



システムパフォーマンスを監視 VCP

NetApp
November 18, 2025

目次

| | |
|--|----|
| システムパフォーマンスを監視 | 1 |
| Reporting オプションを使用してシステムパフォーマンスを監視します | 1 |
| 詳細については、こちらをご覧ください | 1 |
| 概要ページでクラスタ全体の健全性を監視します | 1 |
| レポート概要ページのデータ | 1 |
| 詳細については、こちらをご覧ください | 3 |
| システムアラートを監視する | 3 |
| 詳細については、こちらをご覧ください | 5 |
| システムアラートのリスト | 5 |
| イベントログを監視してトラブルシューティングを行う | 22 |
| イベントタイプ | 22 |
| 詳細については、こちらをご覧ください | 24 |
| ボリュームのパフォーマンスを監視 | 24 |
| ボリュームのパフォーマンスデータ | 25 |
| 詳細については、こちらをご覧ください | 25 |
| iSCSI セッションを監視して接続ステータスを確認 | 25 |
| iSCSI セッションデータ | 26 |
| 詳細については、こちらをご覧ください | 26 |
| QoSSIOC イベントを使用して VM のパフォーマンス階層化を監視します | 26 |
| QoSSIOC イベントデータ | 27 |
| 詳細については、こちらをご覧ください | 27 |

システムパフォーマンスを監視

Reporting オプションを使用してシステムパフォーマンスを監視します

NetApp Element Plug-in for VMware vCenter Serverのレポートページを使用して、クラスタのコンポーネントとパフォーマンスに関する情報を表示できます。

vCenter Plug-in を使用すると、次の方法でクラスタコンポーネントとパフォーマンスを監視できます。

- ["概要ページでクラスタ全体の健全性を監視します"](#)
- ["システムアラートを監視する"](#)
- ["イベントログを監視してトラブルシューティングを行う"](#)
- ["ボリュームのパフォーマンスを監視"](#)
- ["iSCSI セッションを監視して接続ステータスを確認"](#)
- ["QoSSIOC イベントを使用して VM のパフォーマンス階層化を監視します"](#)

詳細については、こちらをご覧ください

- ["NetApp HCI のドキュメント"](#)
- ["SolidFire and Element Resources ページにアクセスします"](#)

概要ページでクラスタ全体の健全性を監視します

NetApp Element Plug-in for VMware vCenter ServerのNetApp Element Management拡張ポイントから、レポートタブの概要ページで、選択したクラスタの全体的な容量、効率、パフォーマンスなどのクラスタ情報を確認できます。

手順

1. vCenter Plug-inで、* Reporting *タブを開きます。
 - Element vCenterプラグイン5.0以降では、* NetApp Element リモートプラグイン>管理>レポート*を選択します。
 - Element vCenterプラグイン4.10以前の場合は、* NetApp Element Management > Reporting *の順に選択します。
2. [概要 (Overview *)]ページでデータを監視します。

レポート概要ページのデータ

レポート概要ページには、次のデータが表示されます。

- * クラスタ容量 * : ブロックストレージ、メタデータ、プロビジョニングスペースの残りの容量。しきい値の情報を確認するには、進捗状況バーの上にポインタを移動します。

- * クラスタ情報 * : クラスタ名、クラスタで実行されている NetApp Element ソフトウェアのバージョン、MVIP アドレスと SVIP アドレス、クラスタのノード、4k IOPS、ボリューム、セッションの数など、クラスタに固有の情報。
 - * Cluster Name * : クラスタの名前。
 - * Storage IP (SVIP) * : ストレージ仮想 IP アドレス (SVIP)。
 - * Management IP (MVIP) * : 管理仮想 IP アドレス (MVIP)。
 - * SVIP VLAN Tag * : マスター SVIP アドレスの VLAN 識別子。
 - * MVIP VLAN Tag * : マスター MVIP アドレスの VLAN 識別子。
 - * Node Count * : クラスタ内のアクティブノードの数。
 - * クラスタの 4K IOPS * : クラスタで 1 秒間に読み取り / 書き込みできる 4096 (4K) ブロックの数。
 - * Element OS Version * : クラスタで実行されている NetApp Element ソフトウェアのバージョン。
 - * Volume Count * : クラスタ上の仮想ボリュームを除くボリュームの総数。
 - * Virtual Volume Count * : クラスタの仮想ボリュームの総数。
 - * iSCSI Sessions * : クラスタに接続されている iSCSI セッション。
 - * Fibre Channel Sessions * : クラスタに接続されている Fibre Channel セッション。
- * クラスタ効率 * : シンプロビジョニング、重複排除、および圧縮を考慮した、システム全体の容量。クラスタでの効率化は、シンプロビジョニング、重複排除、および圧縮を使用しない従来のストレージデバイスにおける容量使用率と比較して計算されます。
- * 保護ドメイン * : クラスタの保護ドメイン監視の概要。



保護ドメイン機能は 2 ノードクラスタには対応していません。

- * 保護ドメイン監視レベル * : ユーザが選択した保護ドメインの耐障害性レベル。有効な値は、Chassis または Node です。緑は、クラスタが選択した監視レベルに対応していることを示します。赤は、クラスタが選択した監視レベルに対応しておらず、対処が必要なことを示します。
 - * Remaining Block Capacity * : 選択した耐障害性レベルを維持するために残っているブロック容量の割合を示します。
 - * メタデータ容量 * : データの可用性を中断せずに障害から回復するための十分なメタデータ容量があるかどうかを示します。Normal (緑) は、選択した監視レベルを維持するための十分なメタデータがクラスタにあることを示します。フル (赤) は、クラスタが選択した監視レベルに対応しておらず、対処が必要なことを示します。
- カスタム保護ドメインの正常性: クラスタにカスタム保護ドメインが設定されている場合、クラスタのカスタム保護ドメインの正常性ステータスが表示されます。

次のデータは、クラスタのいずれかのカスタム保護ドメインで障害が発生した場合に使用できる保護を示しています。

- 保護レベル: 全体的な保護レベルのステータスを示します。
- ブロック容量: ブロックサービスサブシステムの現在の保護レベルステータスを示します。

また、耐障害性が失われる合計容量のしきい値も示します。

- メタデータ容量：メタデータサービスサブシステムの現在の保護レベルステータスを示します。
- アンサンブルノード：アンサンブルメンバーサブシステムの現在の保護レベルステータスを示します。
- * プロビジョニングされた IOPS *：クラスタ上のボリュームの IOPS について、オーバースプロビジョニングの状況の概要。プロビジョニングされる IOPS の計算は、クラスタ上のすべてのボリュームの最小 IOPS、最大 IOPS、バースト IOPS の合計を、クラスタの最大 IOPS で割った値になります。



たとえば、クラスタに 4 つのボリュームがあり、それぞれ最小 IOPS が 500、最大 IOPS が 15、000、バースト IOPS が 15、000 の場合、最小 IOPS の合計数は 2、000、最大 IOPS の合計が 6、000、バースト IOPS の合計が 6、000 になります。クラスタの定格の最大 IOPS が 50、000 の場合、計算は次のようになります。* 最小 IOPS *：
 $2000/50000 = 0.04x$ * 最大 IOPS *： $60000/50000 = 1.20x$ * Burst IOPS *： $60000/50000 = 1.20x$
 $0.04x + 1.20x + 1.20x$ は、プロビジョニングされた IOPS がクラスタの IOPS と同じとなるベースラインです。

