



StorageGRID

システムのトラブルシューティングを行う

StorageGRID 11.8

NetApp
March 19, 2024

目次

StorageGRID システムのトラブルシューティングを行う	1
StorageGRID システムのトラブルシューティング：概要	1
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	8
メタデータに関する問題のトラブルシューティング	45
証明書エラーのトラブルシューティングを行う	52
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	53
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	59
外部 syslog サーバのトラブルシューティングを行います	68

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。
問題が定期的発生する場合は、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"> 最近の変更のタイムラインを作成します
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"> "現在のアラートと解決済みのアラートを表示します" "アラームの管理 (従来のシステム)"
イベントを監視する	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。	<ul style="list-style-type: none"> "イベントを監視する"
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	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。	<ul style="list-style-type: none"> "チャートとグラフを使用します" "テキストレポートを使用する"

収集するデータのタイプ	データを収集する理由	手順
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。	<ul style="list-style-type: none"> • ベースラインを設定する
取り込みと読み出しのテストを実行する	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。	<ul style="list-style-type: none"> • "PUT / GET パフォーマンスを監視"
監査メッセージを確認します	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。	<ul style="list-style-type: none"> • "監査メッセージを確認します"
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	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。	<ul style="list-style-type: none"> • "オブジェクト検証処理を監視する" • "オブジェクトデータの場所を確認する" • "オブジェクトの整合性を検証"
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"> • "ログファイルとシステムデータを収集" • "AutoSupportパッケージを手動でトリガーする" • "サポート指標を確認"

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
例： <ul style="list-style-type: none"> ノードのリカバリを開始したのはいつですか？ ソフトウェアのアップグレードはいつ完了しましたか？ プロセスを中断しましたか？ 	どうしましたか？何をしましたか？	変更に関連する詳細を文書化します。例： <ul style="list-style-type: none"> ネットワークの詳細が変更されました。 インストールされたホットフィックス。 クライアントのワークロードの変化 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。

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。
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。

プロパティ (Property)	価値	取得方法
ILM 評価の速度	オブジェクト数 / 秒	<p>ノードページで、 * GRID_NETWORK* > * ILM * を選択します。</p> <p>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。</p>
ILM のスキャン速度	オブジェクト数 / 秒	<p>ノード * > * GRID_NETWORK* > * ILM * を選択します。</p> <p>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。</p>
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	<p>ノード * > * GRID_NETWORK* > * ILM * を選択します。</p> <p>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。</p>
クエリの平均レイテンシ	表示されます	<p>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。</p>

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>問題を定義します</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"> クライアントは以前に正常に接続されていますか？ 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。
	StorageGRID システム ID	<p>[* 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。]</p>
	ソフトウェアのバージョン	<p>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。</p>
	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"> 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？ 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。
	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 * > * Tools * > * 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>"ログファイルとシステムデータを収集"</p>

✓	項目	注：
	ベースライン情報	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。 ベースラインを設定する
	最近の変更のタイムライン	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 最近の変更のタイムラインを作成します
	問題を診断するための取り組みの歴史	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。

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の識別子。監査ログからオブジェクトの CBID を取得できます。CBID はすべて大文字で入力します。
 - * 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ブ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

Version ID (optional)

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 個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。



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: -

Progress: 0% Estimated time to completion: -

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る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

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. 入力するコマンド `cd /var/local/log`
 - 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. 入力するコマンド `zgrep SPUT * | egrep "CSIZ\(UI64\):[0-9]*[5-9][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トをリセットします"](#)。

