ネットアップの要素 **12.0**

ユーザガイド

2020年4月 | 215-14901_2020-04_ja-jp
ng-gpso-jp-documents@netapp.com

NetApp®

目次

本書の内容

このガイドでは、Elementデータ管理ソフトウェアを実行するストレージ システムを設定、管理、および使用する方法について説明します。このガイドは、NetApp Elementソフトウェアを実行するストレージ システムのインストール、管理、またはトラブルシューティングを担当するITプロフェッショナル、ソフトウェア開発者などを対象としています。

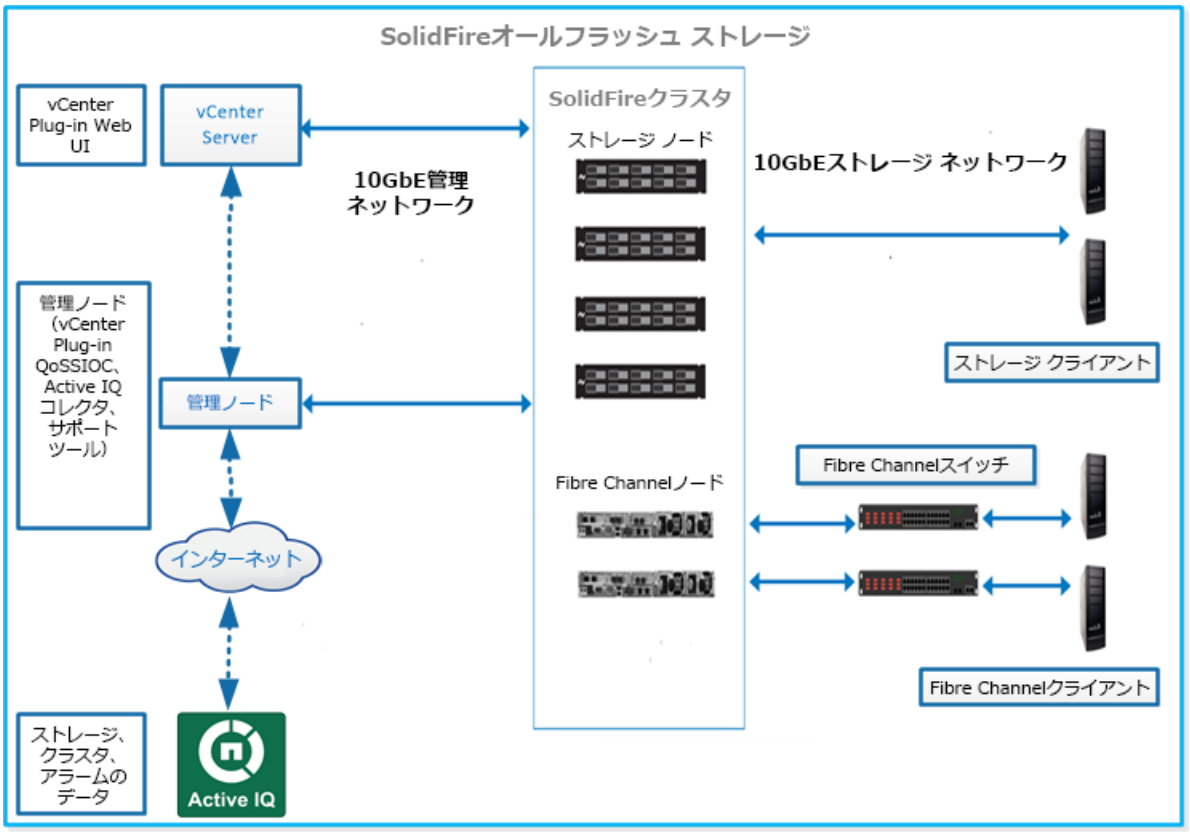
本ガイドの前提条件は以下のとおりです。

- Linuxシステム管理者としての経験があること。
- サーバ ネットワークおよびネットワーク ストレージ（IPアドレス、ネットマスク、ゲートウェイを含む）の詳しい知識があること。

SolidFireストレージ システム

SolidFireオールフラッシュ ストレージ システムは、独立した複数のハードウェア コンポーネント（ドライブとノード）で構成されます。これらのコンポーネントは、各ノードでそれぞれ実行されているNetApp Elementソフトウェアを通じて1つのストレージ リソース プールに集約されます。この統合されたクラスタは、単一のストレージ システムとして外部クライアントに提供され、ElementソフトウェアのUI、API、およびその他の管理ツールによって単一のエンティティとして管理されます。

NetApp Elementソフトウェア ユーザ インターフェイスを使用して、SolidFireクラスタのストレージ容量とパフォーマンスを設定および監視できるほか、マルチテナント インフラ全体のストレージ アクティビティを管理できます。



SolidFireオールフラッシュ ストレージ システムには、次のコンポーネントが含まれます。

- ノード：クラスタにストレージ リソースを提供する物理ハードウェア。ノードには次の2つのタイプがあります。
  - ストレージ ノード：複数のドライブを搭載したサーバ。
  - Fibre Channel（FC）ノード：Fibre Channelスイッチ経由でFCクライアントを接続します。
- クラスタ：SolidFireストレージ システムの中核となるコンポーネントで、4つの以上ノードで構成されます。
- 管理ノード：監視とテレメトリなどのシステム サービスのアップグレードと提供、クラスタのアセットと設定の管理、システムのテストとユーティリティの実行、ネットアップ サポートへのアクセスの許可（トラブルシューティング）を実行できます。管

理ノード（mNode）は、Elementソフトウェアベースのストレージ クラスタと連携して実行される仮想マシンです。
- Active IQ：クラスタ全体のデータの履歴ビューを提供するWebベースのツール。ビューは定期的に更新されます。特定のイベント、しきい値、または指標にアラートを設定できます。Active IQを使用すると、システムのパフォーマンスと容量を監視し、クラスタの健全性を常に把握できます。
- ドライブ：ストレージ ノードで使用され、クラスタのデータを格納します。ストレージ ノードには、次の2種類のドライブが含まれます。
  - ボリューム メタデータ ドライブ：クラスタ内のボリュームやその他オブジェクトの定義情報を格納します。
  - ブロック ドライブ:アプリケーション ボリュームのデータ ブロックを格納します。

クラスタ

クラスタは、SolidFireストレージ システムの中心であり、複数のノードで構成されます。SolidFireのストレージ効率化を実現するには、クラスタに少なくとも4つのノードが必要です。クラスタはネットワーク上では1つの論理グループとして認識され、ブロック ストレージとしてアクセスできます。

新しいクラスタを作成すると、1つのノードがそのクラスタの通信の所有者として初期化され、クラスタ内の各ノードに対してネットワーク通信が確立されます。このプロセスは、クラスタの作成時に一度だけ実行されます。Element UIまたはAPIを使用してクラスタを作成できます。

クラスタをスケールアウトするには、ノードを追加します。新しいノードを追加するときにサービスが中断されることはなく、追加したノードのパフォーマンスと容量がクラスタで自動的に使用されます。

管理者とホストは、仮想IPアドレスを使用してクラスタにアクセスできます。クラスタ内のいずれのノードも仮想IPアドレスをホストできます。管理仮想IP（MVIP）は1GbE接続でのクラスタ管理を提供し、ストレージ仮想IP（SVIP）はホストからストレージへの10GbE接続でのアクセスを提供します。これらの仮想IPアドレスは、SolidFireクラスタのサイズや構成に関係なく、一貫した接続を可能にします。仮想IPアドレスをホストするノードで障害が発生した場合、クラスタ内の別のノードが仮想IPアドレスを引き継ぎます。

注： Elementバージョン11.0以降では、ノードの管理ネットワークにIPv4、IPv6、または両方のアドレスを設定できます。これはストレージ ノードと管理ノードのどちらにも該当します（IPv6がサポートされない管理ノード11.3以降を除く）。クラスタの作成時には、IPv4またはIPv6のどちらかのアドレスを1つだけMVIPに使用でき、これと同じアドレス タイプをすべてのノードで設定する必要があります。

ノード

ノードは個別のハードウェア コンポーネントで、クラスタにグループ化され、ブロック ストレージとしてアクセスされます。SolidFireストレージ システムのノードには、 ストレージ ノードとFibre Channelノードの2つのタイプがあります。

関連概念

ストレージ ノード（10ページ）

SolidFireストレージ ノードは、Bond10Gネットワーク インターフェイスを通じて相互に通信する一連のドライブを搭載したサーバです。ノード上のドライブには、データの格納用と管理用にブロック スペースとメタデータ スペースが確保されます。

Fibre Channelノード（10ページ）

SolidFire Fibre ChannelノードはFibre Channelスイッチへの接続を提供し、Fibre Channelスイッチ はFibre Channelクライアントに接続できます。Fibre Channelノードは、Fibre Channelプ

ロトコルとiSCSIプロトコルの間のプロトコル コンバータとして機能するため、新規または既存のあらゆるSolidFireクラスタへのFibre Channel接続を追加できます。

ドライブ（10ページ）
ストレージ ノードには1つ以上の物理ドライブが搭載され、クラスタのデータの一部が格納されます。クラスタにドライブが追加されると、そのドライブの容量とパフォーマンスがクラスタで使用されるようになります。

ストレージ ノード

SolidFireストレージ ノードは、Bond10Gネットワーク インターフェイスを通じて相互に通信する一連のドライブを搭載したサーバです。ノード上のドライブには、データの格納用と管理用にブロック スペースとメタデータ スペースが確保されます。

ストレージ ノードには次のような特徴があります。

- 各ノードには固有な名前が付けられます。管理者が名前を指定しない場合、ノードにはデフォルトで「SF-XXXX」という名前が付けられます。*xxxx*は、システムによってランダムに生成される任意の4文字です。
- 各ノードに高性能な専用のNon-Volatile Random Access Memory（NVRAM;不揮発性RAM）書き込みキャッシュが搭載されており、システム全体のパフォーマンスの向上と書き込みレイテンシの低減が実現します。
- 各ノードはそれぞれ2つの独立したリンクで2つのネットワーク（ストレージと管理）に接続され、冗長性とパフォーマンスが確保されます。それぞれのノードに各ネットワークのIPアドレスが必要です。
- 新しいストレージ ノードで構成されるクラスタを作成したり、または既存のクラスタにストレージ ノードを追加して、ストレージの容量およびパフォーマンスを拡張できます。
- クラスタに対するノードの追加や削除は、サービスを中断することなくいつでも実行できます。

Fibre Channelノード

SolidFire Fibre Channelノードは Fibre Channelスイッチへの接続を提供し、Fibre Channelスイッチは Fibre Channelクライアントに接続できます。Fibre Channelノードは、Fibre Channelプロトコルと iSCSIプロトコルの間のプロトコル コンバータとして機能するため、新規または既存のあらゆるSolidFireクラスタへのFibre Channel接続を追加できます。

Fibre Channelノードには次の特徴があります。

- Fibre Channelスイッチがファブリックの状態を管理し、相互接続が最適化されます。
- 2つのポート間のトラフィックはスイッチ経由でのみ送信され、他のポートには送信されません。
- ポートの障害は分離され、他のポートの動作には影響しません。
- 1つのファブリック内で複数のポート ペアが同時に通信することができます。

ドライブ

ストレージ ノードには1つ以上の物理ドライブが搭載され、クラスタのデータの一部が格納されます。クラスタにドライブが追加されると、そのドライブの容量とパフォーマンスがクラスタで使用されるようになります。

ストレージ ノードには、次の2種類のドライブが含まれます。

ボリューム メタデータ ドライブ

クラスタ内の各ボリューム、クローン、またはSnapshotの定義情報を圧縮して格納します。システム内のメタデータ ドライブの合計容量により、ボリュームとしてプロビジョニング可能なストレージの最大容量が決まります。プロビジョニング可

能なストレージの最大容量は、クラスタのブロック ドライブに実際に格納されるデータ量とは関係ありません。ボリューム メタデータ ドライブには、Double Helixデータ保護を使用してデータがクラスタ内に重複して格納されます。

注 : 一部のシステム イベント ログおよびエラー メッセージでは、ボリューム メタデータ ドライブではなくスライス ドライブと表記される場合があります。

ブロック ドライブ

サーバ アプリケーション ボリューム用に、重複排除済みのデータ ブロックを圧縮して格納します。ブロック ドライブはシステムのストレージ容量の大部分を占めます。データの書き込み要求に加えて、SolidFireクラスタにすでに格納されているデータの読み取り要求の大部分がブロック ドライブで発生します。格納可能なデータの最大容量は、システム内のブロック ドライブの合計容量に、圧縮、シンプロビジョニング、および重複排除の効果を加味して決まります。

カスタム保護ドメイン

カスタム保護ドメインレイアウトを定義できます。各ノードは 1 つのカスタム保護ドメインに関連付けられ、1 つのカスタム保護ドメインにのみ関連付けられます。デフォルトでは、各ノードは同じデフォルトのカスタム保護ドメインに割り当てられます。

カスタム保護ドメインが割り当てられていない場合：

- クラスタ処理に影響はありません。
- カスタムレベルは、耐障害性も耐障害性もありません。

複数のカスタム保護ドメインが割り当てられている場合、各サブシステムは重複を個別のカスタム保護ドメインに割り当てます。これが不可能な場合は、重複を別々のノードに割り当てます。各サブシステム（ビン、スライス、プロトコルエンドポイントプロバイダ、アンサンブルなど）は、これを個別に実行します。

注 : カスタム保護ドメインを使用する場合、ノードがシャーシを共有していないことを前提としています。

次の API メソッドは、これらの新しい保護ドメインを公開します。

- `GetProtectionDomainLayout` ●各ノードのシャーシとカスタム保護ドメインを表示します。
- `SetProtectionDomainLayout` - カスタム保護ドメインを各ノードに割り当てることができます。

カスタム保護ドメインの使用の詳細については、ネットアップのサポートにお問い合わせください。

関連情報

*Element API*を使用したストレージの管理

Elementソフトウェアの管理ノード

管理ノード（mNode）は、Elementソフトウェアベースの1つ以上のストレージ クラスタと同時に実行される仮想マシンです。このノードは、監視とテレメトリなどのシステム サービスのアップグレードと提供、クラスタのアセットと設定の管理、システムのテストとユーティリティの実行、ネットアップ サポートへのアクセス許可（トラブルシューティング）に使用します。

Element 11.3リリース以降、管理ノードはマイクロサービス ホストとして機能するようになりました。そのため、メジャー リリースを待つことなく、希望するソフトウェア サービスを更新できます。Active IQコレクタ、vCenter Plug-inのQoSSIOC、mNodeサービスなどのマイクロサービス（管理サービス）は、サービス バンドルとして頻繁に更新されま

す。ストレージ ノード ソフトウェアのアップグレード用のHealthToolsやサポート ツール（リモート サポート トンネリング）などのサービスも管理ノードから利用できます。

SolidFireオールフラッシュ ストレージの管理サービス

管理サービスは、SolidFireオールフラッシュ ストレージに幅広い管理機能を一元的に提供します。管理サービスには、Active IQシステム テレメトリ、ログ、サービスの更新、およびElement Plug-in for vCenterのQoSSIOCサービスが含まれます。

永続ボリューム

永続ボリュームを使用すると、管理ノードの設定データをローカルなVMではなく指定したストレージ クラスタに格納できるため、管理ノードが失われた場合や削除された場合でもデータを保持することができます。永続ボリュームはオプションですが、推奨される管理ノード設定です。

永続ボリュームを有効にするオプションは、新しい管理ノード導入時のインストール スクリプトとアップグレード スクリプトに含まれています。永続ボリュームはElementソフトウェアベースのストレージ クラスタ上のボリュームであり、ホスト管理ノードVMのノード設定情報がVMが使用されなくなったあとも格納されます。管理ノードが失われた場合は、交換用の管理ノードVMを再接続して失われたVMの設定データをリカバリできます。

インストールまたはアップグレード時に永続ボリューム機能を有効にすると、「`NetApp-HCI-`」で始まる名前の複数のボリュームが、割り当てられているクラスタに自動的に作成されます。これらのボリュームは、Elementソフトウェアベースのボリューム同様、ElementソフトウェアWeb UI、NetApp Element Plug-in for vCenter Server、またはAPIを使用して表示できます。リカバリに使用できる現在の設定データを保持するためには、永続ボリュームが管理ノードにiSCSI接続された状態で稼働している必要があります。

注意 : 管理サービスに関連付けられた永続ボリュームは、インストール時またはアップグレード時に作成され、新しいアカウントに割り当てられます。永続ボリュームを使用している場合は、ボリュームまたは関連するアカウントを変更または削除しないでください。

SolidFire Active IQ

Active IQは、クラスタ全体のデータの履歴ビューを提供するWebベースのツールです。ビューは定期的に更新されます。特定のイベント、しきい値、または指標にアラートを設定できます。Active IQを使用すると、システムのパフォーマンスと容量を監視し、クラスタの健全性を常に把握できます。

Active IQでは、システムに関する次の情報を確認できます。

- ノードの数およびステータス：健全、オフライン、またはエラー
- CPUとメモリの使用状況をグラフィカルに表示
- ノードに関する詳細（シリアル番号、シャーシ内のスロットの場所、モデル、ストレージ ノードで実行されているNetApp Elementソフトウェアのバージョンなど）
- 仮想マシンのCPUおよびストレージ関連情報

SolidFireソフトウェアのインターフェイス

NetApp Elementソフトウェアのインターフェイスと統合ユーティリティを使用して、SolidFireストレージ システムを管理できます。

NetApp Elementソフトウェア ユーザ インターフェイス

SolidFireストレージをセットアップし、クラスタの容量とパフォーマンスを監視できるほか、マルチテナント インフラ全体のストレージ アクティビティを管理できます。Element は SolidFire クラスタの中心にあるストレージオペレーティングシステムです。 Element ソフトウェアは、クラスタ内のすべてのノードで個別に実行され、クラスタのノードがリソースを結合して、外部クライアントに単一のストレージシステムとして提供できるようにします。 Element Software は、システム全体のすべてのクラスタ調整、拡張、および管理を担当します。 ソフトウェアのインターフェイスは、Element APIを基盤としています。

NetApp Element Plug-in for vCenter Server

Elementソフトウェアを実行しているストレージ クラスタを設定および管理できます。このプラグインは、VMware vSphereでElement UIの代わりとなるインターフェイスを提供します。

NetApp Elementソフトウェア API

一連のオブジェクト、メソッド、ルーチンを使用してSolidFireストレージを管理できます。Element APIは、HTTPS経由のJSON-RPCプロトコルに基づいています。[API Log]を有効にして、Element UIのAPI処理を監視できます。これにより、システムで実行されているメソッドを表示できます。要求と応答の両方を有効にすると、実行したメソッドに対するシステムの応答を確認できます。

管理ノード UI

管理ノードには、 REST ベースのサービスを管理するための UI と、ネットワークとクラスタの設定を管理するためのノード単位の UI 、およびオペレーティングシステムのテストとユーティリティの 2 つの UI があります。REST API UIからは、管理ノード上の管理サービスを制御するサービス関連APIのメニューにアクセスできます。

その他の統合ユーティリティ / ツール

通常はNetApp Element、NetApp Element API、およびNetApp Element Plug-in for vCenter Serverを使用してストレージを管理しますが、その他のユーティリティやツールを使用することもできます。

- ネットアップのダウンロード： *SolidFire vRO*
  VMware vRealize Orchestrator™を使用することで、SolidFire APIを使用してSolidFireストレージ システムを簡単に管理することができます。
- *NetApp* ダウンロード： *Element SDK*
  次のツールを使用して SolidFire クラスタを管理できます。
  - SolidFire コマンドライン
  - SolidFire Postman API テストスイート： SolidFire API 呼び出しをテストするポストマン関数のコレクションを使用できます。
  - SolidFire PowerShell ： SolidFire®®® API を使用して SolidFire ストレージシステムを管理する Microsoft Windows PowerShell 関数のコレクションをプログラマが使用できるようにします。
  - SolidFire SDK Java ： SolidFire API と Java™ プログラミング言語を統合できます。
  - SolidFire SDK .NET ： SolidFire API と .NET プログラミングプラットフォームを統合できます。

  - SolidFire SDK Python: プログラマ™は、 SolidFire API を Python プログラミング言語と統合できます。
- ネットアップのダウンロード： *SolidFire Storage Replication Adapter*
  VMware® Site Recovery Manager™（SRM）と統合して、レプリケートしたSolidFireストレージ クラスタ（アレイ）との通信を可能にし、サポートされているワークフローを実行します。
- ネットアップのダウンロード：*SolidFire VSS Provider*
  VSSシャドウ コピーをSolidFireのSnapshotおよびクローンと統合します。

ネットワーク

SolidFireシステムのネットワーク セットアップは、スイッチとポートの要件で構成されます。これらの要件の実装方法は、システムによって異なります。

関連概念

*Element*ソフトウェアを実行するクラスタのスイッチ設定（14ページ）

NetApp Elementソフトウェア システムには、スイッチに関する要件と、ストレージ パフォーマンスを最適化するためのベストプラクティスがあります。

関連資料

ネットワーク ポート要件（14ページ）

システムをリモートから管理し、クライアントがデータセンターの外部からリソースに接続できるようにするために、データセンターのエッジ ファイアウォールで次のTCPポートを許可する必要があります。システムの使用方法によっては、一部のポートは不要な場合もあります。

Elementソフトウェアを実行するクラスタのスイッチ設定

NetApp Elementソフトウェア システムには、スイッチに関する要件と、ストレージ パフォーマンスを最適化するためのベストプラクティスがあります。

ストレージ ノードには、ノードのハードウェアに応じて、10GbEまたは25GbEのいずれかのイーサネット スイッチが必要です。これらは、iSCSIストレージ サービスおよびノードのクラスタ内サービスの通信に使用されます。次のタイプのトラフィックには1GbEスイッチを使用できます。

- クラスタおよびノードの管理
- クラスタ内のノード間の管理トラフィック
- クラスタ ノードと管理ノード仮想マシンの間のトラフィック

ベストプラクティス : クラスタ トラフィックに使用するイーサネット スイッチを設定する際には、次のベストプラクティスに従う必要があります。

- クラスタ内の非ストレージ トラフィックには、高可用性と負荷分散を実現するために1GbEスイッチのペアを配置します。
- ストレージ ネットワーク スイッチでは、スイッチをペアにして配置し、ジャンボ フレーム（MTUサイズ＝9216バイト）を設定して利用します。これにより、インストールの失敗が回避され、パケットの断片化によるストレージ ネットワーク エラーが解消されます。

ネットワーク ポート要件

システムをリモートから管理し、クライアントがデータセンターの外部からリソースに接続できるようにするために、データセンターのエッジ ファイアウォールで次のTCPポートを許可する必要があります。システムの使用方法によっては、一部のポートは不要な場合もあります。

特に記載がないかぎり、ポートはすべてTCPで、ネットアップ サポート サーバ、管理ノード、およびElementソフトウェアを実行するノードの間の双方向通信を許可する必要があります。

ヒント：管理ノード、Elementソフトウェアを実行するノード、およびクラスタのMVIPの間でICMPを有効にします。

この表では次の略語を使用します。

- MIP：管理IPアドレス（ノードごとのアドレス）
- SIP：ストレージIPアドレス（ノードごとのアドレス）
- MVIP：管理仮想IPアドレス
- SVIP：ストレージ仮想IPアドレス

ソース	デスティネーション	ポート	説明
iSCSIクライアント	ストレージ クラスタのMVIP	443	（オプション）UIおよびAPIアクセス
iSCSIクライアント	ストレージ クラスタのSVIP	3260	クライアントiSCSI通信
iSCSIクライアント	ストレージ ノードのSIP	3260	クライアントiSCSI通信
管理ノード	`sfsupport.solidfire.com`	22	サポート アクセス用リバースSSHトンネル
管理ノード	ストレージ ノードのMIP	22	サポート用SSHアクセス
管理ノード	DNSサーバ	53 TCP / UDP	DNSルックアップ
管理ノード	ストレージ ノードのMIP	442	ストレージノードおよびElementソフトウェアのアップグレードへのUI / APIアクセス
管理ノード	オンラインのソフトウェア リポジトリ： • `https://repo.netapp.com/bintray/api/package` • `https://netapp-downloads.bintray.com`	443	管理ノード サービスのアップグレード
管理ノード	`monitoring.solidfire.com`	443	Active IQに報告するストレージ クラスタ
管理ノード	ストレージ クラスタのMVIP	443	ストレージノードおよびElementソフトウェアのアップグレードへのUI / APIアクセス
管理ノード	`connect.pub.nks.cloud`	443	NKSクラウド プロバイダとホスト型NKSサービスの間のセキュアな通信。たとえば、オンプレミスのNetApp HCIまたはVMwareにNKSが導入されている場合、トラフィックはこのNorthbound MTLSセキュア チャネルを使用します。

ソース	デスティネーション	ポート	説明
管理ノード	api.nks.netapp.io	443	オンプレミスの「リージョン」導入時の初期登録
管理ノード	repo.netapp.com	443	オンプレミス環境のインストール / 更新に必要なコンポーネントへのアクセス
34.208.181.140 34.217.162.31 54.187.65.159 18.236.231.155	管理ノード	443	HTTPS（Kubernetesクラスタ セキュリティ）
		6443	Kubernetes API（Kubernetesクラスタ セキュリティ）
		12443	ダッシュボードへのプロキシ（Kubernetesクラスタ セキュリティ）
		22	Kubernetesのアップグレードおよびその他のタスク（Kubernetesクラスタ セキュリティ）
管理ノード	amazonaws.com	443	ディスパッチ トンネル
SNMPサーバ	ストレージ クラスタのMVIP	161 UDP	SNMPポーリング
SNMPサーバ	ストレージ ノードのMIP	161 UDP	SNMPポーリング
ストレージ ノードのMIP	DNSサーバ	53 TCP / UDP	DNSルックアップ
ストレージ ノードのMIP	管理ノード	80	Elementソフトウェアのアップグレード
ストレージ ノードのMIP	S3 / Swiftエンドポイント	80	（オプション）バックアップとリカバリ用のS3 / Swiftエンドポイントへの HTTP通信
ストレージ ノードのMIP	NTPサーバ	123 UDP	NTP
ストレージ ノードのMIP	管理ノード	162 UDP	（オプション）SNMP トラップ
ストレージ ノードのMIP	SNMPサーバ	162 UDP	（オプション）SNMP トラップ
ストレージ ノードのMIP	LDAPサーバ	389 TCP / UDP	（オプション）LDAP検索
ストレージ ノードのMIP	リモート ストレージ クラスタのMVIP	443	リモート レプリケーションのクラスタ ペアリング通信
ストレージ ノードのMIP	リモート ストレージ ノードのMIP	443	リモート レプリケーションのクラスタ ペアリング通信
ストレージ ノードのMIP	S3 / Swiftエンドポイント	443	（オプション）バックアップとリカバリ用のS3 / Swiftエンドポイントへの HTTPS通信

ソース	デスティネーション	ポート	説明
ストレージ ノードのMIP	管理ノード	10514 TCP / UDP 514 TCP / UDP	syslog転送
ストレージ ノードのMIP	syslogサーバ	10514 TCP / UDP 514 TCP / UDP	syslog転送
ストレージ ノードのMIP	LDAPSサーバ	636 TCP / UDP	LDAPSルックアップ
ストレージ ノードのMIP	リモート ストレージ ノードのMIP	2181	リモート レプリケーション用のクラスタ間通信
ストレージ ノードのSIP	S3 / Swiftエンドポイント	80	（オプション）バックアップとリカバリ用のS3 / Swiftエンドポイントへのhttp通信
ストレージ ノードのSIP	S3 / Swiftエンドポイント	443	（オプション）バックアップとリカバリ用のS3 / Swiftエンドポイントへのhttps通信
ストレージ ノードのSIP	リモート ストレージ ノードのSIP	2181	リモート レプリケーション用のクラスタ間通信
ストレージ ノードのSIP	ストレージ ノードのSIP	3260	ノード間iSCSI
ストレージ ノードのSIP	リモート ストレージ ノードのSIP	4000～4020	リモート レプリケーションのノード間のデータ転送
ストレージ ノードのSIP	コンピューティング ノードのSIP	442	コンピューティング ノードAPI、設定と検証、ソフトウェア インベントリへのアクセス
システム管理者のPC	ストレージ ノードのMIP	80	（NetApp HCIのみ）NetApp Deployment Engineのランディング ページ
システム管理者のPC	管理ノード	442	管理ノードへのhttps UIアクセス
システム管理者のPC	ストレージ ノードのMIP	442	ストレージ ノードへのhttps UIおよびAPIアクセス
			（NetApp HCIのみ）NetApp Deployment Engineでの設定および導入監視
システム管理者のPC	管理ノード	443	管理ノードへのhttps UIおよびAPIアクセス
システム管理者のPC	ストレージ クラスタのMVIP	443	ストレージ クラスタへのhttps UIおよびAPIアクセス
システム管理者のPC	ストレージ ノードのMIP	443	httpsによるストレージ クラスタの作成、ストレージ クラスタへの導入後のUIアクセス

ソース	デスティネーション	ポート	説明
vCenter Server	ストレージ クラスタの MVIP	443	vCenter Plug-inのAPIアクセス
vCenter Server	管理ノード	8443	（オプション）vCenter Plug-inの QoSSIOCサービス。
vCenter Server	ストレージ クラスタの MVIP	8444	vCenter VASAプロバイダ アクセス（VVolのみ）
vCenter Server	管理ノード	9443	vCenter Plug-inの登録。登録完了後はポートを閉じてもかまいません。

システム セットアップ

SolidFireストレージ システムを使用するには、管理ノードをインストールして設定し、個々のノードを設定してクラスタを作成し、クラスタにドライブを追加する必要があります。

SolidFireストレージ システムは、ボリュームを使用してストレージをプロビジョニングします。ボリュームは、iSCSIクライアントまたはFibre Channelクライアントがネットワーク経由でアクセスするブロック デバイスです。クライアントはアカウントを使用してノード上のボリュームに接続します。ノード上のボリュームにアクセスするには、アカウントを作成する必要があります。

システムのセットアップを実行するには、ハードウェアがラックに設置され、ケーブル接続され、電源がオンになっている必要があります。ハードウェアのセットアップ手順は、ハードウェア本体に同梱されています。

SolidFireストレージ システムをセットアップするときは、一連の処理を正しい順序で実行し、ノードとクラスタを正しく設定する必要があります。

環境によってはFibre Channelノードをセットアップすることもできます。

関連タスク

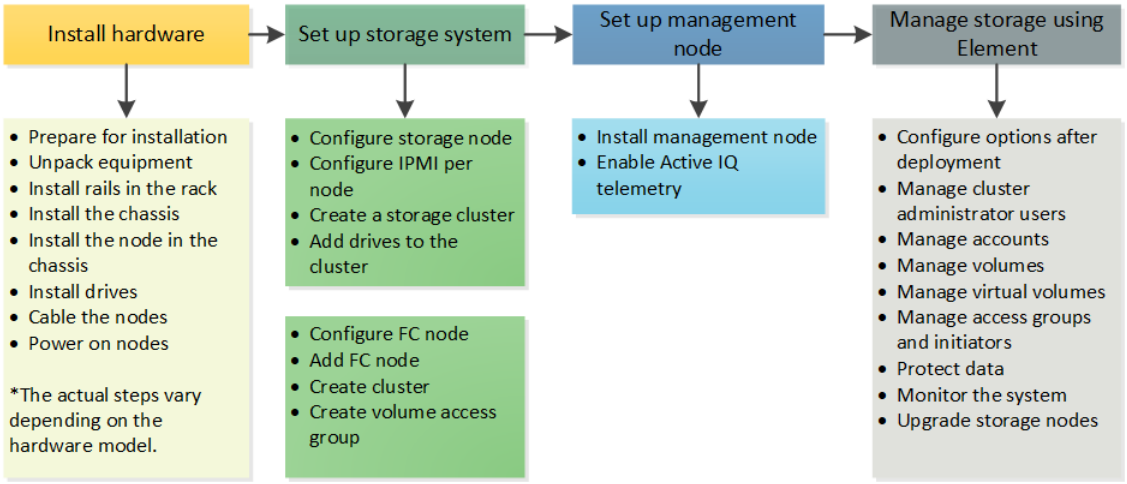
*Element*ソフトウェア*UI*の基本オプションの使用（42ページ）
NetApp Elementソフトウェア Webユーザ インターフェイス（Element UI）を使用して、SolidFireシステムの一般的なタスクを監視および実行することができます。

ユーザ アカウントの使用（77ページ）
SolidFireストレージ システムでは、クライアントはユーザ アカウントを使用してノード上のボリュームに接続します。ボリュームには、作成時に特定のユーザ アカウントが割り当てられます。

ボリュームの使用（80ページ）
SolidFireシステムは、ボリュームを使用してストレージをプロビジョニングします。ボリュームは、iSCSIクライアントまたはFibre Channelクライアントがネットワーク経由でアクセスするブロック デバイスです。[Management]タブの[Volumes]ページで、ノード上のボリュームを作成、変更、クローニング、および削除できます。また、ボリュームの帯域幅とI/O使用量に関する統計も確認できます。

セットアップの概要

開始する前に、NetApp Elementソフトウェアのインストールとセットアップの手順を理解しておくことを推奨します。



インストールするSolidFireコンポーネントの決定

設定および導入方法に応じて、管理ノード、Active IQ、NetApp Monitoring Agent（NMA）などのうち、どのSolidFireコンポーネントをインストールするべきかを確認できます。

タスク概要

次の表は、各追加コンポーネントについてインストールが必要かどうかを示しています。

コンポーネント	スタンドアロンのSolidFireストレージ クラスタ	NetApp HCIクラスタ
管理ノード	推奨	必須（デフォルトでインストールされる）
Active IQ	推奨*	推奨*
NetApp Monitoring Agent	サポート対象外	推奨

*容量ライセンスのSolidFireストレージ クラスタには、Active IQが必要です。

手順

1. どのコンポーネントをインストールするかを決定します。
2. 次の手順に従ってインストールを実行します。

   管理ノードのインストール（30ページ）

   *SolidFire Active IQ*の有効化（36ページ）

   NetApp Monitoring Agentの情報については、導入情報を参照してください。

   *NetApp HCI*ドキュメント センター

Elementストレージ システムのセットアップ

NetApp Elementソフトウェア ストレージ システムのセットアップでは、ストレージ ノードを設定してストレージ クラスタを作成し、クラスタにドライブを追加します。Fibre Channelネットワークを使用する場合は、Fibre Channelノードを設定できます。

手順

1. ストレージ ノードの設定（21ページ）
個々のノードをクラスタに追加する前に、ノードを設定する必要があります。ラックユニットにノードを設置してケーブル接続し、電源をオンにしたあと、ノード単位の UI またはノード端末ユーザインターフェイス（ TUI ）を使用してノードネットワーク設定を行うことができます。先に進む前に、ノードに必要なネットワーク設定情報があることを確認してください。

2. ストレージ クラスタの作成（24ページ）
個々のノードの設定がすべて完了したら、ストレージ クラスタを作成できます。クラスタを作成すると、クラスタ管理者のユーザ アカウントが自動的に作成されます。クラスタ管理者は、すべてのクラスタ属性を管理する権限を持ち、他のクラスタ管理者アカウントを作成できます。

3. *Element*ソフトウェア ユーザ インターフェイスへのアクセス（26ページ）
Element UIには、プライマリ クラスタ ノードの管理仮想IP（MVIP）アドレスを使用してアクセスできます。

4. クラスタへのドライブの追加（26ページ）
クラスタにノードを追加したり、既存のノードに新しいドライブを設置すると、ドライブが自動的に使用可能ドライブとして登録されます。ドライブがクラスタに参加できるようにするためには、Element UIまたはAPIを使用してドライブをクラスタに追加する必要があります。

5. *Fibre Channel*ノードの設定（26ページ）
Fibre Channelノードを使用すると、クラスタをFibre Channelネットワーク ファブリックに接続できます。Fibre Channelノードはペアで追加され、アクティブ / アクティブ モードで動作します（すべてのノードがクラスタのトラフィックをアクティブに処理します）。Elementソフトウェア バージョン9.0以降を実行しているクラスタは、最大4つのノード、9.0より前のバージョンを実行しているクラスタは最大2つのノードをサポートします。

ストレージ ノードの設定

個々のノードをクラスタに追加する前に、ノードを設定する必要があります。ラックユニットにノードを設置してケーブル接続し、電源をオンにしたあと、ノード単位の UI またはノード端末ユーザインターフェイス（ TUI ）を使用してノードネットワーク設定を行うことができます。先に進む前に、ノードに必要なネットワーク設定情報があることを確認してください。