- * クラスタヘルス *：クラスタのハードウェア、容量、およびセキュリティコンポーネント。色分けは次のように表示されます。
 - * 緑 *：健康
 - * 黄 *：重大
 - * 赤 *：エラー
- * クラスタ入出力 *：クラスタで現在実行されている I/O。値は、前回の I/O 測定値と現在の I/O 測定値から計算されます。グラフに表示される測定値を次に示します。
 - * Total *：システムで発生している読み取りと書き込みの IOPS の合計。
 - * Read *：発生している読み取り IOPS。
 - * Write *：書き込み IOPS。
- * クラスタスループット *：クラスタ上の読み取り、書き込み、および合計の帯域幅アクティビティ。
 - * 合計 *：クラスタ内の読み取りと書き込みの両方のアクティビティに使用されている合計 MBps。
 - * Read *：クラスタの読み取りアクティビティ（MB/秒）。
 - * Write *：クラスタの書き込みアクティビティを MBps で示します。
- * パフォーマンス利用率 *：消費されているクラスタ IOPS の割合。たとえば、25 万 IOPS のクラスタが 10 万 IOPS で実行されている場合、消費率は 40% です。

詳細については、こちらをご覧ください

- ["NetApp HCI のドキュメント"](#)
- ["SolidFire and Element Resources ページにアクセスします"](#)

システムアラートを監視する

クラスタの稼働状況を示す情報、警告、またはエラーであるアラートを監視できます。

アラートはクラスタの障害またはエラーであり、発生時に報告されます。ほとんどのエラーは自動的に解決しますが、一部のエラーでは手動での対応が必要です。アラートページの各アラートについて、アラートエラー

コードが報告されます。エラーコードは、アラートが発生したシステムのコンポーネントおよびアラートが生成された理由を判断する場合に役立ちます。を参照してください "[システムアラートのリスト](#)" を参照してください。

問題を解決すると、システムが問題をポーリングし、解決済みであることを特定します。その後、アラートに関するすべての情報（解決日を含む）が解決済みビューに移動します。

手順

1. vCenter Plug-inで、* Management *タブを開きます。
 - Element vCenterプラグイン5.0以降では、* NetApp Element リモートプラグイン>管理>管理*を選択します。
 - Element vCenterプラグイン4.10以前の場合は、* NetApp Element Management > Management *を選択します。
2. **[Reporting>*Alerts*]** を選択します。
3. 次のクラスタアラート情報を監視します。
 - * ID * : クラスタアラートの一意の ID 。
 - * 重大度 *
 - * warning * : 近々対応が必要になる可能性があるが、マイナー問題。この重大度レベルでは、システムのアップグレードは引き続き可能です。
 - * error * : 原因のパフォーマンスが低下したり高可用性（HA）が失われたりする可能性のある障害です。通常、エラーがサービスに影響することはありません。
 - * critical * : サービスに影響する深刻な障害です。システムはAPI 要求またはクライアント I/O 要求を処理できません。この状態で運用を続けると、データが失われる可能性があります。
 - * bestPractice * : 推奨されるシステム構成のベストプラクティスが使用されていません。
 - * タイプ *
 - * node * : ノード全体に影響する障害。
 - * drive * : 個々のドライブに影響する障害。
 - * cluster * : クラスタ全体に影響する障害。
 - * service * : クラスタ上のサービスに影響する障害。
 - * volume * : クラスタ上のボリュームに影響する障害。
 - * Node * : この障害に関連するノードのノード ID。エラーのタイプが node と drive の場合に表示され、それ以外の場合は -（ダッシュ）が表示されます。
 - * Drive ID * : この障害に関連するドライブのドライブ ID。エラーのタイプが drive の場合に表示され、それ以外の場合は -（ダッシュ）が表示されます。
 - * エラーコード * : エラーの原因を示すコード。
 - * 詳細 * : 障害の詳細な概要。
 - * 時間 * : この見出しは、アクティブフィルタビューでのみ表示されます。障害がログに記録された日時。
 - * 解決日 * : この見出しは、解決済みのフィルタビューにのみ表示されます。障害が解決された日時。
4. 問題が解決されたことを確認するには、解決済みビューで を探します。

詳細については、こちらをご覧ください

- ["NetApp HCI のドキュメント"](#)
- ["SolidFire and Element Resources ページにアクセスします"](#)

システムアラートのリスト

各アラートについてエラーコードが報告されるため、アラートが発生したシステムのコンポーネントおよびアラートが生成された理由を確認できます。プラグイン拡張ポイントを使用して、エラーコードを確認できます。

- Element vCenterプラグイン5.0以降では、* NetApp Remote Plugin > Management > Reporting > Alerts *の順に選択します。
- Element vCenterプラグイン4.10以前の場合は、* NetApp Element Management > Reporting > Alerts *の順に選択します。

以下に、各種のシステムアラートの一覧を示します。

- * authenticationServiceFault*

1つ以上のクラスタノードの認証サービスが正常に機能していません。

ネットアップサポートにお問い合わせください。

- * 利用可能な VirtualNetworkIPAddressesLow *

IP アドレスブロック内の仮想ネットワークアドレスの数が少なくなっています。

この問題を解決するには、仮想ネットワークアドレスのブロックに IP アドレスを追加してください。

- * blockClusterFull *

単一ノードの損失をサポートするのに十分なブロックストレージの空き容量がありません。クラスタフルのレベルの詳細については、GetClusterFullThreshold API メソッドを参照してください。このクラスタ障害は、次のいずれかの状態を示します。

- stage3Low (警告) : ユーザ定義のしきい値を超えています。Cluster Full の設定を調整するか、ノードを追加します。
- stage4Critical (エラー) : 1 ノードの障害からリカバリするための十分なスペースがありません。ボリューム、Snapshot、およびクローンは作成できません。
- stage5CompletelyConsumed (Critical) 1 : 書き込みまたは新しい iSCSI 接続は許可されません。現在の iSCSI 接続は維持されます。クラスタに容量を追加するまで書き込みは失敗します。

この問題を解決するには、ボリュームをパージまたは削除するか、ストレージクラスタに別のストレージノードを追加してください。

- * ブロックが劣化しました *

障害により、ブロックデータの完全なレプリケートが行われなくなりました。

| 重大度 | 説明 |
|-----|---------------------------------|
| 警告 | アクセス可能なブロックデータの完全なコピーは 2 つだけです。 |
| エラー | アクセス可能なブロックデータの完全なコピーは 1 つだけです。 |
| 重要 | ブロックデータの完全なコピーにはアクセスできません。 |

- 注意： * 警告ステータスは、トリプル Helix システムでのみ発生します。

この問題を解決するには、オフラインのノードまたはブロックサービスをリストアするか、ネットアップサポートにお問い合わせください。

- * blockServiceTooFull*

ブロックサービスが大量のスペースを使用しています。

この問題を解決するには、プロビジョニング済み容量を追加してください。

- * ブロックされたもの *

ブロックサービスが正常でないことが検出されました：

- 重大度 = 警告：対処は行われません。この警告期間は、cTimeUntilBSIsKilledMSec = 330000 ミリ秒で期限切れになります。
- 重大度 = エラー：データの運用停止処理が自動的に実行され、他の正常なドライブにデータが再レプリケートされます。
- 重大度 = 重大：複数のノードで障害ブロックサービスが発生していますが、レプリケーション数以上になっています（Double Helix の場合は 2）。データを使用できないため、ビンの同期が完了しません。

