



# 監視とトラブルシューティング StorageGRID

NetApp  
December 03, 2025

# 目次

StorageGRIDシステムの監視とトラブルシューティング	1
StorageGRID システムを監視します	1
StorageGRID システムの監視：概要	1
ダッシュボードを表示および管理します	2
Nodes ページを表示します	4
定期的に監視する情報	39
アラートとアラーム	69
ログファイル参照	165
監査メッセージとログの送信先の設定	184
SNMP による監視を使用する	198
追加の StorageGRID データを収集します	211
StorageGRID システムのトラブルシューティングを行う	246
StorageGRID システムのトラブルシューティング：概要	246
オブジェクトやストレージの問題をトラブルシューティングする	253
メタデータに関する問題のトラブルシューティング	291
証明書エラーのトラブルシューティングを行う	298
管理ノードとユーザインターフェイスの問題をトラブルシューティングする	299
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をトラブルシューティングする	305
外部 syslog サーバのトラブルシューティングを行います	314
監査ログを確認します	317
監査ログの確認：概要	317
監査メッセージのフローと保持	318
監査ログファイルにアクセスします	321
監査ログファイルのローテーション	322
監査ログファイルの形式	322
監査メッセージの形式	335
監査メッセージとオブジェクトライフサイクル	340
監査メッセージ	347

# StorageGRIDシステムの監視とトラブルシューティング

## StorageGRID システムを監視します

### StorageGRID システムの監視：概要

StorageGRIDシステムを定期的に監視して、想定どおりに動作していることを確認してください。

作業を開始する前に

- を使用して Grid Manager にサインインします "サポートされている Web ブラウザ"。
- これで完了です "特定のアクセス権限"。



Grid Managerに表示されるストレージ値の単位を変更するには、Grid Managerの右上にあるユーザードロップダウンを選択し、\*[ユーザ設定]\*を選択します。

このタスクについて

ここでは、次の手順について説明します。

- "ダッシュボードを表示および管理します"
- "Nodes ページを表示します"
- "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"
  - "ネットワークおよびシステムリソース"
  - "テナントのアクティビティ"
  - "ロードバランシング操作"
  - "グリッドフェデレーション接続"
  - "アーカイブ容量"
- "アラートと従来のアラームの管理"
- "ログファイルの表示"
- "監査メッセージとログの送信先を設定します"
- "外部 syslog サーバを使用します" 監査情報を収集するには
- "SNMPを使用した監視"
- "追加のStorageGRIDデータを取得する" (指標や診断を含む)

## ダッシュボードを表示および管理します

ダッシュボードを使用すると、システムのアクティビティを一目で監視できます。StorageGRID の実装を監視するためのカスタムダッシュボードを作成できます。



Grid Managerに表示されるストレージ値の単位を変更するには、Grid Managerの右上にあるユーザードロップダウンを選択し、\*[ユーザ設定]\*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。

The screenshot shows the StorageGRID dashboard with the following sections:

- Health status:** Shows a warning icon and 'License 1'.
- Data space usage breakdown:** Shows '2.11 MB (0%) of 3.09 TB used overall' and a table of site usage.
- Total objects in the grid:** Shows '0'.
- Metadata allowed space usage breakdown:** Shows '3.62 MB (0%) of 25.76 GB used in Data Center 1' and a table of metadata usage.

Site name	Data storage usage	Used space	Total space
Data Center 2	0%	682.53 KB	926.62 GB
Data Center 3	0%	646.12 KB	926.62 GB
Data Center 1	0%	779.21 KB	1.24 TB

Site name	Metadata space usage	Used space	Allowed space
Data Center 3	0%	2.71 MB	19.32 GB

## ダッシュボードを表示します

ダッシュボードは、StorageGRID システムに関する特定の情報を表示す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はそのまま使用できます。また、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。

システム提供のダッシュボードタブには、次の種類の情報が記載されたカードが含まれています。

タブをクリックします	が含まれます
概要	アクティブなアラート、スペース使用量、グリッド内のオブジェクトの合計など、グリッドに関する一般的な情報。
パフォーマンス	スペース使用量、経時的に使用されるストレージ、S3またはSwift処理、要求期間、エラー率
ストレージ	テナントクォータ使用量および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を予測します。
ILM	情報ライフサイクル管理のキューと評価レート
ノード	ノード別のCPU、データ、メモリの使用率。ノード別のS3またはSwift処理。ノードからサイトへの分散：

一部のカードは、見やすいように最大化できます。最大化アイコンを選択します  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します

ルート・アクセス権がある場合（を参照 ["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して、表示するStorageGRID 情報とその構成を制御できます。
- ダッシュボードをクローニングしてカスタムダッシュボードを作成する。
- ユーザーの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には、システムが提供するダッシュボードとカスタムダッシュボードがあります。
- 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ます。
- 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。タブは1個以上20個以下にすることができます。
- ダッシュボードを削除します。



Root Access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。



ダッシュボードを設定する

アクティブなダッシュボードをクローニングして新しいダッシュボードを作成するには、[操作]>\*[アクティブなダッシュボードのクローニング]\*を選択します。

既存のダッシュボードを編集またはクローンするには、[アクション]>\*[ダッシュボードの管理]\*を選択します。



システムが提供するダッシュボードは編集または削除できません。

ダッシュボードを設定する際には、次の操作を実行できます。

- タブを追加または削除します
- タブの名前を変更し、新しいタブに一意的な名前を付けます
- 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
- カード上部の\*S、M、L、またはXL\*を選択して、個々のカードのサイズを選択します

Site name	Data storage usage	Used space	Total space
Data Center 1	0%	1.79 MB	1.24 TB
Data Center 2	0%	921.11 KB	926.62 GB
Data Center 3	0%	790.21 KB	926.62 GB

**Nodes** ページを表示します

[Nodes]ページの[Overview]を確認します

StorageGRID システムについて、ダッシュボードの情報よりも詳細な情報が必要な場合は、[Nodes]ページを使用してグリッド全体、グリッド内の各サイト、およびサイト内の各ノードの指標を表示できます。

[Nodes]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表示されます。切断されているノードやアクティブなアラートがあるノードは、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は、特定の指標が使用できないか、サイトおよびグリッドの合計値から除外されることがあります。ノードがグリッドに再接続されたら、値が安定するまで数分待ちます。



Grid Managerに表示されるストレージ値の単位を変更するには、Grid Managerの右上にあるユーザドロップダウンを選択し、\*[ユーザ設定]\*を選択します。

## Nodes

View the list and status of sites and grid nodes.

Search... Total node count: 12

Name	Type	Object data used	Object metadata used	CPU usage
StorageGRID Webscale Deployment	Grid	0%	0%	—
^ DC1	Site	0%	0%	—
DC1-ADM1	Primary Admin Node	—	—	6%
DC1-ARC1	Archive Node	—	—	1%
DC1-G1	Gateway Node	—	—	3%
DC1-S1	Storage Node	0%	0%	6%
DC1-S2	Storage Node	0%	0%	8%
DC1-S3	Storage Node	0%	0%	4%

### 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。

をクリックします。	説明	アクションが必要です
	<p>• 接続されていません - 不明 *</p> <p>理由が不明な場合、ノードが切断されているか、ノードのサービスが予期せず停止しています。たとえば、ノードのサービスが停止したり、電源障害や予期しない停止によってノードのネットワーク接続が失われたりする場合があります。</p> <p>• Unable to communicate with node * アラートがトリガーされる場合もあります。他のアラートもアクティブになる可能性があります。</p>	<p>アクションが必要です</p> <p>すぐに対処する必要があります。"<b>各アラートを選択します</b>"そして推奨される行動に従ってください。</p> <p>たとえば、ノードのホストを停止または再起動したサービスの再起動が必要になることがあります。</p> <p>注：管理されたシャットダウン処理の実行中は、ノードがUnknownと表示されることがあります。このような場合、Unknown 状態は無視してかまいません。</p>
	<p>• 接続されていません - 管理上の理由により停止して</p> <p>想定される理由により、ノードがグリッドに接続されていません。</p> <p>たとえば、ノードまたはノード上のサービスが正常にシャットダウンされた、ノードがリブート中である、ソフトウェアのアップグレード中であるなどの原因が考えられます。1つ以上のアラートがアクティブになっている可能性もあります。</p> <p>基盤となる問題に基づいて、これらのノードは多くの場合、介入なしでオンラインに戻ります。</p>	<p>このノードに影響しているアラートがないかどうかを確認します。</p> <p>アクティブなアラートがある場合は、"<b>各アラートを選択します</b>"そして推奨される行動に従ってください。</p>

ノードがグリッドから切断されている場合、アラートが発生している可能性があります。表示されるのは「Not Connected」アイコンのみです。ノードのアクティブなアラートを表示するには、ノードを選択します。

#### 警告アイコン

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

 **重大**：異常な状態で、StorageGRID ノードまたはサービスの正常な動作が停止しました。基盤となる問題にすぐに対処する必要があります。問題が解決されないと、サービスの停止やデータの損失を招くおそれがあります。

 **Major**:現在の動作に影響しているか、重大アラートのしきい値に近づいている異常な状態です。Major アラートを調査し、根本的な問題に対処して、異常な状態が発生した場合に StorageGRID のノードやサービスが正常に動作しなくなる事態を防ぐ必要があります。

 \* Minor \* : システムは正常に動作していますが、異常な状態が発生しているため、システムの動作に影響

する可能性があります。自動的にクリアされないMinorアラートを監視して解決し、重大な問題が発生しないようにする必要があります。

システム、サイト、またはノードの詳細を表示します

[Nodes]テーブルに表示される情報をフィルタリングするには、**[Search]**\*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、「gat \*」と入力すると、すべてのゲートウェイノードをすばやく特定できます）。

グリッド、サイト、またはノードの情報を表示するには、次の手順を実行します。

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

概要タブを表示します

Overview タブには、各ノードに関する基本的な情報が表示されます。また、ノードに現在影響しているアラートも表示されます。

すべてのノードの Overview（概要）タブが表示されます。

ノード情報

[Overview]タブの[Node Information]セクションには、ノードに関する基本情報が表示されます。

## NYC-ADM1 (Primary Admin Node)

Overview

Hardware

Network

Storage

Load balancer

Tasks

### Node information

Display name:	NYC-ADM1
System name:	DC1-ADM1
Type:	Primary Admin Node
ID:	3adb1aa8-9c7a-4901-8074-47054aa06ae6
Connection state:	 Connected
Software version:	11.7.0
IP addresses:	10.96.105.85 - eth0 (Grid Network)

[Show additional IP addresses](#) 

ノードの概要情報には次のものがあります。

- 表示名（ノードの名前が変更された場合にのみ表示）：ノードの現在の表示名。を使用します ["グリッド、サイト、ノードの名前を変更します"](#) 手順 をクリックしてこの値を更新します。
- システム名：インストール時に入力したノードの名前。システム名は内部StorageGRID 処理に使用され、変更することはできません。
- \* 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、ゲートウェイノード、またはアーカイブノード。



アーカイブノードのサポートは廃止され、今後のリリースで削除される予定です。S3 API を使用してアーカイブノードから外部のアーカイブストレージシステムにオブジェクトを移動する処理は、より多くの機能を提供する ILM Cloud Storage Pools に置き換えられました。

- \* ID \*：ノードの一意の識別子。UUID とも呼ばれます。
- \* 接続状態 \*：3つの状態のいずれか。最も重大な状態のアイコンが表示されます。
  - \* 不明 \* ：原因が不明で、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、電源がオフになっている、サービスが停止しているなどです。\* Unable to communicate with node \* アラートがトリガーされる場合もあります。他のアラートもアクティブになる可能性があります。この状況にはすぐに対処する必要があります。



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

- \* 管理上のダウン \*  : ノードが想定される理由でグリッドに接続されていません。たとえば、ノードまたはノード上のサービスが正常にシャットダウンされた、ノードがリブート中である、ソフトウェアのアップグレード中であるなどの原因が考えられます。1 つ以上のアラートがアクティブになっている可能性もあります。
- \* 接続済み \*  : ノードがグリッドに接続されています。
- \* Storage Used \* : ストレージノードのみ。
  - \* Object data \* : 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に使用可能な合計スペースの割合。
  - \* Object metadata \* : 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使用可能な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。ノードのネットワークインターフェイスがハイアベイラビリティグループに含まれている場合、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かどうかが表示されます。
- \* ip addresses \* : ノードの IP アドレス。Show additional IP addresses \* をクリックして、ノードの IPv4 および IPv6 アドレスとインターフェイスのマッピングを表示します。

## アラート

[Overview] タブの [Alerts] セクションには、が表示されます ["このノードに現在影響しているアラートで、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、その他の詳細と推奨される対処方法が表示されます。

Alert name	Severity	Time triggered	Current values
Low installed node memory 	 Critical	11 hours ago 	Total RAM size: 8.37 GB
The amount of installed memory on a node is low.			

のアラートも含まれます ["ノードの接続状態"](#)。

**[ハードウェア]** タブを表示します

Hardware タブには、各ノードの CPU 利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。



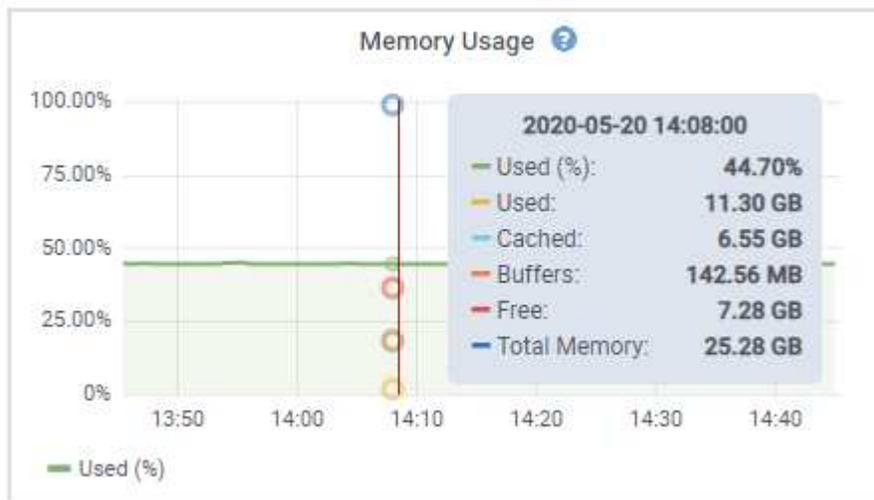
Grid Manager はリリースごとに更新され、このページのスクリーンショットの例とは異なる場合があります。

すべてのノードの Hardware (ハードウェア) タブが表示されます。



別の期間を表示するには、グラフ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、または 1 カ月の期間の情報を表示できます。また、カスタムの間隔を設定して、日時の範囲を指定することもできます。

CPU利用率とメモリ使用率の詳細を確認するには、各グラフにカーソルを合わせます。



ノードがアプライアンスノードの場合は、アプライアンスハードウェアに関する詳細情報を含むセクションも表示されます。

アプライアンスストレージノードに関する情報を表示します

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の健全性と、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、コントローラファームウェアのバージョン、ネットワークリソース、ネットワークインターフェイスも表示されます。ネットワークアドレス、およびデータの送受信。

## 手順

1. ノードページで、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。

Overview タブの Node information 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イス名が含まれます。

- \* 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 \* : アプライアンスの 10、25、または 100GbE の物理ポートの 1 つ。これらのポートをボンディングして、StorageGRID のグリッドネットワーク (eth0) と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 1GbE ポートの 1 つ。1 つ以上の MTC インターフェイスがボンディングされて、StorageGRID 管理ネットワークインターフェイス (eth1) が形成されています。データセンターの技術者がローカルに接続するために、他の MTC インターフェイスを一時的に使用できます。

Overview Hardware Network Storage Objects ILM Tasks

Node information [?](#)

Name: DC2-SGA-010-096-106-021  
 Type: Storage Node  
 ID: f0890e03-4c72-401f-ae92-245511a38e51  
 Connection state: ✔ Connected  
 Storage used: Object data  7% [?](#)  
 Object metadata  5% [?](#)  
 Software version: 11.6.0 (build 20210915.1941.afce2d9)  
 IP addresses: 10.96.106.21 - eth0 (Grid Network)

[Hide additional IP addresses ^](#)

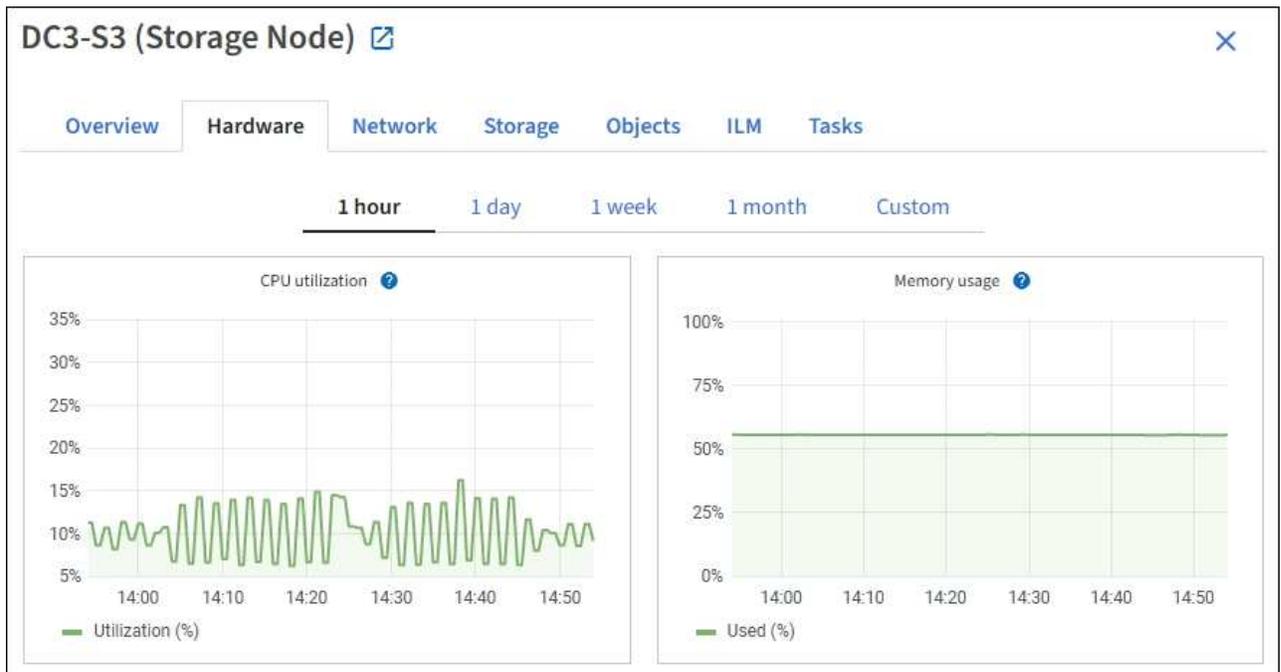
Interface <a href="#">⌵</a>	IP address <a href="#">⌵</a>
eth0 (Grid Network)	10.96.106.21
eth0 (Grid Network)	fe80::2a0:98ff:fe64:6582
hic2	10.96.106.21
hic4	10.96.106.21
mtc2	169.254.0.1

## Alerts

Alert name <a href="#">⌵</a>	Severity <a href="#">?</a> <a href="#">⌵</a>	Time triggered <a href="#">⌵</a>	Current values
<a href="#">ILM placement unachievable</a> <a href="#">🔗</a>	<span style="color: orange;">!</span> Major	2 hours ago <a href="#">?</a>	
A placement instruction in an ILM rule cannot be achieved for certain objects.			

Overview (概要) タブの Alerts (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、「\* Hardware \*」を選択します。
  - a. CPU Utilization および Memory のグラフで、一定期間の CPU およびメモリ使用量の割合を確認します。別の期間を表示するには、グラフ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、または 1 カ月の期間の情報を表示できます。また、カスタムの間隔を設定して、日時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の表を表示します。この表には、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。



Compute Controller BMC IP、Compute hardware などの一部のフィールドは、その機能を持つ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と拡張シェルフが設置に含まれている場合は、アプライアンステーブルの下の個別のテーブルに表示されます。

## StorageGRID Appliance

Appliance model: ?	SG5660	
Storage controller name: ?	StorageGRID-SGA-Lab11	
Storage controller A management IP: ?	10.224.2.192	
Storage controller WWID: ?	600a098000a4a707000000005e8ed5fd	
Storage appliance chassis serial number: ?	1142FG000135	
Storage controller firmware version: ?	08.40.60.01	
Storage hardware: ?	Nominal	
Storage controller failed drive count: ?	0	
Storage controller A: ?	Nominal	
Storage controller power supply A: ?	Nominal	
Storage controller power supply B: ?	Nominal	
Storage data drive type: ?	NL-SAS HDD	
Storage data drive size: ?	2.00 TB	
Storage RAID mode: ?	RAID6	
Storage connectivity: ?	Nominal	
Overall power supply: ?	Nominal	
Compute controller serial number: ?	SV54365519	
Compute controller CPU temperature: ?	Nominal	
Compute controller chassis temperature: ?	Nominal	

## Storage shelves

Shelf chassis serial number ?	Shelf ID ?	Shelf status ?	IOM status ?
SN SV13304553	0	Nominal	N/A

Appliance テーブルのフィールド	説明
アプライアンスのモデル	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 の管理 IP	ストレージコントローラ A 上の管理ポート 1 の IP アドレスこの IP は、ストレージの問題をトラブルシューティングするために SANtricity OS にアクセスする際に使用します。

Appliance テーブルのフィールド	説明
ストレージコントローラ B の管理 IP	<p>ストレージコントローラ B 上の管理ポート 1 の IP アドレスこの IP は、ストレージの問題をトラブルシューティングするために SANtricity OS にアクセスする際に使用します。</p> <p>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 が搭載されていません</p>
ストレージコントローラ WWID	SANtricity OS に表示されるストレージコントローラの World-Wide Identifier。
ストレージアプライアンスの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。
ストレージハードウェア	<p>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 からストレージハードウェアの要注意のステータスが報告された場合、StorageGRID システムからも報告されます。</p> <p>ステータスが「Needs Attention」の場合は、まず SANtricity OS を使用してストレージコントローラを確認します。次に、コンピューティングコントローラに関するアラームが他にないことを確認します。</p>
ストレージコントローラの障害ドライブ数	最適な状態でないドライブの数。
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 が搭載されていません
ストレージコントローラの電源装置 A	ストレージコントローラの電源装置 A のステータス。
ストレージコントローラの電源装置 B	ストレージコントローラの電源装置 B のステータス。
ストレージデータドライブのタイプ	アプライアンス内のドライブのタイプ。HDD（ハードドライブ）や SSD（ソリッドステートドライブ）など。

Appliance テーブルのフィールド	説明
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実効サイズ。  • 注：拡張シェルフを使用するノードの場合は、を使用してください <a href="#">各シェルフのデータドライブのサイズ</a> 代わりに、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	ストレージ接続の状態。
電源装置全体	アプライアンスのすべての電源装置のステータス。
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内の Baseboard Management Controller (BMC ; ベースボード管理コントローラ) 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を搭載していないアプライアンスモデルに対しては表示されません。
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途用意されていないアプライアンスモデルに対しては表示されません。
コントローラの CPU 温度を計算します	コンピューティングコントローラの CPU の温度ステータス。
コントローラシャーシの温度を計算します	コンピューティングコントローラの温度ステータス。

+

ストレージシェルフテーブルの列	説明
シェルフ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。

ストレージシェルフテーブルの列	説明
シェルフ ID	<p>ストレージシェルフの数値識別子。</p> <ul style="list-style-type: none"> <li>• 99 : ストレージコントローラシェルフ</li> <li>• 0 : 最初の拡張シェルフ</li> <li>• 1 : 2 台目の拡張シェルフ</li> </ul> <p>*注: *拡張シェルフはSG6060およびSG6160にのみ適用されます。</p>
シェルフステータス	ストレージシェルフの全体的なステータス。
IOM のステータス	拡張シェルフ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 。
電源装置ステータス	ストレージシェルフの電源装置の全体的なステータス。
ドロワーステータス	ストレージシェルフのドロワーのステータス。N/A は、シェルフにドロワーが搭載されていない場合。
ファンのステータス	ストレージシェルフの冷却ファンの全体的なステータス。
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総数。
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。
[[shelf_data_drive_size]] 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実効サイズ。
キャッシュドライブ	ストレージシェルフ内の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で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のサイズはすべて同じです。
設定ステータス	ストレージシェルフの設定ステータス。

- a. すべてのステータスが「Nominal」であることを確認します。

ステータスが「Nominal」でない場合は、現在のアラートを確認します。SANtricity System Manager を使用して、これらのハードウェアの値の一部を確認することもできます。アプライアンスの設置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。

Network Traffic グラフには、ネットワークトラフィック全体のサマリが表示されます。



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	00:50:56:A7:66:75	10 Gigabit	Full	Off	Up	

次の表に、Network Interfaces テーブルの \* Speed \* 列の値を記載した値を使用して、アプライアンス上の 10 / 25GbE 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設定されているかを判断します。

**i** この表の値は、4つのリンクがすべて使用されていることを前提としています。

リンクモード	ボンディングモード	個々の HIC リンク速度 ( hic1、 hic2、hic3、hic4 )	想定されるグリッド/ クライアントネットワ ーク速度 ( eth0、 eth2 )
アグリゲート	LACP	25	100
固定 ( Fixed )	LACP	25	50です
固定 ( Fixed )	アクティブ / バックアッ プ	25	25
アグリゲート	LACP	10	40
固定 ( Fixed )	LACP	10	20
固定 ( Fixed )	アクティブ / バックアッ プ	10	10

を参照してください "ネットワークリンクを設定する" 10 / 25GbEポートの設定の詳細については、  
を参照してください。

b. 「ネットワーク通信」セクションを確認します。

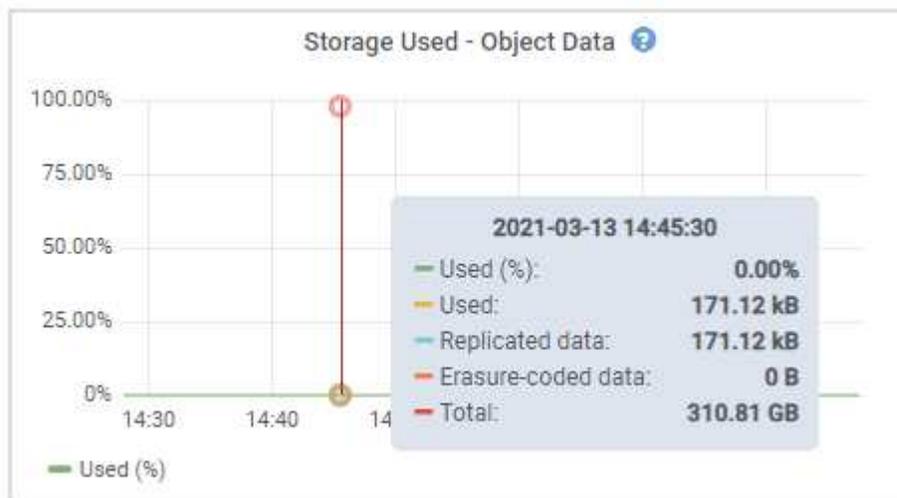
Receive テーブルと Transmit テーブルには、各ネットワークで送受信されたバイト数とパケット数、  
およびその他の送受信メトリックが表示されます。

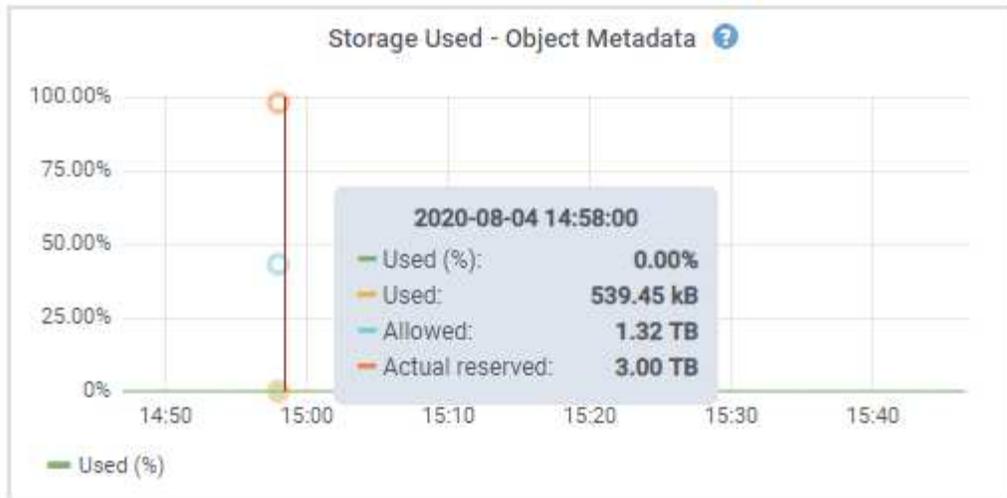
Network communication							
Receive							
Interface	Data	Packets	Errors	Dropped	Frame overruns	Frames	
eth0	2.89 GB	19,421,503	0	24,032	0	0	

Transmit							
Interface	Data	Packets	Errors	Dropped	Collisions	Carrier	
eth0	3.64 GB	18,494,381	0	0	0	0	

5. 「\* Storage \*」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使用されているストレージの割合、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がグラフに表示されます。





- a. 下にスクロールして、各ボリュームとオブジェクトストアに使用可能なストレージ容量を表示します。

各ディスクのWorldwide Name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ている管理ソフトウェア）で標準のボリュームプロパティとして表示されるボリュームのWorld-Wide Identifier（WWID）と同じです。

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と書き込みの統計情報を解釈できるように、Disk Devices テーブルの \* Name \* 列に表示される名前の最初の部分（つまり、*sdc\_sd,sde*）が Volumes テーブルの \* Device \* 列に表示される値と一致していることを確認します。

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

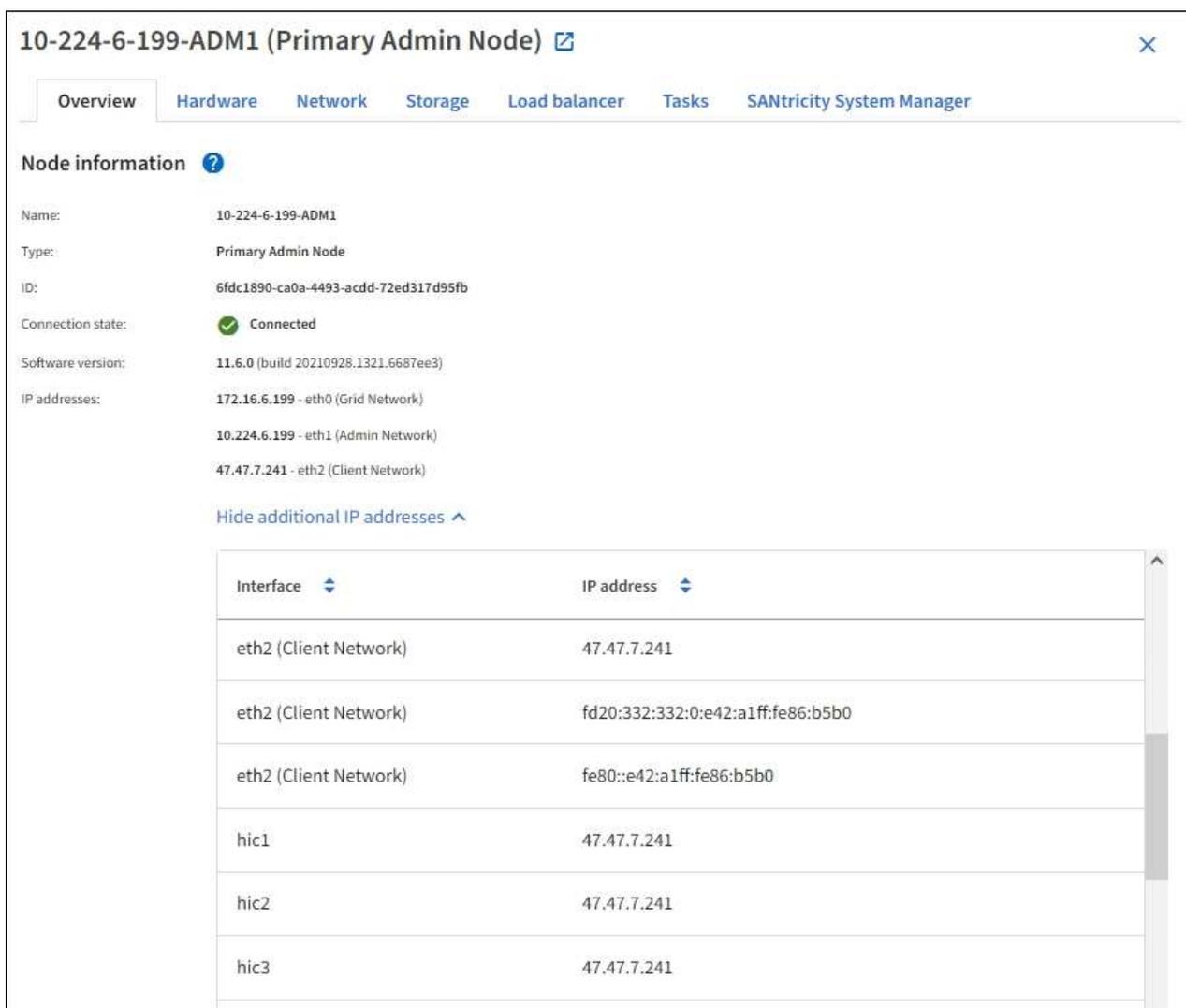
ノードページには、管理ノードまたはゲートウェイノードとして使用される各サービスアプライアンスのサービスの健全性とすべてのコンピューティング、ディスクデバイス、およびネットワークリソースに関する情報が表示されます。メモリ、ストレージハードウェア、ネットワークリソース、ネットワークインターフェイス、ネットワークアドレスも表示できます。データを送受信します。

手順

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

Overview タブの Node information 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イス名が含まれます。

- \* adllb \* および \* adlli \* : 管理ネットワーク・インターフェイスでアクティブ / 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 \* : アプライアンスの 10、25、または 100GbE の物理ポートの 1 つ。これらのポートをボンディングして、StorageGRID のグリッドネットワーク (eth0) と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 1GbE ポートの 1 つ。1 つ以上の MTC インターフェイスがボンディングされて、管理ネットワークインターフェイス (eth1) が形成されています。データセンターの技術者がローカルに接続するために、他の MTC インターフェイスを一時的に使用できます。



10-224-6-199-ADM1 (Primary Admin Node) [🔗](#) ✕

Overview Hardware Network Storage Load balancer Tasks SANtricity System Manager

**Node information** ?

Name: 10-224-6-199-ADM1  
Type: Primary Admin Node  
ID: 6fdc1890-ca0a-4493-acdd-72ed317d95fb  
Connection state: ✔ Connected  
Software version: 11.6.0 (build 20210926.1321.6687ee3)  
IP addresses: 172.16.6.199 - eth0 (Grid Network)  
10.224.6.199 - eth1 (Admin Network)  
47.47.7.241 - eth2 (Client Network)

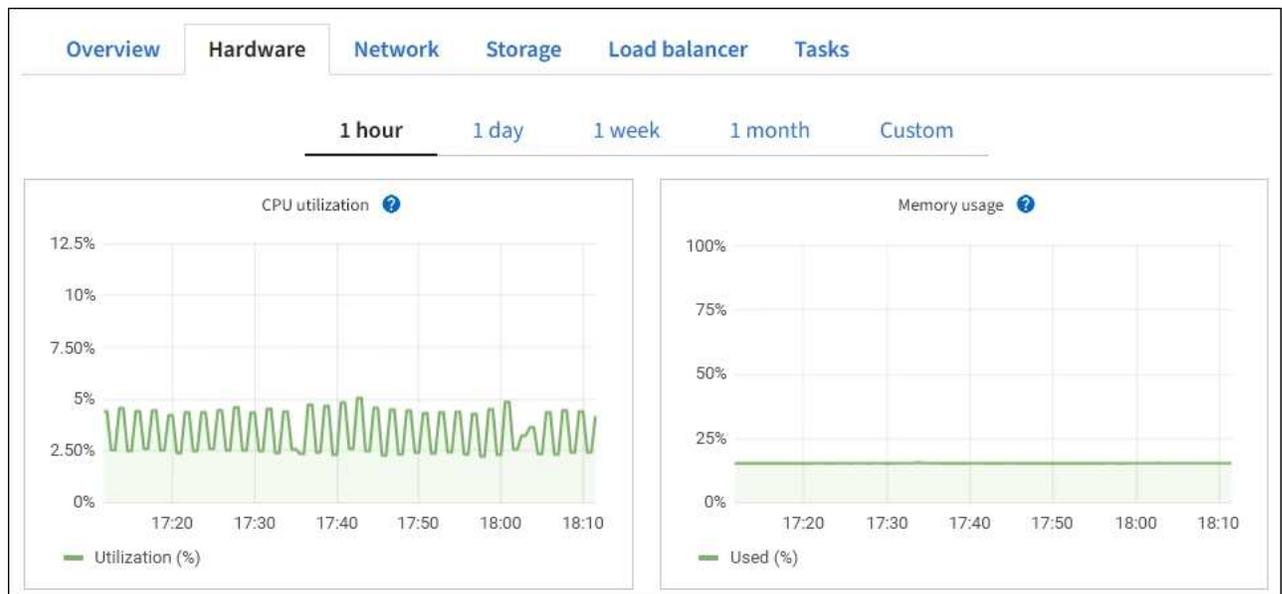
[Hide additional IP addresses](#) ^

Interface	IP address
eth2 (Client Network)	47.47.7.241
eth2 (Client Network)	fd20:332:332:0:e42:a1ff:fe86:b5b0
eth2 (Client Network)	fe80::e42:a1ff:fe86:b5b0
hic1	47.47.7.241
hic2	47.47.7.241
hic3	47.47.7.241

Overview (概要) タブの Alerts (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、「\* Hardware \*」を選択します。
  - a. CPU Utilization および Memory のグラフで、一定期間の CPU およびメモリ使用量の割合を確認しま

す。別の期間を表示するには、グラフ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、または 1 カ月の期間の情報を表示できます。また、カスタムの間隔を設定して、日時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の表を表示します。この表には、モデル名、シリアル番号、コントローラファームウェアのバージョン、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。

### StorageGRID Appliance

Appliance model: ?	SG100	
Storage controller failed drive count: ?	0	
Storage data drive type: ?	SSD	
Storage data drive size: ?	960.20 GB	
Storage RAID mode: ?	RAID1 [healthy]	
Storage connectivity: ?	Nominal	
Overall power supply: ?	Nominal	
Compute controller BMC IP: ?	10.60.8.38	
Compute controller serial number: ?	372038000093	
Compute hardware: ?	Nominal	
Compute controller CPU temperature: ?	Nominal	
Compute controller chassis temperature: ?	Nominal	
Compute controller power supply A: ?	Nominal	
Compute controller power supply B: ?	Nominal	

Appliance テーブルのフィールド	説明
アプライアンスのモデル	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	最適な状態でないドライブの数。
ストレージデータドライブのタイプ	アプライアンス内のドライブのタイプ。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実効サイズ。
ストレージ RAID モード	アプライアンスの RAID モード。
電源装置全体	アプライアンスのすべての電源装置のステータス。
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内の Baseboard Management Controller（BMC；ベースボード管理コントローラ）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、アプライアンスハードウェアを監視および診断することができます。  このフィールドは、BMCを搭載していないアプライアンスモデルに対しては表示されません。
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ハードウェアのステータス。
コントローラの CPU 温度を計算します	コンピューティングコントローラの CPU の温度ステータス。
コントローラシャーシの温度を計算します	コンピューティングコントローラの温度ステータス。

a. すべてのステータスが「Nominal」であることを確認します。

ステータスが「Nominal」でない場合は、現在のアラートを確認します。

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。

Network Traffic グラフには、ネットワークトラフィック全体のサマリが表示されます。



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	

次の表のネットワークインターフェイスの表の「\* Speed \*」列の値を使用して、アプライアンス上の4つの40/100GbE 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設定されているかを確認してください。



この表の値は、4つのリンクがすべて使用されていることを前提としています。

リンクモード	ボンディングモード	個々の HIC リンク速度 ( hic1、 hic2、 hic3、 hic4 )	想定されるグリッド/ クライアントネットワ ーク速度 ( eth0、 eth2 )
アグリゲート	LACP	100	400
固定 ( Fixed )	LACP	100	200
固定 ( Fixed )	アクティブ/バックアッ プ	100	100
アグリゲート	LACP	40	一六〇
固定 ( Fixed )	LACP	40	80
固定 ( Fixed )	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。

受信および送信テーブルには、各ネットワークで送受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。

Network communication							
Receive							
Interface	Data	Packets	Errors	Dropped	Frame overruns	Frames	
eth0	2.89 GB	19,421,503	0	24,032	0	0	
Transmit							
Interface	Data	Packets	Errors	Dropped	Collisions	Carrier	
eth0	3.64 GB	18,494,381	0	0	0	0	

5. サービス・アプライアンス上のディスク・デバイスおよびボリュームに関する情報を表示するには、「\* Storage \*」を選択します。

[Overview](#)[Hardware](#)[Network](#)[Storage](#)[Load balancer](#)[Tasks](#)

## Disk devices

Name <a href="#">?</a> <a href="#">↕</a>	World Wide Name <a href="#">?</a> <a href="#">↕</a>	I/O load <a href="#">?</a> <a href="#">↕</a>	Read rate <a href="#">?</a> <a href="#">↕</a>	Write rate <a href="#">?</a> <a href="#">↕</a>
croot(8:1,sda1)	N/A	0.02%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.03%	0 bytes/s	6 KB/s

## Volumes

Mount point <a href="#">?</a> <a href="#">↕</a>	Device <a href="#">?</a> <a href="#">↕</a>	Status <a href="#">?</a> <a href="#">↕</a>	Size <a href="#">?</a> <a href="#">↕</a>	Available <a href="#">?</a> <a href="#">↕</a>	Write cache status <a href="#">?</a> <a href="#">↕</a>
/	croot	Online	21.00 GB	14.73 GB 	Unknown
/var/local	cvloc	Online	85.86 GB	84.63 GB 	Unknown

[ ネットワーク ] タブを表示します

Network 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送受信されたネットワークトラフィックがグラフで表示されます。

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

別の期間を表示するには、グラフ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、または 1 カ月の期間の情報を表示できます。また、カスタムの間隔を設定して、日時の範囲を指定することもできます。

ノードの場合、各ノードの物理ネットワークポートに関する情報がネットワークインターフェイスの表に表示されます。ネットワーク通信テーブルには、各ノードの送受信処理の詳細と、ドライバから報告された障害カウンタが表示されます。

# DC1-S2 (Storage Node)

Overview

Hardware

Network

Storage

Objects

ILM

Tasks

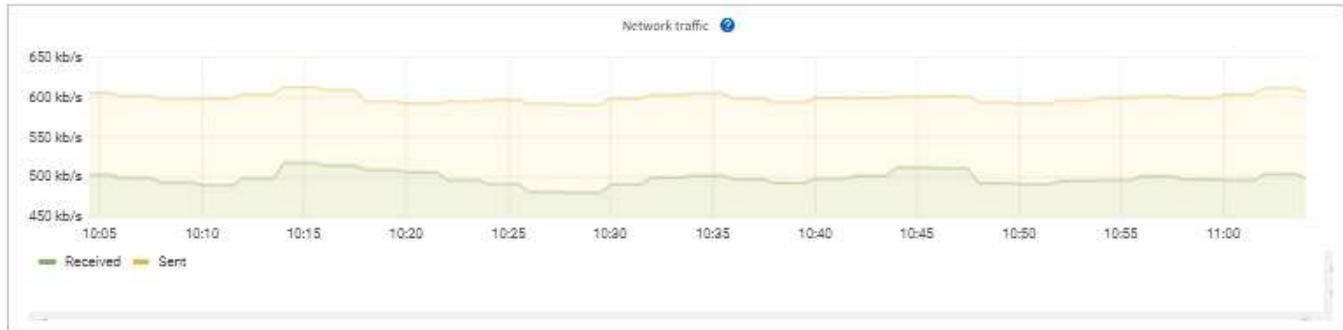
1 hour

1 day

1 week

1 month

Custom



## Network interfaces

Name	Hardware address	Speed	Duplex	Auto-negotiation	Link status
eth0	00:50:56:A7:E8:1D	10 Gigabit	Full	Off	Up

## Network communication

### Receive

Interface	Data	Packets	Errors	Dropped	Frame overruns	Frames
eth0	3.04 GB	20,403,428	0	24,899	0	0

### Transmit

Interface	Data	Packets	Errors	Dropped	Collisions	Carrier
eth0	3.65 GB	19,061,947	0	0	0	0

## 関連情報

"ネットワーク接続とパフォーマンスを監視します"

**Storage** (ストレージ) タブを表示します

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指標が表示されます。

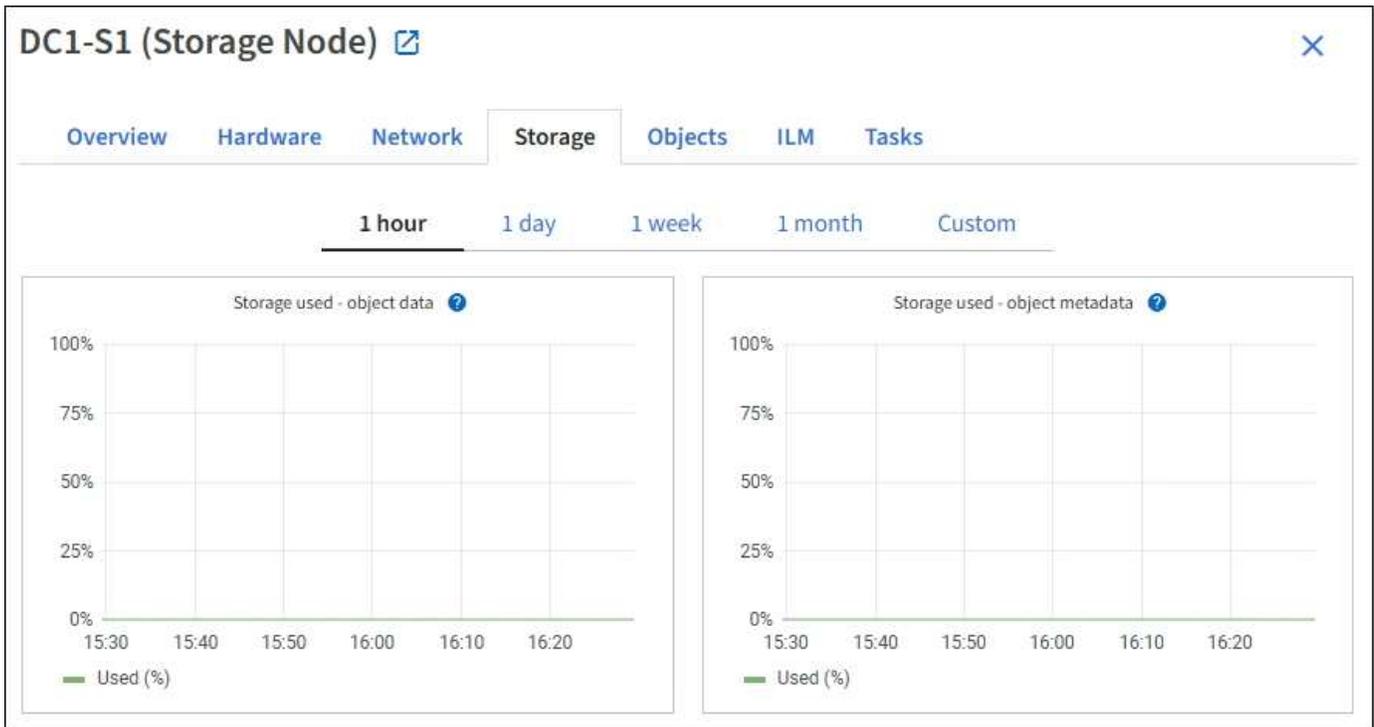
ストレージタブは、すべてのノード、各サイト、およびグリッド全体に対して表示されます。

## Storage Used グラフ

ストレージノード、各サイト、およびグリッド全体が対象である場合は、オブジェクトデータとオブジェクトメタデータで一定期間にわたって使用されているストレージの量を示すグラフがストレージタブに表示されません。



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は、特定の指標が使用できないか、サイトおよびグリッドの合計値から除外されることがあります。ノードがグリッドに再接続されたら、値が安定するまで数分待ちます。



ディスクデバイス、ボリューム、およびオブジェクトはテーブルを格納します

すべてのノードが対象である場合は、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、Object Stores テーブルに各ストレージボリュームの情報が表示されます。

## 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

## 関連情報

["ストレージ容量を監視"](#)

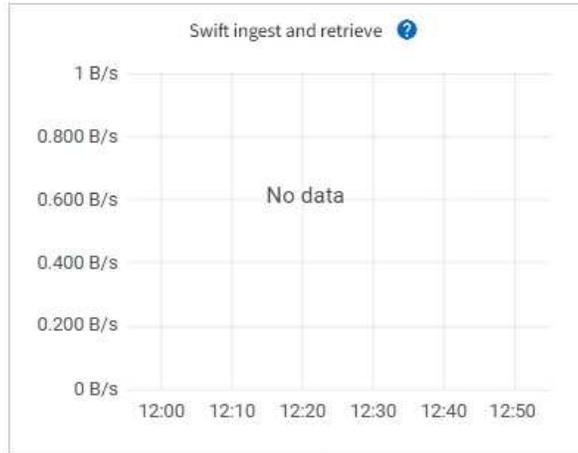
[ オブジェクト ] タブを表示します

[ オブジェクト ] タブには、に関する情報が表示されます "S3" および "Swift" 取り込み速度と読み出し速度の関係です。

各ストレージノード、各サイト、およびグリッド全体のオブジェクトタブが表示されます。ストレージノードが対象である場合は、オブジェクト数や、メタデータクエリやバックグラウンド検証に関する情報も表示されます。

Overview Hardware Network Storage **Objects** ILM Tasks

**1 hour** 1 day 1 week 1 month Custom



### 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 タブを表示します

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

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 ILM タブが表示されます。各サイトおよびグリッドが対象である場合は、ILM キューの状況の推移を示すグラフがこのタブに表示されます。グリッドが対象である場合は、ILM によるすべてのオブジェクトのフルスキャンが完了するまでの推定時間も表示されます。

ストレージノードが対象である場合は、ILM評価とイレイジャーコーディングオブジェクトのバックグラウンド検証の詳細が表示されます。

## DC2-S1 (Storage Node) [🔗](#)

[Overview](#) [Hardware](#) [Network](#) [Storage](#) [Objects](#) **ILM** [Tasks](#)

### Evaluation

Awaiting - all: <a href="#">?</a>	0 objects	
Awaiting - client: <a href="#">?</a>	0 objects	
Evaluation rate: <a href="#">?</a>	0.00 objects / second	
Scan rate: <a href="#">?</a>	0.00 objects / second	

### Erasure coding verification

Status: <a href="#">?</a>	Idle	
Next scheduled: <a href="#">?</a>	2021-09-09 17:36:44 MDT	
Fragments verified: <a href="#">?</a>	0	
Data verified: <a href="#">?</a>	0 bytes	
Corrupt copies: <a href="#">?</a>	0	
Corrupt fragments: <a href="#">?</a>	0	
Missing fragments: <a href="#">?</a>	0	

関連情報

["情報ライフサイクル管理を監視"](#)

["StorageGRID の管理"](#)

## [タスク]タブの使用

[Tasks]タブはすべてのノードに対して表示されます。このタブを使用して、ノードの名前変更やリブート、アプライアンスノードのメンテナンスモードへの切り替えを行うことができます。

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、次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します"
- "グリッドノードをリブートします"
- "アプライアンスをメンテナンスモードにします"

## [Load balancer]タブを表示します

ロードバランサのタブには、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表示されます。

管理ノードとゲートウェイノード、各サイト、およびグリッド全体が対象の場合は、ロードバランサのタブが表示されます。各サイトが対象である場合は、そのサイトのすべてのノードの統計が要約して表示されます。グリッド全体が対象である場合は、すべてのサイトの統計が要約して表示されます。

ロードバランササービスでI/Oが実行されていない場合やロードバランサが設定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。



トラフィックを要求します

このグラフには、ロードバランサエンドポイントと要求を行っているクライアントの間に送信されたデータのスループットの 3 分間の移動平均が、1 秒あたりのビット数で示されます。



この値は、各要求が完了した時点で更新されます。そのため、要求数が少ない場合や要求の実行時間が非常に長い場合は、リアルタイムのスループットと異なる場合があります。[ネットワーク] タブを見ると、現在のネットワーク動作をよりリアルに表示できます。

受信要求レート

このグラフには、1 秒あたりの新しい要求数の 3 分間の移動平均が、要求タイプ（GET、PUT、HEAD、DELETE）別に示されます。この値は、新しい要求のヘッダーが検証されると更新されます。

平均リクエスト時間（エラーなし）

このグラフには、要求期間の 3 分間の移動平均が、要求タイプ（GET、PUT、HEAD、DELETE）別に示されます。要求期間は、要求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時点から始まり、完全な応答本文がクライアントに返された時点で終了します。

## エラー応答速度

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

## 関連情報

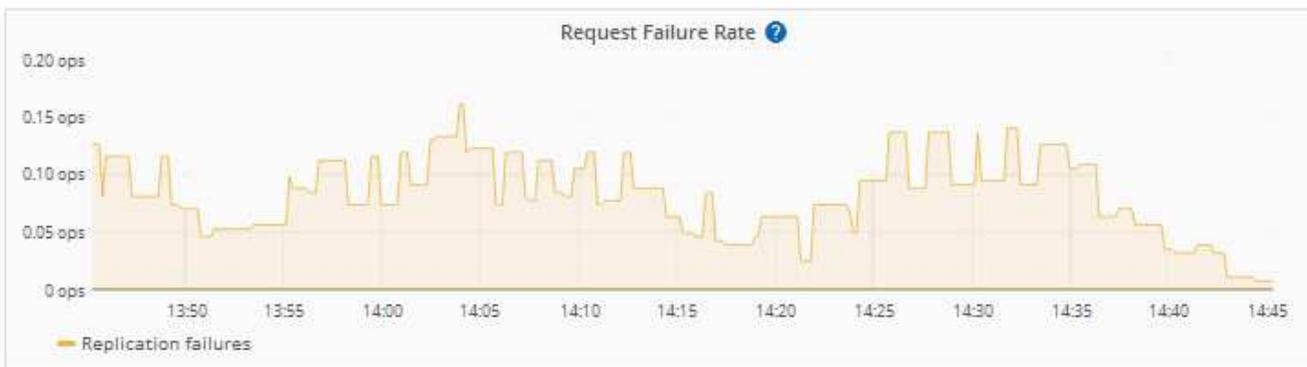
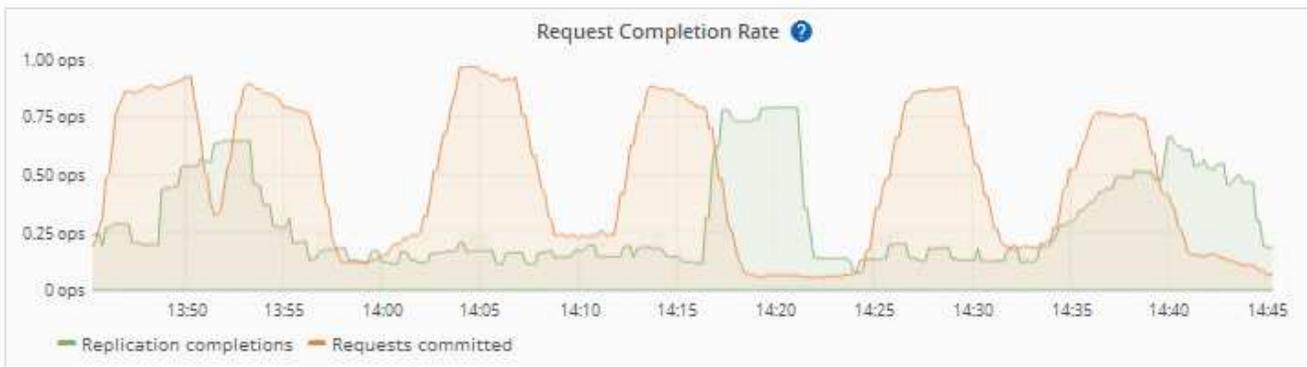
["ロードバランシング処理を監視する"](#)

["StorageGRID の管理"](#)

プラットフォームサービスタブを表示します

プラットフォームサービスタブには、サイトでの S3 プラットフォームサービスの処理に関する情報が表示されます。

各サイトの [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、保留中の要求数、要求の完了率、要求の失敗率などの指標が表示されます。



トラブルシューティングの詳細など、S3プラットフォームサービスの詳細については、[を参照してください](#) "StorageGRIDの管理手順"。

**[Manage Drives]**タブを表示 (SGF6112のみ)

[Manage Drives]タブでは、SGF6112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とメンテナンスのタスクを実行できます。



[Manage Drives]タブは、SGF6112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せん。

[ドライブの管理]タブでは、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する
- 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、シリアル番号が一覧表示された表を表示する
- 各ドライブでトラブルシューティング機能とメンテナンス機能を実行する

[Manage Drives]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Root Access権限](#)"。

[ドライブの管理]タブの使用方法については、[を参照してください。 "\[ドライブの管理\]タブを使用する"](#)。

### SANtricityの[System Manager]タブの表示（Eシリーズのみ）

SANtricity の System Manager タブから、ストレージアプライアンスの管理ポートを設定したり接続したりしなくても、SANtricity の System Manager にアクセスできます。このタブでは、ハードウェア診断と環境情報、およびドライブに関連する問題を確認できます。



SANtricity の[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 システムマネージャを使用すると、次の操作を実行できます。

- ストレージ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のCPU利用率、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、EシリーズAutoSupport の設定など、サポート機能を実行する。



SANtricity System Managerを使用してEシリーズAutoSupport のプロキシを設定する方法については、[を参照してください "StorageGRID経由でEシリーズAutoSupportパッケージを送信"](#)。

グリッドマネージャから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Root Access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 以降が必要です。



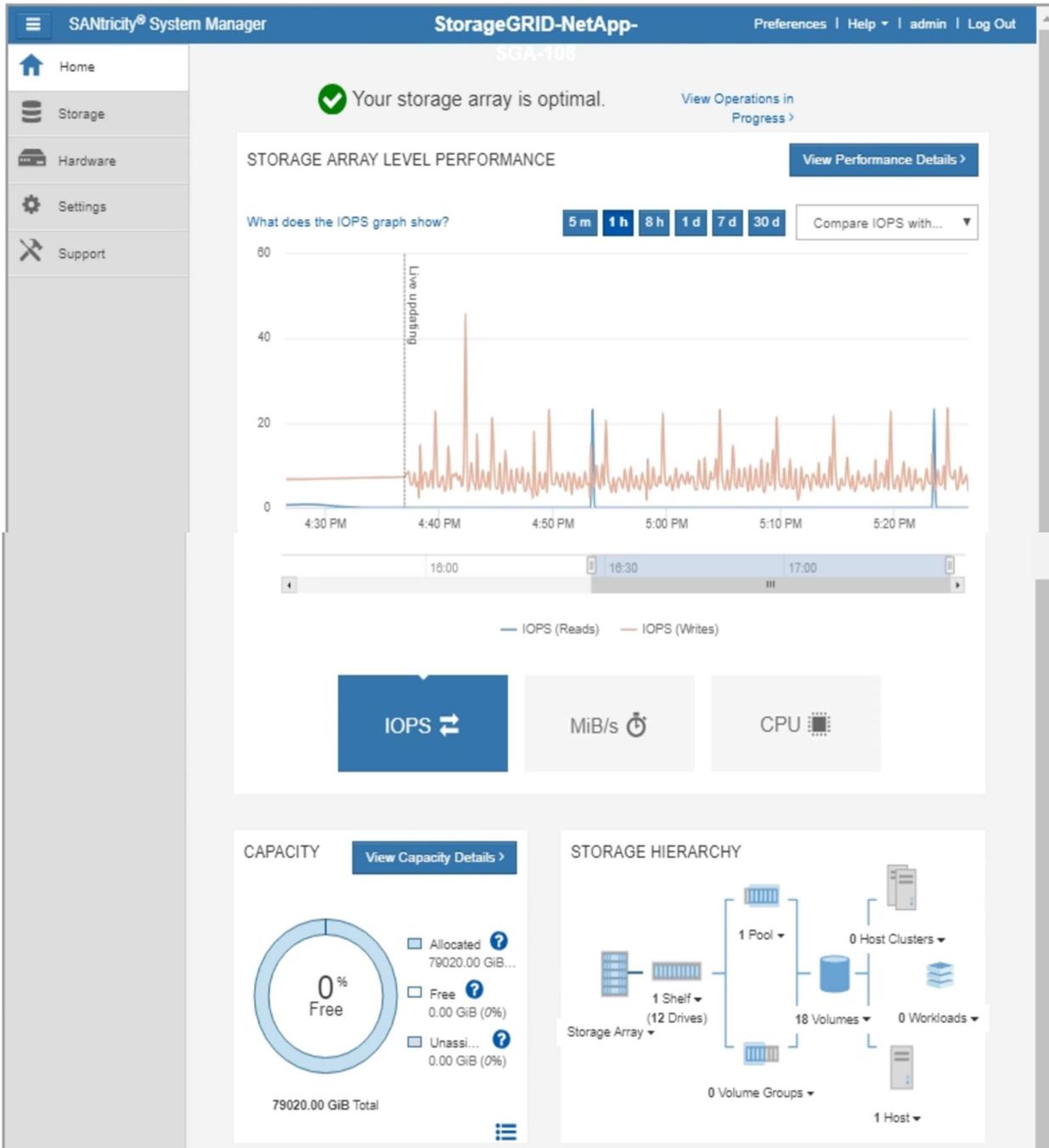
グリッドマネージャから SANtricity システムマネージャにアクセスする手順は、通常、アプライアンスのハードウェアを監視し、Eシリーズ AutoSupport を設定することだけを目的としています。ファームウェアのアップグレードなど、SANtricity System Managerの多くの機能や操作は、StorageGRID アプライアンスの監視には適用されません。問題を回避するために、必ずアプライアンスのハードウェアメンテナンス手順に従ってください。

このタブには、SANtricity システムマネージャのホームページが表示されます。

Use SANtricity System Manager to monitor and manage the hardware components in this storage appliance. From SANtricity System Manager, you can review hardware diagnostic and environmental information as well as issues related to the drives.

**Note:** Many features and operations within SANtricity Storage Manager do not apply to your StorageGRID appliance. To avoid issues, always follow the hardware installation and maintenance instructions for your appliance model.

Open [SANtricity System Manager](#) in a new browser tab.



SANtricity System Manager の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いて確認しやすくなります。

ストレージアレイレベルのパフォーマンスと使用容量の詳細を確認するには、各グラフにカーソルを合わせま

す。

SANtricity の 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、を参照してください ["NetApp E シリーズおよび SANtricity に関するドキュメント"](#)。

## 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 システムは引き続き動作しますが、潜在的な問題がグリッドの効率や可用性に影響する前に監視して対処する必要があります。

作業を開始する前に

- を使用して Grid Manager にサインインします ["サポートされている Web ブラウザ"](#)。
- これで完了です ["特定のアクセス権限"](#)。

タスクの監視について

ビジーシステムでは大量の情報が生成されます。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関するガイダンスを示しています。

監視対象	頻度
<a href="#">"システムヘルスステータス"</a>	毎日
レート <a href="#">"ストレージノードのオブジェクトとメタデータの容量"</a> が使用されています	毎週
<a href="#">"情報ライフサイクル管理のオペレーション"</a>	毎週
<a href="#">"ネットワークおよびシステムリソース"</a>	毎週
<a href="#">"テナントのアクティビティ"</a>	毎週
<a href="#">"S3およびSwiftクライアント処理"</a>	毎週
<a href="#">"ロードバランシング操作"</a>	初期設定後と設定の変更後
<a href="#">"グリッドフェデレーション接続"</a>	毎週
<a href="#">"外部アーカイブストレージシステムの容量"</a>	毎週

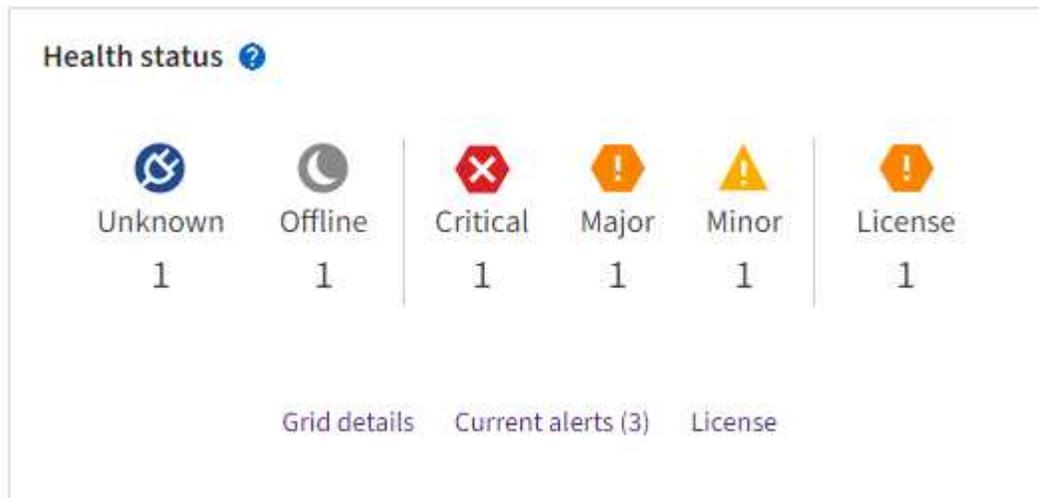
システムヘルスを監視する

StorageGRID システム全体の健全性を毎日監視します。

このタスクについて

StorageGRID システムは、グリッドの一部が使用できない場合でも動作を継続できます。アラートやアラーム（従来のシステム）によって示される潜在的な問題が、必ずしもシステムの処理に問題があるとは限りません。Grid Managerのダッシュボードの[Health]ステータスカードにまとめられた問題を調査します。

アラートがトリガーされるとすぐに通知されるようにすることができます ["アラートのEメール通知を設定する"](#) または ["SNMPトラップを設定します"](#)。



問題が発生している場合は、詳細を確認できるリンクが表示されます。

リンク	表示される状況
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UnknownまたはAdministratively Down）。
現在のアラート（Critical、Major、Minor）	アラートはです <a href="#">現在アクティブです</a> 。
最近解決したアラート	過去1週間にトリガーされたアラート <a href="#">解決されました</a> 。
使用許諾	このStorageGRID システムには、ソフトウェアライセンスが付属した問題 <a href="#">があります</a> 。可能です <a href="#">"必要に応じてライセンス情報を更新します"</a> 。

ノードの接続状態を監視します

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 処理に影響する可能性があります。ノードの接続状態を監視し、問題があれば迅速に対処します。

をクリックします。	説明	アクションが必要です
	<ul style="list-style-type: none"> <li>• 接続されていません - 不明 *</li> </ul> <p>理由が不明な場合、ノードが切断されているか、ノードのサービスが予期せず停止しています。たとえば、ノードのサービスが停止したり、電源障害や予期しない停止によってノードのネットワーク接続が失われたりする場合があります。</p> <ul style="list-style-type: none"> <li>• Unable to communicate with node * アラートがトリガーされる場合もあります。他のアラートもアクティブになる可能性があります。</li> </ul>	<p>アクションが必要です</p> <p>すぐに対処する必要があります。 <a href="#">各アラートを選択します</a> そして推奨される行動に従ってください。</p> <p>たとえば、ノードのホストを停止または再起動したサービスの再起動が必要になることがあります。</p> <p>注：管理されたシャットダウン処理の実行中は、ノードがUnknownと表示されることがあります。このような場合、Unknown 状態は無視してかまいません。</p>
	<ul style="list-style-type: none"> <li>• 接続されていません - 管理上の理由により停止して</li> </ul> <p>想定される理由により、ノードがグリッドに接続されていません。</p> <p>たとえば、ノードまたはノード上のサービスが正常にシャットダウンされた、ノードがリブート中である、ソフトウェアのアップグレード中であるなどの原因が考えられます。1つ以上のアラートがアクティブになっている可能性もあります。</p> <p>基盤となる問題に基づいて、これらのノードは多くの場合、介入なしでオンラインに戻ります。</p>	<p>このノードに影響しているアラートがないかどうかを確認します。</p> <p>アクティブなアラートがある場合は、 <a href="#">各アラートを選択します</a> そして推奨される行動に従ってください。</p>
	<ul style="list-style-type: none"> <li>• 接続済み *</li> </ul> <p>ノードがグリッドに接続されます。</p>	<p>対処は不要です。</p>

現在のアラートと解決済みのアラートを表示します

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。ノードに関するアラートアイコンは、ノードページにも表示されます。状況 ["アラートEメール通知が設定されました"](#)アラートをサイレント化していないかぎり、E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。

必要に応じて、次のビデオを視聴しました。 ["ビデオ：StorageGRID 11.8のアラートの概要"](#)



次の表に、Grid Manager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を示します。

列ヘッダー	説明
名前またはタイトル	アラートの名前と概要。
重大度	<p>アラートの重大度。現在のアラートで複数のアラートがグループ化されている場合は、各重大度で発生しているアラートのインスタンス数がタイトル行に表示されます。</p> <p> <b>重大</b>：異常な状態で、StorageGRID ノードまたはサービスの正常な動作が停止しました。基盤となる問題にすぐに対処する必要があります。問題が解決されないと、サービスの停止やデータの損失を招くおそれがあります。</p> <p> <b>Major</b>:現在の動作に影響しているか、重大アラートのしきい値に近づいている異常な状態です。Major アラートを調査し、根本的な問題に対処して、異常な状態が発生した場合に StorageGRID のノードやサービスが正常に動作しなくなる事態を防ぐ必要があります。</p> <p> <b>* Minor *</b>：システムは正常に動作していますが、異常な状態が発生しているため、システムの動作に影響する可能性があります。自動的にクリアされないMinorアラートを監視して解決し、重大な問題が発生しないようにする必要があります。</p>
トリガーされた時刻	<p>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は、タイトル行にアラートの最新のインスタンス（<code>_newnewest_</code>）と最も古いインスタンス（<code>_oldest_</code>）の時間が表示されます。</p> <p>解決済みアラート：アラートがトリガーされてからの時間。</p>
サイト / ノード	アラートが発生している、または発生している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か、サイレント化されているか、解決されているか。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、サイレント化された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（解決済みアラートのみ）	アラートが解決されてからの時間。
現在の値または_data値_	アラートをトリガーした指標の値。一部のアラートでは、アラートの理解と調査に役立つ値が追加で表示されます。たとえば、Low object data storage * アラートには、使用されているディスクスペースの割合、ディスクスペースの総容量、使用されているディスクスペースの容量の値が表示されます。  *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（解決済みのアラートのみ）	アラートをトリガーした指標の値。一部のアラートでは、アラートの理解と調査に役立つ値が追加で表示されます。たとえば、Low object data storage * アラートには、使用されているディスクスペースの割合、ディスクスペースの総容量、使用されているディスクスペースの容量の値が表示されます。

## 手順

1. または[解決済みのアラート]の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。また、Nodes > \***node**> \* Overview \* を選択し、[Alerts]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。

- 最後に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が1つのグループとして表示されます。
- サイレント化されたアラートは表示されません。
- 特定のノードの特定のアラートが複数の重大度のしきい値に達した場合は、最も重大度の高いアラートのみが表示されます。つまり、アラートが Minor、Major、Critical の各重大度のしきい値に達した場合は、Critical アラートのみが表示されます。

[Current alerts]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、下キャレットを選択します ▼。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、\*[Group alerts]\*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ソートするには、上下の矢印を選択します ⬆️ ⬆️ をクリックします。
  - 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ソートされます。たとえば、グループ内のアラートを「時間トリガー」でソートして、特定のアラートの最新のインスタンスを確認できます。
  - [Group alerts]\*をオフにすると、アラートのリスト全体がソートされます。たとえば、すべてのアラートを \* Node/Site \* でソートして、特定のノードに影響しているすべてのアラートを表示できます。
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\*サイレント\*）でフィルタリングするには、テーブルの上部にあるドロップダウンメニューを使用します。

を参照してください ["アラート通知をサイレント化する"](#)。

6. 解決済みのアラートをソートするには：

- [When triggered]\* 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。
- [\* アラートルール \* (\* Alert rule \*) ] 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て、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リングします。
- 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て、特定のノードに関連する解決済みアラートをフィルタします。

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。選択したアラートの詳細と推奨される対処方法がダイアログボックスに表示されます。

8. (オプション) 特定のアラートの[Silence this alert]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サイレント化します。

を用意しておく必要があります ["アラートまたはRoot Access権限を管理します。"](#) をクリックしてアラートルールをサイレント化します。



アラートルールをサイレント化する場合は注意が必要です。アラートルールがサイレント化されている場合、重大な処理が完了しないかぎり、根本的な問題が検出されないことがあります。

9. アラートルールの現在の条件を表示するには、次の手順を実行します。

- a. アラートの詳細から、\*[条件の表示]\*を選択します。

定義されている各重大度の Prometheus 式がポップアップに表示されます。

- 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。

を用意しておく必要があります ["アラートまたはRoot Access権限を管理します。"](#) をクリックして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が必要です。トリガー値を変更した場合、重大な処理を完了できなくなるまで、根本的な問題が検出されないことがあります。

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

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ようにします。

StorageGRID は、オブジェクトデータとオブジェクトメタデータを別々に格納し、オブジェクトメタデータを含む分散 Cassandra データベース用に一定量のスペースをリザーブします。オブジェクトとオブジェクトメタデータ用に消費されるスペースの合計量のほか、それぞれで消費されるスペース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できます。

可能です "ストレージ容量の情報を表示します" 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。

グリッド全体のストレージ容量を監視します

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用に十分な空きスペースが残っていることを確認します。時間の経過に伴うストレージ容量の変化を理解しておく、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際に役立ちます。

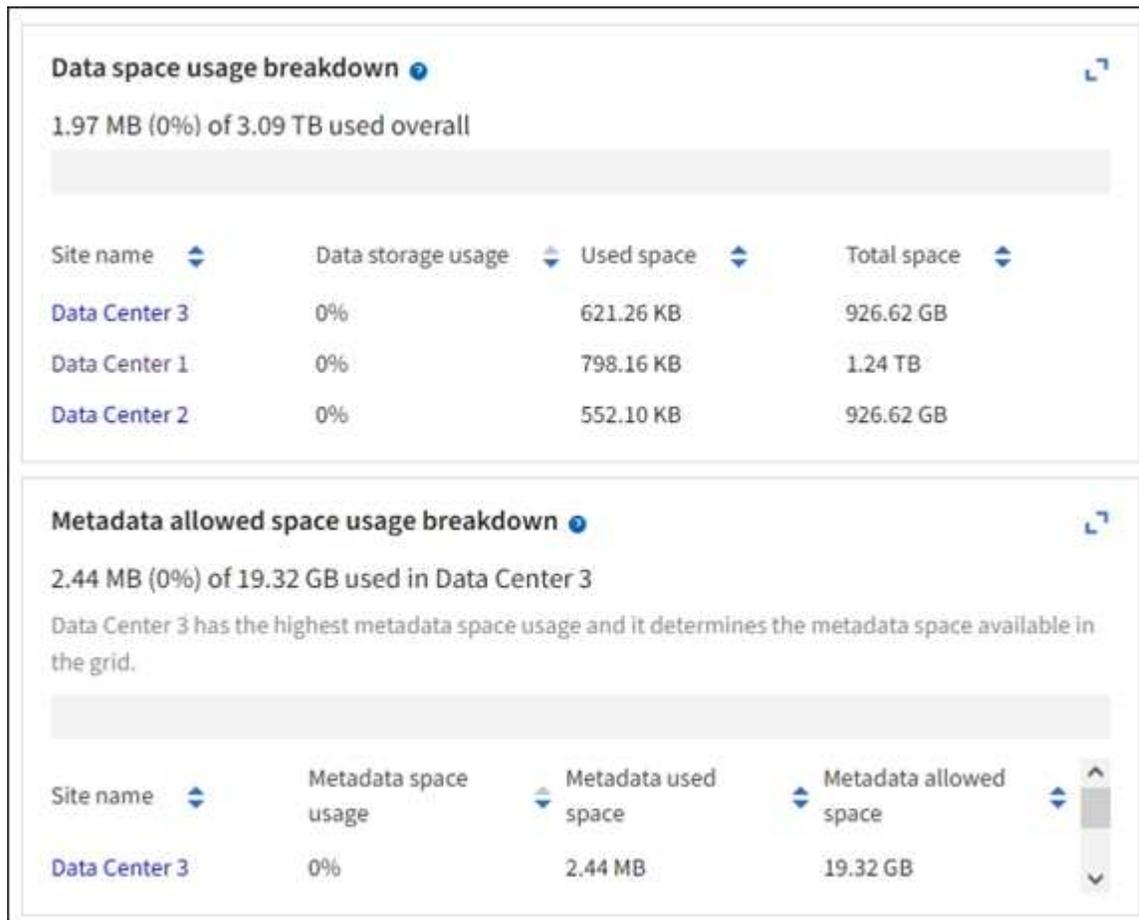
Grid Managerのダッシュボードでは、グリッド全体およびデータセンターごとに使用可能なストレージ容量を簡単に評価できます。ノードページには、オブジェクトデータとオブジェクトメタデータの詳細な値が表示されます。

手順

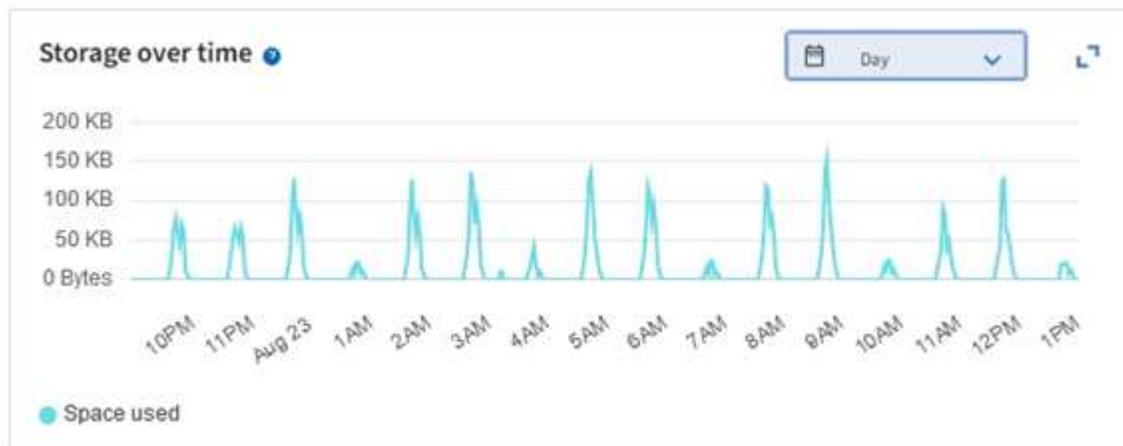
1. グリッド全体および各データセンターで使用可能なストレージ容量を評価します。
  - a. [ダッシュボード]>[概要]\*を選択します。
  - b. [Data space usage]の内訳と[Metadata Allowed space usage]の内訳カードの値をメモします。各カードには、ストレージ使用率、使用済みスペースの容量、サイトで使用可能または許可されている合計スペースが表示されます。



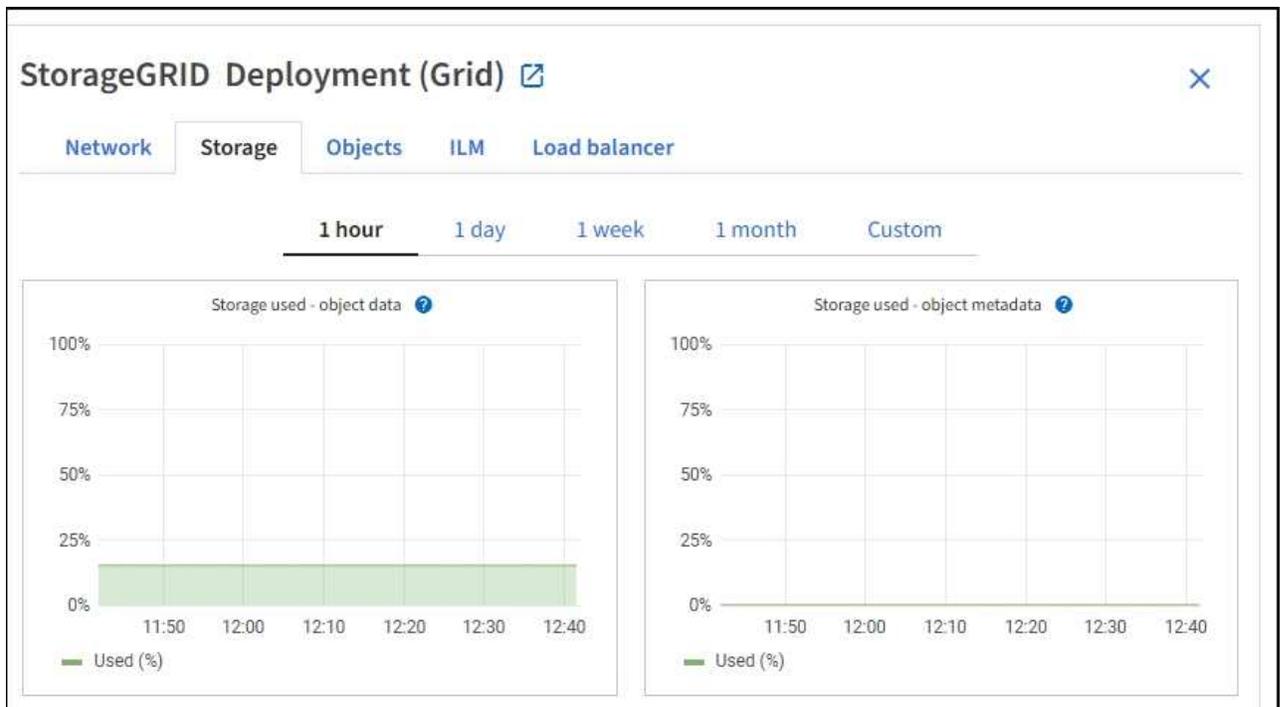
アーカイブメディアはこの概要に含まれません。



- a. [Storage Over Time]カードのグラフをメモします。期間のドロップダウンを使用すると、ストレージの消費速度を確認できます。



2. 使用済みのストレージ容量と、グリッドでオブジェクトデータとオブジェクトメタデータに使用できる残りのストレージ容量の詳細については、[Nodes]ページを使用してください。
  - a. [\* nodes (ノード) ] を選択します
  - b. [grid>\*Storage\*] を選択します。



- c. と[Storage Used - object metadata]\*のグラフにカーソルを合わせ、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容量と使用済み容量の推移を確認します。



サイトまたはグリッドの合計値には、オフラインのノードなど、指標が5分以上報告され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すべて使用される前に、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します。

拡張のタイミングを計画する際には、追加のストレージを調達して設置するのにどれくらいの時間がかかるかを検討します。



ILM ポリシーでイレイジャーコーディングを使用している場合は、既存のストレージノードの使用率が約 70% のときに拡張して、追加する必要のあるノードの数を減らすことができます。

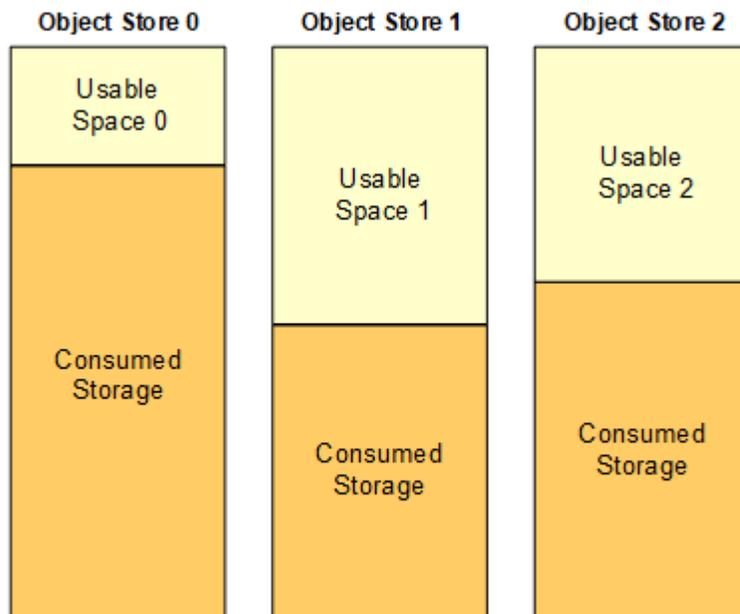
ストレージの拡張計画の詳細については、を参照してください "[StorageGRID の拡張手順](#)"。

