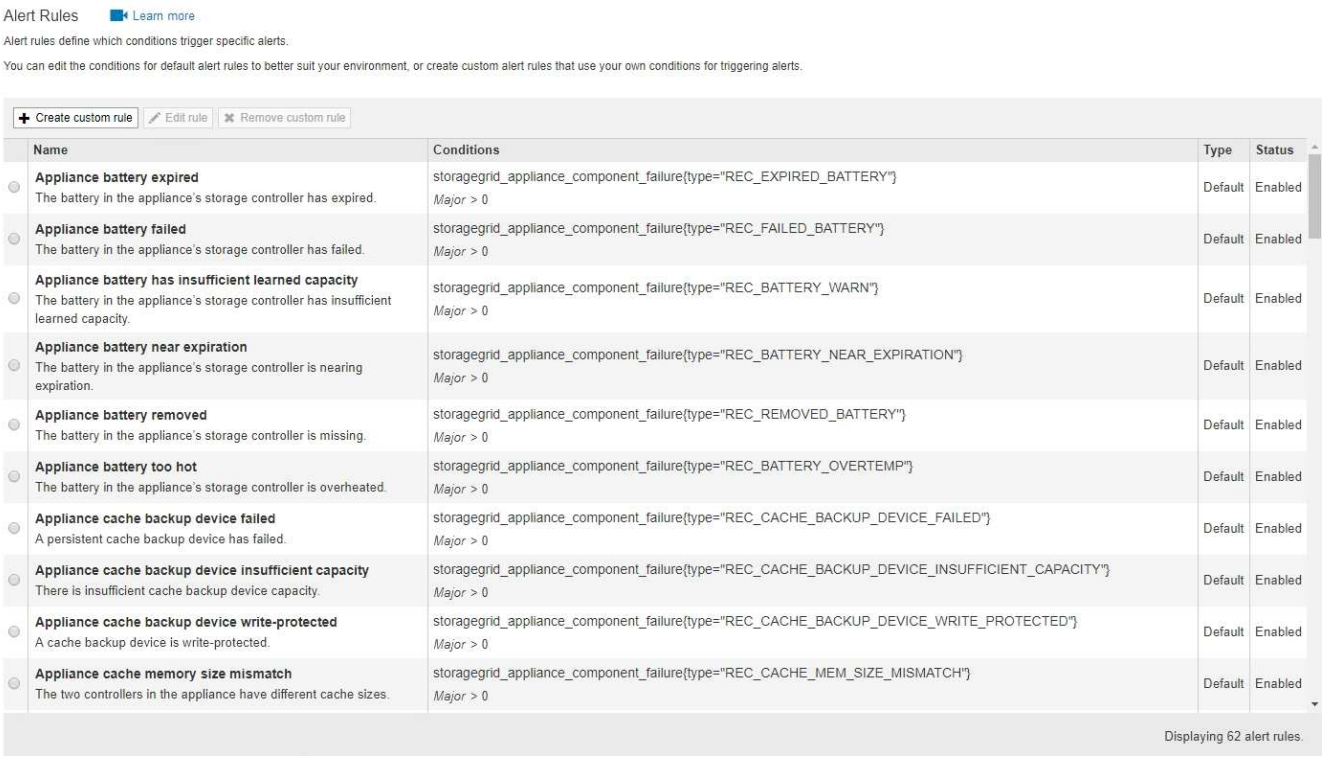
開始する前に

- グリッドマネージャにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは"アラートまたはルートアクセス権限を管理する"。
- オプションとして、ビデオを視聴しました: "ビデオ: アラートの概要"

手順

1. アラート > *ルール*を選択します。

   アラート ルール ページが表示されます。



2. アラート ルール テーブルの情報を確認します。

列ヘッダー	説明
Name	アラート ルールの一意の名前と説明。最初にカスタム アラート ルールがリストされ、その後にデフォルトのアラート ルールがリストされます。アラート ルール名は電子メール通知の件名になります。
条件	このアラートがいつトリガーされるかを決定する Prometheus 式。アラートは、次の 1 つ以上の重大度レベルでトリガーできますが、各重大度に対する条件は必要ありません。 • *致命的* : StorageGRIDノードまたはサービスの通常の操作を停止させる異常な状態が発生しています。根本的な問題に直ちに対処する必要があります。問題が解決されない場合、サービスが中断され、データが失われる可能性があります。 • *選考科目* : 現在の操作に影響を及ぼしているか、重大なアラートのしきい値に近づいている異常な状態が存在します。異常な状態によってStorageGRIDノードまたはサービスの通常の動作が停止しないように、主要なアラートを調査して根本的な問題に対処する必要があります。 • *マイナー* : システムは正常に動作していますが、継続するとシステムの動作能力に影響を及ぼす可能性のある異常な状態が存在します。より深刻な問題を引き起こさないように、自然に消えない軽微なアラートを監視して解決する必要があります。

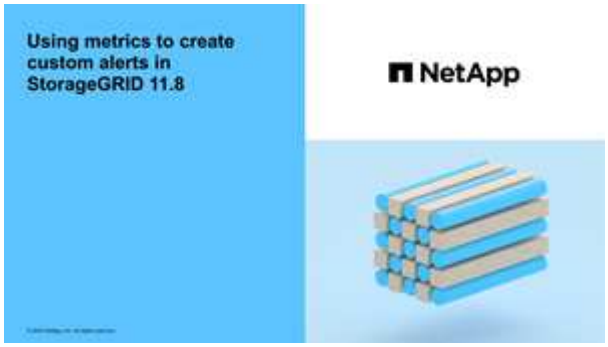
列ヘッダー	説明
タイプ	アラート ルールの種類: • デフォルト: システムに付属するアラート ルール。デフォルトのアラート ルールを無効にしたり、デフォルトのアラート ルールの条件と期間を編集したりできます。デフォルトのアラート ルールを削除することはできません。 • デフォルト*: 編集された条件または期間を含むデフォルトのアラート ルール。必要に応じて、変更した条件を元のデフォルトに簡単に戻すことができます。 • カスタム: 作成したアラート ルール。カスタムアラートルールを無効化、編集、削除できます。
ステータス	このアラート ルールが現在有効か無効かを示します。無効なアラート ルールの条件は評価されないため、アラートはトリガーされません。

カスタムアラートルールを作成する

カスタムアラートルールを作成して、アラートをトリガーするための独自の条件を定義できます。

開始する前に

- グリッドマネージャにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは"アラートまたはルートアクセス権限を管理する"。
- あなたは"よく使われるPrometheusメトリクス"。
- あなたは理解している "Prometheusクエリの構文"。
- オプションとして、ビデオを視聴しました: "ビデオ: カスタムアラート" 。



タスク概要

StorageGRID はカスタムアラートを検証しません。カスタムアラートルールを作成する場合は、次の一般的なガイドラインに従ってください。

- デフォルトのアラート ルールの条件を確認し、それをカスタム アラート ルールの例として使用します。
- アラート ルールに複数の条件を定義する場合は、すべての条件に同じ式を使用します。次に、各条件のし

きい値を変更します。

- 各条件にタイプミスや論理エラーがないか注意深く確認してください。
- グリッド管理 API にリストされているメトリックのみを使用します。
- Grid Management API を使用して式をテストする場合、「成功」応答が空の応答本文 (アラートがトリガーされない) になる可能性があることに注意してください。アラートが実際にトリガーされるかどうかを確認するには、現時点で当てはまると予想される値にしきい値を一時的に設定できます。

  例えば、次の式をテストするには `node_memory_MemTotal_bytes < 24000000000`、まず実行 `node_memory_MemTotal_bytes >= 0`期待どおりの結果が得られたことを確認します (すべてのノードが値を返します)。次に、演算子としきい値を意図した値に戻して再度実行します。結果がない場合は、この表現に現在アラートがないことを示します。

- アラートが予期したとおりにトリガーされることを検証しない限り、カスタム アラートが機能していると想定しないでください。

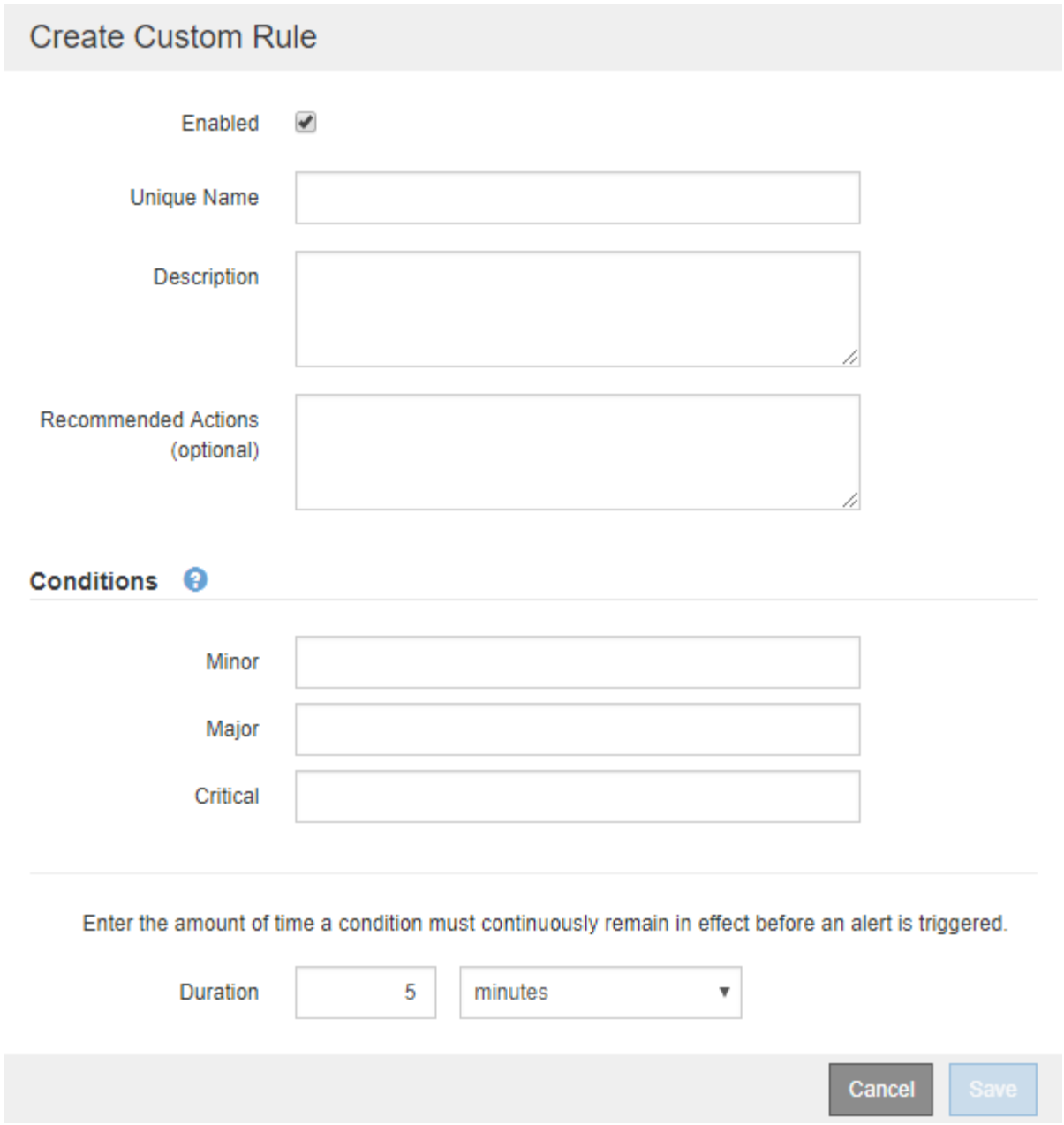
手順

1. アラート > *ルール*を選択します。

   アラート ルール ページが表示されます。

2. *カスタムルールの作成*を選択します。

   [カスタム ルールの作成] ダイアログ ボックスが表示されます。



3. このアラート ルールが現在有効になっているかどうかを確認するには、[有効] チェックボックスをオンにするかオフにします。

   アラート ルールが無効になっている場合、その式は評価されず、アラートはトリガーされません。

4. 次の情報を入力してください。

フィールド	説明
一意の名前	このルールの一意の名前。アラート ルール名は [アラート] ページに表示され、電子メール通知の件名にもなります。アラート ルールの名前は 1 ～ 64 文字まで使用できます。

フィールド	説明
説明	発生している問題の説明。説明は、アラート ページおよび電子メール通知に表示されるアラート メッセージです。アラート ルールの説明は 1 ～ 128 文字まで入力できます。
推奨される対処方法	オプションで、このアラートがトリガーされたときに実行する推奨アクション。推奨アクションをプレーンテキスト（書式コードなし）として入力します。アラート ルールの推奨アクションは、0 ～ 1,024 文字まで指定できます。

5. 条件セクションで、1 つ以上のアラート重大度レベルに対して Prometheus 式を入力します。

   基本的な表現は通常、次の形式になります。

   ```
   [metric] [operator] [value]
   ```

   式の長さは任意ですが、ユーザー インターフェイスでは 1 行に表示されます。少なくとも 1 つの式が必要です。

   この式により、ノードにインストールされている RAM の量が 24,000,000,000 バイト (24 GB) 未満の場合にアラートがトリガーされます。

   ```
   node_memory_MemTotal_bytes < 24000000000
   ```

   利用可能なメトリクスを確認し、Prometheus式をテストするには、ヘルプアイコンを選択してください。グリッド管理 API のメトリック セクションへのリンクをたどります。

6. 期間 フィールドに、アラートがトリガーされるまでに条件が継続的に有効である必要がある時間を入力し、時間の単位を選択します。

   条件が真になったときにすぐにアラートをトリガーするには、「**0**」と入力します。一時的な状況によってアラートがトリガーされるのを防ぐには、この値を増やします。

   デフォルトは5分です。

7. *保存*を選択します。

   ダイアログ ボックスが閉じ、新しいカスタム アラート ルールが [アラート ルール] テーブルに表示されます。

アラートルールを編集する

アラート ルールを編集してトリガー条件を変更できます。カスタム アラート ルールの場合は、ルール名、説明、推奨アクションを更新することもできます。

開始する前に

- グリッドマネージャにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは"アラートまたはルートアクセス権限を管理する"。

タスク概要

デフォルトのアラート ルールを編集するときに、マイナー、メジャー、クリティカル アラートの条件と期間を変更できます。カスタムアラートルールを編集するときに、ルールの名前、説明、推奨アクションも編集できます。

> アラート ルールを編集する場合は注意してください。トリガー値を変更すると、重要な操作が完了できなくなるまで、根本的な問題を検出できない可能性があります。

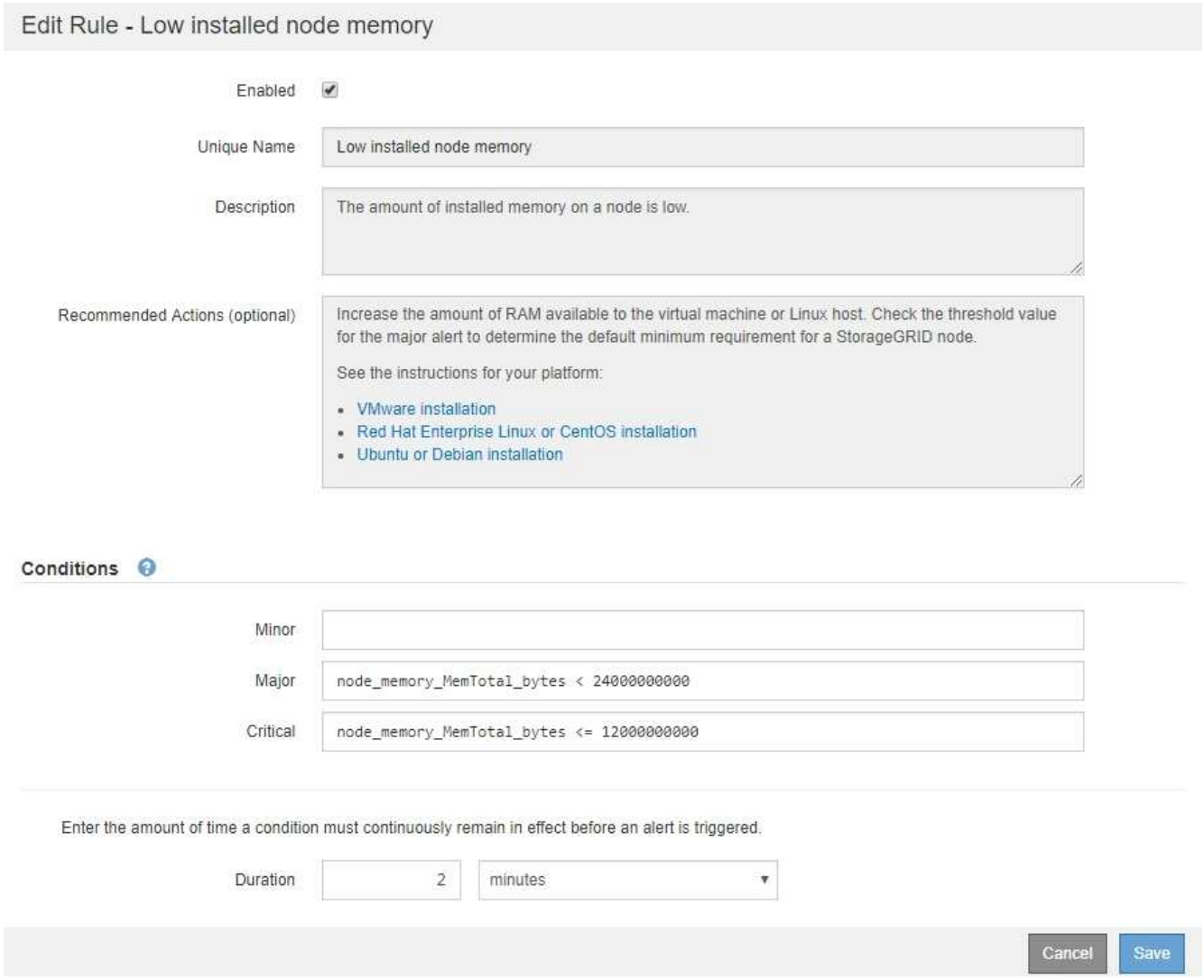
手順

1. アラート > *ルール*を選択します。

   アラート ルール ページが表示されます。

2. 編集するアラート ルールのラジオ ボタンを選択します。
3. *ルールの編集*を選択します。

   [ルールの編集] ダイアログ ボックスが表示されます。この例では、デフォルトのアラート ルールを示しています。一意の名前、説明、推奨アクションのフィールドは無効になっており、編集できません。



4. このアラート ルールが現在有効になっているかどうかを確認するには、[有効] チェックボックスをオンに

するかオフにします。

アラート ルールが無効になっている場合、その式は評価されず、アラートはトリガーされません。

現在のアラートのアラート ルールを無効にする場合は、アラートがアクティブなアラートとして表示されなくなるまで数分間待つ必要があります。

一般に、デフォルトのアラート ルールを無効にすることはお勧めしません。アラート ルールが無効になっている場合、重要な操作が完了できなくなるまで、根本的な問題を検出できない可能性があります。

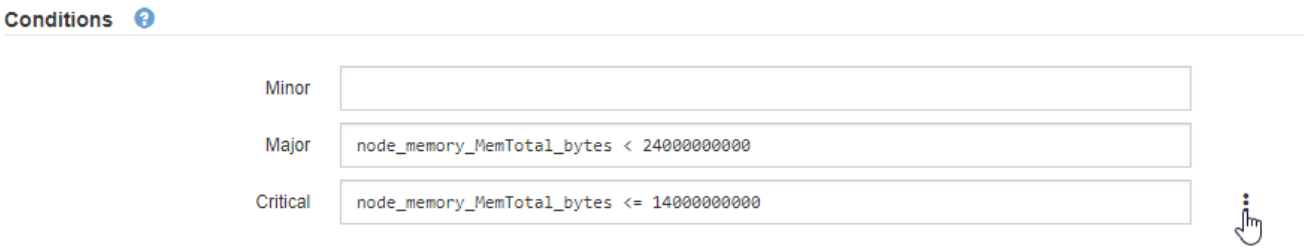
5. カスタムアラートルールの場合は、必要に応じて次の情報を更新します。

デフォルトのアラート ルールのこの情報を編集することはできません。

フィールド	説明
一意の名前	このルールの一意の名前。アラート ルール名は [アラート] ページに表示され、電子メール通知の件名にもなります。アラート ルールの名前は 1 ～ 64 文字まで使用できます。
説明	発生している問題の説明。説明は、アラート ページおよび電子メール通知に表示されるアラート メッセージです。アラート ルールの説明は 1 ～ 128 文字まで入力できます。
推奨される対処方法	オプションで、このアラートがトリガーされたときに実行する推奨アクション。推奨アクションをプレーンテキスト（書式コードなし）として入力します。アラート ルールの推奨アクションは、0 ～ 1,024 文字まで指定できます。

6. 「条件」セクションで、1 つ以上のアラート重大度レベルの Prometheus 式を入力または更新します。

編集したデフォルトのアラート ルールの条件を元の値に戻す場合は、変更した条件の右側にある 3 つのドットを選択します。



現在のアラートの条件を更新した場合、以前の条件が解決されるまで変更が実装されない可能性があります。次にルールの条件の 1 つが満たされると、アラートには更新された値が反映されます。

基本的な表現は通常、次の形式になります。

```
[metric] [operator] [value]
```

式の長さは任意ですが、ユーザー インターフェイスでは 1 行に表示されます。少なくとも 1 つの式が必要です。

この式により、ノードにインストールされている RAM の量が 24,000,000,000 バイト (24 GB) 未満の場合にアラートがトリガーされます。

```
node_memory_MemTotal_bytes < 24000000000
```

7. 期間 フィールドに、アラートがトリガーされるまでに条件が継続的に有効である必要がある時間を入力し、時間の単位を選択します。

   条件が真になったときにすぐにアラートをトリガーするには、「**0**」と入力します。一時的な状況によってアラートがトリガーされるのを防ぐには、この値を増やします。

   デフォルトは5分です。

8. *保存*を選択します。

   デフォルトのアラート ルールを編集した場合、[タイプ] 列に デフォルト* が表示されます。デフォルトまたはカスタムのアラート ルールを無効にした場合、[ステータス] 列に [無効] と表示されます。

アラートルールを無効にする

デフォルトまたはカスタムのアラート ルールの有効/無効状態を変更できます。

開始する前に

- グリッドマネージャにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは"アラートまたはルートアクセス権限を管理する"。

タスク概要

アラート ルールが無効になっている場合、その式は評価されず、アラートはトリガーされません。

> 一般に、デフォルトのアラート ルールを無効にすることはお勧めしません。アラート ルールが無効になっている場合、重要な操作が完了できなくなるまで、根本的な問題を検出できない可能性があります。

手順

1. アラート > *ルール*を選択します。

   アラート ルール ページが表示されます。

2. 無効または有効にするアラート ルールのラジオ ボタンを選択します。
3. *ルールの編集*を選択します。

   [ルールの編集] ダイアログ ボックスが表示されます。

4. このアラート ルールが現在有効になっているかどうかを確認するには、[有効] チェックボックスをオンに

するかオフにします。

アラート ルールが無効になっている場合、その式は評価されず、アラートはトリガーされません。

> 現在のアラートのアラート ルールを無効にする場合は、アラートがアクティブなアラートとして表示されなくなるまで数分間待つ必要があります。

5. *保存*を選択します。

   *ステータス*列に*無効*が表示されます。

カスタムアラートルールを削除する

カスタムアラートルールを使用しなくなった場合は削除できます。

開始する前に

- グリッドマネージャにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは"アラートまたはルートアクセス権限を管理する"。

手順

1. アラート > *ルール*を選択します。

   アラート ルール ページが表示されます。

2. 削除するカスタム アラート ルールのラジオ ボタンを選択します。

   デフォルトのアラート ルールを削除することはできません。

3. *カスタムルールの削除*を選択します。

   確認ダイアログボックスが表示されます。

4. アラート ルールを削除するには、[**OK**] を選択します。

   アラートのアクティブなインスタンスは 10 分以内に解決されます。

アラート通知を管理する

アラート用の**SNMP**通知を設定する

アラートが発生したときにStorageGRID がSNMP 通知を送信するようにするには、StorageGRID SNMP エージェントを有効にし、1 つ以上のトラップ送信先を設定する必要があります。

グリッド マネージャの **CONFIGURATION** > **Monitoring** > **SNMP agent** オプションまたはグリッド管理 API の SNMP エンドポイントを使用して、 StorageGRID SNMP エージェントを有効にして構成できます。SNMP エージェントは、SNMP プロトコルの 3 つのバージョンすべてをサポートします。

SNMPエージェントの設定方法については、"SNMP監視を使用する" 。

StorageGRID SNMP エージェントを構成すると、次の 2 種類のイベント駆動型通知を送信できるようになります。

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

デフォルトまたはカスタムアラートが任意の重大度レベルでトリガーされると、トラップ通知とインフォーム通知が送信されます。アラートの SNMP 通知を抑制するには、アラートのサイレンスを設定する必要があります。見る"サイレントアラート通知" 。

StorageGRID の展開に複数の管理ノードが含まれている場合、プライマリ管理ノードがアラート通知、AutoSupportパッケージ、SNMP トラップおよびインフォームの優先送信元になります。プライマリ管理ノードが利用できなくなった場合、通知は他の管理ノードによって一時的に送信されます。見る"管理ノードとは何ですか?" 。

アラートのメール通知を設定する

アラートが発生したときに電子メール通知を送信する場合は、SMTP サーバーに関する情報を提供する必要があります。アラート通知の受信者の電子メール アドレスも入力する必要があります。

開始する前に

- グリッドマネージャにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは"アラートまたはルートアクセス権限を管理する"。

タスク概要

アラート通知に使用される電子メール設定は、 AutoSupportパッケージでは使用されません。ただし、すべての通知に同じ電子メール サーバーを使用することができます。

StorageGRID の展開に複数の管理ノードが含まれている場合、プライマリ管理ノードがアラート通知、AutoSupportパッケージ、SNMP トラップおよびインフォームの優先送信元になります。プライマリ管理ノードが利用できなくなった場合、通知は他の管理ノードによって一時的に送信されます。見る"管理ノードとは何ですか?" 。

手順

1. アラート > *電子メール設定*を選択します。

   電子メール設定ページが表示されます。

2. アラートが設定されたしきい値に達したときに通知メールを送信するように指定するには、[電子メール通知を有効にする] チェックボックスをオンにします。

   電子メール (SMTP) サーバー、トランスポート層セキュリティ (TLS)、電子メール アドレス、およびフィルターのセクションが表示されます。

3. [電子メール (SMTP) サーバー] セクションで、 StorageGRID がSMTP サーバーにアクセスするために必要な情報を入力します。

   SMTP サーバーで認証が必要な場合は、ユーザー名とパスワードの両方を入力する必要があります。

フィールド	入力
メール サーバ	SMTPサーバの完全修飾ドメイン名（FQDN）またはIPアドレス。
ポート	SMTP サーバーにアクセスするために使用されるポート。 1 ～ 65535 の範囲で指定する必要があります。
ユーザー名（オプション）	SMTP サーバーで認証が必要な場合は、認証に使用するユーザー名を入力します。
パスワード（オプション）	SMTP サーバーで認証が必要な場合は、認証に使用するパスワードを入力します。

4. [電子メール アドレス] セクションで、送信者と各受信者の電子メール アドレスを入力します。

   a. 送信者メール アドレス には、アラート通知の送信元アドレスとして使用する有効なメール アドレスを指定します。

      例： `storagegrid-alerts@example.com`

   b. [受信者] セクションで、アラートが発生したときに電子メールを受信する必要がある各電子メール リストまたはユーザーの電子メール アドレスを入力します。

      プラスアイコンを選択➕受信者を追加します。

5. SMTP サーバーとの通信にトランスポート層セキュリティ (TLS) が必要な場合は、トランスポート層セキュリティ (TLS) セクションで **TLS** が必要 を選択します。

   a. **CA** 証明書 フィールドに、SMTP サーバーの ID を確認するために使用される CA 証明書を入力します。

      このフィールドに内容をコピーして貼り付けるか、「参照」を選択してファイルを選択することもできます。

      各中間発行証明機関 (CA) からの証明書が含まれる単一のファイルを提供する必要があります。このファイルには、PEM でエンコードされた各 CA 証明書ファイルが、証明書チェーンの順序で連結されて含まれている必要があります。

   b. SMTP 電子メール サーバーで電子メールの送信者に認証用のクライアント証明書の提供を要求する場合は、[クライアント証明書の送信] チェックボックスをオンにします。

   c. クライアント証明書 フィールドに、SMTP サーバーに送信する PEM エンコードされたクライアント証明書を入力します。

      このフィールドに内容をコピーして貼り付けるか、「参照」を選択してファイルを選択することもできます。

d. 秘密鍵 フィールドに、暗号化されていない PEM エンコードでクライアント証明書の秘密鍵を入力します。

このフィールドに内容をコピーして貼り付けるか、「参照」を選択してファイルを選択することもできます。

メール設定を編集する必要がある場合は、鉛筆アイコンを選択してください このフィールドを更新します。

6. [フィルター] セクションで、特定のアラートのルールが無効にされていない限り、電子メール通知を生成するアラート重大度レベルを選択します。

重大度	説明
軽微、重大、重大	アラート ルールのマイナー、メジャー、またはクリティカル条件が満たされると、電子メール通知が送信されます。
重大、重篤	アラート ルールの主要な条件または重大な条件が満たされると、電子メール通知が送信されます。軽微なアラートについては通知は送信されません。
クリティカルのみ	アラート ルールの重大な条件が満たされた場合にのみ、電子メール通知が送信されます。マイナーアラートまたはメジャーアラートの場合、通知は送信されません。

7. 電子メール設定をテストする準備ができたら、次の手順を実行します。

a. *テストメールを送信*を選択します。

テストメールが送信されたことを示す確認メッセージが表示されます。

b. すべてのメール受信者の受信トレイを確認し、テストメールが受信されたことを確認します。

数分以内にメールが届かない場合、または*メール通知失敗*アラートがトリガーされた場合は、設定を確認して再試行してください。

c. 他の管理ノードにSign in、テストメールを送信して、すべてのサイトからの接続を確認します。

アラート通知をテストするときは、すべての管理ノードにサインインして接続を確認する必要があります。これは、すべての管理ノードがテスト メールを送信するAutoSupportパッケージのテストとは対照的です。

8. *保存*を選択します。

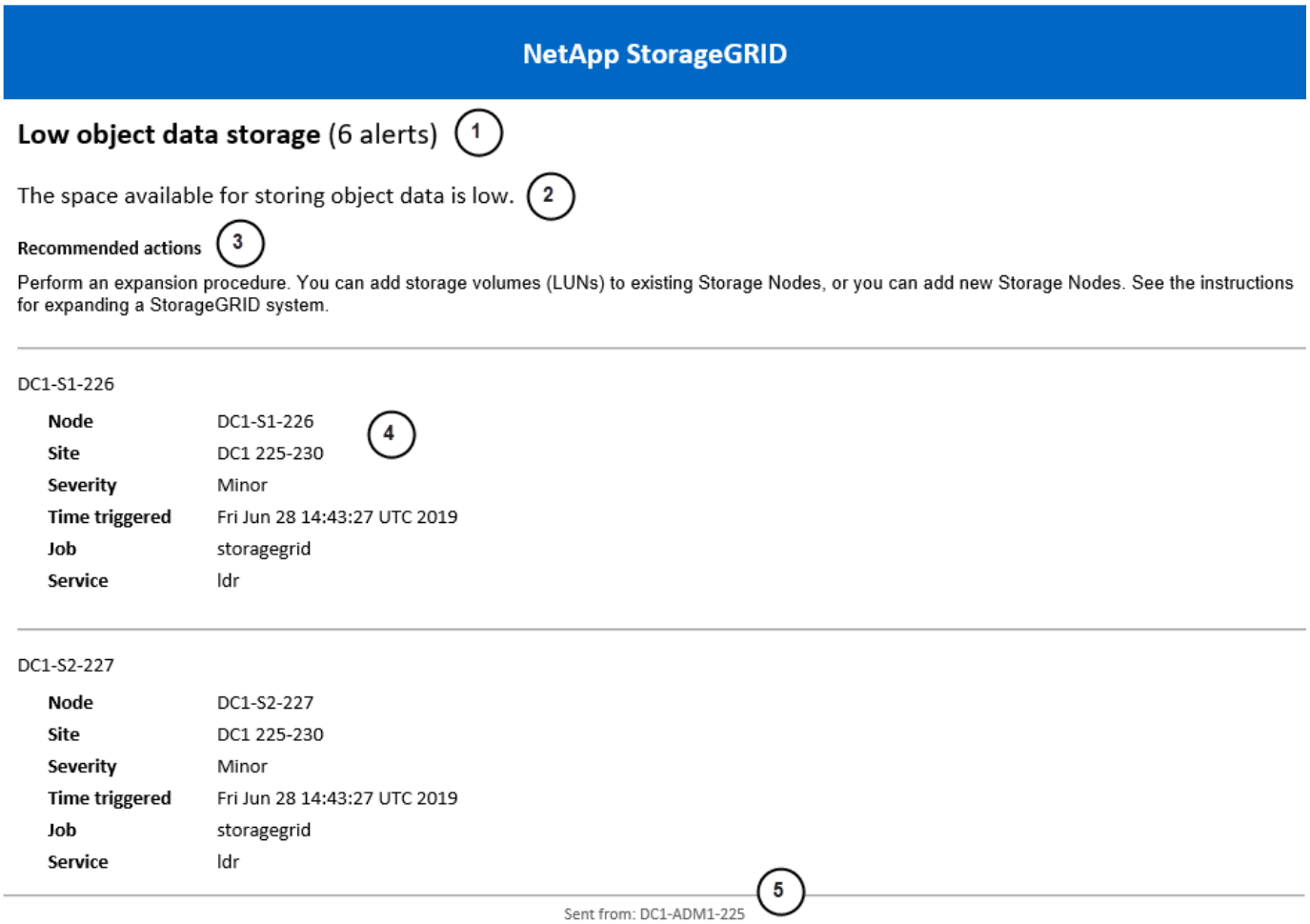
テストメールを送信しても設定は保存されません。 *保存*を選択する必要があります。

メール設定が保存されました。

アラートメール通知に含まれる情報

SMTP 電子メール サーバーを構成すると、アラート ルールがサイレンスによって抑制されていない限り、アラートがトリガーされたときに、指定された受信者に電子メール通知が送信されます。見る"サイレントアラート通知" 。

電子メール通知には次の情報が含まれます。



番号	説明
1	アラートの名前と、その後にこのアラートのアクティブなインスタンスの数が表示されます。
2	アラートの説明。
3	アラートに対する推奨アクション。
4	アラートの各アクティブ インスタンスに関する詳細 (影響を受けるノードとサイト、アラートの重大度、アラート ルールがトリガーされた UTC 時間、影響を受けるジョブとサービスの名前など)。
5	通知を送信した管理ノードのホスト名。

アラートのグループ化方法

アラートがトリガーされたときに過剰な数の電子メール通知が送信されるのを防ぐために、 StorageGRID は複数のアラートを同じ通知にグループ化しようとします。

StorageGRID が電子メール通知で複数のアラートをグループ化する方法の例については、次の表を参照してください。

動作	例
各アラート通知は、同じ名前を持つアラートにのみ適用されます。異なる名前の 2 つのアラートが同時にトリガーされた場合、 2 つの電子メール通知が送信されます。	• アラート A は 2 つのノードで同時にトリガーされます。通知は 1 つだけ送信されます。 • アラート A はノード 1 でトリガーされ、同時にアラート B はノード 2 でトリガーされます。アラートごとに 1 つずつ、合計 2 つの通知が送信されます。
特定のノード上の特定のアラートについては、複数の重大度のしきい値に達した場合、最も重大度の高いアラートに対してのみ通知が送信されます。	• アラート A がトリガーされ、マイナー、メジャー、およびクリティカルのアラートしきい値に達しました。重大なアラートに対して 1 つの通知が送信されます。
初めてアラートがトリガーされると、 StorageGRID は通知を送信する前に 2 分間待機します。その間に同じ名前の他のアラートがトリガーされた場合、 StorageGRID はすべてのアラートを初期通知にグループ化します。	1. アラート A は 08:00 にノード 1 でトリガーされます。通知は送信されません。 2. アラート A は 08:01 にノード 2 でトリガーされます。通知は送信されません。 3. 08:02 に、アラートの両方のインスタンスを報告する通知が送信されます。
同じ名前の別のアラートがトリガーされた場合、 StorageGRID は新しい通知を送信する前に 10 分間待機します。新しい通知では、以前に報告されたものも含め、すべてのアクティブなアラート (現在消音されていないアラート) が報告されます。	1. アラート A は 08:00 にノード 1 でトリガーされます。 08:02に通知が送信されます。 2. アラート A は 08:05 にノード 2 でトリガーされます。 2 回目の通知は 08:15 (10 分後) に送信されます。両方のノードが報告されます。
現在、同じ名前のアラートが複数存在し、そのうちの 1 つが解決された場合、アラートが解決されたノードでアラートが再発しても、新しい通知は送信されません。	1. アラート A はノード 1 に対してトリガーされます。通知が送信されます。 2. アラート A はノード 2 に対してトリガーされます。 2 番目の通知が送信されます。 3. アラート A はノード 2 では解決されていますが、ノード 1 ではアクティブなままです。 4. アラート A がノード 2 に対して再度トリガーされます。ノード 1 のアラートはまだアクティブであるため、新しい通知は送信されません。

動作	例
StorageGRID は、アラートのすべてのインスタンスが解決されるか、アラート ルールが無効になるまで、7 日ごとに電子メール通知を送信し続けます。	1. アラート A は 3 月 8 日にノード 1 に対してトリガーされます。通知が送信されます。 2. アラート A は解決または消音されません。追加の通知は、3 月 15 日、3 月 22 日、3 月 29 日などに送信されます。

アラートメール通知のトラブルシューティング

*電子メール通知失敗*アラートがトリガーされた場合、またはテストアラート電子メール通知を受信できない場合は、次の手順に従って問題を解決してください。

開始する前に

- グリッドマネージャにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは"アラートまたはルートアクセス権限を管理する"。

手順

1. 設定を確認してください。
   a. アラート > *電子メール設定*を選択します。
   b. 電子メール (SMTP) サーバー設定が正しいことを確認します。
   c. 受信者に有効な電子メール アドレスを指定したことを確認します。
2. スパムフィルターをチェックして、メールが迷惑メールフォルダに送信されていないことを確認してください。
3. 送信者アドレスからのメールがブロックされていないことをメール管理者に確認してもらってください。
4. 管理ノードのログ ファイルを収集し、テクニカル サポートに問い合わせてください。

   テクニカル サポートでは、ログの情報を使用して、何が問題であったかを特定できます。たとえば、指定したサーバーに接続すると、prometheus.log ファイルにエラーが表示される場合があります。

   見る"ログファイルとシステムデータを収集する" 。

サイレントアラート通知

必要に応じて、アラート通知を一時的に抑制するサイレンスを構成することもできます。

開始する前に

- グリッドマネージャにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは"アラートまたはルートアクセス権限を管理する"。

タスク概要

グリッド全体、単一のサイト、または単一のノードで、1 つ以上の重大度に対してアラート ルールを無音にすることができます。各サイレンスは、単一のアラート ルールまたはすべてのアラート ルールのすべての通知を抑制します。

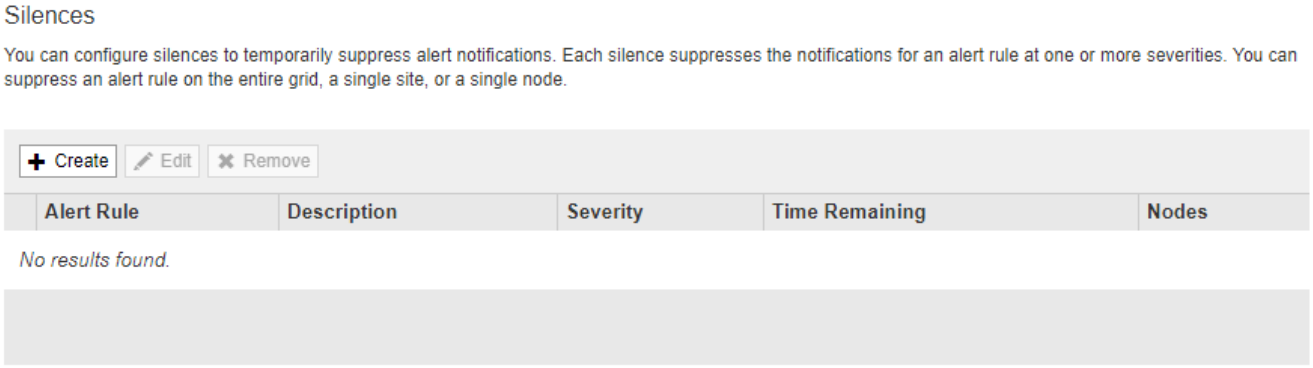
SNMP エージェントを有効にしている場合、サイレンスは SNMP トラップとインフォームも抑制します。

アラート ルールを無音にする場合は注意してください。アラートを無音にすると、重要な操作が完了できなくなるまで、根本的な問題を検出できない可能性があります。

手順

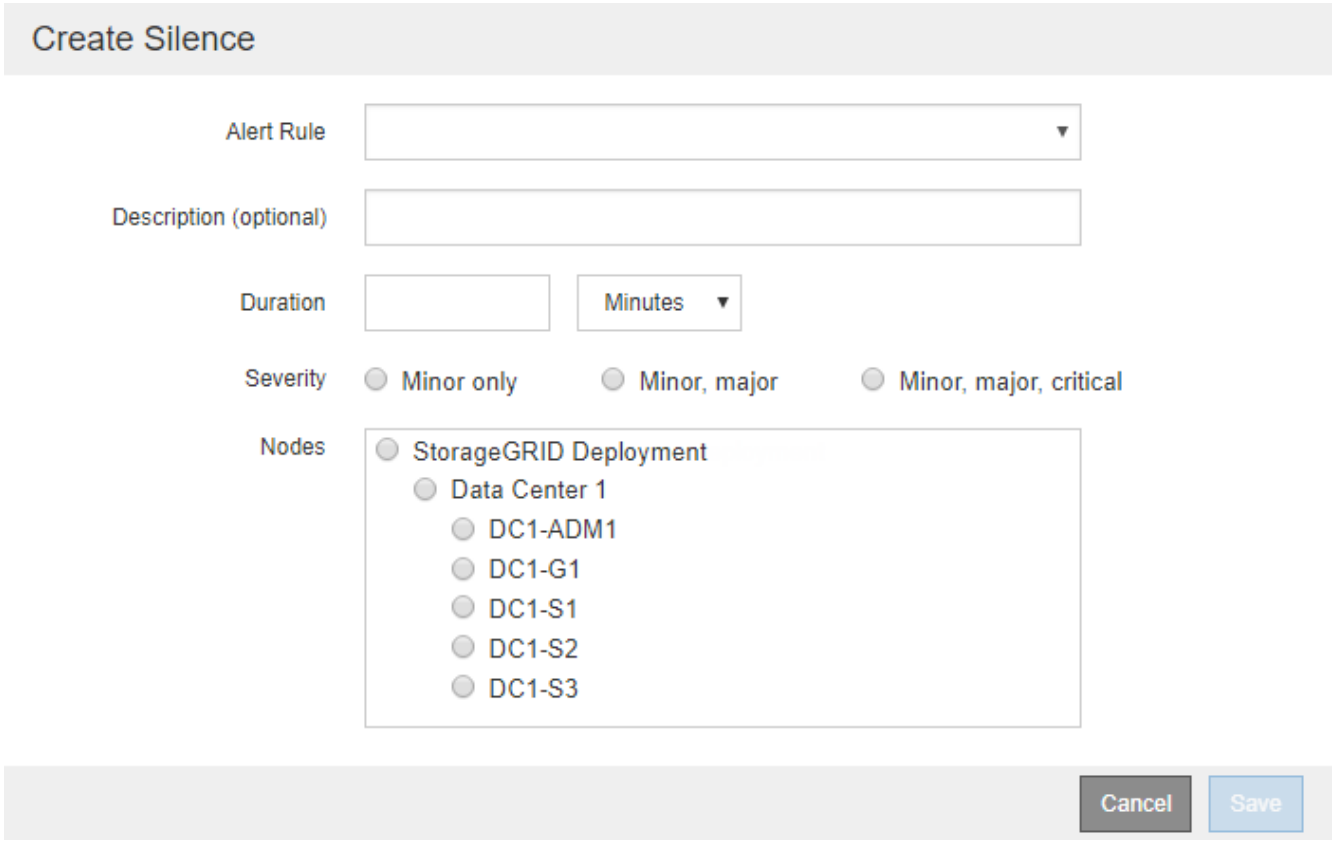
1. アラート > *サイレンス*を選択します。

   「サイレンス」ページが表示されます。



2. *作成*を選択します。

   「無音の作成」ダイアログ ボックスが表示されます。



3. 次の情報を選択または入力します。

フィールド	説明
アラートルール	サイレントにするアラート ルールの名前。アラート ルールが無効になっている場合でも、デフォルトまたはカスタムのアラート ルールを選択できます。 注: このダイアログ ボックスで指定された条件を使用してすべてのアラート ルールを無音にする場合は、[すべてのルール] を選択します。
説明	オプションで、沈黙の説明。たとえば、この沈黙の目的を説明してください。
間隔	この沈黙を有効にする期間（分、時間、または日数）を指定します。沈黙は 5 分から 1,825 日 (5 年) まで有効になります。 注意: アラート ルールを長時間にわたって無音にしないでください。アラート ルールが無効になっている場合、重要な操作の完了が妨げられるまで、根本的な問題を検出できない可能性があります。ただし、サービス アプライアンス リンク ダウン アラートや ストレージ アプライアンス リンク ダウン アラートの場合のように、特定の意図的な構成によってアラートがトリガーされる場合は、拡張サイレンスを使用する必要があることがあります。
重大度	どのアラート重大度をサイレントにするか。選択した重大度のいずれかでアラートがトリガーされた場合、通知は送信されません。
ノード	この無音を適用するノード。グリッド全体、単一のサイト、または単一のノード上のアラート ルールまたはすべてのルールを抑制できます。グリッド全体を選択すると、すべてのサイトとすべてのノードに無音が適用されます。サイトを選択した場合、サイレンスはそのサイトのノードにのみ適用されます。 注意: 各サイレンスに対して複数のノードまたは複数のサイトを選択することはできません。一度に複数のノードまたは複数のサイトで同じアラート ルールを抑制する場合は、追加のサイレンスを作成する必要があります。

4. *保存*を選択します。
5. 有効期限が切れる前にサイレンスを変更または終了したい場合は、編集または削除できます。

オプション	説明
無音部分を編集する	a. アラート > *サイレンス*を選択します。 b. 表から、編集する無音部分のラジオ ボタンを選択します。 c. *編集*を選択します。 d. 説明、残り時間、選択した重大度、または影響を受けるノードを変更します。 e. *保存*を選択します。

オプション	説明
無音部分を削除する	a. アラート > *サイレンス*を選択します。 b. 表から、削除する無音部分のラジオ ボタンを選択します。 c. *削除*を選択します。 d. この無音部分を削除することを確認するには、[**OK**] を選択します。 注: このアラートがトリガーされると、通知が送信されるようになりました (別のサイレンスによって抑制されない限り)。このアラートが現在トリガーされている場合、電子メールまたは SNMP 通知が送信され、アラート ページが更新されるまでに数分かかることがあります。

関連情報

"SNMPエージェントを構成する"

アラート一覧

このリファレンスには、グリッド マネージャーに表示されるデフォルトのアラートの一覧を示します。推奨されるアクションは、受信した警告メッセージに記載されています。

必要に応じて、システム管理アプローチに適合するカスタムアラート ルールを作成できます。

デフォルトのアラートの一部は"Prometheusメトリクス"。

アプライアンスアラート

アラート名	説明
家電製品の電池切れ	アプライアンスのストレージ コントローラのバッテリーの有効期限が切れました。
家電製品のバッテリーが故障しました	アプライアンスのストレージ コントローラのバッテリーが故障しました。
家電製品のバッテリーの学習容量が不十分です	アプライアンスのストレージ コントローラのバッテリーの学習容量が不十分です。
家電製品のバッテリーの有効期限が近づいています	アプライアンスのストレージ コントローラのバッテリーの有効期限が近づいています。
家電製品のバッテリーを取り外しました	アプライアンスのストレージ コントローラのバッテリーがありません。
家電製品のバッテリーが熱すぎる	アプライアンスのストレージ コントローラ内のバッテリーが過熱しています。

アラート名	説明
アプライアンスBMC通信エラー	ベースボード管理コントローラ (BMC) との通信が失われました。
アプライアンスのブートデバイスの障害が検出されました	アプライアンスのブート デバイスに問題が検出されました。
アプライアンス キャッシュ バックアップ デバイスに障害が発生しました	永続キャッシュ バックアップ デバイスに障害が発生しました。
アプライアンスのキャッシュバックアップデバイスの容量が不足しています	キャッシュバックアップデバイスの容量が不足しています。
アプライアンスのキャッシュバックアップデバイスが書き込み保護されています	キャッシュ バックアップ デバイスは書き込み保護されています。
アプライアンスのキャッシュメモリサイズの不一致	アプライアンス内の 2 つのコントローラのキャッシュ サイズが異なります。
アプライアンスのCMOSバッテリー障害	アプライアンスの CMOS バッテリーに問題が検出されました。
アプライアンスのコンピューティング コントローラ シャーシの温度が高すぎます	StorageGRIDアプライアンスのコンピューティング コントローラの温度が公称しきい値を超えました。
アプライアンスのコンピューティング コントローラの CPU 温度が高すぎます	StorageGRIDアプライアンスのコンピューティング コントローラの CPU の温度が公称しきい値を超えました。
アプライアンスのコンピューティング コントローラに注意が必要です	StorageGRIDアプライアンスのコンピューティング コントローラでハードウェア障害が検出されました。
アプライアンスのコンピューティング コントローラの電源 A に問題があります	コンピューティング コントローラーの電源 A に問題があります。
アプライアンスのコンピューティング コントローラの電源 B に問題があります	コンピューティング コントローラーの電源 B に問題があります。

アラート名	説明
アプライアンスのコンピューティング ハードウェア モニター サービスが停止しました	ストレージ ハードウェアの状態を監視するサービスが停止しました。
アプライアンス DAS ドライブが 1 日あたりの書き込みデータ制限を超えています	毎日過剰な量のデータがドライブに書き込まれているため、保証が無効になる可能性があります。
アプライアンスDASドライブ障害が検出されました	アプライアンス内の直接接続ストレージ (DAS) ドライブに問題が検出されました。
アプライアンスDASドライブロケータライトが点灯	アプライアンス ストレージ ノード内の 1 つ以上の直接接続ストレージ (DAS) ドライブのドライブ ロケータ ライトがオンになっています。
アプライアンスDASドライブの再構築	直接接続ストレージ (DAS) ドライブを再構築しています。最近交換または削除/再挿入された場合、この現象が予想されます。
機器のファンの故障が検出されました	アプライアンス内のファン ユニットに問題が検出されました。
アプライアンスのファイバーチャネル障害が検出されました	アプライアンスのストレージ コントローラとコンピューティング コントローラ間でファイバー チャネル リンクの問題が検出されました
アプライアンスのファイバーチャネルHBAポート障害	ファイバー チャネル HBA ポートに障害が発生しているか、または障害が発生しています。
アプライアンスのフラッシュキャッシュドライブは最適化されていない	SSD キャッシュに使用されるドライブは最適ではありません。
アプライアンス相互接続/バッテリーキャニスターを取り外しました	インターコネクト/バッテリーキャニスターがありません。
アプライアンスのLACPポートが見つかりません	StorageGRIDアプライアンス上のポートが LACP ボンドに参加していません。
アプライアンスのNIC障害が検出されました	アプライアンスのネットワーク インターフェイス カード (NIC) に問題が検出されました。
アプライアンス全体の電源が劣化	StorageGRIDアプライアンスの電力が推奨動作電圧から外れています。
アプライアンス SSD の重大な警告	アプライアンス SSD が重大な警告を報告しています。

アラート名	説明
アプライアンスストレージコントローラAの障害	StorageGRIDアプライアンスのストレージ コントローラ A に障害が発生しました。
アプライアンスストレージコントローラBの障害	StorageGRIDアプライアンスのストレージ コントローラ B に障害が発生しました。
アプライアンスのストレージ コントローラ ドライブの障害	StorageGRIDアプライアンス内の 1 つ以上のドライブに障害が発生しているか、最適ではありません。
アプライアンス ストレージ コントローラのハードウェアの問題	SANtricityソフトウェアは、 StorageGRIDアプライアンスのコンポーネントについて「注意が必要」と報告しています。
アプライアンスストレージコントローラ電源Aの障害	StorageGRIDアプライアンスの電源 A が推奨動作電圧から外れています。
アプライアンス ストレージ コントローラの電源 B の障害	StorageGRIDアプライアンスの電源 B が推奨動作電圧から外れています。
アプライアンス ストレージ ハードウェア モニター サービスが停止しました	ストレージ ハードウェアの状態を監視するサービスが停止しました。
家電収納棚の劣化	ストレージ アプライアンスのストレージ シェルフ内のコンポーネントの 1 つのステータスが低下しています。
機器の温度超過	アプライアンスのストレージ コントローラの公称温度または最大温度を超えました。
機器の温度センサーを取り外しました	温度センサーが取り外されました。
アプライアンスのUEFIセキュアブートエラー	アプライアンスは安全に起動されていません。
ディスクI/Oが非常に遅い	非常に遅いディスク I/O がグリッドのパフォーマンスに影響している可能性があります。
ストレージアプライアンスのファンの障害が検出されました	アプライアンスのストレージ コントローラ内のファン ユニットに問題が検出されました。
ストレージアプライアンスのストレージ接続が低下しました	コンピューティング コントローラーとストレージ コントローラー間の 1 つ以上の接続に問題があります。

アラート名	説明
ストレージデバイスにアクセスできません	ストレージデバイスにアクセスできません。

監査と**Syslog**アラート

アラート名	説明
監査ログがメモリ内キューに追加されています	ノードはローカル syslog サーバーにログを送信できず、メモリ内のキューがいっぱいになっています。
外部 syslog サーバ転送エラー	ノードはログを外部 syslog サーバーに転送できません。
大規模な監査キュー	監査メッセージのディスク キューがいっぱいです。この状態に対処しないと、S3 または Swift の操作が失敗する可能性があります。
ログはディスク上のキューに追加されています	ノードはログを外部 syslog サーバーに転送できず、ディスク上のキューがいっぱいになっています。

バケットアラート

アラート名	説明
FabricPoolバケットにはサポートされていないバケット整合性設定があります	FabricPoolバケットは、サポートされていない使用可能または強力なサイト整合性レベルを使用します。
FabricPoolバケットにはサポートされていないバージョン設定があります	FabricPoolバケットではバージョン管理または S3 オブジェクト ロックが有効になっていますが、これらはサポートされていません。

カサンドラアラート

アラート名	説明
Cassandra自動圧縮エラー	Cassandra 自動コンパクターでエラーが発生しました。
Cassandra の自動コンパクターのメトリクスが古い	Cassandra 自動コンパクターを説明するメトリックは古くなっています。
Cassandra通信エラー	Cassandra サービスを実行するノード間で通信に問題が発生しています。
Cassandraの圧縮が過負荷になった	Cassandra 圧縮プロセスが過負荷になっています。

アラート名	説明
Cassandra のオーバーサイズ書き込みエラー	内部のStorageGRIDプロセスが Cassandra に大きすぎる書き込み要求を送信しました。
Cassandraの修復メトリクスが古い	Cassandra 修復ジョブを説明するメトリックは古くなっています。
カサンドラの修復の進捗が遅い	Cassandra データベースの修復の進行が遅いです。
Cassandraの修理サービスは利用できません	Cassandra 修理サービスは利用できません。
Cassandraテーブルの破損	Cassandra はテーブルの破損を検出しました。 Cassandra はテーブルの破損を検出すると自動的に再起動します。

クラウドストレージプールのアラート

アラート名	説明
クラウド ストレージ プールの接続エラー	Cloud Storage Pools のヘルスチェックで 1 つ以上の新しいエラーが検出されました。
IAM Roles Anywhereエンドエンティティ認証の有効期限	IAM Roles Anywhere エンドエンティティ証明書の有効期限が近づいています。

クロスグリッドレプリケーションアラート

アラート名	説明
クロスグリッドレプリケーションの永続的な障害	解決するにはユーザーの介入が必要な、グリッド間レプリケーションエラーが発生しました。
クロスグリッドレプリケーションリソースが利用できません	リソースが利用できないため、クロスグリッド レプリケーション要求は保留中です。

DHCPアラート

アラート名	説明
DHCPリースの有効期限が切れました	ネットワーク インターフェイスの DHCP リースの有効期限が切れました。
DHCPリースがまもなく期限切れになります	ネットワーク インターフェイスの DHCP リースがまもなく期限切れになります。

アラート名	説明
DHCPサーバーが利用できません	DHCP サーバーが利用できません。

デバッグとトレースのアラート

アラート名	説明
デバッグパフォーマンスへの影響	デバッグ モードを有効にすると、システム パフォーマンスに悪影響が出る可能性があります。
トレース構成が有効	トレース構成を有効にすると、システム パフォーマンスに悪影響が及ぶ可能性があります。

電子メールと**AutoSupport**アラート

アラート名	説明
AutoSupportメッセージの送信に失敗しました	最新のAutoSupportメッセージの送信に失敗しました。
ドメイン名解決の失敗	StorageGRIDノードはドメイン名を解決できませんでした。
メール通知の失敗	アラートの電子メール通知を送信できませんでした。
SNMP通知エラー	トラップの宛先に SNMP 情報通知を送信するときにエラーが発生しました。
SSHまたはコンソールログインが検出されました	過去 24 時間以内に、ユーザーが Web コンソールまたは SSH を使用してログインしました。

消失訂正符号（**EC**）アラート

アラート名	説明
ECリバランスの失敗	EC 再バランス手順が失敗したか、停止しました。
EC修復失敗	EC データの修復ジョブが失敗したか、停止しました。
EC修理が行き詰まる	EC データの修復作業が停止しました。
消失訂正符号化フラグメント検証エラー	消失訂正符号化されたフラグメントは検証できなくなります。破損したフラグメントは修復されない可能性があります。

証明書の有効期限の警告

アラート名	説明
管理プロキシ CA 証明書の有効期限	管理プロキシ サーバーの CA バンドル内の 1 つ以上の証明書の有効期限が近づいています。
クライアント証明書の有効期限	1 つ以上のクライアント証明書の有効期限が近づいています。
S3 および Swift のグローバル サーバー証明書の有効期限	S3 および Swift のグローバル サーバー証明書の有効期限が近づいています。
ロードバランサエンドポイント証明書の有効期限	1 つ以上のロード バランサ エンドポイント証明書の有効期限が近づいています。
管理インターフェースのサーバー証明書の有効期限	管理インターフェイスに使用されているサーバー証明書の有効期限が近づいています。
外部 syslog CA 証明書の有効期限	外部 syslog サーバー証明書の署名に使用される証明機関 (CA) 証明書の有効期限が近づいています。
外部 syslog クライアント証明書の有効期限	外部 syslog サーバーのクライアント証明書の有効期限が近づいています。
外部 syslog サーバー証明書の有効期限	外部 syslog サーバーによって提示されたサーバー証明書の有効期限が近づいています。

グリッドネットワークアラート

アラート名	説明
グリッドネットワークMTUの不一致	グリッド ネットワーク インターフェイス (eth0) の MTU 設定は、グリッド内のノード間で大きく異なります。

グリッドフェデレーションアラート

アラート名	説明
グリッドフェデレーション証明書の有効期限	1 つ以上のグリッド フェデレーション証明書の有効期限が近づいています。
グリッドフェデレーション接続失敗	ローカル グリッドとリモート グリッド間のグリッド フェデレーション接続が機能していません。

使用率が高い、または遅延が大きい場合のアラート

アラート名	説明
Javaヒープ使用量が多い	Java ヒープスペースの高い割合が使用されています。
メタデータクエリのレイテンシが高い	Cassandra メタデータ クエリの平均時間が長すぎます。

アイデンティティ連携アラート

アラート名	説明
アイデンティティ連携の同期に失敗しました	アイデンティティ ソースからフェデレーション グループとユーザーを同期できません。
テナントの ID フェデレーション同期の失敗	テナントによって構成された ID ソースからフェデレーション グループとユーザーを同期できません。

情報ライフサイクル管理（**ILM**）アラート

アラート名	説明
ILMの配置は達成不可能	特定のオブジェクトに対して、ILM ルール内の配置指示を実行できません。
ILMスキャン率が低い	ILM スキャン レートは 100 オブジェクト/秒未満に設定されています。

キー管理サーバー（**KMS**）アラート

アラート名	説明
KMS CA証明書の有効期限	キー管理サーバー (KMS) 証明書の署名に使用される証明機関 (CA) 証明書の有効期限が近づいています。
KMSクライアント証明書の有効期限	キー管理サーバーのクライアント証明書の有効期限が近づいています
KMS構成の読み込みに失敗しました	キー管理サーバーの構成は存在しますが、ロードに失敗しました。
KMS接続エラー	アプライアンス ノードは、そのサイトのキー管理サーバーに接続できませんでした。
KMS暗号化キー名が見つかりません	構成されたキー管理サーバーには、指定された名前と一致する暗号化キーがありません。

アラート名	説明
KMS暗号化キーのローテーションに失敗しました	すべてのアプライアンス ボリュームは正常に復号化されましたが、1 つ以上のボリュームを最新のキーにローテーションできませんでした。
KMSが設定されていません	このサイトにはキー管理サーバーが存在しません。
KMS キーがアプライアンス ボリュームの暗号化に失敗しました	ノード暗号化が有効になっているアプライアンス上の 1 つ以上のボリュームを、現在の KMS キーで復号化できませんでした。
KMSサーバー証明書の有効期限	キー管理サーバー (KMS) で使用されるサーバー証明書の有効期限が近づいています。
KMSサーバーの接続障害	アプライアンス ノードは、そのサイトのキー管理サーバー クラスター内の 1 つ以上のサーバーに接続できませんでした。

ロードバランサーアラート

アラート名	説明
ゼロリクエストロードバランサ接続の昇格	リクエストを実行せずに切断されたロード バランサー エンドポイントへの接続の割合が増加しました。

ローカルクロックオフセットアラート

アラート名	説明
ローカルクロックの大きな時間オフセット	ローカル クロックとネットワーク タイム プロトコル (NTP) の時間間のオフセットが大きすぎます。

メモリ不足または空き容量不足の警告

アラート名	説明
監査ログのディスク容量が少ない	監査ログに使用できるスペースが少なくなっています。この状態に対処しないと、S3 または Swift の操作が失敗する可能性があります。
利用可能なノードメモリが少ない	ノード上で使用可能な RAM の量が少ない。
ストレージプールの空き容量が少ない	ストレージ ノード内のオブジェクト データを保存するために使用できるスペースが少なくなっています。
インストールされたノードのメモリが少ない	ノードにインストールされているメモリの量が少ないです。

アラート名	説明
メタデータの保存容量が少ない	オブジェクト メタデータを保存するために使用できるスペースが少なくなっています。
低メトリクスディスク容量	メトリック データベースに使用できるスペースが少なくなっています。
低オブジェクトデータストレージ	オブジェクト データを保存するために使用できるスペースが少なくなっています。
読み取り専用の透かしの上書きが少ない	ストレージ ボリュームのソフト読み取り専用ウォーターマーク オーバーライドが、ストレージ ノードの最小最適化ウォーターマークよりも小さくなっています。
ルートディスク容量が少ない	ルート ディスクの使用可能な容量が少なくなっています。
システムデータ容量が低い	/var/local に使用可能なスペースが少なくなっています。この状態に対処しないと、S3 または Swift の操作が失敗する可能性があります。
tmpディレクトリの空き容量が少ない	/tmp ディレクトリの使用可能なスペースが少なくなっています。

ノードまたはノードネットワークのアラート

アラート名	説明
管理ネットワーク受信使用状況	管理ネットワークの受信使用率が高くなっています。
管理ネットワーク送信使用量	管理ネットワークの送信使用量が高くなっています。
ファイアウォールの設定失敗	ファイアウォール構成の適用に失敗しました。
フォールバックモードの管理インターフェースエンドポイント	すべての管理インターフェースのエンドポイントが、長い間デフォルトポートにフォールバックしています。
ノードネットワーク接続エラー	ノード間でデータを転送中にエラーが発生しました。
ノードネットワーク受信フレームエラー	ノードが受信したネットワーク フレームのかなりの割合にエラーがありました。
ノードがNTPサーバーと同期していません	ノードはネットワーク タイム プロトコル (NTP) サーバーと同期していません。
ノードがNTPサーバーにロックされていません	ノードはネットワーク タイム プロトコル (NTP) サーバーにロックされていません。

アラート名	説明
アプライアンス以外のノードのネットワークがダウンしています	1 つ以上のネットワーク デバイスがダウンしているか、切断されています。
管理ネットワーク上のサービス アプライアンスのリンクがダウンしています	管理ネットワーク (eth1) へのアプライアンス インターフェイスがダウンしているか、切断されています。
管理ネットワーク ポート 1 のサービス アプライアンス リンクがダウンしました	アプライアンスの管理ネットワーク ポート 1 がダウンしているか、切断されています。
クライアントネットワーク上のサービスアプライアンスのリンクがダウンしています	クライアント ネットワーク (eth2) へのアプライアンス インターフェイスがダウンしているか、切断されています。
ネットワーク ポート 1 のサービス アプライアンス リンクがダウンしました	アプライアンスのネットワーク ポート 1 がダウンしているか、切断されています。
ネットワーク ポート 2 のサービス アプライアンス リンクがダウンしました	アプライアンスのネットワーク ポート 2 がダウンしているか、切断されています。
ネットワーク ポート 3 のサービス アプライアンス リンクがダウンしました	アプライアンスのネットワーク ポート 3 がダウンしているか、切断されています。
ネットワーク ポート 4 のサービス アプライアンス リンクがダウンしました	アプライアンスのネットワーク ポート 4 がダウンしているか、切断されています。
管理ネットワーク上のストレージ アプライアンスのリンクがダウンしました	管理ネットワーク (eth1) へのアプライアンス インターフェイスがダウンしているか、切断されています。
管理ネットワークポート1のストレージアプライアンスのリンクがダウンしました	アプライアンスの管理ネットワーク ポート 1 がダウンしているか、切断されています。
クライアントネットワーク上のストレージアプライアンスのリンクがダウンしています	クライアント ネットワーク (eth2) へのアプライアンス インターフェイスがダウンしているか、切断されています。
ネットワーク ポート 1 のストレージ アプライアンスのリンクがダウンしました	アプライアンスのネットワーク ポート 1 がダウンしているか、切断されています。

アラート名	説明
ネットワークポート2のストレージアプライアンスのリンクダウン	アプライアンスのネットワーク ポート 2 がダウンしているか、切断されています。
ネットワークポート3のストレージアプライアンスのリンクがダウンしました	アプライアンスのネットワーク ポート 3 がダウンしているか、切断されています。
ネットワークポート4のストレージアプライアンスのリンクダウン	アプライアンスのネットワーク ポート 4 がダウンしているか、切断されています。
ストレージノードが望ましいストレージ状態ではありません	ストレージノード上のLDRサービスは、内部エラーまたはボリューム関連の問題のため、目的の状態に移行できません。
TCP接続の使用	このノード上の TCP 接続の数は、追跡できる最大数に近づいています。
ノードと通信できません	1 つ以上のサービスが応答しないか、ノードにアクセスできません。
予期しないノードの再起動	過去 24 時間以内にノードが予期せず再起動しました。

オブジェクトアラート

アラート名	説明
オブジェクトの存在チェックに失敗しました	オブジェクト存在チェックジョブが失敗しました。
オブジェクトの存在チェックが停止しました	オブジェクト存在チェックジョブが停止しました。
失われた物	1 つ以上のオブジェクトがグリッドから失われました。
S3 PUT オブジェクトのサイズが大きすぎます	クライアントが S3 のサイズ制限を超える PUT Object 操作を試行しています。
未確認の破損オブジェクトが検出されました	複製オブジェクト ストレージ内に、複製オブジェクトとして識別できないファイルが見つかりました。

プラットフォームサービスアラート

アラート名	説明
プラットフォーム サービスの保留中のリクエスト容量が不足しています	保留中のリクエストのプラットフォーム サービスの数が容量に近づいています。
プラットフォームサービスは利用できません	RSM サービスを備えたストレージ ノードがサイトで実行中または使用可能数が少なすぎます。

ストレージボリュームアラート

アラート名	説明
ストレージ容量に注意が必要	ストレージ ボリュームがオフラインであり、注意が必要です。
ストレージボリュームを復元する必要があります	ストレージ ボリュームが回復されたため、復元する必要があります。
ストレージボリュームがオフライン	ストレージ ボリュームが 5 分以上オフラインになっています。
ストレージボリュームの再マウントを試行しました	ストレージ ボリュームがオフラインになったため、自動再マウントがトリガーされました。これは、ドライブの問題またはファイルシステムのエラーを示している可能性があります。
ボリュームの復元で複製されたデータの修復を開始できませんでした	修復されたボリュームの複製されたデータの修復を自動的に開始できませんでした。

StorageGRIDサービスアラート

アラート名	説明
バックアップ設定を使用したnginxサービス	nginx サービスの構成が無効です。以前の構成が現在使用されています。
バックアップ構成を使用した nginx-gw サービス	nginx-gw サービスの構成が無効です。以前の構成が現在使用されています。
FIPSを無効にするには再起動が必要です	セキュリティ ポリシーでは FIPS モードは必要ありませんが、 NetApp暗号化セキュリティ モジュールが有効になっています。
FIPSを有効にするには再起動が必要です	セキュリティ ポリシーでは FIPS モードが必要ですが、 NetApp暗号化セキュリティ モジュールが無効になっています。
バックアップ構成を使用した SSH サービス	SSH サービスの構成が無効です。以前の構成が現在使用されています。

アラート名	説明
テナントのクォータ使用量が高い	割り当て領域の高い割合が使用されています。このルールは、通知が多すぎる可能性があるため、デフォルトでは無効になっています。

よく使われる**Prometheus**メトリクス

デフォルトのアラート ルールの条件をより深く理解したり、カスタム アラート ルールの条件を構築したりするには、よく使用される Prometheus メトリックのリストを参照してください。