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

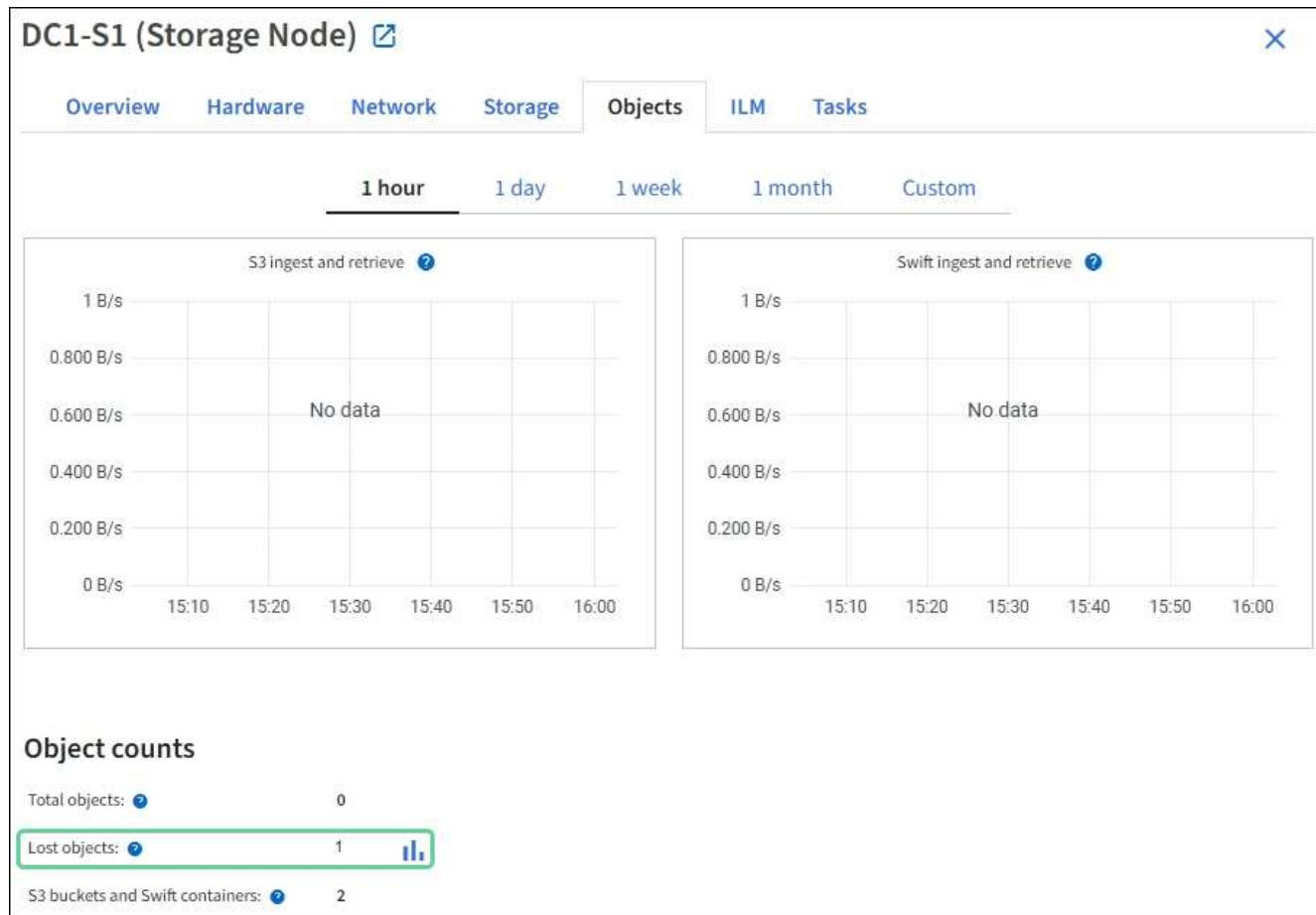
- Objects lost * アラートは、StorageGRID がグリッド内にオブジェクトのコピーがないと判断したことを示します。データが完全に失われた可能性があります。

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。入力するコマンド `cd /var/local/log/`
 - 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 OLSL 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):OLSL][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. Telnet で localhost 1402 に接続して、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 "失われた可能性があるオブジェクトの検索" 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 "オブジェクトを検索してリストアップします" 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 "Grid Managerを使用したオブジェクトデータのリストアップ" および "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"。</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して特定した) 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。 `cd /var/local/log/`