各ストレージノードのストレージ容量を監視します

各ストレージノードの使用可能な合計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。

このタスクについて

使用可能なスペースは、オブジェクトの格納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使用可能な合計スペースは、ノード内のすべてのオブジェクトストアの使用可能なスペースの合計です。



**Total Usable Space = Usable Space 0 + Usable Space 1 + Usable Space 2**

手順

1. ノード \* > \* \_ストレージノード\_ \* > \* ストレージ \* を選択します。

ノードのグラフと表が表示されます。

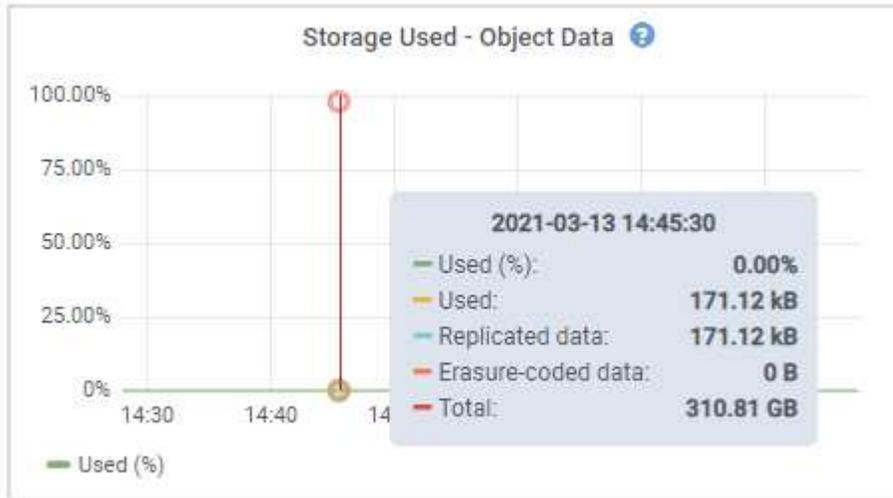
2. [Storage Used - object data]グラフにカーソルを合わせます。

次の値が表示されます。

- \* Used (%) \* : 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。
- \* Used \* : 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。
- \* Replicated data \* : このノード、サイト、またはグリッド上のレプリケートオブジェクトデータの推

定量。

- \* イレイジャーコーディングデータ \* : このノード、サイト、またはグリッドにあるイレイジャーコーディングオブジェクトデータの推定量。
- \* Total \* : このノード、サイト、またはグリッドで使用可能なスペースの総容量。  
使用済みの値はです `storagegrid_storage_utilization_data_bytes` メートル法。



3. グラフの下の Volumes テーブルと Object Stores テーブルで使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  をクリックします。

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

- 一定期間の値を監視して、使用可能なストレージスペースが消費される速度を見積もります。
- システムの正常な運用を維持するには、使用可能なスペースを使い切る前に、ストレージノードを追加するか、ストレージボリュームを追加するか、オブジェクトデータをアーカイブします。

拡張のタイミングを計画する際には、追加のストレージを調達して設置するのにどれくらいの時間がかかるかを検討します。



ILM ポリシーでイレイジャーコーディングを使用している場合は、既存のストレージノードの使用率が約 70% のときに拡張して、追加する必要のあるノードの数を減らすことができます。

ストレージの拡張計画の詳細については、を参照してください "[StorageGRID の拡張手順](#)"。

。"オブジェクトデータのストレージが少ない"アラートは、ストレージノードにオブジェクトデータを格納するための十分なスペースが残っていない場合にトリガーされます。

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します

各ストレージノードのメタデータ使用量を監視して、重要なデータベース処理に使用できるスペースが十分に残っていることを確認します。オブジェクトメタデータが許容されるメタデータスペースの 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。

このタスクについて

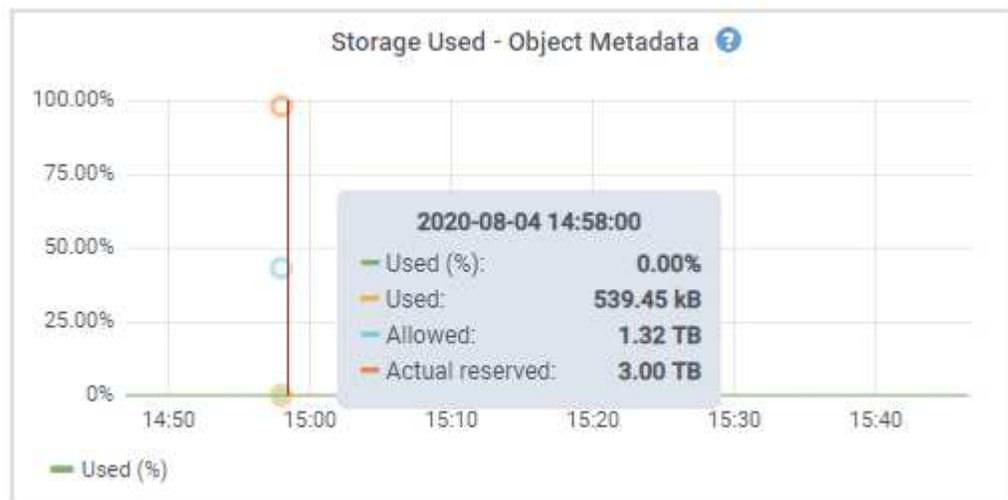
StorageGRID は、冗長性を確保し、オブジェクトメタデータを損失から保護するために、各サイトでオブジェクトメタデータのコピーを 3 つ保持します。3 つのコピーは、各ストレージノードのストレージボリューム 0 でメタデータ用にリザーブされたスペースを使用して、各サイトのすべてのストレージノードに均等に分散されます。

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の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、一般に大量の小さいオブジェクトを取り込む場合は、オブジェクトストレージの容量が十分に残っている場合でも、ストレージノードを追加してメタデータ容量を増やす必要があります。

メタデータの使用量を増やすことができる要因には、ユーザのメタデータとタグのサイズと数、マルチパートアップロードのパートの合計数、ILM のストレージの場所に対する変更の頻度などがあります。

手順

1. ノード \* > \* \_ストレージノード \_ \* > \* ストレージ \* を選択します。
2. [Storage Used - object metadata]グラフにカーソルを合わせると、その時点の値が表示されます。



使用済み (%)

このストレージノードで使用されている使用可能なメタデータスペースの割合。

Prometheus指標： `storagegrid_storage_utilization_metadata_bytes` および `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使用可能なメタデータスペースのバイト数。

Prometheus指標: `storagegrid_storage_utilization_metadata_bytes`

許可されます

このストレージノードでオブジェクトメタデータに使用できるスペース。各ストレージノードの値を決定する方法については、[を参照してください "使用可能なメタデータスペースの完全な概要"](#)。

Prometheus指標: `storagegrid_storage_utilization_metadata_allowed_bytes`

実際の予約

このストレージノードでメタデータ用にリザーブされている実際のスペース。使用可能なスペースと重要なメタデータ処理に必要なスペースが含まれます。この値の計算方法については、[を参照してください "メタデータ用に実際にリザーブされているスペースのフル概要"](#)。

*Prometheus*指標は今後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、オフラインのノードなど、指標が5分以上報告されていないノードは含まれません。

- Used (%) \* 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。



Low metadata storage \* アラートは、「Used (%)」の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の使用スペースが使用可能なスペースの 100% を超えている場合、望ましくない結果が生じる可能性があります。

新しいノードを追加すると、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が自動的にリバランシングされます。[を参照してください "StorageGRID システムの拡張手順"](#)。

スペース使用量の予測を監視します

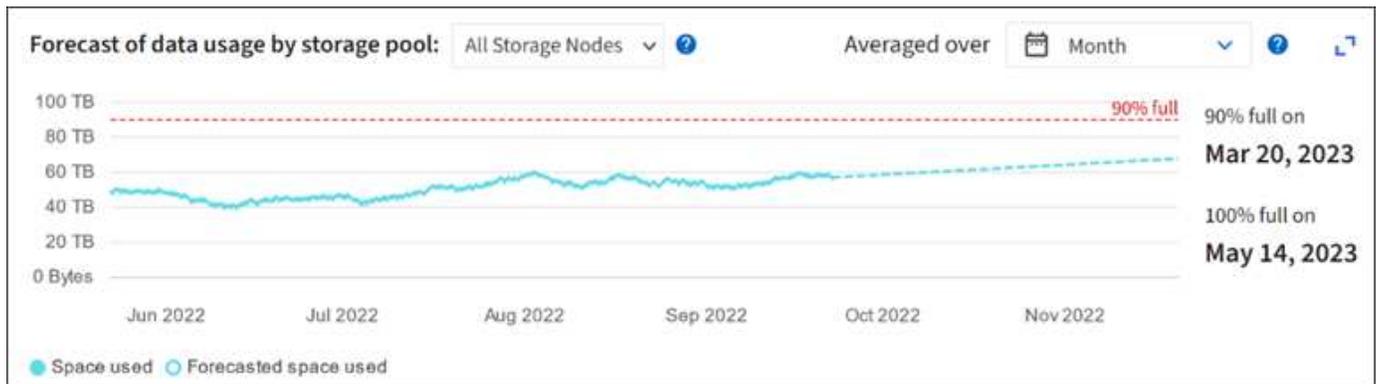
ユーザデータとメタデータのスペース使用量予測を監視して、必要なタイミングを予測します ["グリッドを展開する"](#)。

時間の経過とともに消費率が変化する場合は、[\* Averaged Over \*]プルダウンから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します。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てください。

StorageGRID を新規にインストールした場合は、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が蓄積されていることを確認してください。

手順

- ダッシュボードで、\*[ストレージ]\*を選択します。
- 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。
- 以下の値を使用して、データと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いつ追加する必要があるかを見積もります。



## 情報ライフサイクル管理を監視

Information Lifecycle Management (ILM ; 情報ライフサイクル管理) システムは、グリッドに格納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に対応できるかどうか、またはリソースの追加が必要かどうかを判断するには、ILM処理を監視する必要があります。

### このタスクについて

StorageGRIDシステムは、アクティブなILMポリシーを適用することで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、作成するコピーの数、作成するコピーのタイプ、配置場所、各コピーの保持期間が決まります。

オブジェクトの取り込みやその他のオブジェクト関連アクティビティは、StorageGRIDによるILMの評価速度を超える可能性があります。そのため、ILMの配置手順をほぼリアルタイムで実行できないオブジェクトがキューに登録されます。StorageGRIDがクライアント操作に対応しているかどうかを監視する必要があります。

### Grid Managerのダッシュボードタブを使用する

#### 手順

Grid Managerのダッシュボードの[ILM]タブを使用して、ILMの処理を監視します。

1. Grid Manager にサインインします。
2. ダッシュボードで[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）カードが一時的に急増することが想定されます。ただし、キューが増え続けて減少することがない場合、グリッドが効率的に動作するには、ストレージノードを追加するか、ILMポリシーにオブジェクトがリモートサイトに配置されている場合はネットワーク帯域幅を増やす必要があります。

### [Nodes]ページを使用

#### 手順

さらに、\* nodes \*ページを使用してILMキューを調査します。



StorageGRIDの今後のリリースで、\* nodes \*ページのチャートは対応するダッシュボードカードに置き換えられる予定です。

1. [\* nodes (ノード) ] を選択します
2. **grid name**>\*ilm \* を選択します。
3. ILMキューのグラフにカーソルを合わせると、ある時点における次の属性の値が表示されます。
  - \* Objects queued ( from client operations ) \* : クライアント処理 (取り込みなど) のために ILM による評価を待機しているオブジェクトの総数。
  - \* Objects queued ( from all operations ) \* : ILM による評価を待機しているオブジェクトの総数。
  - \* Scan rate ( objects/sec ) \* : グリッドのオブジェクトがスキャンされて ILM のキューに登録される速度。
  - \* 評価速度 (オブジェクト数 / 秒) \* : グリッド内の ILM ポリシーに照らしてオブジェクトが評価されている現在の速度。
4. ILM キューセクションで、次の属性を確認します。



[ILM queue]セクションはグリッド専用です。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。

- \* Scan Period - Estimated \* : ILMによるすべてのオブジェクトのフルスキャンが完了するまでの推定時間。



フルスキャンが完了しても、ILM がすべてのオブジェクトに適用されるとは限りません。

- \* Repairs Attempted \* : レプリケートデータに対して試行されたオブジェクト修復処理の総数。この数は、ストレージノードがハイリスクオブジェクトの修復を試みるたびに増分します。グリッドがビジー状態になった場合は、リスクの高い ILM の修復が優先されます。



修復後にレプリケーションに失敗した場合は、同じオブジェクトの修復で再び増分される可能性があります。

これらの属性は、ストレージノードのボリュームリカバリの進捗状況を監視する場合に役立ちます。試行された修理の回数が増えなくなり、フルスキャンが完了した場合は、修理が完了している可能性があります。

ネットワークリソースとシステムリソースを監視します

効率的な運用には、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使用量が不可欠です。

ネットワーク接続とパフォーマンスを監視します

ネットワーク接続と帯域幅は、情報ライフサイクル管理 (ILM) ポリシーでサイト間のレプリケートオブジェクトをコピーする場合や、サイト障害からの保護を提供するスキームを使用してイレイジャーコーディングオブジェクトを格納する場合に特に重要になります。サイト間のネットワークを使用できない場合、ネットワークレイテンシが高すぎる場合、またはネットワーク帯域幅が不十分な場合、一部の ILM ルールでオブジェクトが想定どおりに配置されない可能性があります。その結果、取り込みが失敗したり (ILMルールでStrict取り込みオプションが選択されている場合)、取り込みパフォーマンスの低下やILMバックログが発生する可能性があります。

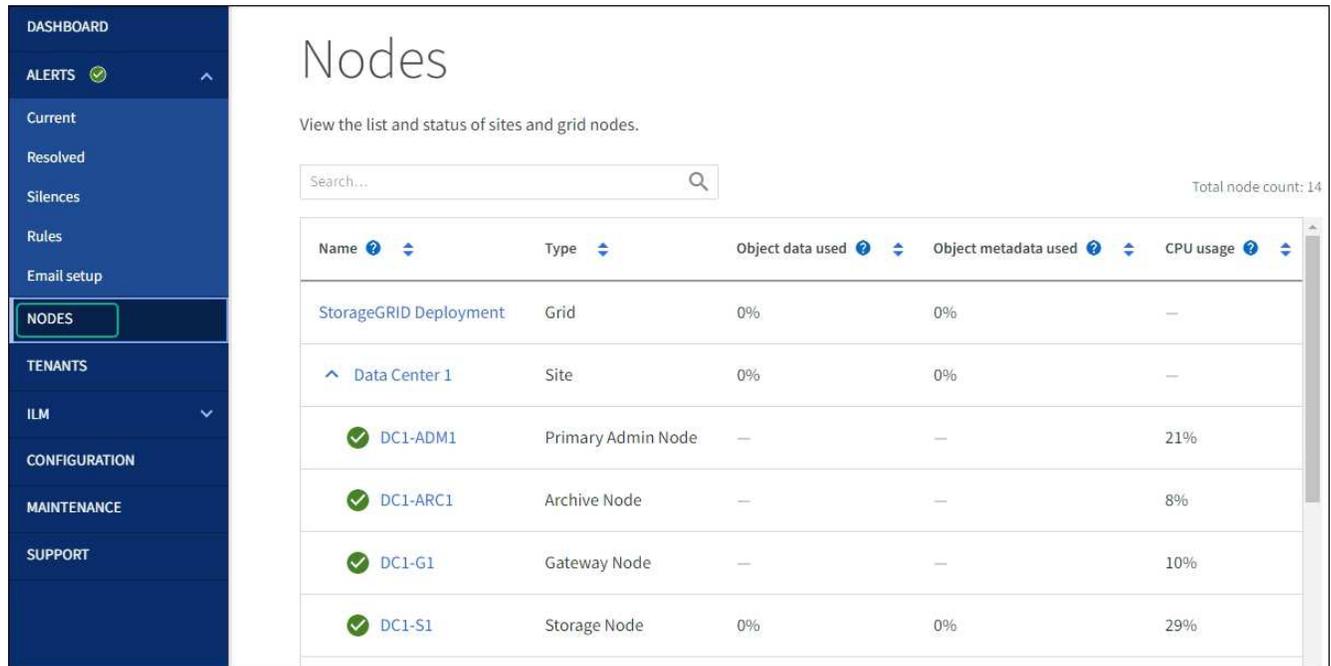
Grid Managerを使用して接続とネットワークのパフォーマンスを監視し、問題に迅速に対処できます。

さらに、検討してください ["ネットワークトラフィック分類ポリシーの作成"](#) これにより、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 (ノード) ] を選択します

Nodes ページが表示されます。グリッド内の各ノードが表形式で表示されます。



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。

このネットワークトラフィックのグラフには、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、ページの「\* ネットワークインターフェイス \*」セクションまでスクロールします。

Name	Hardware address	Speed	Duplex	Auto-negotiation	Link status
eth0	00:50:56:A7:66:75	10 Gigabit	Full	Off	Up

- b. グリッドノードがある場合は、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。

受信および送信テーブルには、各ネットワークで送受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。

Network communication						
Receive						
Interface	Data	Packets	Errors	Dropped	Frame overruns	Frames
eth0	2.89 GB	19,421,503	0	24,032	0	0
Transmit						
Interface	Data	Packets	Errors	Dropped	Collisions	Carrier
eth0	3.64 GB	18,494,381	0	0	0	0

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. \* configuration \* > \* Network \* > \* traffic classification \* を選択します。

[Traffic Classification Policies] ページが表示され、既存のポリシーがテーブルにリストされます。

#### Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.

Name	Description	ID
ERP Traffic Control	Manage ERP traffic into the grid	cd9afbc7-b85e-4208-b6f8-7e8a79e2c574
Fabric Pools	Monitor Fabric Pools	223b0cbb-6968-4646-b32d-7665bddc894b

Displaying 2 traffic classification policies.

- a. ポリシーに関連付けられているネットワーク指標を示すグラフを表示するには、ポリシーの左側にあるオプションボタンを選択し、[\*Metrics] 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ているネットワークトラフィックを把握します。

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、ポリシーがニーズを満たし続け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します"。

#### 関連情報

["\[ネットワーク\] タブを表示します"](#)

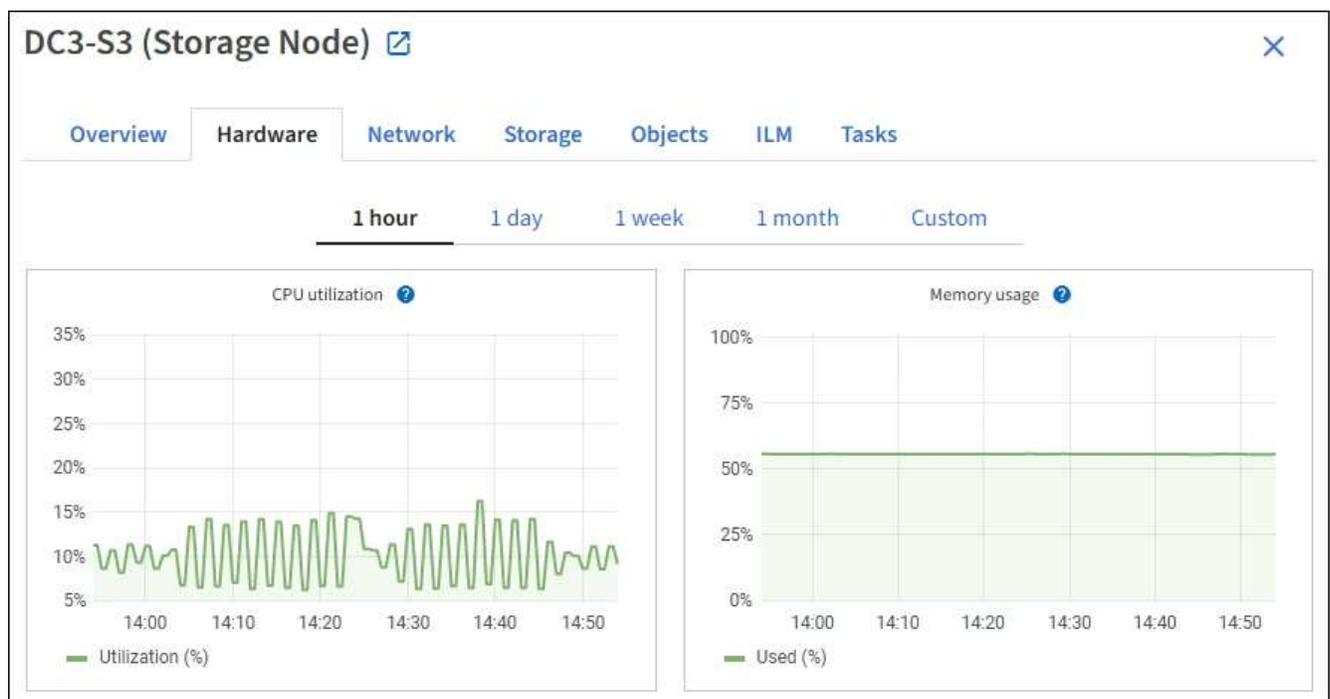
["ノードの接続状態を監視します"](#)

ノードレベルのリソースを監視

個々のグリッドノードを監視して、リソースの使用量レベルを確認します。ノードが常に過負荷状態になっていると、効率的な処理に必要なノードの数が増えます。

#### 手順

1. [\* nodes \* (ノード \* ) ] ページでノードを選択します。
2. **[Hardware]** タブを選択して、CPU 使用率とメモリ使用率のグラフを表示します。



3. 別の期間を表示するには、グラフ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、または 1 カ月の期間の情報を表示できます。また、カスタムの間隔を設定して、日時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表を表示します。すべてのコンポーネントのステータスが「Nominal (公称)」になっている必要があります。その他のステータスの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します"](#)

["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"](#)

テナントのアクティビティを監視する

S3およびSwiftクライアントアクティビティはすべてStorageGRID テナントアカウントに関連付けられています。Grid Managerを使用して、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または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、テナントによるStorageGRID の使用状況に関する詳細情報を収集できます。

作業を開始する前に

- を使用して Grid Manager にサインインします "サポートされている Web ブラウザ"。
- を使用することができます "root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します

[Tenants]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. [Tenant]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、クォータ利用率、クォータ、オブジェクト数が表示されます。テナントにクォータが設定されていない場合、Quota Utilization フィールドと Quota フィールドにはダッシュが表示されます（:）。



使用済みスペースの値は推定値です。これらの推定値は、取り込みのタイミング、ネットワーク接続、ノードのステータスによって左右されます。

### Tenants

View information for each tenant account. Depending on the timing of ingests, network connectivity, and node status, the usage data shown might be out of date. To view more recent values, select the tenant name.

Create Export to CSV Actions Search tenants by name or ID Displaying 5 results

<input type="checkbox"/>	Name	Logical space used	Quota utilization	Quota	Object count	Sign in/Copy URL
<input type="checkbox"/>	Tenant 01	2.00 GB	<div style="width: 10%; background-color: green;"></div> 10%	20.00 GB	100	<a href="#">→</a> <a href="#">📄</a>
<input type="checkbox"/>	Tenant 02	85.00 GB	<div style="width: 85%; background-color: orange;"></div> 85%	100.00 GB	500	<a href="#">→</a> <a href="#">📄</a>
<input type="checkbox"/>	Tenant 03	500.00 TB	<div style="width: 50%; background-color: green;"></div> 50%	1.00 PB	10,000	<a href="#">→</a> <a href="#">📄</a>
<input type="checkbox"/>	Tenant 04	475.00 TB	<div style="width: 95%; background-color: red;"></div> 95%	500.00 TB	50,000	<a href="#">→</a> <a href="#">📄</a>
<input type="checkbox"/>	Tenant 05	5.00 GB	–	–	500	<a href="#">→</a> <a href="#">📄</a>

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 [→](#) [サインイン/URLのコピー (Sign In/Copy URL) ]列に表示されます。

- 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  [サインイン/ URLのコピー (Sign In/Copy URL) ]列に表示されます。
- 必要に応じて、\*[CSVにエクスポート]\*を選択してを表示およびエクスポートします .csv すべてのテナントの使用状況の値を含むファイル。

を開くか保存するかを確認するメッセージが表示されます .csv ファイル。

の内容 .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	1100000000	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

を開くことができます .csv ファイルをスプレッドシートアプリケーションに保存することも、自動化で使用することもできます。

- オブジェクトが表示されない場合は、必要に応じて\*>[削除]\*を選択してテナントを削除します。を参照してください ["テナントアカウントを削除する"](#)。

バケットまたはコンテナが含まれているテナントアカウントは削除できません。

特定のテナントを表示します

特定のテナントの詳細を表示できます。

手順

- [Tenants]ページで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。

## Tenant 02

Tenant ID: 4103 1879 2208 5551 2180 

Protocol: S3

Object count: 500

Quota utilization: 85%

Logical space used: 85.00 GB

Quota: 100.00 GB

[Sign in](#) [Edit](#) [Actions](#) ▾

[Space breakdown](#) [Allowed features](#)

### Bucket space consumption

85.00 GB of 100.00 GB used

15.00 GB remaining (15%).



0 25% 50% 75% 100%

● bucket-01 ● bucket-02 ● bucket-03

### Bucket details

[Export to CSV](#)  

Displaying 3 results

Name 	Region 	Space used 	Object count 
bucket-01		40.00 GB	250
bucket-02		30.00 GB	200
bucket-03		15.00 GB	50

2. ページ上部のテナントの概要を確認します。

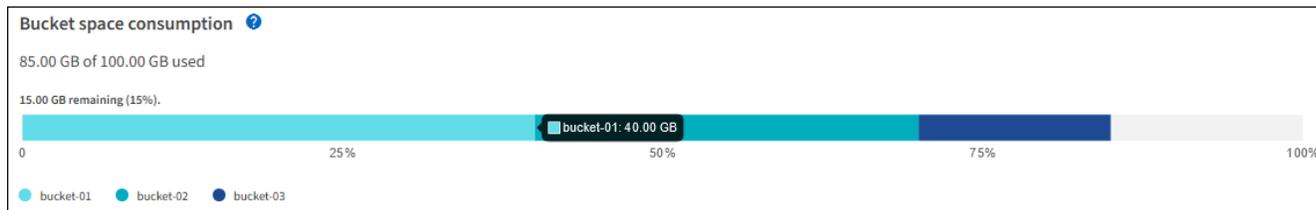
詳細ページのこのセクションには、テナントのオブジェクト数、クォータ使用率、使用済み論理スペース、クォータの設定など、テナントの概要情報が表示されます。

3. [スペースの内訳]タブで、\*[スペースの消費]\*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（またはSwiftコンテナ）のスペース消費の合計が表示されます。

このテナントにクォータが設定されている場合は、クォータの使用済み容量と残り容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で、テキストには使用済みのスペース（例：85.00 GB used）。棒グラフは、各バケットまたはコンテナのクォータの割合を示します。テナントがストレージクォータを1%以上かつ1GB以上超過した場合は、クォータの総容量と超過容量がグラフに表示されます。

棒グラフにカーソルを合わせると、各バケットまたはコンテナで使用されるストレージを確認できます。空きスペースセグメントにカーソルを合わせると、残りのストレージクォータを確認できます。



クォータ使用率は内部の推定値に基づいており、場合によっては超過することがあります。たとえば、テナントがクォータを超えた場合、StorageGRID はテナントがオブジェクトのアップロードを開始したときにクォータをチェックし、新しい取り込みを拒否します。ただし、StorageGRID では、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は考慮されません。オブジェクトが削除された場合、クォータ使用率が再計算されるまでテナントが一時的に新しいオブジェクトをアップロードできなくなることがあります。クォータ使用率の計算には 10 分以上かかることがあります。



テナントのクォータ利用率は、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総容量（論理サイズ）を示します。クォータ利用率は、これらのオブジェクトおよびそのメタデータのコピーを格納するために使用されるスペース（物理サイズ）を表していません。



「\* Tenant quota usage high \*」アラートルールを有効にすると、テナントがクォータを消費しているかどうかを確認できます。有効にすると、テナントのクォータの 90% が使用され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、を参照してください ["アラートルールを編集"](#)。

#### 4. タブで、[Bucket details（バケットの詳細）]\*を確認します。

次の表に、テナントのS3バケット（またはSwiftコンテナ）を示します。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総容量です。この値は、ILM コピーと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しているわけではありません。

#### 5. 必要に応じて、「\* Export to CSV \*」を選択し、各バケットまたはコンテナの使用量の値を含む .csv ファイルを表示してエクスポートします。

個々のS3テナントの内容 .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

を開くことができます .csv ファイルをスプレッドシートアプリケーションに保存することも、自動化で使用することもできます。

#### 6. 必要に応じて、\* Allowed features \*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。を参照してください ["テナントアカウントを編集します"](#) これらの設定のいずれかを変更する必要がある場合。

#### 7. テナントに\* Use grid federation connection 権限がある場合は、必要に応じて Grid federation \*タブを選択して接続の詳細を確認します。

を参照してください ["グリッドフェデレーションとは"](#) および ["グリッドフェデレーションに許可されたテ](#)

[ナントを管理します](#)。

ネットワークトラフィックを表示します

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. `* configuration * > * Network * > * traffic classification *` を選択します。

[Traffic Classification Policies] ページが表示され、既存のポリシーがテーブルにリストされます。

2. ポリシーのリストを確認して、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指標を表示するには、ポリシーの左側にあるラジオボタンを選択し、`*[Metrics]*` 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。

を参照してください "[トラフィック分類ポリシーを管理します](#)" を参照してください。

監査ログを使用します

必要に応じて、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、特定のクライアント処理
- オブジェクトサイズ
- オブジェクトに適用されている ILM ルール
- クライアント要求の送信元 IP

監査ログは、選択したログ分析ツールを使用して分析可能なテキストファイルに書き込まれます。これにより、クライアントアクティビティをよりよく理解したり、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ます。

を参照してください "[監査ログを確認します](#)" を参照してください。

**Prometheus** 指標を使用

必要に応じて、Prometheus 指標を使用してテナントアクティビティをレポートします。

- Grid Manager で、`* support * > * Tools * > * Metrics *` を選択します。S3 の概要など、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。



Metrics ページで使用できるツールは、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。これらのツールの一部の機能およびメニュー項目は、意図的に機能しないようになっています。

- Grid Manager の上部でヘルプアイコンを選択し、`*[API documentation]*` を選択します。グリッド管理 API

の指標セクションの指標を使用して、テナントアクティビティ用のカスタムのアラートルールとダッシュボードを作成できます。

を参照してください ["サポート指標を確認"](#) を参照してください。

### S3およびSwiftクライアント処理を監視する

オブジェクトの取り込み速度と読み出し速度、およびオブジェクト数、クエリ、検証関連の指標を監視できます。StorageGRID システムのオブジェクトに対してクライアントアプリケーションが試みた読み取り、書き込み、変更の各処理について、成功した回数と失敗した回数を表示できます。

作業を開始する前に

- を使用して Grid Manager にサインインします ["サポートされている Web ブラウザ"](#)。

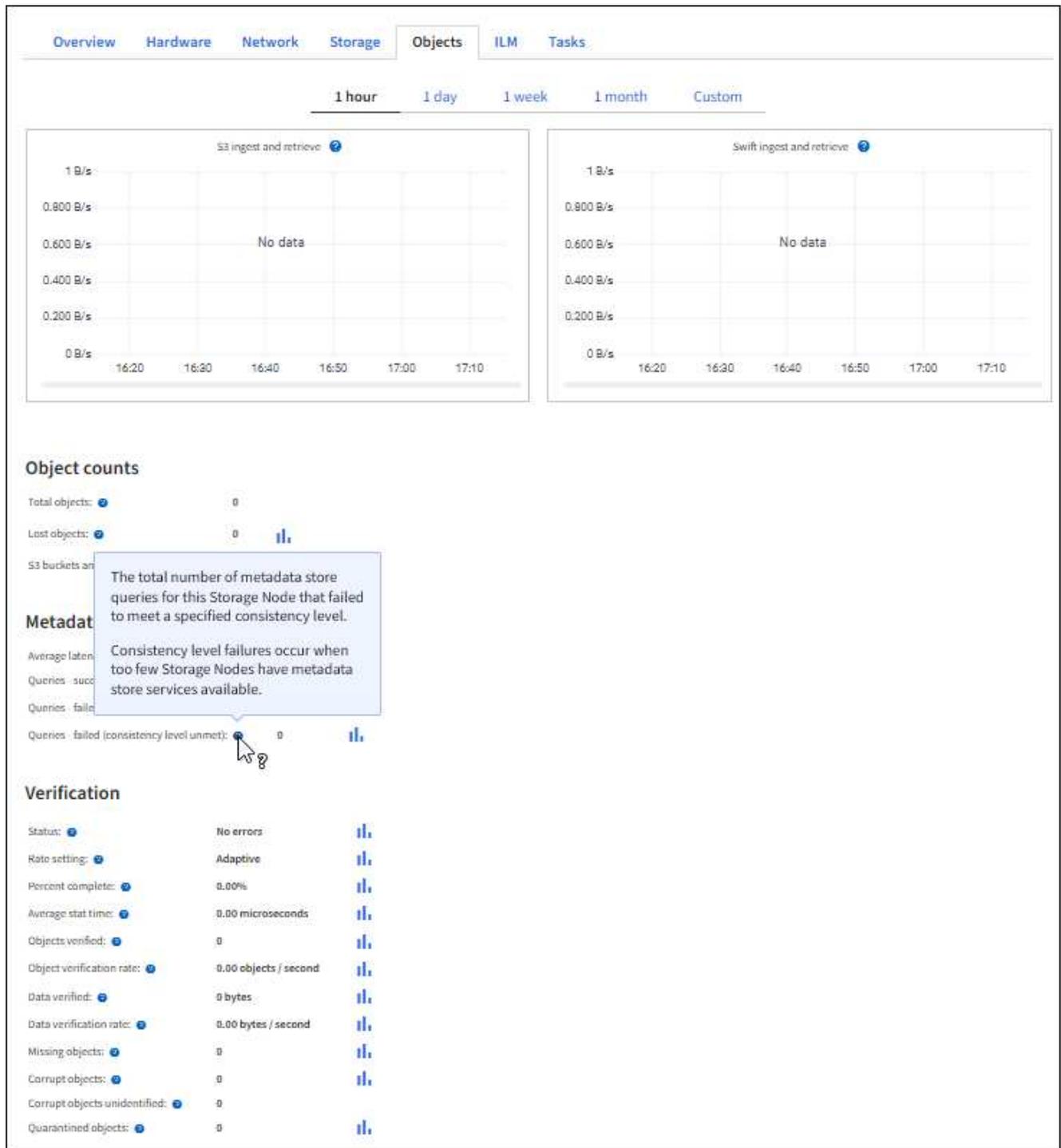
手順

1. ダッシュボードで、\*[パフォーマンス]\*タブを選択します。
2. S3およびSwiftのグラフを参照してください。このグラフには、選択した期間にストレージノードによって実行されたクライアント処理の数と、ストレージノードが受信したAPI要求の数がまとめられています。
3. [Nodes]\*を選択して[Nodes]ページにアクセスします。
4. [Nodes]ホームページ（グリッドレベル）で、\*[Objects]\*タブを選択します。

グラフには、StorageGRIDシステム全体のS3およびSwiftの取り込み速度と読み出したデータの量（1秒あたりのバイト数）が表示されます。時間間隔を選択するか、カスタムの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読み出し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、および検証処理の指標も表示されます。



## ロードバランシング処理を監視する

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、システムを最初に設定したあとと、設定を変更したり拡張を行ったあとに、ロードバランシング処理を監視する必要があります。

### このタスクについて

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、または外部の他社製ロードバランサを使用して、複数のストレージノードにクライアント要求を分散できます。

ロードバランシングを設定したら、オブジェクトの取り込みと読み出しの処理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 は負荷がかかっているクライアント要求への応答性を維持し、クライアントのパフォーマンスを維持できます。

ゲートウェイノードまたは管理ノードのハイアベイラビリティ（HA）グループをアクティブ/バックアップモードで設定した場合、グループ内の 1 つのノードだけ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、を参照してください "[S3 および Swift クライアント接続を設定します](#)"。

## 手順

1. S3 または Swift 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想定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（ノード）] 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 グループに含まれているかどうか、およびノードインターフェイスのロールがプライマリで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、クライアントに要求をアクティブに分散している必要があります。

- d. クライアント要求をアクティブに分散する必要がある各ノードについて、を選択します "[Load Balancer 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チャートを確認して、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 グループのノードでは、Backup ロールが随時割り当てられる場合があります。この間、ノードはクライアント要求を分散しません。
- f. ノードのオブジェクトスループットを確認するには、過去 1 週間のロードバランサの受信要求速度のグラフを確認します。
- g. StorageGRID システムの管理ノードまたはゲートウェイノードごとに上記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で処理されてい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. 「\*\_ストレージノード\_\*>\*LDR\*>\*HTTP\*」を選択します。
- b. 現在確立されている受信セッション数 \* を確認します。
- c. グリッド内のストレージノードごとにこの手順を繰り返します。

セッションの数はすべてのストレージノードでほぼ同じにします。

## グリッドフェデレーション接続を監視する

すべてのに関する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処理に関する Prometheus 指標。接続はどちらのグリッドからも監視できます。

作業を開始する前に

- いずれかのグリッドで、を使用してGrid Managerにサインインしておきます ["サポートされている Web ブラウザ"](#)。
- を使用することができます ["rootアクセス権限"](#) サインインしているグリッドの場合。

すべての接続を表示します

[Grid Federation]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的な情報が表示されます。

手順

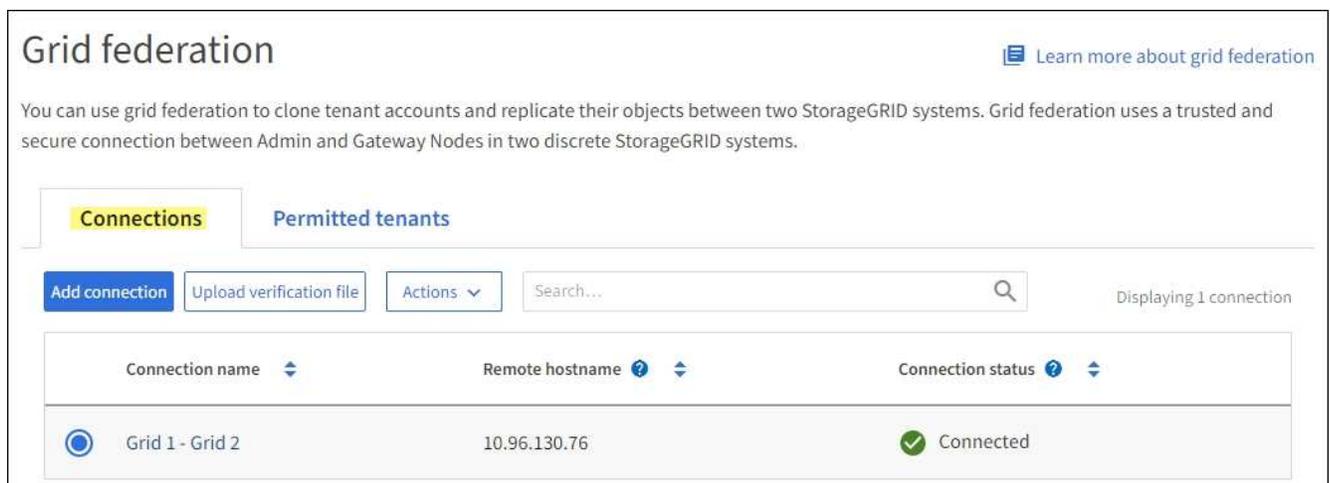
1. >[システム]>[グリッドフェデレーション]\*を選択します。

[Grid Federation]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に関する基本情報を表示するには、\*[接続]\*タブを選択します。

このタブでは、次の操作を実行できます。

- ["新しい接続を作成します"](#)。
- への既存の接続を選択します ["編集またはテスト"](#)。



The screenshot shows the 'Grid federation' page with a 'Connections' tab selected. Below the tabs are buttons for 'Add connection', 'Upload verification file', and 'Actions', along with a search bar. A table displays one connection: 'Grid 1 - Grid 2' with remote hostname '10.96.130.76' and status 'Connected'.

Connection name	Remote hostname	Connection status
Grid 1 - Grid 2	10.96.130.76	Connected

3. 権限があるこのグリッド上のすべてのテナントアカウントに関する基本情報を表示するには、[Permitted tenants]\*タブを選択します。

このタブでは、次の操作を実行できます。

- ["許可されている各テナントの詳細ページを表示します"](#)。
- 各接続の詳細ページを表示します。を参照してください [特定の接続を表示します](#)。
- 許可されているテナントとを選択します ["権限を削除します"](#)。
- グリッド間レプリケーションにエラーがないかどうかを確認し、最後のエラーがある場合はクリアします。を参照してください ["グリッドフェデレーションエラーをトラブルシューティングする"](#)。

## Grid federation [Learn more about grid federation](#)

You can use grid federation to clone tenant accounts and replicate their objects between two StorageGRID systems. Grid federation uses a trusted and secure connection between Admin and Gateway Nodes in two discrete StorageGRID systems.

Connections
Permitted tenants

Remove permission
Clear error

🔍
Displaying one result

	Tenant name	Connection name	Connection status	Remote grid hostname	Last error
<input checked="" type="radio"/>	Tenant A	Grid 1 - Grid 2	<span style="color: green;">✔</span> Connected	10.96.130.76	<a href="#">Check for errors</a>

特定の接続を表示します

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. [Grid Federation]ページで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。

接続の詳細ページでは、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。
- への接続を選択します ["編集、テスト、または削除"](#)。

2. 特定の接続を表示しているときに\*[Permitted Tenants]\*タブを選択すると、その接続で許可されているテナントに関する詳細が表示されます。

このタブでは、次の操作を実行できます。

- ["許可されている各テナントの詳細ページを表示します"](#)。
- ["テナントの権限を削除します"](#) 接続を使用します。
- クロスグリッドレプリケーションエラーがないかどうかを確認し、最後のエラーをクリアします。を参照してください ["グリッドフェデレーションエラーをトラブルシューティングする"](#)。

### Grid 1 - Grid 2

Local hostname (this grid): 10.96.130.64  
Port: 23000  
Remote hostname (other grid): 10.96.130.76  
Connection status: ✔ Connected

[Edit](#) [Download file](#) [Test connection](#) [Remove](#)

**Permitted tenants** [Certificates](#)

[Remove permission](#) [Clear error](#) Search... Displaying one result

Tenant name	Last error
<input checked="" type="radio"/> Tenant A	<a href="#">Check for errors</a>

3. 特定の接続を表示している場合は、\*[証明書]\*タブを選択して、この接続でシステムによって生成されたサーバ証明書とクライアント証明書を表示します。

このタブでは、次の操作を実行できます。

- "接続証明書をローテーションします"。
- 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、\* Server または Client \*を選択します。



手順の詳細については、を参照してください "[サポート指標を確認](#)".

- 複製に失敗したオブジェクトの複製を再試行するには、を参照してください "[失敗したレプリケーション処理を特定して再試行します](#)".

## アーカイブ容量を監視する

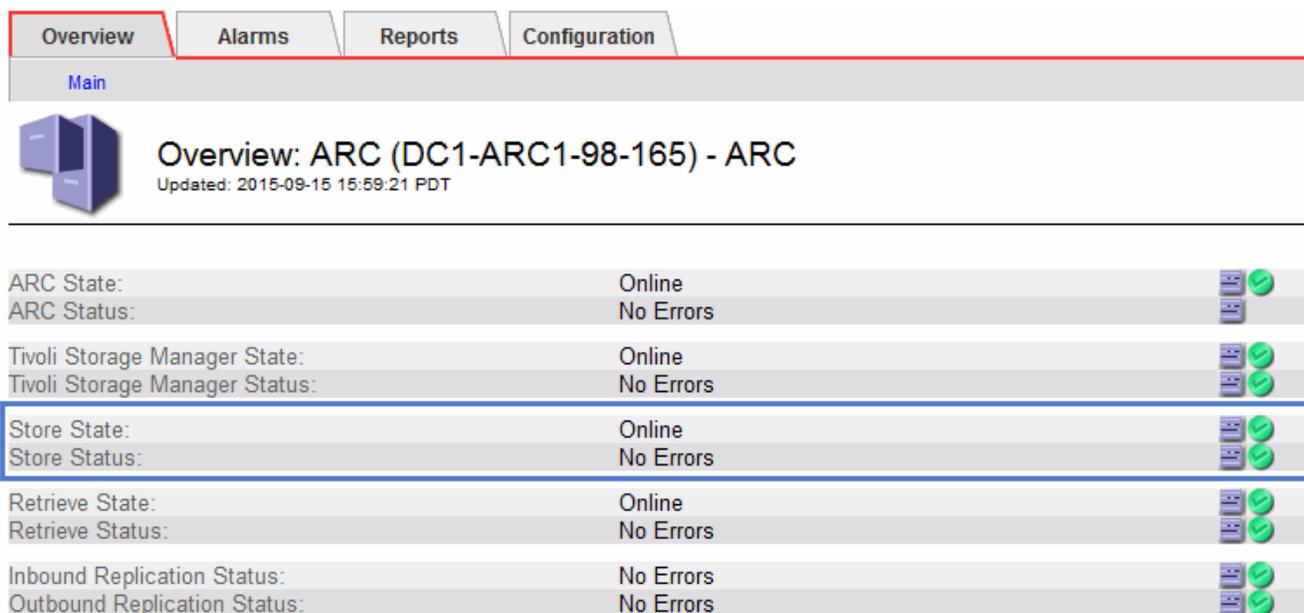
外部アーカイブストレージシステムの容量をStorageGRID システムで直接監視することはできません。ただし、アーカイブノードからアーカイブ先にまだオブジェクトデータを送信できるかを監視することで、アーカイブメディアの拡張が必要かどうかを確認できます。

### このタスクについて

Store コンポーネントを監視することにより、アーカイブノードから対象のアーカイブストレージシステムにまだオブジェクトデータを送信できるかどうかを確認できます。また、Store Failures (ARVF) アラームがトリガーされた場合、対象のアーカイブストレージシステムが容量に達し、オブジェクトデータをそれ以上受け入れられない状態になっている可能性があります。

### 手順

- サポート \* > ツール \* > グリッドトポロジ \* を選択します。
- [[Archive Node](#) > ARC > Overview > Main\*] を選択します。
- Store State 属性と Store Status 属性をチェックして、Store コンポーネントが Online with No Errors であることを確認します。



The screenshot shows the 'Overview' tab selected in a navigation menu. Below the menu is a 'Main' header. The main content area displays the title 'Overview: ARC (DC1-ARC1-98-165) - ARC' with a timestamp 'Updated: 2015-09-15 15:59:21 PDT'. Below this is a table of status indicators:

ARC State:	Online	
ARC Status:	No Errors	
Tivoli Storage Manager State:	Online	
Tivoli Storage Manager Status:	No Errors	
Store State:	Online	
Store Status:	No Errors	
Retrieve State:	Online	
Retrieve Status:	No Errors	
Inbound Replication Status:	No Errors	
Outbound Replication Status:	No Errors	

Store コンポーネントがオフラインになっている場合やエラーがある場合は、対象のアーカイブストレージシステムの容量に達したためにオブジェクトデータをそれ以上受け入れられない状態になっている可能性があります。

## アラートとアラーム

## アラートとアラームの管理：概要

StorageGRID アラートシステムは、注意が必要な運用上の問題について通知するように設計されています。従来のアラームシステムは廃止されました。

### アラートシステム

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

- Grid Manager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分されます。
- このアラートはノード \* の概要ページおよび \* ノード \* > \* \_node\_name > \* Overview \* タブに表示されません。
- SMTP サーバを設定し、受信者に E メールアドレスを提供している場合は、E メール通知が送信されません。
- StorageGRID SNMP エージェントが設定されている場合は、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。

### レガシーアラームシステム

アラートと同様に、属性が定義されたしきい値に達すると、特定の重大度レベルでアラームがトリガーされます。ただし、アラートとは異なり、無視しても問題なくアラートがトリガーされるアラームが多数あるため、E メールや SNMP 通知が大量に送信されることがあります。



アラームシステムは廃止され、今後のリリースで削除される予定です。引き続き古いアラームを使用する場合は、できるだけ早くアラートシステムに完全に移行してください。

アラームがトリガーされると、次の処理が行われます。

- このアラームは、**support**>\* Alarms（レガシー）> Current alarms \* ページに表示されます。
- SMTP サーバを設定して 1 つ以上のメーリングリストを設定している場合は、E メール通知が送信されません。
- StorageGRID SNMP エージェントを設定している場合は、SNMP 通知が送信されることがあります。（SNMP通知は、すべてのアラームまたは重大度について送信されるわけではありません）。

### アラートとアラームを比較します

アラートシステムと従来のアラームシステムにはいくつかの類似点がありますが、アラートシステムには大きなメリットがあり、使いやすくなっています。

同様の処理を実行する方法については、次の表を参照してください。

	アラート	アラーム (レガシーシステム)
アクティブなアラートまたはアラームを確認するにはどうすればよいですか？	<ul style="list-style-type: none"> <li>ダッシュボードの*[Current alerts]*リンクを選択します。</li> <li>ノード * &gt; * 概要 * ページでアラートを選択します。</li> <li>[* alerts * &gt; * current * ] を選択します。</li> </ul> <p>"現在のアラートを表示します"</p>	<p><b>support</b>&gt;* Alarms (レガシー) &gt; Current alarms * を選択します。</p> <p>"アラームの管理 (従来のシステム)"</p>
アラートまたはアラームがトリガーされる原因は何ですか？	<p>アラートは、アラートルールの Prometheus 式で特定のトリガー条件と期間について true と評価されたときにトリガーされます。</p> <p>"アラートルールを表示します"</p>	<p>StorageGRID 属性がしきい値に達すると、アラームがトリガーされます。</p> <p>"アラームの管理 (従来のシステム)"</p>
アラートまたはアラームがトリガーされた場合、原因となっている問題をどのように解決すればよいですか？	<p>アラートの推奨される対処方法は E メール通知に含まれており、Grid Manager のアラートページから確認できます。</p> <p>追加情報は、必要に応じて StorageGRID のドキュメントに記載されています。</p> <p>"アラート一覧"</p>	<p>アラームの詳細については、属性名を選択するか、StorageGRID のドキュメントでアラームコードを検索して確認できます。</p> <p>"アラーム一覧 (従来のシステム)"</p>
解決済みのアラートまたはアラームのリストはどこで確認できますか。	<p>[* alerts * &gt; * Resolved * ] を選択します。</p> <p>"現在のアラートと解決済みのアラートを表示します"</p>	<p><b>[support]</b>&gt; &gt; [* Alarms (legac)]&gt; &gt; [Historical alarms] を選択します。</p> <p>"アラームの管理 (従来のシステム)"</p>
設定を管理する場所	<p>[* alerts] * &gt; [* Rules] を選択します。</p> <p>"アラートの管理"</p>	<p>「* support *」を選択します。次に、メニューの * Alarms (レガシー) * セクションのオプションを使用します。</p> <p>"アラームの管理 (従来のシステム)"</p>

	アラート	アラーム (レガシーシステム)
どのようなユーザグループ権限が必要ですか？	<ul style="list-style-type: none"> <li>Grid Manager にサインインできるユーザは、現在のアラートと解決済みのアラートを表示できます。</li> <li>サイレンス、アラート通知、およびアラートルールを管理するには、Manage alerts権限が必要です。</li> </ul> <p>"StorageGRID の管理"</p>	<ul style="list-style-type: none"> <li>Grid Manager にサインインできるすべてのユーザがレガシーアラームを表示できます。</li> <li>アラームを確認するには、Acknowledge alarms権限が必要です。</li> <li>グローバルアラームとEメール通知を管理するには、Gridトポロジページの設定権限とその他のグリッド設定権限の両方が必要です。</li> </ul> <p>"StorageGRID の管理"</p>
電子メール通知の管理方法を教えてください。	<p>[* alerts*&gt;] &gt; [* Email setup*] を選択します。</p> <ul style="list-style-type: none"> <li>注： * アラームとアラートは独立したシステムなので、アラームと AutoSupport 通知に使用されるメール設定は、アラート通知には使用されません。ただし、すべての通知に同じメールサーバを使用できます。</li> </ul> <p>"アラート用の E メール通知を設定します"</p>	<p><b>support</b>&gt;* Alarms (レガシー) &gt; Legacy email setup* を選択します。</p> <p>"アラームの管理 (従来のシステム)"</p>
SNMP 通知の管理方法を教えてください。	<ul style="list-style-type: none"> <li>configuration * &gt; * Monitoring * &gt; * SNMP agent * を選択します。</li> </ul> <p>"SNMP による監視を使用する"</p>	サポートされていません
通知の受信者を制御するにはどうすればよいですか？	<ol style="list-style-type: none"> <li>[* alerts*&gt;] &gt; [* Email setup*] を選択します。</li> <li>[受信者 *] セクションで、電子メールリストごと、またはアラート発生時に電子メールを受信する必要があるユーザーごとに電子メールアドレスを入力します。</li> </ol> <p>"アラート用の E メール通知を設定します"</p>	<ol style="list-style-type: none"> <li><b>support</b>&gt;* Alarms (レガシー) &gt; Legacy email setup* を選択します。</li> <li>メーリングリストを作成しています。</li> <li>[*Notifications] を選択します。</li> <li>メーリングリストを選択します。</li> </ol> <p>"アラームの管理 (従来のシステム)"</p>

	アラート	アラーム (レガシーシステム)
通知を送信する管理ノードはどれですか？	単一の管理ノード (優先送信者)。  "管理ノードとは"	単一の管理ノード (優先送信者)。  "管理ノードとは"
一部の通知を停止する方法を教えてください。	<ol style="list-style-type: none"> <li>1. [* alerts * &gt; * silences* ] を選択します。</li> <li>2. サイレント化するアラートルールを選択します。</li> <li>3. サイレンスの期間を指定します。</li> <li>4. サイレント化するアラートの重大度を選択します。</li> <li>5. を選択して、グリッド全体、単一サイト、または単一ノードにサイレンスを適用します。  。注：SNMP エージェントを有効にした場合、サイレンスは SNMP トラップおよびインフォームも抑制します。</li> </ol> "アラート通知をサイレント化する"	<ol style="list-style-type: none"> <li>1. <b>support</b>&gt;* Alarms (レガシー) &gt; Legacy email setup* を選択します。</li> <li>2. [*Notifications] を選択します。</li> <li>3. メーリングリストを選択し、* 抑制 * を選択します。</li> </ol> "アラームの管理 (従来のシステム)"
すべての通知を停止するにはどうすればよいですか？	[* alerts * > * silences * ] を選択します。次に、[* すべてのルール * ] を選択します。  • 注：SNMP エージェントを有効にした場合、サイレンスは SNMP トラップおよびインフォームも抑制します。  "アラート通知をサイレント化する"	サポートされていません
条件とトリガーをカスタマイズする方法を教えてください。	<ol style="list-style-type: none"> <li>1. [* alerts] * &gt; [* Rules] を選択します。</li> <li>2. 編集するデフォルトルールを選択するか、* カスタムルールの作成 * を選択します。</li> </ol> "アラートルールを編集"  "カスタムのアラートルールを作成"	<ol style="list-style-type: none"> <li>1. [<b>support</b>&gt;] &gt; [* Alarms (legac)&gt;] &gt; [ Global alarms] を選択します。</li> <li>2. グローバルカスタムアラームを作成して、デフォルトアラームを上書きしたり、デフォルトアラームのない属性を監視したりします。</li> </ol> "アラームの管理 (従来のシステム)"

	アラート	アラーム (レガシーシステム)
個々のアラートまたはアラームを無効にする方法を教えてください。	<ol style="list-style-type: none"> <li>1. [* alerts] * &gt; [* Rules] を選択します。</li> <li>2. ルールを選択し、* ルールの編集 * を選択します。</li> <li>3. [有効]チェックボックスをオフにします。</li> </ol> <p>"アラートルールを無効化"</p>	<ol style="list-style-type: none"> <li>1. [support&gt;] &gt; [* Alarms (legac)&gt;] &gt; [ Global alarms] を選択します。</li> <li>2. ルールを選択し、[編集 (Edit) ] アイコンを選択します。</li> <li>3. [有効]チェックボックスをオフにします。</li> </ol> <p>"アラームの管理 (従来のシステム)"</p>

## アラートの管理

### アラートの管理：概要

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

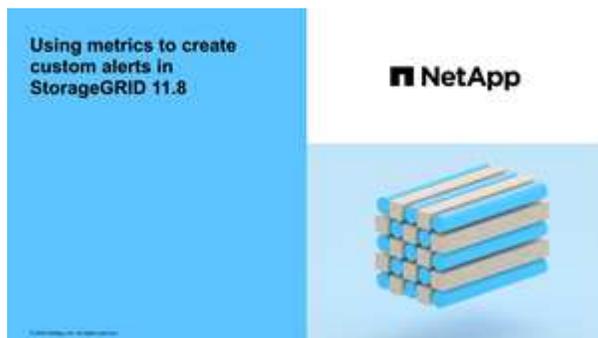
カスタムアラートの作成、アラートの編集または無効化、アラート通知の管理を行うことができます。

詳細については、以下をご覧ください。

- ビデオを確認します。"[ビデオ：StorageGRID 11.8のアラートの概要](#)"



- ビデオを確認します。"[ビデオ：StorageGRID 11.8で指標を使用してカスタムアラートを作成する](#)"



- を参照してください "[アラート一覧](#)".

アラートルールを表示します

アラートルールは、トリガーされる条件を定義します **"特定のアラート"**。StorageGRIDには一連のデフォルトアラートルールが用意されており、そのまま使用したり変更したりすることができます。また、カスタムのアラートルールを作成することもできます。

デフォルトとカスタムのアラートルールをすべて表示して、各アラートをトリガーする条件を確認したり、アラートが無効になっているかどうかを確認したりできます。

作業を開始する前に

- を使用して Grid Manager にサインインします **"サポートされている Web ブラウザ"**。
- を使用することができます **"アラートまたはRoot Access権限を管理します。"**。
- 必要に応じて、次のビデオを視聴しました。 **"ビデオ：StorageGRID 11.8のアラートの概要"**



手順

1. **[\* alerts] \* > [\* Rules]** を選択します。

**[Alert Rules]** ページが表示されます。

Alert Rules [Learn more](#)

Alert rules define which conditions trigger specific alerts.

You can edit the conditions for default alert rules to better suit your environment, or create custom alert rules that use your own conditions for triggering alerts.

Name	Conditions	Type	Status
<input type="radio"/> <b>Appliance battery expired</b> The battery in the appliance's storage controller has expired.	storagegrid_appliance_component_failure(type="REC_EXPIRED_BATTERY") Major > 0	Default	Enabled
<input type="radio"/> <b>Appliance battery failed</b> The battery in the appliance's storage controller has failed.	storagegrid_appliance_component_failure(type="REC_FAILED_BATTERY") Major > 0	Default	Enabled
<input type="radio"/> <b>Appliance battery has insufficient learned capacity</b> The battery in the appliance's storage controller has insufficient learned capacity.	storagegrid_appliance_component_failure(type="REC_BATTERY_WARN") Major > 0	Default	Enabled
<input type="radio"/> <b>Appliance battery near expiration</b> The battery in the appliance's storage controller is nearing expiration.	storagegrid_appliance_component_failure(type="REC_BATTERY_NEAR_EXPIRATION") Major > 0	Default	Enabled
<input type="radio"/> <b>Appliance battery removed</b> The battery in the appliance's storage controller is missing.	storagegrid_appliance_component_failure(type="REC_REMOVED_BATTERY") Major > 0	Default	Enabled
<input type="radio"/> <b>Appliance battery too hot</b> The battery in the appliance's storage controller is overheated.	storagegrid_appliance_component_failure(type="REC_BATTERY_OVERTEMP") Major > 0	Default	Enabled
<input type="radio"/> <b>Appliance cache backup device failed</b> A persistent cache backup device has failed.	storagegrid_appliance_component_failure(type="REC_CACHE_BACKUP_DEVICE_FAILED") Major > 0	Default	Enabled
<input type="radio"/> <b>Appliance cache backup device insufficient capacity</b> There is insufficient cache backup device capacity.	storagegrid_appliance_component_failure(type="REC_CACHE_BACKUP_DEVICE_INSUFFICIENT_CAPACITY") Major > 0	Default	Enabled
<input type="radio"/> <b>Appliance cache backup device write-protected</b> A cache backup device is write-protected.	storagegrid_appliance_component_failure(type="REC_CACHE_BACKUP_DEVICE_WRITE_PROTECTED") Major > 0	Default	Enabled
<input type="radio"/> <b>Appliance cache memory size mismatch</b> The two controllers in the appliance have different cache sizes.	storagegrid_appliance_component_failure(type="REC_CACHE_MEM_SIZE_MISMATCH") Major > 0	Default	Enabled

Displaying 62 alert rules.

2. アラートルールのテーブルの情報を確認します。

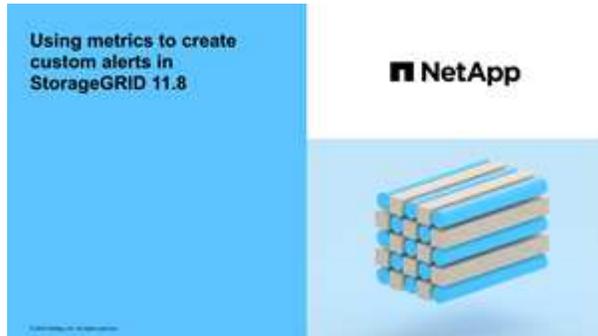
列ヘッダー	説明
名前	アラートルールの一意の名前と概要。カスタムのアラートルールが最初に表示され、そのあとにデフォルトのアラートルールが表示されます。アラートルール名は E メール通知の件名となります。
条件：	<p>このアラートがトリガーされるタイミングを決定する Prometheus 式。アラートは次の 1 つ以上の重大度レベルでトリガーできますが、重大度ごとの条件は不要です。</p> <ul style="list-style-type: none"> <li> <p>* 重要 * ：異常な状態で、StorageGRID のノードやサービスの通常の動作が停止しています。基盤となる問題にすぐに対処する必要があります。問題が解決されないと、サービスの停止やデータの損失を招くおそれがあります。</p> </li> <li> <p>* メジャー * ：異常な状態で、現在の処理に影響しているか、重大アラートのしきい値に近づいています。Major アラートを調査し、根本的な問題に対処して、異常な状態が発生した場合に StorageGRID のノードやサービスが正常に動作しなくなる事態を防ぐ必要があります。</p> </li> <li> <p>* マイナー * ：システムは正常に動作していますが、継続するとシステムの動作に影響する可能性がある異常な状態が発生しています。自動的にクリアされない Minor アラートを監視して解決し、重大な問題が発生しないようにする必要があります。</p> </li> </ul>
を入力します	<p>アラートルールのタイプ。</p> <ul style="list-style-type: none"> <li> <p>* デフォルト *：システムに付属のアラートルール。デフォルトのアラートルールは、無効にするか、条件と期間を編集できます。デフォルトのアラートルールは削除できません。</p> </li> <li> <p>* デフォルト **：条件または期間が編集された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戻すことができます。</p> </li> <li> <p>* Custom *：ユーザが作成したアラートルール。カスタムのアラートルールは、無効化、編集、削除することができます。</p> </li> </ul>
ステータス	このアラートルールが現在有効になっているか無効になっているか。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。

カスタムのアラートルールを作成

カスタムのアラートルールを作成して、アラートをトリガーする条件を独自に定義することができます。

作業を開始する前に

- を使用して Grid Manager にサインインします "サポートされている Web ブラウザ"。
- を使用することができます "アラートまたはRoot Access権限を管理します。"。
- に精通していること "よく使用される Prometheus 指標"。
- を理解しておきます "Prometheus クエリの構文"。
- 必要に応じて、次のビデオを視聴しました。 "ビデオ：StorageGRID 11.8で指標を使用してカスタムアラートを作成する"。



#### このタスクについて

StorageGRID はカスタムアラートを検証しません。カスタムの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参考に、カスタムのアラートルールを作成します。
- 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。その後、各条件のしきい値を変更します。
- 各条件に入力ミスやロジックエラーがないか、慎重にチェックしてください。
- Grid 管理 API にリストされている指標のみを使用してください。
- グリッド管理APIを使用して式をテストする場合、「successful」応答は空の応答本文（アラートがトリガーされない）であ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、現在 true になるしきい値を一時的に設定します。

たとえば、式をテストする場合などで `node_memory_MemTotal_bytes < 24000000000`` を実行します ``node_memory_MemTotal_bytes >= 0` また、想定される結果を確認します（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目的の値に戻して再実行します。結果がない場合は、この式に対するアラートが現在発生していません。

- アラートが想定どおりにトリガーされることを確認していないかぎり、カスタムアラートが機能しているとは思わないでください。

#### 手順

1. [\* alerts] \* > [\* Rules] を選択します。

[Alert Rules] 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。

[Create Custom Rule] ダイアログボックスが表示されます。

## Create Custom Rule

Enabled

Unique Name

Description

Recommended Actions  
(optional)

### Conditions ?

Minor

Major

Critical

Enter the amount of time a condition must continuously remain in effect before an alert is triggered.

Duration

5

minutes

Cancel

Save

3. [有効]\*チェックボックスをオンまたはオフにして、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します。

アラートルールを無効にすると、ルールの様式は評価されず、アラートはトリガーされません。

4. 次の情報を入力します。

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、[Alerts] 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 文字で指定できます。

フィールド	説明
説明	発生している問題の概要。概要は、アラートページおよびE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文字で指定できます。
推奨される対処方法	必要に応じて、このアラートがトリガーされたときに実行する推奨される対処方法を指定します。推奨される対処方法をプレーンテキスト（書式コードなし）で入力します。アラートルールの推奨される対処方法は、0~1、024文字で指定できます。

5. Conditions セクションで、アラートの重大度レベルを1つ以上指定する Prometheus 式を入力します。

基本式は、通常、次の形式で指定します。

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

式の文字数に制限はありませんが、ユーザインターフェイスでは1行で表示されます。少なくとも1つの式が必要です。

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

```
node_memory_MemTotal_bytes < 24000000000
```

使用可能な指標を確認したり、Prometheus 式をテストしたりするには、ヘルプアイコンを選択します  グリッド管理 API のメトリクスセクションへのリンクをクリックします。

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を継続的に有効にしておく必要がある期間を入力し、時間の単位を選択します。

条件が true 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。一時的な状況でアラートがトリガーされないようにするには、この値を大きくし

デフォルトは5分です。

7. [保存 (Save)] 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

アラートルールを編集してトリガー条件を変更したり、カスタムのアラートルールを使用してルール名、概要、および推奨される対処方法を更新したりできます。

作業を開始する前に

- を使用して Grid Manager にサインインします "サポートされている Web ブラウザ"。
- を使用することができます "アラートまたはRoot Access権限を管理します。"。

このタスクについて

デフォルトのアラートルールを編集する場合は、Minor、Major、Criticalの各アラートの条件と期間を変更できます。カスタムのアラートルールを編集する際に、ルールの名前、概要、および推奨される対処方法を編集することもできます。



アラートルールを編集する場合は注意が必要です。トリガー値を変更した場合、重大な処理を完了できなくなるまで、根本的な問題が検出されないことがあります。

#### 手順

1. [\* alerts] \* > [\* Rules] を選択します。

[Alert Rules] 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。

Edit Rule ダイアログボックスが表示されます。この例はデフォルトのアラートルールを示しています。[Unique Name]、概要]、および[Recommended Actions]のフィールドは無効になっており、編集することはできません。

### Edit Rule - Low installed node memory

Enabled

Unique Name

Description

Recommended Actions (optional)

#### Conditions ?

Minor

Major

Critical

Enter the amount of time a condition must continuously remain in effect before an alert is triggered.

Duration

4. [有効]\*チェックボックスをオンまたはオフにして、このアラートルールが現在有効になっているかどうか

を確認します。

アラートルールを無効にすると、ルールの様式は評価されず、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した場合は、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待つ必要があります。



通常は、デフォルトのアラートルールを無効にすることは推奨されません。アラートルールが無効になっている場合は、重大な処理を完了できなくなるまで、根本的な問題が検出されない可能性があります。

5. カスタムのアラートルールの場合は、次の情報を必要に応じて更新します。



この情報はデフォルトのアラートルールでは編集できません。

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、[Alerts] 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 文字で指定できます。
説明	発生している問題の概要。概要は、アラートページおよび E 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 文字で指定できます。
推奨される対処方法	必要に応じて、このアラートがトリガーされたときに実行する推奨される対処方法を指定します。推奨される対処方法をプレーンテキスト（書式コードなし）で入力します。アラートルールの推奨される対処方法は、0~1、024 文字で指定できます。

6. Conditions 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 つの点を選択します。

#### Conditions ⓘ

Minor	<input type="text"/>
Major	<input type="text" value="node_memory_MemTotal_bytes &lt; 2400000000"/>
Critical	<input type="text" value="node_memory_MemTotal_bytes &lt;= 1400000000"/>



現在のアラートの条件を更新した場合は、更新前の条件が解決されるまで変更が適用されないことがあります。ルールのいずれかの条件が次回満たされた時点で、更新された値がアラートに反映されます。

基本式は、通常、次の形式で指定します。

[metric] [operator] [value]

式の文字数に制限はありませんが、ユーザインターフェイスでは1行で表示されます。少なくとも1つの式が必要です。

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

```
node_memory_MemTotal_bytes < 24000000000
```

7. [\* Duration \*（時間\*）]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true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。一時的な状況でアラートがトリガーされないようにするには、この値を大きくし

デフォルトは5分です。

8. [保存（Save）]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は「[タイプ] カラムに **Default\*** と表示されます。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は、\* Status \* 列に \* Disabled \* と表示されます。

アラートルールを無効化

デフォルトまたはカスタムのアラートルールの有効 / 無効の状態を変更できます。

作業を開始する前に

- を使用して Grid Manager にサインインします ["サポートされている Web ブラウザ"](#)。
- を使用することができます ["アラートまたはRoot Access権限を管理します。"](#)。

このタスクについて

アラートルールを無効にすると、ルールの式は評価されず、アラートはトリガーされません。



通常は、デフォルトのアラートルールを無効にすることは推奨されません。アラートルールが無効になっている場合は、重大な処理を完了できなくなるまで、根本的な問題が検出されない可能性があります。

手順

1. [\* alerts] \* > [\* Rules] を選択します。

[Alert Rules] 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。

Edit Rule ダイアログボックスが表示されます。

4. [有効]\*チェックボックスをオンまたはオフにして、このアラートルールが現在有効になっているかどうか

を確認します。

アラートルールを無効にすると、ルールの式は評価されず、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した場合は、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待つ必要があります。

5. [保存 ( Save ) ] を選択します。

- 無効 \* は、 \* ステータス \* 列に表示されます。

カスタムのアラートルールを削除

不要となったカスタムのアラートルールは削除できます。

作業を開始する前に

- を使用して Grid Manager にサインインします "[サポートされている Web ブラウザ](#)"。
- を使用することができます "[アラートまたはRoot Access権限を管理します](#)"。

手順

1. [\* alerts] \* > [\* Rules] を選択します。

[Alert Rules] ページが表示されます。

2. 削除するカスタムの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は削除できません。

3. [\* カスタムルールを削除 \* ] を選択します。

確認のダイアログボックスが表示されます。

4. 「 \* OK \* 」 を選択して、アラートルールを削除します。

アラートのアクティブなインスタンスがあった場合、10分以内に解決されます。

アラート通知を管理します

アラートの **SNMP** 通知を設定します

アラート発生時に StorageGRID から SNMP 通知を送信するには、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。

Grid Manager またはグリッド管理 API の SNMP エンドポイントで \* configuration \* > \* Monitoring \* > \* SNMP エージェント \* オプションを使用して、StorageGRID SNMP エージェントを有効にして設定できます。SNMP エージェントは、3つのバージョンの SNMP プロトコルをすべてサポートします。

SNMP エージェントの設定方法については、を参照してください "[SNMP による監視を使用する](#)"。

StorageGRID SNMP エージェントの設定後に、次の2種類のイベントベースの通知を送信できます。

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

トラップ通知およびインフォーム通知は、デフォルトまたはカスタムアラートがいずれかの重大度レベルでトリガーされたときに送信されます。アラートのSNMP通知を停止するには、アラートのサイレンスを設定する必要があります。を参照してください "[アラート通知をサイレント化する](#)"。

StorageGRID環境に複数の管理ノードが含まれている場合は、プライマリ管理ノードがアラート通知、AutoSupportパッケージ、SNMPトラップとインフォーム、および従来のアラーム通知の優先送信者となります。プライマリ管理ノードが使用できなくなると、他の管理ノードから一時的に通知が送信されます。を参照してください "[管理ノードとは](#)"。

アラート用のEメール通知を設定します

アラート発生時にEメール通知が送信されるようにするには、SMTPサーバに関する情報を指定する必要があります。また、アラート通知の受信者のEメールアドレスを入力する必要があります。

作業を開始する前に

- を使用してGrid Managerにサインインします "[サポートされている Web ブラウザ](#)"。
- を使用することができます "[アラートまたはRoot Access権限を管理します](#)"。

このタスクについて

アラームとアラートは別々のシステムであるため、アラート通知に使用されるEメール設定は、アラーム通知とAutoSupportパッケージには使用されません。ただし、すべての通知に同じEメールサーバを使用できます。

StorageGRID環境に複数の管理ノードが含まれている場合は、プライマリ管理ノードがアラート通知、AutoSupportパッケージ、SNMPトラップとインフォーム、および従来のアラーム通知の優先送信者となります。プライマリ管理ノードが使用できなくなると、他の管理ノードから一時的に通知が送信されます。を参照してください "[管理ノードとは](#)"。

手順

1. [\* alerts\*>] > [\* Email setup\*] を選択します。

[ 電子メールの設定 ] ページが表示されます。

## Email Setup

You can configure the email server for alert notifications, define filters to limit the number of notifications, and enter email addresses for alert recipients.

Use these settings to define the email server used for alert notifications. These settings are not used for alarm notifications and AutoSupport. See [Managing alerts and alarms in the instructions for monitoring and troubleshooting StorageGRID](#).

Enable Email Notifications 

Save

2. [Eメール通知を有効にする]\*チェックボックスをオンにして、アラートが設定されたしきい値に達したときに通知Eメールが送信されるようにします。

電子メール（SMTP）サーバー、Transport Layer Security（TLS）、電子メールアドレス、およびフィルタ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 サーバで認証が必要な場合は、ユーザ名とパスワードの両方を指定する必要があります。

フィールド	入力するコマンド
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 サーバへのアクセスに使用するポート。1~65535 の範囲で指定する必要があります。
ユーザ名（オプション）	SMTP サーバで認証が必要な場合は、認証に使用するユーザ名を入力します。
パスワード（オプション）	SMTP サーバで認証が必要な場合は、で認証するためのパスワードを入力します。

### Email (SMTP) Server

Mail Server 	<input type="text" value="10.224.1.250"/>
Port 	<input type="text" value="25"/>
Username (optional) 	<input type="text" value="smtpuser"/>
Password (optional) 	<input type="password" value="*****"/>

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. \* 送信者電子メールアドレス \* 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電子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、電子メールリストごとに電子メールアドレスを入力するか、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ユーザーを入力します。

プラスアイコンを選択します **+** をクリックします。

#### Email Addresses

Sender Email Address 	<input type="text" value="storagegrid-alerts@example.com"/>	
Recipient 1 	<input type="text" value="recipient1@example.com"/>	
Recipient 2 	<input type="text" value="recipient2@example.com"/>	 

5. SMTP サーバとの通信に Transport Layer Security ( TLS ) が必要な場合は、 Transport Layer Security ( TLS ) セクションで \* Require TLS \* を選択します。

- a. [CA 証明書 \*] フィールドに、SMTP サーバの識別に使用する 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ことも、「\* 参照」を選択してファイルを選択することもできます。

各中間発行認証局 ( CA ) の証明書を含む単一のファイルを指定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して含まれている必要があります。

- b. SMTP EメールサーバでEメール送信者が認証用のクライアント証明書を提供する必要がある場合は、[クライアント証明書を送信]\*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 サーバに送信する PEM でエンコードされたクライアント証明書をを入力します。

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

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

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



Eメールのセットアップを編集する必要がある場合は、鉛筆のアイコンを選択してこのフィールドを更新します。

## Transport Layer Security (TLS)

Require TLS 

CA Certificate 

```
-----BEGIN CERTIFICATE-----  
1234567890abcdefghijklmnopqrstuvwxy  
ABCDEFGHIJKLMN0PQRSTUVWXYZ1234567890  
-----END CERTIFICATE-----
```

Browse

Send Client Certificate 

Client Certificate 

```
-----BEGIN CERTIFICATE-----  
1234567890abcdefghijklmnopqrstuvwxy  
ABCDEFGHIJKLMN0PQRSTUVWXYZ1234567890  
-----END CERTIFICATE-----
```

Browse

Private Key 

```
-----BEGIN PRIVATE KEY-----  
1234567890abcdefghijklmnopqrstuvwxy  
ABCDEFGHIJKLMN0PQRSTUVWXYZ1234567890  
-----BEGIN PRIVATE KEY-----
```

Browse

6. [フィルタ] セクションで、特定のアラートのルールがサイレント化されていない限り、電子メール通知を行うアラート重大度レベルを選択します。

重大度	説明
マイナー、メジャー、クリティカルです	アラートルールの Minor、Major、Critical のいずれかの条件が満たされたときに、Eメール通知が送信されます。
メジャー、クリティカルです	アラートルールの Major または Critical の条件が満たされたときに、Eメール通知が送信されます。マイナーアラートの通知は送信されません。

重大度	説明
重大な問題のみ	アラートルールの Critical 条件が満たされたときにのみ、Eメール通知が送信されます。MinorアラートやMajorアラートの通知は送信されません。

#### Filters

Severity ⓘ  Minor, major, critical  Major, critical  Critical only

Send Test Email

Save

7. Eメールの設定をテストする準備ができたなら、次の手順を実行します。

a. [テストメールの送信]を選択します。

テスト用E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Eメール受信者の受信ボックスを調べて、テスト用Eメールが受信されたことを確認します。



数分以内に電子メールが受信されない場合、または \*電子メール通知エラー\* アラートがトリガーされた場合は、設定を確認してから再試行してください。

c. 他の管理ノードにサインインし、テスト用E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。これに対し、AutoSupportパッケージや従来のアラーム通知のテストでは、すべての管理ノードからテスト用Eメールが送信されます。

8. [保存 ( Save ) ]を選択します。

テスト用Eメールを送信しても設定は保存されません。[保存 ( Save ) ]を選択する必要があります。

Eメール設定が保存されます。

#### アラートEメール通知に記載される情報

SMTP Eメールサーバを設定すると、アラートルールがサイレンスによって停止されていないかぎり、アラートがトリガーされたときにEメール通知が指定の受信者に送信されます。を参照してください ["アラート通知をサイレント化する"](#)。

Eメール通知には次の情報が含まれます。

## Low object data storage (6 alerts) 1

The space available for storing object data is low. 2

### Recommended actions 3

Perform an expansion procedure. You can add storage volumes (LUNs) to existing Storage Nodes, or you can add new Storage Nodes. See the instructions for expanding a StorageGRID system.

DC1-S1-226

**Node** DC1-S1-226 4  
**Site** DC1 225-230  
**Severity** Minor  
**Time triggered** Fri Jun 28 14:43:27 UTC 2019  
**Job** storagegrid  
**Service** ldr

DC1-S2-227

**Node** DC1-S2-227  
**Site** DC1 225-230  
**Severity** Minor  
**Time triggered** Fri Jun 28 14:43:27 UTC 2019  
**Job** storagegrid  
**Service** ldr

5

Sent from: DC1-ADM1-225

コールアウト	説明
1.	アラートの名前と、そのアラートのアクティブなインスタンスの数。
2.	アラートの概要。
3.	アラートの推奨される対処方法。
4.	アラートのアクティブな各インスタンスに関する詳細情報。対象となるノードとサイト、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が含まれます。
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

StorageGRID は、アラートがトリガーされたときに大量の E メール通知が送信されないように、複数のアラートを同じ通知にまとめます。

StorageGRID で複数のアラートを E メール通知でグループ化する例については、次の表を参照してください。

動作	例
各アラート通知は、同じ名前のアラートにのみ適用されます。名前が異なる2つのアラートが同時にトリガーされると、2つのEメール通知が送信されます。	<ul style="list-style-type: none"> <li>アラートAは2つのノードで同時にトリガーされます。1つの通知のみが送信されます。</li> <li>アラートAはノード1でトリガーされ、アラートBはノード2で同時にトリガーされます。2つの通知が送信されます各アラートに1つずつ送信されます</li> </ul>
特定のノードの特定のアラートが複数の重大度のしきい値に達した場合は、最も重大度の高いアラートに関してのみ通知が送信されます。	<ul style="list-style-type: none"> <li>アラートAがトリガーされ、Minor、Major、Criticalの各アラートしきい値に達した場合重大アラートに対して1つの通知が送信されます。</li> </ul>
あるアラートが初めてトリガーされた場合、StorageGRIDは2分待ってから通知を送信します。この時間内に同じ名前のアラートがほかにもトリガーされた場合、StorageGRIDはすべてのアラートを最初の通知の最初のグループにまとめます	<ol style="list-style-type: none"> <li>アラートAは、ノード1で08:00にトリガーされます。通知は送信されません。</li> <li>ノード2の08:01でアラートAがトリガーされます。通知は送信されません。</li> <li>08:02で、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。</li> </ol>
同じ名前の別のアラートがトリガーされた場合、StorageGRIDは10分待ってから新しい通知を送信します。新しい通知では、以前に報告されたものも含めて、アクティブなアラート（サイレント化されていない現在のアラート）がすべて報告されます。	<ol style="list-style-type: none"> <li>アラートAは、ノード1で08:00にトリガーされます。通知が08:02に送信されます。</li> <li>アラートAは、ノード2の08:05でトリガーされます。2回目の通知は8:15（10分後）に送信されます。両方のノードが報告されます。</li> </ol>
同じ名前の現在のアラートが複数あり、そのうちの1つのアラートが解決された場合、そのアラートが解決されたノードでアラートが再度発生しても新しい通知は送信されません。	<ol style="list-style-type: none"> <li>アラートAはノード1に対してトリガーされず。通知が送信されます。</li> <li>アラートAがノード2に対してトリガーされず。2回目の通知が送信されます。</li> <li>アラートAはノード2について解決されましたが、ノード1に対してはアクティブなままです。</li> <li>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のアラートがまだアクティブなため、新しい通知は送信されません。</li> </ol>
StorageGRIDは、アラートのすべてのインスタンスが解決されるか、アラートルールがサイレント化されるまで、7日ごとにEメール通知を送信します。	<ol style="list-style-type: none"> <li>3月8日にノード1のアラートAがトリガーされます。通知が送信されます。</li> <li>アラートAが解決されていないか、サイレント化されていないその他の通知は3月15日、3月22日、3月29日などに送信されます。</li> </ol>

#### アラートEメール通知のトラブルシューティング

- Email notification failure \* アラートがトリガーされた場合、またはテストアラートE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ます。

作業を開始する前に

- を使用して Grid Manager にサインインします "サポートされている Web ブラウザ"。
- を使用することができます "アラートまたはRoot Access権限を管理します。"。

手順

1. 設定を確認します。
  - a. [\* alerts\*>] > [\* Email setup\*] を選択します。
  - b. E メール（SMTP）サーバの設定が正しいことを確認します。
  - c. 受信者の有効な E メールアドレスが指定されていることを確認します。
2. スпамフィルタを確認し、E 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ます。
3. メール管理者に問い合わせ、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確認してください。
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連絡します。

テクニカルサポートは、ログの情報を参考に問題の原因を特定します。たとえば、指定したサーバに接続するときに、prometheus.log ファイルにエラーが表示されることがあります。

を参照してください "ログファイルとシステムデータを収集"。

アラート通知をサイレント化する

必要に応じて、サイレンスを設定してアラート通知を一時的に停止することができます。

作業を開始する前に

- を使用して Grid Manager にサインインします "サポートされている Web ブラウザ"。
- を使用することができます "アラートまたはRoot Access権限を管理します。"。

このタスクについて

アラートルールは、グリッド全体、単一サイト、または単一ノードと、1つ以上の重大度に対してサイレント化できます。各サイレンスは、1つ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停止します。

SNMP エージェントを有効にすると、サイレンスは SNMP トラップおよびインフォームも抑制します。



アラートルールをサイレント化する場合は注意が必要です。アラートをサイレント化すると、重大な処理を完了できなくなるまで、原因となっている問題が検出されない可能性があります。



アラームとアラートは別々のシステムであるため、この機能を使用してアラーム通知を停止することはできません。

手順

1. [\* alerts \* > \* silences\* ] を選択します。

[Silences] ページが表示されます。

## Silences

You can configure silences to temporarily suppress alert notifications. Each silence suppresses the notifications for an alert rule at one or more severities. You can suppress an alert rule on the entire grid, a single site, or a single node.