ネットワーク接続の問題とハードウェアエラーを確認します。特定のハードウェアコンポーネントで障害が発生した場合は、それ以外の障害が発生します。この障害は、ブロックサービスにアクセスできるかサービスが運用停止されると解消されます。

- * BmcSelfTestFailed*

ベースボード管理コントローラ（BMC）のセルフテストに失敗しました。

ネットアップサポートにお問い合わせください。

Element 12.5以降へのアップグレード中は、を使用します BmcSelfTestFailed BMCにすでに障害が発生しているノード、またはアップグレード中にノードのBMCに障害が発生した場合、障害は生成されません。アップグレード中にセルフテストに失敗したBMCは問題 Aになります BmcSelfTestFailed クラス全体のアップグレード完了後に発生する警告。

- * clockSkewExceedsFaultThreshold *

クラスタマスターとトークンを提供しているノードの間の時間差が推奨されるしきい値を超えています。ストレージクラスタは、ノード間の時間スキューを自動的に修正できません。

この問題を解決するには、インストール時のデフォルトではなく、使用するネットワーク内の NTP サーバを使用してください。内部の NTP サーバを使用している場合は、ネットアップサポートにお問い合わせください。

- *** clusterCannotSync***

スペース不足の状態にあり、オフラインのブロックストレージドライブ上のデータをアクティブなドライブと同期できません。

この問題を解決するには、ストレージを追加してください。

- *** clusterFull ***

ストレージクラスタ内の空きストレージスペースが不足しています。

この問題を解決するには、ストレージを追加してください。

- *** clusterIOPSAreOverProvised***

クラスタの IOPS がオーバープロビジョニングされています。QoS の最小 IOPS の合計が、クラスタの想定 IOPS を上回っています。すべてのボリュームで同時に最小 QoS を維持することができません。

この問題を解決するには、ボリュームの最小 QoS IOPS 設定を引き下げてください。

- *** CpuThermalEventThreshold ***

1つ以上のCPUのCPU温度イベントの数が、設定されたしきい値を超えています。

10分以内に新しいCPU温度イベントが検出されない場合、警告は自動的に解決します。

- **disableDriveSecurityFailed**

クラスタはドライブのセキュリティ（保存中のデータの暗号化）を有効にするようには設定されていませんが、少なくとも1つのドライブでドライブのセキュリティが有効になっているため、それらのドライブでドライブのセキュリティを無効にできませんでした。この障害は重大度が「Warning」で記録されません。

この問題を解決するには、ドライブのセキュリティを無効にできなかった理由について障害の詳細を確認してください。考えられる原因は次のとおりです。

- 暗号化キーを取得できませんでした。キーまたは外部キーサーバへのアクセスに関する問題を調査してください。
- ドライブで無効化処理に失敗した場合は、間違ったキーが取得されていないかどうかを確認してください。

どちらでもない場合は、ドライブの交換が必要となる可能性があります。

正しい認証キーを指定してもセキュリティが無効にならないドライブに対して、リカバリを試みることができます。この処理を実行するには、ドライブの状態を Available に変更してシステムから取り外し、ドライブで完全消去を実行してから Active に戻します。

• * 接続解除されたクラスタペア *

クラスタペアが切断されているか、正しく設定されていません。

クラスタ間のネットワーク接続を確認してください。

• * disconnectedRemoteNode * を実行します

リモートノードが切断されているか、正しく設定されていません。

ノード間のネットワーク接続を確認してください。

• * 切断された SnapMirrorEndpoint *

リモート SnapMirror エンドポイントが切断されているか、正しく設定されていません。

クラスタとリモート SnapMirrorEndpoint の間のネットワーク接続を確認してください。

• * 走行可能 *

クラスタ内に利用可能なドライブがあります。通常は、すべてのクラスタにすべてのドライブが追加されており、利用可能な状態のドライブはありません。この問題が予期せずに発生する場合は、ネットアップサポートにお問い合わせください。

この問題を解決するには、使用可能なドライブをすべてストレージクラスタに追加してください。

• * driveFailed *

次のいずれかの状態のドライブで障害が発生すると、クラスタはこのエラーを返します。

- ドライブマネージャがドライブにアクセスできません。
- スライスサービスまたはブロックサービスで障害が発生した回数が多すぎます。おそらくドライブの読み取りまたは書き込みの失敗が原因で再起動できません。
- ドライブがありません。
- ノードのマスターサービスにアクセスできません（ノード内のすべてのドライブが見つからないか障害状態であるとみなされます）。
- ドライブがロックされており、そのドライブの認証キーを取得できません。
- ドライブがロックされているためロック解除処理が失敗します。

この問題を解決するには：

- ノードのネットワーク接続を確認してください。
- ドライブを交換します。
- 認証キーが使用可能であることを確認します。

• * driveHealthFault *

ドライブが SMART ヘルスチェックに失敗したため、ドライブの機能が低下しました。この障害には、Critical 重大度レベルがあります。

- シリアル付きドライブ： <シリアル番号>、スロット： <ノードスロット><ドライブスロット>、SMART 全体のヘルスチェックに失敗しました。

この問題を解決するには、ドライブを交換してください。

- * driveWearFault *

ドライブの残存寿命がしきい値を下回っていますが、まだ機能しています。この障害には、重大度レベルとして「重大」と「警告」の2つのレベルがあります。

- シリアル付きドライブ： <serial number> in slot : <node slot><drive slot> には、重大な摩耗度レベルがあります。
- Serial Number > in slot : <ノードスロット><ドライブスロット> のドライブの摩耗リザーブが少ない。

この問題を解決するには、ドライブをすぐに交換してください。

- * duplicateClusterMasterCandidates *

ストレージクラスマスターの候補が複数検出されました。

ネットアップサポートにお問い合わせください。

- * enableDriveSecurityFailed*

クラスタはドライブのセキュリティ（保存中のデータの暗号化）を要求するように設定されていますが、少なくとも1つのドライブでセキュリティを有効にできませんでした。この障害は重大度が「Warning」で記録されます。

この問題を解決するには、ドライブのセキュリティを有効にできなかった理由について障害の詳細を確認してください。考えられる原因は次のとおりです。

- 暗号化キーを取得できませんでした。キーまたは外部キーサーバへのアクセスに関する問題を調査してください。
- ドライブで有効化処理に失敗した場合は、間違ったキーが取得されていないかどうかを確認してください。どちらでもない場合は、ドライブの交換が必要となる可能性があります。

正しい認証キーを指定してもセキュリティが有効にならないドライブに対して、リカバリを試みることができます。この処理を実行するには、ドライブの状態を Available に変更してシステムから取り外し、ドライブで完全消去を実行してから Active に戻します。