また、 すべての指標の完全なリストを取得する 。

Prometheusクエリの構文の詳細については、以下を参照してください。 "Prometheusのクエリ" 。

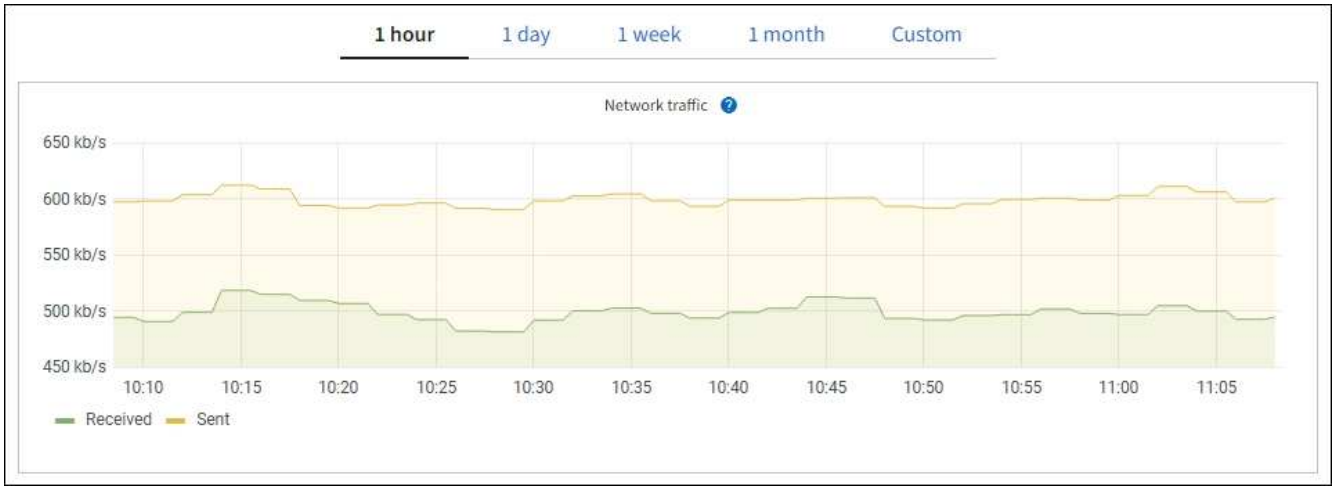
Prometheus メトリックとは何ですか**?**

Prometheus メトリックは時系列測定です。管理ノード上の Prometheus サービスは、すべてのノード上のサービスからこれらのメトリックを収集します。メトリックは、Prometheus データ用に予約されたスペースがいっぱいになるまで各管理ノードに保存されます。いつ `/var/local/mysql_ibdata/` ボリュームが容量に達すると、最も古いメトリックが最初に削除されます。

Prometheus メトリックはどこで使用されますか**?**

Prometheus によって収集されたメトリックは、Grid Manager のいくつかの場所で使用されます。

- ノード ページ: ノード ページから利用できるタブのグラフとチャートは、Grafana 視覚化ツールを使用して、Prometheus によって収集された時系列メトリックを表示します。 Grafana は時系列データをグラフやチャート形式で表示し、Prometheus はバックエンドのデータ ソースとして機能します。



- アラート: Prometheus メトリックを使用するアラート ルール条件が true と評価されると、特定の重大度レベルでアラートがトリガーされます。
- グリッド管理 **API**: カスタム アラート ルールまたは外部自動化ツールで Prometheus メトリックを使用して、 StorageGRIDシステムを監視できます。 Prometheus メトリックの完全なリストは、Grid Management API から入手できます。 (グリッド マネージャーの上部から、ヘルプ アイコンを選択

し、**API** ドキュメント > メトリック を選択します。) 1,000 を超えるメトリックが利用可能ですが、最も重要なStorageGRID操作を監視するために必要なメトリックは比較的少数です。

> 名前に *private* が含まれるメトリックは内部使用のみを目的としており、 StorageGRIDリリース間で予告なく変更されることがあります。

- サポート > ツール > 診断 ページと サポート > ツール > メトリック ページ: これらのページは主にテクニカル サポートによる使用を目的としており、Prometheus メトリックの値を使用するいくつかのツールとグラフを提供します。

> 「メトリクス」ページ内の一部の機能とメニュー項目は意図的に機能せず、変更される可能性があります。

最も一般的な指標のリスト

次のリストには、最も一般的に使用される Prometheus メトリックが含まれています。

> 名前に「*private*」が含まれるメトリックは内部使用のみを目的としており、 StorageGRID のリリース間で予告なく変更されることがあります。

アラートマネージャー通知失敗合計
: 失敗したアラート通知の合計数。

ノードファイルシステムの利用可能なバイト数
: 非ルート ユーザーが使用できるファイル システム領域の量 (バイト単位)。

ノードメモリ使用可能バイト数
: メモリ情報フィールド MemAvailable_bytes。

ノードネットワークキャリア
: キャリア値 `/sys/class/net/iface`。

ノードネットワーク受信エラー合計
: ネットワークデバイスの統計 `receive_errs`。

ノードネットワーク送信エラー合計
: ネットワークデバイスの統計 `transmit_errs`。

ストレージグリッドの管理ダウン
: 予期された理由により、ノードはグリッドに接続されていません。たとえば、ノードまたはノード上のサービスが正常にシャットダウンされた、ノードが再起動中、またはソフトウェアがアップグレード中などです。

ストレージグリッドアプライアンスコンピューティングコントローラーハードウェアステータス
: アプライアンス内のコンピューティング コントローラー ハードウェアのステータス。

ストレージグリッドアプライアンスの障害ディスク

アプライアンス内のストレージ コントローラーの場合、最適ではないドライブの数。

ストレージグリッドアプライアンスストレージコントローラーハードウェアステータス

アプライアンス内のストレージ コントローラ ハードウェアの全体的なステータス。

ストレージグリッドのコンテンツバケットとコンテナ

このストレージノードが認識している S3 バケットと Swift コンテナの合計数。

ストレージグリッドコンテンツオブジェクト

このストレージ ノードが認識している S3 および Swift データ オブジェクトの合計数。カウントは、S3 を介してシステムとインターフェースするクライアント アプリケーションによって作成されたデータ オブジェクトに対してのみ有効です。

ストレージグリッドコンテンツオブジェクトの損失

このサービスがStorageGRIDシステムから欠落していると検出したオブジェクトの合計数。損失の原因を特定し、回復が可能かどうかを確認するための措置を講じる必要があります。

"失われたオブジェクトデータのトラブルシューティング"

ストレージグリッドの**http**セッションの受信試行

ストレージ ノードに対して試行された HTTP セッションの合計数。

ストレージグリッドの**http**セッションが現在確立されている

ストレージ ノード上で現在アクティブな (開いている) HTTP セッションの数。

ストレージグリッドの**http**セッションが失敗しました

不正な HTTP リクエストまたは操作の処理中の失敗により、正常に完了できなかった HTTP セッションの合計数。

ストレージグリッドの**http**セッションが成功しました

正常に完了した HTTP セッションの合計数。

ストレージグリッド**ilm_awaiting_background_objects**

スキャンからの ILM 評価を待機しているこのノード上のオブジェクトの合計数。

ストレージグリッド**ilm**のクライアント評価オブジェクト待機数/秒

このノード上の ILM ポリシーに対してオブジェクトが評価される現在のレート。

ストレージグリッド**ilm**クライアントオブジェクト待機中

クライアント操作 (たとえば、取り込み) からの ILM 評価を待機している、このノード上のオブジェクトの合計数。

ストレージグリッド**ilm**待機オブジェクト合計

ILM 評価を待機しているオブジェクトの合計数。

ストレージグリッド**ilm**スキャンオブジェクト数/秒

このノードが所有するオブジェクトがスキャンされ、ILM のキューに入れられる速度。

ストレージグリッド**ilm**スキャン期間推定分数

このノードで完全な ILM スキャンを完了するのにかかる推定時間。

注意**:** 完全スキャンでは、このノードが所有するすべてのオブジェクトに ILM が適用されていることが保証されるわけではありません。

ストレージグリッドロードバランサーエンドポイント証明書の有効期限

ロード バランサ エンドポイント証明書の有効期限（エポックからの秒数）。

ストレージグリッドメタデータクエリの平均レイテンシーミリ秒

このサービスを通じてメタデータ ストアに対してクエリを実行するのに必要な平均時間。

ストレージグリッドネットワーク受信バイト数

インストール以降に受信したデータの合計量。

ストレージグリッドネットワーク送信バイト数

インストール以降に送信されたデータの合計量。

ストレージグリッドノードの**CPU**使用率

現在このサービスによって使用されている使用可能な CPU 時間の割合。サービスの混雑状況を示します。使用可能な CPU 時間の量は、サーバーの CPU の数によって異なります。

ストレージグリッド**ntp**の選択された時間ソースのオフセットミリ秒

選択された時間ソースによって提供される時間の体系的なオフセット。オフセットは、タイム ソースに到達するまでの遅延が、タイム ソースが NTP クライアントに到達するのに必要な時間と等しくない場合に導入されます。

ストレージグリッド**ntp**ロック

ノードはネットワーク タイム プロトコル (NTP) サーバーにロックされていません。

ストレージグリッド**S3**データ転送バイト数

属性が最後にリセットされてから、S3 クライアントからこのストレージ ノードに取り込まれたデータの合計量。

ストレージグリッド**S3**データ転送バイト取得

属性が最後にリセットされてから、このストレージ ノードから S3 クライアントによって取得されたデータの合計量。

ストレージグリッド**S3**操作失敗

S3 認証失敗によるものを除き、失敗した S3 操作 (HTTP ステータス コード 4xx および 5xx) の合計数。

ストレージグリッド**S3**操作が成功しました

成功した S3 操作の合計数 (HTTP ステータス コード 2xx)。

ストレージグリッド**S3**操作が不正である

承認の失敗の結果として失敗した S3 操作の合計数。

ストレージグリッドサーバー証明書管理インターフェース証明書の有効期限

管理インターフェイス証明書の有効期限が切れるまでの日数。

ストレージグリッドサーバー証明書の有効期限

Object Storage API 証明書の有効期限が切れるまでの日数。

ストレージグリッドサービス**CPU**秒数

インストール以降、このサービスによって CPU が使用された累積時間。

ストレージグリッドサービスのメモリ使用量バイト

このサービスによって現在使用されているメモリ (RAM) の量。この値は、Linux top ユーティリティによって RES として表示される値と同じです。

ストレージグリッドサービスネットワーク受信バイト数

インストール以降にこのサービスが受信したデータの合計量。

ストレージグリッドサービスネットワーク送信バイト数

このサービスによって送信されたデータの合計量。

ストレージグリッドサービスの再起動

サービスが再起動された回数の合計。

ストレージグリッドサービス実行時間秒数

インストール以降にサービスが実行されている合計時間。

ストレージグリッドサービスの稼働時間（秒）

サービスが最後に再起動されてから実行されている合計時間。

ストレージグリッドのストレージ状態_現在

ストレージ サービスの現在の状態。属性値は次のとおりです。

- 10 = オフライン
- 15 = メンテナンス
- 20 = 読み取り専用
- 30 = オンライン

ストレージグリッドストレージステータス

ストレージ サービスの現在のステータス。属性値は次のとおりです。

- 0 = エラーなし
- 10 = 移行中
- 20 = 空き容量不足
- 30 = ボリュームが利用できません
- 40 = エラー

ストレージグリッドのストレージ利用データバイト

ストレージ ノード上の複製および消去コード化されたオブジェクト データの合計サイズの推定値。

ストレージグリッドのストレージ利用メタデータの許容バイト数

オブジェクト メタデータに許可される各ストレージ ノードのボリューム 0 上の合計スペース。この値は、ノード上のメタデータ用に予約されている実際のスペースよりも常に小さくなります。これは、予約されているスペースの一部が、重要なデータベース操作 (圧縮や修復など) や将来のハードウェアおよびソフトウェアのアップグレードに必要となるためです。オブジェクト メタデータに許可されているスペースによって、オブジェクト全体の容量が制御されます。

ストレージグリッドのストレージ利用メタデータバイト

ストレージ ボリューム 0 上のオブジェクト メタデータの量 (バイト単位)。

ストレージグリッドのストレージ使用率の合計スペースバイト

すべてのオブジェクト ストアに割り当てられたストレージ スペースの合計量。

ストレージグリッドのストレージ利用率の使用可能スペースバイト

残っているオブジェクト ストレージ領域の合計量。ストレージ ノード上のすべてのオブジェクト ストアで使用可能なスペースの量を合計して計算されます。

ストレージグリッド**_swift_**データ転送バイト数

属性が最後にリセットされてから、Swift クライアントからこのストレージ ノードに取り込まれたデータの合計量。

ストレージグリッド**_swift_**データ転送バイト取得

属性が最後にリセットされてから、Swift クライアントがこのストレージ ノードから取得したデータの合計量。

ストレージグリッド**_swift_operations_failed**

Swift 認証の失敗によって発生したものを除き、失敗した Swift 操作 (HTTP ステータス コード 4xx および 5xx) の合計数。

ストレージグリッド**_swift_**操作_成功

成功した Swift 操作 (HTTP ステータス コード 2xx) の合計数。

ストレージグリッド**_swift_**操作_無許可

認証失敗 (HTTP ステータス コード 401、403、405) の結果として失敗した Swift 操作の合計数。

ストレージグリッドテナント使用データバイト

テナントのすべてのオブジェクトの論理サイズ。

ストレージグリッドテナント使用オブジェクト数

テナントのオブジェクトの数。

ストレージグリッドテナント使用量クォータバイト

テナントのオブジェクトに使用できる論理スペースの最大量。クォータメトリックが指定されていない場合は、無制限のスペースが利用可能です。

すべての指標のリストを取得する

メトリックの完全なリストを取得するには、Grid Management API を使用します。

1. グリッド マネージャーの上部から、ヘルプ アイコンを選択し、**API** ドキュメント を選択します。
2. **metrics** 操作を見つけます。
3. 実行する `GET /grid/metric-names`手術。
4. 結果をダウンロードしてください。

ログファイルリファレンス

ログファイルリファレンス

StorageGRID は、イベント、診断メッセージ、およびエラー状態をキャプチャするために使用されるログを提供します。トラブルシューティングを支援するために、ログ ファイルを収集してテクニカル サポートに転送するように求められる場合があります。

ログは次のように分類されます。

- "StorageGRIDソフトウェアログ"
- "展開およびメンテナンスのログ"
- "bycast.logについて"

> 各ログ タイプに提供される詳細は参考用です。ログは、テクニカル サポートによる高度なトラブルシューティングを目的としています。監査ログとアプリケーション ログ ファイルを使用して問題の履歴を再構築する高度な手法については、この手順では説明しません。

ログにアクセスする

ログにアクセスするには、"ログファイルとシステムデータを収集する" 1 つ以上のノードから単一のログ ファイル アーカイブとして保存します。または、プライマリ管理ノードが使用できない場合、または特定のノードにアクセスできない場合は、次のようにして各グリッド ノードの個別のログ ファイルにアクセスできます。

1. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
2. 記載されているパスワードを入力してください `Passwords.txt`ファイル。
3. ルートに切り替えるには、次のコマンドを入力します。 `su -`
4. 記載されているパスワードを入力してください `Passwords.txt`ファイル。

ログを**Syslog**サーバーにエクスポートする

ログを Syslog サーバーにエクスポートすると、次の機能が得られます。

- S3 および Swift リクエストに加えて、すべての Grid Manager および Tenant Manager リクエストのリストを受け取ります。
- 監査ログ方法によるパフォーマンスへの影響なしに、エラーを返す S3 リクエストの可視性が向上します。

- 解析しやすい HTTP 層のリクエストとエラー コードにアクセスします。
- ロードバランサーのトラフィック分類器によってブロックされたリクエストの可視性が向上します。

ログをエクスポートするには、"監査メッセージとログの保存先を構成する" 。

ログファイルのカテゴリ

StorageGRIDログ ファイル アーカイブには、各カテゴリについて説明されているログと、メトリックおよびデバッグ コマンド出力を含む追加ファイルが含まれています。

Archive location	説明
audit（監査）	通常のシステム操作中に生成される監査メッセージ。
ベースOSログ	StorageGRIDイメージのバージョンを含む基本オペレーティング システム情報。
バンドル	グローバル構成情報 (バンドル)。
カサンドラ	Cassandra データベース情報と Reaper 修復ログ。
ec	現在のノードに関する VCS 情報とプロファイル ID による EC グループ情報。
グリッド	デバッグを含む一般的なグリッドログ(`bycast.log`） そして `servermanager` ログ。
グリッド.json	すべてのノード間で共有されるグリッド構成ファイル。さらに、 `node.json`現在のノードに固有です。
hagroups	高可用性グループのメトリックとログ。
インストール	`Gdu-server`ログをインストールします。
ラムダ仲裁人	S3 Select プロキシリクエストに関連するログ。
木こり.log	ログ収集に関連するデバッグ メッセージ。
メトリクス	Grafana、Jaeger、ノード エクスポーター、および Prometheus のサービス ログ。
その他	さまざまなアクセスとエラー ログ。
mysql	mariaDB データベース構成と関連ログ。
ネット	ネットワーク関連のスクリプトと Dynip サービスによって生成されたログ。

Archive location	説明
nginx	ロード バランサおよびグリッド フェデレーションの構成ファイルとログ。 Grid Manager および Tenant Manager のトラフィック ログも含まれます。
nginx-gw	• `access.log`: グリッド マネージャーとテナント マネージャーはログ メッセージを要求します。 ◦ これらのメッセージには、 `mgmt`: syslog を使用してエクスポートされた場合。 ◦ これらのログメッセージの形式は `[$time_iso8601] $remote_addr $status $bytes_sent $request_length $request_time "$endpointId" "$request" "$http_host" "$http_user_agent" "$http_referer"` • `cgr-access.log.gz`: 受信クロスグリッドレプリケーション要求。 ◦ これらのメッセージには、 `cgr`: syslog を使用してエクスポートされた場合。 ◦ これらのログメッセージの形式は `[$time_iso8601] $remote_addr $status $bytes_sent $request_length $request_time "$endpointId" "$upstream_addr" "$request" "$http_host"` • `endpoint-access.log.gz`: ロードバランサーエンドポイントへの S3 および Swift リクエスト。 ◦ これらのメッセージには、 `endpoint`: syslog を使用してエクスポートされた場合。 ◦ これらのログメッセージの形式は `[$time_iso8601] $remote_addr $status $bytes_sent $request_length $request_time "$endpointId" "$upstream_addr" "$request" "$http_host"` • `nginx-gw-dns-check.log`: 新しい DNS チェック アラートに関連します。
NTP	NTP 構成ファイルとログ。
孤立したオブジェクト	孤立したオブジェクトに関するログ。
os	ノードとグリッドの状態ファイル（サービスを含む） `pid` 。
その他	ログファイル `/var/local/log`他のフォルダーに収集されないもの。
パフォーマンス	CPU、ネットワーク、ディスク I/O のパフォーマンス情報。
プロメテウスデータ	ログ収集に Prometheus データが含まれている場合の現在の Prometheus メトリック。

Archive location	説明
provisioning（プロビジョニング）	グリッド プロビジョニング プロセスに関連するログ。
ラフト	プラットフォーム サービスで使用される Raft クラスターからのログ。
ssh	SSH 構成とサービスに関連するログ。
snmp	SNMP 通知の送信に使用される SNMP エージェント構成。
ソケットデータ	ネットワークデバッグ用のソケット データ。
システムコマンド.txt	StorageGRIDコンテナ コマンドの出力。ネットワークやディスク使用量などのシステム情報が含まれます。
同期リカバリパッケージ	ADC サービスをホストするすべての管理ノードとストレージ ノード全体で最新のリカバリ パッケージの一貫性を維持することに関連します。

StorageGRIDソフトウェアログ

StorageGRIDログを使用して問題をトラブルシューティングできます。

ログを外部のSyslogサーバーに送信したり、監査情報の送信先を変更したりする場合は、`bycast.log`そして `nms.log`、 見る"監査メッセージとログの保存先を構成する"。

一般的な**StorageGRID**ログ

ファイル名	注記	見つかった場所
/var/local/log/bycast.log	主要なStorageGRIDトラブルシューティング ファイル。サポート > ツール > グリッド トポロジ を選択します。次に、***Site*** > ***Node*** > **SSM** > *イベント*を選択します。	すべてのノード
/var/local/log/bycast-err.log	のサブセットが含まれています `bycast.log`(重大度が ERROR および CRITICAL のメッセージ)。CRITICAL メッセージもシステムに表示されます。サポート > ツール > グリッド トポロジ を選択します。次に、***Site*** > ***Node*** > **SSM** > *イベント*を選択します。	すべてのノード

ファイル名	注記	見つかった場所
/var/local/core/	プログラムが異常終了した場合に作成されるコア ダンプ ファイルが含まれます。考えられる原因としては、アサーションの失敗、違反、スレッドのタイムアウトなどがあります。 注: ファイル ``/var/local/core/kexec_cmd`通常はアプライアンス ノードに存在し、エラーを示すものではありません。	すべてのノード

暗号関連のログ

ファイル名	注記	見つかった場所
/var/local/log/ssh-config-generation.log	SSH 構成の生成と SSH サービスの再読み込みに関連するログが含まれます。	すべてのノード
/var/local/log/nginx/config-generation.log	nginx 構成の生成と nginx サービスの再読み込みに関連するログが含まれます。	すべてのノード
/var/local/log/nginx-gw/config-generation.log	nginx-gw 構成の生成 (および nginx-gw サービスの再読み込み) に関連するログが含まれます。	管理ノードとゲートウェイノード
/var/local/log/update-cipher-configurations.log	TLS および SSH ポリシーの構成に関連するログが含まれます。	すべてのノード

グリッドフェデレーションログ

ファイル名	注記	見つかった場所
/var/local/log/update_grid_federation_config.log	グリッド フェデレーション接続用の nginx および nginx-gw 構成の生成に関連するログが含まれます。	すべてのノード

NMSログ

ファイル名	注記	見つかった場所
/var/local/log/nms.log	• グリッド マネージャーとテナント マネージャーからの通知をキャプチャします。 • NMS サービスの操作に関連するイベントをキャプチャします。たとえば、電子メール通知や構成の変更などです。 • システムで行われた構成の変更の結果として生じた XML バンドルの更新が含まれます。 • 1 日に 1 回実行される属性のダウンサンプリングに関連するエラー メッセージが含まれます。 • ページ生成エラーや HTTP ステータス 500 エラーなどの Java Web サーバー エラー メッセージが含まれます。	管理ノード
/var/local/log/nms.errlog	MySQL データベースのアップグレードに関連するエラー メッセージが含まれています。 対応するサービスの標準エラー (stderr) ストリームが含まれます。サービスごとに 1 つのログ ファイルがあります。サービスに問題がない限り、これらのファイルは通常空です。	管理ノード
/var/local/log/nms.requestlog	管理 API から内部StorageGRIDサービスへの送信接続に関する情報が含まれます。	管理ノード

サーバーマネージャーのログ

ファイル名	注記	見つかった場所
/var/local/log/servermanager.log	サーバー上で実行されている Server Manager アプリケーションのログ ファイル。	すべてのノード
/var/local/log/GridstatBackend.errlog	Server Manager GUI バックエンド アプリケーションのログ ファイル。	すべてのノード
/var/local/log/gridstat.errlog	サーバー マネージャー GUI のログ ファイル。	すべてのノード

StorageGRIDサービスログ

ファイル名	注記	見つかった場所
/var/local/log/acct.errlog		ADC サービスを実行しているストレージノード
/var/local/log/adc.errlog	対応するサービスの標準エラー (stderr) ストリームが含まれます。サービスごとに 1 つのログ ファイルがあります。サービスに問題がない限り、これらのファイルは通常空です。	ADC サービスを実行しているストレージノード
/var/local/log/ams.errlog		管理ノード
/var/local/log/cassandra/system.log	新しいストレージ ノードを追加するときに問題が発生した場合、または nodetool repair タスクが停止した場合に使用できるメタデータ ストア (Cassandra データベース) の情報。	ストレージ ノード
/var/local/log/cassandra-reaper.log	Cassandra データベース内のデータの修復を実行する Cassandra Reaper サービスの情報。	ストレージ ノード
/var/local/log/cassandra-reaper.errlog	Cassandra Reaper サービスのエラー情報。	ストレージ ノード
/var/local/log/chunk.errlog		ストレージ ノード
/var/local/log/cmn.errlog		管理ノード
/var/local/log/cms.errlog	このログ ファイルは、 StorageGRIDの古いバージョンからアップグレードされたシステムに存在する可能性があります。レガシー情報が含まれています。	ストレージ ノード
/var/local/log/dds.errlog		ストレージ ノード
/var/local/log/dmv.errlog		ストレージ ノード
/var/local/log/dynip*	グリッドの動的 IP 変更を監視し、ローカル構成を更新する dynip サービスに関連するログが含まれます。	すべてのノード

ファイル名	注記	見つかった場所
/var/local/log/grafana.log	グリッド マネージャーでのメトリックの視覚化に使用される、Grafana サービスに関連付けられたログ。	管理ノード
/var/local/log/hagroups.log	高可用性グループに関連付けられたログ。	管理ノードとゲートウェイノード
/var/local/log/hagroups_events.log	BACKUP から MASTER または FAULT への移行などの状態の変化を追跡します。	管理ノードとゲートウェイノード
/var/local/log/idnt.errlog		ADC サービスを実行しているストレージノード
/var/local/log/jaeger.log	トレース収集に使用される、Jaeger サービスに関連付けられたログ。	すべてのノード
/var/local/log/kstn.errlog		ADC サービスを実行しているストレージノード
/var/local/log/lambda*	S3 Select サービスのログが含まれます。	管理ノードとゲートウェイノード このログは特定の管理ノードとゲートウェイ ノードにのみ含まれます。参照"S3 Select の管理ノードとゲートウェイノードの要件と制限"。
/var/local/log/ldr.errlog		ストレージ ノード
/var/local/log/miscd/*.log	他のノード上のサービスのクエリと管理、および他のノードで実行されているサービスの状態のクエリなど、ノード上の環境構成の管理のためのインターフェイスを提供する MISCd サービス (Information Service Control Daemon) のログが含まれます。	すべてのノード
/var/local/log/nginx/*.log	nginx サービスのログが含まれます。nginx サービスは、さまざまなグリッド サービス (Prometheus や Dynip など) が HTTPS API を介して他のノード上のサービスと通信できるようにするための認証および安全な通信メカニズムとして機能します。	すべてのノード

ファイル名	注記	見つかった場所
/var/local/log/nginx-gw/*.log	エラー ログや管理ノード上の制限された管理ポートのログなど、nginx-gw サービスに関連する一般的なログが含まれます。	管理ノードとゲートウェイノード
/var/local/log/nginx-gw/cgr-access.log.gz	クロスグリッド レプリケーション トラフィックに関連するアクセス ログが含まれます。	グリッド フェデレーション構成に基づいて、管理ノード、ゲートウェイ ノード、またはその両方。クロスグリッド レプリケーションの宛先グリッドにのみ存在します。
/var/local/log/nginx-gw/エンドポイントアクセス.log.gz	クライアントからストレージ ノードへの S3 トラフィックの負荷分散を提供するロード バランサ サービスのアクセス ログが含まれます。	管理ノードとゲートウェイノード
/var/local/log/persistence*	再起動後も保持する必要があるルート ディスク上のファイルを管理する Persistence サービスのログが含まれます。	すべてのノード
/var/local/log/プロメテウス.log	すべてのノードについて、ノード エクスポータ サービス ログと ade-exporter メトリック サービス ログが含まれます。 管理ノードの場合、Prometheus および Alert Manager サービスのログも含まれます。	すべてのノード
/var/local/log/raft.log	Raft プロトコルの RSM サービスで使用されるライブラリの出力が含まれます。	RSM サービスを備えたストレージノード
/var/local/log/rms.errlog	S3 プラットフォーム サービスに使用される Replicated State Machine Service (RSM) サービスのログが含まれます。	RSM サービスを備えたストレージノード
/var/local/log/ssm.errlog		すべてのノード
/var/local/log/update-s3vs-domains.log	S3 仮想ホスト ドメイン名設定の更新処理に関連するログが含まれます。S3 クライアント アプリケーションの実装手順を参照してください。	管理ノードとゲートウェイノード

ファイル名	注記	見つかった場所
/var/local/log/update-snmp-firewall.*	SNMP 用に管理されているファイアウォール ポートに関連するログが含まれます。	すべてのノード
/var/local/log/update-sysl.log	システムの syslog 構成に加えられた変更に関連するログが含まれます。	すべてのノード
/var/local/log/update-traffic-classes.log	トラフィック分類子の構成の変更に関連するログが含まれます。	管理ノードとゲートウェイノード
/var/local/log/update-utcn.log	このノード上の信頼されていないクライアント ネットワーク モードに関連するログが含まれます。	すべてのノード

関連情報

- "bycast.logについて"
- "S3 REST APIを使用する"

展開およびメンテナンスのログ

デプロイメント ログとメンテナンス ログを使用して、問題をトラブルシューティングできます。

ファイル名	注記	見つかった場所
/var/local/log/インストール.log	ソフトウェアのインストール中に作成されます。インストール イベントの記録が含まれます。	すべてのノード
/var/local/log/拡張進行状況.log	拡張操作中に作成されました。拡張イベントの記録が含まれています。	ストレージ ノード
/var/local/log/pa-move.log	実行中に作成された `pa-move.sh`スクリプト。	プライマリ管理ノード
/var/local/log/pa-move-new_pa.log	実行中に作成された `pa-move.sh`スクリプト。	プライマリ管理ノード
/var/local/log/pa-move-old_pa.log	実行中に作成された `pa-move.sh`スクリプト。	プライマリ管理ノード
/var/local/log/gdu-server.log	GDU サービスによって作成されました。プライマリ管理ノードによって管理されるプロビジョニングおよびメンテナンス手順に関連するイベントが含まれます。	プライマリ管理ノード

ファイル名	注記	見つかった場所
/var/local/log/send_admin_hw.log	インストール中に作成されます。ノードとプライマリ管理ノードとの通信に関連するデバッグ情報が含まれます。	すべてのノード
/var/local/log/アップグレード.log	ソフトウェアのアップグレード中に作成されました。ソフトウェア更新イベントの記録が含まれます。	すべてのノード

bycast.logについて

ファイル `/var/local/log/bycast.log`StorageGRIDソフトウェアの主なトラブルシューティング ファイルです。そこには `bycast.log`グリッド ノードごとにファイルを作成します。ファイルには、そのグリッド ノードに固有のメッセージが含まれています。

ファイル `/var/local/log/bycast-err.log`のサブセットです `bycast.log`。重大度が ERROR および CRITICAL のメッセージが含まれます。

必要に応じて、監査ログの送信先を変更し、監査情報を外部の syslog サーバーに送信することもできます。外部 Syslog サーバーが構成されている場合、監査レコードのローカル ログは引き続き生成され、保存されます。見る"監査メッセージとログの保存先を構成する" 。

bycast.log のファイルローテーション

いつ `bycast.log`ファイルが 1 GB に達すると、既存のファイルが保存され、新しいログ ファイルが開始されます。

保存したファイルの名前が変更されます `bycast.log.1`、新しいファイルの名前は `bycast.log`。新しい `bycast.log`1GBに達すると、 `bycast.log.1`名前が変更され、圧縮されて `bycast.log.2.gz`、 そして `bycast.log`名前が変更されました `bycast.log.1`。

回転限界 `bycast.log`21 ファイルです。 22番目のバージョンでは、 `bycast.log`ファイルが作成されると、最も古いファイルが削除されます。

回転限界 `bycast-err.log`ファイルは7つです。

> ログ ファイルが圧縮されている場合は、書き込まれた場所と同じ場所に解凍しないでください。ファイルを同じ場所に解凍すると、ログローテーション スクリプトの動作が妨げられる可能性があります。

必要に応じて、監査ログの送信先を変更し、監査情報を外部の syslog サーバーに送信することもできます。外部 Syslog サーバーが構成されている場合、監査レコードのローカル ログは引き続き生成され、保存されます。見る"監査メッセージとログの保存先を構成する" 。

関連情報

"ログファイルとシステムデータを収集する"

bycast.log 内のメッセージ

メッセージ `bycast.log`ADE (非同期分散環境) によって記述されます。 ADE は、各グリッド ノードのサービスによって使用されるランタイム環境です。

ADE メッセージの例:

```
May 15 14:07:11 um-sec-rg1-agn3 ADE: |12455685    0357819531
SVMR EVHR 2019-05-05T27T17:10:29.784677| ERROR 0906 SVMR: Health
check on volume 3 has failed with reason 'TOUT'
```

ADE メッセージには次の情報が含まれます。

メッセージセグメント	例の値
ノードID	12455685
ADEプロセスID	0357819531
モジュール名	SVMR
メッセージ識別子	EVHR
UTCシステム時間	2019-05-05T27T17:10:29.784677 (YYYY-MM-DDTHH:MM:SS.uuuuuu)
重大度レベル	ERROR
内部追跡番号	0906
メッセージ	SVMR: ボリューム 3 のヘルス チェックが理由 'TOUT' で失敗しました

bycast.log のメッセージの重大度

メッセージは `bycast.log`重大度レベルが割り当てられます。

例えば：

- 通知 — 記録する必要があるイベントが発生しました。ほとんどのログ メッセージはこのレベルにあります。
- 警告 — 予期しない状態が発生しました。
- エラー — 操作に影響する重大なエラーが発生しました。
- **CRITICAL** — 異常な状態が発生し、通常の操作が停止しました。根本的な症状にすぐに対処する必要があります。

エラーコード `bycast.log`

ほとんどのエラーメッセージは `bycast.log`エラーコードが含まれています。

次の表は、 `bycast.log`数値以外のコードの正確な意味は、それが報告されるコンテキストによって異なります。

エラー コード	説明
サックス	エラーなし
ゲール	不明
CANC	キャンセル
ABRT	中止
すべて	Timeout
非VL	無効
NFND	Not found
ヴァース	version
会議	構成
失敗	失敗
ICPL	不完全
終わり	完了
SUNV	サービスは利用できません

次の表は、 `bycast.log` 。

エラー番号	エラー コード	説明
001	エペルム	Operation not permitted
002	エノエント	そのようなファイル、又はディレクトリはありません
003	エスルチ	そのようなプロセスはありません
004	EINTR	中断されたシステムコール
005	EIO	I/O error
006	エンクシオ	そのようなデバイスまたはアドレスはありません

エラー番号	エラー コード	説明
007	E2ビッグ	引数リストが長すぎます
008	エノエグゼック	実行形式エラー
009	EBADF	ファイル番号が間違っています
010	エチャイルド	子プロセスなし
011	再び	再試行
012	エノメム	メモリ不足です
013	アクセス	許可が拒否されました
014	エフォルト	住所が間違っています
015	ENOTBLK	ブロックデバイスが必要です
016	忙しい	デバイスまたはリソースがビジー状態です
017	存在する	ファイルが存在します
018	エクスデブ	クロスデバイスリンク
019	エノデフ	そのようなデバイスはありません
020	エノティディル	ディレクトリではありません
021	エイスディール	ディレクトリです
022	アインヴァル	無効な引数
023	エンファイル	ファイルテーブルのオーバーフロー
024	EMFILE	開いているファイルが多すぎます
025	エノッティ	タイプライターではない
026	ETXTBSY	テキストファイルがビジー状態です
027	EFBIG	ファイルが大きすぎます

エラー番号	エラー コード	説明
028	ENOSPC	No space left on device
029	エスピア	不正なシーク
030	エロフス	読み取り専用ファイルシステム
031	EMLINK	リンクが多すぎる
032	エパイプ	壊れたパイプ
033	エドム	関数のドメイン外の数学引数
034	エレンジ	数学の結果は表現できません
035	エディアドルク	リソースのデッドロックが発生する
036	エナメトゥーロン	ファイル名が長すぎます
037	エノルク	レコードロックは使用できません
038	エノシス	関数は実装されていません
039	空虚	ディレクトリが空ではありません
040	ELOOP	検出されたシンボリックリンクが多すぎます
041		
042	ENOMSG	希望するタイプのメッセージがありません
043	EIDRM	識別子が削除されました
044	エクロン	チャンネル番号が範囲外です
045	EL2NSYNC	レベル2が同期されていません
046	EL3HLT	レベル3停止
047	EL3RST	レベル3のリセット
048	エルンング	リンク番号が範囲外です

エラー番号	エラー コード	説明
049	ユーナッチ	プロトコル ドライバーが接続されていません
050	エノシ	CSI構造は利用できません
051	EL2HLT	レベル2停止
052	エバデ	無効な交換
053	エバドル	無効なリクエスト記述子
054	エクスフル	交換完了
055	エノアノ	陽極なし
056	EBADRQC	無効なリクエストコード
057	エバズルト	無効なスロット
058		
059	EBFONT	フォントファイル形式が正しくありません
060	エノスター	デバイスはストリームではありません
061	エノデータ	使用できるデータがありません
062	ETIME	タイマー期限切れ
063	エノス	ストリーム外のリソース
064	エノネット	マシンがネットワークに接続されていません
065	有効	パッケージがインストールされていません
066	エレリモート	オブジェクトはリモートです
067	エノリンク	リンクが切断されました
068	EADV	広告エラー
069	ESRMNT	Srmount エラー

エラー番号	エラー コード	説明
070	エココム	送信時に通信エラーが発生しました
071	エプロト	プロトコルエラー
072	エマルティホップ	マルチホップを試行しました
073	エドトドット	RFS固有のエラー
074	EBADMSG	データメッセージではありません
075	オーバーフロー	定義されたデータ型に対して値が大きすぎます
076	エノトニク	名前がネットワーク上で一意ではありません
077	EBADFD	ファイル記述子の状態が不良です
078	エレムチグ	リモートアドレスが変更されました
079	エリバック	必要な共有ライブラリにアクセスできません
080	エリバッド	破損した共有ライブラリへのアクセス
081	エリブスン	
082	エリブマックス	共有ライブラリをリンクしようとしすぎています
083	エリビエグゼック	共有ライブラリを直接実行できない
084	アイルセク	不正なバイトシーケンス
085	エレスタート	中断されたシステムコールは再開する必要がある
086	エストパイプ	ストリームパイプエラー
087	EUSERS	ユーザーが多すぎる
088	エノットソック	非ソケットに対するソケット操作
089	エデスタアドレス要求	宛先住所が必要です
090	EMSGサイズ	メッセージが長すぎます

エラー番号	エラー コード	説明
091	プロトタイプ	ソケットのプロトコルタイプが間違っています
092	エノプロトオプト	プロトコルは利用できません
093	エプロトノサポート	プロトコルはサポートされていません
094	ESOCKTNOSUPPORT	ソケットタイプはサポートされていません
095	EOPNOTSUPP	トランスポートエンドポイントでは操作はサポートされていません
096	EPFNOサポート	プロトコル ファミリはサポートされていません
097	EAFNOサポート	プロトコルでサポートされていないアドレス ファミリ
098	EADDRINUSE	このアドレスは既に使用されています
099	EADDRNOTAVAIL	要求されたアドレスを割り当てることができません
100	エネットダウン	ネットワークがダウンしています
101	エネトゥンリーチ	ネットワークにアクセスできません
102	ENETRESET	リセットによりネットワーク接続が切断されました
103	エコノミスト	ソフトウェアによって接続が終了した
104	エコノリセット	ピアによる接続のリセット
105	エノブフス	バッファスペースがありません
106	アイスコン	トランスポートエンドポイントはすでに接続されています
107	エノトコン	トランスポートエンドポイントが接続されていません
108	シャットダウン	トランスポートエンドポイントのシャットダウン後に送信できません
109	ETOOMANYREFS	参照が多すぎるため、結合できません

エラー番号	エラー コード	説明
110	タイムアウト	接続がタイムアウトしました
111	サービス拒否	接続が拒否されました
112	EHOSTDOWN	ホストがダウンしています
113	EHOSTUNREACH	ホストへのルートがありません
114	すでに	操作はすでに進行中です
115	アインプログレス	操作は現在進行中です
116		
117	ユークリーン	構造物の清掃が必要
118	エノトナム	XENIX の名前付きタイプファイルではありません
119	エナベイル	XENIXセマフォは使用できません
120	アイスナム	名前付きタイプファイルです
121	エレリモート	リモートI/Oエラー
122	エドクォート	割り当て超過
123	エノメディウム	媒体が見つかりません
124	ミディアムタイプ	間違ったメディアタイプ
125	キャンセル	処理がキャンセルされました
126	エノキー	必要なキーが利用できません
127	EKEY期限切れ	キーの有効期限が切れました
128	EKEYが取り消されました	キーは取り消されました
129	EKEY拒否	キーはサービスによって拒否されました
130	所有者死亡	堅牢なミューテックスの場合: 所有者が死亡

エラー番号	エラー コード	説明
131	回復不能	堅牢なミューテックスの場合: 状態は回復不可能

監査メッセージとログの送信先を構成する

外部**Syslog**サーバーの使用に関する考慮事項

外部 Syslog サーバーは、 StorageGRIDの外部にあるサーバーであり、システム監査情報を 1 か所に収集するために使用できます。外部 Syslog サーバーを使用すると、管理ノード上のネットワーク トラフィックを削減し、情報をより効率的に管理できます。StorageGRIDの場合、送信 syslog メッセージ パケット形式は RFC 3164 に準拠しています。

外部 Syslog サーバーに送信できる監査情報の種類は次のとおりです。

- 通常のシステム操作中に生成された監査メッセージを含む監査ログ
- ログインやルートへのエスカレーションなどのセキュリティ関連のイベント
- 発生した問題のトラブルシューティングのためにサポートケースを開く必要がある場合に要求される可能性のあるアプリケーションログ

外部**Syslog**サーバーを使用する場合

外部 syslog サーバーは、大規模なグリッドがある場合、複数の種類の S3 アプリケーションを使用する場合、またはすべての監査データを保持する場合に特に便利です。監査情報を外部 Syslog サーバーに送信すると、次のことが可能になります。

- 監査メッセージ、アプリケーション ログ、セキュリティ イベントなどの監査情報をより効率的に収集および管理します。
- 監査情報は管理ノードを経由せずにさまざまなストレージノードから外部 syslog サーバーに直接転送されるため、管理ノード上のネットワーク トラフィックが削減されます。

> ログが外部 syslog サーバーに送信される場合、外部 syslog サーバーの実装における一般的な制限に準拠するために、8,192 バイトを超える単一ログはメッセージの末尾で切り捨てられます。

> 外部Syslogサーバの障害発生時に完全なデータ復旧のオプションを最大限にするために、監査記録のローカルログを最大20GBまで保存します。(`localaudit.log` ）が各ノードで維持されます。

外部**Syslog**サーバーの設定方法

外部Syslogサーバーの設定方法については、"監査メッセージと外部Syslogサーバーを構成する" 。

TLS または RELP/TLS プロトコルを使用するように構成する場合は、次の証明書が必要です。

- サーバー **CA** 証明書: PEM エンコードで外部 syslog サーバーを検証するための 1 つ以上の信頼できる CA

証明書。省略した場合は、デフォルトのグリッド CA 証明書が使用されます。

- クライアント証明書: PEM エンコードされた外部 syslog サーバーへの認証用のクライアント証明書。
- クライアント秘密キー: PEM エンコードされたクライアント証明書の秘密キー。

> クライアント証明書を使用する場合は、クライアントの秘密キーも使用する必要があります。暗号化された秘密鍵を提供する場合は、パスフレーズも提供する必要があります。暗号化された秘密キーを使用すると、キーとパスフレーズを保存する必要があるため、セキュリティ上の大きな利点はありません。簡素化のため、使用可能な場合は、暗号化されていない秘密キーを使用することをお勧めします。

外部**Syslog**サーバーのサイズを見積もる方法

通常、グリッドは、1 秒あたりの S3 操作数または 1 秒あたりのバイト数で定義される必要なスループットを達成できるようにサイズ設定されます。たとえば、グリッドで 1 秒あたり 1,000 件の S3 操作、または 1 秒あたり 2,000 MB のオブジェクトの取り込みと取得を処理する必要があるとします。グリッドのデータ要件に応じて外部 Syslog サーバーのサイズを決定する必要があります。

このセクションでは、外部 Syslog サーバーが処理できる必要があるさまざまなタイプのログ メッセージのレートと平均サイズを、グリッドの既知または望ましいパフォーマンス特性 (1 秒あたりの S3 操作数) に基づいて見積もるのに役立ついくつかのヒューリスティックな式を示します。

推定式で **1** 秒あたりの **S3** 操作を使用する

グリッドのサイズが 1 秒あたりのバイト数で表されるスループットに合わせて設定されている場合、推定式を使用するには、このサイズを 1 秒あたりの S3 操作数に変換する必要があります。グリッド スループットを変換するには、まず平均オブジェクト サイズを決定する必要があります。これは、既存の監査ログとメトリック (存在する場合) の情報を使用するか、 StorageGRID を使用するアプリケーションに関する知識を使用して行うことができます。たとえば、グリッドが 2,000 MB/秒のスループットを実現するようにサイズ設定され、平均オブジェクト サイズが 2 MB の場合、グリッドは 1 秒あたり 1,000 件の S3 操作 (2,000 MB / 2 MB) を処理できるようにサイズ設定されていることになります。

> 次のセクションの外部 Syslog サーバーのサイズ設定の式は、最悪のケースの見積もりではなく、一般的なケースの見積もりを提供します。構成とワークロードによっては、数式で予測されるよりも syslog メッセージの割合や syslog データの量が多くなったり少なくなったりする場合があります。数式はガイドラインとしてのみ使用してください。

監査ログの推定式

グリッドがサポートすると予想される 1 秒あたりの S3 操作の数以外に S3 ワークロードに関する情報がない場合は、監査レベルをデフォルト値 (ストレージを除くすべてのカテゴリを [通常] に設定、ストレージは [エラー] に設定) のままにしておくことを前提として、次の式を使用して外部 syslog サーバーが処理する必要がある監査ログの量を見積もることができます。

```
Audit Log Rate = 2 x S3 Operations Rate
Audit Log Average Size = 800 bytes
```

たとえば、グリッドのサイズが 1 秒あたり 1,000 件の S3 操作に対応している場合、外部 syslog サーバーのサイズは 1 秒あたり 2,000 件の syslog メッセージをサポートするように設定し、1 秒あたり 1.6 MB の速度で監査ログ データを受信 (通常は保存) できる必要があります。

作業負荷について詳しく知っていれば、より正確な見積もりが可能になります。監査ログの場合、最も重要な追加変数は、PUT (GET と比較) である S3 操作の割合と、次の S3 フィールドの平均サイズ (バイト単位) です (表で使用されている 4 文字の略語は監査ログのフィールド名です)。

コード	フィールド	説明
SACC	S3テナントアカウント名（リクエスト送信者）	リクエストを送信したユーザーのテナント アカウントの名前。匿名のリクエストの場合は空です。
SBAC	S3テナントアカウント名（バケット所有者）	バケット所有者のテナント アカウント名。クロスアカウントまたは匿名アクセスを識別するために使用されます。
S3BK	S3バケット	S3 バケット名。
S3KY	S3キー	バケット名を含まない S3 キー名。バケットに対する操作にはこのフィールドは含まれません。

P を使用して、PUT である S3 操作の割合を表します (0 ≤ P ≤ 1) (つまり、100% PUT ワークロードの場合は P = 1、100% GET ワークロードの場合は P = 0)。

K を使用して、S3 アカウント名、S3 バケット、および S3 キーの合計の平均サイズを表します。 S3 アカウント名が常に my-s3-account (13 バイト) であり、バケットの名前が /my/application/bucket-12345 (28 バイト) のような固定長であり、オブジェクトが 5733a5d7-f069-41ef-8fbd-13247494c69c (36 バイト) のような固定長キーを持っているとします。するとKの値は90（13+13+28+36）になります。

P と K の値を決定できる場合は、監査レベルをデフォルト（ストレージを除くすべてのカテゴリを「通常」に設定、ストレージは「エラー」に設定）のままにしておくことを前提として、次の式を使用して外部 syslog サーバーが処理する必要がある監査ログの量を見積もることができます。

```
Audit Log Rate = ((2 x P) + (1 - P)) x S3 Operations Rate
Audit Log Average Size = (570 + K) bytes
```

たとえば、グリッドのサイズが 1 秒あたり 1,000 件の S3 操作に対応し、ワークロードの 50% が PUT であり、S3 アカウント名、バケット名、およびオブジェクト名の平均が 90 バイトである場合、外部 syslog サーバーは 1 秒あたり 1,500 件の syslog メッセージをサポートするサイズに設定し、監査ログ データを 1 秒あたり約 1 MB の速度で受信 (および通常は保存) できる必要があります。

デフォルト以外の監査レベルの推定式

監査ログに提供される数式では、デフォルトの監査レベル設定 (ストレージを除くすべてのカテゴリが [通常] に設定されているが、ストレージは [エラー] に設定されている) を使用することを前提としています。デフォルト以外の監査レベル設定の監査メッセージのレートと平均サイズを見積もるための詳細な数式は利用できません。ただし、次の表を使用して、レートの大まかな見積もりを行うことができます。監査ログに提供されている平均サイズの計算式を使用することもできますが、「追加の」監査メッセージは平均してデフォルトの監査メッセージよりも小さいため、過大な見積もりになる可能性があることに注意してください。

条件	計算式
レプリケーション: 監査レベルはすべてデバッグまたは通常に設定されています	監査ログレート = 8 x S3 操作レート
消去コーディング: 監査レベルはすべてデバッグまたは通常に設定されています	デフォルト設定と同じ式を使用します

セキュリティイベントの推定式

セキュリティ イベントは S3 操作と相関しておらず、通常はごくわずかな量のログとデータが生成されます。これらの理由により、推定式は提供されません。

アプリケーションログの推定式

グリッドがサポートすると予想される 1 秒あたりの S3 操作の数以外に S3 ワークロードに関する情報がない場合は、次の式を使用して、外部 syslog サーバーが処理する必要があるアプリケーション ログの量を見積もることができます。

```
Application Log Rate = 3.3 x S3 Operations Rate
Application Log Average Size = 350 bytes
```

したがって、たとえば、グリッドのサイズが 1 秒あたり 1,000 回の S3 操作に対応している場合、外部 syslog サーバーのサイズは、1 秒あたり 3,300 回のアプリケーション ログをサポートし、1 秒あたり約 1.2 MB の速度でアプリケーション ログ データを受信 (および保存) できるようにする必要があります。

作業負荷について詳しく知っていれば、より正確な見積もりが可能になります。アプリケーション ログの場合、最も重要な追加変数は、データ保護戦略 (レプリケーションと消去コーディング)、PUT である S3 操作の割合 (GET/その他と比較)、および次の S3 フィールドの平均サイズ (バイト単位) です (表で使用されている 4 文字の略語は監査ログ フィールド名です)。

コード	フィールド	説明
SACC	S3テナントアカウント名（リクエスト送信者）	リクエストを送信したユーザーのテナント アカウントの名前。匿名のリクエストの場合は空です。
SBAC	S3テナントアカウント名（バケット所有者）	バケット所有者のテナント アカウント名。クロスアカウントまたは匿名アクセスを識別するために使用されます。
S3BK	S3バケット	S3 バケット名。
S3KY	S3キー	バケット名を含まない S3 キー名。バケットに対する操作にはこのフィールドは含まれません。

このセクションでは、次のデータ保護方法でグリッドの推定式を使用する方法の例について説明します。

- レプリケーション
- イレイジャー コーディング

データ保護のためにレプリケーションを使用する場合

P は、PUT である S3 操作の割合を表します。ここで、0 ≤ P ≤ 1 です (つまり、100% PUT ワークロードの場合は P = 1、100% GET ワークロードの場合は P = 0)。

K は、S3 アカウント名、S3 バケット、および S3 キーの合計の平均サイズを表します。 S3 アカウント名が常に my-s3-account (13 バイト) であり、バケットの名前が /my/application/bucket-12345 (28 バイト) のような固定長であり、オブジェクトが 5733a5d7-f069-41ef-8fbd-13247494c69c (36 バイト) のような固定長キーを持っているとします。するとKの値は90（13+13+28+36）になります。

P と K の値を特定できる場合は、次の式を使用して、外部 syslog サーバーが処理する必要があるアプリケーション ログの量を見積もることができます。

```
Application Log Rate = ((1.1 x P) + (2.5 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (220 + K)) + ((1 - P) x (240 + (0.2 x
K))) Bytes
```

したがって、たとえば、グリッドのサイズが 1 秒あたり 1,000 件の S3 操作に対応し、ワークロードの 50% が PUT であり、S3 アカウント名、バケット名、およびオブジェクト名の平均が 90 バイトである場合、外部 syslog サーバーは 1 秒あたり 1,800 件のアプリケーション ログをサポートするようにサイズ設定する必要があり、0.5 MB/秒の速度でアプリケーション データを受信 (および通常は保存) することになります。

データ保護のために消失訂正符号を使用する場合

P は、PUT である S3 操作の割合を表します。ここで、0 ≤ P ≤ 1 です (つまり、100% PUT ワークロードの場合は P = 1、100% GET ワークロードの場合は P = 0)。

K は、S3 アカウント名、S3 バケット、および S3 キーの合計の平均サイズを表します。 S3 アカウント名が常に my-s3-account (13 バイト) であり、バケットの名前が /my/application/bucket-12345 (28 バイト) のような固定長であり、オブジェクトが 5733a5d7-f069-41ef-8fbd-13247494c69c (36 バイト) のような固定長キーを持っているとします。するとKの値は90（13+13+28+36）になります。

P と K の値を特定できる場合は、次の式を使用して、外部 syslog サーバーが処理する必要があるアプリケーション ログの量を見積もることができます。

```
Application Log Rate = ((3.2 x P) + (1.3 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (240 + (0.4 x K))) + ((1 - P) x (185 +
(0.9 x K))) Bytes
```

したがって、たとえば、グリッドのサイズが 1 秒あたり 1,000 件の S3 操作に対応し、ワークロードの 50% が PUT であり、S3 アカウント名、バケット名、およびオブジェクト名の平均が 90 バイトである場合、外部 syslog サーバーは 1 秒あたり 2,250 件のアプリケーション ログをサポートするサイズに設定し、0.6 MB/秒の

速度でアプリケーション データを受信 (および通常は保存) できる必要があります。

監査メッセージと外部**Syslog**サーバーを構成する

監査メッセージに関連するさまざまな設定を構成できます。記録される監査メッセージの数を調整したり、クライアントの読み取りおよび書き込み監査メッセージに含めるHTTP 要求ヘッダーを定義したり、外部 Syslog サーバーを構成したり、監査ログ、セキュリティ イベント ログ、およびStorageGRIDソフトウェア ログの送信先を指定したりできます。

監査メッセージとログは、システム アクティビティとセキュリティ イベントを記録し、監視とトラブルシューティングに不可欠なツールです。すべてのStorageGRIDノードは、システム アクティビティとイベントを追跡するために監査メッセージとログを生成します。

必要に応じて、監査情報をリモートで保存するように外部 syslog サーバーを構成することもできます。外部サーバーを使用すると、監査データの完全性を低下させることなく、監査メッセージのログ記録によるパフォーマンスへの影響を最小限に抑えることができます。外部 syslog サーバーは、大規模なグリッドがある場合、複数の種類の S3 アプリケーションを使用する場合、またはすべての監査データを保持する場合に特に便利です。見る"監査メッセージと外部Syslogサーバーを構成する"詳細については。

開始する前に

- グリッドマネージャにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは"メンテナンスまたはルートアクセス権限"。
- 外部Syslogサーバーを設定する予定の場合は、"外部Syslogサーバーの使用に関する考慮事項"また、サーバーにログ ファイルを受信して保存するのに十分な容量があることを確認しました。
- TLS または RELP/TLS プロトコルを使用して外部 syslog サーバーを構成する場合は、必要なサーバー CA およびクライアント証明書とクライアント秘密キーが必要です。

監査メッセージのレベルの変更

監査ログ内の次のメッセージ カテゴリごとに異なる監査レベルを設定できます。

監査カテゴリ	デフォルトの設定	詳細情報
システム	平常時	"システム監査メッセージ"
ストレージ	エラー	"オブジェクトストレージ監査メッセージ"
管理	平常時	"経営監査メッセージ"
クライアントが読む	平常時	"クライアント読み取り監査メッセージ"
クライアントが書く	平常時	"クライアント書き込み監査メッセージ"

監査カテゴリ	デフォルトの設定	詳細情報
ILM	平常時	"ILM監査メッセージ"
クロスグリッドレプリケーション	エラー	"CGRR: クロスグリッドレプリケーション要求"

これらのデフォルトは、最初にバージョン 10.3 以降を使用してStorageGRIDをインストールした場合に適用されます。最初にStorageGRIDの以前のバージョンを使用した場合、すべてのカテゴリのデフォルトは [標準] に設定されています。

アップグレード中は、監査レベルの構成はすぐには有効になりません。

手順

1. 構成 > 監視 > 監査および **syslog** サーバー を選択します。
2. 監査メッセージのカテゴリごとに、ドロップダウン リストから監査レベルを選択します。

監査レベル	説明
オフ	このカテゴリからの監査メッセージは記録されません。
エラー	エラー メッセージ (結果コードが「成功」(SUCS) ではなかった監査メッセージ) のみがログに記録されます。
平常時	標準のトランザクション メッセージ (カテゴリのこの手順にリストされているメッセージ) がログに記録されます。
デバッグ	廃止されました。このレベルは、通常の監査レベルと同じように動作します。

特定のレベルに含まれるメッセージには、上位レベルで記録されるメッセージも含まれます。たとえば、通常レベルにはすべてのエラー メッセージが含まれます。

S3 アプリケーションのクライアント読み取り操作の詳細な記録が必要ない場合は、オプションで クライアント読み取り 設定を エラー に変更して、監査ログに記録される監査メッセージの数を減らします。

3. *保存*を選択します。

緑色のバナーは、設定が保存されたことを示します。

HTTPリクエストヘッダーを定義する

オプションで、クライアントの読み取りおよび書き込み監査メッセージに含める HTTP 要求ヘッダーを定義できます。これらのプロトコル ヘッダーは S3 リクエストにのみ適用されます。

手順

1. 監査プロトコル ヘッダー セクションで、クライアントの読み取りおよび書き込み監査メッセージに含める HTTP 要求ヘッダーを定義します。

   0 個以上の文字を一致させるには、アスタリスク (*) をワイルドカードとして使用します。リテラルのアスタリスクと一致させるには、エスケープ シーケンス (*) を使用します。

2. 必要に応じて、「別のヘッダーを追加」* を選択して追加のヘッダーを作成します。

   リクエスト内に HTTP ヘッダーが見つかった場合、それらは監査メッセージの HTRH フィールドの下に含められます。

   > 監査プロトコル要求ヘッダーは、*クライアント読み取り*または*クライアント書き込み*の監査レベルが*オフ*でない場合にのみログに記録されます。

3. *保存*を選択

   緑色のバナーは、設定が保存されたことを示します。

外部**syslog**サーバーを使用する

オプションで、監査ログ、アプリケーション ログ、セキュリティ イベント ログをグリッド外部の場所に保存するように外部 Syslog サーバーを構成することもできます。

> 外部のSyslogサーバーを使用しない場合は、この手順をスキップして、監査情報の送信先を選択する 。

> この手順で利用できる設定オプションが要件を満たすほど柔軟でない場合は、 `audit-destinations`エンドポイントは、"グリッド管理API" 。たとえば、異なるノード グループに異なる syslog サーバーを使用する場合は、API を使用できます。

Syslog情報を入力する

外部 Syslog サーバーの構成ウィザードにアクセスし、 StorageGRID が外部 Syslog サーバーにアクセスするために必要な情報を提供します。

手順

1. 監査および Syslog サーバー ページで、外部 **Syslog** サーバーの構成*を選択します。または、以前に外部 **Syslog** サーバーを設定している場合は、[*外部 **Syslog** サーバーの編集] を選択します。

   外部 Syslog サーバーの構成ウィザードが表示されます。

2. ウィザードの **Syslog** 情報の入力 ステップでは、ホスト フィールドに外部 Syslog サーバーの有効な完全修飾ドメイン名または IPv4 または IPv6 アドレスを入力します。
3. 外部 Syslog サーバーの宛先ポートを入力します (1 ～ 65535 の整数である必要があります)。デフォルトポートは514です。
4. 監査情報を外部 syslog サーバーに送信するために使用するプロトコルを選択します。

   TLS または **RELP/TLS** の使用をお勧めします。これらのいずれかのオプションを使用するには、サーバー証明書をアップロードする必要があります。証明書を使用すると、グリッドと外部 syslog サーバー間

の接続を保護できます。詳細については、以下を参照してください。 "セキュリティ証明書を管理する" 。

すべてのプロトコル オプションには、外部 syslog サーバーによるサポートと構成が必要です。外部 syslog サーバーと互換性のあるオプションを選択する必要があります。

> 信頼性の高いイベント ログ プロトコル (RELP) は、syslog プロトコルの機能を拡張して、イベント メッセージの信頼性の高い配信を実現します。 RELP を使用すると、外部 syslog サーバーを再起動する必要がある場合に監査情報が失われるのを防ぐことができます。

5. *続行*を選択します。
6. **TLS** または **RELP/TLS** を選択した場合は、サーバー CA 証明書、クライアント証明書、およびクライアント秘密キーをアップロードします。
   a. 使用する証明書またはキーについては*参照*を選択します。
   b. 証明書またはキー ファイルを選択します。
   c. ファイルをアップロードするには、[開く] を選択します。

      証明書またはキー ファイル名の横に緑色のチェックが表示され、正常にアップロードされたことが通知されます。
7. *続行*を選択します。

Syslogコンテンツの管理

外部 syslog サーバーに送信する情報を選択できます。

手順

1. ウィザードの **Syslog** コンテンツの管理 ステップで、外部 Syslog サーバーに送信する監査情報の各タイプを選択します。
   - 監査ログを送信: StorageGRIDイベントとシステムアクティビティを送信します
   - セキュリティイベントを送信: 権限のないユーザーがサインインしようとしたときや、ユーザーがルートとしてサインインしたときなどのセキュリティイベントを送信します。
   - アプリケーションログを送信: 送信"StorageGRIDソフトウェア ログ ファイル"次のようなトラブルシューティングに役立ちます:
     - `bycast-err.log`
     - `bycast.log`
     - `jaeger.log`
     - `nms.log`(管理ノードのみ)
     - `prometheus.log`
     - `raft.log`
     - `hagroups.log`
   - アクセス ログの送信: Grid Manager、Tenant Manger、構成されたロード バランサのエンドポイント、およびリモート システムからのグリッド フェデレーション要求への外部要求の HTTP アクセス ログを送信します。

2. ドロップダウン メニューを使用して、送信する監査情報の各カテゴリの重大度と機能 (メッセージの種類) を選択します。

   重大度とファシリティの値を設定すると、カスタマイズ可能な方法でログを集約し、分析を容易にすることができます。

   a. *重大度*では*パススルー*を選択するか、0～7の重大度値を選択します。

      値を選択すると、選択した値がこのタイプのすべてのメッセージに適用されます。重大度を固定値で上書きすると、さまざまな重大度に関する情報が失われます。

重大度	説明
パススルー	外部 syslog に送信される各メッセージには、ノードにローカルに記録されたときと同じ重大度値が設定されます。 • 監査ログの場合、重大度は「情報」です。 • セキュリティ イベントの場合、重大度の値はノード上の Linux ディストリビューションによって生成されます。 • アプリケーション ログの場合、問題の内容に応じて重大度は「情報」と「通知」の間で異なります。たとえば、NTP サーバーを追加して HA グループを構成すると、値は「info」になりますが、SSM または RSM サービスを意図的に停止すると、値は「notice」になります。 • アクセス ログの場合、重大度は「情報」です。
0	緊急事態: システムが使用できません
1	警告: 直ちに行動を起こす必要があります
2	重大: 重大な状態
3	エラー: エラー状態
4	警告: 警告条件
5	通知: 正常だが重大な状態
6	情報: 情報メッセージ
7	デバッグ: デバッグレベルのメッセージ

   b. **Facilty** の場合は、**Passthrough** を選択するか、0 から 23 の間の facility 値を選択します。

      値を選択すると、このタイプのすべてのメッセージに適用されます。 facility を固定値で上書きすると、さまざまな facility に関する情報が失われます。

ファシリティ	説明
パススルー	外部 syslog に送信される各メッセージには、ノードにローカルに記録されたときと同じファシリティ値が設定されます。 • 監査ログの場合、外部 Syslog サーバーに送信される機能は「local7」です。 • セキュリティ イベントの場合、ファシリティ値はノード上の Linux ディストリビューションによって生成されます。 • アプリケーション ログの場合、外部 Syslog サーバーに送信されるアプリケーション ログには次のファシリティ値が設定されます。 ◦ `bycast.log`: ユーザーまたはデーモン ◦ `bycast-err.log`: ユーザー、デーモン、local3、または local4 ◦ `jaeger.log`: ローカル2 ◦ `nms.log`: ローカル3 ◦ `prometheus.log`: ローカル4 ◦ `raft.log`: ローカル5 ◦ `hagroups.log`: ローカル6 • アクセス ログの場合、外部 syslog サーバーに送信される機能は「local0」です。
0	kern（カーネルメッセージ）
1	ユーザー（ユーザーレベルのメッセージ）
2	郵便
3	デーモン（システムデーモン）
4	auth (セキュリティ/承認メッセージ)
5	syslog (syslogd によって内部的に生成されたメッセージ)
6	lpr（ラインプリンターサブシステム）
7	ニュース（ネットワークニュースサブシステム）
8	UUCP
9	cron（クロックデーモン）

ファシリティ	説明
10	セキュリティ（セキュリティ/認証メッセージ）
11	FTP
12	NTP
13	logaudit（ログ監査）
14	logalert（ログアラート）
15	クロック（クロックデーモン）
16	ローカル0
17	ローカル1
18	ローカル2
19	ローカル3
20	ローカル4
21	ローカル5
22	ローカル6
23	ローカル7

3. *続行*を選択します。

テストメッセージを送信する

外部 Syslog サーバーの使用を開始する前に、グリッド内のすべてのノードが外部 Syslog サーバーにテストメッセージを送信するように要求する必要があります。外部 syslog サーバーにデータを送信する前に、これらのテスト メッセージを使用して、ログ収集インフラストラクチャ全体を検証する必要があります。

外部 Syslog サーバーがグリッド内の各ノードからテスト メッセージを受信し、メッセージが期待どおりに処理されたことを確認するまで、外部 Syslog サーバーの構成を使用しないでください。

手順

1. 外部 syslog サーバーが適切に構成されており、グリッド内のすべてのノードから監査情報を受信できることが確実なため、テスト メッセージを送信したくない場合は、[スキップして終了] を選択します。

緑色のバナーは、設定が保存されたことを示します。

2. それ以外の場合は、[テスト メッセージを送信] を選択します (推奨)。

   テストを停止するまで、テスト結果はページに継続的に表示されます。テストの進行中は、監査メッセージは以前に設定した送信先に引き続き送信されます。

3. Syslog サーバーの構成中または実行時にエラーが発生した場合は、エラーを修正して、テスト メッセージの送信 を再度選択してください。

   見る"外部 syslog サーバーのトラブルシューティング"エラーを解決するのに役立ちます。

4. すべてのノードがテストに合格したことを示す緑色のバナーが表示されるまで待ちます。
5. Syslog サーバーをチェックして、テスト メッセージが期待どおりに受信され、処理されているかどうかを確認します。

   UDP を使用している場合は、ログ収集インフラストラクチャ全体を確認してください。UDP プロトコルでは、他のプロトコルほど厳密なエラー検出はできません。

6. *停止して終了*を選択します。

   監査および **syslog** サーバー ページに戻ります。緑色のバナーは、Syslog サーバーの構成が保存されたことを示します。

   外部 Syslog サーバを含む宛先を選択するまで、 StorageGRID監査情報は外部 Syslog サーバに送信されません。

監査情報の送信先を選択する

監査ログ、セキュリティイベントログ、"StorageGRIDソフトウェアログ"送信されます。

StorageGRIDはデフォルトでローカルノードの監査先を設定し、監査情報を `/var/local/log/localaudit.log`。

使用する場合 `/var/local/log/localaudit.log`、グリッド マネージャおよびテナント マネージャの監査ログ エントリがストレージ ノードに送信される場合があります。どのノードに最新のエントリがあるかは、 `run-each-node --parallel "zgrep MGAU /var/local/log/localaudit.log | tail"`指示。

一部の宛先は、外部 Syslog サーバーが設定されている場合にのみ使用できます。

手順

1. 「監査および Syslog サーバー」ページで、監査情報の送信先を選択します。

   通常、ローカル ノードのみ と 外部 **syslog** サーバー の方がパフォーマンスが向上します。

オプション	説明
ローカルノードのみ（デフォルト）	監査メッセージ、セキュリティ イベント ログ、アプリケーション ログは管理ノードに送信されません。代わりに、それらはそれを生成したノード (「ローカル ノード」) にのみ保存されます。各ローカルノードで生成された監査情報は、`/var/local/log/localaudit.log` 。 注: StorageGRID は、スペースを解放するために、定期的にローカル ログをローテーションで削除します。ノードのログ ファイルが 1 GB に達すると、既存のファイルが保存され、新しいログ ファイルが開始されます。ログのローテーション制限は 21 ファイルです。ログ ファイルの 22 番目のバージョンが作成されると、最も古いログ ファイルが削除されます。平均して、各ノードには約 20 GB のログ データが保存されます。
管理ノード/ローカルノード	監査メッセージは管理ノードの監査ログに送信され、セキュリティ イベント ログとアプリケーション ログはそれらを生成したノードに保存されます。監査情報は次のファイルに保存されます。 • 管理ノード (プライマリおよび非プライマリ): `/var/local/audit/export/audit.log` • すべてのノード: `/var/local/log/localaudit.log`通常、ファイルは空であるか、存在しません。一部のメッセージの追加コピーなどの二次情報が含まれる場合があります。
外部 syslog サーバー	監査情報は外部のSyslogサーバーに送信され、ローカルノードに保存されます。(`/var/local/log/localaudit.log` ）。送信される情報の種類は、外部 Syslog サーバーの設定方法によって異なります。このオプションは、外部 Syslog サーバーを構成した後にのみ有効になります。
管理ノードと外部Syslogサーバー	監査メッセージは監査ログに送信されます (`/var/local/audit/export/audit.log`）が管理ノード上に作成され、監査情報は外部のSyslogサーバーに送信され、ローカルノードに保存されます。(`/var/local/log/localaudit.log` ）。送信される情報の種類は、外部 Syslog サーバーの設定方法によって異なります。このオプションは、外部 Syslog サーバーを構成した後にのみ有効になります。