Alert Rule	Description	Severity	Time Remaining	Nodes
No results found.				

2. 「\* Create \*」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。

### Create Silence

Alert Rule

Description (optional)

Duration  Minutes

Severity  Minor only  Minor, major  Minor, major, critical

Nodes  StorageGRID Deployment  
 Data Center 1  
 DC1-ADM1  
 DC1-G1  
 DC1-S1  
 DC1-S2  
 DC1-S3

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	<p>サイレント化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、任意の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。</p> <ul style="list-style-type: none"> <li>注：このダイアログボックスで指定した条件を使用してすべてのアラートルールをサイレント化する場合は、「*すべてのルール*」を選択します。</li> </ul>
説明	<p>必要に応じて、サイレンスの概要。たとえば、このサイレンスの目的を入力します。</p>
期間	<p>このサイレンスを有効にしておく期間（分、時間、または日数）。サイレンスを有効にできる期間は、5分から1、825日（5年）です。</p> <ul style="list-style-type: none"> <li>注：*アラートルールを長時間サイレント化しないでください。アラートルールがサイレント化されている場合、重大な処理が完了しないかぎり、根本的な問題が検出されないことがあります。ただし、*サービスアプライアンスリンク停止*アラートや*ストレージアプライアンスリンク停止*アラートなど、特定の意図的な設定によってアラートがトリガーされた場合は、拡張サイレンスを使用する必要があります。</li> </ul>
重大度	<p>サイレント化するアラートの重大度。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。</p>
ノード	<p>このサイレンスを適用するノード。アラートルール、またはグリッド全体、単一サイト、または単一ノード上のすべてのルールを抑制することができます。グリッド全体を選択環境する場合は、すべてのサイトとすべてのノードをサイレント化します。サイトを選択すると、そのサイトのノードにのみサイレンスが適用されます。</p> <p>*注：*サイレンスごとに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。同じアラートルールを複数のノードまたは複数のサイトで一度に停止するには、追加のサイレンスを作成する必要があります。</p>

4. [保存（Save）]を選択します。

5. 期限が切れる前に変更または終了するには、サイレンスを編集または削除できます。

オプション	説明
サイレンスを編集する	<ol style="list-style-type: none"> <li>[* alerts * &gt; * silences*]を選択します。</li> <li>テーブルで、編集するサイレンスのラジオボタンを選択します。</li> <li>「*編集*」を選択します。</li> <li>概要、残り時間、選択した重大度、または対象となるノードを変更します。</li> <li>[保存（Save）]を選択します。</li> </ol>

オプション	説明
サイレンスを削除する	<p>a. [* alerts * &gt; * silences* ] を選択します。</p> <p>b. テーブルで、削除するサイレンスのラジオボタンを選択します。</p> <p>c. 「* 削除」を選択します。</p> <p>d. このサイレンスを削除することを確認するには、「* OK」を選択します。</p> <p>◦ 注* : このアラートがトリガーされると（別のサイレンスで停止されていないかぎり）通知が送信されるようになりました。このアラートが現在トリガーされている場合は、EメールまたはSNMP通知の送信やアラートページの更新に数分かかることがあります。</p>

## 関連情報

- ["SNMP エージェントを設定します"](#)

## アラート一覧

このリファレンスでは、Grid Managerに表示されるデフォルトアラートを示します。推奨される対処方法は、受信したアラートメッセージに記載されています。

必要に応じて、システムの管理方法に合わせてカスタムのアラートルールを作成できます。

一部のデフォルトアラートではが使用されます ["Prometheus 指標"](#)。

## アプライアンスのアラート

アラート名	説明
アプライアンスのバッテリーの有効期間が終了し	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間が終了しました。
アプライアンスのバッテリーに問題があります	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に障害が発生しました。
アプライアンスバッテリーの学習容量が不足しています	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で学習容量が不足しています。
アプライアンス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。
アプライアンスのバッテリーが取り外されました	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。
アプライアンスのバッテリーが高温になっています	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が過熱しています。

アラート名	説明
アプライアンスの 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	永続的キャッシュバックアップデバイスで障害が発生しました。
アプライアンスキャッシュバックアップデバイスに十分な容量がありません	キャッシュバックアップデバイスに十分な容量がありません。
アプライアンスのキャッシュ・バックアップ・デバイスの書き込み保護	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が一致しません	アプライアンスの 2 台のコントローラは、キャッシュサイズが異なります。
アプライアンス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の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 温度が公称の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を確認する必要があります	StorageGRID アプライアンスのコンピューティングコントローラでハードウェア障害が検出されました。
アプライアンスコンピューティングコントローラの電源装置 A に問題があります	コンピューティングコントローラの電源装置 A に問題があります。
アプライアンスコンピューティングコントローラの電源装置 B に問題があります	コンピューティングコントローラの電源装置 B に問題があります。
アプライアンスコンピューティングハードウェアモニタのサービスが停止する	ストレージハードウェアのステータスを監視するサービスが停止しました。
アプライアンスの DAS ドライブが 1 日に書き込まれるデータの制限を超えています	ドライブに毎日大量のデータが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。

アラート名	説明
アプライアンスのDASドライブ障害が検出されました	アプライアンスの直接接続型ストレージ (DAS) ドライブで問題が検出されました。
アプライアンスのDASドライブの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つ以上の直接接続型ストレージ (DAS) ドライブのドライブロケータライトが点灯しています。
アプライアンスDASドライブのリビルド	直接接続型ストレージ (DAS) ドライブのリビルド中。これは、最近交換または取り外し/再挿入された場合に想定される現象です。
アプライアンスのファン障害が検出されました	アプライアンス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・チャネル障害が検出されました	アプライアンス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の間でFibre Channel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・チャネル HBA ポート障害	Fibre Channel HBA ポートで障害が発生しているか、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が最適な状態ではありません	SSD キャッシュに使用されているドライブが最適な状態ではありません。
アプライアンスインターコネクト / バッテリキャニスターが取り外されました	インターコネクト / バッテリキャニスターがありません。
アプライアンスの LACP ポートがありません	StorageGRID アプライアンスのポートが LACP ボンドに参加していません。
アプライアンスNICの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装置がデグレード状態になりました	StorageGRID アプライアンスの電源が、推奨される動作電圧から逸脱しています。
アプライアンスSSDの重大な警告です	アプライアンスSSDから重大な警告が報告されています。
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 で障害が発生した。
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 で障害が発生した。

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のドライブ障害	StorageGRID アプライアンスの 1 つ以上のドライブで障害が発生しているか、または最適な状態ではありません。
アプライアンスストレージコントローラハードウェア問題	SANtricity ソフトウェアから、StorageGRID アプライアンスのコンポーネントについて「Needs Attention」が報告されます。
アプライアンスストレージコントローラの電源装置 A に障害が発生しました	StorageGRID アプライアンスの電源装置 A が、推奨される動作電圧から逸脱しています。
アプライアンスストレージコントローラの電源装置 B に障害が発生しました	StorageGRID アプライアンスの電源装置 B が、推奨される動作電圧から逸脱しています。
アプライアンスストレージハードウェアモニタのサービスが停止する	ストレージハードウェアのステータスを監視するサービスが停止しました。
アプライアンスストレージシェルフがデグレード状態になります	ストレージアプライアンスのストレージシェルフのいずれかのコンポーネントのステータスがデグレードになっています。
アプライアンスの温度が超過しました	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。
アプライアンスの温度センサーが取り外されました	温度センサーが取り外されました。
アプライアンスUEFIセキュアブートエラー	アプライアンスが安全にブートされていません。
ディスク I/O が非常に遅い	ディスク I/O が非常に遅い場合は、グリッドのパフォーマンスに影響す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で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のファンユニットで問題が検出されました。
ストレージアプライアンスストレージの接続がデグレードされました	コンピューティングコントローラとストレージコントローラ間の接続に問題があります。
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。

監査およびsyslogアラート

アラート名	説明
監査ログをメモリ内キューに追加しています	ノードからローカル syslog サーバにログを送信できず、メモリ内キューがいっぱいになっています。
外部 syslog サーバの転送エラーです	ノードから外部 syslog サーバにログを転送できません。
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。この状況に対処しないと、S3処理またはSwift処理が失敗する可能性があります。
ログをディスク上キューに追加しています	ノードから外部 syslog サーバにログを転送できず、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 バケットにサポート対象外のバケット整合性設定があります	FabricPoolバケットでは、availableまたはstrong-siteの整合性レベルが使用されますが、この整合性レベルはサポートされていません。

Cassandraアラート

アラート名	説明
Cassandra 自動コンパクターエラーです	Cassandra 自動コンパクターでエラーが発生しました。
Cassandra 自動コンパクターメトリックが古くなっています	Cassandra の自動圧縮機能を説明する指標が最新ではありません。
Cassandra 通信エラー	Cassandra サービスを実行するノード間の通信で問題が発生しています。
Cassandra の圧縮処理が過負荷です	Cassandra コンパクションプロセスが過負荷状態です。
Cassandraオーバーサイズ書き込みエラー	内部StorageGRID プロセスがCassandraに送信した書き込み要求が大きすぎます。
Cassandra 修復指標が最新ではありません	Cassandra 修復ジョブを説明する指標が最新ではありません。
Cassandra の修復の進捗が遅い	Cassandra データベースの修復の進捗状況が遅い。

アラート名	説明
Cassandra 修復サービスを使用できません	Cassandra 修復サービスは使用できません。
Cassandra テーブルが破損しています	Cassandra がテーブルの破損を検出しました。テーブルの破損が検出されると、Cassandra が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	クラウドストレージプールの健全性チェックで、新たなエラーが1つ以上検出されました。

#### グリッド間レプリケーションのアラート

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	ユーザの介入を必要とするグリッド間レプリケーションエラーが発生しました。
グリッド間レプリケーションリソースを使用できません	リソースを使用できないため、グリッド間レプリケーション要求が保留になっています。

#### DHCPアラート

アラート名	説明
DHCP リースの期限が切れました	ネットワークインターフェイスの DHCP リースが期限切れです。
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。
DHCP サーバが使用できません	DHCP サーバが使用できない。

#### デバッグおよびトレースアラート

アラート名	説明
パフォーマンスへの影響をデバッグします	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を及ぼす可能性があります。
トレース設定が有効になりました	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を及ぼす可能性があります。

## Eメールアラートと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。
E メール通知のエラーです	アラートの E メール通知を送信できませんでした。

## イレイジャーコーディング (EC) アラート

アラート名	説明
EC のリバランシングに失敗しました	ECリバランシング手順 が失敗したか、停止しました。
EC の修復エラー	ECデータの修復ジョブが失敗したか停止しました。
EC の修復が停止した	ECデータの修復ジョブが停止しました。

## 証明書の有効期限に関するアラート

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証明書の有効期限	S3およびSwiftのグローバルサーバ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。
管理インターフェイスのサーバ証明書の有効期限	管理インターフェイスで使用されるサーバ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 サーバ証明書への署名に使用される認証局 (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 サーバ証明書の有効期限	外部 syslog サーバから提供されるサーバ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のアラート

アラート名	説明
Grid ネットワーク MTU が一致しません	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に失敗しました	ローカルグリッドとリモートグリッドの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。

#### 高使用率または高レイテンシのアラート

アラート名	説明
Java ヒープの使用率が高い	Java ヒープ領域の使用率が高くなっています。
メタデータクエリのレイテンシが高くなっています	Cassandra メタデータクエリの平均時間が長すぎます。

#### アイデンティティフェデレーションアラート

アラート名	説明
アイデンティティフェデレーションの同期に失敗する	アイデンティティソースからフェデレーテッドグループとフェデレーテッドユーザを同期できません。
テナントのアイデンティティフェデレーションの同期が失敗する	テナントで設定されたアイデンティティソースからフェデレーテッドグループとフェデレーテッドユーザを同期できない。

#### 情報ライフサイクル管理 (ILM) のアラート

アラート名	説明
ILM 配置を実現できません	特定のオブジェクトについては、ILM ルールでの配置手順を実行できません。
ILM のスキャン期間が長すぎます	ILMのスキャン、評価、およびオブジェクトへの適用にかかる時間が長すぎます。

アラート名	説明
ILM のスキャン速度が低下しています	ILM のスキャン速度は 100 オブジェクト / 秒未満に設定されます。

#### キー管理サーバ (KMS) のアラート

アラート名	説明
KMS CA 証明書の有効期限	キー管理サーバ (KMS) 証明書への署名に使用する 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	キー管理サーバのクライアント証明書の有効期限が近づいています
KMS の設定をロードできませんでした	キー管理サーバの設定は存在しますが、ロードできませんでした。
KMS 接続エラー	アプライアンスノードがサイトのキー管理サーバ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	設定されているキー管理サーバに、指定した名前と一致する暗号化キーがありません。
KMS 暗号化キーのローテーションに失敗しました	アプライアンスのボリュームはすべて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 は設定されていません	このサイトにはキー管理サーバがありません。
KMS キーでアプライアンスボリュームを復号化できませんでした	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 サーバ証明書の有効期限	キー管理サーバ (KMS) で使用されるサーバ証明書の有効期限が近づいています。

#### 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・ラージ・タイム・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) 時間のオフセットが大きすぎます。

#### メモリ不足またはスペース不足のアラート

アラート名	説明
監査ログのディスク容量が不足しています	監査ログに使用できるスペースが少なくなっています。この状況に対処しないと、S3処理またはSwift処理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くなっています	ノードの使用可能な RAM の容量が少なくなっています。
ストレージプールの空き容量が不足しています	ストレージノードにオブジェクトデータを格納できるスペースが少なくなっています。
ノードメモリが不足しています	ノードに搭載されているメモリの容量が少なくなっています。
メタデータストレージが不足しています	オブジェクトメタデータを格納できるスペースが少なくなっています。
ディスク容量不足です	指標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。
オブジェクトデータのストレージが少ない	オブジェクトデータを格納できるスペースが少なくなっています。
読み取り専用のローウォーターマークの上書き	Storage Volume Soft Read-Only Watermark の上書きが、ストレージノードに対して最適化された最小ウォーターマークを下回っています。
ルートディスク容量が不足しています	ルートディスクの使用可能なスペースが少なくなっています。
システムのデータ容量が不足しています	/var/localに使用できるスペースが少なくなっています。この状況に対処しないと、S3処理またはSwift処理が失敗する可能性があります。
tmp ディレクトリの空きスペースが不足しています	/tmp ディレクトリのスペースが不足しています。

#### ノードまたはノードのネットワークアラート

アラート名	説明
管理ネットワークの受信使用量	管理ネットワークで受信の使用率が高くなっています。
管理ネットワークの転送使用量	管理ネットワークでの転送使用率が高くなっています。
ファイアウォールの設定に失敗しました	ファイアウォール設定を適用できませんでした。
フォールバックモードの管理インターフェイスエンドポイント	すべての管理インターフェイスエンドポイントがデフォルトポートに長時間フォールバックしています。

アラート名	説明
ノードの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	ノードで受信したネットワークフレームの割合が高いとエラーが発生していました。
ノードが NTP サーバと同期されていません	ノードがネットワークタイムプロトコル (NTP) サーバと同期されていません。
NTP サーバでノードがロックされていません	ノードがネットワークタイムプロトコル (NTP) サーバにロックされていません。
非アプライアンスノードのネットワークが停止しています	1 つ以上のネットワークデバイスが停止しているか切断されています。
管理ネットワークでサービスアプライアンスのリンクが停止しています	アプライアンスの管理ネットワーク (eth1) へのインターフェイスが停止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停止しています	アプライアンスの管理ネットワークポート 1 が停止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でサービスアプライアンスのリンクが停止しています	アプライアンスのクライアントネットワーク (eth2) へのインターフェイスが停止しているか切断されています。
ネットワークポート1でサービスアプライアンスのリンクが停止しています	アプライアンスのネットワークポート1が停止しているか切断されています。
ネットワークポート2でサービスアプライアンスのリンクが停止しています	アプライアンスのネットワークポート2が停止しているか切断されています。
ネットワークポート3でサービスアプライアンスのリンクが停止しています	アプライアンスのネットワークポート3が停止しているか切断されています。
ネットワークポート4でサービスアプライアンスのリンクが停止しています	アプライアンスのネットワークポート4が停止しているか切断されています。
管理ネットワークでのストレージアプライアンスのリンクが停止しています	アプライアンスの管理ネットワーク (eth1) へのインターフェイスが停止しているか切断されています。

アラート名	説明
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停止しています	アプライアンスの管理ネットワークポート 1 が停止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でストレージアプライアンスのリンクが停止しています	アプライアンスのクライアントネットワーク (eth2) へのインターフェイスが停止しているか切断されています。
ネットワークポート1でストレージアプライアンスのリンクが停止しています	アプライアンスのネットワークポート1が停止しているか切断されています。
ネットワークポート2でストレージアプライアンスのリンクが停止しています	アプライアンスのネットワークポート2が停止しているか切断されています。
ネットワークポート3でストレージアプライアンスのリンクが停止しています	アプライアンスのネットワークポート3が停止しているか切断されています。
ネットワークポート4でストレージアプライアンスのリンクが停止しています	アプライアンスのネットワークポート4が停止しているか切断されています。
ストレージノードが目的のストレージ状態ではありません	内部エラーまたはボリューム関連の問題が原因で、ストレージノードのLDRサービスを目的の状態に移行できない
TCP接続の使用状況	このノードのTCP接続数が追跡可能な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ていないか、ノードに到達できません。
予期しないノードのリポートです	過去 24 時間以内にノードが予期せずリポートされました。

#### 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	オブジェクトの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	オブジェクトの存在チェックジョブが停止しました。
オブジェクトが失われた	グリッドから 1 つ以上のオブジェクトが失われました。

アラート名	説明
S3 PUTオブジェクト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処理を試行しています。
未識別の破損オブジェクトが検出されました	レプリケートオブジェクトストレージにファイルが見つかりましたが、レプリケートオブジェクトとして識別できませんでした。

#### プラットフォームサービスのアラート

アラート名	説明
プラットフォームサービス保留中の要求容量が少なくなっています	保留中のPlatform Servicesリクエストの数が上限に近づいています。
プラットフォームサービスを利用できません	実行中または利用可能な状態の、RSM サービスを搭載したストレージノードがサイトで不足しています。

#### ストレージボリュームのアラート

アラート名	説明
ストレージボリュームで対応が必要です	ストレージボリュームはオフラインで、対応が必要です。
ストレージボリュームをリストアする必要があります	ストレージボリュームがリカバリされたため、リストアが必要です。
ストレージボリュームはオフラインです	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。ボリュームのフォーマット中にノードがリブートされた可能性があります。
ボリュームのリストアでレプリケート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レプリケートデータの修復を自動的に開始できませんでした。

#### StorageGRID サービスのアラート

アラート名	説明
バックアップ構成を使用するnginxサービス	nginxサービスの設定が無効です。以前の設定が使用されています。
バックアップ設定を使用するnginx-gwサービス	nginx-gwサービスの設定が無効です。以前の設定が使用されています。
FIPSを無効にするにはリブートが必要	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。

アラート名	説明
FIPSを有効にするにはリブートが必要です	セキュリティポリシーには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。
バックアップ設定を使用したSSHサービス	SSHサービスの設定が無効です。以前の設定が使用されています。

#### テナントアラート

アラート名	説明
テナントクォータの使用率が高い	クォータスペースの使用率が高くなっています。通知の原因が多すぎる可能性があるため、このルールはデフォルトで無効になっています。

#### よく使用される Prometheus 指標

デフォルトのアラートルールの条件を詳しく理解したり、カスタムのアラートルールの条件を作成したりするには、ここに示すPrometheus指標のよく使用されるリストを参照してください。

また可能です [すべての指標の完全なリストを取得します](#)。

Prometheusクエリの構文の詳細については、[を参照してください "Prometheusを照会しています"](#)。

#### Prometheus指標とは

Prometheus指標は時系列の測定値です。管理ノードのPrometheusサービスは、すべてのノード上のサービスからこれらの指標を収集します。指標は、Prometheusデータ用にリザーブされたスペースがフルになるまで各管理ノードに保存されます。をクリックします `/var/local/mysql_ibdata/` ボリュームが容量に達し、最も古い指標から順に削除されます。

#### Prometheus指標はどこで使用されますか？

Prometheusで収集された指標は、Grid Managerのいくつかの場所で使用されます。

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



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



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

- support > Tools > Diagnostics ページと support > Tools > Metrics \*ページ：これらのページは主にテクニカルサポートが使用することを目的としており、Prometheus指標の値を使用するいくつかのツールとチャートを提供します。



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

最も一般的な指標のリスト

次に、よく使用されるPrometheus指標を示します。



名前に *\_private\_* が含まれる指標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場合があります。

### **alertmanager\_notifications\_failed\_total**

失敗したアラート通知の総数。

### **node\_filesystem\_avail\_bytes** です

root以外のユーザが使用できるファイルシステムスペースの量 (バイト)。

### **node\_memory\_MemAvailable\_bytes**

Memory information (メモリ情報) フィールド MemAvailable\_bytes。

## Node\_network\_carrier

のキャリア値 `/sys/class/net/iface。`

## Node\_network\_receive\_errs\_total

ネットワークデバイスの統計情報 `receive_errs。`

## Node\_network\_transmit\_errs\_total

ネットワークデバイスの統計情報 `transmit_errs。`

## storagegrid\_administrative\_down

想定内の理由でノードがグリッドに接続されていません。たとえば、ノードまたはノード上のサービスが正常にシャットダウンされた、ノードがリブート中である、ソフトウェアのアップグレード中であるなどの原因が考えられます。

## storagegrid\_apply\_compute\_controller\_hardware\_status

アプライアンスのコンピューティングコントローラハードウェアのステータス。

## storagegrid\_apply\_failed\_disks を指定します

アプライアンス内のストレージコントローラの場合、最適な状態でないドライブの数。

## storagegrid\_apply\_storage\_controller\_hardware\_status

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。

## storagegrid\_content\_b Buckets\_or\_containers

このストレージノードによって認識されている S3 バケットと Swift コンテナの総数。

## storagegrid\_content\_objects を参照してください

このストレージノードによって認識されている S3 および Swift データオブジェクトの総数。S3 または Swift 経由でシステムとやり取りするクライアントアプリケーションで作成されたデータオブジェクトのみが対象です。

## storagegrid\_content\_objects\_lost

StorageGRID システムに存在しないことが検出されたオブジェクトの合計数。損失の原因 を特定し、リカバリが可能かどうかを確認する必要があります。

"失われたオブジェクトデータと欠落しているオブジェクトデータのトラブルシューティング"

## storagegrid\_http\_session\_ining\_attempted 」というメッセージが表示されます

ストレージノードに対して試行された HTTP セッションの総数。

## storagegrid\_http\_session\_ining\_currently\_established

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。

## storagegrid\_http\_session\_ining\_failed

不正な形式の HTTP 要求または処理中のエラーが原因で、正常に完了しなかった HTTP セッションの総数。

## storagegrid\_http\_session\_ining\_successful

正常に完了した HTTP セッションの総数。

**storagegrid\_ilm\_Awaiting\_background\_objects**

スキャンによる ILM に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です。

**storagegrid\_ilm\_Awaiting\_client\_evaluation\_objects\_per\_second**

このノードで ILM ポリシーに照らしてオブジェクトが評価されている現在の速度です。

**storagegrid\_ilm\_Awaiting\_client\_objects**

クライアント処理（取り込みなど）の ILM に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です。

**storagegrid\_ilm\_Awaiting\_total\_objects**

ILM 評価を待っているオブジェクトの合計数です。

**storagegrid\_ilm\_scan\_objects\_per\_second**

このノードが所有するオブジェクトが ILM 用にスキャンされてキューに登録される速度です。

**storagegrid\_ilm\_scan\_periodEstimated \_ minutes** （ StorageGRID \_ ILM \_ スキャン期間 \_ 推定 \_ 分）

このノードで ILM のフルスキャンが完了するまでの推定時間です。

- ・注：\* フルスキャンは、このノードが所有するすべてのオブジェクトに ILM が適用されたことを保証するものではありません。

**storagegrid\_load-balancer\_endpoint\_cert\_expiry\_time**

エポックからのロードバランサエンドポイント証明書の有効期限（秒数）。

**storagegrid\_meta\_query\_average\_latency\_milliseconds**

このサービスを使用し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。

**storagegrid\_network\_received\_bytes**

インストール後に受信したデータの総容量。

**storagegrid\_network\_transmitted\_bytes**

インストール後に送信されたデータの総容量。

**storagegrid\_node\_name**

使用可能な CPU 時間のうち、このサービスが現在使用している割合。サービスのビジー状態を示します。使用可能な CPU 時間は、サーバの CPU 数によって異なります。

**storagegrid\_ntp\_Chosen\_time\_source\_offset\_milliseconds**

選択した時間ソースによって提供される体系的な時間オフセット。オフセットは、時間ソースに到達するまでの遅延が、時間ソースが NTP クライアントに到達するために必要な時間と等しくない場合に適用されます。

**storagegrid\_ntp\_locked**

ノードがネットワークタイムプロトコル（NTP）サーバにロックされていません。

**storagegrid\_s3\_data\_transfers\_bytes\_取り込み 済み**

属性の前回リセット後に 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総容量。

**storagegrid\_s3\_data\_transfers\_bytes Retrieved**」のように表示されます

属性の前回リセット後に S3 クライアントがこのストレージノードから読み出したデータの総容量。

**storagegrid\_s3\_operations\_failed**」というエラーが表示されます

失敗した S3 処理（HTTP ステータスコード 4xx と 5xx）の総数。S3 の認証エラーが原因のものは除きます。

**storagegrid\_s3\_operations\_successful**

成功した S3 処理（HTTP ステータスコード 2xx）の総数。

**storagegrid\_s3\_operations\_unauthorized**

認証エラーが原因で失敗した S3 処理の総数。

**storagegrid\_servercertificate\_management\_interface\_cert\_expiry\_days** のように指定します

管理インターフェイス証明書が期限切れになるまでの日数。

**storagegrid\_servercertificate\_storage\_api\_endpoints\_cert\_expiry\_days** のように指定します

オブジェクトストレージ API 証明書が期限切れになるまでの日数。

**storagegrid\_service\_cpu\_seconds** で指定します

インストール後にこのサービスが CPU を使用した時間の累計。

**storagegrid\_service\_memory\_usage\_bytes**

このサービスが現在使用しているメモリ（RAM）の容量。この値は、Linux の top ユーティリティで RES として表示される値と同じです。

**storagegrid\_service\_network\_received\_bytes**

インストール後にこのサービスが受信したデータの総容量。

**storagegrid\_service\_network\_transmitted** バイト数

このサービスから送信されたデータの総容量。

**storagegrid\_service\_restarts**

サービスが再起動された回数。

**storagegrid\_service\_runtime\_seconds**

インストール後にサービスが実行されていた合計時間。

**storagegrid\_service\_uptime** を指定します

前回のサービス再起動以降にサービスが実行されていた時間の合計。

**storagegrid\_storage\_state\_current**

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

**storagegrid\_storage\_status** のように指定します

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 = 空きスペースが不足しています
- 30 = ボリュームを使用できません
- 40 = エラー

**storagegrid\_storage\_utilization\_data\_bytes**

ストレージノード上のレプリケートオブジェクトデータとイレイジャーコーディングオブジェクトデータの推定合計サイズ。

**storagegrid\_storage\_utilization\_meta\_allowed\_bytes**

オブジェクトメタデータに使用でき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、ノードでメタデータ用にリザーブ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、重要なデータベース処理（コンパクションや修復など）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なリザーブスペースの一部が必要なためです。オブジェクトメタデータ用の許可スペースは、オブジェクトの全体的な容量を制御します。

**storagegrid\_storage\_utilization\_metadata\_bytes**

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バイト数。

**storagegrid\_storage\_utilization\_total\_space\_bytes**

すべてのオブジェクトストアに割り当てられているストレージスペースの総容量。

**storagegrid\_storage\_utilization\_usable\_space\_bytes**

オブジェクトストレージスペースの残り容量。ストレージノード上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算出されます。

**storagegrid\_swifty\_data\_transfers\_bytes\_取り込み 済み**

属性の前回リセット以降にこのストレージノードに取り込まれたデータの総容量。

**storagegrid\_wift\_data\_transfers\_byts\_retrieved**

属性の前回リセット後に Swift クライアントがこのストレージノードから読み出したデータの総容量。

**storagegrid\_swift\_operations\_failed** というエラーが発生しました

失敗した Swift 処理（HTTP ステータスコード 4xx と 5xx）の総数。Swift の認証エラーが原因のものは除きます。

**storagegrid\_swift\_operations\_successful**

成功した Swift 処理（HTTP ステータスコード 2xx）の総数。

**storagegrid\_swift\_operations\_unauthorized**

認証エラーが原因で失敗した Swift 処理（HTTP ステータスコード 401、403、405）の総数。

### storagegrid\_stenantUsagedata\_bytes

テナントのすべてのオブジェクトの論理サイズ。

### storagegrid\_stenantUsageobject\_count

テナントのオブジェクトの数。

### storagegrid\_tenant\_dusation\_QUOTA\_bytes

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容量。クォータ指標を指定しない場合、使用可能なスペースは無制限です。

すべての指標のリストを取得します

すべての指標のリストを取得するには、グリッド管理APIを使用します。

1. Grid Managerの上部でヘルプアイコンを選択し、\*[API documentation]\*を選択します。
2. 指標 \* 処理を探します。
3. を実行します GET /grid/metric-names 操作。
4. 結果をダウンロードします。

### アラームの管理（従来のシステム）

#### アラームの管理（従来のシステム）

StorageGRID アラームシステムは、通常の動作中に発生することがある問題点を特定するために使用される従来のシステムです。



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

### アラームクラス（レガシーシステム）

レガシーアラームは、相互に排他的な 2 つのアラームクラスのいずれかに属することができます。

- デフォルトアラームはStorageGRID システムごとに用意されており、変更することはできません。ただし、グローバルカスタムアラームを定義して、デフォルトアラームを無効にしたり上書きしたりすることができます。
- グローバルカスタムアラームは、StorageGRID システムの特定のタイプのサービスすべてのステータスを監視します。グローバルカスタムアラームを作成して、デフォルトアラームを上書きすることができます。新しいグローバルカスタムアラームを作成することもできます。これは、StorageGRID システムについて独自の状況を監視する場合に役立ちます。

### アラームトリガーロジック（レガシーシステム）

StorageGRID 属性が、あるアラームクラス（デフォルトまたはグローバルカスタム）とアラームの重大度レベルの組み合わせに対して true と評価されるしきい値に達すると、それまでのアラームがトリガーされません。

をクリックします。	色 (Color)	アラームの重大度	意味
	黄色	注意	ノードはグリッドに接続されていますが、正常な状態ではありません。通常の動作に影響はありません。
	薄いオレンジ	マイナー	ノードはグリッドに接続されていますが、正常な状態ではありません。将来的に動作に影響する可能性があります。さらに重大な問題にならないように調査が必要です。
	濃いオレンジ	メジャー (Major)	ノードはグリッドに接続されていますが、正常な状態ではありません。すでに動作に影響が及んでいます。エスカレーションを防ぐために早急な対応が必要です。
	赤	重要	ノードはグリッドに接続されていますが、正常な状態ではありません。正常に動作しなくなっています。問題にはすぐに対処する必要があります。

アラームの重大度と対応するしきい値は、すべての数値属性に設定できます。各管理ノード上の NMS サービスは、設定されたしきい値に照らして現在の属性値を継続的に監視します。アラームがトリガーされると、指定した担当者全員に通知が送信されます。

重大度レベルが「Normal」の場合、アラームはトリガーされません。

属性値は、その属性に対して定義されている有効なアラームのリストに照らして評価されます。アラームのリストは次の順序でチェックされ、属性に対して定義された有効なアラームを含む最初のアラームクラスが特定されます。

1. アラームの重大度が「Critical」から「Notice」までのグローバルカスタムアラーム
2. アラームの重大度が「Critical Down」から「Notice」に設定されているデフォルトアラームです。

NMS サービスは、上位のアラームクラスで属性に対する有効なアラームを検出すると、そのクラス内でのみ評価し、NMS サービスは、他の優先順位の低いクラスとは比較しません。つまり、ある属性に対してグローバルカスタムアラームが有効になっている場合、NMS サービスはグローバルカスタムアラームに対してのみ属性値を評価します。デフォルトアラームは評価されません。したがって、ある属性の有効なデフォルトアラームがアラームのトリガーに必要な条件を満たしていても、同じ属性の（指定した条件を満たさない）グローバルカスタムアラームが有効な場合はトリガーされません。アラームはトリガーされず、通知は送信されません。

#### アラームのトリガー例

次の例を参考に、グローバルカスタムアラームとデフォルトアラームのトリガー方法について理解してください。

次の例では、次の表に示すように、ある属性に対してグローバルカスタムアラームとデフォルトアラームが定義されて有効になっています。

	グローバルカスタムアラームしきい値 (有効)	デフォルトのアラームしきい値 (有効)
注意	1500 以上	>=1000
マイナー	15、000 以上	>=1000
メジャー (Major)	15、000 以上	>= 25、000

値が 1000 のときにこの属性が評価されると、アラームはトリガーされず、通知は送信されません。

グローバルカスタムアラームはデフォルトアラームより優先されます。1000 という値は、グローバルカスタムアラームのどの重大度レベルのしきい値にも達していません。その結果、アラームレベルは Normal と評価されます。

このシナリオのあとでグローバルカスタムアラームを無効にしても、何も変わりません。新しいアラームレベルがトリガーされるためには、属性値が再評価される必要があります。

グローバルカスタムアラームが無効な状態で属性値が再評価されると、属性値はデフォルトアラームのしきい値に照らして評価されます。その結果 Notice レベルのアラームがトリガーされ、指定した担当者に E メール通知が送信されます。

同じ重大度のアラームです

同じ属性に対する2つのグローバルカスタムアラームの重大度が同じ場合、アラームは優先順位の高い順で評価されます。

たとえば、UMEM が 50MB に下がった場合、最初のアラーム (= 50000000) はトリガーされますが、その下のアラーム (<= 100000000) はトリガーされません。



**Global Alarms**

Updated: 2016-03-17 16:05:31 PDT

### Global Custom Alarms (0 Result(s))

Enabled	Service	Attribute	Severity	Message	Operator	Value	Additional Recipients	Actions
<input checked="" type="checkbox"/>	SSM	UMEM (Available Memory)	Minor	Under 50	=	5000		
<input checked="" type="checkbox"/>	SSM	UMEM (Available Memory)	Minor	under100	<=	1000		

アラームの順序を逆にした場合、UMEM が 100MB に下がると、最初のアラーム (<= 100000000) はトリガーされますが、その下のアラーム (= 50000000) はトリガーされません。



## Global Custom Alarms (0 Result(s))

Enabled	Service	Attribute	Severity	Message	Operator	Value	Additional Recipients	Actions
<input checked="" type="checkbox"/>	SSM	UMEM (Available Memory)	Minor	under10i	<=	1000		
<input checked="" type="checkbox"/>	SSM	UMEM (Available Memory)	Minor	Under 50	=	5000		

## Default Alarms

Filter by Disabled Defaults

0 Result(s)

Enabled	Service	Attribute	Severity	Message	Operator	Value	Actions
---------	---------	-----------	----------	---------	----------	-------	---------

Apply Changes

## 通知

通知には、アラームの発生またはサービスの状態の変更が報告されます。アラーム通知は E メールまたは SNMP で送信できます。

あるアラームしきい値に達したときに複数のアラームと通知が送信されないようにするために、アラームの重大度が属性の現在のアラームの重大度に照らしてチェックされます。変更がない場合、それ以上のアクションは実行されません。つまり、NMS サービスは、システムの監視を継続するにあたり、ある属性のアラーム状態を初めて検出したときにのみアラームを生成して通知を送信します。属性の新しいしきい値に達したことが検出された場合は、アラームの重大度が変わり、新しい通知が送信されます。条件が Normal レベルに戻ると、アラームはクリアされます。

アラーム状態の通知に表示されるトリガー値は、小数点以下 3 桁に四捨五入されます。したがって、1.9999 の属性値はしきい値が「2.0 未満」のアラームをトリガーしますが、アラーム通知にはトリガー値が 2.0 と表示されます。

## 新しいサービス

新しいグリッドノードまたはサイトの追加によって新しいサービスが追加されると、そのサービスにはデフォルトアラームとグローバルカスタムアラームが継承されます。

## アラームとテーブル

テーブルに表示されるアラーム属性は、システムレベルで無効にすることができます。テーブル内の個々の行に対してアラームを無効にすることはできません。

たとえば、次の表に、Critical レベルの VMFI (Entries Available) アラームを 2 つ示します。(\* support \* > \* Tools \* > \* Grid topology \* を選択します。次に、「\*\_ストレージノード\_\* > \* SSM \* > \* リソース \*」を選択します。)

CriticalレベルのVMFIアラームがトリガーされないように、VMFIアラームを無効にすることができます（Criticalレベルのアラームは両方とも緑で表に表示されます）。ただし、表の行の1つのアラームを無効にして、一方のVMFIアラームがCriticalレベルのアラームとして表示され、もう一方が緑のままになるようにすることはできません。

## Volumes

Mount Point	Device	Status	Size	Space Available	Total Entries	Entries Available	Write Cache
/	sda1	Online	10.6 GB	7.46 GB	655,360	559,263	Enabled
/var/local	sda3	Online	63.4 GB	59.4 GB	3,932,160	3,931,842	Unknown
/var/local/rangedb/0	sdb	Online	53.4 GB	53.4 GB	52,428,800	52,427,856	Enabled
/var/local/rangedb/1	sdc	Online	53.4 GB	53.4 GB	52,428,800	52,427,848	Enabled
/var/local/rangedb/2	sdd	Online	53.4 GB	53.4 GB	52,428,800	52,427,856	Enabled

現在のアラーム（従来のシステム）を確認応答する

システム属性がアラームのしきい値に達すると、従来のアラームがトリガーされます。レガシーアラームのリストを縮小またはクリアする場合は、アラームを確認することができます。

作業を開始する前に

- を使用して Grid Manager にサインインする必要があります ["サポートされている Web ブラウザ"](#)。
- Acknowledge alarms権限が必要です。

このタスクについて

レガシーアラームシステムは引き続きサポートされるため、新しいアラームが発生するたびに、Current Alarms ページのレガシーアラームのリストが増加します。通常、アラームは無視してかまいません（アラートによってシステムが見やすくなるため）。また、アラームを確認済みにすることもできます。



必要に応じて、アラートシステムに完全に移行した場合は、各レガシーアラームを無効にして、アラームがトリガーされないようにしたり、レガシーアラームの数に追加されたりしないようにすることができます。

アラームを確認すると、そのアラームはグリッドマネージャの Current Alarms ページに表示されなくなります。ただし、アラームが次の重大度レベルでトリガーされるか、解決されて再び発生する場合は除きます。



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

手順

1. **support>\* Alarms**（レガシー）> **Current alarms \*** を選択します。

The alarm system is the legacy system. The alert system offers significant benefits and is easier to use. See [Managing alerts and alarms](#) in the instructions for monitoring and troubleshooting StorageGRID.

## Current Alarms

Last Refreshed: 2020-05-27 09:41:39 MDT

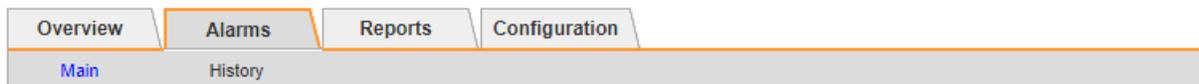
Show Acknowledged Alarms (1 - 1 of 1)

Severity	Attribute	Service	Description	Alarm Time	Trigger Value	Current Value
 Major	ORSU (Outbound Replication Status)	Data Center 1/DC1-ARC1/ARC	Storage Unavailable	2020-05-26 21:47:18 MDT	Storage Unavailable	Storage Unavailable

Show  Records Per Page  Previous < 1 > Next

2. テーブルでサービス名を選択します。

選択したサービスの Alarms タブが表示されます（ \* support \* > \* Tools \* > \* Grid topology \* > \* Grid Node\* > \* Service\* > \* Alarms \* ）。



### Alarms: ARC (DC1-ARC1) - Replication

Updated: 2019-05-24 10:46:48 MDT

Severity	Attribute	Description	Alarm Time	Trigger Value	Current Value	Acknowledge Time	Acknowledge
 Major	ORSU (Outbound Replication Status)	Storage Unavailable	2019-05-23 21:40:08 MDT	Storage Unavailable	Storage Unavailable		<input type="checkbox"/>

Apply Changes 

3. アラームの\*チェックボックスを選択し、[変更の適用]\*をクリックします。

ダッシュボードまたは[Current Alarms]ページにアラームが表示されなくなります。



アラームを確認しても、他の管理ノードには通知されません。そのため、別の管理ノードからダッシュボードを表示した場合、アクティブなアラームが引き続き表示されることがあります。

4. 必要に応じて、確認済みのアラームを表示します。
  - a. **support**>\* Alarms (レガシー) > Current alarms \* を選択します。
  - b. 「 \* 確認済みアラームを表示」を選択します。

確認済みのアラームが表示されます。

The alarm system is the legacy system. The alert system offers significant benefits and is easier to use. See [Managing alerts and alarms in the instructions for monitoring and troubleshooting StorageGRID](#).

## Current Alarms

Last Refreshed: 2020-05-27 17:38:58 MDT

Show Acknowledged Alarms (1 - 1 of 1)

Severity	Attribute	Service	Description	Alarm Time	Trigger Value	Current Value	Acknowledge Time
 Major	ORSU (Outbound Replication Status)	<a href="#">Data Center 1/DC1-ARC1/ARC</a>	Storage Unavailable	2020-05-26 21:47:18 MDT	Storage Unavailable	Storage Unavailable	2020-05-27 17:38:14 MDT

Show  Records Per Page  Previous « 1 » Next

デフォルトアラームの表示（従来のシステム）

すべてのデフォルトのレガシーアラームのリストを表示できます。

作業を開始する前に

- を使用して Grid Manager にサインインする必要があります ["サポートされている Web ブラウザ"](#)。
- これで完了です ["特定のアクセス権限"](#)。



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

手順

1. **[support>]** > **[\* Alarms (legac)>]** > **[ Global alarms]** を選択します。
2. **[フィルタ条件]** で、**[\* 属性コード\*]** または **[\* 属性名\*]** を選択します。
3. **[等しい]** には、アスタリスクを入力します。 \*
4. 矢印をクリックします  または、**Enter** キーを押します。

すべてのデフォルトアラームが表示されます。



## Global Custom Alarms (0 Result(s))

Enabled	Service	Attribute	Severity	Message	Operator	Value	Additional Recipients	Actions
<input type="checkbox"/>								

## Default Alarms

Filter by Attribute Code equals \*

## 221 Result(s)

Enabled	Service	Attribute	Severity	Message	Operator	Value	Actions
<input checked="" type="checkbox"/>		IQSZ (Number of Objects)	Major	Greater than 10,000,000	>=	10000000	
<input checked="" type="checkbox"/>		IQSZ (Number of Objects)	Minor	Greater than 1,000,000	>=	1000000	
<input checked="" type="checkbox"/>		IQSZ (Number of Objects)	Notice	Greater than 150,000	>=	150000	
<input checked="" type="checkbox"/>		XCVF (% Completion)	Notice	Foreground Verification Completed	=	100	
<input checked="" type="checkbox"/>	ADC	ADCA (ADC Status)	Minor	Error	>=	10	
<input checked="" type="checkbox"/>	ADC	ADCE (ADC State)	Notice	Standby	=	10	
<input checked="" type="checkbox"/>	ADC	ALIS (Inbound Attribute Sessions)	Notice	Over 100	>=	100	
<input checked="" type="checkbox"/>	ADC	ALOS (Outbound Attribute Sessions)	Notice	Over 200	>=	200	

## 過去のアラームとアラーム頻度の確認（従来のシステム）

問題のトラブルシューティングでは、過去に過去のアラームがトリガーされた頻度を確認できます。

作業を開始する前に

- を使用して Grid Manager にサインインする必要があります "サポートされている Web ブラウザ"。
- これで完了です "特定のアクセス権限"。



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

## 手順

1. 一定の期間にトリガーされたすべてのアラームのリストを表示する手順は、次のとおりです。
  - a. **[support>] > [\* Alarms (legac)>] > [ Historical alarms]** を選択します。
  - b. 次のいずれかを実行します。
    - いずれかの期間をクリックします。

- カスタム範囲を入力し、\* カスタムクエリ \* をクリックします。
2. 特定の属性に対してアラームがトリガーされた頻度を確認するには、次の手順を実行します。
    - a. サポート \* > ツール \* > グリッドトポロジ \* を選択します。
    - b. **grid node**>*service* または *component*>\* Alarms > History \* を選択します
    - c. リストから属性を選択します。
    - d. 次のいずれかを実行します。

- いずれかの期間をクリックします。
- カスタム範囲を入力し、\* カスタムクエリ \* をクリックします。

アラームは新しいものから順番に表示されます。

- e. [ALARMS HISTORY REQUEST] フォームに戻るには、[\* 履歴 \*] をクリックします。

## グローバルカスタムアラームの作成 (従来のシステム)

従来のシステムでグローバルカスタムアラームを使用して特定の監視要件に対処している場合があります。グローバルカスタムアラームでは、デフォルトアラームよりも優先されるアラームレベルを設定したり、デフォルトアラームのない属性を監視したりできます。

作業を開始する前に

- を使用して Grid Manager にサインインする必要があります ["サポートされている Web ブラウザ"](#)。
- これで完了です ["特定のアクセス権限"](#)。



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

グローバルカスタムアラームはデフォルトアラームを上書きします。デフォルトアラームの値は、どうしても必要な場合以外は変更しないでください。デフォルトアラームを変更すると、アラームとなるはずの問題が発覚しなくなる危険があります。



アラーム設定を変更する場合は注意してください。たとえば、あるアラームのしきい値を引き上げると、根本的な問題が検出されない可能性があります。アラームの設定を変更する前に、変更案についてテクニカルサポートと検討してください。

手順

1. [**support**>] > [\* Alarms (legac)>] > [Global alarms] を選択します。
2. グローバルカスタムアラームのテーブルに新しい行を追加します。
  - 新しいアラームを追加するには、\* Edit \* をクリックします  (最初のエントリの場合) または \* Insert \* を入力します  アイコン"]。



Global Custom Alarms (0 Result(s))

Enabled	Service	Attribute	Severity	Message	Operator	Value	Additional Recipients	Actions
<input checked="" type="checkbox"/>	ARC	ARCE (ARC State)	Notice	Standby	=	10		
<input checked="" type="checkbox"/>	ARC	AROQ (Objects Queued)	Minor	At least 6000	>=	6000		
<input checked="" type="checkbox"/>	ARC	AROQ (Objects Queued)	Notice	At least 3000	>=	3000		

Default Alarms

Filter by Attribute Code equals AR\*

9 Result(s)

Enabled	Service	Attribute	Severity	Message	Operator	Value	Actions
<input checked="" type="checkbox"/>	ARC	ARCE (ARC State)	Notice	Standby	=	10	
<input checked="" type="checkbox"/>	ARC	AROQ (Objects Queued)	Minor	At least 6000	>=	6000	
<input checked="" type="checkbox"/>	ARC	AROQ (Objects Queued)	Notice	At least 3000	>=	3000	
<input checked="" type="checkbox"/>	ARC	ARRF (Request Failures)	Major	At least 1	>=	1	
<input checked="" type="checkbox"/>	ARC	ARRV (Verification Failures)	Major	At least 1	>=	1	
<input checked="" type="checkbox"/>	ARC	ARVF (Store Failures)	Major	At least 1	>=	1	
<input checked="" type="checkbox"/>	NMS	ARRC (Remaining Capacity)	Notice	Below 10	<=	10	
<input checked="" type="checkbox"/>	NMS	ARRS (Repository Status)	Major	Disconnected	<=	9	
<input checked="" type="checkbox"/>	NMS	ARRS (Repository Status)	Notice	Standby	<=	19	

Apply Changes

- デフォルトアラームを変更するには、デフォルトアラームを検索します。
  - i. [フィルタ条件]で、[\*属性コード\*]または[\*属性名\*]を選択します。
  - ii. 検索文字列を入力します。

4文字を指定するか、ワイルドカードを使用します(例: a????またはAB\*)。アスタリスク(\*)は複数の文字を表し、疑問符(?)は単一の文字を表します。

- iii. 矢印をクリックします を押すか、\*Enter\*を押します。
- iv. 結果のリストで、\*コピー\*をクリックします をクリックします。

デフォルトアラームがグローバルカスタムアラームのテーブルにコピーされます。

3. グローバルカスタムアラームの設定に必要な変更を加えます。

見出し	説明
有効	このチェックボックスをオンまたはオフにして、アラームを有効または無効にします。

見出し	説明
属性	<p>選択したサービスまたはコンポーネントに該当するすべての属性のリストから、監視対象の属性の名前とコードを選択します。 属性に関する情報を表示するには、* 情報 * をクリックします  をクリックします。</p>
重大度	<p>アラームのレベルを示すアイコンとテキスト。</p>
メッセージ	<p>アラームの理由です（例： connection lost 、 storage space below 10% ）。</p>
演算子	<p>値のしきい値に対して現在の属性値をテストするための演算子：</p> <ul style="list-style-type: none"> <li>• = 等しい</li> <li>• &gt; より大きい</li> <li>• &lt; より小さい</li> <li>• &gt;= より大きいか等しい</li> <li>• &lt;= 以下</li> <li>• ≠ 等しくありません</li> </ul>
価値	<p>アラームのしきい値。演算子を使用して属性の実際の値に対してテストします。 1つの数値、コロンで指定した数値範囲（1：3）、または数値と範囲をカンマで区切ったリストを入力できます。</p>
受信者の追加	<p>アラームがトリガーされたときに通知を受け取る E メールアドレスの追加リストです。これは、 <b>[Alarms&gt;*Email Setup*]</b> ページに設定されているメーリングリストに加えて行われます。カンマで区切って指定します。</p> <p>*注:*メーリングリストを操作するには、SMTPサーバーのセットアップが必要です。メーリングリストを追加する前に、SMTP が設定されていることを確認してください。 カスタムアラームの通知で、グローバルカスタムアラームまたはデフォルトアラームの通知を上書きすることができます。</p>

見出し	説明
アクション	<p>次の操作を行うためのコントロールボタン  行を編集します</p> <p>[+]  アイコン"] 行を挿入します</p> <p>[+]  行を削除します</p> <p>[+]  行を上下にドラッグします</p> <p>[+]  行をコピーします</p>

4. [変更の適用 \*] をクリックします。

#### アラームの無効化（従来のシステム）

従来のアラームシステムのアラームはデフォルトで有効になっていますが、不要なアラームは無効にすることができます。新しいアラートシステムに完全に移行したあとに、古いアラームを無効にすることもできます。



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

#### デフォルトアラームの無効化（レガシーシステム）

システム全体でいずれかの従来のデフォルトアラームを無効にすることができます。

作業を開始する前に

- を使用して Grid Manager にサインインする必要があります "[サポートされている Web ブラウザ](#)"。
- これで完了です "[特定のアクセス権限](#)"。

このタスクについて

現在アラームがトリガーされている属性のアラームを無効にしても、現在のアラームはクリアされません。次回その属性がアラームのしきい値を超えるとアラームが無効になります。または、トリガーされたアラームをクリアできます。



新しいアラートシステムに完全に移行するまでは、従来のアラームを無効にしないでください。そうしないと、重大な処理を完了できなくなるまで、根本的な問題が検出されない可能性があります。

手順

1. [**support**>] > [\* Alarms (legac)>] > [Global alarms] を選択します。
2. 無効にするデフォルトアラームを検索します。
  - a. [デフォルトアラーム] セクションで、[\* フィルタを \* > \* 属性コード \* でフィルタ] または [\* 属性名 \*] を選択します。

b. 検索文字列を入力します。

4文字を指定するか、ワイルドカードを使用します（例：a????またはAB\*）。アスタリスク（\*）は複数の文字を表し、疑問符（?）は単一の文字を表します。

c. 矢印をクリックします  を押すか、\* Enter \* を押します。



[\*Disabled Defaults] を選択すると、現在無効になっているすべてのデフォルトアラームのリストが表示されます。

3. 検索結果リストから、[編集]アイコンをクリックします  をクリックします。



## Global Alarms

Updated: 2017-03-30 15:47:43 MDT

### Global Custom Alarms (0 Result(s))

Enabled	Service	Attribute	Severity	Message	Operator	Value	Additional Recipients	Actions
<input type="checkbox"/>								   

### Default Alarms

Filter by Attribute Code equals U\* 

3 Result(s)

Enabled	Service	Attribute	Severity	Message	Operator	Value	Actions
<input checked="" type="checkbox"/>	SSM	UMEM (Available Memory)	 Critical	Under 10000000	<=	10000000	 
<input checked="" type="checkbox"/>	SSM	UMEM (Available Memory)	 Major	Under 50000000	<=	50000000	 
<input type="checkbox"/>	SSM	UMEM (Available Memory)	 Minor	Under 100000000	<=	100000000	 

Apply Changes 

選択したアラームの\* Enabled \*チェックボックスがアクティブになります。

4. [有効]チェックボックスをオフにします。

5. [変更の適用\*]をクリックします。

デフォルトアラームは無効です。

グローバルカスタムアラームの無効化（従来のシステム）

システム全体で従来のグローバルカスタムアラームを無効にすることができます。

作業を開始する前に

- を使用して Grid Manager にサインインする必要があります ["サポートされている Web ブラウザ"](#)。
- これで完了です ["特定のアクセス権限"](#)。

このタスクについて

現在アラームがトリガーされている属性のアラームを無効にしても、現在のアラームはクリアされません。次回その属性がアラームのしきい値を超えるとアラームが無効になります。または、トリガーされたアラームをクリアできます。

手順

1. [support>] > [\* Alarms (legac)>] > [ Global alarms] を選択します。
2. Global Custom Alarms テーブルで、\* Edit \* をクリックします  をクリックします。
3. [有効]チェックボックスをオフにします。



Global Custom Alarms (1 Result(s))

Enabled	Service	Attribute	Severity	Message	Operator	Value	Additional Recipients	Actions
<input type="checkbox"/>	All	RDTE (Tivoli Storage Manager State)	Major	Offline	=	10		   

Default Alarms

Filter by Disabled Defaults 

0 Result(s)

Enabled	Service	Attribute	Severity	Message	Operator	Value	Actions
---------	---------	-----------	----------	---------	----------	-------	---------

Apply Changes 

4. [変更の適用 \*] をクリックします。

グローバルカスタムアラームは無効になっています。

トリガーされたアラームのクリア（従来のシステム）

古いアラームがトリガーされた場合は、確認せずにクリアできます。

作業を開始する前に

- を用意しておく必要があります Passwords.txt ファイル。

現在アラームがトリガーされている属性のアラームを無効にしても、アラームはクリアされません。このアラームは、属性が変わったときに無効になります。アラームを確認することも、属性値の変化（アラームの状態の変化）を待たずにアラームをすぐにクリアしたい場合は、トリガーされたアラームをクリアできます。これは、値があまり変化しない属性（状態属性など）に対してアラームをすぐにクリアしたい場合に便利です。

1. アラームを無効にします。
2. 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. に記載されているパスワードを入力します Passwords.txt ファイル。
  - c. 次のコマンドを入力してrootに切り替えます。 `su -`

d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

`root`としてログインすると、プロンプトがから変わります `$` 終了: `#`。

3. NMSサービスを再開します。 `service nms restart`

4. 管理ノードからログアウトします。 `exit`

アラームが解除されます。

#### アラームの通知の設定 (従来のシステム)

StorageGRID システムでは、Eメールとを自動的に送信できます "SNMP 通知" アラームがトリガーされるか、サービスの状態が変わったとき。

デフォルトでは、アラームのEメール通知は送信されません。Eメール通知の場合は、Eメールサーバを設定し、Eメール受信者を指定する必要があります。SNMP通知の場合は、SNMP エージェントを設定する必要があります。

#### アラーム通知のタイプ (従来のシステム)

レガシーアラームがトリガーされると、StorageGRID システムは重大度レベルとサービス状態の2種類のアラーム通知を送信します。

#### 重大度レベルの通知

選択した重大度レベルのレガシーアラームがトリガーされると、アラーム Eメール通知が送信されます。

- 注意
- マイナー
- メジャー (Major)
- 重要

メーリングリストは、選択した重大度のアラームに関連するすべての通知を受信します。また、アラームが解決されたか、別の重大度レベルになったことによって、アラームレベルが解除されたときにも通知が送信されます。

#### サービス状態の通知

サービス状態の通知は、サービス (LDR サービスや NMS サービスなど) が選択したサービス状態になったとき、および選択したサービス状態でなくなったときに送信されます。サービス状態通知は、サービスが次のサービス状態になったとき、またはその状態になったときに送信されます。

- 不明です
- 意図的な停止

メーリングリストは、選択した状態の変更に関連するすべての通知を受信します。

## アラーム用 E メールサーバの設定（従来型システム）

従来のアラームがトリガーされたときに StorageGRID から E メール通知を送信するには、SMTP メールサーバ設定を指定する必要があります。StorageGRID システムは電子メールのみを送信し、電子メールを受信することはできません。

作業を開始する前に

- を使用して Grid Manager にサインインする必要があります ["サポートされている Web ブラウザ"](#)。
- これで完了です ["特定のアクセス権限"](#)。

このタスクについて

以下の設定を使用して、従来のアラーム E メール通知と AutoSupport E メールメッセージに使用する SMTP サーバを定義します。これらの設定は、アラート通知には使用されません。



AutoSupportパッケージのプロトコルとしてSMTPを使用する場合は、すでにSMTPメールサーバが設定されている可能性があります。アラームの E メール通知には同じ SMTP サーバが使用されるため、この手順はスキップしてかまいません。を参照してください ["StorageGRID の管理手順"](#)。

SMTP は、Eメールの送信用にサポートされている唯一のプロトコルです。

手順

1. **support>**\* Alarms（レガシー）> Legacy email setup\* を選択します。
2. [電子メール]メニューから、[**Server**]を選択します。

[Email Server] ページが表示されます。このページは、AutoSupportパッケージ用のEメールサーバの設定にも使用されます。

Use these settings to define the email server used for alarm notifications and for AutoSupport messages. These settings are not used for alert notifications. See [Managing alerts and alarms](#) in the instructions for monitoring and troubleshooting StorageGRID.



## Email Server

Updated: 2016-03-17 11:11:59 PDT

### E-mail Server (SMTP) Information

Mail Server	<input type="text"/>
Port	<input type="text"/>
Authentication	<input type="button" value="Off"/>
Authentication Credentials	Username: <input type="text" value="root"/> Password: <input type="password" value="*****"/>
From Address	<input type="text"/>
Test E-mail	To: <input type="text"/> <input type="checkbox"/> Send Test E-mail

Apply Changes

3. 次の SMTP メールサーバ設定を追加します。

項目	説明
メールサーバ	SMTP メールサーバの IP アドレス。以前に管理ノードで DNS を設定している場合は、IP アドレスではなくホスト名を入力できます。
ポート	SMTP メールサーバにアクセスするためのポート番号。
認証	SMTP メールサーバの認証を許可します。デフォルトでは、認証はオフです。
認証クレデンシャル	SMTP メールサーバのユーザ名とパスワード。認証がオンに設定されている場合は、SMTP メールサーバにアクセスするためのユーザ名とパスワードを指定する必要があります。

4. [送信元アドレス \*] に、SMTP サーバが送信元電子メールアドレスとして認識する有効な電子メールアドレスを入力します。これは、E メールメッセージの送信元となる公式な E メールアドレスです。
5. 必要に応じて、テスト用 E メールを送信して SMTP メールサーバの設定が正しいことを確認します。
  - a. [電子メールのテスト > 宛先 \*] ボックスに、アクセスできるアドレスを 1 つ以上追加します。

1 つの E メールアドレスまたは E メールアドレスのカンマ区切りのリストを入力できます。テスト用 E メールを送信しても NMS サービスでは成功したかどうかを確認されないため、テスト受信者の受信ボックスを確認する必要があります。

b. [ テスト電子メールの送信 \*] を選択します。

6. [ 変更の適用 \*] をクリックします。

SMTP メールサーバの設定が保存されます。テスト用 E メールを入力した場合は、その E メールが送信されます。テストメールはすぐにメールサーバに送信され、通知キューからは送信されません。複数の管理ノードがあるシステムでは、各管理ノードから E メールが送信されます。テスト用 E メールが届けば、SMTP メールサーバの設定は正しく、NMS サービスはメールサーバに正常に接続しています。NMS サービスとメールサーバの接続に問題がある場合は、Minor 重大度レベルの Legacy MINS ( NMS Notification Status ) アラームがトリガーされます。

## アラーム E メールテンプレートの作成 (従来のシステム)

E メールテンプレートを使用して、従来のアラーム E メール通知のヘッダー、フッター、および件名をカスタマイズできます。E メールテンプレートを使用すると、本文に同じ内容を含む一意の通知をさまざまなメーリングリストに送信できます。

作業を開始する前に

- を使用して Grid Manager にサインインする必要があります "サポートされている Web ブラウザ"。
- これで完了です "特定のアクセス権限"。

このタスクについて

以下の設定を使用して、従来のアラーム通知に使用する E メールテンプレートを定義します。これらの設定は、アラート通知には使用されません。

メーリングリストごとに異なる連絡先情報が必要になる場合があります。テンプレートには、メールメッセージの本文は含まれません。

手順

1. **support>\* Alarms** (レガシー) > **Legacy email setup\*** を選択します。
2. [ 電子メール ] メニューから、[ **Templates** ] を選択します。
3. [ **編集 ( Edit )** ] をクリックします。  (または \* Insert \* )  アイコン] 最初のテンプレートではない場合) をクリックします。



Template (0 - 0 of 0)

Template Name	Subject Prefix	Header	Footer	Actions
Template One	Notifications	All Email Lists	From SGWS	

Show  Records Per Page



4. 新しい行に次の項目を追加します。

項目	説明
テンプレート名	テンプレートの識別に使用する一意の名前。テンプレート名は重複できません。
件名の接頭辞	任意。Eメールの件名の先頭に表示されるプレフィックスです。プレフィックスを使用すると、メールフィルタを簡単に設定し、通知を整理できます。
ヘッダー	任意。メール本文の先頭に表示されるヘッダーテキストです。ヘッダーテキストを使用すると、会社名や住所などの情報を本文の前に配置できます。
フッター	任意。メッセージ本文の末尾に表示されるフッターテキストです。フッターテキストを使用すると、連絡先の電話番号や Web サイトへのリンクなどのリマインダ情報を本文の末尾に配置できます。

5. [変更の適用 \*] をクリックします。

通知の新しいテンプレートが追加されます。

### アラーム通知のメーリングリストの作成 (従来システム)

メーリングリストを使用すると、古いアラームがトリガーされたときやサービスの状態が変わったときに通知を送信することができます。アラームの E メール通知を送信するには、少なくとも 1 つのメーリングリストを作成する必要があります。1 人の受信者に通知を送信するには、1 つの E メールアドレスを含むメーリングリストを作成します。

作業を開始する前に

- を使用して Grid Manager にサインインする必要があります ["サポートされている Web ブラウザ"](#)。

- これで完了です "特定のアクセス権限"。
- メーリングリストに E メールテンプレート（カスタムのヘッダー、フッター、件名）を指定する場合は、テンプレートを作成しておく必要があります。

このタスクについて

以下の設定を使用して、従来のアラーム E メール通知に使用するメーリングリストを定義します。これらの設定は、アラート通知には使用されません。

手順

1. **support**>\* Alarms（レガシー）> Legacy email setup\* を選択します。
2. [E メール] メニューから [\* リスト \*] を選択します。
3. [編集（Edit）] をクリックします。 （または \* Insert \*）  アイコン] 最初のメーリングリストではない場合）をクリックします。



## Email Lists

Updated: 2016-03-17 11:56:24 PDT

Lists (0 - 0 of 0)

Group Name	Recipients	Template	Actions
<input type="text"/>	<input type="text"/>	<input type="text"/>	  

Show  Records Per Page

« »

Apply Changes 

4. 新しい行に次の項目を追加します。

項目	説明
グループ名	<p>メーリングリストを識別する一意の名前。メーリングリスト名は重複できません。</p> <ul style="list-style-type: none"> <li>• 注意： * メーリングリストの名前を変更しても、そのメーリングリスト名を使用する他の場所に変更は反映されません。新しいメーリングリスト名を使用するように、設定済みの通知をすべて手動で更新する必要があります。</li> </ul>
受信者	<p>通知の送信先となる単独の E メールアドレス、設定済みのメーリングリスト、または E メールアドレスおよびメーリングリストをカンマで区切って指定します。</p> <ul style="list-style-type: none"> <li>• 注意： * 電子メールアドレスが複数のメーリングリストに属している場合は、通知をトリガーするイベントが発生すると、1 通の電子メール通知のみが送信されます。</li> </ul>

項目	説明
テンプレート	必要に応じて、Eメールテンプレートを選択し、このメーリングリストのすべての受信者に送信される通知に一意的ヘッダー、フッター、および件名を追加します。

5. [変更の適用 \*] をクリックします。

新しいメーリングリストが作成されます。

#### アラームの E メール通知の設定（従来のシステム）

従来のアラームシステムのEメール通知を受信するには、受信者がメーリングリストのメンバーであり、そのリストが[Notifications]ページに追加されている必要があります。通知は、指定した重大度レベルのアラームがトリガーされた場合やサービスの状態が変わった場合にのみ、受信者に E メールを送信するように設定されています。このため、受信者は受信する必要がある通知のみを受信します。

作業を開始する前に

- 使用して Grid Manager にサインインする必要があります ["サポートされている Web ブラウザ"](#)。
- これで完了です ["特定のアクセス権限"](#)。
- 設定済みの E メールリストが必要です。

このタスクについて

以下の設定を使用して、従来のアラームの通知を設定します。これらの設定は、アラート通知には使用されません。

E メールアドレス（またはリスト）が複数のメーリングリストに属している場合、通知をトリガーするイベントが発生すると E メール通知は 1 通だけ送信されます。たとえば、重大度に関係なくすべてのアラームの通知を受信するように、組織内の 1 つの管理者グループを設定できます。また、別のグループは、重大度が Critical のアラームの通知のみ必要とします。両方のリストに所属できます。Critical レベルのアラームがトリガーされると通知が 1 通だけ送信されます。

手順

1. **support>\* Alarms**（レガシー）> **Legacy email setup\*** を選択します。
2. [電子メール]メニューから、**[Notifications]** を選択します。
3. [編集（Edit）] をクリックします。 （または \* Insert \*）  アイコン"] 最初の通知ではない場合）をクリックします。
4. [電子メールリスト] でメーリングリストを選択します。
5. 1 つ以上のアラーム重大度レベルとサービス状態を選択します。
6. [変更の適用 \*] をクリックします。

選択したアラーム重大度レベルまたはサービス状態のアラームがトリガーまたは変更されると、メーリングリストに通知が送信されます。

## メーリングリスト（従来のシステム）のアラーム通知を停止する

メーリングリストでアラームに関する通知を受信しないようにするには、メーリングリストのアラーム通知を停止します。たとえば、に移行したあとに、古いアラームに関する通知をアラート E メール通知を停止することができます。

作業を開始する前に

- を使用して Grid Manager にサインインする必要があります ["サポートされている Web ブラウザ"](#)。
- これで完了です ["特定のアクセス権限"](#)。

以下の設定を使用して、レガシーアラームシステムの E メール通知を停止します。これらの設定は、アラート E メール通知には適用されません。



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

手順

1. **support>\* Alarms**（レガシー）> Legacy email setup\* を選択します。
2. [電子メール]メニューから、**[Notifications]** を選択します。
3. [編集（Edit）] をクリックします。  をクリックします。
4. [Suppress]で、停止するメーリングリストの横にあるチェックボックスを選択するか、列の上部にある\*[Suppress]\*を選択してすべてのメーリングリストを停止します。
5. [変更の適用 \*] をクリックします。

選択したメーリングリストに対して古いアラーム通知が停止されます。

従来のアラームを表示します

システム属性がアラームのしきい値に達すると、アラーム（従来のシステム）がトリガーされます。現在アクティブなアラームは、Current Alarms ページから表示できます。



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

作業を開始する前に

- を使用して Grid Manager にサインインする必要があります ["サポートされている Web ブラウザ"](#)。

手順

1. **support>\* Alarms**（レガシー）> Current alarms \* を選択します。

The alarm system is the legacy system. The alert system offers significant benefits and is easier to use. See [Managing alerts and alarms in the instructions for monitoring and troubleshooting StorageGRID](#).

## Current Alarms

Last Refreshed: 2020-05-27 09:41:39 MDT

Show Acknowledged Alarms (1 - 1 of 1)

Severity	Attribute	Service	Description	Alarm Time	Trigger Value	Current Value
 Major	ORSU (Outbound Replication Status)	Data Center 1/DC1-ARC1/ARC	Storage Unavailable	2020-05-26 21:47:18 MDT	Storage Unavailable	Storage Unavailable

Show  Records Per Page  Previous < 1 > Next

アラームアイコンは、各アラームの重大度を次のように示します。

をクリックします。	色 (Color)	アラームの重大度	意味
	黄色	注意	ノードはグリッドに接続されていますが、正常な状態ではありません。通常の動作に影響はありません。
	薄いオレンジ	マイナー	ノードはグリッドに接続されていますが、正常な状態ではありません。将来的に動作に影響する可能性があります。さらに重大な問題にならないように調査が必要です。
	濃いオレンジ	メジャー (Major)	ノードはグリッドに接続されていますが、正常な状態ではありません。すでに動作に影響が及んでいます。エスカレーションを防ぐために早急な対応が必要です。
	赤	重要	ノードはグリッドに接続されていますが、正常な状態ではありません。正常に動作しなくなっています。問題にはすぐに対処する必要があります。

- アラームをトリガーした原因となった属性を確認するには、テーブルで属性名を右クリックします。
- アラームのその他の詳細情報を表示するには、テーブルでサービス名をクリックします。

選択したサービスの Alarms タブが表示されます (\* support \* > \* Tools \* > \* Grid topology \* > \* Grid Node\* > \* Service\* > \* Alarms \* )。



## Alarms: ARC (DC1-ARC1) - Replication

Updated: 2019-05-24 10:46:48 MDT

Severity	Attribute	Description	Alarm Time	Trigger Value	Current Value	Acknowledge Time	Acknowledge
Major	ORSU (Outbound Replication Status)	Storage Unavailable	2019-05-23 21:40:08 MDT	Storage Unavailable	Storage Unavailable		<input type="checkbox"/>

Apply Changes

4. 現在のアラームの数を消去するには、必要に応じて次の操作を行います。

- アラームを確認します。確認済みのアラームは、重大度レベルが次のレベルでトリガーされるか、解決されてから再度発生するまで、レガシーアラームの数に含まれなくなります。
- システム全体で特定のデフォルトアラームまたはグローバルカスタムアラームを無効にして、再度トリガーされないようにします。

### 関連情報

"アラーム一覧 (従来のシステム) "

"現在のアラーム (従来のシステム) に確認応答する"

"アラームの無効化 (従来のシステム) "

アラーム一覧 (従来のシステム)

次の表に、これらの従来のデフォルトアラームをすべて示します。アラームがトリガーされた場合は、この表のアラームコードを参照して、推奨される対処方法を確認できます。



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

コード	名前	サービス	推奨される対処方法
ABRL	使用可能な属性リレー	BADC、BAMS、BARC、BCLB、BCMN、BCMN、BLDR、BNMS、BSSM、BDDS	Attribute Relay Service を実行しているサービス (ADC サービス) への接続をできるだけ早くリストアします。属性リレーが接続されていないと、グリッドノードからNMSサービスに属性の値を報告できません。そのため、NMS サービスでサービスのステータスの監視やサービスの属性の更新を行うことができなくなります。  問題が解決しない場合は、テクニカルサポートにお問い合わせください。

コード	名前	サービス	推奨される対処方法
ACMS	使用可能なメタデータサービス	BARC、BLDR、BCMN	<p>LDR サービスまたは ARC サービスからの DDS サービスへの接続が失われた場合にアラームがトリガーされます。この場合、取り込みまたは読み出しのトランザクションを処理できません。DDS サービスを使用できない状態が短時間の一時問題のみである場合は、トランザクションが遅延する可能性があります。</p> <p>このアラームを解除し、サービスのすべての機能を復旧するには、DDS サービスへの接続を確認してリストアします。</p>
ACTS	クラウドの階層化サービスのステータス	円弧 (Arc)	<p>ターゲットタイプが「Cloud Tiering - Simple Storage Service (S3)」のアーカイブノードにのみ適用されます。</p> <p>アーカイブノードの ACTS 属性が「Read-Only Enabled」または「Read-Write Disabled」に設定されている場合、「Read-Write Enabled」に設定する必要があります。</p> <p>認証エラーによって Major アラームがトリガーされた場合は、デスティネーションバケットに関連付けられているクレデンシャルを確認し、必要に応じて値を更新します。</p> <p>それ以外の理由で Major アラームがトリガーされた場合は、テクニカルサポートに連絡してください。</p>
ADCA	ADC ステータス	ADC	<p>アラームがトリガーされた場合は、<code>* support * &gt; * Tools * &gt; * Grid topology *</code> を選択します。次に、<code>* site_ * &gt; * _ grid node * &gt; * ADC * &gt; * Overview * &gt; * Main * and * ADC * &gt; * Alarms * &gt; * Main *</code> を選択して、アラームの原因を確認します。</p> <p>問題が解決しない場合は、テクニカルサポートにお問い合わせください。</p>
ADCE	ADC State のことです	ADC	<p>「ADC State」の値が「Standby」の場合は、しばらくサービスを監視し、問題が解決しなければテクニカルサポートに連絡します。</p> <p>「ADC State」の値が「Offline」の場合は、サービスを再起動します。問題が解決しない場合は、テクニカルサポートにお問い合わせください。</p>

コード	名前	サービス	推奨される対処方法
AITE	読み出し状態	BARC	<p>ターゲットタイプが「Tivoli Storage Manager (TSM)」のアーカイブノードにのみ適用されます。</p> <p>「Retrieve State」の値が「Waiting for Target」の場合は、TSM ミドルウェアサーバを調べ、正常に動作していることを確認します。アーカイブノードを StorageGRID システムに追加したばかりの場合は、アーカイブノードから対象の外部アーカイブストレージシステムへの接続が正しく設定されていることを確認します。</p> <p>「Archive Retrieve State」の値が「Offline」の場合は、状態を「Online」に更新できるか試します。サポート * &gt; ツール * &gt; グリッドトポロジ * を選択します。次に、 * site _ * &gt; _ grid node * &gt; ARC * &gt; Retrieve * &gt; Configuration * &gt; Main * を選択し、 * Archive Retrieve State * &gt; Online * を選択して、 * Apply Changes * をクリックします。</p> <p>問題が解決しない場合は、テクニカルサポートにお問い合わせください。</p>
AITU	ステータスを取得します	BARC	<p>「Retrieve Status」の値が「Target Error」の場合は、対象の外部アーカイブストレージシステムにエラーがないかを確認します。</p> <p>「Archive Retrieve Status」の値が「Session Lost」の場合は、対象の外部アーカイブストレージシステムがオンラインで正常に動作していることを確認します。ターゲットとのネットワーク接続を確認します。</p> <p>「Archive Retrieve Status」の値が「Unknown Error」の場合は、テクニカルサポートに連絡してください。</p>
ALIS	インバウンド属性セッション	ADC	<p>属性リレーのインバウンド属性セッション数が大幅に増加している場合、StorageGRID システムのバランスが悪くなっている可能性があります。通常の状態であれば、属性セッションはADC サービスに均等に分散されます。バランスが悪い状態が続くと、パフォーマンスの問題につながる可能性があります。</p> <p>問題が解決しない場合は、テクニカルサポートにお問い合わせください。</p>
ALOS	アウトバウンド属性セッション	ADC	<p>ADC サービスの属性セッションが多く、過負荷状態になっています。このアラームがトリガーされた場合は、テクニカルサポートに連絡してください。</p>

コード	名前	サービス	推奨される対処方法
ALUR	到達不能な属性リポジットリ	ADC	<p>NMS サービスとのネットワーク接続を調べ、属性リポジットリに接続できることを確認します。</p> <p>このアラームがトリガーされ、ネットワーク接続に問題がない場合は、テクニカルサポートに連絡してください。</p>
AMQS (AMQS)	キューに登録された監査メッセージ	BADC、BAMS、BARC、BCLB、BCMN、BCMN、BLDR、BNMS、BDDS	<p>監査メッセージを監査リレーまたは監査リポジットリにすぐに転送できない場合、メッセージはディスクキューに格納されます。ディスクキューがいっぱいになると、システムが停止する可能性があります。</p> <p>時間内に対応して停止を回避できるように、ディスクキュー内のメッセージ数が次のしきい値に達すると AMQS アラームがトリガーされます。</p> <ul style="list-style-type: none"> <li>• Notice : 10 万件を超えるメッセージ</li> <li>• Minor : 50 万件以上のメッセージ</li> <li>• Major : 200 万件以上のメッセージ</li> <li>• Critical : 500 万件以上のメッセージ</li> </ul> <p>AMQS アラームがトリガーされた場合は、システムの負荷を確認します。大量のトランザクションが発生していた場合は、時間が経つとアラームは自然に解消されます。この場合、このアラームは無視してかまいません。</p> <p>アラームが解除されず重大度が上がった場合は、キューサイズのグラフを確認します。数時間から数日にわたって数値が増え続けている場合は、監査の負荷がシステムの監査キャパシティを超えている可能性があります。クライアントの処理率を下げるか、監査レベルを「Error」または「Off」に変更して、ログに記録される監査メッセージの数を減らしてください。を参照してください <a href="#">"監査メッセージとログの送信先を設定します"</a>。</p>

コード	名前	サービス	推奨される対処方法
AOTE	ストアの状態	BARC	<p>ターゲットタイプが「Tivoli Storage Manager (TSM)」のアーカイブノードにのみ適用されます。</p> <p>「Store State」の値が「Waiting for Target」の場合は、外部アーカイブストレージシステムを調べ、正常に動作していることを確認します。アーカイブノードを StorageGRID システムに追加したばかりの場合は、アーカイブノードから対象の外部アーカイブストレージシステムへの接続が正しく設定されていることを確認します。</p> <p>「Store State」の値が「Offline」の場合は、「Store Status」の値を確認します。問題がある場合は解決してから、「Store State」を「Online」に戻します。</p>
AOTU	ストアのステータス	BARC	<p>「Store Status」の値が「Session Lost」の場合は、外部アーカイブストレージシステムが接続されてオンラインになっていることを確認します。</p> <p>「Target Error」の値を入力して、外部アーカイブストレージシステムにエラーがないかを確認します。</p> <p>「Store Status」の値が「Unknown Error」の場合は、テクニカルサポートに連絡してください。</p>
APMS	ストレージマルチパス接続	SSM のことです	<p>マルチパス状態アラームが「Degraded」と表示された場合は (* support &gt; Tools &gt; Grid topology、*<b>site</b> &gt; *<b>grid node</b>* &gt; * SSM &gt; Events * を選択)、次の手順を実行します。</p> <ol style="list-style-type: none"> <li>インジケータライトが表示されていないケーブルを接続するか交換します。</li> <li>1~5 分ほど待ちます。</li> </ol> <p>最初のケーブルを接続してから少なくとも5分後までは、もう一方のケーブルを抜かないでください。それよりも早くケーブルを取り外すと原因、ルートボリュームが読み取り専用になり、ハードウェアの再起動が必要になります。</p> <ol style="list-style-type: none"> <li>SSM &gt; Resources * ページに戻り、[Storage Hardware]セクションでマルチパスのステータスが「Degraded」が「Nominal」に変わったことを確認します。</li> </ol>

コード	名前	サービス	推奨される対処方法
ARCE	アークの状態	円弧 (Arc)	<p>ARC サービスの状態は、ARC のすべてのコンポーネント (Replication、Store、Retrieve、Target) が起動されるまでは「Standby」となり、その後、Online に移行します。</p> <p>「ARC State」の値が「Standby」から「Online」に切り替わらない場合は、ARC のコンポーネントのステータスを確認します。</p> <p>「ARC State」の値が「Offline」の場合は、サービスを再起動します。問題が解決しない場合は、テクニカルサポートにお問い合わせください。</p>
AROQ	Objects Queued (オブジェクトのキュー)	円弧 (Arc)	<p>このアラームは、対象の外部アーカイブストレージシステムの問題が原因でリムーバブルストレージデバイスが低速になっている場合や、複数の読み取りエラーが発生している場合にトリガーされることがあります。外部アーカイブストレージシステムにエラーがないかどうかを確認し、正常に動作していることを確認します。</p> <p>このエラーは、データ要求の割合が高いことが原因で発生することがあります。この場合は、システムアクティビティが少なくなるとキューに登録されたオブジェクトの数も少なくなります</p>

コード	名前	サービス	推奨される対処方法
ARRF	要求の失敗	円弧 (Arc)	<p>対象の外部アーカイブストレージシステムからの読み出しに失敗した場合、一時的な問題が原因である可能性があるため、アーカイブノードで読み出しが再試行されます。ただし、オブジェクトデータが破損している場合や完全に使用できないものとしてマークされている場合は、読み出しが失敗することはありません。この場合、アーカイブノードで読み出しの再試行が繰り返され、「Request Failures」の値が増え続けることとなります。</p> <p>このアラームは、要求されたデータを格納するストレージメディアが破損していることを示している可能性があります。外部アーカイブストレージシステムを調べて問題を詳しく診断します。</p> <p>オブジェクトデータがアーカイブにないことが判明した場合は、オブジェクトを StorageGRID システムから削除する必要があります。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。</p> <p>このアラームをトリガーした問題が解消されたら、障害数をリセットします。サポート &gt; ツール &gt; グリッドトポロジ * を選択します。次に、 * site_ * &gt; * _grid node * &gt; * ARC * &gt; * Retrieve * &gt; * Configuration * &gt; * Main * を選択し、 * Reset Request Failure Count * を選択して、 * Apply Changes * をクリックします。</p>
ARRV	検証エラー	円弧 (Arc)	<p>この問題の診断と修正については、テクニカルサポートにお問い合わせください。</p> <p>このアラームをトリガーした問題を解決したら、障害数をリセットします。サポート &gt; ツール &gt; グリッドトポロジ * を選択します。次に、 * site_ * &gt; * _grid node * &gt; * ARC * &gt; * Retrieve * &gt; * Configuration * &gt; * Main * を選択し、 * Reset Verification Failure Count * を選択して * Apply Changes * をクリックします。</p>

コード	名前	サービス	推奨される対処方法
ARVF	Store Failures (ストア障害)	円弧 (Arc)	<p>このアラームは、対象の外部アーカイブストレージシステムのエラーが原因で発生することがあります。外部アーカイブストレージシステムにエラーがないかどうかを確認し、正常に動作していることを確認します。</p> <p>このアラームをトリガーした問題が解消されたら、障害数をリセットします。サポート &gt; ツール &gt; グリッドトポロジ * を選択します。次に、 * site_ * &gt; * _grid node * &gt; * ARC * &gt; * Retrieve * &gt; * Configuration * &gt; * Main * を選択し、 * Reset Store Failure Count * を選択して、 * Apply Changes * をクリックします。</p>
ASXP	監査共有	AMS	<p>「Audit Shares」の値が「Unknown」の場合にアラームがトリガーされます。このアラームは、管理ノードのインストールまたは設定に問題があることを示している可能性があります。</p> <p>問題が解決しない場合は、テクニカルサポートにお問い合わせください。</p>
AUMA	AMSステータス	AMS	<p>「AMS Status」の値が「DB Connectivity Error」の場合は、グリッドノードを再起動します。</p> <p>問題が解決しない場合は、テクニカルサポートにお問い合わせください。</p>
AUME	AMSの状態	AMS	<p>「AMS State」の値が「Standby」の場合は、しばらく StorageGRID システムを監視し、問題が解決しない場合は、テクニカルサポートにお問い合わせください。</p> <p>「AMS State」の値が「Offline」の場合は、サービスを再起動します。問題が解決しない場合は、テクニカルサポートにお問い合わせください。</p>
補助	監査エクスポートのステータス	AMS	<p>アラームがトリガーされた場合は、原因となっている問題を修正し、AMS サービスを再起動します。</p> <p>問題が解決しない場合は、テクニカルサポートにお問い合わせください。</p>
BADD	ストレージコントローラ障害ドライブ数	SSM のことです	<p>このアラームは、StorageGRID アプライアンスの1つ以上のドライブが故障したか、または最適な状態でない場合にトリガーされます。必要に応じてドライブを交換します。</p>