- * ensembleDegraded *

1つ以上のアンサンブルノードで、ネットワーク接続または電源が失われました。

この問題を解決するには、ネットワーク接続または電源を復旧してください。

- * 例外 *

通常の障害以外の障害が報告されました。これらの障害は、障害キューから自動的に消去されることはありません。

ネットアップサポートにお問い合わせください。

• * 失敗した SpaceTooFull *

ブロックサービスがデータ書き込み要求に 응답していません。スライスサービスが失敗した書き込みを格納するためのスペースが不足します。

この問題を解決するには、書き込みを正常に続行し、失敗した書き込みのスペースをスライスサービスからフラッシュできるように、ブロックサービス機能をリストアしてください。

• * fanSensor *

ファンセンサーに障害が発生しているか、ファンセンサーがありません。

この問題を解決するには、障害が発生したハードウェアを交換してください。

• * fibreChannelAccessDegraded *

Fibre Channel ノードが自身のストレージ IP でストレージクラスタ内の他のノードに一定期間 응답していません。この状態になると、ノードは 응답していないと判断され、クラスタ障害が生成されます。

ネットワーク接続を確認してください。

• * fibreChannelAccessUnavailable*

すべての Fibre Channel ノードが 응답していません。ノード ID が表示されます。

ネットワーク接続を確認してください。

• * fibreChannelActiveIxl *

iXL Nexus 数は、サポートされるファイバチャネルノードあたりのアクティブセッション数が最大 8000 に近づいています。

- ベストプラクティスの上限は 5500 です。
- 警告の上限は 7500 です。
- 上限（必須ではない）は 8192 です。

この問題を解決するには、iXL Nexus の数をベストプラクティスの上限である 5500 未満に減らしてください。

• * fibreChannelConfig *

このクラスタ障害は、次のいずれかの状態を示します。

- PCI スロットに予期しないファイバチャネルポートがあります。
- 想定外の Fibre Channel HBA モデルが使用されています。
- Fibre Channel HBA のファームウェアに問題があります。
- Fibre Channel ポートがオンラインではありません。
- Fibre Channel パススルーを設定している永続的な問題があります。

ネットアップサポートにお問い合わせください。

- * fibreChannelIOPS*

合計 IOPS 数がクラスタ内の Fibre Channel ノードの IOPS 制限に近づいています。制限は次のとおりです。

- FC0025 : 450、000 IOPS 制限 (Fibre Channel ノードあたり 4K ブロックサイズ)
- FCN001 : 625K OPS 制限 (Fibre Channel ノードあたり 4K ブロックサイズ)。

この問題を解決するには、使用可能なすべての Fibre Channel ノードに負荷を分散してください。

- * fibreChannelStaticIxl *

iXL Nexus の数は、サポートされるファイバチャネルノードあたりの静的セッションの上限である 16000 に近づいています。

- ベストプラクティスの上限は 11000 です。
- 警告制限は 15000 です。
- 最大制限 (強制) は 16384 です。

この問題を解決するには、iXL Nexus の数をベストプラクティスの上限である 11000 未満に減らしてください。

- * fileSystemCapacityLow *

いずれかのファイルシステムでスペースが不足しています。

この問題を解決するには、ファイルシステムに容量を追加してください。

- * fileSystemIsReadOnly*

ファイルシステムが読み取り専用モードに移行しました。

ネットアップサポートにお問い合わせください。

- * FipsDrivesMismatch *

FIPS 対応ストレージノードに FIPS 非対応ドライブが挿入されているか、FIPS 非対応ストレージノードに FIPS 対応ドライブが挿入されています。ノードごとにエラーが生成され、影響を受けるすべてのドライブが表示されます。

この問題を解決するには、該当するドライブを取り外すか交換してください。

- * FipsDrivesOutOfCompliance]

FIPS ドライブ機能を有効にしたあとに保存データの暗号化を無効にしたことが検出されました。このエラーは、FIPS ドライブ機能が有効になっていて、FIPS 非対応のドライブまたはノードがストレージクラスタに配置されている場合にも生成されます。

この問題を解決するには、保存データの暗号化を有効にするか、FIPS 非対応のハードウェアをストレージクラスタから取り外してください。

- * fipsSelfTestFailure*

FIPS サブシステムのセルフテスト中に障害が検出されました。

ネットアップサポートにお問い合わせください。

• * ハードウェア構成の不一致 *

このクラスタ障害は、次のいずれかの状態を示します。

- 構成がノード定義と一致しません。
- このタイプのノードに対して正しくないドライブサイズが使用されています。
- サポート対象外のドライブが検出されました。原因としては、インストールされている Element のバージョンがこのドライブを認識しないことが考えられます。このノードで Element ソフトウェアを更新することを推奨します。
- ドライブファームウェアが一致しません。
- ドライブの暗号化対応がノードと一致しません。

ネットアップサポートにお問い合わせください。

• **idPCertificateExpiration**

サードパーティのアイデンティティプロバイダ (IdP) で使用するクラスタのサービスプロバイダの SSL 証明書の有効期限が近づいているか、または有効期限が切れています。この問題では、緊急性に基づいて次の重大度が使用されます。

| 重大度 | 説明 |
|-----|-------------------------------------|
| 警告 | 証明書は 30 日以内に期限切れになります。 |
| エラー | 証明書は 7 日以内に期限切れになります。 |
| 重要 | 証明書は 3 日以内に期限切れになるか、すでに期限切れになっています。 |

この問題を解決するには、有効期限が切れる前に SSL 証明書を更新してください。

で `UpdateIdpConfiguration` API メソッドを使用します `refreshCertificateExpirationTime=true` 更新された SSL 証明書を指定します。

• * **inconsistentBondModes** *

VLAN デバイスのボンディングモードが見つかりません。想定されるボンディングモードと使用中のボンディングモードが表示されます。

• * **inconsistentMtus** *

このクラスタ障害は、次のいずれかの状態を示します。

- **Bond1G mismatch** : Bond1G インターフェイス間で異なる MTU が設定されています。
- **Bond10G mismatch** : Bond10G インターフェイス間で異なる MTU が設定されています。

該当するノードと関連付けられている MTU 値が表示されます。

- * inconsistentRoutingRules*

このインターフェイスのルーティングルールが矛盾しています。

- * inconsistentSubnetMas*

VLAN デバイスのネットワークマスクが、内部的に記録された VLAN のネットワークマスクと一致しません。想定されるネットワークマスクと使用中のネットワークマスクが表示されます。

- * incorrectBondPortCount *

ボンドポートの数が正しくありません。

- * invalidConfiguredFibreChannelNodeCount *

想定される 2 つの Fibre Channel ノード接続のいずれかがデグレード状態です。この障害は、Fibre Channel ノードが 1 つしか接続されていない場合に発生します。

この問題を解決するには、クラスタのネットワークの接続状態とケーブル配線を確認し、障害が発生したサービスがないかを確認してください。ネットワークやサービスに問題がない場合は、ネットアップサポートに連絡して Fibre Channel ノードを交換してください。

- **irqBalanceFailed**

割り込みのバランス調整中に例外が発生しました。

ネットアップサポートにお問い合わせください。

- * kmipCertificateFault * :

- ルート認証局 (CA) 証明書の有効期限が近づいています。

この問題を解決するには、有効期限まで 30 日以上ある新しい証明書をルート CA から取得し、ModifyKeyServerKmpip を使用して更新されたルート CA 証明書を提供します。