ストレージノードの設定には、次の 2 つのオプションがあります。

ノード単位の UI

ノードごとの UI （`https://<node management IP>:442`）を使用して、ノードのネットワーク設定を行います。

注 : TUI 上部のメニューバーに表示される DHCP 1G 管理 IP アドレスを使用して、ノード単位の UI にアクセスします。

TUI

ノードを設定するには、ノードのターミナルユーザインターフェイス（ TUI ）を使用します。

DHCP によって割り当てられた IP アドレスを持つノードをクラスタに追加することはできません。DHCP IP アドレスを使用して、ノード単位の UI 、 TUI 、または API でノードを初期設定できます。この初期設定では、静的 IP アドレス情報を追加して、クラスタにノードを追加できます。

初期設定が完了したら、ノードの管理IPアドレスを使用してノードにアクセスできます。その後、ノード設定を変更したり、クラスタにノードを追加したり、またはノードを使用してクラスタを作成することができます。また、Elementソフトウェアapiメソッドを使用して新しいノードを設定することもできます。

注 : Elementバージョン11.0以降では、ノードの管理ネットワークにIPv4、IPv6、または両方のアドレスを設定できます。これはストレージ ノードと管理ノードのどちらにも該当します（IPv6がサポートされない管理ノード11.3以降を除く）。クラスタの作成時には、IPv4またはIPv6のどちらかのアドレスを1つだけMVIPに使用でき、これと同じアドレス タイプをすべてのノードで設定する必要があります。

関連タスク

ノード単位の *UI* を使用したストレージノードの設定（22ページ）
ノードは、ノード単位のユーザインターフェイスを使用して設定できます。

*TUI*を使用したノードの設定（23ページ）
ターミナル ユーザ インターフェイス（TUI）を使用して、新しいノードの初期設定を実行できます。

ストレージ クラスタの作成（24ページ）
個々のノードの設定がすべて完了したら、ストレージ クラスタを作成できます。クラスタを作成すると、クラスタ管理者のユーザ アカウントが自動的に作成されます。クラスタ管理者は、すべてのクラスタ属性を管理する権限を持ち、他のクラスタ管理者アカウントを作成できます。

関連資料

ノードの状態（24ページ）
設定のレベルによって、ノードは次のいずれかの状態になります。

関連情報

NetApp SolidFire Installation

ノード単位の UI を使用したストレージノードの設定

ノードは、ノード単位のユーザインターフェイスを使用して設定できます。

タスク概要

- IPv4アドレスまたはIPv6アドレスを使用するようにノードを設定できます。
- ノードにアクセスするには、TUIに表示されるDHCPアドレスが必要です。DHCPアドレスを使用して、ノードをクラスタに追加することはできません。

注意 : 管理（ bond1G ）インターフェイスとストレージ（ bond10G ）インターフェイスは、別々のサブネット用に設定する必要があります。同じサブネットに設定された bond1G インターフェイスと bond10G インターフェイスは、 bond1G インターフェイスを介してストレージトラフィックが送信されるときにルーティングの問題を引き起こします。管理トラフィックとストレージ トラフィックに同じサブネットを使用する必要がある場合は、Bond10Gインターフェイスを使用するように管理トラフィックを手動で設定してください。**Cluster Settings**これは、ノードごとの UI のページを使用して、各ノードに対して実行できます。

手順

1. ブラウザ ウィンドウで、ノードのDHCP IPアドレスを入力します。
   ノードにアクセスするには、末尾に「:442」を追加する必要があります（例:https://172.25.103.6:442）。
   Network SettingsBond1G「」セクションが表示されたタブが開きます。
2. 1G の管理ネットワーク設定を入力します。
3. **Apply Changes**をクリックします。
4. クリック**Bond10G**すると、 10G ストレージのネットワーク設定が表示されます。
5. 10G ストレージのネットワーク設定を入力します。
6. **Apply Changes**をクリックします。
7. **Cluster Settings**をクリックします。
8. 10Gネットワークのホスト名を入力します。
9. クラスタ名を入力します。

   重要 : クラスタを作成する前に、この名前をすべてのノードの構成に追加する必要があります。クラスタ内のすべてのノードのクラスタ名が同じである必要があります。クラスタ名では大文字と小文字が区別されます。

10. **Apply Changes**をクリックします。

関連タスク

*TUI*を使用したノードの設定（23ページ）
ターミナル ユーザ インターフェイス（TUI）を使用して、新しいノードの初期設定を実行できます。

関連資料

ノード単位の *UI*からのネットワーク設定の詳細（186ページ）
ストレージノードのネットワーク設定を変更して、ノードに新しいネットワーク属性のセットを割り当てることができます。

クラスタ設定の詳細は、ノード単位の *UI*から取得します（187ページ）
クラスタ構成後にストレージノードのクラスタ設定を確認し、ノードのホスト名を変更できます。

TUIを使用したノードの設定

ターミナル ユーザ インターフェイス（TUI）を使用して、新しいノードの初期設定を実行できます。

タスク概要

bond1G （管理）インターフェイスと bond10G （ストレージ）インターフェイスは、別々のサブネット用に設定する必要があります。同じサブネットにBond1Gインターフェイスと Bond10Gインターフェイスを設定すると、ストレージ トラフィックがBond1Gインターフェイス経由で送信される場合にルーティングの問題が発生します。管理トラフィックとストレージ トラフィックに同じサブネットを使用する必要がある場合は、Bond10Gインターフェイスを使用するように管理トラフィックを手動で設定してください。**Cluster** > **Nodes**Elementは、エレメント UI のページを使用して、各ノードで実行できます。

手順

1. キーボードとモニタをノードに接続し、ノードの電源をオンにします。
   TUI の NetApp Storage メインメニューが、 TTY1 端末に表示されます。

注 : ノードが設定サーバにアクセスできない場合は、TUIにエラー メッセージが表示されます。このエラーを解決するには、設定サーバの接続またはネットワーク接続を確認してください。

2. **Network** > **Network Config**の順に選択します。

   ヒント : メニュー内を移動するには、上矢印キーまたは下矢印キーを押します。別のボタンまたはボタンのフィールド**Tab**に移動するには、を押します。フィールド間を移動するには、上矢印キーまたは下矢印キーを使用します。

3. **Bond1G (Management)**または**Bond10G (Storage)**を選択して、ノードの 1G および 10G ネットワークを設定します。
4. ボンドモードフィールド**Tab**とステータスフィールドで、を押してヘルプボタンを選択し、使用可能なオプションを確認します。

   クラスタ内のすべてのノードのクラスタ名が同じである必要があります。クラスタ名では大文字と小文字が区別されます。使用可能なIPアドレスのあるネットワーク上でDHCPサーバが稼働している場合は、1GbEのアドレスが[Address]フィールドに表示されます。
5. を押して**TabOK**ボタンを選択し、変更を保存します。

   ノードが保留状態になり、既存のクラスタまたは新しいクラスタに追加できます。

関連タスク

ノード単位の *UI* を使用したストレージノードの設定（22ページ）

ノードは、ノード単位のユーザインターフェイスを使用して設定できます。

ノードの状態

設定のレベルによって、ノードは次のいずれかの状態になります。

利用可能

ノードにはクラスタ名が関連付けられておらず、まだクラスタの一部ではありません。

保留

ノードが設定され、指定されたクラスタに追加できます。

このノードにアクセスするための認証は不要です。

保留中のアクティブ

互換性のある Element ソフトウェアをノードにインストールしています。完了すると、ノードはアクティブ状態に移行します。

Active

ノードはクラスタに参加しています。

このノードを変更するには、認証が必要です。

上記の各状態では、一部のフィールドは読み取り専用です。

ストレージ クラスタの作成

個々のノードの設定がすべて完了したら、ストレージ クラスタを作成できます。クラスタを作成すると、クラスタ管理者のユーザ アカウントが自動的に作成されます。クラスタ管理者は、すべてのクラスタ属性を管理する権限を持ち、他のクラスタ管理者アカウントを作成できます。

開始する前に

- 管理ノードをインストールしておきます。
- 個々のノードの設定をすべて完了しておきます。

タスク概要

各ノードには、設定時に1Gまたは10Gの管理IP（MIP）アドレスが複数割り当てられています。Create a New Clusterページを開くには、設定時に作成したノード IP アドレスのいずれかを使用する必要があります。使用するIPアドレスは、クラスタ管理用に選択したネットワークによって決まります。

注 : 新しいクラスタを作成する場合：

- 共有シャーシにあるストレージノードを使用する場合は、保護ドメイン機能を使用してシャーシレベルの障害保護を設計することを検討してください。
- 共有シャーシが使用されていない場合は、カスタム保護ドメインレイアウトを定義できます。

手順

1. ブラウザ ウィンドウで、ノードのMIPアドレスを入力します。
2. で**Create a New Cluster**、次の情報を入力します。
   - Management VIP : ネットワーク管理タスク用の、1GbEまたは10GbEネットワーク上のルーティング可能な仮想IP。

     注 : 新しいクラスタはIPv4またはIPv6のアドレスを使用して作成できます。
   - iSCSI (storage) VIP：ストレージおよびiSCSI検出用の10GbEネットワーク上の仮想IP。

     注 : クラスタを作成したあとにMVIP、SVIP、またはクラスタ名を変更することはできません。
   - User name：クラスタへの認証されたアクセスに使用するプライマリ クラスタ管理者ユーザ名。このユーザ名は、あとで参照できるように記録しておく必要があります。

     注 : ユーザ名とパスワードには、大文字と小文字のアルファベット、特殊文字、および数字を使用できます。
   - Password：クラスタへの認証されたアクセスに使用するパスワード。このパスワードは、あとで参照できるように記録しておく必要があります。

   双方向のデータ保護がデフォルトで有効になります。この設定は変更できません。
3. エンドユーザライセンス契約を読み、**I Agree**をクリックします。
4. オプション: [Nodes]リストで、クラスタに含めないノードのチェック ボックスがオフになっていることを確認します。
5. **Create Cluster**をクリックします。

   クラスタ内のノードの数によっては、クラスタの作成に数分かかることがあります。適切に設定したネットワークで、5ノードの小規模なクラスタを作成する場合の所要時間は1分未満です。クラスタの作成後Create a New Cluster 、ウィンドウはクラスタの MVIP URL アドレスにリダイレクトされ、要素 UI が表示されます。

関連情報

*Element API*を使用したストレージの管理

Elementソフトウェア ユーザ インターフェイスへのアクセス

Element UIには、プライマリ クラスタ ノードの管理仮想IP（MVIP）アドレスを使用してアクセスできます。

開始する前に

ブラウザでポップアップ ブロックとNoScriptの設定が無効になっていることを確認する必要があります。

タスク概要

クラスタ作成時の設定に応じて、IPv4またはIPv6アドレスを使用してUIにアクセスできます。

手順

1. 次のいずれかを選択します。
   - IPv6：「`https://[IPv6 MVIP address]`」を入力します。次に例を示します。

     ```
     https://[fd20:8b1e:b256:45a::1234]/
     ```
   - IPv4：「`https://<IPv4 MVIP address>`」を入力します。次に例を示します。

     ```
     https://10.123.456.789/
     ```
2. DNSのホスト名を入力します。
3. 認証証明書のメッセージが表示されたら該当するボタンをクリックして確認します。

クラスタへのドライブの追加

クラスタにノードを追加したり、既存のノードに新しいドライブを設置すると、ドライブが自動的に使用可能ドライブとして登録されます。ドライブがクラスタに参加できるようにするためには、Element UIまたはAPIを使用してドライブをクラスタに追加する必要があります。

タスク概要

次の場合、ドライブは[Available Drives]リストに表示されません。

- ドライブがActive、Removing、Erasing、Failedのいずれかの状態である。
- ドライブが含まれているノードがPending状態である。

手順

1. Elementユーザ インターフェイスから、**[Cluster]** > **[Drives]**を選択します。
2. **[Available]**をクリックして、使用可能ドライブのリストを表示します。
3. 次のいずれかを実行します。
   - 個々のドライブを追加するには、追加するドライブの**[Actions]**アイコンをクリックし、**[Add]**をクリックします。
   - 複数のドライブを追加するには、追加するドライブのチェック ボックスをオンにし、**[Bulk Actions]**をクリックしてから**[Add]**をクリックします。

関連情報

How to calculate max provisioned space in a SolidFire cluster

Fibre Channelノードの設定

Fibre Channelノードを使用すると、クラスタをFibre Channelネットワーク ファブリックに接続できます。Fibre Channelノードはペアで追加され、アクティブ / アクティブ モードで動作します（すべてのノードがクラスタのトラフィックをアクティブに処理します）。

Elementソフトウェア バージョン9.0以降を実行しているクラスタは、最大4つのノード、9.0より前のバージョンを実行しているクラスタは最大2つのノードをサポートします。

Fibre Channelノードを設定する前に、次の条件を満たしていることを確認する必要があります。

- 少なくとも2つのFibre ChannelノードがFibre Channelスイッチに接続されている。
- すべてのSolidFire Fibre ChannelポートがFibre Channelファブリックに接続されている。4つのSolidFire Bond10Gネットワーク接続がスイッチ レベルで1つのLACPボンド グループに接続されている。これにより、Fibre Channelシステム全体で最高のパフォーマンスを実現できます。
- このネットアップ ナレッジベースの記事に記載されているファイバチャネルクラスタに関するすべてのベストプラクティスを確認し、検証します。
  ネットアップ ナレッジベースの回答*1091832*：「*SolidFire FC cluster best practice*」

ネットワークとクラスタの設定手順は、Fibre Channelノードとストレージ ノードで同じです。

Fibre ChannelノードとSolidFireストレージ ノードを含む新しいクラスタを作成すると、ノードのWorld Wide Port Name（WWPN）アドレスがElement UIで使用できるようになります。WWPNアドレスを使用して、Fibre Channelスイッチをゾーニングできます。

WWPNは、ノードを含む新しいクラスタの作成時にシステムに登録されます。Element UIFC PortsCluster では、タブの WWPN カラムから WWPN アドレスを検索できます。このタブには、タブからアクセスできます。

関連タスク

ノード単位の *UI* を使用したストレージノードの設定（22ページ）
ノードは、ノード単位のユーザインターフェイスを使用して設定できます。

*TUI*を使用したノードの設定（23ページ）
ターミナル ユーザ インターフェイス（TUI）を使用して、新しいノードの初期設定を実行できます。

ストレージ クラスタの作成（24ページ）
個々のノードの設定がすべて完了したら、ストレージ クラスタを作成できます。クラスタを作成すると、クラスタ管理者のユーザ アカウントが自動的に作成されます。クラスタ管理者は、すべてのクラスタ属性を管理する権限を持ち、他のクラスタ管理者アカウントを作成できます。

関連情報

SolidFire Fibre Channel Configuration Guide

クラスタへのFibre Channelノードの追加

ストレージの追加が必要になったとき、またはクラスタ作成時に、クラスタにFibre Channelノードを追加できます。Fibre Channelノードは、初回の電源投入時に初期設定を行う必要があります。設定が完了したノードは、保留状態のノードのリストに表示され、クラスタに追加できるようになります。

タスク概要

クラスタ内の各Fibre Channelノードは、互換性のあるソフトウェア バージョンを実行している必要があります。クラスタにFibre Channelノードを追加すると、必要に応じて新しいノードにElementのクラスタ バージョンがインストールされます。

手順

1. **[Cluster]** > **[Nodes]**の順に選択します。
2. **[Pending]**をクリックして、保留状態のノードのリストを表示します。

3. 次のいずれかを実行します。
   - 個々のノードを追加するには、追加するノードの**[Actions]**アイコンをクリックします。
   - 複数のノードを追加するには、追加するノードのチェック ボックスをオンにして、**[Bulk Actions]**を選択します。

     注 :

     追加するノードのElementのバージョンがクラスタで実行されているバージョンと異なる場合は、クラスタ マスターで実行されているElementのバージョンに非同期的に更新されます。更新されたノードは、自動的にクラスタに追加されます。この非同期プロセスの実行中、ノードの状態はpendingActiveになります。

4. **[Add]**をクリックします。
   ノードがアクティブなノードのリストに表示されます。

Fibre Channelノードを含む新しいクラスタの作成

個々のFibre Channelノードの設定が完了したら、新しいクラスタを作成できます。クラスタを作成すると、クラスタ管理者のユーザ アカウントが自動的に作成されます。クラスタ管理者は、すべてのクラスタ属性を管理する権限を持ち、他のクラスタ管理者アカウントを作成できます。

開始する前に

個々のFibre Channelノードの設定を完了しておきます。

タスク概要

各ノードには、設定時に1Gまたは10Gの管理IP（MIP）アドレスが複数割り当てられています。[Create a New Cluster]ページを開くには、設定時に作成されたいずれかのノードIPアドレスを使用する必要があります。使用するIPアドレスは、クラスタ管理用に選択したネットワークによって決まります。

手順

1. ブラウザ ウィンドウで、ノードのMIPアドレスを入力します。
2. **[Create a New Cluster]**で、次の情報を入力します。
   - Management VIP : ネットワーク管理タスク用の、1GbEまたは10GbEネットワーク上のルーティング可能な仮想IP。
   - iSCSI (storage) VIP：ストレージおよびiSCSI検出用の10GbEネットワーク上の仮想IP。

     注 : クラスタを作成したあとにSVIPを変更することはできません。
   - User name：クラスタへの認証されたアクセスに使用するプライマリ クラスタ管理者ユーザ名。このユーザ名は、あとで参照できるように記録しておく必要があります。

     注 : ユーザ名には、大文字と小文字のアルファベット、特殊文字、および数字を使用できます。
   - Password：クラスタへの認証されたアクセスに使用するパスワード。このパスワードは、あとで参照できるように記録しておく必要があります。

   双方向のデータ保護がデフォルトで有効になります。この設定は変更できません。
3. エンド ユーザ ライセンス契約を読み、**[I Agree]**をクリックします。
4. オプション: [Nodes]リストで、クラスタに含めないノードのチェック ボックスがオフになっていることを確認します。

5. **[Create Cluster]**をクリックします。

   クラスタ内のノードの数によっては、クラスタの作成に数分かかることがあります。適切に設定したネットワークで、5ノードの小規模なクラスタを作成する場合の所要時間は1分未満です。クラスタが作成されると、[Create a New Cluster]ウィンドウからクラスタのMVIP URLアドレスにリダイレクトされ、Web UIが表示されます。

Fibre Channelノードのゾーニング

Fibre ChannelノードとSolidFireストレージ ノードを含む新しいクラスタを作成すると、ノードのWorld Wide Port Name（WWPN）アドレスがWeb UIで使用できるようになります。WWPNアドレスを使用して、Fibre Channelスイッチをゾーニングできます。

WWPNは、ノードを含む新しいクラスタの作成時にシステムに登録されます。Element UIでは、[FC Ports]タブ（[Cluster]タブからアクセス）の[WWPN]列でWWPNアドレスを確認できます。

Fibre Channelクライアントのボリューム アクセス グループの作成

ボリューム アクセス グループによって、Fibre ChannelクライアントとSolidFireストレージ システム上のボリューム間の通信が可能になります。Fibre Channelクライアントのイニシエータ（WWPN）をボリューム アクセス グループ内のボリュームにマッピングすることで、Fibre ChannelネットワークとSolidFireボリュームの間の安全なデータI/O通信が実現します。

タスク概要

iSCSIイニシエータをボリューム アクセス グループに追加することもできます。これにより、イニシエータはボリューム アクセス グループ内の同じボリュームにアクセスできるようになります。

手順

1. **[Management]** > **[Access Groups]**の順にクリックします。
2. **[Create Access Group]**をクリックします。
3. **[Name]**フィールドにボリューム アクセス グループの名前を入力します。
4. **[Unbound Fibre Channel Initiators]**リストからFibre Channelイニシエータを選択して追加します。

   注 : イニシエータはあとから追加または削除できます。

5. オプション: **[Initiators]**リストからiSCSIイニシエータを選択して追加します。
6. ボリュームをアクセス グループに接続するには、次の手順を実行します。
   1. **[Volumes]**リストからボリュームを選択します。
   2. **[Attach Volume]**をクリックします。
7. **[Create Access Group]**をクリックします。

管理ノードのセットアップ

NetApp Elementソフトウェア管理ノード（mNode）をインストールできます。管理ノードは、Elementソフトウェアベースのストレージ クラスタと連携して実行される仮想マシンです。このノードは、監視とテレメトリなどのシステム サービスのアップグレードと提供、クラスタのアセットと設定の管理、システムのテストとユーティリティの実行、ネットアップ サポートへのアクセス許可（トラブルシューティング）に使用します。

手順

1. 管理ノードのインストール（30ページ）

NetApp Elementソフトウェアを実行しているクラスタの管理ノードは、構成に応じたイメージを使用して手動でインストールできます。この手動プロセスは、管理ノードのインストールにNetApp Deployment Engineを使用していないSolidFireオールフラッシュ ストレージ管理者およびNetApp HCI管理者を対象としています。

2. ストレージ *NIC* の設定（35ページ）
ストレージに追加の NIC を使用している場合は、管理ノードに SSH で接続するか、vCenter コンソールを使用して cURL コマンドを実行し、そのネットワークインターフェイスを設定できます。

3. *SolidFire Active IQ*の有効化（36ページ）
NetApp Elementソフトウェアを実行するクラスタの管理ノードのインストール時に、SolidFire Active IQを手動で有効にすることができます。

管理ノードのインストール

NetApp Elementソフトウェアを実行しているクラスタの管理ノードは、構成に応じたイメージを使用して手動でインストールできます。この手動プロセスは、管理ノードのインストールにNetApp Deployment Engineを使用していないSolidFireオールフラッシュ ストレージ管理者およびNetApp HCI管理者を対象としています。

開始する前に

- クラスタでNetApp Elementソフトウェア11.3以降を実行している必要があります。
- インストール環境でIPv4を使用している必要があります。管理ノード11.3ではIPv6がサポートされません。

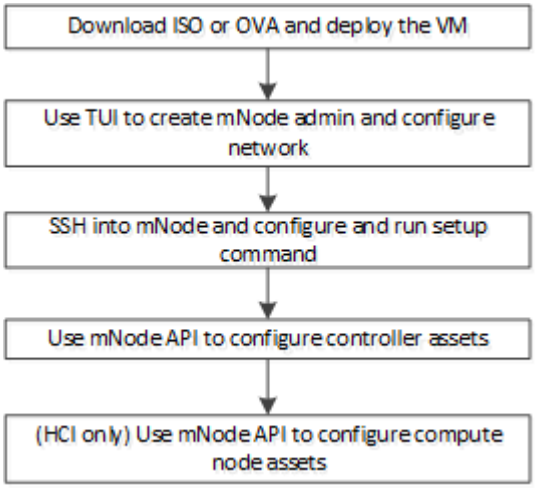
  注 : IPv6のサポートが必要な場合は、管理ノード11.1を使用してください。
- ネットアップ サポート サイトからソフトウェアをダウンロードする権限が必要です。
- 使用するプラットフォームに適した管理ノード イメージの種類を特定しておきます。次の表を参考にしてください。

プラットフォーム	インストール イメージの種類
Microsoft Hyper-V	`.iso`
KVM	`.iso`
VMware vSphere	`.iso`, `.ova`
Citrix XenServer	`.iso`
OpenStack	`.iso`

タスク概要

この手順を実行する前に、永続ボリュームについて理解し、永続ボリュームを使用するかどうかを決定しておく必要があります。永続ボリュームを使用すると、管理ノードのデータを指定したストレージ クラスタに格納できるため、管理ノードが失われた場合や削除された場合でもデータを保持することができます。

次の図に、この手順の概要を示します。



手順

1. ネットアップ サポート サイトから、インストール環境に対応したOVAまたはISOをダウンロードします。
   - Elementソフトウェア：
   - NetApp HCI：

   1. ダウンロードするソフトウェアのバージョン番号を選択します。
   2. **Go**をクリックします。
   3. 表示されるプロンプトをそれぞれクリックして確認し、EULAに同意し、ダウンロードする管理ノードのイメージを選択します。
2. OVAをダウンロードした場合は、次の手順を実行します。
   1. OVAを導入します。
   2. ストレージクラスタが管理ノード（ eth0 ）とは別のサブネット上にあり、同一ボリュームを使用する場合は、ストレージサブネット（ eth1 など）上の VM に 2 つ目のネットワークインターフェイスコントローラ（ NIC ）を追加するか、管理ネットワークがストレージネットワークにルーティングできることを確認します。
3. ISOをダウンロードした場合は、次の手順を実行します。
   1. 以下の構成でハイパーバイザーから新しい64ビットの仮想マシンを作成します。
      - 仮想CPU×6
      - 12GB RAM
      - 400GBの仮想ディスク、シンプロビジョニング
      - インターネット アクセスとストレージMVIPへのアクセスが可能な仮想ネットワーク インターフェイス×1
      - （SolidFireオールフラッシュ ストレージの場合はオプション）ストレージ クラスタへの管理ネットワーク アクセスが可能な仮想ネットワーク インターフェイス×1。ストレージ クラスタが管理ノード（eth0）とは別のサブネット上にある環境で永続ボリュームを使用する場合は、ストレージ サブネット（eth1）上のVMに2つ目のネットワーク インターフェイス コントローラ（NIC）を追加するか、管理ネットワークからストレージ ネットワークへルーティング可能なことを確認します。

      注意 : このあとの手順で指示があるまでは仮想マシンの電源をオンにしないでください。

2. 仮想マシンにISOを接続し、 .isoインストール イメージでブートします。

   注 : イメージを使用して管理ノードをインストールすると、スプラッシュ画面が表示されるまでに30秒程度かかることがあります。

4. インストールが完了したら、管理ノードの仮想マシンの電源をオンにします。
5. ターミナル ユーザ インターフェイス（TUI）を使用して、管理ノードの管理ユーザを作成します。

   ヒント : メニューオプション間を移動するには、上矢印キーまたは下矢印キーを押します。ボタン間を移動するに**Tab**は、を押します。ボタンからフィールド**Tab**に移動するには、を押します。フィールド間を移動するには、上矢印キーまたは下矢印キーを押します。

6. 管理ノード ネットワーク（eth0）を設定します。

   注 : ストレージトラフィックを分離するために追加の NIC が必要な場合は、別の NIC の設定手順を参照してください。

   ストレージ *NIC* の設定（35ページ）

7. 管理ノードにSSH接続します。
8. SSHを使用して次のコマンドを実行し、root権限を取得します。プロンプトが表示されたら、パスワードを入力します。

   ```
   sudo su
   ```

9. 管理ノードとストレージ クラスタの間で時刻が同期されている（NTP）ことを確認します。

   注 : vSphere で**Synchronize guest time with host**は、 VM オプションのボックスをオンにする必要があります。今後VMを変更する場合はこのオプションを無効にしないでください。

10. 管理ノードのセットアップ コマンドを設定します。

    注 : セキュアプロンプトでパスワードを入力するように求められます。クラスタがプロキシ サーバの背後にある場合、パブリック ネットワークに接続できるようにプロキシを設定する必要があります。

    ```
    /sf/packages/mnode/setup-mnode --mnode_admin_user [username] --storage_mvip [mvip] --
    storage_username [username] --telemetry_active [true]
    ```

    1. 次の各必須パラメータについて、[ ]内の値（かっこを含む）を置き換えます。

       注 : ( )内はコマンドの省略名で、正式な名前の代わりに使用できます。

       --mnode_admin_user (-mu) [username]
       管理ノードの管理者アカウントのユーザ名。一般には、管理ノードへのログインに使用したユーザ アカウントのユーザ名です。

       --storage_mvip (-sm) [MVIP address]
       Elementソフトウェアを実行しているストレージ クラスタのMVIP（管理仮想IPアドレス）。

       --storage_username (-su) [username]
       --storage_mvipパラメータで指定したクラスタのストレージ クラスタ管理者のユーザ名。

--telemetry_active (-t) [true]

trueのままにして、Active IQによる分析のためのデータ収集を有効にします。

2. （オプション）： アクティブな IQ エンドポイントパラメータをコマンドに追加します。

--remote_host (-rh) [AIQ_endpoint]

Active IQのテレメトリ データが処理される送信先エンドポイント。このパラメータを指定しない場合、デフォルトのエンドポイントが使用されます。

3. （オプション）： 永続ボリュームに関する以下のパラメータを追加します。

注意 : 永続ボリューム機能用に作成された
アカウントとボリュームを変更または削除
しないでください。変更または削除すると、
管理機能が失われます。

--use_persistent_volumes (-pv) [true/false, default: false]

永続ボリュームを有効または無効にします。永続ボリューム機能を有効にするには、trueを入力します。

--persistent_volumes_account (-pva) [account_name]

--use_persistent_volumesをtrueに設定した場合、永続ボリュームに使用するストレージ アカウント名をこのパラメータに入力します。

注 : 永続ボリュームには、クラスタ上の既存のアカウント名とは異なる一意のアカウント名を使用してください。永続ボリュームのアカウントを他の環境から切り離すことが非常に重要です。

--persistent_volumes_mvip (-pvm) [mvip]

永続ボリュームを使用する、Elementソフトウェアを実行しているストレージ クラスタのMVIP（管理仮想IPアドレス）を入力します。このパラメータは、管理ノードで複数のストレージ クラスタが管理されている場合にのみ必須です。複数のクラスタを管理していない場合は、デフォルトのクラスタMVIPが使用されます。

4. プロキシ サーバを設定します。

--use_proxy (-up) [true/false, default: false]

プロキシの使用を有効または無効にします。プロキシ サーバを設定する場合、このパラメータは必須です。

--proxy_hostname_or_ip (-pi) [host]

プロキシのホスト名またはIP。プロキシを使用する場合には必須です。このパラメータを指定すると、--proxy_portの入力を求められます。

--proxy_username (-pu) [username]

プロキシ ユーザ名。このパラメータは省略可能です。

--proxy_password (-pp) [password]

プロキシ パスワード。このパラメータは省略可能です。

--proxy_port (-pq) [port, default: 0]

プロキシ ポート。このパラメータを指定すると、プロキシのホスト名またはIP（--proxy_hostname_or_ip）の入力を求められます。

--proxy_ssh_port (-ps) [port, default: 443]

SSHプロキシ ポート。デフォルト値はポート443です。

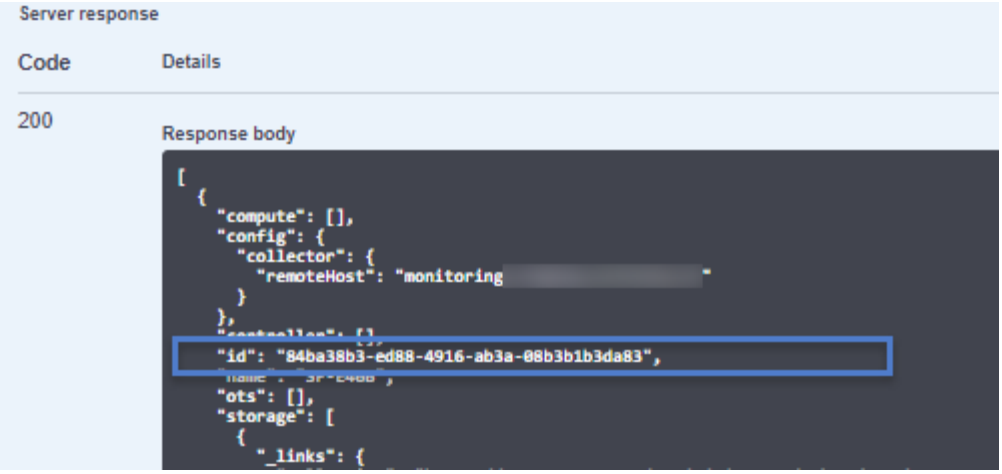
11. （オプション）各パラメータに関する詳細情報が必要な場合は、helpパラメータを使用します。

    --help (-h)

    各パラメータに関する情報を返します。パラメータは、初期導入時の構成に基づいて必須かオプションかが決まります。アップグレードと再導入ではパラメータの要件が異なる場合があります。

12. `setup-mnode`コマンドを実行します。
13. ブラウザから、管理ノード REST API UI にログインします。
    1. Storage MVIP にアクセスしてログインします。
       次の手順用に証明書が承認されます。
    2. 管理ノードで REST API UI を開きます。 `https://[management node IP]/mnode`
14. Management Node REST API UI で**Authorize**、または任意のロックアイコンをクリックし、次の手順を実行します。
    1. クラスタのユーザ名とパスワードを入力します。
    2. `mnode-client`の値がまだ入力されていない場合は、クライアントIDを入力します。
    3. **Authorize**クリックするとセッションが開始されます。
15. 次**GET /assets**の手順で必要なベースアセット ID を検索するには、を実行します。
    1. [**GET /assets**
    2. **Try it out**をクリックします。
    3. **Execute**をクリックします。
    4. ベース アセットの`"id"`の値をクリップボードにコピーします。

       注 : インストール環境には、インストール時またはアップグレード時に作成されたベース アセットの構成が含まれています。



16. HCI 監視用の vCenter コントローラ資産（ NetApp HCI インストールのみ）とハイブリッドクラウド制御（すべてのインストール用）を、管理ノードの既知の資産に追加します。
    1. **POST /assets/{asset_id}/controllers**クリックすると、コントローラのサブアセットが追加されます。
    2. **Try it out**をクリックします。
    3. **Model**タブで定義されている必要なペイロード値を vCenter と vCenter のクレデンシャルのタイプで入力します。

4. クリップボードにコピーし**asset_id**た親ベースアセット ID を「」フィールドに入力します。
5. **Execute**をクリックします。

17. （ NetApp HCI の場合のみ）管理ノードの既知の資産にコンピューティングノード資産を追加します。

1. **POST/assets/{asset_id}/compute-nodes**クリックすると、コンピュートノードアセットの資格情報を含むコンピュートノードサブアセットが追加されます。
2. **Try it out**をクリックします。
3. ペイロードに**Model**、タブで定義されている必要なペイロード値を入力します。`ESXi` ホストを入力し、 "Hardware_Tag" パラメータを削除します。
4. クリップボードにコピーし**asset_id**た親ベースアセット ID を「」フィールドに入力します。
5. **Execute**をクリックします。

関連概念

永続ボリューム（12ページ）
永続ボリュームを使用すると、管理ノードの設定データをローカルなVMではなく指定したストレージ クラスタに格納できるため、管理ノードが失われた場合や削除された場合でもデータを保持することができます。永続ボリュームはオプションですが、推奨される管理ノード設定です。

管理ノードの使用（191ページ）
管理ノード（mNode）は、システム サービスのアップグレード、クラスタのアセットと設定の管理、システムのテストとユーティリティの実行、Active IQへの接続（システム監視）、ネットアップ サポートへのアクセス許可（トラブルシューティング）に使用します。

関連タスク

管理ノードのノード*UI*へのアクセス（192ページ）
ノードUIからは、ネットワークとクラスタの設定にアクセスし、システムのテストとユーティリティを利用できます。

管理ノードの*REST API UI*へのアクセス（193ページ）
Elementソフトウェア バージョン11.3以降、管理ノードには2つのUIが装備されています。RESTベースのサービスを管理するためのUIと、ネットワーク / クラスタ設定の管理とオペレーティング システムのテスト / ユーティリティを実行するためのノードUIです。REST API UIからは、管理ノード上の管理サービスを制御するサービス関連APIのメニューにアクセスできます。

*TUI*を使用したノードの設定（23ページ）
ターミナル ユーザ インターフェイス（TUI）を使用して、新しいノードの初期設定を実行できます。

ストレージ NIC の設定

ストレージに追加の NIC を使用している場合は、管理ノードに SSH で接続するか、vCenter コンソールを使用して cURL コマンドを実行し、そのネットワークインターフェイスを設定できます。

開始する前に

- eth0 の IP アドレスがわかっている。
- クラスタでNetApp Elementソフトウェア11.3以降を実行している必要があります。
- 管理ノード11.3以降を導入しておきます。

手順

1. SSHまたはvCenterコンソールを開きます。
2. 新しいストレージネットワークインターフェイスに必要な各パラメータについて、次のコマンドテンプレート（ $ で表示）の値を置き換えます。

   注 : 次のテンプレートのクラスタオブジェクトは必須であり、管理ノードのホスト名の名前変更に使用できます。本番環境では、 --insecure または -k オプションを使用しないでください。

```
curl -u $mnode_user_name : $mnode_password -- 安全でない -x post\
https://$mnode_ip:442/json-rpc/10.0\
 -H 'Content-Type: application/json' \
 -H 'cache-control: no-cache' \
 -d '  {
       "params": {
               "network": {
                       "$eth1" : {
                           "# default" : false 、
                           " アドレス " : "$storage_ip" 、
                           "auto" : true 、
                            「ファミリー」:「 INET 」
                            「方法」:「静的」、
                            「 MTU 」:「 9000 」、
                            「ネットマスク」:「 252.0 」、
                            「ステータス」:「アップ」
                       }
     },
               "cluster": {
                       " 名前 " : "$mnode_host_name"
               }
        },
        "method": "SetConfig"
}
'
```