コード	名前	サービス	推奨される対処方法
BASF	使用可能なオブジェクト ID	CMN	<p>StorageGRID システムのプロビジョニング時、CMN サービスに決まった数のオブジェクト ID が割り当てられます。このアラームは、StorageGRID システムでオブジェクト ID が不足し始めるとトリガーされます。</p> <p>ID の割り当てを増やすには、テクニカルサポートにお問い合わせください。</p>
低音	ID ブロック割り当てステータス	CMN	<p>デフォルトでは、ADCのクォーラムに到達できないためにオブジェクトIDを割り当てることができない場合にアラームがトリガーされます。</p> <p>CMN サービスでの ID ブロックの割り当てには、オンラインで接続されている ADC サービスがクォーラム（過半数）に達している必要があります。クォーラムが使用できない場合、ADCクォーラムが再確立されるまでCMNサービスは新しい識別子ブロックを割り当てることができません。ADC のクォーラムが失われても、グリッドのどこかに約 1 カ月分の ID がキャッシュされているため、通常は StorageGRID システムにすぐに影響が及ぶことはありません（クライアントによるコンテンツの取り込みと読み出しは引き続き可能です）。ただし、この状態が続くと、StorageGRID システムは新しいコンテンツを取り込むことができなくなります。</p> <p>アラームがトリガーされた場合は、ADC のクォーラムが失われた理由（ネットワークやストレージノードの障害など）を調べて適切に対処します。</p> <p>問題が解決しない場合は、テクニカルサポートにお問い合わせください。</p>
BRDT	コンピューティングコントローラシャーシの温度	SSM のことです	<p>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のしきい値を超えるとアラームがトリガーされます。</p> <p>過熱の原因となっているハードウェアコンポーネントや環境の問題を確認します。必要に応じて、コンポーネントを交換します。</p>

コード	名前	サービス	推奨される対処方法
BTOF	オフセット (Offset)	BADC、BLDR、BNMS、BAMS、BCLB、BCMN、BARC	<p>サービスの時間 (秒) とオペレーティングシステムの時間が大きく異なる場合にアラームがトリガーされます。通常の状態であれば、サービスは自動的に再同期されます。サービスの時間とオペレーティングシステムの時間のずれが大きくなると、システムの運用に影響を及ぼすことがあります。StorageGRID システムの時間ソースが正しいことを確認します。</p> <p>問題が解決しない場合は、テクニカルサポートにお問い合わせください。</p>
BTSE	クロックの状態	BADC、BLDR、BNMS、BAMS、BCLB、BCMN、BARC	<p>サービスの時間がオペレーティングシステムで追跡された時間と同期されていない場合にアラームがトリガーされます。通常の状態であれば、サービスは自動的に再同期されます。オペレーティングシステムの時間とのずれが大きくなると、システムの運用に影響を及ぼすことがあります。StorageGRID システムの時間ソースが正しいことを確認します。</p> <p>問題が解決しない場合は、テクニカルサポートにお問い合わせください。</p>
CAHP	Java ヒープ使用率	DDS	<p>Java のガベージコレクションが追いつかず、システムの正常な動作に必要なヒープスペースを確保できなくなった場合にアラームがトリガーされます。アラームは、DDS のメタデータストアに対するユーザーのワークロードがシステム全体で利用できるリソースを超えていることを示している可能性があります。ダッシュボードでILMのアクティビティを確認するか、* support &gt; Tools &gt; Grid topology を選択し、*<i>site</i>&gt;*<i>grid node</i>*&gt;* DDS &gt; Resources &gt; Overview &gt; Main *を選択します。</p> <p>問題が解決しない場合は、テクニカルサポートにお問い合わせください。</p>

コード	名前	サービス	推奨される対処方法
カーサ	データストアのステータス	DDS	<p>Cassandra のメタデータストアが使用できなくなるとアラームが生成されます。</p> <p>Cassandra のステータスを確認します。</p> <ol style="list-style-type: none"> <li>1. ストレージノードで、adminおよびとしてログインします su Passwords.txtファイルに記載されているパスワードを使用してrootに変更します。</li> <li>2. 入力するコマンド <code>service cassandra status</code></li> <li>3. Cassandraが実行されていない場合は再起動します。 <code>service cassandra restart</code></li> </ol> <p>このアラームは、ストレージノードに対するメタデータストア（Cassandra データベース）のリビルドが必要なことを示している可能性もあります。</p> <p>の Services : Status - Cassandra (SVST) アラームのトラブルシューティングに関する情報を参照してください "<a href="#">メタデータに関する問題のトラブルシューティング</a>"。</p> <p>問題が解決しない場合は、テクニカルサポートにお問い合わせください。</p>
ケース	データストアの状態	DDS	<p>このアラームは、インストール時または拡張時にトリガーされ、新しいデータストアがグリッドに追加されていることを示します。</p>
CCNA	コンピューティングハードウェア	SSM のことです	<p>このアラームは、StorageGRID アプライアンスのコンピューティングコントローラハードウェアのステータスが「Needs Attention」になるとトリガーされます。</p>

コード	名前	サービス	推奨される対処方法
CDLP	Metadata Used Space (Percent)	DDS	<p>このアラームは、「Metadata Effective Space (CEMS)」が 70% 使用済み (Minor アラーム)、90% 使用済み (Major アラーム)、100% 使用済み (Critical アラーム) に達した場合に、それぞれトリガーされます。</p> <p>このアラームが90%のしきい値に達すると、Grid Managerのダッシュボードに警告が表示されます。できるだけ早く拡張手順を実行して新しいストレージノードを追加する必要があります。を参照してください "<a href="#">グリッドを展開する</a>"。</p> <p>このアラームが 100% のしきい値に達した場合は、オブジェクトの取り込みを停止し、すぐにストレージノードを追加する必要があります。Cassandra は、コンパクションや修復などの必須処理を実行するために一定量のスペースを必要とします。オブジェクトメタデータの使用スペースが使用可能なスペースの 100% を超えると、これらの処理に影響します。望ましくない結果が生じる可能性があります。</p> <ul style="list-style-type: none"> <li>注：ストレージノードを追加できない場合は、テクニカルサポートにお問い合わせください。</li> </ul> <p>新しいストレージノードが追加されると、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が自動的にリバランシングされ、アラームが解除されません。</p> <p>の Low metadata storage アラートのトラブルシューティングに関する情報も参照してください "<a href="#">メタデータに関する問題のトラブルシューティング</a>"。</p> <p>問題が解決しない場合は、テクニカルサポートにお問い合わせください。</p>

コード	名前	サービス	推奨される対処方法
CMNA	CMNステータス	CMN	<p>CMN Status の値が Error の場合は、* support * &gt; * Tools * &gt; * Grid topology * を選択し、* _site_ * &gt; * _grid node_name * &gt; * CMN * &gt; * Overview * &gt; * Main * and * CMN * &gt; * Alarms * &gt; * Main * を選択してエラーの原因を確認し、問題のトラブルシューティングを行います。</p> <p>プライマリ管理ノードのハードウェアの更新時に CMN の状態が切り替わると（「CMN State」の値が「Standby」から「Online」に変わると）、アラームがトリガーされ、「CMN Status」の値が「No Online CMN」になります。</p> <p>問題が解決しない場合は、テクニカルサポートにお問い合わせください。</p>
CPRC	残り容量	NMS	<p>残り容量（NMS データベースに対して確立できる接続の数）が設定されたアラームの重大度を下回るとアラームがトリガーされます。</p> <p>アラームがトリガーされた場合は、テクニカルサポートに連絡してください。</p>
cPSA	コンピューティングコントローラの電源装置 A	SSM のことです	<p>StorageGRID アプライアンスのコンピューティングコントローラに電源装置 A を搭載した問題がある場合にアラームがトリガーされます。</p> <p>必要に応じて、コンポーネントを交換します。</p>
cPSB	コンピューティングコントローラの電源装置 B	SSM のことです	<p>StorageGRID アプライアンスのコンピューティングコントローラに電源装置 B を搭載した問題がある場合、アラームがトリガーされます。</p> <p>必要に応じて、コンポーネントを交換します。</p>
CPUT	コンピューティングコントローラの CPU 温度	SSM のことです	<p>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 の温度が公称のしきい値を超えるとアラームがトリガーされます。</p> <p>ストレージノードが StorageGRID アプライアンスである場合は、StorageGRID システムのコントローラを調査する必要があります。</p> <p>過熱の原因となっているハードウェアコンポーネントや環境の問題を確認します。必要に応じて、コンポーネントを交換します。</p>

コード	名前	サービス	推奨される対処方法
DNST	DNSステータス	SSM のことです	インストールが完了すると、SSM サービスで DNST アラームがトリガーされます。DNS の設定が完了し、新しいサーバの情報がすべてのグリッドノードに送られると、アラームはキャンセルされます。
ECCD	破損フラグメントが検出されました	LDR	<p>バックグラウンド検証プロセスでイレイジャーコーディングフラグメントの破損が検出されるとアラームがトリガーされます。破損したフラグメントが検出された場合、フラグメントの再構築が試行されます。「Corrupt Fragments Detected」属性と「Copies Lost」属性を 0 にリセットし、それらのカウントが再び増えるかどうかを確認します。カウントが増える場合は、ストレージノードの基盤となるストレージに問題がある可能性があります。イレイジャーコーディングオブジェクトデータのコピーは、失われたフラグメントまたは破損したフラグメントの数がイレイジャーコーディングのフォールトトレランスを超えないかぎり欠落とはみなされません。そのため、破損したフラグメントがあってもオブジェクトの読み出しは引き続き可能です。</p> <p>問題が解決しない場合は、テクニカルサポートにお問い合わせください。</p>
ECST	検証ステータス	LDR	<p>このアラームは、このストレージノード上のイレイジャーコーディングオブジェクトデータに対するバックグラウンド検証プロセスの現在のステータスを示します。</p> <p>バックグラウンド検証プロセスでエラーが発生すると、Major アラームがトリガーされます。</p>
FOPN	オープンファイル記述子	BADC、BAMS、BARC、BCLB、BCM N、BCM N、BLDR、BNMS、BSSM、BDDS	アクティビティのピーク時に FOPN が大きくなることがあります。アクティビティが少ない時間帯も低下しない場合は、テクニカルサポートにお問い合わせください。
HSTE	HTTPの状態	BLDR	HSTU の推奨処置を参照してください。

コード	名前	サービス	推奨される対処方法
ステュディオ	HTTPステータス	BLDR	<p>HSTEとHSTUは、S3、Swift、およびその他の内部StorageGRID トラフィックを含むすべてのLDRトラフィックのHTTPに関連しています。アラームは、次のいずれかの状況が発生したことを示します。</p> <ul style="list-style-type: none"> <li>• HTTPが手動でオフラインになっています。</li> <li>• Auto-Start HTTP 属性が無効になりました。</li> <li>• LDR サービスがシャットダウン中である。</li> </ul> <p>Auto-Start HTTP 属性はデフォルトで有効になっています。この設定を変更すると、再起動後も HTTP がオフラインのままになる可能性があります。</p> <p>必要に応じて、LDR サービスが再起動するまで待ちます。</p> <p>サポート * &gt; * ツール * &gt; * グリッドトポロジ * を選択します。次に、「*_ストレージ・ノード_* &gt; * LDR * &gt; * Configuration *」を選択します。HTTPがオフラインの場合は、オンラインにします。Auto-Start HTTP 属性が有効になっていることを確認します。</p> <p>HTTPがオフラインのままの場合は、テクニカルサポートにお問い合わせください。</p>
HTAS	HTTP を自動起動します	LDR	<p>起動時に HTTP サービスを自動的に開始するかどうかを指定します。これはユーザ指定の設定オプションです。</p>
IRSU	インバウンドレプリケーションステータス	BLDR、BARC	<p>インバウンドレプリケーションが無効になっていることを示します。構成設定を確認します。* support * &gt; * Tools * &gt; * Grid topology * を選択します。次に、*_site_* &gt; *_grid node_name* &gt; * LDR * &gt; * Replication * &gt; * Configuration * &gt; * Main * を選択します。</p>

コード	名前	サービス	推奨される対処方法
LATA (LATA)	平均レイテンシ	NMS	<p>接続に問題がないかを確認します。</p> <p>システムアクティビティを調べ、システムアクティビティが増えていることを確認します。システムアクティビティが増えれば、属性データアクティビティも増えます。このアクティビティが増加すると、属性データの処理に遅延が生じます。これは正常なシステムアクティビティであり、自然に解消されません。</p> <p>複数のアラームがないか確認します。トリガーされたアラームの数が多すぎると、平均レイテンシが高くなることがあります。</p> <p>問題が解決しない場合は、テクニカルサポートにお問い合わせください。</p>
LDRE	LDRの状態	LDR	<p>「LDR State」の値が「Standby」の場合は、引き続き状況を監視し、問題が解決しない場合はテクニカルサポートに連絡してください。</p> <p>「LDR State」の値が「Offline」の場合は、サービスを再起動します。問題が解決しない場合は、テクニカルサポートにお問い合わせください。</p>
失われました	Lost Objects	DDS、LDR	<p>要求されたオブジェクトのコピーを StorageGRID システム内のいずれの場所からも読み出せない場合にトリガーされます。LOST (Lost Objects) アラームがトリガーされる前に、欠落オブジェクトをシステム内の他の場所から読み出して置き換えることができます。</p> <p>損失オブジェクトとは、データが失われたことを表します。Lost Objects 属性の値は、ILM ポリシーを満たすためにコンテンツが DDS サービスで意図的にパーズされた場合を除き、オブジェクトの場所の数が 0 になるたびに増えていきます。</p> <p>LOST (Lost Object) アラームはすぐに調査する必要があります。問題が解決しない場合は、テクニカルサポートにお問い合わせください。</p> <p>"失われたオブジェクトデータと欠落しているオブジェクトデータのトラブルシューティング"</p>

コード	名前	サービス	推奨される対処方法
MCEP	管理インターフェイス証明書の有効期限	CMN	<p>管理インターフェイスへのアクセスに使用される証明書の有効期限が近づくとトリガーされます。</p> <ol style="list-style-type: none"> <li>1. Grid Manager から、 * configuration * &gt; * Security * &gt; * Certificates * を選択します。</li> <li>2. [* グローバル *] タブで、 [* 管理インターフェイス証明書 *] を選択します。</li> <li>3. "新しい管理インターフェイス証明書をアップロードします。"</li> </ol>
MINQ	キューに登録された電子メール通知	NMS	<p>NMS サービスをホストするサーバと外部のメールサーバのネットワーク接続を確認します。また、Eメールサーバの設定が正しいことを確認します。</p> <p>"アラーム用 E メールサーバの設定 (従来型システム)"</p>
分	電子メール通知のステータス	BNMS	<p>NMS サービスでメールサーバに接続できない場合に Minor アラームがトリガーされます。NMS サービスをホストするサーバと外部のメールサーバのネットワーク接続を確認します。また、Eメールサーバの設定が正しいことを確認します。</p> <p>"アラーム用 E メールサーバの設定 (従来型システム)"</p>
お見逃しなく	NMS インターフェイスエンジンステータス	BNMS	<p>インターフェイスコンテンツを収集および生成する管理ノードの NMS インターフェイスエンジンがシステムから切断されている場合にアラームがトリガーされます。Server Manager で、サーバの個々のアプリケーションが停止しているかどうかを確認します。</p>
ナン	ネットワーク自動ネゴシエーション設定	SSM のことです	<p>ネットワークアダプタの設定を確認します。設定は、ネットワークのルータとスイッチの設定と一致する必要があります。</p> <p>設定が正しくないと、システムのパフォーマンスに重大な影響を及ぼす可能性があります。</p>
NDUP (NDUP)	ネットワークのデュプレックス設定	SSM のことです	<p>ネットワークアダプタの設定を確認します。設定は、ネットワークのルータとスイッチの設定と一致する必要があります。</p> <p>設定が正しくないと、システムのパフォーマンスに重大な影響を及ぼす可能性があります。</p>

コード	名前	サービス	推奨される対処方法
NLNK	ネットワークリンク検出	SSM のことです	<p>ポートとスイッチのネットワークケーブル接続を確認します。</p> <p>ネットワークルータ、スイッチ、およびアダプタの設定を確認します。</p> <p>サーバを再起動します。</p> <p>問題が解決しない場合は、テクニカルサポートにお問い合わせください。</p>
NRER	受信エラー	SSM のことです	<p>NRER アラームの原因としては、次のようなものが考えられます。</p> <ul style="list-style-type: none"> <li>• Forward Error Correction (FEC; 前方誤り訂正) の不一致</li> <li>• スイッチポートと NIC の MTU が一致しません</li> <li>• リンクエラー率が高くなっています</li> <li>• NIC リングバッファオーバーラン</li> </ul> <p>の Network Receive Error (NRER) アラームのトラブルシューティングに関する情報を参照してください <a href="#">"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をトラブルシューティングする"</a>。</p>
NRLY の場合	使用可能な監査リレー	BADC、BARC、BCLB、BCMNM、BLDR、BNMS、BDDS	<p>監査リレーがADCサービスに接続されていないと、監査イベントを報告できません。接続がリストアされるまではキューに登録され、ユーザには提供されません。</p> <p>できるだけ早く ADC サービスへの接続をリストアします。</p> <p>問題が解決しない場合は、テクニカルサポートにお問い合わせください。</p>
NSCA	NMSステータス	NMS	<p>「NMS Status」の値が「DB Connectivity Error」の場合は、サービスを再起動します。問題が解決しない場合は、テクニカルサポートにお問い合わせください。</p>

コード	名前	サービス	推奨される対処方法
NSCE	NMS State (NMS 状態)	NMS	<p>「NMS State」の値が「Standby」の場合は、しばらく状況を監視し、問題が解決しなければテクニカルサポートに連絡します。</p> <p>「NMS State」の値が「Offline」の場合は、サービスを再起動します。問題が解決しない場合は、テクニカルサポートにお問い合わせください。</p>
NSPD	スピード	SSM のことです	<p>ネットワーク接続またはドライバの互換性の問題が原因である可能性があります。問題が解決しない場合は、テクニカルサポートにお問い合わせください。</p>
NTBR	空きテーブルスペース	NMS	<p>アラームがトリガーされた場合は、データベースの使用量がどのくらいのペースで変化しているかを確認します。時間とともに徐々に変化するのではなく、急激に低下した場合は、エラー状態を示します。問題が解決しない場合は、テクニカルサポートにお問い合わせください。</p> <p>アラームのしきい値を調整することで、追加のストレージの割り当てが必要になったときにプロアクティブに管理できます。</p> <p>使用可能なスペースがしきい値の下限（アラームのしきい値を参照）に達した場合は、テクニカルサポートに連絡してデータベースの割り当てを変更します。</p>
入力します	送信エラー	SSM のことです	<p>これらのエラーは、手動でリセットしなくても解消されます。クリアされない場合は、ネットワークハードウェアを確認してください。アダプタのハードウェアとドライバが正しくインストールされ、ネットワークのルータやスイッチと連携するように設定されていることを確認します。</p> <p>原因となっている問題を解決したら、カウンタをリセットします。サポート * &gt; ツール * &gt; グリッドポロジ * を選択します。次に、 * site_ * &gt; _grid node * &gt; SSM * &gt; Resources * &gt; Configuration * &gt; Main * を選択し、 * Reset Transmit Error Count * を選択して、 * Apply Changes * をクリックします。</p>
NTFQ	NTP 周波数オフセット	SSM のことです	<p>周波数オフセットが設定されたしきい値を超えている場合は、ハードウェアのローカルクロックに問題がある可能性があります。問題が解決しない場合は、テクニカルサポートに連絡して交換を手配してください。</p>

コード	名前	サービス	推奨される対処方法
NCLK	NTP ロック	SSM のことです	NTP デーモンが外部の時間ソースにロックされていない場合は、指定された外部時間ソースへのネットワーク接続とそれらの可用性および安定性を確認します。
NTOF	NTP 時間オフセット	SSM のことです	時間オフセットが設定されたしきい値を超えている場合は、ハードウェアのローカルクロックのオシレーターに問題がある可能性があります。問題が解決しない場合は、テクニカルサポートに連絡して交換を手配してください。
NTSJ	選択された時間ソースジッタ	SSM のことです	この値は、ローカルサーバ上の NTP が参照として使用している時間ソースの信頼性と安定性を示します。  アラームがトリガーされた場合は、時間ソースのオシレーターが故障しているか、時間ソースへの WAN リンクに問題がある可能性があります。
NTSU	NTPステータス	SSM のことです	「NTP Status」の値が「Not Running」の場合は、テクニカルサポートに連絡してください。
OPST の場合	全体的な電源ステータス	SSM のことです	StorageGRID アプライアンスの電源が推奨される動作電圧と大きく異なる場合にアラームがトリガーされます。  電源装置 A と B のステータスを調べ、どちらの電源装置に異常があるかを確認します。  必要に応じて、電源装置を交換します。
OQRT の場合	隔離されたオブジェクト	LDR	StorageGRID システムでオブジェクトが自動的にリストアされたあと、隔離されたオブジェクトを隔離ディレクトリから削除できます。  1. サポート * > ツール * > グリッドトポロジ * を選択します。 2. サイト * > ストレージノード * > LDR * > Verification * > Configuration * > Main * の順に選択します。 3. [* 隔離オブジェクトの削除 *] を選択します。 4. [変更の適用 *] をクリックします。  隔離されたオブジェクトが削除され、数がゼロにリセットされます。

コード	名前	サービス	推奨される対処方法
ORSU	アウトバウンドレプリケーションステータス	BLDR、BARC	<p>アウトバウンドレプリケーションを実行できず、ストレージがオブジェクトを読み出せない状態になっていることを示します。アウトバウンドレプリケーションが手動で無効になった場合にアラームがトリガーされます。サポート * &gt; ツール * &gt; グリッドトポロジ * を選択します。次に、 *_site_* &gt; *_grid node_name &gt; * LDR * &gt; * Replication * &gt; * Configuration * を選択します。</p> <p>LDR サービスでレプリケーションを実行できない場合にもアラームがトリガーされます。サポート * &gt; ツール * &gt; グリッドトポロジ * を選択します。次に、 *_site_* &gt; *_grid node_name * &gt; * ldr * &gt; * Storage * を選択します。</p>
OSLF	シェルフステータス	SSM のことです	<p>ストレージアプライアンスのストレージシェルフのいずれかのコンポーネントのステータスがデグレードになると、アラームがトリガーされます。ストレージシェルフコンポーネントには、IOM、ファン、電源装置、ドライブドロワーが含まれます。このアラームがトリガーされた場合は、アプライアンスのメンテナンス手順を参照してください。</p>
PMEM	サービスメモリ使用率（パーセント）	BADC、BAMS、BARC、BCLB、BCMN、BCMN、BLDR、BNMS、BSSM、BDDS	<p>には、Over Y% RAM の値を指定できます。Y は、サーバで使用されているメモリの割合を表します。</p> <p>80% 未満であれば問題ありません。90% を超える場合は問題があると考えられます。</p> <p>1つのサービスのメモリ使用率が高い場合は、状況を監視して調査します。</p> <p>問題が解決しない場合は、テクニカルサポートにお問い合わせください。</p>
PSAS	Power Supply A Status の順に選択します	SSM のことです	<p>StorageGRID アプライアンスの電源装置 A が推奨される動作電圧と大きく異なる場合にアラームがトリガーされます。</p> <p>必要に応じて、電源装置 A を交換します</p>
PSBS	電源装置 B のステータス	SSM のことです	<p>StorageGRID アプライアンスの電源装置 B が推奨される動作電圧と大きく異なる場合にアラームがトリガーされます。</p> <p>必要に応じて、電源装置 B を交換します</p>

コード	名前	サービス	推奨される対処方法
RDTE	Tivoli Storage Manager の状態	BARC	<p>ターゲットタイプが「Tivoli Storage Manager (TSM)」のアーカイブノードにのみ適用されます。</p> <p>「Tivoli Storage Manager State」の値が「Offline」の場合は、「Tivoli Storage Manager Status」を確認して問題を解決します。</p> <p>コンポーネントをオンラインに戻します。サポート * &gt; ツール * &gt; グリッドトポロジ * を選択します。次に、 * site _ * &gt; * _ grid node * &gt; * ARC * &gt; * Target * &gt; * Configuration * &gt; * Main * を選択し、 * Tivoli Storage Manager State * &gt; * Online * を選択して、 * Apply Changes * をクリックします。</p>
RDTU	Tivoli Storage Manager のステータス	BARC	<p>ターゲットタイプが「Tivoli Storage Manager (TSM)」のアーカイブノードにのみ適用されます。</p> <p>「Tivoli Storage Manager Status」の値が「Configuration Error」で、アーカイブノードを StorageGRID システムに追加したばかりの場合は、TSM ミドルウェアサーバが正しく設定されていることを確認します。</p> <p>「Tivoli Storage Manager Status」の値が「Connection Failure」または「Connection Failure、Retrying」の場合は、TSM ミドルウェアサーバのネットワーク設定、および TSM ミドルウェアサーバと StorageGRID システムの間のネットワーク接続を確認します。</p> <p>「Tivoli Storage Manager Status」の値が「Authentication Failure」または「Authentication Failure、Reconnecting」の場合、StorageGRID システムは TSM ミドルウェアサーバに接続できませんが、接続を認証できません。TSM ミドルウェアサーバでユーザ、パスワード、および権限が正しく設定されていることを確認し、サービスを再起動します。</p> <p>「Tivoli Storage Manager Status」の値が「Session Failure」の場合は、確立されたセッションが予期せずに切断されています。TSM ミドルウェアサーバと StorageGRID システムの間のネットワーク接続を確認します。ミドルウェアサーバにエラーがないかを確認します。</p> <p>「Tivoli Storage Manager Status」の値が「Unknown Error」の場合は、テクニカルサポートに連絡してください。</p>

コード	名前	サービス	推奨される対処方法
RIRF	インバウンドレプリケーション—失敗	BLDR、BARC	<p>このアラームは、負荷が高いときやネットワークが一時的に停止しているときに発生する可能性があります。このアラームは、システムアクティビティが減ると解除されます。レプリケーションの失敗回数が増え続ける場合は、ネットワークに問題がないかを調べ、ソースとデスティネーションの LDR サービスおよび ARC サービスがオンラインで使用可能な状態になっていることを確認します。</p> <p>カウントをリセットするには、* support * &gt; * Tools * &gt; * Grid topology * を選択し、* _site_ * &gt; * _grid node_name * &gt; * ldr * &gt; * Replication * &gt; * Configuration * &gt; * Main * を選択します。「* インバウンド複製エラー数のリセット *」を選択し、「* 変更を適用 *」をクリックします。</p>
RIRQ	Inbound Replications — Queued (インバウンドレプリケーション—キューイング済み)	BLDR、BARC	<p>負荷が高いときやネットワークが一時的に停止しているときにアラームが発生することがあります。このアラームは、システムアクティビティが減ると解除されます。レプリケーションのキューが増え続ける場合は、ネットワークに問題がないかを調べ、ソースとデスティネーションの LDR サービスおよび ARC サービスがオンラインで使用可能な状態になっていることを確認します。</p>
RORQ	Outbound Replications - Queued (アウトバウンドレプリケーション—キューイング済み)	BLDR、BARC	<p>アウトバウンドレプリケーションのキューには、ILM ルールを満たすためにコピーされるオブジェクトデータと、クライアントから要求されたオブジェクトが含まれます。</p> <p>システムが過負荷になると、アラームが発生することがあります。このアラームはシステムアクティビティが減ると解除されるため、しばらく状況を監視します。アラームが繰り返し発生する場合は、ストレージノードを追加して容量を増やします。</p>
SAVP の	使用可能な合計スペース (割合)	LDR	<p>使用可能なスペースがしきい値の下限に達した場合は、StorageGRID システムを拡張するか、オブジェクトデータをアーカイブノード経由でアーカイブに移動します。</p>

コード	名前	サービス	推奨される対処方法
SCAS	ステータス	CMN	<p>アクティブなグリッドタスクの「Status」の値が「Error」の場合は、グリッドタスクのメッセージを検索します。サポート * &gt; ツール * &gt; グリッドトポロジ * を選択します。次に、 *_site_* &gt; *_grid node_name_* &gt; * CMN * &gt; * Grid Tasks * &gt; * Overview * &gt; * Main * の順に選択します。グリッドタスクのメッセージにエラーに関する情報が表示されます（「check failed on node 12130011」など）。</p> <p>問題の調査と修正が完了したら、グリッドタスクを再起動します。サポート * &gt; ツール * &gt; グリッドトポロジ * を選択します。次に、 *_site_* &gt; *_grid node_name_* &gt; * CMN * &gt; * Grid Tasks * &gt; * Configuration * &gt; * Main * を選択し、 * Actions * &gt; * Run * を選択します。</p> <p>「Stopped」中のグリッドタスクの「Status」の値が「Error」の場合は、グリッドタスクをもう一度終了します。</p> <p>問題が解決しない場合は、テクニカルサポートにお問い合わせください。</p>
SCEP (SCEP)	ストレージ API サービスエンドポイントの証明書有効期限	CMN	<p>ストレージ API エンドポイントへのアクセスに使用される証明書の有効期限が近づくとトリガーされます。</p> <ol style="list-style-type: none"> <li>[ * configuration * &gt; * Security * &gt; * Certificates * ] を選択します。</li> <li>Global * タブで、 * S3 および Swift API 証明書 * を選択します。</li> <li><a href="#">"新しい S3 および Swift API 証明書をアップロードします。"</a></li> </ol>
SCHR	ステータス	CMN	<p>過去のグリッドタスクの「Status」の値が「Aborted」の場合は、原因を調べ、必要に応じてもう一度タスクを実行します。</p> <p>問題が解決しない場合は、テクニカルサポートにお問い合わせください。</p>
SCSA	ストレージコントローラ A	SSM のことです	<p>StorageGRID アプライアンスにストレージコントローラ A を搭載した問題があると、アラームがトリガーされます。</p> <p>必要に応じて、コンポーネントを交換します。</p>

コード	名前	サービス	推奨される対処方法
SCSB	ストレージコントローラ B	SSM のことです	StorageGRID アプライアンスにストレージコントローラ B を搭載した問題がある場合にアラームがトリガーされます。  必要に応じて、コンポーネントを交換します。  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 が搭載されていません
SHLH	健全性	LDR	オブジェクトストアの「Health」の値が「Error」の場合は、以下を確認して修正します。  <ul style="list-style-type: none"> <li>マウントされているボリュームの問題</li> <li>ファイルシステムエラー</li> </ul>
slsa	CPU Load Average (CPU 負荷平均)	SSM のことです	この値が大きいほど、システムはビジーになります。  「CPU Load Average」の値が高いまま推移している場合は、システムのトランザクション数を調べ、一時的な負荷の増加によるものかどうかを確認する必要があります。CPU 負荷の平均値のグラフを表示します。サポート > ツール > グリッドトポロジ * を選択します。次に、 *_site_* > *_grid node_name > * SSM * > * Resources * > * Reports * > * Charts * を選択します。  システムの負荷が高くない状況でも問題が解決しない場合は、テクニカルサポートにお問い合わせください。
SMST	Log Monitor State の略	SSM のことです	「Log Monitor State」の値が「Connected」にならない状態が続く場合は、テクニカルサポートに連絡してください。

コード	名前	サービス	推奨される対処方法
SMTT	合計イベント数	SSM のことです	<p>「 Total Events 」の値が 0 より大きい場合は、原因となる既知のイベント（ネットワーク障害など）がないかを確認します。これらのエラーが解消されていない（カウントが 0 にリセットされていない）と、 Total Events アラームがトリガーされる可能性があります。</p> <p>問題 が解決したら、カウンタをリセットしてアラームを解除します。ノード * &gt; * _site * &gt; * _grid node_name &gt; * Events * &gt; * Reset event counts * を選択します。</p> <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;">  イベント数をリセットするには、Grid トポロジページの設定権限が必要です。 </div> <p>「 Total Events 」の値が 0 の場合や数が増えて問題が解決しない場合は、テクニカルサポートに連絡してください。</p>
SNST	ステータス	CMN	<p>グリッドタスクバンドルの格納に問題があることを示します。「 Status 」の値が「 Checkpoint Error 」または「 Quorum Not Reached 」の場合は、半数を超える ADC サービスが StorageGRID システムに接続されていることを確認し、そのまま数分待ちます。</p> <p>問題が解決しない場合は、テクニカルサポートにお問い合わせください。</p>
SOSS	ストレージオペレーティングシステムのステータス	SSM のことです	<p>SANtricity OSでStorageGRIDアプライアンスのコンポーネントを含む問題「Needs Attention」が報告されるとアラームがトリガーされます。</p> <p>[* nodes（ノード）] を選択します次に、* アプライアンス・ストレージ・ノード * &gt; * ハードウェア * を選択します。下にスクロールして各コンポーネントのステータスを確認します。SANtricity OSでは、他のアプライアンスコンポーネントをチェックして問題を分離します。</p>
SSMA	SSMステータス	SSM のことです	<p>「 SSM Status 」の値が「 Error 」の場合は、「 * support * &gt; * Tools * &gt; * Grid topology * 」を選択し、「 * site _ * &gt; * _grid node * &gt; * SSM * &gt; * Main * and * SSM * &gt; * Overview * &gt; * Alarms * 」を選択して、アラームの原因を判断します。</p> <p>問題が解決しない場合は、テクニカルサポートにお問い合わせください。</p>

コード	名前	サービス	推奨される対処方法
SSME	SSMの状態	SSM のことです	<p>「SSM State」の値が「Standby」の場合は、しばらく状況を監視し、問題が解決しなければテクニカルサポートに連絡します。</p> <p>「SSM State」の値が「Offline」の場合は、サービスを再起動します。問題が解決しない場合は、テクニカルサポートにお問い合わせください。</p>
SSTS のコマンドです	ストレージステータス	BLDR	<p>「Storage Status」の値が「Insufficient Usable Space」の場合は、ストレージノードの使用可能なストレージがなくなり、データの取り込みが他の使用可能なストレージノードにリダイレクトされています。このグリッドノードからの読み出し要求は引き続き可能です。</p> <p>ストレージを追加する必要があります。エンドユーザの作業には影響しませんが、ストレージを追加しないかぎりアラームは解除されません。</p> <p>「Storage Status」の値が「Volume (s) Unavailable」の場合は、ストレージの一部が使用できない状態になっています。これらのボリュームでは格納も読み出しも実行できません。ボリュームの健全性を確認して詳細を確認します。 * support * &gt; * Tools * &gt; * Grid topology * を選択します。次に、 * site _ * &gt; * _grid node* &gt; * LDR * &gt; * Storage * &gt; * Overview * &gt; * Main * を選択します。ボリュームの健全性がオブジェクトストアのリストに表示されません。</p> <p>「Storage Status」の値が「Error」の場合は、テクニカルサポートに連絡してください。</p> <p><a href="#">"Storage Status (SSTS) アラームをトラブルシューティングします"</a></p>

コード	名前	サービス	推奨される対処方法
SVST	ステータス	SSM のことです	<p>このアラームは、サービスの実行の問題に関する他のアラームが解決されると解除されます。ソース側のサービスのアラームを追跡してリストアします。</p> <p>サポート * &gt; * ツール * &gt; * グリッドトポロジ * を選択します。次に、 * site _ * &gt; * _ grid node * &gt; * SSM * &gt; * Services * &gt; * Overview * &gt; * Main * の順に選択します。サービスのステータスが「Not Running」と表示される場合は、状態が「Administratively Down」です。サービスのステータスが「Not Running」と表示される状況は次のとおりです。</p> <ul style="list-style-type: none"> <li>• サービスが手動で停止されました (/etc/init.d/&lt;service&gt; stop)。</li> <li>• MySQL データベースを持つ問題 があり 'Server Manager' によって MI サービスがシャットダウンされます</li> <li>• グリッドノードが追加されたが開始されていない。</li> <li>• インストール時にグリッドノードが管理ノードに接続されていない。</li> </ul> <p>サービスが「Not Running」と表示される場合は、サービスを再起動します (/etc/init.d/&lt;service&gt; restart)。</p> <p>このアラームは、ストレージノードに対するメタデータストア (Cassandra データベース) のリビルドが必要なことを示している可能性もあります。</p> <p>問題が解決しない場合は、テクニカルサポートにお問い合わせください。</p> <p>"Services : Status - Cassandra (SVST) アラームのトラブルシューティングを行います"</p>
TMEM	メモリを取り付けた	SSM のことです	<p>ノードの搭載メモリが 24GiB 未満の場合、パフォーマンスの問題が発生し、システムが不安定になることがあります。システムの搭載メモリを 24GiB 以上に増やす必要があります。</p>
TPOP	保留中の処理です	ADC	<p>メッセージのキューが形成されている場合、ADC サービスが過負荷状態になっている可能性があります。StorageGRID システムに接続されている ADC サービスの数が少なすぎるのが考えられます。大規模な環境では、ADC サービスのコンピューティングリソースを増やすか、システムに ADC サービスを追加することが必要になる可能性があります。</p>

コード	名前	サービス	推奨される対処方法
UMEM	使用可能なメモリ	SSM のことです	使用可能な RAM が少なくなった場合は、ハードウェア問題 とソフトウェア RAM のどちらであるかを確認します。ハードウェア問題 以外の場合、または使用可能なメモリが 50MB（デフォルトのアラームのしきい値）を下回った場合は、テクニカルサポートに連絡してください。
VMFI	エントリが使用可能です	SSM のことです	追加のストレージが必要なことを示しています。テクニカルサポートにお問い合わせください。
VMFR	使用可能なスペース	SSM のことです	<p>「Space Available」の値が低すぎる（アラームのしきい値を参照）場合は、大きくなりすぎているログファイルや大量のディスクスペースを消費しているオブジェクト（アラームのしきい値を参照）がないかどうかを調べ、必要に応じてそれらを減らすか削除します。</p> <p>問題が解決しない場合は、テクニカルサポートにお問い合わせください。</p>
VMST	ステータス	SSM のことです	マウントされたボリュームの「Status」の値が「Unknown」の場合にアラームがトリガーされます。値が「Unknown」または「Offline」の場合は、基盤となるストレージデバイスの問題が原因でボリュームをマウントまたはアクセスできないことを示している可能性があります。
VPRI（VPRI）	検証の優先順位	BLDR、BARC	「Verification Priority」のデフォルトの値は「Adaptive」です。「Verification Priority」が「High」に設定されている場合、ストレージの検証が優先されてサービスの通常の運用に影響する可能性があるため、アラームがトリガーされます。
VSTU	オブジェクトの検証ステータス	BLDR	<p>サポート * &gt; * ツール * &gt; * グリッドトポロジ * を選択します。次に、 * site _ * &gt; * _ grid node * &gt; * LDR * &gt; * Storage * &gt; * Overview * &gt; * Main * を選択します。</p> <p>オペレーティングシステムで、ブロックデバイスやファイルシステムのエラーの兆候がないかどうかを確認します。</p> <p>「Object Verification Status」の値が「Unknown Error」の場合は、通常、下位レベルのファイルシステムやハードウェアの問題（I/O エラー）が原因で、ストレージ検証タスクが格納されたコンテンツにアクセスできないことを示します。テクニカルサポートにお問い合わせください。</p>

コード	名前	サービス	推奨される対処方法
XAMS の場合	到達不能な監査リポジトリ	BADC、BARC、BCLB、BCMN、BLDR、BNMS	管理ノードをホストするサーバへのネットワーク接続を確認します。  問題が解決しない場合は、テクニカルサポートにお問い合わせください。

## ログファイル参照

### ログファイルリファレンス：概要

StorageGRID には、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が用意されています。テクニカルサポートにトラブルシューティングを依頼すると、ログファイルを収集して転送するように求められることがあります。

ログは次のように分類されます。

- ["StorageGRID ソフトウェアのログ"](#)
- ["導入とメンテナンスのログ"](#)
- ["サードパーティソフトウェアのログ"](#)
- ["bystream.log について"](#)



各ログタイプの詳細情報は参考用です。これらのログは、テクニカルサポートが高度なトラブルシューティングに使用することを目的としています。監査ログや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ていません。

### ログにアクセスします

ログにアクセスするには、次の手順を実行します ["ログファイルとシステムデータを収集します"](#) 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アーカイブ。または、プライマリ管理ノードを使用できない場合や特定のノードに到達できない場合は、次の手順で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. に記載されているパスワードを入力します `Passwords.txt` ファイル。
3. 次のコマンドを入力してrootに切り替えます。 `su -`
4. に記載されているパスワードを入力します `Passwords.txt` ファイル。

### 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、カテゴリごとに説明されているログ、およびメトリックと debug コマンドの出力が含まれている追加ファイルが含まれています。

アーカイブの場所	説明
監査	通常のシステム動作中に生成される監査メッセージです。
base-os-logs	StorageGRID イメージのバージョンなど、ベースとなるオペレーティングシステムの情報。
バンドル	グローバル構成情報（バンドル）。
Cassandra	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（Grid）	デバッグを含む一般的なグリッドログ (bycast.log) および servermanager ログ。
grid.xml	グリッド構成ファイルをすべてのノードで共有
シュラウド	ハイアベイラビリティグループの指標とログ。
をインストールします	Gdu-server インストールログを確認します。
lumberjack.log	ログ収集に関連するデバッグメッセージ。
Lambda - アービトレータ	S3 Select プロキシ要求に関連するログです。
指標	Grafana、Jaeger、ノードエクスポート、および Prometheus のサービスログ。
計算ミス	Miscd アクセスログとエラーログ。
MySQL	MariaDB データベースの設定と関連ログ。
ネット	ネットワーク関連のスクリプトおよび Dyip サービスによって生成されるログ。
nginx	ロードバランサとグリッドフェデレーションの設定ファイルとログ。Grid Manager と Tenant Manager のトラフィックログも含まれます。
nginx-gw と入力します	ロードバランサとグリッドフェデレーションの設定ファイルとログ。
NTP	NTP 構成ファイルとログ：
OS	ノードとグリッドの状態ファイル（サービスを含む） pid。

アーカイブの場所	説明
その他	にログファイルがあります /var/local/log 他のフォルダには収集されていません。
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
prometheus-data	ログ収集に Prometheus データが含まれている場合、現在の Prometheus 指標。
プロビジョニング	グリッドのプロビジョニングプロセスに関連するログです。
ラフト	プラットフォームサービスで使用される Raft クラスタのログ。
SSH	SSHの設定およびサービスに関連するログ。
SNMP	SNMP エージェント設定およびアラーム許可 / 拒否リストは、SNMP 通知の送信に使用されます。
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。
system-commands.txt	StorageGRID コンテナコマンドの出力。ネットワークやディスクの使用状況などのシステム情報が含まれます。

## StorageGRID ソフトウェアのログ

StorageGRID のログを問題のトラブルシューティングに使用できます。



ログを外部syslogサーバに送信したり、監査情報の保存先を変更したりする場合（など）`broadcast.log` および ``nms.log`` を参照してください "[監査メッセージとログの送信先を設定します](#)"。

一般的な StorageGRID ログです

ファイル名	注：	にあります
/var/local/log/broadcast.log	プライマリ 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、[ <b>Site</b> >* <b>Node</b> >*SSM*>*Events] を選択します。	すべてのノード

ファイル名	注：	にあります
/var/local/log/bycast-err.log	のサブセットが含まれます bycast.log (ERRORとCRITICALの重大度のメッセージ)。クリティカルなメッセージはシステムにも表示されます。サポート * > * ツール * > * グリッドポロジ * を選択します。次に、 <b>[Site&gt;*Node*&gt;SSM*&gt;Events]</b> を選択します。	すべてのノード
/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格納されます。原因としては、アサーションエラー、違反、スレッドのタイムアウトなどが考えられます。  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、エラーを示しているわけではありません。	すべてのノード

#### 暗号関連のログ

ファイル名	注：	にあります
/var/local/log/ssh-config-generation.log	SSH設定の生成およびSSHサービスのリロードに関連するログが記録されます。	すべてのノード
/var/local/log/nginx/config-generation.log	nginx構成の生成とnginxサービスのリロードに関連するログが記録されます。	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サービスのリロード）に関連するログが記録されます。	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ポリシーの設定に関連するログが記録されます。	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：	にあります
/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構成とnginx-gw構成の生成に関連するログが記録されます。	すべてのノード

## NMS ログ

ファイル名	注：	にあります
/var/local/log/nms.log	<ul style="list-style-type: none"> <li>Grid Manager と Tenant Manager からの通知が記録されます。</li> <li>アラーム処理、Eメール通知、設定の変更など、NMS サービスの処理に関連するイベントが記録されます。</li> <li>システムで行われた設定の変更に伴う XML バンドルの更新が格納されます。</li> <li>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格納されます。</li> <li>ページ生成エラーや HTTP ステータス 500 エラーなど、Java Web サーバのエラーメッセージが格納されます。</li> </ul>	管理ノード
/var/local/log/nms.errlog	<p>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格納されます。</p> <p>対応するサービスの標準エラー（stderr）ストリームが格納されます。サービスごとに1つのログファイルがあります。これらのファイルは、サービスに問題がなければ通常は空になります。</p>	管理ノード
/var/local/log/nms.requestlog	管理 API から内部 StorageGRID サービスへの発信接続に関する情報が含まれます。	管理ノード

## Server Manager のログです

ファイル名	注：	にあります
/var/local/log/servermanager.log	サーバで実行されている Server Manager アプリケーションのログファイルです。	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です。	すべてのノード
/var/local/log/gridstat.errlog	Server Manager GUI のログファイルです。	すべてのノード

StorageGRID サービスのログ

ファイル名	注：	にあります
/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）ストリームが格納されます。サービスごとに1つのログファイルがあります。これらのファイルは、サービスに問題がなければ通常は空になります。	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/arc.errlog		アーカイブノード
/var/local/log/cassandra/system.log	メタデータストア（Cassandra データベース）の情報。新しいストレージノードの追加時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ます。	ストレージノード
/var/local/log/cassandra-reaper.log	Cassandra Reaper サービスの情報。Cassandra データベース内のデータの修復を実行します。	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、古いバージョンの StorageGRID からアップグレードされたシステムに存在する場合があります。古い情報が含まれています。	ストレージノード
/var/local/log/cts.errlog	このログファイルは、ターゲットタイプが * Cloud Tiering - Simple Storage Service（S3）.* の場合にのみ作成されます	アーカイブノード
/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

ファイル名	注：	にあります
/var/local/log/dynip *	グリッドで IP の動的な変更を監視してローカル設定を更新する dynip サービスに関連するログが記録されます。	すべてのノード
/var/local/log/grafana.log	Grid Manager で指標を視覚化するために使用される 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	ハイアベイラビリティグループに関連付けられているログ。	管理ノードとゲートウェイノード
/var/local/log/hagroups (events.log)	バックアップからマスターまたは障害への移行など、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	Jaeger サービスに関連付けられたログ。これは、トレース収集に使用されます。	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 サービスのログが記録されず。	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記録されます。を参照してください " <a href="#">S3 Select の管理ノードとゲートウェイノードの要件と制限事項</a> "。
/var/local/log/ldr.errlog		ストレージノード
/var/local/log/miscd/*。log	MISCd ( Information Service Control Daemon ) サービスのログが記録されます。このサービスは、他のノード上のサービスの照会と管理、およびノードの環境設定の管理 (他のノードで実行されているサービスの状態の照会など) を行うためのインターフェイスを提供します。	すべてのノード

ファイル名	注：	にあります
/var/local/log/nginx/*。log	nginx サービスのログが記録されます。このサービスは、各種のグリッドサービス（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、認証とセキュアな通信のメカニズムとして機能します。	すべてのノード
/var/local/log/nginx-gw/*。log	nginx-gwサービスに関連する一般的なログ（エラーログ、管理ノード上の制限された管理ポートのログなど）が記録されます。	管理ノードとゲートウェイノード
/var/local/log/nginx-gw/cgr-access.log 。gz	グリッド間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記録されます。	グリッドフェデレーション設定に応じて、管理ノード、ゲートウェイノード、またはその両方を選択します。グリッド間レプリケーションのデステイネーショングリッドでのみ検出されます。
/var/local/log/nginx-gw/endpoint-access.log。gz	クライアントからストレージノードへのS3およびSwiftトラフィックのロードバランシングを提供するロードバランササービスのアクセスログが記録されます。	管理ノードとゲートウェイノード
/var/local/log/persistence *	Persistence サービスのログが記録されます。このサービスは、リブート後も維持する必要があるルートディスク上のファイルを管理します。	すべてのノード
/var/local/log/prometheus.log	すべてのノードを対象に、node exporter サービスのログと ade-exporter サービスのログが記録されます。  管理ノードについては、Prometheus サービスと Alert Manager サービスのログも記録されます。	すべてのノード
/var/local/log/raft.log	RSM サービスで Rraft プロトコルに使用されるライブラリの出力が含まれます。	RSM サービスを搭載しているストレージノードです

ファイル名	注：	にあります
/var/local/log/rms.errlog	S3 プラットフォームサービスで使用される Replicated State Machine (RSM) サービスのログが記録されます。	RSM サービスを搭載しているストレージノードです
/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の処理に関連するログが記録されます。S3 クライアントアプリケーションを実装する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
/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記録されます。	すべてのノード
/var/local/log/update-syslog	システムの syslog 設定に対する変更に関連するログが記録されます。	すべてのノード
/var/local/log/update-traffic-classes.log	トラフィック分類子設定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	このノードでの「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記録されます。	すべてのノード

#### 関連情報

["bicast.log について"](#)

["S3 REST APIを使用する"](#)

#### 導入とメンテナンスのログ

導入とメンテナンスのログを問題のトラブルシューティングに使用できます。

ファイル名	注：	にあります
/var/local/log/install.log	ソフトウェアのインストール時に作成されます。インストールイベントが記録されます。	すべてのノード
/var/local/log/expansion-progress.log	拡張処理中に作成されます。拡張イベントが記録されます。	ストレージノード
/var/local/log/pa-move.log	の実行中に作成されます pa-move.sh スクリプト：	プライマリ管理ノード

ファイル名	注：	にあります
/var/local/log/pa-move-new (pa.log)	の実行中に作成されます 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)	の実行中に作成されます 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す。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とメンテナンスの手順に関連するイベントが記録されます。	プライマリ管理ノード
/var/local/log/send (admin_hw.log)	インストール時に作成されます。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記録されます。	すべてのノード
/var/local/log/upgrade.log	ソフトウェアのアップグレード中に作成されます。ソフトウェア更新イベントが記録されます。	すべてのノード

### サードパーティソフトウェアのログ

サードパーティソフトウェアのログを問題のトラブルシューティングに使用できます。

カテゴリ	ファイル名	注：	にあります
アーカイブ	/var/local/log/dsierror.log	TSM クライアント API のエラー情報。	アーカイブノード
MySQL	/var/local/log/mysql.err /var/local/log/mysql-slow.log	MySQL によって生成されるログファイルです。  mysql.err データベースのエラーや、起動やシャットダウンなどのイベントをキャプチャします。  mysql-slow.log (スロークエリログ) には、実行に10秒以上かかったSQLステートメントが記録されます。	管理ノード
オペレーティングシステム	/var/local/log/messages	このディレクトリには、オペレーティングシステムのログファイルが格納されます。これらのログに記録されたエラーは、Grid Manager にも表示されます。サポート * > * ツール * > * グリッドトポロジ * を選択します。次に、* Topology * > * Site * > * Node * > * SSM * > * Events * を選択します。	すべてのノード

カテゴリ	ファイル名	注：	にあります
NTP	/var/local/log/ntp.log  /var/lib/ntp/var/log/ntpstats/	<p>/var/local/log/ntp.log NTPのエラーメッセージのログファイルが格納されます。</p> <p>/var/lib/ntp/var/log/ntpstats/Directoryには、NTPタイミグ統計情報が格納されます</p> <p>loopstats ループフィルタの統計情報を記録します。</p> <p>peerstats には、ピア統計情報が記録されます</p>	すべてのノード

### bycast.log について

ファイル /var/local/log/bycast.log は、StorageGRID ソフトウェアのトラブルシューティングに使用する主要なファイルです。が `bycast.log` ファイルを選択します。ファイルに、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 はのサブセットです `bycast.log`。ERROR と CRITICAL の重大度のメッセージが含まれています。

必要に応じて、監査ログのデスティネーションを変更したり、監査情報を外部 syslog サーバに送信したりできます。外部 syslog サーバが設定されても、監査レコードのローカルログは引き続き生成および格納されます。を参照してください "[監査メッセージとログの送信先を設定します](#)"。

### bycast.log ファイルのローテーション

をクリックします `bycast.log` ファイルが1GBに達し、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。

保存されたファイルの名前が変更されます `bycast.log.1`` をクリックすると、新しいファイルの名前がになります ``bycast.log`。新しいとき `bycast.log` 1GBに達しました。 `bycast.log.1` が圧縮されて名前がに変更されます `bycast.log.2.gz`` および ``bycast.log` の名前がに変更され `bycast.log.1`。

の回転制限です `bycast.log` は21ファイルです。の22番目のバージョン `bycast.log` ファイルが作成され、最も古いファイルが削除されます。

の回転制限です `bycast-err.log` は7つのファイルです。



圧縮されたログファイルは、ファイルが圧縮された同じ場所に解凍しないでください。ファイルと同じ場所で解凍すると、ログローテーションスクリプトの妨げになることがあります。

必要に応じて、監査ログのデスティネーションを変更したり、監査情報を外部 syslog サーバに送信したりできます。外部 syslog サーバが設定されても、監査レコードのローカルログは引き続き生成および格納されます。を参照してください "[監査メッセージとログの送信先を設定します](#)"。

### 関連情報

## "ログファイルとシステムデータを収集"

**bycast.log** のメッセージです

のメッセージ `bycast.log` ADE (Asynchronous Distributed Environment) によって記述されます。ADE は、グリッドノードの各サービスで使用されるランタイム環境です。

ADE のメッセージの例：

```
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 のメッセージには次の情報が含まれています。

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 ID	EVHR
UTC システム時間	2019-05-05T27T17 : 10 : 29.784677 (YYYY-MM-DDTHH : MM : SS.ffffffffffff)
重大度レベル	エラー
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失敗しました。理由 : 「TOUT」

**bycast.log** のメッセージの重大度

のメッセージ `bycast.log` 重大度レベルが割り当てられている。

例：

- `*notice *` -- 記録すべき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です。
- `*warning *` — 予期しない状態が発生しました。
- `*error *` — 操作に影響を与える大きなエラーが発生しました。
- `*critical *` — 異常な状態が発生し、通常の動作が停止しました。原因となった状態にすぐに対処する必要

があります。クリティカルなメッセージは Grid Manager にも表示されます。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 \* > \* Events \* を選択します。

のエラーコード bycast.log

のほとんどのエラーメッセージです bycast.log エラーコードを含む。

次の表に、の代表的な非数値コードを示します bycast.log。非数値コードの正確な意味は、レポートされるコンテキストによって異なります。

エラーコード	意味
SUCS	エラーはありません
GERR	不明です
CANC	キャンセルされました
ABRT	中止しました
TOUT	タイムアウト
INVL	無効です
NFND	が見つかりません
vers	バージョン
会議	設定
失敗	失敗しました
ICPL	不完全です
完了しました	完了しました
SUNV	サービスを利用できません

次の表に、の数値エラーコードを示します bycast.log。

エラー番号	エラーコード	意味
001	EPERM	操作は許可されていません

エラー番号	エラーコード	意味
002	ENOENT	指定したファイルまたはディレクトリは存在しません
003	ESRCH	そのようなプロセスはありません
004.00	EINTR	システムコールが中断されました
005	EIO	I/O エラー
6、6	ENXIO	該当するデバイスまたはアドレスはありません
007	E2BIG	引数リストが長すぎます
008	ENOEXEC	EXEC フォーマットエラー
009	EBADF	ファイル番号が正しくありません
010	ECHILD	子プロセスはありません
011	EAGAIN	再試行してください
012	ENOMEM	メモリ不足です
013	EACCES	権限が拒否されました
014	デフォルト	アドレスが無効です
015	ENOTBLK	ブロックデバイスが必要です
016	EBUSY	デバイスまたはリソースがビジー
017	EEXIST	ファイルが存在します
018	EXDEV の場合	クロスデバイスリンク
019	ENODEV	該当するデバイスはありません
020	ENOTDIR	ディレクトリではありません
021	EISDIR	はディレクトリです

エラー番号	エラーコード	意味
022	EINVAL	引数が無効です
023	ENFILE	ファイルテーブルオーバーフローです
024	EMFILE	開いているファイルが多すぎます
025	ENOTTY	タイプライターではありません
026	ETXTBSY	テキストファイルがビジーです
027	EFBIG	ファイルが大きすぎます
028	ENOSPC	デバイスにスペースが残っていません
029	ESPIPE	不正なシークです
030	EROFS	読み取り専用ファイルシステム
031	EMLINK	リンクが多すぎます
032	EPIPE	パイプ破損
033	エドム	関数のドメイン外の数学引数
034	エスランゲ	数学結果は表現できません
035	EDEADLK	リソースのデッドロックが発生する
036	ENAMETOOLONG	ファイル名が長すぎます
037	ENOLCK	使用可能なレコードロックがありません
038	ENOSYS	関数が実装されていません
039	ENOTEMPTY	ディレクトリが空ではありません
040	ELOOP	シンボリックリンクが多すぎます
041		
042	ENOMSG	必要なタイプのメッセージがありません

エラー番号	エラーコード	意味
043	EIDRM	識別子が削除されました
044	ECHRNG	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 が停止しました
047	EL3RST	レベル 3 リセット
048	ELNRNG	リンク番号が範囲外です
049	EUNATCH	プロトコルドライバが接続されていません
050	ENOCSI	CSI 構造がありません
051	EL2HLT	レベル2停止
052	EBADE の実行	無効な交換です
053	EBADR	無効な要求記述子です
054	EXFULL (完全)	Exchange がいっぱいです
055	ENOANO	アノードなし
056	EBADRQC	無効な要求コードです
057	EBADSLT	無効なスロットです
058		
059	EBFONT	フォントファイルの形式が正しくありません
060	ENOSTR	デバイスはストリームではありません
061	ENODATA	使用できるデータがありません
062	イータイム	タイマーが切れました
063	ENOSR	Out of Streams のリソース

エラー番号	エラーコード	意味
064	ENONET	マシンがネットワーク上にありません
065	ENOPKG	パッケージがインストールされていません
066	EREMOTE	オブジェクトがリモートです
067	ENOLINK	リンクが切断されました
068	EADV	アドバタイズエラー
069	ESRMNT	Srmount エラー
070	エコム	送信時の通信エラーです
071	EPROTO	プロトコルエラー
072	EMULTIHOP	マルチホップが試行されました
073	EDOTDOT	RFS 固有のエラー
074	EBADMSG と入力します	データメッセージではありません
075	EOVERFLOW	定義されたデータ型の値が大きすぎます
076	ENOTUNIQ	名前がネットワーク上で一意ではありません
077	EBADFD	ファイル記述子が無効な状態です
078	エルム変更	リモートアドレスが変更されました
079	ELIBACC	必要な共有ライブラリにアクセスできません
080	ELIBBAD 社	破損した共有ライブラリにアクセスしています
081	ELIBSCN	
082	ELIBMAX	リンクしようとしている共有ライブラリが多すぎます
083	ELIBEXEC	共有ライブラリを直接実行することはできません

エラー番号	エラーコード	意味
084	EILSEQ	不正なバイトシーケンスです
085	ERESTART	中断されたシステムコールを再開する必要があります
086	ESTRPIPE	ストリームパイプエラー
087	EUSERS	ユーザが多すぎます
088	ENOTSOCK	ソケット以外でのソケット操作
089	EDESTADDRREQ	送信先アドレスは必須です
090	EMSGSIZE	メッセージが長すぎます
091	EPROTOTYPE	ソケットのプロトコルタイプが正しくありません
092	ENOPROTOOPT	プロトコルを使用できません
093	EPROTONOSUPPORT	サポートされていないプロトコルです
094	ESOCKTNOSUPPORT の略	ソケットタイプはサポートされていません
095	EOPNOZ TSUPP	この処理は転送エンドポイントではサポートされません
096	EPFNOSUPPORT	サポートされていないプロトコルファミリーです
097	EAFNOSUPPORT	アドレスファミリーはプロトコルでサポートされていません
098	EADDRINUSE	アドレスはすで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	ENETDOWN	ネットワークが停止しています
101です	ENETUNREACH	ネットワークに到達できません
一〇二	ENETRESET	リセットのためネットワークが接続を切断しました
103	ECONNABORTED	ソフトウェアが原因で接続が終了しました

エラー番号	エラーコード	意味
104	ECONNRESET	ピアによって接続がリセットされました
105	ENOBUFS	使用可能なバッファスペースがありません
106	EISCONN	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	ENOTCONN	トランスポートエンドポイントが接続されていません
一〇八	ESH ダウンタウン	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	参照が多すぎます：接続できません
110	ETIMEDOUT	接続がタイムアウトしました
———	ECONNREFUSED	接続が拒否されました
112	EHOSTDOWN	ホストが停止しています
113	EHOSTUNREACH	ホストへのルートがありません
114	エアルレーダド	処理をすでに実行中です
115	実行中	処理を実行中です
116		
117	EUCLEAN	構造はクリーニングが必要です
118	ENOTNAM	XENIX という名前のファイルではありません
119 番	ENAVAIL	XENIX セマフォがありません
一二〇	EISNAM	は、名前付きタイプファイルです
一二一	EREMOTEIO	リモート I/O エラーです
122	EDQUOT	クォータを超過しました
一二三	ENOMEDIUM	メディアが見つかりません

エラー番号	エラーコード	意味
124	EMEDIUMTYPE	メディアタイプが正しくありません
一二五	ECANCELED	処理がキャンセルされました
126	ENOKEY	必要なキーがありません
127	エクイメピ RED も含まれています	キーの有効期限が切れました
128	エーケヨヴォエド	キーが取り消されました
129	EKEYREJECTED	キーがサービスによって拒否されました
130	EOWNERDEAD の場合	堅牢な mutex のため：所有者は死んだ
131	ENOTRECOVERABLE	堅牢な mutex の場合：状態は回復できません

## 監査メッセージとログの送信先の設定

### 外部syslogサーバを使用する場合の考慮事項

外部 syslog サーバは、StorageGRID の外部にあるサーバであり、1箇所でシステム監査情報を収集できます。外部のsyslogサーバを使用すると、管理ノードのネットワークトラフィックを軽減し、情報をより効率的に管理できます。StorageGRIDの場合、発信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 サーバに送信できる監査情報のタイプは次のとおりです。

- 通常のシステム運用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、セキュリティ関連のイベント
- アプリケーションログ：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オープンする必要がある場合に要求されることがあります

### 外部syslogサーバを使用する状況

外部のsyslogサーバは、大規模なグリッドを使用する場合、複数のタイプの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役立ちます。外部 syslog サーバに監査情報を送信すると、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。
- 監査情報はさまざまなストレージノードから外部syslogサーバに直接転送されるため、管理ノードのネットワークトラフィックを削減します。管理ノードを経由する必要はありません。



外部syslogサーバにログを送信すると、8、192バイトを超える単一のログがメッセージの最後で切り捨てられ、外部syslogサーバの実装における一般的な制限事項に準拠します。



外部syslogサーバに障害が発生した場合にフルデータリカバリのオプションを最大化するには、最大20 GBの監査レコードのローカルログを使用します。(localaudit.log) は各ノードで維持されます。

#### 外部syslogサーバの設定方法

外部syslogサーバの設定方法については、[を参照してください。](#) **"監査メッセージと外部syslogサーバの設定"**。

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

- サーバ**CA**証明書：PEMエンコードで外部syslogサーバを検証するための1つ以上の信頼されたCA証明書。省略すると、デフォルトの Grid CA 証明書が使用されます。
- クライアント証明書：PEMエンコードによる外部syslogサーバへの認証用のクライアント証明書。
- クライアント秘密鍵：PEMエンコードでのクライアント証明書の秘密鍵。



クライアント証明書を使用する場合は、クライアント秘密鍵も使用する必要があります。暗号化された秘密鍵を指定する場合は、パスフレーズも指定する必要があります。暗号化された秘密鍵を使用した場合、セキュリティ上の大きなメリットはありません。これは、鍵とパスフレーズを格納する必要があるためです。暗号化されていない秘密鍵を使用することを推奨します（使用可能な場合）。

#### 外部 syslog サーバ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 処理数または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するようにサイジングされます。たとえば、1秒あたりの S3 処理数が1、000件、つまり1秒あたり2、000 MB のオブジェクトの取り込みと読み出しをグリッドで処理する必要があるとします。外部 syslog サーバのサイズは、グリッドのデータ要件に応じて決定する必要があります。

このセクションでは、外部 syslog サーバが処理可能であ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 処理数）で見積もるためのヒューリスティック計算式をいくつか示します。

#### 1秒あたりの S3 処理数を推定式で使用します

グリッドをスループット用に1秒あたりのバイト数で表した場合、試算式を使用するには、このサイジングを1秒あたりの S3 処理に変換する必要があります。グリッドのスループットを変換するには、最初に平均オブジェクトサイズを確認する必要があります。これには、既存の監査ログと指標の情報を使用するか（存在する場合）、StorageGRID を使用するアプリケーションに関する知識が必要です。たとえば、グリッドのサイズが2、000 MB/秒で、平均オブジェクトサイズが2MBの場合、1秒あたり1、000 S3 処理可能なサイズ（2、000 MB/秒）になるようにグリッドをサイジングしました。



以降のセクションで説明する外部 syslog サーバのサイジングの計算式は、一般的な推定値（ワーストケースの見積もり値ではありません）を示しています。設定やワークロードによっては、syslog メッセージや syslog データの量が、式で予測される値よりも増減することがあります。式はガイドラインとしてのみ使用することを意図しています。

## 監査ログの推定式

グリッドでサポートされる 1 秒あたりの S3 処理数以外の 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 サーバで処理する必要がある監査ログのボリュームを推定できます。監査レベルをデフォルト値のままにしておくという前提では、次のようになります（[エラー]に設定されている[ストレージ]を除くすべてのカテゴリは[通常]に設定されています）。

```
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 S3 処理の場合、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外部 syslog サーバをサイジングし、1 秒あたり 1.6 MB の割合で監査ログデータを受信（通常は格納）できるようにする必要があります。

ワークロードの詳細がわかっている場合は、より正確な概算が可能です。監査ログの場合、最も重要な追加変数は、PUT される S3 処理の割合（とが表示されます。次の S3 フィールドの平均サイズ（バイト）（このテーブルで使用される 4 文字の省略形は監査ログのフィールド名）も表示されます。

コード	フィールド	説明
SACC	S3 テナントアカウント名（要求の送信者）	要求を送信したユーザのテナントアカウントの名前。匿名の要求の場合は空です。
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。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。
S3BK	S3バケット	S3 バケット名。
S3KY	S3キー	バケット名を除く S3 キーの名前。バケットに対する処理では、このフィールドは指定されません。

P を使用して、PUT の S3 処理の割合を表します。ここでは、 $0 \leq P \leq 1$  である（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  $P = 0$ ）。

ここでは、S3アカウント名、S3バケット、S3キーの合計の平均サイズをKで表します。S3 アカウント名が常に my-s3 アカウント（13 バイト）、バケット名が /my-application/bucket-12345（28 バイト）のような固定長の名前、オブジェクト名が 5733a5d7-f069-41ef-8fbd-132474c69c（36 バイト）のような固定長のキーを持つとします。K の値は 90（13+13+28+36）です。

P と K の値を決定できる場合は、次の式を使用して、外部 syslog サーバで処理する必要がある監査ログのボリュームを見積もることができます。これは、監査レベルをデフォルト（Storage を除くすべてのカテゴリは Normal に設定されたまま）にしておくことを前提としています。エラーに設定されているもの）：

$$\text{Audit Log Rate} = ((2 \times P) + (1 - P)) \times \text{S3 Operations Rate}$$

$$\text{Audit Log Average Size} = (570 + K) \text{ bytes}$$

たとえば、グリッドのサイズが1秒あたり1、000 S3 処理の場合、ワークロードの配置は50%で、S3 アカウント名やバケット名はオブジェクト名の平均値は90バイトで、1秒あたり1、500のsyslogメッセージをサポートするように外部syslogサーバをサイジングし、1秒あたり約1MBの割合で監査ログデータを受信（通常は格納）できるようにする必要があります。

#### デフォルト以外の監査レベルの推定式

監査ログ用に提供される式では、デフォルトの監査レベル設定（「Error」に設定されているストレージを除く、すべてのカテゴリが「Normal」に設定されている）を使用するものとします。デフォルト以外の監査レベル設定に対する監査メッセージの割合と平均サイズを見積もるための詳細な式は使用できません。ただし、次の表を使用して料金を大まかに見積もることができます。監査ログに提供されている平均サイズの式を使用することもできますが、「余分な」監査メッセージの平均サイズはデフォルトの監査メッセージよりも小さくなるため、見積もりが過剰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：すべての監査レベルをデバッグまたは通常に設定します	監査ログ速度 = 8 x S3処理速度
イレイジャーコーディング：すべての監査レベルをデバッグまたは正常に設定	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処理とは関係なく、一般に生成されるログやデータの量はごくわずかです。そのため、計算式は提供されません。

#### アプリケーションログの推定式

グリッドでサポートされる1秒あたりのS3処理数以外の情報がS3ワークロードにない場合は、次の式を使用して、外部syslogサーバで処理する必要があるアプリケーションログのボリュームを推定できます。

$$\text{Application Log Rate} = 3.3 \times \text{S3 Operations Rate}$$

$$\text{Application Log Average Size} = 350 \text{ bytes}$$

たとえば、グリッドの1秒あたりのS3処理数が1、000の場合、1秒あたりのアプリケーションログ数が3、300になるように外部syslogサーバをサイジングし、1秒あたり約1.2MBの割合でアプリケーションログデータを受信（格納）できるようにする必要があります。

ワークロードの詳細がわかっている場合は、より正確な概算が可能です。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イレイジャーコーディング）。PUTのS3処理の割合（対GET/OTHER）と、次のS3フィールドの平均サイズ（バイト）（テーブルで使用される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 (要求の送信者)	要求を送信したユーザのテナントアカウントの名前。匿名の要求の場合は空です。
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。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。
S3BK	S3バケット	S3 バケット名。
S3KY	S3キー	バケット名を除く S3 キーの名前。バケットに対する処理では、このフィールドは指定されません。

#### サイジング試算の例

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を説明します。

- レプリケーション
- イレイジャーコーディング

#### レプリケーションをデータ保護に使用する場合

P は、PUT の S3 処理の割合を表します。ここでは、 $0 \leq P \leq 1$  である (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 S3 アカウント名、S3 バケット、S3 キーの合計の平均サイズとします。S3 アカウント名が常に my-s3 アカウント (13 バイト)、バケット名が /my-application/bucket-12345 (28 バイト) のような固定長の名前、オブジェクト名が 5733a5d7-f069-41ef-8fbd-132474c69c (36 バイト) のような固定長のキーを持つとします。K の値は 90 (13+13+28+36) です。

P と K の値を決定できる場合は、次の式を使用して、外部 syslog サーバで処理可能なアプリケーションログのボリュームを推定できます。

$$\begin{aligned} \text{Application Log Rate} &= ((1.1 \times P) + (2.5 \times (1 - P))) \times \text{S3 Operations Rate} \\ \text{Application Log Average Size} &= (P \times (220 + K)) + ((1 - P) \times (240 + (0.2 \times K))) \text{ Bytes} \end{aligned}$$

たとえば、グリッドのサイズが 1 秒あたり 1、000 S3 処理の場合、ワークロードの配置が 50% で、S3 アカウント名、バケット名、オブジェクト名の平均値が 90 バイトの場合、1 秒あたりのアプリケーションログ数が 1800 になるように外部 syslog サーバをサイジングする必要があります。そして、アプリケーションデータを 0.5 MB/秒のレートで受信 (通常は保存) します。

イレイジャーコーディングをデータ保護に使用する場合

P は、PUT の S3 処理の割合を表します。ここでは、 $0 \leq P \leq 1$  である（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 S3 アカウント名、S3 バケット、S3 キーの合計の平均サイズとします。S3 アカウント名が常に my-s3 アカウント（13 バイト）、バケット名が /my-application/bucket-12345（28 バイト）のような固定長の名前、オブジェクト名が 5733a5d7-f069-41ef-8fbd-132474c69c（36 バイト）のような固定長のキーを持つとします。K の値は 90（13+13+28+36）です。

P と K の値を決定できる場合は、次の式を使用して、外部 syslog サーバで処理可能なアプリケーションログのボリュームを推定できます。

```
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
```

たとえば、グリッドのサイズが1秒あたり1,000 S3処理に対応している場合、ワークロードは50%のPUTになり、S3アカウント名、バケット名、オブジェクト名の平均は90バイトです。外部syslogサーバは、1秒あたり2,250個のアプリケーションログをサポートするようにサイズを設定し、1秒あたり0.6MBの速度でアプリケーションデータを受信（格納）できるようにする必要があります。

#### 監査メッセージと外部syslogサーバの設定

監査メッセージに関連するいくつかの設定を行うことができます。記録する監査メッセージの数の調整、クライアントの読み取り/書き込み監査メッセージに含めるHTTP要求ヘッダーの定義、外部syslogサーバの設定、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の指定を行うことができます。

監査メッセージとログには、システムのアクティビティとセキュリティイベントが記録され、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 ノードで監査メッセージとログが生成され、システムアクティビティとイベントが追跡されます。

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サーバを設定できます。外部サーバを使用すると、監査データの完全性を損なうことなく、監査メッセージロギング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。外部のsyslogサーバは、大規模なグリッドを使用する場合、複数のタイプの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役立ちます。を参照してください ["外部 syslog サーバに関する考慮事項"](#) を参照してください。

作業を開始する前に

- を使用して Grid Manager にサインインします ["サポートされている Web ブラウザ"](#)。
- を使用することができます ["Maintenance権限またはRoot Access権限"](#)。
- 外部syslogサーバを設定する場合は、["外部syslogサーバを使用する場合の考慮事項"](#) また、ログファイルを受信して保存するのに十分な容量がサーバにあることを確認します。
- TLSまたはRELP/TLSプロトコルを使用して外部syslogサーバを設定する場合は、必要なサーバCAとクライアント証明書、およびクライアント秘密鍵が必要です。

監査ログでは、次のカテゴリのメッセージごとに異なる監査レベルを設定できます。

監査カテゴリ	デフォルト設定です	詳細情報
システム	正常	"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	正常	"管理監査メッセージ"
クライアント読み取り	正常	"クライアント読み取り監査メッセージ"
クライアントからの書き込み	正常	"クライアント書き込み監査メッセージ"
ILM	正常	"ILM監査メッセージ"
グリッド間レプリケーション	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値は、StorageGRID 10.3 以降を最初にインストールした場合に適用されます。以前のバージョンのStorageGRIDを最初に使用した場合、すべてのカテゴリのデフォルトは[標準]に設定されます。



アップグレード中は、監査レベルの設定はすぐには有効になりません。

#### 手順

1. \* configuration \* > \* Monitoring \* > \* Audit and syslog server \* 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	このカテゴリの監査メッセージはログに記録されません。
エラー	エラーメッセージのみがログに記録されます — 結果コードが「成功」（SUCS）以外の監査メッセージ。
正常	標準のトランザクション・メッセージはログに記録されますこのメッセージは ' カテゴリに関する次の手順に記載されています
デバッグ	非推奨。このレベルの動作は Normal 監査レベルと同じです。

特定のレベルに含まれるメッセージには、上位レベルでロギングされるメッセージも含まれます。たとえば、Normal レベルには Error レベルのメッセージがすべて含まれます。



S3アプリケーションに対するクライアント読み取り処理の詳細なレコードを確認する必要がない場合は、必要に応じて\* Client Reads 設定を Error \*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 ( Save ) ] 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要求ヘッダーの定義

必要に応じて、クライアントの読み取り/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要求とSwift要求にのみ適用されます。

#### 手順

1. [Audit protocol headers]セクションで、クライアントの読み取り/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 個以上の文字に一致させるには、ワイルドカードとしてアスタリスク ( \\* ) を使用します。リテラルアスタリスクに一致させるには、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。

要求に HTTP ヘッダーが含まれている場合、HTTP ヘッダーは HTRH フィールドの下の監査メッセージに含まれます。



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 \* でない場合にのみ記録されます。

3. [保存 ( Save ) ] 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。

#### [use-external-syslog-server]外部syslogサーバを使用する

必要に応じて、監査ログ、アプリケーションログ、およびセキュリティイベントログをグリッドの外部の場所に保存するように外部のsyslogサーバを設定できます。



外部syslogサーバを使用しない場合は、この手順を省略してに進みます [監査情報の送信先を選択します](#)。



この手順で使用可能な構成オプションが要件を満たすのに十分な柔軟性を備えていない場合は、audit-destinations エンドポイント (のプライベートAPIセクションにあります) ["Grid 管理 API"](#)。たとえば、ノードのグループごとに異なるsyslogサーバを使用する場合は、APIを使用できます。

## syslog情報の入力

外部syslogサーバの設定ウィザードにアクセスし、StorageGRIDが外部syslogサーバにアクセスするために必要な情報を入力します。

### 手順

1. 監査および syslog サーバページで、\* 外部 syslog サーバの設定 \* を選択します。または、以前に外部syslogサーバを設定した場合は、\*[外部syslogサーバの編集]\*を選択します。

Configure external syslog server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、\* Host \*フィールドに外部syslogサーバ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 サーバのデスティネーションポートを入力します（1~65535の整数で指定する必要があります）。デフォルトのポートは514です。
4. 外部 syslog サーバへの監査情報の送信に使用するプロトコルを選択します。

TLS または RELP/TLS \*を使用することを推奨します。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。証明書を使用して、グリッドと外部 syslog サーバの間の接続を保護できます。詳細については、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で、外部 syslog サーバによるサポートおよび設定が必要です。外部 syslog サーバと互換性のあるオプションを選択する必要があります。



Reliable Event Logging Protocol (RELP) は、syslog プロトコルの機能を拡張し、信頼性の高いイベントメッセージ配信を実現します。RELP を使用すると、外部 syslog サーバを再起動する必要がある場合に監査情報が失われないようにすることができます。

5. 「\* Continue \*」を選択します。
6. [\[\[attach-certificate\]](#)\* TLS または RELP/TLS \*を選択した場合は、サーバCA証明書、クライアント証明書、およびクライアント秘密鍵をアップロードします。
  - a. 使用する証明書またはキーの [[\\* 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のチェックマークが表示され、正常にアップロードされたことを通知します。

7. 「\* Continue \*」を選択します。

## syslog の内容を管理します

外部syslogサーバ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サーバに送信する監査情報の種類をそれぞれ選択します。

- 監査ログの送信：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の送信:許可されてい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rootとしてサインインしようとしたときなど、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：次のようなトラブルシューティングに役立つログファイルを送信します。
  - bycast-err.log
  - bycast.log
  - jaeger.log
  - nms.log (管理ノードのみ)
  - prometheus.log
  - raft.log
  - hagrroups.log

StorageGRIDソフトウェアログの詳細については、[を参照してください。](#) **"StorageGRID ソフトウェアのログ"**。

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カテゴリごとに重大度とファシリティ（メッセージのタイプ）を選択します。

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

- a. では、[Passthrough]\*を選択するか、重大度値を0~7で選択します。

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。固定値で重大度を上書きすると、異なる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	<p>外部syslogに送信される各メッセージの重大度は、ノードにローカルにログインしたときと同じになります。</p> <ul style="list-style-type: none"> <li>• 監査ログの場合、重大度は「info」です。</li> <li>• 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。</li> <li>• アプリケーションログの重大度は、問題の内容に応じて「info」と「notice」の間で異なります。たとえば、NTPサーバを追加してHAグループを設定すると値が「info」になり、SSMサービスまたはRSMサービスを意図的に停止すると値が「notice」になります。</li> </ul>
0	EMERGENCY：システムが使用できない
1.	ALERT：早急に対処が必要です
2.	Critical：クリティカルな状態です

重大度	説明
3.	Error : エラー状態
4.	Warning : 警告状態です
5.	通知 : 通常の状態だが重要な状態
6.	INFORMATIONAL : 情報メッセージです
7.	DEBUG : デバッグレベルのメッセージ

b. \*Facilty\*では、\*Passthrough\*を選択するか、0~23のファシリティ値を選択します。

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。固定値でファシリティを上書きすると、さまざまなファシリティ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	<p>外部syslogに送信される各メッセージのファシリティ値は、ノードにローカルにログインしたときと同じです。</p> <ul style="list-style-type: none"> <li>• 監査ログの場合、外部syslogサーバに送信されるファシリティは「local7」です。</li> <li>• 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。</li> <li>• アプリケーションログの場合、外部syslogサーバに送信されるアプリケーションログのファシリティ値は次のとおりです。 <ul style="list-style-type: none"> <li>◦ bycast.log: ユーザーまたはデーモン</li> <li>◦ bycast-err.log : user、daemon、local3、またはlocal4</li> <li>◦ jaeger.log : local2</li> <li>◦ nms.log: local3</li> <li>◦ prometheus.log : local4</li> <li>◦ raft.log: local5</li> <li>◦ hagroups.log : local6</li> </ul> </li> </ul>
0	kern (カーネルメッセージ)
1.	ユーザ (ユーザレベルのメッセージ)
2.	メール

ファシリティ	説明
3.	デーモン (システムデーモン)
4.	AUTH (セキュリティ / 認証メッセージ)
5.	syslog ( syslogd で内部的に生成されるメッセージ)
6.	LPR (ラインプリンタサブシステム)
7.	News (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
10	セキュリティ (セキュリティ / 認可メッセージ)
11	FTP
12	NTP
13	logaudit (ログ監査)
14	logalert (ログアラート)
15	clock ( clock 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	「 LOCAL4 」
21.	ローカル5
22	ローカル6
23	ローカル7

3. 「\* Continue \*」を選択します。

テストメッセージを送信します

外部 syslog サーバ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 サーバへのデータ送信にコミットする前に、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全体を検証する必要があります。



外部syslogサーバ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、メッセージが想定どおりに処理されたことを確認するまでは、外部syslogサーバの設定を使用しないでください。

手順

1. 外部syslogサーバが適切に設定され、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にあるためにテストメッセージを送信しない場合は、\*[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（推奨）を選択します。

テスト結果は、テストを停止するまでページに継続的に表示されます。テストの実行中も、以前に設定した送信先に監査メッセージが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。

を参照してください ["外部 syslog サーバのトラブルシューティングを行います"](#) エラーの解決に役立ちます。

4. すべてのノードがテストに合格したことを示す緑のバナーが表示されるまで待ちます。
5. syslog サーバを調べて、テストメッセージが正常に受信および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ます。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許可されていません。プロトコル。

6. 「\* ストップ & フィニッシュ \*」を選択します。

監査および syslog サーバ \* ページに戻ります。緑色のバナーは、syslogサーバの設定が保存されたことを示します。



外部syslogサーバを含むデスティネーションを選択するまで、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します

監査ログ、セキュリティイベントログ、["StorageGRID ソフトウェアのログ"](#) が送信されます。

StorageGRIDはデフォルトでローカルノードの監査先に設定され、監査情報をに格納します  
/var/local/log/localaudit.log。



を使用する`/var/local/log/localaudit.log`と、Grid Managerと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ことがあります。最新のエントリがあるノードを確認するには、コマンドを使用し`run-each-node --parallel "zgrep MGAU /var/local/log/localaudit.log | tail"`ます。