2. *保存*を選択します。

   警告メッセージが表示されます。

3. 監査情報の保存先を変更することを確認するには、[**OK**] を選択します。

   緑色のバナーは、監査構成が保存されたことを示します。

   新しいログは選択した宛先に送信されます。既存のログは現在の場所に残ります。

SNMP監視を使用する

SNMP監視を使用する

簡易ネットワーク管理プロトコル (SNMP) を使用してStorageGRID を監視する場合は、StorageGRIDに含まれている SNMP エージェントを構成する必要があります。

- "SNMPエージェントを構成する"
- "SNMPエージェントを更新する"

機能

各StorageGRIDノードは、MIB を提供する SNMP エージェントまたはデーモンを実行します。 StorageGRID MIB には、アラートのテーブルと通知の定義が含まれています。 MIB には、各ノードのプラットフォームやモデル番号などのシステム記述情報も含まれています。各StorageGRIDノードは、MIB-II オブジェクトのサブセットもサポートします。

見る"MIBファイルにアクセスする"グリッド ノードに MIB ファイルをダウンロードする場合。

最初は、すべてのノードで SNMP が無効になっています。 SNMP エージェントを構成すると、すべてのStorageGRIDノードは同じ構成を受け取ります。

StorageGRID SNMP エージェントは、SNMP プロトコルの 3 つのバージョンすべてをサポートします。クエリに対して読み取り専用の MIB アクセスを提供し、管理システムに 2 種類のイベント駆動型通知を送信できます。

罠

トラップは、管理システムによる確認を必要としない、SNMP エージェントによって送信される通知です。トラップは、アラートがトリガーされるなど、 StorageGRID内で何かが発生したことを管理システムに通知するために使用されます。

トラップは、SNMP の 3 つのバージョンすべてでサポートされています。

通知する

インフォームはトラップに似ていますが、管理システムによる確認が必要です。 SNMP エージェントが一定時間内に確認応答を受信しない場合、確認応答を受信するか最大再試行値に達するまで、情報を再送信します。

インフォームは、SNMPv2c および SNMPv3 でサポートされています。

トラップ通知とインフォーム通知は、次の場合に送信されます。

- デフォルトまたはカスタムのアラートは、どの重大度レベルでもトリガーされます。アラートのSNMP通知を抑制するには、"サイレンスを設定する"警告のため。アラート通知は、"優先送信者管理ノード" 。

  各アラートは、アラートの重大度レベルに基づいて、activeMinorAlert、activeMajorAlert 、activeCriticalAlert の 3 つのトラップ タイプのいずれかにマッピングされます。これらのトラップを作動させる可能性のあるアラートのリストについては、"アラート一覧" 。

SNMPバージョンのサポート

この表には、各 SNMP バージョンでサポートされている内容の概要が示されています。

	SNMPv1	**SNMPv2c**	**SNMPv3**
クエリ （GETとGETNEXT）	読み取り専用MIBクエリ	読み取り専用MIBクエリ	読み取り専用MIBクエリ
クエリ認証	コミュニティ文字列	コミュニティ文字列	ユーザーベースセキュリティモデル（USM）ユーザー
通知 （トラップと情報）	トラップのみ	罠と情報	罠と情報
通知認証	デフォルトのトラップコミュニティまたは各トラップ宛先のカスタムコミュニティ文字列	デフォルトのトラップコミュニティまたは各トラップ宛先のカスタムコミュニティ文字列	各トラップ宛先のUSMユーザー

制限事項

- StorageGRID は読み取り専用の MIB アクセスをサポートします。読み取り/書き込みアクセスはサポートされていません。
- グリッド内のすべてのノードは同じ構成を受け取ります。
- SNMPv3: StorageGRID はトランスポート サポート モード (TSM) をサポートしていません。
- SNMPv3: サポートされる認証プロトコルは SHA (HMAC-SHA-96) のみです。
- SNMPv3: サポートされている唯一のプライバシー プロトコルは AES です。

SNMPエージェントを構成する

読み取り専用の MIB アクセスと通知にサードパーティの SNMP 管理システムを使用するようにStorageGRID SNMP エージェントを設定できます。

開始する前に

- グリッドマネージャにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは"ルートアクセス権限"。

タスク概要

StorageGRID SNMP エージェントは、SNMPv1、SNMPv2c、および SNMPv3 をサポートします。エージェントを 1 つ以上のバージョンに対して構成できます。 SNMPv3 では、ユーザー セキュリティ モデル (USM) 認証のみがサポートされます。

グリッド内のすべてのノードは同じ SNMP 構成を使用します。

基本設定を指定する

最初のステップとして、 StorageGRID SMNP エージェントを有効にし、基本情報を提供します。

手順

1. 構成 > 監視 > **SNMP** エージェント を選択します。

   SNMP エージェント ページが表示されます。

2. すべてのグリッド ノードで SNMP エージェントを有効にするには、[**SNMP** を有効にする] チェックボックスをオンにします。
3. 基本設定セクションに次の情報を入力します。

フィールド	説明
システム連絡先	オプション。 StorageGRIDシステムの主な連絡先。SNMP メッセージでは sysContact として返されます。 システム連絡先は通常、電子メール アドレスです。この値は、StorageGRIDシステム内のすべてのノードに適用されます。 システム連絡先 は最大 255 文字までです。
システムの場所	オプション。 StorageGRIDシステムの場所。SNMP メッセージでは sysLocation として返されます。 システムの場所には、 StorageGRIDシステムの場所を識別するのに役立つ任意の情報を指定できます。たとえば、施設の住所を使用する場合があります。この値は、 StorageGRIDシステム内のすべてのノードに適用されます。 システムの場所 は最大 255 文字までです。
SNMPエージェント通知を有効にする	• 選択すると、 StorageGRID SNMP エージェントはトラップ通知とインフォーム通知を送信します。 • 選択されていない場合、SNMP エージェントは読み取り専用の MIB アクセスをサポートしますが、SNMP 通知は送信しません。
認証トラップを有効にする	選択すると、 StorageGRID SNMP エージェントは、不適切に認証されたプロトコル メッセージを受信した場合に認証トラップを送信します。

コミュニティ文字列を入力してください

SNMPv1 または SNMPv2c を使用する場合は、コミュニティ文字列セクションを入力します。

管理システムがStorageGRID MIB を照会すると、コミュニティ文字列が送信されます。コミュニティ文字列がここで指定された値のいずれかと一致する場合、SNMP エージェントは管理システムに応答を送信します。

手順

1. 読み取り専用コミュニティ の場合は、オプションでコミュニティ文字列を入力して、IPv4 および IPv6 エージェント アドレスでの読み取り専用 MIB アクセスを許可します。

   StorageGRIDシステムのセキュリティを確保するには、コミュニティ文字列として「public」を使用しないでください。このフィールドを空白のままにすると、SNMP エージェントはコミュニティ文字列としてStorageGRIDシステムのグリッド ID を使用します。

   各コミュニティ文字列は最大 32 文字で、空白文字を含めることはできません。

2. 追加の文字列を追加するには、「別のコミュニティ文字列を追加」を選択します。

   最大 5 つの文字列が許可されます。

トラップ先を作成する

[その他の構成] セクションの [トラップの送信先] タブを使用して、 StorageGRIDトラップまたはインフォーム通知の 1 つ以上の送信先を定義します。 SNMP エージェントを有効にして [保存] を選択すると、アラートがトリガーされたときにStorageGRID は定義済みの各宛先に通知を送信します。サポートされている MIB-II エンティティ (ifDown や coldStart など) についても標準通知が送信されます。

手順

1. デフォルトのトラップ コミュニティ フィールドに、必要に応じて、SNMPv1 または SNMPv2 トラップの宛先に使用するデフォルトのコミュニティ文字列を入力します。

   必要に応じて、特定のトラップの宛先を定義するときに、異なる (「カスタム」) コミュニティ文字列を指定できます。

   デフォルトのトラップ コミュニティ は最大 32 文字で、空白文字を含めることはできません。

2. トラップの宛先を追加するには、[作成] を選択します。
3. このトラップの宛先に使用する SNMP バージョンを選択します。
4. 選択したバージョンのトラップ宛先の作成フォームに入力します。

SNMPv1

バージョンとして SNMPv1 を選択した場合は、これらのフィールドに入力します。

フィールド	説明
タイプ	SNMPv1 の場合はトラップである必要があります。
ホスト	トラップを受信するための IPv4 または IPv6 アドレス、あるいは完全修飾ドメイン名 (FQDN)。
ポート	別の値を使用する必要がない限り、SNMP トラップの標準ポートである 162 を使用します。
プロトコル	TCP を使用する必要がない限り、標準の SNMP トラップ プロトコルである UDP を使用します。
コミュニティ文字列	デフォルトのトラップ コミュニティが指定されている場合はそれを使用するか、このトラップの宛先にカスタム コミュニティ文字列を入力します。 カスタム コミュニティ文字列は最大 32 文字までで、空白を含めることはできません。

SNMPv2c

バージョンとして SNMPv2c を選択した場合は、これらのフィールドに入力します。

フィールド	説明
タイプ	宛先がトラップまたはインフォームに使用されるかどうか。
ホスト	トラップを受信する IPv4 または IPv6 アドレスまたは FQDN。
ポート	別の値を使用する必要がない限り、SNMP トラップの標準ポートである 162 を使用します。
プロトコル	TCP を使用する必要がない限り、標準の SNMP トラップ プロトコルである UDP を使用します。
コミュニティ文字列	デフォルトのトラップ コミュニティが指定されている場合はそれを使用するか、このトラップの宛先にカスタム コミュニティ文字列を入力します。 カスタム コミュニティ文字列は最大 32 文字までで、空白を含めることはできません。

SNMPv3

バージョンとして SNMPv3 を選択した場合は、これらのフィールドに入力します。

フィールド	説明
タイプ	宛先がトラップまたはインフォームに使用されるかどうか。
ホスト	トラップを受信する IPv4 または IPv6 アドレスまたは FQDN。
ポート	別の値を使用する必要がない限り、SNMP トラップの標準ポートである 162 を使用します。
プロトコル	TCP を使用する必要がない限り、標準の SNMP トラップ プロトコルである UDP を使用します。
USMユーザ	認証に使用される USM ユーザー。 • **Trap** を選択した場合は、権限のあるエンジン ID を持たない USM ユーザーのみが表示されます。 • **Inform** を選択した場合は、権限のあるエンジン ID を持つ USM ユーザーのみが表示されます。 • ユーザーが表示されない場合: i. トラップの宛先を作成して保存します。 ii. へ移動USMユーザーを作成するユーザーを作成します。 iii. トラップの宛先タブに戻り、テーブルから保存した宛先を選択して、*編集*を選択します。 iv. ユーザーを選択します。

5. *作成*を選択します。

   トラップの宛先が作成され、テーブルに追加されます。

エージェントアドレスを作成する

必要に応じて、[その他の構成] セクションの [エージェント アドレス] タブを使用して、1 つ以上の「リスニング アドレス」を指定します。これらは、SNMP エージェントがクエリを受信できるStorageGRIDアドレスです。

エージェント アドレスを設定しない場合、デフォルトのリスニング アドレスはすべてのStorageGRIDネットワーク上の UDP ポート 161 になります。

手順

1. *作成*を選択します。
2. 以下の情報を入力してください。

フィールド	説明
インターネットプロトコル	このアドレスが IPv4 を使用するか IPv6 を使用するかを指定します。 デフォルトでは、SNMP は IPv4 を使用します。
転送プロトコル	このアドレスが UDP を使用するか TCP を使用するかを指定します。 デフォルトでは、SNMP は UDP を使用します。
StorageGRIDネットワーク	エージェントがリッスンするStorageGRIDネットワーク。 • グリッド、管理、およびクライアント ネットワーク: SNMP エージェントは、3 つのネットワークすべてでクエリをリッスンします。 • グリッド ネットワーク • 管理者ネットワーク • クライアント ネットワーク 注意: 安全でないデータにクライアント ネットワークを使用し、クライアント ネットワークのエージェント アドレスを作成する場合は、SNMP トラフィックも安全でないことに注意してください。
ポート	オプションで、SNMP エージェントがリッスンするポート番号。 SNMP エージェントのデフォルトの UDP ポートは 161 ですが、未使用のポート番号を入力できます。 注: SNMP エージェントを保存すると、 StorageGRID は内部ファイアウォール上のエージェント アドレス ポートを自動的に開きます。外部ファイアウォールがこれらのポートへのアクセスを許可していることを確認する必要があります。

3. *作成*を選択します。

   エージェント アドレスが作成され、テーブルに追加されます。

USMユーザーを作成する

SNMPv3 を使用している場合は、[その他の構成] セクションの [USM ユーザー] タブを使用して、MIB を照会したり、トラップやインフォームを受信したりする権限を持つ USM ユーザーを定義します。

> SNMPv3 *inform* 宛先には、エンジン ID を持つユーザーが必要です。 SNMPv3 *trap* の宛先には、エンジン ID を持つユーザーを指定できません。

SNMPv1 または SNMPv2c のみを使用している場合、これらの手順は適用されません。

手順

1. *作成*を選択します。
2. 以下の情報を入力してください。

フィールド	説明
ユーザー名	この USM ユーザーの一意の名前。 ユーザー名は最大 32 文字までで、空白文字を含めることはできません。ユーザーの作成後はユーザー名を変更できません。
読み取り専用MIBアクセス	選択すると、このユーザーには MIB への読み取り専用アクセス権が与えられます。
権限のあるエンジンID	このユーザーが通知先で使用される場合、このユーザーの権限のあるエンジン ID。 スペースなしで 10 ～ 64 文字 (5 ～ 32 バイト) の 16 進文字を入力します。この値は、通知のトラップ送信先で選択される USM ユーザーに必要です。この値は、トラップのトラップ送信先で選択される USM ユーザーには許可されません。 注意: 読み取り専用 MIB アクセスを持つ USM ユーザーはエンジン ID を持つことができないため、読み取り専用 **MIB** アクセス を選択した場合、このフィールドは表示されません。
セキュリティレベル	USM ユーザーのセキュリティ レベル: • **authPriv**: このユーザーは認証とプライバシー (暗号化) を使用して通信します。認証プロトコルとパスワード、およびプライバシー プロトコルとパスワードを指定する必要があります。 • **authNoPriv**: このユーザーは認証あり、プライバシーなし (暗号化なし) で通信します。認証プロトコルとパスワードを指定する必要があります。
認証プロトコル	常に、唯一サポートされているプロトコルである SHA (HMAC-SHA-96) に設定されます。
パスワード	このユーザーが認証に使用するパスワード。
プライバシー プロトコル	**authPriv** を選択し、常に AES に設定した場合にのみ表示されます。AES は、唯一サポートされているプライバシー プロトコルです。
パスワード	**authPriv** を選択した場合にのみ表示されます。このユーザーがプライバシーのために使用されるパスワード。

3. *作成*を選択します。

   USM ユーザーが作成され、テーブルに追加されます。

4. SNMP エージェントの設定が完了したら、[保存] を選択します。

   新しい SNMP エージェント構成がアクティブになります。

SNMPエージェントを更新する

SNMP 通知を無効にしたり、コミュニティ文字列を更新したり、エージェント アドレス、USM ユーザー、トラップの送信先を追加または削除したりできます。

開始する前に

- グリッドマネージャにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは"ルートアクセス権限"。

タスク概要

見る"SNMPエージェントを構成する"SNMP エージェント ページの各フィールドの詳細については、こちらをご覧ください。各タブで行った変更を確定するには、ページの下部にある [保存] を選択する必要があります。

手順

1. 構成 > 監視 > **SNMP** エージェント を選択します。

   SNMP エージェント ページが表示されます。

2. すべてのグリッド ノードで SNMP エージェントを無効にするには、[SNMP を有効にする] チェックボックスをオフにし、[保存] を選択します。

   SNMP エージェントを再度有効にすると、以前の SNMP 構成設定はすべて保持されます。

3. 必要に応じて、基本構成セクションの情報を更新します。

   a. 必要に応じて、*システムの連絡先*と*システムの場所*を更新します。

   b. 必要に応じて、[SNMP エージェント通知を有効にする] チェックボックスをオンまたはオフにして、StorageGRID SNMP エージェントがトラップ通知とインフォーム通知を送信するかどうかを制御します。

      このチェックボックスをオフにすると、SNMP エージェントは読み取り専用の MIB アクセスをサポートしますが、SNMP 通知は送信しません。

   c. オプションで、[認証トラップを有効にする] チェックボックスをオンまたはオフにして、StorageGRID SNMP エージェントが不適切に認証されたプロトコル メッセージを受信したときに認証トラップを送信するかどうかを制御します。

4. SNMPv1 または SNMPv2c を使用する場合は、必要に応じて、コミュニティ文字列セクションで 読み取り専用コミュニティ を更新または追加します。

5. トラップの送信先を更新するには、[その他の構成] セクションの [トラップの送信先] タブを選択します。

   このタブを使用して、 StorageGRIDトラップまたはインフォーム通知の 1 つ以上の宛先を定義します。

SNMP エージェントを有効にして [保存] を選択すると、アラートがトリガーされたときにStorageGRIDは定義済みの各宛先に通知を送信します。サポートされている MIB-II エンティティ (ifDown や coldStart など) についても標準通知が送信されます。

入力内容の詳細については、"トラップ先を作成する" 。

- 必要に応じて、デフォルトのトラップ コミュニティを更新または削除します。

  デフォルトのトラップ コミュニティを削除する場合は、まず既存のトラップの送信先でカスタム コミュニティ文字列が使用されていることを確認する必要があります。

- トラップの宛先を追加するには、[作成] を選択します。
- トラップの宛先を編集するには、ラジオ ボタンを選択し、[編集] を選択します。
- トラップの宛先を削除するには、ラジオ ボタンを選択し、[削除] を選択します。
- 変更を確定するには、ページの下部にある [保存] を選択します。

6. エージェント アドレスを更新するには、[その他の構成] セクションの [エージェント アドレス] タブを選択します。

   このタブを使用して、1 つ以上の「リスニング アドレス」を指定します。これらは、SNMP エージェントがクエリを受信できるStorageGRIDアドレスです。

   入力内容の詳細については、"エージェントアドレスを作成する" 。

   - エージェント アドレスを追加するには、[作成] を選択します。
   - エージェント アドレスを編集するには、ラジオ ボタンを選択し、[編集] を選択します。
   - エージェント アドレスを削除するには、ラジオ ボタンを選択し、[削除] を選択します。
   - 変更を確定するには、ページの下部にある [保存] を選択します。

7. USM ユーザーを更新するには、[その他の構成] セクションで [USM ユーザー] タブを選択します。

   このタブを使用して、MIB を照会したり、トラップやインフォームを受信したりする権限を持つ USM ユーザーを定義します。

   入力内容の詳細については、"USMユーザーを作成する" 。

   - USM ユーザーを追加するには、[作成] を選択します。
   - USM ユーザーを編集するには、ラジオ ボタンを選択し、[編集] を選択します。

     既存の USM ユーザーのユーザー名は変更できません。ユーザー名を変更する必要がある場合は、ユーザーを削除して新しいユーザーを作成する必要があります。

     > ユーザーの権限のあるエンジン ID を追加または削除し、そのユーザーが現在宛先に選択されている場合は、宛先を編集または削除する必要があります。そうしないと、SNMP エージェント構成を保存するときに検証エラーが発生します。

   - USM ユーザーを削除するには、ラジオ ボタンを選択し、[削除] を選択します。

削除したユーザーが現在トラップの送信先として選択されている場合は、送信先を編集または削除する必要があります。そうしないと、SNMP エージェント構成を保存するときに検証エラーが発生します。

- 変更を確定するには、ページの下部にある [保存] を選択します。

8. SNMP エージェントの設定を更新したら、[保存] を選択します。

MIBファイルにアクセスする

MIB ファイルには、グリッド内のノードの管理対象リソースとサービスのプロパティに関する定義と情報が含まれています。 StorageGRIDのオブジェクトと通知を定義するMIB ファイルにアクセスできます。これらのファイルはグリッドを監視するのに役立ちます。

見る"SNMP監視を使用する"SNMP および MIB ファイルの詳細については、こちらをご覧ください。

MIBファイルにアクセスする

MIB ファイルにアクセスするには、次の手順に従います。

手順

1. 構成 > 監視 > **SNMP** エージェント を選択します。
2. SNMP エージェント ページで、ダウンロードするファイルを選択します。
   - **NETAPP-STORAGEGRID-MIB.txt**: すべての管理ノードでアクセス可能なアラート テーブルと通知 (トラップ) を定義します。
   - **ES-NETAPP-06-MIB.mib**: E シリーズ ベースのアプライアンスのオブジェクトと通知を定義します。
   - **MIB_1_10.zip**: BMCインターフェースを備えたアプライアンスのオブジェクトと通知を定義します。

     任意のStorageGRIDノード上の次の場所にある MIB ファイルにアクセスすることもできます。 `/usr/share/snmp/mibs`

3. MIB ファイルからStorageGRID OID を抽出するには:
   a. StorageGRID MIB のルートの OID を取得します。

   ```
   root@user-adm1:~ # snmptranslate -On -IR storagegrid
   ```

   結果： `.1.3.6.1.4.1.789.28669` (`28669`は常にStorageGRIDのOIDです)

   a. ツリー全体でStorageGRID OIDをGrepします（ `paste`線を結合する):

   ```
   root@user-adm1:~ # snmptranslate -Tso | paste -d " " - - | grep 28669
   ```

その `snmptranslate`コマンドには、MIB の調査に役立つ多くのオプションがあります。このコマンドは、どのStorageGRIDノードでも使用できます。

MIBファイルの内容

すべてのオブジェクトはStorageGRID OID の下にあります。

オブジェクト名	オブジェクト**ID (OID)**	説明
		NetApp StorageGRIDエンティティの MIB モジュール。

MIBオブジェクト

オブジェクト名	オブジェクト**ID (OID)**	説明
アクティブアラートカウント		activeAlertTable 内のアクティブなアラートの数。
アクティブアラートテーブル		StorageGRID内のアクティブなアラートの表。
アクティブアラートID		アラートの ID。現在アクティブなアラートのセット内でのみ一意です。
アクティブアラート名		アラートの名前。
アクティブアラートインスタンス		アラートを生成したエンティティの名前。通常はノード名です。
アクティブアラート重大度		アラートの重大度。
アクティブアラート開始時間		アラートがトリガーされた日時。

通知の種類（トラップ）

すべての通知には、varbind として次の変数が含まれます。

- アクティブアラートID
- アクティブアラート名
- アクティブアラートインスタンス
- アクティブアラート重大度
- アクティブアラート開始時間

通知の種類	オブジェクトID (OID)	説明
アクティブマイナーアラート		軽微な重大度のアラート
アクティブな重大警報		重大な重大度の警報
アクティブなクリティカルアラート		重大な重大度のアラート

追加のStorageGRIDデータを収集する

チャートやグラフを使う

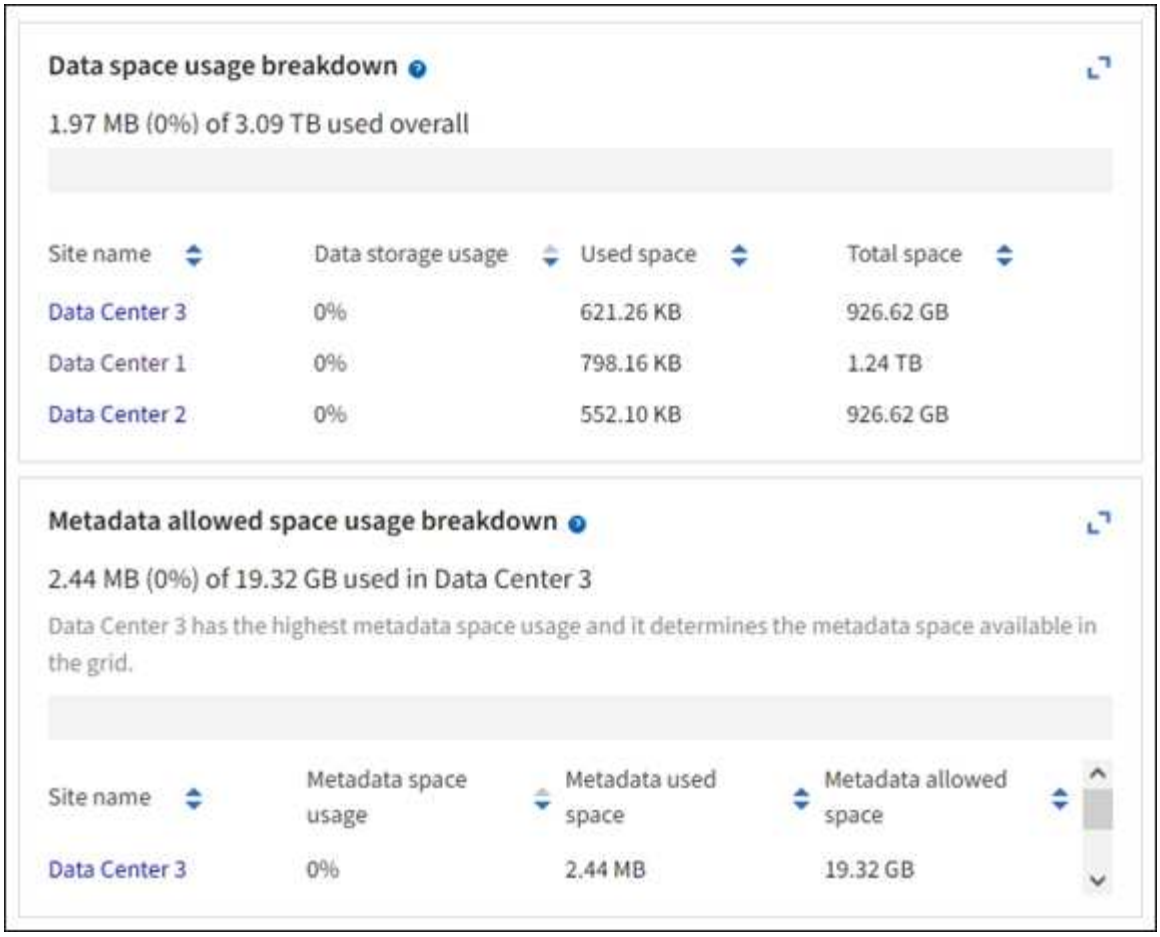
グラフとレポートを使用して、 StorageGRIDシステムの状態を監視し、問題をトラブルシューティングできます。

> グリッド マネージャーはリリースごとに更新されるため、このページのサンプルのスクリーンショットと一致しない場合があります。

チャートの種類

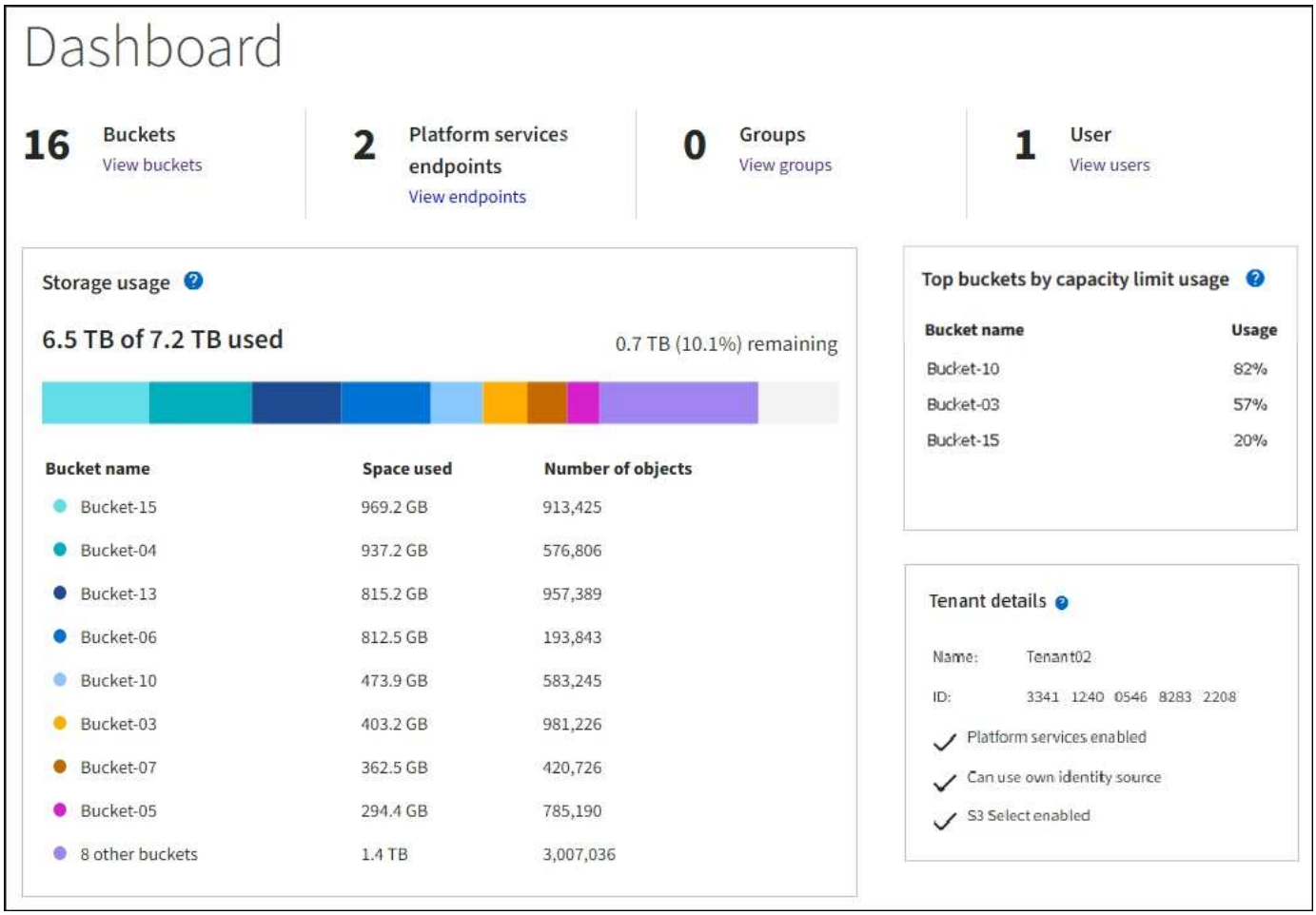
チャートとグラフは、特定のStorageGRIDメトリックと属性の値を要約します。

グリッド マネージャー ダッシュボードには、グリッドと各サイトで使用可能なストレージをまとめたカードが含まれています。



テナント マネージャー ダッシュボードのストレージ使用量パネルには、次の情報が表示されます。

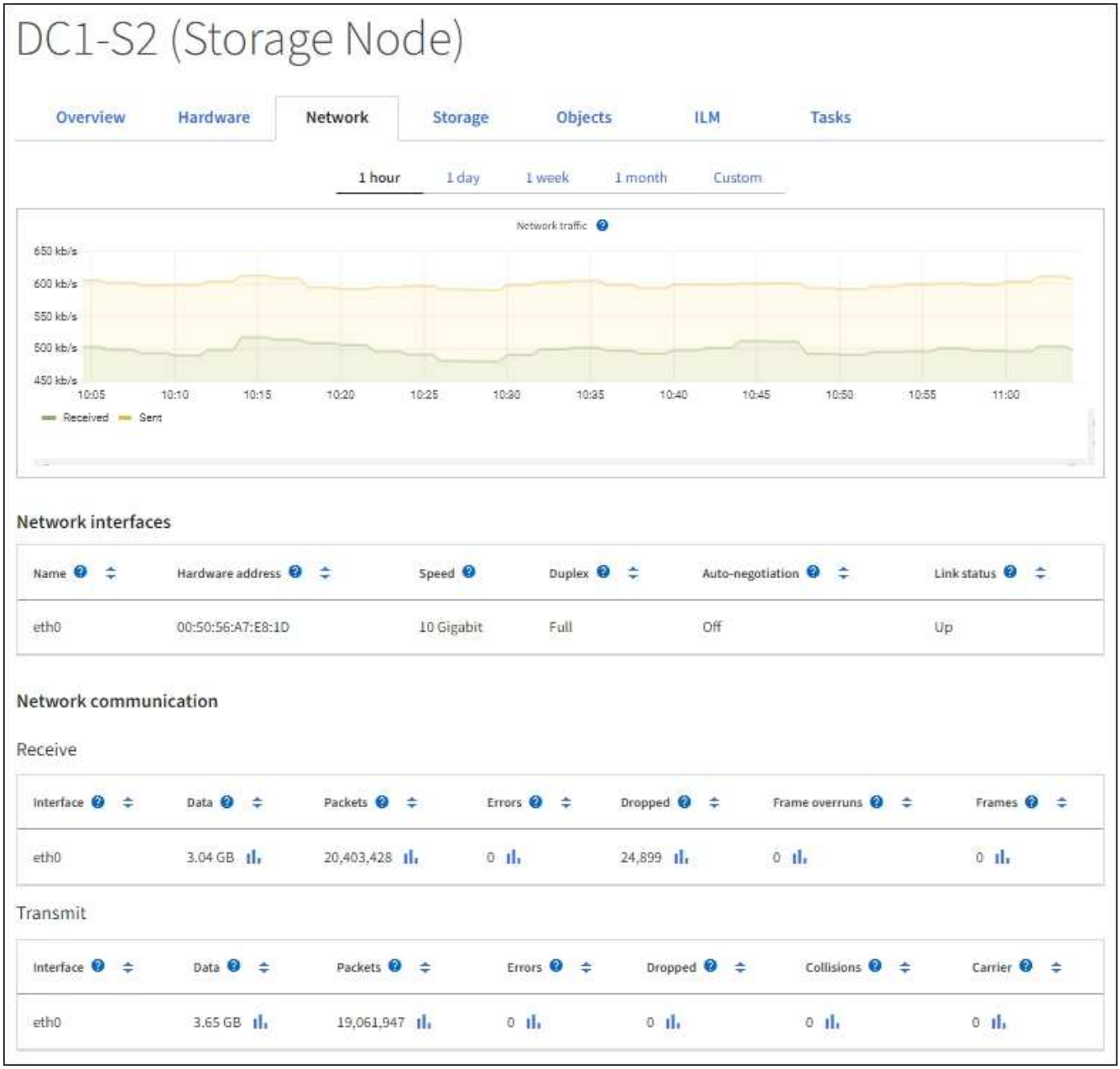
- テナントの最大のバケット（S3）またはコンテナ（Swift）のリスト
- 最大のバケツまたはコンテナの相対的なサイズを表す棒グラフ
- 使用されているスペースの合計量、およびクォータが設定されている場合は、残りのスペースの量と割合



さらに、 StorageGRIDメトリックと属性が時間の経過とともにどのように変化するかを示すグラフは、[ノード] ページと [サポート] > [ツール] > [グリッド トポロジ] ページから入手できます。

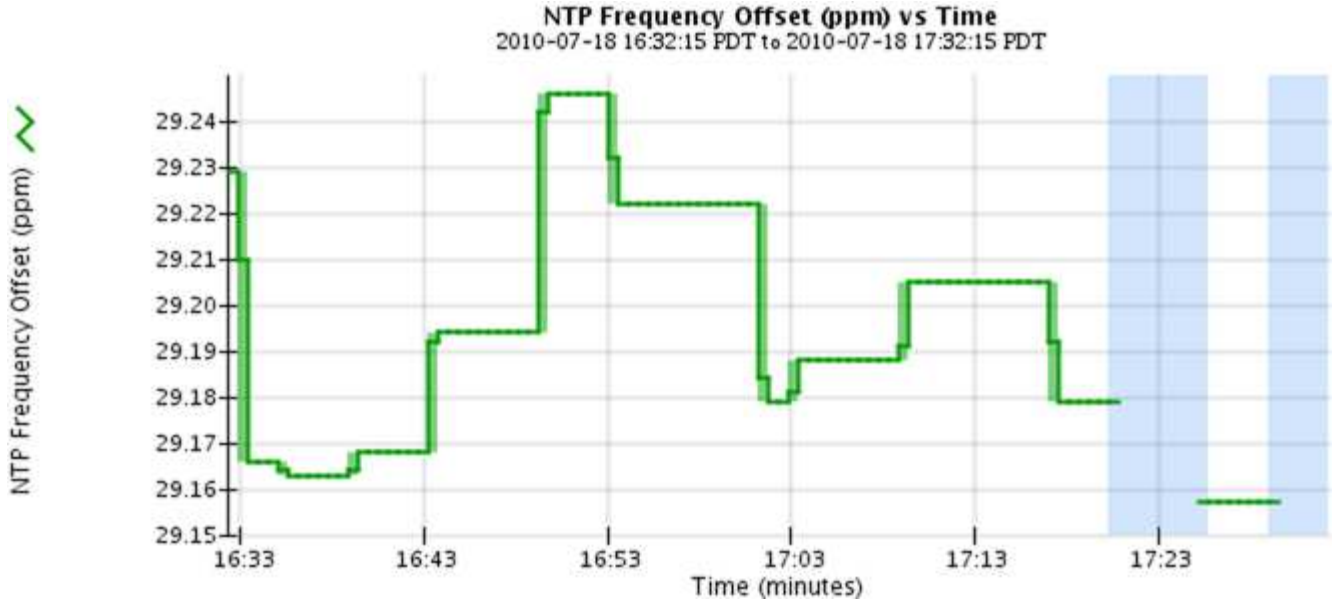
グラフには次の 4 つの種類があります。

- **Grafana** チャート: ノード ページに表示される Grafana チャートは、時間の経過に伴う Prometheus メトリックの値をプロットするために使用されます。たとえば、ストレージ ノードの **NODES** > **Network** タブには、ネットワーク トラフィックの Grafana チャートが含まれています。

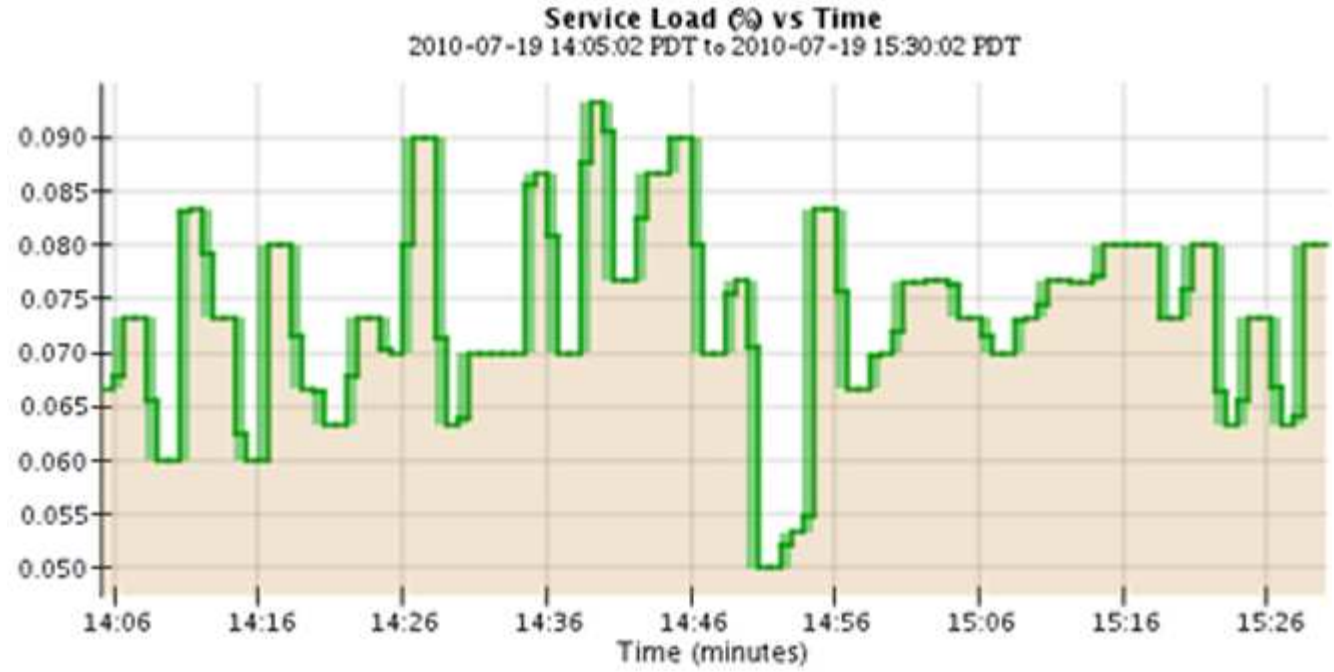


Grafana チャートは、サポート > ツール > メトリック ページから利用できる事前構築されたダッシュボードにも含まれています。

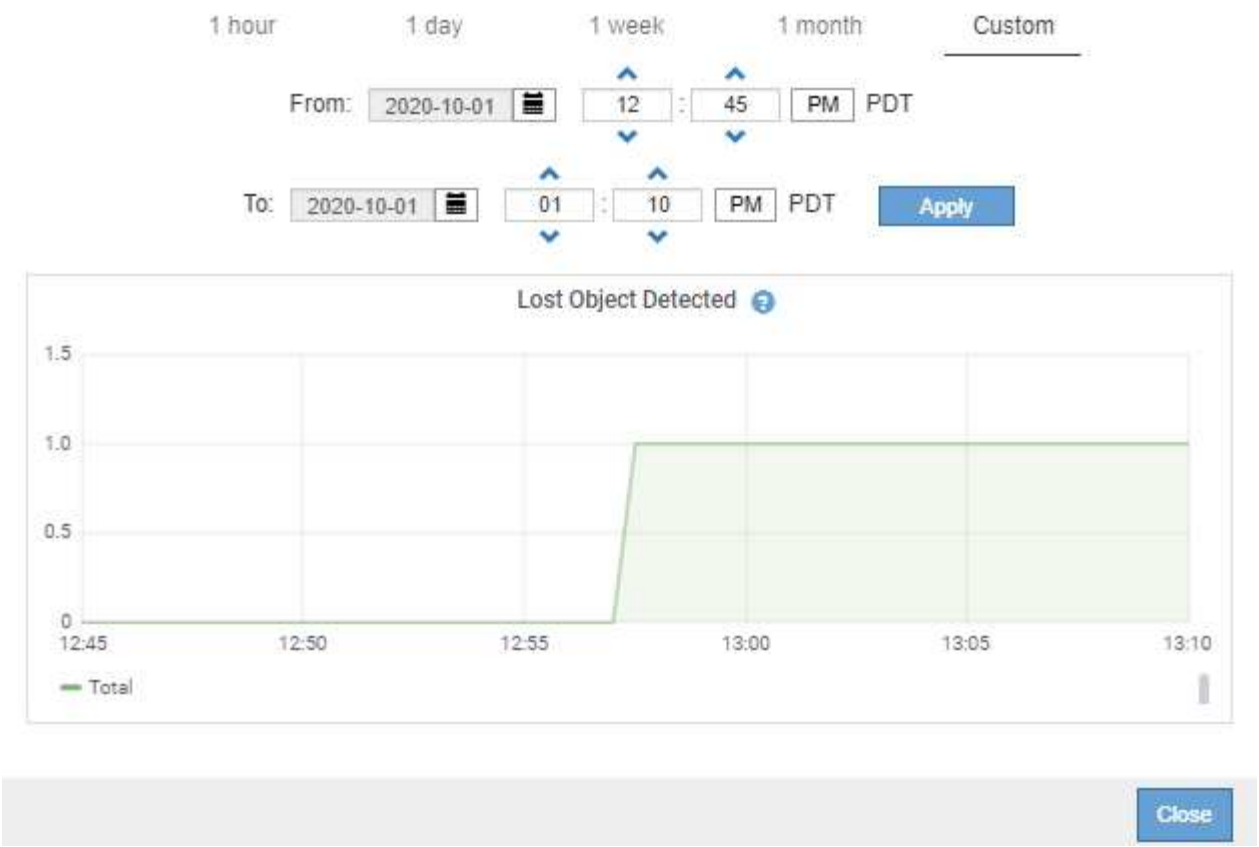
- 折れ線グラフ: ノードページおよび*サポート* > ツール > *グリッドトポロジ*ページから利用できます（グラフアイコンを選択）折れ線グラフは、データ値の後に続く単位値 (NTP 周波数オフセット (ppm 単位) など) を持つStorageGRID属性の値をプロットするために使用されます。値の変化は、時間の経過に伴って一定のデータ間隔 (ビン) でプロットされます。



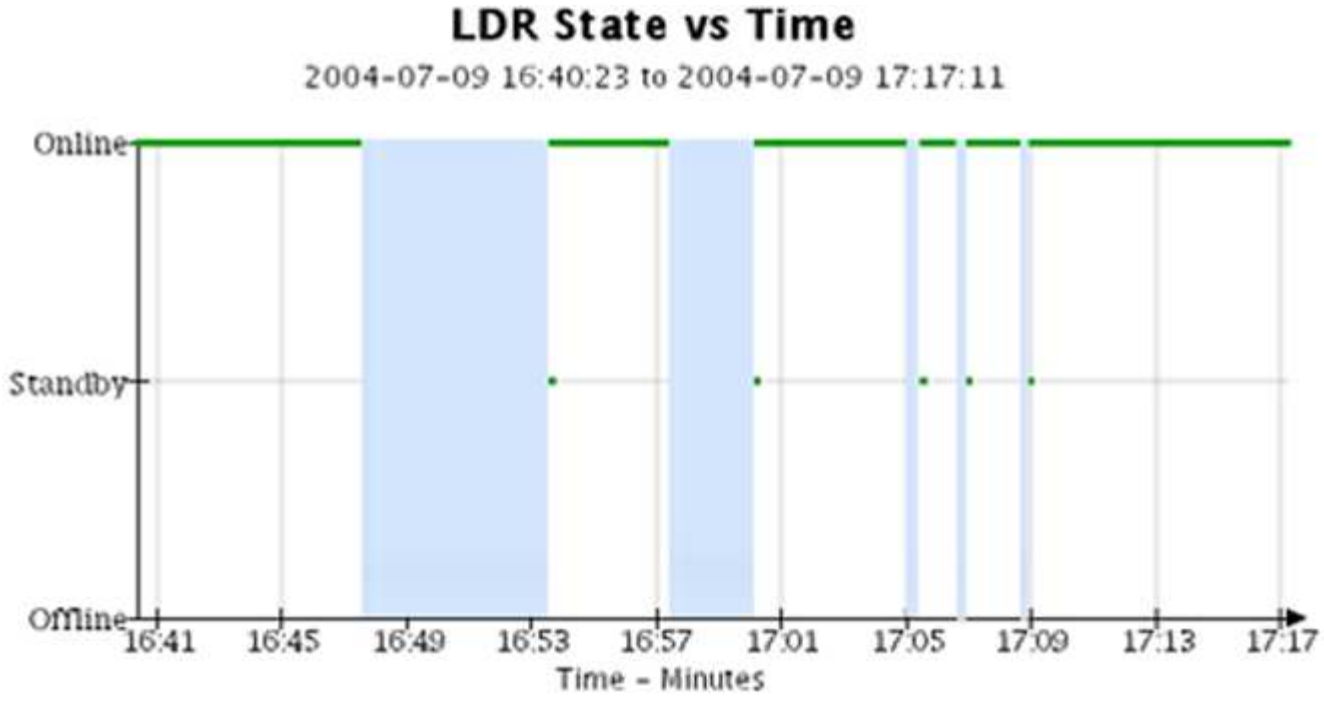
- 面グラフ: ノードページおよび*サポート* > ツール > *グリッドトポロジ*ページから利用できます（グラフアイコンを選択）面グラフは、データ値の後に続く部分で、オブジェクト数やサービス負荷値などの体積属性量をプロットするために使用されます。面グラフは折れ線グラフに似ていますが、線の下に薄茶色の陰影が付きます。値の変化は、時間の経過に伴って一定のデータ間隔 (ビン) でプロットされます。



- 一部のグラフは異なる種類のチャートアイコンで表示されます形式が異なります:



- 状態グラフ: サポート > ツール > グリッドトポロジ ページから利用可能です（チャートアイコンを選択）状態グラフは、データ値の後に続く部分など、オンライン、スタンバイ、オフラインなどのサービス状態などの個別の状態を表す属性値をプロットするために使用されます。状態グラフは折れ線グラフに似ていますが、遷移は不連続です。つまり、値がある状態値から別の状態値にジャンプします。

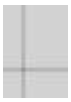


関連情報

- "ノードページを表示する"
- "グリッドトポロジツリーを表示する"
- "サポート指標を確認する"

チャートの凡例

グラフを描くために使用される線と色には特定の意味があります。

例	説明
	報告された属性値は濃い緑色の線でプロットされます。
	濃い緑色の線の周りの薄い緑色の陰影は、その時間範囲内の実際の値が変化しており、プロットを高速化するために「ビン化」されていることを示しています。濃い線は加重平均を表します。薄緑色の範囲は、ビン内の最大値と最小値を示します。明るい茶色の陰影は、体積データを示す面グラフで使用されます。
	空白領域 (データがプロットされていない) は、属性値が利用できなかったことを示します。背景は、属性を報告するサービスの状態に応じて、青、灰色、または灰色と青の混合になります。
	薄い青色の網掛けは、その時点での属性値の一部またはすべてが不確定であったことを示します。つまり、サービスが不明な状態であったため、属性は値を報告していませんでした。
	灰色の網掛けは、属性を報告するサービスが管理上ダウンしていたため、その時点で属性値の一部またはすべてが不明であったことを示します。
	灰色と青色の混在した陰影は、その時点で属性値の一部が不確定であったこと (サービスが不明な状態であったため)、また、属性を報告するサービスが管理上ダウンしていたため他の属性値が不明であったことを示します。

チャートとグラフを表示する

ノード ページには、ストレージ容量やスループットなどの属性を監視するために定期的にアクセスする必要があるチャートとグラフが含まれています。場合によっては、特にテクニカル サポートと連携している場合は、[サポート] > [ツール] > [グリッド トポロジ] ページを使用して追加のグラフにアクセスできます。

開始する前に

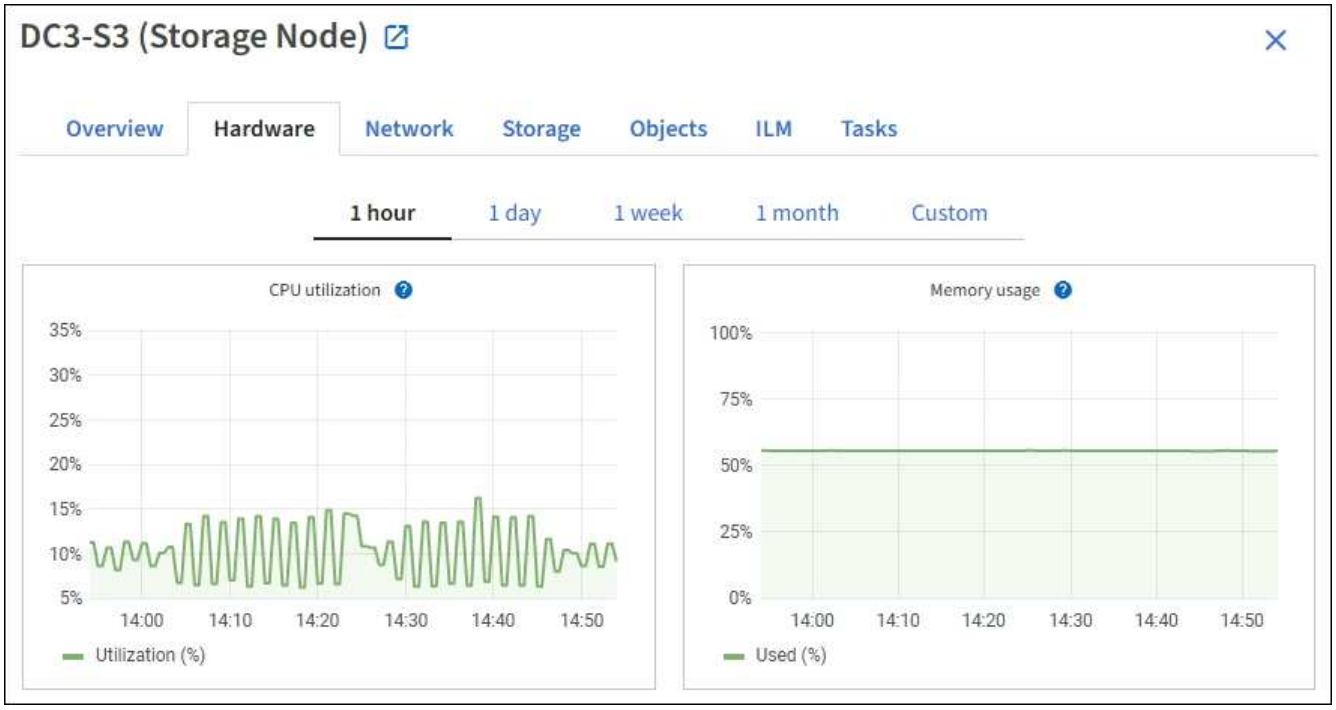
グリッドマネージャにサインインするには、"サポートされているウェブブラウザ" 。

手順

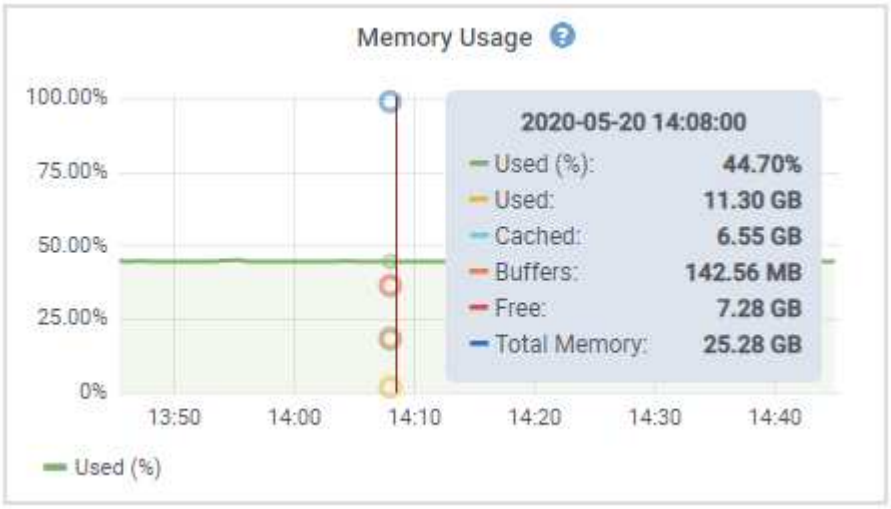
1. 「NODES」を選択します。次に、ノード、サイト、またはグリッド全体を選択します。
2. 情報を表示するタブを選択します。

   一部のタブには、時間の経過に伴う Prometheus メトリックの値をプロットするために使用される 1 つ以

上の Grafana チャートが含まれています。たとえば、ノードの **NODES** > **Hardware** タブには、2 つの Grafana チャートが含まれます。



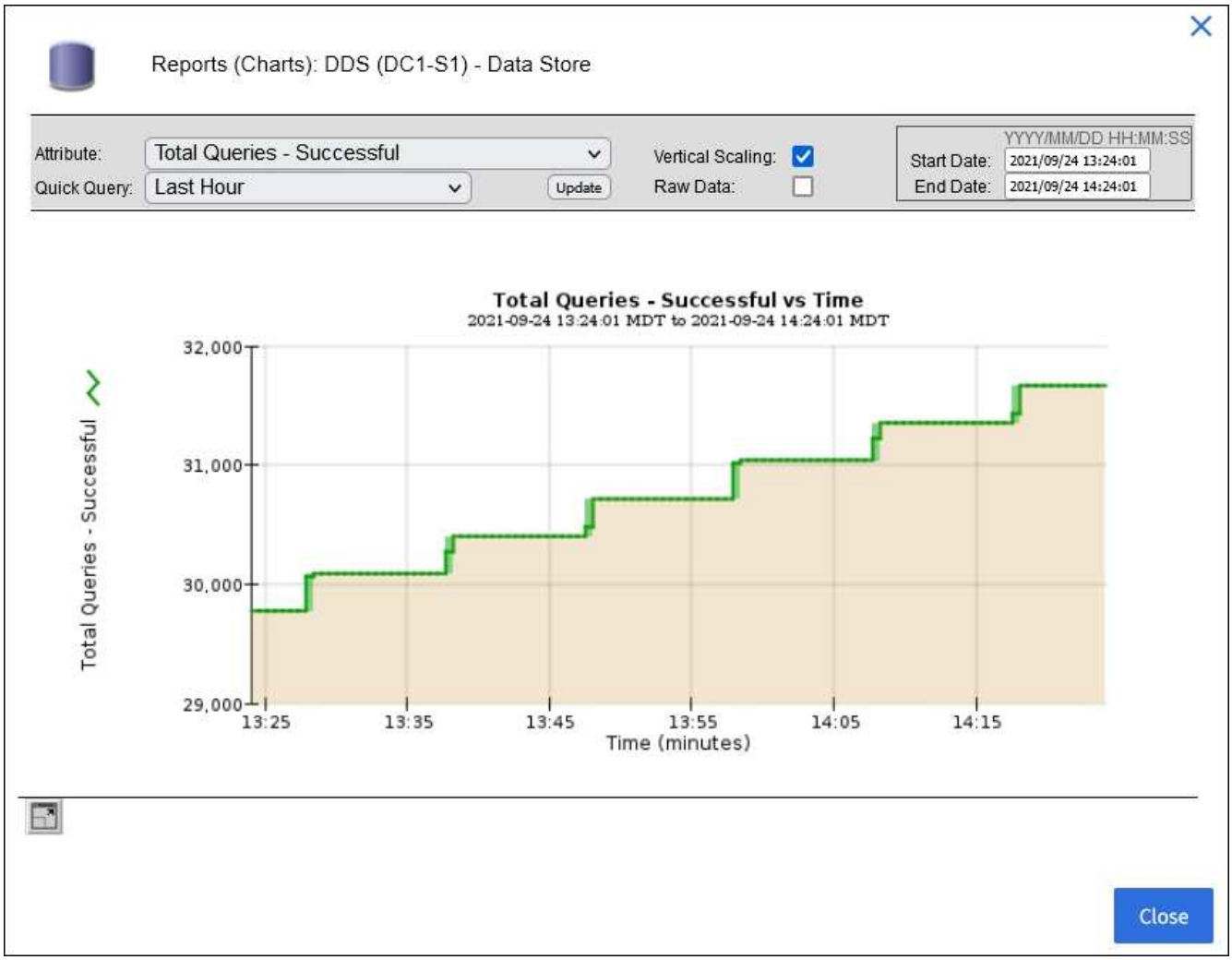
3. 必要に応じて、グラフの上にカーソルを置くと、特定の時点のより詳細な値が表示されます。

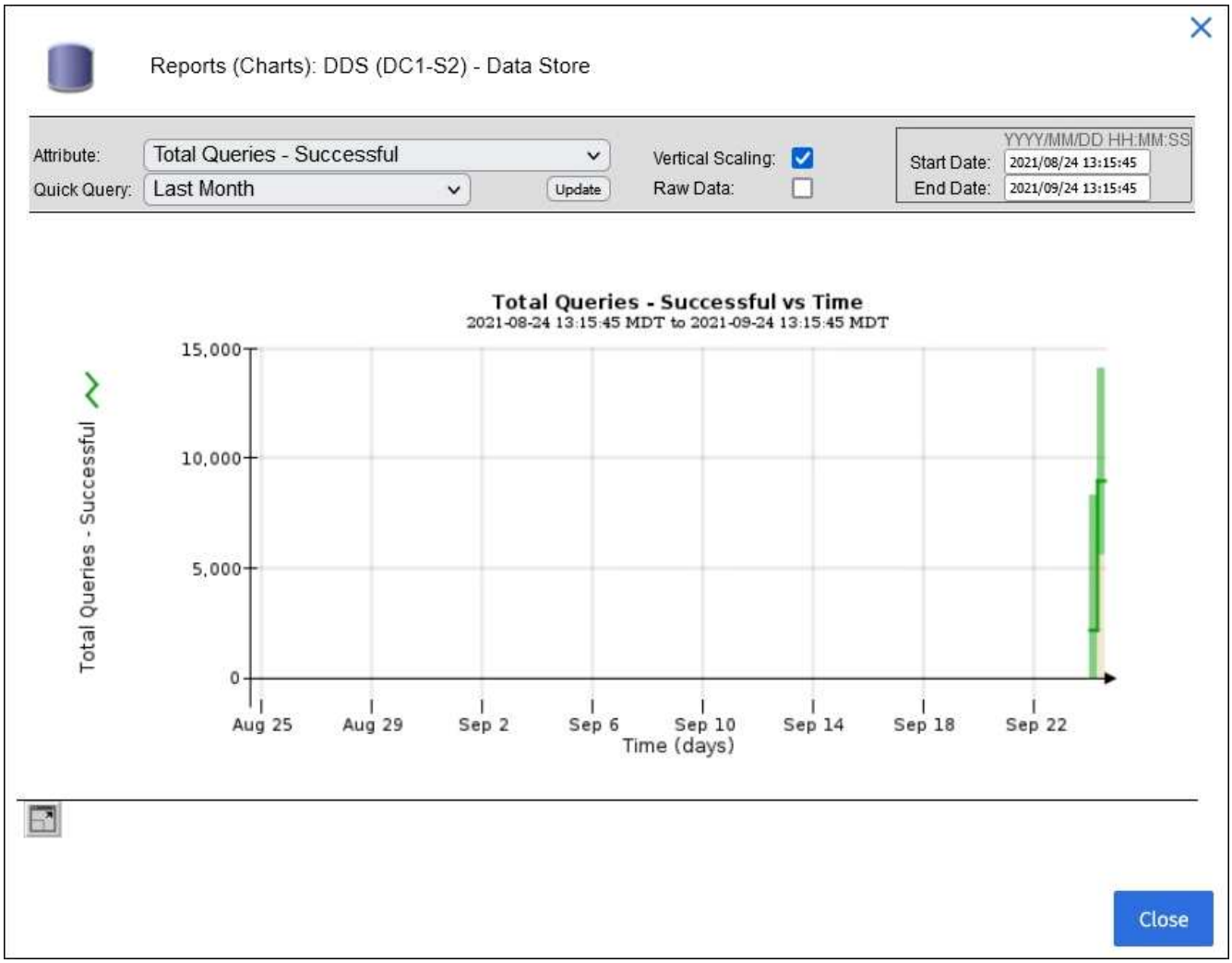


4. 必要に応じて、特定の属性またはメトリックのグラフを表示できることがよくあります。ノードページの表からチャートアイコンを選択します属性名の右側。

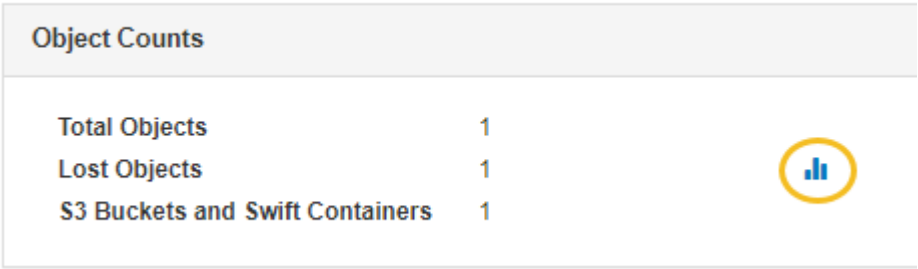
すべての指標と属性でグラフを利用できるわけではありません。

例**1**: ストレージノードのオブジェクトタブからチャートアイコンを選択します。ストレージ ノードの成功したメタデータ ストア クエリの合計数を確認します。

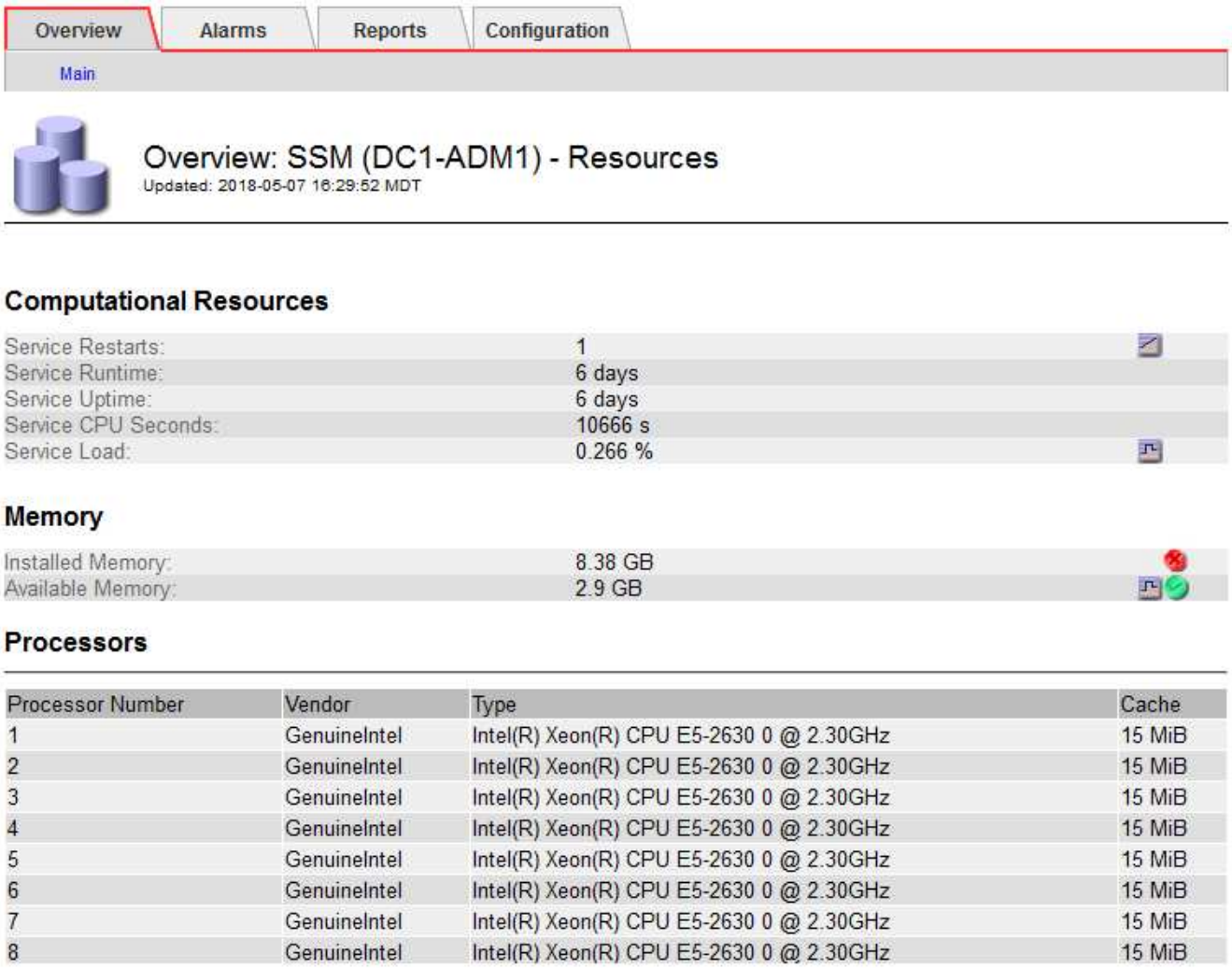

Reports (Charts): DDS (DC1-S1) - Data Store
Attribute:
Total Queries - Successful
Quick Query:
Last Hour
Update
Vertical Scaling:
Raw Data:
YYYY/MM/DD HH:MM:SS
Start Date:
2021/09/24 13:24:01
End Date:
2021/09/24 14:24:01
Total Queries - Successful vs Time
2021-09-24 13:24:01 MDT to 2021-09-24 14:24:01 MDT
Total Queries - Successful
32,000
31,000
30,000
29,000
13:25
13:35
13:45
13:55
14:05
14:15
Time (minutes)
Close



例**2**: ストレージノードのオブジェクトタブからチャートアイコンを選択できます。時間の経過に伴って検出された失われたオブジェクトの数の Grafana グラフを表示します。



5. ノード ページに表示されない属性のグラフを表示するには、サポート > ツール > グリッド トポロジ を選択します。
6. ***grid node*** > ***component or service*** > 概要 > メイン を選択します。



7. チャートアイコンを選択属性の横にあります。

   表示は自動的に*レポート* > *チャート*ページに変わります。グラフには、過去 1 日間の属性のデータが表示されます。

チャートを生成する

チャートには、属性データ値のグラフィカルな表現が表示されます。データ センター サイト、グリッド ノード、コンポーネント、またはサービスについてレポートできます。

開始する前に

- グリッドマネージャにサインインするには、"サポートされているウェブブラウザ" 。
- あなたが持っている"特定のアクセス権限"。

手順

1. サポート > ツール > グリッド トポロジ を選択します。
2. ***grid node*** > ***component or service*** > レポート > *チャート*を選択します。
3. *属性*ドロップダウンリストからレポートする属性を選択します。
4. Y 軸を強制的にゼロから開始するには、[垂直スケーリング] チェックボックスをオフにします。

5. 値を完全な精度で表示するには、[生データ] チェックボックスをオンにします。値を小数点以下最大 3 桁に丸めるには (たとえば、パーセンテージとして報告される属性の場合)、[生データ] チェックボックスをオフにします。
6. クイック クエリ ドロップダウン リストからレポートする期間を選択します。

   特定の時間範囲を選択するには、カスタム クエリ オプションを選択します。

   しばらくするとチャートが表示されます。長い時間範囲の集計には数分かかります。

7. カスタム クエリを選択した場合は、*開始日*と*終了日*を入力して、グラフの期間をカスタマイズします。

   フォーマットを使用する `*YYYY/MM/DDHH:MM:SS*`現地時間で。形式を一致させるには先頭のゼロが必要です。たとえば、2017/4/6 7:30:00 は検証に失敗します。正しい形式は、2017/04/06 07:30:00 です。

8. *更新*を選択します。

   数秒後にチャートが生成されます。長い時間範囲の集計には数分かかります。クエリに設定された時間の長さに応じて、生のテキスト レポートまたは集計テキスト レポートのいずれかが表示されます。

テキストレポートを使用する

テキスト レポートには、NMS サービスによって処理された属性データ値のテキスト表現が表示されます。レポートの期間に応じて生成されるレポートには、1 週間未満の期間の場合は生のテキスト レポート、1 週間を超える期間の場合は集計テキスト レポートの 2 種類があります。