3. コマンドを実行します。

SolidFire Active IQの有効化

NetApp Elementソフトウェアを実行するクラスタの管理ノードのインストール時に、SolidFire Active IQを手動で有効にすることができます。

開始する前に

- クラスタでNetApp Elementソフトウェア11.3以降を実行している必要があります。

手順

管理ノードのインストール情報に記載されている手順に従います。セットアップ スクリプトで使用される--telemetry_activeパラメータは、Active IQによる分析のためのデータ収集を有効にします。

管理ノードのインストール（30ページ）

関連概念

SolidFire Active IQ（12ページ）
Active IQは、クラスタ全体のデータの履歴ビューを提供するWebベースのツールです。ビューは定期的に更新されます。特定のイベント、しきい値、または指標にアラートを設定できます。Active IQを使用すると、システムのパフォーマンスと容量を監視し、クラスタの健全性を常に把握できます。

関連タスク

*SolidFire*オールフラッシュ ストレージに対する*Active IQ*コレクタ サービスの有効化（199ページ）

インストールまたはアップグレード時にSolidFireオールフラッシュ ストレージに対して ストレージのテレメトリ（Active IQコレクタ サービス）を有効にしていない場合、有効 にすることができます。AIQコレクタ サービスは、履歴データのレポートおよびほぼリア ルタイムのパフォーマンス監視用に、設定データとElementソフトウェアベースのクラス タ パフォーマンス データをNetApp SolidFire Active IQに転送します。

導入後のSolidFireシステムのオプションの設定

SolidFireシステムをセットアップしたら、いくつかのオプションのタスクを実行できます。また、複数要素認証、外部キー管理、連邦情報処理標準（ FIPS ）セキュリティの設定を行うこともできます。

関連概念

マルチファクタ認証のイネーブル化（52ページ）
マルチファクタ認証（ MFA ）では、 Security Assertion Markup Language （ SAML ）を介してサードパーティ ID プロバイダ（ IdP ）を使用してユーザセッションを管理します。MFA を使用すると、管理者は、パスワード、テキストメッセージ、パスワード、電子メールメッセージなど、必要に応じて認証の追加要素を設定できます。

外部キー管理の概要（74ページ）
External Key Management （ EKM ）は、 Secure Authentication Key （ AK ）管理と、 Off-Cluster External Key Server（ EK; 外部キーサーバ）を提供します。EKSを使用することで、AKの安全な生成と保管が可能になります。

関連タスク

*FIPS*ドライブをサポートするクラスタの作成（69ページ）
お客様の環境へソリューションを導入するにあたり、セキュリティの重要性はますます高まっています。Federal Information Processing Standard（FIPS;連邦情報処理標準）は、コンピュータのセキュリティと相互運用性に関する標準です。FIPS 140-2認定の保存データの暗号化は、全体的なセキュリティ ソリューションに欠かせない要素です。

Elementソフトウェアのデフォルトの SSL証明書の変更

NetApp Element APIを使用して、クラスタ内のストレージ ノードのデフォルトSSLの証明書と秘密鍵を変更できます。

NetApp Elementソフトウェア クラスタを作成すると、一意の自己署名Secure Sockets Layer（SSL）証明書と、Element UI、ノードUI、またはノードAPIを経由するすべてのHTTPS通信に使用される秘密鍵が作成されます。Elementソフトウェアは、自己署名証明書に加えて、信頼できる認証局（CA）が発行して検証する証明書をサポートします。

次のAPIメソッドを使用して、デフォルトのSSL証明書に関する詳細情報を確認し、変更を加えることができます。各メソッドについては、*NetApp Element*ソフトウェア*API*リファレンス ガイドを参照してください。

GetSSLCertificate

現在インストールされているSSL証明書に関する情報（証明書のすべての詳細情報を含む）を取得できます。

SetSSLCertificate

クラスタおよび各ノードに独自のSSL証明書と秘密鍵を設定できます。この証明書と秘密鍵はシステムで検証されるため、無効な証明書が適用されることはありません。

RemoveSSLCertificate

現在インストールされているSSL証明書と秘密鍵を削除できます。削除後は、クラスタで新しい自己署名証明書と秘密鍵が生成されます。

注 : クラスタのSSL証明書は、クラスタに追加される新しいノードに自動的に適用されます。クラスタから削除したノードの証明書は自己署名証明書に戻され、ユーザが定義した証明書と秘密鍵の情報はすべてノードから削除されます。

関連概念

管理ノードの使用（191ページ）

管理ノード（mNode）は、システム サービスのアップグレード、クラスタのアセットと設定の管理、システムのテストとユーティリティの実行、Active IQへの接続（システム監視）、ネットアップ サポートへのアクセス許可（トラブルシューティング）に使用します。

関連情報

*Element API*を使用したストレージの管理

ストレージ ノードのアップグレード

HealthTools スイートを使用して、クラスタのストレージノード上のエレメントソフトウェアをアップグレードできます。HealthTools は、接続されたサイトまたはダークサイトから使用できます。最新の HealthTools を使用するには、管理ノード 11.0 、 11.1 、またはそれ以降を使用する必要があります。

エンドツーエンドのシステムアップグレードの一環としてエレメントストレージを更新するには、システムのアップグレード手順に従ってください。 *NetApp* のマニュアル：「アップグレードの概要」を参照してください

重要： H610S シリーズノードを Element 12.0 以降にアップグレードする場合は、各ノードのストレージアップグレードを完了するために追加の手順が必要です。H610S の手順については、次のトピックを参照してください。 *NetApp* のマニュアル： *Upgrade Element Storage*

Elementストレージベースインストールの管理サービスの更新

管理ノード 11.3 のリリース時点では、管理ノードはマイクロサービスホストとして機能するため、NetApp HCI および SolidFire オールフラッシュストレージのメジャーリリース以外では、選択したソフトウェアサービスを迅速に更新できます。これらのマイクロサービスまたは管理サービスは、オンライン ソフトウェア リポジトリでサービス バンドルとして随時更新されます。Hybrid Cloud Controlを使用して、管理サービスを最新バージョンに更新できます。また、管理ノードから実行可能な管理サービスREST APIを使用して最新の状態に保つことができます。

エンドツーエンドのエレメントストレージシステムアップグレードの一環として管理サービスを更新するには、 *NetApp* のマニュアル：アップグレードの概要を参照してください

主要なストレージリリース以外の管理サービスを更新するには、 *NetApp* のドキュメント『 *Update Management Services* 』を参照してください

Elementソフトウェアの基本オプションの使用

NetApp ElementソフトウェアWebユーザ インターフェイス（Element UI）を使用して、SolidFireシステムの一般的なタスクを監視および実行することができます。

タスク概要

フィルタを使用した情報検索、リストのソート、UI操作によって実行されたAPIコマンドの表示、およびフィードバックの送信が可能です。

関連タスク

フィルタを使用した結果の絞り込み（43ページ）
Element UIの各ページでは、リスト情報をフィルタリングできます。リスト（ボリュームやSnapshotなど）を表示する際に、フィルタを1つ以上追加することで情報が絞り込まれて簡単にページに収まるようになります。

*API*アクティビティの表示（43ページ）
Elementシステムの各種機能は、NetApp Element APIをその基盤として使用します。Element UIでは、画面での操作に連動して、システム上のさまざまな種類のAPIアクティビティをリアルタイムで確認できます。APIログでは、ユーザが開始したバックグラウンドのシステムAPIアクティビティと、現在表示しているページ上で実行したAPI呼び出しを確認できます。

リストの並べ替え（43ページ）
Element UIの一部のページでは、リストの情報を1つ以上の基準でソートできます。これにより、画面に表示される情報を並べ替えることができます。

フィードバック（45ページ）
Elementソフトウェアの Webユーザ インターフェイス（UI）からフィードバック フォームにアクセスして、UIの改善案や問題点を報告することができます。

関連資料

*Element*インターフェイスのアイコン（44ページ）
NetApp Elementソフトウェアのインターフェイスには、システム リソースに対して実行できる操作を表すアイコンが表示されます。

Elementソフトウェア ユーザ インターフェイスへのアクセス

Element UIには、プライマリ クラスタ ノードの管理仮想IP（MVIP）アドレスを使用してアクセスできます。

開始する前に

ブラウザでポップアップ ブロックとNoScriptの設定が無効になっていることを確認する必要があります。

タスク概要

クラスタ作成時の設定に応じて、IPv4またはIPv6アドレスを使用してUIにアクセスできます。

手順

1. 次のいずれかを選択します。
   - IPv6：「`https://[IPv6 MVIP address]`」を入力します。次に例を示します。

     ```
     https://[fd20:8b1e:b256:45a::1234]/
     ```
   - IPv4：「`https://<IPv4 MVIP address>`」を入力します。次に例を示します。

```
https://10.123.456.789/
```

2. DNSのホスト名を入力します。
3. 認証証明書のメッセージが表示されたら該当するボタンをクリックして確認します。

フィルタを使用した結果の絞り込み

Element UIの各ページでは、リスト情報をフィルタリングできます。リスト（ボリュームやSnapshotなど）を表示する際に、フィルタを1つ以上追加することで情報が絞り込まれて簡単にページに収まるようになります。

手順

1. リスト情報を表示した状態で、**[Filter]**をクリックします。
2. **[Filter By]**フィールドを展開します。
3. フィールドの左端の要素から、フィルタの基準とする列を選択します。
4. 列の制約を選択します。
5. フィルタの基準とするテキストを入力します。
6. **[Add]**をクリックします。
   リスト内の情報に対して新しいフィルタが実行され、新しいフィルタが[Filter By]フィールドに一時的に保存されます。
7. オプション: 別のフィルタを追加するには、**[Add]**をクリックしてもう一度フィルタを選択します。
8. オプション: **[Clear All]**をクリックしてフィルタのリストを削除し、フィルタなしのリスト情報を表示します。

リストの並べ替え

Element UIの一部のページでは、リストの情報を1つ以上の基準でソートできます。これにより、画面に表示される情報を並べ替えることができます。

手順

1. 1つの列でソートするには、列見出しをクリックします。
2. 複数の列を使用してソートするには、ソートの基準とする各列の列見出しをクリックします。

   複数の列を使用してソートすると、[Sort]ボタンが表示されます。
3. ソート基準の順序を変更するには、次の手順を実行します。
   1. **[Sort]**をクリックします。
      [Sort By]フィールドに、選択した列が表示されます。
   2. [Sort By]フィールドで、希望するソート順になるように列を並べ替えます。
      リスト情報がソートされます。
4. ソート基準を削除するには、ソート基準の名前の横にある**[Remove]**アイコンをクリックします。
5. オプション: すべてのソート基準を削除するには、**[Clear All]**をクリックします。

APIアクティビティの表示

Elementシステムの各種機能は、NetApp Element APIをその基盤として使用します。Element UIでは、画面での操作に連動して、システム上のさまざまな種類のAPIアクティビティをリアルタイムで確認できます。APIログでは、ユーザが開始したバックグラウンドのシステムAPIアクティビティと、現在表示しているページ上で実行したAPI呼び出しを確認できます。

タスク概要

APIログを使用すると、特定のタスクにどのAPIメソッドが使用されるかを特定し、APIのメソッドおよびオブジェクトを使用してカスタム アプリケーションを構築する方法を確認できます。各メソッドについては、*NetApp Element*ソフトウェア*API*リファレンス ガイドを参照してください。

手順

1. Element UIナビゲーション バーから、**[API Log]**をクリックします。
2. **[API Log]**ウィンドウに表示されるAPIアクティビティの種類を変更するには、次の手順を実行します。
   1. API要求トラフィックを表示する場合は、**[Requests]**を選択します。
   2. API応答トラフィックを表示する場合は、**[Responses]**を選択します。
   3. APIトラフィックのタイプをフィルタリングする場合は、次のいずれかを選択します。
      - **User Initiated**：このWeb UIセッション中のユーザのアクティビティによるAPIトラフィック。
      - **Background Polling**：バックグラウンド システム アクティビティによって生成されるAPIトラフィック。
      - **Current Page**：現在表示しているページ上のタスクによって生成されるAPIトラフィック。

関連情報

*Element API*を使用したストレージの管理

インターフェイス更新間隔へのクラスタ負荷の影響

APIの応答時間によっては、表示しているNetApp Elementソフトウェアのページの一部に関してクラスタがデータの更新間隔を自動的に調整することがあります。

ブラウザでページをリロードすると、更新間隔はデフォルトにリセットされます。ページの右上のクラスタ名をクリックすると、現在の更新間隔を確認できます。この間隔は、データがサーバから返される速さではなく、API要求の実行間隔です。

クラスタの負荷が高い場合は、Element UIからのAPI要求がキューに登録されることがあります。ごくまれに、ネットワーク接続が低速でクラスタがビジーな場合など、システム応答が大幅に遅延し、キューに登録されているAPI要求に対するシステムの応答に時間がかかる場合、Element UIからログアウトされることがあります。ログアウト画面にリダイレクトされた場合は、最初のブラウザ認証画面を無視すれば再度ログインできます。概要ページに戻ると、クラスタ クレデンシャルがブラウザで保存されていない場合はクレデンシャルの入力を求められることがあります。

Elementインターフェイスのアイコン

NetApp Elementソフトウェアのインターフェイスには、システム リソースに対して実行できる操作を表すアイコンが表示されます。

次の表に概要を示します。

アイコン	説明
	操作
	バックアップ先
	クローンまたはコピー

アイコン	説明
	削除またはパージ
	編集
	フィルタ
	ペア
	リフレッシュ
	リストア
	リストア元
	ロールバック
	Snapshot

フィードバック

Elementソフトウェアの Webユーザ インターフェイス（UI）からフィードバック フォームにアクセスして、UIの改善案や問題点を報告することができます。

手順

1. Element UIの任意のページで、**[Feedback]**ボタンをクリックします。
2. [Summary]フィールドと[Description]フィールドに関連する情報を入力します。
3. スクリーンショットがあれば添付します。
4. 名前とEメール アドレスを入力します。
5. 現在の環境に関するデータを含めるには、対応するチェック ボックスをオンにします。
6. **[Submit]**をクリックします。

システム管理

システムはElement UIで管理できます。たとえば、クラスタ管理者の作成と管理、クラスタ設定の管理、ソフトウェアのアップグレードなどを実行できます。

関連概念

クラスタ管理者ユーザ アカウントの管理（46ページ）
SolidFireストレージ システムのクラスタ管理者アカウントを管理できます。実行できる処理は、クラスタ管理者アカウントの作成 / 削除 / 編集、クラスタ管理者パスワードの変更、ユーザのシステム アクセスを管理するためのLDAPの設定です。

クラスタの設定（54ページ）
Element UIの[Cluster]タブでは、クラスタ全体の設定を表示および変更できるほか、クラスタ固有のタスクを実行できます。

クラスタ管理者ユーザ アカウントの管理

SolidFireストレージ システムのクラスタ管理者アカウントを管理できます。実行できる処理は、クラスタ管理者アカウントの作成 / 削除 / 編集、クラスタ管理者パスワードの変更、ユーザのシステム アクセスを管理するためのLDAPの設定です。

関連概念

ストレージ クラスタ管理者アカウントのタイプ（47ページ）
NetApp Elementソフトウェアを実行するストレージ クラスタには、2つのタイプの管理者アカウント（プライマリ クラスタ管理者アカウントとクラスタ管理者アカウント）があります。

関連タスク

クラスタ管理者アカウントの作成（48ページ）
新しいクラスタ管理者アカウントを作成し、ストレージ システムの特定の領域へのアクセスを許可または制限する権限を付与できます。クラスタ管理者アカウントの権限を設定すると、割り当てていない権限については読み取り専用権限が付与されます。

クラスタ管理者の権限の編集（49ページ）
レポート作成、ノード、ドライブ、ボリューム、アカウント、およびクラスタレベルのアクセス用のクラスタ管理者アカウントの権限を変更できます。権限を有効にすると、そのレベルの書き込みアクセスが割り当てられます。選択しなかったレベルについては、読み取り専用アクセスが付与されます。

クラスタ管理者アカウントのパスワードの変更（49ページ）
Element UIを使用してクラスタ管理者のパスワードを変更できます。

*LDAP*の設定（50ページ）
ストレージ システムと既存のLDAPサーバとの統合を設定できます。これにより、LDAP管理者はストレージ システムへのユーザ アクセスを一元管理できます。

*LDAP*の無効化（52ページ）
Element UIを使用して、LDAPとの統合を無効にすることができます。

関連資料

クラスタ管理者の詳細（47ページ）

[Users]タブの[Cluster Admins]ページでは、次の情報を確認できます。

ストレージ クラスタ管理者アカウントのタイプ

NetApp Elementソフトウェアを実行するストレージ クラスタには、2つのタイプの管理者アカウント（プライマリ クラスタ管理者アカウントとクラスタ管理者アカウント）があります。

プライマリ クラスタ管理者アカウント

この管理者アカウントは、クラスタ作成時に作成されます。クラスタへの最高レベルのアクセス権を持つプライマリの管理アカウントです。このアカウントは、Linuxシステムのrootユーザに相当します。この管理者アカウントのパスワードは変更可能です。

クラスタ管理者アカウント

クラスタ管理者アカウントには、クラスタ内で特定のタスクを実行するための限定的な管理アクセスを付与できます。各クラスタ管理者アカウントに割り当てられたクレデンシャルを使用して、ストレージ システム内でのAPIやElement UIの要求が認証されます。

注 : ノードUIからクラスタ内のアクティブ ノードにアクセスするには、ローカル（LDAP以外）のクラスタ管理者アカウントが必要です。まだクラスタに含まれていないノードにアクセスする場合、アカウントのクレデンシャルは必要ありません。

クラスタ管理者の詳細

[Users]タブの[Cluster Admins]ページでは、次の情報を確認できます。

ID

クラスタ管理者アカウントに割り当てられている連番。

Username

クラスタ管理者アカウントの作成時に指定した名前。

Access

ユーザ アカウントに割り当てられているユーザ権限。有効な値は次のとおりです。

- read
- reporting
- nodes
- drives
- volumes
- accounts
- clusterAdmins
- administrator

注 : administratorアクセス タイプには、すべての権限が割り当てられています。

Type

クラスタ管理者のタイプ。有効な値は次のとおりです。

- Cluster
- Ldap

Attributes

Element APIを使用して作成されたクラスタ管理者アカウントに対し、作成時に設定された名前と値のペアが表示されます。*NetApp Element*ソフトウェア*API*リファレンス ガイドを参照してください。

関連情報

*Element API*を使用したストレージの管理

クラスタ管理者アカウントの作成

新しいクラスタ管理者アカウントを作成し、ストレージ システムの特定の領域へのアクセスを許可または制限する権限を付与できます。クラスタ管理者アカウントの権限を設定すると、割り当てていない権限については読み取り専用権限が付与されます。

開始する前に

LDAPクラスタ管理者アカウントを作成する場合は、作成を開始する前にクラスタでLDAPが設定されていることを確認します。

タスク概要

レポート作成、ノード、ドライブ、ボリューム、アカウント、およびクラスタレベルのアクセス用のクラスタ管理者アカウントの権限をあとから変更できます。権限を有効にすると、そのレベルの書き込みアクセスが割り当てられます。選択しなかったレベルについては、読み取り専用アクセスが付与されます。

システム管理者が作成したクラスタ管理者ユーザ アカウントをあとから削除することもできます。クラスタの作成時に作成されたプライマリ クラスタ管理者アカウントを削除することはできません。

手順

1. クラスタ全体（LDAP以外）のクラスタ管理者アカウントを作成するには、次の操作を実行します。
   1. **[Users]** > **[Cluster Admins]**の順にクリックします。
   2. **[Create Cluster Admin]**をクリックします。
   3. **[Cluster]**ユーザ タイプを選択します。
   4. アカウントのユーザ名とパスワードを入力し、確認のためにパスワードをもう一度入力します。
   5. アカウントに適用するユーザ権限を選択します。
   6. エンド ユーザ ライセンス契約に同意するチェック ボックスをオンにします。
   7. **[Create Cluster Admin]**をクリックします。
2. LDAPディレクトリにクラスタ管理者アカウントを作成するには、次の操作を実行します。
   1. **[Cluster]** > **[LDAP]**の順にクリックします。
   2. LDAP認証が有効になっていることを確認します。
   3. **[Test User Authentication]**をクリックし、ユーザまたはユーザが属しているグループの識別名を、あとで貼り付けられるようにコピーします。
   4. **[Users]** > **[Cluster Admins]**の順にクリックします。
   5. **[Create Cluster Admin]**をクリックします。
   6. **[LDAP]**ユーザ タイプを選択します。
   7. [Distinguished Name]フィールドに、テキスト ボックスに表示された例に従ってユーザまたはグループの完全な識別名を入力します。または、先ほどコピーした識別名を貼り付けます。

      識別名がグループの一部である場合、LDAPサーバ上のそのグループのメンバーであるユーザには、この管理者アカウントの権限が与えられます。
   8. アカウントに適用するユーザ権限を選択します。
   9. エンド ユーザ ライセンス契約に同意するチェック ボックスをオンにします。
   10. **[Create Cluster Admin]**をクリックします。

関連タスク

*LDAP*の設定（50ページ）

ストレージ システムと既存のLDAPサーバとの統合を設定できます。これにより、LDAP管理者はストレージ システムへのユーザ アクセスを一元管理できます。

クラスタ管理者の権限の編集

レポート作成、ノード、ドライブ、ボリューム、アカウント、およびクラスタレベルのアクセス用のクラスタ管理者アカウントの権限を変更できます。権限を有効にすると、そのレベルの書き込みアクセスが割り当てられます。選択しなかったレベルについては、読み取り専用アクセスが付与されます。

手順

1. **[Users]** > **[Cluster Admins]**の順にクリックします。
2. 編集するクラスタ管理者の[Actions]アイコンをクリックします。
3. **[Edit]**をクリックします。
4. アカウントに適用するユーザ権限を選択します。
5. **[Save Changes]**をクリックします。

クラスタ管理者アカウントのパスワードの変更

Element UIを使用してクラスタ管理者のパスワードを変更できます。

タスク概要

注 : MNode REST API UI でクラスタ管理者のパスワードを変更するには、「ストレージ クラスタ管理者のパスワードの変更」を参照してください

手順

1. **Users** > **Cluster Admins**をクリックします。
2. 編集するクラスタ管理者の[Actions]アイコンをクリックします。
3. **Edit**をクリックします。
4. [Change Password]フィールドに新しいパスワードを入力し、確認のためにもう一度入力します。
5. **Save Changes**をクリックします。

関連概念

ストレージ クラスタ管理者アカウントのタイプ（47ページ）

NetApp Elementソフトウェアを実行するストレージ クラスタには、2つのタイプの管理者アカウント（プライマリ クラスタ管理者アカウントとクラスタ管理者アカウント）があります。

LDAPの管理

Lightweight Directory Access Protocol（LDAP）を設定して、SolidFireストレージへのセキュアなディレクトリベースのログイン機能を有効にすることができます。LDAPをクラスタレベルで設定し、LDAPユーザおよびグループを許可することができます。

注 : IPv4とIPv6の両方のアドレスを使用できます。

LDAPの設定

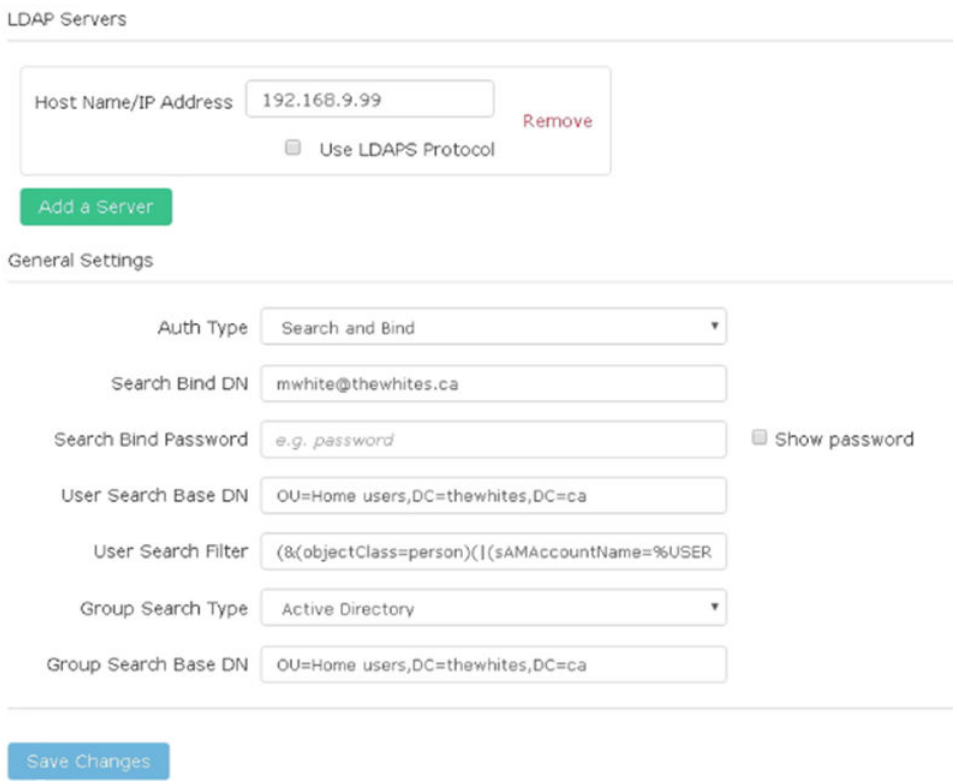
ストレージ システムと既存のLDAPサーバとの統合を設定できます。これにより、LDAP管理者はストレージ システムへのユーザ アクセスを一元管理できます。

手順

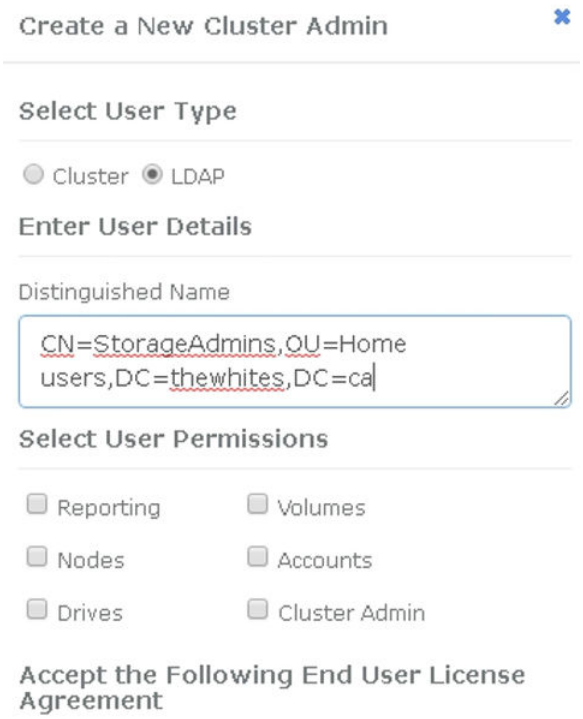
1. **Cluster** > **LDAP**をクリックします。
2. **Yes**LDAP 認証を有効にする場合にクリックします。
3. **Add a Server**をクリックします。
4. **Host Name/IP Address**を入力します。

   注 : オプションのカスタムポート番号を入力することもできます。

   たとえば、カスタムポート番号を追加するには、と入力します `<host name or ip address>:<port number>`
5. オプション: **Use LDAPS Protocol**を選択します。
6. に必要な情報を入力**General Settings**します。
   LDAPの詳細（51ページ）



7. **Enable LDAP**をクリックします。
8. **Test User Authentication**ユーザのサーバアクセスをテストする場合にクリックします。
9. あとでクラスタ管理者を作成するときに使用できるように、表示された識別名とユーザ グループの情報をコピーします。
10. オプション: クリックする**Save Changes**と、新しい設定が保存されます。
11. このグループにユーザを作成して、誰でもログインできるようにするには、次の手順を実行します。
    1. **User** > **View**をクリックします。



2. 新しいユーザ**LDAP**の場合は、ユーザタイプをクリックし、コピーしたグループを [Distinguished Name] フィールドに貼り付けます。
3. 権限（通常はすべての権限）を選択します。
4. End User License Agreement までスクロールダウンし**I accept**て、をクリックします。
5. **Create Cluster Admin**をクリックします。
   これで、 Active Directory グループの値を持つユーザが作成されました。

終了後の操作

Elementには、エレメント UI からログアウトし、そのグループのユーザーとして再度ログインします。

関連タスク

クラスタ管理者アカウントの作成（48ページ）

新しいクラスタ管理者アカウントを作成し、ストレージ システムの特定の領域へのアクセスを許可または制限する権限を付与できます。クラスタ管理者アカウントの権限を設定すると、割り当てていない権限については読み取り専用権限が付与されます。

関連資料

*LDAP*の詳細（51ページ）

LDAPCluster「」タブの「」ページには、次の設定に関する情報が表示されます。

LDAPの詳細

LDAPCluster「」タブの「」ページには、次の設定に関する情報が表示されます。

注 : LDAPの設定を確認するためには、LDAPを有効にする必要があります。

ホスト名 / IP アドレス

LDAPまたはLDAPSディレクトリ サーバのアドレス。

Auth Type

ユーザの認証方法。有効な値は次のとおりです。

- 直接バインド
- 検索とバインド

Search Bind DN

ユーザのLDAP検索を実行するためにログインで使用する完全修飾DN（LDAPディレクトリへのバインドレベルのアクセスが必要）。

Search Bind Password

LDAPサーバへのアクセスを認証するためのパスワード。

User Search Base DN

ユーザ検索を開始するツリーのベースDN。指定した場所からサブツリーが検索されます。

User Search Filter

ドメイン名を使用して次のように入力します。

```
&(objectClass=person)(|(sAMAccountName=%USERNAME%)(userPrincipalName=%USERNAME%)))
```

Group Search Type

検索のタイプ。タイプに応じてデフォルトのグループ検索フィルタが決まります。有効な値は次のとおりです。

- `Active Directory`：ユーザのすべての LDAP グループのネストされたメンバーシップ。
- グループなし：グループはサポートされません。
- メンバー `DN` ：メンバー DN スタイルグループ（単一レベル）。

Group Search Base DN

グループ検索を開始するツリーのベースDN。指定した場所からサブツリーが検索されます。

Test User Authentication

LDAPの設定後に、LDAPサーバのユーザ名とパスワードによる認証をテストする場合に使用します。すでに存在するアカウントを入力してテストしてください。識別名とユーザ グループの情報が表示されます。この情報をコピーして、あとでクラスタ管理者を作成する際に使用できます。

LDAPの無効化

Element UIを使用して、LDAPとの統合を無効にすることができます。

開始する前に

LDAPを無効にすると設定がすべて消去されるため、すべての設定をメモしておきます。

手順

1. **[Cluster]** > **[LDAP]**の順にクリックします。
2. **[No]**をクリックします。
3. **[Disable LDAP]**をクリックします。

マルチファクタ認証のイネーブル化

マルチファクタ認証（ MFA ）では、 Security Assertion Markup Language （ SAML ）を介してサードパーティ ID プロバイダ（ IdP ）を使用してユーザセッションを管理します。MFA を使用すると、管理者は、パスワード、テキストメッセージ、パスワード、電子メールメッセージなど、必要に応じて認証の追加要素を設定できます。

マルチファクタ認証の設定

エレメント API を使用してこれらの基本的な手順を実行すると、マルチファクタ認証を使用するようにクラスタを設定できます。各APIメソッドの詳細については、『NetApp Element APIリファレンス ガイド』を参照してください。

手順

1. 次の API メソッドを呼び出し、 IdP メタデータを JSON 形式で渡して、クラスタの新しいサードパーティ ID プロバイダ（ IdP ）設定を作成します。

   `CreateIdpConfiguration`

   IdP メタデータは、プレーンテキスト形式で、サードパーティの IdP から取得されます。このメタデータは、 JSON 形式で正しくフォーマットされるように検証する必要があります。使用できる JSON フォーマッタアプリケーションは多数あります。たとえば、次のようになります。
2. 次の API メソッドを呼び出して、 spMetadataURL を使用してクラスタメタデータを取得し、サードパーティの IdP にコピーします。

   `ListIdpConfigurations`

   spMetadataURL は、信頼関係を確立するために、 IdP のクラスタからサービスプロバイダーメタデータを取得するために使用される URL です。
3. サードパーティの IdP で SAML アサーションを設定して、監査ログ用のユーザを一意に識別し、単一のログアウトが正しく機能するように「 nameID 」属性を含めます。
4. 次の API メソッドを呼び出して、サードパーティ製の IdP で認証された 1 つ以上のクラスタ管理者ユーザアカウントを作成し、認可を受けます。

   `AddIdpClusterAdmin`

   注 : IdP クラスタ管理者のユーザ名は、次の例に示すように、目的の効果の SAML 属性名 / 値マッピングと一致する必要があります。

   - email=bob@company.com ： SAML 属性の電子メールアドレスを解放するように IdP を設定します。
   - group=cluster-administrator ：すべてのユーザがアクセスできるグループプロパティを解放するように IdP を設定します。

   SAML 属性名と値のペアは、セキュリティ上の理由から大文字と小文字が区別されることにも注意してください。
5. 次の API メソッドを呼び出して、クラスタの MFA を有効にします。

   `EnableIdpAuthentication`

マルチファクタ認証の追加情報

マルチファクタ認証に関する次の注意事項に注意してください。

- 有効ではなくなった IdP 証明書を更新するには、非 IdP 管理者ユーザを使用して次の API メソッドを呼び出す必要があります。

  `UpdateIdpConfiguration`
- MFA は、長さが 2048 ビット未満の証明書と互換性がありません。デフォルトでは、クラスタに 2048 ビットの SSL 証明書が作成されます。API メソッドを呼び出すときは、小さいサイズの証明書を設定しないでください。

  `SetSSLCertificate`

注 : アップグレード前の 2048 ビット未満の証明書をクラスタで使用している場合は、 Element 12.0 以降にアップグレードした後に、クラスタ証明書を 2048 ビット以上の証明書で更新する必要があります。

- IdP 管理者ユーザは、 API コールを直接（たとえば、 SDK や Postman を介して）発信したり、他の統合（ OpenStack Cinder や vCenter プラグインなど）に使用したりすることはできません。これらの機能を持つユーザを作成する必要がある場合は、 LDAP クラスタ管理ユーザまたはローカルクラスタ管理ユーザのいずれかを追加します。

関連情報

*Element API*を使用したストレージの管理

クラスタの設定

Element UIの[Cluster]タブでは、クラスタ全体の設定を表示および変更できるほか、クラスタ固有のタスクを実行できます。

設定可能な項目は、クラスタ フルしきい値、サポート アクセス、保存データの暗号化、仮想ボリューム、SnapMirror、NTPブロードキャスト クライアントなどです。

関連概念

仮想ボリュームの使用（93ページ）
Element UIを使用して、仮想ボリュームおよび仮想ボリュームに関連付けられたストレージ コンテナ、プロトコル エンドポイント、バインド、およびホストの情報を確認し、タスクを実行できます。

利用条件バナーの管理（56ページ）
ユーザ向けのメッセージを含むバナーを設定できます。

*SNMP*の管理（58ページ）
クラスタに簡易ネットワーク管理プロトコル（SNMP）を設定できます。

ドライブの管理（60ページ）
各ノードには1つ以上の物理ドライブが搭載され、クラスタのデータの一部が格納されます。クラスタにドライブが追加されると、そのドライブの容量とパフォーマンスがクラスタで使用されるようになります。Element UIを使用してドライブを管理できます。

ノードの管理（61ページ）
SolidFire ストレージノードNodesClusterとファイバチャネルノードは、タブのページから管理できます。

仮想ネットワークの管理（65ページ）
SolidFireストレージの仮想ネットワークを使用すると、別々の論理ネットワークに属する複数のクライアント間のトラフィックを1つのクラスタに接続できます。クラスタへの各接続は、VLANタギングを使用してネットワーク スタック内で分離されます。

関連タスク

*Element*クラスタと*ONTAP*クラスタ間での*SnapMirror*レプリケーション（141ページ）
NetApp Element UIの[Data Protection]タブで、SnapMirror関係を作成することができます。この情報をユーザ インターフェイスで確認するには、SnapMirror機能を有効にする必要があります。