一部の送信先は、外部syslogサーバを設定した場合にのみ使用できます。

## 手順

1. [Audit and syslog server]ページで、監査情報の保存先を選択します。



\*ローカルノードのみ\*および\*外部syslogサーバ\*の方が一般的に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）	<p>監査メッセージ、セキュリティイベントログ、および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、それらはそれらを生じたノード（「ローカルノード」）にのみ保存されます。すべてのローカルノードで生成された監査情報はに格納されます /var/local/log/localaudit.log。</p> <p>注：StorageGRIDは定期的にローカルログをローテーションで削除し、スペースを解放します。ノードのログファイルが1GB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の上限は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。各ノードには平均約20GBのログデータが格納されます。</p>
管理ノード/ローカルノード	<p>監査メッセージは管理ノード上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じたノードに格納されます。監査情報は次のファイルに格納されます。</p> <ul style="list-style-type: none"><li>• 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</li><li>• All nodes（すべてのノード）：`/var/local/log/localaudit.log`通常、ファイルが空であるか欠落しています。一部のメッセージの追加コピーなど、セカンダリ情報が含まれている場合があります。</li></ul>
外部 syslog サーバ	<p>監査情報は外部syslogサーバに送信され、ローカルノードに保存され（`/var/local/log/localaudit.log`ます）。送信される情報の種類は、外部 syslog サーバ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 サーバを設定した場合にのみ有効になります。</p>

オプション	説明
管理ノードと外部 syslog サーバ	監査メッセージは(/var/local/audit/export/audit.log`管理ノード上の監査ログに送信され、監査情報は外部syslogサーバに送信されてローカルノードに保存され (/var/local/log/localaudit.log`ます)。送信される情報の種類は、外部 syslog サーバ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 サーバを設定した場合にのみ有効になります。

2. [保存 ( Save ) ] を選択します。

警告メッセージが表示されます。

3. [OK]\*を選択して、監査情報の保存先を変更することを確認します。

緑色のバナーは、監査設定が保存されたことを示します。

選択した送信先に新しいログが送信されます。既存のログは現在の場所に残ります。

## SNMP による監視を使用する

### SNMP監視の使用：概要

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 に含まれる SNMP エージェントを設定する必要があります。

- ["SNMP エージェントを設定します"](#)
- ["SNMP エージェントを更新します"](#)

### 機能

各StorageGRID ノードは、MIBを提供するSNMPエージェント ( デーモン ) を実行します。StorageGRID の MIB には、アラートおよびアラームのテーブルおよび通知定義が含まれています。この MIB には、各ノードのプラットフォームやモデル番号など、システムの概要 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ています。



を参照してください ["MIBファイルにアクセスします"](#) 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 エージェントを設定すると、すべての StorageGRID ノードに同じ設定が適用されます。

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

### トラップ

トラップはSNMPエージェントによって送信される通知で、管理システムによる確認応答は必要ありません。トラップは、アラートがトリガーされているなど、StorageGRID 内で何らかの問題が発生したことを

管理システムに通知するために使用されます。

トラップは、SNMP の 3 つのバージョンすべてでサポートされています。

## 情報

通知はトラップと似ていますが、管理システムによる確認応答が必要です。SNMPエージェントは、一定の時間内に確認応答を受信しなかった場合、確認応答を受信するか、最大再試行値に達するまで、インフォームを再送信します。

インフォームは SNMPv2c および SNMPv3 でサポートされます。

トラップ通知およびインフォーム通知は、次の場合に送信されます。

- デフォルトまたはカスタムのアラートはいずれかの重大度レベルでトリガーされます。アラートのSNMP通知を停止するには、次の手順を実行する必要があります。"[サイレンスの設定](#)" をクリックします。アラート通知はから送信されます "[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、および 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トリガーできるアラートのリストについては、[を参照してください](#) "[アラート一覧](#)"。

- 特定 "[アラーム \(従来のシステム\)](#)" 指定された重大度レベル以上でトリガーされます。



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

## SNMP バージョンサポート

次の表に、各 SNMP バージョンでサポートされる内容の概要を示します。

	SNMPv1	SNMPv2c	SNMPv3
クエリ (GETおよび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	コミュニティストリング	コミュニティストリング	ユーザベースのセキュリティモデル (USM) ユーザ
通知 (トラップと通知)	トラップのみ	トラップおよびインフォーム	トラップおよびインフォーム

	SNMPv1	SNMPv2c	SNMPv3
通知認証	トラップの送信先ごとに、デフォルトのトラップコミュニティまたはカスタムのコミュニティストリングを指定します	トラップの送信先ごとに、デフォルトのトラップコミュニティまたはカスタムのコミュニティストリングを指定します	トラップの送信先ごとのUSM ユーザ

#### 制限

- StorageGRID は、読み取り専用 MIB アクセスをサポートしています。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が同じ設定を受信します。
- SNMPv3 : StorageGRID は TSM ( Transport Support Mode ) をサポートしていません。
- SNMPv3 : SHA ( HMAC-SHA-96 ) だけがサポートされています。
- SNMPv3 : AES のみがサポートされています。

#### SNMP エージェントを設定します

読み取り専用のMIBアクセスと通知にサードパーティ製の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。

#### 作業を開始する前に

- を使用して Grid Manager にサインインします "[サポートされている Web ブラウザ](#)"。
- を使用することができます "[rootアクセス権限](#)"。

#### このタスクについて

StorageGRIDのSNMPエージェントは、SNMPv1、SNMPv2c、およびSNMPv3をサポートしています。エージェントは1つ以上のバージョンに設定できます。

SNMPv3では、ユーザ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が同じSNMP設定を使用します。

#### 基本設定の指定

最初の手順として、StorageGRID SNMPエージェントを有効にし、基本情報を提供します。

#### 手順

1. \* configuration \* > \* Monitoring \* > \* SNMP agent \* を選択します。

[SNMP agent]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選択します。
3. [Basic configuration]セクションに次の情報を入力します。

フィールド	説明
システムの連絡先	任意。StorageGRIDシステムのプライマリ連絡先。SNMPメッセージでsysContactとして返されます。  システムの連絡先は通常、E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を環境に設定します。*システム連絡先*は最大255文字です。
システムの場所	任意。StorageGRIDシステムの場所。SNMPメッセージでsysLocationとして返されます。  システムの場所には、StorageGRIDシステムの場所を特定するのに役立つ任意の情報を指定できます。たとえば、施設の住所を使用できます。この値は、StorageGRIDシステム内のすべてのノードを環境に設定します。*システムの場所*の最大文字数は255文字です。
SNMPエージェント通知の有効化	<ul style="list-style-type: none"> <li>• 選択すると、StorageGRID SNMPエージェントはトラップおよびインフォーム通知を送信します。</li> <li>• 選択しない場合、SNMPエージェントは読み取り専用MIBアクセスをサポートしますが、SNMP通知は送信しません。</li> </ul>
認証トラップを有効にする	このオプションを選択すると、不適切に認証されたプロトコルメッセージを受信すると、StorageGRID SNMPエージェントは認証トラップを送信します。

#### コミュニティストリングの入力

SNMPv1またはSNMPv2cを使用する場合は、[Community Strings]セクションに情報を入力します。

管理システムが StorageGRID MIB を照会すると、コミュニティストリングが送信されます。コミュニティストリングがここで指定した値のいずれかと一致すると、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\*には、必要に応じてコミュニティストリングを入力し、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ために、コミュニティストリングとして「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、StorageGRIDシステムのグリッドIDがコミュニティストリングとして使用されます。

各コミュニティストリングの最大文字数は32文字で、空白文字は使用できません。

2. [別のコミュニティ文字列を追加する]\*を選択して、文字列を追加します。

最大 5 つの文字列を指定できます。

## トラップ送信先の作成

[Other configurations]セクションの[Trap destinations]タブを使用して、StorageGRIDトラップまたはインフォーム通知の送信先を1つ以上定義します。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から定義された各送信先に通知が送信されます。標準通知は、サポートされている MIB-II エンティティ（ifdown や coldStart など）についても送信されます。

### 手順

1. [Default trap community]フィールドに、SNMPv1またはSNMPv2トラップの送信先に使用するデフォルトのコミュニティストリングをオプションで入力します。

特定のトラップ送信先を定義するときは、必要に応じて別の（「カスタム」）コミュニティストリングを指定できます。

\*デフォルトのトラップコミュニティ\*は最大32文字で、空白文字は使用できません。

2. トラップ送信先を追加するには、\*[作成]\*を選択します。
3. このトラップ送信先に使用するSNMPのバージョンを選択します。
4. [トラップ送信先の作成]フォームに、選択したバージョンの情報を入力します。

## 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値を入力します。

フィールド	説明
を入力します	SNMPv1の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IPv4またはIPv6アドレス、また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。
コミュニティストリング	デフォルトのトラップコミュニティ (指定されている場合) を使用するか、このトラップ送信先のカスタムコミュニティストリングを入力します。  カスタムコミュニティストリングの最大文字数は32文字で、空白は使用できません。

## 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値を入力します。

フィールド	説明
を入力します	送信先をトラップまたはインフォームのどちらに使用するか。
ホスト	トラップを受信するIPv4、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。
コミュニティストリング	デフォルトのトラップコミュニティ (指定されている場合) を使用するか、このトラップ送信先のカスタムコミュニティストリングを入力します。  カスタムコミュニティストリングの最大文字数は32文字で、空白は使用できません。

## 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値を入力します。

フィールド	説明
を入力します	送信先をトラップまたはインフォームのどちらに使用するか。
ホスト	トラップを受信するIPv4、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かぎり、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かぎり、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	認証に使用するUSMユーザ。 <ul style="list-style-type: none"><li>• [*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 ユーザだけが表示されます。</li><li>• *INFORM を選択した場合は、権限のあるエンジン ID を持つ USM ユーザのみが表示されます。</li><li>• ユーザが表示されない場合：<ol style="list-style-type: none"><li>i. トラップ送信先を作成して保存します。</li><li>ii. に進みます <a href="#">USMユーザの作成</a> ユーザを作成します。</li><li>iii. [トラップ送信先]タブに戻り、テーブルから保存先を選択して*[編集]*を選択します。</li><li>iv. ユーザを選択します。</li></ol></li></ul>

5. 「\* Create \*」を選択します。

トラップの送信先が作成され、テーブルに追加されます。

#### エージェントアドレスの作成

必要に応じて、[その他の設定]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。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 ネットワークのUDPポート161です。

#### 手順

1. 「\* Create \*」を選択します。
2. 次の情報を入力します。

フィールド	説明
インターネットプロトコル	このアドレスでIPv4とIPv6のどちらを使用するか。  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とTCPのどちらを使用するか。  デフォルトでは、SNMPはUDPを使用します。
StorageGRIDネットワーク	エージェントがリスンするStorageGRIDネットワーク。  <ul style="list-style-type: none"> <li>グリッドネットワーク、管理ネットワーク、クライアントネットワーク：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スンします。</li> <li>Grid ネットワーク</li> <li>管理ネットワーク</li> <li>クライアントネットワーク</li> </ul> <p>注：セキュア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トラフィックもセキュアではないことに注意してください。</p>
ポート	必要に応じて、SNMPエージェントがリ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は任意に入力できます。  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のエージェントアドレスポートを自動的に開きます。これらのポートへのアクセスが外部ファイアウォールで許可されていることを確認してください。

### 3. 「\* Create \*」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ユーザの作成

SNMPv3を使用している場合は、[Other configurations]セクションの[USM Users]タブを使用して、MIBの照会やトラップとインフォームの受信を許可するUSMユーザを定義します。



SNMPv3\_inform\_destinationsには、エンジンIDを持つユーザが必要です。SNMPv3\_trap\_destinationには、エンジンIDを持つユーザを指定できません。

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

手順

1. 「\* Create \*」を選択します。
2. 次の情報を入力します。

フィールド	説明
ユーザ名	このUSMユーザの一意の名前。  ユーザ名の最大文字数は32文字で、空白文字は使用できません。ユーザの作成後にユーザ名を変更することはできません。
読み取り専用MIBアクセス	選択した場合、このユーザにはMIBへの読み取り専用アクセス権が必要です。
信頼できるエンジンID	このユーザをインフォーム送信先で使用する場合は、このユーザの信頼できるエンジンID。  10～64の16進数（5～32バイト）をスペースなしで入力します。この値は、インフォームのトラップ送信先で選択されるUSMユーザに必要です。トラップのトラップ送信先で選択されるUSMユーザにはこの値を指定できません。  注：*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。これは、読み取り専用MIBアクセスを持つUSMユーザにはエンジンIDを設定できないためです。
セキュリティレベル	USMユーザのセキュリティレベル：  <ul style="list-style-type: none"> <li>• * authPriv *：認証とプライバシー（暗号化）と通信します。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。</li> <li>• * authNoPriv *：このユーザは認証と通信し、プライバシーはありません（暗号化なし）。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。</li> </ul>
認証プロトコル	常に、サポートされている唯一のプロトコル（HMAC-SHA-96）であるSHAに設定します。
パスワード	このユーザが認証に使用するパスワード。
プライバシープロトコル	<ul style="list-style-type: none"> <li>• * authPriv *を選択し、常にAES（サポートされている唯一のプライバシープロトコル）に設定されている場合にのみ表示されます。</li> </ul>
パスワード	「* authPriv *」を選択した場合にのみ表示されます。このユーザがプライバシーのために使用するパスワード。

3. 「\* Create \*」を選択します。

USM ユーザが作成され、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 エージェント設定がアクティブになります。

## SNMP エージェントを更新します

SNMP通知を無効にしたり、コミュニティストリングを更新したり、エージェントアドレス、USMユーザ、トラップ送信先を追加または削除したりできます。

作業を開始する前に

- を使用して Grid Manager にサインインします "[サポートされている Web ブラウザ](#)".
- を使用することができます "[rootアクセス権限](#)".

このタスクについて

を参照してください "[SNMP エージェントを設定します](#)" を参照してください。各タブで行った変更をコミットするには、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. \* configuration \* > \* Monitoring \* > \* SNMP agent \* を選択します。

[SNMP agent]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、**[Enable SNMP]**\*チェックボックスをオフにし、[Save]\*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設定がすべて保持されます。

3. 必要に応じて、[Basic configuration]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および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. 必要に応じて、\*[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、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StorageGRID SNMPエージェントが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[コミュニティストリング]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. トラップ送信先を更新するには、[Other configurations]セクションの[Trap destinations]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から定義され

た各送信先に通知が送信されます。標準通知は、サポートされている MIB-II エンティティ（ifdown や coldStart など）についても送信されます。

入力内容の詳細については、を参照してください。"[トラップ送信先の作成](#)"。

- 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、既存のトラップ送信先でカスタムのコミュニティストリングが使用されていることを最初に確認する必要があります。

- トラップ送信先を追加するには、\*[作成]\*を選択します。
- トラップ送信先を編集するには、ラジオボタンを選択し、\*[編集]\*を選択します。
- トラップ送信先を削除するには、ラジオボタンを選択して\*[削除]\*を選択します。
- 変更をコミットするには、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、[その他の設定]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つまたは複数の「リスニングアドレス」を指定します。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、を参照してください。"[エージェントアドレスの作成](#)"。

- 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。
- 変更をコミットするには、ページの下部にある\*[保存]\*を選択します。

7. USMユーザを更新するには、[Other configurations]セクションで[USM Users]タブを選択します。

このタブを使用して、MIBの照会またはトラップおよびインフォームの受信を許可されているUSMユーザを定義します。

入力内容の詳細については、を参照してください。"[USMユーザの作成](#)"。

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

既存のUSMユーザのユーザ名は変更できません。ユーザ名を変更する必要がある場合は、ユーザを削除して新しいユーザ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、そのユーザーが宛先に対して現在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 エージェント設定を保存したときに検証エラーが発生します。

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



削除したユーザがトラップ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 エージェント設定を保存したときに検証エラーが発生します。

◦ 変更をコミットするには、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します

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の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、グリッドの監視に役立ちます。

を参照してください ["SNMP による監視を使用する"](#) SNMPおよびMIBファイルの詳細については、を参照してください。

### MIBファイルにアクセスします

MIBファイルにアクセスする手順は、次のとおりです。

#### 手順

1. \* configuration \* > \* Monitoring \* > \* SNMP agent \* を選択します。
2. [SNMP agent]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インターフェイスを使用するアプライアンスのオブジェクトと通知を定義します。



また、任意のStorageGRIDノードの次の場所にある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、次の手順を実行します。

a. StorageGRID MIBのルート 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)

a. ツリー全体のStorageGRID OIDをgrepで指定します (paste ラインを結合するには :

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



。snmptranslate コマンドには、MIBの探索に役立つ多くのオプションがあります。このコマンドは、任意のStorageGRID ノードで使用できます。

## 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
iso.org.dod.internet (英語) [+] 民間企業[+] ネットアップstoragegrid		NetApp StorageGRIDエンティティ用の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
activeAlertCount	1.3.6.1.4.1.[+] 789.28669.1.3	activeAlertTable内のアクティブなアラートの数。
activeAlertTableの略	1.3.6.1.4.1.[+] 789.28669.1.4	StorageGRID のアクティブなアラートのテーブル。
activeAlertId	1.3.6.1.4.1.[+] 789.28669.1.4.1.1	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。
activeAlertNameの略	1.3.6.1.4.1.[+] 789.28669.1.4.1.2	アラートの名前。
activeAlertInstanceの略	1.3.6.1.4.1.[+] 789.28669.1.4.1.3	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）。
activeAlertSeverityの略	1.3.6.1.4.1.[+] 789.28669.1.4.1.4	アラートの重大度。
activeAlertStartTimeの略	1.3.6.1.4.1.[+] 789.28669.1.4.1.5	アラートがトリガーされた日時。

## 通知タイプ (トラップ)

すべての通知には、変数バインドとして次の変数が含まれます。

- activeAlertId
- activeAlertNameの略
- activeAlertInstanceの略

- activeAlertSeverityの略
- activeAlertStartTimeの略

通知のタイプ	オブジェクトID (OID)	説明
activeMinorAlertの略	1.3.6.1.4.1.[+] 789.28669.0.6	重大度がMinorのアラート
activeMajorAlertの略	1.3.6.1.4.1.[+] 789.28669.0.7	Major重大度のアラート
activeCriticalAlertの略	1.3.6.1.4.1.[+] 789.28669.0.8	重大度がCriticalのアラート

## 追加の **StorageGRID** データを収集します

チャートとグラフを使用します

グラフやレポートを使用して、StorageGRID システムの状態を監視し、問題のトラブルシューティングを行うことができます。

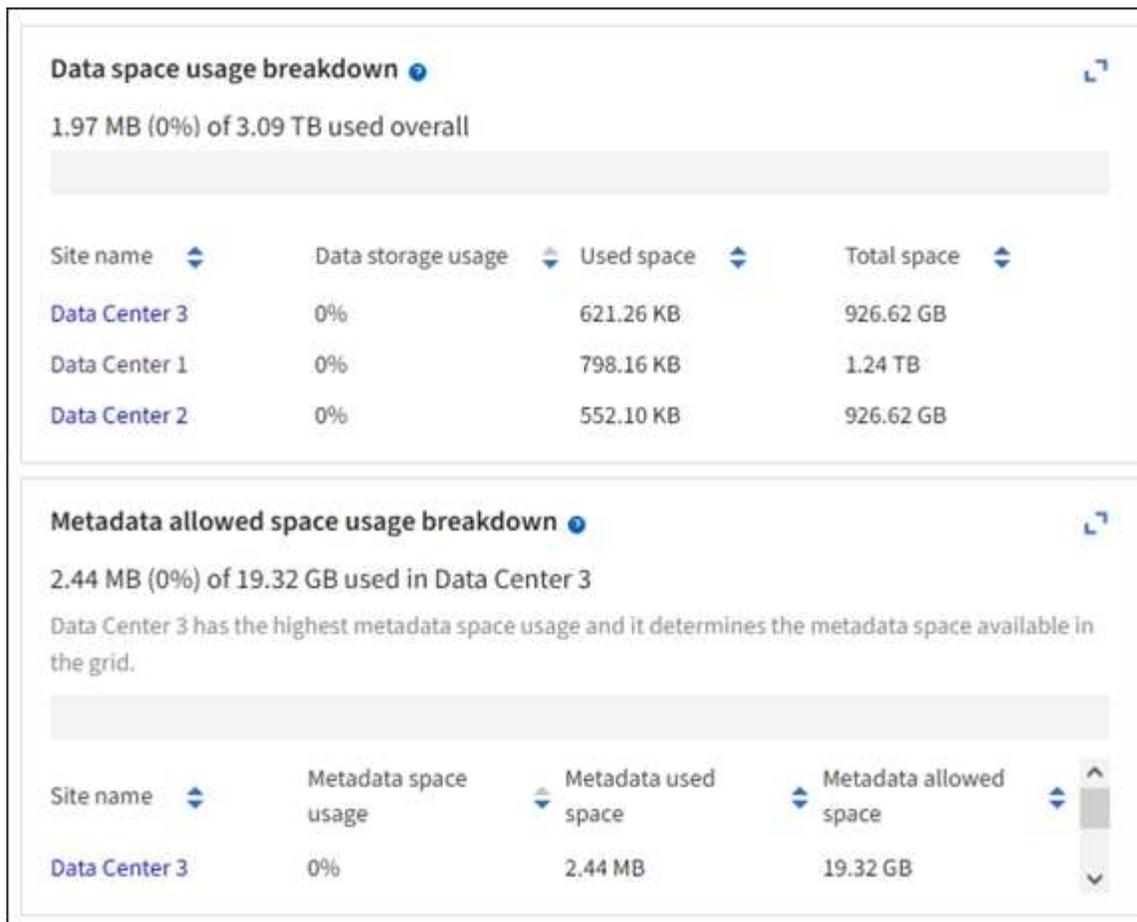


Grid Managerはリリースごとに更新され、このページのスクリーンショットの例とは異なる場合があります。

### グラフのタイプ

グラフには、特定の StorageGRID 指標や属性の値がまとめて表示されます。

Grid Manager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表示されます。



Tenant Managerダッシュボードの[Storage usage]パネルには、次の情報が表示されます。

- テナントの最大バケット（S3）またはコンテナ（Swift）のリスト
- 最大のバケットまたはコンテナの相対サイズを表す棒グラフ
- 使用済みスペースの合計。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

# Dashboard

**16** Buckets  
View buckets

**2** Platform services endpoints  
View endpoints

**0** Groups  
View groups

**1** User  
View users

## Storage usage [?](#)

6.5 TB of 7.2 TB used

0.7 TB (10.1%) remaining



Bucket name	Space used	Number of objects
Bucket-15	969.2 GB	913,425
Bucket-04	937.2 GB	576,806
Bucket-13	815.2 GB	957,389
Bucket-06	812.5 GB	193,843
Bucket-10	473.9 GB	583,245
Bucket-03	403.2 GB	981,226
Bucket-07	362.5 GB	420,726
Bucket-05	294.4 GB	785,190
8 other buckets	1.4 TB	3,007,036

## Total objects

8,418,886  
objects

## Tenant details [?](#)

Name: Tenant02  
ID: 3341 1240 0546 8283 2208  
 Platform services enabled  
 Can use own identity source  
 S3 Select enabled

また、StorageGRID の指標や属性の変化を示すグラフは、Nodes ページと \* support \* > \* Tools \* > \* Grid Topology \* ページからも見ることができます。

グラフには次の 4 種類があります。

- \* Grafana チャート \* : ノードページで表示される、Grafana チャートは、時間の経過に伴う Prometheus 指標の値のプロットに使用されます。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に使用する Grafana チャートが含まれています。

# DC1-S2 (Storage Node)

Overview

Hardware

Network

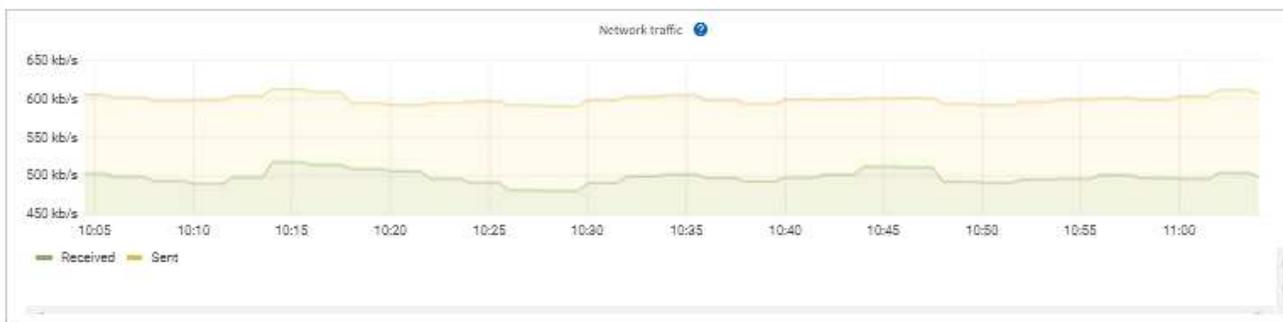
Storage

Objects

ILM

Tasks

1 hour 1 day 1 week 1 month Custom



## Network interfaces

Name	Hardware address	Speed	Duplex	Auto-negotiation	Link status
eth0	00:50:56:A7:E8:1D	10 Gigabit	Full	Off	Up

## Network communication

### Receive

Interface	Data	Packets	Errors	Dropped	Frame overruns	Frames
eth0	3.04 GB	20,403,428	0	24,899	0	0

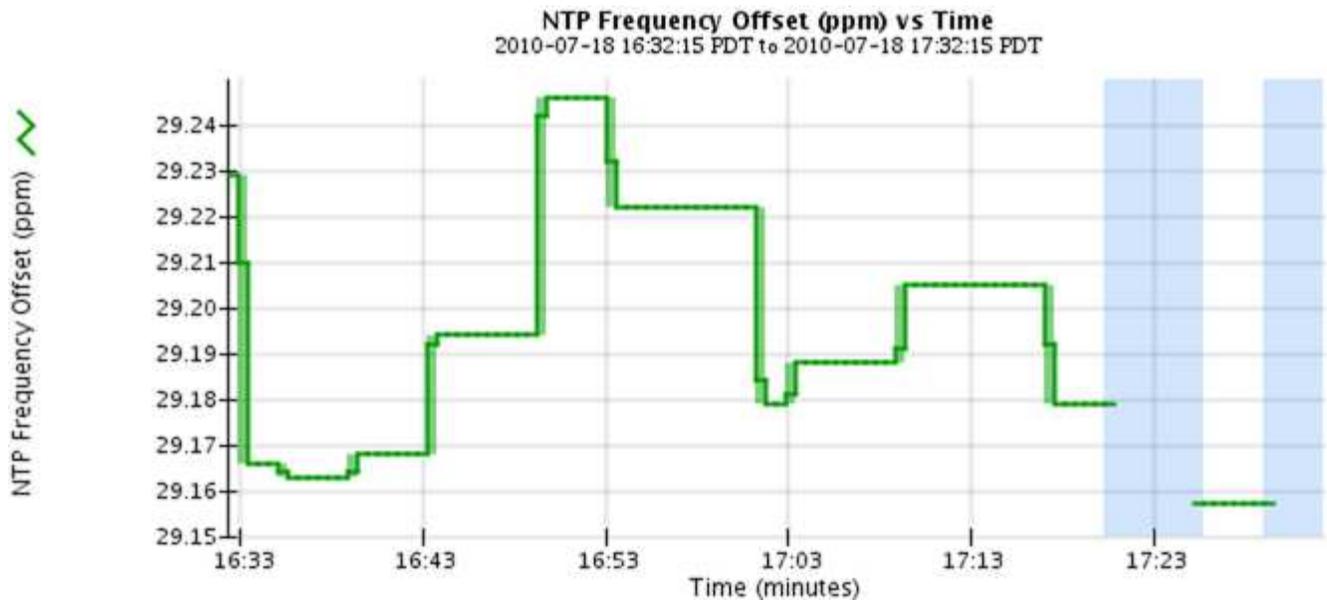
### Transmit

Interface	Data	Packets	Errors	Dropped	Collisions	Carrier
eth0	3.65 GB	19,061,947	0	0	0	0

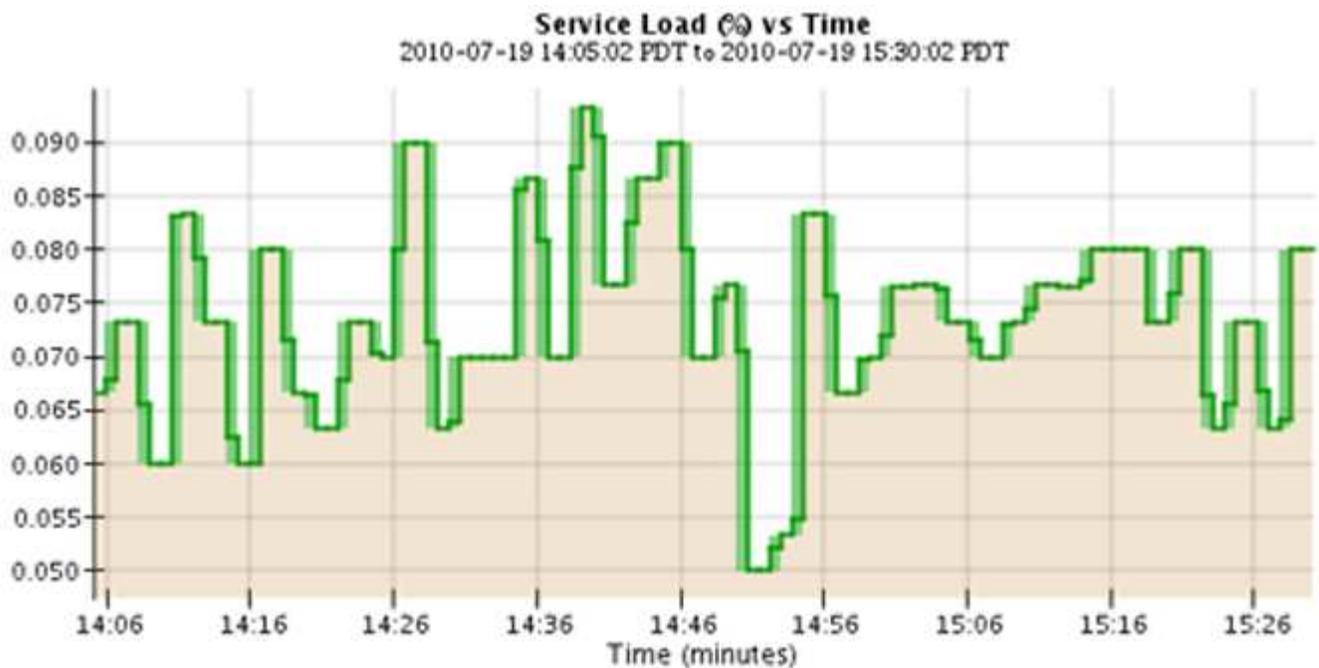


Grafana チャートは、\* support \* > \* Tools \* > \* Metrics \* ページで使用できる事前構築済みのダッシュボードにも含まれています。

- \* 折れ線グラフ \* : ノードページおよび \* support \* > \* Tools \* > \* Grid topology \* ページ (グラフアイコンを選択) から選択できます。  データ値のあとに線グラフを使用して、単位値 (NTP 周波数オフセットの ppm など) を含む StorageGRID 属性の値がプロットされます。値の変化が時間の経過に合わせて一定の間隔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 (グラフアイコンを選択) から使用できます  データ値のあとに) オブジェクト数やサービスの負荷の値など、容量の属性値のプロットには面グラフが使用されます。面グラフは折れ線グラフに似ていますが、線の下部分の背景が薄い茶色になります。値の変化が時間の経過に合わせて一定の間隔でプロットされます。



- グラフの中には、別の種類のグラフアイコンで示されるものもあります  また、形式が異なります。

1 hour    1 day    1 week    1 month    Custom

From: 2020-10-01 12 : 45 PM PDT

To: 2020-10-01 01 : 10 PM PDT Apply

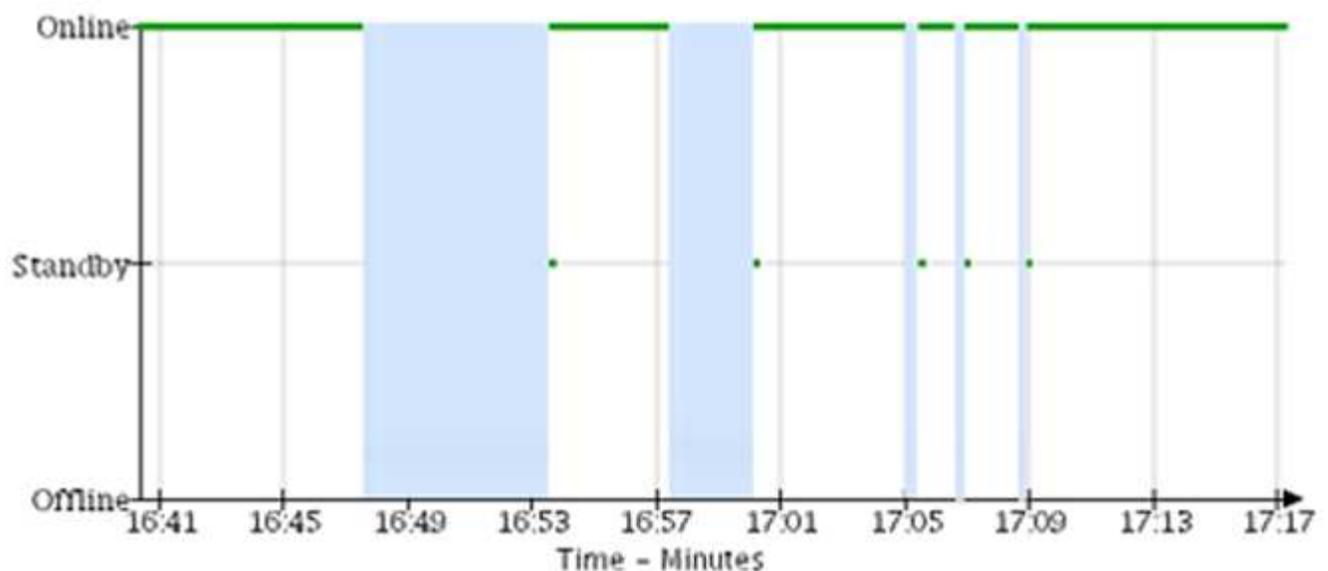


Close

- \* 状態グラフ \* : サポート \* > \* ツール \* > \* グリッドポジ \* ページで使用できます (グラフアイコンを選択します)  データ値のあとに) 状態グラフを使用して、オンライン、スタンバイ、オフラインのいずれかの状態を表す属性値がプロットされます。状態グラフは折れ線グラフに似ていますが、値が連続しておらず、別の状態に切り替わると値が飛んで表示されます。

### LDR State vs Time

2004-07-09 16:40:23 to 2004-07-09 17:17:11



関連情報

"Nodes ページを表示します"

"グリッドトポロジツリーを表示します"

"サポート指標を確認"

グラフの凡例

グラフの描画に使用される線と色には特定の意味があります。

例	意味
	レポートされる属性値は濃い緑の線でプロットされます。
	濃い緑の線の周りの薄い緑の背景は、その時間範囲内の実際の値が変化し、より高速なプロットのために「バインド」されていることを示します。濃い線は加重平均を表し、薄い緑は最大値から最小値までの範囲を示します。薄い茶色の背景は面グラフで累計データを示すために使用されます。
	データがプロットされていない空白の部分は、属性値が使用できなかったことを示します。背景色は、属性をレポートするサービスの状態に応じて、青、グレー、またはグレーと青の中間色になります。
	薄い青の背景は、サービスの状態が不明なため属性値がレポートされず、一部またはすべての属性値を特定できなかった時間範囲を示します。
	グレーの背景は、属性をレポートするサービスが管理上の理由で停止しているために、一部またはすべての属性値を取得できなかった時間範囲を示します。
	グレーと青の中間色の背景は、サービスの状態が不明なために属性値を特定できなかったか、属性をレポートするサービスが管理上の理由で停止しているために属性値を取得できなかった時間範囲を示します。

グラフとグラフを表示します

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グラフとグラフが含まれています。一部のケース、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 \* ページを使用して他のチャートにアクセスできます。

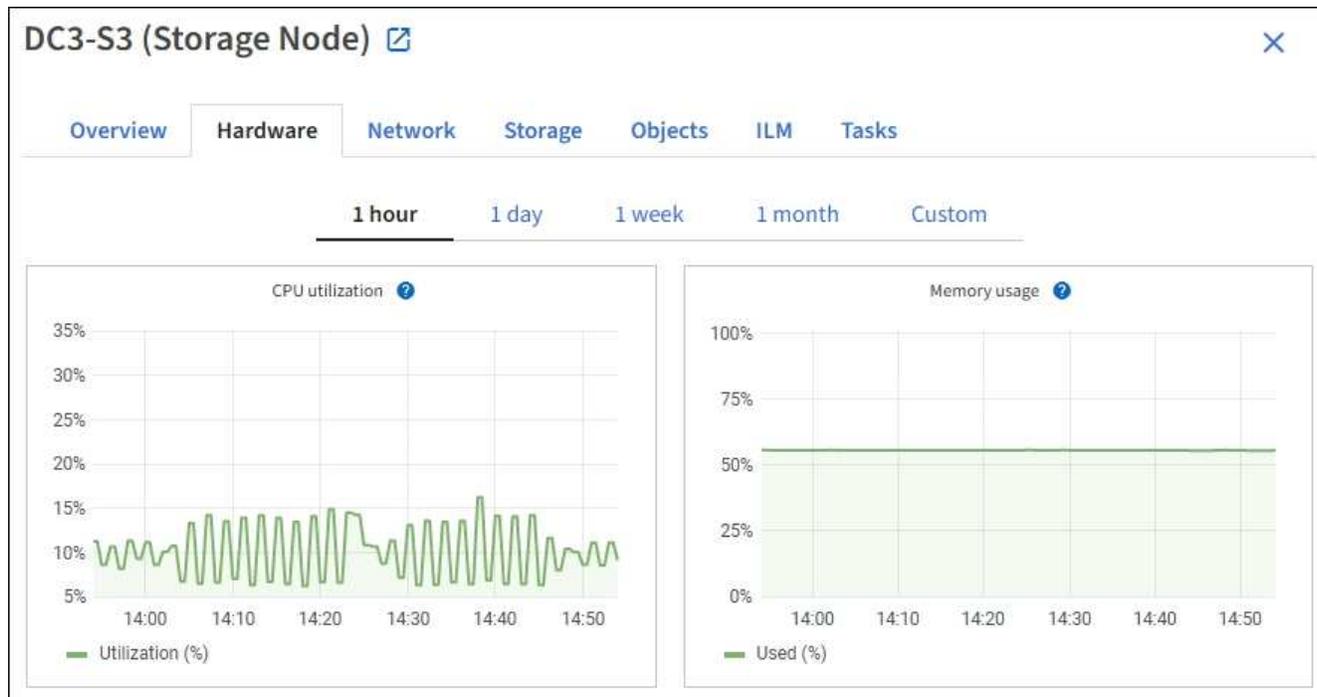
作業を開始する前に

を使用して Grid Manager にサインインする必要があります ["サポートされている Web ブラウザ"](#)。

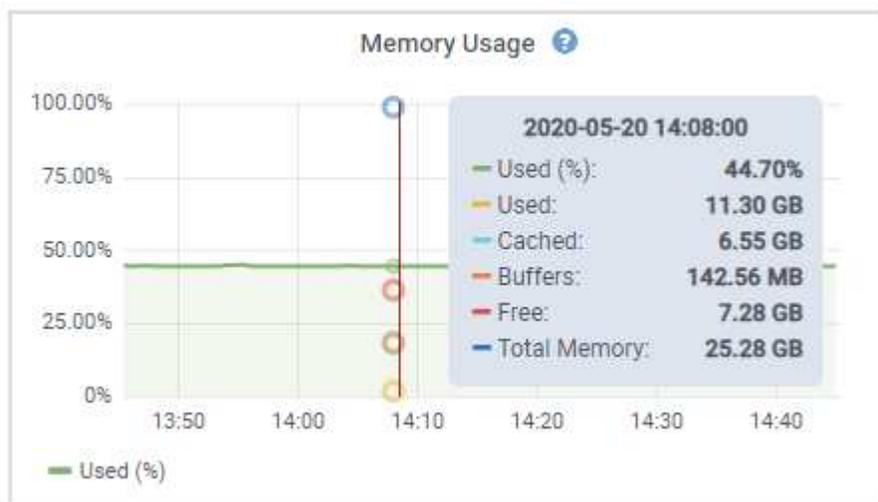
手順

1. [\* nodes (ノード) ] 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、Prometheus 指標の値の経時的プロットに使用される 1 つ以上の Grafana チャートがあります。たとえば、ノードの \*nodes\* > \*Hardware\* タブには、2 つの Grafana チャートがあります。



3. 必要に応じて、グラフにカーソルを合わせると、特定の時点の詳細な値が表示されます。



4. 必要に応じて、特定の属性や指標のグラフを表示することもできます。ノードページのテーブルで、グラフアイコンを選択します  をクリックします。

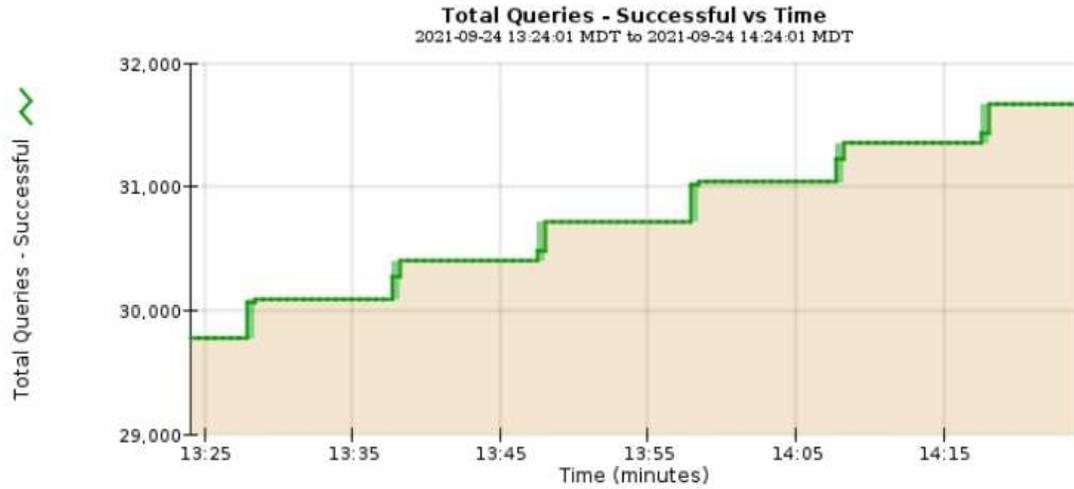


グラフは、すべての指標と属性で使用できるわけではありません。

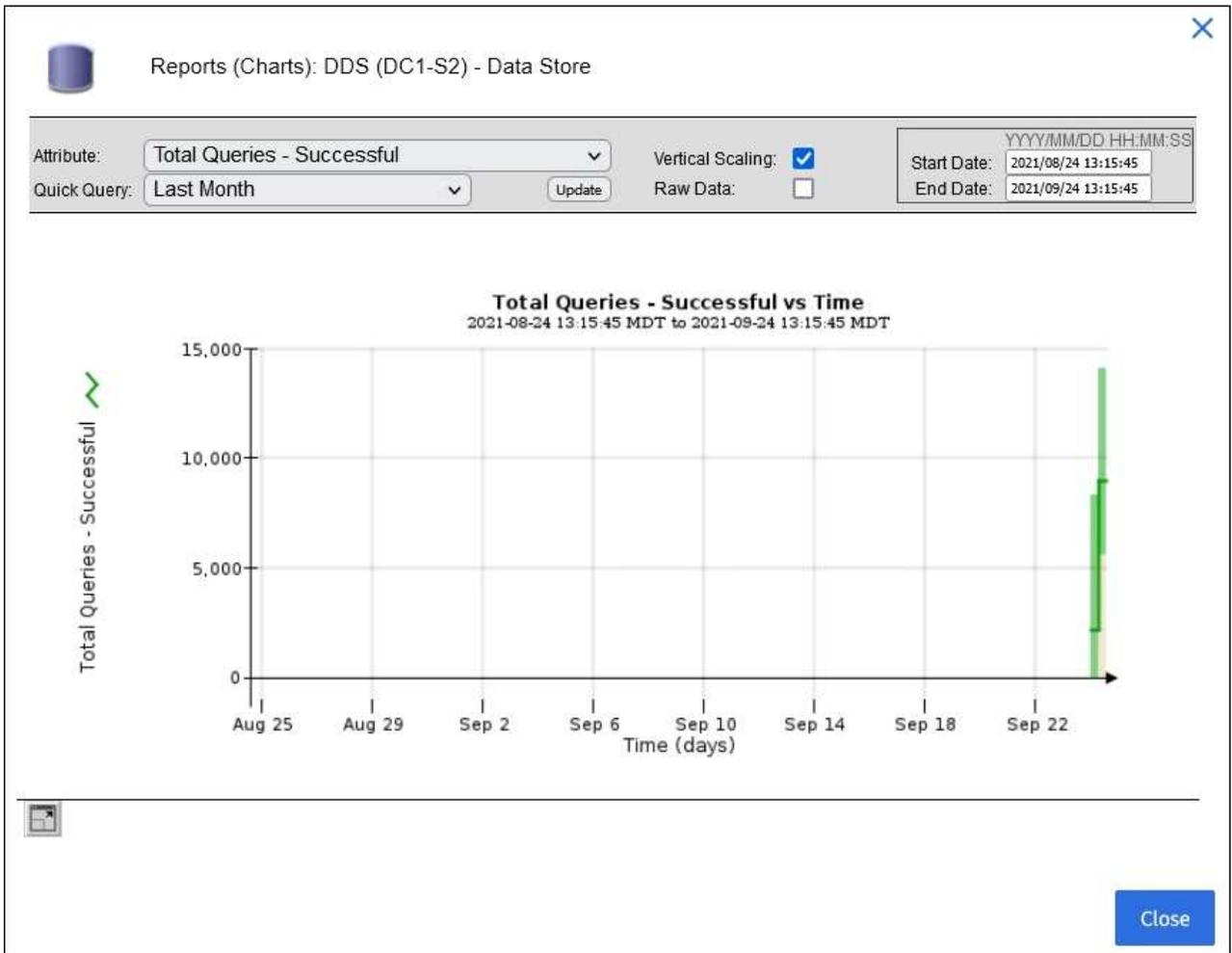
◦ 例 1\* : ストレージノードの [オブジェクト] タブで、グラフアイコンを選択できます  ストレージノードに対して成功したメタデータストアクエリの合計数を確認できます。



Attribute: Total Queries - Successful Vertical Scaling:  Start Date: 2021/09/24 13:24:01  
Quick Query: Last Hour Update Raw Data:  End Date: 2021/09/24 14:24:01



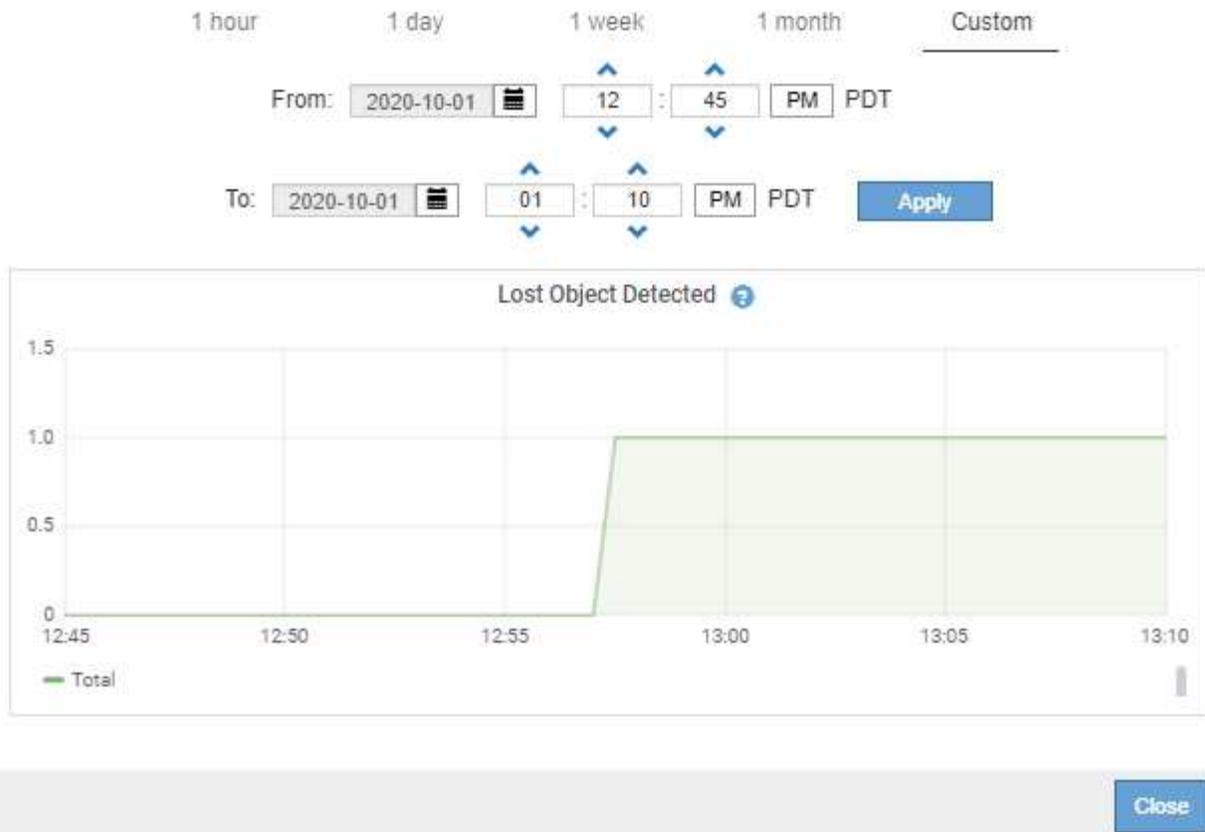
Close



\*例2\* : ストレージノードの[Objects]タブで、グラフアイコン  一定の期間に検出された損失オブジェクトの数の Grafana グラフを確認する場合。

Object Counts	
Total Objects	1
Lost Objects	1
S3 Buckets and Swift Containers	1





5. [ノード]ページに表示されていない属性のグラフを表示するには、\* support > Tools > Grid topology \*を選択します。
6. **grid node**>\*component または **SERVICE**>\* Overview > Main \* を選択します。

### Computational Resources

Service Restarts:	1	
Service Runtime:	6 days	
Service Uptime:	6 days	
Service CPU Seconds:	10666 s	
Service Load:	0.266 %	

### Memory

Installed Memory:	8.38 GB	
Available Memory:	2.9 GB	

### Processors

Processor Number	Vendor	Type	Cache
1	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
2	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
3	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
4	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
5	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
6	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
7	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
8	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB

7. グラフアイコンを選択します  をクリックします。

表示は自動的に \* Reports \* > \* Charts \* ページに変わります。このグラフには、過去 1 日間の属性のデータが表示されます。

グラフを生成します

グラフには、属性データ値がグラフィカルな形式で表示されます。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のレポートを作成できます。

作業を開始する前に

- を使用して Grid Manager にサインインする必要があります "サポートされている Web ブラウザ"。
- これで完了です "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* または *SERVICE*>\* Reports > Charts \* を選択します。
3. [\* 属性 \* ( \* Attribute \* ) ] 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. 正確な値を表示するには、**[Raw Data]\***チェックボックスをオンにします。値を小数点以下**3**桁までに丸めるには（割合でレポートされる属性など）、**[Raw Data]\***チェックボックスをオフにします。

6. **[\*Quick Query]** 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。

カスタムクエリオプションを選択して、特定の期間を選択します。

グラフが表示されるまでに少し時間がかかります。期間が長い場合は集計に数分かかることもあります。

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。

の形式を使用します **YYYY/MM/DDHH:MM:SS** 現地時間。この形式に一致するには、先頭にゼロを補う必要があります。たとえば、「2017/4/6 7 : 30 : 00」と入力すると検証に失敗します。正しい形式は「2017/04/06 07 : 30 : 00」です。

8. 「**\* Update \***」を選択します。

グラフは数秒後に生成されます。期間が長い場合は集計に数分かかることもあります。クエリで設定した時間の長さに応じて、フルレポートか要約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 サービスで処理された属性データの値がテキスト形式で表示されます。レポート対象の期間に応じて、フルレポートと要約レポートの2種類が生成されます。期間が1週間未満の場合はフルレポート、期間が1週間を超える場合は要約レポートです。

#### フルレポート

フルレポートには、選択した属性に関する詳細が表示されます。

- **Time Received** : 属性のデータのサンプル値が NMS サービスで処理された日付と時刻。
- **Sample Time** : ソースで属性値がサンプリングまたは変更された現地の日時。
- **Value** : サンプル時の属性値です。

## 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 %

### 要約レポート

要約レポートには、フルレポートよりも長い期間（通常は 1 週間）のデータが表示されます。一定の期間の複数の属性値が NMS サービスによって集計され、その結果から計算された平均値、最大値、および最小値が 1 つのエントリとして表示されます。

各エントリには、次の情報が表示されます。

- Aggregate Time : 変更された一連の属性値が NMS サービスで最後に集計（収集）された日時（現地時間）です。
- Average Value : 集計期間における属性の平均値です。
- Minimum Value : 集計期間における最小値です。
- Maximum Value : 集計期間における最大値です。

## 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します

テキストレポートには、NMS サービスで処理された属性データの値がテキスト形式で表示されます。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のレポートを作成できます。

作業を開始する前に

- を使用して Grid Manager にサインインする必要があります ["サポートされている Web ブラウザ"](#)。
- これで完了です ["特定のアクセス権限"](#)。

このタスクについて

継続的に変化することが想定される属性データについては、NMS サービス（ソース側）によって一定の間隔でデータがサンプリングされます。変化の少ない属性データ（状態やステータスが変わったときに変化するデータなど）については、属性の値が変わったときに 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、設定されている期間によって異なります。デフォルトでは、期間が 1 週間を超える場合は要約レポートが生成されます。

グレーのテキストは、サンプリング中にサービスが管理上の理由で停止していた期間を示します。青のテキストは、サービスの状態が不明であることを示します。

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* または *SERVICE* > \* Reports > Text \* を選択します。
3. [\* 属性 \* ( \* Attribute \* ) ] 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. 1 ページあたりの結果数を [\* 1 ページあたりの結果数 \* ( \* Results per Page \* ) ] ドロップダウンリストから選択します。
5. 値を小数点以下3桁までに丸めるには（割合でレポートされる属性など）、\* Raw Data \* チェックボックスをオフにします。
6. [\* Quick Query ] 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。

カスタムクエリオプションを選択して、特定の期間を選択します。

レポートが表示されるまでに少し時間がかかります。期間が長い場合は集計に数分かかることもあります。

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。

の形式を使用します YYYY/MM/DDHH:MM:SS 現地時間。この形式に一致するには、先頭にゼロを補う必要があります。たとえば、「2017/4/6 7 : 30 : 00」と入力すると検証に失敗します。正しい形式は「2017/04/06 07 : 30 : 00」です。

8. [更新 (Update) ] をクリックします。

テキストレポートが生成されるまでに少し時間がかかります。期間が長い場合は集計に数分かかることもあります。クエリで設定した時間の長さに応じて、フルレポートか要約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

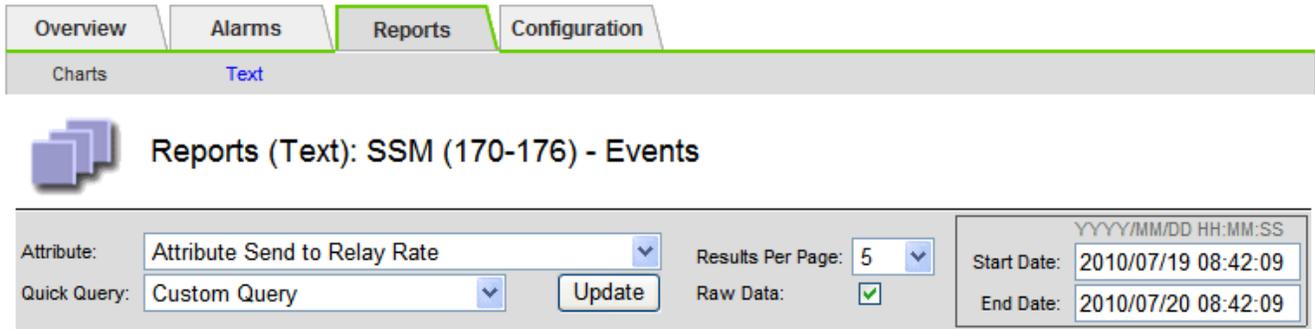
テキストレポートをエクスポートすると、ブラウザの新しいタブが開き、データを選択してコピーできます。

このタスクについて

コピーしたデータを新しいドキュメント (スプレッドシートなど) に保存して、StorageGRID システムのパフォーマンスの分析に使用できます。

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 (Export) ] をクリックします .



### Text Results for Attribute Send to Relay Rate

2010-07-19 08:42:09 PDT To 2010-07-20 08:42:09 PDT

1 - 5 of 254 

Time Received	Sample Time	Value
2010-07-20 08:40:46	2010-07-20 08:40:46	0.274981485 Messages/s
2010-07-20 08:38:46	2010-07-20 08:38:46	0.274989 Messages/s
2010-07-20 08:36:46	2010-07-20 08:36:46	0.283317543 Messages/s
2010-07-20 08:34:46	2010-07-20 08:34:46	0.274982493 Messages/s
2010-07-20 08:32:46	2010-07-20 08:32:46	0.291646426 Messages/s

Previous « 1 2 3 4 5 » Next

Export Text Report ウィンドウが開き、レポートが表示されます。

Grid ID: 000 000

OID: 2.16.124.113590.2.1.400019.1.1.1.1.16996732.200

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。

このデータを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るようになりました。

## PUT / GET パフォーマンスを監視

オブジェクトストアや読み出しなどの特定の処理のパフォーマンスを監視して、詳しい調査が必要な変更を特定することができます。

このタスクについて

PUT および GET 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、またはオープンソースの S3tester アプリケーションを使用して、S3 および Swift コマンドを実行します。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 の外部にある要因とは関係なくパフォーマンスを評価できます。

PUT 処理と GET 処理のテストを実行するときは、次のガイドラインに従ってください。

- グリッドに通常取り込むオブジェクトと同等のサイズのオブジェクトを使用します。
- ローカルサイトとリモートサイトの両方に対して処理を実行します。

のメッセージ ["監査ログ"](#) 特定の処理の実行に必要な合計時間を示します。たとえば、S3 GET 要求に対する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。次の処理の監査メッセージで TIME 属性を確認することもできます。

- \* S3 \* : DELETE、GET、HEAD、Metadata Updated、POST、PUT
- \* Swift \* : DELETE、GET、HEAD、PUT

結果を分析する際には、要求を満たすために必要な平均時間と、達成可能な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。

- 可能です ["github から S3tester をダウンロードします"](#)。

オブジェクト検証処理を監視する

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て、オブジェクトの破損や欠落の有無を確認します。

作業を開始する前に

- を使用して Grid Manager にサインインします ["サポートされている Web ブラウザ"](#)。
- を使用することができます ["Maintenance権限またはRoot Access権限"](#)。

このタスクについて

2つ ["検証プロセス"](#) 連携してデータの整合性を確保：

- **\* バックグラウンド検証 \*** は、オブジェクトデータの正確性を継続的にチェックするために自動的に実行されます。

バックグラウンド検証では、すべてのストレージノードが自動的にかつ継続的にチェックされて、レプリケートオブジェクトデータとイレイジャーコーディングオブジェクトデータのコピーが破損していないかどうかを確認されます。問題が見つかった場合、StorageGRID システムは、システム内の別の場所に格納されているコピーから、破損したオブジェクトデータを自動的に置き換えます。バックグラウンド検証は、アーカイブノードやクラウドストレージプール内のオブジェクトに対しては実行されません。



自動的に修正できない破損オブジェクトが検出されると、\* Unidentified corrupt object detected \*アラートがトリガーされます。

- **\* オブジェクトの存在チェック \*** は、オブジェクトデータの有無（正確性ではなく）をより迅速に確認するためにユーザによってトリガーされます。

オブジェクトの存在チェックでは、オブジェクトとイレイジャーコーディングフラグメントの想定されるレプリケートコピーがすべてストレージノードに存在するかどうかを検証されます。オブジェクトの存在チェックは、ストレージデバイスの整合性を検証する手段を提供します。特に、最新のハードウェア問題がデータの整合性に影響を与える可能性がある場合に役立ちます。

バックグラウンド検証の結果を定期的に確認し、オブジェクトの存在をチェックする必要があります。オブジェクトデータの破損や欠落が見つかった場合は、すぐに調べてルートを特定します。

手順

1. バックグラウンド検証の結果を確認します。
  - a. ノード `* > * _ストレージノード _ * > * オブジェクト *` を選択します。
  - b. 検証結果を確認します。
    - レプリケートされたオブジェクトデータの検証を確認するには、Verification セクションの属性を確認します。

### Verification

Status: ?	No errors	
Percent complete: ?	0.00%	
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	

- ・ イレイジャーコーディングフラグメントの検証を確認するには、「\*\_ストレージノード\_\*>\*\_ILM\_\*」を選択し、イレイジャーコーディングの検証セクションの属性を確認します。

### Erasure coding verification

Status: ?	Idle	
Next scheduled: ?	2021-10-08 10:45:19 MDT	
Fragments verified: ?	0	
Data verified: ?	0 bytes	
Corrupt copies: ?	0	
Corrupt fragments: ?	0	
Missing fragments: ?	0	

疑問符を選択します ? をクリックして、ヘルプテキストを表示します。

- オブジェクト存在チェックジョブの結果を確認します。
  - [\*\_maintenance\_\* (メンテナンス \*) ]>[\* Object existence check\_\* (オブジェクトの存在確認 \*) ]>[\* Job history\_\* (ジョブ
  - Missing object copies Detected 列をスキャンします。100個以上のオブジェクトコピーが欠落しているジョブがあり、\*\_Objects lost\_\*アラートがトリガーされている場合は、テクニカルサポートに連絡してください。

# Object existence check

Perform an object existence check if you suspect storage volumes have been damaged or are corrupt. You can verify that objects defined by your ILM policy, still exist on the volumes.

Active job		Job history		
Delete	Search...			
<input type="checkbox"/>	Job ID ?	Status	Nodes (volumes) ?	Missing object copies detected ?
<input type="checkbox"/>	15816859223101303015	Completed	DC2-S1 (3 volumes)	0
<input type="checkbox"/>	12538643155010477372	Completed	DC1-S3 (1 volume)	0
<input type="checkbox"/>	5490044849774982476	Completed	DC1-S2 (1 volume)	0
<input type="checkbox"/>	3395284277055907678	Completed	DC1-S1 (3 volumes) DC1-S2 (3 volumes) DC1-S3 (3 volumes) and <a href="#">7 more</a>	0

## イベントを監視する

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。これには、syslog サーバに記録されたイベントを追跡するために作成したカスタムイベントも含まれます。グリッドマネージャに表示される Last Event メッセージには、最新のイベントに関する詳細が表示されます。

イベントメッセージは、にも表示されます `/var/local/log/bycast-err.log` ログファイル：を参照してください "[ログファイル参照](#)"。

SMTT (Total events) アラームは、ネットワークの問題、電源の停止、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。ここでは、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、イベントを調査する方法について説明します。既知の問題が原因でイベントが発生した場合、イベントカウンタをリセットしても安全です。

## 手順

- 各グリッドノードのシステムイベントを確認します。
  - サポート \* > ツール \* > グリッドトポロジ \* を選択します。
  - [[site \\*](#)] > [[\\*\\_grid node\\*](#)] > ssm \* > Events \* > Overview \* > Main \* の順に選択します。
- 以前のイベントメッセージのリストを生成して、過去に発生した問題を特定します。

- 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 \* > \* Events \* > \* Reports \* ] を選択します。
- c. 「 \* テキスト \* 」を選択します。
  - Last Event \* 属性には表示されません "グラフビュー"。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. 「 \* Update \* 」を選択します。

#### カスタム syslog イベントを作成する

カスタムイベントでは、カーネル、デーモン、エラーとクリティカルのレベルのユーザイベントなど、syslog サーバに記録されるすべての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（ネットワークセキュリティイベントやハードウェア障害）の発生を監視するのに役立ちます。

#### このタスクについて

繰り返し発生する問題については、カスタムイベントの作成を検討してください。カスタムイベントを使用する際は、次の点を考慮する必要があります

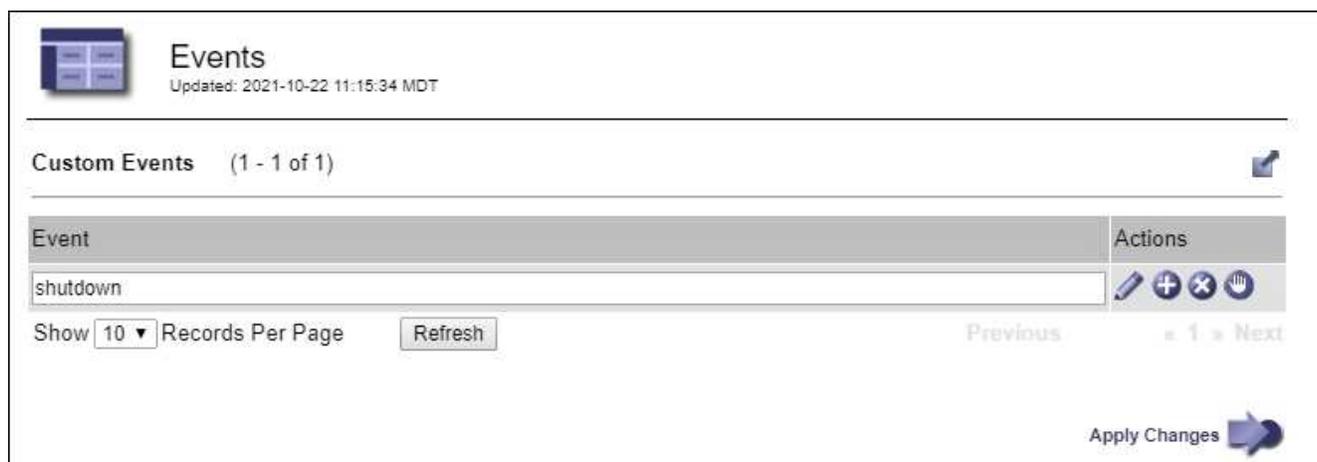
- カスタムイベントが作成されると、該当するイベントが発生するたびに監視されます。
- でキーワードに基づいてカスタムイベントを作成します /var/local/log/messages ファイル。これらのファイルのログは次のようにする必要があります。
  - カーネルによって生成されます
  - デーモンまたはユーザプログラムによってエラーまたはクリティカルのレベルで生成されます

\*注：\*内のすべてのエントリが含まれているわけではありません /var/local/log/messages 上記の要件を満たしていないファイルは照合されます。

#### 手順

1. support>\* Alarms (レガシー) > Custom events \* を選択します。

2. [編集 (Edit)] をクリックします。  (または \*Insert\*)  最初のイベントではない場合) をクリックします。
3. shutdown などのカスタムイベント文字列を入力します



4. 「\* 変更を適用する \*」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 > Events \* を選択します。
7. Events テーブルで Custom Events のエントリを探し、\* Count \* の値を監視します。

カウントが増えていけば、そのグリッドノードで監視しているカスタムイベントがトリガーされています。

Overview: SSM (DC1-ADM1) - Events  
Updated: 2021-10-22 11:19:18 MDT

### System Events

Log Monitor State: Connected

Total Events: 0

Last Event: No Events

Description	Count
Abnormal Software Events	0
Account Service Events	0
Cassandra Errors	0
Cassandra Heap Out Of Memory Errors	0
Chunk Service Events	0
<b>Custom Events</b>	<b>0</b>
Data-Mover Service Events	0
File System Errors	0
Forced Termination Events	0
Grid Node Errors	0
Hotfix Installation Failure Events	0
I/O Errors	0
IDE Errors	0
Identity Service Events	0
Kernel Errors	0
Kernel Memory Allocation Failure	0
Keystone Service Events	0
Network Receive Errors	0
Network Transmit Errors	0
Out Of Memory Errors	0
Replicated State Machine Service Events	0
SCSI Errors	0

カスタムイベントのカウンタを 0 にリセットします

カスタムイベントのカウンタのみをリセットする場合は、の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。一方、アラームを確認した場合は、次のしきい値レベルに達したときにのみ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 \* > \* Events \* > \* Configuration \* > \* Main \* を選択します。
3. [Custom Events]の[Reset]チェックボックスをオンにします。

Overview			Alarms			Reports			Configuration		
Main			Alarms								
 <b>Configuration: SSM (DC2-ADM1) - Events</b> Updated: 2018-04-11 10:35:44 MDT											
Description	Count	Reset									
Abnormal Software Events	0	<input type="checkbox"/>									
Account Service Events	0	<input type="checkbox"/>									
Cassandra Errors	0	<input type="checkbox"/>									
Cassandra Heap Out Of Memory Errors	0	<input type="checkbox"/>									
Custom Events	0	<input checked="" type="checkbox"/>									
File System Errors	0	<input type="checkbox"/>									
Forced Termination Events	0	<input type="checkbox"/>									

4. 「 \* 変更を適用する \* 」を選択します。

監査メッセージを確認します

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

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

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

各管理ノードで、監査メッセージがテキストファイルに保存されます。監査共有には、アクティブファイル（audit.log）と、圧縮された過去の監査ログが含まれています。グリッド内の各ノードには、ノードで生成された監査情報のコピーも格納されます。

監査ログに簡単にアクセスするために、を使用できます ["NFSの監査クライアントアクセスを設定します"](#)。管理ノードのコマンドラインから直接監査ログファイルにアクセスすることもできます。

StorageGRIDでは、デフォルトで監査情報を送信することも、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デスティネーションに設定されます。
- 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ことがあります。

す。

- 必要に応じて、監査ログのデスティネーションを変更したり、監査情報を外部 syslog サーバに送信したりできます。外部 syslog サーバが設定されても、監査レコードのローカルログは引き続き生成および格納されます。
- ["監査メッセージとログの送信先の設定について"](#)です。

監査ログファイル、監査メッセージの形式、監査メッセージのタイプ、および監査メッセージの分析に使用できるツールの詳細については、[を参照してください "監査ログを確認します"](#)。

## ログファイルとシステムデータを収集

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（設定データを含む）を取得できます。

### 作業を開始する前に

- プライマリ管理ノードで、[を使用してGrid Managerにサインインする必要があります "サポートされている Web ブラウザ"](#)。
- これで完了です ["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。

### このタスクについて

Grid Manager を使用して収集できます ["ログファイル"](#)をクリックします。収集されたデータは .tar.gz ファイルにアーカイブされ、ローカルコンピュータにダウンロードできます。

必要に応じて、監査ログのデスティネーションを変更したり、監査情報を外部 syslog サーバに送信したりできます。外部 syslog サーバが設定されても、監査レコードのローカルログは引き続き生成および格納されます。[を参照してください "監査メッセージとログの送信先を設定します"](#)。

### 手順

1. [ \* support \* > \* Tools \* > \* Logs \* ] 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、\* Start Time \* および \* End Time \* を選択します。

非常に長い期間を選択したり、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りすると、ログアーカイブが大きくなりすぎてノードに格納できなくなったり、ダウンロード用にプライマリ管理ノードに保存できなくなったりすることがあります。その場合は、より小さな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. 収集するログのタイプを選択します。

- \* 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、使用可能なアプリケーションログの一部です。
- \* Audit Logs \* : 通常のシステム運用中に生成された監査メッセージを含むログ。
- \* Network Trace \* : ネットワーク・デバッグに使用するログ。
- \* Prometheus Database \* : すべてのノード上のサービスからの時系列の指標。

5. 必要に応じて、収集するログファイルに関するメモを \* Notes \* テキストボックスに入力します。

このメモを使用して、ログファイルを収集する原因となった問題に関するテクニカルサポート情報を入力できます。メモはというファイルに追加されます `info.txt``と、ログファイルの収集に関するその他の情報。 ``info.txt` ファイルはログファイルのアーカイブパッケージに保存されます。

- StorageGRID システムのプロビジョニングパスフレーズを \* プロビジョニングパスフレーズ \* テキストボックスに入力します。
- [Collect Logs] を選択します。

新しい要求を送信すると、以前に収集されたログファイルは削除されます。

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捗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た場合は、ログを収集する期間を短縮するか、またはノードの数を減らしてください。

- ログファイルの収集が完了したら、「\* Download \*」を選択します。

完了後

必要に応じて、ログファイルのアーカイブパッケージはあとから再度ダウンロードできます。

必要に応じて、\* Delete \* 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・スペースを解放できます。ログファイルの現在の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

テクニカルサポートによるStorageGRIDシステムの問題のトラブルシューティングを支援するために、送信するAutoSupportパッケージを手動でトリガーできます。

作業を開始する前に

- を使用して Grid Manager にサインインする必要があります ["サポートされている Web ブラウザ"](#)。
- Root Access権限またはその他のグリッド設定権限が必要です。

手順

- [\* support \* > \* Tools \* > \* AutoSupport \*] を選択します。
- [アクション]タブで、\*[ユーザートリガー型AutoSupportの送信]\*を選択します。

StorageGRIDはAutoSupportパッケージをNetApp Support Siteに送信しようとします。試行に成功した場合は、[結果 (Results)] タブの [最新結果 (Recent Result)] \* 値と [前回成功した時間 (Last Successful Time)] \* 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パッケージを再送信しません。

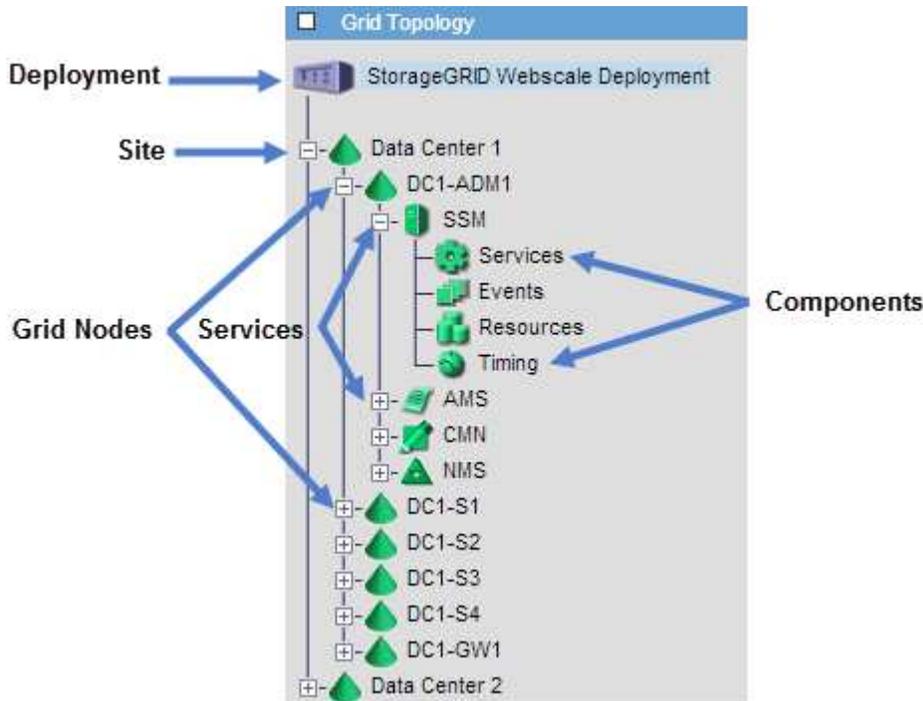


User-triggered AutoSupportパッケージを送信したら、1分後にブラウザのAutoSupportページを更新して最新の結果にアクセスしてください。

グリッドトポロジツリーを表示します

グリッドトポロジツリーを使用すると、サイト、グリッドノード、サービス、コンポーネントなど、StorageGRID の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、グリッドトポロジツリーへのアクセスが必要になるのは、ドキュメントで指示されているとき、またはテクニカルサポートとともに作業するときに限られます。

グリッドトポロジツリーにアクセスするには、 \* support \* > \* Tools \* > \* Grid Topology \* 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、をクリックします **+** または **-** をクリックします。サイト全体または各ノード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について、値とステータスを報告します。属性値は、グリッドノードごと、サイトごと、およびグリッド全体について収集されます。

StorageGRID 属性は、グリッドマネージャのいくつかの場所で使用されます。

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

### 属性値

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

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

## サポート指標を確認

問題のトラブルシューティングでは、テクニカルサポートと協力して StorageGRID システムの詳細な指標とグラフを確認することができます。

### 作業を開始する前に

- を使用して Grid Manager にサインインする必要があります ["サポートされている Web ブラウザ"](#)。
- これで完了です ["特定のアクセス権限"](#)。

### このタスクについて

Metrics ページでは、Prometheus と Grafana のユーザインターフェイスにアクセスできます。Prometheus は指標を収集するオープンソースソフトウェアです。Grafana は指標を視覚化するオープンソースソフトウェアです。



Metrics ページで使用可能なツールは、テクニカルサポートが使用することを目的としています。これらのツールの一部の機能およびメニュー項目は意図的に機能しないため、変更される場合があります。のリストを参照してください ["よく使用される Prometheus 指標"](#)。

### 手順

1. テクニカルサポートの指示に従って、`* support *` > `* Tools *` > `* Metrics *` を選択します。

ここでは、[Metrics] ページの例を示します。

# Metrics

Access charts and metrics to help troubleshoot issues.

 The tools available on this page are intended for use by technical support. Some features and menu items within these tools are intentionally non-functional.

## Prometheus

Prometheus is an open-source toolkit for collecting metrics. The Prometheus interface allows you to query the current values of metrics and to view charts of the values over time.

Access the Prometheus UI using the link below. You must be signed in to the Grid Manager.

- <https://...>

## Grafana

Grafana is open-source software for metrics visualization. The Grafana interface provides pre-constructed dashboards that contain graphs of important metric values over time.

Access the Grafana dashboards using the links below. You must be signed in to the Grid Manager.

<a href="#">ADE</a>	<a href="#">EC Overview</a>	<a href="#">Replicated Read Path Overview</a>
<a href="#">Account Service Overview</a>	<a href="#">Grid</a>	<a href="#">S3 - Node</a>
<a href="#">Alertmanager</a>	<a href="#">ILM</a>	<a href="#">S3 Overview</a>
<a href="#">Audit Overview</a>	<a href="#">Identity Service Overview</a>	<a href="#">S3 Select</a>
<a href="#">Cassandra Cluster Overview</a>	<a href="#">Ingests</a>	<a href="#">Site</a>
<a href="#">Cassandra Network Overview</a>	<a href="#">Node</a>	<a href="#">Support</a>
<a href="#">Cassandra Node Overview</a>	<a href="#">Node (Internal Use)</a>	<a href="#">Traces</a>
<a href="#">Cross Grid Replication</a>	<a href="#">OSL - AsyncIO</a>	<a href="#">Traffic Classification Policy</a>
<a href="#">Cloud Storage Pool Overview</a>	<a href="#">Platform Services Commits</a>	<a href="#">Usage Processing</a>
<a href="#">EC - ADE</a>	<a href="#">Platform Services Overview</a>	<a href="#">Virtual Memory (vmstat)</a>
<a href="#">EC - Chunk Service</a>	<a href="#">Platform Services Processing</a>	

- StorageGRID 指標の現在の値を照会し、一定期間の値のグラフを表示するには、Prometheus セクション内のリンクをクリックします。

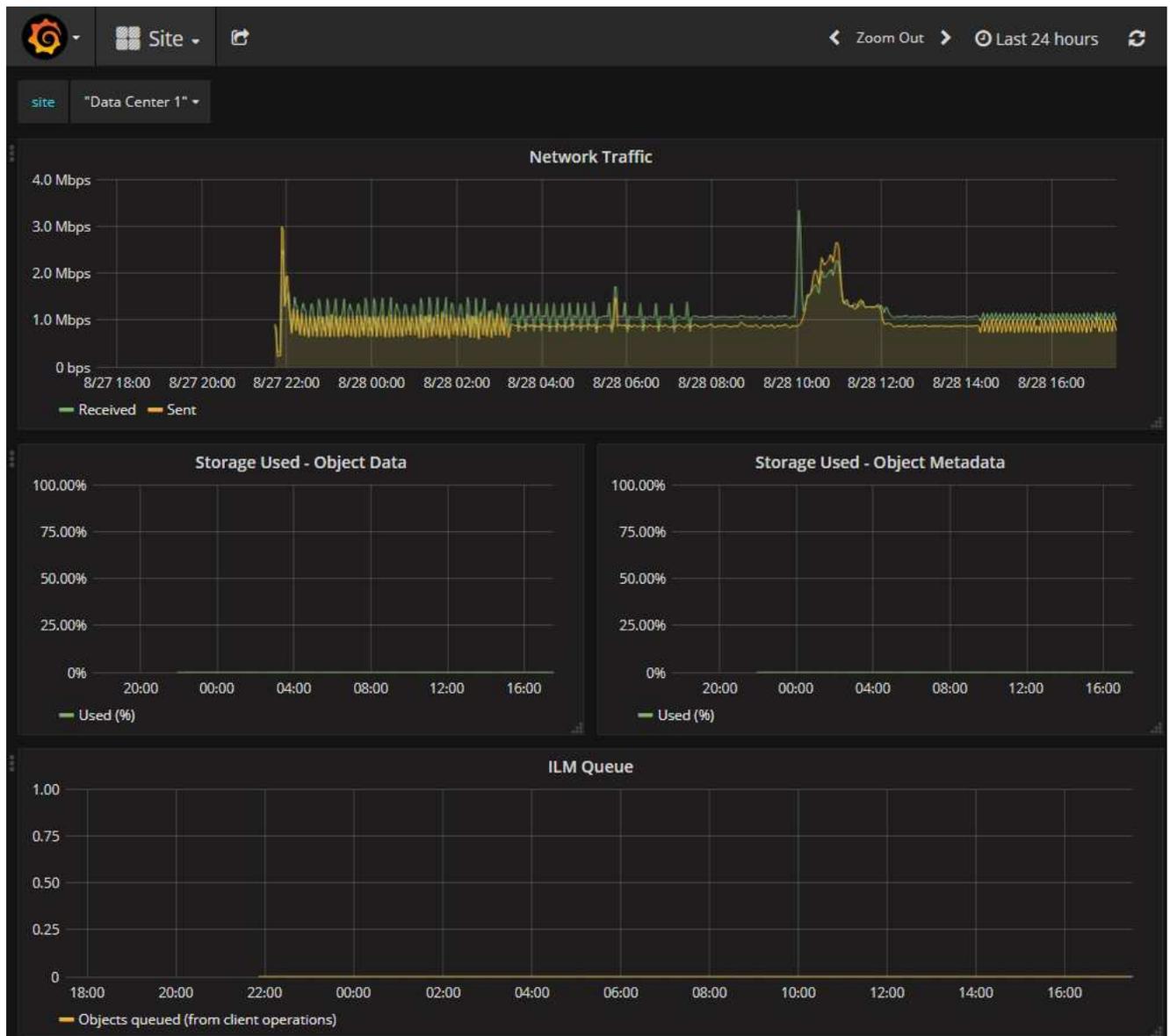
Prometheus インターフェイスが表示されます。このインターフェイスでは、使用可能な StorageGRID 指標に対してクエリを実行したり、StorageGRID 指標の推移をグラフ化したりできます。



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

- 時間の経過に伴う StorageGRID 指標のグラフを含む構築済みのダッシュボードにアクセスするには、Grafana セクションのリンクをクリックします。

選択したリンクに対応した Grafana インターフェイスが表示されます。



診断を実行します

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協力して StorageGRID システムの診断を実行し、結果を確認します。

- "サポート指標を確認"
- "よく使用される Prometheus 指標"

作業を開始する前に

- を使用して Grid Manager にサインインします "サポートされている Web ブラウザ"。
- これで完了です "特定のアクセス権限"。

このタスクについて

Diagnostics (診断) ページでは、グリッドの現在の状態に対して一連の診断チェックが実行されます。各診断点検には、次の3つのいずれかのステータスがあります。

-  \* 標準 \* : すべての値が標準範囲内です。
-  \* 注意 \* : 1 つ以上の値が正常範囲外です。
-  \* 注意 \* : 1 つ以上の値が通常の範囲外です。

診断ステータスは現在のアラートとは関係なく、グリッドで発生している処理の問題を示しているとは限りません。たとえば、アラートがトリガーされていない場合でも、診断チェックで警告ステータスが表示されることがあります。

#### 手順

1. サポート \* > ツール \* > 診断 \* を選択します。

Diagnostics（診断）ページが表示され、診断チェックごとの結果がリストされます。結果は重大度（[注意]、[注意]、[標準]）でソートされます。それぞれの重大度の中で、結果はアルファベット順にソートされます。

この例では、すべての診断のステータスは Normal です。

## Diagnostics

This page performs a set of diagnostic checks on the current state of the grid. A diagnostic check can have one of three statuses:

-  **Normal:** All values are within the normal range.
-  **Attention:** One or more of the values are outside of the normal range.
-  **Caution:** One or more of the values are significantly outside of the normal range.