- クライアント証明書の有効期限が近づいています。

この問題を解決するには、GetClientCertificateSigningRequest を使用して新しい CSR を作成し、新しい有効期限まで 30 日以上あることを確認して署名し、ModifyKeyServerKmpip を使用して期限切れになる KMIP クライアント証明書を新しい証明書に置き換えます。

- ルート認証局 (CA) 証明書の有効期限が切れています。

この問題を解決するには、有効期限まで 30 日以上ある新しい証明書をルート CA から取得し、ModifyKeyServerKmpip を使用して更新されたルート CA 証明書を提供します。

- クライアント証明書の期限が切れています。

この問題を解決するには、GetClientCertificateSigningRequest を使用して新しい CSR を作成し、新しい有効期限まで 30 日以上あることを確認して署名し、ModifyKeyServerKmpip を使用して期限切れの KMIP クライアント証明書を新しい証明書に置き換えます。

- ルート認証局 (CA) 証明書のエラーです。

この問題を解決するには、正しい証明書が指定されていることを確認し、必要に応じてルート CA から証明書を再取得します。ModifyKeyServerKmpip を使用して、正しい KMIP クライアント証明書をインストールします。

- クライアント証明書エラーです。

この問題を解決するには、正しい KMIP クライアント証明書がインストールされていることを確認します。クライアント証明書のルート CA が EKS にインストールされている必要があります。ModifyKeyServerKmpip を使用して、正しい KMIP クライアント証明書をインストールします。

• * kmipServerFault * :

- 接続に失敗しました

この問題を解決するには、外部キーサーバが稼働しており、ネットワーク経由でアクセスできることを確認してください。TestKeyServerKimp と TestKeyProviderKmpip を使用して、接続をテストします。

- 認証に失敗しました

この問題を解決するには、正しいルート CA および KMIP クライアント証明書が使用されていることと、秘密鍵と KMIP クライアント証明書が一致することを確認します。

- サーバエラーです

この問題を解決するには、エラーの詳細を確認します。エラーによっては、外部キーサーバでのトラブルシューティングが必要になる場合があります。

• * memyEccThreshold *

修正可能な ECC エラーまたは修正不可能な ECC エラーが多数検出されました。この問題では、緊急性に基づいて次の重大度が使用されます。

| イベント | 重大度 | 説明 |
|---|-----|---|
| 1 つの DIMM cErrorCount が cDimmCorrectableErrWarnThreshold に到達しました。 | 警告 | DIMM のしきい値を超えている修正可能な ECC メモリエラー： <Processor><DIMM Slot> |
| DIMM の cErrorFaultTimer が期限切れになるまで、1 つの DIMM cErrorCount は cDimmCorrectableErrWarnThreshold よりも高くなります。 | エラー | DIMM のしきい値を超えている修正可能な ECC メモリエラー： <Processor><DIMM> |
| メモリコントローラが cMemCtrlCorrectableErrWarnThreshold より上の cErrorCount を報告し、cMemCtrlCorrectableErrWarnDuration を指定します。 | 警告 | 修正可能な ECC メモリエラーがメモリコントローラのしきい値を超えています： <Processor><Memory Controller> |

| | | |
|--|-----|--|
| メモリコントローラでは、メモリコントローラの cErrorFaultTimer の期限が切れるまで、メモリコントローラから cMemCtrlCorrectableErrWarnThreshold が報告されます。 | エラー | DIMM のしきい値を超えている修正可能な ECC メモリエラー： <Processor><DIMM> |
| 1つの DIMM がゼロより大きい uErrorCount を報告していますが、cDimmUncorrectableErrFaultThreshold よりも小さくなっています。 | 警告 | DIMM で修正不可能な ECC メモリエラーが検出されました： <Processor><DIMM Slot> |
| 1つの DIMM で少なくとも cDimmUncorrectableErrFaultThreshold の uErrorCount が報告されます。 | エラー | DIMM で修正不可能な ECC メモリエラーが検出されました： <Processor><DIMM Slot> |
| メモリコントローラがゼロより大きい uErrorCount を報告していますが、cMemCtrlUncorrectableErrFaultThreshold よりも小さくなっています。 | 警告 | メモリコントローラで修正不可能な ECC メモリエラーが検出されました：<Processor><Memory Controller> |
| メモリコントローラが少なくとも cMemCtrlUncorrectableErrFaultThreshold の uErrorCount を報告しています。 | エラー | メモリコントローラで修正不可能な ECC メモリエラーが検出されました：<Processor><Memory Controller> |

この問題を解決するには、ネットアップサポートにお問い合わせください。

• * memoryUsageThreshold *

メモリ使用量が正常値を上回っています。この問題では、緊急性に基づいて次の重大度が使用されます。



エラーの種類の詳細については、エラーの「* 詳細 *」の見出しを参照してください。

| 重大度 | 説明 |
|-----|-----------------------|
| 警告 | システムメモリが不足しています。 |
| エラー | システムメモリが非常に少なくなっています。 |
| 重要 | システムメモリが完全に消費されています。 |

この問題を解決するには、ネットアップサポートにお問い合わせください。

• * メタデータの ClusterFull *

単一ノードの損失をサポートするのに十分なメタデータストレージの空き容量がありません。クラスタフルのレベルの詳細については、GetClusterFullThreshold API メソッドを参照してください。このクラスタ障害は、次のいずれかの状態を示します。

- stage3Low (警告) : ユーザ定義のしきい値を超えています。Cluster Full の設定を調整するか、ノードを追加します。
- stage4Critical (エラー) : 1 ノードの障害からリカバリするための十分なスペースがありません。ボリューム、Snapshot、およびクローンは作成できません。
- stage5CompletelyConsumed (Critical) 1 : 書き込みまたは新しい iSCSI 接続は許可されません。現在の iSCSI 接続は維持されます。クラスタに容量を追加するまで書き込みは失敗します。データをパージまたは削除するか、ノードを追加します。

この問題を解決するには、ボリュームをパージまたは削除するか、ストレージクラスタに別のストレージノードを追加してください。

• * mtuCheckFailure*

ネットワークデバイスに適切な MTU サイズが設定されていません。

この問題を解決するには、すべてのネットワークインターフェイスとスイッチポートでジャンボフレームが設定されている (MTU が最大 9、000 バイト) ことを確認してください。

• * networkConfig *

このクラスタ障害は、次のいずれかの状態を示します。

- 想定されるインターフェイスが存在しません。
- インターフェイスが重複しています。
- 設定されたインターフェイスが停止しています。
- ネットワークの再起動が必要です。

ネットアップサポートにお問い合わせください。

• * 利用不可 VirtualNetworkIPAddresses*

IP アドレスのブロックに使用可能な仮想ネットワークアドレスがありません。

- virtualNetworkID タグ (\##) には、使用可能なストレージ IP アドレスがありません。クラスタにノードを追加することはできません。

この問題を解決するには、仮想ネットワークアドレスのブロックに IP アドレスを追加してください。

• * nodeHardwareFault (ネットワークインターフェイス <name> が停止しているか、ケーブルが接続されていません) *

ネットワークインターフェイスが停止しているか、ケーブルが取り外されています。

この問題を解決するには、ノードのネットワーク接続を確認してください。

• * nodeHardwareFault (ドライブ暗号化対応状態がスロット <node slot><drive slot> のドライブのノード

の暗号化対応状態と一致しません) *

ドライブが、搭載されているストレージノードと暗号化機能が一致しません。

- * nodeHardwareFault (このノードタイプのスロット >< ドライブスロット >にあるドライブの < ドライブタイプ > ドライブサイズ < 実際のサイズ > が正しくありません。 < ドライブスロット > このノードタイプが想定される < 想定サイズ >) *