クラスタ フルしきい値の設定（55ページ）
ブロッククラスタのフルネス警告が生成されるレベルは、次の手順で変更できます。`ModifyClusterFullThreshold`さらに、 API メソッドを使用して、ブロックまたはメタデータの警告を生成するレベルを変更できます。

サポート アクセスの有効化と無効化（55ページ）

サポート アクセスを有効にすると、ネットアップ サポートの担当者がトラブルシューティングのために一時的にSSH経由でストレージ ノードにアクセスできるようになります。

クラスタでの暗号化の有効化と無効化（56ページ）
保存データの暗号化をクラスタ全体で有効または無効にすることができます。この機能は、デフォルトでは有効になっていません。

ブロードキャスト クライアントの有効化（57ページ）
ブロードキャスト クライアントの設定を使用して、クラスタ内の各ノードがネットワーク タイム プロトコル（NTP）サーバで更新を照会するのではなくNTPブロードキャストをリスンするように設定できます。

*Fibre Channel*ポートの詳細の表示（65ページ）
[FC Ports]ページで、Fibre Channelポートの詳細（ステータス、名前、ポート アドレスなど）を確認できます。

関連情報

How to calculate SolidFire system error alert percentage

クラスタ フルしきい値の設定

ブロッククラスタのフルネス警告が生成されるレベルは、次の手順で変更できます。`ModifyClusterFullThreshold`さらに、 API メソッドを使用して、ブロックまたはメタデータの警告を生成するレベルを変更できます。

開始する前に

クラスタ管理者の権限が必要です。

手順

1. **Cluster** > **Settings**をクリックします。
2. [Cluster Full Settings] セクション**Raise a warning alert when _% capacity remains before Helix could not recover from a node failure**に、のパーセンテージを入力します。
3. **Save Changes**をクリックします。

関連情報

How to calculate SolidFire system error alert percentage

サポート アクセスの有効化と無効化

サポート アクセスを有効にすると、ネットアップ サポートの担当者がトラブルシューティングのために一時的にSSH経由でストレージ ノードにアクセスできるようになります。

開始する前に

サポート アクセスを変更するには、クラスタ管理者の権限が必要です。

手順

1. **[Cluster]** > **[Settings]**の順にクリックします。
2. [Enable / Disable Support Access]セクションで、サポートにアクセスを許可する期間（時間）を入力します。
3. **[Enable Support Access]**をクリックします。
4. オプション: サポート アクセスを無効にするには、**[Disable Support Access]**をクリックします。

クラスタでの暗号化の有効化と無効化

保存データの暗号化をクラスタ全体で有効または無効にすることができます。この機能は、デフォルトでは有効になっていません。

開始する前に

- 暗号化の設定を変更するには、クラスタ管理者の権限が必要です。
- 暗号化の設定を変更する前に、クラスタが正常な状態であることを確認します。

ヒント : ローカルのNTPサーバを参照するようにクラスタのNTPを設定してください。DNSホスト名ではなくIPアドレスを使用する必要があります。クラスタの作成時に設定されるデフォルトのNTPサーバはus.pool.ntp.orgです。ただしSolidFireクラスタの物理的な場所によっては、このサイトへの接続を確立できないこともあります。

手順

1. **[Cluster]** > **[Settings]**の順にクリックします。
2. **[Enable Encryption at Rest]**をクリックします。
3. オプション: 保存データの暗号化を無効にするには、**[Disable Encryption at Rest]**をクリックします。

関連概念

保存データの暗号化（56ページ）

SolidFireクラスタでは、クラスタに保管されているすべてのデータを暗号化できます。

保存データの暗号化

SolidFireクラスタでは、クラスタに保管されているすべてのデータを暗号化できます。

ストレージ ノード内の暗号化に対応したドライブはいずれも、ドライブ レベルのAES 256ビット暗号化を利用します。各ドライブには、ドライブが最初に初期化された際に作成される、専用の暗号化キーがあります。暗号化機能を有効にすると、クラスタ全体のパスワードが作成され、チャンクに分割されてクラスタ内のすべてのノードに配信されます。いずれか1つのノードにパスワード全体が格納されることはありません。このパスワードを使用して、ドライブへのすべてのアクセスが保護されます。ドライブのロックを解除するにはパスワードが必要で、その後、ドライブの電源がオフになるかドライブがロックされるまでは必要ありません。

保存データの暗号化機能を有効にしても、クラスタのパフォーマンスや処理効率には影響しません。また、暗号化が有効なドライブやノードをElement APIまたはElement UIでクラスタから削除すると、保存データの暗号化がドライブで無効になります。削除したドライブは、`SecureEraseDrives` APIメソッドを使用して安全に消去できます。ドライブやノードがクラスタから強制的に削除された場合も、データはクラスタ全体のパスワードおよび各ドライブ専用の暗号化キーで引き続き保護されます。

利用条件バナーの管理

ユーザ向けのメッセージを含むバナーを設定できます。

利用条件の有効化

ユーザがElement UIにログインしたときに表示される利用条件のバナーを有効にすることができます。ユーザがバナーをクリックすると、クラスタに対して設定したメッセージを含むテキスト ダイアログ ボックスが表示されます。バナーはいつでも無効にすることができます。

開始する前に

利用条件機能を有効にするには、クラスタ管理者の権限が必要です。

手順

1. **[Users]** > **[Terms of Use]**の順にクリックします。
2. **[Terms of Use]**フォームで、[Terms of Use]ダイアログ ボックスに表示するテキストを入力します。

   注 : 最大文字数は4096文字です。
3. **[Enable]**をクリックします。

利用条件の編集

ユーザが利用条件のログイン バナーを選択したときに表示されるテキストを編集できます。

開始する前に

- 利用条件を設定するには、クラスタ管理者の権限が必要です。
- 利用条件機能が有効になっていることを確認します。

手順

1. **[Users]** > **[Terms of Use]**の順にクリックします。
2. **[Terms of Use]**ダイアログ ボックスで、表示するテキストを編集します。

   注 : 最大文字数は4096文字です。
3. **[Save Changes]**をクリックします。

利用条件の無効化

利用条件のバナーを無効にできます。バナーを無効にすると、ユーザがElement UIを使用する際に利用条件の同意を求められなくなります。

開始する前に

- 利用条件を設定するには、クラスタ管理者の権限が必要です。
- 利用条件が有効になっていることを確認します。

手順

1. **[Users]** > **[Terms of Use]**の順にクリックします。
2. **[Disable]**をクリックします。

ブロードキャスト クライアントの有効化

ブロードキャスト クライアントの設定を使用して、クラスタ内の各ノードがネットワーク タイム プロトコル（NTP）サーバで更新を照会するのではなくNTPブロードキャストをリスンするように設定できます。

開始する前に

- この設定には、クラスタ管理者の権限が必要です。
- ネットワーク上のNTPサーバをブロードキャスト サーバとして設定する必要があります。

タスク概要

NTPは、ネットワークを介してクロックを同期するために使用します。内部または外部のNTPサーバへの接続は、クラスタの初期セットアップ時に行う必要があります。

NTPサーバは最大5つまで入力できます。

注 : IPv4とIPv6の両方のアドレスを使用できます。

手順

1. **[Cluster]** > **[Settings]**の順にクリックします。
2. [Network Time Protocol Settings]で、**[Yes]**を選択してブロードキャスト クライアントとして使用します。
3. **[Server]**フィールドに、ブロードキャスト モードで設定したNTPサーバを入力します。
4. **[Save Changes]**をクリックします。

SNMPの管理

クラスタに簡易ネットワーク管理プロトコル（SNMP）を設定できます。

SNMPリクエスタの選択、使用するSNMPのバージョンの選択、SNMP User-based Security Model（USM;ユーザベースのセキュリティ モデル）ユーザの識別、SolidFireクラスタを監視するためのトラップの設定を行うことができます。管理情報ベース（MIB）ファイルを表示し、アクセスすることもできます。

注 : IPv4とIPv6の両方のアドレスを使用できます。

SNMPの詳細

[Cluster]タブの[SNMP]ページでは、次の情報を確認できます。

SNMP MIBs

表示またはダウンロード可能なMIBファイル。

General SNMP Settings

SNMPを有効または無効にすることができます。SNMPを有効にしたら、使用するバージョンを選択できます。バージョン2を使用する場合はリクエスタを追加できます。バージョン3を使用する場合はUSMユーザをセットアップできます。

SNMP Trap Settings

取得するトラップを指定できます。トラップ受信者ごとにホスト、ポート、およびコミュニティ ストリングを設定できます。

SNMPリクエスタの設定

SNMPバージョン2が有効な場合は、リクエスタを有効または無効にできるほか、許可されたSNMP要求を受信するリクエスタを設定できます。

手順

1. **[Cluster]** > **[SNMP]**の順にクリックします。
2. **[General SNMP Settings]**で、**[Yes]**をクリックしてSNMPを有効にします。
3. **[Version]**リストで、**[Version 2]**を選択します。
4. **[Requestors]**セクションの**[Community String]**と**[Network]**に、コミュニティ ストリングとネットワークを入力します。

   注 : デフォルトでは、コミュニティ ストリングはpublicに、ネットワークはlocalhostに設定されます。これらのデフォルト設定は変更可能です。
5. オプション: 別のリクエスタを追加するには、**[Add a Requestor]**をクリックし、**[Community String]**と**[Network]**に情報を入力します。
6. **[Save Changes]**をクリックします。

関連タスク

*SNMP*トラップの設定（59ページ）

システム管理者は、SNMPトラップ（通知とも呼ばれます）を使用してSolidFireクラスタの健全性を監視できます。

管理情報ベース ファイルを使用した管理対象オブジェクト データの表示（59ページ）
個々の管理対象オブジェクトの定義に使用されている管理情報ベース（MIB）ファイルを表示およびダウンロードできます。SNMP機能では、SolidFire-StorageCluster-MIBで定義されているオブジェクトへの読み取り専用アクセスがサポートされます。

SNMP USMユーザの設定

SNMPバージョン3を有効にした場合は、許可されたSNMP要求を受信するUSMユーザを設定する必要があります。

手順

1. **[Cluster]** > **[SNMP]**の順にクリックします。
2. **[General SNMP Settings]**で、**[Yes]**をクリックしてSNMPを有効にします。
3. **[Version]**リストで、**[Version 3]**を選択します。
4. **[USM Users]**セクションで、名前、パスワード、およびパスフレーズを入力します。
5. オプション: 別のUSMユーザを追加するには、**[Add a USM User]**をクリックして、名前、パスワード、およびパスフレーズを入力します。
6. **[Save Changes]**をクリックします。

SNMPトラップの設定

システム管理者は、SNMPトラップ（通知とも呼ばれます）を使用してSolidFireクラスタの健全性を監視できます。

タスク概要

SNMPトラップが有効になっている場合は、SolidFireクラスタでイベント ログ エントリとシステム アラートに関連するトラップが生成されます。SNMP通知を受信するには、生成するトラップを選択し、トラップ情報の受信者を指定する必要があります。デフォルトでは、トラップは生成されません。

手順

1. **[Cluster]** > **[SNMP]**をクリックします。
2. **[SNMP Trap Settings]**セクションで生成する必要があるトラップの種類を選択します。
   - Cluster Fault Traps
   - Cluster Resolved Fault Traps
   - Cluster Event Traps
3. **[Trap Recipients]**セクションに、受信者のホスト、ポート、コミュニティ ストリングの情報を入力します。
4. オプション: 別のトラップ受信者を追加するには、**[Add a Trap Recipient]**をクリックして、ホスト、ポート、コミュニティ ストリングの情報を入力します。
5. **[Save Changes]**をクリックします。

管理情報ベース ファイルを使用した管理対象オブジェクト データの表示

個々の管理対象オブジェクトの定義に使用されている管理情報ベース（MIB）ファイルを表示およびダウンロードできます。SNMP機能では、SolidFire-StorageCluster-MIBで定義されているオブジェクトへの読み取り専用アクセスがサポートされます。

タスク概要

MIBには、以下のオブジェクトについて、システム アクティビティの統計情報が保存されています。

- クラスタの統計
- ボリュームの統計
- アカウント別ボリュームの統計
- ノードの統計
- その他のデータ（レポート、エラー、システム イベントなど）

また、SFシリーズ製品への上位のアクセス ポイント（OID）を含んでいるMIBファイルへのアクセスもサポートされます。

手順

1. **[Cluster]** > **[SNMP]**の順にクリックします。
2. **[SNMP MIBs]**で、ダウンロードするMIBファイルをクリックします。
3. 表示されたダウンロード ウィンドウで、MIBファイルを開くか、または保存します。

ドライブの管理

各ノードには1つ以上の物理ドライブが搭載され、クラスタのデータの一部が格納されます。クラスタにドライブが追加されると、そのドライブの容量とパフォーマンスがクラスタで使用されるようになります。Element UIを使用してドライブを管理できます。

関連タスク

クラスタへのドライブの追加（26ページ）

クラスタにノードを追加したり、既存のノードに新しいドライブを設置すると、ドライブが自動的に使用可能ドライブとして登録されます。ドライブがクラスタに参加できるようにするためには、Element UIまたはAPIを使用してドライブをクラスタに追加する必要があります。

ドライブの詳細

[Cluster]タブの[Drives]ページには、クラスタ内のアクティブ ドライブのリストが表示されます。このページは、[Active]、[Available]、[Removing]、[Erasing]、[Failed]の各タブに分かれています。

クラスタを最初に初期化した時点では、アクティブ ドライブのリストは空です。新しいSolidFireクラスタが作成されたら、[Available]タブに表示されている、クラスタに割り当てられていないドライブを追加できます。

アクティブ ドライブのリストに表示される項目は次のとおりです。

Drive ID
ドライブに割り当てられている連番。

Node ID
クラスタへの追加時にノードに割り当てられたノード番号。

Node Name
ドライブが格納されているノードの名前。

Slot
ドライブが物理的に配置されているスロットの番号。

Capacity
ドライブのサイズ（GB）。

Serial
ドライブのシリアル番号。

Wear Remaining
摩耗レベル インジケータ。

ストレージ システムからは、各ソリッドステート ドライブ（SSD）でデータの書き込み / 消去に利用できるおおよその残容量が報告されます。ドライブの設計上の書き込み / 消去サイクルの5%が消費されている場合は、摩耗度残量が95%と報告されます。ドライブの摩耗度情報は自動では更新されません。情報を更新するには、ページを更新するか、またはページを開きなおします。

Type

ドライブのタイプ。blockまたはmetadataのいずれかです。

ノードの管理

SolidFire ストレージノードNodesClusterとファイバチャネルノードは、タブのページから管理できます。

新しく追加されたノードがクラスタ全体の容量の 50% を超える場合、このノードの容量の一部が使用できなくなり（「孤立」）、容量ルールに準拠します。これは、ストレージを追加するまでの間は変わりません。容量ルールに違反する非常に大きなノードが追加されると、以前に孤立したノードは孤立しなくなり、新しく追加されたノードは孤立状態になります。この問題を回避するには、容量を必ずペアで追加する必要があります。ノードが孤立した場合は、適切なクラスタ障害がスローされます。

関連タスク

クラスタへのノードの追加（61ページ）

ストレージの追加が必要になったとき、またはクラスタ作成後に、クラスタにノードを追加できます。ノードは、初回の電源投入時に初期設定を行う必要があります。設定が完了したノードは、保留状態のノードのリストに表示され、クラスタに追加できるようになります。

関連資料

ノードの状態（24ページ）

設定のレベルによって、ノードは次のいずれかの状態になります。

クラスタへのノードの追加

ストレージの追加が必要になったとき、またはクラスタ作成後に、クラスタにノードを追加できます。ノードは、初回の電源投入時に初期設定を行う必要があります。設定が完了したノードは、保留状態のノードのリストに表示され、クラスタに追加できるようになります。

タスク概要

クラスタ内の各ノードは、互換性のあるソフトウェア バージョンを実行している必要があります。クラスタにノードを追加すると、必要に応じて新しいノードにElementソフトウェアのクラスタ バージョンがインストールされます。

既存のクラスタには、大小さまざまな容量のノードを追加できます。クラスタの容量を拡大するには、大容量のノードを追加します。小容量のノードで構成されるクラスタに大容量のノードを追加するときは、ペアにして追加する必要があります。これにより、一方の大容量ノードで障害が発生しても、Double Helixでデータを移動する十分なスペースが確保されます。大容量ノード クラスタのパフォーマンスを向上させるには、小容量ノードを追加します。

注 : 新しく追加されたノードがクラスタ全体の容量の 50% を超える場合、このノードの容量の一部が使用できなくなり（「孤立」）、容量ルールに準拠します。これは、ストレージを追加するまでの間は変わりません。容量ルールに違反する非常に大きなノードが追加されると、以前に孤立したノードは孤立しなくなり、新しく追加されたノードは孤立状態になります。この問題を回避するには、容量を必ずペアで追加する必要があります。ノードが孤立状態になると、 StrandedCapacity クラスタ障害がスローされます。

ネットアップのビデオ: *Scale on Your Terms: Expanding a SolidFire Cluster*

手順

1. **Cluster** > **Nodes**の順に選択します。
2. **Pending**クリックすると、保留中のノードのリストが表示されます。
3. 次のいずれかを実行します。
   - 個**Actions**々のノードを追加するには、追加するノードのアイコンをクリックします。
   - 複数のノード**Bulk Actions**を追加するには、追加するノードのチェックボックスをオンにしてから、

     注 : 追加するノードのElementソフトウェアのバージョンがクラスタで実行されているバージョンと異なる場合は、クラスタ マスターで実行されているElementソフトウェアのバージョンに非同期的に更新されます。更新されたノードは、自動的にクラスタに追加されます。この非同期プロセスの実行中、ノードの状態はpendingActiveになります。
4. **Add**をクリックします。

   ノードがアクティブなノードのリストに表示されます。

関連概念

ノードのバージョンと互換性（62ページ）
ノードの互換性は、ノードにインストールされているElementソフトウェアのバージョンに基づきます。ノードとクラスタのバージョンに互換性がない場合、Elementソフトウェアベースのストレージ クラスタは、ノードをクラスタ上のElementソフトウェアのバージョンに自動で更新します。

*Fibre Channel*ノードの設定（26ページ）
Fibre Channelノードを使用すると、クラスタをFibre Channelネットワーク ファブリックに接続できます。Fibre Channelノードはペアで追加され、アクティブ / アクティブ モードで動作します（すべてのノードがクラスタのトラフィックをアクティブに処理します）。Elementソフトウェア バージョン9.0以降を実行しているクラスタは、最大4つのノード、9.0より前のバージョンを実行しているクラスタは最大2つのノードをサポートします。

ノードのバージョンと互換性

ノードの互換性は、ノードにインストールされているElementソフトウェアのバージョンに基づきます。ノードとクラスタのバージョンに互換性がない場合、Elementソフトウェアベースのストレージ クラスタは、ノードをクラスタ上のElementソフトウェアのバージョンに自動で更新します。

以下に、Elementソフトウェアのバージョン番号を構成するソフトウェアのリリース レベルを示します。

メジャー

ソフトウェアのリリースを示す最初の番号。あるメジャー番号のノードを、メジャー番号が異なるノードを含むクラスタに追加することはできません。また、メジャー バージョンが異なるノードが混在したクラスタを作成することはできません。

マイナー

メジャー リリースに対して行われた既存のソフトウェア機能に対する小規模な機能追加や拡張を示す2番目の番号。マイナー コンポーネントはメジャー コンポーネントに対して増分され、マイナー コンポーネントの異なるElementソフトウェア リリース間に互換性はありません。たとえば、11.0と11.1には互換性はなく、11.1と11.2にも互換性はありません。

マイクロ

「major.minor」の形式で表されるElementソフトウェア バージョンへの互換性のあるパッチ（差分リリース）を示す3番目の番号。たとえば、11.0.1は11.0.2と互換性があり、11.0.2は11.0.3と互換性があります。

バージョン間に互換性があるためには、メジャー バージョンとマイナー バージョンの番号が一致する必要があります。マイクロ バージョンの番号は一致する必要はありません。

ノード混在環境でのクラスタ容量

1つのクラスタ内で異なるタイプのノードを混在させることができます。クラスタ内に混在させることができるのは、SFシリーズ2405、3010、4805、6010、9605、9010、19210、38410、およびHシリーズです。

Hシリーズのノードには、H610S-1、H610S-2、およびH610S-4があります。これらのノードは10GbEと25GbEの両方に対応しています。

暗号化されているノードとされていないノードは混在させないことを推奨します。ノードが混在するクラスタでは、1つのノードがクラスタの総容量の33%を超えることはできません。たとえば、SFシリーズ4805のノードが4つあるクラスタの場合、単独で追加できる最大のノードはSFシリーズ9605です。クラスタ容量のしきい値は、最大のノードが失われた場合を基準に計算されます。

ノードの状態

設定のレベルによって、ノードは次のいずれかの状態になります。

利用可能

ノードにはクラスタ名が関連付けられておらず、まだクラスタの一部ではありません。

保留

ノードが設定され、指定されたクラスタに追加できます。

このノードにアクセスするための認証は不要です。

保留中のアクティブ

互換性のある Element ソフトウェアをノードにインストールしています。完了すると、ノードはアクティブ状態に移行します。

Active

ノードはクラスタに参加しています。

このノードを変更するには、認証が必要です。

上記の各状態では、一部のフィールドは読み取り専用です。

ノードの詳細

[Cluster]タブの[Nodes]ページでは、ノードの情報（ID、名前、設定されているIOPS、ロール タイプなど）を確認できます。

Node ID

システムによって生成されたノードのID。

Node Name

システムによって生成されたノード名。

Available 4k IOPS

ノードに設定されたIOPS。

Node Role

クラスタでのノードのロール。有効な値は次のとおりです。

- Cluster Master：クラスタ全体の管理タスクを実行し、MVIPとSVIPを含むノード。
- Ensemble Node：クラスタに参加するノード。クラスタのサイズに応じて、3つまたは5つのアンサンブル ノードがあります。
- Fibre Channel：クラスタ内のノード。

Node Type

ノードのモデル タイプ。

Active Drives

ノード内のアクティブ ドライブの数。

Management IP

ノードに割り当てられた管理IP（MIP）アドレス。1GbEまたは10GbEネットワークの管理タスクで使用されます。

Cluster IP

ノードに割り当てられたクラスタIP（CIP）アドレス。同じクラスタ内のノード間の通信に使用されます。

Storage IP

ノードに割り当てられたストレージIP（SIP）アドレス。iSCSIネットワークの検出およびすべてのデータ ネットワーク トラフィックに使用されます。

Management VLAN ID

管理ローカル エリア ネットワークの仮想ID。

Storage VLAN ID

ストレージ ローカル エリア ネットワークの仮想ID。

Version

各ノードで実行されているソフトウェアのバージョン。

Replication Port

リモート レプリケーションに使用されるノードのポート。

Service Tag

ノードに割り当てられた一意のサービス タグ番号。

個々のノードの詳細の表示

個々のノードの詳細を確認できます。サービス タグやドライブの詳細のほか、利用率やドライブの統計のグラフも参照できます。[Cluster]タブの[Nodes]ページにある[Version]列で、各ノードのソフトウェア バージョンを確認できます。

手順

1. **[Cluster]** > **[Nodes]**の順にクリックします。
2. ノードの[Actions]アイコンをクリックします。
3. **[View Details]**をクリックします。

Fibre Channelポートの詳細の表示

[FC Ports]ページで、Fibre Channelポートの詳細（ステータス、名前、ポート アドレスなど）を確認できます。

手順

1. **[Cluster]** > **[FC Ports]**の順にクリックします。
2. このページの情報をフィルタリングするには、**[Filter]**をクリックします。

関連資料

*Fibre Channel*ポートの詳細（65ページ）

[Cluster]タブの[FC Ports]ページには、クラスタに接続されているFibre Channelポートに関する情報が表示されます。

Fibre Channelポートの詳細

[Cluster]タブの[FC Ports]ページには、クラスタに接続されているFibre Channelポートに関する情報が表示されます。

クラスタに接続されているFibre Channelポートに関する情報は次のとおりです。

Node ID

接続のセッションをホストしているノード。

Node Name

システムによって生成されたノード名。

Slot

Fibre Channelポートが配置されているスロットの番号。

HBA Port

Fibre Channelホスト バス アダプタ（HBA）上の物理ポート

WWNN

World Wide Node Name。

WWPN

ターゲットのWorld Wide Port Name。

Switch WWN

Fibre ChannelスイッチのWorld Wide Name。

Port State

ポートの現在の状態。

nPort ID

Fibre Channelファブリック上のノード ポートID。

Speed

ネゴシエートされたFibre Channel速度。有効な値は次のとおりです。

- 4Gbps
- 8Gbps
- 16Gbps

仮想ネットワークの管理

SolidFireストレージの仮想ネットワークを使用すると、別々の論理ネットワークに属する複数のクライアント間のトラフィックを1つのクラスタに接続できます。クラスタへの各接続は、VLANタギングを使用してネットワーク スタック内で分離されます。

関連タスク

仮想ネットワークの追加（66ページ）
クラスタ構成に新しい仮想ネットワークを追加すると、マルチテナント環境からElement ソフトウェアを実行しているクラスタに接続できるようになります。

仮想ルーティング /転送の有効化（67ページ）
仮想ルーティング / 転送（VRF）を有効にすることができます。これにより、ルーティング テーブルの複数のインスタンスをルータ内に共存させ、同時に使用できます。この機能はストレージ ネットワークでのみ使用できます。

仮想ネットワークの編集（68ページ）
VLAN名、ネットマスク、IPアドレス ブロックのサイズなどのVLAN属性を変更できます。VLANのVLANタグおよびSVIPは変更できません。ゲートウェイ属性は、非VRF VLANの有効なパラメータではありません。

*VRF VLAN*の編集（68ページ）
VLAN名、ネットマスク、ゲートウェイ、IPアドレス ブロックなどのVRF VLAN属性を変更できます。

仮想ネットワークの削除（68ページ）
仮想ネットワーク オブジェクトを削除することができます。仮想ネットワークを削除する前に、アドレス ブロックを別の仮想ネットワークに追加する必要があります。

仮想ネットワークの詳細

[Cluster]タブの[Network]ページでは、仮想ネットワークに関する情報（ID、VLANタグ、SVIP、ネットマスクなど）を確認できます。

ID

システムによって割り当てられたVLANネットワークの一意のID。

Name

VLANネットワークにユーザが割り当てた一意の名前。

VLAN Tag

仮想ネットワークの作成時に割り当てられたVLANタグ。

SVIP

仮想ネットワークに割り当てられたストレージ仮想IPアドレス。

Netmask

この仮想ネットワークのネットマスク。

Gateway

仮想ネットワーク ゲートウェイの一意のIPアドレス。VRFが有効になっている必要があります。

VRF Enabled

仮想ルーティング / 転送が有効になっているかどうか。

IPs Used

仮想ネットワークで使用される仮想ネットワークIPアドレスの範囲。

仮想ネットワークの追加

クラスタ構成に新しい仮想ネットワークを追加すると、マルチテナント環境からElement ソフトウェアを実行しているクラスタに接続できるようになります。

開始する前に

- クラスタ ノード上の仮想ネットワークに割り当てるIPアドレス範囲を特定します。

- NetApp Elementのすべてのストレージ トラフィックのエンドポイントとして使用するストレージ ネットワークIP（SVIP）アドレスを特定します。

  注意 : この構成では、次の条件を考慮する必要があります。

  - VRFが有効でないVLANでは、SVIPと同じサブネットにイニシエータが含まれている必要があります。
  - VRFが有効なVLANでは、SVIPと同じサブネットにイニシエータが含まれている必要はなく、ルーティングがサポートされます。
  - デフォルトのSVIPでは、SVIPと同じサブネットにイニシエータが含まれている必要はなく、ルーティングがサポートされます。

タスク概要

仮想ネットワークを追加すると、各ノードのインターフェイスが作成され、そのそれぞれに仮想ネットワークIPアドレスが必要となります。新しい仮想ネットワークを作成する際に指定するIPアドレスの数は、クラスタ内のノードの数以上であることが必要です。仮想ネットワーク アドレスはまとめてプロビジョニングされ、個々のノードに自動的に割り当てられます。仮想ネットワーク アドレスをクラスタ内のノードに手動で割り当てる必要はありません。

手順

1. **[Cluster]** > **[Network]**の順にクリックします。
2. **[Create VLAN]**をクリックします。
3. **[Create a New VLAN]**ダイアログ ボックスで、次のフィールドに値を入力します。
   - **VLAN Name**
   - **VLAN Tag**
   - **SVIP**
   - **Netmask**
   - （オプション）**Description**
4. **[IP Address Blocks]**の**[Starting IP]**に、IPアドレス範囲の開始IPアドレスを入力します。
5. IP範囲の**[Size]**に、範囲に含めるIPアドレスの数を入力します。
6. **[Add a Block]**をクリックして、このVLANの連続しないIPアドレス ブロックを追加します。
7. **[Create VLAN]**をクリックします。

仮想ルーティング / 転送の有効化

仮想ルーティング / 転送（VRF）を有効にすることができます。これにより、ルーティング テーブルの複数のインスタンスをルータ内に共存させ、同時に使用できます。この機能はストレージ ネットワークでのみ使用できます。

タスク概要

VRFは、VLANの作成時にのみ有効にすることができます。非VRFに戻す場合は、VLANを削除して再作成する必要があります。

手順

1. **[Cluster]** > **[Network]**の順にクリックします。
2. 新しいVLANでVRFを有効にするには、**[Create VLAN]**を選択します。

1. 新しいVRF / VLANに関連する情報を入力します。「仮想ネットワークの追加」を参照してください。
2. **[Enable VRF]**チェック ボックスをオンにします。
3. オプション: ゲートウェイを入力します。

3. **[Create VLAN]**をクリックします。

関連タスク

仮想ネットワークの追加（66ページ）

クラスタ構成に新しい仮想ネットワークを追加すると、マルチテナント環境からElementソフトウェアを実行しているクラスタに接続できるようになります。

仮想ネットワークの編集

VLAN名、ネットマスク、IPアドレス ブロックのサイズなどのVLAN属性を変更できます。VLANのVLANタグおよびSVIPは変更できません。ゲートウェイ属性は、非VRF VLANの有効なパラメータではありません。

タスク概要

iSCSI、リモート レプリケーション、またはその他のネットワーク セッションの実行中は、変更に失敗することがあります。

手順

1. **[Cluster]** > **[Network]**の順にクリックします。
2. 編集するVLANの[Actions]アイコンをクリックします。
3. **[Edit]**をクリックします。
4. **[Edit VLAN]**ダイアログ ボックスで、VLANの新しい属性を入力します。
5. **[Add a Block]**をクリックして、仮想ネットワークの連続しないIPアドレス ブロックを追加します。
6. **[Save Changes]**をクリックします。

VRF VLANの編集

VLAN名、ネットマスク、ゲートウェイ、IPアドレス ブロックなどのVRF VLAN属性を変更できます。

手順

1. **[Cluster]** > **[Network]**の順にクリックします。
2. 編集するVLANの[Actions]アイコンをクリックします。
3. **[Edit]**をクリックします。
4. **[Edit VLAN]**ダイアログ ボックスで、VRF VLANの新しい属性を入力します。
5. **[Save Changes]**をクリックします。

仮想ネットワークの削除

仮想ネットワーク オブジェクトを削除することができます。仮想ネットワークを削除する前に、アドレス ブロックを別の仮想ネットワークに追加する必要があります。

手順

1. **[Cluster]** > **[Network]**の順にクリックします。
2. 削除するVLANの[Actions]アイコンをクリックします。
3. **[Delete]**をクリックします。
4. メッセージを確認します。

関連タスク

仮想ネットワークの編集（68ページ）

VLAN名、ネットマスク、IPアドレス ブロックのサイズなどのVLAN属性を変更できます。VLANのVLANタグおよびSVIPは変更できません。ゲートウェイ属性は、非VRF VLANの有効なパラメータではありません。

FIPSドライブをサポートするクラスタの作成

お客様の環境へソリューションを導入するにあたり、セキュリティの重要性はますます高まっています。Federal Information Processing Standard（FIPS;連邦情報処理標準）は、コンピュータのセキュリティと相互運用性に関する標準です。FIPS 140-2認定の保存データの暗号化は、全体的なセキュリティ ソリューションに欠かせない要素です。

手順

1. *FIPS*ドライブの対応が異なるノードの混在回避（69ページ）
FIPSドライブ機能を有効にする準備として、FIPSドライブに対応しているノードと対応していないノードが混在しないようにする必要があります。
2. 保存データの暗号化の有効化（70ページ）
保存データの暗号化をクラスタ全体で有効または無効にすることができます。この機能は、デフォルトでは有効になっていません。FIPSドライブをサポートするには、保存データの暗号化を有効にする必要があります。
3. ノードが*FIPS*ドライブ機能に対応しているかどうかの確認（70ページ）
ストレージ クラスタ内のすべてのノードがFIPSドライブに対応しているかどうかを確認するには、NetApp ElementソフトウェアのGetFipsReport APIメソッドを使用します。
4. *FIPS*ドライブ機能の有効化（71ページ）
FIPSドライブ機能を有効にするには、NetApp ElementソフトウェアのEnableFeature APIメソッドを使用します。
5. *FIPS*ドライブのステータス確認（71ページ）
FIPSドライブ機能がクラスタで有効になっているかどうかを確認するには、NetApp ElementソフトウェアのGetFeatureStatus APIメソッドを使用します。このメソッドを実行すると、FIPSドライブの有効化ステータス（trueまたはfalse）が返されます。
6. *FIPS*ドライブ機能のトラブルシューティング（71ページ）
NetApp ElementソフトウェアUIを使用して、システムにおけるFIPSドライブ機能関連のクラスタ障害 / エラーに関するアラートを確認できます。

FIPSドライブの対応が異なるノードの混在回避

FIPSドライブ機能を有効にする準備として、FIPSドライブに対応しているノードと対応していないノードが混在しないようにする必要があります。

タスク概要

次の条件を満たす場合、クラスタはFIPSドライブに準拠していると見なされます。

- すべてのドライブがFIPSドライブとして認定されている。
- すべてのノードがFIPSドライブ ノードである。
- 保存データの暗号化（EAR）が有効になっている。
- FIPSドライブ機能が有効になっている。FIPSドライブ機能を有効にするには、すべてのドライブとノードがFIPSに対応し、保存データの暗号化が有効になっている必要があります。

保存データの暗号化の有効化

保存データの暗号化をクラスタ全体で有効または無効にすることができます。この機能は、デフォルトでは有効になっていません。FIPSドライブをサポートするには、保存データの暗号化を有効にする必要があります。

手順

1. NetApp Elementソフトウェアuiで、**[Cluster]** > **[Settings]**をクリックします。
2. **[Enable Encryption at Rest]**をクリックします。

関連概念

保存データの暗号化（56ページ）

SolidFireクラスタでは、クラスタに保管されているすべてのデータを暗号化できます。

関連タスク

クラスタでの暗号化の有効化と無効化（56ページ）

保存データの暗号化をクラスタ全体で有効または無効にすることができます。この機能は、デフォルトでは有効になっていません。

ノードがFIPSドライブ機能に対応しているかどうかの確認

ストレージ クラスタ内のすべてのノードがFIPSドライブに対応しているかどうかを確認するには、NetApp ElementソフトウェアのGetFipsReport APIメソッドを使用します。

タスク概要

生成されるレポートには、次のいずれかのステータスが表示されます。

- None：ノードはFIPSドライブ機能に対応していません。
- Partial：ノードはFIPSに対応していますが、一部のドライブがFIPSドライブではありません。
- Ready：ノードはFIPSに対応しており、すべてのドライブがFIPSドライブです（ドライブが存在しない場合も含む）。

手順

1. Element APIで次のように入力し、ストレージ クラスタ内のノードとドライブがFIPSドライブに対応しているかどうかを確認します。

   ```
   GetFipsReport
   ```

2. 結果を確認し、ステータスが「Ready」になっていないノードを確認します。
3. ステータスが「Ready」になっていないノードについて、ドライブがFIPSドライブ機能に対応しているかどうかを確認します。
   - Element APIで次のように入力します。`GetHardwareList`
   - **DriveEncryptionCapabilityType**の値を確認します。値が「fips」の場合、そのハードウェアはFIPSドライブ機能に対応しています。

   詳細については、*NetApp Element API*リファレンス ガイドの`GetFipsReport`または`ListDriveHardware`の説明を参照してください。
4. ドライブがFIPSドライブ機能に対応していない場合は、ハードウェア（ノードまたはドライブ）をFIPS対応のハードウェアに交換します。