生のテキストレポート

生のテキスト レポートには、選択した属性の詳細が表示されます。

- 受信時刻: 属性データのサンプル値が NMS サービスによって処理されたローカルの日時。
- サンプル時間: 属性値がソースでサンプリングまたは変更されたローカルの日時。
- 値: サンプル時の属性値。

Text Results for Services: Load - System Logging

2010-07-18 15:58:39 PDT To 2010-07-19 15:58:39 PDT

Time Received	Sample Time	Value
2010-07-19 15:58:09	2010-07-19 15:58:09	0.016 %
2010-07-19 15:56:06	2010-07-19 15:56:06	0.024 %
2010-07-19 15:54:02	2010-07-19 15:54:02	0.033 %
2010-07-19 15:52:00	2010-07-19 15:52:00	0.016 %
2010-07-19 15:49:57	2010-07-19 15:49:57	0.008 %
2010-07-19 15:47:54	2010-07-19 15:47:54	0.024 %
2010-07-19 15:45:50	2010-07-19 15:45:50	0.016 %
2010-07-19 15:43:47	2010-07-19 15:43:47	0.024 %
2010-07-19 15:41:43	2010-07-19 15:41:43	0.032 %
2010-07-19 15:39:40	2010-07-19 15:39:40	0.024 %
2010-07-19 15:37:37	2010-07-19 15:37:37	0.008 %
2010-07-19 15:35:34	2010-07-19 15:35:34	0.016 %
2010-07-19 15:33:31	2010-07-19 15:33:31	0.024 %
2010-07-19 15:31:27	2010-07-19 15:31:27	0.032 %
2010-07-19 15:29:24	2010-07-19 15:29:24	0.032 %
2010-07-19 15:27:21	2010-07-19 15:27:21	0.049 %
2010-07-19 15:25:18	2010-07-19 15:25:18	0.024 %
2010-07-19 15:21:12	2010-07-19 15:21:12	0.016 %
2010-07-19 15:19:09	2010-07-19 15:19:09	0.008 %
2010-07-19 15:17:07	2010-07-19 15:17:07	0.016 %

集計テキストレポート

集計テキスト レポートには、生のテキスト レポートよりも長い期間 (通常は 1 週間) にわたるデータが表示されます。各エントリは、NMS サービスによって時間の経過に伴って複数の属性値 (属性値の集計) が集計から導出された平均値、最大値、最小値を含む単一のエントリにまとめられた結果です。

各エントリには次の情報が表示されます。

- 集約時刻: NMS サービスが変更された属性値のセットを集約 (収集) した最後のローカル日時。
- 平均値: 集計された期間にわたる属性の値の平均。
- 最小値: 集計期間における最小値。
- 最大値: 集計期間における最大値。

Text Results for Attribute Send to Relay Rate

2010-07-11 16:02:46 PDT To 2010-07-19 16:02:46 PDT

Aggregate Time	Average Value	Minimum Value	Maximum Value
2010-07-19 15:59:52	0.271072196 Messages/s	0.266649743 Messages/s	0.274983464 Messages/s
2010-07-19 15:53:52	0.275585378 Messages/s	0.266562352 Messages/s	0.283302736 Messages/s
2010-07-19 15:49:52	0.279315709 Messages/s	0.233318712 Messages/s	0.333313579 Messages/s
2010-07-19 15:43:52	0.28181323 Messages/s	0.241651024 Messages/s	0.374976601 Messages/s
2010-07-19 15:39:52	0.284233141 Messages/s	0.249982001 Messages/s	0.324971987 Messages/s
2010-07-19 15:33:52	0.325752083 Messages/s	0.266641993 Messages/s	0.358306197 Messages/s
2010-07-19 15:29:52	0.278531507 Messages/s	0.274984766 Messages/s	0.283320999 Messages/s
2010-07-19 15:23:52	0.281437642 Messages/s	0.274981961 Messages/s	0.291577735 Messages/s
2010-07-19 15:17:52	0.261563307 Messages/s	0.258318006 Messages/s	0.266655787 Messages/s
2010-07-19 15:13:52	0.265159147 Messages/s	0.258318557 Messages/s	0.26663986 Messages/s

テキストレポートを生成する

テキスト レポートには、NMS サービスによって処理された属性データ値のテキスト表現が表示されます。データ センター サイト、グリッド ノード、コンポーネント、またはサービスについてレポートできます。

開始する前に

- グリッドマネージャにサインインするには、"サポートされているウェブブラウザ" 。
- あなたが持っている"特定のアクセス権限"。

タスク概要

継続的に変更されると予想される属性データの場合、この属性データは NMS サービス (ソース) によって定期的にサンプリングされます。頻繁に変更されない属性データ (たとえば、状態やステータスの変更などのイベントに基づくデータ) の場合、属性値が変更されると、その値が NMS サービスに送信されます。

表示されるレポートの種類は、設定された期間によって異なります。デフォルトでは、1 週間を超える期間の集計テキスト レポートが生成されます。

灰色のテキストは、サンプリング時にサービスが管理上ダウンしていたことを示します。青いテキストは、サービスが不明な状態であったことを示します。

手順

1. サポート > ツール > グリッド トポロジ を選択します。
2. ***grid node*** > ***component or service*** > レポート > *テキスト*を選択します。
3. *属性*ドロップダウンリストからレポートする属性を選択します。
4. *ページあたりの結果数*ドロップダウンリストからページあたりの結果数を選択します。
5. 値を小数点以下最大 3 桁に丸めるには (たとえば、パーセンテージとして報告される属性の場合)、[生データ] チェックボックスをオフにします。
6. クイック クエリ ドロップダウン リストからレポートする期間を選択します。

   特定の時間範囲を選択するには、カスタム クエリ オプションを選択します。

しばらくするとレポートが表示されます。長い時間範囲の集計には数分かかります。

7. カスタム クエリを選択した場合は、*開始日*と*終了日*を入力して、レポートする期間をカスタマイズする必要があります。

   フォーマットを使用する `YYYY/MM/DDHH:MM:SS`現地時間で。形式を一致させるには先頭のゼロが必要です。たとえば、2017/4/6 7:30:00 は検証に失敗します。正しい形式は、2017/04/06 07:30:00 です。

8. *更新*をクリックします。

   しばらくするとテキスト レポートが生成されます。長い時間範囲の集計には数分かかります。クエリに設定された時間の長さに応じて、生のテキスト レポートまたは集計テキスト レポートのいずれかが表示されます。

テキストレポートをエクスポートする

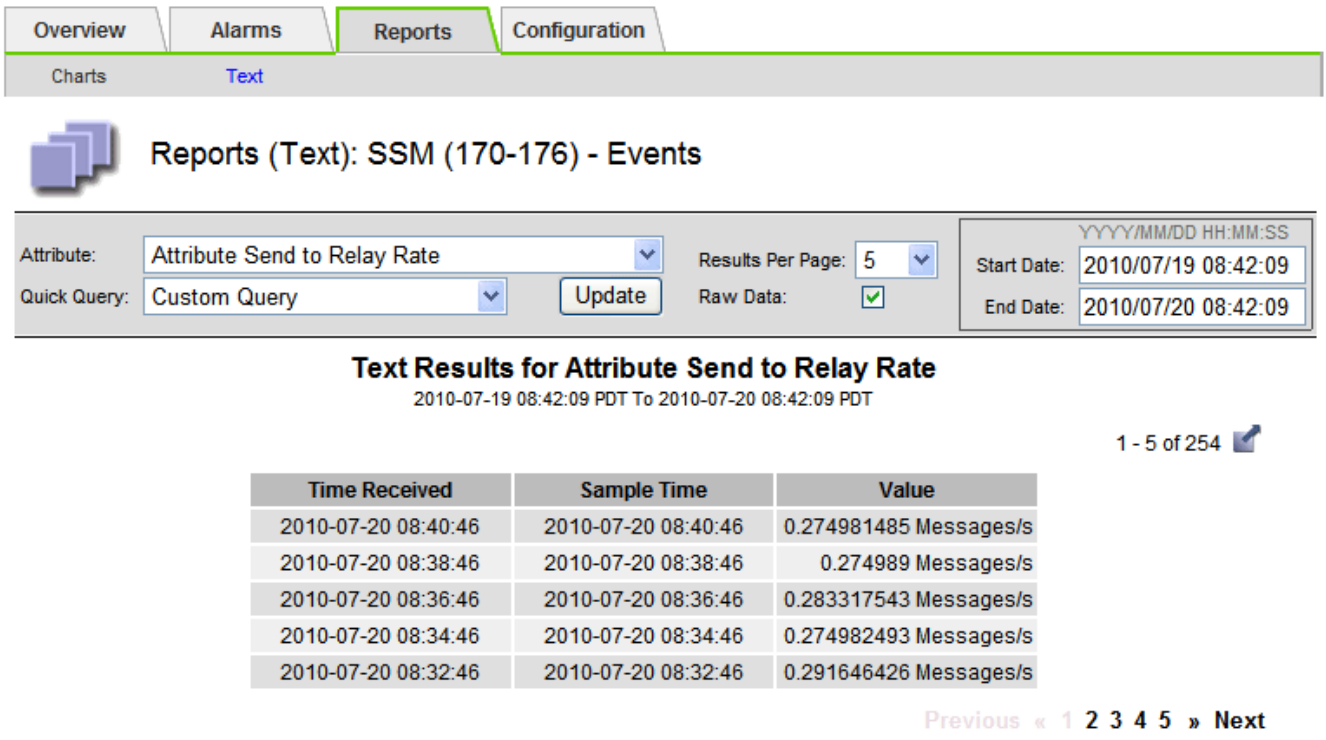
エクスポートされたテキスト レポートでは新しいブラウザー タブが開き、データを選択してコピーできるようになります。

タスク概要

コピーされたデータは新しいドキュメント (スプレッドシートなど) に保存し、 StorageGRIDシステムのパフォーマンスを分析するために使用できます。

手順

1. サポート > ツール > グリッド トポロジ を選択します。
2. テキストレポートを作成します。
3. *エクスポート*をクリックします。



「テキスト レポートのエクスポート」ウィンドウが開き、レポートが表示されます。

```
Grid ID: 000 000
OID: 2.16.124.113590.2.1.400019.1.1.1.16996732.200
Node Path: Site/170-176/SSM/Events
Attribute: Attribute Send to Relay Rate (ABSR)
Query Start Date: 2010-07-19 08:42:09 PDT
Query End Date: 2010-07-20 08:42:09 PDT
Time Received,Time Received (Epoch),Sample Time,Sample Time (Epoch),Value,Type
2010-07-20 08:40:46,1279640446559000,2010-07-20 08:40:46,1279640446537209,0.274981485 Messages/s,U
2010-07-20 08:38:46,1279640326561000,2010-07-20 08:38:46,1279640326529124,0.274989 Messages/s,U
2010-07-20 08:36:46,1279640206556000,2010-07-20 08:36:46,1279640206524330,0.283317543 Messages/s,U
2010-07-20 08:34:46,1279640086540000,2010-07-20 08:34:46,1279640086517645,0.274982493 Messages/s,U
2010-07-20 08:32:46,1279639966543000,2010-07-20 08:32:46,1279639966510022,0.291646426 Messages/s,U
2010-07-20 08:30:46,1279639846561000,2010-07-20 08:30:46,1279639846501672,0.308315369 Messages/s,U
2010-07-20 08:28:46,1279639726527000,2010-07-20 08:28:46,1279639726494673,0.291657509 Messages/s,U
2010-07-20 08:26:46,1279639606526000,2010-07-20 08:26:46,1279639606490890,0.266627739 Messages/s,U
2010-07-20 08:24:46,1279639486495000,2010-07-20 08:24:46,1279639486473368,0.258318523 Messages/s,U
2010-07-20 08:22:46,1279639366480000,2010-07-20 08:22:46,1279639366466497,0.274985902 Messages/s,U
2010-07-20 08:20:46,1279639246469000,2010-07-20 08:20:46,1279639246460346,0.283253871 Messages/s,U
2010-07-20 08:18:46,1279639126469000,2010-07-20 08:18:46,1279639126426669,0.274982804 Messages/s,U
2010-07-20 08:16:46,1279639006437000,2010-07-20 08:16:46,1279639006419168,0.283315503 Messages/s,U
```

4. テキスト レポートのエクスポート ウィンドウの内容を選択してコピーします。

   このデータは、スプレッドシートなどのサードパーティのドキュメントに貼り付けることができます。

PUTと**GET**のパフォーマンスを監視する

オブジェクトの保存や取得などの特定の操作のパフォーマンスを監視して、さらに調査が必要となる可能性のある変更を特定することができます。

タスク概要

PUT および GET のパフォーマンスを監視するには、ワークステーションから直接 S3 コマンドを実行するか、オープンソースの S3tester アプリケーションを使用します。これらの方法を使用すると、クライアントアプリケーションの問題や外部ネットワークの問題など、 StorageGRIDの外部の要因に左右されずにパフォーマンスを評価できます。

PUT および GET 操作のテストを実行するときは、次のガイドラインに従います。

- 通常グリッドに取り込むオブジェクトと同等のオブジェクト サイズを使用します。
- ローカル サイトとリモート サイトの両方に対して操作を実行します。

メッセージ"監査ログ"特定の操作を実行するために必要な合計時間を示します。たとえば、S3 GET リクエストの合計処理時間を確認するには、SGET 監査メッセージの TIME 属性の値を確認します。また、次のS3操作の監査メッセージにはTIME属性が含まれています: DELETE、GET、HEAD、メタデータ更新、POST 、PUT

結果を分析するときは、リクエストを満たすのに必要な平均時間と、達成できる全体的なスループットを確認します。同じテストを定期的に繰り返し、結果を記録して、調査が必要な傾向を特定できるようにします。

- あなたはできる "githubからS3testerをダウンロードする"。

StorageGRIDシステムは、破損したオブジェクトと欠落したオブジェクトの両方をチェックし、ストレージ ノード上のオブジェクト データの整合性を検証できます。

開始する前に

- グリッドマネージャにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは"メンテナンスまたはルートアクセス権限"。

タスク概要

二"検証プロセス"データの整合性を確保するために協力します。

- *バックグラウンド検証*が自動的に実行され、オブジェクト データの正確性を継続的にチェックします。

  バックグラウンド検証では、すべてのストレージ ノードを自動的かつ継続的にチェックし、複製および消去コード化されたオブジェクト データの破損したコピーがあるかどうかを判断します。問題が見つかった場合、 StorageGRIDシステムは、破損したオブジェクト データをシステム内の他の場所に保存されているコピーから自動的に置き換えようとします。バックグラウンド検証は、クラウド ストレージ プール内のオブジェクトでは実行されません。

  > ⓘ システムが自動的に修正できない破損したオブジェクトを検出すると、未確認の破損オブジェクトが検出されました アラートがトリガーされます。

- オブジェクト存在チェック は、ユーザーがトリガーして、オブジェクト データの存在 (正確性ではない) をより迅速に検証できます。

  オブジェクト存在チェックは、オブジェクトの予想されるすべての複製コピーと消去コード化フラグメントがストレージ ノード上に存在するかどうかを確認します。オブジェクト存在チェックは、特に最近のハードウェアの問題がデータの整合性に影響を与えている可能性がある場合に、ストレージ デバイスの整合性を確認する方法を提供します。

背景検証とオブジェクトの存在チェックの結果を定期的に確認する必要があります。オブジェクト データが破損または欠落している場合は、直ちに調査して根本原因を特定してください。

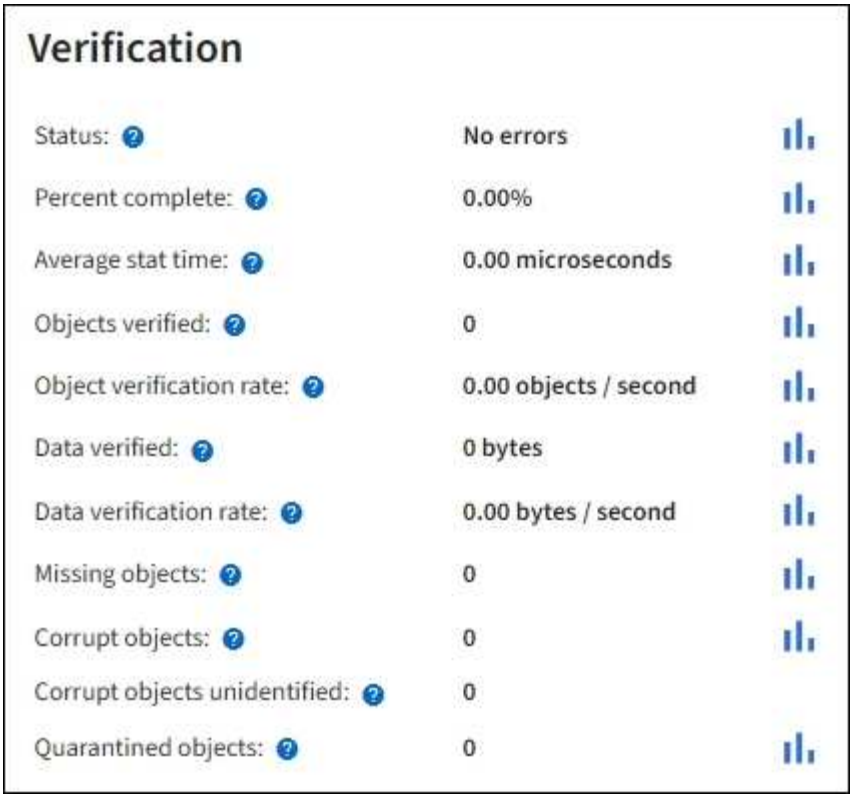
手順

1. 背景検証の結果を確認します。

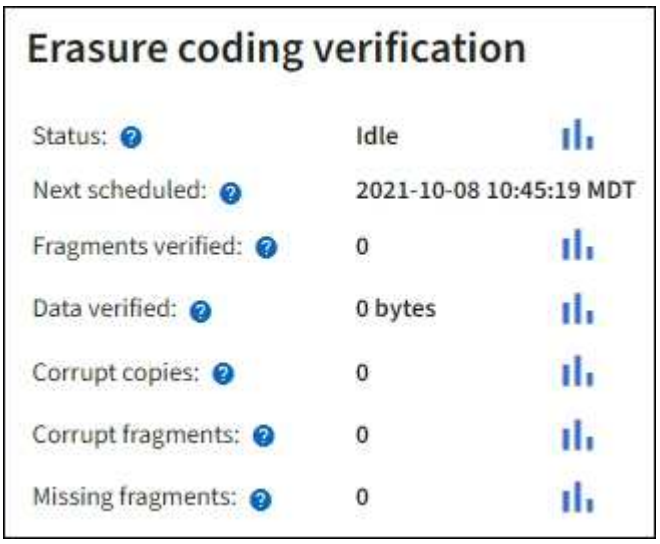
   a. **NODES** > ***Storage Node*** > **Objects** を選択します。

   b. 検証結果を確認します。

      - 複製されたオブジェクト データの検証を確認するには、検証セクションの属性を確認します。

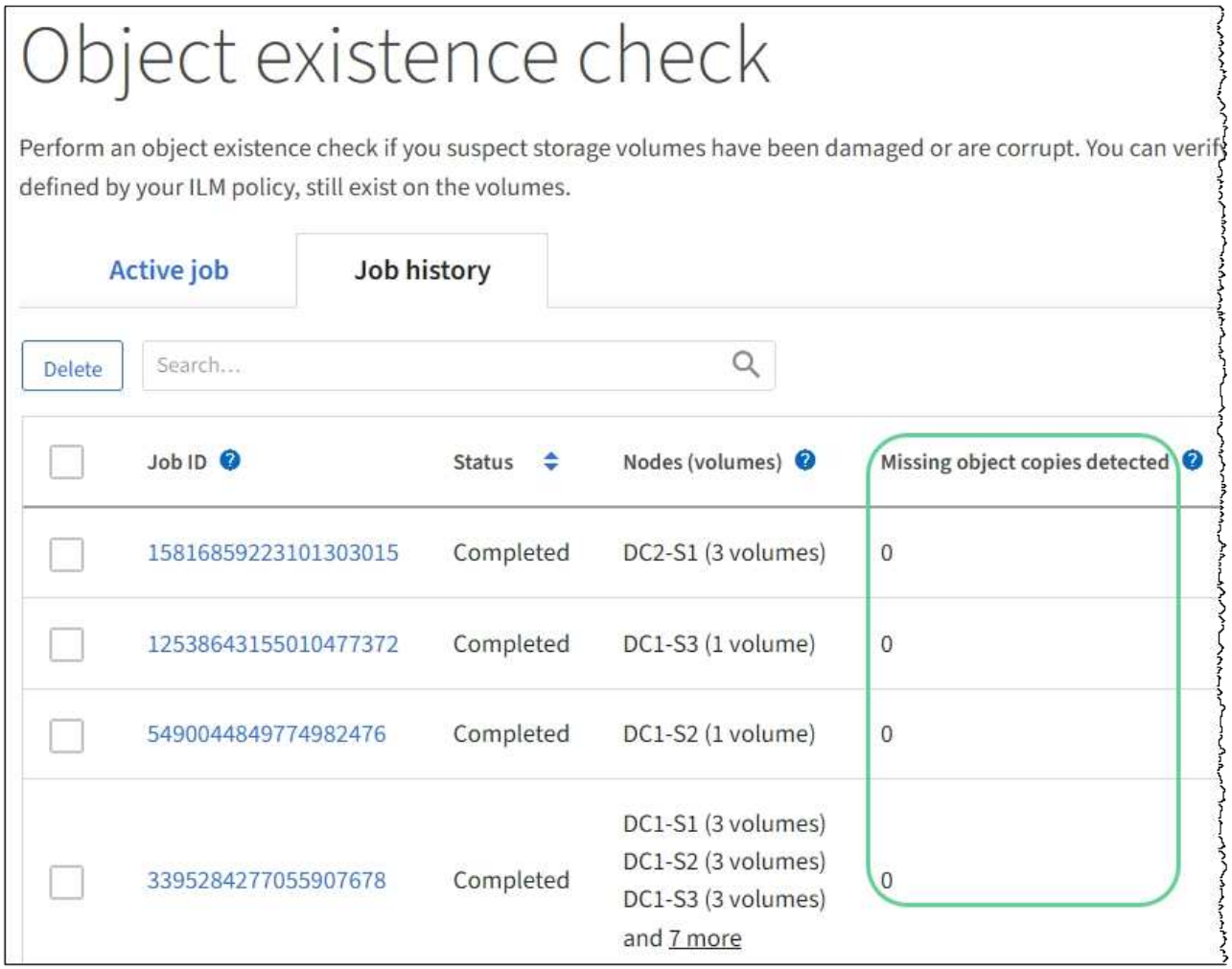


- 消失訂正符号化フラグメント検証を確認するには、***Storage Node*** > **ILM** を選択し、消失訂正符号化検証セクションの属性を確認します。



疑問符を選択属性名の横に をクリックすると、ヘルプ テキストが表示されます。

2. オブジェクト存在チェックジョブの結果を確認します。
   a. メンテナンス > オブジェクト存在チェック > *ジョブ履歴*を選択します。
   b. 不足しているオブジェクトのコピーが検出された列をスキャンします。いずれかのジョブで 100 個以上のオブジェクトのコピーが失われ、「オブジェクトが失われました」というアラートがトリガーされた場合は、テクニカル サポートにお問い合わせください。



イベントを監視する

Syslog サーバーに記録されるイベントを追跡するために作成したカスタム イベントを含む、グリッド ノードによって検出されたイベントを監視できます。グリッド マネージャーに表示される最後のイベント メッセージには、最新のイベントに関する詳細情報が提供されます。

イベントメッセージは、 `/var/local/log/bycast-err.log`ログファイル。参照"ログファイルリファレンス"。

SMTT (合計イベント数) アラームは、ネットワークの問題、停電、アップグレードなどの問題によって繰り返しトリガーされることがあります。このセクションには、これらのアラームが発生した理由をよりよく理解できるようにするためのイベントの調査に関する情報が記載されています。既知の問題が原因でイベントが発生した場合は、イベント カウンターをリセットしても安全です。

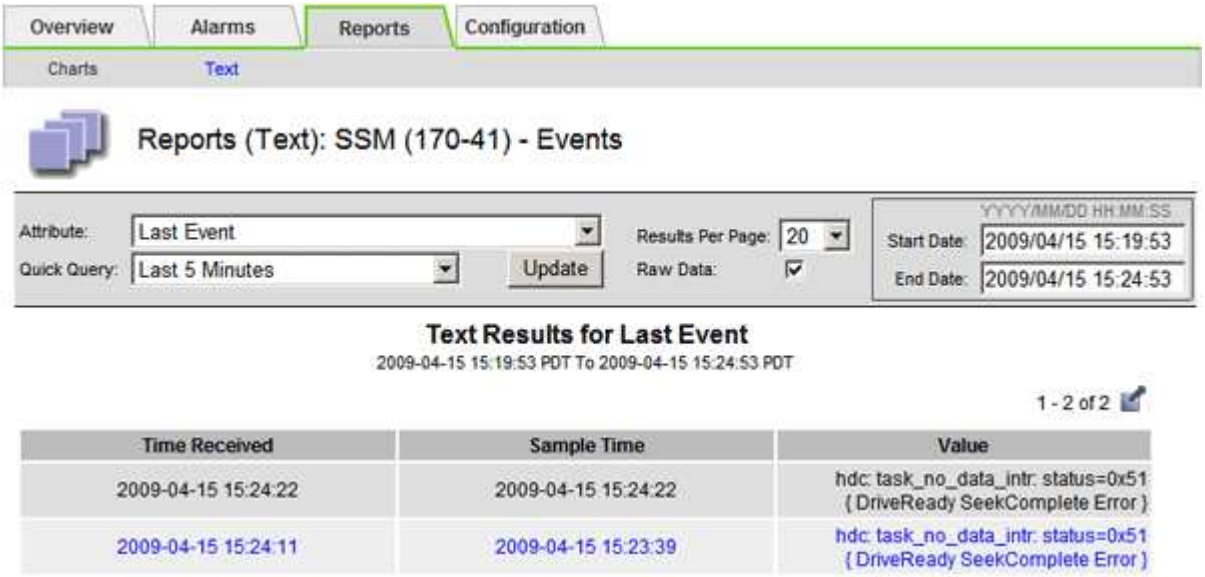
手順

1. 各グリッド ノードのシステム イベントを確認します。
   a. サポート > ツール > グリッド トポロジ を選択します。
   b. ***site*** > ***grid node*** > **SSM** > イベント > 概要 > メイン を選択します。
2. 過去に発生した問題を特定するために、以前のイベント メッセージのリストを生成します。

a. サポート > ツール > グリッド トポロジ を選択します。
b. ***site*** > ***grid node*** > **SSM** > イベント > レポート を選択します。
c. *テキスト*を選択します。

   *最後のイベント*属性は、"チャートビュー" 。表示するには:

d. *属性*を*最後のイベント*に変更します。
e. 必要に応じて、「クイック クエリ」の期間を選択します。
f. *更新*を選択します。



カスタム **Syslog** イベントを作成する

カスタム イベントを使用すると、Syslog サーバーに記録されたすべてのカーネル、デーモン、エラー、および重大レベルのユーザー イベントを追跡できます。カスタム イベントは、システム ログ メッセージ (およびネットワーク セキュリティ イベントとハードウェア障害) の発生を監視するのに役立ちます。

タスク概要

繰り返し発生する問題を監視するためにカスタム イベントを作成することを検討してください。カスタム イベントには次の考慮事項が適用されます。

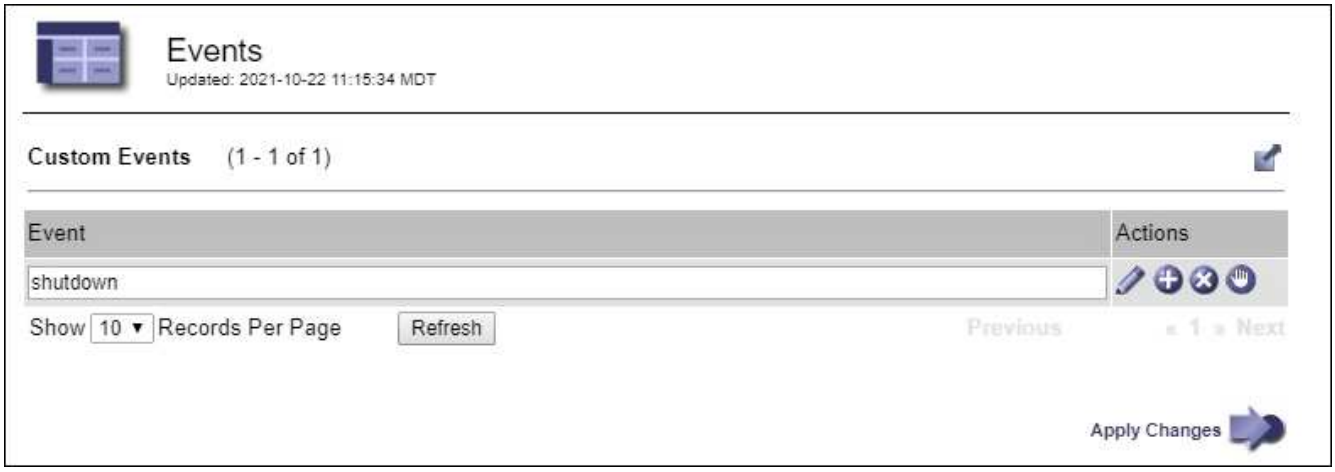
- カスタム イベントが作成されると、そのイベントの発生がすべて監視されます。
- キーワードに基づいてカスタムイベントを作成するには `/var/local/log/messages`ファイルの場合、それらのファイル内のログは次のようになります。
  - カーネルによって生成される
  - デーモンまたはユーザープログラムによってエラーまたはクリティカルレベルで生成された

注: すべてのエントリが `/var/local/log/messages`上記の要件を満たさない限り、ファイルは一致しません。

手順

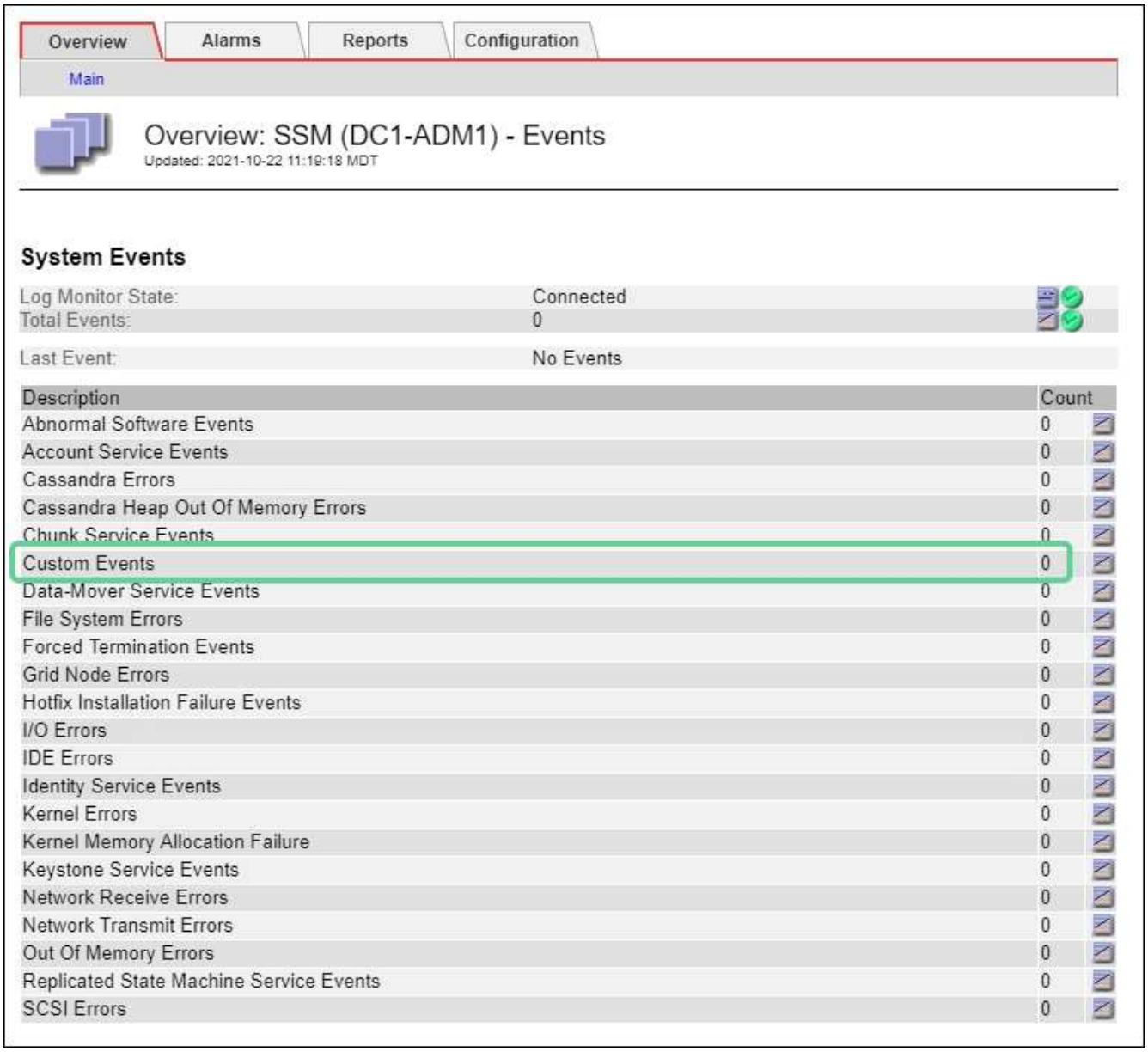
1. サポート > アラーム（レガシー） > カスタム イベント を選択します。

2. *編集*をクリック（または*挿入*(これが最初のイベントでない場合)。
3. カスタムイベント文字列を入力します（例：シャットダウン）



4. *変更を適用*を選択します。
5. サポート > ツール > グリッド トポロジ を選択します。
6. ***grid node*** > **SSM** > *イベント*を選択します。
7. イベント テーブルでカスタム イベントのエントリを見つけて、**Count** の値を監視します。

   カウントが増加すると、監視しているカスタム イベントがそのグリッド ノードでトリガーされます。



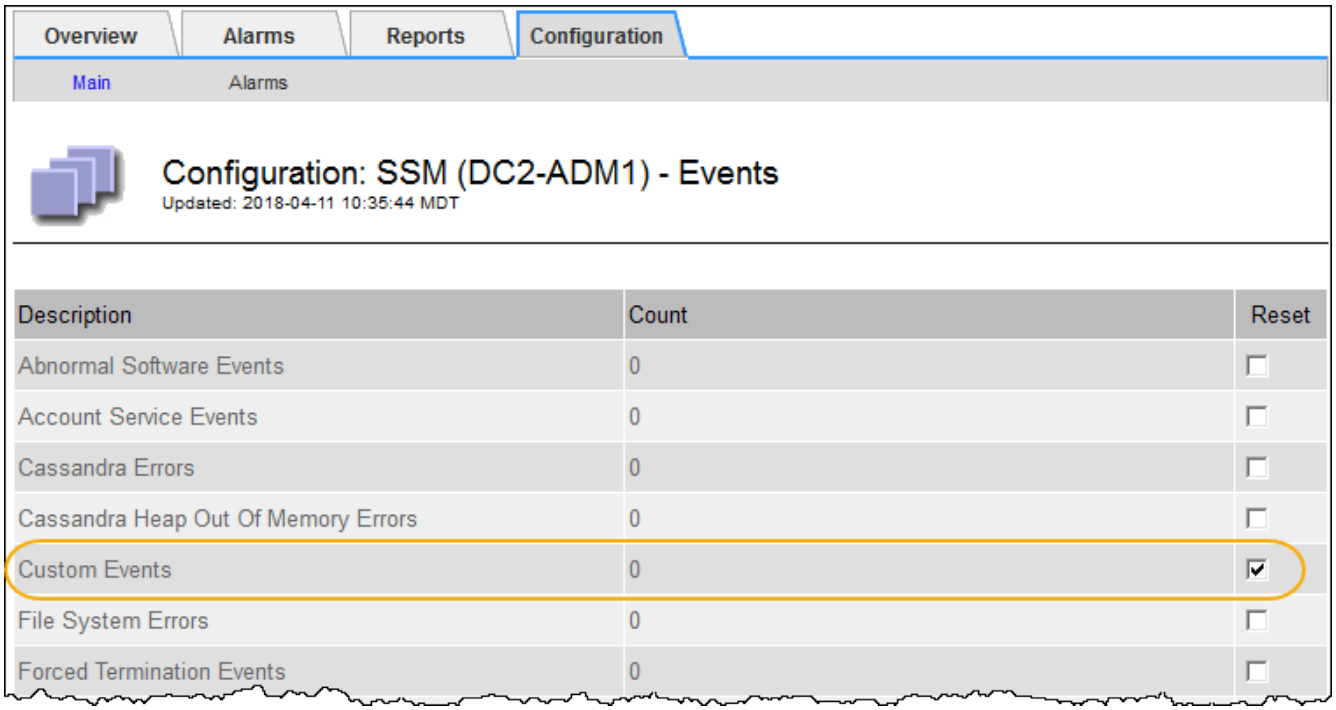
カスタムイベントのカウントをゼロにリセットします

カスタム イベントのカウンターのみをリセットする場合は、[サポート] メニューの [グリッド トポロジ] ページを使用する必要があります。

カウンターをリセットすると、次のイベントによってアラームがトリガーされます。対照的に、アラームを確認すると、次のしきい値レベルに達した場合にのみそのアラームが再度トリガーされます。

手順

1. サポート > ツール > グリッド トポロジ を選択します。
2. ***grid node*** > **SSM** > イベント > 構成 > メイン を選択します。
3. カスタム イベントの [リセット] チェックボックスを選択します。



4. *変更を適用*を選択します。

監査メッセージを確認する

監査メッセージは、 StorageGRIDシステムの詳細な操作をより深く理解するのに役立ちます。監査ログを使用して、問題のトラブルシューティングやパフォーマンスの評価を行うことができます。

通常のシステム操作中、すべてのStorageGRIDサービスは次のように監査メッセージを生成します。

- システム監査メッセージは、監査システム自体、グリッド ノードの状態、システム全体のタスク アクティビティ、およびサービス バックアップ操作に関連しています。
- オブジェクト ストレージ監査メッセージは、オブジェクトの保存と取得、グリッド ノード間の転送、検証など、 StorageGRID内のオブジェクトの保存と管理に関連しています。
- S3 クライアント アプリケーションがオブジェクトの作成、変更、または取得を要求すると、クライアントの読み取りおよび書き込み監査メッセージが記録されます。
- 管理監査メッセージには、管理 API へのユーザー リクエストが記録されます。

各管理ノードは監査メッセージをテキスト ファイルに保存します。監査共有には、アクティブ ファイル (audit.log) と、前日からの圧縮された監査ログが含まれます。グリッド内の各ノードには、ノード上で生成された監査情報のコピーも保存されます。

管理ノードのコマンド ラインから監査ログ ファイルに直接アクセスできます。

StorageGRID はデフォルトで監査情報を送信できますが、送信先を変更することもできます。

- StorageGRID はデフォルトでローカル ノードの監査宛先を使用します。
- Grid Manager および Tenant Manager の監査ログ エントリがストレージ ノードに送信される場合があります。

- 必要に応じて、監査ログの送信先を変更し、監査情報を外部の syslog サーバーに送信することもできます。外部 Syslog サーバーが構成されている場合、監査レコードのローカル ログは引き続き生成され、保存されます。
- "監査メッセージとログの送信先の設定について学習します" 。

監査ログファイル、監査メッセージの形式、監査メッセージの種類、監査メッセージを分析するために使用できるツールの詳細については、以下を参照してください。"監査ログを確認する" 。

ログファイルとシステムデータを収集する

Grid Manager を使用して、 StorageGRIDシステムのログ ファイルとシステム データ (構成データを含む) を取得できます。

開始する前に

- プライマリ管理ノードのグリッドマネージャにサインインする必要があります。"サポートされているウェブブラウザ" 。
- あなたが持っている"特定のアクセス権限"。
- プロビジョニング パスフレーズが必要です。

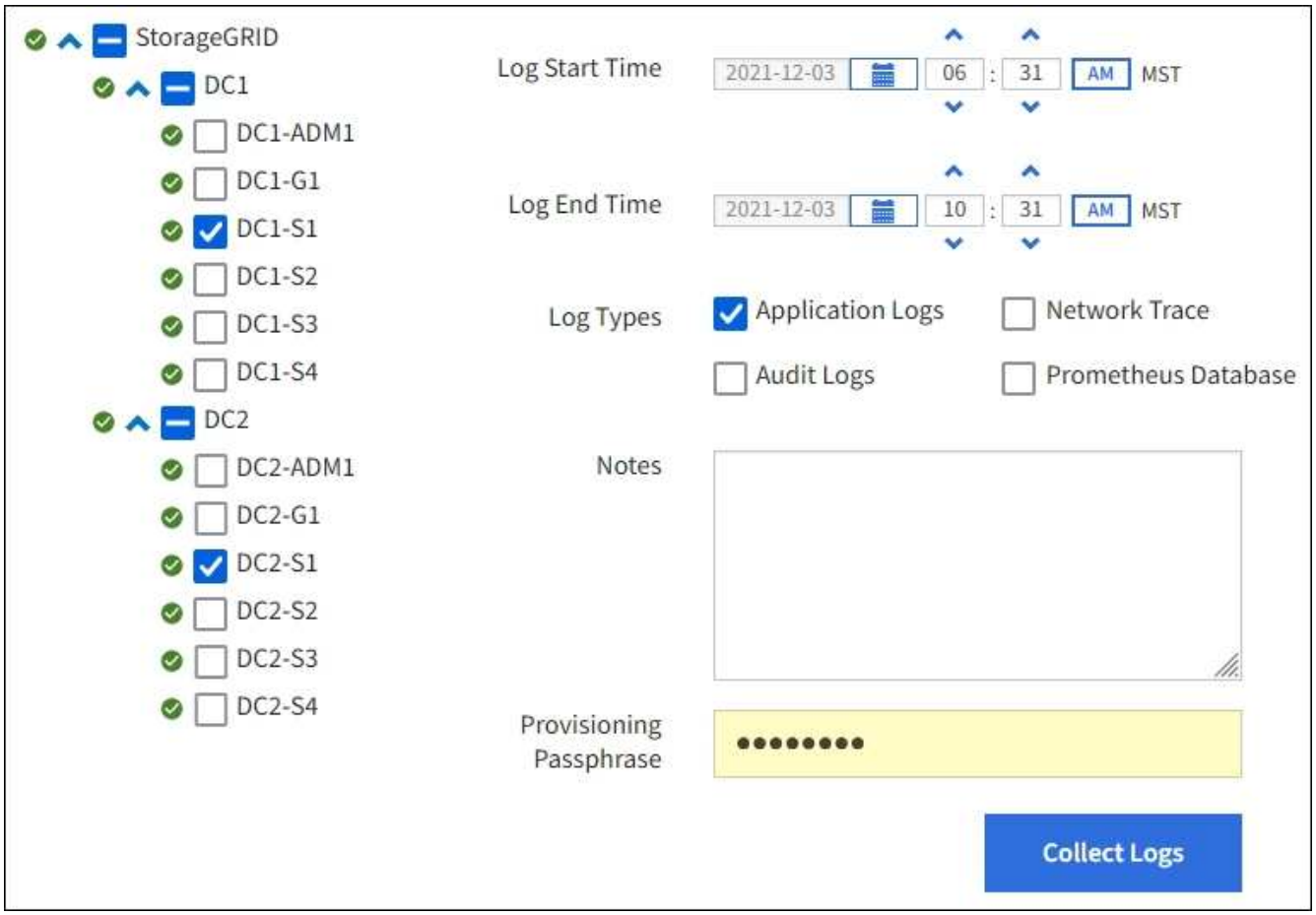
タスク概要

グリッドマネージャーを使用して収集できます"ログ ファイル"選択した期間の任意のグリッド ノードからのシステム データおよび構成データを取得します。データは収集され、.tar.gz ファイルにアーカイブされ、その後ローカル コンピューターにダウンロードできます。

必要に応じて、監査ログの送信先を変更し、監査情報を外部の syslog サーバーに送信することもできます。外部 Syslog サーバーが構成されている場合、監査レコードのローカル ログは引き続き生成され、保存されます。見る"監査メッセージとログの保存先を構成する" 。

手順

1. サポート > ツール > ログ を選択します。



2. ログ ファイルを収集するグリッド ノードを選択します。

   必要に応じて、グリッド全体またはデータセンター サイト全体のログ ファイルを収集できます。

3. ログ ファイルに含めるデータの時間範囲を設定するには、開始時刻 と 終了時刻 を選択します。

   非常に長い期間を選択した場合、または大規模なグリッド内のすべてのノードからログを収集した場合、ログ アーカイブが大きくなりすぎてノードに保存できなくなったり、ダウンロード用にプライマリ管理ノードに収集できなくなる可能性があります。この問題が発生した場合は、より小さいデータ セットを使用してログ収集を再開する必要があります。

4. 収集するログの種類を選択します。

   - アプリケーション ログ: テクニカル サポートがトラブルシューティングに最も頻繁に使用するアプリケーション固有のログ。収集されるログは、利用可能なアプリケーション ログのサブセットです。
   - 監査ログ: 通常のシステム操作中に生成された監査メッセージを含むログ。
   - ネットワーク トレース: ネットワークのデバッグに使用されるログ。
   - **Prometheus** データベース: すべてのノード上のサービスからの時系列メトリック。

5. 必要に応じて、**Notes** テキスト ボックスに収集するログ ファイルに関するメモを入力します。

   これらのメモを使用して、ログ ファイルを収集するように促された問題に関する技術サポート情報を提供できます。メモは、 `info.txt`ログ ファイル収集に関するその他の情報も表示されます。その `info.txt`ファイルはログ ファイル アーカイブ パッケージに保存されます。

6. プロビジョニング パスフレーズ テキスト ボックスに、 StorageGRIDシステムのプロビジョニング パスフレーズを入力します。
7. *ログを収集*を選択します。

   新しいリクエストを送信すると、以前のログ ファイルのコレクションは削除されます。

   「ログ」ページを使用して、各グリッド ノードのログ ファイル収集の進行状況を監視できます。

   ログ サイズに関するエラー メッセージが表示される場合は、期間を短くするか、ノードの数を減らしてログを収集してみてください。

8. ログファイルの収集が完了したら、[ダウンロード] を選択します。

   .tar.gz ファイルには、ログ収集が成功したすべてのグリッド ノードからのすべてのログ ファイルが含まれます。結合された *.tar.gz* ファイル内には、グリッド ノードごとに 1 つのログ ファイル アーカイブがあります。

終了後の操作

必要に応じて、後でログ ファイル アーカイブ パッケージを再度ダウンロードできます。

オプションで、[削除] を選択してログ ファイル アーカイブ パッケージを削除し、ディスク領域を解放することもできます。現在のログ ファイル アーカイブ パッケージは、次回ログ ファイルを収集するときに自動的に削除されます。

AutoSupportパッケージを手動でトリガーする

StorageGRIDシステムの問題のトラブルシューティングでテクニカル サポートを支援するために、 AutoSupportパッケージの送信を手動でトリガーできます。

開始する前に

- グリッドマネージャにサインインするには、"サポートされているウェブブラウザ" 。
- ルート アクセスまたはその他のグリッド構成権限が必要です。

手順

1. サポート > ツール > * AutoSupport* を選択します。
2. *アクション*タブで、*ユーザーがトリガーしたAutoSupportの送信*を選択します。

   StorageGRID は、 AutoSupportパッケージをNetAppサポート サイトに送信しようとします。試行が成功すると、[結果] タブの [最新の結果] と [前回の成功時刻] の値が更新されます。問題がある場合は、「最新の結果」の値が「失敗」に更新され、 StorageGRID はAutoSupportパッケージの再送信を試行しません。

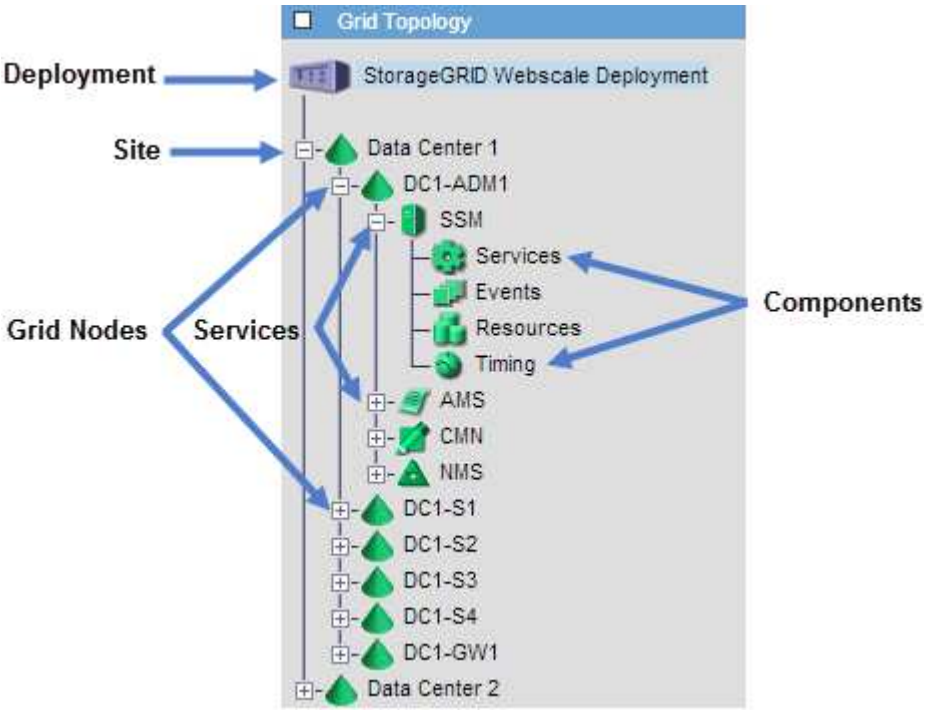
   ユーザーがトリガーしたAutoSupportパッケージを送信した後、1 分後にブラウザでAutoSupportページを更新して、最新の結果にアクセスします。

グリッドトポロジツリーを表示する

グリッド トポロジ ツリーでは、サイト、グリッド ノード、サービス、コンポーネントなどのStorageGRIDシステム要素に関する詳細情報にアクセスできます。ほとんどの場

合、ドキュメントで指示されている場合、またはテクニカル サポートと連携している場合にのみ、グリッド トポロジ ツリーにアクセスする必要があります。

グリッド トポロジ ツリーにアクセスするには、サポート > ツール > グリッド トポロジ を選択します。



グリッドトポロジツリーを展開または折りたたむには、⊞または⊟サイト、ノード、またはサービス レベルで。サイト全体または各ノード内のすべての項目を展開または折りたたむには、**<Ctrl>** キーを押しながらクリックします。

StorageGRID属性

属性は、 StorageGRIDシステムの多くの機能の値とステータスを報告します。属性値は、各グリッド ノード、各サイト、およびグリッド全体で使用できます。

StorageGRID属性は、グリッド マネージャーのいくつかの場所で使用されます。

- ノード ページ: ノード ページに表示される値の多くはStorageGRID属性です。 (Prometheus メトリックはノード ページにも表示されます。)
- グリッド トポロジ ツリー: 属性値は、グリッド トポロジ ツリーに表示されます (サポート > ツール > グリッド トポロジ)。
- イベント: システム イベントは、特定の属性がネットワーク エラーなどのノードのエラーまたは障害状態を記録したときに発生します。

属性値

属性はベストエフォート方式で報告され、ほぼ正確です。サービスのクラッシュやグリッド ノードの障害と再構築など、状況によっては属性の更新が失われる場合があります。

さらに、伝播の遅延により、属性のレポートが遅くなる可能性があります。ほとんどの属性の更新された値は、一定の間隔でStorageGRIDシステムに送信されます。更新がシステムに表示されるまでには数分かかる場合があり、ほぼ同時に変更された 2 つの属性がわずかに異なる時間に報告されることもあります。

問題のトラブルシューティングを行うときは、テクニカル サポートと協力して、StorageGRIDシステムの詳細なメトリックとグラフを確認できます。

開始する前に

- グリッドマネージャにサインインするには、"サポートされているウェブブラウザ" 。
- あなたが持っている"特定のアクセス権限"。

タスク概要

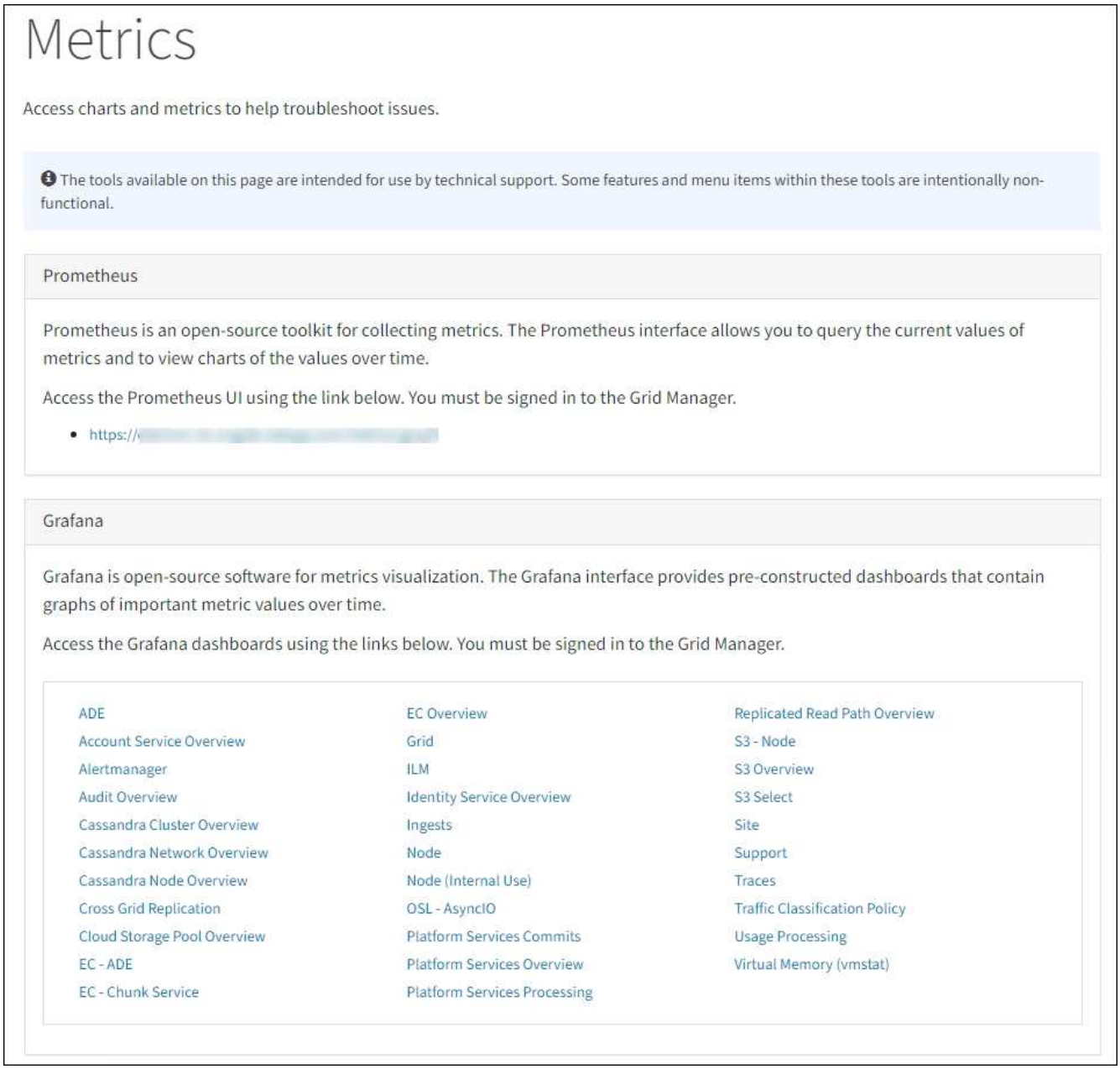
メトリクス ページでは、Prometheus および Grafana ユーザー インターフェースにアクセスできます。 Prometheus はメトリックを収集するためのオープンソース ソフトウェアです。 Grafana は、メトリックの視覚化のためのオープンソース ソフトウェアです。

> メトリクス ページで利用できるツールは、テクニカル サポートが使用することを目的としています。これらのツール内の一部の機能とメニュー項目は意図的に機能せず、変更される可能性があります。リストを見る"よく使われるPrometheusメトリクス"。

手順

1. テクニカル サポートの指示に従って、[サポート] > [ツール] > [メトリック] を選択します。

   メトリック ページの例を以下に示します。



2. StorageGRIDメトリックの現在の値を照会し、時間の経過に伴う値のグラフを表示するには、Prometheus セクションのリンクをクリックします。

   Prometheus インターフェースが表示されます。このインターフェースを使用して、利用可能なStorageGRIDメトリックに対してクエリを実行し、時間の経過に伴うStorageGRIDメトリックのグラフを作成できます。

   > 名前に *private* が含まれるメトリックは内部使用のみを目的としており、 StorageGRIDリリース間で予告なく変更されることがあります。

3. StorageGRIDメトリックの経時的なグラフを含む事前構築されたダッシュボードにアクセスするには、Grafana セクションのリンクをクリックします。

   選択したリンクの Grafana インターフェースが表示されます。

診断を実行する

問題のトラブルシューティングを行う場合、テクニカル サポートと連携してStorageGRIDシステムの診断を実行し、結果を確認することができます。

- "サポート指標を確認する"
- "よく使われるPrometheusメトリクス"

開始する前に

- グリッドマネージャにサインインするには、"サポートされているウェブブラウザ" 。
- あなたが持っている"特定のアクセス権限"。

タスク概要

診断ページでは、グリッドの現在の状態に関する一連の診断チェックを実行します。各診断チェックには、次の 3 つのステータスのいずれかがあります。

- 正常: すべての値が正常範囲内です。
- 注意: 1 つ以上の値が正常範囲外です。
- 注意: 1 つ以上の値が正常範囲から大幅に外れています。

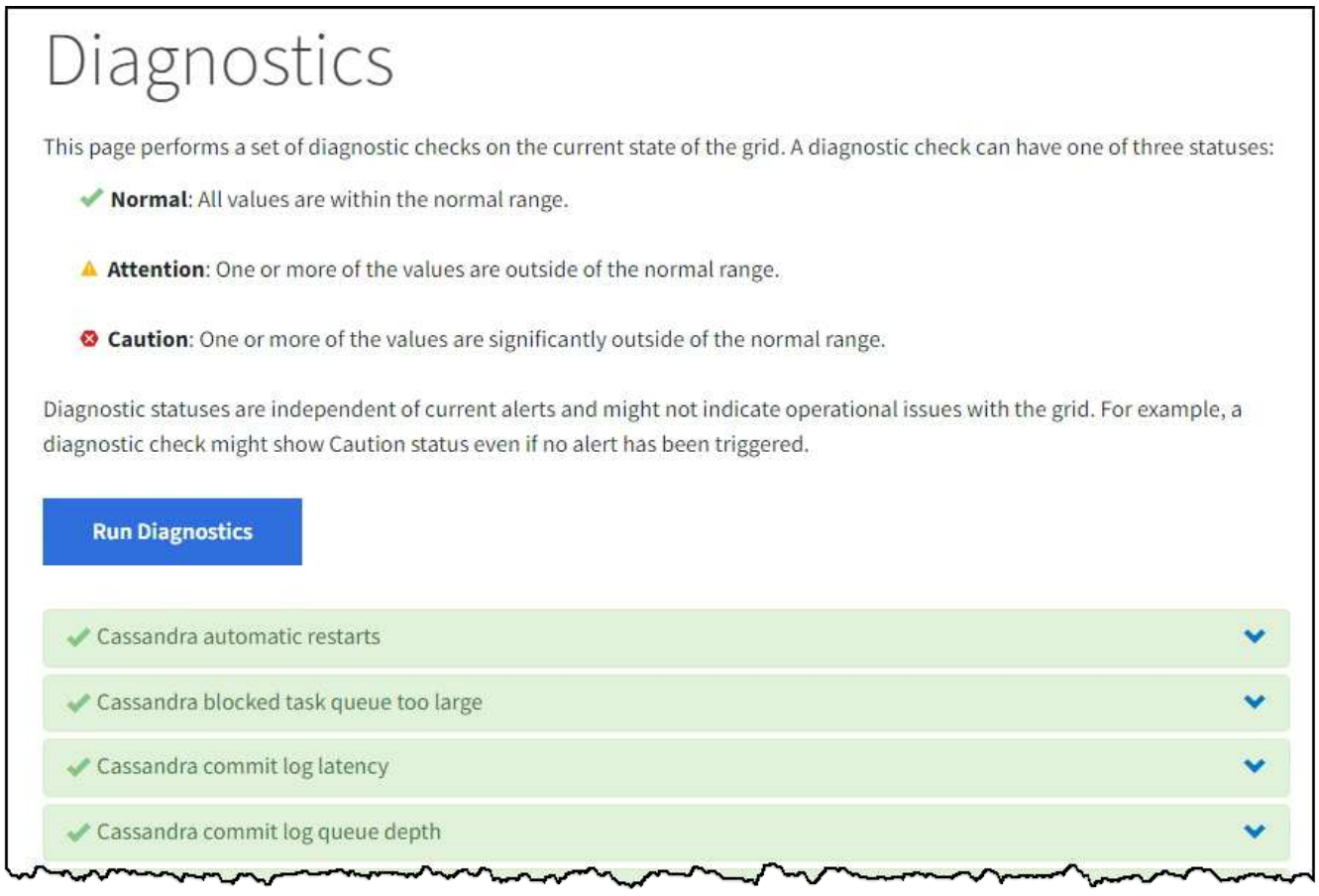
診断ステータスは現在のアラートとは無関係であり、グリッドの運用上の問題を示すものではない可能性があります。たとえば、アラートがトリガーされていない場合でも、診断チェックで注意ステータスが表示される場合があります。

手順

1. サポート > ツール > *診断*を選択します。

   「診断」ページが表示され、各診断チェックの結果がリストされます。結果は重大度順（注意、注目、正常）にソートされます。各重大度内で、結果はアルファベット順に並べられます。

   この例では、すべての診断のステータスは正常です。



2. 特定の診断の詳細を確認するには、行内の任意の場所をクリックします。

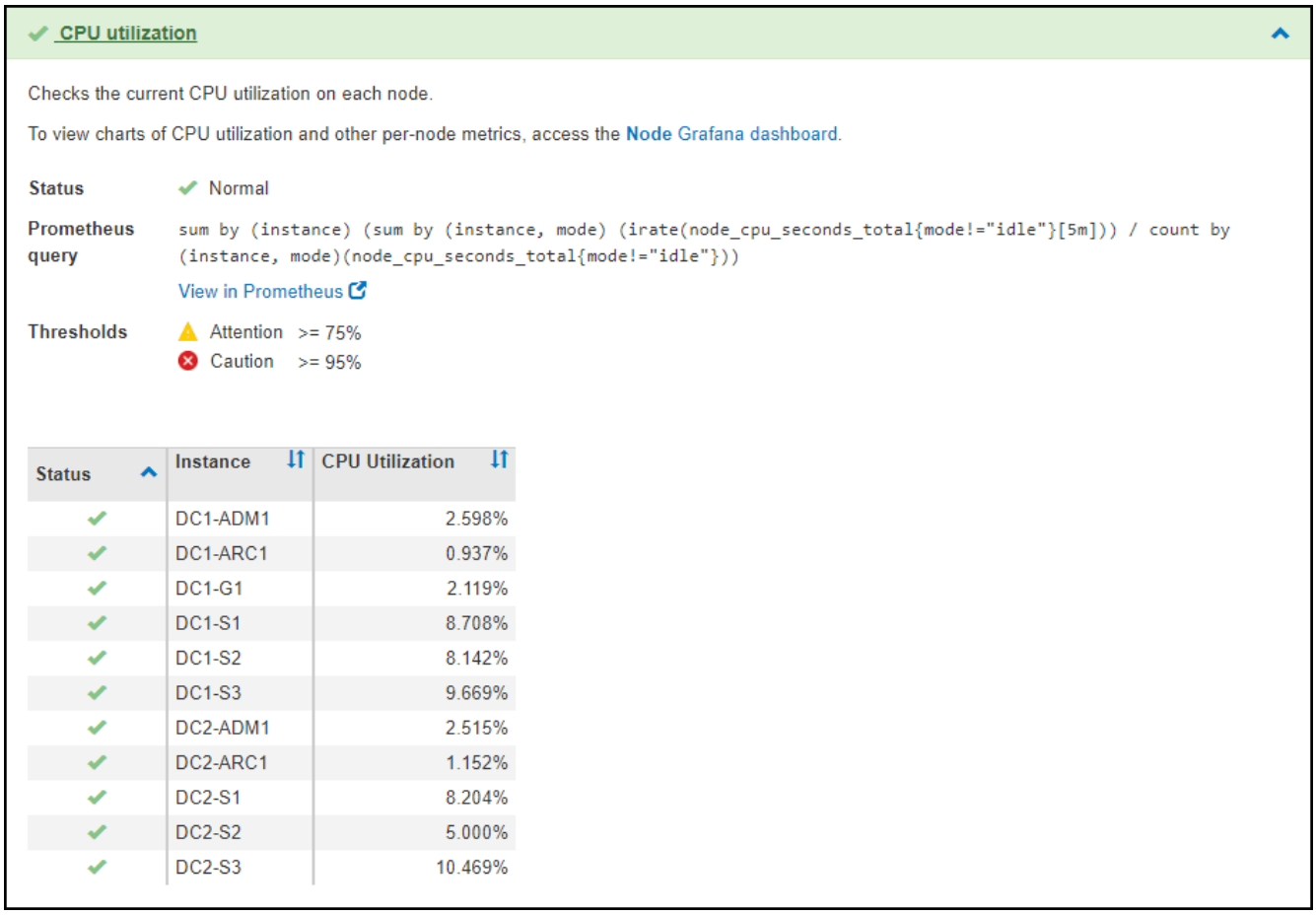
   診断の詳細と現在の結果が表示されます。以下の詳細がリストされます:

   - ステータス: この診断の現在のステータス: 正常、注意、または注意。
   - **Prometheus** クエリ: 診断に使用する場合、ステータス値を生成するために使用された Prometheus 式。 (Prometheus 式はすべての診断に使用されるわけではありません。)

- しきい値: 診断で使用可能な場合、各異常診断ステータスのシステム定義のしきい値。(しきい値はすべての診断に使用されるわけではありません。)

  これらのしきい値を変更することはできません。

- ステータス値: StorageGRIDシステム全体の診断のステータスと値を示す表。この例では、StorageGRIDシステム内の各ノードの現在の CPU 使用率が表示されます。すべてのノード値が「注意」および「警告」のしきい値を下回っているため、診断の全体的なステータスは「正常」です。



3. オプション: この診断に関連する Grafana チャートを表示するには、**Grafana** ダッシュボード リンクをクリックします。

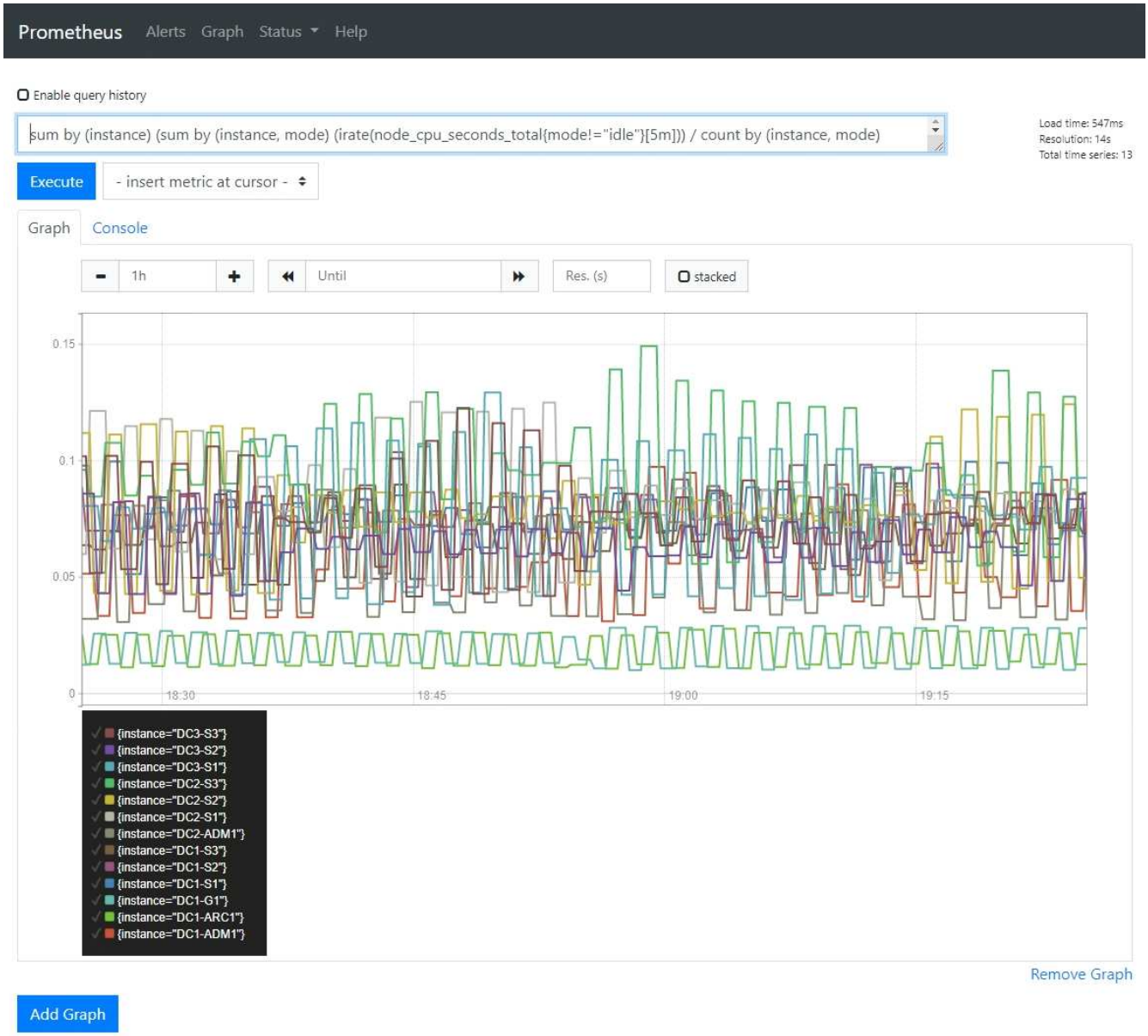
   このリンクはすべての診断で表示されるわけではありません。

   関連する Grafana ダッシュボードが表示されます。この例では、ノード ダッシュボードが表示され、このノードの CPU 使用率の推移と、ノードのその他の Grafana チャートが表示されます。

   サポート > ツール > メトリック ページの Grafana セクションから、事前に構築された Grafana ダッシュボードにアクセスすることもできます。

4. オプション: Prometheus 式のグラフを時間経過に沿って表示するには、[**Prometheus** で表示] をクリックします。

   診断で使用される式の Prometheus グラフが表示されます。



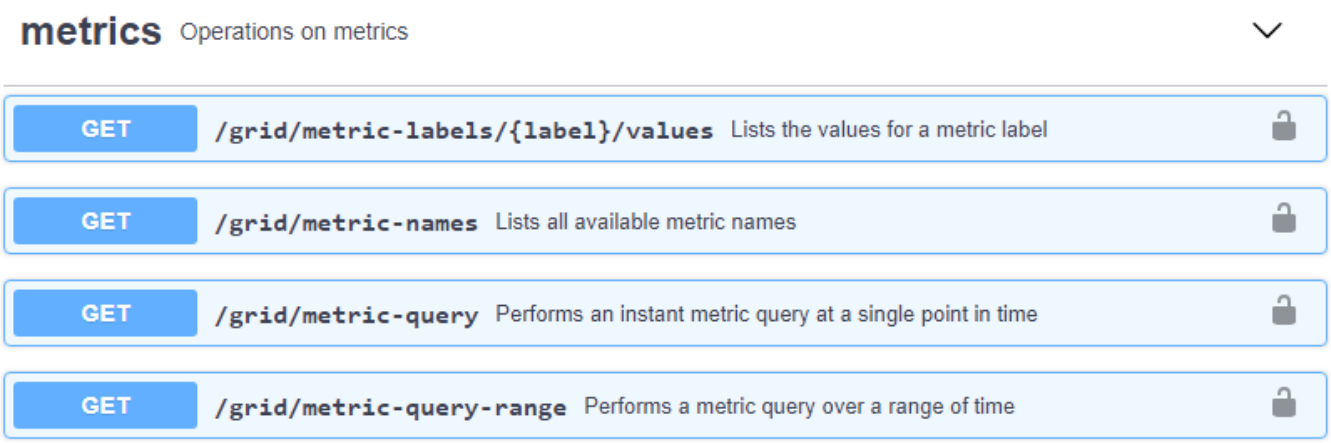
カスタム監視アプリケーションを作成する

Grid Management API から利用できるStorageGRIDメトリックを使用して、カスタム監視アプリケーションとダッシュボードを構築できます。

Grid Manager の既存のページに表示されないメトリックを監視する場合、またはStorageGRIDのカスタム ダッシュボードを作成する場合は、Grid Management API を使用してStorageGRIDメトリックを照会できます。

Grafana などの外部監視ツールを使用して Prometheus メトリックに直接アクセスすることもできます。外部ツールを使用するには、セキュリティのためにStorageGRID がツールを認証できるように、管理クライアント証明書をアップロードまたは生成する必要があります。参照"StorageGRIDの管理手順"。

使用可能なメトリックの完全なリストを含むメトリック API 操作を表示するには、グリッド マネージャーに移動します。ページの上部からヘルプ アイコンを選択し、**API** ドキュメント > メトリック を選択します。



カスタム監視アプリケーションの実装方法の詳細については、このドキュメントの範囲外です。

StorageGRIDシステムのトラブルシューティング

StorageGRIDシステムのトラブルシューティング

StorageGRIDシステムの使用中に問題が発生した場合は、このセクションのヒントとガイドラインを参照して、問題を特定し解決してください。

多くの場合、問題は自分で解決できますが、一部の問題はテクニカル サポートにエスカレーションする必要がある場合もあります。

問題を定義する

問題を解決するための第一歩は、問題を明確に定義することです。

この表は、問題を定義するために収集する可能性のある情報の種類の例を示しています。

質問	回答例
StorageGRIDシステムは何を実行し、何を実行しないのでしょうか? その症状は何ですか?	クライアント アプリケーションは、オブジェクトをStorageGRIDに取り込むことができないと報告しています。
問題はいつ始まったのですか?	オブジェクトの取り込みは、2020 年 1 月 8 日の 14:50 頃に初めて拒否されました。
最初に問題に気づいたのは何ですか?	クライアント アプリケーションから通知されました。アラートメール通知も受信しました。
問題は継続的に発生しますか、それとも時々だけ発生しますか?	問題は継続中です。

質問	回答例
問題が定期的に発生する場合、どのような手順で発生するか	クライアントがオブジェクトを取り込もうとするたびに問題が発生します。
問題が断続的に発生する場合、いつ発生しますか? 把握している各インシデントの時間を記録します。	問題は断続的に発生するものではありません。
これまでにこの問題を見たことがありますか? 過去にこの問題がどのくらいの頻度で発生しましたか?	この問題を見るのは今回が初めてです。

システムへのリスクと影響を評価する

問題を定義したら、 StorageGRIDシステムに対するリスクと影響を評価します。たとえば、重大なアラートが発生しているからといって、必ずしもシステムがコア サービスを提供していないということではありません。

この表は、例の問題がシステム運用に与える影響をまとめたものです。

質問	回答例
StorageGRIDシステムはコンテンツを取り込むことができますか?	デスティネーション
クライアント アプリケーションはコンテンツを取得できますか?	一部のオブジェクトは取得できますが、他のオブジェクトは取得できません。
データは危険にさらされていますか?	デスティネーション
業務遂行能力に重大な影響がありますか?	はい。クライアント アプリケーションはオブジェクトをStorageGRIDシステムに保存できず、データを一貫して取得できないためです。

データを収集する

問題を定義し、そのリスクと影響を評価した後、分析用のデータを収集します。収集するのに最も役立つデータの種類は、問題の性質によって異なります。

収集するデータの種類	なぜこのデータを収集するのか	手順
最近の変更のタイムラインを作成する	StorageGRIDシステム、その構成、またはその環境に変更を加えると、新しい動作が発生する可能性があります。	• 最近の変更のタイムラインを作成する

収集するデータの種類	なぜこのデータを収集するのか	手順
アラートを確認する	アラートは、問題の原因となっている可能性のある根本的な問題に関する重要な手がかりを提供することで、問題の根本原因を迅速に特定するのに役立ちます。 現在のアラートのリストを確認し、 StorageGRID が問題の根本原因を特定したかどうかを確認します。 追加の分析情報を得るには、過去にトリガーされたアラートを確認します。	• "現在のアラートと解決済みのアラートを表示する"
イベントを監視する	イベントには、ネットワーク エラーなどのエラーを含む、ノードのシステム エラーや障害イベントが含まれます。問題の詳細を把握したり、トラブルシューティングに役立てるためにイベントを監視します。	• "イベントを監視する"
グラフやテキストレポートを使用して傾向を特定する	傾向は、問題が最初に発生した時期に関する貴重な手がかりを提供し、物事がどれだけ速く変化しているかを理解するのに役立ちます。	• "チャートやグラフを使う" • "テキストレポートを使用する"
ベースラインを確立する	さまざまな動作値の正常レベルに関する情報を収集します。これらのベースライン値と、これらのベースラインからの逸脱は、貴重な手がかりを提供します。	• ベースラインを確立する
取り込みと取得のテストを実行する	取り込みと取得に関するパフォーマンスの問題をトラブルシューティングするには、ワークステーションを使用してオブジェクトを保存および取得します。結果を、クライアント アプリケーションを使用したときに表示される結果と比較します。	• "PUTとGETのパフォーマンスを監視する"
監査メッセージを確認する	監査メッセージを確認して、 StorageGRID の操作を詳細に追跡します。監査メッセージの詳細は、パフォーマンスの問題を含むさまざまな種類の問題のトラブルシューティングに役立ちます。	• "監査メッセージを確認する"
オブジェクトの場所とストレージの整合性を確認する	ストレージに問題がある場合は、オブジェクトが期待どおりの場所に配置されていることを確認してください。ストレージ ノード上のオブジェクト データの整合性を確認します。	• "オブジェクト検証操作を監視する" • "オブジェクトデータの場所を確認する" • "オブジェクトの整合性を検証する"

収集するデータの種類	なぜこのデータを収集するのか	手順
技術サポートのためのデータを収集する	テクニカル サポートでは、問題のトラブルシューティングに役立つように、データの収集や特定の情報の確認を依頼する場合があります。	• "ログファイルとシステムデータを収集する" • "AutoSupportパッケージを手動でトリガーする" • "サポート指標を確認する"

最近の変更のタイムラインを作成する

問題が発生した場合は、最近何が変わったのか、その変化がいつ起こったのかを検討する必要があります。

- StorageGRIDシステム、その構成、またはその環境に変更を加えると、新しい動作が発生する可能性があります。
- 変更のタイムラインは、どの変更が問題の原因となっている可能性があるか、また各変更が問題の進行にどのように影響したかを特定するのに役立ちます。

システムへの最近の変更の表を作成します。この表には、各変更がいつ発生したか、変更に関する関連詳細、変更の進行中に他に何が起こっていたかなどの情報が含まれます。

変化の時	変更の種類	詳細
例えば： • ノードリカバリをいつ開始しましたか? • ソフトウェアのアップグレードはいつ完了しましたか? • プロセスを中断しましたか?	どうしたの？あなたは何をしましたか？	変更に関する関連する詳細を文書化します。例えば： • ネットワーク変更の詳細。 • どの修正プログラムがインストールされたか。 • クライアントのワークロードがどのように変化したか。 複数の変更が同時に発生していた場合は必ず注意してください。たとえば、この変更はアップグレードの進行中に行われましたか?