ストレージノードに、このノードに対してサイズが正しくないドライブが含まれています。

- * nodeHardwareFault (サポートされていないドライブがスロット <node slot><drive slot> で検出されました。ドライブの統計情報と健全性情報が使用できません) *

ストレージノードに含まれているドライブはサポートされません。

- * nodeHardwareFault (スロット < ノードスロット >< ドライブスロット > のドライブでファームウェアバージョン < 想定バージョン > を使用している必要がありますが、サポートされていないバージョン < 実際のバージョン > を使用しています) *

ストレージノードに、サポート対象外のファームウェアバージョンを実行しているドライブが含まれています。

- * nodeMaintenanceMode*

ノードがメンテナンスモードになりました。この問題では、緊急性に基づいて次の重大度が使用されません。

| 重大度 | 説明 |
|-----|---|
| 警告 | ノードがまだメンテナンスモードになっていることを示します。 |
| エラー | メンテナンスモードを無効にできなかったことを示します。通常は、スタンバイが失敗したかアクティブなスタンバイが原因です。 |

この問題を解決するには、メンテナンスが完了したらメンテナンスモードを無効にしてください。エラーレベルの問題が解決しない場合は、ネットアップサポートにお問い合わせください。

- * nodeOffline *

Element ソフトウェアが指定されたノードと通信できません。ネットワーク接続を確認してください。

- * notUsingLACpBondMode *

LACP ボンディングモードが設定されていません。

この問題を解決するには、ストレージノードの導入時に LACP ボンディングを使用してください。LACP を有効にして適切に設定していないと、クライアントでパフォーマンスの問題が発生する可能性があります。

- * ntpServerUnreachable*

ストレージクラスタが指定された NTP サーバと通信できません。

この問題を解決するには、NTP サーバ、ネットワーク、およびファイアウォールの設定を確認してください。

• * ntpTimeNotInSync *

ストレージクラスタと指定された NTP サーバで時刻に大きな差があります。ストレージクラスタはこの時間差を自動的に修正できません。

この問題を解決するには、インストール時のデフォルトではなく、使用するネットワーク内の NTP サーバを使用してください。内部の NTP サーバを使用しても問題が維持される場合は、ネットアップサポートにお問い合わせください。

• * nvramDeviceStatus *

NVRAM デバイスでエラーが発生しているか、障害が発生しているか、障害が発生しています。この問題には次の重大度があります。

| 重大度 | 説明 |
|-----|--|
| 警告 | <p>ハードウェアによって警告が検出されました。この状態は、温度警告などの一時的なものです。</p> <ul style="list-style-type: none">• nvmetimeError• nvmetimeStatus• energySourceLifetimeStatus• energySourceTemperatureStatus• warningThresholdExceeded |
| エラー | <p>ハードウェアによってエラーまたは重大ステータスが検出されました。クラスタマスターがスライドライブの処理を中止しようとします（ドライブ削除イベントが生成されます）。セカンダリスライスサービスを使用できない場合、ドライブは削除されません。警告レベルのエラーに加えて返されるエラー：</p> <ul style="list-style-type: none">• NVRAM デバイスマウントポイントが存在しません。• NVRAM デバイスパーティションが存在しません。• NVRAM デバイスパーティションは存在しますが、マウントされていません。 |

| | |
|-----------|---|
| <p>重要</p> | <p>ハードウェアによってエラーまたは重大ステータスが検出されました。クラスタマスターがスライスドライブの処理を中止しようとします（ドライブ削除イベントが生成されます）。セカンダリスライスサービスを使用できない場合、ドライブは削除されません。</p> <ul style="list-style-type: none"> • 永続性ホスト • armStatusSaveNArmed • csaveStatusError |
|-----------|---|

ノード内の障害が発生したハードウェアを交換します。それでも問題が解決しない場合は、ネットアップサポートにお問い合わせください。

• * powerSupplyError *

このクラスタ障害は、次のいずれかの状態を示します。

- 電源装置がありません。
- 電源装置で障害が発生しました。
- 電源装置の入力が見つからないか、範囲外です。

この問題を解決するには、冗長電源がすべてのノードに供給されていることを確認してください。ネットアップサポートにお問い合わせください。

• * provisionedSpaceTooFull*

クラスタのプロビジョニング済み容量がいっぱいです。

この問題を解決するには、プロビジョニング済みスペースを追加するか、またはボリュームを削除およびパーズしてください。

• * remoteRepAsyncDelayExceeded *

レプリケーションに設定されている非同期遅延を超えました。クラスタ間のネットワーク接続を確認してください。

• * remoteRepClusterFull *

ターゲットストレージクラスタがいっぱいのため、ボリュームがリモートレプリケーションを停止しました。

この問題を解決するには、ターゲットストレージクラスタのスペースを解放してください。

• * remoteRepSnapshotClusterFull *

ターゲットストレージクラスタがいっぱいのため、ボリュームが Snapshot のリモートレプリケーションを停止しました。

この問題を解決するには、ターゲットストレージクラスタのスペースを解放してください。

- * remoteRepSnapshotsExceededLimit *

ターゲットストレージクラスタのボリュームが Snapshot の上限を超えたため、ボリュームが Snapshot のリモートレプリケーションを停止しました。

この問題を解決するには、ターゲットストレージクラスタの Snapshot の制限を引き上げます。

- * scheduleActionError *

スケジュールされたアクティビティの 1 つ以上を実行しましたが、失敗しました。

スケジュールされたアクティビティが再び実行されて成功するか、スケジュールされたアクティビティが削除されるか、またはアクティビティが一時停止されて再開されると、障害はクリアされます。

- * sensorReadingFailed*

センサーがベースボード管理コントローラ（BMC）と通信できませんでした。

ネットアップサポートにお問い合わせください。

- * serviceNotRunning *

必要なサービスが実行されていません。

ネットアップサポートにお問い合わせください。

- * sliceServiceTooFull*

スライスサービスに割り当てられたプロビジョニング済み容量が少なすぎます。

この問題を解決するには、プロビジョニング済み容量を追加してください。

- * sliceServiceUnhealthy * が表示されます

スライスサービスが正常な状態でないことが検出され、サービスが自動的に停止されました。

- 重大度 = 警告：対処は行われません。この警告期間は 6 分後に終了します。

- 重大度 = エラー：データの運用停止処理が自動的に実行され、他の正常なドライブにデータが再レプリケートされます。

ネットワーク接続の問題とハードウェアエラーを確認します。特定のハードウェアコンポーネントで障害が発生した場合は、それ以外の障害が発生します。スライスサービスにアクセスできるかサービスが運用停止されると、障害は解消されます。