Diagnostic statuses are independent of current alerts and might not indicate operational issues with the grid. For example, a diagnostic check might show Caution status even if no alert has been triggered.

Run Diagnostics

 Cassandra automatic restarts	▼
 Cassandra blocked task queue too large	▼
 Cassandra commit log latency	▼
 Cassandra commit log queue depth	▼

2. 特定の診断の詳細については、行の任意の場所をクリックしてください。

診断とその現在の結果の詳細が表示されます。以下の詳細が表示されます。

- \* 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 \* : 診断に使用した場合、ステータス値の生成に使用した Prometheus 式。（

Prometheus 式は一部の診断には使用されません。

- \* しきい値 \* : 診断に使用できる場合は、異常な診断ステータスごとに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)。



これらのしきい値は変更できません。

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

✓ CPU utilization

Checks the current CPU utilization on each node.

To view charts of CPU utilization and other per-node metrics, access the [Node Grafana dashboard](#).

Status ✓ Normal

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

Thresholds ⚠ Attention >= 75%  
✖ Caution >= 95%

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

3. \* オプション \* : この診断に関連した Grafana チャートを表示するには、\* Grafana dashboard dashboard \* 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、このノードの CPU 利用率とノードの他の Grafana チャートを示すノードダッシュボードが表示されます。



また、構築済みの Grafana ダッシュボードには、\* support \* > \* Tools \* > \* Metrics \* ページの Grafana セクションからアクセスできます。



4. \* オプション \* :一定の期間にわたる Prometheus 式のチャートを表示するには、\* Prometheus で表示 \* をクリックします。

診断に使用された式の Prometheus グラフが表示されます。

Enable query history

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

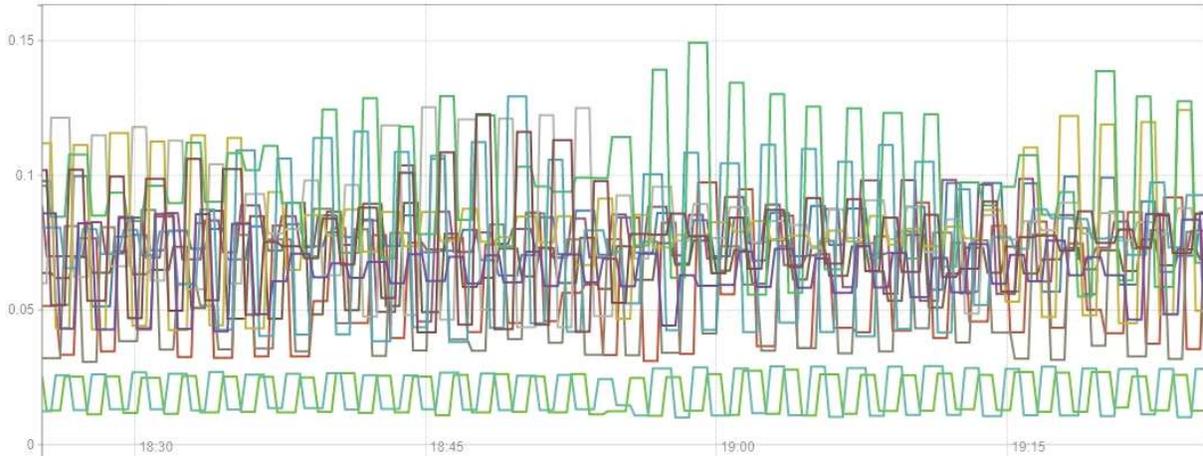
Load time: 547ms  
Resolution: 14s  
Total time series: 13

Execute

- insert metric at cursor -

Graph Console

1h    +    << Until >>    Res. (s)     stacked



- {instance="DC3-S3"}
- {instance="DC3-S2"}
- {instance="DC3-S1"}
- {instance="DC2-S3"}
- {instance="DC2-S2"}
- {instance="DC2-S1"}
- {instance="DC2-ADM1"}
- {instance="DC1-S3"}
- {instance="DC1-S2"}
- {instance="DC1-S1"}
- {instance="DC1-G1"}
- {instance="DC1-ARC1"}
- {instance="DC1-ADM1"}

Remove Graph

Add Graph

カスタムの監視アプリケーションを作成

グリッド管理 API から取得される StorageGRID 指標を使用して、カスタムの監視アプリケーションやダッシュボードを構築できます。

グリッドマネージャの既存のページに表示されていない指標を監視する場合や、StorageGRID 用のカスタムダッシュボードを作成する場合は、グリッド管理APIを使用してStorageGRID 指標を照会できます。

また、Grafana などの外部監視ツールを使用して、Prometheus 指標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、管理用クライアント証明書をアップロードまたは生成して、StorageGRID でセキュリティを確保するためにツールを認証する必要があります。を参照してください ["StorageGRID の管理手順"](#)。

使用可能なすべての指標を含む指標 API 処理を表示するには、Grid Manager に移動します。ページ上部のヘルプアイコンを選択し、\* API documentation > metrics \*を選択します。



GET	<code>/grid/metric-labels/{label}/values</code> Lists the values for a metric label	
GET	<code>/grid/metric-names</code> Lists all available metric names	
GET	<code>/grid/metric-query</code> Performs an instant metric query at a single point in time	
GET	<code>/grid/metric-query-range</code> Performs a metric query over a range of time	

[API documentation][Metrics]セクション"]

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、このドキュメントでは説明していません。

## StorageGRID システムのトラブルシューティングを行う

### StorageGRID システムのトラブルシューティング：概要

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考に、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、一部の問題をテクニカルサポートにエスカレーションする必要があります。

#### 問題を定義します

問題を解決するための最初のステップは、問題を明確に定義することです。

次の表に、問題を定義するために収集する情報の種類の例を示します。

質問	応答例
StorageGRID システムはどのような状況にあり、どのような症状があるか？	オブジェクトをStorageGRID に取り込めないことがクライアントアプリケーションから報告されている。
問題はいつ発生しましたか？	2020年1月8日 14：50 頃にオブジェクトの取り込みが最初に拒否された。
最初にどのようにして問題に気付いたか。	クライアントアプリケーションから通知される。アラートのEメール通知も受け取った。
問題は一貫して発生しますか、または時々発生しますか？	問題は現在も続いています。

質問	応答例
問題が定期的が発生する場合は、原因 を実行する手順を確認してください	問題は、クライアントがオブジェクトの取り込みを試みるたびに発生します。
問題が断続的に発生する場合は、いつ発生しますか？各インシデントの発生時刻を記録します。	問題は間欠的ではありません。
この問題を以前に見たことがありますか？過去にこの問題が発生した頻度はどのくらいですか？	この問題 を初めて見たときです。

### システムに対するリスクと影響を評価

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、クリティカルなアラートがあるからといって、システムがコアサービスを提供していないわけではありません。

次の表は、前述の問題の例について、システムの運用に対する影響をまとめたものです。

質問	応答例
StorageGRID システムでコンテンツを取り込むことはできますか。	いいえ
クライアントアプリケーションでコンテンツを読み出せるかどうか	読み出すことができるオブジェクトと読み出すことができないオブジェクトがあります。
データがリスクにさらされているかどうか	いいえ
業務を遂行する能力に重大な影響はありますか。	はい。クライアントアプリケーションからStorageGRID システムにオブジェクトを格納できず、データを一貫して読み出すことができないためです。

### データを収集

問題を定義し、リスクと影響を評価したら、分析のためにデータを収集します。収集に最も役立つデータの種類の、問題の内容によって異なります。

収集するデータのタイプ	データを収集する理由	手順
最近の変更のタイムラインを作成します	StorageGRID システム、その設定、または環境を変更すると、原因 の新しい動作を開始できます。	<ul style="list-style-type: none"> <li>最近の変更のタイムラインを作成します</li> </ul>

収集するデータのタイプ	データを収集する理由	手順
アラートとアラームを確認します	<p>アラートとアラームを使用すると、原因となっている問題に関する重要な手がかりを提供して、問題のルート原因をすばやく特定することができます。</p> <p>現在のアラートとアラームのリストを確認して、StorageGRID が問題のルート原因を特定したかどうかを確認します。</p> <p>過去にトリガーされたアラートやアラームを確認して、詳細な分析情報を入手できます。</p>	<ul style="list-style-type: none"> <li>• "現在のアラートと解決済みのアラートを表示します"</li> <li>• "アラームの管理 (従来のシステム) "</li> </ul>
イベントを監視する	<p>イベントには、ノードのシステムエラーまたは障害イベント、ネットワークエラーなどのエラーが含まれます。イベントを監視して、問題の詳細やトラブルシューティングに役立てることができます。</p>	<ul style="list-style-type: none"> <li>• "イベントを監視する"</li> </ul>
グラフとテキストレポートを使用して傾向を特定します	<p>傾向は、問題が発生したときに役立つヒントを提供し、変化の速さを把握するのに役立ちます。</p>	<ul style="list-style-type: none"> <li>• "チャートとグラフを使用します"</li> <li>• "テキストレポートを使用する"</li> </ul>
ベースラインを設定する	<p>さまざまな運用値の通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偏差は、貴重な手がかりとなります。</p>	<ul style="list-style-type: none"> <li>• ベースラインを設定する</li> </ul>
取り込みと読み出しのテストを実行する	<p>取り込みと読み出しに関するパフォーマンスの問題のトラブルシューティングを行うには、ワークステーションを使用してオブジェクトの格納と読み出しを行います。クライアントアプリケーションを使用して確認した結果と比較します。</p>	<ul style="list-style-type: none"> <li>• "PUT / GET パフォーマンスを監視"</li> </ul>
監査メッセージを確認します	<p>StorageGRID の処理の詳細については、監査メッセージを確認してください。監査メッセージの詳細は、パフォーマンスの問題など、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。</p>	<ul style="list-style-type: none"> <li>• "監査メッセージを確認します"</li> </ul>
オブジェクトの場所とストレージの整合性をチェックする	<p>ストレージに問題がある場合は、オブジェクトが想定どおりに配置されていることを確認します。ストレージノード上のオブジェクトデータの整合性をチェックします。</p>	<ul style="list-style-type: none"> <li>• "オブジェクト検証処理を監視する"</li> <li>• "オブジェクトデータの場所を確認する"</li> <li>• "オブジェクトの整合性を検証"</li> </ul>

収集するデータのタイプ	データを収集する理由	手順
テクニカルサポートに使用するデータを収集します	テクニカルサポートに問い合わせた際に、問題のトラブルシューティングに役立つデータの収集や特定の情報の確認を求められることがあります。	<ul style="list-style-type: none"> <li>• "ログファイルとシステムデータを収集"</li> <li>• "AutoSupportパッケージを手動でトリガーする"</li> <li>• "サポート指標を確認"</li> </ul>

最近の変更のタイムラインを作成します

問題が発生した場合は、最近の変更内容と、その変更がいつ行われたかを検討する必要があります。

- StorageGRID システム、その設定、または環境を変更すると、原因の新しい動作を開始できます。
- 変更のスケジュールを確認することで、問題の担当となる変更を特定し、各変更がその開発にどのような影響を及ぼすかを特定できます。

システムに最近行われた変更の表を作成します。この表には、各変更がいつ行われたかに関する情報と、変更の進行中に他に何が行われたかに関する関連情報が含まれます。

変更時刻	変更のタイプ	詳細
<p>例：</p> <ul style="list-style-type: none"> <li>• ノードのリカバリを開始したのはいつですか？</li> <li>• ソフトウェアのアップグレードはいつ完了しましたか？</li> <li>• プロセスを中断しましたか？</li> </ul>	<p>どうしましたか？何をしましたか？</p>	<p>変更に関連する詳細を文書化します。例：</p> <ul style="list-style-type: none"> <li>• ネットワークの詳細が変更されました。</li> <li>• インストールされたホットフィックス。</li> <li>• クライアントのワークロードの変化</li> </ul> <p>同時に複数の変更が発生した場合は注意してください。たとえば、アップグレードの実行中にこの変更が行われたかどうかを確認します。</p>

### 最近の重要な変更の例

重要な変更の例をいくつか示します。

- StorageGRID システムのインストール、拡張、リカバリを最近行ったかどうか
- システムは最近アップグレードされましたか？ホットフィックスが適用されましたか？
- ハードウェアの修理や交換を最近行ったかどうか
- ILM ポリシーは更新されているか。
- 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に変化はありますか。
- ロードバランスを変更したか、管理ノードまたはゲートウェイノードのハイアベイラビリティグループを追加または削除したか。

- 開始されたタスクのうち、完了までに時間がかかるものはありますか？たとえば、次のようなもの
  - 障害が発生したストレージノードのリカバリ
  - ストレージノードの運用停止
- テナントの追加や LDAP 設定の変更など、ユーザ認証に変更がないかどうか
- データ移行を実行中かどうか
- プラットフォームサービスが最近有効化または変更されましたか？
- 最近、コンプライアンスを有効にしましたか？
- クラウドストレージプールは追加または削除されていますか？
- ストレージの圧縮や暗号化に変更がないかどうか
- ネットワークインフラに変更はありますか。たとえば、VLAN、ルータ、DNS などです。
- NTP ソースに変更がないかどうか
- グリッド、管理、クライアントの各ネットワークインターフェイスに変更がないかどうか
- アーカイブノードの設定に変更がないかどうか
- StorageGRID システムや環境にその他の変更がないかどうか

#### ベースラインを設定する

さまざまな運用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設定できます。将来的には、現在の値をこれらのベースラインと比較して、異常な値を検出して解決することができます。

プロパティ ( Property )	価値	取得方法
ストレージの平均消費量	1日あたりの GB 消費量 1日あたりの消費率	Grid Manager 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。  Storage Used - Object Data チャートで、この線がかなり安定している期間を探します。グラフにカーソルを合わせて、各日のストレージ消費量を見積もります  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。
メタデータの平均消費量	1日あたりの GB 消費量 1日あたりの消費率	Grid Manager 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。  Storage Used - Object Metadata チャートで、この線がかなり安定している期間を探します。グラフにカーソルを合わせて、各日のメタデータストレージ消費量を見積もります  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 ( Property )	価値	取得方法
S3 / Swift 処理のレート	処理数 / 秒	Grid Managerダッシュボードで、[パフォーマンス]>* S3処理]または[パフォーマンス]> Swift処理*を選択します。  特定のサイトまたはノードの取り込み速度と読み出し速度、および数を表示するには、* nodes * > * site または Storage Node* > * Objects * を選択します。S3またはSwiftの[Ingest and Retrieve]グラフにカーソルを合わせます。
失敗した S3 / Swift 処理	処理	サポート * > * ツール * > * グリッドトポロジ * を選択します。API Operations セクションの Overview タブで、S3 Operations - Failed または Swift Operations - Failed の値を確認します。
ILM 評価の速度	オブジェクト数 / 秒	ノードページで、* GRID_NETWORK* > * ILM * を選択します。  ILM キューグラフで、この線がかなり安定している期間を探します。グラフにカーソルを合わせて、システムの*評価レート*のベースライン値を推定します。
ILM のスキャン速度	オブジェクト数 / 秒	ノード * > * GRID_NETWORK* > * ILM * を選択します。  ILM キューグラフで、この線がかなり安定している期間を探します。グラフにカーソルを合わせて、システムの*スキャン速度*のベースライン値を推定します。
クライアント処理からキューに登録されたオブジェクト	オブジェクト数 / 秒	ノード * > * GRID_NETWORK* > * ILM * を選択します。  ILM キューグラフで、この線がかなり安定している期間を探します。グラフにカーソルを合わせて、システムの* Objects queued (クライアント処理からの ) *のベースライン値を推定します。
クエリの平均レイテンシ	表示されます	ノード * > * _ストレージノード_ * > * オブジェクト * を選択します。クエリテーブルで、平均レイテンシの値を確認します。

## データを分析する

収集した情報を使用して、問題の原因 と潜在的な解決策を特定します。

分析方法は問題の内容によって異なりますが、一般的には次の手順に従ってください。

- アラームを使用して、障害が発生したポイントやボトルネックを特定します。
- アラーム履歴とチャートを使用して、問題の履歴を再構築します。
- チャートを使用して異常を特定し、問題の状況を通常の動作と比較します。

## エスカレーション情報のチェックリスト

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、次の表に記載された問題解決に必要な情報を収集してください。

✓	項目	注：
	問題点	<p>問題の症状は何ですか？問題はいつ発生しましたか？一貫して、または断続的に発生しますか？断続的に発生した場合、何回起きましたか？</p> <p><a href="#">問題を定義します</a></p>
	影響の評価	<p>問題の重大度はどの程度ですか。クライアントアプリケーションにはどのような影響がありますか？</p> <ul style="list-style-type: none"> <li>• クライアントは以前に正常に接続されていますか？</li> <li>• クライアントはデータの取り込み、読み出し、削除を実行できますか。</li> </ul>
	StorageGRID システム ID	[* maintenance * (メンテナンス *) ] > [* System * (システム *) ] > [* License * (ライセンス *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。]
	ソフトウェアのバージョン	グリッドマネージャの上部から、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。
	カスタマイズ	<p>StorageGRID システムの構成をまとめます。たとえば、次のように指定します。</p> <ul style="list-style-type: none"> <li>• グリッドでストレージ圧縮、ストレージ暗号化、コンプライアンスを使用していますか？</li> <li>• ILMによってレプリケートオブジェクトまたはイレイジャーコーディングオブジェクトが作成されるか、ILMによってサイトの冗長性が確保されるか、ILMルールでBalanced、Strict、Dual Commitの取り込み動作が使用されているか。</li> </ul>

✓	項目	注：
	ログファイルとシステムデータ	<p>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。[* support * &gt; * Tools * &gt; * Logs * ]を選択します。</p> <p>ログは、グリッド全体または選択したノードについて収集できます。</p> <p>選択したノードのログのみを収集する場合は、ADC サービスがあるストレージノードを1つ以上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ADC サービスが含まれています）。</p> <p><a href="#">"ログファイルとシステムデータを収集"</a></p>
	ベースライン情報	<p>取り込み処理、読み出し処理、およびストレージ消費量に関するベースライン情報を収集します。</p> <p><a href="#">ベースラインを設定する</a></p>
	最近の変更のタイムライン	<p>システムや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</p> <p><a href="#">最近の変更のタイムラインを作成します</a></p>
	問題を診断するための取り組みの歴史	<p>問題の診断またはトラブルシューティングの手順を自分で実行した場合は、実行した手順と結果を記録しておいてください。</p>

## オブジェクトやストレージの問題をトラブルシューティングする

オブジェクトデータの場所を確認する

問題によっては、実行することもできます ["オブジェクトデータの格納先を確認"](#)。たとえば、ILM ポリシーが想定どおりに機能し、オブジェクトデータが意図した場所に格納されていることを確認できます。

作業を開始する前に

- 次のいずれかのオブジェクト ID が必要です。
  - **UUID** : オブジェクトの Universally Unique Identifier です。UUID はすべて大文字で入力します。
  - **\* CBID \*** : StorageGRID 内のオブジェクトの一意的識別子。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ます。
  - **\* S3バケットとオブジェクトキー\*** : オブジェクトがから取り込まれたとき ["S3インターフェイス"](#) 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格納および識別します。
  - **\* Swiftコンテナとオブジェクト名\*** : を使用してオブジェクトが取り込まれたとき ["Swiftインターフェイス"](#) の場合、クライアントアプリケーションはコンテナとオブジェクト名の組み合わせを使用してオ

プロジェクトを格納および識別します。

#### 手順

1. ILM \* > \* Object metadata lookup \* を選択します。
2. [\* 識別子 \* (\* Identifier \*) ] 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)。



Object Metadata Lookup

Enter the identifier for any object stored in the grid to view its metadata.

Identifier: source/testobject

Version ID (optional): MEJGMkMyQzgtNEY5OC0xMUU3LTkzMEYtRDkyNTAwQkY5N0Mx

Look Up

4. 「\* 検索 \*」を選択します。

。「[オブジェクトメタデータの検索結果](#)」表示されます。このページには、次の種類の情報が表示されます。

- システムメタデータ (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、コンテナの名前、テナントアカウントの名前または ID、オブジェクトの論理サイズ、オブジェクトの作成日時、オブジェクトの最終変更日時など)。
- オブジェクトに関連付けられているカスタムユーザメタデータのキーと値のペア。
- S3 オブジェクトの場合、オブジェクトに関連付けられているオブジェクトタグのキーと値のペア。
- レプリケートオブジェクトコピーの場合、各コピーの現在の格納場所。
- イレイジャーコーディングオブジェクトコピーの場合、各フラグメントの現在の格納場所。
- クラウドストレージ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とマルチパートオブジェクトの場合、セグメント ID 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は、最初の 100 個のセグメントだけが表示されます。
- 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。この未加工のメタデータには、リリース間で維持されるとはかぎらない内部のシステムメタデータが含まれます。

次の例では、2つのレプリケートコピーとして格納された S3 テストオブジェクトのオブジェクトメタデータの検索結果が表示されています。

## System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

## Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H\$ TFbnQQ} CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H\$ TFboW28 CXG%

## Raw Metadata

```
{
  "TYPE": "CTNT",
  "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
  "NAME": "testobject",
  "CBID": "0x88230E7EC7C10416",
  "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
  "PPTH": "source",
  "META": {
    "BASE": {
      "PAWS": "2",

```

オブジェクトストア（ストレージボリューム）の障害

ストレージノードの基盤となるストレージは、複数の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の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

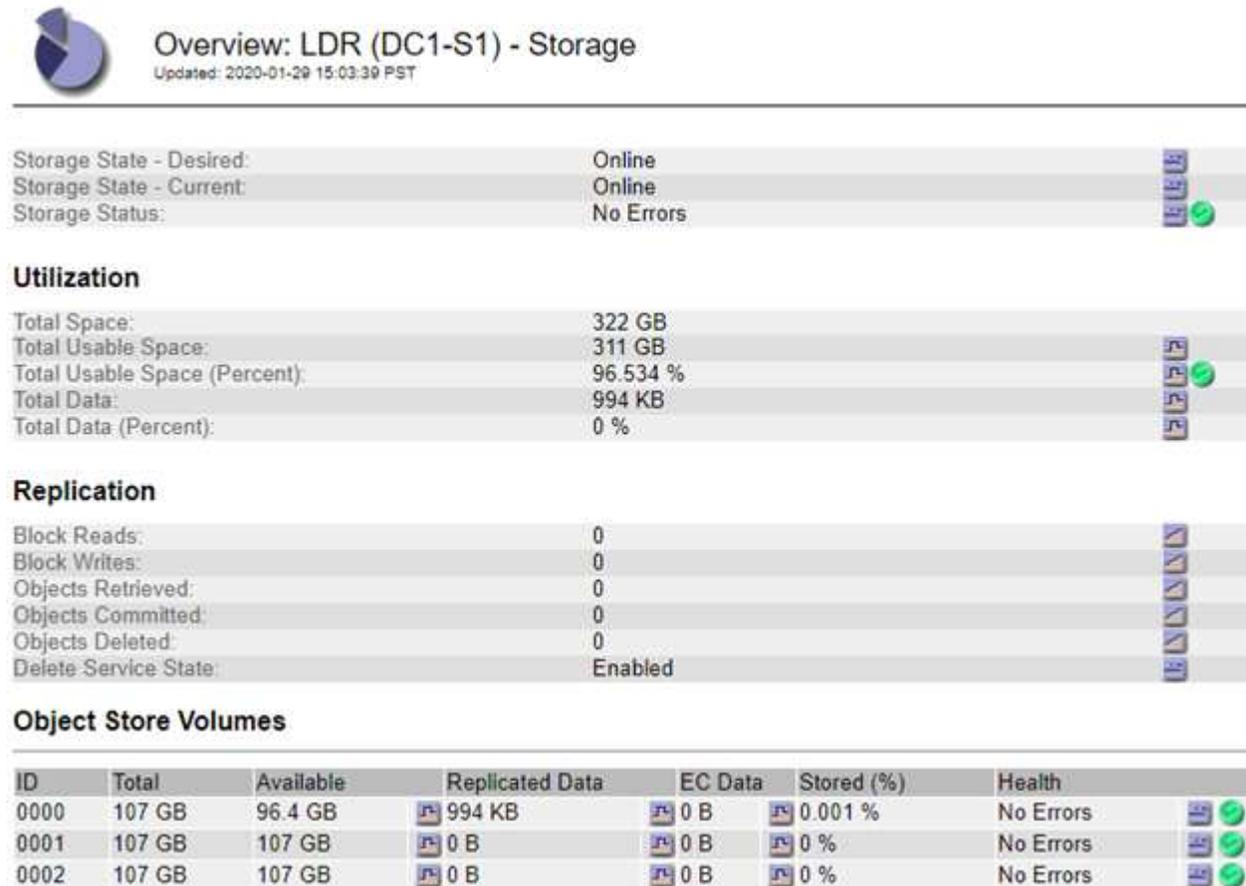
Mount point  	Device  	Status  	Size  	Available  	Write cache status  
/	croot	Online	21.00 GB	14.73 GB 	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB 	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB 	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB 	Enabled
/var/local/rangedb/2	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

もっと見るために "各ストレージノードの詳細"、次の手順を実行します。

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\* ] > [\* Overview\* ] > [\* Main\* ] を選択します。



**Overview: LDR (DC1-S1) - Storage**  
Updated: 2020-01-29 15:03:39 PST

Storage State - Desired: Online  
Storage State - Current: Online  
Storage Status: No Errors

**Utilization**

Total Space:	322 GB
Total Usable Space:	311 GB
Total Usable Space (Percent):	96.534 %
Total Data:	994 KB
Total Data (Percent):	0 %

**Replication**

Block Reads:	0
Block Writes:	0
Objects Retrieved:	0
Objects Committed:	0
Objects Deleted:	0
Delete Service State:	Enabled

**Object Store Volumes**

ID	Total	Available	Replicated Data	EC Data	Stored (%)	Health
0000	107 GB	96.4 GB	994 KB	0 B	0.001 %	No Errors
0001	107 GB	107 GB	0 B	0 B	0 %	No Errors
0002	107 GB	107 GB	0 B	0 B	0 %	No Errors

ストレージボリュームの障害は、障害の性質に応じて、ストレージのステータスまたはオブジェクトストアの健全性のアラームに反映されます。ストレージボリュームに障害が発生した場合は、ストレージノードのすべての機能を復旧するために、障害が発生したストレージボリュームをできるだけ早く修復する必要があります。必要に応じて、\* Configuration \* タブとに移動できます "ストレージノードを読み取り専用状態にします" これにより、サーバの完全なリカバリの準備中に、StorageGRID システムがデータの取得に使用できるようになります。

オブジェクトの整合性を検証

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、オブジェクトの破損や欠落の有無を確認します。

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の存在チェック（旧称フォアグラウンド検証）の2つがあります。データの整合性を確保するために連携して機能します。バックグラウンド検証は、オブジェクトデータの正確性を継続的にチェックするために自動的に実行されます。オブジェクトの存在チェックは、オブジェクトの有無（正確性ではなく）をより迅速に確認するためにユーザによってトリガーされることがあります。

バックグラウンド検証とは何ですか？

バックグラウンド検証プロセスは、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どうかを自動的かつ継続的にチェックし、問題が見つかった場合は自動的に修復を試みます。

バックグラウンド検証は、レプリケートオブジェクトとイレイジャーコーディングオブジェクトの整合性を次の方法でチェックします。

- **\* レプリケートオブジェクト \***：バックグラウンド検証プロセスで破損したレプリケートオブジェクトが検出された場合、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他の場所に隔離されます。その後、アクティブなILMポリシーに従って新しい破損していな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ていたストレージノードに配置されるとはかぎりません。



破損したオブジェクトデータは、引き続きアクセスできるように、システムから削除されるのではなく隔離されます。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。

- **\* イレイジャーコーディングオブジェクト \***：バックグラウンド検証プロセスでイレイジャーコーディングオブジェクトのフラグメントの破損が検出された場合、StorageGRID は自動的に残りのデータ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に欠落フラグメントの再構築を試みます。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。読み出しに成功すると、ILM 評価が実行されて、イレイジャーコーディングオブジェクトの置き換え用の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チェックされます。アーカイブノード上または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。バックグラウンド検証を実行するには、4 日以上経過したオブジェクトが必要です。

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定された間隔で継続的に実行されます。バックグラウンド検証を停止することはできません。ただし、問題があると疑われる場合は、バックグラウンド検証の回数を増やして、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。

バックグラウンド検証に関連するアラートとアラーム（レガシー）

破損したオブジェクトが検出され、自動的に修正できない場合（破損によってオブジェクトを特定できないため）は、\* Unidentified corrupt object detected \*アラートがトリガーされます。

別のコピーが見つからないため、バックグラウンド検証で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、\* Objects lost \*アラートがトリガーされます。

バックグラウンド検証レートを変更します

データ整合性に関する懸念事項がある場合は、バックグラウンド検証によってストレージノード上のレプリケートオブジェクトデータをチェックする速度を変更できます。

作業を開始する前に

- を使用して Grid Manager にサインインする必要があります ["サポートされている Web ブラウザ"](#)。
- これで完了です ["特定のアクセス権限"](#)。

このタスクについて

ストレージノードに対するバックグラウンド検証の検証レートを変更できます。

- Adaptive：デフォルト設定です。最大 4MB/ 秒または 10 オブジェクト / 秒（先に超過した方）で検証するようにタスクが設計されます。
- High：ストレージ検証は高速で実行され、通常のシステムアクティビティの処理速度が低下する可能性があります。

この設定は、ハードウェアまたはソフトウェアの障害により、オブジェクトデータが破損している可能性がある場合にのみ使用します。優先度の高い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. 「\*\_ストレージノード\_\* > \* LDR \* > \* Verification \*」を選択します。
3. \* Configuration \* > \* Main \* を選択します。
4. 「\*\_LDR\_\* > \* Verification \* > \* Configuration \* > \* Main \*」に移動します。
5. バックグラウンド検証で、\* 検証レート \* > \* 高 \* または \* 検証レート \* > \* 適応 \* を選択します。

The screenshot shows the 'Configuration' tab for 'LDR (Storage Node) - Verification'. The 'Verification Rate' dropdown menu is highlighted with a green box and is currently set to 'Adaptive'. Other settings include checkboxes for 'Reset Missing Objects Count', 'Reset Corrupt Objects Count', and 'Delete Quarantined Objects'. An 'Apply Changes' button with a blue arrow icon is located at the bottom right of the configuration area.



Verification Rate を High に設定すると、Notice レベルで VPRI（Verification Rate）レガシーアラームがトリガーされます。

6. [変更の適用 \*] をクリックします。
7. レプリケート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. ノード \* > \* 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」および「破損したオブジェクトの特定なし」の値を監視します。

バックグラウンド検証で破損したレプリケートオブジェクトデータが見つかった場合は、「破損した

オブジェクト \*」指標が増分され、StorageGRID は次のようにデータからオブジェクト ID の抽出を試みます。

- オブジェクト ID を抽出できる場合は、StorageGRID によってオブジェクトデータの新しいコピーが自動的に作成されます。新しいコピーは、アクティブなILMポリシーを満たしていれば、StorageGRIDシステム内のどこにでも作成できます。
- オブジェクトIDが破損しているために抽出できない場合は、\* Corrupt Objects Unidentified 指標が増分され、Unidentified corrupt object detected \*アラートがトリガーされます。

c. 破損したレプリケート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ルート原因を確認します。

8. イレイジャーコーディングオブジェクトのバックグラウンド検証の結果を監視します。

バックグラウンド検証でイレイジャーコーディングオブジェクトデータの破損したフラグメントが検出された場合は、Corrupt Fragments Detected 属性がその分だけ増分します。StorageGRID は、破損したフラグメントを同じストレージノード上に再構築して、この状況からリカバリします。

- a. サポート \* > ツール \* > グリッドトポロジ \* を選択します。
- b. 「\*\_ストレージノード\_\* > LDR \* > イレイジャーコーディング \*」を選択します。
- c. Verification Results テーブルで、Corrupt Fragments Detected (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リストアされたら、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. 「\*\_ストレージノード\_\* > LDR \* > Verification \* > Configuration \*」を選択します。
- c. 「破損オブジェクト数をリセット」を選択します。
- d. [変更の適用 \*] 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している場合は、それらのオブジェクトを削除できます。



Objects Lost \* アラートまたは LOST (Lost Objects) レガシー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して、基になる問題のデバッグやデータリカバリを試みることができます。

- a. サポート \* > ツール \* > グリッドトポロジ \* を選択します。
- b. 「\*\_ストレージノード\_\* > LDR \* > Verification \* > Configuration \*」を選択します。
- c. [\* 隔離オブジェクトの削除 \*] を選択します。
- d. 「\* 変更を適用する \*」を選択します。

オブジェクトの存在チェックとは何ですか？

オブジェクトの存在チェックでは、オブジェクトとイレイジャーコーディングフラグメントの想定されるレプリケートコピーがすべてストレージノードに存在するかどうかを検証されます。オブジェクトの存在チェックでは、オブジェクトデータ自体は検証されません（バックグラウンド検証で検証されます）。代わりに、ストレージデバイスの整合性を検証する方法が提供されます。特に、最新のハードウェア問題がデータの整合性に影響を与える可能性がある場合に役立ちます。

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。

オブジェクトの存在チェックでは、StorageGRID に格納されているすべてのオブジェクトのメタデータが読み取られ、レプリケートされたオブジェクトコピーとイレイジャーコーディングされたオブジェクトフラグメントの両方の存在が検証されます。不足しているデータは次のように処理されます。

- **\* Replicated Copies \*** : レプリケートオブジェクトデータのコピーが見つからない場合、StorageGRID はシステム内の別の場所に格納されているコピーからコピーを自動的に置き換えます。ストレージノードは既存のコピーに対して ILM を評価します。これにより、別のコピーがないために、このオブジェクトに関して現在の ILM ポリシーは満たされていないという結果となります。システムのアクティブな ILM ポリシーに従って新しいコピーが生成されて配置されます。この新しいコピーは、欠落したコピーが格納されていた場所に配置されるとはかぎりません。
- **\* イレイジャーコーディングされたフラグメント \*** : イレイジャーコーディング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 は自動的に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に欠落フラグメントの再構築を試みます。失われたフラグメントが多すぎるために欠落フラグメントを再構築できない場合、ILM はオブジェクトの別のコピーを探し、このコピーを使用して新しいイレイジャーコーディングフラグメントを生成します。

オブジェクトの存在チェックを実行します

オブジェクト存在チェックジョブは、一度に 1 つずつ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。また、ジョブの整合性も選択します。

作業を開始する前に

- を使用して Grid Manager にサインインします **"サポートされている Web ブラウザ"**。
- を使用することができます **"Maintenance権限またはRoot Access権限"**。
- チェック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ておきます。ノードの表を表示するには、**\* nodes \*** を選択します。チェック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ないようにします。
- チェックするノードで次の手順が **\* 実行されていないことを確認** します。
  - Grid の拡張：ストレージノードを追加
  - ストレージノードの運用停止
  - 障害ストレージボリュームのリカバリ
  - 障害システムドライブがあるストレージノードのリカバリ
  - EC のリバランシング
  - アプライアンスノードのクローン

これらの手順の実行中は、オブジェクトの存在チェックで有用な情報が得られません。

このタスクについて

オブジェクトの存在確認ジョブは、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、選択した整合性によって、完了するまでに数日から数週間かかることがあります。一度に実行できるジョブは 1 つだけですが、同時に複数のストレージノードとボリュームを選択することもできます。

手順

1. [**\* maintenance \*** (メンテナンス \*) ] > [**\* Tasks \*** (タスク \*) ] > [**\* Object existence check \*** (オブジェクトの存在

2. 「\* ジョブの作成 \*」を選択します。Create an object existence check job ウィザードが表示されます。
3. 検証するボリュームが含まれているノードを選択します。オンラインノードをすべて選択するには、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は選択できません。

4. 「\* Continue \*」を選択します。
5. リスト内のノードごとに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。

選択した各ノードで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選択します。

6. 「\* Continue \*」を選択します。
7. ジョブの整合性を選択します。

整合性によって、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。

- \* strong-site \* : 単一のサイトにおけるメタデータのコピーが2つ
- \* strong-global \* : 各サイトにおけるメタデータのコピーが2つ
- \* all \* (デフォルト) : 各サイトに3つのメタデータのすべてのコピーを格納します。

整合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. 「\* Continue \*」を選択します。
9. 選択内容を確認します。「\* Previous \*」を選択すると、ウィザードの前の手順に進み、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、次のいずれかが実行され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た場合。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。
- ジョブが停止します。Object existence check has ストール \* アラートがトリガーされます。アラートに対して指定された対処方法に従います。
- ジョブが失敗します。\* Object existence check has failed \* というアラートがトリガーされます。アラートに対して指定された対処方法に従います。
- 「Service Unavailable」または「Internal server error」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、[オブジェクトの有無]チェックページから移動して、ジョブの監視を続行することができます。

10. ジョブの実行中に、「\* Active job \*」タブを表示して、検出されたオブジェクトコピーが欠落しているこ

とを確認します。

この値は、レプリケートオブジェクトとイレイジャーコーディングオブジェクトの欠落コピーのうち、1つ以上のフラグメントが欠落しているものの合計数を表します。

検出された欠落オブジェクトコピーの数が 100 を超える場合は、ストレージノードのストレージを含む問題が存在する可能性があります。

Object existence check

Perform an object existence check if you suspect some storage volumes have been damaged or are corrupt and you want to verify that objects still exist on these volumes.

If you have questions about running object existence check, contact technical support.

Active job | Job history

Status: Accepted | Consistency control: All | Job ID: 2334602652907829302 | Start time: 2021-11-10 14:43:02 MST | Missing object copies detected: 0 | Elapsed time: - | Estimated time to completion: - | Progress: 0%

Pause | Cancel

Volumes | Details

Selected node	Selected storage volumes	Site
DC1-S1	0, 1, 2	Data Center 1
DC1-S2	0, 1, 2	Data Center 1
DC1-S3	0, 1, 2	Data Center 1

11. ジョブが完了したら、さらに必要なアクションを実行します。

- 欠落オブジェクトコピーが 0 であることが検出された場合、問題は見つかりませんでした。対処は不要です。
- 欠落オブジェクトコピーがゼロより大きいことが検出され、「Objects lost \*」アラートがトリガーされていない場合は、欠落しているすべてのコピーがシステムによって修復されました。ハードウェアの問題が修正され、オブジェクトコピーが今後破損しないようになっていることを確認する。
- 欠落オブジェクトコピーがゼロより大きいことが検出され、「\* Objects lost \*」アラートがトリガーされた場合は、データの整合性に影響す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と、損失オブジェクトコピーを調査できます。grep LLST audit\_file\_name。

この手順はのものと似ています ["損失オブジェクトを調査しています"](#) (ただし、オブジェクトコピーの場合は検索します) LLST ではなく OLST。

12. ジョブでstrong-site整合性またはstrong-global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、同じボリュームに対してジョブを再実行します。

ジョブに含まれるノードとボリュームでメタデータの整合性を維持するための時間がかかっていた場合、誤って報告された欠落オブジェクトコピーまたは原因を見逃していたオブジェクトコピーをジョブで再実行することで解決できます。 StorageGRID

- a. [\* maintenance \* (メンテナンス \*) ] > [\* Object existence check \* (オブジェクトの存在確認 \*) ] > [\* Job history \* (ジョブ
- b. 再実行する準備ができていないジョブを特定します。
  - i. 3週間以上前に実行されたジョブを特定するには、「\* End time \*」列を参照してください。
  - ii. これらのジョブについては、コンシステンシコントロール列をスキャンして、強サイトまたは強グローバルを確認します。
- 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。

Object existence check

Perform an object existence check if you suspect some storage volumes have been damaged or are corrupt and you want to verify that objects still exist on these volumes.

If you have questions about running object existence check, contact technical support.

Active job | Job history

Delete | Rerun | Search by Job ID/ node name/ consistency control/ start time

Displaying 4 results

<input type="checkbox"/>	Job ID	Status	Nodes (volumes)	Missing object copies detected	Consistency control	Start time	End time
<input checked="" type="checkbox"/>	2334602652907829302	Completed	DC1-S1 (3 volumes) DC1-S2 (3 volumes) DC1-S3 (3 volumes) and 7 more	0	All	2021-11-10 14:43:02 MST	2021-11-10 14:43:06 MST (3 weeks ago)
<input type="checkbox"/>	11725651898848823235 (Rerun job)	Completed	DC1-S2 (2 volumes) DC1-S3 (2 volumes) DC1-S4 (2 volumes) and 4 more	0	Strong-site	2021-11-10 14:42:10 MST	2021-11-10 14:42:11 MST (17 minutes ago)

- 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、および整合性を確認します。
- e. ジョブを再実行する準備ができたなら、\*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の一貫性のある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が一覧表示されます。

完了後

データの整合性についてまだ懸念がある場合は、\* support \* > \* Tools \* > \* Grid Topology \* > \* site \_ \* > \* \_ Storage Node \* > \* LDR \* > \* Verification \* > \* Configuration \* > \* Main \* に移動し、バックグラウンド検証レー

トを増やします。バックグラウンド検証は、格納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検出して修復することで、データ損失のリスクが軽減されます。

### S3 PUT Object size too largeアラートのトラブルシューティングを行う

S3 PUT Object size too largeアラートは、S3サイズの上限である5GiBを超えるマルチパートでないPutObject処理をテナントが試行するとトリガーされます。

作業を開始する前に

- を使用して Grid Manager にサインインします "サポートされている Web ブラウザ"。
- これで完了です "特定のアクセス権限"。

5GiBを超えるオブジェクトを使用しているテナントを確認して、通知できるようにします。

手順

1. >[監視]>[監査とsyslogサーバ]\*に移動します。
2. クライアントからの書き込みがNormalの場合は、監査ログにアクセスします。
  - a. 入力するコマンド `ssh admin@primary_Admin_Node_IP`
  - b. に記載されているパスワードを入力します Passwords.txt ファイル。
  - c. 次のコマンドを入力してrootに切り替えます。 `su -`
  - d. に記載されているパスワードを入力します Passwords.txt ファイル。  
  
rootとしてログインすると、プロンプトがから変わります \$ 終了： #。
  - e. 監査ログが格納されているディレクトリに移動します。

監査ログディレクトリおよび該当するノードは、監査デスティネーションの設定によって異なります。

オプション	宛先
ローカルノード (デフォルト)	<code>/var/local/log/localaudit.log</code>
管理ノード/ローカルノード	<ul style="list-style-type: none"><li>• 管理ノード (プライマリおよび非プライマリ) : <code>/var/local/audit/export/audit.log</code></li><li>• すべてのノード : <code>/var/local/log/localaudit.log</code> 通常、このモードではファイルが空か欠落しています。</li></ul>
外部 syslog サーバ	<code>/var/local/log/localaudit.log</code>

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、を参照して "監査情報の送信先を選択します"ください。

f. 5GiB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. 結果に表示された各監査メッセージについて、を参照してください S3AI フィールドに入力してテナントアカウントIDを確認します。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ていたIPアドレスを確認します。

コード	説明
saip	送信元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):80431733
3][SAIP(IPAD):"10.96.99.127"][S3AI(CSTR):"93390849266154004343"][SACC(CS
TR):"bhavna"][S3AK(CSTR):"06OX85M40Q90Y280B7YT"][SUSR(CSTR):"urn:sgws:id
entity::93390849266154004343:root"][SBAI(CSTR):"93390849266154004343"][S
BAC(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):12220
829][AMID(FC32):S3RQ][ATID(UI64):4333283179807659119]]
```

3. [Client Writes]が[Normal]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特定します。

a. \* support > Tools > Logs \*に移動します。アラートで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. ファイルを展開し、に進みます `bycast.log` :

```
/GID<grid_id>_<time_stamp>/<site_node>/<time_stamp>/grid/bycast.log
```

c. ログでを検索します `method=PUT` およびでクライアントを特定します `clientIP` フィールド。

▪ `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. テナントに、PutObjectの最大サイズが5GiBであり、5GiBを超えるオブジェクトにマルチパートアップロードを使用するように伝えます。
5. アプリケーションが変更されている場合は、警告を1週間無視します。

## 失われたオブジェクトデータと欠落しているオブジェクトデータのトラブルシューティング

### オブジェクトデータの損失と欠落のトラブルシューティング：概要

オブジェクトはさまざまな理由で読み出されます。たとえば、クライアントアプリケーションからの読み取り要求、レプリケートされたオブジェクトデータのバックグラウンド検証、ILM ルールによる再評価、ストレージノードのリカバリ時のオブジェクトデータのリストアなどの目的で行われます。

StorageGRID システムは、オブジェクトのメタデータに記載された場所の情報を使用して、オブジェクトの読み出し元の場所を特定します。想定される場所でオブジェクトのコピーが見つからない場合、システムは ILM ポリシーにオブジェクトのコピーを複数保持するルールが含まれているものとして、システム内の他の場所から別のコピーを読み出そうとします。

この読み出しに成功すると、欠落しているオブジェクトのコピーが StorageGRID システムによって置き換えられます。それ以外の場合は、\* Objects lost \* アラートが次のようにトリガーされます。

- レプリケートコピーについては、別のコピーを読み出せない場合、オブジェクトが失われたとみなされてアラートがトリガーされます。
- イレイジャーコーディングコピーの場合、想定される場所からコピーを読み出せない場合は、別の場所からの読み出しが試行される前に、Corrupt Copies Detected (ECOR) 属性の値が1つ増分されます。他のコピーが見つからない場合は、アラートがトリガーされます。

すべての \* Objects Lost \* アラートをすぐに調査して損失のルート原因を特定し、オフラインなどの何らかの理由で現在使用できないストレージノードやアーカイブノードにオブジェクトが残っていないかどうかを確認する必要があります。を参照してください ["損失オブジェクトを調査する"](#)。

コピーがないオブジェクトデータが失われた場合、リカバリ解決策はありません。ただし、損失オブジェクトカウンタをリセットして、既知の損失オブジェクトが新しい損失オブジェクトをマスキングしないようにする必要があります。を参照してください ["損失オブジェクトと欠落オブジェクトのカウンタをリセットします"](#)。

### 損失オブジェクトを調査する

Objects lost \* 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。

作業を開始する前に

- を使用して Grid Manager にサインインする必要があります "サポートされている Web ブラウザ"。
- これで完了です "特定のアクセス権限"。
- を用意しておく必要があります Passwords.txt ファイル。

このタスクについて

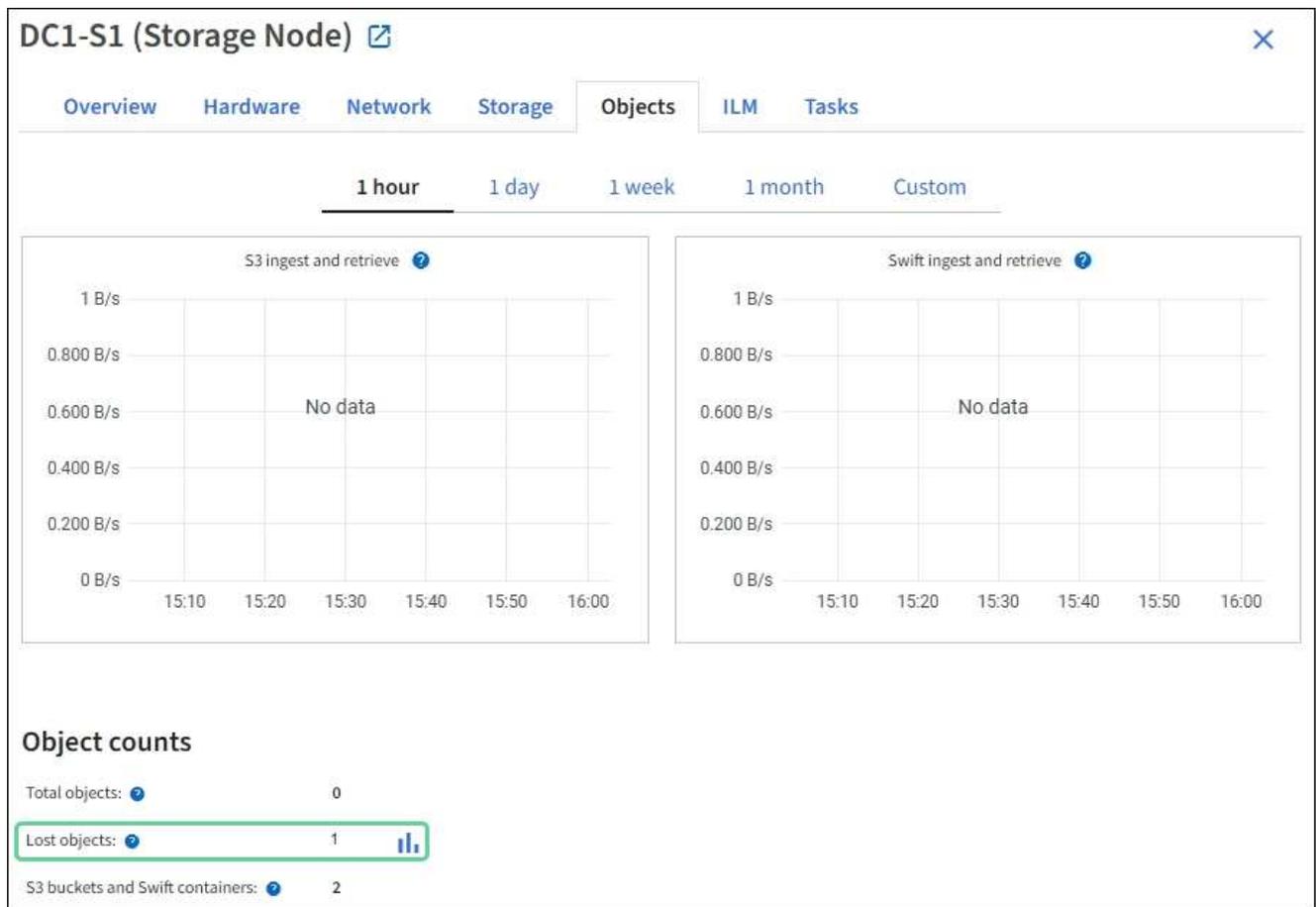
- Objects lost \* アラートは、StorageGRID がグリッド内にオブジェクトのコピーがないと判断したことを示します。データが完全に失われた可能性があります。

損失オブジェクトのアラートをただちに調査してください。これ以上のデータ損失を防ぐための対処が必要になる場合があります。迅速に対処すれば、損失オブジェクトをリストアできる場合があります。

手順

1. [\* nodes (ノード) ] を選択します
2. [**Storage Node**>\* Objects\*] を選択します。
3. オブジェクト数の表に表示された損失オブジェクトの数を確認します。

この数値は、StorageGRID システム全体で欠落していることがグリッドノードで検出されたオブジェクトの合計数を示します。この値は、LDR サービスと DDS サービスに含まれるデータストアコンポーネントの損失オブジェクトカウンタの合計です。



4. 管理ノードから、"監査ログにアクセスします" Objects Lost \*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) を確認するには、次の手順を実行します。

- 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. に記載されているパスワードを入力します `Passwords.txt` ファイル。
  - iii. 次のコマンドを入力してrootに切り替えます。 `su -`
  - iv. に記載されているパスワードを入力します `Passwords.txt` ファイル。  
rootとしてログインすると、プロンプトがから変わります \$ 終了: #。
- b. 監査ログが格納されているディレクトリに移動します。

監査ログディレクトリおよび該当するノードは、監査デスティネーションの設定によって異なります。

オプション	宛先
ローカルノード (デフォルト)	<code>/var/local/log/localaudit.log</code>
管理ノード/ローカルノード	<ul style="list-style-type: none"> <li>• 管理ノード (プライマリおよび非プライマリ) : <code>/var/local/audit/export/audit.log</code></li> <li>• すべてのノード: <code>`var/local/log/localaudit.log`</code> 通常、このモードではファイルが空か欠落しています。</li> </ul>
外部 syslog サーバ	<code>/var/local/log/localaudit.log</code>

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、を参照して ["監査情報の送信先を選択します"](#) ください。

- c. `grep` を使用して Object Lost (OLST) 監査メッセージを抽出します。入力するコマンド `grep OLST audit_file_name`
- d. メッセージに含まれている UUID の値をメモします。

```
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. を使用します `ObjectByUUID` コマンドを使用して識別子 (UUID) でオブジェクトを検索し、データにリスクがあるかどうかを確認できます。
  - a. SSHを使用して任意のストレージノードにログインします。次に「`telnet 0 1402`」と入力してLDRコ

ンソールにアクセスします。

b. 入力するコマンド `/proc/OBRP/ObjectByUUID UUID_value`

この最初の例では、を持つオブジェクトです UUID 926026C4-00A4-449B-AC72-BCCA72DD1311  
には2つの場所が表示されて

```
ade 12448208: /proc/OBRP > ObjectByUUID 926026C4-00A4-449B-AC72-
BCCA72DD1311

{
  "TYPE(Object Type)": "Data object",
  "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
  "NAME": "cats",
  "CBID": "0x38186FE53E3C49A5",
  "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-
ACBB00BB82DD",
  "PPTH(Parent path)": "source",
  "META": {
    "BASE(Protocol metadata)": {
      "PAWS(S3 protocol version)": "2",
      "ACCT(S3 account ID)": "44084621669730638018",
      "*ctp(HTTP content MIME type)": "binary/octet-stream"
    },
    "BYCB(System metadata)": {
      "CSIZ(Plaintext object size)": "5242880",
      "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
      "BSIZ(Content block size)": "5252084",
      "CVER(Content block version)": "196612",
      "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
      "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
      "ITME": "1581534970983000"
    },
    "CMSM": {
      "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
    },
    "AWS3": {
      "LOCC": "us-east-1"
    }
  },
  "CLCO(Locations)": \[
  \{
    "Location Type": "CLDI(Location online)",
```

```

        "NOID\ (Node ID\)": "12448208",
        "VOLI\ (Volume ID\)": "3222345473",
        "Object File Path":
"/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila\#3udu",
        "LTIM\ (Location timestamp\)": "2020-02-
12T19:36:17.880569"
    \},
    \{
        "Location Type": "CLDI\ (Location online\)",
        "NOID\ (Node ID\)": "12288733",
        "VOLI\ (Volume ID\)": "3222345984",
        "Object File Path":
"/var/local/rangedb/0/p/19/11/00rH0%DkRt78Rrb\#3s;L",
        "LTIM\ (Location timestamp\)": "2020-02-
12T19:36:17.934425"
    }
]
}

```

2番目の例では、を指定したオブジェクトです UUID 926026C4-00A4-449B-AC72-BCCA72DD1311 場所が表示されていません。

```

ade 12448208: / > /proc/OBRP/ObjectByUUID 926026C4-00A4-449B-AC72-
BCCA72DD1311

{
  "TYPE(Object Type)": "Data object",
  "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
  "NAME": "cats",
  "CBID": "0x38186FE53E3C49A5",
  "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-ACBB00BB82DD",
  "PPTH(Parent path)": "source",
  "META": {
    "BASE(Protocol metadata)": {
      "PAWS(S3 protocol version)": "2",
      "ACCT(S3 account ID)": "44084621669730638018",
      "*ctp(HTTP content MIME type)": "binary/octet-stream"
    },
    "BYCB(System metadata)": {
      "CSIZ(Plaintext object size)": "5242880",
      "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
      "BSIZ(Content block size)": "5252084",
      "CVER(Content block version)": "196612",
      "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
      "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
      "ITME": "1581534970983000"
    },
    "CMSM": {
      "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
    },
    "AWS3": {
      "LOCC": "us-east-1"
    }
  }
}

```

a. /proc/OBRP/ObjectByUUID の出力を確認し、適切な処理を実行します。

メタデータ	まとめ
オブジェクトが見つかりません ("ERROR" : "")	<p>オブジェクトが見つからない場合は「ERROR」：というメッセージが返されます。</p> <p>オブジェクトが見つからない場合は、* Objects lost * の数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、意図的に削除されたオブジェクトであることを示しています。</p>
場所が 0 より大きい	<p>出力に場所が表示されている場合は、* Objects lost * アラートが誤った正の値である可能性があります。</p> <p>オブジェクトが存在することを確認します。出力に表示されたノード 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た場所にあることを確認します。</p> <p>(の手順 <a href="#">"失われた可能性があるオブジェクトの検索"</a> ノード ID を使用して正しいストレージノードを特定する方法について説明します)。</p> <p>オブジェクトが存在する場合は、* Objects lost * の数をリセットしてアラートをクリアできます。</p>
場所 = 0	<p>出力に場所が表示されない場合は、オブジェクトが欠落している可能性があります。試してみてください <a href="#">"オブジェクトを検索してリストアップします"</a> または、テクニカルサポートにお問い合わせください。</p> <p>テクニカルサポートに問い合わせた際に、実行中のストレージリカバリ手順がないかどうかを確認するように求められることがあります。の情報を参照してください <a href="#">"Grid Managerを使用したオブジェクトデータのリストアップ"</a> および <a href="#">"ストレージボリュームへのオブジェクトデータのリストアップ"</a>。</p>

失われた可能性があるオブジェクトを検索してリストアップします

Lost Objects (LOST) アラームと \* Object lost \* アラートをトリガーした (失われた可能性があると特定した) オブジェクトを検索してリストアップできる場合があります。

作業を開始する前に

- で特定した損失オブジェクトのUUIDを確認しておきます ["損失オブジェクトを調査する"](#)。
- を使用することができます Passwords.txt ファイル。

このタスクについて

この手順を使用して、グリッド内の他の場所で損失オブジェクトのレプリケートコピーを検索できます。ほとんどの場合、損失オブジェクトは見つかりません。ただし、迅速に対処すれば、損失レプリケートオブジェクトを検索してリストアップできる場合があります。



この手順の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. 管理ノードの監査ログで、オブジェクトが存在する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. に記載されているパスワードを入力します `Passwords.txt` ファイル。
- iii. 次のコマンドを入力してrootに切り替えます。 `su -`
- iv. に記載されているパスワードを入力します `Passwords.txt` ファイル。  
rootとしてログインすると、プロンプトがから変わります \$ 終了: #。

b. 監査ログが格納されているディレクトリに移動します。

監査ログディレクトリおよび該当するノードは、監査デスティネーションの設定によって異なります。

オプション	宛先
ローカルノード (デフォルト)	<code>/var/local/log/localaudit.log</code>
管理ノード/ローカルノード	<ul style="list-style-type: none"> <li>• 管理ノード (プライマリおよび非プライマリ) : <code>/var/local/audit/export/audit.log</code></li> <li>• すべてのノード: <code>`var/local/log/localaudit.log`</code> 通常、このモードではファイルが空か欠落しています。</li> </ul>
外部 syslog サーバ	<code>/var/local/log/localaudit.log</code>

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、を参照して ["監査情報の送信先を選択します"](#) ください。

c. `grep` を使用してを展開します ["損失の可能性のあるオブジェクトに関連付けられている監査メッセージ"](#) 出力ファイルに送信します。入力するコマンド `grep uuid-valueaudit_file_name >  
output_file_name`

例:

```
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。入力するコマンド `grep LLST output_file_name`

例:

```
Admin: # grep LLST /var/local/tmp/messages_about_lost_objects.txt
```

LLST監査メッセージの例を次に示します。

```
[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
86871083190743409]]
```

e. LLST メッセージで PCLD フィールドと NOID フィールドを検索します。

PCLD の値は、欠落しているレプリケートオブジェクト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のある 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、オブジェクトをリストアできる場合があります。

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探します。Grid Manager で、`* support * > * Tools * > * Grid topology *` 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、[Node Information]テーブルに表示されます。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. 監査メッセージで指定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. に記載されているパスワードを入力します Passwords.txt ファイル。
- iii. 次のコマンドを入力してrootに切り替えます。su -
- iv. に記載されているパスワードを入力します Passwords.txt ファイル。

rootとしてログインすると、プロンプトがから変わります \$ 終了: #。

b. オブジェクトのファイルパスが存在するかどうかを確認します。

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'
```



コマンドでは、オブジェクトファイルパスを常に一重引用符で囲み、特殊文字をエスケープします。

- オブジェクトの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リストア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 にリストアできます。

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 にリストアします。

- 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。入力するコマンド `chown ldr-user:bycast 'file_path_of_object'`
- b. SSHを使用して任意のストレージノードにログインします。次に「telnet 0 1402」と入力してLDRコンソールにアクセスします。
- c. 入力するコマンド `cd /proc/STOR`
- d. 入力するコマンド `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'
```

を発行します `Object\_Found` コマンドは、グリッドにオブジェクトの場所を通知します。また、アクティブなILMポリシーがトリガーされ、各ポリシーの指定に従って追加のコピーが作成されます。



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は、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。オンラインのストレージノードの `/var/local/rangedb` ディレクトリにオブジェクトを配置します。次に、問題を実行します `Object\_Found` コマンドを使用し、オブジェクトへのファイルパスを指定します。

- オブジェクトをリストアできない場合は、を実行します `Object\_Found` コマンドが失敗します。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 に正常にリストアされた場合は、成功を伝えるメッセージが表示されます。例：

```
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 に正常にリストアされた場合は、新しい場所が作成されていることを確認し

ます。

- a. 入力するコマンド `cd /proc/OBRP`
- b. 入力するコマンド `ObjectByUUID UUID_value`

次の例は、UUID 926026C4-00A4-449B-AC72-BCCA72DD1311 のオブジェクトに 2 つの場所があることを示しています。

```
ade 12448208: /proc/OBRP > ObjectByUUID 926026C4-00A4-449B-AC72-
BCCA72DD1311

{
  "TYPE(Object Type)": "Data object",
  "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
  "NAME": "cats",
  "CBID": "0x38186FE53E3C49A5",
  "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-ACBB00BB82DD",
  "PPTH(Parent path)": "source",
  "META": {
    "BASE(Protocol metadata)": {
      "PAWS(S3 protocol version)": "2",
      "ACCT(S3 account ID)": "44084621669730638018",
      "*ctp(HTTP content MIME type)": "binary/octet-stream"
    },
    "BYCB(System metadata)": {
      "CSIZ(Plaintext object size)": "5242880",
      "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
      "BSIZ(Content block size)": "5252084",
      "CVER(Content block version)": "196612",
      "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
      "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
      "ITME": "1581534970983000"
    },
    "CMSM": {
      "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
    },
    "AWS3": {
      "LOCC": "us-east-1"
    }
  },
  "CLCO\ (Locations\)": \[
  \{
```

```

        "Location Type": "CLDI\ (Location online\)",
        "NOID\ (Node ID\)": "12448208",
        "VOLI\ (Volume ID\)": "3222345473",
        "Object File Path":
"/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila\#3udu",
        "LTIM\ (Location timestamp\)": "2020-02-12T19:36:17.880569"
    \},
    \{
        "Location Type": "CLDI\ (Location online\)",
        "NOID\ (Node ID\)": "12288733",
        "VOLI\ (Volume ID\)": "3222345984",
        "Object File Path":
"/var/local/rangedb/0/p/19/11/00rH0%DkRt78Rrb\#3s;L",
        "LTIM\ (Location timestamp\)": "2020-02-12T19:36:17.934425"
    }
]
}

```

- a. LDR コンソールからサインアウトします。入力するコマンド `exit`
5. 管理ノードから、監査ログを検索してこのオブジェクトを ORLM 監査メッセージで探し、必要に応じて情報ライフサイクル管理（ILM）によっ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. に記載されているパスワードを入力します `Passwords.txt` ファイル。
- iii. 次のコマンドを入力してrootに切り替えます。 `su -`
- iv. に記載されているパスワードを入力します `Passwords.txt` ファイル。  
rootとしてログインすると、プロンプトがから変わります `$ 終了: #`。

- b. 監査ログが格納されているディレクトリに移動します。を参照してください [手順1.b](#)。

- c. `grep` を使用して、オブジェクトに関連付けられている監査メッセージを出力ファイルに抽出します。  
入力するコマンド `grep uuid-valueaudit_file_name > output_file_name`

例：

```

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。  
入力するコマンド `grep ORLM output_file_name`

例：

```
Admin: # grep ORLM /var/local/tmp/messages_about_restored_object.txt
```

次の例は、ORLM監査メッセージの例を示しています。

```
[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. 監査メッセージで LOCS フィールドを検索します。

このフィールドの 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、2つのオブジェクトコピーがグリッド内の2つの場所に作成されたことを示しています。

6. ["損失オブジェクトと欠落オブジェクトのカウントをリセットします"](#) をクリックします。

損失オブジェクトと欠落オブジェクトのカウントをリセットします

StorageGRID システムを調査し、記録されたすべての損失オブジェクトが完全に失われていること、または誤ったアラームであることを確認できたら、Lost Objects 属性の値を 0 にリセットできます。

作業を開始する前に

- を使用して Grid Manager にサインインする必要があります ["サポートされている Web ブラウザ"](#)。
- これで完了です ["特定のアクセス権限"](#)。

このタスクについて

Lost Objects カウンタは次のどちらかのページからリセットできます。

- [サポート > ツール > Grid Topology > \\_ Site\\_ > \\_ Storage Node\\_ > LDR > Data Store > Overview > Main](#)
- [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](#)

これらの手順は、[Idr>Data Store](#) ページからカウンタをリセットする方法を示しています。

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. 警告または LOST アラームが発生しているストレージノードについて、「[\\_ Site\\_ > \\_ ストレージノード\\_ > LDR > Data Store > Configuration](#)」を選択します。
3. 「[\\_ Lost Objects Count](#) をリセット」を選択します。



## Configuration: LDR (99-94) - Data Store

Updated: 2017-05-11 14:56:13 PDT

Reset Lost Objects Count

Apply Changes

#### 4. [変更の適用 \*] をクリックします。

Lost Objects 属性が 0 にリセットされ、\* Objects lost \* アラートと LOST アラームが解除されます。これには数分かかることがあります。

#### 5. 必要に応じて、損失オブジェクトを特定するプロセスで増分された可能性がある、その他の関連属性の値をリセットできます。

- [Site>\*Storage Node\*>Idr\*>erasure Coding\*>Configuration\*] を選択します。
- 「Reset Reads Failure Count」と「Reset Corrupt Copies Detected Count」を選択します。
- [変更の適用 \*] をクリックします。
- [\*\_ サイト \_\*>\*\_ ストレージ・ノード \_\*>\* LDR \*>\* Verification \*>\* Configuration \*] を選択します。
- 「Reset Missing Objects Count」（不足オブジェクト数のリセット）および「Reset Corrupt Objects Count」（破損オブジェクト数のリセット）を選択します
- 隔離されたオブジェクトが不要であることが確実な場合は、\*[Delete Quarantined Objects]\*を選択します。

隔離されたオブジェクトは、バックグラウンド検証で破損したレプリケートオブジェクトコピーが確認されると作成されます。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、隔離されたオブジェクトを削除しても安全です。ただし、\* Objects lost \* アラートがトリガーされた場合や、LOST アラームがトリガーされた場合は、テクニカルサポートが隔離されたオブジェクトにアクセスすることを推奨します。

#### g. [変更の適用 \*] をクリックします。

[変更の適用 (Apply Changes)] 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。

### Low object data storage アラートのトラブルシューティングを行います

Low object data storage \* アラートは、オブジェクトデータを格納可能な各ストレージノードのスペースを監視します。

作業を開始する前に

- を使用して Grid Manager にサインインします "サポートされている Web ブラウザ"。

- これで完了です "特定のアクセス権限"。

このタスクについて

Low object data storage \*アラートは、ストレージノード上のレプリケートオブジェクトデータとイレイジャーコーディングオブジェクトデータの合計量がアラートルールで設定されている条件のいずれかを満たすとトリガーされます。

デフォルトでは、次の条件が true と評価されると、Major 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
```

この条件では、次のように

- storagegrid\_storage\_utilization\_data\_bytes は、ストレージノードのレプリケートオブジェクトデータとイレイジャーコーディングオブジェクトデータの推定合計サイズです。
- storagegrid\_storage\_utilization\_usable\_space\_bytes は、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総容量です。

Major または Minor \* Low object data storage \* 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。

[Alerts] ページが表示されます。

2. アラートの表で、必要に応じて「 \* 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で詳細を確認し、次の点に注意してください。

- トリガーされた時刻
- サイトとノードの名前
- このアラートに関する指標の現在の値

4. ノード \* > \* \_ストレージノードまたは Site\_ \* > \* ストレージ \* を選択します。

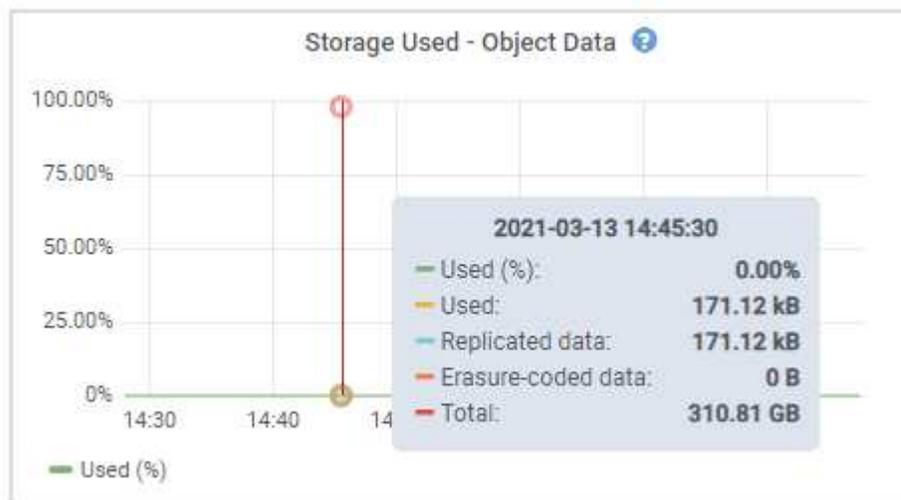
5. [Storage Used - Object Data] グラフにカーソルを合わせます。

次の値が表示されます。

- \* Used ( % ) \* : 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。
- \* Used \* : 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。
- \* Replicated data \* : このノード、サイト、またはグリッド上のレプリケートオブジェクトデータの推

定量。

- \* イレイジャーコーディングデータ \* : このノード、サイト、またはグリッドにあるイレイジャーコーディングオブジェクトデータの推定量。
- \* Total \* : このノード、サイト、またはグリッドで使用可能なスペースの総容量。  
使用済みの値は `storagegrid_storage_utilization_data_bytes` メートル法。



6. グラフ上部の時間コントロールを選択して、期間を変えながらストレージの使用状況を確認します。

ストレージの使用状況の推移を確認することで、アラートがトリガーされた前後のストレージの使用量がわかり、ノードの残りのスペースがいっぱいになるまでの時間を予測できます。

7. できるだけ早く、**"ストレージ容量を追加"** あなたのグリッドに。

既存のストレージノードにストレージボリューム（LUN）を追加するか、または新しいストレージノードを追加することができます。



詳細については、を参照してください ["ストレージノードがいっぱいになったときの管理"](#)。

## 関連情報

["Storage Status \(SSTS\) アラーム \(従来の\) のトラブルシューティング"](#)

[読み取り専用のロー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、「読み取り専用の低ウォーターマーク上書き \*」アラートを解決する必要があります。可能であれば、最適化された値の使用を開始するようにシステムを更新してください。

以前のリリースでは ["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：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ていた。StorageGRID 11.6 以降では、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、ストレージボリュームごとに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する場合を除き、最適化された読み取り専用ウォーターマークと読み取り/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。

- システムは容量に近く、最適化されたウォーターマークが適用されている場合は新しいデータを受け入れられません。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をカスタム値に設定している。StorageGRID では、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、Storage Volume Soft Read-Only Watermark のカスタム値が小さすぎると、StorageGRID は「Low read-only watermark override\*」アラートをトリガーする場合があります。

アラートを確認します

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 \* 読み取り専用の低ウォーターマーク上書き \* 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、\* Storage Volume Soft Read-Only Watermark \* のカスタム値が、そのストレージノードの最適化された最小値より小さくなっていることを示しています。カスタム設定を引き続き使用すると、ストレージノードのスペースが非常に少なくなる可能性があります。この値を超えると、ストレージノードは読み取り専用状態に安全に移行できます。ノードの容量が上限に達すると、一部のストレージボリュームにアクセスできなくなる（自動的にアンマウントされる）ことがあります。

たとえば、\* Storage Volume Soft Read-Only Watermark \* を 5GB に設定しているとします。次に、ストレージノード A の 4 つのストレージボリュームについて、StorageGRID が次の最適化値を計算したとします。

ボリューム0	12GB
ボリューム 1	12GB
巻2	11GB
巻三	15 GB

カスタムのウォーターマーク（5GB）がそのノード内のすべてのボリュームに対する最小最適値（11GB）よりも小さいため、「Low read-only watermark override\*」アラートがストレージノード A に対してトリガーされます。カスタム設定を引き続き使用すると、ノードが読み取り専用状態に安全に移行できるようになる前に、ノードのスペースが非常に少なくなる可能性があります。

アラートを解決します

1つ以上の \* 読み取り専用の低ウォーターマーク上書き \* アラートがトリガーされた場合は、次の手順を実行します。また、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、この手順を使用できます。

作業を開始する前に

- StorageGRID 11.6以降へのアップグレードが完了している。
- を使用して Grid Manager にサインインします "[サポートされている Web ブラウザ](#)"。
- を使用することができます "[rootアクセス権限](#)"。

このタスクについて

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の上書きに更新することにより '読み取り専用のロー・ウォーターマーク・オーバーライド \* 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いっぱいに近づいている場合や特別な 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て、そのノードを安全に使用できるかどうかを確認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使用量を評価します

手順

1. [\* nodes (ノード) ] を選択します
2. グリッド内のサイトごとに、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について、「\* Object Data Used \*」列に表示されている割合値を確認します。

Name	Type	Object data used	Object metadata used	CPU usage
StorageGRID	Grid	61%	4%	—
▲ Data Center 1	Site	56%	3%	—
DC1-ADM	Primary Admin Node	—	—	6%
DC1-GW	Gateway Node	—	—	1%
! DC1-SN1	Storage Node	71%	3%	30%
! DC1-SN2	Storage Node	25%	3%	42%
! DC1-SN3	Storage Node	63%	3%	42%
! DC1-SN4	Storage Node	65%	3%	41%

4. 該当する手順を実行します。
  - a. ほぼすべてのストレージノードが上限に近い場合（使用済みオブジェクトデータがすべて \* されている値が 80% 未満の場合など）は、無視設定を使用できます。に進みます [最適化されたウォーターマークを使用](#)。
  - b. ILMルールの取り込み動作がStrictに設定されている場合や特定のストレージプールがフルに近い場合は、この手順を実行します。 [最適化されたストレージウォーターマークを表示する](#) および [最適化されたウォーターマークを使用できるかどうかを確認します](#)。

## 最適化されたストレージのウォーターマークの表示

StorageGRID は、2 つの Prometheus 指標を使用して、\* Storage Volume Soft Read-Only Watermark \* に対して計算された最適値を表示します。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. [**support**>]、[\*Tools]、[\*Metrics] の順に選択します。
2. Prometheus セクションで、Prometheus ユーザーインターフェイスへのリンクを選択します。
3. 推奨されるソフト読み取り専用の最小ウォーターマークを確認するには、次の Prometheus 指標を入力し、\* Execute \* 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に対して Soft Read-Only Watermark の最小最適値が表示されます。この値が \* Storage Volume Soft Read - Only Watermark \* 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. 推奨されるソフト読み取り専用の最大ウォーターマークを確認するには、次の Prometheus 指標を入力し、\* Execute \* 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に対して Soft Read-Only Watermark の最大最適値が表示されます。

5. [[maximum\_optimized\_value] 各ストレージノードの最適化された最大値をメモします。

## 最適化されたウォーターマークを使用できるかどうかを判断する

### 手順

1. [\* nodes (ノード) ] を選択します
2. オンラインのストレージノードごとに上記の手順を繰り返します。
  - a. [**Storage Node**>\* Storage\*] を選択します。
  - b. [Object Stores] 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用にメモした最大最適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上の少なくとも 1 つのボリュームに、そのノードの最大最適ウォーターマークを超える使用可能なスペースがある場合は、に進みます [最適化されたウォーターマークを使用](#) 最適化されたウォーターマーク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。または ["ストレージボリュームを追加します"](#) を既存のノードまたはに追加します ["新しいストレージノードを追加します"](#)。次に、に進みます [最適化されたウォーターマークを使用](#) ウォーターマーク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、**"無音"** または **"- 無効にします"** 「\* 読み取り専用のロー・ウォーターマーク・オーバーライド \*」アラート。



各ストレージノード上の各ストレージボリュームには、同じカスタムのウォーターマーク値が適用されます。ストレージボリュームのウォーターマーク原因に推奨よりも小さい値を使用すると、ノードの容量に達したときに一部のストレージボリュームにアクセスできなくなる（自動的にアンマウントされる）ことがあります。

最適化されたウォーターマークを使用する

手順

1. >[その他]>[ストレージのウォーターマーク]\*を選択します。
2. [最適化された値を使用する]チェックボックスをオンにします。
3. [保存 ( Save ) ]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、ストレージボリュームごとに最適化されたストレージボリュームのウォーターマーク設定が有効になりました。

**Storage Status ( SSTS )** アラームをトラブルシューティングします

Storage Status ( SSTS ) アラームは、ストレージノードにオブジェクトストレージ用の十分な空きスペースが残っていない場合にトリガーされます。

作業を開始する前に

- を使用して Grid Manager にサインインする必要があります ["サポートされている Web ブラウザ"](#)。
- これで完了です ["特定のアクセス権限"](#)。

このタスクについて

ストレージノード内のすべてのボリュームの空きスペース量が Storage Volume Soft Read Only Watermark ( \* configuration \* > \* System \* > \* Storage options \* ) の値を下回ると、SSTS ( Storage Status ) アラームが Notice レベルでトリガーされます。



## Storage Options Overview

Updated: 2019-10-09 13:09:30 MDT

### Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1 GB

### Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark	30 GB
Storage Volume Soft Read-Only Watermark	10 GB
Storage Volume Hard Read-Only Watermark	5 GB
Metadata Reserved Space	3,000 GB

たとえば、Storage Volume Soft Read-Only Watermark がデフォルト値の 10GB に設定されているとします。ストレージノード内の各ストレージボリュームに残っている使用可能スペースが 10GB 未満になると、SSTS アラームがトリガーされます。いずれかのボリュームに 10GB 以上の空き容量があれば、アラームはトリガーされません。

SSTS アラームがトリガーされた場合は、次の手順を実行して問題を詳しく把握する必要があります。

手順

1. **support**>\* Alarms (レガシー) > Current alarms \* を選択します。
2. Service 列で、SSTS アラームに関連付けられているデータセンター、ノード、およびサービスを選択します。

Grid Topology ページが表示されます。Alarms タブには、選択したノードおよびサービスのアクティブなアラームが表示されます。

Severity	Attribute	Description	Alarm Time	Trigger Value	Current Value	Acknowledge Time	Acknowledge
Notice	SSTS (Storage Status)	Insufficient Free Space	2019-10-09 12:42:51 MDT	Insufficient Free Space	Insufficient Free Space		<input type="checkbox"/>
Notice	SAVP (Total Usable Space (Percent))	Under 10 %	2019-10-09 12:43:21 MDT	7.95 %	7.95 %		<input type="checkbox"/>
Normal	SHLH (Health)						<input type="checkbox"/>

この例では、SSTS (Storage Status) アラームと SAVP (Total Usable Space (Percent)) アラームの両方が Notice レベルでトリガーされています。



通常は、SSTS アラームと SAVP アラームの両方がほぼ同時にトリガーされます。ただし、両方のアラームがどちらトリガーされるかはウォーターマークの設定 (GB) と SAVP アラームの設定で決まります。

3. 実際に使用可能なスペース量を確認するには、**ldr**>\*Storage\*>\*Overview\* を選択し、Total Usable Space (STAS) 属性を検索します。

Overview Alarms Reports Configuration

Main

 Overview: LDR (:DC1-S1-101-193) - Storage  
Updated: 2019-10-09 12:51:07 MDT

Storage State - Desired:	Online	
Storage State - Current:	Read-only	
Storage Status:	Insufficient Free Space	 

### Utilization

Total Space:	164 GB	
Total Usable Space:	19.6 GB	
Total Usable Space (Percent):	11.937 %	 
Total Data:	139 GB	
Total Data (Percent):	84.567 %	

### Replication

Block Reads:	0	
Block Writes:	2,279,881	
Objects Retrieved:	0	
Objects Committed:	88,882	
Objects Deleted:	16	
Delete Service State:	Enabled	

### Object Store Volumes

ID	Total	Available	Replicated Data	EC Data	Stored (%)	Health
0000	54.7 GB	2.93 GB	 46.2 GB	 0 B	 84.486 %	No Errors  
0001	54.7 GB	8.32 GB	 46.3 GB	 0 B	 84.644 %	No Errors  
0002	54.7 GB	8.36 GB	 46.3 GB	 0 B	 84.57 %	No Errors  

この例のストレージノードでは、164GB 中 19.6GB しか使用可能なスペースが残っていません。合計は3つのオブジェクトストアボリュームの「使用可能な」\* 値の合計です。3つのストレージボリュームのそれぞれに10GB 未満の空きスペースがあったため、SSTS アラームがトリガーされました。

4. 一定期間にわたるストレージの使用状況を確認するには、\* Reports \* タブを選択し、過去数時間の Total Usable Space のプロットを使用します。

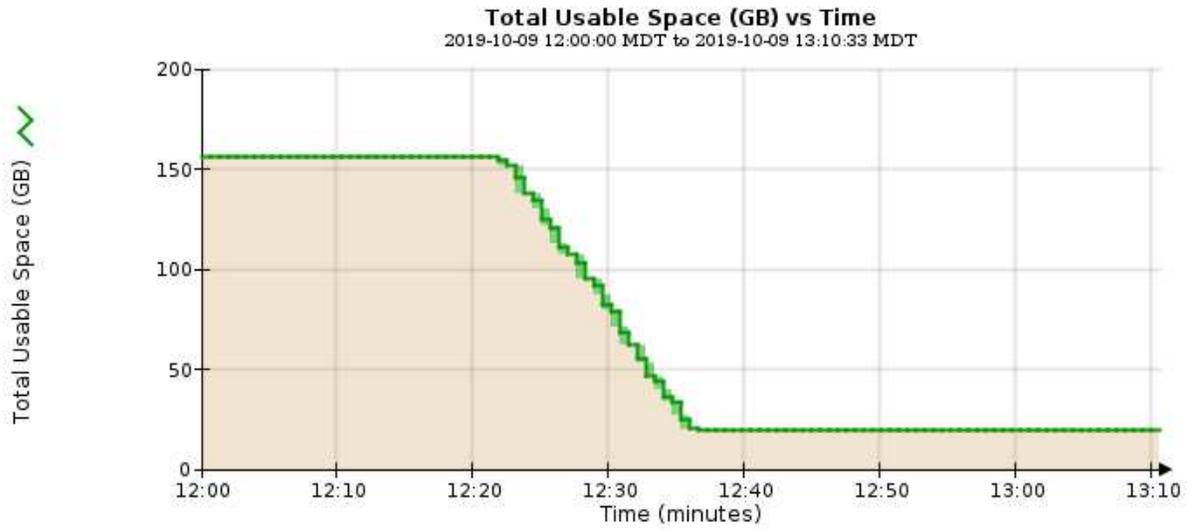
この例では、12 : 00 の時点の使用可能な合計スペースは約 155 GB でしたが、12 : 35 には 20 GB まで減り、その時点で SSTS アラームがトリガーされています。



## Reports (Charts): LDR (DC1-S1-101-193) - Storage

Attribute:	Total Usable Space	Vertical Scaling:	<input checked="" type="checkbox"/>	Start Date:	2019/10/09 12:00:00
Quick Query:	Custom Query	Raw Data:	<input type="checkbox"/>	End Date:	2019/10/09 13:10:33

Update



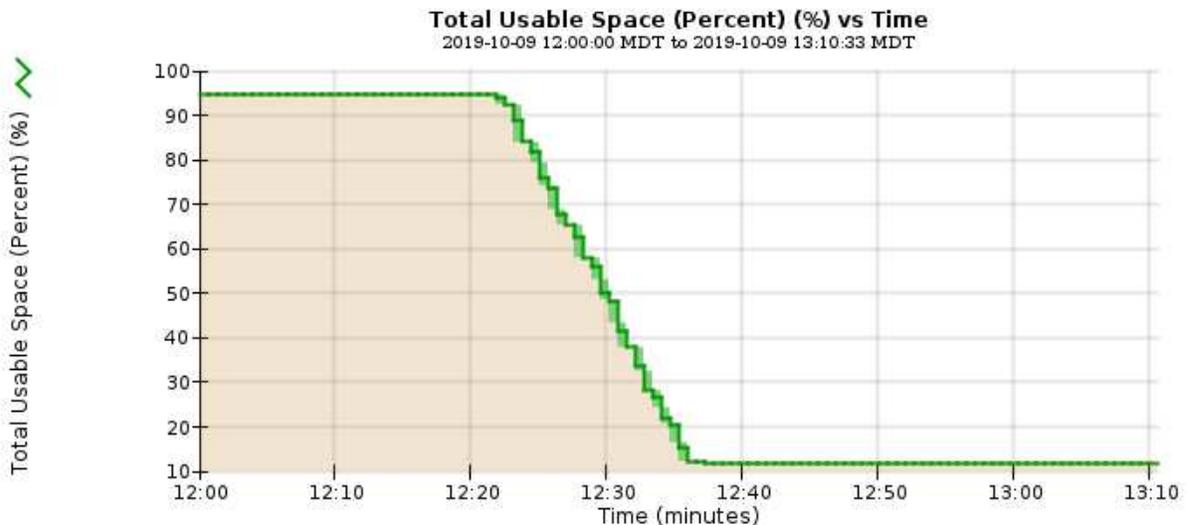
5. 合計容量の割合としてストレージがどのように使用されているかを確認するには、過去数時間の合計使用可能スペース（割合）をプロットします。

この例では、ほぼ同じタイミングで使用可能な合計スペースが 95% から 10% 強に減少しています。



## Reports (Charts): LDR (DC1-S1-101-193) - Storage

Attribute:	Total Usable Space (Percent) ▼	Vertical Scaling:	<input checked="" type="checkbox"/>	Start Date:	2019/10/09 12:00:00
Quick Query:	Custom Query ▼	Raw Data:	<input type="checkbox"/>	End Date:	2019/10/09 13:10:33
		Update			



6. 必要に応じて、"ストレージ容量を追加"。

も参照してください"ストレージノードがいっぱいになったときの管理"。

プラットフォームサービスメッセージの配信のトラブルシューティング ( **SMTT** アラーム)

データを受信できないデスティネーションにプラットフォームサービスメッセージが配信されると、Total Events (SMTT) アラームがGrid Managerでトリガーされます。

このタスクについて

たとえば、設定されているエンドポイントに関連するレプリケーションまたは通知メッセージを配信できなくても、S3マルチパートアップロードは成功します。または、CloudMirrorレプリケーションのメッセージはメタデータが長すぎると配信できません。

SMTTアラームには、Failed to publish notifications for *bucket-name object key*通知が失敗した最後のオブジェクト

イベントメッセージは、にも表示されます /var/local/log/bycast-err.log ログファイル：を参照してください"ログファイル参照"。

追加情報の場合は、を参照してください"プラットフォームサービスのトラブルシューティングを行う"。必要に応じて"Tenant Manager からテナントにアクセスします"プラットフォームサービスのエラーをデバッグするには、次の手順を実行

## 手順

1. アラームを表示するには、 \* nodes \* > \* \_site \* > \* \_grid node\_name \* > \* Events \* を選択します。
2. 表の一番上に Last Event が表示されます。

イベントメッセージは、にも表示されます /var/local/log/bycast-err.log。

3. SMTT アラームに記載されている指示に従って問題 を修正します。
4. [\* イベントカウントをリセット \*] を選択します。
5. プラットフォームサービスメッセージが配信されていないオブジェクトについてテナントに通知します。
6. テナントで、オブジェクトのメタデータまたはタグを更新することで、失敗したレプリケーションまたは通知をトリガーするよう指定します。

## メタデータに関する問題のトラブルシューティング

メタデータに関する問題の原因を特定するのに役立ついくつかのタスクを実行できません。

### Low metadata storage アラート

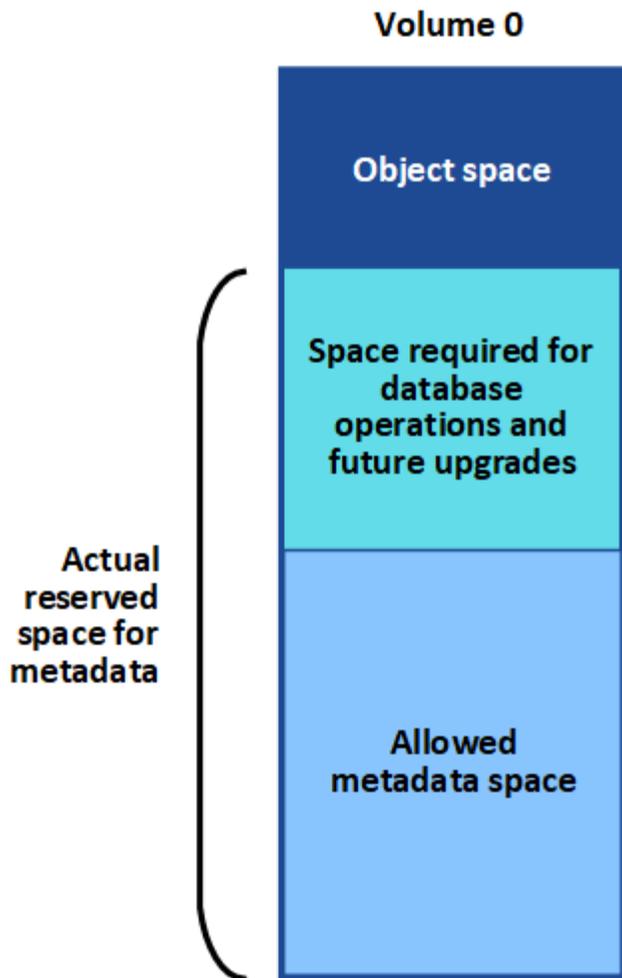
Low metadata storage \* アラートがトリガーされた場合は、新しいストレージノードを追加する必要があります。

作業を開始する前に

- を使用して Grid Manager にサインインします "[サポートされている Web ブラウザ](#)"。

このタスクについて

StorageGRID は、各ストレージノードのボリューム 0 上にオブジェクトメタデータ用に一定量のスペースをリザーブします。このスペースは、実際のリザーブスペースと呼ばれ、オブジェクトメタデータに使用できるスペース（許可されるメタデータスペース）と、コンパクションや修復などの重要なデータベース処理に必要なスペースに分割されます。許可されるメタデータスペースは、オブジェクトの全体的な容量を決定します。



オブジェクトメタデータがメタデータに使用できるスペースの100%を超えると、データベース処理を効率的に実行できず、エラーが発生します。

可能です ["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します"](#) エラーを予測し、発生前に修正できるようにします。

StorageGRID は、次の Prometheus 指標を使用して、許可されているメタデータスペースの使用状況を測定します。

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utilization_metadata_allowed_bytes
```

この Prometheus 式が特定のしきい値に達すると、**\* Low metadata storage \*** アラートがトリガーされます。

- **\* Minor \*** : オブジェクトメタデータが、許可されているメタデータスペースの 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。
- **\* Major \*** : オブジェクトメタデータが使用しているメタデータスペースが 90% 以上あります。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使用可能なメタデータスペースの90%以上を使用している場合は、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の使用量は、使用できるスペースの 100% を超えないようにする必要があります。

- **\* クリティカル \*** : オブジェクトメタデータが使用可能なメタデータスペースの 100% 以上を使用しており、重要なデータベース処理に必要なスペースを使い始めています。新しいオブジェクトの取り込みを停止し、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。

次の例では、オブジェクトメタデータが使用しているメタデータスペースが 100% を超えています。これは重大な状況であり、データベース処理の効率低下とエラーの発生につながります。

The following Storage Nodes are using more than 90% of the space allowed for object metadata:

Node	% Used	Used	Allowed
DC1-S2-227	104.51%	6.73 GB	6.44 GB
DC1-S3-228	104.36%	6.72 GB	6.44 GB
DC2-S2-233	104.20%	6.71 GB	6.44 GB
DC1-S1-226	104.20%	6.71 GB	6.44 GB
DC2-S3-234	103.43%	6.66 GB	6.44 GB

Undesirable results can occur if object metadata uses more than 100% of the allowed space. You must add new Storage Nodes immediately or contact support.