最近の重要な変化の例

潜在的に重要な変更の例をいくつか示します。

- StorageGRIDシステムは最近インストール、拡張、または回復されましたか?
- 最近システムはアップグレードされましたか? 修正プログラムは適用されましたか?
- 最近、ハードウェアが修理または変更されましたか?
- ILM ポリシーは更新されましたか?
- クライアントのワークロードは変化しましたか?

- クライアント アプリケーションまたはその動作は変更されましたか?
- ロード バランサーを変更しましたか? あるいは、管理ノードまたはゲートウェイ ノードの高可用性グループを追加または削除しましたか?
- 完了までに長い時間がかかる可能性があるタスクは開始されていますか? 例:
  - 障害が発生したストレージノードの復旧
  - ストレージノードの廃止
- テナントの追加や LDAP 構成の変更など、ユーザー認証に変更が加えられましたか?
- データの移行は行われていますか?
- プラットフォーム サービスは最近有効化または変更されましたか?
- 最近コンプライアンスが有効になりましたか?
- クラウド ストレージ プールは追加または削除されましたか?
- ストレージの圧縮や暗号化に変更はありましたか?
- ネットワーク インフラストラクチャに何か変更はありましたか? たとえば、VLAN、ルーター、DNS などです。
- NTP ソースに変更はありましたか?
- グリッド、管理、またはクライアント ネットワーク インターフェイスに変更は加えられましたか?
- StorageGRIDシステムまたはその環境に他に何か変更はありましたか?

ベースラインを確立する

さまざまな動作値の通常レベルを記録することで、システムのベースラインを確立できます。将来的には、現在の値とこれらのベースラインを比較して、異常な値を検出し解決することができます。

プロパティ	**Value**	入手方法
平均ストレージ消費量	1日あたりの消費GB数 1日あたりの消費量の割合	グリッド マネージャーに移動します。 [ノード] ページで、グリッド全体またはサイトを選択し、[ストレージ] タブに移動します。 「使用済みストレージ - オブジェクト データ」グラフで、線がかなり安定している期間を見つけます。チャートの上にカーソルを置くと、1日あたりに消費されるストレージの量を推定できます。 この情報は、システム全体または特定のデータセンターについて収集できます。

プロパティ	**Value**	入手方法
平均メタデータ消費量	1日あたりの消費GB数 1日あたりの消費量の割合	グリッド マネージャーに移動します。 [ノード] ページで、グリッド全体またはサイトを選択し、[ストレージ] タブに移動します。 使用済みストレージ - オブジェクト メタデータ グラフで、線がかなり安定している期間を見つけます。グラフの上にカーソルを置くと、メタデータストレージが毎日どれだけ消費されているかを推定できます。 この情報は、システム全体または特定のデータセンターについて収集できます。
S3/Swift 操作のレート	操作数/秒	グリッド マネージャー ダッシュボードで、パフォーマンス > **S3** 操作 または パフォーマンス > **Swift** 操作 を選択します。 特定のサイトまたはノードの取り込みおよび取得レートと数を確認するには、[ノード] > [サイトまたはストレージ ノード] > [オブジェクト] を選択します。S3 の取り込みと取得チャートの上にカーソルを置きます。
S3/Swift 操作が失敗しました	オペレーション	サポート > ツール > グリッド トポロジ を選択します。 API 操作セクションの [概要] タブで、[S3 操作 - 失敗] または [Swift 操作 - 失敗] の値を確認します。
ILM評価率	オブジェクト/秒	[ノード] ページで、***grid*** > **ILM** を選択します。 ILM キュー チャートで、線がかなり安定している期間を見つけます。チャートの上にカーソルを置くと、システムの*評価率*のベースライン値を推定できます。
ILMスキャンレート	オブジェクト/秒	**NODES** > ***grid*** > **ILM** を選択します。 ILM キュー チャートで、線がかなり安定している期間を見つけます。チャートの上にカーソルを置くと、システムの スキャン レート のベースライン値を推定できます。
クライアント操作からキューに入れられたオブジェクト	オブジェクト/秒	**NODES** > ***grid*** > **ILM** を選択します。 ILM キュー チャートで、線がかなり安定している期間を見つけます。グラフの上にカーソルを置くと、システムの キューに入れられたオブジェクト **(**クライアント操作から**)** のベースライン値を推定できます。

プロパティ	**Value**	入手方法
平均クエリレイテンシ	ミリ秒	**NODES** > ***Storage Node*** > **Objects** を選択します。クエリ テーブルで、平均待機時間の値を確認します。

データを分析する

収集した情報を使用して、問題の原因と考えられる解決策を特定します。

分析は問題によって異なりますが、一般的には次のようになります。

- アラートを使用して障害点とボトルネックを特定します。
- アラート履歴とグラフを使用して問題の履歴を再構築します。
- チャートを使用して異常を見つけ、問題のある状況を通常の動作と比較します。

エスカレーション情報チェックリスト

自分で問題を解決できない場合は、テクニカル サポートにお問い合わせください。テクニカル サポートに連絡する前に、問題解決を容易にするために、次の表に記載されている情報を収集してください。

✔	項目	注記
	問題の説明	問題の症状は何ですか? 問題はいつ始まったのですか? それは継続的に起こりますか、それとも断続的に起こりますか? 断続的である場合、何回発生しましたか? 問題を定義する
	影響評価	問題の深刻度はどの程度ですか? クライアント アプリケーションへの影響は何ですか? • 以前にクライアントは正常に接続したことがありますか? • クライアントはデータを取り込み、取得し、削除できますか?
	StorageGRID システム ID	メンテナンス > システム > *ライセンス*を選択します。StorageGRIDシステム ID は、現在のライセンスの一部として表示されます。
	ソフトウェア バージョン	Grid Manager の上部からヘルプ アイコンを選択し、[バージョン情報] を選択してStorageGRID のバージョンを確認します。

✔	項目	注記
	カスタマイズ	StorageGRIDシステムの構成方法を要約します。たとえば、次のものをリストします。 • グリッドはストレージ圧縮、ストレージ暗号化、またはコンプライアンスを使用していますか? • ILM は複製されたオブジェクトや消去コード化されたオブジェクトを作成しますか? ILM はサイトの冗長性を保証しますか? ILM ルールでは、Balanced、Strict、または Dual Commit の取り込み動作が使用されますか?
	ログファイルとシステムデータ	システムのログ ファイルとシステム データを収集します。サポート > ツール > ログ を選択します。 グリッド全体または選択したノードのログを収集できます。 選択したノードのログのみを収集する場合は、ADC サービスを持つストレージ ノードを少なくとも 1 つ含めるようにしてください。(サイトの最初の 3 つのストレージ ノードには ADC サービスが含まれます。) "ログファイルとシステムデータを収集する"
	ベースライン情報	取り込み操作、取得操作、およびストレージ消費に関するベースライン情報を収集します。 ベースラインを確立する
	最近の変更のタイムライン	システムまたはその環境に対する最近の変更をまとめたタイムラインを作成します。 最近の変更のタイムラインを作成する
	問題を診断するための取り組みの歴史	自分で問題を診断またはトラブルシューティングする手順を実行した場合は、実行した手順と結果を必ず記録してください。

オブジェクトとストレージの問題のトラブルシューティング

オブジェクトデータの場所を確認する

問題によっては、"オブジェクトデータが保存されている場所を確認する" 。たとえば、ILM ポリシーが期待どおりに実行され、オブジェクト データが意図した場所に保存されていることを確認したい場合があります。

開始する前に

- 次のいずれかのオブジェクト識別子が必要です:

- **UUID**: オブジェクトのユニバーサルユニーク識別子。UUID はすべて大文字で入力してください。
- **CBID**: StorageGRID内のオブジェクトの一意の識別子。監査ログからオブジェクトの CBID を取得できます。CBID はすべて大文字で入力してください。
- **S3**バケットとオブジェクトキー: オブジェクトがS3バケットを通じて取り込まれると、"S3インターフェース"クライアント アプリケーションは、バケットとオブジェクト キーの組み合わせを使用してオブジェクトを保存および識別します。

手順

1. **ILM** > オブジェクト メタデータ検索 を選択します。
2. 識別子 フィールドにオブジェクトの識別子を入力します。

   UUID、CBID、S3 バケット/オブジェクトキー、または Swift コンテナ/オブジェクト名を入力できます。

3. オブジェクトの特定のバージョンを検索する場合は、バージョン ID を入力します (オプション)。

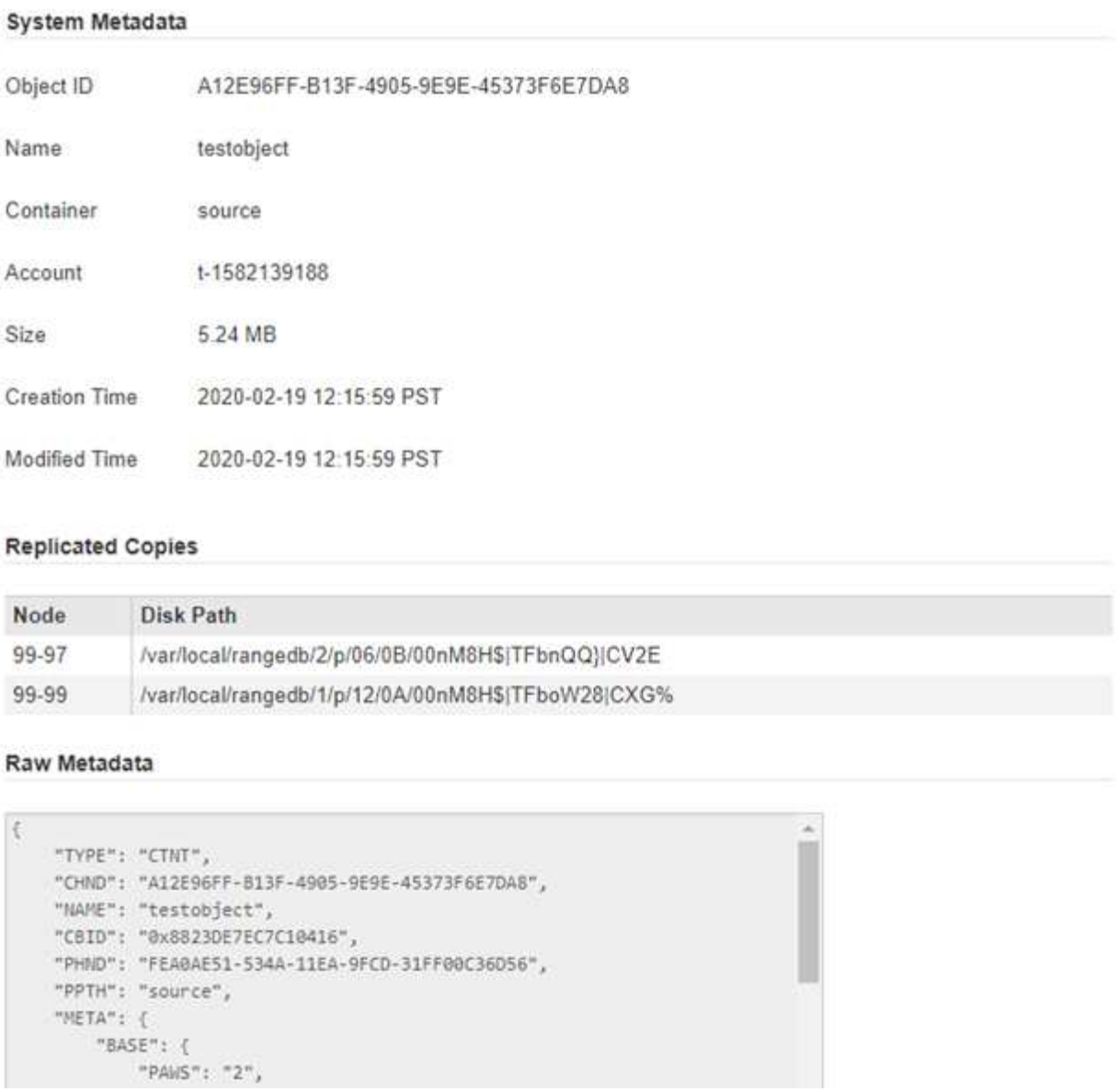
4. *検索*を選択します。

   その"オブジェクトメタデータ検索結果"現れる。このページには、次の種類の情報がリストされます。

   - システム メタデータには、オブジェクト ID (UUID)、バージョン ID (オプション)、オブジェクト名、コンテナーの名前、テナント アカウント名または ID、オブジェクトの論理サイズ、オブジェクトが最初に作成された日時、オブジェクトが最後に変更された日時が含まれます。
   - オブジェクトに関連付けられたカスタム ユーザー メタデータのキーと値のペア。
   - S3 オブジェクトの場合、オブジェクトに関連付けられたオブジェクト タグのキーと値のペア。
   - 複製されたオブジェクトのコピーの場合、各コピーの現在の保存場所。
   - 消失訂正符号化オブジェクトのコピーの場合、各フラグメントの現在の保存場所。
   - Cloud Storage プール内のオブジェクト コピーの場合、外部バケットの名前とオブジェクトの一意の識別子を含むオブジェクトの場所。
   - セグメント化されたオブジェクトおよびマルチパート オブジェクトの場合、セグメント識別子とデータ サイズを含むオブジェクト セグメントのリスト。 100 を超えるセグメントを持つオブジェクトの場合、最初の 100 セグメントのみが表示されます。
   - 未処理の内部ストレージ形式のすべてのオブジェクト メタデータ。この生のメタデータには、リリース間で保持されることが保証されていない内部システム メタデータが含まれます。

     次の例は、2 つの複製されたコピーとして保存されている S3 テスト オブジェクトのオブジェクト メ

タデータ検索結果を示しています。



オブジェクトストア（ストレージボリューム）の障害

ストレージ ノード上の基盤となるストレージは、オブジェクト ストアに分割されます。オブジェクト ストアは、ストレージ ボリュームとも呼ばれます。

各ストレージ ノードのオブジェクト ストア情報を表示できます。オブジェクト ストアは、**NODES** > ***Storage Node*** > **Storage** ページの下部に表示されます。

Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
sdc(8:16,sdb)	N/A	0.05%	0 bytes/s	4 KB/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s
sdf(8:64,sde)	N/A	0.00%	0 bytes/s	82 bytes/s
sdg(8:80,sdf)	N/A	0.00%	0 bytes/s	82 bytes/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	4 KB/s
cvloc(8:2,sda2)	N/A	0.95%	0 bytes/s	52 KB/s

Volumes

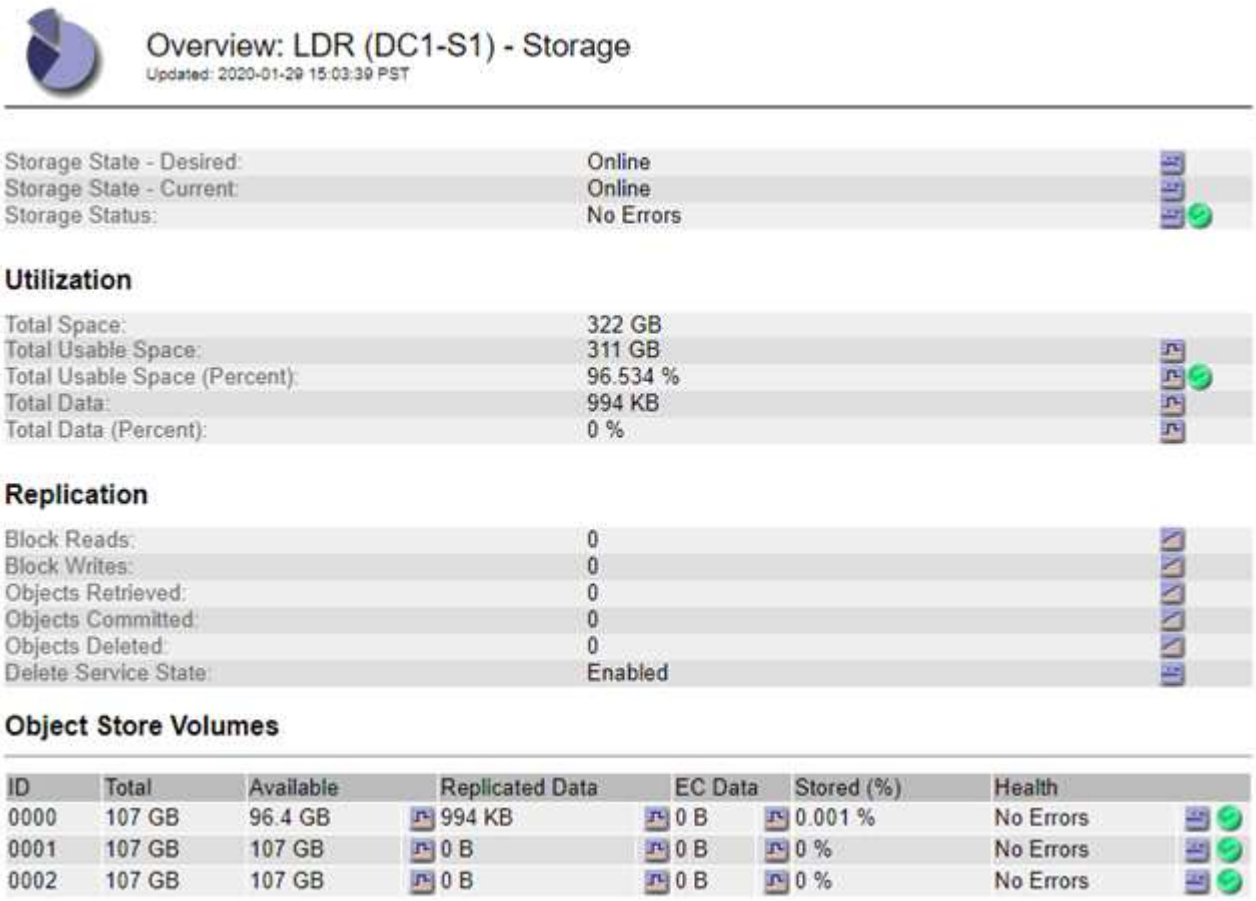
Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.73 GB	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/3	sdf	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/4	sdg	Online	107.32 GB	107.18 GB	Enabled

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	1.55 MB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0003	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0004	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

もっと見る"各ストレージノードの詳細"、次の手順に従ってください。

1. サポート > ツール > グリッド トポロジ を選択します。
2. ***site*** > ***Storage Node*** > **LDR** > **Storage** > 概要 > メイン を選択します。



障害の性質に応じて、ストレージボリュームの障害は、"ストレージボリュームアラート" 。ストレージ ボリュームに障害が発生した場合は、障害の発生したストレージ ボリュームを修復して、ストレージ ノードの完全な機能をできるだけ早く復元する必要があります。必要に応じて、[設定]タブに移動して"ストレージノードを読み取り専用状態にする"サーバーの完全復旧を準備する間に、 StorageGRIDシステムがデータ取得に使用できるようにします。

オブジェクトの整合性を検証する

StorageGRIDシステムは、ストレージ ノード上のオブジェクト データの整合性を検証し、破損したオブジェクトと欠落したオブジェクトの両方をチェックします。

検証プロセスには、バックグラウンド検証とオブジェクト存在チェック (以前はフォアグラウンド検証と呼ばれていました) の 2 つがあります。これらは連携してデータの整合性を確保します。バックグラウンド検証は自動的に実行され、オブジェクト データの正確性を継続的にチェックします。オブジェクトの存在チェックは、ユーザーがトリガーして、オブジェクトの存在（正確性ではない）をより迅速に検証することができます。

身元確認とは何ですか?

バックグラウンド検証プロセスでは、ストレージ ノードにオブジェクト データの破損したコピーがないか自動的に継続的にチェックし、見つかった問題を自動的に修復しようとします。

バックグラウンド検証では、次のように、複製されたオブジェクトと消去コード化されたオブジェクトの整合性をチェックします。

- 複製されたオブジェクト: バックグラウンド検証プロセスで破損した複製されたオブジェクトが見つかった場合、破損したコピーはその場所から削除され、ストレージ ノード上の別の場所に隔離されます。次に、アクティブな ILM ポリシーを満たすように、破損していない新しいコピーが生成されて配置されます。新しいコピーは、元のコピーに使用されたストレージ ノードに配置されない可能性があります。

> ⓘ 破損したオブジェクト データはシステムから削除されるのではなく隔離されるため、引き続きアクセスできます。隔離されたオブジェクト データへのアクセスの詳細については、テクニカル サポートにお問い合わせください。

- 消去コード化オブジェクト: バックグラウンド検証プロセスで消去コード化オブジェクトのフラグメントが破損していることが検出されると、 StorageGRID は残りのデータ フラグメントとパリティ フラグメントを使用して、同じストレージ ノード上で失われたフラグメントを自動的に再構築しようとします。破損したフラグメントを再構築できない場合は、オブジェクトの別のコピーを取得しようとします。取得が成功した場合、ILM 評価が実行され、消失訂正符号化オブジェクトの置換コピーが作成されます。

  バックグラウンド検証プロセスでは、ストレージ ノード上のオブジェクトのみがチェックされます。クラウド ストレージ プール内のオブジェクトはチェックされません。背景検証の対象となるには、オブジェクトは 4 日以上経過している必要があります。

バックグラウンド検証は、通常のシステム アクティビティを妨げないように設計された継続的な速度で実行されます。背景検証を停止することはできません。ただし、問題が疑われる場合は、バックグラウンド検証レートを上げて、ストレージ ノードの内容をより迅速に検証することができます。

身元調査に関するアラート

システムが自動的に修正できない破損したオブジェクトを検出した場合 (破損によってオブジェクトを識別できないため)、識別されていない破損したオブジェクトが検出されました というアラートがトリガーされます。

バックグラウンド検証で別のコピーが見つからないために破損したオブジェクトを置き換えることができない場合は、「オブジェクトが失われました」というアラートがトリガーされます。

背景検証率を変更する

データの整合性に懸念がある場合は、バックグラウンド検証がストレージ ノード上の複製されたオブジェクト データをチェックする頻度を変更できます。

開始する前に

- グリッドマネージャにサインインするには、"サポートされているウェブブラウザ" 。
- あなたが持っている"特定のアクセス権限"。

タスク概要

ストレージ ノードのバックグラウンド検証の検証レートを変更できます。

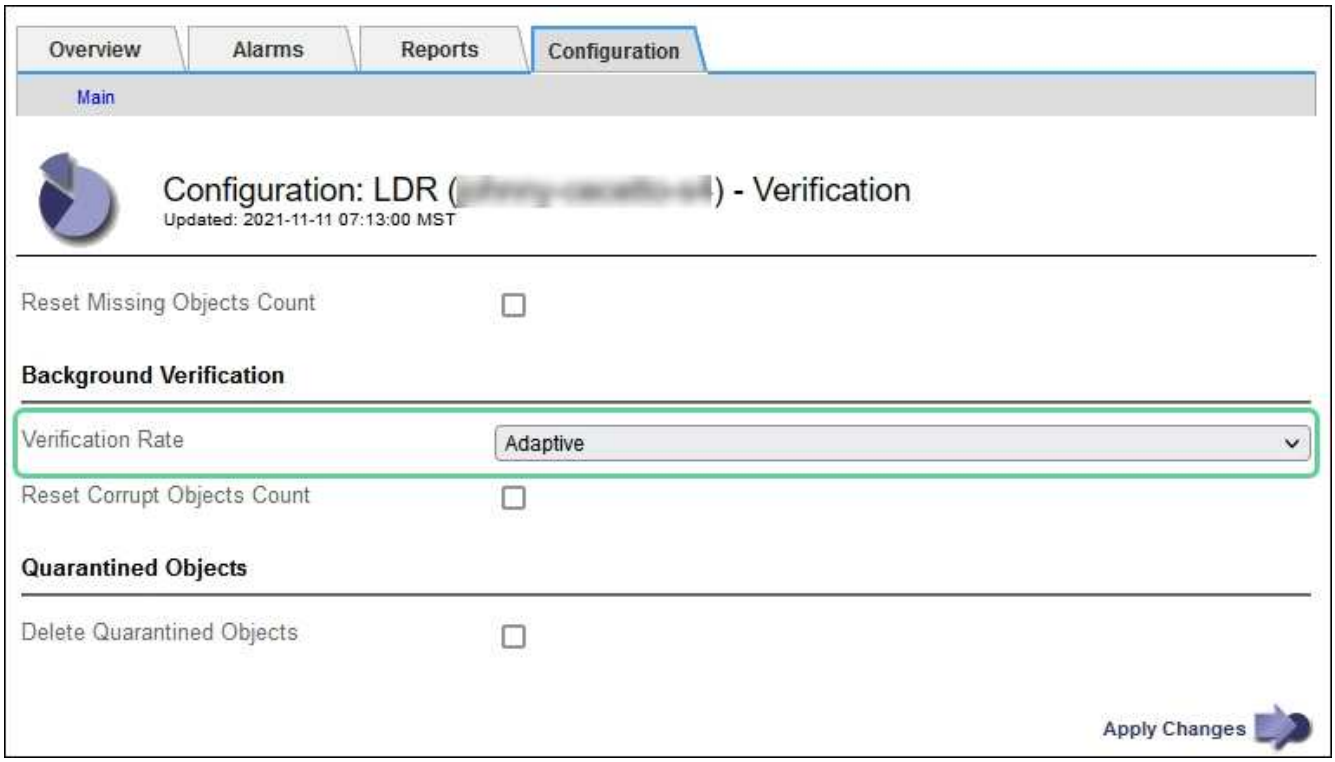
- アダプティブ: デフォルト設定。タスクは、最大 4 MB/秒または 10 オブジェクト/秒 (いずれか早い方) で検証するように設計されています。
- 高: ストレージ検証は高速で進行しますが、その速度によって通常のシステム アクティビティが遅くなる

可能性があります。

ハードウェアまたはソフトウェアの障害によってオブジェクト データが破損した可能性がある場合にのみ、高検証率を使用してください。高優先度のバックグラウンド検証が完了すると、検証レートは自動的に「適応型」にリセットされます。

手順

1. サポート > ツール > グリッド トポロジ を選択します。
2. ***Storage Node*** > **LDR** > *検証*を選択します。
3. 構成 > *メイン*を選択します。
4. **LDR** > 検証 > 構成 > メイン に移動します。
5. [バックグラウンド検証] で、[検証率] > [高] または [検証率] > [適応型] を選択します。



6. *変更を適用*をクリックします。
7. 複製されたオブジェクトのバックグラウンド検証の結果を監視します。
   a. **NODES** > ***Storage Node*** > **Objects** に移動します。
   b. 検証セクションで、*破損したオブジェクト*と*識別されていない破損オブジェクト*の値を監視します。

      バックグラウンド検証で破損した複製オブジェクト データが見つかった場合、破損オブジェクト メトリックが増加し、 StorageGRID は次のようにデータからオブジェクト識別子を抽出しようとします。

      - オブジェクト識別子を抽出できる場合、 StorageGRID はオブジェクト データの新しいコピーを自動的に作成します。新しいコピーは、アクティブな ILM ポリシーを満たすStorageGRIDシステム内の任意の場所に作成できます。
      - オブジェクト識別子を抽出できない場合 (破損しているため) は、識別されていない破損オブジェクト メトリックが増加し、識別されていない破損オブジェクトが検出されました アラートがトリ

ガーされます。

c. 破損したレプリケートされたオブジェクト データが見つかった場合は、テクニカル サポートに連絡して破損の根本原因を特定してください。

8. 消去コード化されたオブジェクトのバックグラウンド検証の結果を監視します。

   バックグラウンド検証で、消去コード化されたオブジェクト データの破損したフラグメントが見つかった場合、Corrupt Fragments Detected 属性が増加します。 StorageGRID は、破損したフラグメントを同じストレージ ノード上で再構築することで回復します。

   a. サポート > ツール > グリッド トポロジ を選択します。

   b. ***Storage Node*** > **LDR** > **Erasure Coding** を選択します。

   c. 検証結果テーブルで、破損したフラグメントの検出 (ECCD) 属性を監視します。

9. 破損したオブジェクトがStorageGRIDシステムによって自動的に復元された後、破損したオブジェクトの数をリセットします。

   a. サポート > ツール > グリッド トポロジ を選択します。

   b. ***Storage Node*** > **LDR** > 検証 > 構成 を選択します。

   c. *破損したオブジェクトの数をリセット*を選択します。

   d. *変更を適用*をクリックします。

10. 隔離されたオブジェクトが不要であると確信できる場合は、削除できます。

    *オブジェクトが失われました*アラートがトリガーされた場合、テクニカル サポートは、根本的な問題のデバッグやデータ復旧を試みるために、隔離されたオブジェクトにアクセスする場合があります。

    a. サポート > ツール > グリッド トポロジ を選択します。

    b. ***Storage Node*** > **LDR** > 検証 > 構成 を選択します。

    c. *隔離されたオブジェクトの削除*を選択します。

    d. *変更を適用*を選択します。

オブジェクト存在チェックとは何ですか?

オブジェクト存在チェックは、オブジェクトの予想されるすべての複製コピーと消去コード化フラグメントがストレージ ノード上に存在するかどうかを確認します。オブジェクト存在チェックでは、オブジェクト データ自体が検証されるわけではありません (バックグラウンド検証で実行されます)。代わりに、特に最近のハードウェアの問題がデータの整合性に影響を与えている可能性がある場合に、ストレージ デバイスの整合性を検証する方法を提供します。

自動的に実行されるバックグラウンド検証とは異なり、オブジェクト存在チェック ジョブは手動で開始する必要があります。

オブジェクト存在チェックは、 StorageGRIDに保存されているすべてのオブジェクトのメタデータを読み取り、複製されたオブジェクトのコピーと消去コード化されたオブジェクト フラグメントの両方の存在を確認します。欠落したデータは次のように処理されます。

- 複製されたコピー: 複製されたオブジェクト データのコピーが欠落している場合、 StorageGRID はシステム内の他の場所に保存されているコピーでそのコピーを自動的に置き換えようとします。ストレージ ノ

ードは、既存のコピーに対して ILM 評価を実行し、別のコピーが欠落しているため、このオブジェクトに対して現在の ILM ポリシーが満たされていないことを判断します。システムのアクティブな ILM ポリシーを満たすように新しいコピーが生成され、配置されます。この新しいコピーは、失われたコピーが保存されていた場所と同じ場所に配置されない可能性があります。

- 消去コード化されたフラグメント: 消去コード化されたオブジェクトのフラグメントが欠落している場合、 StorageGRID は残りのフラグメントを使用して、同じストレージ ノード上で欠落しているフラグメントを自動的に再構築しようとします。失われたフラグメントを再構築できない場合 (フラグメントが多すぎるため)、ILM はオブジェクトの別のコピーを見つけようとします。このコピーを使用して、新しい消失訂正符号化フラグメントを生成できます。

オブジェクトの存在チェックを実行する

一度に 1 つのオブジェクト存在チェック ジョブを作成して実行します。ジョブを作成するときに、検証するストレージ ノードとボリュームを選択します。ジョブの一貫性も選択します。

開始する前に

- グリッドマネージャにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは"メンテナンスまたはルートアクセス権限"。
- 確認するストレージ ノードがオンラインであることを確認しました。ノードのテーブルを表示するには、「**NODES**」を選択します。確認するノードのノード名の横にアラート アイコンが表示されていないことを確認します。
- 確認するノードで以下の手順が実行されていないことを確認しました。
  - ストレージノードを追加するためのグリッド拡張
  - ストレージノードの廃止
  - 障害が発生したストレージボリュームの回復
  - システムドライブに障害が発生したストレージノードの復旧
  - ECの再均衡
  - アプライアンスノードのクローン

これらの手順の進行中は、オブジェクトの存在チェックでは有用な情報は提供されません。

タスク概要

オブジェクト存在チェック ジョブは、グリッド内のオブジェクトの数、選択したストレージ ノードとボリューム、および選択した一貫性に応じて、完了するまでに数日または数週間かかる場合があります。一度に実行できるジョブは 1 つだけですが、複数のストレージ ノードとボリュームを同時に選択できます。

手順

1. メンテナンス > タスク > *オブジェクト存在チェック*を選択します。
2. *ジョブの作成*を選択します。オブジェクト存在チェックジョブの作成ウィザードが表示されます。
3. 検証するボリュームを含むノードを選択します。すべてのオンライン ノードを選択するには、列ヘッダーの ノード名 チェックボックスをオンにします。

   ノード名またはサイトで検索できます。

   グリッドに接続されていないノードを選択することはできません。

4. *続行*を選択します。
5. リスト内の各ノードに対して 1 つ以上のボリュームを選択します。ストレージ ボリューム番号またはノード名を使用してボリュームを検索できます。

   選択した各ノードのすべてのボリュームを選択するには、列ヘッダーの ストレージ ボリューム チェックボックスをオンにします。

6. *続行*を選択します。
7. ジョブの一貫性を選択します。

   一貫性により、オブジェクトの存在チェックに使用されるオブジェクト メタデータのコピーの数が決まります。

   - 強力なサイト: 単一のサイトにメタデータのコピーが 2 つあります。
   - 強力なグローバル: 各サイトにメタデータのコピーが 2 つあります。
   - すべて (デフォルト): 各サイトのメタデータの 3 つのコピーすべて。

     一貫性の詳細については、ウィザードの説明を参照してください。

8. *続行*を選択します。
9. 選択内容を確認して検証します。 「前へ」を選択すると、ウィザードの前のステップに戻り、選択内容を更新できます。

   オブジェクト存在チェック ジョブが生成され、次のいずれかが発生するまで実行されます。

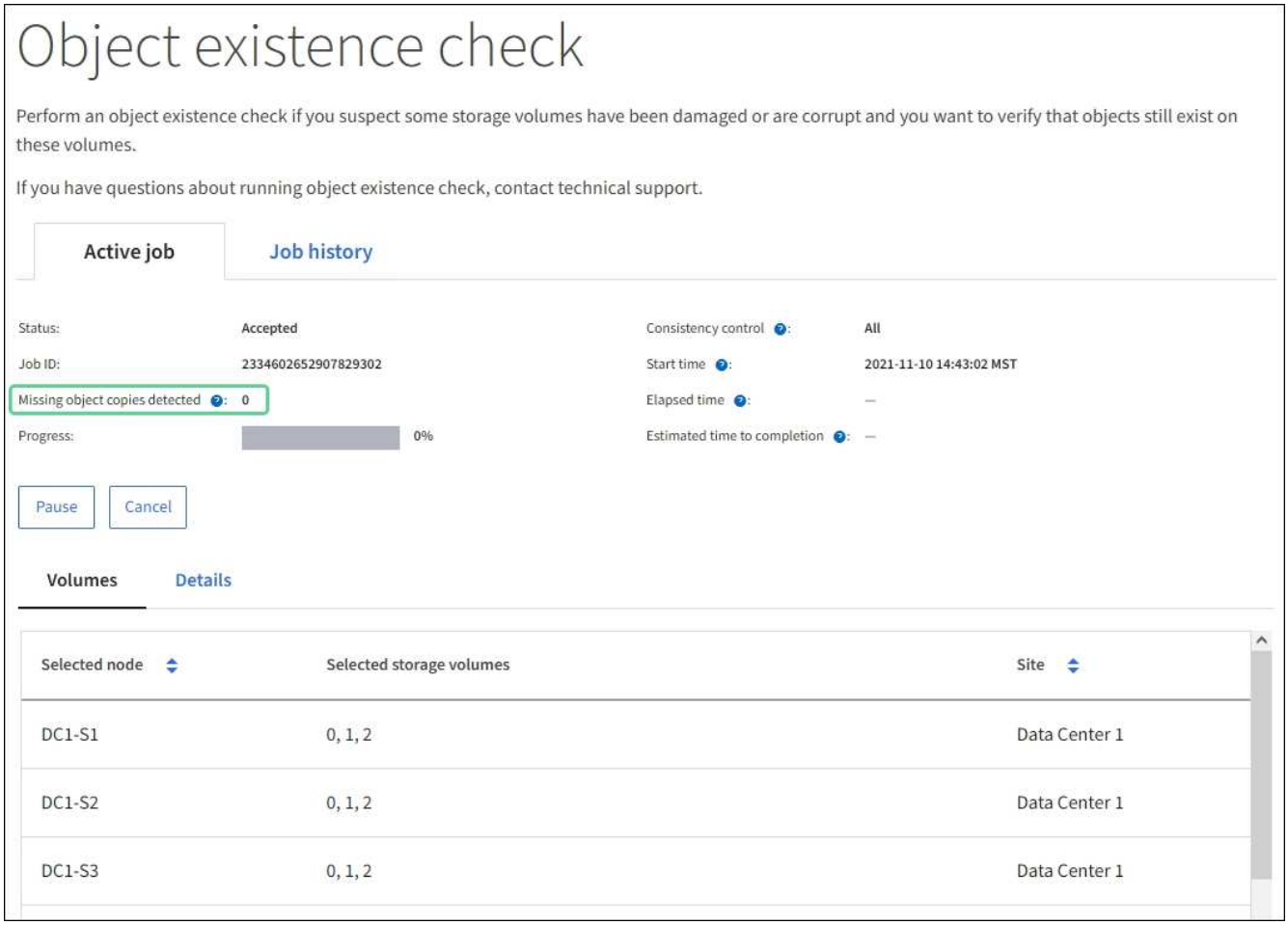
   - ジョブが完了します。
   - ジョブを一時停止またはキャンセルします。一時停止したジョブは再開できますが、キャンセルしたジョブは再開できません。
   - 仕事は行き詰まる。 *オブジェクトの存在チェックが停止しました*アラートがトリガーされます。アラートに指定された是正措置に従ってください。
   - ジョブは失敗します。 *オブジェクトの存在チェックに失敗しました*アラートがトリガーされます。アラートに指定された是正措置に従ってください。
   - 「サービスは利用できません」または「内部サーバーエラー」というメッセージが表示されます。 1 分後にページを更新してジョブの監視を続行します。

   > ⓘ 必要に応じて、オブジェクト存在チェック ページから移動し、戻ってジョブの監視を続行できます。

10. ジョブの実行中に、[アクティブ ジョブ] タブを表示し、[不足しているオブジェクトのコピーが検出されました] の値をメモします。

    この値は、複製されたオブジェクトと、1 つ以上のフラグメントが欠落している消去コード化されたオブジェクトの欠落したコピーの合計数を表します。

    検出された欠落オブジェクトのコピー数が 100 を超える場合、ストレージ ノードのストレージに問題がある可能性があります。



11. ジョブが完了したら、必要な追加のアクションを実行します。
    - 検出された欠落オブジェクトのコピーがゼロの場合、問題は見つかりませんでした。対処は不要です。
    - 検出された欠落オブジェクトのコピー数が 0 より大きく、オブジェクト損失 アラートがトリガーされていない場合、すべての欠落コピーはシステムによって修復されています。オブジェクトのコピーが将来損傷するのを防ぐために、ハードウェアの問題が修正されていることを確認します。
    - 検出されたオブジェクトのコピーの不足数がゼロより大きく、*オブジェクトが失われました*アラートがトリガーされた場合、データの整合性が影響を受ける可能性があります。テクニカル サポートにお問い合わせください。
    - grep を使用して LLST 監査メッセージを抽出することで、失われたオブジェクトのコピーを調査できます。 `grep LLST audit_file_name` 。

      この手順は、"紛失物の調査"ただし、オブジェクトのコピーを検索する場合は、 `LLST`の代わりに `OLST`。

12. ジョブに強力なサイト整合性または強力なグローバル整合性を選択した場合は、メタデータの整合性が確保されるまで約 3 週間待ってから、同じボリュームでジョブを再度実行します。

    StorageGRID がジョブに含まれるノードとボリュームのメタデータの一貫性を実現する時間があった場合、ジョブを再実行すると、誤って報告された不足しているオブジェクト コピーがクリアされるか、不足しているオブジェクト コピーがある場合は追加のオブジェクト コピーがチェックされる可能性があります。

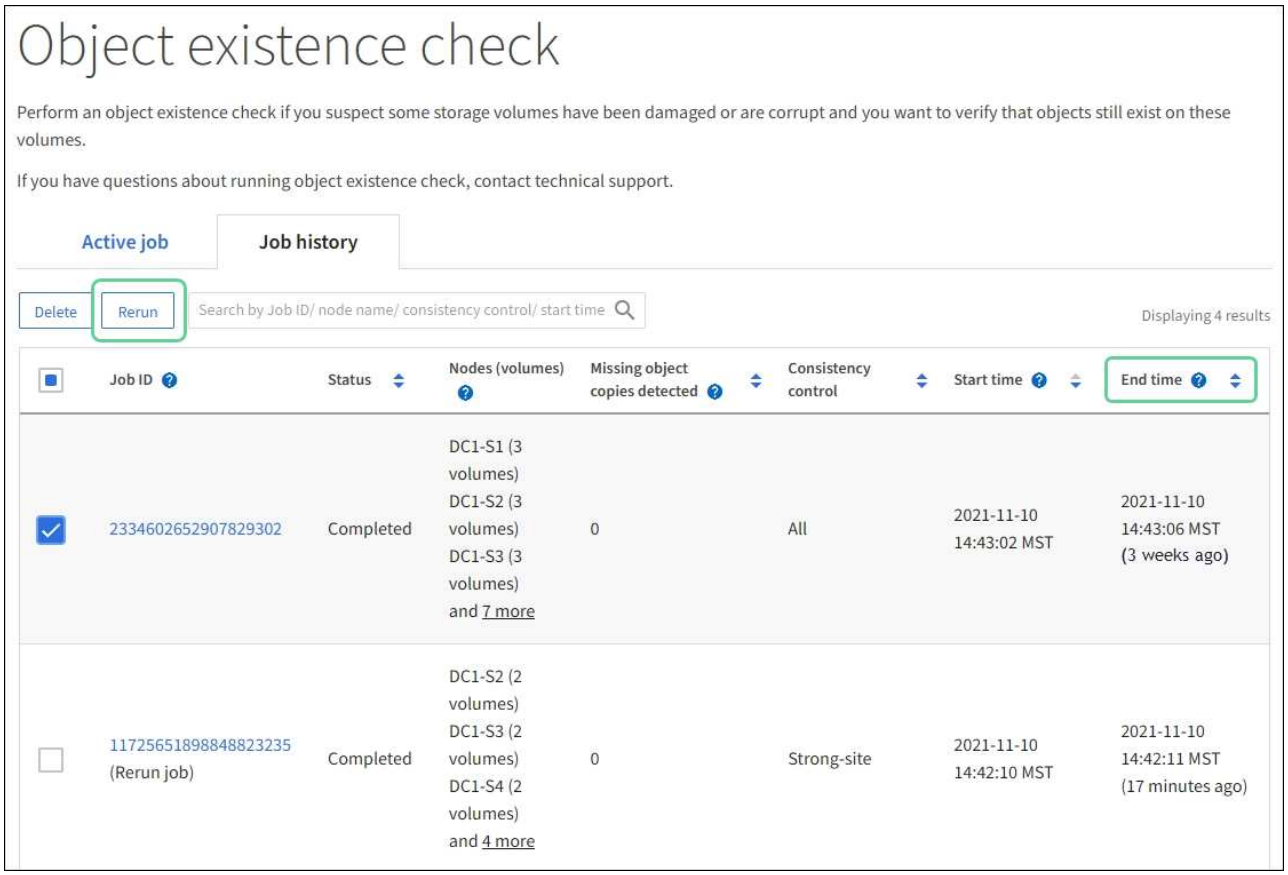
a. メンテナンス > オブジェクト存在チェック > *ジョブ履歴*を選択します。

b. 再実行の準備ができているジョブを判別します。

   i. *終了時刻*列を確認して、3 週間以上前に実行されたジョブを特定します。

   ii. これらのジョブの場合、一貫性制御列で strong-site または strong-global をスキャンします。

c. 再実行する各ジョブのチェックボックスをオンにして、「再実行」を選択します。



d. ジョブの再実行ウィザードで、選択したノードとボリュームおよび一貫性を確認します。

e. ジョブを再実行する準備ができたら、「再実行」を選択します。

アクティブジョブタブが表示されます。選択したすべてのジョブは、strong-site の一貫性で 1 つのジョブとして再実行されます。詳細セクションの 関連ジョブ フィールドには、元のジョブのジョブ ID がリストされます。

終了後の操作

データの整合性について依然として懸念がある場合は、サポート > ツール > グリッド トポロジ > ***site*** > ストレージ ノード > **LDR** > 検証 > 構成 > メイン に移動して、バックグラウンド検証率を上げてください。バックグラウンド検証では、保存されているすべてのオブジェクト データの正確性を確認し、見つかった問題を修復します。潜在的な問題をできるだけ早く発見して修復することで、データ損失のリスクを軽減できます。

S3 PUT オブジェクトサイズが大きすぎるというアラートのトラブルシューティング

テナントが 5 GiB の S3 サイズ制限を超える非マルチパート PutObject 操作を試行すると、S3 PUT オブジェクト サイズが大きすぎるというアラートがトリガーされます。

開始する前に

- グリッドマネージャにサインインするには、"サポートされているウェブブラウザ" 。
- あなたが持っている"特定のアクセス権限"。

5 GiB を超えるオブジェクトを使用するテナントを特定し、通知できるようにします。

手順

1. 構成 > 監視 > 監査および **syslog** サーバー に移動します。
2. クライアント書き込みが正常の場合は、監査ログにアクセスします。

   a. 入力 `ssh admin@primary_Admin_Node_IP`

   b. 記載されているパスワードを入力してください `Passwords.txt`ファイル。

   c. ルートに切り替えるには、次のコマンドを入力します。 `su -`

   d. 記載されているパスワードを入力してください `Passwords.txt`ファイル。

   ルートとしてログインすると、プロンプトは `$`に `#`。

   e. 監査ログが保存されているディレクトリに変更します。

   監査ログ ディレクトリと適用可能なノードは、監査の宛先設定によって異なります。

オプション	デスティネーション
ローカルノード（デフォルト）	`/var/local/log/localaudit.log`
管理ノード/ローカルノード	• 管理ノード (プライマリおよび非プライマリ): `/var/local/audit/export/audit.log` • すべてのノード: `/var/local/log/localaudit.log`このモードでは通常、ファイルは空であるか、存在しません。
外部 syslog サーバー	`/var/local/log/localaudit.log`

   監査先の設定に応じて、次のように入力します。 `cd /var/local/log`または `/var/local/audit/export/`

   詳細については、"監査情報の送信先を選択する" 。

   f. 5 GiB を超えるオブジェクトを使用しているテナントを特定します。

      i. 入力 `zgrep SPUT * | egrep "CSIZ\(UI64\):([5-9]|[1-9][0-9]+)[0-9]{9}"`

      ii. 結果の各監査メッセージについては、 `S3AI`テナント アカウント ID を決定するフィールド。メッセージ内の他のフィールドを使用して、クライアント、バケット、およびオブジェクトによって使用された IP アドレスを判別します。

コード	説明
SAIP	ソースIP
S3AI	テナントID
S3BK	バケット
S3KY	オブジェクト
CSIZ	サイズ（バイト）

監査ログ結果の例

```
audit.log:2023-01-05T18:47:05.525999
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1672943621106262][TIME(UI64):804317333][SAIP(IPAD):"10.96.99.127"][S3AI(CSTR):"93390849266154004343"][SACC(CSTR):"bhavna"][S3AK(CSTR):"06OX85M40Q90Y280B7YT"][SUSR(CSTR):"urn:sgws:identity::93390849266154004343:root"][SBAI(CSTR):"93390849266154004343"][SBAC(CSTR):"bhavna"][S3BK(CSTR):"test"][S3KY(CSTR):"large-object"][CBID(UI64):0x077EA25F3B36C69A][UUID(CSTR):"A80219A2-CD1E-466F-9094-
B9C0FDE2FFA3"][CSIZ(UI64):6040000000][MTME(UI64):1672943621338958][AVER(UI32):10][ATIM(UI64):1672944425525999][ATYP(FC32):SPUT][ANID(UI32):12220829][AMID(FC32):S3RQ][ATID(UI64):4333283179807659119]]
```

3. クライアント書き込みが正常でない場合は、アラートのテナント ID を使用してテナントを識別します。

   a. サポート > ツール > ログ に移動します。アラート内のストレージ ノードのアプリケーション ログを収集します。アラートの前後 15 分を指定します。

   b. ファイルを解凍して `bycast.log`:

      ```
      /GID<grid_id>_<time_stamp>/<site_node>/<time_stamp>/grid/bycast.log
      ```

   c. ログを検索する `method=PUT`そしてクライアントを識別します `clientIP`分野。

      bycast.logの例

      ```
      Jan  5 18:33:41 BHAVNAJ-DC1-S1-2-65 ADE: |12220829 1870864574 S3RQ %CEA 2023-01-05T18:33:41.208790| NOTICE   1404 af23cb66b7e3efa5 S3RQ: EVENT_PROCESS_CREATE - connection=1672943621106262 method=PUT name=</test/4MiB-0> auth=<V4> clientIP=<10.96.99.127>
      ```

4. PutObject の最大サイズは 5 GiB であり、5 GiB を超えるオブジェクトにはマルチパートアップロードを

使用するようにテナントに通知します。

5. アプリケーションが変更された場合は、1 週間アラートを無視してください。

失われたオブジェクトデータのトラブルシューティング

失われたオブジェクトデータのトラブルシューティング

オブジェクトは、クライアント アプリケーションからの読み取り要求、複製されたオブジェクト データのバックグラウンド検証、ILM の再評価、ストレージ ノードの回復中のオブジェクト データの復元など、さまざまな理由で取得できます。

StorageGRIDシステムは、オブジェクトのメタデータ内の場所情報を使用して、オブジェクトを取得する場所を決定します。オブジェクトのコピーが予期された場所に見つからない場合、システムは、ILM ポリシーにオブジェクトのコピーを 2 つ以上作成するルールが含まれていると想定して、システム内の他の場所からオブジェクトの別のコピーを取得しようとします。

この取得が成功すると、 StorageGRIDシステムはオブジェクトの失われたコピーを置き換えます。それ以外の場合は、次のように「オブジェクトが失われました」というアラートがトリガーされます。

- 複製されたコピーの場合、別のコピーを取得できない場合、オブジェクトは失われたとみなされ、アラートがトリガーされます。
- 消去コード化されたコピーの場合、予想される場所からコピーを取得できない場合、別の場所からコピーを取得しようとする前に、破損コピー検出 (ECOR) 属性が 1 増加します。他のコピーが見つからない場合、アラートがトリガーされます。

すべての「オブジェクト損失」アラートをただちに調査して、損失の根本原因を特定し、オブジェクトがオフラインまたは現在利用できないストレージ ノードにまだ存在するかどうかを確認する必要があります。見る"紛失物の調査" 。

コピーのないオブジェクト データが失われた場合、回復ソリューションはありません。ただし、既知の紛失オブジェクトによって新しい紛失オブジェクトが隠されないように、紛失オブジェクト カウンターをリセットする必要があります。見る"紛失した物や行方不明の物の数をリセットする" 。

紛失物の調査

*オブジェクト紛失*アラートがトリガーされた場合は、すぐに調査する必要があります。影響を受けるオブジェクトに関する情報を収集し、テクニカル サポートに連絡してください。

開始する前に

- グリッドマネージャにサインインするには、"サポートされているウェブブラウザ" 。
- あなたが持っている"特定のアクセス権限"。
- あなたは `Passwords.txt`ファイル。

タスク概要

オブジェクトが失われました アラートは、 StorageGRID がグリッド内にオブジェクトのコピーが存在しないと判断していることを示します。データは永久に失われた可能性があります。

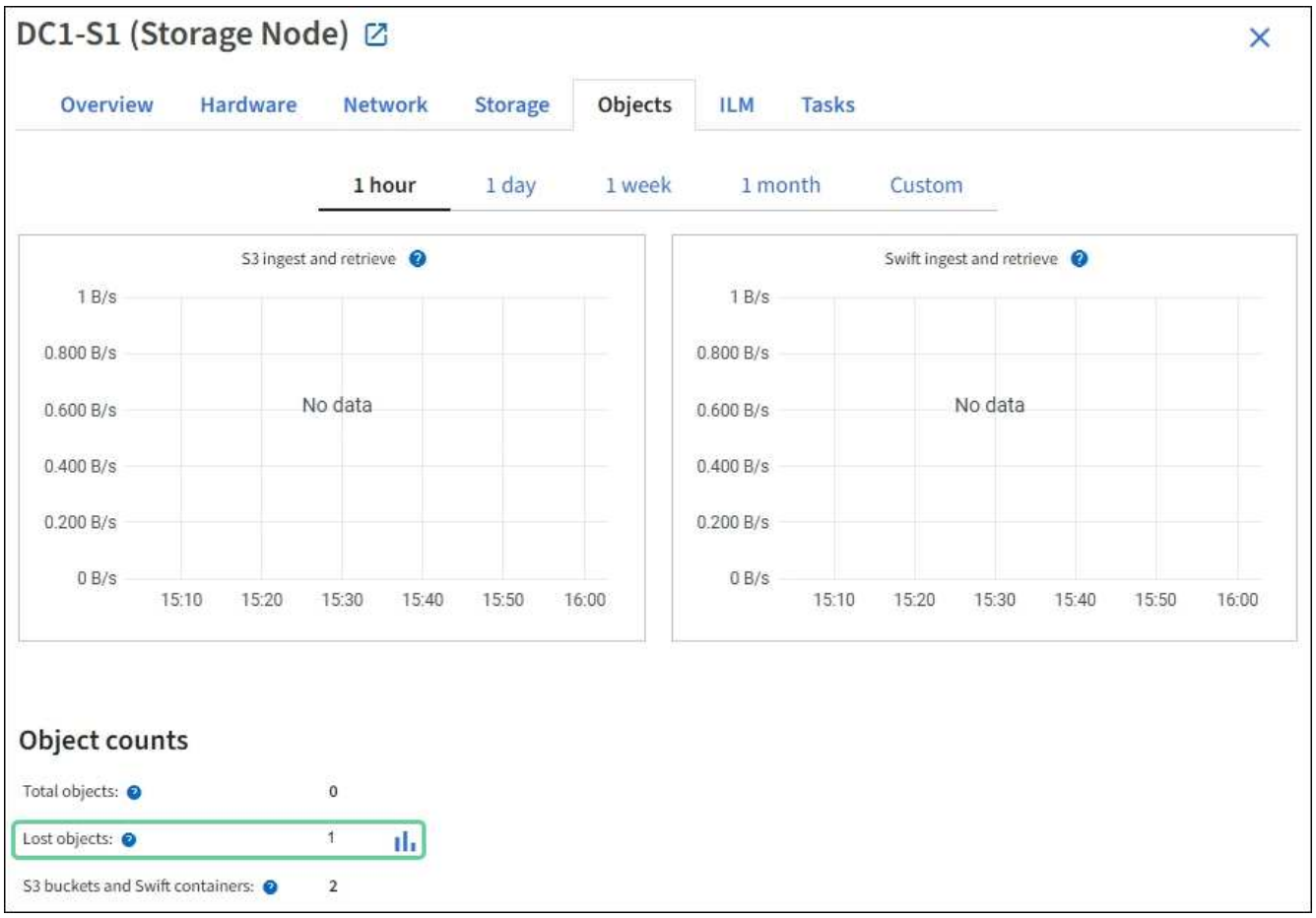
紛失物アラートを直ちに調査してください。さらなるデータ損失を防ぐために、対策を講じる必要がある場合

があります。場合によっては、迅速な対応を行えば、失われたオブジェクトを復元できる可能性があります。

手順

1. 「NODES」を選択します。
2. ストレージノード > *オブジェクト*を選択します。
3. オブジェクト数テーブルに表示されている紛失オブジェクトの数を確認します。

   この数値は、このグリッド ノードがStorageGRIDシステム全体から欠落していると検出したオブジェクトの合計数を示します。この値は、LDR および DDS サービス内のデータ ストア コンポーネントの失われたオブジェクト カウンターの合計です。



4. 管理ノードから、"監査ログにアクセスする" *オブジェクト紛失*アラートをトリガーしたオブジェクトの一意の識別子 (UUID) を判別するには:
   a. グリッド ノードにログインします。
      i. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
      ii. 記載されているパスワードを入力してください `Passwords.txt`ファイル。
      iii. ルートに切り替えるには、次のコマンドを入力します。 `su -`
      iv. 記載されているパスワードを入力してください `Passwords.txt`ファイル。ルートとしてログインすると、プロンプトは `$`に `#`。
   b. 監査ログが保存されているディレクトリに変更します。

監査ログ ディレクトリと適用可能なノードは、監査の宛先設定によって異なります。

オプション	デスティネーション
ローカルノード（デフォルト）	`/var/local/log/localaudit.log`
管理ノード/ローカルノード	• 管理ノード (プライマリおよび非プライマリ): `/var/local/audit/export/audit.log` • すべてのノード: `/var/local/log/localaudit.log`このモードでは通常、ファイルは空であるか、存在しません。
外部 syslog サーバー	`/var/local/log/localaudit.log`

監査先の設定に応じて、次のように入力します。 `cd /var/local/log`または `/var/local/audit/export/`

詳細については、"監査情報の送信先を選択する" 。

c. grep を使用して、オブジェクト損失 (OLST) 監査メッセージを抽出します。入力： `grep OLST audit_file_name`

d. メッセージに含まれる UUID 値をメモします。

```
Admin: # grep OLST audit.log
2020-02-12T19:18:54.780426
[AUDT:[CBID(UI64):0x38186FE53E3C49A5][UUID(CSTR):"926026C4-00A4-449B-
AC72-BCCA72DD1311"]
[PATH(CSTR):"source/cats"][NOID(UI32):12288733][VOLI(UI64):3222345986
][RSLT(FC32):NONE][AVER(UI32):10]
[ATIM(UI64):1581535134780426][ATYP(FC32):OLST][ANID(UI32):12448208][A
MID(FC32):ILMX][ATID(UI64):7729403978647354233]]
```

5. UUID を使用して、失われたオブジェクトのメタデータを検索します。

a. **ILM** > オブジェクト メタデータ検索 を選択します。

b. UUIDを入力し、「検索」を選択します。

c. メタデータ内の場所を確認し、適切なアクションを実行します。

メタデータ	まとめ
オブジェクト <object_identifier> が見つかりません	オブジェクトが見つからない場合は、メッセージ「ERROR":""」が返されます。 オブジェクトが見つからない場合は、「失われたオブジェクト」のカウントをリセットしてアラートをクリアできます。オブジェクトがない場合は、オブジェクトが意図的に削除されたことを示します。

メタデータ	まとめ
場所 > 0	出力に場所がリストされている場合、「オブジェクトが失われました」アラートは誤検知である可能性があります。 オブジェクトが存在することを確認します。出力にリストされているノード ID とファイル パスを使用して、オブジェクト ファイルがリストされている場所にあることを確認します。 （手順"紛失した可能性のある物を探す"ノード ID を使用して正しいストレージ ノードを見つける方法について説明します。 オブジェクトが存在する場合は、「失われたオブジェクト」の数をリセットしてアラートをクリアできます。
場所 = 0	出力に場所がリストされていない場合は、オブジェクトが欠落している可能性があります。試してみることができます"オブジェクトを検索して復元する"ご自身で確認いただくか、テクニカル サポートにお問い合わせください。 テクニカル サポートから、ストレージ回復手順が進行中かどうかを確認するよう依頼される場合があります。に関する情報を見る"グリッド マネージャーを使用してオブジェクト データを復元する"そして"オブジェクトデータをストレージボリュームに復元する"。

紛失した可能性のあるオブジェクトを検索して復元する

*オブジェクト紛失*アラートと従来の紛失オブジェクト (LOST) アラームをトリガーし、紛失の可能性があると特定されたオブジェクトを見つけて復元できる可能性があります。

開始する前に

- 紛失したオブジェクトのUUIDは、"紛失物の調査" 。
- あなたは `Passwords.txt`ファイル。

タスク概要

この手順に従って、グリッド内の他の場所で失われたオブジェクトの複製されたコピーを探すことができます。ほとんどの場合、紛失した物は見つかりません。ただし、場合によっては、迅速な対応を行えば、失われた複製オブジェクトを見つけて復元できる可能性があります。

この手順に関するサポートについては、テクニカル サポートにお問い合わせください。

手順

1. 管理ノードから、監査ログでオブジェクトの可能性のある場所を検索します。

   a. グリッド ノードにログインします。

      i. 次のコマンドを入力します。 `ssh admin@grid_node_IP`

ii. 記載されているパスワードを入力してください `Passwords.txt`ファイル。

iii. ルートに切り替えるには、次のコマンドを入力します。 `su -`

iv. 記載されているパスワードを入力してください `Passwords.txt`ファイル。ルートとしてログインすると、プロンプトは `$`に `#`。

b. 監査ログが保存されているディレクトリに変更します。

監査ログ ディレクトリと適用可能なノードは、監査の宛先設定によって異なります。

オプション	デスティネーション
ローカルノード（デフォルト）	`/var/local/log/localaudit.log`
管理ノード/ローカルノード	• 管理ノード (プライマリおよび非プライマリ): `/var/local/audit/export/audit.log` • すべてのノード: `/var/local/log/localaudit.log`このモードでは通常、ファイルは空であるか、存在しません。
外部 syslog サーバー	`/var/local/log/localaudit.log`