- 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 >
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 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):
1581535134379225][ATYP(FC32):LLST][ANID(UI32):12448208][AMID(FC32):CL
SM]
[ATID(UI64):7086871083190743409]]
```

- 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. Telnet で localhost 1402 に接続して、LDR コンソールにアクセスします。入力するコマンド `telnet 0 1402`
- 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。 `cd /var/local/log/`
- 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 >
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 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tr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tr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

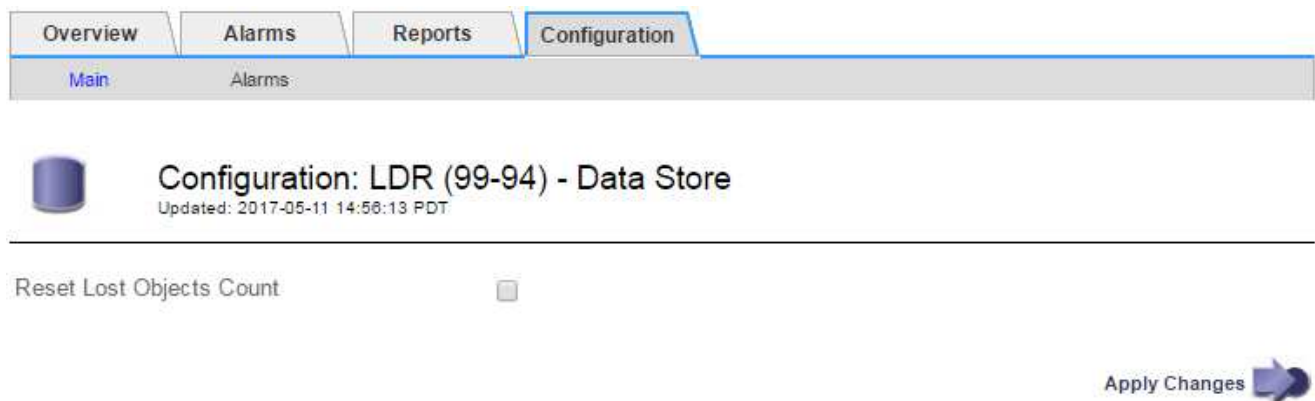
Lost Objects カウンtrは次のどちらかのページからリセットできます。

- * サポート * > * Tools * > * 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、**ldr>*Data Store*** ページからカウンtr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。



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。

- a. [Site>Storage Node>LDR>erasure Coding>Configuration] を選択します。
- b. 「Reset Reads Failure Count」と「Reset Corrupt Copies Detected Count」を選択します。
- c. [変更の適用 *] をクリックします。
- d. [*_サイト_*>*_ストレージ・ノード_*>LDR*>Verification*>Configuration*] を選択します。
- e. 「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。
- f. 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

プロ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。

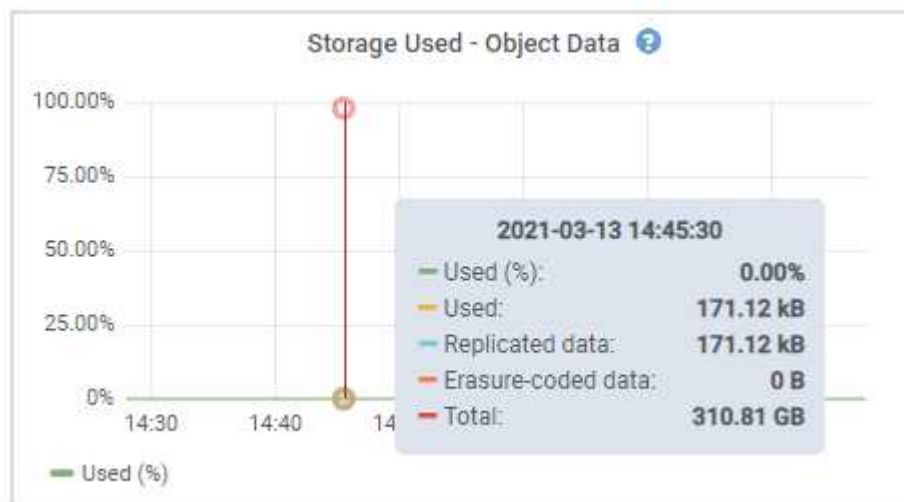