関連情報

*Element API*を使用したストレージの管理

FIPSドライブ機能の有効化

FIPSドライブ機能を有効にするには、NetApp ElementソフトウェアのEnableFeature APIメソッドを使用します。

開始する前に

クラスタで保存データの暗号化が有効になっている必要があります。また、すべてのノードとドライブがFIPSに対応している（`GetFipsReport`ですべてのノードのステータスが「Ready」と表示される）必要があります。

手順

Element APIで次のように入力し、すべてのドライブでFIPSを有効にします。

```
EnableFeature params: FipsDrives
```

関連情報

*Element API*を使用したストレージの管理

FIPSドライブのステータス確認

FIPSドライブ機能がクラスタで有効になっているかどうかを確認するには、NetApp ElementソフトウェアのGetFeatureStatus APIメソッドを使用します。このメソッドを実行すると、FIPSドライブの有効化ステータス（trueまたはfalse）が返されます。

手順

1. Element APIで次のように入力し、クラスタのFIPSドライブ機能を確認します。

   ```
   GetFeatureStatus
   ```

2. `GetFeatureStatus` API呼び出しの結果を確認します。FIPSドライブのenabledの値がtrueであれば、FIPSドライブ機能が有効になっています。

   ```
   {"enabled": true,
   "feature": "FipsDrives"
   }
   ```

関連情報

*Element API*を使用したストレージの管理

FIPSドライブ機能のトラブルシューティング

NetApp ElementソフトウェアUIを使用して、システムにおけるFIPSドライブ機能関連のクラスタ障害 / エラーに関するアラートを確認できます。

手順

1. Element UIで、**[Reporting]** > **[Alerts]**の順に選択します。
2. 次のクラスタ障害を探します。
   - FIPS drives mismatched
   - FIPS drives out of compliance
3. 推奨される解決方法については、クラスタ障害コードに関する情報を参照してください。

関連資料

クラスタ障害コード（165ページ）

Alertsページに表示されている障害コードを生成すると、エラーまたは該当する可能性のある状態が報告されます。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。

クラスタでのHTTPSのFIPS 140-2の有効化

`EnableFeature` APIメソッドを使用して、HTTPS通信のFIPS 140-2動作モードを有効にすることができます。

タスク概要

NetApp Elementソフトウェアを使用すると、クラスタでFederal Information Processing Standards（FIPS;連邦情報処理標準）140-2動作モードを有効にすることができます。このモードを有効にすると、NetApp Cryptographic Security Module（NCSM）がアクティブになり、NetApp Element UIおよびAPIとのHTTPS経由の通信にFIPS 140-2レベル1認定の暗号化が適用されるようになります。

注意 : 一度有効にしたFIPS 140-2モードを無効にすることはできません。FIPS 140-2モードを有効にすると、クラスタ内の各ノードがリブートされてセルフテストが実行され、NCSMが正しく有効化されてFIPS 140-2認定モードで動作していることが確認されます。その際、クラスタでは管理接続とストレージ接続の両方が中断します。このモードの使用は慎重に計画する必要があり、このモードが提供する暗号化メカニズムを必要とする環境でのみ有効にするようにしてください。

詳細については、Element APIの情報を参照してください。

FIPSを有効にするAPI要求の例を次に示します。

```
{
  "method": "EnableFeature",
    "params": {
        "feature" : "fips"
    },
    "id": 1
}
```

この動作モードを有効にすると、すべてのHTTPS通信でFIPS 140-2で承認された暗号が使用されるようになります。

関連資料

*SSL*暗号（73ページ）
Secure Socket Layer（SSL）暗号は、ホストがセキュアな通信を確立するために使用する暗号化アルゴリズムです。Elementソフトウェアでサポートされる標準の暗号と、FIPS 140-2モードが有効な場合にサポートされる非標準の暗号があります。

関連情報

*Element API*を使用したストレージの管理

SSL暗号

Secure Socket Layer（SSL）暗号は、ホストがセキュアな通信を確立するために使用する暗号化アルゴリズムです。Elementソフトウェアでサポートされる標準の暗号と、FIPS 140-2モードが有効な場合にサポートされる非標準の暗号があります。

以下は、Elementソフトウェアでサポートされる標準のSSL暗号と、FIPS 140-2モードが有効になっている場合にサポートされるSSL暗号の一覧です。

FIPS 140-2が無効な場合

TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C

TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A

TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A

TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A

TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A

TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A

TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A

TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (rsa 2048) - A

TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (rsa 2048) - A

TLS_RSA_WITH_IDEA_CBC_SHA (rsa 2048) - A

TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - C

TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - C

TLS_RSA_WITH_SEED_CBC_SHA (rsa 2048) - A

FIPS 140-2が有効な場合

TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (dh 2048) - A

TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 2048) - A

TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (dh 2048) - A

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 2048) - A

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A

TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C

TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A

TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A

TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A

TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A

TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A

TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A

関連タスク

クラスタでのHTTPSのFIPS 140-2の有効化（72ページ）

`EnableFeature` APIメソッドを使用して、HTTPS通信のFIPS 140-2動作モードを有効にすることができます。

外部キー管理の概要

External Key Management （ EKM ）は、 Secure Authentication Key （ AK ）管理と、 Off-Cluster External Key Server（ EK; 外部キーサーバ）を提供します。EKSを使用することで、AKの安全な生成と保管が可能になります。

AKは、クラスタで保存データの暗号化（EAR）が有効になっている場合に、自己暗号化ドライブ（SED）をロックおよびロック解除するために使用されます。クラスタは、OASISで定義された標準プロトコルであるKey Management Interoperability Protocol（KMIP）を使用して、EKSと通信します。

手順

1. 外部キー管理の設定（74ページ）
Element API を使用してこれらの基本的な手順を使用して、外部キー管理機能を設定できます。各APIメソッドの詳細については、『NetApp Element APIリファレンス ガイド』を参照してください。
2. アクセス不可または無効な認証キーのリカバリ（75ページ）
場合によっては、ユーザの操作が必要なエラーが発生することがあります。エラーが発生すると、クラスタ障害（クラスタ障害コードと呼ばれる）が生成されます。ここでは、最も可能性の高い2つのケースについて説明します。
3. 外部キー管理*API*コマンド（75ページ）
EKMの管理と設定に使用できるすべてのAPIのリストです。

外部キー管理の設定

Element API を使用してこれらの基本的な手順を使用して、外部キー管理機能を設定できます。各APIメソッドの詳細については、『NetApp Element APIリファレンス ガイド』を参照してください。

手順

1. 外部キー サーバ（EKS）との信頼関係を確立します。
    1. 次のAPIメソッドを呼び出して、キー サーバとの信頼関係を確立するために使用する、Elementクラスタの公開鍵と秘密鍵のペアを作成します。

        `CreatePublicPrivateKeyPair`
    2. 認証局による署名が必要な証明書署名要求（CSR）を取得します。CSRによって、キー サーバはキーにアクセスするElementクラスタがElementクラスタとして認証されていることを確認できます。次のAPIメソッドを呼び出します。

        `GetClientCertificateSignRequest`
    3. EKSと認証局を使用して、取得したCSRに署名します。詳細については、他社のドキュメントを参照してください。
2. クラスタにサーバとプロバイダを作成して、EKSと通信します。キー プロバイダはキーを取得する場所を定義し、サーバは通信するEKSの特定の属性を定義します。
    1. 次のAPIメソッドを呼び出して、キー サーバの詳細が格納されるキー プロバイダを作成します。

        `CreateKeyProviderKmip`
    2. 次のAPIメソッドを呼び出して、署名付き証明書と認証局の公開鍵を提供するキー サーバを作成します。

        `CreateKeyServerKmip`

TestKeyServerKmip

テストに失敗した場合は、サーバの接続と設定を確認します。その後、テストを繰り返します。

3. 次のAPIメソッドを呼び出して、キー サーバをキー プロバイダ コンテナに追加します。

AddKeyServerToProviderKmip

TestKeyProviderKmip

テストに失敗した場合は、サーバの接続と設定を確認します。その後、テストを繰り返します。

3. 保存データの暗号化を有効にします。

1. 次のAPIメソッドを呼び出して、キーの格納に使用されるキー サーバを含むキー プロバイダのIDを指定し、保存データの暗号化を有効にします。

EnableEncryptionAtRest

注 : 外部キー管理設定を使用する保存データの暗号化を有効にするには、APIで保存データの暗号化を有効にする必要があります。既存のElement UIから有効にすると、内部で生成されたキーの使用に戻ります。

関連概念

保存データの暗号化（56ページ）

SolidFireクラスタでは、クラスタに保管されているすべてのデータを暗号化できます。

関連タスク

クラスタでの暗号化の有効化と無効化（56ページ）

保存データの暗号化をクラスタ全体で有効または無効にすることができます。この機能は、デフォルトでは有効になっていません。

関連情報

Element APIを使用したストレージの管理

アクセス不可または無効な認証キーのリカバリ

場合によっては、ユーザの操作が必要なエラーが発生することがあります。エラーが発生すると、クラスタ障害（クラスタ障害コードと呼ばれる）が生成されます。ここでは、最も可能性の高い2つのケースについて説明します。

1. `KmipServerFault`クラスタ障害のため、クラスタがドライブのロックを解除できません。このエラーは、クラスタの初回起動時に、キー サーバにアクセスできないか、必要なキーを使用できない場合に発生します。

1. クラスタ障害コードのリカバリ手順に従います（該当する場合）。

2. メタデータ ドライブがエラーとしてマークされながら「Available」状態になっているために、`sliceServiceUnhealthy`障害が生成されることがあります。

1. ドライブを追加し直してください。

2. 3～4分経過したら`sliceServiceUnhealthy`障害が解消されたことを確認します。

クラスタ障害コードの情報を参照してください。

クラスタ障害コード（165ページ）

外部キー管理APIコマンド

EKMの管理と設定に使用できるすべてのAPIのリストです。

クラスタと外部の顧客所有サーバ間の信頼関係を確立するために使用されます。

- CreatePublicPrivateKeyPair
- GetClientCertificateSignRequest

外部の顧客所有サーバの詳細を定義するために使用されます。

- CreateKeyServerKmip
- ModifyKeyServerKmip
- DeleteKeyServerKmip
- GetKeyServerKmip
- ListKeyServersKmip
- TestKeyServerKmip

外部キー サーバを管理するキー プロバイダの作成と保守に使用されます。

- CreateKeyProviderKmip
- DeleteKeyProviderKmip
- AddKeyServerToProviderKmip
- RemoveKeyServerFromProviderKmip
- GetKeyProviderKmip
- ListKeyProvidersKmip
- TestKeyProviderKmip

APIメソッドについては、APIリファレンス情報を参照してください。

*Element API*を使用したストレージの管理

データ管理

Elementソフトウェアを実行しているクラスタのデータは、Element UIの[Management]タブで管理できます。実行可能なクラスタ管理機能には、データ ボリューム、ユーザ アカウント、ボリューム アクセス グループ、イニシエータ、およびQoSポリシーの作成と管理などがあります。

関連概念

仮想ボリュームの使用（93ページ）
Element UIを使用して、仮想ボリュームおよび仮想ボリュームに関連付けられたストレージ コンテナ、プロトコル エンドポイント、バインド、およびホストの情報を確認し、タスクを実行できます。

ボリューム アクセス グループとイニシエータの使用（103ページ）
iSCSIイニシエータまたはFibre Channelイニシエータを使用して、ボリューム アクセス グループ内に定義されたボリュームにアクセスできます。

関連タスク

ユーザ アカウントの使用（77ページ）
SolidFireストレージ システムでは、クライアントはユーザ アカウントを使用してノード上のボリュームに接続します。ボリュームには、作成時に特定のユーザ アカウントが割り当てられます。

ボリュームの使用（80ページ）
SolidFireシステムは、ボリュームを使用してストレージをプロビジョニングします。ボリュームは、iSCSIクライアントまたはFibre Channelクライアントがネットワーク経由でアクセスするブロック デバイスです。[Management]タブの[Volumes]ページで、ノード上のボリュームを作成、変更、クローニング、および削除できます。また、ボリュームの帯域幅とI/O使用量に関する統計も確認できます。

ユーザ アカウントの使用

SolidFireストレージ システムでは、クライアントはユーザ アカウントを使用してノード上のボリュームに接続します。ボリュームには、作成時に特定のユーザ アカウントが割り当てられます。

タスク概要

アカウントには、そのアカウントに割り当てられているボリュームへのアクセスに必要なCHAP認証が含まれています。

アカウントには最大2,000個のボリュームを関連付けることができますが、1つのボリュームが属することのできるアカウントは1つだけです。

関連タスク

アカウントの作成（78ページ）
アカウントを作成し、ボリュームへのアクセスを許可することができます。

個々のアカウントのパフォーマンスの詳細の表示（79ページ）
個々のアカウントのパフォーマンス アクティビティをグラフ形式で表示できます。

アカウントの編集（79ページ）
アカウントを編集して、ステータス、CHAPシークレット、またはアカウント名を変更できます。

アカウントの削除（80ページ）

不要になったアカウントを削除できます。

アカウントの作成

アカウントを作成し、ボリュームへのアクセスを許可することができます。

タスク概要

各アカウント名はシステム内で一意である必要があります。

手順

1. **[Management]** > **[Accounts]**の順に選択します。
2. **[Create Account]**をクリックします。
3. **[Username]**を入力します。
4. **[CHAP Settings]**セクションで、次の情報を入力します。
   - **Initiator Secret**：CHAPノード セッション認証用のイニシエータ シークレット。
   - **Target Secret**：CHAPノード セッション認証用のターゲット シークレット。

   注 : パスワードを自動生成する場合は、クレデンシャル フィールドを空白のままにします。
5. **[Create Account]**をクリックします。

アカウントの詳細

[Management]タブの[Accounts]ページには、システム内の各アカウントに関する情報（ID、ユーザ名、アカウントに割り当てられているボリュームの削減率の詳細など）が表示されます。

ID

システムによって生成されたアカウントのID。

Username

アカウントの作成時に指定した名前。

Status

アカウントのステータス。有効な値は次のとおりです。

- `active`：アクティブ アカウント。
- `locked`：ロック済みアカウント。
- `removed`：削除およびパージされたアカウント。

Active Volumes

アカウントに割り当てられているアクティブ ボリュームの数。

Compression

アカウントに割り当てられているボリュームの圧縮による削減率。

Deduplication

アカウントに割り当てられているボリュームの重複排除による削減率。

Thin Provisioning

アカウントに割り当てられているボリュームのシンプロビジョニングによる削減率。

Overall Efficiency

アカウントに割り当てられているボリュームの全体的な削減率。

個々のアカウントのパフォーマンスの詳細の表示

個々のアカウントのパフォーマンス アクティビティをグラフ形式で表示できます。

タスク概要

グラフには、アカウントのI/Oとスループットの情報が表示されます。AverageとPeakのアクティビティ レベルが、10秒間隔で表示されます。これらの統計は、アカウントに割り当てられているすべてのボリュームのアクティビティを対象とします。

手順

1. **[Management]** > **[Accounts]**を選択します。
2. アカウントの[Actions]アイコンをクリックします。
3. **[View Details]**をクリックします。

アカウントの編集

アカウントを編集して、ステータス、CHAPシークレット、またはアカウント名を変更できます。

タスク概要

アカウントのCHAP設定を変更したり、アクセス グループからイニシエータやボリュームを削除したりすると、イニシエータがボリュームにアクセスできなくなることがあります。ボリュームへのアクセスが予期せず失われないことを確認するには、アカウントまたはアクセスグループの変更の影響を受ける iSCSI セッションを常にログアウトし、イニシエータの設定とクラスタ設定の変更が完了した後にイニシエータがボリュームに再接続できることを確認します。

注意 : 管理サービスに関連付けられている永続ボリュームは、インストールまたはアップグレード時に作成される新しいアカウントに割り当てられます。永続ボリュームを使用している場合は、関連するアカウントを変更または削除しないでください。

手順

1. **Management** > **Accounts**の順に選択します。
2. アカウントの[Actions]アイコンをクリックします。
3. 表示されるメニューで**Edit**、を選択します。
4. オプション: を編集**Username**します。 .
5. オプション: **Status**ドロップダウンリストをクリックして、別のステータスを選択します。

   注意 : ステータスを**locked**に変更すると、アカウントへのすべての iSCSI 接続が終了し、アカウントにアクセスできなくなります。アカウントに関連付けられたボリュームは維持されますが、ボリュームは iSCSI で検出できません。

6. オプション: **CHAP SettingsInitiator SecretTarget Secret**で、ノードセッション認証に使用するクレデンシャルとクレデンシャルを編集します。

   注 : CHAP Settingsクレデンシャルを変更しない場合、クレデンシャルは変更されません。クレデンシャルのフィールドを空白にすると、システムによって新しいパスワードが生成されます。

7. **Save Changes**をクリックします。

アカウントの削除

不要になったアカウントを削除できます。

開始する前に

アカウントを削除する前に、そのアカウントに関連付けられているボリュームを削除およびパージします。

注意 : 管理サービスに関連付けられている永続ボリュームは、インストールまたはアップグレード時に作成される新しいアカウントに割り当てられます。永続ボリュームを使用している場合は、関連するアカウントを変更または削除しないでください。

手順

1. **Management** > **Accounts**の順に選択します。
2. 削除するアカウントの[Actions]アイコンをクリックします。
3. 表示されるメニューで**Delete**、を選択します。
4. 操作を確定します。

ボリュームの使用

SolidFireシステムは、ボリュームを使用してストレージをプロビジョニングします。ボリュームは、iSCSIクライアントまたはFibre Channelクライアントがネットワーク経由でアクセスするブロック デバイスです。[Management]タブの[Volumes]ページで、ノード上のボリュームを作成、変更、クローニング、および削除できます。また、ボリュームの帯域幅とI/O使用量に関する統計も確認できます。

関連概念

QoS（81ページ）
SolidFireストレージ クラスタでは、サービス品質（QoS）パラメータをボリューム単位で指定できます。QoSを定義する3つの設定可能なパラメータであるMin IOPS、Max IOPS、およびBurst IOPSを使用して、IOPS（1秒あたりの入出力）で測定されるクラスタ パフォーマンスを保証することができます。

関連タスク

*QoS*ポリシーの作成（84ページ）
QoSポリシーを作成し、ボリュームの作成時に適用することができます。

*QoS*ポリシーの編集（85ページ）
既存のQoSポリシーの名前を変更したり、ポリシーに関連付けられている値を編集したりできます。QoSポリシーの変更は、そのポリシーに関連付けられているすべてのボリュームに反映されます。

*QoS*ポリシーの削除（85ページ）
不要になったQoSポリシーを削除できます。QoSポリシーを削除すると、そのポリシーに関連付けられているすべてのボリュームのQoS設定は維持されますが、ポリシーとの関連付けは解除されます。

ボリュームの作成（85ページ）
ボリュームを作成して、特定のアカウントに関連付けることができます。すべてのボリュームをアカウントに関連付ける必要があります。この関連付けにより、アカウントは、iSCSIイニシエータ経由でCHAPクレデンシャルを使用してボリュームにアクセスできます。

個々のボリュームのパフォーマンスの詳細の表示（87ページ）

個々のボリュームのパフォーマンス統計を表示できます。

アクティブ ボリュームの編集（87ページ）
QoS値、ボリュームのサイズ、バイト値の算出単位など、ボリュームの属性を変更できます。レプリケーションで使用するため、またはボリュームへのアクセスを制限するために、アカウント アクセスを変更することもできます。

ボリュームの削除（89ページ）
エレメントストレージクラスタから 1 つ以上のボリュームを削除できます。

削除したボリュームのリストア（90ページ）
システムから削除したボリュームは、パージされていなければリストアできます。削除したボリュームは約8時間後に自動的にパージされます。パージ済みのボリュームはリストアできません。

ボリュームのパージ（90ページ）
パージしたボリュームは、システムから完全に削除されます。ボリューム内のデータはすべて失われます。

ボリュームのクローニング（90ページ）
単一のボリュームまたは複数のボリュームのクローンを作成して、データのポイントインタイム コピーを作成できます。ボリュームをクローニングすると、ボリュームのSnapshotが作成され、次にそのSnapshotが参照しているデータのコピーが作成されます。これは非同期のプロセスであり、クローニングするボリュームのサイズおよび現在のクラスタの負荷によって所要時間が異なります。

*Fibre Channel*ボリュームへの*LUN*の割り当て（92ページ）
ボリューム アクセス グループ内のFibre Channelボリュームに対するLUNの割り当てを変更できます。ボリューム アクセス グループを作成する際に、Fibre Channelボリュームに LUNを割り当てることもできます。

ボリュームへの*QoS*ポリシーの適用（92ページ）
既存のQoSポリシーを1つ以上のボリュームに一括して適用できます。

ボリュームの*QoS*ポリシーの関連付けの解除（92ページ）
カスタムのQoS設定を選択することで、ボリュームのQoSポリシーの関連付けを解除できます。

QoS

SolidFireストレージ クラスタでは、サービス品質（QoS）パラメータをボリューム単位で指定できます。QoSを定義する3つの設定可能なパラメータであるMin IOPS、Max IOPS、およびBurst IOPSを使用して、IOPS（1秒あたりの入出力）で測定されるクラスタ パフォーマンスを保証することができます。

注 : SolidFire Active IQにはQoSに関する推奨ページがあり、QoSの最適な設定とセットアップに関するアドバイスを提供します。

各IOPSパラメータの定義は次のとおりです。

Min IOPS

ストレージ クラスタがボリュームに提供する平常時の最小IOPS。ボリュームに設定されたMin IOPSは、そのボリュームに対して最低限保証されるパフォーマンス レベルです。パフォーマンスがこのレベルを下回ることはありません。

Max IOPS

ストレージ クラスタがボリュームに提供する平常時の最大IOPS。クラスタのIOPSレベルが非常に高い場合も、IOPSパフォーマンスはこのレベル以下に抑えられます。

Burst IOPS

短時間のバースト時に許容される最大IOPS。ボリュームがMax IOPS未満で動作している間は、バースト クレジットが蓄積されます。パフォーマンス レベルが非常に高くなって最大レベルに達した場合、ボリュームでIOPSの短時間のバーストが許容されます。

Elementソフトウェアでは、IOPS使用率が低い状態でクラスタが稼働しているときにBurst IOPSが使用されます。

個々のボリュームは、蓄積したバースト クレジットを使用して、一定の「バースト期間」中はMax IOPSを最大でBurst IOPSレベルまで一時的に超過することができます。ボリュームのバースト時間は最大で60秒です。クラスタの容量にバーストに対応できるだけの余力があることが条件になります。

ボリュームは、Max IOPS未満で動作している1秒ごとに、1秒分のバースト クレジットを蓄積します（最大60秒）。

Burst IOPSには2つの制限があります。

- ボリュームは、蓄積したバースト クレジット数と同じ秒数だけMax IOPSを超過できます。
- ボリュームがMax IOPSの設定を超えた場合は、Burst IOPSの設定によって制限されます。つまり、バースト時のIOPSがボリュームのBurst IOPSの設定を超えることはありません。

Effective Max Bandwidth

最大帯域幅は、（QoS曲線に基づく）IOPSにIOサイズを掛けて計算されます。

例：

QoSパラメータをMin IOPS = 100、Max IOPS = 1000、Burst IOPS = 1500に設定した場合、パフォーマンスの品質は次のようになります。

- 各ワークロードは、クラスタでIOPSに対するワークロードの競合が発生するまで、最大で1000 IOPSを持続的に使用できます。競合が発生すると、すべてのボリュームのIOPSが指定のQoS範囲内に戻ってパフォーマンスの競合が解消されるまで、IOPSが少しずつ引き下げられます。
- すべてのボリュームのパフォーマンスは、最大でMin IOPSの100まで引き下げられます。Min IOPSである100を下回ることはなく、ワークロードの競合が解消されれば100 IOPSよりも高いレベルにとどまることが可能です。
- パフォーマンスは長期間にわたって1000 IOPSを超えることも、100 IOPSを下回ることもありません。1500 IOPS（Burst IOPS）のパフォーマンスは、Max IOPS未満で動作することでバースト クレジットを蓄積したボリュームに対して短時間の間のみ許容されます。バースト レベルが持続することはありません。

QoS値の制限

ここでは、指定可能なサービス品質（QoS）の最小値と最大値について説明します。

			I/Oサイズの最大値			
パラメータ	**最小値**	**デフォルト**	**4KB**	**8KB**	**16KB**	**262KB**
Min IOPS	50	50	15,000	9,375*	5556*	385*
Max IOPS	100	15,000	200,000**	125,000	74,074	5128
Burst IOPS	100	15,000	200,000**	125,000	74,074	5128

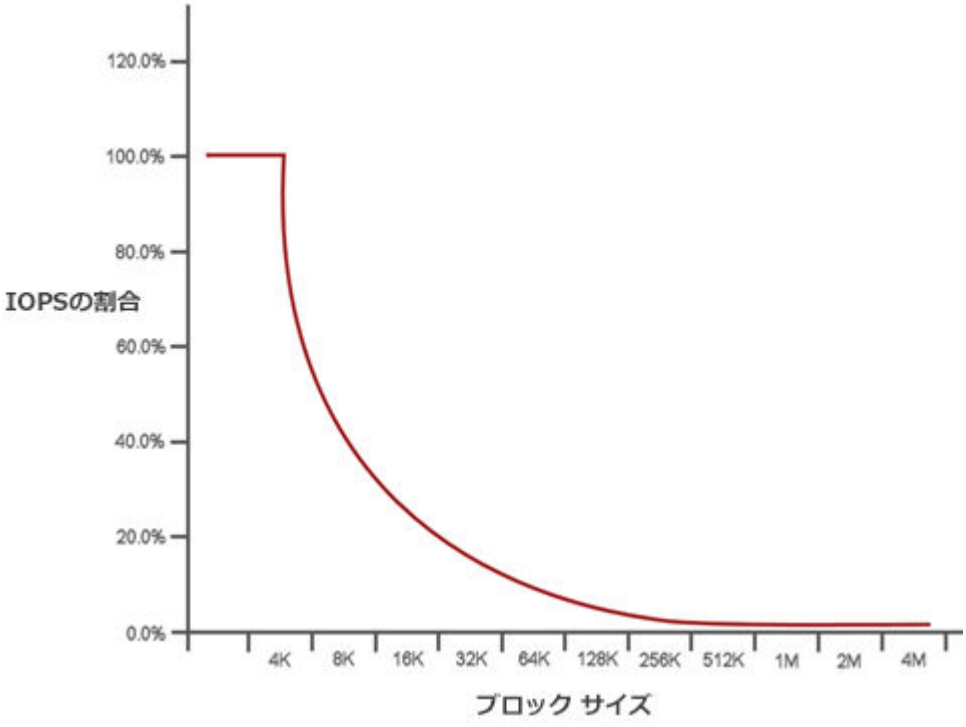
			I/Oサイズの最大値			
パラメータ	最小値	デフォルト	4KB	8KB	16KB	262KB
*これらは概算値です。 **Max IOPSとBurst IOPSは最大200,000に設定できます。ただし、この設定は、ボリュームのパフォーマンスの制限を意図的に解放する目的でのみ使用できます。実際のボリュームの最大パフォーマンスは、クラスタの使用率と各ノードのパフォーマンスによって制限されます。						

QoSパフォーマンス曲線

サービス品質（QoS）パフォーマンス曲線は、ブロック サイズとIOPSの割合の関係を示します。

アプリケーションが取得できるIOPSには、ブロック サイズと帯域幅が直接影響します。Elementソフトウェアは、ブロック サイズを4kに正規化することで受信したブロック サイズを考慮します。システムは、ワークロードに応じてこのブロック サイズを増やすことがあります。ブロック サイズが大きくなると、システムはそのブロック サイズを処理するために必要なレベルまで帯域幅を増やします。帯域幅が増えると、システムが処理可能なIOPSは減少します。

QoSパフォーマンス曲線は、ブロック サイズの増大とIOPSの割合の減少の関係を示しています。



たとえば、ブロック サイズが4kで帯域幅が4000KBpsであれば、IOPSは1000です。ブロック サイズが8kに増え、帯域幅が5000KBpsに増えると、IOPSは625まで減少します。ブロック サイズを考慮することで、ブロック サイズが大きく優先度の低いワークロード（バックアップやハイパーバイザーの処理など）によって、ブロック サイズが小さく優先度の高いトラフィックで必要とされるパフォーマンスが大きな影響を受けないよう調整されます。

QoSポリシー

標準的なサービス品質（QoS）設定をQoSポリシーとして作成および保存して、複数のボリュームに適用することができます。タブQoS PoliciesのページManagementから QoS ポリシーを作成、編集、および削除できます。

注 : QoS ポリシーを使用している場合は、ボリュームでカスタム QoS を使用しないでください。カスタム QoS は、ボリューム QoS 設定の QoS ポリシー値を上書きおよび調整します。

ネットアップのビデオ*: SolidFire Quality of Service Policies*

関連タスク

*QoS*ポリシーの作成（84ページ）
QoSポリシーを作成し、ボリュームの作成時に適用することができます。

*QoS*ポリシーの編集（85ページ）
既存のQoSポリシーの名前を変更したり、ポリシーに関連付けられている値を編集したりできます。QoSポリシーの変更は、そのポリシーに関連付けられているすべてのボリュームに反映されます。

*QoS*ポリシーの削除（85ページ）
不要になったQoSポリシーを削除できます。QoSポリシーを削除すると、そのポリシーに関連付けられているすべてのボリュームのQoS設定は維持されますが、ポリシーとの関連付けは解除されます。

QoSポリシーの作成

QoSポリシーを作成し、ボリュームの作成時に適用することができます。

手順

1. **[Management]** > **[QoS Policies]**の順に選択します。
2. **[Create QoS Policy]**をクリックします。
3. **[Policy Name]**を入力します。
4. **[Min IOPS]**、**[Max IOPS]**、および**[Burst IOPS]**の値を入力します。
5. **[Create QoS Policy]**をクリックします。

QoSポリシーの詳細

[Management]タブで、QoSポリシーの詳細を確認できます。

ID

システムによって生成されたQoSポリシーのID。

Name

ユーザが定義したQoSポリシーの名前。

Min IOPS

ボリュームに対して保証されている最小IOPS。

Max IOPS

ボリュームに対して許可されている最大IOPS。

Burst IOPS

ボリュームに対して短期間で許可されている最大IOPS。デフォルト値は15,000です。

Volumes

ポリシーを使用しているボリュームの数。数字をクリックすると、ポリシーが適用されたボリュームのリストが表示されます。

QoSポリシーの編集

既存のQoSポリシーの名前を変更したり、ポリシーに関連付けられている値を編集したりできます。QoSポリシーの変更は、そのポリシーに関連付けられているすべてのボリュームに反映されます。

手順

1. **[Management]** > **[QoS Policies]**の順に選択します。
2. 編集するQoSポリシーの[Actions]アイコンをクリックします。
3. 表示されたメニューで**[Edit]**を選択します。
4. **[Edit QoS Policy]**ダイアログ ボックスで、次のプロパティを必要に応じて変更します。
   - Policy Name
   - Min IOPS
   - Max IOPS
   - Burst IOPS
5. **[Save Changes]**をクリックします。

QoSポリシーの削除

不要になったQoSポリシーを削除できます。QoSポリシーを削除すると、そのポリシーに関連付けられているすべてのボリュームのQoS設定は維持されますが、ポリシーとの関連付けは解除されます。

タスク概要

注 : ボリュームと QoS ポリシーの関連付けを解除しようとする場合は、そのボリュームの QoS 設定をカスタムに変更できます。

手順

1. **Management** > **QoS Policies**の順に選択します。
2. 削除する QoS ポリシーの Actions アイコンをクリックします。
3. 表示されるメニューで**Delete**、を選択します。
4. 操作を確定します。

関連タスク

ボリュームの*QoS*ポリシーの関連付けの解除（92ページ）

カスタムのQoS設定を選択することで、ボリュームのQoSポリシーの関連付けを解除できます。

ボリュームの作成

ボリュームを作成して、特定のアカウントに関連付けることができます。すべてのボリュームをアカウントに関連付ける必要があります。この関連付けにより、アカウントは、iSCSIイニシエータ経由でCHAPクレデンシャルを使用してボリュームにアクセスできます。

タスク概要

作成中に、ボリュームのQoS設定を指定できます。

手順

1. **[Management]** > **[Volumes]**の順に選択します。
2. **[Create Volume]**をクリックします。
3. **[Create a New Volume]**ダイアログ ボックスで、**[Volume Name]**にボリューム名を入力します。
4. ボリュームの合計サイズを入力します。

   注 : デフォルトのボリューム サイズの単位はGBです。GBまたはGiB単位のサイズを使用してボリュームを作成できます。

   - 1GB=1,000,000,000バイト
   - 1GiB=1,073,741,824バイト

5. ボリュームの**ブロック サイズ**を選択します。
6. **[Account]**ドロップダウン リストをクリックし、ボリュームへのアクセスを許可するアカウントを選択します。

   アカウントが存在しない場合は、**[Create Account]**リンクをクリックし、新しいアカウント名を入力して**[Create]**をクリックします。アカウントが作成され、新しいボリュームに関連付けられます。

   注 : アカウント数が50個を超える場合、リストは表示されません。名前の先頭部分を入力すると、オートコンプリート機能によって、候補が表示されます。

7. **[Quality of Service]**で、次のいずれかを実行します。
   1. **[Policy]**で、既存のQoSポリシーを選択します。
   2. **[Custom Settings]**で、IOPSの最小値、最大値、およびバースト値をカスタマイズするか、デフォルトのQoS値を使用します。

      最大IOPSまたはバーストIOPSの値が20,000 IOPSを超える場合、単一のボリュームでこのレベルのIOPSを実現するには、キュー深度を深くするか、複数のセッションが必要になる場合があります。
8. **[Create Volume]**をクリックします。

ボリュームの詳細

[Management]タブの[Volumes]ページには、アクティブ ボリュームの情報（名前、アカウント、関連付けられているアクセス グループ、サイズなど）が表示されます。

ID

システムによって生成されたボリュームのID。

Name

ボリュームの作成時に指定した名前。

Account

ボリュームに割り当てられているアカウントの名前。

Access Groups

ボリューム アクセス グループまたはボリュームが所属するグループの名前。

Access

ボリュームの作成時に割り当てられたアクセスのタイプ。有効な値は次のとおりです。

- Read / Write：すべての読み取りと書き込みが許可されます。
- Read Only：すべての読み取りが許可されます。書き込みは許可されません。

- Locked：管理者アクセスのみが許可されます。
- ReplicationTarget：レプリケートされたボリューム ペアのターゲット ボリューム として指定されています。

Used

ボリューム内の使用済みスペースのパーセンテージ。

Size

ボリュームの合計サイズ（GB）。

Snapshots

ボリュームに対して作成されたSnapshotの数。

QoS Policy

ユーザが定義したQoSポリシーの名前とリンク。

Min IOPS

ボリュームに対して保証されている最小IOPS。

Max IOPS

ボリュームに対して許可されている最大IOPS。

Burst IOPS

ボリュームに対して短期間で許可されている最大IOPS。デフォルト値は15,000です。

Attributes

APIメソッドを使用してキーと値のペアとしてボリュームに割り当てられている属性。

512e

ボリュームで512eが有効になっているかどうか。有効な値は次のとおりです。

- Yes
- No

Created On

ボリュームが作成された日時。

個々のボリュームのパフォーマンスの詳細の表示

個々のボリュームのパフォーマンス統計を表示できます。

手順

1. **[Reporting]** > **[Volume Performance]**の順に選択します。
2. ボリューム リストで、ボリュームの[Actions]アイコンをクリックします。
3. **[View Details]**をクリックします。
   ボリュームの一般的な情報がページの下部に表示されます。
4. ボリュームの詳細を確認するには、**[See More Details]**をクリックします。
   ボリュームの詳細情報とパフォーマンス グラフが表示されます。

アクティブ ボリュームの編集

QoS値、ボリュームのサイズ、バイト値の算出単位など、ボリュームの属性を変更できます。レプリケーションで使用するため、またはボリュームへのアクセスを制限するために、アカウント アクセスを変更することもできます。

タスク概要

次の状況下でクラスタに十分なスペースがある場合は、ボリュームのサイズを変更できます。

- 正常な動作状態。
- ボリュームのエラーまたは障害が報告されている。
- ボリュームのクローニング中。
- ボリュームの再同期中。

手順

1. **Management** > **Volumes**の順に選択します。
2. **Active**ウィンドウで、編集するボリュームのアクションアイコンをクリックします。
3. **Edit**をクリックします。
4. オプション: ボリュームの合計サイズを変更します。

   注 :