監査先の設定に応じて、次のように入力します。 `cd /var/local/log`または `/var/local/audit/export/`

詳細については、"監査情報の送信先を選択する" 。

c. grepを使用して抽出します"失われた可能性のあるオブジェクトに関連付けられた監査メッセージ"出力ファイルに送信します。入力： `grep uuid-value audit_file_name > output_file_name`

例えば：

```
Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
/var/local/tmp/messages_about_lost_object.txt
```

d. grep を使用して、この出力ファイルから Location Lost (LLST) 監査メッセージを抽出します。入力： `grep LLST output_file_name`

例えば：

```
Admin: # grep LLST /var/local/tmp/messages_about_lost_objects.txt
```

LLST 監査メッセージは、このサンプル メッセージのようになります。

```
[AUDT:[NOID(UI32):12448208][CBIL(UI64):0x38186FE53E3C49A5]
[UUID(CSTR):"926026C4-00A4-449B-AC72-BCCA72DD1311"][LTYP(FC32):CLDI]
[PCLD(CSTR):"/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA#3tN6"]
[TSRC(FC32):SYST][RSLT(FC32):NONE][AVER(UI32):10][ATIM(UI64):15815351
34379225]
[ATYP(FC32):LLST][ANID(UI32):12448208][AMID(FC32):CLSM][ATID(UI64):70
868710831907434 09]]
```

e. LLST メッセージ内の PCLD フィールドと NOID フィールドを見つけます。

存在する場合、PCLD の値は、不足している複製されたオブジェクトのコピーへのディスク上の完全なパスです。 NOID の値は、オブジェクトのコピーが存在する可能性がある LDR のノード ID です。

オブジェクトの場所が見つかった場合は、オブジェクトを復元できる可能性があります。

a. この LDR ノード ID に関連付けられているストレージ ノードを検索します。グリッド マネージャーで、サポート > ツール > グリッド トポロジ を選択します。次に、データセンター > ストレージノード > **LDR** を選択します。

LDR サービスのノード ID は、ノード情報テーブルにあります。この LDR をホストしているストレージ ノードが見つかるまで、各ストレージ ノードの情報を確認します。

2. 監査メッセージに示されているストレージ ノードにオブジェクトが存在するかどうかを確認します。

a. グリッド ノードにログインします。

i. 次のコマンドを入力します。 `ssh admin@grid_node_IP`

ii. 記載されているパスワードを入力してください `Passwords.txt`ファイル。

iii. ルートに切り替えるには、次のコマンドを入力します。 `su -`

iv. 記載されているパスワードを入力してください `Passwords.txt`ファイル。

ルートとしてログインすると、プロンプトは `$`に `#`。

b. オブジェクトのファイル パスが存在するかどうかを判断します。

オブジェクトのファイル パスには、LLST 監査メッセージの PCLD の値を使用します。

たとえば、次のように入力します。

```
ls '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'
```

特殊文字をエスケープするには、コマンド内のオブジェクト ファイル パスを常に一重引用符で囲みます。

- オブジェクト パスが見つからない場合、オブジェクトは失われ、この手順を使用して復元することはできません。テクニカル サポートにお問い合わせください。

- オブジェクト パスが見つかった場合は、次の手順に進みます。見つかったオブジェクトをStorageGRIDに復元することができます。

3. オブジェクト パスが見つかった場合は、オブジェクトをStorageGRIDに復元します。
   a. 同じストレージノードから、オブジェクト ファイルの所有権を変更して、 StorageGRIDで管理できるようにします。入力： `chown ldr-user:bycast 'file_path_of_object'`
   b. LDR コンソールにアクセスするには、localhost 1402 に Telnet します。入力： `telnet 0 1402`
   c. 入力： `cd /proc/STOR`
   d. 入力： `Object_Found 'file_path_of_object'`

      たとえば、次のように入力します。

      ```
      Object_Found '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'
      ```

      発行 `Object_Found`コマンドは、オブジェクトの位置をグリッドに通知します。また、アクティブな ILM ポリシーをトリガーし、各ポリシーで指定されたとおりに追加のコピーを作成します。

      > ⓘ オブジェクトが見つかったストレージ ノードがオフラインの場合、オンラインの任意のストレージ ノードにオブジェクトをコピーできます。オブジェクトをオンライン ストレージ ノードの任意の /var/local/rangedb ディレクトリに配置します。次に、`Object_Found`オブジェクトへのファイル パスを使用してコマンドを実行します。

      - オブジェクトを復元できない場合は、 `Object_Found`コマンドは失敗します。テクニカル サポートにお問い合わせください。
      - オブジェクトがStorageGRIDに正常に復元された場合は、成功メッセージが表示されます。例えば：

        ```
        ade 12448208: /proc/STOR > Object_Found
        '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'

        ade 12448208: /proc/STOR > Object found succeeded.
        First packet of file was valid. Extracted key: 38186FE53E3C49A5
        Renamed '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6' to
        '/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila#3udu'
        ```

        次の手順に進みます。

4. オブジェクトがStorageGRIDに正常に復元された場合は、新しい場所が作成されたことを確認します。
   a. グリッドマネージャーにSign inには、"サポートされているウェブブラウザ" 。
   b. **ILM** > オブジェクト メタデータ検索 を選択します。
   c. UUIDを入力し、「検索」を選択します。
   d. メタデータを確認し、新しい場所を確認します。
5. 管理ノードから、このオブジェクトの ORLM 監査メッセージの監査ログを検索し、情報ライフサイクル

管理 (ILM) によって必要に応じてコピーが配置されていることを確認します。

a. グリッド ノードにログインします。

   i. 次のコマンドを入力します。 `ssh admin@grid_node_IP`

   ii. 記載されているパスワードを入力してください `Passwords.txt`ファイル。

   iii. ルートに切り替えるには、次のコマンドを入力します。 `su -`

   iv. 記載されているパスワードを入力してください `Passwords.txt`ファイル。ルートとしてログインすると、プロンプトは `$`に `#`。

b. 監査ログが保存されているディレクトリに変更します。参照サブステップ1.b。

c. grep を使用して、オブジェクトに関連付けられた監査メッセージを出力ファイルに抽出します。入力：`grep uuid-value audit_file_name > output_file_name`

   例えば：

```
Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
/var/local/tmp/messages_about_restored_object.txt
```

d. grep を使用して、この出力ファイルから Object Rules Met (ORLM) 監査メッセージを抽出します。入力：`grep ORLM output_file_name`

   例えば：

```
Admin: # grep ORLM /var/local/tmp/messages_about_restored_object.txt
```

   ORLM 監査メッセージは、このサンプル メッセージのようになります。

```
[AUDT:[CBID(UI64):0x38186FE53E3C49A5][RULE(CSTR):"Make 2 Copies"]
[STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"926026C4-00A4-449B-AC72-
BCCA72DD1311"]
[LOCS(CSTR):"**CLDI 12828634 2148730112**, CLDI 12745543 2147552014"]
[RSLT(FC32):SUCS][AVER(UI32):10][ATYP(FC32):ORLM][ATIM(UI64):15633982306
69]
[ATID(UI64):15494889725796157557][ANID(UI32):13100453][AMID(FC32):BCMS]]
```

a. 監査メッセージ内の LOCS フィールドを見つけます。

   存在する場合、LOCS 内の CLDI の値は、オブジェクト コピーが作成されたノード ID とボリューム ID です。このメッセージは、ILM が適用され、グリッド内の 2 つの場所に 2 つのオブジェクト コピーが作成されたことを示します。

6. "紛失した物や行方不明の物の数をリセットする"グリッド マネージャーで。

StorageGRIDシステムを調査し、記録されたすべての失われたオブジェクトが永久に失われたか、または誤報であることを確認した後、Lost Objects 属性の値を 0 にリセットできます。

開始する前に

- グリッドマネージャにサインインするには、"サポートされているウェブブラウザ" 。
- あなたが持っている"特定のアクセス権限"。

タスク概要

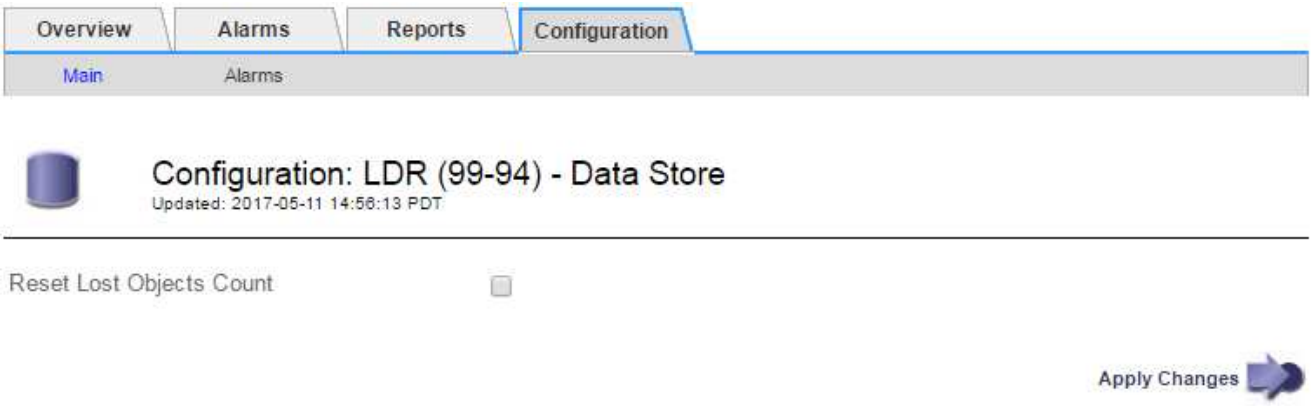
紛失したオブジェクトのカウンターは、次のいずれかのページからリセットできます。

- サポート > ツール > グリッドトポロジ > サイト > ストレージノード > **LDR** > データストア > 概要 > メイン
- サポート > ツール > グリッドトポロジ > サイト > ストレージノード > **DDS** > データストア > 概要 > メイン

これらの手順では、**LDR** > データ ストア ページからカウンターをリセットする方法を示します。

手順

1. サポート > ツール > グリッド トポロジ を選択します。
2. オブジェクト損失*アラートまたは**LOST**アラームが発生しているストレージノードの*サイト > ストレージノード > **LDR** > データストア > *構成*を選択します。
3. *紛失したオブジェクトの数をリセット*を選択します。



4. *変更を適用*をクリックします。

   紛失したオブジェクトの属性は 0 にリセットされ、オブジェクト紛失 アラートと LOST アラームがクリアされます。これには数分かかる場合があります。

5. オプションとして、失われたオブジェクトを識別するプロセスで増加した可能性のあるその他の関連属性値をリセットします。

   a. サイト > ストレージノード > **LDR** > 消去コーディング > 構成 を選択します。

   b. *読み取り失敗回数のリセット*および*破損したコピーの検出回数のリセット*を選択します。

c. *変更を適用*をクリックします。

d. サイト > ストレージノード > **LDR** > 検証 > 構成 を選択します。

e. *不足しているオブジェクトの数をリセット*および*破損したオブジェクトの数をリセット*を選択します。

f. 隔離されたオブジェクトが不要であると確信できる場合は、「隔離されたオブジェクトの削除」を選択できます。

   バックグラウンド検証によって破損した複製オブジェクトのコピーが特定されると、隔離されたオブジェクトが作成されます。ほとんどの場合、 StorageGRID は破損したオブジェクトを自動的に置き換えるため、隔離されたオブジェクトを削除しても安全です。ただし、「オブジェクトが失われました」というアラートまたは LOST アラームがトリガーされた場合、テクニカル サポートは隔離されたオブジェクトにアクセスする場合があります。

g. *変更を適用*をクリックします。

*変更を適用*をクリックした後、属性がリセットされるまでに少し時間がかかる場合があります。

低オブジェクトデータストレージアラートのトラブルシューティング

オブジェクト データ ストレージ不足 アラートは、各ストレージ ノードでオブジェクト データを格納するために使用できるスペースの量を監視します。

開始する前に

- グリッドマネージャにサインインするには、"サポートされているウェブブラウザ" 。
- あなたが持っている"特定のアクセス権限"。

タスク概要

オブジェクト データ ストレージ不足 アラートは、ストレージ ノード上の複製および消去コード化されたオブジェクト データの合計量がアラート ルールで構成された条件のいずれかを満たすときにトリガーされます。

デフォルトでは、この条件が true と評価されると、重大なアラートがトリガーされます。

```
(storagegrid_storage_utilization_data_bytes/
(storagegrid_storage_utilization_data_bytes +
storagegrid_storage_utilization_usable_space_bytes)) >=0.90
```

この状態では：

- `storagegrid_storage_utilization_data_bytes`ストレージ ノードの複製および消去コード化されたオブジェクト データの合計サイズの推定値です。
- `storagegrid_storage_utilization_usable_space_bytes`ストレージ ノードに残っているオブジェクト ストレージ スペースの合計量です。

メジャーまたはマイナーの「オブジェクト データ ストレージ不足」アラートがトリガーされた場合は、できるだけ早く拡張手順を実行する必要があります。

手順

1. **ALERTS** > **Current** を選択します。

   アラート ページが表示されます。

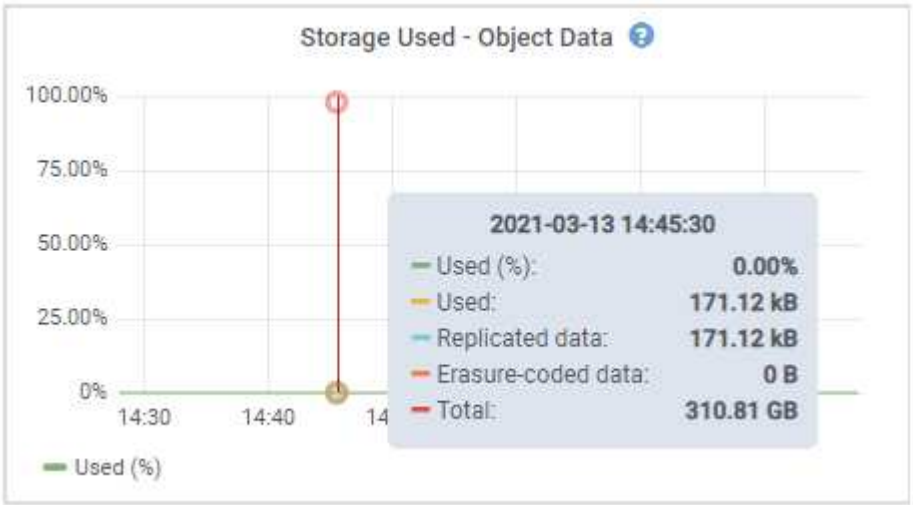
2. 必要に応じて、アラート テーブルから **Low object data storage** アラート グループを展開し、表示するアラートを選択します。

   アラートのグループの見出しではなく、アラートを選択します。

3. ダイアログ ボックスの詳細を確認し、次の点に注意してください。
   - トリガー時間
   - サイトとノードの名前
   - このアラートの指標の現在の値
4. **NODES** > ストレージ ノードまたはサイト > ストレージ を選択します。
5. 使用済みストレージ - オブジェクト データ グラフの上にカーソルを置きます。

   次の値が表示されます。

   - 使用済み **(%)**: オブジェクト データに使用されている合計使用可能スペースの割合。
   - 使用済み: オブジェクト データに使用されている合計使用可能スペースの量。
   - 複製されたデータ: このノード、サイト、またはグリッド上の複製されたオブジェクト データの量の推定値。
   - 消去コード化データ: このノード、サイト、またはグリッド上の消去コード化オブジェクト データの量の推定値。
   - 合計: このノード、サイト、またはグリッド上の使用可能なスペースの合計量。使用価値は `storagegrid_storage_utilization_data_bytes`メトリック。



6. グラフの上にある時間コントロールを選択すると、さまざまな期間にわたるストレージの使用状況が表示されます。

   ストレージの使用状況を時系列で確認すると、アラートがトリガーされる前と後にどれだけのストレージ

が使用されたかを把握し、ノードの残りのスペースがいっぱいになるまでにどれくらいの時間がかかるかを見積もるのに役立ちます。

7. できるだけ早く、"ストレージ容量を追加する"グリッドに追加します。

   既存のストレージ ノードにストレージ ボリューム (LUN) を追加したり、新しいストレージ ノードを追加したりできます。

   詳細については、以下を参照してください。 "完全なストレージノードを管理する" 。

低読み取り専用ウォーターマーク上書きアラートのトラブルシューティング

ストレージ ボリュームのウォーターマークにカスタム値を使用する場合は、読み取り専用の低いウォーターマークのオーバーライド アラートを解決する必要がある場合があります。可能であれば、最適化された値を使用するようにシステムを更新する必要があります。

以前のリリースでは、3つの"ストレージボリュームのウォーターマーク"グローバル設定であり、すべてのストレージ ノード上のすべてのストレージ ボリュームに同じ値が適用されます。 StorageGRID 11.6 以降では、ソフトウェアはストレージ ノードのサイズとボリュームの相対容量に基づいて、各ストレージ ボリュームのこれらのウォーターマークを最適化できます。

StorageGRID 11.6 以降にアップグレードすると、次のいずれかに該当しない限り、最適化された読み取り専用および読み取り/書き込みウォーターマークがすべてのストレージ ボリュームに自動的に適用されます。

- システムの容量が近づいており、最適化されたウォーターマークが適用されると新しいデータを受け入れることができなくなります。この場合、 StorageGRID はウォーターマーク設定を変更しません。
- 以前に、ストレージ ボリュームのウォーターマークのいずれかをカスタム値に設定しました。 StorageGRID は、カスタム ウォーターマーク設定を最適化された値で上書きしません。ただし、ストレージ ボリュームのソフト読み取り専用ウォーターマークのカスタム値が小さすぎる場合、 StorageGRID は*読み取り専用ウォーターマークの低いオーバーライド* アラートをトリガーする可能性があります。

警告を理解する

ストレージ ボリュームのウォーターマークにカスタム値を使用すると、1 つ以上のストレージ ノードに対して 読み取り専用ウォーターマークの低いオーバーライド アラートがトリガーされる可能性があります。

アラートの各インスタンスは、ストレージ ボリュームのソフト読み取り専用ウォーターマークのカスタム値が、そのストレージ ノードの最小最適化値よりも小さいことを示します。カスタム設定を引き続き使用すると、ストレージ ノードが安全に読み取り専用状態に移行する前に、空き容量が極端に少なくなる可能性があります。ノードの容量がいっぱいになると、一部のストレージ ボリュームがアクセス不能になる (自動的にマウント解除される) 場合があります。

たとえば、以前にストレージ ボリュームのソフト読み取り専用ウォーターマークを 5 GB に設定したとします。ここで、 StorageGRID がストレージ ノード A の 4 つのストレージ ボリュームに対して次の最適化された値を計算したとします。

第0巻	12 GB

第1巻	12 GB
第2巻	11 GB
第3巻	15 GB

カスタム ウォーターマーク (5 GB) がそのノード内のすべてのボリュームの最小最適化値 (11 GB) よりも小さいため、ストレージ ノード A に対して 読み取り専用ウォーターマーク オーバーライドの低さ アラートがトリガーされます。カスタム設定を引き続き使用すると、ノードが安全に読み取り専用状態に移行する前に、ノードの空き容量が極端に少なくなる可能性があります。

アラートを解決する

1 つ以上の **Low read-only watermark override** アラートがトリガーされた場合は、次の手順に従ってください。現在カスタムのウォーターマーク設定を使用しており、アラートがトリガーされていない場合でも最適化された設定の使用を開始する場合にも、これらの手順を使用できます。

開始する前に

- StorageGRID 11.6 以降へのアップグレードが完了しました。
- グリッドマネージャにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは"ルートアクセス権限"。

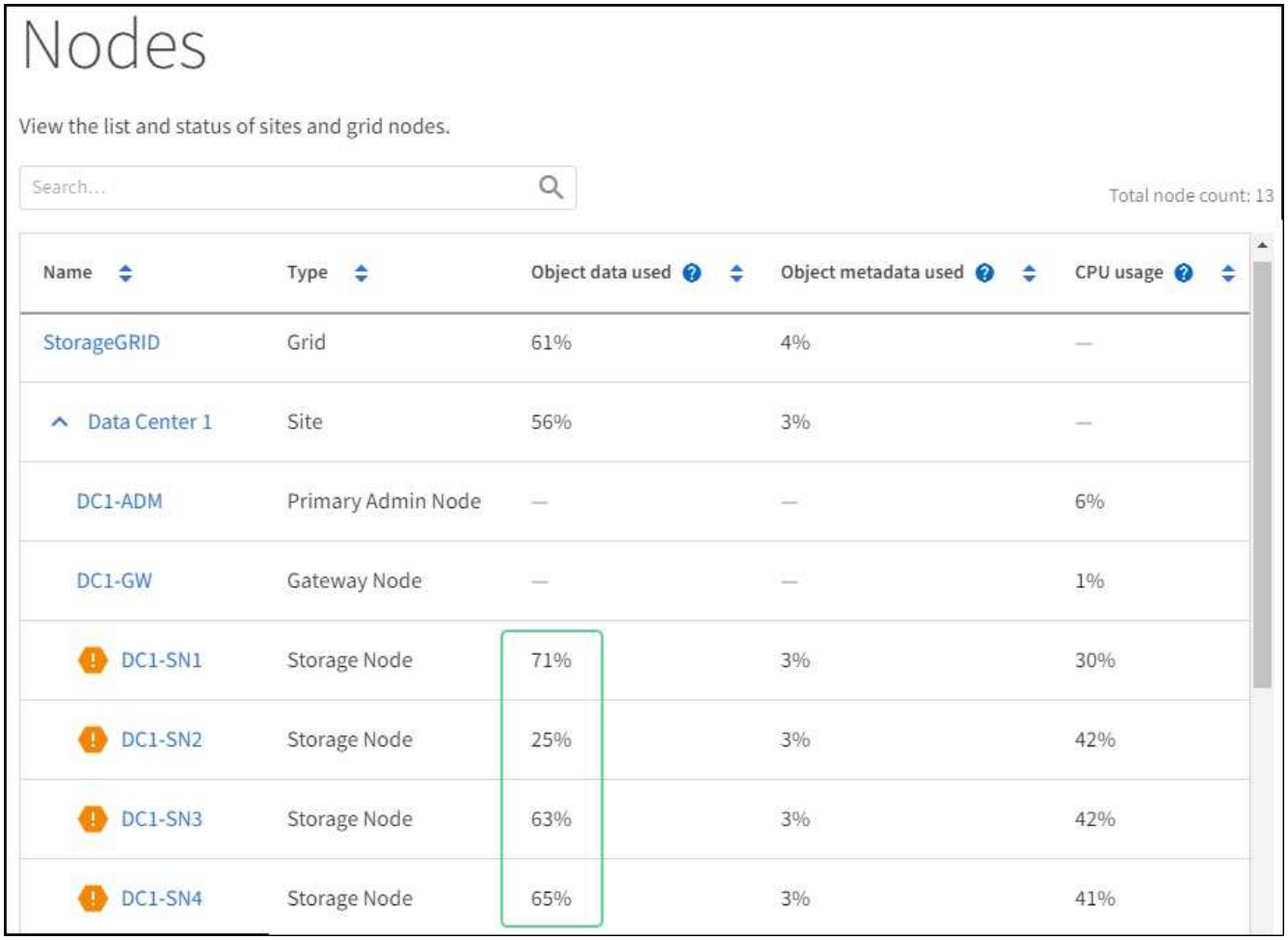
タスク概要

カスタム ウォーターマーク設定を新しいウォーターマーク オーバーライドに更新することで、読み取り専用ウォーターマーク オーバーライドが低い というアラートを解決できます。ただし、1 つ以上のストレージ ノードが満杯に近い場合、または特別な ILM 要件がある場合は、まず最適化されたストレージ ウォーターマークを表示し、使用しても安全かどうかを判断する必要があります。

グリッド全体のオブジェクトデータの使用状況を評価する

手順

1. 「NODES」を選択します。
2. グリッド内の各サイトについて、ノードのリストを展開します。
3. 各サイトの各ストレージ ノードの 使用されたオブジェクト データ 列に表示されるパーセンテージ値を確認します。



4. 適切な手順に従ってください。

   a. どのストレージ ノードも満杯に近づいていない場合 (たとえば、すべての オブジェクト データ使用率の値が 80% 未満の場合)、オーバーライド設定の使用を開始できます。へ移動最適化された透かしを使用する。

   b. ILMルールが厳密な取り込み動作を使用している場合、または特定のストレージプールが満杯に近い場合は、以下の手順を実行します。最適化されたストレージのウォーターマークを表示するそして最適化された透かしを使用できるかどうかを判断する。

最適化されたストレージウォーターマークを表示する

StorageGRID は2 つの Prometheus メトリックを使用して、ストレージ ボリュームのソフト読み取り専用ウォーターマークに対して計算された最適化された値を表示します。グリッド内の各ストレージ ノードの最適化された最小値と最大値を表示できます。

手順

1. サポート > ツール > *メトリック*を選択します。
2. Prometheus セクションで、Prometheus ユーザー インターフェースにアクセスするためのリンクを選択します。
3. 推奨される最小ソフト読み取り専用ウォーターマークを確認するには、次の Prometheus メトリックを入力し、[実行] を選択します。

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

最後の列には、各ストレージ ノード上のすべてのストレージ ボリュームのソフト読み取り専用ウォーターマークの最小最適化値が表示されます。この値がストレージ ボリュームのソフト読み取り専用ウォーターマークのカスタム設定より大きい場合、ストレージ ノードに対して **Low read-only watermark override** アラートがトリガーされます。

4. 推奨される最大のソフト読み取り専用ウォーターマークを確認するには、次の Prometheus メトリックを入力し、[実行] を選択します。

   ```
   storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
   ```

   最後の列には、各ストレージ ノード上のすべてのストレージ ボリュームのソフト読み取り専用ウォーターマークの最適化された最大値が表示されます。

5. 各ストレージノードの最大最適化値をメモします。

最適化された透かしを使用できるかどうかを判断する

手順

1. 「NODES」を選択します。
2. 各オンライン ストレージ ノードに対してこれらの手順を繰り返します。
   a. ストレージノード > *ストレージ*を選択します。
   b. オブジェクト ストア テーブルまで下にスクロールします。
   c. 各オブジェクト ストア (ボリューム) の **Available** 値を、そのストレージ ノードに対して記録した最大の最適化されたウォーターマークと比較します。
3. 各オンラインストレージノードの少なくとも1つのボリュームに、そのノードの最大最適化ウォーターマークを超える空き容量がある場合は、最適化された透かしを使用する最適化された透かしの使用を開始します。

   それ以外の場合は、できるだけ早くグリッドを拡張してください。どちらか"ストレージボリュームを追加する"既存のノードまたは"新しいストレージノードを追加する"。次に、最適化された透かしを使用する透かしの設定を更新します。

4. ストレージボリュームのウォーターマークにカスタム値を引き続き使用する必要がある場合は、"沈黙"または"無効にする"読み取り専用透かしの上書きが低い という警告。

> ⓘ 同じカスタム ウォーターマーク値が、すべてのストレージ ノード上のすべてのストレージ ボリュームに適用されます。ストレージ ボリュームのウォーターマークに推奨値よりも小さい値を使用すると、ノードが容量に達したときに一部のストレージ ボリュームがアクセス不能になる (自動的にマウント解除される) 可能性があります。

最適化された透かしを使用する

手順

1. サポート > その他 > ストレージのウォーターマーク に移動します。
2. *最適化された値を使用する*チェックボックスを選択します。
3. *保存*を選択します。

ストレージ ノードのサイズとボリュームの相対容量に基づいて、各ストレージ ボリュームに対して最適化されたストレージ ボリューム ウォーターマーク設定が有効になるようになりました。

メタデータの問題のトラブルシューティング

メタデータの問題が発生した場合、アラートによって問題の原因と推奨されるアクションが通知されます。特に、メタデータ ストレージ不足アラートがトリガーされた場合は、新しいストレージ ノードを追加する必要があります。

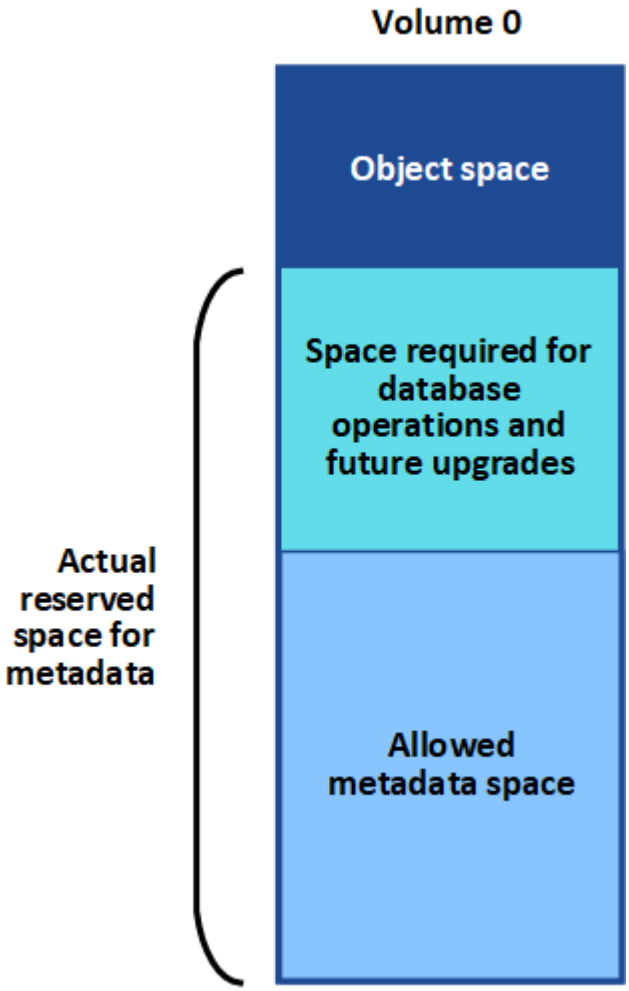
開始する前に

グリッドマネージャにサインインするには、"サポートされているウェブブラウザ" 。

タスク概要

トリガーされたメタデータ関連のアラートごとに推奨されるアクションに従います。 メタデータ ストレージ不足 アラートがトリガーされた場合は、新しいストレージ ノードを追加する必要があります。

StorageGRID は、オブジェクト メタデータ用に各ストレージ ノードのボリューム 0 に一定量のスペースを予約します。このスペースは、実際の予約済みスペース と呼ばれ、オブジェクト メタデータに許可されたスペース (許可されたメタデータ スペース) と、圧縮や修復などの基本的なデータベース操作に必要なスペースに分割されます。許可されたメタデータ領域によって、オブジェクト全体の容量が決まります。



オブジェクト メタデータがメタデータに許可されているスペースの 100% 以上を消費すると、データベース

操作が効率的に実行されず、エラーが発生します。

あなたはできる"各ストレージノードのオブジェクトメタデータ容量を監視する"エラーを予測し、発生する前に修正するのに役立ちます。

StorageGRID は、次の Prometheus メトリックを使用して、許可されたメタデータ領域の使用量を測定します。

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utiliza
tion_metadata_allowed_bytes
```

この Prometheus 式が特定のしきい値に達すると、「メタデータ ストレージ不足」アラートがトリガーされます。

- マイナー: オブジェクト メタデータは、許可されたメタデータ領域の 70% 以上を使用しています。できるだけ早く新しいストレージノードを追加する必要があります。
- メジャー: オブジェクト メタデータは、許可されたメタデータ領域の 90% 以上を使用しています。新しいストレージ ノードをすぐに追加する必要があります。

> オブジェクト メタデータが許可されたメタデータ領域の 90% 以上を使用している場合、ダッシュボードに警告が表示されます。この警告が表示された場合は、すぐに新しいストレージ ノードを追加する必要があります。オブジェクト メタデータが許可されたスペースの 100% を超える使用を許可しないでください。

- 重大: オブジェクト メタデータは、許可されたメタデータ領域の 100% 以上を使用しており、重要なデータベース操作に必要な領域を消費し始めています。新しいオブジェクトの取り込みを停止し、新しいストレージ ノードをすぐに追加する必要があります。

> ボリューム 0 のサイズがメタデータ予約済みスペース ストレージ オプションよりも小さい場合 (たとえば、非実稼働環境の場合)、「メタデータ ストレージ不足」アラートの計算が不正確になる可能性があります。

手順

1. **ALERTS** > **Current** を選択します。
2. アラート テーブルから、必要に応じて **Low metadata storage** アラート グループを展開し、表示する特定のアラートを選択します。
3. アラート ダイアログ ボックスで詳細を確認します。
4. 重大な「メタデータ ストレージ不足」アラートがトリガーされた場合は、すぐに拡張を実行してストレージ ノードを追加してください。

> StorageGRID は各サイトですべてのオブジェクト メタデータの完全なコピーを保持するため、グリッド全体のメタデータ容量は最小のサイトのメタデータ容量によって制限されます。 1つのサイトにメタデータ容量を追加する必要がある場合は、"他のサイトを展開する"同じ数のストレージ ノードによって。

拡張を実行すると、 StorageGRID は既存のオブジェクト メタデータを新しいノードに再配布し、グリッドの全体的なメタデータ容量が増加します。ユーザーの操作は必要ありません。 *メタデータストレージ不足*アラートがクリアされました。

証明書エラーのトラブルシューティング

Web ブラウザ、S3 クライアント、または外部監視ツールを使用してStorageGRIDに接続しようとしたときにセキュリティまたは証明書の問題が見つかった場合は、証明書を確認する必要があります。

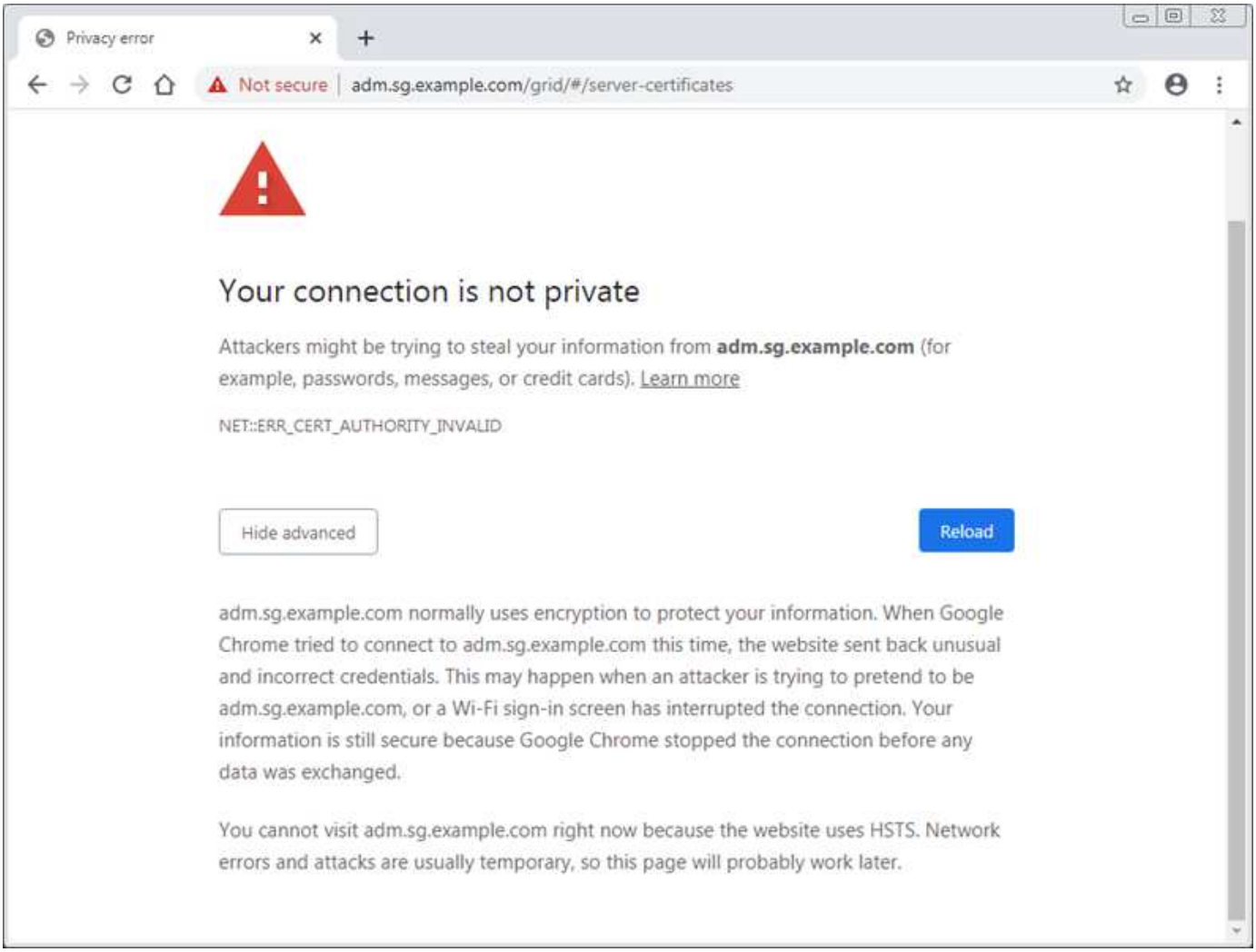
タスク概要

Grid Manager、Grid Management API、Tenant Manager、または Tenant Management API を使用してStorageGRIDに接続しようとすると、証明書エラーによって問題が発生する可能性があります。 S3 クライアントまたは外部監視ツールに接続しようとしたときにも証明書エラーが発生する可能性があります。

IP アドレスではなくドメイン名を使用して Grid Manager または Tenant Manager にアクセスしている場合、次のいずれかが発生すると、ブラウザにバイパス オプションのない証明書エラーが表示されます。

- カスタム管理インターフェース証明書の有効期限が切れます。
- カスタム管理インターフェイス証明書からデフォルトのサーバー証明書に戻します。

次の例は、カスタム管理インターフェース証明書の有効期限が切れたときの証明書エラーを示しています。



失敗したサーバー証明書によって操作が中断されないように、サーバー証明書の有効期限が近づくと、*管理インターフェイスのサーバー証明書の有効期限*アラートがトリガーされます。

外部 Prometheus 統合にクライアント証明書を使用している場合、 StorageGRID管理インターフェイス証明書またはクライアント証明書によって証明書エラーが発生する可能性があります。クライアント証明書の有効期限が近づくと、*証明書ページで構成されたクライアント証明書の有効期限*アラートがトリガーされます。

手順

期限切れの証明書に関するアラート通知を受け取った場合は、証明書の詳細にアクセスします。構成 > セキュリティ > *証明書*を選択し、"適切な証明書タブを選択します" 。

1. 証明書の有効期間を確認してください。 + 一部の Web ブラウザおよび S3 クライアントは、有効期間が 398 日を超える証明書を受け入れません。
2. 証明書の有効期限が切れているか、もうすぐ切れる場合は、新しい証明書をアップロードまたは生成します。
   - サーバー証明書については、"グリッドマネージャとテナントマネージャのカスタムサーバー証明書を構成する" 。
   - クライアント証明書については、"クライアント証明書の設定" 。
3. サーバー証明書エラーの場合は、次のいずれかまたは両方のオプションを試してください。
   - 証明書のサブジェクト別名 (SAN) が入力されていること、および SAN が接続先のノードの IP アドレスまたはホスト名と一致していることを確認します。
   - ドメイン名を使用してStorageGRIDに接続しようとしている場合:
     i. 接続エラーを回避してグリッド マネージャーにアクセスするには、ドメイン名の代わりに管理ノードの IP アドレスを入力します。
     ii. グリッドマネージャから*構成* > セキュリティ > *証明書*を選択し、"適切な証明書タブを選択します"新しいカスタム証明書をインストールするか、デフォルトの証明書を続行します。
     iii. StorageGRIDの管理手順については、"グリッドマネージャとテナントマネージャのカスタムサーバー証明書を構成する" 。

管理ノードとユーザーインターフェースの問題のトラブルシューティング

管理ノードおよびStorageGRIDユーザー インターフェイスに関連する問題の原因を特定するために、いくつかのタスクを実行できます。

管理ノードのサインインエラー

StorageGRID管理ノードにサインインする際にエラーが発生した場合は、システムに問題がある可能性があります。"ネットワーク"または "ハードウェア"問題、問題"管理ノードサービス"、または"Cassandraデータベースの問題"接続されたストレージノード上。

開始する前に

- グリッドマネージャにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは `Passwords.txt`ファイル。
- あなたが持っている"特定のアクセス権限"。

タスク概要

管理ノードにサインインしようとしたときに次のいずれかのエラー メッセージが表示される場合は、次のトラブルシューティング ガイドラインを使用してください。

- `Your credentials for this account were invalid. Please try again.`
- `Waiting for services to start…`
- `Internal server error. The server encountered an error and could not complete your request. Please try again. If the problem persists, contact Technical Support.`
- `Unable to communicate with server. Reloading page…`

手順

1. 10 分待ってから、もう一度サインインしてください。

   エラーが自動的に解決されない場合は、次の手順に進みます。

2. StorageGRIDシステムに複数の管理ノードがある場合は、別の管理ノードから Grid Manager にサインインして、使用できない管理ノードのステータスを確認してください。
   - サインインできる場合は、ダッシュボード、ノード、アラート、および*サポート*オプションを使用して、エラーの原因を特定できます。
   - 管理ノードが 1 つしかない場合、またはまだサインインできない場合は、次の手順に進みます。
3. ノードのハードウェアがオフラインかどうかを判断します。
4. StorageGRIDシステムでシングルサインオン（SSO）が有効になっている場合は、"シングルサインオンの設定" 。

   問題を解決するには、単一の管理ノードに対して SSO を一時的に無効にしてから再度有効にする必要がある場合があります。

   > SSO が有効になっている場合、制限されたポートを使用してサインオンすることはできません。ポート443を使用する必要があります。

5. 使用しているアカウントがフェデレーション ユーザーに属しているかどうかを確認します。

   フェデレーション ユーザー アカウントが機能しない場合は、root などのローカル ユーザーとして Grid Manager にサインインしてみてください。

   - ローカル ユーザーがサインインできる場合:
     i. アラートを確認します。
     ii. 構成 > アクセス制御 > *アイデンティティ連携*を選択します。
     iii. LDAP サーバーの接続設定を検証するには、「テスト接続」をクリックします。
     iv. テストが失敗した場合は、構成エラーを解決してください。
   - ローカル ユーザーがサインインできない場合、資格情報が正しいと確信できる場合は、次の手順に進みます。
6. セキュア シェル (ssh) を使用して管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@Admin_Node_IP`
   b. 記載されているパスワードを入力してください `Passwords.txt`ファイル。
   c. ルートに切り替えるには、次のコマンドを入力します。 `su -`

d. 記載されているパスワードを入力してください `Passwords.txt`ファイル。

ルートとしてログインすると、プロンプトは `$`に `#`。

7. グリッド ノードで実行されているすべてのサービスのステータスを表示します。 `storagegrid-status`

nms、mi、nginx、mgmt api サービスがすべて実行されていることを確認します。

サービスのステータスが変更されると、出力はすぐに更新されます。

```
$ storagegrid-status
Host Name                      99-211
IP Address                     10.96.99.211
Operating System Kernel        4.19.0          Verified
Operating System Environment   Debian 10.1     Verified
StorageGRID Webscale Release   11.4.0          Verified
Networking                                     Verified
Storage Subsystem                              Verified
Database Engine                5.5.9999+default Running
Network Monitoring             11.4.0          Running
Time Synchronization           1:4.2.8p10+dfsg Running
ams                            11.4.0          Running
cmn                            11.4.0          Running
nms                            11.4.0          Running
ssm                            11.4.0          Running
mi                             11.4.0          Running
dynip                          11.4.0          Running
nginx                          1.10.3          Running
tomcat                         9.0.27          Running
grafana                        6.4.3           Running
mgmt api                       11.4.0          Running
prometheus                     11.4.0          Running
persistence                    11.4.0          Running
ade exporter                   11.4.0          Running
alertmanager                   11.4.0          Running
attrDownPurge                  11.4.0          Running
attrDownSamp1                  11.4.0          Running
attrDownSamp2                  11.4.0          Running
node exporter                  0.17.0+ds       Running
sg snmp agent                  11.4.0          Running
```

8. nginx-gwサービスが実行中であることを確認する `# service nginx-gw status`
9. Lumberjack を使用して丸太を収集します。 `# /usr/local/sbin/lumberjack.rb`

過去に認証に失敗した場合は、Lumberjack スクリプトの --start および --end オプションを使用して適切な時間範囲を指定できます。これらのオプションの詳細については、lumberjack -h を使用してください。

端末への出力には、ログ アーカイブがコピーされた場所が示されます。

10. 次のログを確認します。
    - `/var/local/log/bycast.log`
    - `/var/local/log/bycast-err.log`
    - `/var/local/log/nms.log`
    - `**/*commands.txt`
11. 管理ノードに問題が見つからない場合、次のいずれかのコマンドを発行して、サイトで ADC サービスを実行する 3 つのストレージ ノードの IP アドレスを確認します。通常、これらはサイトにインストールされた最初の 3 つのストレージ ノードです。

    ```
    # cat /etc/hosts
    ```

    ```
    # gpt-list-services adc
    ```

    管理ノードは認証プロセス中に ADC サービスを使用します。
12. 管理ノードから、識別した IP アドレスを使用して、ssh を使用して各 ADC ストレージ ノードにログインします。
13. グリッド ノードで実行されているすべてのサービスのステータスを表示します。 `storagegrid-status`

    idnt、acct、nginx、cassandra サービスがすべて実行されていることを確認します。
14. 手順を繰り返す木こりを使って丸太を集めるそしてログを確認するストレージ ノードのログを確認します。
15. 問題を解決できない場合は、テクニカル サポートにお問い合わせください。

    収集したログをテクニカル サポートに提供します。参照"ログファイルリファレンス" 。

ユーザ インターフェイスに関する問題

StorageGRIDソフトウェアをアップグレードすると、Grid Manager または Tenant Manager のユーザー インターフェイスが期待どおりに応答しない場合があります。

手順

1. 必ず"サポートされているウェブブラウザ"。
2. Web ブラウザのキャッシュをクリアします。

   キャッシュをクリアすると、以前のバージョンのStorageGRIDソフトウェアで使用されていた古いリソースが削除され、ユーザー インターフェイスが再び正しく動作するようになります。手順については、Web ブラウザのドキュメントを参照してください。

ネットワーク、ハードウェア、プラットフォームの問題のトラブルシューティング

StorageGRIDネットワーク、ハードウェア、およびプラットフォームの問題に関連する問題の原因を特定するために実行できるタスクがいくつかあります。

「422: 処理できないエンティティ」エラー

エラー 422: 処理できないエンティティはさまざまな理由で発生する可能性があります。エラー メッセージを確認して、問題の原因を特定します。

リストされているエラー メッセージのいずれかが表示された場合には、推奨されるアクションを実行してください。

エラー メッセージ	根本原因と是正措置

`422: Unprocessable Entity`
 	
`Validation failed. Please check`
`the values you entered for errors. Test connection failed.`
`Please verify your configuration. Unable to authenticate, please verify your username and password: LDAP Result Code 8 "Strong Auth Required": 00002028: LdapErr: DSID-0C090256, comment: The server requires`
`binds to turn on integrity checking if SSL\TLS are not already active on the connection, data 0, v3839`
	このメッセージは、Windows Active Directory (AD) を使用して ID フェデレーションを構成するときに、トランスポート層セキュリティ (TLS) に対して **TLS** を使用しない オプションを選択した場合に表示されることがあります。
	
	LDAP 署名を強制する AD サーバーでは、「TLS を使用しない」オプションの使用はサポートされていません。 TLS の場合は、**STARTTLS** を使用する オプションまたは **LDAPS** を使用する オプションのいずれかを選択する必要があります。

エラー メッセージ	根本原因と是正措置

`422: Unprocessable Entity`
 	
`Validation failed. Please check`
`the values you entered for errors. Test connection failed.`
`Please verify your configuration.Unable to begin TLS, verify your certificate and TLS configuration: LDAP Result Code 200 "Network Error": TLS handshake failed (EOF)`
	このメッセージは、サポートされていない暗号を使用して、StorageGRIDから ID フェデレーションまたはクラウド ストレージ プールに使用される外部システムへのトランスポート層セキュリティ (TLS) 接続を確立しようとした場合に表示されます。
	
	外部システムによって提供される暗号を確認します。システムは、次のいずれかを使用する必要があります。"StorageGRIDでサポートされている暗号" StorageGRID の管理手順に示されているように、送信 TLS 接続用です。

グリッド ネットワーク **MTU** 不一致アラート

グリッド ネットワーク **MTU** 不一致 アラートは、グリッド ネットワーク インターフェイス (eth0) の最大転送単位 (MTU) 設定がグリッド内のノード間で大幅に異なる場合にトリガーされます。

タスク概要

MTU 設定の違いは、eth0 ネットワークのすべてではなく一部がジャンボ フレーム用に設定されていることを示している可能性があります。 MTU サイズの不一致が 1000 を超えると、ネットワーク パフォーマンスの問題が発生する可能性があります。

手順

1. すべてのノード上の eth0 の MTU 設定を一覧表示します。
   - グリッド マネージャーで提供されるクエリを使用します。
   - 移動先 *`primary Admin Node IP address`*`/metrics/graph`次のクエリを入力します。
     `node_network_mtu_bytes{device="eth0"}`
2. "MTU設定の変更"必要に応じて、すべてのノードのグリッド ネットワーク インターフェイス (eth0) で同じになるようにします。
   - Linux および VMware ベースのノードの場合は、次のコマンドを使用します。 `/usr/sbin/change-ip.py [-h] [-n node] mtu network [network...]`

     例： `change-ip.py -n node 1500 grid admin`

     注意: Linuxベースのノードでは、コンテナ内のネットワークの必要なMTU値がホストインターフェースで既に設定されている値を超える場合、まずホストインターフェースに必要なMTU値を設定し、その後 `change-ip.py`コンテナ内のネットワークの MTU 値を変更するスクリプト。

     Linux または VMware ベースのノードで MTU を変更するには、次の引数を使用します。

位置引数	説明
`mtu`	設定する MTU。 1280 ～ 9216 の範囲でなければなりません。
`network`	MTU を適用するネットワーク。次のネットワーク タイプを 1 つ以上含めます。 • グリッド • admin • client（クライアント）

+

Optional arguments	説明
`-h, - help`	ヘルプ メッセージを表示して終了します。
`-n node, --node node`	ノード。デフォルトはローカルノードです。

ノードネットワーク受信フレームエラーアラート

ノード ネットワーク受信フレーム エラー アラートは、 StorageGRIDとネットワーク ハードウェア間の接続の問題によって発生する可能性があります。根本的な問題が解決されると、このアラートは自動的にクリアされます。

タスク概要

ノード ネットワーク受信フレーム エラー アラートは、 StorageGRIDに接続するネットワーク ハードウェアの次の問題によって発生する可能性があります。

- 前方誤り訂正（FEC）は必須だが使用されていない
- スイッチポートとNIC MTUの不一致
- 高いリンクエラー率
- NICリングバッファオーバーラン

手順

1. ネットワーク構成に応じて、このアラートの考えられるすべての原因に対するトラブルシューティング手順に従ってください。
2. エラーの原因に応じて次の手順を実行します。

FEC の不一致

これらの手順は、 StorageGRIDアプライアンスの FEC 不一致によって発生する ノード ネットワーク受信フレーム エラー アラートにのみ適用されます。

a. StorageGRIDアプライアンスに接続されているスイッチのポートの FEC ステータスを確認します。

b. アプライアンスからスイッチまでのケーブルの物理的な整合性を確認します。

c. FEC設定を変更してアラートを解決する場合は、まずStorageGRIDアプライアンスインストーラの[リンク構成]ページでアプライアンスが*自動*モードに設定されていることを確認してください（アプライアンスの手順を参照してください）。

   - "SG6160"
   - "SGF6112"
   - "SG6000"
   - "SG5800"
   - "SG5700"
   - "SG110とSG1100"
   - "SG100とSG1000"

d. スイッチ ポートの FEC 設定を変更します。 StorageGRIDアプライアンス ポートは、可能な場合は FEC 設定を一致するように調整します。

   StorageGRIDアプライアンスでは FEC 設定を構成できません。代わりに、アプライアンスは接続されているスイッチ ポート上の FEC 設定を検出し、ミラーリングしようとします。リンクが 25 GbE または 100 GbE のネットワーク速度に強制されると、スイッチと NIC が共通の FEC 設定をネゴシエートできない可能性があります。共通の FEC 設定がない場合、ネットワークは「FEC なし」モードに戻ります。 FEC が有効になっていない場合、接続は電気ノイズによるエラーの影響を受けやすくなります。

   StorageGRIDアプライアンスは、Firecode (FC) および Reed Solomon (RS) FEC をサポートしますが、FEC なしもサポートします。

スイッチポートと**NIC MTU**の不一致

アラートの原因がスイッチ ポートと NIC MTU の不一致である場合は、ノードに設定されている MTU サイズがスイッチ ポートの MTU 設定と同じであることを確認します。

ノードに設定されている MTU サイズは、ノードが接続されているスイッチ ポートの設定よりも小さい可能性があります。この構成ではStorageGRIDノードが MTU よりも大きいイーサネット フレームを受信する可能性がありますが、その場合、「ノード ネットワーク受信フレーム エラー」アラートが報告される可能性があります。このような状況になっていると思われる場合は、エンドツーエンドの MTU の目標または要件に応じて、スイッチ ポートの MTU をStorageGRIDネットワーク インターフェイスの MTU と一致するように変更するか、 StorageGRIDネットワーク インターフェイスの MTU をスイッチ ポートと一致するように変更します。

最適なネットワーク パフォーマンスを得るには、すべてのノードのグリッド ネットワーク インターフェイスで同様の MTU 値を構成する必要があります。個々のノード上のグリッド ネットワークの MTU 設定に大きな違いがある場合、グリッド ネットワーク **MTU** 不一致 アラートがトリガーされます。 MTU 値はすべてのネットワーク タイプで同じである必要はありません。見るグリッドネットワークMTU不一致アラートのトラブルシューティング詳細についてはこちらをご覧ください。

こちらもご覧ください "MTU設定を変更する"。

高いリンクエラー率

a. FEC がまだ有効になっていない場合は有効にします。
b. ネットワーク ケーブルの品質が良好であり、破損や不適切な接続がないことを確認します。
c. ケーブルに問題がないようであれば、テクニカル サポートにお問い合わせください。

電気ノイズが多い環境では、エラー率が高くなる可能性があります。

NICリングバッファオーバーラン

エラーが NIC リング バッファ オーバーランである場合は、テクニカル サポートにお問い合わせください。

StorageGRIDシステムが過負荷になり、ネットワーク イベントをタイムリーに処理できなくなると、リング バッファがオーバーランする可能性があります。

3. 問題を監視し、アラートが解決されない場合はテクニカル サポートに連絡してください。

時刻同期エラー

グリッド内の時間同期に問題が発生する可能性があります。

時刻同期の問題が発生した場合は、それぞれ Stratum 3 以上の参照を提供する少なくとも 4 つの外部 NTP ソースが指定されていること、およびすべての外部 NTP ソースが正常に動作しており、 StorageGRIDノードからアクセスできることを確認してください。

いつ"外部NTPソースの指定"運用レベルのStorageGRIDインストールでは、Windows Server 2016 より前のバージョンの Windows で Windows Time (W32Time) サービスを使用しないでください。以前のバージョンの Windows のタイム サービスは精度が十分でないため、StorageGRIDなどの高精度環境で使用することは Microsoft によってサポートされていません。

Linux: ネットワーク接続の問題

Linux ホストでホストされているStorageGRIDノードのネットワーク接続に問題が発生する可能性があります。

MACアドレスの複製

場合によっては、MAC アドレスの複製を使用することでネットワークの問題を解決できます。仮想ホストを使用している場合は、ノード構成ファイルで各ネットワークの MAC アドレス複製キーの値を「true」に設定

します。この設定により、 StorageGRIDコンテナの MAC アドレスはホストの MAC アドレスを使用するようになります。ノード構成ファイルを作成するには、"Red Hat Enterprise Linux"または"UbuntuまたはDebian"。

> Linux ホスト OS で使用するための個別の仮想ネットワーク インターフェイスを作成します。Linux ホスト OS とStorageGRIDコンテナに同じネットワーク インターフェイスを使用すると、ハイパーバイザーでプロミスキャス モードが有効になっていない場合に、ホスト OS にアクセスできなくなる可能性があります。

MACクローンを有効にする方法の詳細については、"Red Hat Enterprise Linux"または"UbuntuまたはDebian"。

プロミスキャスモード

MAC アドレスの複製を使用せず、ハイパーバイザーによって割り当てられたもの以外の MAC アドレスのデータをすべてのインターフェイスで受信および送信できるようにする場合は、仮想スイッチおよびポート グループ レベルのセキュリティ プロパティが、無差別モード、MAC アドレスの変更、および偽造送信に対して承認 に設定されていることを確認します。仮想スイッチに設定された値はポート グループ レベルの値によって上書きされる可能性があるため、両方の場所で設定が同じであることを確認してください。

プロミスキャスモードの使用に関する詳細は、"Red Hat Enterprise Linux"または"UbuntuまたはDebian"。

Linux: ノードのステータスが「孤立」です

孤立状態の Linux ノードは通常、ノードのコンテナを制御するストレージ グリッド サービスまたはStorageGRIDノード デーモンのいずれかが予期せず停止したことを示します。

タスク概要

Linux ノードが孤立状態にあると報告された場合は、次の対応を行う必要があります。

- ログでエラーとメッセージを確認します。
- ノードを再度起動してみます。
- 必要に応じて、コンテナ エンジン コマンドを使用して既存のノード コンテナを停止します。
- ノードを再起動します。

手順

1. サービス デーモンと孤立ノードの両方のログをチェックして、明らかなエラーや予期しない終了に関するメッセージがないか確認します。
2. root として、または sudo 権限を持つアカウントを使用してホストにログインします。
3. 次のコマンドを実行して、ノードを再度起動してみます。 `$ sudo storagegrid node start node-name`

   ```
   $ sudo storagegrid node start DC1-S1-172-16-1-172
   ```

   ノードが孤立している場合、応答は次のようになります。

```
Not starting ORPHANED node DC1-S1-172-16-1-172
```

4. Linux から、コンテナ エンジンと制御する storagegrid-node プロセスを停止します。例： `sudo docker stop --time secondscontainer-name`

   のために `seconds`コンテナが停止するまで待機する秒数を入力します (通常は 15 分以内)。例えば：

```
sudo docker stop --time 900 storagegrid-DC1-S1-172-16-1-172
```

5. ノードを再起動します。 `storagegrid node start node-name`

```
storagegrid node start DC1-S1-172-16-1-172
```

Linux: IPv6 サポートのトラブルシューティング

Linux ホストにStorageGRIDノードをインストールし、IPv6 アドレスがノード コンテナに期待どおりに割り当てられていないことに気付いた場合は、カーネルで IPv6 サポートを有効にする必要がある場合があります。

タスク概要

グリッド ノードに割り当てられている IPv6 アドレスを確認するには、次の手順を実行します。

1. **NODES** を選択し、ノードを選択します。
2. [概要] タブの [IP アドレス] の横にある [追加の IP アドレスを表示] を選択します。

IPv6 アドレスが表示されず、ノードが Linux ホストにインストールされている場合は、次の手順に従ってカーネルで IPv6 サポートを有効にします。

手順

1. root として、または sudo 権限を持つアカウントを使用してホストにログインします。
2. 次のコマンドを実行します。 `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@SG:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

   結果は0になるはずです。

```
net.ipv6.conf.all.disable_ipv6 = 0
```

> ⓘ 結果が0でない場合は、オペレーティングシステムのドキュメントを参照して変更してください。 `sysctl`設定。次に、続行する前に値を 0 に変更します。

3. StorageGRIDノード コンテナを入力します。 `storagegrid node enter node-name`
4. 次のコマンドを実行します。 `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@DC1-S1:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

結果は 1 になるはずです。

```
net.ipv6.conf.all.disable_ipv6 = 1
```

> ⓘ 結果が 1 以外の場合、この手順は適用されません。テクニカル サポートにお問い合わせください。

5. コンテナを終了します。 `exit`

```
root@DC1-S1:~ # exit
```

6. root として、次のファイルを編集します。 `/var/lib/storagegrid/settings/sysctl.d/net.conf` 。

```
sudo vi /var/lib/storagegrid/settings/sysctl.d/net.conf
```

7. 次の 2 行を見つけて、コメント タグを削除します。次に、ファイルを保存して閉じます。

```
net.ipv6.conf.all.disable_ipv6 = 0
```

```
net.ipv6.conf.default.disable_ipv6 = 0
```

8. 次のコマンドを実行して、 StorageGRIDコンテナを再起動します。