- トリガーされた時刻
- サイトとノードの名前
- このアラートに関する指標の現在の値

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

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ほぼ完全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。

Nodes

View the list and status of sites and grid nodes.

Search... Total node count: 13

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。

- 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](#)。
- 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

- [**support**>]、[*Tools]、[*Metrics] の順に選択します。
- 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。
- 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

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。



Alarms: LDR (DC1-S3-101-195) - Storage

Updated: 2019-10-09 12:52:43 MDT

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"/>

Apply Changes

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。

- 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。

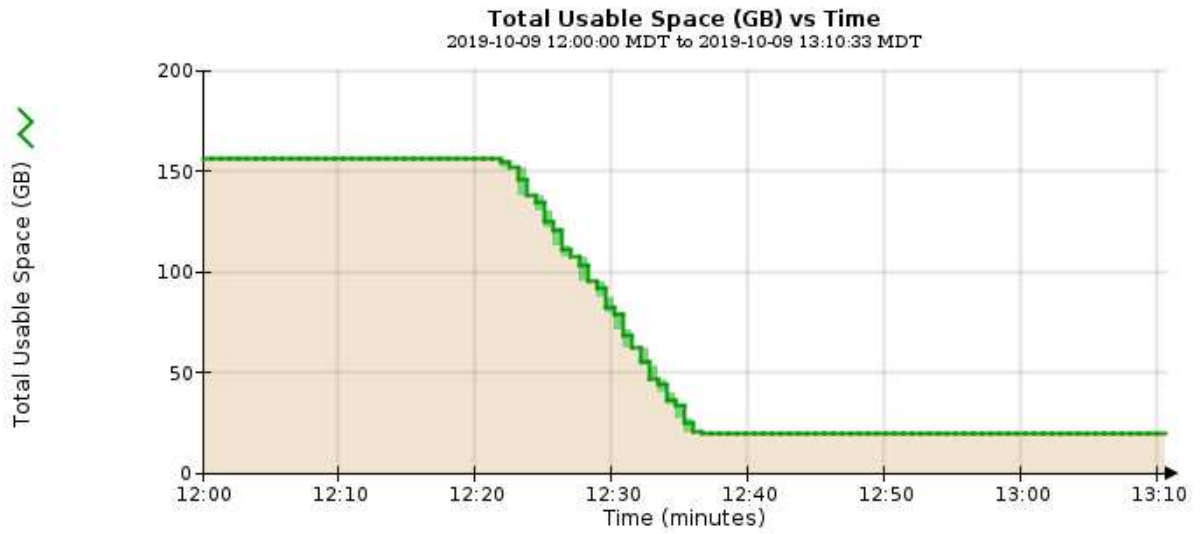
この例では、12 : 00 の時点の使用可能な合計スペースは約 155 GB でしたが、12 : 35 には 20 GB まで減り、その時点で SSTS アラームがトリガーされています。



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。

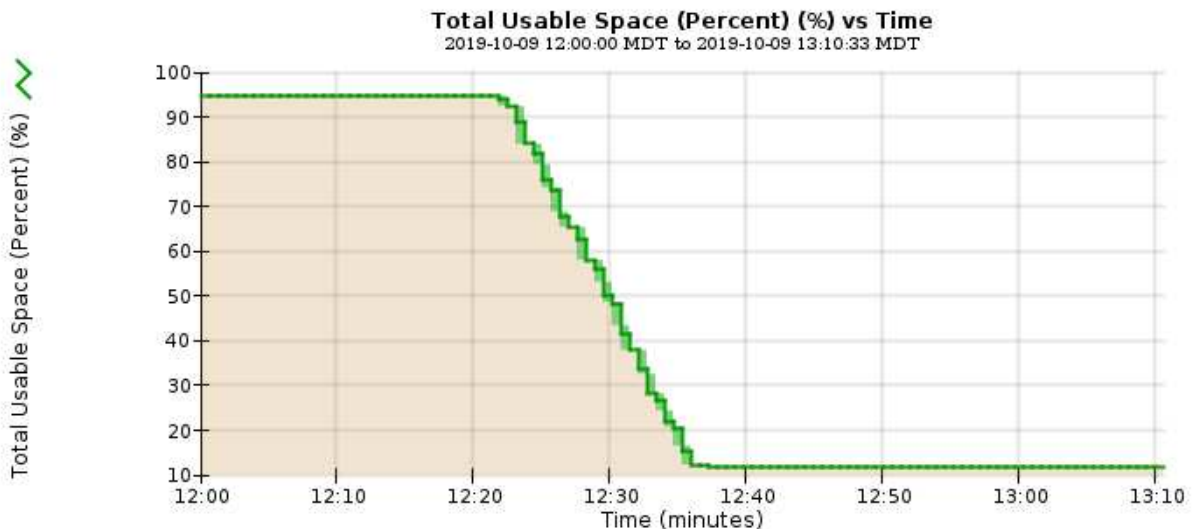
この例では、ほぼ同じタイミングで使用可能な合計スペースが 95% から 10% 強に減少しています。

Overview | Alarms | **Reports** | Configuration

Charts | Text

 Reports (Charts): LDR (DC1-S1-101-193) - Storage

Attribute: Total Usable Space (Percent) Vertical Scaling: Start Date: 2019/10/09 12:00:00
 Quick Query: Custom Query Update Raw Data: End Date: 2019/10/09 13:10:33