   - ボリュームのサイズは、増やすことはできますが、減らすことはできません。1回の処理でサイズ変更できるのは、1つのボリュームのみです。ガベージ コレクションやソフトウェアのアップグレードを実行しても、サイズ変更処理は中断されません。
   - レプリケーション用にボリューム サイズを調整するときは、レプリケーション ターゲットとして割り当てられているボリュームのサイズを先に拡張する必要があります。次に、ソース ボリュームのサイズを変更します。ターゲット ボリュームのサイズは、ソース ボリュームと同じかそれ以上にすることはできますが、ソース ボリュームより小さくすることはできません。

   注 : デフォルトのボリューム サイズの単位はGBです。GBまたはGiB単位のサイズを使用してボリュームを作成できます。

   - 1GB=1,000,000,000バイト
   - 1GiB=1,073,741,824バイト

5. オプション: 別のアカウント アクセス レベルを選択します。次のいずれかを選択できます。
   - Read Only
   - Read/Write
   - Locked
   - Replication Target
6. オプション: ボリュームへのアクセスを許可するアカウントを選択します。

   アカウントが存在**Create AccountCreate**しない場合は、リンクをクリックし、新しいアカウント名を入力して、をクリックします。アカウントが作成され、ボリュームに関連付けられます。

   注 : アカウント数が50個を超える場合、リストは表示されません。名前の先頭部分を入力すると、オートコンプリート機能によって、候補が表示されます。

7. オプション: で選択を変更する**Quality of Service**には、次のいずれかの操作を行います。
   1. で**Policy**は、既存の QoS ポリシーがある場合は、そのポリシーを選択できます。
   2. で**Custom Settings**、 IOPS のカスタマイズされた最小値、最大値、およびバースト値を設定するか、デフォルトの QoS 値を使用します。

注 : ボリュームで QoS ポリシーを使用している場合は、カスタム QoS を設定して、ボリュームとの QoS ポリシーの関係を削除できます。カスタム QoS は、ボリューム QoS 設定の QoS ポリシー値を上書きおよび調整します。

ヒント : IOPSの値は、10または100単位で増減する必要があります。また、有効な整数を入力する必要があります。

ヒント : ボリュームのバースト値はできるだけ高くします。バースト値を非常に高く設定することで、たまに発生する大規模ブロックのシーケンシャル ワークロードを迅速に処理できる一方で、平常時のIOPSは引き続き抑制することができます。

8. **Save Changes**をクリックします。

ボリュームの削除

エレメントストレージクラスタから 1 つ以上のボリュームを削除できます。

タスク概要

削除されたボリュームはすぐにはパージされず、約8時間は使用可能な状態です。この間にリストアしたボリュームはオンラインに戻り、iSCSI接続が再度確立されます。

Snapshotの作成に使用されたボリュームを削除すると、関連するSnapshotは非アクティブになります。削除したソース ボリュームがパージされると、関連する非アクティブなSnapshotもシステムから削除されます。

注意 : 管理サービスに関連付けられた永続ボリュームは、インストール時またはアップグレード時に作成され、新しいアカウントに割り当てられます。永続ボリュームを使用している場合は、ボリュームまたは関連するアカウントを変更または削除しないでください。

手順

1. **Management** > **Volumes**の順に選択します。
2. 単一のボリュームを削除するには、次の手順を実行します。
   1. 削除するボリュームの[Actions]アイコンをクリックします。
   2. 表示されるメニューで**Delete**、をクリックします。
   3. 操作を確定します。

   ボリュームが**DeletedVolumes**ページの領域に移動します。
3. 複数のボリュームを削除するには、次の手順を実行します。
   1. ボリュームのリストで、削除するボリュームの横のボックスをオンにします。
   2. **Bulk Actions**をクリックします。
   3. 表示されるメニューで**Delete**、をクリックします。
   4. 操作を確定します。
      ボリュームが**DeletedVolumes**ページの領域に移動します。

削除したボリュームのリストア

システムから削除したボリュームは、パージされていなければリストアできます。削除したボリュームは約8時間後に自動的にパージされます。パージ済みのボリュームはリストアできません。

手順

1. **[Management]** > **[Volumes]**の順に選択します。
2. **[Deleted]**タブをクリックして、削除したボリュームを表示します。
3. リストアするボリュームの[Actions]アイコンをクリックします。
4. 表示されたメニューで**[Restore]**をクリックします。
5. 操作を確定します。
   ボリュームが**[Active]**ボリューム リストに配置され、ボリュームへのiSCSI接続がリストアされます。

ボリュームのパージ

パージしたボリュームは、システムから完全に削除されます。ボリューム内のデータはすべて失われます。

タスク概要

削除したボリュームは、8時間後に自動的にパージされます。ただし、スケジュールされている時刻より前にボリュームをパージすることも可能です。

手順

1. **[Management]** > **[Volumes]**の順に選択します。
2. **[Deleted]**ボタンをクリックします。
3. 次の手順を実行して、単一のボリュームまたは複数のボリュームをパージします。

オプション	手順
単一のボリュームのパージ	1. パージするボリュームの[Actions]アイコンをクリックします。 2. **[Purge]**をクリックします。 3. 操作を確定します。
複数のボリュームのパージ	1. パージするボリュームを選択します。 2. **[Bulk Actions]**をクリックします。 3. 表示されたメニューで**[Purge]**を選択します。 4. 操作を確定します。

ボリュームのクローニング

単一のボリュームまたは複数のボリュームのクローンを作成して、データのポイントインタイム コピーを作成できます。ボリュームをクローニングすると、ボリュームのSnapshotが作成され、次にそのSnapshotが参照しているデータのコピーが作成されます。これは非同期のプロセスであり、クローニングするボリュームのサイズおよび現在のクラスタの負荷によって所要時間が異なります。

タスク概要

クラスタでは、ボリューム1個につき一度に実行できるクローン要求は最大2つ、アクティブなボリュームのクローン処理は最大8件までサポートされます。これらの制限を超える要求はキューに登録され、あとから処理されます。

注 : オペレーティングシステムは、クローンボリュームの処理方法が異なります。VMware ESXi は、クローンボリュームをボリュームコピーまたはスナップショットボリュームとして処理します。ボリュームは、新しいデータストアの作成に使用できるデバイスになります。クローンボリュームのマウントと Snapshot LUN の処理の詳細については、 VMFS データストアコピーのマウントと重複する VMFS データストアの管理に関する VMware のドキュメントを参照してください。 .

注意 : 小さいサイズにクローニングすることによってクローン ボリュームのサイズを切り詰める場合は、小さいボリュームに収まるように事前にパーティションを準備してください。

手順

1. **Management** > **Volumes**の順に選択します。
2. 単一のボリュームをクローニングするには、次の手順を実行します。
   1. **Active**ページのボリュームのリストで、クローニングするボリュームの Actions アイコンをクリックします。
   2. 表示されるメニューで**Clone**、をクリックします。
   3. **Clone Volume**ウィンドウで、新しくクローニングされたボリュームのボリューム名を入力します。
   4. **Volume Size**スピンボックスとリストを使用して、ボリュームのサイズと測定値を選択します。

      注 : デフォルトのボリューム サイズの単位はGBです。GBまたはGiB単位のサイズを使用してボリュームを作成できます。

      - 1GB=1,000,000,000バイト
      - 1GiB=1,073,741,824バイト

   5. 新しいクローン ボリュームのアクセスのタイプを選択します。
   6. **Account**新しくクローンされたボリュームに関連付けるアカウントをリストから選択します。

      注 : Create Account リンクをクリック**Create**してアカウント名を入力し、をクリックすると、この手順でアカウントを作成できます。アカウント**Account**を作成すると、アカウントが自動的にリストに追加されます。
3. 複数のボリュームをクローニングするには、次の手順を実行します。
   1. **Active**ページのボリュームのリストで、クローニングするボリュームの横にあるチェックボックスをオンにします。
   2. **Bulk Actions**をクリックします。
   3. 表示されるメニューで**Clone**、を選択します。
   4. **Clone Multiple Volumes**ダイアログボックス**New Volume Name Prefix**で、複製されたボリュームのプレフィックスをフィールドに入力します。
   5. クローンボリュームに関連付けるアカウント**Account**をリストから選択します。
   6. クローン ボリュームのアクセスのタイプを選択します。
4. **Start Cloning**をクリックします。

   注 : クローンのボリューム サイズを拡張すると、末尾に空きスペースが追加された新しいボリュームが作成されます。ボリュームの使用方法によっては、新しい空きスペースを使用するために、空きスペースでパーティションの拡張または新しいパーティションの作成が必要になる場合があります。

Fibre Channelボリュームへの LUNの割り当て

ボリューム アクセス グループ内のFibre Channelボリュームに対するLUNの割り当てを変更できます。ボリューム アクセス グループを作成する際に、Fibre Channelボリュームに LUNを割り当てることもできます。

タスク概要

新しいFibre Channel LUNの割り当ては高度な機能であり、接続しているホストで想定外の状況が生じる可能性があります。たとえば、新しいLUN IDを自動的に検出できないホストでは、新しいLUN IDを検出するために再スキャンが必要となります。

手順

1. **[Management]** > **[Access Groups]**の順に選択します。
2. 編集するアクセス グループの[Actions]アイコンをクリックします。
3. 表示されたメニューで**[Edit]**を選択します。
4. **[Edit Volume Access Group]**ダイアログ ボックスの**[Assign LUN IDs]**で、**[LUN Assignments]**リストの矢印をクリックします。
5. LUNを割り当てるリスト内の各ボリュームの**[LUN]**フィールドに、新しい値を入力します。
6. **[Save Changes]**をクリックします。

ボリュームへのQoSポリシーの適用

既存のQoSポリシーを1つ以上のボリュームに一括して適用できます。

開始する前に

一括して適用するQoSポリシーを用意しておきます。

手順

1. **[Management]** > **[Volumes]**の順に選択します。
2. ボリュームのリストで、QoSポリシーを適用するボリュームの横のボックスをオンにします。
3. **[Bulk Actions]**をクリックします。
4. 表示されたメニューで**[Apply QoS Policy]**をクリックします。
5. ドロップダウン リストからQoSポリシーを選択します。
6. **[Apply]**をクリックします。

関連概念

*QoS*ポリシー（84ページ）

標準的なサービス品質（QoS）設定をQoSポリシーとして作成および保存して、複数のボリュームに適用することができます。タブQoS PoliciesのページManagementから QoS ポリシーを作成、編集、および削除できます。

ボリュームのQoSポリシーの関連付けの解除

カスタムのQoS設定を選択することで、ボリュームのQoSポリシーの関連付けを解除できます。

開始する前に

変更するボリュームにQoSポリシーが関連付けられていることが前提です。

手順

1. **[Management]** > **[Volumes]**の順に選択します。

2. 変更するQoSポリシーが含まれているボリュームの[Actions]アイコンをクリックします。
3. **[Edit]**をクリックします。
4. 表示されたメニューで、**[Quality of Service]**の**[Custom Settings]**をクリックします。
5. **[Min IOPS]**、**[Max IOPS]**、および**[Burst IOPS]**の値を変更するか、デフォルトの設定のままにします。
6. **[Save Changes]**をクリックします。

関連タスク

*QoS*ポリシーの削除（85ページ）

不要になったQoSポリシーを削除できます。QoSポリシーを削除すると、そのポリシーに関連付けられているすべてのボリュームのQoS設定は維持されますが、ポリシーとの関連付けは解除されます。

仮想ボリュームの使用

Element UIを使用して、仮想ボリュームおよび仮想ボリュームに関連付けられたストレージ コンテナ、プロトコル エンドポイント、バインド、およびホストの情報を確認し、タスクを実行できます。

Virtual Volumes（VVol）機能は、NetApp Elementソフトウェア ストレージ システムの出荷時点では無効になっています。Element UIで、vSphere VVol機能を手動で有効にする必要があります（この操作は1度だけ実行します）。

VVol機能を有効にすると、ユーザ インターフェイスに［VVols］タブが表示されて、VVolに関連する監視オプションと一部の管理オプションを選択できるようになります。また、ストレージ側のソフトウェア コンポーネント（VASA Provider）が、vSphereのストレージ認識サービスとして機能します。ほとんどのVVolコマンド（VVolの作成、クローニング、編集など）は、vCenter ServerまたはESXiホストによって開始され、VASA ProviderによってElementソフトウェア ストレージ システム用のElement APIに変換されます。ストレージ コンテナの作成、削除、管理および仮想ボリュームの削除を実行するコマンドは、Element UIを使用して開始できます。

Elementソフトウェア ストレージ システムでVirtual Volumes（VVol）機能を使用するために必要な設定の大部分は、vSphereで行います。vCenterへのVASA Providerの登録、VVolデータストアの作成と管理、およびポリシーに基づくストレージの管理を実行するには、*VMware vSphere Virtual Volumes for SolidFire Storage Configuration Guide*を参照してください。

注 : VASA Provider を vCenter にすでに登録している場合は、複数の vCenter 向けの VASA サポートをアップグレードパッチとして利用できます。 インストールするにネットアップElementは、 VASA 39 マニフェストの指示に従って、 NetApp ソフトウェアダウンロードサイトから .tar.gz ファイルをダウンロードします。 NetApp Element VASA Provider は、 NetApp 証明書を使用します。 このパッチでは、 VASA および VVol で使用する複数の vCenter をサポートするために、証明書は vCenter によって変更されずに使用されます。 証明書は変更しないでください。 カスタム SSL 証明書は VASA ではサポートされていません。

関連概念

プロトコル エンドポイント（101ページ）

プロトコル エンドポイントは、ホストがNetApp Elementソフトウェアを実行しているクラスタ上のストレージに対処する際に使用するアクセス ポイントです。ユーザがプロトコル エンドポイントを削除または変更することはできません。プロトコル エンドポイントはアカウントには関連付けられず、またボリューム アクセス グループに追加することはできません。

バインド（102ページ）
仮想ボリュームを使用してI/O処理を実行するには、最初にESXiホストから仮想ボリュームをバインドする必要があります。

関連タスク

*Virtual Volumes*の有効化（94ページ）
NetApp Elementソフトウェアを使用して、vSphere Virtual Volumes（VVol）機能を手動で有効にする必要があります。Elementソフトウェア システムの VVol機能はデフォルトでは無効になっており、新規インストール時やアップグレード時に自動的に有効になることはありません。VVol機能の有効化は1度だけ実行します。

仮想ボリュームの削除（98ページ）
仮想ボリュームの削除は必ずVMware管理レイヤから実行する必要がありますが、仮想ボリュームを削除する機能自体はElement UIから有効にします。vSphereがSolidFireストレージ上の仮想ボリュームをクリーンアップできない場合など、どうしても必要な場合以外は、Element UIから仮想ボリュームを削除しないでください。

ストレージ コンテナの作成（99ページ）
Elementでストレージ コンテナを作成し、vCenterで検出できます。VVolを使用する仮想マシンのプロビジョニングを開始するためには、少なくとも1つのストレージ コンテナを作成する必要があります。

ストレージ コンテナの編集（100ページ）
Element UIでストレージ コンテナのCHAP認証を変更できます。

ストレージ コンテナの削除（101ページ）
Element UIからストレージ コンテナを削除できます。

関連資料

ホストの詳細（102ページ）
[VVols]タブの[Hosts]ページには、仮想ボリュームをホストしているVMware ESXiホストに関する情報が表示されます。

Virtual Volumesの有効化

NetApp Elementソフトウェアを使用して、vSphere Virtual Volumes（VVol）機能を手動で有効にする必要があります。Elementソフトウェア システムの VVol機能はデフォルトでは無効になっており、新規インストール時やアップグレード時に自動的に有効になることはありません。VVol機能の有効化は1度だけ実行します。

開始する前に

- クラスタでElement 9.0以降が実行されている必要があります。
- クラスタがVVolに対応したESXi 6.0以降の環境に接続されている必要があります。
- Element 11.3以降を使用している場合は、クラスタをESXi 6.0 Update 3以降の環境に接続する必要があります。

タスク概要

注意 : vSphere Virtual Volumes機能を有効にすると、Elementソフトウェアの設定が永続的に変更されます。クラスタがVMware ESXi VVolに対応した環境に接続されている場合にのみ、VVol機能を有効にしてください。VVol機能を無効にしてデフォルト設定に戻すには、クラスタを工場出荷時のイメージに戻す必要があります。これにより、システム上のデータがすべて削除されます。

手順

1. **[Clusters]** > **[Settings]**の順に選択します。
2. Virtual Volumes用のクラスタ固有の設定を探します。
3. **[Enable Virtual Volumes]**をクリックします。
4. **[Yes]**をクリックして、Virtual Volumes設定の変更を確定します。
   Element UIに**[VVols]**タブが表示されます。

   注 : VVol機能を有効にすると、SolidFireクラスタはVASA Providerを起動してVASAトラフィック用のポート8444を開き、vCenterおよびすべてのESXiホストから検出可能なプロトコル エンドポイントを作成します。
5. **[Clusters]** > **[Settings]**で、Virtual Volumes（VVol）設定からVASA ProviderのURLをコピーします。このURLは、VASA ProviderをvCenterに登録する際に使用します。
6. **[VVols]** > **[Storage Containers]**でストレージ コンテナを作成します.

   注 : VVolデータストアに対してVMをプロビジョニングできるようにするには、ストレージ コンテナを少なくとも1つ作成する必要があります。
7. **[VVols]** > **[Protocol Endpoints]**の順に選択します。
8. クラスタ内のノードごとにプロトコル エンドポイントが作成されていることを確認します。

   注 : vSphereで追加の設定が必要です。vCenterへのVASA Providerの登録、VVolデータストアの作成と管理、およびポリシーに基づくストレージの管理を実行するには、*VMware vSphere Virtual Volumes for SolidFire Storage Configuration Guide*を参照してください。

関連情報

VMware vSphere Virtual Volumes for SolidFire Storage Configuration Guide

仮想ボリュームの詳細の表示

Element UIでは、クラスタ上のすべてのアクティブな仮想ボリュームに関する情報を確認できます。また、各仮想ボリュームのパフォーマンス アクティビティ（入力、出力、スループット、レイテンシ、キュー深度、ボリューム情報など）を表示することもできます。

開始する前に

- クラスタのElement UIでVVol機能を有効にしておきます。
- 関連するストレージ コンテナを作成しておく必要があります。
- Elementソフトウェアの VVol機能を使用するようにvSphereクラスタを設定しておきます。
- vSphereで少なくとも1つのVMを作成しておきます。

手順

1. **[VVols]** > **[Virtual Volumes]**の順にクリックします。
   すべてのアクティブな仮想ボリュームに関する情報が表示されます。
2. 確認する仮想ボリュームの[Actions]アイコンをクリックします。
3. 表示されたメニューで**[View Details]**を選択します。

仮想ボリュームの詳細

[VVols]タブの[Virtual Volumes]ページには、クラスタ上のアクティブな仮想ボリュームごとに、ボリュームID、Snapshot ID、親仮想ボリュームID、仮想ボリュームIDなどの情報が表示されます。

Volume ID

基盤となるボリュームのID。

Snapshot ID

基盤となるボリュームSnapshotのID。仮想ボリュームがSolidFire Snapshotではない場合、値は0です。

Parent Virtual Volume ID

親仮想ボリュームの仮想ボリュームID。このIDがゼロの場合、仮想ボリュームは独立しており、親ボリュームへのリンクはありません。

Virtual Volume ID

仮想ボリュームのUUID。

Name

仮想ボリュームに割り当てられている名前。

Storage Container

仮想ボリュームを所有するストレージ コンテナ。

Guest OS Type

仮想ボリュームに関連付けられたオペレーティング システム。

Virtual Volume Type

仮想ボリュームのタイプ（Config、Data、Memory、Swap、またはOther）。

Access

仮想ボリュームに割り当てられている読み取り / 書き込み権限。

Size

仮想ボリュームのサイズ（GBまたはGiB）。

Snapshots

関連付けられているSnapshotの数。数値をクリックすると、Snapshotの詳細が表示されます。

Min IOPS

仮想ボリュームのQoS設定 - 最小IOPS。

Max IOPS

仮想ボリュームのQoS設定 - 最大IOPS。

Burst IOPS

仮想ボリュームのQoS設定 - バーストIOPS。

VMW_VmID

「VMW_」で始まるフィールド内の情報は、VMwareによって定義されます。

Create Time

仮想ボリュームの作成タスクが完了した時刻。

個々の仮想ボリュームの詳細

[VVols]タブの[Virtual Volumes]ページでは、仮想ボリュームを個別に選択してその詳細を表示し、次の仮想ボリューム情報を確認できます。

VMW_XXX

「VMW_」で始まるフィールド内の情報は、VMwareによって定義されます。

Parent Virtual Volume ID

親仮想ボリュームの仮想ボリュームID。このIDがゼロの場合、仮想ボリュームは独立しており、親ボリュームへのリンクはありません。

Virtual Volume ID

仮想ボリュームのUUID。

Virtual Volume Type

仮想ボリュームのタイプ（Config、Data、Memory、Swap、またはOther）。

Volume ID

基盤となるボリュームのID。

Access

仮想ボリュームに割り当てられている読み取り / 書き込み権限。

Account Name

ボリュームが含まれているアカウントの名前。

Access Groups

関連付けられているボリューム アクセス グループ。

Total Volume Size

プロビジョニング済み容量の合計（バイト）。

Non-Zero Blocks

前回のガベージ コレクション完了後、データが含まれる4KiBブロックの総数。

Zero Blocks

前回のガベージ コレクション完了後、データが含まれない4KiBブロックの総数。

Snapshots

関連付けられているSnapshotの数。数値をクリックすると、Snapshotの詳細が表示されます。

Min IOPS

仮想ボリュームのQoS設定 - 最小IOPS。

Max IOPS

仮想ボリュームのQoS設定 - 最大IOPS。

Burst IOPS

仮想ボリュームのQoS設定 - バーストIOPS。

Enable 512

仮想ボリュームは常に512バイトのブロック サイズのエミュレーションを使用するため、設定は常にyesです。

Volumes Paired

ボリュームがペアリングされているかどうか。

Create Time

仮想ボリュームの作成タスクが完了した時刻。

Blocks Size

ボリューム上のブロックのサイズ。

Unaligned Writes

512eボリュームの場合、4kセクターの境界に沿っていない書き込み処理の数。アラインしていない書き込みが多数ある場合は、パーティションのアライメントが適切でない可能性があります。

Unaligned Reads

512eボリュームの場合、4kセクターの境界に沿っていない読み取り処理の数。アラインされていない読み取りが多数ある場合は、パーティションのアライメントが適切でない可能性があります。

scsiEUIDeviceID

ボリュームのSCSIデバイスのグローバル一意識別子（EUI-64ベースの16バイト形式）。

scsiNAADeviceID

ボリュームのSCSIデバイスのグローバル一意識別子（NAA IEEE Registered Extended形式）。

Attributes

JSONオブジェクト形式の名前と値のペアのリスト。

仮想ボリュームの削除

仮想ボリュームの削除は必ずVMware管理レイヤから実行する必要がありますが、仮想ボリュームを削除する機能自体はElement UIから有効にします。vSphereがSolidFireストレージ上の仮想ボリュームをクリーンアップできない場合など、どうしても必要な場合以外は、Element UIから仮想ボリュームを削除しないでください。

手順

1. **[VVols]** > **[Virtual Volumes]**の順に選択します。
2. 削除する仮想ボリュームの[Actions]アイコンをクリックします。
3. 表示されたメニューで**[Delete]**を選択します。

注意 : 削除される前に仮想ボリュームのバインドが正しく解除されるよう、仮想ボリュームはVMware管理レイヤから削除する必要があります。vSphereがSolidFireストレージ上の仮想ボリュームをクリーンアップできない場合など、どうしても必要な場合以外は、Element UIから仮想ボリュームを削除しないでください。Element UIから仮想ボリュームを削除すると、ボリュームはただちにパージされます。

4. 操作を確定します。
5. 仮想ボリュームのリストを更新して、仮想ボリュームが削除されたことを確認します。
6. オプション: **[Reporting]** > **[Event Log]**の順に選択して、パージが成功したことを確認します。

ストレージ コンテナ

ストレージ コンテナはvSphereのデータストアに相当し、Elementソフトウェアを実行するクラスタ上に作成されます。

作成されたストレージ コンテナはNetApp Elementアカウントに関連付けられます。Elementストレージ上に作成されたストレージ コンテナは、vCenterおよびESXiではvSphereデータストアとして表示されます。ストレージ コンテナにはElementストレージのスペースはいっさい割り当てられず、 単に仮想ボリュームを論理的に関連付けるために使用されます。

クラスタごとに最大4つのストレージ コンテナがサポートされます。VVol機能を有効にするには、少なくとも1つのストレージ コンテナが必要です。

ストレージ コンテナの作成

Elementでストレージ コンテナを作成し、vCenterで検出できます。VVolを使用する仮想マシンのプロビジョニングを開始するためには、少なくとも1つのストレージ コンテナを作成する必要があります。

開始する前に

クラスタのElement UIでVVol機能を有効にしておきます。

手順

1. **[VVols]** > **[Storage Containers]**の順に選択します。
2. **[Create Storage Containers]**ボタンをクリックします。
3. **[Create a New Storage Container]**ダイアログ ボックスにストレージ コンテナ情報を入力します。
   1. ストレージ コンテナの名前を入力します。
   2. CHAP用のイニシエータ シークレットとターゲット シークレットを設定します。

      ヒント : シークレットを自動生成する場合は、[CHAP Settings]フィールドを空白のままにしてください。

   3. **[Create Storage Container]**ボタンをクリックします。
4. 新しいストレージ コンテナが**[Storage Containers]**サブタブのリストに表示されていることを確認します。

   注 : NetApp ElementアカウントIDは自動的に作成されてストレージ コンテナに割り当てられるため、アカウントを手動で作成する必要はありません。

ストレージ コンテナの詳細

[VVols]タブの[Storage Containers]ページでは、クラスタ上のすべてのアクティブなストレージ コンテナに関する情報を確認できます。

Account ID

ストレージ コンテナに関連付けられたNetApp ElementアカウントのID。

Name

ストレージ コンテナの名前。

Status

ストレージ コンテナのステータス。有効な値は次のとおりです。

- `Active`：ストレージ コンテナは使用中です。
- `Locked`：ストレージ コンテナはロックされています。

PE Type
プロトコル エンドポイントのタイプ（Elementソフトウェアで使用可能なプロトコルはSCSIのみです）。

Storage Container ID
仮想ボリュームのストレージ コンテナのUUID。

Active Virtual Volumes
ストレージ コンテナに関連付けられたアクティブな仮想ボリュームの数。

個々のストレージ コンテナの詳細

[VVols]タブの[Storage Containers]ページでは、ストレージ コンテナを個別に選択してその情報を確認できます。

Account ID
ストレージ コンテナに関連付けられたNetApp ElementアカウントのID。

Name
ストレージ コンテナの名前。

Status
ストレージ コンテナのステータス。有効な値は次のとおりです。

- `Active`：ストレージ コンテナは使用中です。
- `Locked`：ストレージ コンテナはロックされています。

Chap Initiator Secret
イニシエータの一意のCHAPシークレット。

Chap Target Secret
ターゲットの一意のCHAPシークレット。

Storage Container ID
仮想ボリュームのストレージ コンテナのUUID。

Protocol Endpoint Type
プロトコル エンドポイントのタイプを示します（使用可能なプロトコルはSCSIのみです）。

ストレージ コンテナの編集

Element UIでストレージ コンテナのCHAP認証を変更できます。

手順

1. **[VVols]** > **[Storage Containers]**の順に選択します。
2. 編集するストレージ コンテナの[Actions]アイコンをクリックします。
3. 表示されたメニューで**[Edit]**を選択します。
4. [CHAP Settings]の[Initiator Secret]および[Target Secret]で、認証に使用するクレデンシャルを編集します。

   ヒント： [CHAP Settings]を変更しない場合、同じクレデンシャルが使用されます。クレデンシャルのフィールドを空白にすると、新しいシークレットがシステムによって自動生成されます。

5. **[Save Changes]**をクリックします。

ストレージ コンテナの削除

Element UIからストレージ コンテナを削除できます。

開始する前に

すべての仮想マシンをVVolデータストアから削除しておく必要があります。

手順

1. **[VVols]** > **[Storage Containers]**の順に選択します。
2. 削除するストレージ コンテナの[Actions]アイコンをクリックします。
3. 表示されたメニューで**[Delete]**を選択します。
4. 操作を確定します。
5. **[Storage Containers]**サブタブでストレージ コンテナのリストを更新して、ストレージ コンテナが削除されていることを確認します。

プロトコル エンドポイント

プロトコル エンドポイントは、ホストがNetApp Elementソフトウェアを実行しているクラスタ上のストレージに対処する際に使用するアクセス ポイントです。ユーザがプロトコル エンドポイントを削除または変更することはできません。プロトコル エンドポイントはアカウントには関連付けられず、またボリューム アクセス グループに追加することはできません。

Elementソフトウェアを実行しているクラスタでは、クラスタ内のストレージ ノードごとに1つのプロトコル エンドポイントが自動的に作成されます。たとえば、6ノードのストレージ クラスタでは、6つのプロトコル エンドポイントが作成されて各ESXiホストにマッピングされます。プロトコル エンドポイントはElementソフトウェアによって動的に管理され、必要に応じて手動操作なしに作成、移動、または削除されます。プロトコル エンドポイントはマルチパスのターゲットであり、補助LUNのI/Oプロキシとして機能します。各プロトコル エンドポイントは、標準のiSCSIターゲットと同様に、利用可能なSCSIアドレスを使用します。プロトコル エンドポイントは、vSphere Clientでは単一ブロック（512バイト）のストレージ デバイスとして表示されますが、このストレージ デバイスをストレージとしてフォーマットしたり使用したりすることはできません。

サポートされるプロトコルはiSCSIだけです。Fibre Channelプロトコルはサポートされません。

プロトコル エンドポイントの詳細

[VVols]タブの[Protocol Endpoints]ページには、プロトコル エンドポイントの情報が表示されます。

Primary Provider ID

プライマリ プロトコル エンドポイント プロバイダのID。

Secondary Provider ID

セカンダリ プロトコル エンドポイント プロバイダのID。

Protocol Endpoint ID

プロトコル エンドポイントのUUID。

Protocol Endpoint State

プロトコル エンドポイントのステータス。有効な値は次のとおりです。

- `Active`：プロトコル エンドポイントは使用中です。
- `Start`：プロトコル エンドポイントは起動中です。
- `Failover`：プロトコル エンドポイントはフェイルオーバーしました。

- `Reserved`：プロトコル エンドポイントはリザーブされています。

Provider Type

プロトコル エンドポイント プロバイダのタイプ。有効な値は次のとおりです。

- `Primary`
- `Secondary`

SCSI NAA Device ID

プロトコル エンドポイントのSCSIデバイスのグローバル一意識別子（NAA IEEE Registered Extended形式）。

バインド

仮想ボリュームを使用してI/O処理を実行するには、最初にESXiホストから仮想ボリュームをバインドする必要があります。

SolidFireクラスタは、最適なプロトコル エンドポイントを選択し、ESXiホストと仮想ボリュームをそのプロトコル エンドポイントに関連付けるバインドを作成し、ESXiホストにバインドを返します。バインドが完了すると、ESXiホストはバインドされた仮想ボリュームを使用してI/O処理を実行できます。

バインドの詳細

[VVols]タブの[Bindings]ページには、各仮想ボリュームのバインド情報が表示されます。

次の情報が表示されます。

Host ID

仮想ボリュームをホストしていて、クラスタが認識しているESXiホストのUUID。

Protocol Endpoint ID

SolidFireクラスタ内の各ノードに対応するプロトコル エンドポイントID。

Protocol Endpoint in Band ID

プロトコル エンドポイントのSCSI NAAデバイスID。

Protocol Endpoint Type

プロトコル エンドポイント タイプ。

VVol Binding ID

仮想ボリュームのバインドのUUID。

VVol ID

仮想ボリュームのUniversally Unique Identifier（UUID）。

VVol Secondary ID

仮想ボリュームのセカンダリID（SCSIの第2レベルのLUN ID）。

ホストの詳細

[VVols]タブの[Hosts]ページには、仮想ボリュームをホストしているVMware ESXiホストに関する情報が表示されます。

次の情報が表示されます。

Host ID

仮想ボリュームをホストしていて、クラスタが認識しているESXiホストのUUID。

Host Address

ESXiホストのIPアドレスまたはDNS名。

Bindings
ESXiホストによってバインドされたすべての仮想ボリュームのバインドID。

ESX Cluster ID
vSphereホスト クラスタIDまたはvCenter GUID。

Initiator IQNs
仮想ボリュームのホストのイニシエータIQN。

SolidFire Protocol Endpoint IDs
現在ESXiホストが認識できるプロトコル エンドポイント。

ボリューム アクセス グループとイニシエータの使用

iSCSIイニシエータまたはFibre Channelイニシエータを使用して、ボリューム アクセス グループ内に定義されたボリュームにアクセスできます。

アクセス グループを作成するには、iSCSIイニシエータのIQNまたはFibre ChannelのWWPNをボリュームのグループにマッピングします。アクセス グループに追加した各IQNは、CHAP認証なしでグループ内の各ボリュームにアクセスできます。

CHAP認証には次の2種類の方法があります。

- アカウントレベルのCHAP認証：アカウントにCHAP認証を割り当てることができます。
- イニシエータレベルのCHAP認証：1つのアカウントを1つのCHAPにバインドすることなく、特定のイニシエータに一意のCHAPターゲットとシークレットを割り当てることができます。このCHAPレベル認証は、アカウントレベルのクレデンシャルよりも優先されます。

必要に応じて、イニシエータ単位のCHAPを使用して、イニシエータの承認とイニシエータごとのCHAP認証を適用することができます。これらのオプションはイニシエータ単位で定義可能であり、アクセス グループにはオプションの異なるイニシエータを混在させることができます。

アクセス グループに追加した各WWPNは、アクセス グループ内のボリュームへのFibre Channelネットワーク アクセスを許可します。

注 : ボリューム アクセス グループには次の制限があります。

- 1つのアクセス グループに含めることができるIQNまたはWWPNは最大64個です。
- 1つのアクセス グループに含めることができるボリュームは最大2,000個です。
- 1つのIQNまたはWWPNが属することのできるアクセス グループは1つだけです。
- 1つのボリュームが最大4つのアクセス グループに属することができます。

関連タスク

ボリューム アクセス グループの作成（104ページ）
安全なアクセスを確保するために、ボリュームのグループにイニシエータをマッピングしてボリューム アクセス グループを作成できます。その後、アカウントのCHAPイニシエータ シークレットとターゲット シークレットを使用して、グループ内のボリュームへのアクセスを付与します。

アクセス グループへのボリュームの追加（106ページ）
ボリューム アクセス グループにボリュームを追加することができます。各ボリュームは、複数のボリューム アクセス グループに属することが可能です。各ボリュームが属しているグループは、**[Active Volumes]**ページで確認できます。

アクセス グループからのボリュームの削除（107ページ）

アクセス グループからボリュームを削除すると、グループはそのボリュームにアクセスできなくなります。

イニシエータの作成（107ページ）
iSCSIまたはFibre Channelイニシエータを作成し、オプションでエイリアスを割り当てることができます。

イニシエータの編集（108ページ）
既存のイニシエータのエイリアスを変更するか、既存のエイリアスがない場合はエイリアスを追加できます。

ボリューム アクセス グループへの単一のイニシエータの追加（108ページ）
既存のボリューム アクセス グループにイニシエータを追加できます。

ボリューム アクセス グループへの複数のイニシエータの追加（109ページ）
既存のボリューム アクセス グループに複数のイニシエータを追加すると、そのグループ内のボリュームにCHAP認証の有無にかかわらずアクセスできるようになります。

アクセス グループからのイニシエータの削除（110ページ）
ボリューム アクセス グループからイニシエータを削除すると、そのイニシエータはそのグループ内のボリュームにアクセスできなくなります。ボリュームへの通常のアカウント アクセスは引き続き可能です。

アクセス グループの削除（110ページ）
不要になったアクセス グループを削除できます。ボリューム アクセス グループを削除する前に、イニシエータIDとボリュームIDをそのグループから削除する必要はありません。アクセス グループを削除すると、ボリュームへのグループ アクセスが切断されます。

イニシエータの削除（110ページ）
不要になったイニシエータを削除できます。イニシエータを削除すると、関連するすべてのボリューム アクセス グループから削除されます。該当するイニシエータを使用した接続は、接続をリセットするまでは有効なままです。