```
storagegrid node stop node-name
```

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

外部 **syslog** サーバーのトラブルシューティング

次の表では、外部 Syslog サーバーの使用に関連する可能性のあるエラー メッセージに

ついて説明し、修正アクションを示します。

外部 Syslog サーバーが正しく構成されていることを確認するためのテスト メッセージの送信で問題が発生した場合、外部 Syslog サーバーの構成ウィザードによってこれらのエラーが表示されます。

実行時に問題が発生する場合は、"外部 syslog サーバ転送エラー"警告。このアラートを受け取った場合は、アラートの指示に従ってテスト メッセージを再送信し、詳細なエラー メッセージを取得してください。

監査情報を外部 Syslog サーバーに送信する方法の詳細については、以下を参照してください。

- "外部Syslogサーバーの使用に関する考慮事項"
- "監査メッセージと外部Syslogサーバーを構成する"

エラー メッセージ	説明と推奨アクション
ホスト名を解決できません	Syslog サーバーに入力した FQDN を IP アドレスに解決できませんでした。 1. 入力したホスト名を確認してください。 IP アドレスを入力した場合は、それが WXYZ (ドット付き 10 進数) 表記の有効な IP アドレスであることを確認してください。 2. DNS サーバーが正しく設定されていることを確認します。 3. 各ノードが DNS サーバーの IP アドレスにアクセスできることを確認します。
接続が拒否されました	Syslog サーバーへの TCP または TLS 接続が拒否されました。ホストの TCP または TLS ポートをリッスンしているサービスがないか、ファイアウォールがアクセスをブロックしている可能性があります。 1. Syslog サーバーの正しい FQDN または IP アドレス、ポート、プロトコルを入力したことを確認します。 2. Syslog サービスのホストが、指定されたポートでリッスンしている Syslog デーモンを実行していることを確認します。 3. ファイアウォールがノードから Syslog サーバーの IP およびポートへの TCP/TLS 接続へのアクセスをブロックしていないことを確認します。
ネットワークにアクセスできません	Syslog サーバーは直接接続されたサブネット上にありません。ルータは、リストされたノードからのテスト メッセージを syslog サーバーに転送できなかったことを示す ICMP 障害メッセージを返しました。 1. Syslog サーバーの正しい FQDN または IP アドレスを入力したことを確認します。 2. リストされている各ノードについて、グリッド ネットワーク サブネット リスト、管理ネットワーク サブネット リスト、およびクライアント ネットワーク ゲートウェイを確認します。これらが、予想されるネットワーク インターフェイスとゲートウェイ (グリッド、管理、またはクライアント) を介して syslog サーバーにトラフィックをルーティングするように構成されていることを確認します。

エラー メッセージ	説明と推奨アクション
ホストに到達できません	Syslog サーバーは、直接接続されたサブネット (リストされたノードのグリッド、管理、またはクライアント IP アドレスに使用されるサブネット) 上にあります。ノードはテスト メッセージを送信しようとしましたが、Syslog サーバーの MAC アドレスに対する ARP 要求への応答を受信しませんでした。 1. Syslog サーバーの正しい FQDN または IP アドレスを入力したことを確認します。 2. syslog サービスを実行しているホストが起動していることを確認します。
接続がタイムアウトしました	TCP/TLS 接続を試行しましたが、長時間にわたって syslog サーバーからの応答が受信されませんでした。ルーティングの設定に誤りがあるか、ファイアウォールが応答を送信せずにトラフィックをドロップしている可能性があります (一般的な設定)。 1. Syslog サーバーの正しい FQDN または IP アドレスを入力したことを確認します。 2. リストされている各ノードについて、グリッド ネットワーク サブネット リスト、管理ネットワーク サブネット リスト、およびクライアント ネットワーク ゲートウェイを確認します。 Syslog サーバーに到達すると予想されるネットワーク インターフェイスとゲートウェイ (グリッド、管理、またはクライアント) を使用して、Syslog サーバーにトラフィックをルーティングするようにこれらが構成されていることを確認します。 3. ファイアウォールが、リストされているノードから Syslog サーバーの IP とポートへの TCP/TLS 接続へのアクセスをブロックしていないことを確認します。
パートナーによって接続が閉じられました	Syslog サーバーへの TCP 接続は正常に確立されましたが、その後閉じられました。これには次のような理由が考えられます: • Syslog サーバーが再起動またはリブートされた可能性があります。 • ノードと syslog サーバーの TCP/TLS 設定が異なる場合があります。 • 中間ファイアウォールがアイドル状態の TCP 接続を閉じている可能性があります。 • syslog サーバー ポートをリッスンしている非 syslog サーバーが接続を閉じた可能性があります。 この問題を解決するには: 1. Syslog サーバーの正しい FQDN または IP アドレス、ポート、プロトコルを入力したことを確認します。 2. TLS を使用している場合は、syslog サーバーも TLS を使用していることを確認してください。 TCP を使用している場合は、syslog サーバーも TCP を使用していることを確認してください。 3. 中間ファイアウォールがアイドル状態の TCP 接続を閉じるように構成されていないことを確認します。

エラー メッセージ	説明と推奨アクション
TLS証明書エラー	Syslog サーバーから受信したサーバー証明書は、指定した CA 証明書バンドルおよびクライアント証明書と互換性がありません。 1. CA 証明書バンドルとクライアント証明書 (存在する場合) が syslog サーバー上のサーバー証明書と互換性があることを確認します。 2. Syslog サーバーからのサーバー証明書の ID に、予想される IP または FQDN 値が含まれていることを確認します。
転送停止	Syslog レコードが Syslog サーバーに転送されなくなり、 StorageGRID はその理由を検出できません。 このエラーとともに提供されるデバッグ ログを確認して、根本原因を特定してください。
TLSセッションが終了しました	Syslog サーバーが TLS セッションを終了しましたが、 StorageGRID はその理由を検出できません。 1. このエラーとともに提供されるデバッグ ログを確認して、根本原因を特定してください。 2. Syslog サーバーの正しい FQDN または IP アドレス、ポート、プロトコルを入力したことを確認します。 3. TLS を使用している場合は、syslog サーバーも TLS を使用していることを確認してください。 TCP を使用している場合は、syslog サーバーも TCP を使用していることを確認してください。 4. CA 証明書バンドルとクライアント証明書 (存在する場合) が syslog サーバーのサーバー証明書と互換性があることを確認します。 5. Syslog サーバーからのサーバー証明書の ID に、予想される IP または FQDN 値が含まれていることを確認します。
結果クエリに失敗しました	Syslog サーバーの構成とテストに使用される管理ノードは、リストされているノードからテスト結果を要求できません。 1 つ以上のノードがダウンしている可能性があります。 1. 標準的なトラブルシューティング手順に従って、ノードがオンラインであり、必要なすべてのサービスが実行されていることを確認します。 2. リストされたノードで miscd サービスを再起動します。

監査ログを確認する

監査メッセージとログ

これらの手順には、 StorageGRID監査メッセージと監査ログの構造と内容に関する情報が含まれています。この情報を使用して、システム アクティビティの監査証跡を読み取って分析できます。

これらの手順は、 StorageGRIDシステムの監査メッセージの分析を必要とするシステム アクティビティと使用状況のレポートを作成する責任を持つ管理者を対象としています。

テキスト ログ ファイルを使用するには、管理ノードで構成された監査共有にアクセスできる必要があります。

監査メッセージレベルの設定と外部Syslogサーバの使用については、以下を参照してください。"監査メッセージとログの保存先を構成する" 。

監査メッセージフローと保持

すべてのStorageGRIDサービスは、通常のシステム操作中に監査メッセージを生成します。これらの監査メッセージがStorageGRIDシステムを経由してどのように移動するかを理解する必要があります。 `audit.log`ファイル。

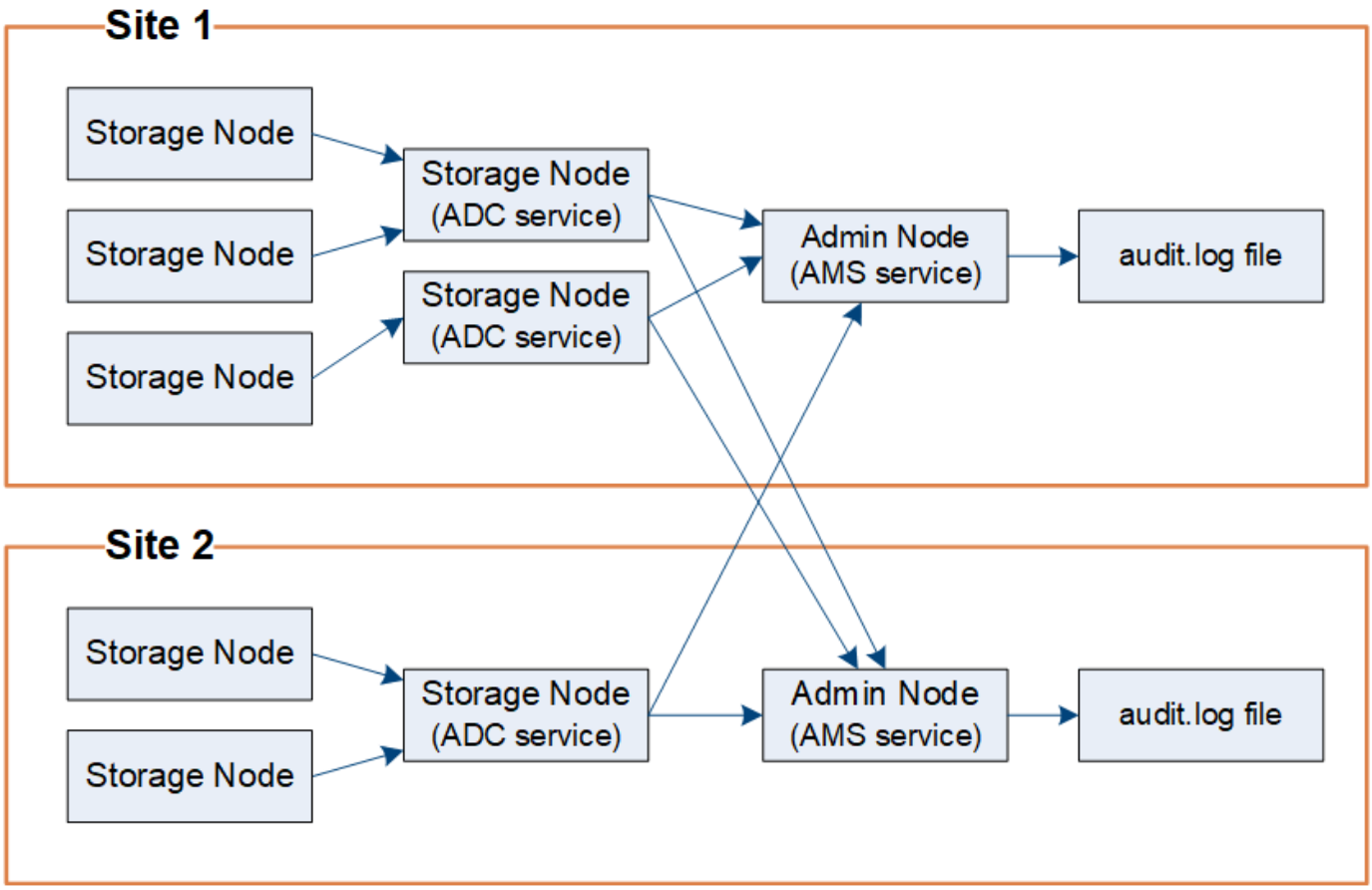
監査メッセージフロー

監査メッセージは、管理ノードと、管理ドメイン コントローラ (ADC) サービスを持つストレージ ノードによって処理されます。

監査メッセージ フロー図に示されているように、各StorageGRIDノードは、データ センター サイトの ADC サービスの 1 つに監査メッセージを送信します。 ADC サービスは、各サイトにインストールされた最初の 3 つのストレージ ノードに対して自動的に有効になります。

次に、各 ADC サービスはリレーとして機能し、監査メッセージのコレクションをStorageGRIDシステム内のすべての管理ノードに送信します。これにより、各管理ノードにシステム アクティビティの完全な記録が提供されます。

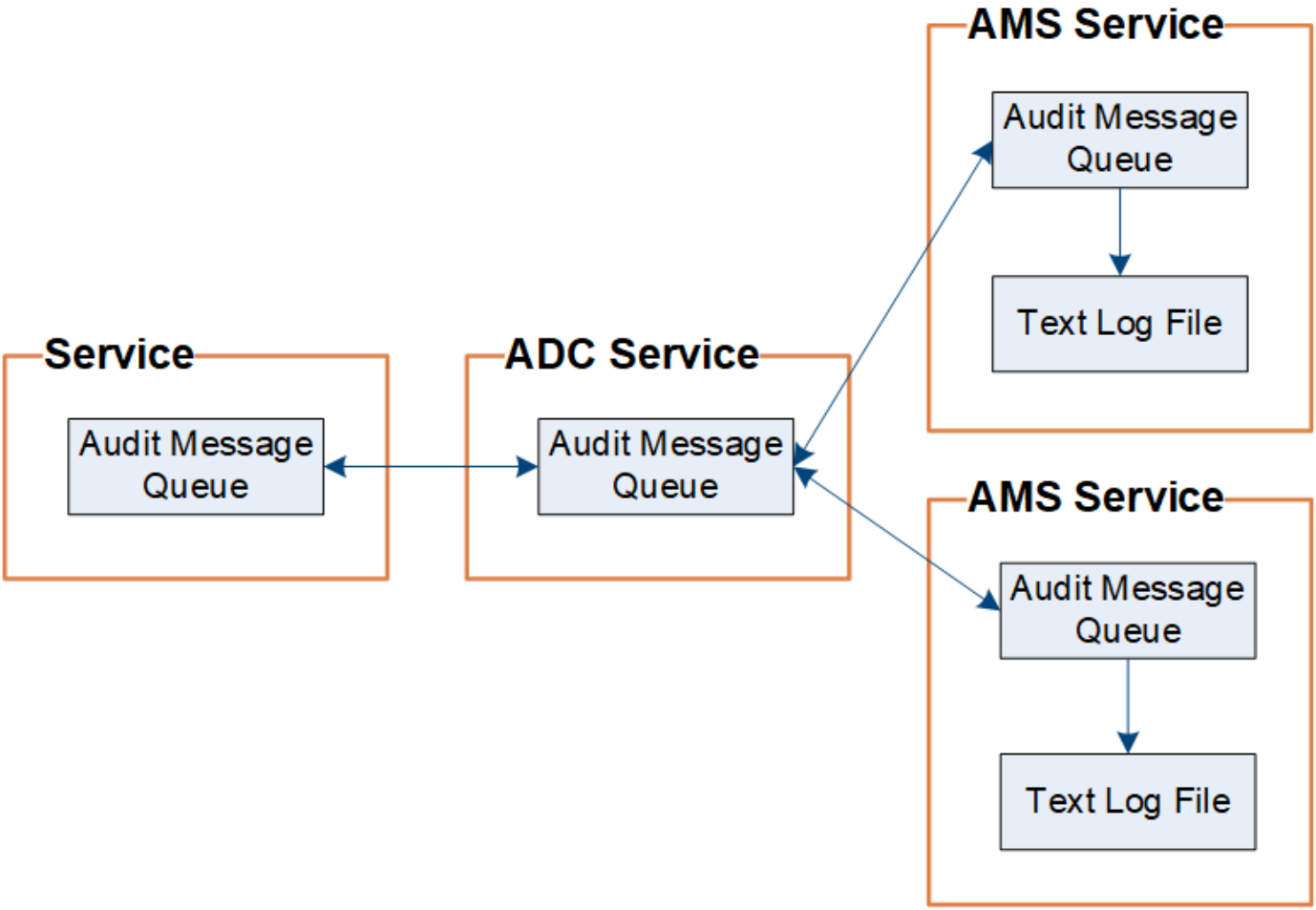
各管理ノードは監査メッセージをテキストログファイルに保存します。アクティブなログファイルの名前は `audit.log`。



監査メッセージの保持

StorageGRID はコピーおよび削除のプロセスを使用して、監査メッセージが監査ログに書き込まれる前に失われないようにします。

ノードが監査メッセージを生成または中継すると、そのメッセージはグリッド ノードのシステム ディスク上の監査メッセージ キューに格納されます。メッセージのコピーは、管理ノードの監査ログファイルにメッセージが書き込まれるまで、常に監査メッセージキューに保持されます。 `/var/local/log`ディレクトリ。これにより、転送中に監査メッセージが失われるのを防ぐことができます。



ネットワーク接続の問題や監査容量の不足により、監査メッセージ キューが一時的に増加する場合があります。キューが増加すると、各ノードの利用可能なスペースをより多く消費するようになります。 `/var/local/` ディレクトリ。問題が解決せず、ノードの監査メッセージ ディレクトリがいっぱいになると、個々のノードはバックログの処理を優先し、一時的に新しいメッセージを処理できなくなります。

具体的には、次のような動作が見られる場合があります。

- もし `/var/local/log`管理ノードが使用するディレクトリがいっぱいになると、ディレクトリがいっぱいでなくなるまで、管理ノードは新しい監査メッセージに使用できないというフラグが付けられます。S3 クライアント要求は影響を受けません。監査リポジトリに到達できない場合、XAMS (到達不能監査リポジトリ) アラームがトリガーされます。
- もし `/var/local/`ADC サービスを使用するストレージ ノードによって使用されるディレクトリが 92% いっぱいになると、ディレクトリが 87% いっぱいになるまで、ノードは監査メッセージに使用できないというフラグが付けられます。他のノードへの S3 クライアント要求は影響を受けません。監査リレーに到達できない場合、NRLY (使用可能な監査リレー) アラームがトリガーされます。

> ADCサービスに利用可能なストレージノードがない場合、ストレージノードは監査メッセージをローカルに保存します。 `/var/local/log/localaudit.log`ファイル。

- もし `/var/local/`ストレージノードが使用するディレクトリが85%いっぱいになると、ノードはS3クライアントのリクエストを拒否し始めます。 `503 Service Unavailable`。

次の種類の問題により、監査メッセージ キューが非常に大きくなる可能性があります。

- ADC サービスを備えた管理ノードまたはストレージ ノードの停止。システムのノードの 1 つがダウンすると、残りのノードがバックログになる可能性があります。
- システムの監査能力を超える持続的なアクティビティ レート。
- その `/var/local/`監査メッセージとは関係のない理由で、ADC ストレージ ノードのスペースがいっぱいになります。このような状況が発生すると、ノードは新しい監査メッセージの受け入れを停止し、現在のバックログを優先するため、他のノードでバックログが発生する可能性があります。

大規模な監査キューアラートと監査メッセージキュー（**AMQS**）アラーム

監査メッセージ キューのサイズを長期にわたって監視できるように、ストレージ ノード キューまたは管理ノード キュー内のメッセージ数が特定のしきい値に達すると、**Large audit queue** アラートと従来の AMQS アラームがトリガーされます。

大きな監査キュー アラートまたは従来の AMQS アラームがトリガーされた場合は、まずシステムの負荷を確認します。最近大量のトランザクションが発生している場合は、アラートとアラームは時間の経過とともに解決されるため、無視できます。

アラートまたはアラームが継続して発生し、重大度が増す場合は、キュー サイズのグラフを表示します。数時間または数日にわたってその数が着実に増加している場合は、監査負荷がシステムの監査能力を超えている可能性があります。クライアント書き込みとクライアント読み取りの監査レベルをエラーまたはオフに変更して、クライアント操作率を下げるか、ログに記録される監査メッセージの数を減らします。見る"監査メッセージとログの保存先を構成する" 。

重複メッセージ

StorageGRIDシステムは、ネットワークまたはノードの障害が発生した場合に保守的なアプローチを採用します。このため、監査ログに重複したメッセージが存在する可能性があります。

アクセス監査ログファイル

監査シェアにはアクティブな `audit.log`ファイルおよび圧縮された監査ログ ファイル。管理ノードのコマンド ラインから監査ログ ファイルに直接アクセスできます。

開始する前に

- あなたが持っている"特定のアクセス権限"。
- あなたは `Passwords.txt`ファイル。
- 管理ノードの IP アドレスを知っておく必要があります。

手順

1. 管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`
   b. 記載されているパスワードを入力してください `Passwords.txt`ファイル。
   c. ルートに切り替えるには、次のコマンドを入力します。 `su -`
   d. 記載されているパスワードを入力してください `Passwords.txt`ファイル。

      ルートとしてログインすると、プロンプトは `$`に `#`。

2. 監査ログ ファイルが含まれているディレクトリに移動します。

```
cd /var/local/log
```

3. 必要に応じて、現在の監査ログ ファイルまたは保存された監査ログ ファイルを表示します。

監査ログファイルのローテーション

監査ログファイルは管理ノードの `/var/local/log`ディレクトリ。アクティブな監査ログファイルの名前は `audit.log。

必要に応じて、監査ログの送信先を変更し、監査情報を外部の syslog サーバーに送信することもできます。外部 Syslog サーバーが構成されている場合、監査レコードのローカル ログは引き続き生成され、保存されます。見る"監査メッセージとログの保存先を構成する" 。

1日1回、アクティブ `audit.log`ファイルが保存され、新しい `audit.log`ファイルが開始されます。保存されたファイルの名前は、保存された日時を示し、 *`yyyy-mm-dd.txt`* 。 1日に複数の監査ログが作成される場合、ファイル名にはファイルが保存された日付に数字が付加され、次の形式になります。 *`yyyy-mm-dd.txt.n`* 。例えば、 `2018-04-15.txt`そして `2018-04-15.txt.1`これらは、2018 年 4 月 15 日に作成され保存された最初のログ ファイルと 2 番目のログ ファイルです。

1日後、保存されたファイルは圧縮され、名前が変更され、形式は次のようになります。 *`yyyy-mm-dd.txt.gz`* 、元の日付が保持されます。時間が経つにつれて、管理ノード上の監査ログに割り当てられたストレージが消費されることになります。スクリプトは監査ログのスペース消費を監視し、必要に応じてログファイルを削除して、 `/var/local/log`ディレクトリ。監査ログは作成日に基づいて削除され、最も古いものから順に削除されます。次のファイルでスクリプトのアクションを監視できます。 `/var/local/log/manage-audit.log 。

この例では、アクティブな `audit.log`ファイル、前日のファイル（`2018-04-15.txt`）、および前日の圧縮ファイル(2018-04-14.txt.gz）。

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

監査ログファイルの形式

監査ログファイルの形式

監査ログ ファイルはすべての管理ノード上に存在し、個々の監査メッセージのコレクションが含まれています。

各監査メッセージには次の内容が含まれます。

- 監査メッセージ (ATIM) をトリガーしたイベントの協定世界時 (UTC) を ISO 8601 形式で示し、その後にスペースを 1 つ入力します。

  `YYYY-MM-DDTHH:MM:SS.UUUUUU`、 どこ *`UUUUUU`* マイクロ秒です。

- 監査メッセージ自体は角括弧で囲まれ、 `AUDT` 。

次の例は、監査ログ ファイル内の 3 つの監査メッセージを示しています (読みやすくするために改行が追加されています)。これらのメッセージは、テナントが S3 バケットを作成し、そのバケットに 2 つのオブジェクトを追加したときに生成されました。

```
2019-08-07T18:43:30.247711
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991681][TIME(UI64):73520][SAI
P(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][AVER(UI32):10][ATIM(UI64):1565203410247711]
[ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):7074142
142472611085]]

2019-08-07T18:43:30.783597
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991696][TIME(UI64):120713][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-0"]
[CBID(UI64):0x779557A069B2C037][UUID(CSTR):"94BA6949-38E1-4B0C-BC80-
EB44FB4FCC7F"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410783597][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):8439606722108456022]]

2019-08-07T18:43:30.784558
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991693][TIME(UI64):121666][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-2000"]
[CBID(UI64):0x180CBD8E678EED17][UUID(CSTR):"19CE06D0-D2CF-4B03-9C38-
E578D66F7ADD"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410784558][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):13489590586043706682]]
```

デフォルトの形式では、監査ログ ファイル内の監査メッセージは読みやすく解釈しにくいものです。使用することができます"監査説明ツール"監査ログ内の監査メッセージの簡略化された要約を取得します。使用することができます"監査合計ツール"記録された書き込み、読み取り、削除操作の数と、これらの操作にかかった

時間を要約します。

監査説明ツールを使用する

使用することができます `audit-explain`監査ログ内の監査メッセージを読みやすい形式に変換するツール。

開始する前に

- あなたが持っている"特定のアクセス権限"。
- あなたは `Passwords.txt`ファイル。
- プライマリ管理ノードの IP アドレスを知っておく必要があります。

タスク概要

その `audit-explain`プライマリ管理ノードで利用可能なツールは、監査ログ内の監査メッセージの簡略化された概要を提供します。

> その `audit-explain`このツールは主に、トラブルシューティング操作中にテクニカル サポートが使用することを目的としています。処理 `audit-explain`クエリは大量の CPU パワーを消費する可能性があり、 StorageGRID の操作に影響を与える可能性があります。

この例は、 `audit-explain`道具。これら4つ"吐き出す"アカウント ID 92484777680322627870 の S3 テナントが S3 PUT リクエストを使用して「bucket1」という名前のバケットを作成し、そのバケットに 3 つのオブジェクトを追加したときに、監査メッセージが生成されました。

```
SPUT S3 PUT bucket bucket1 account:92484777680322627870 usec:124673
SPUT S3 PUT object bucket1/part1.txt tenant:92484777680322627870
cbid:9DCB157394F99FE5 usec:101485
SPUT S3 PUT object bucket1/part2.txt tenant:92484777680322627870
cbid:3CFBB07AB3D32CA9 usec:102804
SPUT S3 PUT object bucket1/part3.txt tenant:92484777680322627870
cbid:5373D73831ECC743 usec:93874
```

その `audit-explain`このツールは次のことができます。

- プレーンまたは圧縮された監査ログを処理します。例えば：

  ```
  audit-explain audit.log

  audit-explain 2019-08-12.txt.gz
  ```

- 複数のファイルを同時に処理します。例えば：

  ```
  audit-explain audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz

  audit-explain /var/local/log/*
  ```

- パイプからの入力を受け入れ、入力をフィルタリングしたり前処理したりすることができます。 `grep`命令またはその他の手段。例えば：

```
grep SPUT audit.log | audit-explain

grep bucket-name audit.log | audit-explain
```

監査ログは非常に大きく、解析に時間がかかるため、確認したい部分をフィルタリングして実行することで時間を節約できます。 `audit-explain`ファイル全体ではなく、部分ごとに行います。

> その `audit-explain`ツールはパイプ入力として圧縮ファイルを受け入れません。圧縮ファイルを処理するには、コマンドライン引数としてファイル名を指定するか、 `zcat`まずファイルを解凍するツールです。例えば：
>
> ```
> zcat audit.log.gz | audit-explain
> ```

使用 `help (-h)`利用可能なオプションを表示するには、オプションを選択します。例えば：

```
$ audit-explain -h
```

手順

1. プライマリ管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`
   b. 記載されているパスワードを入力してください `Passwords.txt`ファイル。
   c. ルートに切り替えるには、次のコマンドを入力します。 `su -`
   d. 記載されているパスワードを入力してください `Passwords.txt`ファイル。

      ルートとしてログインすると、プロンプトは `$`に `#`。
2. 次のコマンドを入力します。 `/var/local/log/audit.log`分析するファイルの名前と場所を表します。

   ```
   $ audit-explain /var/local/log/audit.log
   ```

   その `audit-explain`このツールは、指定されたファイル内のすべてのメッセージの人間が読める形式の解釈を出力します。

   > 行の長さを短くし、読みやすくするために、タイムスタンプはデフォルトでは表示されません。タイムスタンプを確認したい場合は、タイムスタンプを使用してください(`-t`） オプション。

監査合計ツールを使用する

使用することができます `audit-sum`書き込み、読み取り、ヘッド、削除の監査メッセージをカウントし、各操作タイプの最小時間、最大時間、平均時間 (またはサイズ) を確認するツール。

開始する前に

- あなたが持っている"特定のアクセス権限"。
- あなたは `Passwords.txt`ファイル。

- プライマリ管理ノードの IP アドレスを知っておく必要があります。

タスク概要

その `audit-sum`プライマリ管理ノードで利用可能なツールは、ログに記録された書き込み、読み取り、削除操作の数と、これらの操作にかかった時間を要約します。

> その `audit-sum`このツールは主に、トラブルシューティング操作中にテクニカル サポートが使用することを目的としています。処理 `audit-sum`クエリは大量の CPU パワーを消費する可能性があり、 StorageGRID の操作に影響を与える可能性があります。

この例は、 `audit-sum`道具。この例では、プロトコル操作にかかった時間を示します。

```
  message group            count     min(sec)        max(sec)
average(sec)
  =============            =====     ========        ========
============
  IDEL                       274
  SDEL                    213371        0.004          20.934
0.352
  SGET                    201906        0.010        1740.290
1.132
  SHEA                     22716        0.005           2.349
0.272
  SPUT                   1771398        0.011        1770.563
0.487
```

その `audit-sum`このツールは、監査ログ内の次の S3、Swift、および ILM 監査メッセージの数と時間を提供します。

> 機能が廃止されると、監査コードは製品およびドキュメントから削除されます。ここに記載されていない監査コードが発生した場合は、このトピックの以前のバージョンで古い SG リリースを確認してください。例： "StorageGRID 11.8 監査合計ツールの使用に関するドキュメント" 。

コード	説明	参照
アイデル	ILM による削除の開始: ILM がオブジェクトの削除プロセスを開始したときにログに記録します。	"IDEL: ILM による削除開始"
SDEL	S3 DELETE: オブジェクトまたはバケットを削除する成功したトランザクションをログに記録します。	"SDEL: S3 削除"
SGET	S3 GET: オブジェクトを取得したり、バケット内のオブジェクトを一覧表示したりするための成功したトランザクションをログに記録します。	"SGET: S3 ゲット"

コード	説明	参照
シア	S3 HEAD: オブジェクトまたはバケットの存在を確認するために成功したトランザクションをログに記録します。	"シア：S3ヘッド"
吐き出す	S3 PUT: 新しいオブジェクトまたはバケットを作成するための成功したトランザクションをログに記録します。	"スプット: S3 プット"
WDEL	Swift DELETE: オブジェクトまたはコンテナを削除する成功したトランザクションをログに記録します。	"WDEL: 迅速な削除"
WGET	Swift GET: オブジェクトを取得したり、コンテナー内のオブジェクトを一覧表示したりするための成功したトランザクションをログに記録します。	"WGET: Swift GET"
ウィー	Swift HEAD: オブジェクトまたはコンテナの存在を確認するために成功したトランザクションをログに記録します。	"WHEA: Swift HEAD"
WPUT	Swift PUT: 新しいオブジェクトまたはコンテナーを作成するための成功したトランザクションをログに記録します。	"WPUT: Swift PUT"

その `audit-sum`このツールは次のことができます。

- プレーンまたは圧縮された監査ログを処理します。例えば：

```
audit-sum audit.log

audit-sum 2019-08-12.txt.gz
```

- 複数のファイルを同時に処理します。例えば：

```
audit-sum audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz

audit-sum /var/local/log/*
```

- パイプからの入力を受け入れ、入力をフィルタリングしたり前処理したりすることができます。 `grep`命令またはその他の手段。例えば：

```
grep WGET audit.log | audit-sum

grep bucket1 audit.log | audit-sum

grep SPUT audit.log | grep bucket1 | audit-sum
```

このツールは、パイプ入力として圧縮ファイルを受け入れません。圧縮ファイルを処理するには、コマンドライン引数としてファイル名を指定するか、 `zcat`まずファイルを解凍するツールです。例えば：

```
audit-sum audit.log.gz

zcat audit.log.gz | audit-sum
```

コマンドライン オプションを使用すると、オブジェクトの操作とは別にバケットの操作を要約したり、バケット名、期間、またはターゲット タイプごとにメッセージの概要をグループ化したりできます。デフォルトでは、要約には最小、最大、平均操作時間が表示されますが、 `size (-s)`代わりにオブジェクトのサイズを確認するオプション。

使用 `help (-h)`利用可能なオプションを表示するには、オプションを選択します。例えば：

```
$ audit-sum -h
```

手順

1. プライマリ管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`
   b. 記載されているパスワードを入力してください `Passwords.txt`ファイル。
   c. ルートに切り替えるには、次のコマンドを入力します。 `su -`
   d. 記載されているパスワードを入力してください `Passwords.txt`ファイル。

      ルートとしてログインすると、プロンプトは `$`に `#`。
2. 書き込み、読み取り、ヘッド、削除操作に関連するすべてのメッセージを分析する場合は、次の手順に従います。
   a. 次のコマンドを入力します。 `/var/local/log/audit.log`分析するファイルの名前と場所を表します。

      ```
      $ audit-sum /var/local/log/audit.log
      ```

      この例は、 `audit-sum`道具。この例では、プロトコル操作にかかった時間を示します。

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  IDEL                      274
  SDEL                   213371        0.004          20.934
0.352
  SGET                   201906        0.010        1740.290
1.132
  SHEA                    22716        0.005           2.349
0.272
  SPUT                 1771398        0.011        1770.563
0.487
```

この例では、SGET (S3 GET) 操作の平均時間が 1.13 秒で最も遅いですが、SGET 操作と SPUT (S3 PUT) 操作はどちらも最悪で約 1,770 秒という長い時間を示しています。

b. 最も遅い10件の取得操作を表示するには、grepコマンドを使用してSGETメッセージのみを選択し、長い出力オプションを追加します。(`-l`) を使用してオブジェクト パスを含めます。

```
grep SGET audit.log | audit-sum -l
```

結果にはタイプ (オブジェクトまたはバケット) とパスが含まれるため、監査ログで grep を実行して、これらの特定のオブジェクトに関連する他のメッセージを検索できます。

```
Total:          201906 operations
    Slowest:      1740.290 sec
    Average:         1.132 sec
    Fastest:         0.010 sec
    Slowest operations:
        time(usec)       source ip         type      size(B) path
        ========== ============== ============ ============ ====
        1740289662   10.96.101.125       object   5663711385
backup/r9O1OaQ8JB-1566861764-4519.iso
        1624414429   10.96.101.125       object   5375001556
backup/r9O1OaQ8JB-1566861764-6618.iso
        1533143793   10.96.101.125       object   5183661466
backup/r9O1OaQ8JB-1566861764-4518.iso
             70839   10.96.101.125       object        28338
bucket3/dat.1566861764-6619
             68487   10.96.101.125       object        27890
bucket3/dat.1566861764-6615
             67798   10.96.101.125       object        27671
bucket5/dat.1566861764-6617
             67027   10.96.101.125       object        27230
bucket5/dat.1566861764-4517
             60922   10.96.101.125       object        26118
bucket3/dat.1566861764-4520
             35588   10.96.101.125       object        11311
bucket3/dat.1566861764-6616
             23897   10.96.101.125       object        10692
bucket3/dat.1566861764-4516
```

+
この出力例から、最も遅い 3 つの S3 GET リクエストは、サイズが約 5 GB のオブジェクトに対するものであり、他のオブジェクトよりもはるかに大きいことがわかります。サイズが大きいと、最悪の場合、取得時間が遅くなります。

3. グリッドに取り込まれるオブジェクトのサイズとグリッドから取得されるオブジェクトのサイズを決定するには、サイズオプションを使用します。(`-s`):

```
audit-sum -s audit.log
```

```
  message group            count       min(MB)          max(MB)
average(MB)
  =============            =====     ========        ========
============
  IDEL                       274        0.004        5000.000
1654.502
  SDEL                    213371        0.000          10.504
1.695
  SGET                    201906        0.000        5000.000
14.920
  SHEA                     22716        0.001          10.504
2.967
  SPUT                   1771398        0.000        5000.000
2.495
```

この例では、SPUT の平均オブジェクト サイズは 2.5 MB 未満ですが、SGET の平均サイズははるかに大きくなります。 SPUT メッセージの数は SGET メッセージの数よりもはるかに多く、ほとんどのオブジェクトが取得されないことを示しています。

4. 昨日の取得が遅かったかどうかを判断したい場合:

   a. 適切な監査ログに対してコマンドを発行し、時間別グループオプションを使用します。(`-gt` ）の後に期間（例：15M、1H、10S）を続けます。

      ```
      grep SGET audit.log | audit-sum -gt 1H
      ```

```
  message group           count    min(sec)       max(sec)
average(sec)
  =============           =====     ========        ========
============
  2019-09-05T00            7591        0.010        1481.867
1.254
  2019-09-05T01            4173        0.011        1740.290
1.115
  2019-09-05T02           20142        0.011        1274.961
1.562
  2019-09-05T03           57591        0.010        1383.867
1.254
  2019-09-05T04          124171        0.013        1740.290
1.405
  2019-09-05T05          420182        0.021        1274.511
1.562
  2019-09-05T06         1220371        0.015        6274.961
5.562
  2019-09-05T07          527142        0.011        1974.228
2.002
  2019-09-05T08          384173        0.012        1740.290
1.105
  2019-09-05T09           27591        0.010        1481.867
1.354
```

これらの結果は、S3 GET トラフィックが 06:00 から 07:00 の間に急増したことを示しています。これらの時間では、最大時間と平均時間はどちらもかなり長くなっており、カウントが増加しても徐々に増加することはありません。これは、ネットワークまたはグリッドのリクエスト処理能力のどこかで容量が超過したことを示しています。

b. 昨日1時間ごとに取得されたオブジェクトのサイズを確認するには、サイズオプションを追加します。(`-s`) をコマンドに追加します:

```
grep SGET audit.log | audit-sum -gt 1H -s
```

```
  message group           count       min(B)          max(B)
average(B)
  =============           =====     ========        ========
============
  2019-09-05T00            7591        0.040        1481.867
1.976
  2019-09-05T01            4173        0.043        1740.290
2.062
  2019-09-05T02           20142        0.083        1274.961
2.303
  2019-09-05T03           57591        0.912        1383.867
1.182
  2019-09-05T04          124171        0.730        1740.290
1.528
  2019-09-05T05          420182        0.875        4274.511
2.398
  2019-09-05T06         1220371        0.691  5663711385.961
51.328
  2019-09-05T07          527142        0.130        1974.228
2.147
  2019-09-05T08          384173        0.625        1740.290
1.878
  2019-09-05T09           27591        0.689        1481.867
1.354
```

これらの結果は、全体的な検索トラフィックが最大になったときに、非常に大規模な検索がいくつか発生したことを示しています。

c. さらに詳しく見るには、"監査説明ツール"その時間中のすべての SGET 操作を確認します。

```
grep 2019-09-05T06 audit.log | grep SGET | audit-explain | less
```

grepコマンドの出力が複数行になることが予想される場合は、 `less`監査ログ ファイルの内容を一度に 1 ページ (1 画面) ずつ表示するコマンド。

5. バケットに対する SPUT 操作がオブジェクトに対する SPUT 操作よりも遅いかどうかを確認するには、次の手順を実行します。

a. まずは `-go`オブジェクト操作とバケット操作のメッセージを個別にグループ化するオプション:

```
grep SPUT sample.log | audit-sum -go
```

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  SPUT.bucket                 1        0.125           0.125
0.125
  SPUT.object                12        0.025           1.019
0.236
```

結果は、バケットに対する SPUT 操作は、オブジェクトに対する SPUT 操作とは異なるパフォーマンス特性を持つことを示しています。

b. SPUT操作が最も遅いバケットを特定するには、 `-gb`メッセージをバケットごとにグループ化するオプション:

```
grep SPUT audit.log | audit-sum -gb
```

```
  message group                  count     min(sec)        max(sec)
average(sec)
  =============                  =====     ========        ========
============
  SPUT.cho-non-versioning        71943        0.046        1770.563
1.571
  SPUT.cho-versioning            54277        0.047        1736.633
1.415
  SPUT.cho-west-region           80615        0.040          55.557
1.329
  SPUT.ldt002                  1564563        0.011          51.569
0.361
```

c. SPUTオブジェクトのサイズが最も大きいバケットを特定するには、 `-gb`そして `-s`オプション:

```
grep SPUT audit.log | audit-sum -gb -s
```

```
  message group                    count       min(B)          max(B)
average(B)
  =============                    =====     ========        ========
============
  SPUT.cho-non-versioning          71943        2.097        5000.000
21.672
  SPUT.cho-versioning              54277        2.097        5000.000
21.120
  SPUT.cho-west-region             80615        2.097         800.000
14.433
  SPUT.ldt002                    1564563        0.000         999.972
0.352
```

監査メッセージの形式

監査メッセージの形式

StorageGRIDシステム内で交換される監査メッセージには、すべてのメッセージに共通する標準情報と、報告されるイベントまたはアクティビティを説明する特定のコンテンツが含まれます。

提供された概要情報が"監査説明"そして"監査合計"ツールだけでは不十分な場合は、このセクションを参照して、すべての監査メッセージの一般的な形式を理解してください。

以下は、監査ログ ファイルに表示される監査メッセージの例です。

```
2014-07-17T03:50:47.484627
[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP(F
C32):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265006
03516]]
```

各監査メッセージには、属性要素の文字列が含まれています。文字列全体が括弧で囲まれている(`[ ]`) であり、文字列内の各属性要素には次の特性があります。

- 括弧内 `[ ]`
- 文字列によって導入 `AUDT`監査メッセージを示す
- 前後に区切り文字（カンマやスペースなし）なし
- 改行文字で終了する `\n`

各要素には、属性コード、データ型、および次の形式で報告される値が含まれます。

```
[ATTR(type):value][ATTR(type):value]...
[ATTR(type):value]\n
```

メッセージ内の属性要素の数は、メッセージのイベント タイプによって異なります。属性要素は特定の順序でリストされていません。

次のリストは、属性要素について説明しています。

- `ATTR`報告される属性の 4 文字のコードです。すべての監査メッセージに共通する属性と、イベント固有の属性があります。
- `type`UI64、FC32 など、値のプログラミング データ型の 4 文字の識別子です。型は括弧で囲まれます `( )。
- `value`属性の内容であり、通常は数値またはテキスト値です。値は常にコロンの後に続きます (:`）。データ型 CSTR の値は二重引用符 " " で囲まれます。

データ型

監査メッセージに情報を格納するために、さまざまなデータ型が使用されます。

タイプ	説明
UI32	符号なし長整数 (32 ビット)。0 から 4,294,967,295 までの数値を格納できます。
UI64	符号なし倍精度整数 (64 ビット)。0 から 18,446,744,073,709,551,615 までの数値を格納できます。
FC32	4 文字の定数。「ABCD」などの 4 つの ASCII 文字として表される 32 ビットの符号なし整数値。
iPad	IP アドレスに使用されます。
CSTR	UTF-8 文字の可変長配列。文字は次の規則に従ってエスケープできます。 • バックスラッシュは \\ です。 • キャリッジリターンは \r です。 • 二重引用符は \" です。 • 改行(新しい行)は\nです。 • 文字は、それに相当する 16 進数値 (\xHH 形式、HH は文字を表す 16 進数値) に置き換えることができます。

イベント固有のデータ

監査ログ内の各監査メッセージには、システム イベントに固有のデータが記録されます。

オープニングに続いて `[AUDT:`メッセージ自体を識別するコンテナーの次の属性セットは、監査メッセージによって記述されたイベントまたはアクションに関する情報を提供します。これらの属性は次の例で強調表示されています。

2018-12-05T08:24:45.921845 [AUDT:*\[RSLT\(FC32\):SUCS\]*
\[TIME\(UI64\):11454\]\[SAIP\(IPAD\):"10.224.0.100"\]\[S3AI\(CSTR\):"60025621595611246499"\]
\[SACC\(CSTR\):"アカウント**"\]\[S3AK\(CSTR\):"SGKH4_Nc8SO1H6w3w0nCOFCGgk__E6dYzKlumRsKJA=="\]**
\[SUSR\(CSTR\):"urn:sgws:identity::60025621595611246499:root"\]
\[SBAI\(CSTR\):"60025621595611246499"\]\[SBAC\(CSTR\):"アカウント**"\]\[S3BK\(CSTR\):"**バケット**"\] \[S3KY\(CSTR\):"**オブジェクト**"\]\[CBID\(UI64\):0xCC128B9B9E428347\]**
\[UUID\(CSTR\):"B975D2CE-E4DA-4D14-8A23-1CB4B83F2CD8"\]\[CSIZ\(UI64\):30720\][AVER(UI32):10]
\[ATIM(UI64):1543998285921845]\[ATYP\(FC32\):SHEA\][ANID(UI32):12281045][AMID(FC32):S3RQ]
\[ATID(UI64):15552417629170647261]]

その `ATYP`要素 (例では下線部) は、メッセージを生成したイベントを識別します。このサンプルメッセージには、"シア"メッセージ コード ([ATYP(FC32):SHEA])。これは、S3 HEAD 要求が成功したことによって生成されたことを示します。

監査メッセージの共通要素

すべての監査メッセージには共通の要素が含まれています。

コード	タイプ	説明
真ん中	FC32	モジュール ID: メッセージを生成したモジュール ID の 4 文字の識別子。これは、監査メッセージが生成されたコード セグメントを示します。
アニド	UI32	ノード ID: メッセージを生成したサービスに割り当てられたグリッド ノード ID。 StorageGRIDシステムが構成およびインストールされたときに、各サービスに一意の識別子が割り当てられます。このIDは変更できません。
ASES	UI64	監査セッション識別子: 以前のリリースでは、この要素は、サービスの起動後に監査システムが初期化された時刻を示していました。この時間値は、オペレーティング システムのエポック (1970 年 1 月 1 日 00:00:00 UTC) からのマイクロ秒単位で測定されました。 注: この要素は廃止されており、監査メッセージには表示されなくなりました。
ASQN	UI64	シーケンス カウント: 以前のリリースでは、このカウンタはグリッド ノード (ANID) で生成された監査メッセージごとに増加し、サービスの再起動時にゼロにリセットされていました。 注: この要素は廃止されており、監査メッセージには表示されなくなりました。

コード	タイプ	説明
ATID	UI64	トレース ID: 単一のイベントによってトリガーされたメッセージのセットによって共有される識別子。
アティム	UI64	タイムスタンプ: 監査メッセージをトリガーしたイベントが生成された時刻。オペレーティング システムのエポック (1970 年 1 月 1 日 00:00:00 UTC) からのマイクロ秒単位で測定されます。タイムスタンプをローカルの日付と時刻に変換するための利用可能なツールのほとんどは、ミリ秒に基づいていることに注意してください。 ログに記録されたタイムスタンプの丸めまたは切り捨てが必要になる場合があります。監査メッセージの冒頭に表示される、人間が読める形式の時刻。 `audit.log`ファイルは `ISO 8601` 形式の `ATIM` 属性です。日付と時刻は次のように表されます `*YYYY-MMDDTHH:MM:SS.UUUUUU*`、ここで `T`日付の時間セグメントの開始を示すリテラル文字列文字です。 `*UUUUUU*`マイクロ秒です。
ATYP	FC32	イベント タイプ: 記録されるイベントの 4 文字の識別子。これは、メッセージの「ペイロード」コンテンツ、つまり含まれる属性を制御します。
アバー	UI32	バージョン: 監査メッセージのバージョン。 StorageGRIDソフトウェアが進化するにつれて、新しいバージョンのサービスに監査レポートの新しい機能が組み込まれる可能性があります。このフィールドにより、AMS サービスでの下位互換性が有効になり、古いバージョンのサービスからのメッセージを処理できるようになります。
RSLT	FC32	結果: イベント、プロセス、またはトランザクションの結果。メッセージに関連しない場合は、メッセージが誤ってフィルタリングされないように、SUCS ではなく NONE が使用されます。

監査メッセージの例

各監査メッセージに詳細情報が記載されています。すべての監査メッセージは同じ形式を使用します。

以下は、監査メッセージの例です。 `audit.log`ファイル：

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPUT
][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224144
102530435]]
```

監査メッセージには、記録されるイベントに関する情報と、監査メッセージ自体に関する情報が含まれます。

監査メッセージによって記録されるイベントを識別するには、ATYP 属性 (以下に強調表示) を探します。

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224
144102530435]]
```

ATYP 属性の値は SPUT です。"吐き出す"バケットへのオブジェクトの取り込みを記録する S3 PUT トランザクションを表します。

次の監査メッセージには、オブジェクトが関連付けられているバケットも表示されます。

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK\(CSTR\):"s3small1"][S3
KY(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):
0][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPU
T][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):157922414
4102530435]]
```

PUT イベントがいつ発生したかを確認するには、監査メッセージの先頭にある協定世界時 (UTC) のタイムスタンプに注目してください。この値は、監査メッセージ自体の ATIM 属性の人間が読めるバージョンです。

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM\(UI64\):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):15792241
44102530435]]
```

ATIM は、UNIX エポックの開始からの時間をマイクロ秒単位で記録します。この例では、値 `1405631878959669`2014年7月17日木曜日 21:17:59 UTC に翻訳されます。

監査メッセージとオブジェクトのライフサイクル

監査メッセージはいつ生成されますか?

オブジェクトが取り込まれたり、取得されたり、削除されたりするたびに、監査メッセージが生成されます。 S3 API 固有の監査メッセージを見つけることで、監査ログでこれらのトランザクションを識別できます。

監査メッセージは、各プロトコルに固有の識別子を通じてリンクされます。

プロトコル	コード
S3操作のリンク	S3BK（バケット）、S3KY（キー）、またはその両方
Swift操作のリンク	WCON（コンテナ）、WOBJ（オブジェクト）、またはその両方
内部業務の連携	CBID（オブジェクトの内部識別子）

監査メッセージのタイミング

グリッド ノード間のタイミングの違い、オブジェクトのサイズ、ネットワークの遅延などの要因により、さまざまなサービスによって生成される監査メッセージの順序は、このセクションの例に示されている順序と異なる場合があります。

オブジェクト取り込みトランザクション

S3 API 固有の監査メッセージを見つけることで、監査ログでクライアントの取り込みトランザクションを識別できます。

取り込みトランザクション中に生成されるすべての監査メッセージが次の表に記載されているわけではありません。取り込みトランザクションのトレースに必要なメッセージのみが含まれます。

S3 取り込み監査メッセージ

コード	**Name**	説明	トレース	詳細については、
吐き出す	S3 PUTトランザクション	S3 PUT 取り込みトランザクションが正常に完了しました。	CBID、S3BK、S3KY	"スプット: S3 プット"
オーム	オブジェクトルールが満たされました	このオブジェクトに対して ILM ポリシーが満たされました。	CBID	"ORLM: オブジェクトルールが満たされました"

Swift の監査メッセージの取り込み

コード	**Name**	説明	トレース	詳細については、
WPUT	Swift PUTトランザクション	Swift PUT 取り込みトランザクションが正常に完了しました。	CBID、WCON、WOBJ	"WPUT: Swift PUT"
オーム	オブジェクトルールが満たされました	このオブジェクトに対して ILM ポリシーが満たされました。	CBID	"ORLM: オブジェクトルールが満たされました"

例: **S3** オブジェクトの取り込み

以下の一連の監査メッセージは、S3 クライアントがオブジェクトをストレージ ノード (LDR サービス) に取り込むときに生成され、監査ログに保存される監査メッセージの例です。

この例では、アクティブな ILM ポリシーに「2 つのコピーを作成」ILM ルールが含まれています。

> 以下の例には、トランザクション中に生成されるすべての監査メッセージがリストされているわけではありません。 S3 取り込みトランザクション (SPUT) に関連するものだけがリストされます。

この例では、S3 バケットが以前に作成されていることを前提としています。

スプット: **S3** プット

SPUT メッセージは、特定のバケットにオブジェクトを作成するために S3 PUT トランザクションが発行されたことを示すために生成されます。

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):25771][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"][S3BK(CSTR):"example"][S3KY(CSTR):"testobject-0-
3"][CBID\(UI64\):0x8EF52DF8025E63A8][CSIZ(UI64):30720][AVER(UI32):10][ATIM
(UI64):150032627859669][ATYP\(FC32\):SPUT][ANID(UI32):12086324][AMID(FC32)
:S3RQ][ATID(UI64):14399932238768197038]]
```

ORLM: オブジェクトルールが満たされました

ORLM メッセージは、このオブジェクトに対して ILM ポリシーが満たされていることを示します。メッセージには、オブジェクトの CBID と適用された ILM ルールの名前が含まれます。

複製されたオブジェクトの場合、LOCS フィールドにはオブジェクトの場所の LDR ノード ID とボリューム ID が含まれます。

```
2019-07-
17T21:18:31.230669[AUDT:[CBID\(UI64\):0x50C4F7AC2BC8EDF7][RULE(CSTR):"Make
2 Copies"][STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"0B344E18-98ED-4F22-
A6C8-A93ED68F8D3F"][LOCS(CSTR):"CLDI 12828634 2148730112, CLDI 12745543
2147552014"][RSLT(FC32):SUCS][AVER(UI32):10][ATYP\(FC32\):ORLM][ATIM(UI64)
:1563398230669][ATID(UI64):15494889725796157557][ANID(UI32):13100453][AMID
(FC32):BCMS]]
```

消失訂正符号化オブジェクトの場合、LOCSフィールドには消失訂正符号化プロファイルIDと消失訂正符号化グループIDが含まれます。

```
2019-02-23T01:52:54.647537
[AUDT:[CBID(UI64):0xFA8ABE5B5001F7E2][RULE(CSTR):"EC_2_plus_1"][STAT(FC32)
:DONE][CSIZ(UI64):10000][UUID(CSTR):"E291E456-D11A-4701-8F51-
D2F7CC9AFECA"][LOCS(CSTR):"CLEC 1 A471E45D-A400-47C7-86AC-
12E77F229831"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1550929974537]\[
ATYP\(FC32\):ORLM\][ANID(UI32):12355278][AMID(FC32):ILMX][ATID(UI64):41685
59046473725560]]
```

PATH フィールドには、使用された API に応じて、S3 バケットとキーの情報、または Swift コンテナとオブジェクトの情報が含まれます。

```
2019-09-15.txt:2018-01-24T13:52:54.131559
[AUDT:[CBID(UI64):0x82704DFA4C9674F4][RULE(CSTR):"Make 2
Copies"][STAT(FC32):DONE][CSIZ(UI64):3145729][UUID(CSTR):"8C1C9CAC-22BB-
4880-9115-
CE604F8CE687"][PATH(CSTR):"frisbee_Bucket1/GridDataTests151683676324774_1_
1vf9d"][LOCS(CSTR):"CLDI 12525468, CLDI
12222978"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1568555574559][ATYP(
FC32):ORLM][ANID(UI32):12525468][AMID(FC32):OBDI][ATID(UI64):3448338865383
69336]]
```

オブジェクト削除トランザクション

S3 API 固有の監査メッセージを見つけることで、監査ログ内のオブジェクト削除トランザクションを識別できます。

削除トランザクション中に生成されるすべての監査メッセージが次の表に記載されているわけではありません。削除トランザクションのトレースに必要なメッセージのみが含まれます。

S3 監査メッセージ削除

コード	Name	説明	トレース	詳細については、
SDEL	S3 削除	バケットからオブジェクトを削除するリクエストが行われました。	CBID、S3KY	"SDEL: S3 削除"

監査メッセージを迅速に削除

コード	Name	説明	トレース	詳細については、
WDEL	迅速な削除	コンテナからオブジェクトまたはコンテナを削除する要求。	CBID、WOBJ	"WDEL: 迅速な削除"

例: **S3** オブジェクトの削除

S3 クライアントがストレージ ノード (LDR サービス) からオブジェクトを削除すると、監査メッセージが生成され、監査ログに保存されます。

削除トランザクション中に生成されるすべての監査メッセージが以下の例にリストされているわけではありません。 S3 削除トランザクション (SDEL) に関連するものだけがリストされます。

SDEL: S3 削除

オブジェクトの削除は、クライアントが LDR サービスに DeleteObject 要求を送信すると開始されます。メッセージには、オブジェクトを削除するバケットと、オブジェクトを識別するために使用されるオブジェクトの S3 キーが含まれています。

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):14316][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"]\[S3BK\(CSTR\):"example"\]\[S3KY\(CSTR\):"testobject-0-
7"\][CBID\(UI64\):0x339F21C5A6964D89][CSIZ(UI64):30720][AVER(UI32):10][ATI
M(UI64):150032627859669][ATYP\(FC32\):SDEL][ANID(UI32):12086324][AMID(FC32
):S3RQ][ATID(UI64):4727861330952970593]]
```

オブジェクト取得トランザクション

S3 API 固有の監査メッセージを見つけることで、監査ログ内のオブジェクト取得トランザクションを識別できます。

取得トランザクション中に生成されるすべての監査メッセージが次の表に記載されているわけではありません。取得トランザクションのトレースに必要なメッセージのみが含まれます。

S3 取得監査メッセージ

コード	Name	説明	トレース	詳細については、
SGET	S3 GET	バケットからオブジェクトを取得する要求が行われました。	CBID、S3BK、S3KY	"SGET: S3 ゲット"

監査メッセージの迅速な取得

コード	Name	説明	トレース	詳細については、
WGET	Swift GET	コンテナからオブジェクトを取得する要求。	CBID、WCON、WOBJ	"WGET: Swift GET"

例: S3 オブジェクトの取得

S3 クライアントがストレージ ノード (LDR サービス) からオブジェクトを取得すると、監査メッセージが生成され、監査ログに保存されます。

以下の例には、トランザクション中に生成されるすべての監査メッセージがリストされているわけではないことに注意してください。 S3 取得トランザクション (SGET) に関連するものだけがリストされます。

SGET: S3 ゲット

オブジェクトの取得は、クライアントが LDR サービスに GetObject 要求を送信すると開始されます。メッセージには、オブジェクトを取得するバケットと、オブジェクトを識別するために使用されるオブジェクトの S3 キーが含まれています。

```
2017-09-20T22:53:08.782605
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):47807][SAIP(IPAD):"10.96.112.26"][S3AI(
CSTR):"43979298178977966408"][SACC(CSTR):"s3-account-
a"][S3AK(CSTR):"SGKHt7GzEcu0yXhFhT_rL5mep4nJt1w75GBh-
O_FEw=="][SUSR(CSTR):"urn:sgws:identity::43979298178977966408:root"][SBAI(
CSTR):"43979298178977966408"][SBAC(CSTR):"s3-account-
a"]\[S3BK\(CSTR\):"bucket-
anonymous"\]\[S3KY\(CSTR\):"Hello.txt"\][CBID(UI64):0x83D70C6F1F662B02][CS
IZ(UI64):12][AVER(UI32):10][ATIM(UI64):1505947988782605]\[ATYP\(FC32\):SGE
T\][ANID(UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):17742374343649889669]
]
```

バケット ポリシーで許可されている場合、クライアントは匿名でオブジェクトを取得したり、別のテナント アカウントが所有するバケットからオブジェクトを取得したりできます。監査メッセージにはバケット所有者のテナント アカウントに関する情報が含まれているため、これらの匿名リクエストやアカウント間リクエストを追跡できます。

次のサンプル メッセージでは、クライアントは、自分が所有していないバケットに保存されているオブジェクトに対して GetObject リクエストを送信します。 SBAI および SBAC の値には、バケット所有者のテナン

ト アカウント ID と名前が記録されます。これは、S3AI および SACC に記録されるクライアントのテナント アカウント ID と名前とは異なります。

```
2017-09-20T22:53:15.876415
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):53244][SAIP(IPAD):"10.96.112.26"]\[S3AI
\(CSTR\):"17915054115450519830"\]\[SACC\(CSTR\):"s3-account-
b"\][S3AK(CSTR):"SGKHpoblWlP_kBkqSCbTi754Ls8lBUog67I2LlSiUg=="][SUSR(CSTR)
:"urn:sgws:identity::17915054115450519830:root"]\[SBAI\(CSTR\):"4397929817
8977966408"\]\[SBAC\(CSTR\):"s3-account-a"\][S3BK(CSTR):"bucket-
anonymous"][S3KY(CSTR):"Hello.txt"][CBID(UI64):0x83D70C6F1F662B02][CSIZ(UI
64):12][AVER(UI32):10][ATIM(UI64):1505947995876415][ATYP(FC32):SGET][ANID(
UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):6888780247515624902]]
```

例: オブジェクトに対する**S3 Select**

S3 クライアントがオブジェクトに対して S3 Select クエリを発行すると、監査メッセージが生成され、監査ログに保存されます。

以下の例には、トランザクション中に生成されるすべての監査メッセージがリストされているわけではないことに注意してください。 S3 Select トランザクション (SelectObjectContent) に関連するものだけがリストされます。

各クエリの結果、2 つの監査メッセージが生成されます。1 つは S3 Select リクエストの承認を実行するメッセージ (S3SR フィールドは「select」に設定されます)、もう 1 つは処理中にストレージからデータを取得する後続の標準 GET 操作です。

```
2021-11-08T15:35:30.750038
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636385730715700][TIME(UI64):29173][SAI
P(IPAD):"192.168.7.44"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Ten
ant1636027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:id
entity::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBA
C(CSTR):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"][S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):0][S3SR(CSTR):"select"][AVER(UI32):10][ATIM(UI64
):1636385730750038][ATYP(FC32):SPOS][ANID(UI32):12601166][AMID(FC32):S3RQ]
[ATID(UI64):1363009709396895985]]
```

```
2021-11-08T15:35:32.604886
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636383069486504][TIME(UI64):430690][SA
IP(IPAD):"192.168.7.44"][HTRH(CSTR):"{\"x-forwarded-
for\":\"unix:\"}"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Tenant16
36027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:identit
y::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBAC(CST
R):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"][S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):10185581][MTME(UI64):1636380348695262][AVER(UI32
):10][ATIM(UI64):1636385732604886][ATYP(FC32):SGET][ANID(UI32):12733063][A
MID(FC32):S3RQ][ATID(UI64):16562288121152341130]]
```

メタデータ更新メッセージ

監査メッセージは、S3 クライアントがオブジェクトのメタデータを更新したときに生成されます。

S3 メタデータ更新監査メッセージ

コード	Name	説明	トレース	詳細については、
SUPD	S3 メタデータが更新されました	S3 クライアントが取り込んだオブジェクトのメタデータを更新したときに生成されます。	CBID、S3KY、HTRH	"SUPD: S3 メタデータが更新されました"

例: **S3** メタデータの更新

この例では、既存の S3 オブジェクトのメタデータを更新する成功したトランザクションを示します。

SUPD: S3 メタデータの更新

S3クライアントは指定されたメタデータを更新するリクエスト（SUPD）を発行します。(`x-amz-meta-\*`) を S3 オブジェクト (S3KY) 用に作成します。この例では、監査プロトコル ヘッダーとして構成されているため (構成 > 監視 > 監査および **syslog** サーバー)、要求ヘッダーは HTRH フィールドに含まれています。見る"監査メッセージとログの保存先を構成する" 。

```
2017-07-11T21:54:03.157462
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):17631][SAIP(IPAD):"10.96.100.254"]
[HTRH(CSTR):"{\"accept-encoding\":\"identity\",\"authorization\":\"AWS
LIUF17FGJARQHPY2E761:jul/hnZs/uNY+aVvV0lTSYhEGts=\",
\"content-length\":\"0\",\"date\":\"Tue, 11 Jul 2017 21:54:03
GMT\",\"host\":\"10.96.99.163:18082\",
\"user-agent\":\"aws-cli/1.9.20 Python/2.7.6 Linux/3.13.0-119-generic
botocore/1.3.20\",
\"x-amz-copy-source\":\"/testbkt1/testobj1\",\"x-amz-metadata-
directive\":\"REPLACE\",\"x-amz-meta-city\":\"Vancouver\"}"]
[S3AI(CSTR):"20956855414285633225"][SACC(CSTR):"acct1"][S3AK(CSTR):"SGKHyy
v9ZQqWRbJSQc5vI7mgioJwrdplShE02AUaww=="]
[SUSR(CSTR):"urn:sgws:identity::20956855414285633225:root"]
[SBAI(CSTR):"20956855414285633225"][SBAC(CSTR):"acct1"][S3BK(CSTR):"testbk
t1"]
[S3KY(CSTR):"testobj1"][CBID(UI64):0xCB1D5C213434DD48][CSIZ(UI64):10][AVER
(UI32):10]
[ATIM(UI64):1499810043157462][ATYP(FC32):SUPD][ANID(UI32):12258396][AMID(F
C32):S3RQ]
[ATID(UI64):8987436599021955788]]
```

監査メッセージ

監査メッセージの説明

システムによって返される監査メッセージの詳細な説明は、次のセクションに記載されています。各監査メッセージは、まず、メッセージが表すアクティビティのクラス別に関連するメッセージをグループ化したテーブルにリストされます。これらのグループ化は、監査されるアクティビティの種類を理解する場合と、必要な監査メッセージ フィルタリングの種類を選択する場合の両方に役立ちます。

監査メッセージも 4 文字のコードごとにアルファベット順にリストされます。このアルファベット順のリストを使用すると、特定のメッセージに関する情報を見つけることができます。

この章全体で使用される 4 文字のコードは、次の例メッセージに示すように、監査メッセージで見つかった ATYP 値です。