- * sshEnabled *

ストレージクラスタ内の 1 つ以上のノードで SSH サービスが有効になっています。

この問題を解決するには、該当するノードの SSH サービスを無効にするか、ネットアップサポートにお問い合わせください。

- * sslCertificateExpiration*

このノードに関連付けられている SSL 証明書の有効期限が近づいているか、期限が切れています。この

問題では、緊急性に基づいて次の重大度が使用されます。

| 重大度 | 説明 |
|-----|-------------------------------------|
| 警告 | 証明書は 30 日以内に期限切れになります。 |
| エラー | 証明書は 7 日以内に期限切れになります。 |
| 重要 | 証明書は 3 日以内に期限切れになるか、すでに期限切れになっています。 |

この問題を解決するには、SSL 証明書を更新してください。必要に応じて、ネットアップサポートにお問い合わせください。

- * strandedCapacity *

1 つのノードがストレージクラスタの容量の半分を超えています。

データの冗長性を維持するために、最大のノードの容量がシステムによって削減され、ブロック容量の一部が孤立（使用されない）状態になります。

この問題を解決するには、既存のストレージノードにドライブを追加するか、クラスタにストレージノードを追加してください。

- * tempSensor *

温度センサーが正常よりも高い温度を報告しています。この問題は、powerSupplyError または fanSensor とともに発生する可能性があります。

ストレージクラスタの近くに通気を妨げる障害物がないかどうかを確認してください。必要に応じて、ネットアップサポートにお問い合わせください。

- * アップグレード *

アップグレードが 24 時間以上実行中です。

この問題を解決するには、アップグレードを再開するか、ネットアップサポートにお問い合わせください。

- * 無対応サービス *

サービスが応答しなくなりました。

ネットアップサポートにお問い合わせください。

- * virtualNetworkConfig *

このクラスタ障害は、次のいずれかの状態を示します。

- インターフェイスが存在しません。
- インターフェイス上のネームスペースが正しくありません。

- ネットマスクが正しくありません。
- IP アドレスが正しくありません。
- インターフェイスが稼働していません。
- ノード上に不要なインターフェイスがあります。

ネットアップサポートにお問い合わせください。

- * volumesDegraded *

セカンダリボリュームのレプリケートと同期が終了していません。このメッセージは、同期が完了するとクリアされます。

- * volumesOffline *

ストレージクラスタ内の 1 つ以上のボリュームがオフラインです。「* volumeDegraded 」 * エラーも発生します。

ネットアップサポートにお問い合わせください。

イベントログを監視してトラブルシューティングを行う

選択したクラスタで実行された処理のイベントログと、発生する可能性があるクラスタ障害を確認できます。ほとんどのエラーはシステムによって自動的に解決されます。それ以外の障害では手動での対応が必要になる場合

手順

1. vCenter Plug-in で、* Management * タブを開きます。
 - Element vCenter プラグイン 5.0 以降では、* NetApp Element リモートプラグイン > 管理 > 管理 * を選択します。
 - Element vCenter プラグイン 4.10 以前の場合は、* NetApp Element Management > Management * を選択します。
2. **Reporting > * Event Log *** を選択します。
3. 詳細を確認するには、イベントを選択して * Details * をクリックします。
4. 次のイベント情報を確認します。
 - * Event Type * : API イベントやクローンイベントなど、ログに記録されるイベントのタイプ。
 - * Service ID * : イベントを報告したサービスの ID (該当する場合)。障害がサービスに関連付けられていない場合、値は 0 です。
 - * Node * or * Drive ID * : イベントを報告したノードまたはドライブの ID (該当する場合)。

イベントタイプ

システムからは複数のタイプのイベントが報告されます。各イベントは、システムが完了した処理を表します。イベントには、日常的に発生するイベント、正常なイベント、または管理者による対応が必要なイベントがあります。[イベントログ] ページの [イベントタイプ] 列には、システムのどの部分でイベントが発生したかが示されます。



読み取り専用の API コマンドはイベントログに記録されません。

イベントログに表示されるイベントのタイプは次のとおりです。

- * apiEvent * : ユーザが API または Web UI から開始した、設定を変更するイベント。
- **binAssignmentsEvent**: データビンの割り当てに関連するイベント。ピンは基本的にデータを保持するコンテナであり、クラスタ全体にマッピングされます。
- **binSyncEvent** : ブロックサービス間でのデータの再割り当てに関連するシステムイベント。
- **bsCheckEvent**: ブロックサービスチェックに関連するシステムイベント。
- **bsKillEvent**: ブロックサービスの終了に関連するシステムイベント。
- * bulkOpEvent * : バックアップ、リストア、Snapshot、クローンなど、ボリューム全体で実行される処理に関連するイベント。
- * cloneEvent * : ボリュームクローニングに関連するイベント。
- * clusterMasterEvent * : ノードの追加や削除など、クラスタの初期化時またはクラスタの構成変更時に表示されるイベント。
- **csumEvent**: ディスク上の無効なデータチェックサムに関連するイベント。
- **DataEvent**: データの読み取りと書き込みに関連するイベント。
- * dbEvent * : クラスタ内のアンサンブルノードによって管理されているグローバルデータベースに関連するイベント。
- * driveEvent * : ドライブの処理に関連するイベント。
- * encryptionAtRestEvent * : クラスタでの暗号化プロセスに関連するイベント。
- * ensembleEvent * : アンサンブル内のノード数の増減に関連するイベント。
- * fibreChannelEvent * : ノードの設定と接続に関連するイベント。
- **gcEvent** : ブロックドライブ上のストレージを再利用するために 60 分ごとに実行されるプロセスに関連するイベント。このプロセスはガベージコレクションとも呼ばれます。
- * ieEvent * : 内部システムエラー。
- **installEvent**: 自動ソフトウェアインストールイベント。保留状態のノードにソフトウェアが自動的にインストールされています。
- **iSCSIEvent**: システムでの iSCSI の問題に関連するイベント。
- * limitEvent * : アカウントまたはクラスタ内で許可されているボリュームまたは仮想ボリュームの最大数に近づいていることを示すイベント。
- * maintenanceModeEvent * : ノードの無効化など、ノードのメンテナンスモードに関連するイベント。
- **networkEvent**: 仮想ネットワークのステータスに関連するイベント。
- * platformHardwareEvent * : ハードウェアデバイスで検出された問題に関連するイベント。
- * remoteClusterEvent * : リモートクラスタペアリングに関連するイベント。
- **schedulerEvent** : スケジュールされた Snapshot に関連するイベント。
- **serviceEvent** : システムサービスのステータスに関連するイベント。
- * sliceEvent * : メタデータドライブやボリュームの削除など、スライスサーバに関連するイベント。

スライスの再割り当てイベントには、ボリュームが割り当てられているサービスに関する情報を含む 3 種類の再割り当てイベントがあります。

- 反転：プライマリサービスを新しいプライマリサービスに変更します

'slicelDoldPrimaryServiceID→ newPrimaryServiceID'

- 移動：セカンダリサービスを新しいセカンダリサービスに変更します

'licelD{oldSecondaryServiceID(s)} → {newSecondaryServiceID(s)}'

- pruning : 一連のサービスからボリュームを削除する

'licelD{oldSecondaryServiceID(s)}'

- **snmpTrapEvent**: SNMP トラップに関連するイベント。
- **statEvent**: システム統計に関連するイベント。
- **tsEvent**: システム転送サービスに関連するイベント。
- * unexpectedException * : 予期しないシステム例外に関連するイベント。
- **ureEvent**: ストレージデバイスからの読み取り中に発生した回復不能な読み取りエラーに関連するイベント。
- * vasaProviderEvent * : VASA (vSphere APIs for Storage Awareness) Provider に関連するイベント。