ボリューム アクセス グループの作成

安全なアクセスを確保するために、ボリュームのグループにイニシエータをマッピングしてボリューム アクセス グループを作成できます。その後、アカウントのCHAPイニシエータ シークレットとターゲット シークレットを使用して、グループ内のボリュームへのアクセスを付与します。

タスク概要

イニシエータベースのCHAPを使用する場合は、ボリューム アクセス グループ内の1つのイニシエータにCHAPクレデンシャルを追加して、セキュリティを強化できます。これにより、すでに存在するボリューム アクセス グループにこのオプションを適用できます。

手順

1. **[Management]** > **[Access Groups]**の順にクリックします。
2. **[Create Access Group]**をクリックします。
3. **[Name]**フィールドにボリューム アクセス グループの名前を入力します。
4. 次のいずれかの方法でボリューム アクセス グループにイニシエータを追加します。

オプション	説明
Fibre Channelイニシエータの追加	1. [Add Initiators]で、[Unbound Fibre Channel Initiators]リストから既存のFibre Channelイニシエータを選択します。 2. **[Add FC Initiator]**をクリックします。 **注 :** この手順でイニシエータを作成することもできます。その場合は、**[Create Initiator]**リンクをクリックし、イニシエータ名を入力して**[Create]**をクリックします。 作成したイニシエータは、自動的に[Initiators]リストに追加されます。形式の例を次に示します。 `5f:47:ac:c0:5c:74:d4:02`
iSCSIイニシエータの追加	[Add Initiators]で、[Initiators]リストから既存のイニシエータを選択します。 **注 :** この手順でイニシエータを作成することもできます。その場合は、**[Create Initiator]**リンクをクリックし、イニシエータ名を入力して**[Create]**をクリックします。 作成したイニシエータは、自動的に[Initiators]リストに追加されます。形式の例を次に示します。 `iqn.2010-01.com.solidfire:c2r9.fc0.2100000e1e09bb8b` **ヒント :** 各ボリュームのイニシエータIQNを確認するには、**[Management]** > **[Volumes]** > **[Active]**リスト上のボリュームの[Actions]メニューで**[View Details]**を選択します。 イニシエータを変更する際に`requiredCHAP`属性を`True`に切り替えると、ターゲット イニシエータ シークレットを設定できるようになります。詳細については、`ModifyInitiator` APIメソッドに関するAPI情報を参照してください。 *Element APIを使用したストレージの管理*

5. オプション: 必要に応じてイニシエータを追加します。
6. [Add Volumes]で、**[Volumes]**リストからボリュームを選択します。
   [Attached Volumes]リストにボリュームが表示されます。
7. オプション: 必要に応じてボリュームを追加します。
8. **[Create Access Group]**をクリックします。

関連タスク

アクセス グループへのボリュームの追加（106ページ）

ボリューム アクセス グループにボリュームを追加することができます。各ボリュームは、複数のボリューム アクセス グループに属することが可能です。各ボリュームが属しているグループは、**[Active Volumes]**ページで確認できます。

ボリューム アクセス グループの詳細

[Management]タブの[Access Groups]ページには、ボリューム アクセス グループに関する情報が表示されます。

次の情報が表示されます。

ID

システムによって生成されたアクセス グループのID。

Name
アクセス グループの作成時に指定した名前。

Active Volumes
アクセス グループ内のアクティブ ボリュームの数。

Compression
アクセス グループの圧縮による削減率。

Deduplication
アクセス グループの重複排除による削減率。

Thin Provisioning
アクセス グループのシンプロビジョニングによる削減率。

Overall Efficiency
アクセス グループの全体的な削減率。

Initiators
アクセス グループに接続されているイニシエータの数。

個々のアクセス グループの詳細の表示

個々のアクセス グループの詳細（接続されているボリュームやイニシエータなど）をグラフ形式で表示できます。

手順

1. **[Management]** > **[Access Groups]**の順にクリックします。
2. アクセス グループの[Actions]アイコンをクリックします。
3. **[View Details]**をクリックします。

アクセス グループへのボリュームの追加

ボリューム アクセス グループにボリュームを追加することができます。各ボリュームは、複数のボリューム アクセス グループに属することが可能です。各ボリュームが属しているグループは、**[Active Volumes]**ページで確認できます。

タスク概要

ここで説明する手順は、Fibre Channelボリューム アクセス グループにボリュームを追加する場合にも使用できます。

手順

1. **[Management]** > **[Access Groups]**の順にクリックします。
2. ボリュームを追加するアクセス グループの[Actions]アイコンをクリックします。
3. **[Edit]**ボタンをクリックします。
4. [Add Volumes]で、**[Volumes]**リストからボリュームを選択します。
   さらにボリュームを追加するには、この手順を繰り返します。
5. **[Save Changes]**をクリックします。

アクセス グループからのボリュームの削除

アクセス グループからボリュームを削除すると、グループはそのボリュームにアクセスできなくなります。

タスク概要

アカウントのCHAP設定を変更したり、アクセス グループからイニシエータやボリュームを削除したりすると、イニシエータがボリュームにアクセスできなくなることがあります。ボリュームへのアクセスが突然失われないようにするには、アカウントまたはアクセス グループの変更の影響を受けるiSCSIセッションからログアウトし、イニシエータやクラスタの設定に対する変更が完了したあとにイニシエータからボリュームに再接続できることを確認します。

手順

1. **[Management]** > **[Access Groups]**の順にクリックします。
2. ボリュームを削除するアクセス グループの[Actions]アイコンをクリックします。
3. **[Edit]**をクリックします。
4. **[Edit Volume Access Group]**ダイアログ ボックスの[Add Volumes]で、**[Attached Volumes]**リストの矢印をクリックします。
5. リストから削除するボリュームを選択し、**[x]**アイコンをクリックして削除します。
   さらにボリュームを削除するには、この手順を繰り返します。
6. **[Save Changes]**をクリックします。

イニシエータの作成

iSCSIまたはFibre Channelイニシエータを作成し、オプションでエイリアスを割り当てることができます。

タスク概要

API呼び出しを使用して、イニシエータベースのCHAP属性を割り当てることもできます。イニシエータごとにCHAPアカウント名とクレデンシャルを追加するには、`CreateInitiator` API呼び出しを使用して、CHAPアクセスと属性を削除および追加する必要があります。詳細については、APIリファレンス情報を参照してください。

*Element API*を使用したストレージの管理

手順

1. **[Management]** > **[Initiators]**の順にクリックします。
2. **[Create Initiator]**をクリックします。
3. 次の手順を実行して、単一のイニシエータまたは複数のイニシエータを作成します。

オプション	手順
単一のイニシエータを作成する	1. **[Create a Single Initiator]**をクリックします。 2. イニシエータのIQNまたはWWPNを**[IQN/WWPN]**フィールドに入力します。 3. イニシエータのフレンドリ名を**[Alias]**フィールドに入力します。 4. **[Create Initiator]**をクリックします。

オプション	手順
複数のイニシエータを作成する	1. **[Bulk Create Initiators]**をクリックします。 2. IQNまたはWWPNのリストをテキスト ボックスに入力します。 3. **[Add Initiators]**をクリックします。 4. 表示されたリストからイニシエータを選択し、**[Alias]**列で対応する[Add]アイコンをクリックしてイニシエータのエイリアスを追加します。 5. チェック マークをクリックして新しいエイリアスを確認します。 6. **[Create Initiators]**をクリックします。

イニシエータの編集

既存のイニシエータのエイリアスを変更するか、既存のエイリアスがない場合はエイリアスを追加できます。

タスク概要

イニシエータごとにCHAPアカウント名とクレデンシャルを追加するには、`ModifyInitiator` API呼び出しを使用して、CHAPアクセスと属性を削除および追加する必要があります。詳細については、API情報を参照してください。

*Element API*を使用したストレージの管理

手順

1. **[Management]** > **[Initiators]**の順にクリックします。
2. 編集するイニシエータの[Actions]アイコンをクリックします。
3. **[Edit]**をクリックします。
4. イニシエータの新しいエイリアスを**[Alias]**フィールドに入力します。
5. **[Save Changes]**をクリックします。

ボリューム アクセス グループへの単一のイニシエータの追加

既存のボリューム アクセス グループにイニシエータを追加できます。

タスク概要

ボリューム アクセス グループに追加されたイニシエータは、そのボリューム アクセス グループ内のすべてのボリュームにアクセスできます。

ヒント : 各ボリュームのイニシエータを確認するには、アクティブ ボリュームのリストでボリュームの[Actions]アイコンをクリックし、**[View Details]**を選択します。

イニシエータベースのCHAPを使用する場合は、ボリューム アクセス グループ内の1つのイニシエータにCHAPクレデンシャルを追加して、セキュリティを強化できます。これにより、すでに存在するボリューム アクセス グループにこのオプションを適用できます。

手順

1. **[Management]** > **[Access Groups]**の順にクリックします。
2. 編集するアクセス グループの[Actions]アイコンをクリックします。
3. **[Edit]**ボタンをクリックします。
4. Fibre Channelイニシエータをボリューム アクセス グループに追加するには、次の手順を実行します。
   1. [Add Initiators]で、**[Unbound Fibre Channel Initiators]**リストから既存のFibre Channelイニシエータを選択します。

2. **[Add FC Initiator]**をクリックします。

   注 : この手順でイニシエータを作成することもできます。その場合は、**[Create Initiator]**リンクをクリックし、イニシエータ名を入力して**[Create]**をクリックします。 作成したイニシエータは、自動的に**[Initiators]**リストに追加されます。

   形式の例を次に示します。

   ```
   5f:47:ac:c0:5c:74:d4:02
   ```

5. iSCSIイニシエータをボリューム アクセス グループに追加するには、[Add Initiators]で、**[Initiators]**リストから既存のイニシエータを選択します。

   注 : この手順でイニシエータを作成することもできます。その場合は、**[Create Initiator]**リンクをクリックし、イニシエータ名を入力して**[Create]**をクリックします。 作成したイニシエータは、自動的に**[Initiators]**リストに追加されます。

   イニシエータIQNの有効な形式は、iqn.yyyy-mmです。yとmは数字で、続けて任意の文字列を指定します。使用できる文字は、数字、小文字のアルファベット、ピリオド（.）、コロン（:）、ダッシュ（-）です。

   形式の例を次に示します。

   ```
   iqn.2010-01.com.solidfire:c2r9.fc0.2100000e1e09bb8b
   ```

   ヒント : 各ボリュームのイニシエータIQNを確認するには、**[Management]** > **[Volumes]**の[Active Volumes]ページで、ボリュームの[Actions]アイコンをクリックし、**[View Details]**を選択します。

6. **[Save Changes]**をクリックします。

ボリューム アクセス グループへの複数のイニシエータの追加

既存のボリューム アクセス グループに複数のイニシエータを追加すると、そのグループ内のボリュームにCHAP認証の有無にかかわらずアクセスできるようになります。

タスク概要

ボリューム アクセス グループに追加されたイニシエータは、そのボリューム アクセス グループ内のすべてのボリュームにアクセスできます。

ヒント : 各ボリュームのイニシエータを確認するには、アクティブ ボリュームのリストでボリュームの[Actions]アイコンをクリックし、**[View Details]**をクリックします。

既存のボリューム アクセス グループに複数のイニシエータを追加すると、そのグループ内のボリュームにアクセスし、グループ内の各イニシエータに一意のCHAPクレデンシャルを割り当てることができるようになります。これにより、すでに存在するボリューム アクセス グループにこのオプションを適用できます。

イニシエータベースのCHAP属性を割り当てるには、API呼び出しを使用します。イニシエータごとにCHAPアカウント名とクレデンシャルを追加するには、`ModifyInitiator` API呼び出しを使用して、CHAPアクセスと属性を削除および追加する必要があります。詳細については、APIリファレンス情報を参照してください。

*Element API*を使用したストレージの管理

手順

1. **[Management]** > **[Initiators]**の順にクリックします。
2. アクセス グループに追加するイニシエータを選択します。
3. **[Bulk Actions]**ボタンをクリックします。

4. **[Add to Volume Access Group]**をクリックします。
5. [Add to Volume Access Group]ダイアログ ボックスで、**[Volume Access Group]**リストからアクセス グループを選択します。
6. **[Add]**をクリックします。

アクセス グループからのイニシエータの削除

ボリューム アクセス グループからイニシエータを削除すると、そのイニシエータはそのグループ内のボリュームにアクセスできなくなります。ボリュームへの通常のアカウント アクセスは引き続き可能です。

タスク概要

アカウントのCHAP設定を変更したり、アクセス グループからイニシエータやボリュームを削除したりすると、イニシエータがボリュームにアクセスできなくなることがあります。ボリュームへのアクセスが突然失われないようにするには、アカウントまたはアクセス グループの変更の影響を受けるiSCSIセッションからログアウトし、イニシエータやクラスタの設定に対する変更が完了したあとにイニシエータからボリュームに再接続できることを確認します。

手順

1. **[Management]** > **[Access Groups]**の順にクリックします。
2. イニシエータを削除するアクセス グループの[Actions]アイコンをクリックします。
3. 表示されたメニューで**[Edit]**を選択します。
4. **[Edit Volume Access Group]**ダイアログ ボックスの[Add Initiators]で、**[Initiators]**リストの矢印をクリックします。
5. アクセス グループから削除する各イニシエータの[x]アイコンを選択します。
6. **[Save Changes]**をクリックします。

アクセス グループの削除

不要になったアクセス グループを削除できます。ボリューム アクセス グループを削除する前に、イニシエータIDとボリュームIDをそのグループから削除する必要はありません。アクセス グループを削除すると、ボリュームへのグループ アクセスが切断されます。

手順

1. **[Management]** > **[Access Groups]**の順にクリックします。
2. 削除するアクセス グループの[Actions]アイコンをクリックします。
3. 表示されたメニューで**[Delete]**をクリックします。
4. このアクセス グループに関連付けられているイニシエータも削除するには、**[Delete initiators in this access group]**チェック ボックスをオンにします。
5. 操作を確定します。

イニシエータの削除

不要になったイニシエータを削除できます。イニシエータを削除すると、関連するすべてのボリューム アクセス グループから削除されます。該当するイニシエータを使用した接続は、接続をリセットするまでは有効なままです。

手順

1. **[Management]** > **[Initiators]**の順にクリックします。
2. 次の手順を実行して、1つまたは複数のイニシエータを削除します。

オプション	手順
単一のイニシエータの削除	1. 削除するイニシエータの[Actions]アイコンをクリックします。 2. **[Delete]**をクリックします。 3. 操作を確定します。
複数のイニシエータの削除	1. 削除するイニシエータの横にあるチェック ボックスをオンにします。 2. **[Bulk Actions]**ボタンをクリックします。 3. 表示されたメニューで**[Delete]**を選択します。 4. 操作を確定します。

データ保護

NetApp Elementソフトウェアでは、個々のボリュームまたはボリューム グループのSnapshot、Elementで実行されているクラスタとボリュームの間のレプリケーション、ONTAPシステムへのレプリケーションなど、さまざまな機能を使用してデータを保護できます。

Snapshot

Snapshotのみのデータ保護では、特定の時点における変更済みのデータをリモート クラスタにレプリケートします。ソース クラスタで作成されたSnapshotだけがレプリケートされます。ソース ボリュームのアクティブな書き込みはレプリケートされません。

Elementで実行されているクラスタとボリュームの間のレプリケーション

フェイルオーバーやフェイルバックの際には、Elementで実行されているクラスタ ペアのどちらかのクラスタからボリュームのデータを同期または非同期でレプリケートできます。

SnapMirrorテクノロジを使用したElementクラスタとONTAPクラスタ間のレプリケーション

NetApp SnapMirrorテクノロジを使用すると、ディザスタ リカバリを目的として、Elementを使用して作成されたSnapshotをONTAPにレプリケートできます。SnapMirror関係では、Elementが一方のエンドポイントで、ONTAPがもう一方のエンドポイントです。

関連タスク

ボリューム*Snapshot*を使用したデータ保護（113ページ）
ボリュームSnapshotは、ボリュームのポイントインタイム コピーです。ボリュームのSnapshotを作成し、あとでボリュームをSnapshot作成時の状態にロールバックする必要が生じた場合に使用できます。

*NetApp Element*ソフトウェアを実行するクラスタ間でのリモート レプリケーションの実行（126ページ）
Elementソフトウェアを実行するクラスタでは、リアルタイム レプリケーションを使用してボリューム データのリモート コピーを迅速に作成できます。1つのストレージ クラスタを最大4つの他のストレージ クラスタとペアリングすることができます。フェイルオーバーやフェイルバックの際には、クラスタ ペアのどちらかのクラスタからボリュームのデータを同期または非同期でレプリケートできます。

*Element*クラスタと*ONTAP*クラスタ間での*SnapMirror*レプリケーション（141ページ）
NetApp Element UIの[Data Protection]タブで、SnapMirror関係を作成することができます。この情報をユーザ インターフェイスで確認するには、SnapMirror機能を有効にする必要があります。

ボリュームのバックアップとリストア（155ページ）

他のSolidFireストレージ、およびAmazon S3またはOpenStack Swiftと互換性のあるセカンダリ オブジェクト ストアに対して、ボリュームのバックアップとリストアを実行できます。

ボリュームSnapshotを使用したデータ保護

ボリュームSnapshotは、ボリュームのポイントインタイム コピーです。ボリュームのSnapshotを作成し、あとでボリュームをSnapshot作成時の状態にロールバックする必要が生じた場合に使用できます。

タスク概要

Snapshotはボリュームのクローンに似ています。ただし、Snapshotはボリューム メタデータの単なるレプリカであるため、マウントや書き込みはできません。ボリュームSnapshotの作成には少量のシステム リソースとスペースしか使用されないため、クローニングよりも短い時間で完了します。

個々のボリュームまたは一連のボリュームのSnapshotを作成できます。

必要に応じて、Snapshotをリモート クラスタにレプリケートして、ボリュームのバックアップ コピーとして使用できます。レプリケートしたSnapshotを使用すると、ボリュームを特定の時点にロールバックできます。または、レプリケートしたSnapshotからボリュームのクローンを作成できます。

関連タスク

個々のボリューム*Snapshot*を使用したデータ保護タスク（113ページ）
ボリュームSnapshotは、ボリュームのポイントインタイム コピーです。ボリュームのグループではなく個々のボリュームをSnapshotに使用できます。

グループ*Snapshot*を使用したデータ保護タスク（118ページ）
関連する一連のボリュームのグループSnapshotを作成して、各ボリュームのメタデータのポイントインタイム コピーを保持できます。グループSnapshotは、後日バックアップまたはロールバックとして使用して、ボリューム グループを以前の状態にリストアすることができます。

*Snapshot*のスケジュール設定（123ページ）
ボリュームSnapShotが指定した間隔で作成されるようにスケジュールを設定することで、ボリュームまたはボリューム グループ上のデータを保護できます。1つのボリュームのSnapshotまたはグループのSnapshotを自動的に実行するスケジュールを設定できます。

個々のボリュームSnapshotを使用したデータ保護タスク

ボリュームSnapshotは、ボリュームのポイントインタイム コピーです。ボリュームのグループではなく個々のボリュームをSnapshotに使用できます。

関連タスク

ボリューム*Snapshot*の作成（114ページ）
アクティブ ボリュームのSnapshotを作成すると、任意の時点におけるボリューム イメージを保持できます。1つのボリュームに最大32個のSnapshotを作成できます。

*Snapshot*保持期間の編集（115ページ）
Snapshotの保持期間を変更して、Snapshotを削除するかどうか、および削除するタイミングを制御できます。指定した保持期間は、新しい間隔の開始時点からの期間です。保持期間を設定する際には、現在の時刻から始まる期間を選択できます（保持期間はSnapshotの作成時間からは計算されません）。間隔は、分、時間、および日数で指定できます。

*Snapshot*の削除（115ページ）

Elementソフトウェアを実行しているストレージ クラスタからボリュームSnapshotを削除できます。削除したSnapshotは、システムからただちに削除されます。

*Snapshot*からのボリュームのクローニング（116ページ）
ボリュームのSnapshotから新しいボリュームを作成できます。この処理では、Snapshotの作成時点でボリュームに含まれていたデータを使用して新しいボリュームをクローニングします。新しく作成されたボリュームには、ボリュームの他のSnapshotに関する情報も保存されます。

*Snapshot*へのボリュームのロールバック（116ページ）
ボリュームは以前のSnapshotにいつでもロールバックできます。そのSnapshotの作成後にボリュームに対して行われた変更はすべて元に戻ります。

*Amazon S3*オブジェクト ストアへのボリューム*Snapshot*のバックアップ（116ページ）
Amazon S3と互換性のある外部のオブジェクト ストアにSolidFire Snapshotをバックアップできます。

*OpenStack Swift*オブジェクト ストアへのボリューム*Snapshot*のバックアップ（117ページ）
OpenStack Swiftと互換性のあるセカンダリ オブジェクト ストアにSolidFire Snapshotをバックアップできます。

*SolidFire*クラスタへのボリューム*Snapshot*のバックアップ（117ページ）
SolidFireクラスタ上にあるボリュームSnapshotをリモートのSolidFireクラスタにバックアップできます。

ボリュームSnapshotの作成

アクティブ ボリュームのSnapshotを作成すると、任意の時点におけるボリューム イメージを保持できます。1つのボリュームに最大32個のSnapshotを作成できます。

手順

1. **[Management]** > **[Volumes]**の順にクリックします。
2. Snapshotに使用するボリュームの[Actions]アイコンをクリックします。
3. 表示されたメニューで**[Snapshot]**を選択します。
4. **[Create Snapshot of Volume]**ダイアログ ボックスで、新しいSnapshot名を入力します。
5. オプション: 親ボリュームがペアリングされている場合にレプリケーションにSnapshotも含まれるようにするには、**[Include Snapshot in Replication When Paired]**チェック ボックスをオンにします。
6. Snapshotの保持を設定するには、次のいずれかのオプションを選択します。
   - Snapshotをシステム上に無期限に保持するには、**[Keep Forever]**をクリックします。
   - Snapshotを保持する期間を指定するには、**[Set Retention Period]**をクリックし、日付のスピン ボックスを使用します。
7. 単一のSnapshotを今すぐ作成するには、次の手順を実行します。
   1. **[Take Snapshot Now]**をクリックします。
   2. **[Create Snapshot]**をクリックします。
8. スケジュールを設定してあとでSnapshotを作成するには、次の手順を実行します。
   1. **[Create Snapshot Schedule]**をクリックします。
   2. **[New Schedule Name]**にスケジュール名を入力します。
   3. **[Schedule Type]**をリストから選択します。
   4. オプション: スケジュールしたSnapshotの作成を定期的に繰り返すには、**[Recurring Schedule]**チェック ボックスをオンにします。
   5. **[Create Schedule]**をクリックします。

関連タスク

*Snapshot*のスケジュール設定（123ページ）

ボリュームSnapShotが指定した間隔で作成されるようにスケジュールを設定することで、ボリュームまたはボリューム グループ上のデータを保護できます。1つのボリュームのSnapshotまたはグループのSnapshotを自動的に実行するスケジュールを設定できます。

Snapshot保持期間の編集

Snapshotの保持期間を変更して、Snapshotを削除するかどうか、および削除するタイミングを制御できます。指定した保持期間は、新しい間隔の開始時点からの期間です。保持期間を設定する際には、現在の時刻から始まる期間を選択できます（保持期間はSnapshotの作成時間からは計算されません）。間隔は、分、時間、および日数で指定できます。

手順

1. **[Data Protection]** > **[Snapshots]**の順にクリックします。
2. 編集するSnapshotの[Actions]アイコンをクリックします。
3. 表示されたメニューで**[Edit]**をクリックします。
4. オプション: 親ボリュームがペアリングされている場合にレプリケーションにSnapshotも含まれるようにするには、**[Include Snapshot in Replication When Paired]**チェック ボックスをオンにします。
5. オプション: Snapshotの保持オプションを選択します。
   - Snapshotをシステム上に無期限に保持するには、**[Keep Forever]**をクリックします。
   - Snapshotを保持する期間を選択するには、**[Set Retention Period]**をクリックし、日付のスピン ボックスを使用します。
6. **[Save Changes]**をクリックします。

Snapshotの削除

Elementソフトウェアを実行しているストレージ クラスタからボリュームSnapshotを削除できます。削除したSnapshotは、システムからただちに削除されます。

タスク概要

レプリケート中のSnapshotをソース クラスタから削除できます。ターゲット クラスタと同期中のSnapshotを削除すると、同期レプリケーションが完了した時点でソース クラスタからSnapshotが削除されます。ターゲット クラスタからは削除されません。

ターゲットにレプリケート済みのSnapshotを、ターゲット クラスタから削除することもできます。削除したSnapshotは、ターゲットがソース クラスタでSnapshotが削除されたことを検知するまで、ターゲットの削除済みSnapshotのリストに保持されます。ソースSnapshotが削除されたことをターゲットが検知すると、ターゲットはそのSnapshotのレプリケーションを停止します。

ソース クラスタからSnapshotを削除しても、ターゲット クラスタのSnapshotには影響はありません（逆も同じ）。

手順

1. **[Data Protection]** > **[Snapshots]**の順にクリックします。
2. 削除するSnapshotの[Actions]アイコンをクリックします。
3. 表示されたメニューで**[Delete]**を選択します。
4. 操作を確定します。

Snapshotからのボリュームのクローニング

ボリュームのSnapshotから新しいボリュームを作成できます。この処理では、Snapshotの作成時点でボリュームに含まれていたデータを使用して新しいボリュームをクローニングします。新しく作成されたボリュームには、ボリュームの他のSnapshotに関する情報も保存されます。

手順

1. **[Data Protection]** > **[Snapshots]**の順にクリックします。
2. ボリュームのクローンに使用するSnapshotの[Actions]アイコンをクリックします。
3. 表示されたメニューで、**[Clone Volume From Snapshot]**をクリックします。
4. **[Clone Volume From Snapshot]**ダイアログ ボックスで**[Volume Name]**を入力します。
5. **[Total Size]**で新しいボリュームのサイズと単位を選択します。
6. **[Access]**でボリュームのアクセス タイプを選択します。
7. 新しいボリュームに関連付ける**[Account]**をリストから選択します。
8. **[Start Cloning]**をクリックします。

Snapshotへのボリュームのロールバック

ボリュームは以前のSnapshotにいつでもロールバックできます。そのSnapshotの作成後にボリュームに対して行われた変更はすべて元に戻ります。

手順

1. **[Data Protection]** > **[Snapshots]**の順にクリックします。
2. ボリュームのロールバックに使用するSnapshotの[Actions]アイコンをクリックします。
3. 表示されたメニューで**[Rollback Volume To Snapshot]**を選択します。
4. オプション: Snapshotにロールバックする前にボリュームの現在の状態を保存するには、次の手順を実行します。
   1. **[Rollback To Snapshot]**ダイアログ ボックスで、**[Save volume's current state as a snapshot]**を選択します。
   2. 新しいSnapshotの名前を入力します。
5. **[Rollback Snapshot]**をクリックします。

ボリュームSnapshotのバックアップ処理

統合型バックアップ機能を使用して、ボリュームSnapshotをバックアップできます。Snapshotは、SolidFireクラスタから外部のオブジェクト ストア、または別のSolidFireクラスタにバックアップできます。Snapshotを外部のオブジェクト ストアにバックアップする場合は、オブジェクト ストアに接続していて、読み取りおよび書き込み処理が許可されている必要があります。

Amazon S3オブジェクト ストアへのボリュームSnapshotのバックアップ

Amazon S3と互換性のある外部のオブジェクト ストアにSolidFire Snapshotをバックアップできます。

手順

1. **[Data Protection]** > **[Snapshots]**の順にクリックします。
2. バックアップするSnapshotの[Actions]アイコンをクリックします。
3. 表示されたメニューで**[Backup to]**をクリックします。
4. **[Integrated Backup]**ダイアログ ボックスの**[Backup to]**で、**[S3]**を選択します。
5. **[Data Format]**で、次のいずれかのオプションを選択します。
   - **Native**：SolidFireストレージ システムのみが読み取り可能な圧縮形式。

- **Uncompressed**：他のシステムと互換性がある非圧縮形式。

6. **[Hostname]**フィールドにオブジェクト ストアへのアクセスに使用するホスト名を入力します。
7. **[Access Key ID]**フィールドにアカウントのアクセス キーIDを入力します。
8. **[Secret Access Key]**フィールドにアカウントのシークレット アクセス キーを入力します。
9. **[S3 Bucket]**フィールドにバックアップの格納先とするS3バケットを入力します。
10. オプション: **[Nametag]**フィールドにプレフィックスに付加するネームタグを入力します。
11. **[Start Read]**をクリックします。

OpenStack Swiftオブジェクト ストアへのボリュームSnapshotのバックアップ

OpenStack Swiftと互換性のあるセカンダリ オブジェクト ストアにSolidFire Snapshotをバックアップできます。

手順

1. **[Data Protection]** > **[Snapshots]**の順にクリックします。
2. バックアップするSnapshotの[Actions]アイコンをクリックします。
3. 表示されたメニューで**[Backup to]**をクリックします。
4. **[Integrated Backup]**ダイアログ ボックスの**[Backup to]**で、**[Swift]**を選択します。
5. **[Data Format]**で、次のいずれかのオプションを選択します。
   - **Native**：SolidFireストレージ システムのみが読み取り可能な圧縮形式。
   - **Uncompressed**：他のシステムと互換性がある非圧縮形式。
6. オブジェクト ストアへのアクセスに使用する**[URL]**を入力します。
7. アカウントの**[Username]**を入力します。
8. アカウントの**[Authentication Key]**を入力します。
9. バックアップの格納先とする**[Container]**を入力します。
10. オプション: **[Nametag]**を入力します。
11. **[Start Read]**をクリックします。

SolidFireクラスタへのボリュームSnapshotのバックアップ

SolidFireクラスタ上にあるボリュームSnapshotをリモートのSolidFireクラスタにバックアップできます。

開始する前に

ソース クラスタとターゲット クラスタがペアリングされていることを確認します。

タスク概要

クラスタ間でバックアップまたはリストアを実行する際には、システムによってクラスタ間の認証に使用するキーが生成されます。ソース クラスタはこのボリュームの一括書き込みキーを使用してデスティネーション クラスタに対して認証し、デスティネーション ボリュームへの書き込みがセキュリティで保護されます。バックアップまたはリストアを実行する際には、処理を開始する前に、デスティネーション ボリュームからボリュームの一括書き込みキーを生成する必要があります。

手順

1. デスティネーション クラスタで、**[Management]** > **[Volumes]**の順にクリックします。
2. デスティネーション ボリュームの[Actions]アイコンをクリックします。
3. 表示されたメニューで**[Restore from]**をクリックします。

4. **[Integrated Restore]**ダイアログ ボックスの**[Restore from]**で、**[SolidFire]**を選択します。
5. **[Data Format]**で、次のいずれかのデータ形式を選択します。
   - **Native**：SolidFireストレージ システムのみが読み取り可能な圧縮形式。
   - **Uncompressed**：他のシステムと互換性がある非圧縮形式。
6. **[Generate Key]**をクリックします。
7. **[Bulk Volume Write Key]**ボックスからクリップボードへキーをコピーします。
8. ソース クラスタで、**[Data Protection]** > **[Snapshots]**の順にクリックします。
9. バックアップに使用するSnapshotの[Actions]アイコンをクリックします。
10. 表示されたメニューで**[Backup to]**をクリックします。
11. **[Integrated Backup]**ダイアログ ボックスの**[Backup to]**で、**[SolidFire]**を選択します。
12. **[Data Format]**フィールドで、前の手順で選択したデータ形式と同じ形式を選択します。
13. **[Remote Cluster MVIP]**フィールドにデスティネーション ボリュームのクラスタの管理仮想IPアドレスを入力します。
14. **[Remote Cluster Username]**フィールドにリモート クラスタのユーザ名を入力します。
15. **[Remote Cluster Password]**フィールドにリモート クラスタのパスワードを入力します。
16. デスティネーション クラスタで生成したキーを**[Bulk Volume Write Key]**フィールドに貼り付けます。
17. **[Start Read]**をクリックします。

グループSnapshotを使用したデータ保護タスク

関連する一連のボリュームのグループSnapshotを作成して、各ボリュームのメタデータのポイントインタイム コピーを保持できます。グループSnapshotは、後日バックアップまたはロールバックとして使用して、ボリューム グループを以前の状態にリストアすることができます。

関連タスク

グループ *Snapshot*の作成（119ページ）
ボリューム グループのSnapshotを作成できます。また、グループSnapshotスケジュールを作成して、グループSnapshotの作成を自動化することもできます。1つのグループSnapshotには一度に最大32個のボリュームのSnapshotを含めることができます。

グループ *Snapshot*の編集（120ページ）
既存のグループSnapshotのレプリケーションと保持の設定を編集できます。

グループ *Snapshot*のメンバーの編集（121ページ）
既存のグループSnapshotのメンバーの保持の設定を編集できます。

グループ *Snapshot*の削除（121ページ）
システムからグループSnapshotを削除できます。グループSnapshotを削除する場合は、グループに関連付けられているすべてのSnapshotについて、削除するか個別のSnapshotとして保持するかを選択できます。

グループ *Snapshot*へのボリュームのロールバック（121ページ）
ボリューム グループを、グループSnapshotにいつでもロールバックできます。

複数ボリュームのクローニング（122ページ）

複数のボリュームのクローンを一度に作成して、ボリューム グループ上のデータのポイントインタイム コピーを作成できます。

グループ *Snapshot*からの複数ボリュームのクローニング（122ページ）
ボリュームのグループをポイントインタイムのグループSnapshotからクローニングできます。この処理を実行するにはボリュームのグループSnapshotが必要です。このグループSnapshotを基にボリュームが作成されます。作成したボリュームは、システム内の他のボリュームと同様に使用できます。

グループSnapshotの詳細

[Data Protection]タブの[Group Snapshots]ページには、グループSnapshotに関する情報が表示されます。

ID

システムによって生成されたグループSnapshotのID。

UUID

グループSnapshotの一意のID。

Name

ユーザが定義したグループSnapshotの名前。

Create Time

グループSnapshotが作成された時刻。

Status

Snapshotの現在のステータス。有効な値は次のとおりです。

- `Preparing`：Snapshotは使用準備中で、まだ書き込みができません。
- `Done`：Snapshotの準備が完了し、使用可能な状態です。
- `Active`：Snapshotはアクティブです。

 # Volumes

グループ内のボリュームの数。

Retain Until

Snapshotが削除される日時。

Remote Replication

リモートのSolidFireクラスタへのSnapshotのレプリケーションが有効かどうか。有効な値は次のとおりです。

- `Enabled`：Snapshotのリモート レプリケーションが有効です。
- `Disabled`：Snapshotのリモート レプリケーションが無効です。

グループSnapshotの作成

ボリューム グループのSnapshotを作成できます。また、グループSnapshotスケジュールを作成して、グループSnapshotの作成を自動化することもできます。1つのグループSnapshotには一度に最大32個のボリュームのSnapshotを含めることができます。

手順

1. **[Management]** > **[Volumes]**の順にクリックします。
2. チェック ボックスを使用して、ボリューム グループに含めるボリュームを選択します。
3. **[Bulk Actions]**をクリックします。
4. **[Group Snapshot]**をクリックします。

5. [Create Group Snapshot of Volumes]ダイアログ ボックスで、新しいグループSnapshotの名前を入力します。
6. オプション: 親ボリュームがペアリングされている場合にレプリケーションにSnapshotも含まれるようにするには、**[Include Each Group Snapshot Member in Replication When Paired]**チェック ボックスをオンにします。
7. グループSnapshotの保持オプションを選択します。
   - Snapshotをシステム上に無期限に保持するには、**[Keep Forever]**をクリックします。
   - Snapshotを保持する期間を指定するには、**[Set Retention Period]**をクリックし、日付のスピン ボックスを使用します。
8. 単一のSnapshotを今すぐ作成するには、次の手順を実行します。
   1. **[Take Group Snapshot Now]**をクリックします。
   2. **[Create Group Snapshot]**をクリックします。
9. スケジュールを設定してあとでSnapshotを作成するには、次の手順を実行します。
   1. **[Create Group Snapshot Schedule]**をクリックします。
   2. **[New Schedule Name]**にスケジュール名を入力します。
   3. **[Schedule Type]**をリストから選択します。
   4. オプション: スケジュールしたSnapshotの作成を定期的に繰り返すには、**[Recurring Schedule]**チェック ボックスをオンにします。
   5. **[Create Schedule]**をクリックします。