ボリューム 0 のサイズが Metadata Reserved Space ストレージオプションより小さい場合（非本番環境など）は、「Low metadata storage \*」アラートが正確に計算されないことがあります。

#### 手順

1. [ \* alerts \* > \* current \* ] を選択します。
2. アラートの表で、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. Major または Critical の \* Low metadata storage \* 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ます。



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も小規模な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も、追加する必要があります **"他のサイトを展開します"** 同じ数のストレージノードで異なります。

拡張の実行後、StorageGRID によって既存のオブジェクトメタデータが新しいノードに再配分され、グリッドの全体的なメタデータ容量が増加します。ユーザーによる操作は必要ありません。Low metadata storage \* アラートがクリアされます。

#### Services : Status - Cassandra (SVST) アラーム

Services : Status - Cassandra (SVST) アラームは、ストレージノードに対する Cassandra データベースのリビルドが必要となる可能性があることを示します。Cassandra は StorageGRID 用のメタデータストアとして使用されます。

作業を開始する前に

- を使用して Grid Manager にサインインする必要があります "サポートされている Web ブラウザ"。
- これで完了です "特定のアクセス権限"。
- を用意しておく必要があります Passwords.txt ファイル。

このタスクについて

Cassandra が停止している（ストレージノードの電源がオフになっているなど）期間が 15 日を超える場合、ノードがオンライン状態に戻っても Cassandra は起動されません。この場合、該当する DDS サービスの Cassandra データベースをリビルドする必要があります。

可能です "診断を実行します" グリッドの現在の状態に関する追加情報 を取得します。



複数のCassandraデータベースサービスが15日以上停止している場合は、次の手順は実行せずにテクニカルサポートに連絡してください。

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. アラームを表示するには、[Site>\*Storage Node\*>\*SSM\*>\*Services\*>\*Alarm\*>\*Main\*] を選択します。

この例は、SVST アラームがトリガーされたことを示しています。

Severity Attribute	Description	Alarm Time	Trigger Value	Current Value	Acknowledge Time	Acknowledge
Minor SVST (Services: Status - Cassandra)	Not Running	2014-08-14 14:56:28 PDT	Not Running	Not Running		<input type="checkbox"/>

SSM Services のメインページには、Cassandra が実行されていないことも表示されます。

Overview Alarms Reports Configuration

Main

 Overview: SSM (DC2-S1) - Services  
Updated: 2017-03-30 09:53:53 MDT

---

Operating System: Linux  
3.16.0-4-amd64

### Services

Service	Version	Status	Threads	Load	Memory
Account Service	10.4.0-20161224.0333.803cd91	Running 	7	0.002 %	12 MB
Administrative Domain Controller (ADC)	10.4.0-20170329.0039.8800cae	Running 	52	0.14 %	63.1 MB
Cassandra	4.6.12-1.byc.0-20170308.0109.ba3598a	Not Running 	0	0 %	0 B
Content Management System (CMS)	10.4.0-20170220.1846.1a76aed	Running 	18	0.055 %	20.6 MB
Distributed Data Store (DDS)	10.4.0-20170329.0039.8800cae	Running 	104	1.301 %	76 MB
Identity Service	10.4.0-20170203.2038.a457d45	Running 	6	0 %	8.75 MB
Keystone Service	10.4.0-20170104.1815.6e52138	Running 	5	0 %	7.77 MB
Local Distribution Router (LDR)	10.4.0-20170329.0039.8800cae	Running 	109	0.218 %	96.6 MB
Server Manager	10.4.0-20170306.2303.9649faf	Running 	4	3.58 %	19.1 MB

3. ストレージノードからCassandraを再起動してみます。

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. に記載されているパスワードを入力します `Passwords.txt` ファイル。

iii. 次のコマンドを入力してrootに切り替えます。 `su -`

iv. に記載されているパスワードを入力します `Passwords.txt` ファイル。  
rootとしてログインすると、プロンプトがから変わります `$ 終了: #`。

b. 入力するコマンド `/etc/init.d/cassandra status`

c. Cassandraが実行されていない場合は再起動します。 `/etc/init.d/cassandra restart`

4. Cassandra が再起動されない場合は、Cassandra が停止していた期間を調べます。Cassandra の停止期間が 15 日を超えている場合、Cassandra データベースをリビルドする必要があります。



複数のCassandraデータベースサービスが停止している場合は、次の手順は実行せずにテクニカルサポートに連絡してください。

グラフを作成するか、`servermanager.log` ファイルを確認することで、Cassandra が停止していた期間を調べることができます。

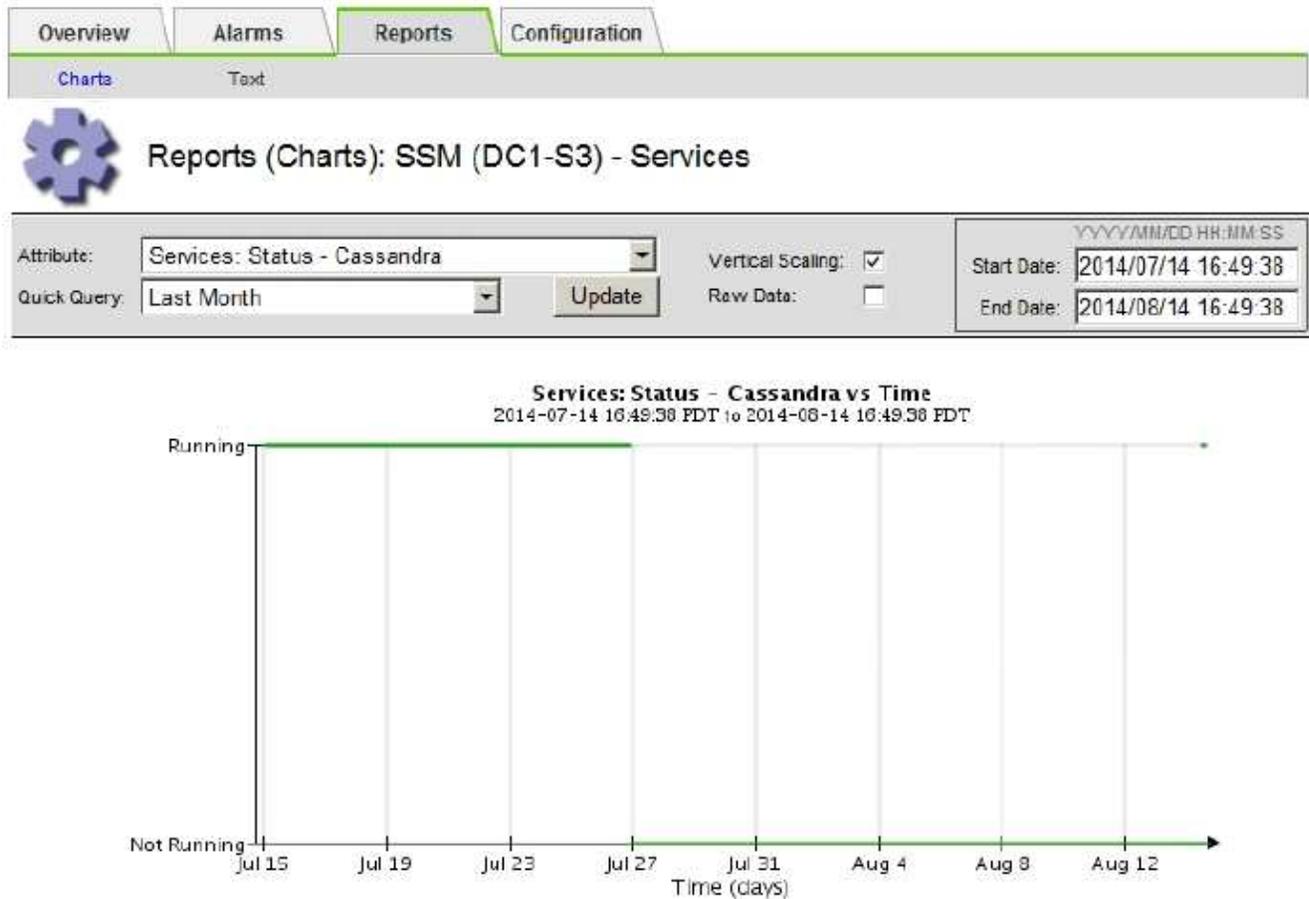
5. Cassandra のグラフを確認する手順は次

a. サポート \* > ツール \* > グリッドトポロジ \* を選択します。次に、[\*\_サイト\_\* > \*\_ストレージノード\_\* > SSM\* > サービス\* > レポート\* > チャート\*]を選択します。

b. 「\* Attribute \* > Service : Status - Cassandra \*」を選択します。

- c. [開始日]には、現在の日付よりも **16** 日前の日付を入力します。[終了日\*]には、現在の日付を入力します。
- d. [更新 (Update)] をクリックします。
- e. グラフから Cassandra の停止期間が 15 日を超えていることがわかった場合は、Cassandra データベースをリビルドします。

次のグラフの例では、Cassandra が少なくとも 17 日間は停止していることがわかります。



6. ストレージノードで servermanager.log ファイルを確認するには、次の手順を実行します。

- 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. に記載されているパスワードを入力します Passwords.txt ファイル。
  - iii. 次のコマンドを入力してrootに切り替えます。 `su -`
  - iv. に記載されているパスワードを入力します Passwords.txt ファイル。  
rootとしてログインすると、プロンプトがから変わります \$ 終了: #。
- b. 入力するコマンド `cat /var/local/log/servermanager.log`

servermanager.log ファイルの内容が表示されます。

Cassandra の停止期間が 15 日を超えている場合、servermanager.log ファイルに次のメッセージが表示されます。

```
"2014-08-14 21:01:35 +0000 | cassandra | cassandra not
started because it has been offline for longer than
its 15 day grace period - rebuild cassandra
```

- a. このメッセージのタイムスタンプが手順に従って Cassandra の再起動を試行した時間になっていることを確認してください [ストレージノードから Cassandra を再起動します](#)。

Cassandra のエントリは 1 つとは限らないため、最新のエントリを確認する必要があります。

- b. Cassandra の停止期間が 15 日を超えている場合、Cassandra データベースをリビルドする必要があります。

手順については、を参照してください "[ストレージノードを 15 日以上停止した状態にリカバリします](#)"。

- c. Cassandra の再構築後にアラームがクリアされない場合は、テクニカルサポートにお問い合わせください。

### Cassandra Out of Memory エラー (SMTT アラーム)

Total Events (SMTT) アラームは、Cassandra データベースでメモリ不足エラーが発生するとトリガーされます。このエラーが発生した場合は、テクニカルサポートに連絡して問題の処理を依頼してください。

このタスクについて

Cassandra データベースにメモリ不足エラーが発生すると、ヒープダンプが作成され、Total Events (SMTT) アラームがトリガーされて、Cassandra Heap Out Of Memory Errors のカウントが 1 つ増えます。

手順

1. イベントを表示:
  - a. サポート > ツール > [グリッドトポロジ](#) を選択します。
  - b. サイトを展開し、[grid\\_node](#) を選択します。
  - c. **SSM** を選択し、イベント > 構成 を選択します。
2. Cassandra Heap Out Of Memory Errors のカウントが 1 以上であることを確認します。

可能です ["診断を実行します"](#) グリッドの現在の状態に関する追加情報を取得します。

3. SSH を使用して選択したノードに「admin」としてログインし、ローカルの root ユーザーに切り替えます。
4. に進みます `/var/local/core/`` を圧縮します ``Cassandra.hprof` ファイルを保存してテクニカルサポートに送信します。
5. のバックアップを作成します `Cassandra.hprof` ファイルを選択し、から削除します `/var/local/core/ directory`。

このファイルは 24GB もの大きさになることがあるため、削除してスペースを解放してください。

6. 問題が解決されたら、[Cassandra Heap Out of Memory Errors]数の\*[Reset]\*チェックボックスを選択します。次に、\* [変更を適用](#) \* を選択します。



イベント数をリセットするには、Gridトポロジページの設定権限が必要です。

## 証明書エラーのトラブルシューティングを行う

Web ブラウザ、S3 または Swift クライアント、または外部の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表示される場合は、証明書を確認してください。

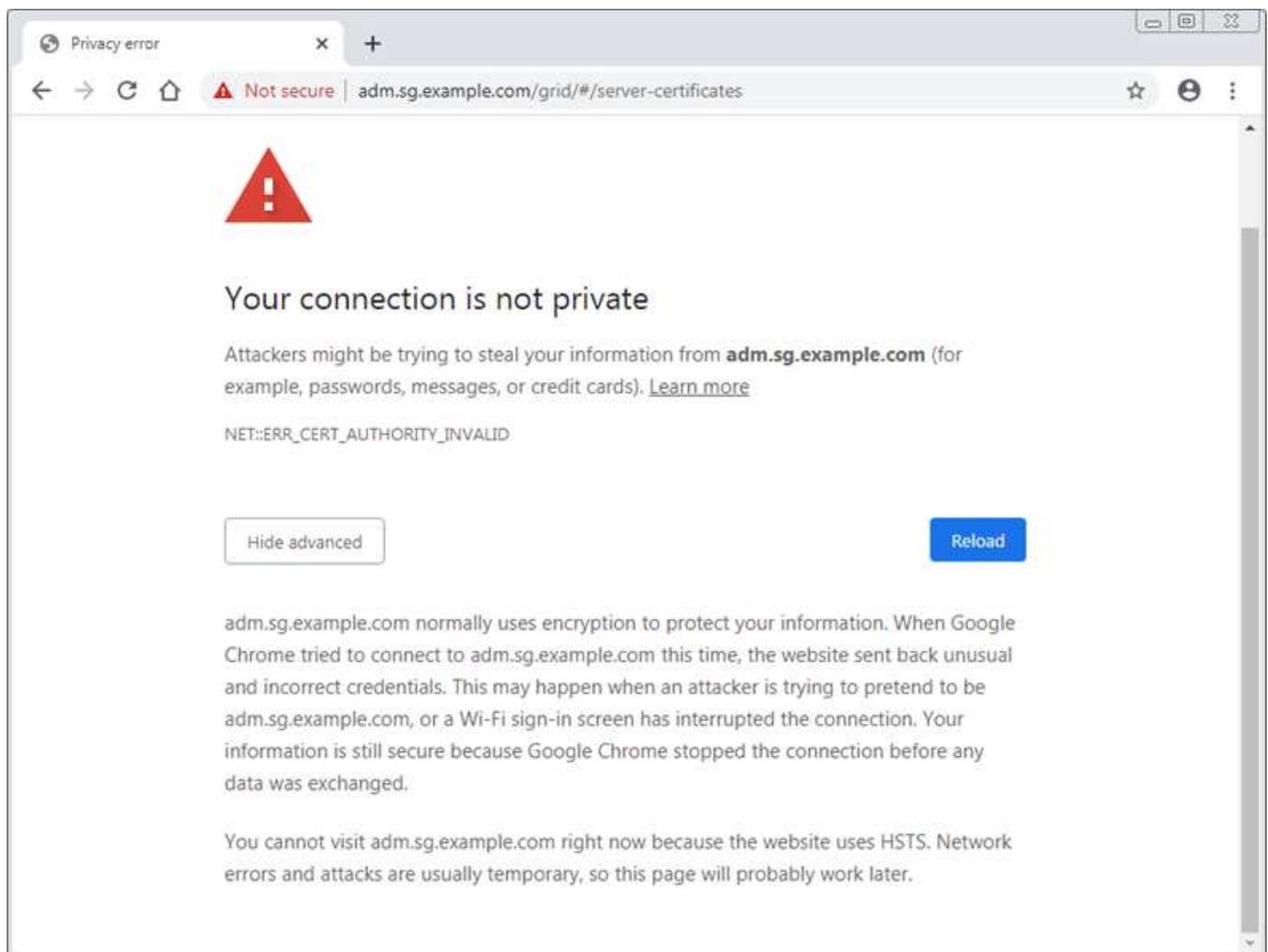
このタスクについて

証明書エラーは、グリッドマネージャ、グリッド管理 API、テナントマネージャ、またはテナント管理 API を使用して StorageGRID に接続しようとしたときに、原因で発生する可能性があります。証明書のエラーは、S3 / Swift クライアントまたは外部の監視ツールを使用して接続しようとした場合にも発生します。

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 にアクセスする場合は、次のいずれかの場合に証明書のエラーが表示され、バイパスするオプションはありません。

- カスタム管理インターフェイス証明書の有効期限が切れます。
- カスタムの管理インターフェイス証明書をデフォルトのサーバ証明書に戻した場合。

次の例は、カスタム管理インターフェイ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。



サーバ証明書の問題によって処理が中断されないようにするために、サーバ証明書の有効期限が近づくと\* Expiration of server certificate for Management Interface \*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、証明書のエラーは、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が原因で発生することがあります。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 \* アラートで設定されたクライアント証明書の有効期限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。

。「 \* configuration \* > \* Security \* > \* Certificates \* 」を選択し、次にを選択します ["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ます。 [+]  
一部のWebブラウザおよびS3またはSwiftクライアントでは、有効期間が398日を超える証明書が受け入れられません。
2. 証明書の有効期限が切れているか、まもなく期限切れになる場合は、新しい証明書をアップロードまたは生成します。
  - サーバ証明書については、の手順を参照してください ["Grid Manager および Tenant Manager 用のカスタムサーバ証明書を設定する"](#)。
  - クライアント証明書については、の手順を参照してください ["クライアント証明書を設定しています"](#)。
3. サーバ証明書エラーの場合は、次のいずれかまたは両方を実行してください。
  - 証明書の Subject Alternative Name ( SAN ) が設定されていること、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てください。
  - ドメイン名を使用して StorageGRID に接続しようとしている場合は、次の手順を実行します。
    - i. 接続エラーをバイパスして Grid Manager にアクセスするために、ドメイン名ではなく管理ノードの IP アドレスを入力します。
    - ii. Grid Manager で、 \* configuration \* > \* Security \* > \* Certificates \* を選択してから ["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使用して続行します。
    - iii. StorageGRID の管理手順については、の手順を参照してください ["Grid Manager および Tenant Manager 用のカスタムサーバ証明書を設定する"](#)。

## 管理ノードとユーザインターフェイスの問題をトラブルシューティングする

ここでは、管理ノードと StorageGRID ユーザインターフェイスに関連する問題の原因を特定するのに役立ついくつかのタスクを紹介します。

### サインオンエラー

StorageGRID 管理ノードへのサインイン時にエラーが発生した場合は、システムに問題 が搭載されている可能性があります ["アイデンティティフェデレーションの設定"](#)、 a ["ネットワーク"](#) または ["ハードウェア"](#) 問題があります。問題 があります ["管理ノードサービス"](#)または ["問題 とCassandraデータベース"](#)（接続されているストレージノード上）。

作業を開始する前に

- 使用することができます Passwords.txt ファイル。
- これで完了です "[特定のアクセス権限](#)"。

#### このタスクについて

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た場合は、以下のトラブルシューティングのガイドラインに従ってください。

- 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グリッドマネージャにサインインしてみます。
  - 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\*、\*サポート\*の各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つしかない場合や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確認します。
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、この手順を参照してください "[シングルサインオンを設定しています](#)"。

問題を解決するには、1つの管理ノードのSSOを一時的に無効にしてから再度有効にする必要があります。



SSOが有効になっている場合は、制限されたポートを使用してサインオンできません。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テッドユーザに属しているかどうかを確認します。

フェデレーテッドユーザアカウントが機能していない場合は、rootなどのローカルユーザとして Grid Manager にサインインしてみてください。

- ローカルユーザがサインインできる場合は、次の手順を実行します。
  - i. 表示されているアラームを確認します。
  - ii. [\* configuration] \* > [\* Access Control] \* > [\* Identity federation] を選択します。
  - iii. [接続のテスト \*] をクリックして、LDAP サーバーの接続設定を確認します。
  - iv. テストに失敗した場合は、設定エラーを解決します。

- ローカルユーザがサインインできず、クレデンシャルが正しいことが確実な場合は、次の手順に進みます。

6. Secure Shell (SSH) を使用して管理ノードにログインします。

- 次のコマンドを入力します。 `ssh admin@Admin_Node_IP`
- に記載されているパスワードを入力します `Passwords.txt` ファイル。
- 次のコマンドを入力してrootに切り替えます。 `su -`
- に記載されているパスワードを入力します `Passwords.txt` ファイル。

rootとしてログインすると、プロンプトがから変わります \$ 終了: #。

7. グリッドノード上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 の各 API サービスがすべて実行されていることを確認します。

出力は、サービスのステータスが変わると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サービスが実行されていることを確認します # `service nginx-gw status`

9. `[[use_Lumberjack_to_collect_logs、start=9]]` Lumberjackを使用してログを収集します。 # `/usr/local/sbin/lumberjack.rb`

過去に認証に失敗したことがある場合は、`--start` および `--end` Lumberjack スクリプトオプションを使用して適切な期間を指定します。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。

ログアーカイブがコピーされた場所がターミナル画面に出力されます。

10. `[[review_logs,start=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. 管理ノードで問題を特定できなかった場合は、次のいずれかのコマンドを問題 で実行し、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
```

```
# vi /var/local/gpt-data/specs/grid.xml
```

管理ノードは認証プロセスで ADC サービスを使用します。

12. 特定した IP アドレスを使用して、管理ノードから各 ADC ストレージ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@grid_node_IP`
- b. に記載されているパスワードを入力します Passwords.txt ファイル。
- c. 次のコマンドを入力してrootに切り替えます。 `su -`
- d. に記載されているパスワードを入力します Passwords.txt ファイル。

rootとしてログインすると、プロンプトがから変わります \$ 終了: #。

13. グリッドノード上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、および Cassandra のサービスがすべて実行されていることを確認します。

14. 手順を繰り返します [Lumberjack を使用してログを収集します](#) および [ログを確認します](#) をクリックしてストレージノード上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送信します。も参照してください "[ログファイル参照](#)"。

ユーザインターフェイスに問題があります

StorageGRID ソフトウェアのアップグレード後に、Grid ManagerまたはTenant Managerのユーザインターフェイスが想定どおりに応答しないことがあります。

手順

1. を使用していることを確認します "[サポートされている Web ブラウザ](#)"。



サポートされるブラウザは、StorageGRID のリリースごとに変更される場合があります。使用しているStorageGRID のバージョンでサポートされているブラウザを使用していることを確認します。

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。

使用できない管理ノードです

StorageGRID システムに複数の管理ノードが含まれている場合、使用できない管理ノードのステータスを別の管理ノードから確認できます。

作業を開始する前に

これで完了です "[特定のアクセス権限](#)"。

手順

1. 使用可能な管理ノードから、を使用して Grid Manager にサインインします "[サポートされている Web ブラウザ](#)"。
2. サポート \* > \* ツール \* > \* グリッドトポロジ \* を選択します。
3. [[site>](#)] > [**Unavailable Admin Node**] > [\* SSM\*] > [\* Services] \* [\* Overview\*] > [\* Main\*] を選択します。
4. ステータスが「Not Running」で、青で表示されているサービスがないかどうかを確認します。



## Overview: SSM (MM-10-224-4-81-ADM1) - Services

Updated: 2017-01-27 11:52:51 EST

Operating System: Linux  
3.16.0-4-amd64

### Services

Service	Version	Status	Threads	Load	Memory
Audit Management System (AMS)	10.4.0-20170113.2207.3ec2cd0	Running	52	0.043 %	35.7 MB
CIFS Filesharing (nmbd)	2:4.2.14+dfsg-0+deb8u2	Running	1	0 %	5.5 MB
CIFS Filesharing (smbd)	2:4.2.14+dfsg-0+deb8u2	Running	1	0 %	14.5 MB
CIFS Filesharing (winbindd)	2:4.2.14+dfsg-0+deb8u2	Not Running	0	0 %	0 B
Configuration Management Node (CMN)	10.4.0-20170113.2207.3ec2cd0	Running	52	0.055 %	41.3 MB
Database Engine	5.5.53-0+deb8u1	Running	47	0.354 %	1.33 GB
Grid Deployment Utility Server	10.4.0-20170112.2125.c4253bb	Running	3	0 %	32.8 MB
Management Application Program Interface (mgmt-api)	10.4.0-20170113.2136.07c4997	Not Running	0	0 %	0 B
NFS Filesharing	10.4.0-20161224.0333.803cd91	Not Running	0	0 %	0 B
NMS Data Cleanup	10.4.0-20161224.0333.803cd91	Running	22	0.008 %	52.4 MB
NMS Data Downsampler 1	10.4.0-20161224.0333.803cd91	Running	22	0.049 %	195 MB
NMS Data Downsampler 2	10.4.0-20161224.0333.803cd91	Running	22	0.009 %	157 MB
NMS Processing Engine	10.4.0-20161224.0333.803cd91	Running	40	0.132 %	200 MB

- アラームがトリガーされているかどうかを確認します。
- 適切な方法で問題を解決します。

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をトラブルシューティングする

ここでは、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のに役立ついくつかのタスクを紹介します。

#### "422: Unprocessable Entity"エラー

エラー422: Unprocessable Entity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調べて、問題の原因を特定します。

表示されたいずれかのエラーメッセージが表示された場合は、推奨される対処方法を実行してください。

エラーメッセージです	ルート原因 および対処方法
<pre>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</pre>	<p>このメッセージは、Windows Active Directory (AD) を使用してアイデンティティフェデレーションを設定するときに、Transport Layer Security (TLS) で「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。</p> <p>LDAP 署名を強制する AD サーバでは、「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。STARTTLS を使用する * オプションまたは TLS に 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。</p>
<pre>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)</pre>	<p>このメッセージは、サポートされない暗号を使用して、StorageGRID からフェデレーションまたはクラウドストレージプールの識別に使用する外部システムへの Transport Layer Security (TLS) 接続を試みた場合に表示されます。</p> <p>外部システムで提供されている暗号を確認します。システムでは、のいずれかを使用する必要があります <b>"StorageGRID でサポートされている暗号"</b> StorageGRID の管理手順を参照してください。</p>

### グリッドネットワーク MTU mismatch アラート

グリッドネットワークインターフェイス (eth0) の最大伝送ユニット (MTU) 設定がグリッド内のノード間で大きく異なる場合に、\* Grid Network MTU mismatch \* アラートがトリガーされます。

#### このタスクについて

MTU 設定の違いから、eth0 ネットワークの一部がジャンボフレーム用に設定されているが、すべてではないことがわかります。MTU サイズが 1000 を超えると、原因の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. すべてのノードの eth0 についての MTU 設定を表示します。
  - Grid Manager に用意されているクエリを使用する。
  - に移動します `primary Admin Node IP address/metrics/graph` をクリックし、次のクエリを入力します。 `node_network_mtu_bytes{device="eth0"}`
2. "MTUの設定を変更します" 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) で同じにする必要があります。
  - Linuxベースおよび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：Linuxベースのノードでは、コンテナのネットワークに必要なMTU値がホストインターフェイスですで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イスを設定して必要なMTU値を設定し、を使用する必要があります `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。

位置指定引数	説明
mtu	設定する MTU。1280 ~ 9216 の範囲内にある必要があります。
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 つ以上指定します。 <ul style="list-style-type: none"><li>• グリッド (Grid)</li><li>• 管理</li><li>• クライアント</li></ul>

+

オプションの引数	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。

## Network Receive Error (NRER) アラーム

ネットワーク受信エラー (NRER) アラームは、StorageGRID とネットワークハードウェア間の接続の問題が原因で発生することがあります。場合によっては、NRER エラーが手動操作なしでクリアされることがあります。エラーがクリアされない場合は、推奨される対処方法を実行します。

このタスクについて

NRER アラームは、StorageGRID に接続するネットワークハードウェアに関する次の問題が原因で発生する可能性があります。

- Forward Error Correction (FEC; 前方誤り訂正) が必要で、使用されていません
- スイッチポートと NIC の MTU が一致しません
- リンクエラー率が高くなっています
- NIC リングバッファオーバーラン

#### 手順

1. ネットワーク設定によっては、NRER アラームの潜在的な原因に対処するためのトラブルシューティング手順を実行してください。
2. エラーの原因に応じて、次の手順を実行します。

## FECが一致しません



これらの手順は、StorageGRID アプライアンスでFEC不一致が原因で発生したNRER エラー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へのケーブルの物理的な整合性をチェックしてください。
- c. NRERアラームを解決するためにFEC設定を変更する場合は、まずStorageGRID アプライアンスインストーラの[Link Configuration]ページで、アプライアンスが\* Auto \*モードに設定されていることを確認します（使用しているアプライアンスの手順を参照してください）。
  - "SG6160"
  - "SGF6112を参照してください"
  - "SG6000を使用します"
  - "SG5800"
  - "SG5700"
  - "SG110およびSG1100"
  - "SG100およびSG1000"
- d. スイッチポートのFEC設定を変更します。StorageGRID アプライアンスのポートは、可能であれば、FEC 設定を調整して一致させます。

StorageGRID アプライアンスではFECを設定できません。アプライアンスは、接続先のスイッチポートで FEC 設定を検出し、ミラーリングしようとしています。リンクが 25GbE または 100GbE のネットワーク速度に強制的に設定されている場合、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「no-FEC」モードに戻ります。FECが有効になっていない場合、接続は電氣的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、NO FECに加えて、Firecode (FC) FECとReed Solomon (RS) FECをサポートしています。

## スイッチポートと NIC の MTU が一致しません

エラー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てください。

ノードに設定されている MTU サイズは、その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場合があります。StorageGRID ノードが MTU より大きいイーサネットフレームを受信すると、この設定では NRER アラームが報告される場合があります。このような状況が発生していると思われる場合は、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 に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 をスイッチポートに合わせて変更します。MTU の目的または要件に応じて変更します。



ネットワークのパフォーマンスを最大限に高めるには、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 MTU 値がほぼ同じになるように設定する必要があります。個々のノード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は、\* Grid Network MTU mismatch \* 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。を参照してください [Grid Network MTU mismatch アラートのトラブルシューティングを行います](#) を参照してください。



も参照してください "[MTU 設定を変更します](#)".

リンクエラー率が高くなっています

- a. まだイネーブルになっていない場合は、FEC をイネーブル
- b. ネットワークケーブルの品質が良好で、損傷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場合は、テクニカルサポートにお問い合わせください。



電氣的ノイズが大きい環境では、エラー率が高くなることがあります。

**NIC** リングバッファオーバーラン

エラーが NIC リングの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連絡してください。

StorageGRID システムが過負荷になっていて、ネットワークイベントをタイムリーに処理できない場合、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. 原因となっている問題を解決したら、エラーカウンタをリセットします。
  - a. サポート \* > ツール \* > グリッドトポロジ \* を選択します。
  - b. \_site \* > \_grid node\_name > SSM \* > Resources \* > Configuration \* > Main \* を選択します。
  - c. [\* 受信エラーカウントをリセットする \*] を選択し、[\* 変更を適用する \*] をクリックします。

関連情報

"[アラーム一覧 \(従来のシステム\)](#)"

時刻同期エラー

グリッドで時刻の同期に関する問題が発生する可能性があります。

時刻の同期の問題が発生する場合は、少なくとも 4 つの外部 NTP ソースが指定されており、それぞれ Stratum 3 以上であることを確認します。それらのすべての外部 NTP ソースが正常に動作しており、StorageGRID のノードからアクセスできることを確認する必要があります。



いつ "[外部NTPソースの指定](#)" 本番レベルのStorageGRID インストールの場合は、Windows Server 2016より前のバージョンのWindowsでWindows Time (W32Time)サービスを使用しないでください。以前のバージョンのWindowsのタイムサービスは精度が十分でないため、StorageGRID などの高精度環境での使用はMicrosoftで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 アドレスのクローニング

ネットワークの問題は、MAC アドレスのクローニングを使用して解決できる場合があります。仮想ホストを使用している場合は、各ネットワークの MAC アドレスクローニングキーの値をノード構成ファイルで「true」に設定します。この設定により、StorageGRID コンテナの MAC アドレスがホストの 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、の手順を参照してください "[Red Hat Enterprise Linux の場合](#)" または "[Ubuntu または Debian](#)"。



Linux ホスト OS で使用する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 原因 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、ホスト OS が到達不能になることがあります。

MACクローニングのイネーブル化の詳細については、の手順を参照してください "[Red Hat Enterprise Linux の場合](#)" または "[Ubuntu または Debian](#)"。

プロミスキャスモードです

MACアドレスクローニングを使用せず、ハイパーバイザーによって割り当てられたMACアドレス以外のMACアドレスのデータをすべてのインターフェイスで送受信できるようにする場合は、[Promiscuous Mode]、[MAC Address Changes]、および[Forged Transmits]で、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[Accept]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できるため、両方のレベル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方法の詳細については、の手順を参照してください "[Red Hat Enterprise Linux の場合](#)" または "[Ubuntu または Debian](#)"。

## Linux : ノードのステータスが「orphaned」になっている

orphaned 状態の Linux ノードは、通常、StorageGRID サービスまたはノードのコンテナを制御しているStorageGRID ノードデーモンが予期せず停止したことを示しています。

このタスクについて

Linux ノードが orphaned 状態になった場合は、次のように対応策を実行してください。

- ログでエラーとメッセージを確認します。
- ノードを再起動してみます。
- 必要に応じて、コンテナエンジンの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 orphaned 状態のノードの両方のログを調べ、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. ホストに root としてログインするか、sudo 権限を持つアカウントを使ってログインします。

3. 次のコマンドを実行して、ノードの再起動を試行します。 `$ 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、コンテナエンジンおよび StorageGRID ノードを制御しているすべてのプロセスを停止します。例：`sudo docker stop --time secondscontainer-name`

の場合 `seconds` で、コンテナの停止を待機する秒数を入力します（通常は15分以下）。例：

```
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を行います

Linux ホストに StorageGRID ノードをインストールしていて、IPv6 アドレスが想定どおりにノードコンテナに割り当てられていない場合は、カーネルでの IPv6 サポートの有効化が必要となることがあります。

このタスクについて

Grid Manager の次の場所で、グリッドノードに割り当てられている IPv6 アドレスを確認できます。

- ノードを選択し、ノードを選択します。次に、[概要] タブの [\* IP アドレス \* の横にある [さらに \* 表示] を選択します。

**DC1-S2 (Storage Node)**

Overview Hardware Network Storage Objects ILM Tasks

**Node information**

Name: DC1-S2  
 Type: Storage Node  
 ID: 352bd978-ff3e-45c5-aac1-24c7278206fa  
 Connection state: ✔ Connected  
 Storage used: Object data 0%  
 Object metadata 0%  
 Software version: 11.6.0 (build 20210924.1557.00a5eb9)  
 IP addresses: 172.16.1.227 - eth0 (Grid Network)  
 10.224.1.227 - eth1 (Admin Network)  
[Hide additional IP addresses](#)

Interface	IP address
eth0 (Grid Network)	172.16.1.227
eth0 (Grid Network)	fd20:328:328:0:250:56ff:fe87:b532

- サポート \* > ツール \* > グリッドトポロジ \* を選択します。次に、 \* Node \* > SSM \* > Resources \* を選択します。IPv6 アドレスが割り当てられている場合は、「 \* ネットワークアドレス \* 」セクションの IPv4 アドレスの下に表示されます。

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. ホストに root としてログインするか、sudo 権限を持つアカウントを使ってログインします。
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 になります。

```
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で変更方法を確認してください。 `sysctl` 設定：次に進む前に、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でない場合、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行を探して、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** サーバのトラブルシューティングを行います

次の表に、を使用した外部syslogサーバに関するエラーメッセージと対処方法を示します。

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 サーバの転送エラーです](#)"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。

外部syslogサーバへの監査情報の送信の詳細については、次の項を参照してください。

- "[外部syslogサーバを使用する場合の考慮事項](#)"
- "[監査メッセージと外部syslogサーバの設定](#)"

エラーメッセージです	概要 および推奨される対処方法
ホスト名を解決できません	<p>syslog サーバに対して入力した FQDN を IP アドレスに解決できませんでした。</p> <ol style="list-style-type: none"><li>1. 入力したホスト名を確認します。IPアドレスを入力した場合は、W.X.Y.Z（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。</li><li>2. DNS サーバが正しく設定されていることを確認します。</li><li>3. 各ノードから DNS サーバの IP アドレスにアクセスできることを確認します。</li></ol>
接続が拒否されました	<p>syslog サーバへの TCP または TLS 接続が拒否されました。ホストの TCP ポートまたは TLS ポートをリ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。</p> <ol style="list-style-type: none"><li>1. 入力した syslog サーバの FQDN または IP アドレス、ポート、およびプロトコルが正しいことを確認してください。</li><li>2. syslog サービスのホストが、指定したポートをリスンしている syslog デモンを実行していることを確認します。</li><li>3. ファイアウォールがノードから syslog サーバの 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。</li></ol>
ネットワークに到達できません	<p>syslog サーバは直接接続されたサブネット上にはありません。ルータが、リストされたノードから syslog サーバにテストメッセージを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。</p> <ol style="list-style-type: none"><li>1. syslog サーバの正しい FQDN または IP アドレスが入力されていることを確認してください。</li><li>2. 表示された各ノードについて、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。想定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）を介してトラフィックが syslog サーバにルーティングされるように設定されていることを確認します。</li></ol>

エラーメッセージです	概要 および推奨される対処方法
ホストに到達できません	<p>syslog サーバは直接接続されたサブネット上にあります（表示されたノードのグリッド IP、管理 IP、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）。ノードはテストメッセージを送信しようとしたが、syslog サーバの 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。</p> <ol style="list-style-type: none"> <li>1. syslog サーバの正しい FQDN または IP アドレスが入力されていることを確認してください。</li> <li>2. syslog サービスを実行しているホストが稼働していることを確認します。</li> </ol>
接続がタイムアウトしました	<p>TCP / TLS 接続が試行されましたが、syslog サーバからの応答が長時間受信されませんでした。ルーティングが正しく設定されていないか、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）。</p> <ol style="list-style-type: none"> <li>1. syslog サーバの正しい FQDN または IP アドレスが入力されていることを確認してください。</li> <li>2. 表示された各ノードについて、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サーバに到達する予定のネットワークインターフェイスおよびゲートウェイ（グリッド、管理、またはクライアント）を使用して、トラフィックがsyslogサーバにルーティングされるように設定されていることを確認します。</li> <li>3. ファイアウォールによって syslog サーバの IP とポートにリストされているノードからの TCP / TLS 接続へのアクセスがブロックされていないことを確認します。</li> </ol>
パートナーによる接続が切断されました	<p>syslog サーバへの 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あります。</p> <ul style="list-style-type: none"> <li>• syslog サーバが再起動またはリブートされた可能性があります。</li> <li>• ノードと syslog サーバで TCP / TLS 設定が異なる場合があります。</li> <li>• 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。</li> <li>• syslog サーバのポートをリスンしている非 syslog サーバが接続を閉じた可能性があります。</li> </ul> <p>この問題を解決するには：</p> <ol style="list-style-type: none"> <li>1. 入力した syslog サーバの FQDN または IP アドレス、ポート、およびプロトコルが正しいことを確認してください。</li> <li>2. TLS を使用している場合は、syslog サーバでも TLS が使用されていることを確認します。TCP を使用している場合は、syslog サーバも TCP を使用していることを確認します。</li> <li>3. アイドル状態の TCP 接続を閉じるように中間ファイアウォールが設定されていないことを確認します。</li> </ol>

エラーメッセージです	概要 および推奨される対処方法
TLS 証明書エラーです	<p>syslog サーバから受信したサーバ証明書が、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でした。</p> <ol style="list-style-type: none"> <li>1. CA 証明書バンドルおよびクライアント証明書（存在する場合）が syslog サーバ上のサーバ証明書と互換性があることを確認します。</li> <li>2. syslog サーバのサーバ証明書に想定される IP 値または FQDN 値が含まれていることを確認します。</li> </ol>
転送が中断されました	<p>syslog レコードが syslog サーバに転送されなくなり、StorageGRID が原因を検出できなくなりました。</p> <p>このエラーが表示されたデバッグログを確認して、ルート原因 を特定します。</p>
TLS セッションが終了しました	<p>syslog サーバが TLS セッションを終了し、StorageGRID が原因を検出できません。</p> <ol style="list-style-type: none"> <li>1. このエラーが表示されたデバッグログを確認して、ルート原因 を特定します。</li> <li>2. 入力した syslog サーバの FQDN または IP アドレス、ポート、およびプロトコルが正しいことを確認してください。</li> <li>3. TLS を使用している場合は、syslog サーバでも TLS が使用されていることを確認します。TCP を使用している場合は、syslog サーバも TCP を使用していることを確認します。</li> <li>4. CA 証明書バンドルおよびクライアント証明書（存在する場合）が syslog サーバのサーバ証明書と互換性があることを確認します。</li> <li>5. syslog サーバのサーバ証明書に想定される IP 値または FQDN 値が含まれていることを確認します。</li> </ol>
結果の照会に失敗しました	<p>syslog サーバの設定およびテストに使用されている管理ノードが、表示されているノードにテスト結果を要求できません。1 つ以上のノードが停止している可能性があります。</p> <ol style="list-style-type: none"> <li>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、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。</li> <li>2. 表示されたノードで miscd サービスを再起動します。</li> </ol>

## 監査ログを確認します

### 監査ログの確認：概要

ここでは、StorageGRID 監査メッセージおよび監査ログの構造と内容について説明します。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判読し、分析できます。

ここに記載する手順は、システムのアクティビティおよび使用状況のレポート生成を担当する管理者を対象としています。このようなレポートの生成には、StorageGRID システムの監査メッセージの分析が必要となります。

テキストログファイルを使用するには、管理ノード上に設定されている監査共有へのアクセスが必要です。

監査メッセージレベルの設定および外部syslogサーバの使用については、を参照してください ["監査メッセージとログの送信先を設定します"](#)。

## 監査メッセージのフローと保持

すべての StorageGRID サービスは通常のシステム運用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 システムからどのように転送されるかを理解しておく必要があります `audit.log` ファイル。

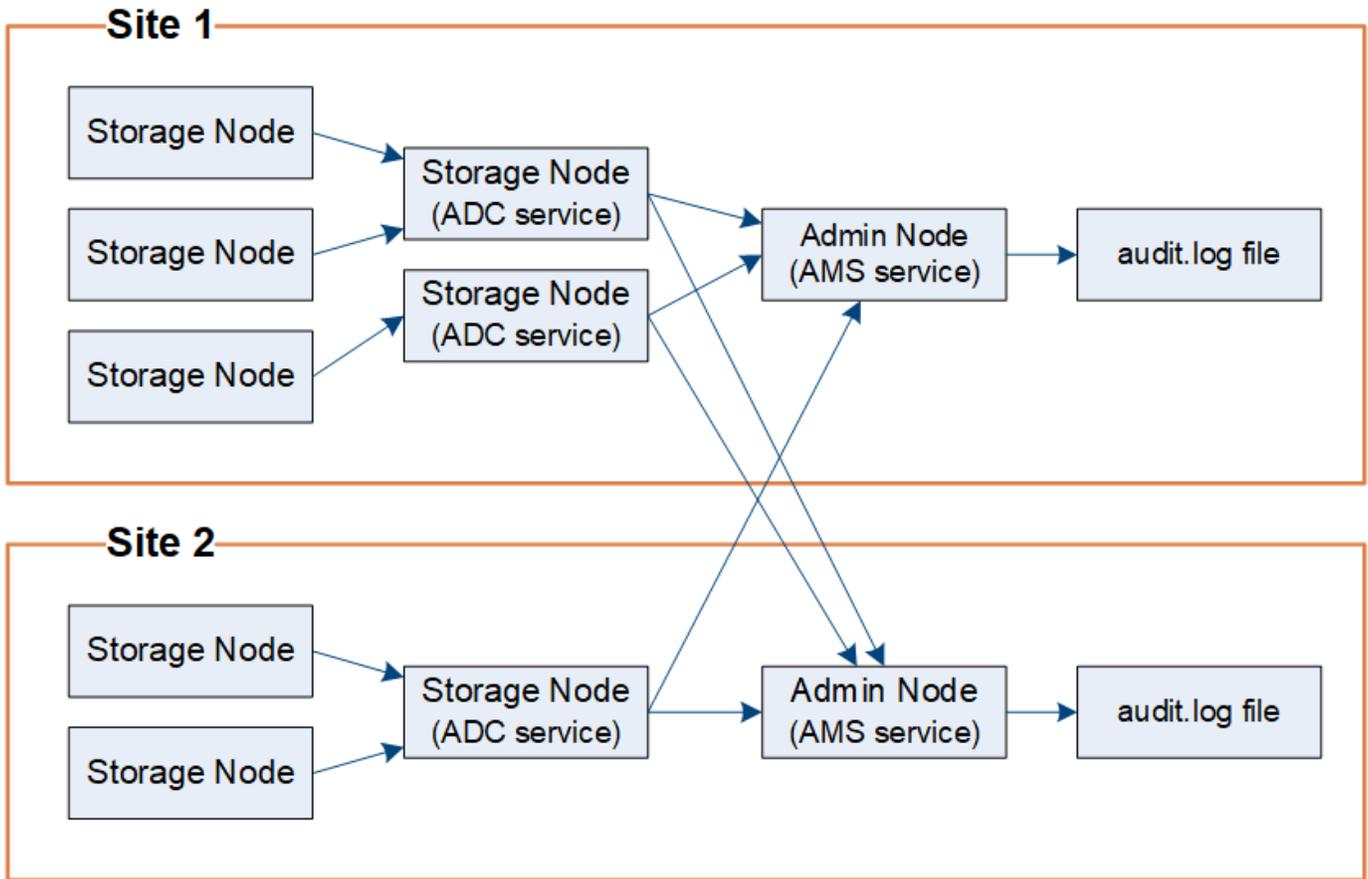
### 監査メッセージのフロー

監査メッセージは、管理ノードおよび Administrative Domain Controller (ADC) サービスが用意されているストレージノードによって処理されます。

監査メッセージのフロー図に示すように、各 StorageGRID ノードは監査メッセージをデータセンターサイトにあるいずれかの ADC サービスに送信します。ADC サービスは、各サイトに設置されている最初の 3 つのストレージノードで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、監査メッセージの集合を 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、システムアクティビティの完全な記録が各管理ノードに提供されます。

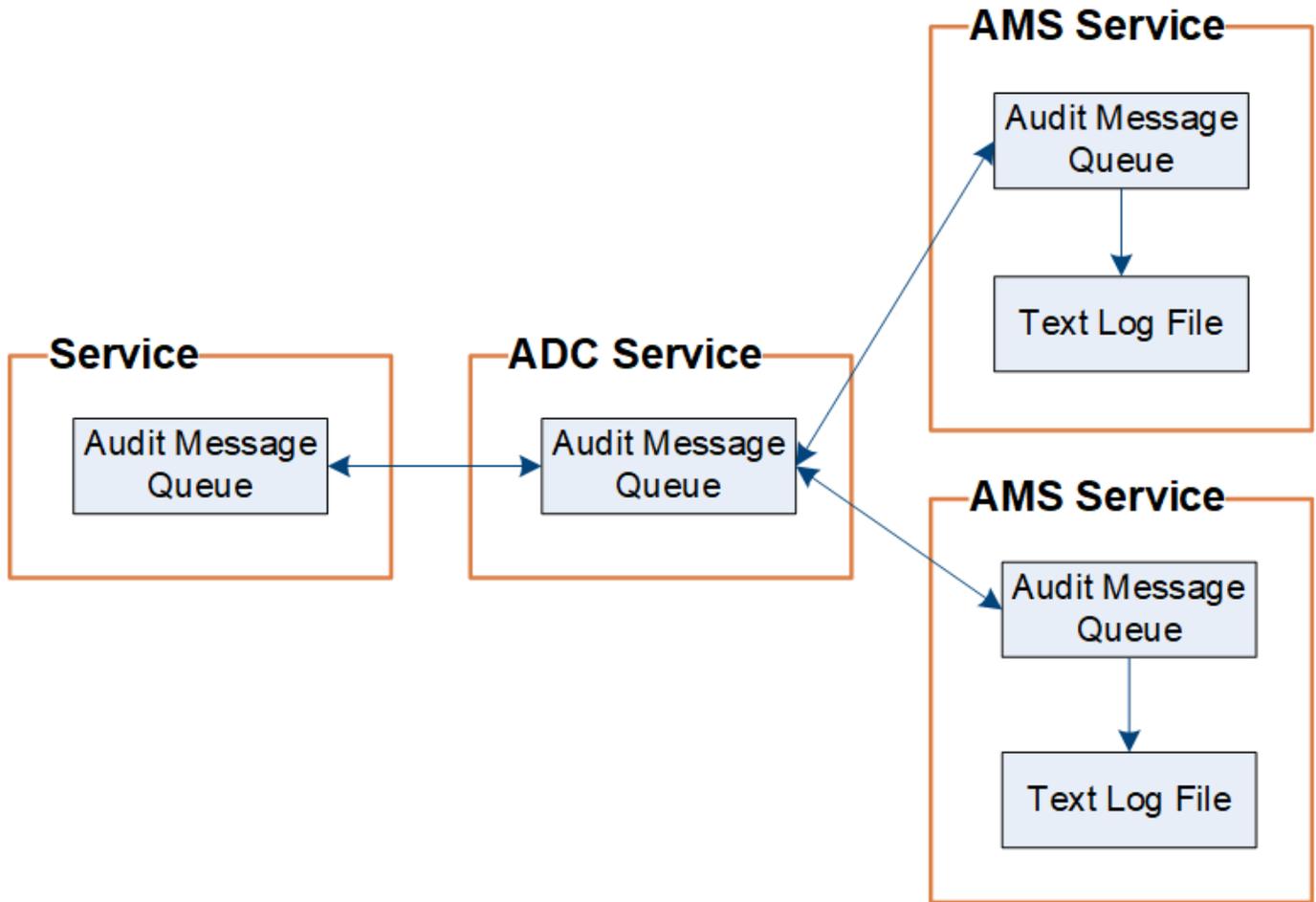
各管理ノードでは、監査メッセージがテキストログファイルに保存されます。アクティブなログファイルの名前は `audit.log`。



#### 監査メッセージの保持

StorageGRID では、コピー / 削除プロセスを使用して、監査ログに書き込まれる前に監査メッセージが失われないようにします。

ノードが生成またはリレーした監査メッセージは、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。メッセージが管理ノード内の監査ログファイルに書き込まれるまで、メッセージのコピーは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、監査メッセージが転送中に失われることはありません。



ネットワーク接続の問題または監査容量の不足が原因で、監査メッセージキューが一時的に増加する可能性があります。キューが増加すると、各ノードの使用可能スペースがキューによってさらに消費されます `/var/local/` ディレクトリ。問題が解除されず、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、個々のノードがバックログの処理の優先順位を設定し、一時的に新しいメッセージに使用できなくなります。

具体的には、次のような動作が発生することがあります。

- 状況に応じて `/var/local/log` 管理ノードで使用されるディレクトリがいっぱいになると、ディレクトリに空きが出るまでその管理ノードを新しい監査メッセージに使用できないことを示すフラグが設定されます。S3およびSwiftクライアント要求には影響しません。監査リポジトリにアクセスできない場合に XAMS ( Unreachable Audit Repositories ) アラームがトリガーされます。
- 状況に応じて `/var/local/` ADCサービスを採用するストレージノードで使用されるディレクトリが92%フルになると、ディレクトリが87%フルになるまでそのノードを監査メッセージに使用できないことを示すフラグが設定されます。他のノードへのS3およびSwiftクライアント要求には影響しません。監査リレーにアクセスできない場合に NRLY ( Available Audit Relays ) アラームがトリガーされます。



ADCサービスを使用する使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のに格納します `/var/local/log/localaudit.log` ファイル。

- 状況に応じて `/var/local/` ストレージノードで使用されるディレクトリが85%フルになると、ノードはS3およびSwiftクライアントの要求を拒否し始めます `503 Service Unavailable`。

原因 監査メッセージキューが大幅に増加すると、次のような問題が発生する可能性があります。

- 管理ノードまたは ADC サービスを採用するストレージノードの停止。システムのいずれかのノードが停止すると、残りのノードはバックログ状態になる可能性があります。
- システムの監査キャパシティを超えるアクティビティ率の継続。
- `/var/local/` 監査メッセージには関連のない理由で ADC ストレージノード上のスペースがいっぱいになる。この場合、ノードは新しい監査メッセージの受け入れを停止し、現在のバックログの優先順位を設定します。これにより、他のノードで原因 バックログが発生する可能性があります。

#### Large audit queue アラートと Audit Messages Queued (AMQS) アラーム

時間の経過に伴う監査メッセージキューのサイズを監視できるように、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の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。

「`Large audit queue *`」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、最初にシステムの負荷を確認します。最近のトランザクションの数が膨大であった場合は、アラートとアラームは時間が経過すると解決するため、無視してかまいません。

アラートまたはアラームが解決せず重大度が上がった場合は、キューサイズのグラフを確認します。数時間から数日にわたって数値が増え続けている場合は、監査の負荷がシステムの監査キャパシティを超えている可能性があります。クライアントの書き込みとクライアントの読み取りでエラーまたはオフの監査レベルを変更して、クライアントの処理速度を下げるか、ログに記録される監査メッセージの数を減らしてください。を参照してください ["監査メッセージとログの送信先を設定します"](#)。

重複メッセージです

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。そのため、監査ログでメッセージが重複する可能性があります。

### 監査ログファイルにアクセスします

監査共有にはアクティブなが含まれています `audit.log` ファイルおよび圧縮された監査ログファイル。監査ログファイルには、管理ノードのコマンドラインから直接アクセスできます。

作業を開始する前に

- これで完了です ["特定のアクセス権限"](#)。
- を用意しておく必要があります `Passwords.txt` ファイル。
- 管理ノードの IP アドレスを確認し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. に記載されているパスワードを入力します `Passwords.txt` ファイル。
  - c. 次のコマンドを入力して root に切り替えます。 `su -`
  - d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

rootとしてログインすると、プロンプトがから変わります \$ 終了: #。

2. 監査ログファイルが保存さ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に保存されます /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、監査ログのデスティネーションを変更したり、監査情報を外部 syslog サーバに送信したりできます。外部 syslog サーバが設定されても、監査レコードのローカルログは引き続き生成および格納されます。を参照してください ["監査メッセージとログの送信先を設定します"](#)。

1日に1回、アクティブな `audit.log` ファイルが保存され、新しいファイルが作成されます `audit.log` ファイルが開始されました。保存されたファイルの名前は、保存された日時をの形式で示しています `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と番号が付加された日付が使用されます `yyyy-mm-dd.txt.n`。例: `2018-04-15.txt` および `2018-04-15.txt.1` 2018年4月15日に作成および保存された1つ目のログファイルおよび2つ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、という形式で名前が変更されます `yyyy-mm-dd.txt.gz` 元の日付を保持します。そのため、時間の経過とともに、管理ノード上の監査ログ用に割り当てられたストレージが消費されます。スクリプトによって監査ログのスペース消費が監視され、のスペースを解放するために、必要に応じてログファイルが削除されます `/var/local/log` ディレクトリ。監査ログは、作成日に基づいて、古い順に削除されます。スクリプトの処理は、次のファイルで監視できます。 `/var/local/log/manage-audit.log`。

この例は、アクティブを示しています `audit.log` ファイル。前日のファイルです (`2018-04-15.txt`)、および前日の圧縮ファイルです (`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: 概要

監査ログファイルはすべての管理ノードに存在し、一連の監査メッセージが格納されています。

各監査メッセージには次の情報が含まれます。

- 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 形式で表した値

と、末尾のスペース。

YYYY-MM-DDTHH:MM:SS.UUUUUU、ここで UUUUUU はマイクロ秒です。

- 監査メッセージ。全体が角かっこで囲まれ、で始まる 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しています）。これらのメッセージは、テナントが S3 バケットを作成し、オブジェクトを 2 つバケットに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][SAIP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWnt-PhoTDwB9Jok7PtyLkQmA="][SUSR(CSTR):"urn:sgws:identity::17530064241597054718:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"bucket1"][AVER(UI32):10][ATIM(UI64):1565203410247711]
[ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):7074142142472611085]]
```

```
2019-08-07T18:43:30.783597
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991696][TIME(UI64):120713][SAIP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWnt-PhoTDwB9Jok7PtyLkQmA="][SUSR(CSTR):"urn:sgws:identity::17530064241597054718:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"bucket1"][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(FC32):S3RQ][ATID(UI64):8439606722108456022]]
```

```
2019-08-07T18:43:30.784558
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991693][TIME(UI64):121666][SAIP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWnt-PhoTDwB9Jok7PtyLkQmA="][SUSR(CSTR):"urn:sgws:identity::17530064241597054718:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"bucket1"][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(FC32):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の読みやすさや解釈が容易ではありません。を使用できます "audit-explainツール" を使用して、監査ログ内の監査メッセージの簡単な概要を取得します。を使用できます "audit-sumツール" ログに記録された書き込み、読み取り、削除の各処理の所要時間をまとめます。

**audit-explain** ツールを使用してください

を使用できます `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。

作業を開始する前に

- これで完了です "特定のアクセス権限"。
- を用意しておく必要があります `Passwords.txt` ファイル。
- プライマリ管理ノードの IP アドレスを確認しておく必要があります。

このタスクについて

。 `audit-explain` ツールはプライマリ管理ノードで使用でき、監査ログ内の監査メッセージの簡単な概要を取得できます。



。 `audit-explain` ツールは、主にトラブルシューティング処理の際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。処理中です `audit-explain` クエリは大量のCPUパワーを消費する可能性があるため、StorageGRID の処理に影響を及ぼす場合があります。

次の例は、からの一般的な出力を示しています `audit-explain` ツール。この4人 "SPUT" アカウントID が92484777680322627870のS3テナントがS3 PUT要求を使用して「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場合に、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
```

。 `audit-explain` ツールでは次の操作を実行できます。

- プレーンまたは圧縮された監査ログを処理します。例：

```
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：

```
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ます。これにより、を使用して入力をフィルタリングおよび前処理できます。grep コマンドまたはその他の手段。例：

```
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ことがあるため、確認して実行する部分をフィルタリング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、部分的に。



。audit-explain ツールは圧縮ファイルをパイプ付き入力として受け入れません。圧縮ファイル进行处理するには、ファイル名をコマンドライン引数として指定するか、を使用します。zcat 最初にファイルを解凍するツール。例：

```
zcat audit.log.gz | audit-explain
```

を使用します help (-h) 使用可能なオプションを表示するためのオプション。例：

```
$ 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. に記載されているパスワードを入力します Passwords.txt ファイル。
  - c. 次のコマンドを入力してrootに切り替えます。su -
  - d. に記載されているパスワードを入力します Passwords.txt ファイル。

rootとしてログインすると、プロンプトがから変わります \$ 終了： #。

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
```

。audit-explain ツールは、指定されたファイル内のすべてのメッセージを、判読可能な形式に変換して出力します。



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。タイムスタンプを表示するには、タイムスタンプを使用します (-t) をクリックします。

**audit-sum** ツールを使用します

を使用できます audit-sum 書き込み、読み取り、HEAD、削除の各監査メッセージをカウントし、それぞれの処理タイプの最小、最大、平均時間（またはサイズ）を表示するツールです。

作業を開始する前に

- これで完了です "特定のアクセス権限"。
- を用意しておく必要があります Passwords.txt ファイル。
- プライマリ管理ノードの IP アドレスを確認しておく必要があります。

このタスクについて

。 audit-sum ツールはプライマリ管理ノードで使用でき、ログに記録された書き込み、読み取り、削除の処理数と、それらの処理に要した時間を取得できます。



。 audit-sum ツールは、主にトラブルシューティング処理の際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。処理中です audit-sum クエリは大量のCPUパワーを消費する可能性があるため、StorageGRID の処理に影響を及ぼす場合があります。

次の例は、からの一般的な出力を示しています audit-sum ツール。この例は、プロトコル処理に要した時間を示しています。

```
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
```

。 audit-sum 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取得します。

コード	説明	を参照してください
ARCT	アーカイブをクラウド階層から取得します	"ARCT : クラウド階層からアーカイブを取得します"
▽ SCT。 △	アーカイブストア - クラウド階層	"ASCT : アーカイブストアのクラウド階層"
IDEL	ILM Initiated Delete : ILM がオブジェクトを削除する処理を開始すると記録されます。	"IDEL : ILM Initiated Delete"
SDEL	S3 DELETE : オブジェクトまたはバケットを削除するトランザクションの成功をログに記録します。	"SDEL : S3 DELETE"

コード	説明	を参照してください
SGET	S3 GET : バケット内のオブジェクトを読み出しまたはリストアップするトランザクションの成功をログに記録します。	"SGET : S3 GET"
Shea	S3 HEAD : オブジェクトまたはバケットの存在を確認するトランザクションの成功をログに記録します。	"Shea : S3 ヘッド"
SPUT	S3 PUT : オブジェクトまたはバケットを新規に作成するトランザクションの成功をログに記録します。	"SPUT : S3 PUT"
WDEL	Swift DELETE : オブジェクトまたはコンテナを削除するトランザクションの成功をログに記録します。	"WDEL : Swift の削除"
wget	Swift GET : コンテナ内のオブジェクトを読み出しまたはリストアップするトランザクションの成功をログに記録します。	"wget : Swift GET"
WHEA	Swift HEAD : オブジェクトまたはコンテナの存在を確認するトランザクションの成功をログに記録します。	"WHEA : Swift ヘッド"
WPUT	Swift PUT : オブジェクトまたはコンテナを新規に作成するトランザクションの成功をログに記録します。	"WPUT : Swift PUT"

。 audit-sum ツールでは次の操作を実行できます。

- プレーンまたは圧縮された監査ログを処理します。例：

```
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：

```
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ます。これにより、を使用して入力をフィルタリングおよび前処理できます  
grep コマンドまたはその他の手段。例：

```
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、圧縮ファイルをパイプ付き入力として受け入れません。圧縮ファイル进行处理するには、ファイル名をコマンドライン引数として指定するか、を使用します `zcat` 最初にファイルを解凍するツール。例：

```
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して、バケットに対する処理をオブジェクトに対する処理とは別にまとめたり、メッセージの概要をバケット名、期間、ターゲットタイプ別にグループ化したりできます。デフォルトでは、概要には最小、最大、平均の処理時間が表示されますが、を使用することもできます `size (-s)` オブジェクトサイズを表示するオプションです。

を使用します `help (-h)` 使用可能なオプションを表示するためのオプション。例：

```
$ 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. に記載されているパスワードを入力します `Passwords.txt` ファイル。
- c. 次のコマンドを入力してrootに切り替えます。 `su -`
- d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

rootとしてログインすると、プロンプトがから変わります \$ 終了： #。

2. 書き込み、読み取り、HEAD、削除の処理に関連するすべてのメッセージを分析するには、次の手順を実行します。

- 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
```

次の例は、からの一般的な出力を示しています `audit-sum` ツール。この例は、プロトコル処理に要した時間を示しています。

message group average(sec)	count	min(sec)	max(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、平均処理時間では SGET（S3 GET）処理が 1.13 秒と最も長い一方で、最大処理時間では SGET 処理と SPUT（S3 PUT）処理がどちらも約 1、770 秒と一番長くなっています。

- b. 最も時間がかかった読み出し処理を 10 件表示するには、grep コマンドを使用して SGET メッセージのみを選択し、long 出力オプションを追加します (-l) オブジェクトパスを含めるには：

```
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）とパスが含まれます。この情報を使用して、監査ログを grep してこれらのオブジェクトに関連する他のメッセージを出力できます。

```

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/r9010aQ8JB-1566861764-4519.iso
1624414429  10.96.101.125      object  5375001556
backup/r9010aQ8JB-1566861764-6618.iso
1533143793  10.96.101.125      object  5183661466
backup/r9010aQ8JB-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

```

+

この出力例からは、最も時間がかかった 3 個の S3 GET 要求が、他のオブジェクトよりもはるかに大きい約 5GB のオブジェクトに対して実行されたことがわかります。サイズが大きいと、最悪の場合の読み出し時間が長くなります。

3. グリッドに取り込まれているオブジェクトとグリッドから読み出されているオブジェクトのサイズを特定するには、size オプションを使用します (-s) :

```
audit-sum -s audit.log
```

message group average (MB)	count	min (MB)	max (MB)
=====	=====	=====	=====
IDEL 1654.502	274	0.004	5000.000
SDEL 1.695	213371	0.000	10.504
SGET 14.920	201906	0.000	5000.000
SHEA 2.967	22716	0.001	10.504
SPUT 2.495	1771398	0.000	5000.000

この例では、SPUT の平均オブジェクトサイズは 2.5MB 未満ですが、SGET の平均サイズははるかに大きいことがわかります。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読み出されていないことを示しています。

4. 昨日の読み出しに時間がかかっていないかどうかを確認するには、次の手順を実行
  - a. 該当する監査ログに対してコマンドを問題 処理し、group-by-time オプションを使用します (-gt) に続けて期間 (例: 15M、1H、10S) を指定します。

```
grep SGET audit.log | audit-sum -gt 1H
```

message group average(sec)	count	min(sec)	max(sec)
=====	=====	=====	=====
2019-09-05T00 1.254	7591	0.010	1481.867
2019-09-05T01 1.115	4173	0.011	1740.290
2019-09-05T02 1.562	20142	0.011	1274.961
2019-09-05T03 1.254	57591	0.010	1383.867
2019-09-05T04 1.405	124171	0.013	1740.290
2019-09-05T05 1.562	420182	0.021	1274.511
2019-09-05T06 5.562	1220371	0.015	6274.961
2019-09-05T07 2.002	527142	0.011	1974.228
2019-09-05T08 1.105	384173	0.012	1740.290
2019-09-05T09 1.354	27591	0.010	1481.867

上記の結果は、06：00と07：00の間にS3 GETトラフィックが急増したことを示しています。この時間帯は最大時間と平均時間も大幅に長くなっており、データの増加に伴って徐々に長くなっているわけではありません。このことから、ネットワークまたはグリッドによる要求の処理能力のどこかでキャパシティを超えた可能性があります。

- b. どのサイズのオブジェクトが前日に読み出されていたかを1時間単位で確認するには、size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 average (B)	count	min (B)	max (B)
=====	=====	=====	=====
2019-09-05T00 1.976	7591	0.040	1481.867
2019-09-05T01 2.062	4173	0.043	1740.290
2019-09-05T02 2.303	20142	0.083	1274.961
2019-09-05T03 1.182	57591	0.912	1383.867
2019-09-05T04 1.528	124171	0.730	1740.290
2019-09-05T05 2.398	420182	0.875	4274.511
2019-09-05T06 51.328	1220371	0.691	5663711385.961
2019-09-05T07 2.147	527142	0.130	1974.228
2019-09-05T08 1.878	384173	0.625	1740.290
2019-09-05T09 1.354	27591	0.689	1481.867

この結果から、読み出しトラフィックの量が最大に達したときに、非常に大容量の読み出しが発生したことがわかります。

- c. 詳細を確認するには、を使用します **"audit-explainツール"** その時間内のすべてのSGET処理を確認するには、次の手順を実行します。

```
grep 2019-09-05T06 audit.log | grep SGET | audit-explain | less
```

grepコマンドの出力が多く行になると予想される場合は、を追加します less 監査ログファイルの内容を一度に1ページ（1画面）表示するコマンド。

- 5. バケットに対する SPUT 処理にオブジェクトに対する SPUT 処理よりも時間がかかっているかどうかを確認するには、次の手順を実行します。
  - a. 最初にを使用します -go オプション。オブジェクト処理とバケット処理でメッセージをグループ化します。

```
grep SPUT sample.log | audit-sum -go
```

message group	count	min(sec)	max(sec)
SPUT.bucket	1	0.125	0.125
SPUT.object	12	0.025	1.019

上記の結果から、バケットに対する SPUT 処理とオブジェクトに対する SPUT 処理でパフォーマンス特性が異なることがわかります。

- b. SPUT処理に最も時間がかかっているバケットを特定するには、を使用します `-gb` オプション。バケットごとにメッセージをグループ化します。

```
grep SPUT audit.log | audit-sum -gb
```

message group	count	min(sec)	max(sec)
SPUT.cho-non-versioning	71943	0.046	1770.563
SPUT.cho-versioning	54277	0.047	1736.633
SPUT.cho-west-region	80615	0.040	55.557
SPUT.ldt002	1564563	0.011	51.569

- 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、両方を使用します `-gb` および `-s` オプション：

```
grep SPUT audit.log | audit-sum -gb -s
```

message group average (B)	count	min (B)	max (B)
=====	=====	=====	=====
SPUT.cho-non-versioning 21.672	71943	2.097	5000.000
SPUT.cho-versioning 21.120	54277	2.097	5000.000
SPUT.cho-west-region 14.433	80615	2.097	800.000
SPUT.ldt002 0.352	1564563	0.000	999.972

## 監査メッセージの形式

監査メッセージの形式：概要

StorageGRID システム内でやり取りされる監査メッセージには、すべてのメッセージに共通の標準情報と、報告対象のイベントまたはアクティビティを説明する固有のコンテンツが含まれます。

によって提供された概要情報の場合 ["監査-説明する"](#) および ["audit-sumの略"](#) ツールで十分ではありません。すべての監査メッセージの一般的な形式を把握するには、このセクションを参照してください。

以下は、監査ログファイルに記録されてい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(FC32):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):9445736326500603516]]
```

各監査メッセージには、一連の属性要素で構成されます。文字列全体が角かっこで囲まれます ([ ])、および文字列内の各属性要素には、次の特性があります。

- 角かっこで囲まれています [ ]
- 文字列で導入されます `AUDT` を指定します
- 前後に区切り記号（カンマやスペース）がない
- 改行文字で終了します \n

各要素には、次の形式で報告される属性コード、データ型、および値が含まれます。

```
[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ません。

次に、属性要素について説明します。

- ATTR は、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 は、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。タイプはかっこで囲まれます ( )。
- value は属性の内容で、通常は数値またはテキスト値です。値の前には常にコロンが付きます (:)。データ型CStrの値は二重引用符で囲まれます。

## データ型

監査メッセージ内の情報の格納にはさまざまなデータタイプが使用されます。

を入力します	説明
UI32	符号なし長整数（32ビット）。0~4、294、967、295の数値を格納できます。
UI64	符号なし倍精度長整数（64ビット）。0~18、446、744、073、709、551、615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文字で表される32ビットの符号なし整数値です。
iPad	IPアドレスに使用されます。
CSTR	UTF-8文字の可変長配列。文字は次の方法でエスケープできます。 <ul style="list-style-type: none"><li>• バックスラッシュは \。</li><li>• 復帰文字は \r です</li><li>• 二重引用符は \"。</li><li>• 改行（新しい行）は \n です</li><li>• 文字は、それぞれに相当する16進数に置き換えることができます（\xHHの形式、HHは該当する文字を表す16進値）。</li></ul>

## イベント固有のデータ

監査ログ内の各監査メッセージはシステムイベントに固有のデータを記録します。

開口部に続いて [AUDT: メッセージ自体を識別するコンテナ。次の一連の属性は、監査メッセージによって記述されるイベントまたはアクションに関する情報を提供します。以下の例では、これらの属性を強調表示しています。

```
2018-12-05T08:24:45.921845 [AUDT: \[RST\ (FC32) : SUCS\]
\[time\ (UI64):11454\]\[SAIP\ (iPAd):"10.224.0.100"\]\[S3AI\ (CStr):"60025621595611246499"\]
\[SACC\ (CStr):"account"\]\[S3AK\ (CStr):"SGKH4_Nc8SO1H6w3w0nCOFCGK__E6dYzKlumRsKJA
=="\]
\[SUSR\ (CStr) : "urn : sgws : identity : : 60025621595611246499 : root"\]
\[SBAI\ (CStr) : "60025621595611246499"\]\[SBAC\ (CStr) : "account"\]\[S3BK\ (CStr)
: "bucket"\]
\[S3KY\ (CStr) : "object"\]\[CBID\ (UI64) : 0xCC128B9B9E428347\]
\[UID\ (CStr) : "B975D2CE-E4DA-4D14-8A23-1CB4B83F2CD8"\]\[CSIZ\ (UI64) : 30720\]\[aver
(UI32) : 10\]
\[ATIM (UI64) : 1543998285921845\]\[ATYP\ (FC32) : Shea\]\[ANID (UI32) : 12281045\]\[AMID
(FC32) : S3RQ\]
\[ATID (UI64) : 15552417629170647261\]
```

。ATYP 要素（この例では下線付き）は、メッセージを生成したイベントを識別します。このメッセージ例には、が含まれています "Shea" メッセージコード ([ATYP (FC32) : Shea])。S3 HEAD要求が成功し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	を入力します	説明
AMid	FC32	Module 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。
ANID	UI32	Node 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。各サービスには、StorageGRID システムの設定およびインストール時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	Audit Session Identifier : 以前のリリースでは、この要素はサービスの開始後に監査システムが初期化された時間を示していました。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）からのマイクロ秒数で計測されていました。  <ul style="list-style-type: none"> <li>注 : * この要素は廃止され、監査メッセージには表示されなくなりました。</li> </ul>

コード	を入力します	説明
ASQN	UI64	Sequence Count : 以前のリリースでは、このカウンタはグリッドノード (ANID) 上で監査メッセージが生成されるたびに増分し、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、監査メッセージには表示されなくなりました。
ATID	UI64	Trace ID : 1つのイベントによってトリガーされた一連のメッセージで共有される識別子。
ATIM	UI64	Timestamp : 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) からのマイクロ秒数で計測されます。タイムスタンプをローカルの日時に変換するためのツールは、ほとんどがミリ秒に基づいています。  ログに記録されたタイムスタンプの丸めや切り捨てが必要な場合があります。の監査メッセージの先頭に表示される判読可能な時刻 <code>audit.log</code> fileは、ISO 8601形式のATIM属性です。日付と時刻はこの形式で表示されます <code>YYYY-MMDDTHH:MM:SS.UUUUUU</code> を参照してください。`T` は、日付の時間セグメントの先頭を示すリテラル文字です。 <code>UUUUUU</code> はマイクロ秒です。
ATYP	FC32	Event Type : ログに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管理します。
バージョン	UI32	Version : 監査メッセージのバージョン。StorageGRID ソフトウェアのバージョンアップに伴い、新しいバージョンのサービスによって新しい機能が監査レポートに組み込まれる可能性があります。このフィールドは、旧バージョンのサービスのメッセージを処理できるように、AMS サービスにおける下位互換性を可能にします。
RSLT	FC32	Result : イベント、プロセス、またはトランザクションの結果。該当しないメッセージの場合は、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は詳細な情報が含まれています。監査メッセージはすべて同じ形式です。

以下は、に表示される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):"s3small11"][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、記録された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ています。

監査メッセージによって記録されているイベントは、ATYP 属性（以下で強調表示されている部分）で識別します。

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small11"][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。"**SPUT**" S3 PUT トランザクションを表し、バケットへのオブジェクトの取り込みをログに記録します。

次の監査メッセージは、オブジェクトが関連付けられているバケットも示しています。

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK\CSTR\:"s3small11"][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調べるには、監査メッセージの先頭の世界標準時（UTC）のタイムスタンプを確認します。この値は、監査メッセージ自体の ATIM 属性を判読できる形式です。

**2014-07-17T21:17:58.959669**

```
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small11"][S3KY(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):1579224144102530435]]
```

ATIM は、UNIX エポックの開始時点からの時間をマイクロ秒数で記録します。この例では、の値を指定します 1405631878959669 2014年7月17日（木） 21：17：59 UTCに変換されます。

## 監査メッセージとオブジェクトライフサイクル

監査メッセージはいつ生成されますか？

監査メッセージは、オブジェクトの取り込み、読み出し、または削除が行われるたびに生成されます。監査ログでこれらのトランザクションを特定するには、API 固有の（S3 または Swift）監査メッセージを検索します。

監査メッセージは各プロトコルに固有な識別子によってリンクされます。

プロトコル	コード
S3 処理をリンクしています	S3BK（バケット）、S3KY（キー）、またはその両方
Swift 処理をリンクしています	WCON（コンテナ）、WOBJ（オブジェクト）、またはその両方
内部処理をリンクしています	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、オブジェクトサイズ、ネットワーク遅延などの要因により、各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に記載する例とは異なる場合があります。

#### アーカイブノード

アーカイブノードから外部アーカイブストレージシステムにオブジェクトデータを送信するときに生成される一連の監査メッセージは、SCMT（Store Object Commit）メッセージがないことを除き、ストレージノードの場合と似ています。さらに、オブジェクトデータのアーカイブコピーごとに ATCE（Archive Object Store Begin）メッセージと ASCE（Archive Object Store End）メッセージが生成されます。

アーカイブノードが外部のアーカイブストレージシステムからオブジェクトデータを読み出すときに生成される一連の監査メッセージは、ストレージノードの場合と似ていますが、オブジェクトデータのアーカイブコピーごとに ARCB（Archive Object Retrieve Begin）メッセージと ARCE（Archive Object Retrieve End）メ