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す。

Low metadata storage アラート

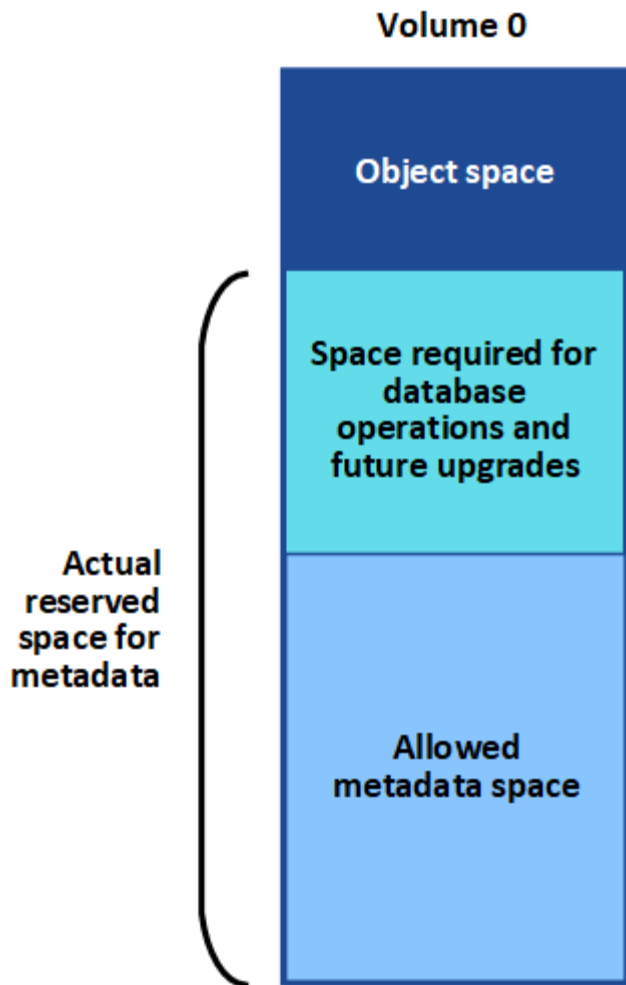
Low metadata storage * アラートがトリガーされた場合は、新しいストレージノードを追加する必要があります。

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。



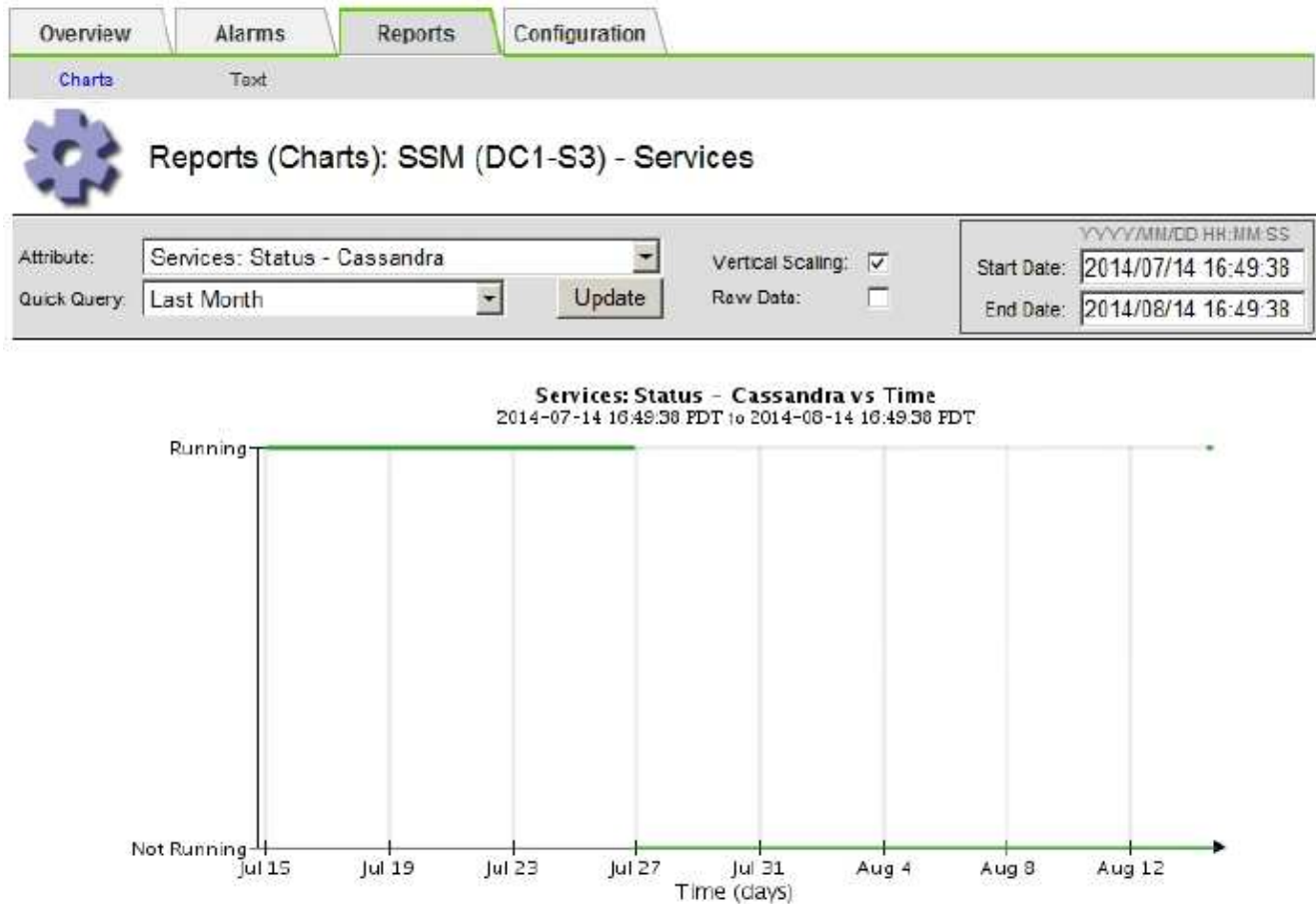
複数のCassandraデータベースサービスが停止している場合は、次の手順は実行せずにテクニカルサポートに連絡してください。

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. イベントを表示するには、* support * > * Tools * > * Grid topology * > * Configuration * 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. 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。
4. 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。

5. 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。

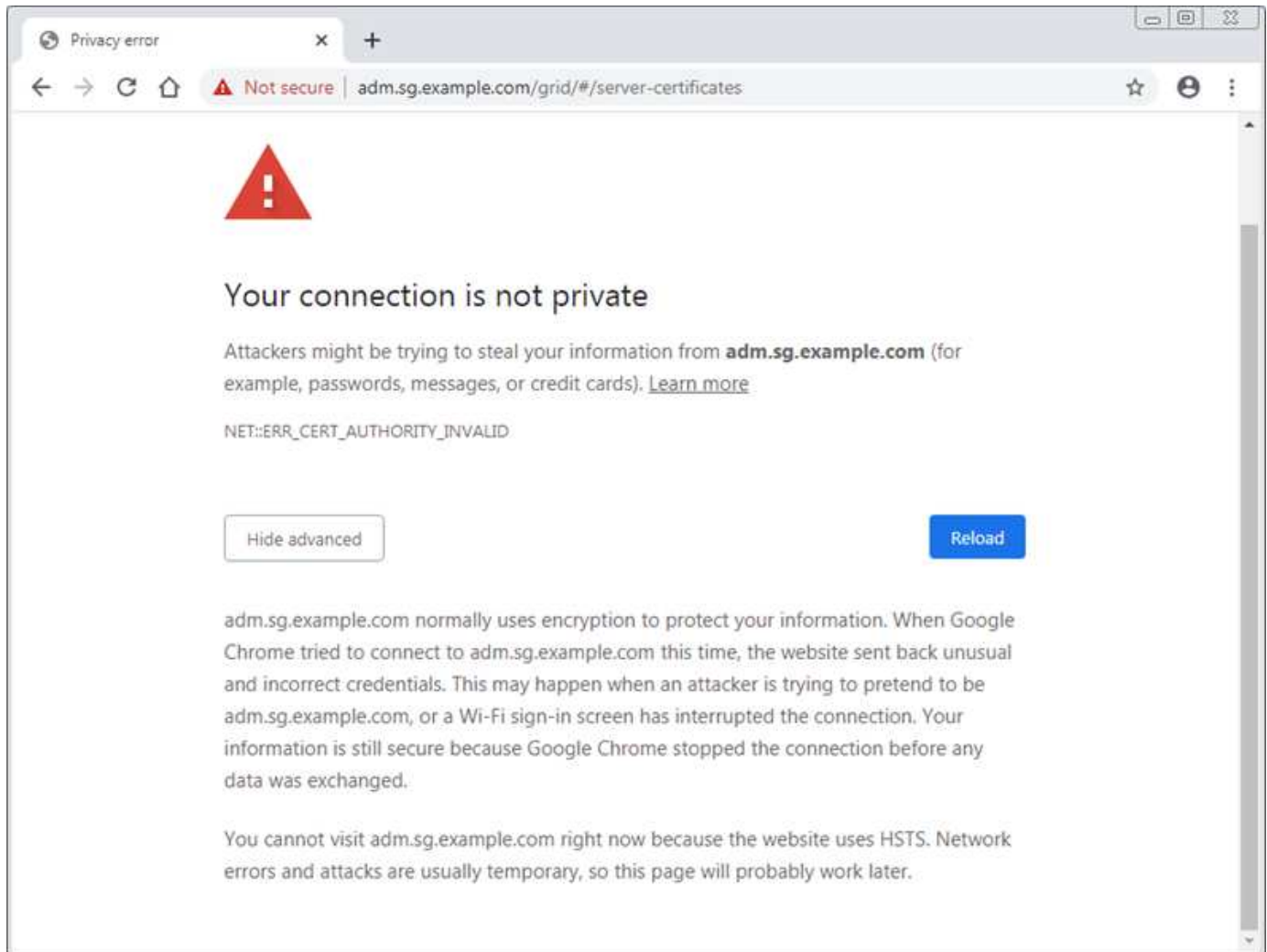
このタスクについて

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、**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。

- a. 次のコマンドを入力します。 `ssh admin@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: `#`。

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](#)"。

ユーザー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のユーザー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 "StorageGRID でサポートされている暗号" 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">• グリッド (Grid)• 管理• クライアント

+

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）。
 - ["SGF6112を参照してください"](#)
 - ["SG6000を使用します"](#)
 - ["SG5700"](#)