```
2014-07-17T03:50:47.484627
\[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP\
(FC32\):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265
00603516]]
```

監査メッセージのレベルの設定、ログの保存先の変更、監査情報用の外部Syslogサーバーの使用については、以下を参照してください。"監査メッセージとログの保存先を構成する"

システム監査メッセージ

システム監査カテゴリに属する監査メッセージは、監査システム自体、グリッド ノードの状態、システム全体のタスク アクティビティ (グリッド タスク)、およびサービス バックアップ操作に関連するイベントに使用されます。

コード	メッセージのタイトルと説明	詳細については、
ECMC	消失コード化データ フラグメントの欠落: 消失コード化データ フラグメントの欠落が検出されたことを示します。	"ECMC: 消失符号化データフラグメントの欠落"
ECOC	破損した消去符号化データ フラグメント: 破損した消去符号化データ フラグメントが検出されたことを示します。	"ECOC: 破損した消去符号化データフラグメント"
ETAF	セキュリティ認証に失敗しました: トランスポート層セキュリティ (TLS) を使用した接続試行が失敗しました。	"ETAF: セキュリティ認証に失敗しました"
GNRG	GNDS 登録: サービスがStorageGRIDシステム内で自身の情報を更新または登録しました。	"GNRG: GNDS登録"
グヌール	GNDS 登録解除: サービスがStorageGRIDシステムから登録解除されました。	"GNUR: GNDS 登録解除"
GTED	グリッド タスクが終了しました: CMN サービスはグリッド タスクの処理を終了しました。	"GTED: グリッドタスクが終了しました"
GTST	グリッド タスクが開始されました: CMN サービスがグリッド タスクの処理を開始しました。	"GTST: グリッドタスクが開始されました"
GTSU	グリッド タスクが送信されました: グリッド タスクが CMN サービスに送信されました。	"GTSU: グリッドタスクが送信されました"
LLST	場所の紛失: この監査メッセージは、場所が失われたときに生成されます。	"LLST: 位置情報が失われました"
オルスト	オブジェクトの損失: 要求されたオブジェクトがStorageGRIDシステム内に見つかりません。	"OLST: システムが紛失物体を検出しました"
サッド	セキュリティ監査の無効化: 監査メッセージのログ記録がオフになりました。	"SADD: セキュリティ監査の無効化"

コード	メッセージのタイトルと説明	詳細については、
サデ	セキュリティ監査の有効化: 監査メッセージのログ記録が復元されました。	"SADE: セキュリティ監査の有効化"
SVRF	オブジェクト ストア検証失敗: コンテンツ ブロックが検証チェックに失敗しました。	"SVRF: オブジェクトストア検証失敗"
SVRU	オブジェクト ストアの検証が不明です: オブジェクトストアで予期しないオブジェクト データが検出されました。	"SVRU: オブジェクトストアの検証が不明です"
システム	ノード停止: シャットダウンが要求されました。	"SYSD: ノード停止"
システム	ノードの停止: サービスが正常な停止を開始しました。	"SYST: ノード停止"
シス	ノードの開始: サービスが開始されました。前回のシャットダウンの性質がメッセージに示されます。	"SYSU: ノード開始"

オブジェクトストレージ監査メッセージ

オブジェクト ストレージ監査カテゴリに属する監査メッセージは、 StorageGRIDシステム内のオブジェクトの保存と管理に関連するイベントに使用されます。これらには、オブジェクトの保存と取得、グリッド ノード間の転送、検証が含まれます。

機能が廃止されると、監査コードは製品およびドキュメントから削除されます。ここに記載されていない監査コードが発生した場合は、このトピックの以前のバージョンで古い SG リリースを確認してください。例： "StorageGRID 11.8 オブジェクトストレージ監査メッセージ" 。

コード	説明	詳細については、
ブロル	バケット読み取り専用要求: バケットが読み取り専用モードになったか、読み取り専用モードを終了しました。	"BROR: バケット読み取り専用リクエスト"
CBSE	オブジェクト送信終了: ソース エンティティがグリッド ノード間のデータ転送操作を完了しました。	"CBSE: オブジェクト送信終了"
CBRE	オブジェクト受信終了: 宛先エンティティがグリッド ノード間のデータ転送操作を完了しました。	"CBRE: オブジェクト受信終了"
CGRR	クロスグリッド レプリケーション要求: StorageGRIDは、グリッド フェデレーション接続内のバケット間でオブジェクトを複製するために、クロスグリッド レプリケーション操作を試行しました。	"CGRR: クロスグリッド レプリケーション要求"

コード	説明	詳細については、
EBDL	空のバケットの削除: ILM スキャナーは、すべてのオブジェクトを削除するバケット内のオブジェクトを削除しました (空のバケット操作を実行しています)。	"EBDL: 空のバケットの削除"
EBKR	空のバケットのリクエスト: ユーザーが空のバケットをオンまたはオフにするリクエスト (つまり、バケット オブジェクトを削除するか、オブジェクトの削除を停止するリクエスト) を送信しました。	"EBKR: 空のバケットリクエスト"
SCMT	オブジェクト ストア コミット: コンテンツ ブロックが完全に保存され、検証されたため、要求できるようになりました。	"SCMT: オブジェクトストアコミット要求"
SREM	オブジェクト ストアの削除: コンテンツ ブロックがグリッド ノードから削除されたため、直接要求できなくなりました。	"SREM: オブジェクトストアの削除"

クライアント読み取り監査メッセージ

S3 クライアント アプリケーションがオブジェクトの取得を要求すると、クライアント読み取り監査メッセージが記録されます。

コード	説明	使用者	詳細については、
S3SL	S3 Select リクエスト: S3 Select リクエストがクライアントに返された後の完了をログに記録します。S3SL メッセージには、エラー メッセージとエラー コードの詳細が含まれる場合があります。リクエストが成功しなかった可能性があります。	S3クライアント	"S3SL: S3 選択リクエスト"
SGET	S3 GET: オブジェクトを取得したり、バケット内のオブジェクトを一覧表示したりするための成功したトランザクションをログに記録します。 注: トランザクションがサブリソースに対して実行される場合、監査メッセージにはフィールド S3SR が含まれます。	S3クライアント	"SGET: S3 ゲット"
シア	S3 HEAD: オブジェクトまたはバケットの存在を確認するために成功したトランザクションをログに記録します。	S3クライアント	"シア：S3ヘッド"
WGET	Swift GET: オブジェクトを取得したり、コンテナー内のオブジェクトを一覧表示したりするための成功したトランザクションをログに記録します。	Swiftクライアント	"WGET: Swift GET"

コード	説明	使用者	詳細については、
ウィー	Swift HEAD: オブジェクトまたはコンテナの存在を確認するために成功したトランザクションをログに記録します。	Swiftクライアント	"WHEA: Swift HEAD"

クライアント書き込み監査メッセージ

S3 クライアント アプリケーションがオブジェクトの作成または変更を要求すると、クライアント書き込み監査メッセージが記録されます。

コード	説明	使用者	詳細については、
オーバーブレーカー	オブジェクトの上書き: あるオブジェクトを別のオブジェクトで上書きするトランザクションを記録します。	S3 および Swift クライアント	"OVWR: オブジェクトの上書き"
SDEL	S3 DELETE: オブジェクトまたはバケットを削除する成功したトランザクションをログに記録します。 注: トランザクションがサブリソースに対して実行される場合、監査メッセージにはフィールド S3SR が含まれます。	S3クライアント	"SDEL: S3 削除"
スポス	S3 POST: AWS Glacier ストレージからクラウド ストレージ プールにオブジェクトを復元する成功したトランザクションをログに記録します。	S3クライアント	"SPOS: S3 ポスト"
吐き出す	S3 PUT: 新しいオブジェクトまたはバケットを作成するための成功したトランザクションをログに記録します。 注: トランザクションがサブリソースに対して実行される場合、監査メッセージにはフィールド S3SR が含まれます。	S3クライアント	"スプット: S3 プット"
SUPD	S3 メタデータの更新: 既存のオブジェクトまたはバケットのメタデータを更新する成功したトランザクションをログに記録します。	S3クライアント	"SUPD: S3 メタデータが更新されました"
WDEL	Swift DELETE: オブジェクトまたはコンテナを削除する成功したトランザクションをログに記録します。	Swiftクライアント	"WDEL: 迅速な削除"
WPUT	Swift PUT: 新しいオブジェクトまたはコンテナーを作成するための成功したトランザクションをログに記録します。	Swiftクライアント	"WPUT: Swift PUT"

管理カテゴリは、管理 API へのユーザー リクエストを記録します。

コード	メッセージのタイトルと説明	詳細については、
MGAU	管理 API 監査メッセージ: ユーザー リクエストのログ。	"MGAU: 経営監査メッセージ"

ILM監査メッセージ

ILM 監査カテゴリに属する監査メッセージは、情報ライフサイクル管理 (ILM) 操作に関連するイベントに使用されます。

コード	メッセージのタイトルと説明	詳細については、
アイデル	ILM による削除の開始: この監査メッセージは、ILM がオブジェクトの削除プロセスを開始したときに生成されます。	"IDEL: ILM による削除開始"
LKCU	上書きされたオブジェクトのクリーンアップ。この監査メッセージは、上書きされたオブジェクトが自動的に削除され、ストレージ領域が解放されたときに生成されます。	"LKCU: 上書きされたオブジェクトのクリーンアップ"
オーム	オブジェクト ルールが満たされました: この監査メッセージは、オブジェクト データが ILM ルールで指定されたとおりに保存されたときに生成されます。	"ORLM: オブジェクトルールが満たされました"

監査メッセージの参照

BROR: バケット読み取り専用リクエスト

LDR サービスは、バケットが読み取り専用モードになったとき、または読み取り専用モードを終了したときに、この監査メッセージを生成します。たとえば、すべてのオブジェクトが削除されている間、バケットは読み取り専用モードになります。

コード	フィールド	説明
BKHD	バケットUUID	バケット ID。
ブロブ	バケット読み取り専用リクエスト値	バケットが読み取り専用になるか、読み取り専用状態から抜けるか (1 = 読み取り専用、0 = 読み取り専用ではない)。
ブラザーズ	バケット読み取り専用の理由	バケットが読み取り専用にされる理由、または読み取り専用状態が解除される理由。たとえば、emptyBucket。

コード	フィールド	説明
S3AI	S3テナントアカウントID	リクエストを送信したテナント アカウントの ID。空の値は匿名アクセスを示します。
S3BK	S3バケット	S3 バケット名。

CBRB: オブジェクト受信開始

通常のシステム操作中は、データがアクセスされ、複製され、保持されるにつれて、コンテンツ ブロックは異なるノード間で継続的に転送されます。あるノードから別のノードへのコンテンツ ブロックの転送が開始されると、このメッセージは宛先エンティティによって発行されます。

コード	フィールド	説明
CNID	接続識別子	ノード間セッション/接続の一意の識別子。
CBID	コンテンツブロック識別子	転送されるコンテンツ ブロックの一意の識別子。
CTDR	転送方向	CBID 転送がプッシュ開始かプル開始かを示します。 PUSH: 送信エンティティによって転送操作が要求されました。 PULL: 転送操作は受信側エンティティによって要求されました。
CTSR	ソースエンティティ	CBID 転送のソース (送信者) のノード ID。
CTDS	宛先エンティティ	CBID 転送の宛先 (受信側) のノード ID。
CTSS	開始シーケンス数	要求された最初のシーケンス数を示します。成功した場合、転送はこのシーケンス カウントから開始されます。
CTES	予想される終了シーケンス数	要求された最後のシーケンス数を示します。成功した場合、このシーケンス カウントが受信された時点で転送が完了したとみなされます。
RSLT	転送開始ステータス	転送開始時のステータス: SUCS: 転送が正常に開始されました。

この監査メッセージは、コンテンツ ブロック識別子によって識別される単一のコンテンツに対してノード間データ転送操作が開始されたことを意味します。この操作では、「開始シーケンス カウント」から「予想される終了シーケンス カウント」までのデータが要求されます。送信ノードと受信ノードはノード ID によって識別されます。この情報は、システム データ フローを追跡するために使用でき、ストレージ監査メッセージ

と組み合わせてレプリカ数を確認するために使用できます。

CBRE: オブジェクト受信終了

あるノードから別のノードへのコンテンツ ブロックの転送が完了すると、宛先エンティティによってこのメッセージが発行されます。

コード	フィールド	説明
CNID	接続識別子	ノード間セッション/接続の一意の識別子。
CBID	コンテンツブロック識別子	転送されるコンテンツ ブロックの一意の識別子。
CTDR	転送方向	CBID 転送がプッシュ開始かプル開始かを示します。 PUSH: 送信エンティティによって転送操作が要求されました。 PULL: 転送操作は受信側エンティティによって要求されました。
CTSR	ソースエンティティ	CBID 転送のソース (送信者) のノード ID。
CTDS	宛先エンティティ	CBID 転送の宛先 (受信側) のノード ID。
CTSS	開始シーケンス数	転送が開始されたシーケンス数を示します。
CTAS	実際の終了シーケンス数	正常に転送された最後のシーケンス数を示します。実際の終了シーケンス数が開始シーケンス数と同じで、転送結果が成功しなかった場合、データは交換されませんでした。
RSLT	転送結果	転送操作の結果（送信エンティティの観点から）: SUCS: 転送が正常に完了しました。要求されたすべてのシーケンス カウントが送信されました。 CONL: 転送中に接続が失われました CTMO: 確立または転送中に接続がタイムアウトしました UNRE: 宛先ノードIDに到達できません CRPT: 破損または無効なデータを受信したため転送が終了しました

この監査メッセージは、ノード間のデータ転送操作が完了したことを意味します。転送結果が成功した場合、操作によって「開始シーケンス カウント」から「実際の終了シーケンス カウント」にデータが転送されました。送信ノードと受信ノードはノード ID によって識別されます。この情報を使用して、システムのデータ フ

ローを追跡し、エラーを特定、表にまとめ、分析することができます。ストレージ監査メッセージと組み合わせると、レプリカ数の検証にも使用できます。

CBSB: オブジェクト送信開始

通常のシステム操作中は、データがアクセスされ、複製され、保持されるにつれて、コンテンツ ブロックは異なるノード間で継続的に転送されます。あるノードから別のノードへのコンテンツ ブロックの転送が開始されると、ソース エンティティによってこのメッセージが発行されます。

コード	フィールド	説明
CNID	接続識別子	ノード間セッション/接続の一意の識別子。
CBID	コンテンツブロック識別子	転送されるコンテンツ ブロックの一意の識別子。
CTDR	転送方向	CBID 転送がプッシュ開始かプル開始かを示します。 PUSH: 送信エンティティによって転送操作が要求されました。 PULL: 転送操作は受信側エンティティによって要求されました。
CTSR	ソースエンティティ	CBID 転送のソース (送信者) のノード ID。
CTDS	宛先エンティティ	CBID 転送の宛先 (受信側) のノード ID。
CTSS	開始シーケンス数	要求された最初のシーケンス数を示します。成功した場合、転送はこのシーケンス カウントから開始されます。
CTES	予想される終了シーケンス数	要求された最後のシーケンス数を示します。成功した場合、このシーケンス カウントが受信された時点で転送が完了したとみなされます。
RSLT	転送開始ステータス	転送開始時のステータス: SUCS: 転送が正常に開始されました。

この監査メッセージは、コンテンツ ブロック識別子によって識別される単一のコンテンツに対してノード間データ転送操作が開始されたことを意味します。この操作では、「開始シーケンス カウント」から「予想される終了シーケンス カウント」までのデータが要求されます。送信ノードと受信ノードはノード ID によって識別されます。この情報は、システム データ フローを追跡するために使用でき、ストレージ監査メッセージと組み合わせてレプリカ数を確認するために使用できます。

CBSE: オブジェクト送信終了

あるノードから別のノードへのコンテンツ ブロックの転送が完了すると、ソース エンテ

ィティによってこのメッセージが発行されます。

コード	フィールド	説明
CNID	接続識別子	ノード間セッション/接続の一意の識別子。
CBID	コンテンツブロック識別子	転送されるコンテンツ ブロックの一意の識別子。
CTDR	転送方向	CBID 転送がプッシュ開始かプル開始かを示します。 PUSH: 送信エンティティによって転送操作が要求されました。 PULL: 転送操作は受信側エンティティによって要求されました。
CTSR	ソースエンティティ	CBID 転送のソース (送信者) のノード ID。
CTDS	宛先エンティティ	CBID 転送の宛先 (受信側) のノード ID。
CTSS	開始シーケンス数	転送が開始されたシーケンス数を示します。
CTAS	実際の終了シーケンス数	正常に転送された最後のシーケンス数を示します。実際の終了シーケンス数が開始シーケンス数と同じで、転送結果が成功しなかった場合、データは交換されませんでした。
RSLT	転送結果	転送操作の結果（送信エンティティの観点から）: SUCS: 転送が正常に完了しました。要求されたシーケンス カウントがすべて送信されました。 CONL: 転送中に接続が失われました CTMO: 確立または転送中に接続がタイムアウトしました UNRE: 宛先ノードIDに到達できません CRPT: 破損または無効なデータを受信したため転送が終了しました

この監査メッセージは、ノード間のデータ転送操作が完了したことを意味します。転送結果が成功した場合、操作によって「開始シーケンス カウント」から「実際の終了シーケンス カウント」にデータが転送されました。送信ノードと受信ノードはノード ID によって識別されます。この情報を使用して、システムのデータ フローを追跡し、エラーを特定、表にまとめ、分析することができます。ストレージ監査メッセージと組み合わせると、レプリカ数の検証にも使用できます。

CGRR: クロスグリッドレプリケーション要求

このメッセージは、 StorageGRID がグリッド フェデレーション接続内のバケット間でオブジェクトを複製するクロス グリッド レプリケーション操作を試行したときに生成されます。

コード	フィールド	説明
CSIZ	オブジェクトサイズ	オブジェクトのサイズ（バイト）。 CSIZ 属性はStorageGRID 11.8 で導入されました。その結果、StorageGRID 11.7 から 11.8 へのアップグレードにまたがるクロスグリッド レプリケーション要求では、オブジェクトの合計サイズが不正確になる可能性があります。
S3AI	S3テナントアカウントID	オブジェクトの複製元となるバケットを所有するテナント アカウントの ID。
GFID	グリッドフェデレーション接続ID	クロスグリッドレプリケーションに使用されているグリッドフェデレーション接続の ID。
オペラ	CGR操作	試行されたクロスグリッド レプリケーション操作のタイプ: • 0 = オブジェクトを複製する • 1 = マルチパートオブジェクトを複製する • 2 = 削除マーカーを複製する
S3BK	S3バケット	S3 バケット名。
S3KY	S3キー	バケット名を含まない S3 キー名。
VSID	バージョン ID	複製されていたオブジェクトの特定のバージョンのバージョン ID。
RSLT	結果コード	成功 (SUCS) または一般エラー (GERR) を返します。

EBDL: 空のバケットの削除

ILM スキャナーは、すべてのオブジェクトを削除するバケット内のオブジェクトを削除しました (空のバケット操作を実行しています)。

コード	フィールド	説明
CSIZ	オブジェクトサイズ	オブジェクトのサイズ（バイト）。

コード	フィールド	説明
パス	S3 バケット/キー	S3 バケット名と S3 キー名。
SEGC	コンテナUUID	セグメント化されたオブジェクトのコンテナの UUID。この値は、オブジェクトがセグメント化されている場合にのみ使用できます。
UUID	ユニバーサルユニーク識別子	StorageGRIDシステム内のオブジェクトの識別子。
RSLT	削除操作の結果	イベント、プロセス、またはトランザクションの結果。メッセージに関連しない場合は、メッセージが誤ってフィルタリングされないように、SUCS ではなく NONE が使用されます。

EBKR: 空のバケットリクエスト

このメッセージは、ユーザーが空のバケットをオンまたはオフにする（つまり、バケット オブジェクトを削除するか、オブジェクトの削除を停止する）要求を送信したことを示します。

コード	フィールド	説明
ビルド	バケットUUID	バケット ID。
EBJS	空のバケットのJSON構成	現在の空のバケット構成を表す JSON が含まれます。
S3AI	S3テナントアカウントID	リクエストを送信したユーザーのテナント アカウント ID。空の値は匿名アクセスを示します。
S3BK	S3 バケット	S3 バケット名。

ECMC: 消失符号化データフラグメントの欠落

この監査メッセージは、システムが消失訂正符号化データ フラグメントの欠落を検出したことを示します。

コード	フィールド	説明
VCMC	VCS ID	不足しているチャンクを含む VCS の名前。
MCID	チャンクID	欠落した消去コード化フラグメントの識別子。

コード	フィールド	説明
RSLT	結果	このフィールドの値は「NONE」です。 RSLT は必須のメッセージ フィールドですが、この特定のメッセージには関係ありません。このメッセージはフィルタリングされないように、「SUCS」ではなく「NONE」が使用されます。

ECOC: 破損した消去符号化データフラグメント

この監査メッセージは、システムが破損した消去符号化データ フラグメントを検出したことを示します。

コード	フィールド	説明
VCCO	VCS ID	破損したチャンクを含む VCS の名前。
VLID	ボリューム ID	破損した消去コード化フラグメントを含む RangeDB ボリューム。
CCID	チャンクID	破損した消去コード化フラグメントの識別子。
RSLT	結果	このフィールドの値は「NONE」です。 RSLT は必須のメッセージ フィールドですが、この特定のメッセージには関係ありません。このメッセージはフィルタリングされないように、「SUCS」ではなく「NONE」が使用されます。

ETAF: セキュリティ認証に失敗しました

このメッセージは、トランスポート層セキュリティ (TLS) を使用した接続試行が失敗したときに生成されます。

コード	フィールド	説明
CNID	接続識別子	認証が失敗した TCP/IP 接続の一意のシステム識別子。
ルイド	ユーザーID	リモート ユーザーの ID を表すサービス依存の識別子。

コード	フィールド	説明
RSLT	理由コード	失敗の理由： SCNI: 安全な接続の確立に失敗しました。 CERM: 証明書が見つかりません。 CERT: 証明書が無効でした。 CERE: 証明書の有効期限が切れています。 CERR: 証明書は取り消されました。 CSGN: 証明書の署名が無効です。 CSGU: 証明書の署名者が不明です。 UCRM: ユーザー資格情報が見つかりません。 UCRI: ユーザー資格情報が無効です。 UCRU: ユーザー資格情報が許可されませんでした。 TOUT: 認証がタイムアウトしました。

TLS を使用する安全なサービスへの接続が確立されると、TLS プロファイルとサービスに組み込まれた追加ロジックを使用して、リモート エンティティの資格情報が検証されます。無効、予期しない、または許可されていない証明書または資格情報のためにこの認証が失敗した場合、監査メッセージが記録されます。これにより、不正なアクセスの試みやその他のセキュリティ関連の接続の問題を照会できるようになります。

このメッセージは、リモート エンティティの構成が誤っているか、無効または許可されていない資格情報をシステムに提示しようとしたことが原因で発生する可能性があります。システムへの不正アクセスの試みを検出するには、この監査メッセージを監視する必要があります。

GNRG: GNDS登録

CMN サービスは、サービスがStorageGRIDシステム内で自身の情報を更新または登録したときに、この監査メッセージを生成します。

コード	フィールド	説明
RSLT	結果	更新リクエストの結果: • SUCS: 成功 • SUNV: サービスは利用できません • GERR: その他の障害
GNID	ノードID	更新要求を開始したサービスのノード ID。

コード	フィールド	説明
GNTP	デバイスタイプ	グリッド ノードのデバイス タイプ (たとえば、LDR サービスの場合は BLDR)。
GNDV	デバイスモデル バージョン	DMDL バンドル内のグリッド ノードのデバイス モデル バージョンを識別する文字列。
GNGP	グループ	グリッド ノードが属するグループ (リンク コストとサービス クエリのランキングのコンテキスト)。
グニア	IP アドレス	グリッド ノードの IP アドレス。

このメッセージは、グリッド ノードがグリッド ノード バンドル内のエントリを更新するたびに生成されます。

GNUR: GNDS 登録解除

CMN サービスは、サービスがStorageGRIDシステムから自身に関する情報を登録解除したときに、この監査メッセージを生成します。

コード	フィールド	説明
RSLT	結果	更新リクエストの結果: • SUCS: 成功 • SUNV: サービスは利用できません • GERR: その他の障害
GNID	ノードID	更新要求を開始したサービスのノード ID。

GTED: グリッドタスクが終了しました

この監査メッセージは、CMN サービスが指定されたグリッド タスクの処理を完了し、タスクを履歴テーブルに移動したことを示します。結果が SUCS、ABRT、または ROLF の場合、対応するグリッド タスク開始監査メッセージが表示されます。その他の結果は、このグリッド タスクの処理が開始されなかったことを示しています。

コード	フィールド	説明
TSID	タスクID	このフィールドは、生成されたグリッド タスクを一意に識別し、グリッド タスクをそのライフサイクルにわたって管理できるようにします。 注: タスク ID は、グリッド タスクが送信されたときではなく、生成されたときに割り当てられます。特定のグリッド タスクが複数回送信される可能性がありますが、この場合、タスク ID フィールドでは、送信済み、開始済み、および終了済みの監査メッセージを一意にリンクするには不十分です。
RSLT	結果	グリッド タスクの最終ステータス結果: • SUCS: グリッド タスクは正常に完了しました。 • ABRT: グリッド タスクはロールバック エラーなしで終了しました。 • ROLF: グリッド タスクが終了し、ロールバック プロセスを完了できませんでした。 • CANC: グリッド タスクは、開始される前にユーザーによってキャンセルされました。 • EXPR: グリッド タスクは開始される前に期限が切れました。 • IVLD: グリッド タスクが無効でした。 • AUTH: グリッド タスクは許可されていません。 • DUPL: グリッド タスクは重複として拒否されました。

GTST: グリッドタスクが開始されました

この監査メッセージは、CMN サービスが指定されたグリッド タスクの処理を開始したことを示します。監査メッセージは、内部グリッド タスク送信サービスによって開始され、自動アクティブ化が選択されたグリッド タスクのグリッド タスク送信メッセージの直後に表示されます。保留テーブルに送信されたグリッド タスクの場合、ユーザーがグリッド タスクを開始したときにこのメッセージが生成されます。

コード	フィールド	説明
TSID	タスクID	このフィールドは、生成されたグリッド タスクを一意に識別し、タスクをそのライフサイクル全体にわたって管理できるようにします。 注: タスク ID は、グリッド タスクが送信されたときではなく、生成されたときに割り当てられます。特定のグリッド タスクが複数回送信される可能性がありますが、この場合、タスク ID フィールドでは、送信済み、開始済み、および終了済みの監査メッセージを一意にリンクするには不十分です。

コード	フィールド	説明
RSLT	結果	結果。このフィールドには 1 つの値のみが含まれます。 • SUCS: グリッド タスクが正常に開始されました。

GTSU: グリッドタスクが送信されました

この監査メッセージは、グリッド タスクが CMN サービスに送信されたことを示します。

コード	フィールド	説明
TSID	タスクID	生成されたグリッド タスクを一意に識別し、タスクをそのライフサイクルにわたって管理できるようにします。 注: タスク ID は、グリッド タスクが送信されたときではなく、生成されたときに割り当てられます。特定のグリッド タスクが複数回送信される可能性がありますが、この場合、タスク ID フィールドでは、送信済み、開始済み、および終了済みの監査メッセージを一意にリンクするには不十分です。
TTYP	タスクタイプ	グリッド タスクのタイプ。
TVER	タスクバージョン	グリッド タスクのバージョンを示す番号。
TDSC	Task Description	グリッド タスクの人間が読める形式の説明。
VATS	タイムスタンプの有効期限	グリッド タスクが有効になる最も早い時刻 (1970 年 1 月 1 日からの UINT64 マイクロ秒 - UNIX 時間)。
VBTS	有効期限前タイムスタンプ	グリッド タスクが有効な最終時刻 (1970 年 1 月 1 日からの UINT64 マイクロ秒 - UNIX 時間)。
TSRC	ソース	タスクのソース: • TXTB: グリッド タスクは、署名されたテキスト ブロックとしてStorageGRIDシステムを通じて送信されました。 • GRID: グリッド タスクは、内部のグリッド タスク送信サービスを通じて送信されました。

コード	フィールド	説明
ACTV	アクティベーションタイプ	アクティベーションの種類: • AUTO: グリッド タスクは自動アクティブ化のために送信されました。 • PEND: グリッド タスクが保留中のテーブルに送信されました。これは、TXTB ソースの唯一の可能性です。
RSLT	結果	提出の結果: • SUCS: グリッド タスクが正常に送信されました。 • 失敗: タスクは履歴テーブルに直接移動されました。

IDEL: ILM による削除開始

このメッセージは、ILM がオブジェクトの削除プロセスを開始したときに生成されます。

IDEL メッセージは、次のいずれかの状況で生成されます。

- 準拠 **S3** バケット内のオブジェクトの場合: このメッセージは、オブジェクトの保持期間が終了したために ILM がオブジェクトの自動削除プロセスを開始したときに生成されます (自動削除設定が有効になっていて、法的保留がオフになっていると想定)。
- 非準拠の **S3** バケット内のオブジェクトの場合。このメッセージは、アクティブな ILM ポリシー内の配置指示が現在オブジェクトに適用されていないため、ILM がオブジェクトの削除プロセスを開始したときに生成されます。

コード	フィールド	説明
CBID	コンテンツブロック識別子	オブジェクトの CBID。
CMPA	コンプライアンス: 自動削除	準拠した S3 バケット内のオブジェクトのみ対象です。 0 (false) または 1 (true)。バケットが法的保留中でない限り、準拠オブジェクトを保持期間の終了時に自動的に削除するかどうかを示します。
CMPL	コンプライアンス: 法的保留	準拠した S3 バケット内のオブジェクトのみ対象です。 0 (false) または 1 (true)。バケットが現在法的保留中かどうかを示します。
CMPR	コンプライアンス: 保存期間	準拠した S3 バケット内のオブジェクトのみ対象です。オブジェクトの保持期間の長さ（分）。
CTME	コンプライアンス: 取り込み時間	準拠した S3 バケット内のオブジェクトのみ対象です。オブジェクトの取り込み時間。この値に保持期間（分単位）を追加して、バケットからオブジェクトを削除できるタイミングを決定できます。

コード	フィールド	説明
DMRK	マーカーバージョンIDを削除	バージョン管理されたバケットからオブジェクトを削除するときに作成される削除マーカーのバージョン ID。バケットに対する操作にはこのフィールドは含まれません。
CSIZ	コンテンツサイズ	オブジェクトのサイズ（バイト）。
LOCS	場所	StorageGRIDシステム内のオブジェクト データの保存場所。オブジェクトに場所がない場合（たとえば、削除されている場合）、LOCS の値は "" になります。 CLEC: 消去コード化オブジェクトの場合、オブジェクトのデータに適用される消去コード化プロファイル ID と消去コード化グループ ID。 CLDI: 複製されたオブジェクトの場合、オブジェクトの場所の LDR ノード ID とボリューム ID。 CLNL: オブジェクト データがアーカイブされている場合のオブジェクトの場所の ARC ノード ID。
パス	S3 バケット/キー	S3 バケット名と S3 キー名。
RSLT	結果	ILM 操作の結果。 SUCS: ILM 操作は成功しました。
ルール	ルールラベル	• 準拠 S3 バケット内のオブジェクトが保持期間の期限切れにより自動的に削除されている場合、このフィールドは空白になります。 • 現在オブジェクトに適用されている配置指示がなくなったためにオブジェクトが削除されている場合、このフィールドには、オブジェクトに適用された最後の ILM ルールの判読可能なラベルが表示されます。
SGRP	サイト（グループ）	存在する場合、オブジェクトは指定されたサイトで削除されましたが、そのサイトはオブジェクトが取り込まれたサイトではありません。
UUID	ユニバーサルユニーク識別子	StorageGRIDシステム内のオブジェクトの識別子。
VSID	バージョン ID	削除されたオブジェクトの特定のバージョンのバージョン ID。バケットおよびバージョン管理されていないバケット内のオブジェクトに対する操作には、このフィールドは含まれません。

LKCU: 上書きされたオブジェクトのクリーンアップ

このメッセージは、ストレージ領域を解放するために以前にクリーンアップが必要だった上書きされたオブジェクトをStorageGRID が削除したときに生成されます。 S3 クライアントが、すでにオブジェクトが含まれているパスにオブジェクトを書き込むと、オブジェクトは上書きされます。削除プロセスは自動的にバックグラウンドで実行されます。

コード	フィールド	説明
CSIZ	コンテンツサイズ	オブジェクトのサイズ（バイト）。
LTYP	クリーンアップの種類	社内使用のみ。
ルイド	削除されたオブジェクトのUUID	削除されたオブジェクトの識別子。
パス	S3 バケット/キー	S3 バケット名と S3 キー名。
SEGC	コンテナUUID	セグメント化されたオブジェクトのコンテナの UUID。この値は、オブジェクトがセグメント化されている場合にのみ使用できます。
UUID	ユニバーサルユニーク識別子	まだ存在するオブジェクトの識別子。この値は、オブジェクトが削除されていない場合にのみ使用できます。

LKDM: リークされたオブジェクトのクリーンアップ

このメッセージは、リークされたチャンクがクリーンアップまたは削除されたときに生成されます。チャンクは、複製されたオブジェクトまたは消去エンコードされたオブジェクトの一部になることができます。

コード	フィールド	説明
クロック	チャンクの位置	削除されたリークされたチャンクのファイル パス。

CTYP	チャンクタイプ	チャンクの種類:
		
		`ec: Erasure-coded object chunk`
		
		`repl: Replicated object chunk`

コード	フィールド	説明

LTYP	リークタイプ	検出できる漏れの 5 つのタイプ:
		
		`object_leaked: Object doesn’t exist in the grid`
		
		`location_leaked: Object exists in the grid, but found location doesn’t belong to object`
		
		`mup_seg_leaked: Multipart upload was stopped or not completed, and the segment/part was left out`
		
		`segment_leaked: Parent UUID/CBID (associated container object) is valid but doesn’t contain this segment`
		
		`no_parent: Container object is deleted, but object segment was left out and not deleted`

CTIM	チャンク作成時間	リークされたチャンクが作成された時刻。
UUID	ユニバーサルユニーク識別子	チャンクが属するオブジェクトの識別子。
CBID	コンテンツブロック識別子	リークされたチャンクが属するオブジェクトの CBID。
CSIZ	コンテンツサイズ	チャンクのサイズ（バイト単位）。

LLST: 位置情報が失われました

このメッセージは、オブジェクト コピー (複製または消去コード化) の場所が見つからない場合に生成されます。

コード	フィールド	説明
CBIL	CBID	影響を受ける CBID。
ECPR	消失訂正符号化プロファイル	消失訂正符号化オブジェクトデータ用。使用される消去コーディング プロファイルの ID。
LTYP	場所の種類	CLDI（オンライン）：複製されたオブジェクトデータ用 CLEC（オンライン）：消失訂正符号化オブジェクトデータ用 CLNL（ニアライン）：アーカイブされた複製オブジェクトデータ用

コード	フィールド	説明
ノイド	ソースノードID	場所が失われたノード ID。
PCLD	複製されたオブジェクトへのパス	失われたオブジェクト データのディスクの場所への完全なパス。 LTYP の値が CLDI の場合 (つまり、複製されたオブジェクトの場合) のみ返されます。 形式は `/var/local/rangedb/2/p/13/13/00oJs6X%{h{U)SeUFxE@`
RSLT	結果	常になし。 RSLT は必須のメッセージ フィールドですが、このメッセージには関係ありません。このメッセージがフィルタリングされないように、SUCS ではなく NONE が使用されます。
TSRC	トリガーソース	ユーザー: ユーザーがトリガー SYST: システムが起動しました
UUID	ユニバーサルユニークID	StorageGRIDシステム内の影響を受けるオブジェクトの識別子。

MGAU: 経営監査メッセージ

管理カテゴリは、管理 API へのユーザー リクエストを記録します。有効な API URI への GET または HEAD リクエストではないすべての HTTP リクエストでは、ユーザー名、IP、および API へのリクエストの種類を含む応答がログに記録されます。無効な API URI (/api/v3-authorize など) および有効な API URI への無効なリクエストはログに記録されません。

コード	フィールド	説明
MDIP	宛先IPアドレス	サーバー（宛先）の IP アドレス。
遺伝子組み換えDNA	ドメイン名	ホストドメイン名。
MPAT	Request PATH	リクエストパス。
MPQP	リクエストクエリパラメータ	リクエストのクエリ パラメータ。

コード	フィールド	説明
MRBD	リクエスト本文	リクエスト本体の内容。デフォルトではレスポンス本文がログに記録されますが、レスポンス本文が空の場合、特定のケースではリクエスト本文がログに記録されます。次の情報はレスポンス本文では取得できないため、次の POST メソッドのリクエスト本文から取得されます。 • **POST authorize** のユーザー名とアカウント ID • **POST /grid/grid-networks/update** での新しいサブネット構成 • **POST /grid/ntp-servers/update** の新しい NTP サーバー • **POST /grid/servers/decommission** 内の廃止されたサーバー ID 注**:** 機密情報は削除されるか (S3 アクセス キーなど)、アスタリスクでマスクされます (パスワードなど)。
MRMD	リクエスト方法	HTTP リクエストメソッド: • POST • PUT • DELETE • PATCH
MRSC	応答コード	応答コード。
MRSP	応答の本文	応答の内容 (応答本体) はデフォルトでログに記録されます。 注**:** 機密情報は削除されるか (S3 アクセス キーなど)、アスタリスクでマスクされます (パスワードなど)。
MSIP	送信元IPアドレス	クライアント (送信元) IP アドレス。
ムーン	ユーザーURN	リクエストを送信したユーザーの URN (Uniform Resource Name)。
RSLT	結果	成功 (SUCS) またはバックエンドによって報告されたエラーを返します。

OLST: システムが紛失物体を検出しました

このメッセージは、DDS サービスがStorageGRIDシステム内でオブジェクトのコピーを見つけられない場合に生成されます。

コード	フィールド	説明
CBID	コンテンツブロック識別子	紛失したオブジェクトの CBID。

コード	フィールド	説明
ノイド	ノードID	入手可能な場合、紛失した物体の最後の既知の直接位置または近距離位置。ボリューム情報が利用できない場合は、ボリューム ID なしでノード ID のみを持つことが可能です。
パス	S3 バケット/キー	可能な場合は、S3 バケット名と S3 キー名。
RSLT	結果	このフィールドの値は NONE です。 RSLT は必須のメッセージ フィールドですが、このメッセージには関係ありません。このメッセージがフィルタリングされないように、SUCS ではなく NONE が使用されます。
UUID	ユニバーサルユニークID	StorageGRIDシステム内で失われたオブジェクトの識別子。
ヴォリ	ボリューム ID	利用可能な場合、失われたオブジェクトの最後の既知の場所のストレージ ノードのボリューム ID。

ORLM: オブジェクトルールが満たされました

このメッセージは、ILM ルールで指定されたとおりにオブジェクトが正常に保存およびコピーされたときに生成されます。

ポリシー内の別のルールがオブジェクト サイズの詳細フィルターを使用している場合、デフォルトの 2 つのコピーを作成するルールによってオブジェクトが正常に保存されても、ORLM メッセージは生成されません。

コード	フィールド	説明
ビルド	バケットヘッダー	バケット ID フィールド。内部操作に使用されます。 STAT が PRGD の場合にのみ表示されます。
CBID	コンテンツブロック識別子	オブジェクトの CBID。
CSIZ	コンテンツサイズ	オブジェクトのサイズ（バイト）。

コード	フィールド	説明
LOCS	場所	StorageGRIDシステム内のオブジェクト データの保存場所。オブジェクトに場所がない場合（たとえば、削除されている場合）、LOCS の値は "" になります。 CLEC: 消去コード化オブジェクトの場合、オブジェクトのデータに適用される消去コード化プロファイル ID と消去コード化グループ ID。 CLDI: 複製されたオブジェクトの場合、オブジェクトの場所の LDR ノード ID とボリューム ID。 CLNL: オブジェクト データがアーカイブされている場合のオブジェクトの場所の ARC ノード ID。
パス	S3 バケット/キー	S3 バケット名と S3 キー名。
RSLT	結果	ILM 操作の結果。 SUCS: ILM 操作は成功しました。
ルール	ルールラベル	このオブジェクトに適用された ILM ルールに与えられた、人間が判読できるラベル。
SEGC	コンテナUUID	セグメント化されたオブジェクトのコンテナの UUID。この値は、オブジェクトがセグメント化されている場合にのみ使用できます。
SGCB	コンテナCBID	セグメント化されたオブジェクトのコンテナの CBID。この値は、セグメント化されたオブジェクトとマルチパート オブジェクトに対してのみ使用できます。
統計	ステータス	ILM 操作のステータス。 完了: オブジェクトに対する ILM 操作が完了しました。 DFER: オブジェクトは将来の ILM 再評価の対象としてマークされています。 PRGD: オブジェクトはStorageGRIDシステムから削除されました。 NLOC: オブジェクト データがStorageGRIDシステム内に見つかりません。このステータスは、オブジェクト データのすべてのコピーが欠落しているか破損していることを示している可能性があります。
UUID	ユニバーサルユニーク識別子	StorageGRIDシステム内のオブジェクトの識別子。

コード	フィールド	説明
VSID	バージョン ID	バージョン管理されたバケットに作成された新しいオブジェクトのバージョン ID。バケットおよびバージョン管理されていないバケット内のオブジェクトに対する操作には、このフィールドは含まれません。

ORLM 監査メッセージは、単一のオブジェクトに対して複数回発行できます。たとえば、次のいずれかのイベントが発生するたびに発行されます。

- オブジェクトの ILM ルールは永久に満たされます。
- このエポックでは、オブジェクトの ILM ルールが満たされています。
- ILM ルールによってオブジェクトが削除されました。
- バックグラウンド検証プロセスにより、複製されたオブジェクト データのコピーが破損していることが検出されます。 StorageGRIDシステムは ILM 評価を実行して、破損したオブジェクトを置き換えます。

関連情報

- "オブジェクト取り込みトランザクション"
- "オブジェクト削除トランザクション"

OVWR: オブジェクトの上書き

このメッセージは、外部 (クライアントが要求した) 操作によって 1 つのオブジェクトが別のオブジェクトによって上書きされたときに生成されます。

コード	フィールド	説明
CBID	コンテンツブロック識別子（新規）	新しいオブジェクトの CBID。
CSIZ	前のオブジェクトのサイズ	上書きされるオブジェクトのサイズ（バイト単位）。
OCBD	コンテンツブロック識別子（前）	前のオブジェクトの CBID。
UUID	ユニバーサルユニークID（新規）	StorageGRIDシステム内の新しいオブジェクトの識別子。
OUID	ユニバーサルユニークID（前）	StorageGRIDシステム内の前のオブジェクトの識別子。
パス	S3 オブジェクトパス	以前のオブジェクトと新しいオブジェクトの両方に使用されるS3オブジェクトパス

コード	フィールド	説明
RSLT	結果コード	オブジェクト上書きトランザクションの結果。結果は常に次のようになります: SUCS: 成功
SGRP	サイト（グループ）	存在する場合、上書きされたオブジェクトは指定されたサイトで削除されましたが、そのサイトは上書きされたオブジェクトが取り込まれたサイトではありません。

S3SL: S3 選択リクエスト

このメッセージは、S3 Select リクエストがクライアントに返された後の完了を記録します。 S3SL メッセージには、エラー メッセージとエラー コードの詳細が含まれる場合があります。リクエストが成功しなかった可能性があります。

コード	フィールド	説明
BYSC	スキャンされたバイト数	ストレージ ノードからスキャン (受信) されたバイト数。 オブジェクトが圧縮されている場合、BYSC と BYPR は異なる可能性があります。オブジェクトが圧縮されている場合、BYSC には圧縮されたバイト数が含まれ、BYPR には解凍後のバイト数が含まれます。
BYPR	処理されたバイト数	処理されたバイト数。 S3 Select ジョブによって実際に処理または操作された「スキャンされたバイト数」を示します。
BYRT	返されたバイト数	S3 Select ジョブがクライアントに返したバイト数。
再広報	処理されたレコード	S3 Select ジョブがストレージノードから受信したレコードまたは行の数。
RERT	返されたレコード	S3 Select ジョブがクライアントに返したレコードまたは行の数。
ジョフィ	仕事完了	S3 Select ジョブの処理が完了したかどうかを示します。これが false の場合、ジョブは完了に失敗し、エラー フィールドにデータが含まれる可能性があります。クライアントは部分的な結果を受け取ったか、まったく結果を受け取った可能性があります。
リード	Request ID	S3 Select リクエストの識別子。
外務省	実行時間	S3 選択ジョブが完了するまでにかかった時間 (秒)。

コード	フィールド	説明
ERMG	エラー メッセージ	S3 Select ジョブによって生成されたエラー メッセージ。
エルティ	エラーの種類	S3 Select ジョブによって生成されたエラーの種類。
ERST	エラースタックトレース	S3 Select ジョブによって生成されたエラー スタック トレース。
S3BK	S3バケット	S3 バケット名。
S3AK	S3 アクセスキー ID (リクエスト送信者)	リクエストを送信したユーザーの S3 アクセスキー ID。
S3AI	S3テナントアカウントID（リクエスト送信者）	リクエストを送信したユーザーのテナント アカウント ID。
S3KY	S3キー	バケット名を含まない S3 キー名。

SADD: セキュリティ監査の無効化

このメッセージは、発信元サービス (ノード ID) が監査メッセージのログ記録をオフにしたことを示します。監査メッセージは収集も配信もされなくなりました。

コード	フィールド	説明
AETM	有効化メソッド	監査を無効にするために使用される方法。
アウン	ユーザー名	監査ログを無効にするコマンドを実行したユーザー名。
RSLT	結果	このフィールドの値は NONE です。 RSLT は必須のメッセージ フィールドですが、このメッセージには関係ありません。このメッセージがフィルタリングされないように、SUCS ではなく NONE が使用されます。

このメッセージは、以前はログ記録が有効だったが、現在は無効になっていることを示しています。これは通常、システム パフォーマンスを向上させるために一括取り込み時にのみ使用されます。一括アクティビティの後、監査が復元され (SADE)、監査を無効にする機能が永続的にブロックされます。

SADE: セキュリティ監査の有効化

このメッセージは、発信元サービス (ノード ID) が監査メッセージのログ記録を復元し、監査メッセージが再び収集および配信されていることを示します。

コード	フィールド	説明
AETM	有効化メソッド	監査を有効にするために使用される方法。
アウン	ユーザー名	監査ログを有効にするコマンドを実行したユーザー名。
RSLT	結果	このフィールドの値は NONE です。 RSLT は必須のメッセージ フィールドですが、このメッセージには関係ありません。このメッセージがフィルタリングされないように、SUCS ではなく NONE が使用されます。

このメッセージは、以前はログ記録が無効 (SADD) だったが、現在は復元されていることを示しています。これは通常、システム パフォーマンスを向上させるために一括取り込み時にのみ使用されます。一括アクティビティの後、監査が復元され、監査を無効にする機能が永続的にブロックされます。

SCMT: オブジェクトストアコミット

グリッド コンテンツは、コミットされるまで (つまり永続的に保存されるまで) 使用可能にならず、保存済みとして認識されません。永続的に保存されたコンテンツはディスクに完全に書き込まれ、関連する整合性チェックに合格しました。このメッセージは、コンテンツ ブロックがストレージにコミットされたときに発行されます。

コード	フィールド	説明
CBID	コンテンツブロック識別子	永続ストレージにコミットされたコンテンツ ブロックの一意の識別子。
RSLT	結果コード	オブジェクトがディスクに保存された時点のステータス: SUCS: オブジェクトは正常に保存されました。

このメッセージは、特定のコンテンツ ブロックが完全に保存され、検証され、要求できる状態になったことを意味します。システム内のデータフローを追跡するために使用できます。

SDEL: S3 削除

S3 クライアントが DELETE トランザクションを発行すると、指定されたオブジェクトまたはバケットを削除するか、バケット/オブジェクトのサブリソースを削除するように要求されます。トランザクションが成功した場合、このメッセージはサーバーによって発行されます。

コード	フィールド	説明
CBID	コンテンツブロック識別子	要求されたコンテンツ ブロックの一意の識別子。 CBID が不明な場合、このフィールドは 0 に設定されます。バケットに対する操作にはこのフィールドは含まれません。

コード	フィールド	説明
CNCH	一貫性制御ヘッダー	リクエスト内に存在する場合の Consistency-Control HTTP リクエストヘッダーの値。
CNID	接続識別子	TCP/IP 接続の一意のシステム識別子。
CSIZ	コンテンツサイズ	削除されたオブジェクトのサイズ（バイト単位）。バケットに対する操作にはこのフィールドは含まれません。
DMRK	マーカーバージョンIDを削除	バージョン管理されたバケットからオブジェクトを削除するときに作成される削除マーカーのバージョン ID。バケットに対する操作にはこのフィールドは含まれません。
GFID	グリッドフェデレーション接続ID	クロスグリッド レプリケーション削除要求に関連付けられたグリッドフェデレーション接続の接続 ID。宛先グリッドの監査ログにのみ含まれます。
GFSA	グリッドフェデレーションソースアカウントID	クロスグリッド レプリケーション削除リクエストのソース グリッド上のテナントのアカウント ID。宛先グリッドの監査ログにのみ含まれます。
HTRH	HTTPリクエストヘッダー	構成時に選択された、ログに記録された HTTP 要求ヘッダー名と値のリスト。 `X-Forwarded-For`リクエストに存在し、 `X-Forwarded-For`値が要求送信者の IP アドレス (SAIP 監査フィールド) と異なります。 `x-amz-bypass-governance-retention`リクエスト内に存在する場合は自動的に含まれます。
MTME	最終更新日時	オブジェクトが最後に変更された時刻を示す、マイクロ秒単位の Unix タイムスタンプ。
RSLT	結果コード	DELETE トランザクションの結果。結果は常に次のようになります: SUCS: 成功
S3AI	S3テナントアカウントID（リクエスト送信者）	リクエストを送信したユーザーのテナント アカウント ID。空の値は匿名アクセスを示します。
S3AK	S3 アクセスキー ID (リクエスト送信者)	リクエストを送信したユーザーのハッシュ化された S3 アクセスキー ID。空の値は匿名アクセスを示します。

コード	フィールド	説明
S3BK	S3 バケット	S3 バケット名。
S3KY	S3キー	バケット名を含まない S3 キー名。バケットに対する操作にはこのフィールドは含まれません。
S3SR	S3 サブリソース	該当する場合、操作対象のバケットまたはオブジェクト サブリソース。
SACC	S3テナントアカウント名（リクエスト送信者）	リクエストを送信したユーザーのテナント アカウントの名前。匿名のリクエストの場合は空です。
SAIP	IPアドレス（リクエスト送信者）	要求を行ったクライアント アプリケーションの IP アドレス。
SBAC	S3テナントアカウント名（バケット所有者）	バケット所有者のテナント アカウント名。クロスアカウントまたは匿名アクセスを識別するために使用されます。
SBAI	S3 テナントアカウント ID (バケット所有者)	ターゲット バケットの所有者のテナント アカウント ID。クロスアカウントまたは匿名アクセスを識別するために使用されます。
SGRP	サイト（グループ）	存在する場合、オブジェクトは指定されたサイトで削除されましたが、そのサイトはオブジェクトが取り込まれたサイトではありません。
SUSR	S3 ユーザー URN (リクエスト送信者)	テナント アカウント ID と、リクエストを行っているユーザーのユーザー名。ユーザーはローカル ユーザーまたは LDAP ユーザーのいずれかになります。例： `urn:sgws:identity::03393893651506583485:root` 匿名のリクエストの場合は空です。
時間	Time	リクエストの合計処理時間（マイクロ秒単位）。
TLIP	信頼できるロードバランサのIPアドレス	リクエストが信頼できるレイヤー 7 ロード バランサによってルーティングされた場合は、ロード バランサの IP アドレス。
UUDM	削除マーカーのユニバーサルユニーク識別子	削除マーカーの識別子。監査ログ メッセージは UUDM または UUID のいずれかを指定します。UUDM はオブジェクト削除要求の結果として作成された削除マーカーを示し、UUID はオブジェクトを示します。

コード	フィールド	説明
UUID	ユニバーサルユニーク識別子	StorageGRIDシステム内のオブジェクトの識別子。
VSID	バージョン ID	削除されたオブジェクトの特定のバージョンのバージョン ID。バケットおよびバージョン管理されていないバケット内のオブジェクトに対する操作には、このフィールドは含まれません。

SGET: S3 ゲット

S3 クライアントが GET トランザクションを発行すると、オブジェクトを取得するかバケット内のオブジェクトを一覧表示するか、バケット/オブジェクトのサブリソースを削除する要求が行われます。トランザクションが成功した場合、このメッセージはサーバーによって発行されます。

コード	フィールド	説明
CBID	コンテンツブロック識別子	要求されたコンテンツ ブロックの一意の識別子。 CBID が不明な場合、このフィールドは 0 に設定されます。バケットに対する操作にはこのフィールドは含まれません。
CNCH	一貫性制御ヘッダー	リクエスト内に存在する場合の Consistency-Control HTTP リクエストヘッダーの値。
CNID	接続識別子	TCP/IP 接続の一意のシステム識別子。
CSIZ	コンテンツサイズ	取得したオブジェクトのサイズ（バイト単位）。バケットに対する操作にはこのフィールドは含まれません。
HTRH	HTTPリクエストヘッダー	構成時に選択された、ログに記録された HTTP 要求ヘッダー名と値のリスト。 `X-Forwarded-For`リクエストに存在し、 `X-Forwarded-For`値が要求送信者の IP アドレス (SAIP 監査フィールド) と異なります。
リティ	リストオブジェクトV2	_v2 形式_の応答が要求されました。詳細については、 "AWS ListObjectsV2" 。 GET バケット操作のみ。
NCHD	子供の数	キーと一般的なプレフィックスが含まれます。 GET バケット操作のみ。

コード	フィールド	説明
鳴った	範囲読み取り	範囲読み取り操作のみ。この要求によって読み取られたバイトの範囲を示します。スラッシュ (/) の後の値は、オブジェクト全体のサイズを示します。
RSLT	結果コード	GET トランザクションの結果。結果は常に次のようになります: SUCS: 成功
S3AI	S3テナントアカウントID（リクエスト送信者）	リクエストを送信したユーザーのテナント アカウント ID。空の値は匿名アクセスを示します。
S3AK	S3 アクセスキー ID (リクエスト送信者)	リクエストを送信したユーザーのハッシュ化された S3 アクセスキー ID。空の値は匿名アクセスを示します。
S3BK	S3 バケット	S3 バケット名。
S3KY	S3キー	バケット名を含まない S3 キー名。バケットに対する操作にはこのフィールドは含まれません。
S3SR	S3 サブリソース	該当する場合、操作対象のバケットまたはオブジェクト サブリソース。
SACC	S3テナントアカウント名（リクエスト送信者）	リクエストを送信したユーザーのテナント アカウントの名前。匿名のリクエストの場合は空です。
SAIP	IPアドレス（リクエスト送信者）	要求を行ったクライアント アプリケーションの IP アドレス。
SBAC	S3テナントアカウント名（バケット所有者）	バケット所有者のテナント アカウント名。クロスアカウントまたは匿名アクセスを識別するために使用されます。
SBAI	S3 テナントアカウント ID (バケット所有者)	ターゲット バケットの所有者のテナント アカウント ID。クロスアカウントまたは匿名アクセスを識別するために使用されます。
SUSR	S3 ユーザー URN (リクエスト送信者)	テナント アカウント ID と、リクエストを行っているユーザーのユーザー名。ユーザーはローカル ユーザーまたは LDAP ユーザーのいずれかになります。例： `urn:sgws:identity::03393893651506583485:root` 匿名のリクエストの場合は空です。

コード	フィールド	説明
時間	Time	リクエストの合計処理時間（マイクロ秒単位）。
TLIP	信頼できるロードバランサのIPアドレス	リクエストが信頼できるレイヤー 7 ロード バランサによってルーティングされた場合は、ロード バランサの IP アドレス。
北キプロス共和国	切り捨てまたは切り捨てなし	すべての結果が返された場合は false に設定します。返される結果がさらにある場合は true に設定します。 GET バケット操作のみ。
UUID	ユニバーサルユニーク識別子	StorageGRIDシステム内のオブジェクトの識別子。
VSID	バージョン ID	要求されたオブジェクトの特定のバージョンのバージョン ID。バケットおよびバージョン管理されていないバケット内のオブジェクトに対する操作には、このフィールドは含まれません。

シア：**S3**ヘッド

S3 クライアントが HEAD トランザクションを発行すると、オブジェクトまたはバケットの存在を確認し、オブジェクトに関するメタデータを取得する要求が行われます。トランザクションが成功した場合、このメッセージはサーバーによって発行されます。

コード	フィールド	説明
CBID	コンテンツブロック識別子	要求されたコンテンツ ブロックの一意の識別子。 CBID が不明な場合、このフィールドは 0 に設定されます。バケットに対する操作にはこのフィールドは含まれません。
CNID	接続識別子	TCP/IP 接続の一意のシステム識別子。
CSIZ	コンテンツサイズ	チェックされたオブジェクトのサイズ（バイト単位）。バケットに対する操作にはこのフィールドは含まれません。
HTRH	HTTPリクエストヘッダー	構成時に選択された、ログに記録された HTTP 要求ヘッダー名と値のリスト。 `X-Forwarded-For`リクエストに存在し、 `X-Forwarded-For`値が要求送信者の IP アドレス (SAIP 監査フィールド) と異なります。
RSLT	結果コード	GET トランザクションの結果。結果は常に次のようになります: SUCS: 成功

コード	フィールド	説明
S3AI	S3テナントアカウントID（リクエスト送信者）	リクエストを送信したユーザーのテナント アカウント ID。空の値は匿名アクセスを示します。
S3AK	S3 アクセスキー ID (リクエスト送信者)	リクエストを送信したユーザーのハッシュ化された S3 アクセスキー ID。空の値は匿名アクセスを示します。
S3BK	S3 バケット	S3 バケット名。
S3KY	S3キー	バケット名を含まない S3 キー名。バケットに対する操作にはこのフィールドは含まれません。
SACC	S3テナントアカウント名（リクエスト送信者）	リクエストを送信したユーザーのテナント アカウントの名前。匿名のリクエストの場合は空です。
SAIP	IPアドレス（リクエスト送信者）	要求を行ったクライアント アプリケーションの IP アドレス。
SBAC	S3テナントアカウント名（バケット所有者）	バケット所有者のテナント アカウント名。クロスアカウントまたは匿名アクセスを識別するために使用されます。
SBAI	S3 テナントアカウント ID (バケット所有者)	ターゲット バケットの所有者のテナント アカウント ID。クロスアカウントまたは匿名アクセスを識別するために使用されます。
SUSR	S3 ユーザー URN (リクエスト送信者)	テナント アカウント ID と、リクエストを行っているユーザーのユーザー名。ユーザーはローカル ユーザーまたは LDAP ユーザーのいずれかになります。例： `urn:sgws:identity::03393893651506583485:root` 匿名のリクエストの場合は空です。
時間	Time	リクエストの合計処理時間（マイクロ秒単位）。
TLIP	信頼できるロードバランサのIPアドレス	リクエストが信頼できるレイヤー 7 ロード バランサによってルーティングされた場合は、ロード バランサの IP アドレス。
UUID	ユニバーサルユニーク識別子	StorageGRIDシステム内のオブジェクトの識別子。

コード	フィールド	説明
VSID	バージョン ID	要求されたオブジェクトの特定のバージョンのバージョン ID。バケットおよびバージョン管理されていないバケット内のオブジェクトに対する操作には、このフィールドは含まれません。

SPOS: S3 ポスト

S3 クライアントが POST オブジェクト リクエストを発行すると、トランザクションが成功するとサーバーによってこのメッセージが発行されます。

コード	フィールド	説明
CBID	コンテンツブロック識別子	要求されたコンテンツ ブロックの一意の識別子。 CBID が不明な場合、このフィールドは 0 に設定されます。
CNCH	一貫性制御ヘッダー	リクエスト内に存在する場合の Consistency-Control HTTP リクエストヘッダーの値。
CNID	接続識別子	TCP/IP 接続の一意のシステム識別子。
CSIZ	コンテンツサイズ	取得したオブジェクトのサイズ（バイト単位）。
HTRH	HTTPリクエストヘッダー	構成時に選択された、ログに記録された HTTP 要求ヘッダー名と値のリスト。 `X-Forwarded-For`リクエストに存在し、 `X-Forwarded-For`値が要求送信者の IP アドレス (SAIP 監査フィールド) と異なります。 (SPOS では予想されません)。
RSLT	結果コード	RestoreObject 要求の結果。結果は常に次のようになります: SUCS: 成功
S3AI	S3テナントアカウントID（リクエスト送信者）	リクエストを送信したユーザーのテナント アカウント ID。空の値は匿名アクセスを示します。
S3AK	S3 アクセスキー ID (リクエスト送信者)	リクエストを送信したユーザーのハッシュ化された S3 アクセスキー ID。空の値は匿名アクセスを示します。

コード	フィールド	説明
S3BK	S3 バケット	S3 バケット名。
S3KY	S3キー	バケット名を含まない S3 キー名。バケットに対する操作にはこのフィールドは含まれません。
S3SR	S3 サブリソース	該当する場合、操作対象のバケットまたはオブジェクト サブリソース。 S3 Select 操作の場合は「select」に設定します。
SACC	S3テナントアカウント名（リクエスト送信者）	リクエストを送信したユーザーのテナント アカウントの名前。匿名のリクエストの場合は空です。
SAIP	IPアドレス（リクエスト送信者）	要求を行ったクライアント アプリケーションの IP アドレス。
SBAC	S3テナントアカウント名（バケット所有者）	バケット所有者のテナント アカウント名。クロスアカウントまたは匿名アクセスを識別するために使用されます。
SBAI	S3 テナントアカウント ID (バケット所有者)	ターゲット バケットの所有者のテナント アカウント ID。クロスアカウントまたは匿名アクセスを識別するために使用されます。
SRCF	サブリソース構成	情報を復元します。
SUSR	S3 ユーザー URN (リクエスト送信者)	テナント アカウント ID と、リクエストを行っているユーザーのユーザー名。ユーザーはローカル ユーザーまたは LDAP ユーザーのいずれかになります。例： `urn:sgws:identity::03393893651506583485:root` 匿名のリクエストの場合は空です。
時間	Time	リクエストの合計処理時間（マイクロ秒単位）。
TLIP	信頼できるロードバランサのIPアドレス	リクエストが信頼できるレイヤー 7 ロード バランサによってルーティングされた場合は、ロード バランサの IP アドレス。
UUID	ユニバーサルユニーク識別子	StorageGRIDシステム内のオブジェクトの識別子。

コード	フィールド	説明
VSID	バージョン ID	要求されたオブジェクトの特定のバージョンのバージョン ID。バケットおよびバージョン管理されていないバケット内のオブジェクトに対する操作には、このフィールドは含まれません。

スプット: **S3** プット

S3 クライアントが PUT トランザクションを発行すると、新しいオブジェクトまたはバケットを作成するか、バケット/オブジェクトのサブリソースを削除するように要求されます。トランザクションが成功した場合、このメッセージはサーバーによって発行されます。

コード	フィールド	説明
CBID	コンテンツブロック識別子	要求されたコンテンツ ブロックの一意の識別子。 CBID が不明な場合、このフィールドは 0 に設定されます。バケットに対する操作にはこのフィールドは含まれません。
CMPS	コンプライアンス設定	リクエスト内に存在する場合、バケットの作成時に使用されたコンプライアンス設定 (最初の 1024 文字に切り捨てられます)。
CNCH	一貫性制御ヘッダー	リクエスト内に存在する場合の Consistency-Control HTTP リクエストヘッダーの値。
CNID	接続識別子	TCP/IP 接続の一意のシステム識別子。
CSIZ	コンテンツサイズ	取得したオブジェクトのサイズ（バイト単位）。バケットに対する操作にはこのフィールドは含まれません。
GFID	グリッドフェデレーション接続ID	クロスグリッド レプリケーション PUT 要求に関連付けられたグリッドフェデレーション接続の接続 ID。宛先グリッドの監査ログにのみ含まれます。
GFSA	グリッドフェデレーションソースアカウントID	クロスグリッド レプリケーション PUT リクエストのソース グリッド上のテナントのアカウント ID。宛先グリッドの監査ログにのみ含まれます。

コード	フィールド	説明
HTRH	HTTPリクエストヘッダー	構成時に選択された、ログに記録された HTTP 要求ヘッダー名と値のリスト。 `X-Forwarded-For`リクエストに存在し、 `X-Forwarded-For`値が要求送信者の IP アドレス (SAIP 監査フィールド) と異なります。 `x-amz-bypass-governance-retention`リクエスト内に存在する場合は自動的に含まれます。
ルケン	オブジェクトロックが有効	リクエストヘッダーの値 x-amz-bucket-object-lock-enabled（リクエスト内に存在する場合）。
LKLH	オブジェクトロック法的保留	リクエストヘッダーの値 `x-amz-object-lock-legal-hold`PutObject リクエストに存在する場合。
LKMD	オブジェクトロック保持モード	リクエストヘッダーの値 `x-amz-object-lock-mode`PutObject リクエストに存在する場合。
LKRU	オブジェクトロックの保持期限	リクエストヘッダーの値 `x-amz-object-lock-retain-until-date`PutObject リクエストに存在する場合。値は、オブジェクトが取り込まれた日付から 100 年以内に制限されます。
MTME	最終更新日時	オブジェクトが最後に変更された時刻を示す、マイクロ秒単位の Unix タイムスタンプ。
RSLT	結果コード	PUT トランザクションの結果。結果は常に次のようになります: SUCS: 成功
S3AI	S3テナントアカウントID（リクエスト送信者）	リクエストを送信したユーザーのテナント アカウント ID。空の値は匿名アクセスを示します。
S3AK	S3 アクセスキー ID (リクエスト送信者)	リクエストを送信したユーザーのハッシュ化された S3 アクセスキー ID。空の値は匿名アクセスを示します。
S3BK	S3 バケット	S3 バケット名。
S3KY	S3キー	バケット名を含まない S3 キー名。バケットに対する操作にはこのフィールドは含まれません。

コード	フィールド	説明
S3SR	S3 サブリソース	該当する場合、操作対象のバケットまたはオブジェクト サブリソース。
SACC	S3テナントアカウント名（リクエスト送信者）	リクエストを送信したユーザーのテナント アカウントの名前。匿名のリクエストの場合は空です。
SAIP	IPアドレス（リクエスト送信者）	要求を行ったクライアント アプリケーションの IP アドレス。
SBAC	S3テナントアカウント名（バケット所有者）	バケット所有者のテナント アカウント名。クロスアカウントまたは匿名アクセスを識別するために使用されます。
SBAI	S3 テナントアカウント ID (バケット所有者)	ターゲット バケットの所有者のテナント アカウント ID。クロスアカウントまたは匿名アクセスを識別するために使用されます。
SRCF	サブリソース構成	新しいサブリソース構成 (最初の 1024 文字に切り捨てられます)。
SUSR	S3 ユーザー URN (リクエスト送信者)	テナント アカウント ID と、リクエストを行っているユーザーのユーザー名。ユーザーはローカル ユーザーまたは LDAP ユーザーのいずれかになります。例： `urn:sgws:identity::03393893651506583485:root` 匿名のリクエストの場合は空です。
時間	Time	リクエストの合計処理時間（マイクロ秒単位）。
TLIP	信頼できるロードバランサのIPアドレス	リクエストが信頼できるレイヤー 7 ロード バランサによってルーティングされた場合は、ロード バランサの IP アドレス。
ULID	アップロードID	CompleteMultipartUpload 操作の SPUT メッセージにのみ含まれます。すべてのパーツがアップロードされ、組み立てられたことを示します。
UUID	ユニバーサルユニーク識別子	StorageGRIDシステム内のオブジェクトの識別子。
VSID	バージョン ID	バージョン管理されたバケットに作成された新しいオブジェクトのバージョン ID。バケットおよびバージョン管理されていないバケット内のオブジェクトに対する操作には、このフィールドは含まれません。

コード	フィールド	説明
VSST	バージョン管理状態	バケットの新しいバージョン管理状態。使用される状態は、「有効」または「一時停止」の 2 つです。オブジェクトに対する操作にはこのフィールドは含まれません。

SREM: オブジェクトストアの削除

このメッセージは、コンテンツが永続ストレージから削除され、通常の API 経由でアクセスできなくなったときに発行されます。

コード	フィールド	説明
CBID	コンテンツブロック識別子	永続ストレージから削除されたコンテンツ ブロックの一意の識別子。
RSLT	結果コード	コンテンツ削除操作の結果を示します。次の値のみが定義されています。 SUCS: 永続ストレージからコンテンツが削除されました

この監査メッセージは、特定のコンテンツ ブロックがノードから削除され、直接要求できなくなったことを意味します。このメッセージは、システム内で削除されたコンテンツの流れを追跡するために使用できます。

SUPD: S3 メタデータが更新されました

このメッセージは、S3 クライアントが取り込んだオブジェクトのメタデータを更新したときに、S3 API によって生成されます。メタデータの更新が成功した場合、サーバーによってメッセージが発行されます。

コード	フィールド	説明
CBID	コンテンツブロック識別子	要求されたコンテンツ ブロックの一意の識別子。 CBID が不明な場合、このフィールドは 0 に設定されます。バケットに対する操作にはこのフィールドは含まれません。
CNCH	一貫性制御ヘッダー	バケットのコンプライアンス設定を更新するときの、Consistency-Control HTTP リクエスト ヘッダーの値 (リクエスト内に存在する場合)。
CNID	接続識別子	TCP/IP 接続の一意のシステム識別子。
CSIZ	コンテンツサイズ	取得したオブジェクトのサイズ（バイト単位）。バケットに対する操作にはこのフィールドは含まれません。

コード	フィールド	説明
HTRH	HTTPリクエストヘッダー	構成時に選択された、ログに記録された HTTP 要求ヘッダー名と値のリスト。 `X-Forwarded-For`リクエストに存在し、 `X-Forwarded-For`値が要求送信者の IP アドレス (SAIP 監査フィールド) と異なります。
RSLT	結果コード	GET トランザクションの結果。結果は常に次のようになります: SUCS: 成功
S3AI	S3テナントアカウントID（リクエスト送信者）	リクエストを送信したユーザーのテナント アカウント ID。空の値は匿名アクセスを示します。
S3AK	S3 アクセスキー ID (リクエスト送信者)	リクエストを送信したユーザーのハッシュ化された S3 アクセスキー ID。空の値は匿名アクセスを示します。
S3BK	S3 バケット	S3 バケット名。
S3KY	S3キー	バケット名を含まない S3 キー名。バケットに対する操作にはこのフィールドは含まれません。
SACC	S3テナントアカウント名（リクエスト送信者）	リクエストを送信したユーザーのテナント アカウントの名前。匿名のリクエストの場合は空です。
SAIP	IPアドレス（リクエスト送信者）	要求を行ったクライアント アプリケーションの IP アドレス。
SBAC	S3テナントアカウント名（バケット所有者）	バケット所有者のテナント アカウント名。クロスアカウントまたは匿名アクセスを識別するために使用されます。
SBAI	S3 テナントアカウント ID (バケット所有者)	ターゲット バケットの所有者のテナント アカウント ID。クロスアカウントまたは匿名アクセスを識別するために使用されます。

コード	フィールド	説明
SUSR	S3 ユーザー URN (リクエスト送信者)	テナント アカウント ID と、リクエストを行っているユーザーのユーザー名。ユーザーはローカル ユーザーまたは LDAP ユーザーのいずれかになります。例： `urn:sgws:identity::03393893651506583485:root` 匿名のリクエストの場合は空です。
時間	Time	リクエストの合計処理時間（マイクロ秒単位）。
TLIP	信頼できるロードバランサのIPアドレス	リクエストが信頼できるレイヤー 7 ロード バランサによってルーティングされた場合は、ロード バランサの IP アドレス。
UUID	ユニバーサルユニーク識別子	StorageGRIDシステム内のオブジェクトの識別子。
VSID	バージョン ID	メタデータが更新されたオブジェクトの特定のバージョンのバージョンID。バケットおよびバージョン管理されていないバケット内のオブジェクトに対する操作には、このフィールドは含まれません。

SVRF: オブジェクトストア検証失敗

このメッセージは、コンテンツ ブロックが検証プロセスに失敗するたびに発行されます。複製されたオブジェクト データがディスクから読み取られたり、ディスクに書き込まれたりするときは毎回、要求元のユーザーに送信されるデータがシステムに最初に取り込まれたデータと同一であることを確認するために、いくつかの検証と整合性チェックが実行されます。これらのチェックのいずれかが失敗した場合、システムは破損した複製オブジェクト データを自動的に隔離し、再度取得されないようにします。

コード	フィールド	説明
CBID	コンテンツブロック識別子	検証に失敗したコンテンツ ブロックの一意の識別子。

コード	フィールド	説明
RSLT	結果コード	検証失敗の種類: CRCF: 巡回冗長検査 (CRC) に失敗しました。 HMAC: ハッシュベースのメッセージ認証コード (HMAC) チェックに失敗しました。 EHSH: 予期しない暗号化されたコンテンツ ハッシュ。 PHSH: 予期しない元のコンテンツ ハッシュ。 SEQC: ディスク上のデータ シーケンスが正しくありません。 PERR: ディスク ファイルの構造が無効です。 DERR: ディスク エラー。 FNAM: ファイル名が間違っています。

このメッセージは注意深く監視する必要があります。コンテンツ検証の失敗は、ハードウェア障害が差し迫っていることを示している可能性があります。

どの操作によってメッセージがトリガーされたかを確認するには、AMID (モジュール ID) フィールドの値を確認します。たとえば、SVFY 値は、メッセージが Storage Verifier モジュール (つまりバックグラウンド検証) によって生成されたことを示し、STOR は、メッセージがコンテンツの取得によってトリガーされたことを示します。

SVRU: オブジェクトストアの検証が不明です

LDR サービスのストレージ コンポーネントは、オブジェクト ストア内の複製されたオブジェクト データのすべてのコピーを継続的にスキャンします。このメッセージは、複製されたオブジェクト データの不明なまたは予期しないコピーがオブジェクト ストアで検出され、隔離ディレクトリに移動されたときに発行されます。

コード	フィールド	説明
FPTH	ファイルパス	予期しないオブジェクト コピーのファイル パス。
RSLT	結果	このフィールドの値は「NONE」です。 RSLT は必須のメッセージ フィールドですが、このメッセージには関係ありません。このメッセージはフィルタリングされないように、「SUCS」ではなく「NONE」が使用されます。

SVRU: オブジェクト ストアの検証不明監査メッセージを注意深く監視する必要があります。これは、オブジェクト ストアでオブジェクト データの予期しないコピーが検出されたことを意味します。この状況はハードウェア障害の兆候を示している可能性があるため、これらのコピーがどのように作成されたかを判断するためにすぐに調査する必要があります。

SYSD: ノード停止

サービスが正常に停止されると、シャットダウンが要求されたことを示すこのメッセージが生成されます。通常、監査メッセージ キューはシャットダウン前にクリアされないため、このメッセージはその後の再起動後にのみ送信されます。サービスが再起動されていない場合は、シャットダウン シーケンスの開始時に送信される SYST メッセージを探します。

コード	フィールド	説明
RSLT	クリーンシャットダウン	シャットダウンの性質: SUCS: システムは正常にシャットダウンされました。

メッセージには、ホスト サーバーが停止されているかどうかは示されず、レポート サービスのみが示されます。 SYSD の RSLT は、「クリーン」シャットダウンによってのみメッセージが生成されるため、「ダーティ」シャットダウンを示すことはできません。

SYST: ノード停止

サービスが正常に停止されると、シャットダウンが要求され、サービスがシャットダウン シーケンスを開始したことを示すこのメッセージが生成されます。 SYST は、サービスが再起動される前にシャットダウンが要求されたかどうかを判断するために使用できます (通常、サービスの再起動後に送信される SYSD とは異なります)。

コード	フィールド	説明
RSLT	クリーンシャットダウン	シャットダウンの性質: SUCS: システムは正常にシャットダウンされました。

メッセージには、ホスト サーバーが停止されているかどうかは示されず、レポート サービスのみが示されます。 SYST メッセージの RSLT コードは、「クリーン」シャットダウンによってのみメッセージが生成されるため、「ダーティ」シャットダウンを示すことはできません。

SYSU: ノード開始

サービスが再起動されると、前回のシャットダウンが正常 (コマンドによる) であったか、異常 (予期しない) であったかを示すこのメッセージが生成されます。

コード	フィールド	説明
RSLT	クリーンシャットダウン	シャットダウンの性質: SUCS: システムは正常にシャットダウンされました。 DSDN: システムが正常にシャットダウンされませんでした。 VRGN: サーバーのインストール (または再インストール) 後にシステムが初めて起動されました。

メッセージには、ホスト サーバーが起動されたかどうかは示されず、レポート サービスのみが示されます。このメッセージは次の目的で使用できます。

- 監査証跡の不連続性を検出します。
- 操作中にサービスに障害が発生しているかどうかを判断します (StorageGRIDシステムの分散性により、これらの障害が隠される可能性があるため)。サーバー マネージャーは障害が発生したサービスを自動的に再起動します。

WDEL: 迅速な削除

Swift クライアントが DELETE トランザクションを発行すると、指定されたオブジェクトまたはコンテナを削除する要求が行われます。トランザクションが成功した場合、このメッセージはサーバーによって発行されます。

コード	フィールド	説明
CBID	コンテンツブロック識別子	要求されたコンテンツ ブロックの一意の識別子。 CBID が不明な場合、このフィールドは 0 に設定されます。コンテナに対する操作にはこのフィールドは含まれません。
CSIZ	コンテンツサイズ	削除されたオブジェクトのサイズ（バイト単位）。コンテナに対する操作にはこのフィールドは含まれません。
HTRH	HTTPリクエストヘッダー	構成時に選択された、ログに記録された HTTP 要求ヘッダー名と値のリスト。 `X-Forwarded-For`リクエストに存在し、 `X-Forwarded-For`値が要求送信者の IP アドレス (SAIP 監査フィールド) と異なります。
MTME	最終更新日時	オブジェクトが最後に変更された時刻を示す、マイクロ秒単位の Unix タイムスタンプ。

コード	フィールド	説明
RSLT	結果コード	DELETE トランザクションの結果。結果は常に次のようになります: SUCS: 成功
SAIP	要求元クライアントのIPアドレス	要求を行ったクライアント アプリケーションの IP アドレス。
SGRP	サイト（グループ）	存在する場合、オブジェクトは指定されたサイトで削除されましたが、そのサイトはオブジェクトが取り込まれたサイトではありません。
時間	Time	リクエストの合計処理時間（マイクロ秒単位）。
TLIP	信頼できるロードバランサのIPアドレス	リクエストが信頼できるレイヤー 7 ロード バランサによってルーティングされた場合は、ロード バランサの IP アドレス。
UUID	ユニバーサルユニーク識別子	StorageGRIDシステム内のオブジェクトの識別子。
WACC	SwiftアカウントID	StorageGRIDシステムによって指定された一意のアカウント ID。
WCON	Swiftコンテナ	Swift コンテナ名。
WOBJ	Swiftオブジェクト	Swift オブジェクト識別子。コンテナに対する操作にはこのフィールドは含まれません。
WUSR	Swiftアカウントユーザー	トランザクションを実行するクライアントを一意に識別する Swift アカウントのユーザー名。

WGET: Swift GET

Swift クライアントが GET トランザクションを発行すると、オブジェクトの取得、コンテナー内のオブジェクトのリスト、またはアカウント内のコンテナーのリストの取得の要求が行われます。トランザクションが成功した場合、このメッセージはサーバーによって発行されます。

コード	フィールド	説明
CBID	コンテンツブロック識別子	要求されたコンテンツ ブロックの一意の識別子。 CBID が不明な場合、このフィールドは 0 に設定されます。アカウントおよびコンテナに対する操作にはこのフィールドは含まれません。

コード	フィールド	説明
CSIZ	コンテンツサイズ	取得したオブジェクトのサイズ（バイト単位）。アカウントおよびコンテナに対する操作にはこのフィールドは含まれません。
HTRH	HTTPリクエストヘッダー	構成時に選択された、ログに記録された HTTP 要求ヘッダー名と値のリスト。 `X-Forwarded-For`リクエストに存在し、 `X-Forwarded-For`値が要求送信者の IP アドレス（SAIP 監査フィールド）と異なります。
RSLT	結果コード	GET トランザクションの結果。結果は常に SUCS: 成功
SAIP	要求元クライアントのIPアドレス	要求を行ったクライアント アプリケーションの IP アドレス。
時間	Time	リクエストの合計処理時間（マイクロ秒単位）。
TLIP	信頼できるロードバランサのIPアドレス	リクエストが信頼できるレイヤー 7 ロード バランサによってルーティングされた場合は、ロード バランサの IP アドレス。
UUID	ユニバーサルユニーク識別子	StorageGRIDシステム内のオブジェクトの識別子。
WACC	SwiftアカウントID	StorageGRIDシステムによって指定された一意のアカウント ID。
WCON	Swiftコンテナ	Swift コンテナ名。アカウントに対する操作にはこのフィールドは含まれません。
WOBJ	Swiftオブジェクト	Swift オブジェクト識別子。アカウントおよびコンテナに対する操作にはこのフィールドは含まれません。
WUSR	Swiftアカウントユーザー	トランザクションを実行するクライアントを一意に識別する Swift アカウントのユーザー名。

WHEA: Swift HEAD

Swift クライアントが HEAD トランザクションを発行すると、アカウント、コンテナ、またはオブジェクトの存在を確認し、関連するメタデータを取得する要求が行われま

す。トランザクションが成功した場合、このメッセージはサーバーによって発行されます。

コード	フィールド	説明
CBID	コンテンツブロック識別子	要求されたコンテンツ ブロックの一意の識別子。 CBID が不明な場合、このフィールドは 0 に設定されます。アカウントおよびコンテナに対する操作にはこのフィールドは含まれません。
CSIZ	コンテンツサイズ	取得したオブジェクトのサイズ（バイト単位）。アカウントおよびコンテナに対する操作にはこのフィールドは含まれません。
HTRH	HTTPリクエストヘッダー	構成時に選択された、ログに記録された HTTP 要求ヘッダー名と値のリスト。 `X-Forwarded-For`リクエストに存在し、 `X-Forwarded-For`値が要求送信者の IP アドレス（SAIP 監査フィールド）と異なります。
RSLT	結果コード	HEAD トランザクションの結果。結果は常に次のようになります: SUCS: 成功
SAIP	要求元クライアントのIPアドレス	要求を行ったクライアント アプリケーションの IP アドレス。
時間	Time	リクエストの合計処理時間（マイクロ秒単位）。
TLIP	信頼できるロードバランサのIPアドレス	リクエストが信頼できるレイヤー 7 ロード バランサによってルーティングされた場合は、ロード バランサの IP アドレス。
UUID	ユニバーサルユニーク識別子	StorageGRIDシステム内のオブジェクトの識別子。
WACC	SwiftアカウントID	StorageGRIDシステムによって指定された一意のアカウント ID。
WCON	Swiftコンテナ	Swift コンテナ名。アカウントに対する操作にはこのフィールドは含まれません。
WOBJ	Swiftオブジェクト	Swift オブジェクト識別子。アカウントおよびコンテナに対する操作にはこのフィールドは含まれません。

コード	フィールド	説明
WUSR	Swiftアカウントユーザー	トランザクションを実行するクライアントを一意に識別する Swift アカウントのユーザー名。

WPUT: Swift PUT

Swift クライアントが PUT トランザクションを発行すると、新しいオブジェクトまたはコンテナを作成する要求が行われます。トランザクションが成功した場合、このメッセージはサーバーによって発行されます。

コード	フィールド	説明
CBID	コンテンツブロック識別子	要求されたコンテンツ ブロックの一意の識別子。 CBID が不明な場合、このフィールドは 0 に設定されます。コンテナに対する操作にはこのフィールドは含まれません。
CSIZ	コンテンツサイズ	取得したオブジェクトのサイズ（バイト単位）。コンテナに対する操作にはこのフィールドは含まれません。
HTRH	HTTPリクエストヘッダー	構成時に選択された、ログに記録された HTTP 要求ヘッダー名と値のリスト。 `X-Forwarded-For`リクエストに存在し、 `X-Forwarded-For`値が要求送信者の IP アドレス (SAIP 監査フィールド) と異なります。
MTME	最終更新日時	オブジェクトが最後に変更された時刻を示す、マイクロ秒単位の Unix タイムスタンプ。
RSLT	結果コード	PUT トランザクションの結果。結果は常に次のようになります: SUCS: 成功
SAIP	要求元クライアントのIPアドレス	要求を行ったクライアント アプリケーションの IP アドレス。
時間	Time	リクエストの合計処理時間（マイクロ秒単位）。
TLIP	信頼できるロードバランサのIPアドレス	リクエストが信頼できるレイヤー 7 ロード バランサによってルーティングされた場合は、ロード バランサの IP アドレス。

コード	フィールド	説明
UUID	ユニバーサルユニーク識別子	StorageGRIDシステム内のオブジェクトの識別子。
WACC	SwiftアカウントID	StorageGRIDシステムによって指定された一意のアカウント ID。
WCON	Swiftコンテナ	Swift コンテナ名。
WOBJ	Swiftオブジェクト	Swift オブジェクト識別子。コンテナに対する操作にはこのフィールドは含まれません。
WUSR	Swiftアカウントユーザー	トランザクションを実行するクライアントを一意に識別する Swift アカウントのユーザー名。

著作権に関する情報

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

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

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

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

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

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

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

商標に関する情報

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