ッセージが生成される点が異なります。

アーカイブノードが外部のアーカイブストレージシステムからオブジェクトデータを削除するときに生成される一連の監査メッセージは、ストレージノードのメッセージと似ています。ただし、SREM（Object Store Remove）メッセージがなく、削除要求ごとにAREM（Archive Object Remove）メッセージが生成される点が異なります。

### オブジェクトの取り込みトランザクション

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特定するには、API固有の（S3 または Swift）監査メッセージを検索します。

以下の表には、取り込みトランザクション中に生成されたすべての監査メッセージが含まれているわけではなく、取り込みトランザクションをトレースするために必要なメッセージのみが含まれています。

#### S3 の取り込み監査メッセージ

コード	名前	説明	トレース	を参照してください
SPUT	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	"SPUT : S3 PUT"
ORLM の場合	オブジェクトルールを満たしました	このオブジェクトが ILM ポリシーを満たしました。	CBID	"ORLM : オブジェクトルールが満たされています"

#### Swift の取り込み監査メッセージ

コード	名前	説明	トレース	を参照してください
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"
ORLM の場合	オブジェクトルールを満たしました	このオブジェクトが ILM ポリシーを満たしました。	CBID	"ORLM : オブジェクトルールが満たされています"

#### 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 クライアントがストレージノード（LDR サービス）にオブジェクトを取り込んだときに生成され、監査ログに保存された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Make 2 Copies 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たすべての監査メッセージが含まれているわけではなく、S3 取り込みトランザクション（SPUT）に関連するメッセージだけが示されています。

この例では、S3 バケットは以前に作成済みであることを前提としています。

### SPUT : S3 PUT

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 S3 PUT トランザクションが実行されたことを示します。

```
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ています

ORLM メッセージは、このオブジェクトが ILM ポリシーに準拠し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ています。

レプリケート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 が記録されます。

```
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]]
```

イレイジャーコーディングオブジェクトの場合は、LOCS フィールドにイレイジャーコーディングプロファイル ID とイレイジャーコーディンググループ ID が表示されます。

```
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、使用される 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

クトの情報が記録されます。

```
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]]
```

### オブジェクトの削除トランザクション

監査ログでオブジェクトの削除トランザクションを特定するには、API 固有の（S3 および Swift）監査メッセージを検索します。

以下の表には、削除トランザクション中に生成されたすべての監査メッセージが含まれているわけではなく、削除トランザクションをトレースするために必要なメッセージのみが含まれています。

#### S3 の削除監査メッセージ

コード	名前	説明	トレース	を参照してください
SDEL	S3 削除	バケットからのオブジェクトの削除が要求されました。	CBID、S3KY	"SDEL : S3 DELETE"

#### Swift の削除監査メッセージ

コード	名前	説明	トレース	を参照してください
WDEL	Swift の削除	コンテナまたはコンテナからのオブジェクトの削除が要求されました。	CBID、WOBJ	"WDEL : Swift の削除"

#### 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て監査ログに保存されます。



以下の例には、削除トランザクション中に生成されたすべての監査メッセージが含まれているわけではなく、S3 の削除トランザクション（SDEL）に関連するメッセージだけが示されています。

#### 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要求を送信した時点で開始されます。メ

ッセージには、オブジェクトの削除元のバケットと、オブジェクトの識別に使用される 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_5cLflqajtaFmxJn9461AWRJfBF33gAOg=="][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]]
```

### オブジェクトの読み出しトランザクション

監査ログでオブジェクトの読み出しトランザクションを特定するには、API 固有の（ S3 および Swift ） 監査メッセージを検索します。

以下の表には、読み出しトランザクション中に生成されたすべての監査メッセージが含まれているわけではなく、読み出しトランザクションをトレースするために必要なメッセージのみが含まれています。

#### S3 の読み出し監査メッセージ

コード	名前	説明	トレース	を参照してください
SGET	S3 GET	バケットからのオブジェクトの読み出しが要求されました。	CBID、S3BK、S3KY	"SGET : S3 GET"

#### Swift の読み出し監査メッセージ

コード	名前	説明	トレース	を参照してください
wget	Swift GET	コンテナからのオブジェクトの読み出しが要求されました。	CBID、WCON、WOBJ	"wget : Swift GET"

#### 例： S3 オブジェクトの読み出し

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読み出すと、監査メッセージが生成されて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たすべての監査メッセージが含まれているわけではなく、S3 読み出しトランザクション（ SGET ）に関連するメッセージだけが示されています。

#### SGET : S3 GET

オブジェクトの読み出しは、クライアントがLDRサービスにGetObject要求を送信したときに開始されます。

メッセージには、オブジェクトの読み出し元のバケットと、オブジェクトの識別に使用される 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、クライアントはオブジェクトを匿名で読み出したり、別のテナントアカウントが所有しているバケットからオブジェクトを読み出すことができます。監査メッセージには、このような匿名要求およびクロスアカウント要求を追跡できるように、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ます。

次のメッセージ例では、クライアントが所有していないバケットに格納されているオブジェクトに対するGetObject要求を送信しています。SBAI と 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が、これは S3AI および SACC に記録されているクライアントのテナントアカウント ID および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_kBkqSCbTi754Ls81BUog67I2LlSiUg=="][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：オブジェクトの **S3 Select**

S3 クライアントがオブジェクトに対して S3 Select クエリを実行すると、監査メッセージが生成されて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たすべての監査メッセージが含まれているわけではなく、S3 Select トランザクション (SelectObjectContent) に関連するトランザクションのみが表示されます。

各クエリには2つの監査メッセージが生成されます。1つはS3 Select要求の承認を実行するメッセージ (S3SR フィールドが「select」に設定されている) で、もう1つは処理中にストレージからデータを取得する標準のGET処理です。

2021-11-08T15:35:30.750038

```
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636385730715700][TIME(UI64):29173][SAIP(IPAD):"192.168.7.44"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Tenant1636027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:identity::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBACC(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][SAIP(IPAD):"192.168.7.44"][HTRH(CSTR):"{\"x-forwarded-for\": \"unix:\"}"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Tenant1636027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:identity::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBACC(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):10185581][MTME(UI64):1636380348695262][AVER(UI32):10][ATIM(UI64):1636385732604886][ATYP(FC32):SGET][ANID(UI32):12733063][AMID(FC32):S3RQ][ATID(UI64):16562288121152341130]]
```

メタデータの更新メッセージです

S3 クライアントがオブジェクトのメタデータを更新すると、監査メッセージが生成されます。

### S3 メタデータの更新監査メッセージ

コード	名前	説明	トレース	を参照してください
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まれたオブジェクトのメタデータを更新すると生成されます。	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

次の例は、既存の S3 オブジェクトのメタデータを更新するトランザクションの成功を示しています。

## SUPD : S3 メタデータの更新

S3クライアントが、指定されたメタデータを更新する要求 (SUPD) を実行します (x-amz-meta-\\*) をクリックします。この例では、要求ヘッダーは監査プロトコルヘッダー (**configuration> Monitoring> Audit** および **syslog server**) として設定されているため、HTRH フィールドに含まれています。を参照してください ["監査メッセージとログの送信先を設定します"](#)。

```
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：概要

システムから返される監査メッセージの詳細について、次のセクションで説明します。各監査メッセージをメッセージが表すアクティビティのクラスでグループ化して、表に記載します。これらの分類は、監査対象のアクティビティのタイプを理解し、必要な監査メッセージフィルタリングのタイプを選択する場合に役立ちます。

監査メッセージは、4文字のコードでアルファベット順に一覧表示されます。このアルファベット順のリストでは、特定のメッセージに関する情報を検索できます。

この章で使用する4文字のコードは、次のメッセージ例に示すように、監査メッセージ内の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]]
```

監査メッセージレベルの設定、ログの送信先の変更、および監査情報への外部syslogサーバの使用については、を参照してください ["監査メッセージとログの送信先を設定します"](#)

## 監査メッセージのカテゴリ

### 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処理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概要	を参照してください
ECMC	Missing Erasure-Coded Data Fragment：イレイジャーコーディングされた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：イレイジャーコーディングされたデータフラグメントの欠落"
ECOC	Corrupt Erasure-Coded Data Fragment：イレイジャーコーディングデータフラグメントの破損が検出されたことを示します。	"ECOC：イレイジャーコーディングされたデータフラグメントの破損"
ETAF	Security Authentication Failed：Transport Layer Security（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 Registration：サービスがStorageGRIDシステムに自身に関する情報を更新または登録しました。	"GNRG：GNDS登録"
GNUR	GNDS Unregistration：サービスがStorageGRIDシステムから自身の登録を解除しました。	"GNUR：GNDS登録解除"
GTED	Grid Task Ended：CMN サービスがグリッドタスクの処理を完了しました。	"GTED：Gridタスクが終了しました"
GTSt	Grid Task Started：CMN サービスがグリッドタスクの処理を開始しました。	"GTSt：Gridタスクが開始されました"
GTSU	Grid Task Submitted：グリッドタスクがCMN サービスに送信されました。	"GTSU：Gridタスクが送信されました"

コード	メッセージのタイトルと概要	を参照してください
LLST	Location Lost : 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 : ロケーションが失われました"
OLST	Object Lost : 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: システムが損失オブジェクトを検出しました"
サッド	Security Audit Disable : 監査メッセージのロギングがオフになりました。	"SADD : セキュリティ監査無効"
Sade 社	Security Audit Enable : 監査メッセージのロギングが再開されました。	"Sade : セキュリティ監査を有効にします"
SVRF	Object Store Verify Fail : 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の検証に失敗しました"
SVRU の場合	Object Store Verify Unknown : オブジェクトストアで想定外の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検証が不明です"
SYSD	Node Stop : シャットダウンが要求されました。	"SYSD : ノード停止"
SYST	Node Stopping : サービスが正常な停止を開始しました。	"SYST : ノードを停止しています"
SYSU	Node Start : サービスが開始されました。前回のシャットダウンのタイプがメッセージに示されます。	"SYSU : ノードが開始されました"

#### 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格納と管理に関連するイベントに使用されます。オブジェクトの格納と読み出し、グリッドノードからグリッドノードへの転送、および検証が含まれます。

コード	説明	を参照してください
APCT	Archive Purge from Cloud-Tier : S3 API を使用して StorageGRID に接続する外部アーカイブストレージシステムから、アーカイブされたオブジェクトデータが削除されました。	"APCT : クラウド階層からのアーカイブの削除"
ARCB	Archive Object Retrieve Begin : ARC サービスが、外部アーカイブストレージシステムからオブジェクトデータの読み出しを開始しました。	"ARCB : アーカイブオブジェクトの読み出しが開始されました"

コード	説明	を参照してください
ARCE	Archive Object Retrieve End : オブジェクトデータが外部アーカイブストレージシステムから読み出され、ARC サービスが読み出し処理のステータスをレポートします。	"ARCE : アーカイブオブジェクトの読み出しが終了しました"
ARCT	Archive Retrieve from Cloud-Tier : S3 API を使用して StorageGRID に接続する外部アーカイブストレージシステムから、アーカイブされたオブジェクトデータが読み出されました。	"ARCT : クラウド階層からアーカイブを取得します"
AREM	Archive Object Remove : 外部アーカイブストレージシステムからのコンテンツブロックの削除が成功または失敗しました。	"AREM : アーカイブオブジェクトの削除"
ASCE	Archive Object Store End : コンテンツブロックが外部アーカイブストレージシステムに書き込まれ、ARC サービスが書き込み処理のステータスをレポートします。	"ASCE : アーカイブオブジェクトストアの終了"
▽ SCT。△	Archive Store Cloud-Tier : S3 API を使用して StorageGRID に接続する外部アーカイブストレージシステムに、オブジェクトデータが格納されました。	"ASCT : アーカイブストアのクラウド階層"
ATCE	Archive Object Store Begin : 外部アーカイブストレージへのコンテンツブロックの書き込みが開始されました。	"ATCE : アーカイブオブジェクトストアが開始されました"
AVCC の場合	Archive Validate Cloud-Tier Configuration : 指定されたアカウントおよびバケットの設定の検証に成功または失敗しました。	"AVCC : アーカイブによってクラウド階層の構成を検証"
ブロア	Bucket Read Only Request : バケットが読み取り専用モードになったか、または終了しました。	"BROR : バケット読み取り専用要求"
CBSE	Object Send End : ソースエンティティが、グリッドノードからグリッドノードへのデータ転送処理を完了しました。	"CBSE : オブジェクト送信終了"
CBRE	Object Receive End : デスティネーションエンティティが、グリッドノードからグリッドノードへのデータ転送処理を完了しました。	"CBRE : オブジェクト受信終了"

コード	説明	を参照してください
CGRR	Cross-Grid Replication Request : 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レプリケートするために、グリッド間レプリケーション処理を試行しました。	"CGRR : クロスグリッドレプリケーション要求"
EBDL	Empty Bucket Delete : ILMスキャナが、すべてのオブジェクトを削除中のバケット内のオブジェクトを削除しました (空のバケット処理を実行中)。	"EBDL : 空のバケット削除"
EBKR	Empty Bucket Request : ユーザが、空のバケットをオンまたはオフにする (バケットオブジェクトを削除する、またはオブジェクトの削除を停止する) 要求を送信しました。	"EBKR : バケット要求が空です"
SCMT	Object Store Commit : コンテンツブロックの格納と検証がすべて完了し、要求可能な状態になりました。	"SCMT : オブジェクトストアコミット要求"
SREM	Object Store Remove : コンテンツブロックがグリッドノードから削除され、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

クライアント読み取り監査メッセージは、S3 または Swift クライアントアプリケーションがオブジェクトを読み出す要求を行うときに記録されます。

コード	説明	によって使用されます	を参照してください
S3SL	S3 Select要求 : S3 Select要求がクライアントに返されたあとに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を含めることができます。要求は成功しなかった可能性があります。	S3 クライアント	"S3SL : S3 Select要求"
SGET	S3 GET : バケット内のオブジェクトを読み出したまたはリストアップするトランザクションの成功をログに記録します。  <ul style="list-style-type: none"> <li>注 : トランザクションがサブリソースで動作している場合、監査メッセージには S3SR フィールドが含まれます。</li> </ul>	S3 クライアント	"SGET : S3 GET"
Shea	S3 HEAD : オブジェクトまたはバケットの存在を確認するトランザクションの成功をログに記録します。	S3 クライアント	"Shea : S3 ヘッド"

コード	説明	によって使用され れます	を参照してくだ さい
wget	Swift GET : コンテナ内のオブジェクトを読み出しま たはリストアップするトランザクションの成功をロ グに記録します。	Swift クライアン ト	"wget : Swift GET"
WHEA	Swift HEAD : オブジェクトまたはコンテナの存在を 確認するトランザクションの成功をログに記録しま す。	Swift クライアン ト	"WHEA : Swift ヘッド"

#### クライアント書き込み監査メッセージ

クライアント書き込み監査メッセージは、S3 または Swift クライアントアプリケーションがオブジェクトを作成または変更する要求を行うときに記録されます。

コード	説明	によって使用され れます	を参照してくだ さい
OWR	Object Overwrite : 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ログに記録し ます。	S3およびSwiftク ライアント	"OWR : オブ ジェクトを上書 き"
SDEL	S3 DELETE : オブジェクトまたはバケットを削除す るトランザクションの成功をログに記録します。  <ul style="list-style-type: none"> <li>注: トランザクションがサブリソースで動作して いる場合、監査メッセージには S3SR フィールド が含まれます。</li> </ul>	S3 クライアント	"SDEL : S3 DELETE"
SPO	S3 POST : オブジェクトを AWS Glacier ストレージ からクラウドストレージプールにリストアするトラ ンザクションの成功をログに記録します。	S3 クライアント	"SPO : S3 POST"
SPUT	S3 PUT : オブジェクトまたはバケットを新規に作成 するトランザクションの成功をログに記録します。  <ul style="list-style-type: none"> <li>注: トランザクションがサブリソースで動作して いる場合、監査メッセージには S3SR フィールド が含まれます。</li> </ul>	S3 クライアント	"SPUT : S3 PUT"
SUPD	S3 Metadata Updated : 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トランザクション の成功をログに記録します。	S3 クライアント	"SUPD : S3 × 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 するトランザクションの成功をログに記録します。	Swift クライアン ト	"WDEL : Swift の削除"

コード	説明	によって使用され れます	を参照してくだ さい
WPUT	Swift PUT : オブジェクトまたはコンテナを新規に作成するトランザクションの成功をログに記録します。	Swift クライアント	"WPUT : Swift PUT"

#### 管理監査メッセージ

管理カテゴリでは、管理 API に対するユーザ要求がログに記録されます。

コード	メッセージのタイトルと概要	を参照してください
MGAU	管理 API 監査メッセージ：ユーザ要求のログ。	"MGAU : 管理監査メッセージ"

#### 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) 処理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概要	を参照してください
IDEL	ILM Initiated Delete : この監査メッセージは、ILM がオブジェクトを削除する処理を開始すると生成されます。	"IDEL : ILM Initiated Delete"
LCU	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、ストレージスペースを解放するために上書きされたオブジェクトが自動的に削除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"
ORLM の場合	Object Rules Met : この監査メッセージは、ILMルールの指定に従ってオブジェクトデータが格納された場合に生成されます。	"ORLM : オブジェクトルールが満たされています"

#### 監査メッセージリファレンス

##### APCT : クラウド階層からのアーカイブの削除

このメッセージは、S3 API を使用して StorageGRID に接続する外部アーカイブストレージシステムから、アーカイブされたオブジェクトデータが削除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 ID	削除され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
CSIZ	コンテンツサイズ (Content Size)	オブジェクトのサイズ (バイト単位)。常に 0 を返します。
RSLT	結果コード	成功 (SUCS)、またはバックエンドによって報告されたエラーが返されます。
SUID	Storage Unique Identifier の略	オブジェクトが削除されたクラウド階層の一意的識別子 (UUID)。

**ARCB** : アーカイブオブジェクトの読み出しが開始されました

このメッセージは、アーカイブされたオブジェクトデータの読み出し要求が送信されて読み出しプロセスが開始されたときに生成されます。読み出し要求はすぐに処理されますが、順序を変更してテープなどのリニアなメディアからの読み出し効率を高めることができます。

コード	フィールド	説明
CBID	コンテンツブロック ID	外部アーカイブストレージシステムから読み出すコンテンツブロックの一意的識別子。
RSLT	結果	アーカイブ読み出しプロセスを開始した結果を示します。現在定義されている値：SUCS：コンテンツ要求が受信され、読み出しのためにキューに登録されました。

この監査メッセージにはアーカイブ読み出しの時間が記録されます。メッセージを対応する ARCE 終了メッセージと照合することで、アーカイブ読み出しの所要時間および処理が成功したかどうかを判断できます。

**ARCE** : アーカイブオブジェクトの読み出しが終了しました

このメッセージは、アーカイブノードが外部アーカイブストレージシステムからオブジェクトデータを読み出す試行が完了したときに生成されます。成功した場合、メッセージには、要求されたオブジェクトデータがアーカイブ先から完全に読み取られ、検証に成功したことが示されます。読み出しと検証が完了すると、オブジェクトデータは要求元のサービスに配信されます。

コード	フィールド	説明
CBID	コンテンツブロック ID	外部アーカイブストレージシステムから読み出すコンテンツブロックの一意的識別子。
VLID	ボリューム識別子	データがアーカイブされたボリュームの識別子。コンテンツのアーカイブ先が見つからない場合は、ボリュームID 0が返されます。

コード	フィールド	説明
RSLT	取得結果	<p>アーカイブ読み出しプロセスの完了ステータス：</p> <ul style="list-style-type: none"> <li>• SUCS : 成功しました</li> <li>• VRFL : 失敗 (オブジェクトの検証に失敗)</li> <li>• ARUN : 失敗 (外部アーカイブストレージシステムを使用できない)</li> <li>• CANC : 失敗 (読み出し処理がキャンセルされた)</li> <li>• GERR : 失敗 (一般的なエラー)</li> </ul>

このメッセージと対応する ARCB メッセージを組み合わせることで、アーカイブ読み出しの所要時間を特定できます。このメッセージは読み出しが成功したかどうかを示し、失敗した場合には原因がコンテンツブロックの読み出しに失敗したことを示します。

**ARCT** : クラウド階層からアーカイブを取得します

このメッセージは、S3 API を使用して StorageGRID に接続する外部アーカイブストレージシステムから、アーカイブされたオブジェクトデータが読み出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 ID	読み出されたコンテンツブロックの一意的識別子。
CSIZ	コンテンツサイズ (Content Size)	オブジェクトのサイズ (バイト単位)。読み出しが成功した場合にのみ正確な値が表示されます。
RSLT	結果コード	成功 (SUCS)、またはバックエンドによって報告されたエラーが返されます。
SUID	Storage Unique Identifier の略	外部アーカイブストレージシステムの一意的識別子 (UUID)。
時間	時間	要求の合計処理時間 (マイクロ秒)。

**AREM** : アーカイブオブジェクトの削除

Archive Object Remove 監査メッセージは、アーカイブノードからのコンテンツブロックの削除が成功または失敗したことを示します。アーカイブノードが StorageGRID がオブジェクトの場所を解放したことを外部アーカイブストレージシステムに通知した場合、結果は成功です。オブジェクトが外部アーカイブストレージシステムから削除されるかどうかは、システムのタイプと構成によって異なります。

コード	フィールド	説明
CBID	コンテンツブロック ID	外部アーカイブメディアシステムから読み出すコンテンツブロックの一意の識別子。
VLID	ボリューム識別子	オブジェクトデータがアーカイブされていたボリュームの識別子。
RSLT	結果	アーカイブ削除プロセスの完了ステータス： <ul style="list-style-type: none"> <li>• SUCS : 成功しました</li> <li>• ARUN : 失敗 (外部アーカイブストレージシステムを使用できない)</li> <li>• GERR : 失敗 (一般的なエラー)</li> </ul>

**ASCE** : アーカイブオブジェクトストアの終了

このメッセージは、外部アーカイブストレージシステムへのコンテンツブロックの書き込みが終了したことを示します。

コード	フィールド	説明
CBID	Content Block Identifier の略	外部アーカイブストレージシステムに格納されているコンテンツブロックの識別子。
VLID	ボリューム識別子	オブジェクトデータの書き込み先のアーカイブボリュームの一意の識別子。
VREN	検証が有効です	コンテンツブロックに対して検証が実行されるかどうかを示します。現在定義されている値は次のとおり <ul style="list-style-type: none"> <li>• VENA : 検証が有効になっています</li> <li>• VDSA : 検証は無効です</li> </ul>
MCLS	管理クラス	コンテンツブロックが割り当てられている TSM 管理クラスを識別する文字列 (該当する場合)。

コード	フィールド	説明
RSLT	結果	<p>アーカイブプロセスの結果を示します。現在定義されている値は次のとおり</p> <ul style="list-style-type: none"> <li>• SUCS : 成功 (アーカイブプロセスが成功)</li> <li>• OFFL : 失敗 (アーカイブがオフライン)</li> <li>• VRFL : 失敗 (オブジェクトの検証に失敗)</li> <li>• ARUN : 失敗 (外部アーカイブストレージシステムを使用できない)</li> <li>• GERR : 失敗 (一般的なエラー)</li> </ul>

この監査メッセージは、指定されたコンテンツブロックが外部アーカイブストレージシステムに書き込まれたことを意味します。書き込みが失敗した場合は、どこで失敗したかを示す基本的なトラブルシューティング情報が結果として記録されます。より詳細な失敗原因については、StorageGRID システムでアーカイブノードの属性を調べてください。

**ASCT** : アーカイブストアのクラウド階層

このメッセージは、S3 API を使用して StorageGRID に接続する外部アーカイブストレージシステムに、アーカイブされたオブジェクトデータが格納されたときに生成されません。

コード	フィールド	説明
CBID	コンテンツブロック ID	読み出されたコンテンツブロックの一意的識別子。
CSIZ	コンテンツサイズ (Content Size)	オブジェクトのサイズ (バイト単位)。
RSLT	結果コード	成功 (SUCS)、またはバックエンドによって報告されたエラーが返されます。
SUID	Storage Unique Identifier の略	コンテンツ格納先クラウド階層の一意的識別子 (UUID)。
時間	時間	要求の合計処理時間 (マイクロ秒)。

**ATCE** : アーカイブオブジェクトストアが開始されました

このメッセージは、外部アーカイブストレージへのコンテンツブロックの書き込みが開始されたことを示します。

コード	フィールド	説明
CBID	コンテンツブロック ID	アーカイブされるコンテンツブロックの一意的識別子。
VLID	ボリューム識別子	コンテンツブロックの書き込み先のボリュームの一意的識別子。処理に失敗した場合は 0 が返されます。
RSLT	結果	<p>コンテンツブロックの転送結果を示します。現在定義されている値は次のとおり</p> <ul style="list-style-type: none"> <li>• SUCS : 成功 (コンテンツブロックは正常に格納されました)</li> <li>• EXIS : 無視 (コンテンツブロックはすでに格納されています)</li> <li>• ISFD : 失敗 (ディスクスペースが足りません)</li> <li>• STER : 失敗 (CBID の格納エラー)</li> <li>• OFFL : 失敗 (アーカイブがオフライン)</li> <li>• GERR : 失敗 (一般的なエラー)</li> </ul>

**AVCC** : アーカイブによってクラウド階層の構成を検証

このメッセージは、クラウド階層 - Simple Storage Service (S3) ターゲットタイプの構成設定が検証されたときに生成されます。

コード	フィールド	説明
RSLT	結果コード	成功 (SUCS)、またはバックエンドによって報告されたエラーが返されます。
SUID	Storage Unique Identifier の略	検証対象の外部アーカイブストレージシステムに関連付けられている UUID。

**BROR** : バケット読み取り専用要求

この監査メッセージは、バケットが読み取り専用モードになったときまたは終了したときにLDRサービスによって生成されます。たとえば、すべてのオブジェクトが削除されている間にバケットが読み取り専用モードになったとします。

コード	フィールド	説明
BKHD	バケットUUID	バケットID。
プローブ	バケットの読み取り専用要求値	バケットが読み取り専用になっているか、または読み取り専用のままになっているか (1=読み取り専用、0=読み取り専用ではない)。

コード	フィールド	説明
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なっている理由、または読み取り専用状態のままになっている理由。たとえば、emptyBucketなどです。
S3AI	S3テナントアカウントID	要求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であることを示します。
S3BK	S3バケット	S3 バケット名。

**CBRB** : オブジェクト受信が開始されました

通常のシステム運用中は、データへのアクセスおよびデータのレプリケートと保持が行われる際に、異なるノード間でコンテンツブロックが継続的に転送されます。このメッセージは、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したときに転送先のエンティティによって生成されます。

コード	フィールド	説明
CNID	接続識別子	ノード間のセッション / 接続の一意の識別子。
CBID	Content Block Identifier の略	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 (Transfer Direction)	CBID 転送がプッシュで開始されたかプルで開始されたかを示します。 PUSH : 転送処理は送信側エンティティによって要求されました。 PULL : 転送処理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 (送信側) のノード ID。
CTD	デスティネーションエンティティ	CBID 転送のデスティネーション (受信側) のノード ID。
CTSS	開始シーケンスカウント (Start Sequence Count)	最初のシーケンスカウントが要求されたことを示します。成功すると、このシーケンスカウントから転送が開始されます。
CTES	想定される終了シーケンス数	最後に要求されたシーケンスカウントを示します。成功すると、このシーケンスカウントを受信したときに転送が完了したとみなされます。

コード	フィールド	説明
RSLT	転送開始ステータス	転送が開始された時点のステータス：  SUCS : 転送が開始されました。

この監査メッセージは、Content Block Identifier で識別されたとおりに単一のコンテンツでノード間のデータ転送処理が開始されたことを意味します。この処理では、「Start Sequence Count」から「Expected End Sequence Count」までのデータが要求されます。送信側と受信側のノードは、ノード ID によって識別されます。この情報を使用すると、システムのデータフローを追跡できます。ストレージ監査メッセージと組み合わせて使用すると、レプリカ数を検証できます。

**CBRE** : オブジェクト受信終了

このメッセージは、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したときに転送先のエンティティによって生成されます。

コード	フィールド	説明
CNID	接続識別子	ノード間のセッション / 接続の一意の識別子。
CBID	Content Block Identifier の略	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 (Transfer Direction)	CBID 転送がプッシュで開始されたかプルで開始されたかを示します。  PUSH : 転送処理は送信側エンティティによって要求されました。  PULL : 転送処理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 (送信側) のノード ID 。
CTD	デスティネーションエンティティ	CBID 転送のデスティネーション (受信側) のノード ID 。
CTSS	開始シーケンスカウント (Start Sequence Count)	転送が開始されたシーケンスカウントを示します。
CTA	実際の終了シーケンス数	転送に成功した最後のシーケンスカウントを示します。実際の終了シーケンスカウントが開始シーケンスカウントと同じで、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。

コード	フィールド	説明
RSLT	転送結果	<p>(送信側エンティティから見た) 転送処理の結果：</p> <p>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。</p> <p>CONL : 転送中に接続が失われました</p> <p>CTMO : 接続の確立中または転送中に接続がタイムアウトしました</p> <p>UNRE : デスティネーションノード ID に到達できません</p> <p>CRPT : 破損したデータまたは無効なデータの受信が原因で転送が終了しました</p>

この監査メッセージは、ノード間のデータ転送処理が完了したことを意味します。転送結果が成功した場合は、「Start Sequence Count」から「Actual End Sequence Count」にデータが転送されます。送信側と受信側のノードは、ノード ID によって識別されます。この情報を使用すると、システムのデータフローを追跡し、エラーを検出、集計、分析できます。ストレージ監査メッセージと組み合わせれば、レプリカ数の検証にも使用できます。

#### CBSB : オブジェクト送信の開始

通常のシステム運用中は、データへのアクセスおよびデータのレプリケートと保持が行われる際に、異なるノード間でコンテンツブロックが継続的に転送されます。このメッセージは、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したときにソースエンティティによって生成されます。

コード	フィールド	説明
CNID	接続識別子	ノード間のセッション / 接続の一意の識別子。
CBID	Content Block Identifier の略	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 (Transfer Direction)	<p>CBID 転送がプッシュで開始されたかプルで開始されたかを示します。</p> <p>PUSH : 転送処理は送信側エンティティによって要求されました。</p> <p>PULL : 転送処理は受信側エンティティによって要求されました。</p>
CTSR	ソースエンティティ	CBID 転送のソース (送信側) のノード ID。
CTD	デスティネーションエンティティ	CBID 転送のデスティネーション (受信側) のノード ID。

コード	フィールド	説明
CTSS	開始シーケンスカウント ( Start Sequence Count )	最初のシーケンスカウントが要求されたことを示します。成功すると、このシーケンスカウントから転送が開始されます。
CTES	想定される終了シーケンス数	最後に要求されたシーケンスカウントを示します。成功すると、このシーケンスカウントを受信したときに転送が完了したとみなされます。
RSLT	転送開始ステータス	転送が開始された時点のステータス：  SUCS : 転送が開始されました。

この監査メッセージは、Content Block Identifier で識別されたとおりに単一のコンテンツでノード間のデータ転送処理が開始されたことを意味します。この処理では、「Start Sequence Count」から「Expected End Sequence Count」までのデータが要求されます。送信側と受信側のノードは、ノード ID によって識別されます。この情報を使用すると、システムのデータフローを追跡できます。ストレージ監査メッセージと組み合わせて使用すると、レプリカ数を検証できます。

**CBSE** : オブジェクト送信終了

このメッセージは、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したときに転送元のエンティティによって生成されます。

コード	フィールド	説明
CNID	接続識別子	ノード間のセッション / 接続の一意の識別子。
CBID	Content Block Identifier の略	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 ( Transfer Direction )	CBID 転送がプッシュで開始されたかプルで開始されたかを示します。  PUSH : 転送処理は送信側エンティティによって要求されました。  PULL : 転送処理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 (送信側) のノード ID 。
CTD	デスティネーションエンティティ	CBID 転送のデスティネーション (受信側) のノード ID 。

コード	フィールド	説明
CTSS	開始シーケンスカウント ( Start Sequence Count )	転送が開始されたシーケンスカウントを示します。
CTA	実際の終了シーケンス数	転送に成功した最後のシーケンスカウントを示します。実際の終了シーケンスカウントが開始シーケンスカウントと同じで、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	<p>(送信側エンティティから見た) 転送処理の結果：</p> <p>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。</p> <p>CONL : 転送中に接続が失われました</p> <p>CTMO : 接続の確立中または転送中に接続がタイムアウトしました</p> <p>UNRE : デスティネーションノード ID に到達できません</p> <p>CRPT : 破損したデータまたは無効なデータの受信が原因で転送が終了しました</p>

この監査メッセージは、ノード間のデータ転送処理が完了したことを意味します。転送結果が成功した場合は、「Start Sequence Count」から「Actual End Sequence Count」にデータが転送されます。送信側と受信側のノードは、ノード ID によって識別されます。この情報を使用すると、システムのデータフローを追跡し、エラーを検出、集計、分析できます。ストレージ監査メッセージと組み合わせれば、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レプリケートするためにグリッド間レプリケーション処理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	<p>オブジェクトのサイズ (バイト単位)。</p> <p>CSIZ属性はStorageGRID 11.8で導入されました。そのため、StorageGRID 11.7から11.8へのアップグレードにまたがるグリッド間レプリケーション要求で、オブジェクトの合計サイズが不正確になることがあります。</p>
S3AI	S3テナントアカウントID	オブジェクトのレプリケート元のバケットを所有するテナントアカウントのID。

コード	フィールド	説明
GFID	グリッドフェデレーション接続ID	グリッド間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。
オペー	CGR操作	クロスグリッドレプリケーション処理が試行されたタイプ。  <ul style="list-style-type: none"> <li>• 0 =オブジェクトをレプリケートします</li> <li>• 1 =マルチパートオブジェクトをレプリケートします</li> <li>• 2 =削除マーカを複製します</li> </ul>
S3BK	S3バケット	S3 バケット名。
S3KY	S3 キー	バケット名を除く S3 キーの名前。
VSID	バージョン ID	レプリケート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：空のバケット削除

すべてのオブジェクトを削除中のバケット内のオブジェクトがILMスキャナによって削除されました（空のバケット処理を実行中）。

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（バイト単位）。
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	Universally Unique Identifier の略	StorageGRID システム内でのオブジェクトの識別子。
RSLT	削除処理の結果	イベント、プロセス、またはトランザクションの結果。該当しないメッセージの場合は、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** : バケット要求が空です

このメッセージは、ユーザが、空のバケットをオンまたはオフにする（バケットオブジェクトを削除する、または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ています。

コード	フィールド	説明
bUID	バケットUUID	バケットID。
EBJS	空のバケットJSON設定	現在の空のバケットの設定を表すJSONが格納されます。
S3AI	S3テナントアカウントID	要求を送信したユーザのテナントアカウント ID 。空の値は匿名アクセスであることを示します。
S3BK	S3 バケット	S3 バケット名。

**ECMC** : イレイジャーコーディングされたデータフラグメントの欠落

この監査メッセージは、イレイジャーコーディングされたデータフラグメントの欠落がシステムで検出されたことを示します。

コード	フィールド	説明
VCMC	VCS ID を入力します	欠落しているチャンクが含まれている VCS の名前。
MCID	チャンク ID	欠落しているイレイジャーコーディング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、このメッセージには該当しません。このメッセージがフィルタリングされないように、「UCS」ではなく「none」が使用されます。

**ECOC** : イレイジャーコーディングされたデータフラグメントの破損

この監査メッセージは、イレイジャーコーディングされたデータフラグメントの破損がシステムで検出されたことを示します。

コード	フィールド	説明
Vcco	VCS ID を入力します	破損したチャンクが含まれている VCS の名前。

コード	フィールド	説明
VLID	ボリューム ID	破損したイレイジャーコーディングフラグメントが含まれている RangeDB ボリューム。
CCID	チャンク ID	破損したイレイジャーコーディング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、このメッセージには該当しません。このメッセージがフィルタリングされないように、「UCS」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、Transport Layer Security ( TLS ) を使用した接続試行が失敗した場合に生成されます。

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 接続の一意的システム識別子。
RUID	ユーザ ID	リモートユーザの ID を表すサービスに依存する識別子。
RSLT	理由コード	失敗の理由：  SCNI : セキュアな接続を確立できませんでした。  CERM : 証明書がありません。  CERT : 証明書が無効です。  CERE : 証明書が期限切れです。  CERR : 証明書が取り消されています。  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 : ユーザクレデンシャルがありません。  UCRI : ユーザクレデンシャルが無効です。  UCRU : ユーザのクレデンシャルが拒否されました。  TOUT : 認証がタイムアウトしました。

TLS を使用するセキュアなサービスへの接続が確立されると、サービスに組み込まれている TLS プロファイルおよびその他のロジックを使用してリモートエンティティのクレデンシャルが検証されます。無効、想定

外、許可されていない証明書またはクレデンシャルが原因でこの認証が失敗すると、監査メッセージがログに記録されます。これにより、不正アクセスやその他のセキュリティ関連の接続問題を照会できます。

このメッセージは、リモートエンティティの設定が正しくない場合や、無効または許可されていないクレデンシャルをシステムに提示しようとした場合に生成されることがあります。この監査メッセージを監視して、システムへの不正なアクセス試行を検出する必要があります。

#### GNRG : GNDS 登録

CMN サービスは、StorageGRID システムで CMN サービスに関する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： <ul style="list-style-type: none"><li>• SUCS : 成功しました</li><li>• SUNV : サービスを使用できません</li><li>• GERR : その他の失敗</li></ul>
GNID	ノードID	更新要求を開始したサービスのノード ID。
GNTN	デバイスタイプ	グリッドノードのデバイスタイプ (LDR サービスの場合は BLDR など)。
GNDV	デバイスモデルのバージョン	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 - クエリランキングのコンテキストで)。
GNIA	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自身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、StorageGRID システムから CMN サービスに関する情報の登録を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：  <ul style="list-style-type: none"> <li>• SUCS : 成功しました</li> <li>• SUNV : サービスを使用できません</li> <li>• GERR : その他の失敗</li> </ul>
GNID	ノードID	更新要求を開始したサービスのノード ID。

**GTED** : Grid 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 Historical テーブルに移動したことを示します。結果が SUCS、ABRT、ROLF のいずれかである場合は、対応する Grid Task Started 監査メッセージも生成されます。それ以外の結果は、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ます。また、グリッドタスクをライフサイクル全体にわたって管理できます。  <ul style="list-style-type: none"> <li>• 注：* タスク ID は、グリッドタスクが送信された時点ではなく、生成された時点で割り当てられます。特定のグリッドタスクを複数回送信することができます。この場合、送信済み、開始、および終了の監査メッセージを一意にリンクするためのタスク ID フィールドでは不十分です。</li> </ul>
RSLT	結果	グリッドタスクの最終ステータス：  <ul style="list-style-type: none"> <li>• SUCS : グリッドタスクが正常に完了しました。</li> <li>• 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。</li> <li>• Rolf : グリッドタスクは終了し、ロールバックプロセスを完了できませんでした。</li> <li>• CANC : グリッドタスクは開始前にユーザによってキャンセルされました。</li> <li>• EXPR : グリッドタスクは開始前に期限切れとなりました。</li> <li>• IVLD : グリッドタスクは無効でした。</li> <li>• AUTH : グリッドタスクは許可されていませんでした。</li> <li>• DUPL : グリッドタスクは重複として拒否されました。</li> </ul>

**GTSt : Grid** 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。この監査メッセージは、内部の Grid Task Submission サービスによって開始されて自動アクティブ化用に選択されているグリッドタスクの Grid Task Submitted メッセージの直後に生成されます。Pending テーブルに送信されるグリッドタスクの場合、このメッセージはユーザがグリッドタスクを開始するときに生成されません。

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ます。また、タスクをライフサイクル全体にわたって管理できます。  <ul style="list-style-type: none"> <li>注：* タスク ID は、グリッドタスクが送信された時点ではなく、生成された時点で割り当てられます。特定のグリッドタスクを複数回送信することができます。この場合、送信済み、開始、および終了の監査メッセージを一意にリンクするためのタスク ID フィールドでは不十分です。</li> </ul>
RSLT	結果	結果。このフィールドの値は 1 つだけです。  <ul style="list-style-type: none"> <li>SUCS : グリッドタスクが正常に開始されました。</li> </ul>

**GTSU : Grid** 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。  <ul style="list-style-type: none"> <li>注：* タスク ID は、グリッドタスクが送信された時点ではなく、生成された時点で割り当てられます。特定のグリッドタスクを複数回送信することができます。この場合、送信済み、開始、および終了の監査メッセージを一意にリンクするためのタスク ID フィールドでは不十分です。</li> </ul>
ttyp	タスクタイプ (Task Type)	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 概要 の略	グリッドタスクの判読可能な概要。

コード	フィールド	説明
付加価値を提供します	タイムスタンプ後の有効な値	グリッドタスクの有効期間の開始時間（UNIX 時間 1970 年 1 月 1 日からの UINTE64 マイクロ秒数）。
VBTS	タイムスタンプの前に有効です	グリッドタスクの有効期間の終了時間（UNIX 時間 1970 年 1 月 1 日からの UINTE64 マイクロ秒数）。
TsRC	ソース	タスクのソース：  <ul style="list-style-type: none"> <li>• TXTB：グリッドタスクは、StorageGRID システム経由で署名付きテキストブロックとして送信されました。</li> <li>• GRID：グリッドタスクは、内部の Grid Task Submission サービス経由で送信されました。</li> </ul>
ACTV	アクティブ化のタイプ	アクティブ化のタイプ：  <ul style="list-style-type: none"> <li>• Auto：グリッドタスクは自動でアクティブ化されます。</li> <li>• PEND：グリッドタスクは Pending テーブルに追加されました。TXTB ソースの場合はこのタイプのみです。</li> </ul>
RSLT	結果	送信結果：  <ul style="list-style-type: none"> <li>• SUCS：グリッドタスクは正常に送信されました。</li> <li>• FAIL：タスクは Historical テーブルに直接移動されました。</li> </ul>

#### IDEL : ILM Initiated Delete

このメッセージは、ILM によってオブジェクトを削除する処理が開始された場合に生成されます。

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 \*：このメッセージは、保持期間が経過したために ILM によってオブジェクトの自動削除処理が開始された場合に生成されます（自動削除設定が有効になっていて、リーガルホールドがオフの場合）。
- \* 非準拠 S3 バケットまたは Swift コンテナ内のオブジェクト \*。このメッセージは、現在オブジェクトに適用されている配置手順がアクティブな ILM ポリシーにないためにオブジェクトを削除する処理が ILM によって開始された場合に生成されます。

コード	フィールド	説明
CBID	Content Block Identifier の略	オブジェクトの CBID。

コード	フィールド	説明
CMPA	準拠：自動削除	準拠 S3 バケット内のオブジェクトのみが対象。0（false）または 1（true）。バケットがリーガルホールドの対象である場合を除き、保持期間の終了時に準拠オブジェクトを自動的に削除するかどうかを示します。
テンプレート	コンプライアンス：リーガルホールド	準拠 S3 バケット内のオブジェクトのみが対象。0（false）または 1（true）。バケットが現在リーガルホールドの対象であるかどうかを示します。
CMPR	準拠：保持期間	準拠 S3 バケット内のオブジェクトのみが対象。オブジェクトの保持期間の長さ（分）。
CTME	準拠：取り込み時間	準拠 S3 バケット内のオブジェクトのみが対象。オブジェクトの取り込み時間。この値に保持期間を分単位で追加することで、オブジェクトをバケットから削除できるタイミングを判断できます。
dmrk	マーカーバージョン ID を削除します	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た削除マーカーのバージョン ID。バケットに対する処理では、このフィールドは指定されません。
CSIZ	コンテンツのサイズ	オブジェクトのサイズ（バイト単位）。
LOCS	ロケーション	StorageGRID システム内のオブジェクトデータの格納場所。オブジェクトに場所がない場合（削除されている場合など）、LOCS の値は "" です。  CLEC：イレイジャーコーディングオブジェクトの場合、オブジェクトのデータに適用されているイレイジャーコーディングプロファイルIDとイレイジャーコーディンググループID。  CLDI：レプリケート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は、オブジェクトの場所の ARC ノード ID。
パス	S3 バケット / キーまたは Swift コンテナ / オブジェクト ID	S3 バケット名と S3 キー名、または Swift コンテナ名と Swift オブジェクト識別子。
RSLT	結果	ILM 処理の結果。  SUCS：ILM 処理が成功しました。

コード	フィールド	説明
ルール	ルールラベル (Rules Label)	<ul style="list-style-type: none"> <li>保持期間が経過したために準拠 S3 バケット内のオブジェクトが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。</li> <li>現在オブジェクトに適用される配置手順がない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。</li> </ul>
SgRP	サイト (グループ)	オブジェクトが存在する場合は、指定したサイトで削除されています。このサイトは、オブジェクトが取り込まれたサイトではありません。
UUID	Universally Unique Identifier の略	StorageGRID システム内で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。バージョン管理に対応していないバケット内のバケットおよびオブジェクトに対する処理には、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、ストレージスペースを解放するためにクリーンアップが必要な上書きされたオブジェクトを StorageGRID が削除した場合に生成されます。オブジェクトがすでに含まれているパスに S3 または Swift クライアントがオブジェクトを書き込むと、オブジェクトが上書きされます。削除処理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	コンテンツのサイズ	オブジェクトのサイズ (バイト単位)。
LTyp	クリーンアップのタイプ	_ 内部使用のみ。 _
LUID (LUID)	オブジェクト UUID が削除されました	削除されたオブジェクトの識別子。
パス	S3 バケット / キーまたは Swift コンテナ / オブジェクト ID	S3 バケット名と S3 キー名、または Swift コンテナ名と Swift オブジェクト識別子。
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。

コード	フィールド	説明
UUID	Universally Unique Identifier の略	まだ存在するオブジェクトの ID 。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。

LLST : ロケーションが失われました

このメッセージは、オブジェクトコピー（レプリケートまたはイレイジャーコーディング）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	イレイジャーコーディングプロファイル	イレイジャーコーディングされたオブジェクトデータ用。使用されているイレイジャーコーディングプロファイルの ID 。
LTYP	保管場所タイプ	CLDI（Online）：レプリケートされたオブジェクトデータ用 CLEC（Online）：イレイジャーコーディングされたオブジェクトデータ用 CLNL（Nearline）：アーカイブされたレプリケートオブジェクトデータ用
NOID	ソースノード ID	場所が失われたノード ID 。
PCLD	レプリケートオブジェクトへのパス	損失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（つまりレプリケートオブジェクトの場合）の場合にのみ返されます。  フォームを使用します /var/local/rangedb/2/p/13/13/00oJs6X%{h{U}SeUFxE@
RSLT	結果	常に NONE 。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該当しません。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	トリガ元	USER : ユーザがトリガーしました  SYST : システムがトリガーされました
UUID	Universally Unique ID の略	StorageGRID システムでの該当オブジェクトの識別子。

管理カテゴリでは、管理 API に対するユーザ要求がログに記録されます。API に対する GET または HEAD 以外のすべての要求は、応答に加えて要求のユーザ名、IP、およびタイプをログに記録します。

コード	フィールド	説明
MDIP	宛先 IP アドレス	サーバ (デスティネーション) の IP アドレス。
MDNA	ドメイン名	ホストのドメイン名。
MPAT	要求のパス	要求のパス。
MPQP	要求クエリパラメータ	要求のクエリパラメータ。
MRBD の略	本文を要求します	<p>要求の本文の内容。応答の本文はデフォルトでログに記録されますが、要求の本文は応答の本文が空の特定のケースでログに記録されます。応答の本文には次の情報が含まれていないため、それぞれの POST メソッドの要求本文から取り込まれます。</p> <ul style="list-style-type: none"> <li>• ユーザ名とアカウント ID : * POST authorize *</li> <li>• 新しいサブネット設定 : * POST /grid/grid-networks/update *</li> <li>• 新しい NTP サーバ : * POST /grid/ntp-servers /update * に含まれています</li> <li>• 運用停止されたサーバ ID は、 * POST /grid/servers/decommission * に記載されています</li> <li>• 注 : * 機密情報は、削除 ( S3 アクセスキーなど) またはアスタリスクでマスク (パスワードなど) されます。</li> </ul>
検査	要求メソッド	<p>HTTP 要求メソッド :</p> <ul style="list-style-type: none"> <li>• 投稿 ( Post )</li> <li>• PUT</li> <li>• 削除</li> <li>• パッチ</li> </ul>
MRSC	応答コード	応答コード。
MRSP	応答の本文	<p>デフォルトでは、応答の内容 ( 応答の本文) がログに記録されます。</p> <ul style="list-style-type: none"> <li>• 注 : * 機密情報は、削除 ( S3 アクセスキーなど) またはアスタリスクでマスク (パスワードなど) されます。</li> </ul>

コード	フィールド	説明
MSIP	送信元 IP アドレス	クライアント（送信元）の IP アドレス。
MUUN	ユーザの URN	要求を送信したユーザの 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が返されます。

**OLST:** システムが損失オブジェクトを検出しました

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ることができない場合に生成されます。

コード	フィールド	説明
CBID	Content Block Identifier の略	損失オブジェクトの CBID。
NOID	ノードID	損失オブジェクトが最後に確認された直接またはニアラインの場所（該当する場合）。ボリューム情報がない場合は、ノード ID だけでボリューム ID がないケースもあります。
パス	S3 バケット / キーまたは Swift コンテナ / オブジェクト ID	該当する場合は、S3 バケット名と S3 キー名、または Swift コンテナ名と Swift オブジェクト識別子。
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、このメッセージには該当しません。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	Universally Unique ID の略	StorageGRID システム内の損失オブジェクトの識別子。
ヴォル	ボリューム ID	使用可能な場合は、損失オブジェクトが最後に確認された場所のストレージノードまたはアーカイブ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ています

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格納およびコピーされた場合に生成されます。



ORLM メッセージは、ポリシー内の別のルールで高度なフィルタ「オブジェクトサイズ」が使用されている場合に、オブジェクトがデフォルトの Make 2 Copies ルールによって格納されたときには生成されません。

コード	フィールド	説明
bUID	バケットヘッダー	バケット ID フィールド。内部処理に使用されます。STAT が PRGD の場合にのみ表示されます。
CBID	Content Block Identifier の略	オブジェクトの CBID。
CSIZ	コンテンツのサイズ	オブジェクトのサイズ (バイト単位)。
LOCS	ロケーション	StorageGRID システム内のオブジェクトデータの格納場所。オブジェクトに場所がない場合 (削除されている場合など)、LOCS の値は "" です。  CLEC : イレイジャーコーディングオブジェクトの場合、オブジェクトのデータに適用されているイレイジャーコーディングプロファイルIDとイレイジャーコーディンググループID。  CLDI : レプリケート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は、オブジェクトの場所の ARC ノード ID。
パス	S3 バケット / キーまたは Swift コンテナ / オブジェクト ID	S3 バケット名と S3 キー名、または Swift コンテナ名と Swift オブジェクト識別子。
RSLT	結果	ILM 処理の結果。  SUCS : ILM 処理が成功しました。
ルール	ルールラベル ( Rules Label )	このオブジェクトに適用されている ILM ルールの判読可能なラベル。
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	コンテナの 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。

コード	フィールド	説明
統計	ステータス	ILM 処理のステータス。  DONE : オブジェクトに対する ILM 処理が完了しました。  DFER : ILM によって再評価されるようオブジェクトがマークされました。  PRGD : オブジェクトが StorageGRID システムから削除されました。  NLOC : オブジェクトデータを StorageGRID システムで検出できなくなります。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または破損していることを示している可能性があります。
UUID	Universally Unique Identifier の略	StorageGRID システム内で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で作成された新しいオブジェクトのバージョン ID。バージョン管理に対応していないバケット内のバケットおよびオブジェクトに対する処理には、このフィールドは含まれません。

ORLM 監査メッセージは、1つ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。

- オブジェクトが対応する ILM ルールを無期限に満たしたとき。
- オブジェクトが対応する ILM ルールを一時的に満たしたとき。
- オブジェクトが ILM ルールによって削除されたとき。
- バックグラウンド検証プロセスにより、レプリケート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たとき。StorageGRID システムは、破損したオブジェクトを交換するために ILM 評価を実行します。

#### 関連情報

- ["オブジェクトの取り込みトランザクション"](#)
- ["オブジェクトの削除トランザクション"](#)

#### OVWR : オブジェクトを上書き

このメッセージは、外部（クライアントが要求した）処理によって、あるオブジェクトが別のオブジェクトで上書きされた場合に生成されます。

コード	フィールド	説明
CBID	Content Block Identifier (新規)	新しいオブジェクトの CBID。

コード	フィールド	説明
CSIZ	前のオブジェクトサイズ	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（前のもの）	既存のオブジェクトの CBID。
UUID	Universally Unique ID（新規）	StorageGRID システム内での新しいオブジェクトの識別子。
OUID	Universally Unique ID（旧）	StorageGRID システム内での以前のオブジェクトの識別子。
パス	S3 または Swift オブジェクトのパス	既存のオブジェクトと新しいオブジェクトの両方に使用する S3 または Swift オブジェクトのパス
RSLT	結果コード	Object Overwrite トランザクションの結果。常に次の結果になります。  SUCS : 成功しました
SgRP	サイト（グループ）	上書きされたオブジェクトがある場合は指定したサイトで削除されています。このサイトは、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 Select要求

このメッセージは、S3 Select要求がクライアントに返されたあとに完了を記録します。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を含めることができます。要求は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は圧縮されたバイト数を持ち、BYPRは解凍後のバイト数になります。
BYPR	処理されたバイト数	処理されたバイト数。S3 Selectジョブで実際に処理または処理された「スキャンされたバイト数」の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されたバイト数。

コード	フィールド	説明
レポート	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	レコードが返されました	S3 Selectジョブがクライアントに返されたレコードまたは行の数。
JOFI	ジョブは終了しました	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、ジョブは完了しませんでした。エラーフィールドにはデータが含まれている可能性があります。クライアントに結果が一部しか表示されていない場合や、結果がまったく表示されない場合があります。
リード	リクエスト ID	S3 Select要求の識別子。
EXTM	実行時間	S3 Selectジョブが完了するまでにかかった時間（秒）。
ERMG	エラーメッセージ	S3 Selectジョブが生成されたことを示すエラーメッセージ。
アーティ	エラータイプ	S3 Selectジョブが生成したエラータイプ。
エルスト	スタックトレースエラー	S3 Selectジョブが生成したエラーStacktrace。
S3BK	S3バケット	S3 バケット名。
S3AK	S3 アクセスキー ID (要求の送信者)	要求を送信したユーザのS3アクセスキーID。
S3AI	S3 テナントアカウント ID (要求の送信者)	要求を送信したユーザのテナントアカウント ID 。
S3KY	S3 キー	バケット名を除く S3 キーの名前。

**SADD** :セキュリティ監査無効

このメッセージは、元のサービス（ノード ID）が監査メッセージのロギングをオフにしたことを示します。監査メッセージの収集や配信は停止しています。

コード	フィールド	説明
AETM	enable メソッド	監査を無効にするために使用されたメソッド。

コード	フィールド	説明
EUN	ユーザ名	監査ログを無効にするコマンドを実行したユーザ名。
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該当しません。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、以前は有効だったロギングが現在は無効になっていることを示します。一般には、システムの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実行される処理です。一括アクティビティ後に監査がリストアされ（SADE）、監査を無効にする機能は永続的にブロックされます。

**Sade** : セキュリティ監査を有効にします

このメッセージは、元のサービス（ノード ID）が監査メッセージのロギングをリストアしたことを示します。監査メッセージの収集や配信は再開されています。

コード	フィールド	説明
AETM	enable メソッド	監査を有効にするために使用されたメソッド。
EUN	ユーザ名	監査ログを有効にするコマンドを実行したユーザ名。
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該当しません。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、以前は無効（SADD）だったロギングが現在は有効になっていることを示します。一般には、システムの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実行される処理です。一括アクティビティ後に監査がリストアされ、監査を無効にする機能は永続的にブロックされます。

**SCMT** : オブジェクトストアのコミット

グリッドコンテンツは、コミット（永続的に格納）されるまでは、使用可能にならず、格納済みとして認識されません。永続的に格納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たコンテンツです。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生成されます。

コード	フィールド	説明
CBID	Content Block Identifier の略	永続的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的識別子。
RSLT	結果コード	オブジェクトがディスクに格納された時点のステータス：  SUCS : オブジェクトが正常に格納されました。

このメッセージは、コンテンツブロックの格納と検証がすべて完了し、要求可能な状態になったことを意味し

ます。この機能を使用すると、システム内のデータフローを追跡できます。

#### SDEL : S3 DELETE

S3クライアントがDELETEトランザクションを実行すると、指定したオブジェクトまたはバケットを削除する要求、またはバケット/オブジェクトサブリソースを削除する要求が送信されます。このメッセージは、トランザクションが成功した場合にサーバによって出力されます。

コード	フィールド	説明
CBID	Content Block Identifier の略	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。バケットに対する処理では、このフィールドは指定されません。
CNCH	整合性制御ヘッダー	要求に Consistency-Control HTTP 要求ヘッダーが存在する場合は、その値。
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 (Content Size)	削除されたオブジェクトのサイズ (バイト単位)。バケットに対する処理では、このフィールドは指定されません。
dmrk	マーカージョ ID を削除します	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た削除マーカのバージョン ID。バケットに対する処理では、このフィールドは指定されません。
GFID	グリッドフェデレーション接続 ID	グリッド間レプリケーションの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。デスティネーショングリッドの監査ログにのみ含まれます。
gfsaだ	Gridフェデレーションのソースアカウント ID	グリッド間レプリケーションの削除要求を行うソースグリッド上のテナントのアカウント ID。デスティネーショングリッドの監査ログにのみ含まれます。
HTRH	HTTP 要求ヘッダー	設定時に選択した、ログに記録される HTTP 要求ヘッダーの名前と値のリスト。  <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;"> <p> `X-Forwarded-For` は、要求に存在する場合、およびに存在する場合は自動的に含まれます `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。</p> </div> <p> x-amz-bypass-governance-retention は、要求に含まれている場合は自動的に追加されます。</p>

コード	フィールド	説明
MTME	最終変更時刻	オブジェクトが最後に変更された日時を示す Unix タイムスタンプ（マイクロ秒）。
RSLT	結果コード	DELETE トランザクションの結果。常に次の結果になります。  SUCS : 成功しました
S3AI	S3 テナントアカウント ID（要求の送信者）	要求を送信したユーザのテナントアカウント ID。空の値は匿名アクセスであることを示します。
S3AK	S3 アクセスキー ID（要求の送信者）	要求を送信したユーザのハッシュ済み S3 アクセスキー ID。空の値は匿名アクセスであることを示します。
S3BK	S3 バケット	S3 バケット名。
S3KY	S3 キー	バケット名を除く S3 キーの名前。バケットに対する処理では、このフィールドは指定されません。
S3SR	S3 サブリソース	必要に応じて、処理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（要求の送信者）	要求を送信したユーザのテナントアカウントの名前。匿名の要求の場合は空です。
saip	IP アドレス（要求送信者）	要求を送信し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。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。
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。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。
SgRP	サイト（グループ）	オブジェクトが存在する場合は、指定したサイトで削除されています。このサイトは、オブジェクトが取り込まれたサイトではありません。
サスペンション	S3 ユーザの URN（要求の送信者）	要求を送信しているユーザのテナントアカウント ID とユーザ名。ローカルユーザまたは LDAP ユーザです。例： <code>urn:sgws:identity::03393893651506583485:root</code>  匿名の要求の場合は空です。

コード	フィールド	説明
時間	時間	要求の合計処理時間（マイクロ秒）。
TLIP	信頼できるロードバランサの IP アドレス	要求が信頼できるレイヤ 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 の Universally Unique Identifier (汎用一意識別子)	削除マーカ の識別子。監査ログメッセージでは、UUDM または UUID のいずれかを指定します。UUDM はオブジェクトの削除要求によって作成された削除マーカ、UUID はオブジェクトを示します。
UUID	Universally Unique Identifier の略	StorageGRID システム内で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。バージョン管理に対応していないバケット内のバケットおよびオブジェクトに対する処理には、このフィールドは含まれません。

#### SGET : S3 GET

S3クライアントがGETトランザクションを実行すると、オブジェクトを読み出したりバケット内のオブジェクトをリストしたり、バケット/オブジェクトサブリソースを削除したりする要求が送信されます。このメッセージは、トランザクションが成功した場合にサーバによって出力されます。

コード	フィールド	説明
CBID	Content Block Identifier の略	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。バケットに対する処理では、このフィールドは指定されません。
CNCH	整合性制御ヘッダー	要求に Consistency-Control HTTP 要求ヘッダーが存在する場合は、その値。
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 (Content Size)	読み出されたオブジェクトのサイズ (バイト単位)。バケットに対する処理では、このフィールドは指定されません。

コード	フィールド	説明
HTRH	HTTP 要求ヘッダー	<p>設定時に選択した、ログに記録される HTTP 要求ヘッダーの名前と値のリスト。</p> <div style="border: 1px solid gray; padding: 10px; margin-top: 10px;"> <p>`X-Forwarded-For` は、要求に存在する場合、およびに存在する場合は自動的に含まれます `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。</p> </div>
能力	ListObjectsV2	<code>_v2 format_response</code> が要求されました。詳細については、を参照してください <a href="#">"AWS ListObjectsV2"</a> 。GET Bucket処理の場合のみ。
NCHD	子の数	キーと共通のプレフィックスが含まれます。GET Bucket処理の場合のみ。
rang	範囲の読み取り	範囲読み取り処理の場合のみ。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	<p>GET トランザクションの結果。常に次の結果になります。</p> <p>SUCS : 成功しました</p>
S3AI	S3 テナントアカウント ID (要求の送信者)	要求を送信したユーザのテナントアカウント ID。空の値は匿名アクセスであることを示します。
S3AK	S3 アクセスキー ID (要求の送信者)	要求を送信したユーザのハッシュ済み S3 アクセスキー ID。空の値は匿名アクセスであることを示します。
S3BK	S3 バケット	S3 バケット名。
S3KY	S3 キー	バケット名を除く S3 キーの名前。バケットに対する処理では、このフィールドは指定されません。
S3SR	S3 サブリソース	必要に応じて、処理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 (要求の送信者)	要求を送信したユーザのテナントアカウントの名前。匿名の要求の場合は空です。
saip	IP アドレス (要求送信者)	要求を送信したクライアントアプリケーションの IP アドレス。

コード	フィールド	説明
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。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。
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。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。
サスペンション	S3 ユーザの URN (要求の送信者)	要求を送信しているユーザのテナントアカウント ID とユーザ名。ローカルユーザまたは LDAP ユーザです。例： urn:sgws:identity::03393893651506583485:root  匿名の要求の場合は空です。
時間	時間	要求の合計処理時間 (マイクロ秒)。
TLIP	信頼できるロードバランサの IP アドレス	要求が信頼できるレイヤ 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。
TRNC	切り捨てられる、または切り捨てられない	すべての結果が返された場合はfalseに設定されます。より多くの結果が返される場合はtrueに設定します。GET Bucket処理の場合のみ。
UUID	Universally Unique Identifier の略	StorageGRID システム内で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。バージョン管理に対応していないバケット内のバケットおよびオブジェクトに対する処理には、このフィールドは含まれません。

#### Shea : S3 ヘッド

S3 クライアントが HEAD トランザクションを実行すると、オブジェクトまたはバケットの存在をチェックし、オブジェクトに関するメタデータを読み出す要求が送信されます。このメッセージは、トランザクションが成功した場合にサーバによって出力されません。

コード	フィールド	説明
CBID	Content Block Identifier の略	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。バケットに対する処理では、このフィールドは指定されません。

コード	フィールド	説明
CNID	接続識別子	TCP / IP 接続の一意的システム識別子。
CSIZ	コンテンツサイズ (Content Size)	チェックしたオブジェクトのサイズ (バイト単位)。バケットに対する処理では、このフィールドは指定されません。
HTRH	HTTP 要求ヘッダー	設定時に選択した、ログに記録される HTTP 要求ヘッダーの名前と値のリスト。  <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;"> <p>`X-Forwarded-For` は、要求に存在する場合、およびに存在する場合は自動的に含まれます `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。</p> </div>
RSLT	結果コード	GET トランザクションの結果。常に次の結果になります。  SUCS : 成功しました
S3AI	S3 テナントアカウント ID (要求の送信者)	要求を送信したユーザのテナントアカウント ID。空の値は匿名アクセスであることを示します。
S3AK	S3 アクセスキー ID (要求の送信者)	要求を送信したユーザのハッシュ済み S3 アクセスキー ID。空の値は匿名アクセスであることを示します。
S3BK	S3 バケット	S3 バケット名。
S3KY	S3 キー	バケット名を除く S3 キーの名前。バケットに対する処理では、このフィールドは指定されません。
SACC	S3 テナントアカウント名 (要求の送信者)	要求を送信したユーザのテナントアカウントの名前。匿名の要求の場合は空です。
saip	IP アドレス (要求送信者)	要求を送信し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。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。

コード	フィールド	説明
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。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。
サスペンション	S3 ユーザの URN (要求の送信者)	要求を送信しているユーザのテナントアカウント ID とユーザ名。ローカルユーザまたは LDAP ユーザです。例： urn:sgws:identity::03393893651506583485:root  匿名の要求の場合は空です。
時間	時間	要求の合計処理時間 (マイクロ秒)。
TLIP	信頼できるロードバランサの IP アドレス	要求が信頼できるレイヤ 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	Universally Unique Identifier の略	StorageGRID システム内で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。バージョン管理に対応していないバケット内のバケットおよびオブジェクトに対する処理には、このフィールドは含まれません。

#### SPO : S3 POST

S3 クライアントが POST Object 要求を実行すると、トランザクションが成功した場合にサーバによってこのメッセージが生成されます。

コード	フィールド	説明
CBID	Content Block Identifier の略	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	整合性制御ヘッダー	要求に Consistency-Control HTTP 要求ヘッダーが存在する場合は、その値。
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 (Content Size)	読み出されたオブジェクトのサイズ (バイト単位)。

コード	フィールド	説明
HTRH	HTTP 要求ヘッダー	<p>設定時に選択した、ログに記録される HTTP 要求ヘッダーの名前と値のリスト。</p> <div style="border: 1px solid gray; padding: 10px; margin: 10px 0;"> <p>`X-Forwarded-For` は、要求に存在する場合、およびに存在する場合は自動的に含まれます `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。</p> </div> <p>(SPOS では想定されません)。</p>
RSLT	結果コード	<p>RestoreObject 要求の結果。常に次の結果になります。</p> <p>SUCS : 成功しました</p>
S3AI	S3 テナントアカウント ID (要求の送信者)	要求を送信したユーザのテナントアカウント ID。空の値は匿名アクセスであることを示します。
S3AK	S3 アクセスキー ID (要求の送信者)	要求を送信したユーザのハッシュ済み S3 アクセスキー ID。空の値は匿名アクセスであることを示します。
S3BK	S3 バケット	S3 バケット名。
S3KY	S3 キー	バケット名を除く S3 キーの名前。バケットに対する処理では、このフィールドは指定されません。
S3SR	S3 サブリソース	<p>必要に応じて、処理対象のバケットまたはオブジェクトサブリソース。</p> <p>S3 Select 処理の場合は、を「select」に設定します。</p>
SACC	S3 テナントアカウント名 (要求の送信者)	要求を送信したユーザのテナントアカウントの名前。匿名の要求の場合は空です。
saip	IP アドレス (要求送信者)	要求を送信し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。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。

コード	フィールド	説明
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。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。
SRCF	サブリソースの設定	リストア情報。
サスペンション	S3 ユーザの URN (要求の送信者)	要求を送信しているユーザのテナントアカウント ID とユーザ名。ローカルユーザまたは LDAP ユーザです。例： urn:sgws:identity::03393893651506583485:root  匿名の要求の場合は空です。
時間	時間	要求の合計処理時間 (マイクロ秒)。
TLIP	信頼できるロードバランサの IP アドレス	要求が信頼できるレイヤ 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	Universally Unique Identifier の略	StorageGRID システム内で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。バージョン管理に対応していないバケット内のバケットおよびオブジェクトに対する処理には、このフィールドは含まれません。

#### SPUT : S3 PUT

S3クライアントがPUTトランザクションを実行すると、新しいオブジェクトまたはバケットを作成する要求、またはバケット/オブジェクトサブリソースを削除する要求が送信されます。このメッセージは、トランザクションが成功した場合にサーバによって出力されます。

コード	フィールド	説明
CBID	Content Block Identifier の略	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。バケットに対する処理では、このフィールドは指定されません。
CMP	コンプライアンス設定	バケットの作成時に使用された準拠設定 (要求に存在する場合) (最初の1024文字に切り詰められます)。
CNCH	整合性制御ヘッダー	要求に Consistency-Control HTTP 要求ヘッダーが存在する場合は、その値。

コード	フィールド	説明
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 (Content Size)	読み出されたオブジェクトのサイズ (バイト単位)。バケットに対する処理では、このフィールドは指定されません。
GFID	グリッドフェデレーション接続ID	グリッド間レプリケーション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。デスティネーショングリッドの監査ログにのみ含まれます。
gfsaだ	GridフェデレーションのソースアカウントID	グリッド間レプリケーションPUT要求を行うソースグリッド上のテナントのアカウントID。デスティネーショングリッドの監査ログにのみ含まれます。
HTRH	HTTP 要求ヘッダー	設定時に選択した、ログに記録される HTTP 要求ヘッダーの名前と値のリスト。  <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;"> <p><code>`X-Forwarded-For`</code> は、要求に存在する場合、およびに存在する場合は自動的に含まれます <code>`X-Forwarded-For`</code> 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。</p> </div> <p><code>x-amz-bypass-governance-retention</code> は、要求に含まれている場合は自動的に追加されます。</p>
LKEN	オブジェクトロックが有効になりました	要求ヘッダーの値 <code>x-amz-bucket-object-lock-enabled</code> (リクエストに存在する場合)。
LKLH	オブジェクトロックリーガルホールド	要求ヘッダーの値 <code>x-amz-object-lock-legal-hold</code> (PutObject要求に存在する場合)。
LKMD	オブジェクトロック保持モード	要求ヘッダーの値 <code>x-amz-object-lock-mode</code> (PutObject要求に存在する場合)。
LKRU	オブジェクトロック終了日まで保持	要求ヘッダーの値 <code>x-amz-object-lock-retain-until-date</code> (PutObject要求に存在する場合)。
MTME	最終変更時刻	オブジェクトが最後に変更された日時を示す Unix タイムスタンプ (マイクロ秒)。

コード	フィールド	説明
RSLT	結果コード	PUT トランザクションの結果。常に次の結果になります。  SUCS : 成功しました
S3AI	S3 テナントアカウント ID (要求の送信者)	要求を送信したユーザのテナントアカウント ID。空の値は匿名アクセスであることを示します。
S3AK	S3 アクセスキー ID (要求の送信者)	要求を送信したユーザのハッシュ済み S3 アクセスキー ID。空の値は匿名アクセスであることを示します。
S3BK	S3 バケット	S3 バケット名。
S3KY	S3 キー	バケット名を除く S3 キーの名前。バケットに対する処理では、このフィールドは指定されません。
S3SR	S3 サブリソース	必要に応じて、処理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 (要求の送信者)	要求を送信したユーザのテナントアカウントの名前。匿名の要求の場合は空です。
saip	IP アドレス (要求送信者)	要求を送信し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。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。
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。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。
SRCF	サブリソースの設定	新しいサブリソース設定 (最初の 1024 文字に切り詰められます)。
サスペンション	S3 ユーザの URN (要求の送信者)	要求を送信しているユーザのテナントアカウント ID とユーザ名。ローカルユーザまたは LDAP ユーザです。例： <code>urn:sgws:identity::03393893651506583485:root</code>  匿名の要求の場合は空です。
時間	時間	要求の合計処理時間 (マイクロ秒)。

コード	フィールド	説明
TLIP	信頼できるロードバランサの IP アドレス	要求が信頼できるレイヤ 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	ID をアップロードします	CompleteMultipartUpload処理の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、アSEMBLされたことを示します。
UUID	Universally Unique Identifier の略	StorageGRID システム内で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で作成された新しいオブジェクトのバージョン ID。バージョン管理に対応していないバケット内のバケットおよびオブジェクトに対する処理には、このフィールドは含まれません。
VSST	バージョン管理の状態	バケットの新しいバージョン管理状態。「enabled」または「suspended」の2つの状態が使用されます。オブジェクトに対する処理には、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、コンテンツが永続的ストレージから削除され、通常の API でアクセスできなくなった場合に表示されます。

コード	フィールド	説明
CBID	Content Block Identifier の略	永続的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	コンテンツ削除処理の結果を示します。次の値のみが定義されています。  SUCS : コンテンツが永続的ストレージから削除されました

この監査メッセージは、指定された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。このメッセージを使用して、システム内の削除されたコンテンツのフローを追跡できます。

#### 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まれた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。このメッセージは、メタデータの更新が成功した場合にサーバによって出力されます。

コード	フィールド	説明
CBID	Content Block Identifier の略	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。バケットに対する処理では、このフィールドは指定されません。
CNCH	整合性制御ヘッダー	バケットの準拠設定の更新時に要求に Consistency-Control HTTP 要求ヘッダーが存在する場合は、その値。
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 (Content Size)	読み出されたオブジェクトのサイズ (バイト単位)。バケットに対する処理では、このフィールドは指定されません。
HTRH	HTTP 要求ヘッダー	設定時に選択した、ログに記録される HTTP 要求ヘッダーの名前と値のリスト。  <div style="border: 1px solid gray; padding: 5px; margin: 5px 0;"> <p>``X-Forwarded-For`` は、要求に存在する場合、およびに存在する場合は自動的に含まれます ``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。</p> </div>
RSLT	結果コード	GET トランザクションの結果。常に次の結果になります。  SUCS : 成功しました
S3AI	S3 テナントアカウント ID (要求の送信者)	要求を送信したユーザのテナントアカウント ID。空の値は匿名アクセスであることを示します。
S3AK	S3 アクセスキー ID (要求の送信者)	要求を送信したユーザのハッシュ済み S3 アクセスキー ID。空の値は匿名アクセスであることを示します。
S3BK	S3 バケット	S3 バケット名。
S3KY	S3 キー	バケット名を除く S3 キーの名前。バケットに対する処理では、このフィールドは指定されません。
SACC	S3 テナントアカウント名 (要求の送信者)	要求を送信したユーザのテナントアカウントの名前。匿名の要求の場合は空です。

コード	フィールド	説明
saip	IP アドレス (要求送信者)	要求を送信し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。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。
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。クロスアカウントアクセスまたは匿名アクセスの識別に使用します。
サスペンション	S3 ユーザの URN (要求の送信者)	要求を送信しているユーザのテナントアカウント ID とユーザ名。ローカルユーザまたは LDAP ユーザです。例： urn:sgws:identity::03393893651506583485:root  匿名の要求の場合は空です。
時間	時間	要求の合計処理時間 (マイクロ秒)。
TLIP	信頼できるロードバランサの IP アドレス	要求が信頼できるレイヤ 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	Universally Unique Identifier の略	StorageGRID システム内で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。バージョン管理に対応していないバケット内のバケットおよびオブジェクトに対する処理には、このフィールドは含まれません。

**SVRF** : オブジェクトストアの検証に失敗しました

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したときに生成されます。レプリケートされたオブジェクトデータがディスクに対して読み書きされるたびに、要求元ユーザに送信されるデータがシステムにもともと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複数の検証チェック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、破損したレプリケートオブジェクトデータは再び読み出されないように自動的に隔離されます。

コード	フィールド	説明
CBID	Content Block Identifier の略	検証に失敗したコンテンツブロックの一意的識別子。

コード	フィールド	説明
RSLT	結果コード	<p>検証失敗のタイプ：</p> <p>CRCF : 巡回冗長検査 (CRC) が失敗しました。</p> <p>HMAC : ハッシュベースのメッセージ認証コード (HMAC) チェックが失敗しました。</p> <p>EHSB : 暗号化されたコンテンツハッシュが想定外です。</p> <p>PHSH : 元のコンテンツハッシュが想定外です。</p> <p>SEQC : ディスク上のデータシーケンスが正しくありません。</p> <p>PERR : ディスクファイルの構造が無効です。</p> <p>DERR : ディスクエラーです。</p> <p>FNAM : ファイル名が無効です。</p>



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、ハードウェア障害の兆候を示している可能性があります。

メッセージをトリガーした処理を確認するには、AMID (Module ID) フィールドの値を参照してください。たとえば、SVFY はバックグラウンド検証である Storage Verifier モジュールによってメッセージが生成されたことを示し、STOR はコンテンツの読み出しによってメッセージがトリガーされたことを示します。

**SVRU** : オブジェクトストア検証が不明です

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レプリケート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、レプリケートされたオブジェクトデータの不明または想定外のコピーがオブジェクトストアで検出されて隔離ディレクトリに移動されたときに生成されます。

コード	フィールド	説明
FPTH	ファイルパス	想定外の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該当しません。このメッセージがフィルタリングされないように、「UCS」ではなく「none」が使用されます。



**SVRU** : Object Store Verify Unknown 監査メッセージは注意深く監視する必要があります。オブジェクトストアでオブジェクトデータの想定外のコピーが検出されたことを意味します。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、この状況をすぐに調査してこれらのコピーが作成された方法を特定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ためにこのメッセージが生成されます。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、通常、このメッセージは次の再起動後にのみ送信されます。サービスが再起動していない場合は、シャットダウンシーケンスの最初に送信された SYST メッセージを確認します。

コード	フィールド	説明
RSLT	シャットダウンをクリーニングします	シャットダウンのタイプ： SUCS : システムはクリーンシャットダウンされました。

このメッセージが示すのはレポート元のサービスの停止のみで、ホストサーバの停止については示されません。SYSDのRSLTは、「クリーン」シャットダウンによってのみ生成されるため、「ダーティー」シャットダウンを示すことはできません。

**SYST** : ノードを停止しています

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て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ためにこのメッセージが生成されます。SYSTを使用すると、シャットダウンが要求されたかどうかをサービスが再起動される前に特定できません（SYSDは通常、サービスの再起動後に送信されます）。

コード	フィールド	説明
RSLT	シャットダウンをクリーニングします	シャットダウンのタイプ： SUCS : システムはクリーンシャットダウンされました。

このメッセージが示すのはレポート元のサービスの停止のみで、ホストサーバの停止については示されません。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生成されるため、「ダーティー」シャットダウンを示すことはできません。

**SYSU** : ノードが開始されました

サービスが再起動されると、前回のシャットダウンがクリーン（コマンドによるもの）か不規則（想定外）かを示すため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
RSLT	シャットダウンをクリーニングします	シャットダウンのタイプ： SUCS : システムはクリーンシャットダウンされました。 DSDN : システムはクリーンシャットダウンされませんでした。 VRGN : サーバインストール（または再インストール）後の初めての起動です。

このメッセージが示すのはレポート元のサービスの起動のみで、ホストサーバの起動については示されません。このメッセージは、次の場合に使用できます。

- 監査証跡における不連続を検出します。
- サービスが処理中に失敗していないかどうかを確認します（StorageGRID システムの分散によってこれらのエラーが隠されることがあります）。失敗したサービスは、Server Manager によって自動的に再開されます。

#### WDEL : Swift の削除

Swift クライアントが DELETE トランザクションを実行すると、指定したオブジェクトまたはコンテナを削除する要求が送信されます。このメッセージは、トランザクションが成功した場合にサーバによって出力されます。

コード	フィールド	説明
CBID	Content Block Identifier の略	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 (Content Size)	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 要求ヘッダー	設定時に選択した、ログに記録される HTTP 要求ヘッダーの名前と値のリスト。 <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> `X-Forwarded-For` は、要求に存在する場合、およびに存在する場合は自動的に含まれます `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。 </div>
MTME	最終変更時刻	オブジェクトが最後に変更された日時を示す Unix タイムスタンプ (マイクロ秒)。

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。常に次の結果になります。  SUCS : 成功しました
saip	要求元クライアントの IP アドレス	要求を送信し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)	オブジェクトが存在する場合は、指定したサイトで削除されています。このサイトは、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	時間	要求の合計処理時間 (マイクロ秒)。
TLIP	信頼できるロードバランサの IP アドレス	要求が信頼できるレイヤ 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	Universally Unique Identifier の略	StorageGRID システム内で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 オブジェクトの識別子。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	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名。

#### wget : Swift GET

Swift クライアントが GET トランザクションを実行すると、オブジェクトを読み出す、コンテナ内のオブジェクトを一覧表示する、またはアカウント内のコンテナを一覧表示する要求が送信されます。このメッセージは、トランザクションが成功した場合にサーバによって出力されます。

コード	フィールド	説明
CBID	Content Block Identifier の略	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関する操作には、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 (Content Size)	読み出され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関する操作には、このフィールドは含まれません。
HTRH	HTTP 要求ヘッダー	設定時に選択した、ログに記録される HTTP 要求ヘッダーの名前と値のリスト。  <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p>``X-Forwarded-For`` は、要求に存在する場合、およびに存在する場合は自動的に含まれます ``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。</p> </div>
RSLT	結果コード	GET トランザクションの結果。結果は常にです  SUCS : 成功しました
saip	要求元クライアントの IP アドレス	要求を送信したクライアントアプリケーションの IP アドレス。
時間	時間	要求の合計処理時間 (マイクロ秒)。
TLIP	信頼できるロードバランサの IP アドレス	要求が信頼できるレイヤ 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	Universally Unique Identifier の略	StorageGRID システム内で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。アカウントの操作には、このフィールドは含まれません。
WOBJ	Swift オブジェクト	Swift オブジェクトの識別子。アカウントおよびコンテナに関する操作には、このフィールドは含まれません。
WUSR	Swift アカウントユーザ	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名。

Swift クライアントが HEAD トランザクションを実行すると、アカウント、コンテナ、またはオブジェクトの存在をチェックし、関連するメタデータを読み出す要求が送信されます。このメッセージは、トランザクションが成功した場合にサーバによって出力されます。

コード	フィールド	説明
CBID	Content Block Identifier の略	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関する操作には、このフィールドは含まれません。
CSIZ	コンテンツサイズ (Content Size)	読み出され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関する操作には、このフィールドは含まれません。
HTRH	HTTP 要求ヘッダー	設定時に選択した、ログに記録される HTTP 要求ヘッダーの名前と値のリスト。  <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;"> <p>``X-Forwarded-For`` は、要求に存在する場合、およびに存在する場合は自動的に含まれます ``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。</p> </div>
RSLT	結果コード	HEAD トランザクションの結果。常に次の結果になります。  SUCS : 成功しました
saip	要求元クライアントの IP アドレス	要求を送信したクライアントアプリケーションの IP アドレス。
時間	時間	要求の合計処理時間 (マイクロ秒)。
TLIP	信頼できるロードバランサの IP アドレス	要求が信頼できるレイヤ 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	Universally Unique Identifier の略	StorageGRID システム内で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。

コード	フィールド	説明
WCON	Swift コンテナ	Swift コンテナ名。アカウントの操作には、このフィールドは含まれません。
WOBJ	Swift オブジェクト	Swift オブジェクトの識別子。アカウントおよびコンテナに関する操作には、このフィールドは含まれません。
WUSR	Swift アカウントユーザ	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名。

#### WPUT : Swift PUT

Swift クライアントが PUT トランザクションを実行すると、新しいオブジェクトまたはコンテナを作成する要求が送信されます。このメッセージは、トランザクションが成功した場合にサーバによって出力されます。

コード	フィールド	説明
CBID	Content Block Identifier の略	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 (Content Size)	読み出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 要求ヘッダー	設定時に選択した、ログに記録される HTTP 要求ヘッダーの名前と値のリスト。  <div style="border: 1px solid #ccc; padding: 5px; background-color: #f9f9f9;"> <p>`X-Forwarded-For` は、要求に存在する場合、およびに存在する場合は自動的に含まれます `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。</p> </div>
MTME	最終変更時刻	オブジェクトが最後に変更された日時を示す Unix タイムスタンプ (マイクロ秒)。
RSLT	結果コード	PUT トランザクションの結果。常に次の結果になります。  SUCS : 成功しました
saip	要求元クライアントの IP アドレス	要求を送信したクライアントアプリケーションの IP アドレス。

コード	フィールド	説明
時間	時間	要求の合計処理時間（マイクロ秒）。
TLIP	信頼できるロードバランサの IP アドレス	要求が信頼できるレイヤ 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	Universally Unique Identifier の略	StorageGRID システム内で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 オブジェクトの識別子。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	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权を有し、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权については、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。