詳細については、こちらをご覧ください

- ["NetApp HCI のドキュメント"](#)
- ["SolidFire and Element Resources ページにアクセスします"](#)

ボリュームのパフォーマンスを監視

プラグイン拡張ポイントのReportingタブでは、選択したクラスタ内のすべてのボリュームのパフォーマンス情報を確認できます。

手順

1. vCenter Plug-inで、* Reporting *タブを開きます。
 - Element vCenterプラグイン5.0以降では、* NetApp Element リモートプラグイン>管理>レポート*を選択します。
 - Element vCenterプラグイン4.10以前の場合は、* NetApp Element Management > Reporting *の順に選択します。
2. 「* Volume Performance」を選択します。
3. ページ上のデータの更新頻度を変更するには、[すべてのリストを更新する*]をクリックして値を選択します。

クラスタのボリューム数が1、000個未満の場合、デフォルトの更新間隔は10秒です。それ以外の場合は60秒です。[なし]の値を選択すると、自動ページ更新は無効になります。

ボリュームのパフォーマンスデータ

- * 名前 * : 作成時のボリュームの名前。
- * Account * : ボリュームに割り当てられているアカウントの名前。
- * アクセスグループ * : ボリュームが属するボリュームアクセスグループの名前。
- * ボリューム利用率 %* : ボリュームを使用しているクライアントの割合を示す値。

有効な値は次のとおり

- 0 : クライアントはボリュームを使用していません
- 100 : クライアントは最大値まで使用しています
- >100 : クライアントはバースト値を使用しています
- * 合計 IOPS * : ボリュームに対して実行中の IOPS (読み取りおよび書き込み) の総数。
- * 読み取り IOPS * : ボリュームに対して実行中の読み取り IOPS の総数。
- * 書き込み IOPS * : ボリュームに対して実行中の書き込み IOPS の総数。
- * 合計スループット * : ボリュームに対して実行中のスループット (読み取りおよび書き込み) の総量。
- * Read Throughput * : ボリュームに対して実行中の読み取りスループットの総量。
- * 書き込みスループット * : ボリュームに対して実行中の書き込みスループットの総量。
- * 合計レイテンシ (ミリ秒) * : ボリュームへの読み取りおよび書き込み処理が完了するまでの平均時間 (マイクロ秒)。
- * 読み取りレイテンシ (ミリ秒) * : 過去 500 ミリ秒の、ボリュームへの読み取り処理が完了するまでの平均時間 (マイクロ秒)。
- * 書き込みレイテンシ (ミリ秒) * : 過去 500 ミリ秒の、ボリュームへの書き込み処理を完了するための平均時間 (マイクロ秒)。
- * Queue Depth * : ボリュームに対する未処理の読み取り処理と書き込み処理の数。
- * Average IO Size * : 過去 500 ミリ秒における、ボリュームに対する最近の I/O の平均サイズ (バイト)。

詳細については、こちらをご覧ください

- ["NetApp HCI のドキュメント"](#)
- ["SolidFire and Element Resources ページにアクセスします"](#)

iSCSI セッションを監視して接続ステータスを確認

NetApp Element Plug-in for VMware vCenter Serverで、選択したクラスタに接続されているiSCSIセッションに関する情報を確認できます。

手順

1. vCenter Plug-inで、* Reporting *タブを開きます。
 - Element vCenterプラグイン5.0以降では、* NetApp Element リモートプラグイン>管理>レポート*を選

択します。

- Element vCenterプラグイン4.10以前の場合は、* NetApp Element Management > Reporting *の順に選択します。

2. 「* iSCSI Sessions *」を選択します。

iSCSI セッションデータ

- * Node * : ボリュームのプライマリメタデータパーティションをホストしているノード。
- * Account * : ボリュームを所有するアカウントの名前。値が空白の場合は、ダッシュ (-) が表示されません。
- * Volume * : ノードで識別されているボリュームの名前。
- * Volume ID * : ターゲット IQN に関連付けられたボリュームの ID 。
- * Initiator ID * : システムによって生成されたイニシエータの ID 。
- * イニシエータエイリアス * : イニシエータが多数ある場合に特定のイニシエータを見つけやすくするための別名。
- * Initiator IP * : セッションを開始するエンドポイントの IP アドレス。
- * イニシエータ IQN * : セッションを開始するエンドポイントの IQN 。
- * Target IP * : ボリュームをホストしているノードの IP アドレス。
- * ターゲット IQN * : ボリュームの IQN 。
- * 作成日 * : セッションが確立された日付。

詳細については、こちらをご覧ください

- ["NetApp HCI のドキュメント"](#)
- ["SolidFire and Element Resources ページにアクセスします"](#)

QoSSIOC イベントを使用して VM のパフォーマンス階層化を監視します

QoSSIOC に関連するイベントは、QoS 対応データストアがある VM が再設定された場合、または電源イベントやゲストイベントが発生した場合に表示されます。

QoSSIOCイベントは、NetApp Element Plug-in for vCenter Serverのプラグイン拡張ポイントで確認できます。

QoSSIOC イベントは、ローカルに追加されたクラスタから表示されます。リンクモード環境で、クラスタがローカルに追加されている vSphere Web Client にログインして、そのクラスタの QoSSIOC イベントを表示します。



- Element vCenter Plug-in 5.0以降で使用できるようになりました "[vCenter リンクモード](#)"では、NetApp SolidFire ストレージクラスタを管理するvCenter Serverごとに、Element Plug-inを別の管理ノードから登録します。
- NetApp Element Plug-in for vCenter Server 4.10以前を使用して、他のvCenter Serverのクラスタリソースを管理する "[vCenter リンクモード](#)" はローカルストレージクラスタのみに制限されます。

必要なもの

- クラスタが少なくとも 1 つ追加されて実行されている必要があります。
- プラグインの QoSSIOC 設定ページを使用して、QoSSIOC サービスの設定と確認を行う必要があります。
- 少なくとも 1 つのデータストアで QoSSIOC 自動化が有効になっている必要があります。

手順

1. vSphere Web Clientで、* QoSSIOCイベント*タブを開きます。
 - Element vCenterプラグイン5.0以降では、* NetApp Element リモートプラグイン>設定> QoSSIOCイベント*を選択します。
 - Element vCenterプラグイン4.10以前の場合は、* NetApp Element Configuration > QoSSIOCイベント*を選択します。

QoSSIOC イベントデータ

- * 日付 * : QoSSIOC イベントの日時。
- * データストア名 * : ユーザが定義したデータストア名。
- * Cluster IP * : イベントの発生元であるデータストアが含まれているクラスタの IP アドレス。
- * Volume ID * : システムによって生成された、関連付けられたボリュームの ID 。
- * Min IOPS * : ボリュームの QoS 設定 - 現在の最小 IOPS 。
- * Max IOPS * : ボリュームの QoS 設定 - 現在の最大 IOPS 。
- * Burst IOPS * : ボリュームの現在の最大バースト QoS 設定。
- * バースト時間 * : バーストが許可される期間。

詳細については、こちらをご覧ください

- "[NetApp HCI のドキュメント](#)"
- "[SolidFire and Element Resources ページにアクセスします](#)"

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。