 - ["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이스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이스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이스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 * アラーム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 アラーム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

- まだイネーブルになっていない場合は、FEC をイネーブル
- 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。
- 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可能性があります。

NIC リングバッファオーバーラン

エラーが NIC リング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。

- 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。
 - サポート * > * ツール * > * グリッドトポロジ * を選択します。
 - _site * > * _grid node_name > * SSM * > * Resources * > * Configuration * > * Main * を選択します。
 - [* 受信エラーカウンタをリセットする *] 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
```

- 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
```

- 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">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。2. DNS サーバが正しく設定されていることを確認します。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。
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">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。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。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。
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">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。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。
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">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。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。

エラーメッセージです	概要 および推奨される対処方法
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"> 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。 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。 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。
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"> • 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。 • ノードと syslog サーバで TCP / TLS 設定が異なる場合があります。 • 中間ファイアウォールがアイドル状態の TCP 接続を閉じている可能性があります。 • syslog サーバ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。 <p>この問題を解決するには：</p> <ol style="list-style-type: none"> 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。 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。 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。
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"> 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。 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。

エラーメッセージです	概要 および推奨される対処方法
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"> 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。 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。 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。 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。 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。
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"> 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。 2. 表示されたノードで miscd サービスを再起動します。

著作権に関する情報

Copyright © 2024 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。