グループSnapshotの編集

既存のグループSnapshotのレプリケーションと保持の設定を編集できます。

手順

1. **[Data Protection]** > **[Group Snapshots]**の順にクリックします。
2. 編集するグループSnapshotの[Actions]アイコンをクリックします。
3. 表示されたメニューで**[Edit]**を選択します。
4. オプション: グループSnapshotのレプリケーション設定を変更するには、次の手順を実行します。
   1. **[Current Replication]**の横にある**[Edit]**をクリックします。
   2. 親ボリュームがペアリングされている場合にレプリケーションにSnapshotも含まれるようにするには、**[Include Each Group Snapshot Member in Replication When Paired]**チェック ボックスをオンにします。
5. オプション: グループSnapshotの保持設定を変更するには、次のいずれかのオプションを選択します。
   1. **[Current Retention]**の横にある**[Edit]**をクリックします。
   2. グループSnapshotの保持オプションを選択します。
      - Snapshotをシステム上に無期限に保持するには、**[Keep Forever]**をクリックします。
      - Snapshotを保持する期間を指定するには、**[Set Retention Period]**をクリックし、日付のスピン ボックスを使用します。
6. **[Save Changes]**をクリックします。

グループSnapshotの削除

システムからグループSnapshotを削除できます。グループSnapshotを削除する場合は、グループに関連付けられているすべてのSnapshotについて、削除するか個別のSnapshotとして保持するかを選択できます。

タスク概要

グループSnapshotに含まれているボリュームまたはSnapshotを削除すると、そのグループSnapshotにロールバックできなくなります。ただし、各ボリュームを個別にロールバックすることは可能です。

手順

1. **[Data Protection]** > **[Group Snapshots]**の順にクリックします。
2. 削除するSnapshotの[Actions]アイコンをクリックします。
3. 表示されたメニューで**[Delete]**をクリックします。
4. 確認のダイアログ ボックスで、次のいずれかのオプションを選択します。
   - グループSnapshotとグループ内のSnapshotをすべて削除するには、**[Delete group snapshot AND all group snapshot members]**をクリックします。
   - グループSnapshotを削除し、グループ内のSnapshotは保持するには、**[Retain group snapshot members as individual snapshots]**をクリックします。
5. 操作を確定します。

グループSnapshotへのボリュームのロールバック

ボリューム グループを、グループSnapshotにいつでもロールバックできます。

タスク概要

ボリューム グループをロールバックすると、グループ内のすべてのボリュームが、グループSnapshotが作成されたときの状態にリストアされます。ボリューム サイズも、元のSnapshotに記録されているサイズにリストアされます。ボリュームがパージされている場合は、そのボリュームのすべてのSnapshotもパージ時に削除されています。削除されたボリュームSnapshotはリストアされません。

手順

1. **[Data Protection]** > **[Group Snapshots]**の順にクリックします。
2. ボリュームのロールバックに使用するグループSnapshotの[Actions]アイコンをクリックします。
3. 表示されたメニューで**[Rollback Volumes To Group Snapshot]**を選択します。
4. オプション: Snapshotにロールバックする前にボリュームの現在の状態を保存するには、次の手順を実行します。
   1. **[Rollback To Snapshot]**ダイアログ ボックスで、**[Save volumes' current state as a group snapshot]**を選択します。
   2. 新しいSnapshotの名前を入力します。
5. **[Rollback Group Snapshot]**をクリックします。

グループSnapshotのメンバーの編集

既存のグループSnapshotのメンバーの保持の設定を編集できます。

手順

1. **[Data Protection]** > **[Snapshots]**の順にクリックします。
2. **[Members]**タブをクリックします。
3. 編集するグループSnapshotメンバーの[Actions]アイコンをクリックします。

4. 表示されたメニューで**[Edit]**を選択します。
5. Snapshotの保持設定を変更するには、次のいずれかのオプションを選択します。
   - Snapshotをシステム上に無期限に保持するには、**[Keep Forever]**をクリックします。
   - Snapshotを保持する期間を指定するには、**[Set Retention Period]**をクリックし、日付のスピン ボックスを使用します。
6. **[Save Changes]**をクリックします。

複数ボリュームのクローニング

複数のボリュームのクローンを一度に作成して、ボリューム グループ上のデータのポイントインタイム コピーを作成できます。

タスク概要

ボリュームをクローニングすると、そのボリュームのSnapshotが作成され、Snapshot内のデータから新しいボリュームが作成されます。新しいボリューム クローンは、マウントして書き込むことができます。複数のボリュームのクローニングは非同期のプロセスであり、クローニングするボリュームのサイズと数によって所要時間が異なります。

クローニング処理が完了するまでの時間は、ボリューム サイズおよびクラスタの現在の負荷によって異なります。

手順

1. **[Management]** > **[Volumes]**の順にクリックします。
2. **[Active]**タブをクリックします。
3. チェック ボックスを使用して複数のボリュームを選択し、ボリューム グループを作成します。
4. **[Bulk Actions]**をクリックします。
5. 表示されたメニューで、**[Clone]**をクリックします。
6. **[Clone Multiple Volumes]**ダイアログ ボックスの**[New Volume Name Prefix]**にプレフィックスを入力します。
   このプレフィックスは、グループ内のすべてのボリュームに適用されます。
7. オプション: クローンを割り当てる別のアカウントを選択します。
   アカウントを選択しない場合、新しいボリュームは現在のボリューム アカウントに割り当てられます。
8. オプション: クローン内のボリュームに適用する別のアクセス方法を選択します。
   アクセス方法を選択しない場合、現在のボリューム アクセス方法が使用されます。
9. **[Start Cloning]**をクリックします。

グループSnapshotからの複数ボリュームのクローニング

ボリュームのグループをポイントインタイムのグループSnapshotからクローニングできます。この処理を実行するにはボリュームのグループSnapshotが必要です。このグループSnapshotを基にボリュームが作成されます。作成したボリュームは、システム内の他のボリュームと同様に使用できます。

タスク概要

クローニング処理が完了するまでの時間は、ボリューム サイズおよびクラスタの現在の負荷によって異なります。

手順

1. **[Data Protection]** > **[Group Snapshots]**の順にクリックします。

2. ボリュームのクローンに使用するグループSnapshotの[Actions]アイコンをクリックします。
3. 表示されたメニューで**[Clone Volumes From Group Snapshot]**を選択します。
4. **[Clone Volumes From Group Snapshot]**ダイアログ ボックスの**[New Volume Name Prefix]**にプレフィックスを入力します。
   このプレフィックスは、グループSnapshotから作成されるすべてのボリュームに適用されます。
5. オプション: クローンを割り当てる別のアカウントを選択します。
   アカウントを選択しない場合、新しいボリュームは現在のボリューム アカウントに割り当てられます。
6. オプション: クローン内のボリュームに適用する別のアクセス方法を選択します。
   アクセス方法を選択しない場合、現在のボリューム アクセス方法が使用されます。
7. **[Start Cloning]**をクリックします。

Snapshotのスケジュール設定

ボリュームSnapShotが指定した間隔で作成されるようにスケジュールを設定することで、ボリュームまたはボリューム グループ上のデータを保護できます。1つのボリュームのSnapshotまたはグループのSnapshotを自動的に実行するスケジュールを設定できます。

タスク概要

Snapshotスケジュールには、曜日または日にちに基づく間隔を設定できます。次のSnapshotを作成するまでの日数、時間、および分を指定することもできます。ボリュームがレプリケートされている場合は、作成されたSnapshotをリモート ストレージ システムに格納できます。

関連タスク

*Snapshot*スケジュールの作成（124ページ）
ボリュームのSnapshotのスケジュールを設定し、指定した間隔でSnapshotを自動的に作成できます。

*Snapshot*スケジュールの編集（125ページ）
既存のSnapshotスケジュールを変更できます。変更後、次回のスケジュール実行時に更新された設定が使用されます。元のスケジュールで作成されたSnapshotはストレージ システムに保持されます。

*Snapshot*スケジュールの削除（126ページ）
Snapshotスケジュールを削除できます。スケジュールを削除すると、以降のスケジュールされたSnapshotは実行されません。過去にスケジュールで作成されたSnapshotはストレージ システム上に保持されます。

*Snapshot*スケジュールのコピー（126ページ）
スケジュールをコピーして、現在の設定を継承できます。

Snapshotスケジュールの詳細

[Data Protection] > [Schedules]ページにあるSnapshotスケジュールのリストでは、次の情報を確認できます。

ID
システムによって生成されたSnapshotのID。

Type
スケジュールのタイプ。現時点でサポートされているタイプはSnapshotのみです。

Name

スケジュールの作成時に指定した名前。Snapshotスケジュール名は最大223文字で、使用できる文字はa～z、0～9、およびダッシュ（-）です。

Frequency

スケジュールを実行する頻度。頻度は時間と分、週、または月で設定できます。

Recurring

スケジュールが1回だけ実行されるか、定期的に実行されるか。

Manually Paused

スケジュールが手動で一時停止されているかどうか。

Volume IDs

スケジュールの実行時に使用されるボリュームのID。

Last Run

最後にスケジュールが実行された日時。

Last Run Status

スケジュールの前回の実行結果。有効な値は次のとおりです。

- `Success`
- `Failure`

Snapshotスケジュールの作成

ボリュームのSnapshotのスケジュールを設定し、指定した間隔でSnapshotを自動的に作成できます。

タスク概要

Snapshotスケジュールには、曜日または日にちに基づく間隔を設定できます。繰り返しスケジュールを作成して、次のSnapshotを作成するまでの日数、時間、および分を指定することもできます。

Snapshotのスケジュールを5分以外の間隔で設定した場合、Snapshotは5分単位に繰り上げた時間で実行されます。たとえば、12:42:00 UTCに実行するようにSnapshotのスケジュールを設定した場合、12:45:00 UTCに実行されます。Snapshotのスケジュールを5分未満の間隔で実行するように設定することはできません。

手順

1. **[Data Protection]** > **[Schedules]**の順にクリックします。
2. **[Create Schedule]**をクリックします。
3. **[Volume IDs CSV]**フィールドに、Snapshot処理に含めるボリュームIDまたは複数のボリュームIDをカンマで区切って入力します。
4. 新しいスケジュール名を入力します。
5. スケジュール タイプを選択し、表示されたオプションからスケジュールを設定します。
6. オプション: Snapshotスケジュールを無期限に繰り返すには、**[Recurring Schedule]**を選択します。
7. オプション: **[New Snapshot Name]**フィールドに、新しいSnapshotの名前を入力します。

   このフィールドを空白のままにすると、Snapshotの作成日時が名前として使用されます。

8. オプション: 親ボリュームがペアリングされている場合にレプリケーションにSnapshotも含まれるようにするには、**[Include Snapshots in Replication When Paired]**チェック ボックスをオンにします。
9. Snapshotの保持を設定するには、次のいずれかのオプションを選択します。
   - Snapshotをシステム上に無期限に保持するには、**[Keep Forever]**をクリックします。
   - Snapshotを保持する期間を指定するには、**[Set Retention Period]**をクリックし、日付のスピン ボックスを使用します。
10. **[Create Schedule]**をクリックします。

Snapshotスケジュールの編集

既存のSnapshotスケジュールを変更できます。変更後、次回のスケジュール実行時に更新された設定が使用されます。元のスケジュールで作成されたSnapshotはストレージ システムに保持されます。

手順

1. **[Data Protection]** > **[Schedules]**の順にクリックします。
2. 変更するスケジュールの[Actions]アイコンをクリックします。
3. 表示されたメニューで**[Edit]**をクリックします。
4. **[Volume IDs CSV]**フィールドで、現在Snapshot処理の対象となっているボリュームID（複数の場合はカンマで区切って指定）を変更します。
5. スケジュールを一時停止または再開するには、次のいずれかのオプションを選択します。
   - アクティブなスケジュールを一時停止するには、**[Manually Pause Schedule]**リストから**[Yes]**を選択します。
   - 一時停止したスケジュールを再開するには、**[Manually Pause Schedule]**リストから**[No]**を選択します。
6. 必要に応じて、**[New Schedule Name]**フィールドに別のスケジュール名を入力します。
7. 別の曜日または日にちに実行するようにスケジュールを変更するには、**[Schedule Type]**を選択し、表示されたオプションからスケジュールを変更します。
8. オプション: Snapshotスケジュールを無期限に繰り返すには、**[Recurring Schedule]**を選択します。
9. オプション: **[New Snapshot Name]**フィールドで、新しいSnapshotの名前を入力または変更します。

   このフィールドを空白のままにすると、Snapshotの作成日時が名前として使用されます。
10. オプション: 親ボリュームがペアリングされている場合にレプリケーションにSnapshotも含まれるようにするには、**[Include Snapshots in Replication When Paired]**チェック ボックスをオンにします。
11. 保持設定を変更するには、次のいずれかのオプションを選択します。
    - Snapshotをシステム上に無期限に保持するには、**[Keep Forever]**をクリックします。
    - Snapshotを保持する期間を選択するには、**[Set Retention Period]**をクリックし、日付のスピン ボックスを使用します。
12. **[Save Changes]**をクリックします。

Snapshotスケジュールのコピー

スケジュールをコピーして、現在の設定を継承できます。

手順

1. **[Data Protection]** > **[Schedules]**の順にクリックします。
2. コピーするスケジュールの[Actions]アイコンをクリックします。
3. 表示されたメニューで**[Make a Copy]**をクリックします。

   [Create Schedule]ダイアログ ボックスが、スケジュールの現在の設定が入力された状態で表示されます。
4. オプション: 新しいスケジュールの名前と設定を入力します。
5. **[Create Schedule]**をクリックします。

Snapshotスケジュールの削除

Snapshotスケジュールを削除できます。スケジュールを削除すると、以降のスケジュールされたSnapshotは実行されません。過去にスケジュールで作成されたSnapshotはストレージ システム上に保持されます。

手順

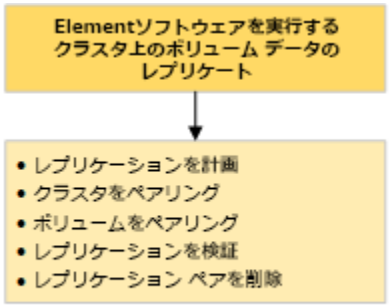
1. **[Data Protection]** > **[Schedules]**の順にクリックします。
2. 削除するスケジュールの[Actions]アイコンをクリックします。
3. 表示されたメニューで**[Delete]**をクリックします。
4. 操作を確定します。

NetApp Elementソフトウェアを実行するクラスタ間でのリモート レプリケーションの実行

Elementソフトウェアを実行するクラスタでは、リアルタイム レプリケーションを使用してボリューム データのリモート コピーを迅速に作成できます。1つのストレージ クラスタを最大4つの他のストレージ クラスタとペアリングすることができます。フェイルオーバーやフェイルバックの際には、クラスタ ペアのどちらかのクラスタからボリュームのデータを同期または非同期でレプリケートできます。

タスク概要

レプリケーション プロセスは以下の手順で構成されます。



手順

1. リアルタイム レプリケーションのためのクラスタとボリュームのペアリング計画（127ページ）

リアルタイムでリモート レプリケーションを行うには、Elementソフトウェアを実行する2つのストレージ クラスタをペアリングし、各クラスタのボリュームをペアリングしてから、レプリケーションを検証する必要があります。レプリケーションが完了したら、ボリューム関係を削除します。

2. クラスタのペアリング（128ページ）
リアルタイム レプリケーション機能を使用するには、最初に2つのクラスタをペアリングする必要があります。2つのクラスタをペアリングして接続したあと、一方のクラスタのアクティブなボリュームをもう一方のクラスタに継続的にレプリケートするように設定することで継続的なデータ保護（CDP）を実現できます。

3. ボリュームのペアリング（131ページ）
クラスタ ペアのクラスタ間の接続を確立したら、一方のクラスタのボリュームをもう一方のクラスタのボリュームとペアリングできます。ボリューム ペアリング関係を確立する際、どちらのボリュームをレプリケーション ターゲットにするかを指定する必要があります。

4. ボリューム レプリケーションの検証（137ページ）
ボリュームがレプリケートされたら、ソース ボリュームとターゲット ボリュームがアクティブになっていることを確認する必要があります。状態がアクティブな場合は、ボリュームがペアリングされ、ソース ボリュームからターゲット ボリュームにデータが送信されて同期されています。

5. レプリケーション後のボリューム関係の削除（137ページ）
レプリケーションが完了してボリューム ペア関係が不要になったら、ボリューム関係を削除できます。

6. ボリューム関係の管理（137ページ）
レプリケーションの一時停止、ボリューム ペアリングの反転、レプリケーション モードの変更、ボリューム ペアの削除、クラスタ ペアの削除など、さまざまな方法でボリューム関係を管理できます。

リアルタイム レプリケーションのためのクラスタとボリュームのペアリング計画

リアルタイムでリモート レプリケーションを行うには、Elementソフトウェアを実行する2つのストレージ クラスタをペアリングし、各クラスタのボリュームをペアリングしてから、レプリケーションを検証する必要があります。レプリケーションが完了したら、ボリューム関係を削除します。

開始する前に

- ペアリングするクラスタの一方または両方に対するクラスタ管理者権限が必要です。
- 管理およびストレージ両方のネットワークのすべてのノードIPアドレスが、ペアリングするクラスタ間で相互にルーティングされている必要があります。
- すべてのペア ノードでMTUが同じでなければならず、クラスタ間でエンドツーエンドでサポートされている必要があります。
- 両方のストレージ クラスタに、一意のクラスタ名、MVIP、SVIP、およびすべてのノードIPアドレスが必要です。
- クラスタのElementソフトウェアのバージョンの違いが1メジャー バージョン以内である必要があります。それよりも離れている場合、データ レプリケーションを実行するには一方のクラスタをアップグレードする必要があります。

注 : ネットアップは、データのレプリケーション時にWANアクセラレータ アプライアンスを使用することを認定していません。データをレプリケートする2つのクラスタ間にこのアプライアンスを配置すると、圧縮および重複排除の妨げとなる場合があります。WANアクセラレータ アプライアンスを本番環境に導入する前に、影響を十分に検証してください。

関連タスク

クラスタのペアリング（128ページ）

リアルタイム レプリケーション機能を使用するには、最初に2つのクラスタをペアリングする必要があります。2つのクラスタをペアリングして接続したあと、一方のクラスタのアクティブなボリュームをもう一方のクラスタに継続的にレプリケートするように設定することで継続的なデータ保護（CDP）を実現できます。

ボリュームのペアリング（131ページ）

クラスタ ペアのクラスタ間の接続を確立したら、一方のクラスタのボリュームをもう一方のクラスタのボリュームとペアリングできます。ボリューム ペアリング関係を確立する際、どちらのボリュームをレプリケーション ターゲットにするかを指定する必要があります。

ペアリングされたボリュームに対するレプリケーションのソースとターゲットの割り当て（135ページ）

ボリュームをペアリングしたら、ソース ボリュームとそのレプリケーション ターゲット ボリュームを割り当てる必要があります。ボリューム ペアのどちらのボリュームをレプリケーションのソースまたはターゲットにしてもかまいません。この手順は、ソース ボリュームが使用できなくなったときに、ソース ボリュームに送信されたデータをリモート ターゲット ボリュームにリダイレクトする場合にも使用できます。

クラスタのペアリング

リアルタイム レプリケーション機能を使用するには、最初に2つのクラスタをペアリングする必要があります。2つのクラスタをペアリングして接続したあと、一方のクラスタのアクティブなボリュームをもう一方のクラスタに継続的にレプリケートするように設定することで継続的なデータ保護（CDP）を実現できます。

開始する前に

- ペアリングするクラスタの一方または両方に対するクラスタ管理者権限が必要です。
- すべてのノードMIPとノードSIPを相互にルーティングする必要があります。
- クラスタ間のラウンドトリップ レイテンシが2,000ミリ秒未満である必要があります。
- 両方のストレージ クラスタに、一意のクラスタ名、MVIP、SVIP、およびすべてのノードIPアドレスが必要です。
- クラスタのElementソフトウェアのバージョンの違いが1メジャー バージョン以内である必要があります。それよりも離れている場合、データ レプリケーションを実行するには一方のクラスタをアップグレードする必要があります。

注 : クラスタをペアリングするには、管理ネットワーク上のノードどうしが完全に接続されている必要があります。レプリケーションを実行するには、ストレージ クラスタ ネットワーク上の個々のノードが接続されている必要があります。

タスク概要

ボリュームのレプリケーション用に、1つのクラスタを最大4つの他のクラスタとペアリングすることができます。同じクラスタ グループに含まれるクラスタどうしをペアリングすることもできます。

関連資料

ネットワーク ポート要件（14ページ）

システムをリモートから管理し、クライアントがデータセンターの外部からリソースに接続できるようにするために、データセンターのエッジ ファイアウォールで次のTCPポートを許可する必要があります。システムの使用方法によっては、一部のポートは不要な場合もあります。

手順

1. *MVIP*またはペアリング キーを使用したクラスタのペアリング（129ページ）
両方のクラスタにクラスタ管理者としてアクセスできる場合は、ターゲット クラスタのMVIPを使用してソースとターゲットのクラスタをペアリングできます。クラスタ ペアの一方のクラスタにしかクラスタ管理者としてアクセスできない場合は、ターゲット クラスタでペアリング キーを使用してクラスタをペアリングします。
2. クラスタ ペア接続の検証（131ページ）
クラスタ ペアリングが完了したら、クラスタ ペアの接続を検証して、レプリケーションが成功したかどうかを確認することができます。

MVIPまたはペアリング キーを使用したクラスタのペアリング

両方のクラスタにクラスタ管理者としてアクセスできる場合は、ターゲット クラスタのMVIPを使用してソースとターゲットのクラスタをペアリングできます。クラスタ ペアの一方のクラスタにしかクラスタ管理者としてアクセスできない場合は、ターゲット クラスタでペアリング キーを使用してクラスタをペアリングします。

手順

次のいずれかの方法を選択してクラスタをペアリングします。

- MVIPを使用したクラスタのペアリング：この方法は、両方のクラスタにクラスタ管理者としてアクセスできる場合に使用します。リモート クラスタのMVIPを使用して2つのクラスタをペアリングします。
- ペアリング キーを使用したクラスタのペアリング：この方法は、一方のクラスタにしかクラスタ管理者としてアクセスできない場合に使用します。ペアリング キーを生成し、そのキーをターゲット クラスタで使用してクラスタをペアリングします。

関連タスク

*MVIP*を使用したクラスタのペアリング（129ページ）
一方のクラスタのMVIPを使用してもう一方のクラスタとの接続を確立することにより、リアルタイム レプリケーション用に2つのクラスタをペアリングできます。この方法を使用するには、両方のクラスタに対するクラスタ管理者アクセスが必要です。クラスタをペアリングする前に、クラスタ管理者のユーザ名とパスワードを使用してクラスタ アクセスを認証します。

ペアリング キーを使用したクラスタのペアリング（130ページ）
ローカル クラスタにはクラスタ管理者としてアクセスできるが、リモート クラスタにはアクセスできない場合は、ペアリング キーを使用してクラスタをペアリングします。ローカル クラスタで生成したペアリング キーをリモート サイトのクラスタ管理者に安全な方法で送信して接続を確立し、リアルタイム レプリケーション用にクラスタをペアリングします。

MVIPを使用したクラスタのペアリング

一方のクラスタのMVIPを使用してもう一方のクラスタとの接続を確立することにより、リアルタイム レプリケーション用に2つのクラスタをペアリングできます。この方法を使用するには、両方のクラスタに対するクラスタ管理者アクセスが必要です。クラスタをペアリングする前に、クラスタ管理者のユーザ名とパスワードを使用してクラスタ アクセスを認証します。

手順

1. ローカル クラスタで、**[Data Protection]** > **[Cluster Pairs]**の順に選択します。
2. **[Pair Cluster]**をクリックします。
3. **[Start Pairing]**をクリックし、リモート クラスタにアクセスできるので**[Yes]**をクリックします。

4. リモート クラスタのMVIPアドレスを入力します。
5. **[Complete pairing on remote cluster]**をクリックします。
   [Authentication Required]ウィンドウで、リモート クラスタのクラスタ管理者のユーザ名とパスワードを入力します。
6. リモート クラスタで、**[Data Protection]** > **[Cluster Pairs]**の順に選択します。
7. **[Pair Cluster]**をクリックします。
8. **[Complete Pairing]**をクリックします。
9. **[Complete Pairing]**ボタンをクリックします。

関連タスク

ペアリング キーを使用したクラスタのペアリング（130ページ）

ローカル クラスタにはクラスタ管理者としてアクセスできるが、リモート クラスタにはアクセスできない場合は、ペアリング キーを使用してクラスタをペアリングします。ローカル クラスタで生成したペアリング キーをリモート サイトのクラスタ管理者に安全な方法で送信して接続を確立し、リアルタイム レプリケーション用にクラスタをペアリングします。

関連情報

Pairing clusters using MVIP (video)

ペアリング キーを使用したクラスタのペアリング

ローカル クラスタにはクラスタ管理者としてアクセスできるが、リモート クラスタにはアクセスできない場合は、ペアリング キーを使用してクラスタをペアリングします。ローカル クラスタで生成したペアリング キーをリモート サイトのクラスタ管理者に安全な方法で送信して接続を確立し、リアルタイム レプリケーション用にクラスタをペアリングします。

手順

1. ローカル クラスタで、**[Data Protection]** > **[Cluster Pairs]**の順に選択します。
2. **[Pair Cluster]**をクリックします。
3. **[Start Pairing]**をクリックし、リモート クラスタにアクセスできないので**[No]**をクリックします。
4. **[Generate Key]**をクリックします。

   注 : この操作により、ペアリング用のテキスト キーが生成され、ローカル クラスタにクラスタ ペアが未設定の状態で作成されます。この手順を途中で中止した場合は、クラスタ ペアを手動で削除する必要があります。
5. クラスタ ペアリング キーをクリップボードにコピーします。
6. このペアリング キーをリモート クラスタ サイトのクラスタ管理者に渡します。

   注 : クラスタ ペアリング キーには、リモート レプリケーション用にボリューム接続を許可するためのMVIPのバージョン、ユーザ名、パスワード、およびデータベース情報が含まれています。このキーの取り扱いには十分に注意し、ユーザ名やパスワードが誤って外部に漏れたり不正に使用されたりしないように適切に管理してください。

   注意 : ペアリング キーの文字はいっさい変更しないでください。変更するとキーは無効になります。
7. リモート クラスタで、**[Data Protection]** > **[Cluster Pairs]**の順に選択します。
8. **[Pair Cluster]**をクリックします。

9. **[Complete Pairing]**をクリックし、**[Pairing Key]**フィールドにペアリング キーを入力します（コピーして貼り付けることを推奨します）。
10. **[Complete Pairing]**をクリックします。

関連タスク

MVIPを使用したクラスタのペアリング（129ページ）
一方のクラスタのMVIPを使用してもう一方のクラスタとの接続を確立することにより、リアルタイム レプリケーション用に2つのクラスタをペアリングできます。この方法を使用するには、両方のクラスタに対するクラスタ管理者アクセスが必要です。クラスタをペアリングする前に、クラスタ管理者のユーザ名とパスワードを使用してクラスタ アクセスを認証します。

関連情報

Pairing clusters using a cluster pairing key (video)

クラスタ ペア接続の検証

クラスタ ペアリングが完了したら、クラスタ ペアの接続を検証して、レプリケーションが成功したかどうかを確認することができます。

手順

1. ローカル クラスタで、**[Data Protection]** > **[Cluster Pairs]**の順に選択します。
2. **[Cluster Pairs]**ウィンドウで、クラスタ ペアが接続されていることを確認します。
3. オプション: ローカル クラスタに戻り、**[Cluster Pairs]**ウィンドウでクラスタ ペアが接続されていることを確認します。

ボリュームのペアリング

クラスタ ペアのクラスタ間の接続を確立したら、一方のクラスタのボリュームをもう一方のクラスタのボリュームとペアリングできます。ボリューム ペアリング関係を確立する際、どちらのボリュームをレプリケーション ターゲットにするかを指定する必要があります。

開始する前に

- クラスタ ペアのクラスタ間の接続を確立しておきます。
- ペアリングするクラスタの一方または両方に対するクラスタ管理者権限が必要です。

タスク概要

接続されたクラスタ ペアの別々のストレージ クラスタに格納されている2つのボリュームをリアルタイム レプリケーション用にペアリングできます。2つのクラスタをペアリングしたあと、一方のクラスタのアクティブなボリュームをもう一方のクラスタに継続的にレプリケートするように設定することで継続的なデータ保護（CDP）を実現できます。また、どちらかのボリュームをレプリケーションのソースまたはターゲットとして割り当てることができます。

ボリュームは常に1対1でペアリングします。別のクラスタのあるボリュームとペアリングしたボリュームをさらに他のボリュームとペアリングすることはできません。

手順

1. 読み取り /書き込みアクセス可能なターゲット ボリュームの作成（132ページ）
レプリケーション プロセスでは2つのエンドポイント（ソース ボリュームとターゲット ボリューム）を使用します。ターゲット ボリュームは、レプリケーション時にデータを受け入れるよう、作成時に自動的に読み取り / 書き込みモードに設定されます。
2. ボリューム*ID*またはペアリング キーを使用したボリュームのペアリング（132ページ）

ペアリング プロセスでは、ボリュームIDまたはペアリング キーを使用して2個のボリュームをペアリングします。

3. ペアリングされたボリュームに対するレプリケーションのソースとターゲットの割り当て（135ページ）
ボリュームをペアリングしたら、ソース ボリュームとそのレプリケーション ターゲット ボリュームを割り当てる必要があります。ボリューム ペアのどちらのボリュームをレプリケーションのソースまたはターゲットにしてもかまいません。この手順は、ソース ボリュームが使用できなくなったときに、ソース ボリュームに送信されたデータをリモート ターゲット ボリュームにリダイレクトする場合にも使用できます。

読み取り / 書き込みアクセス可能なターゲット ボリュームの作成

レプリケーション プロセスでは2つのエンドポイント（ソース ボリュームとターゲット ボリューム）を使用します。ターゲット ボリュームは、レプリケーション時にデータを受け入れるよう、作成時に自動的に読み取り / 書き込みモードに設定されます。

タスク概要

手順

1. **[Management]** > **[Volumes]**の順に選択します。
2. **[Create Volume]**をクリックします。
3. [Create a New Volume]ダイアログ ボックスで、[Volume Name]にボリューム名を入力します。
4. ボリュームの合計サイズを入力し、ブロック サイズを選択して、アクセスを許可するアカウントを選択します。
5. **[Create Volume]**をクリックします。
6. [Active]ウィンドウで、ボリュームの[Actions]アイコンをクリックします。
7. **[Edit]**をクリックします。
8. アカウント アクセス レベルを[Replication Target]に変更します。
9. **[Save Changes]**をクリックします。

ボリュームIDまたはペアリング キーを使用したボリュームのペアリング

ペアリング プロセスでは、ボリュームIDまたはペアリング キーを使用して2個のボリュームをペアリングします。

手順

次のいずれかの方法を選択してボリュームをペアリングします。

- ボリュームIDを使用：この方法は、ボリュームをペアリングする両方のクラスタにクラスタ管理者としてアクセスできる場合に使用します。リモート クラスタのボリュームのボリュームIDを使用して接続を開始します。
- ペアリング キーを使用：この方法は、一方のクラスタにしかクラスタ管理者としてアクセスできない場合に使用します。ペアリング キーを生成し、そのキーをリモート クラスタで使用してボリュームをペアリングします。

  注 : ボリューム ペアリング キーには、暗号化されたボリューム情報が格納されており、機密情報が含まれている場合があります。このキーは必ず安全な方法で共有してください。

関連タスク

ボリューム*ID*を使用したボリュームのペアリング（133ページ）

リモート クラスタのクラスタ管理者のクレデンシャルがあれば、ボリュームをリモート クラスタの別のボリュームとペアリングできます。

ペアリング キーを使用したボリュームのペアリング（134ページ）
リモート クラスタのクラスタ管理者のクレデンシャルがない場合は、ペアリング キーを使用してボリュームをリモート クラスタの別のボリュームとペアリングできます。

ボリュームIDを使用したボリュームのペアリング

リモート クラスタのクラスタ管理者のクレデンシャルがあれば、ボリュームをリモート クラスタの別のボリュームとペアリングできます。

開始する前に

- 該当するボリュームを含むクラスタがペアリングされていることを確認します。
- リモート クラスタに新しいボリュームを作成しておきます。

  注 : ペアリング プロセスの完了後に、レプリケーションのソースとターゲットを割り当てることができます。ボリューム ペアのどちらのボリュームをレプリケーションのソースまたはターゲットにしてもかまいません。データが格納されておらず、かつサイズ、ボリュームのブロック サイズ設定（512eまたは4k）、QoS設定などの特性がソース ボリュームとまったく同じターゲット ボリュームを作成してください。レプリケーション ターゲットとして既存のボリュームを割り当てると、そのボリュームのデータは上書きされます。ターゲット ボリュームのサイズは、ソース ボリュームと同じかそれ以上にすることはできますが、ソース ボリュームより小さくすることはできません。
- ターゲットのボリュームIDを確認します。

手順

1. **[Management]** > **[Volumes]**の順に選択します。
2. ペアリングするボリュームの[Actions]アイコンをクリックします。
3. **[Pair]**をクリックします。
4. **[Pair Volume]**ダイアログ ボックスで、**[Start Pairing]**を選択します。
5. リモート クラスタにアクセスできるので、**[I Do]**を選択します。
6. **[Replication Mode]**をリストから選択します。
   - **Real-time (Asynchronous)** : 書き込みはソース クラスタでコミットされたあとにクライアントに通知されます。
   - **Real-time (Synchronous)** : 書き込みはソース クラスタとターゲット クラスタの両方でコミットされたあとにクライアントに通知されます。
   - **Snapshots Only** : ソース クラスタで作成されたSnapshotだけがレプリケートされます。ソース ボリュームのアクティブな書き込みはレプリケートされません。
7. リモート クラスタをリストから選択します。
8. リモート ボリュームのIDを選択します。
9. **[Start Pairing]**をクリックします。

   Webブラウザのタブが開き、リモート クラスタのElement UIに接続します。クラスタ管理者のクレデンシャルを使用してリモート クラスタにログオンするよう要求される場合があります。
10. リモート クラスタのElement UIで、**[Complete Pairing]**を選択します。
11. **[Confirm Volume Pairing]**で詳細を確認します。
12. **[Complete Pairing]**をクリックします。

ペアリング操作を確定すると、2つのクラスタでペアリング対象のボリュームを接続するプロセスが開始されます。ペアリング プロセス中は、**[Volume Pairs]**ウィンドウの**[Volume Status]**列にメッセージが表示されます。ボリューム ペアのソースとターゲットが割り当てられるまでは、次のメッセージが表示されます。

```
PausedMisconfigured
```

関連タスク

ペアリングされたボリュームに対するレプリケーションのソースとターゲットの割り当て（135ページ）

ボリュームをペアリングしたら、ソース ボリュームとそのレプリケーション ターゲット ボリュームを割り当てる必要があります。ボリューム ペアのどちらのボリュームをレプリケーションのソースまたはターゲットにしてもかまいません。この手順は、ソース ボリュームが使用できなくなったときに、ソース ボリュームに送信されたデータをリモート ターゲット ボリュームにリダイレクトする場合にも使用できます。

関連資料

ボリューム ペアリングに関するメッセージ（140ページ）

[Data Protection]タブの[Volume Pairs]ページで、最初のペアリング プロセスで生成されたメッセージを確認できます。このメッセージは、ペアのソースとターゲットの両方の[Replicating Volumes]リスト ビューに表示されます。

ボリューム ペアリングに関する警告（140ページ）

[Data Protection]タブの[Volume Pairs]ページには、ボリュームをペアリングしたあとに以下のメッセージが表示されます。これらのメッセージは、特に記載がないかぎり、ペアのソースとターゲット両方の[Replicating Volumes]リスト ビューに表示されます。

ペアリング キーを使用したボリュームのペアリング

リモート クラスタのクラスタ管理者のクレデンシャルがない場合は、ペアリング キーを使用してボリュームをリモート クラスタの別のボリュームとペアリングできます。

開始する前に

- 該当するボリュームを含むクラスタがペアリングされていることを確認します。
- ペアリングに使用するボリュームがリモート クラスタにあることを確認します。

注 : ペアリング プロセスの完了後に、レプリケーションのソースとターゲットを割り当てることができます。ボリューム ペアのどちらのボリュームをレプリケーションのソースまたはターゲットにしてもかまいません。データが格納されておらず、かつサイズ、ボリュームのブロック サイズ設定（512eまたは4k）、QoS設定などの特性がソース ボリュームとまったく同じターゲット ボリュームを作成してください。レプリケーション ターゲットとして既存のボリュームを割り当てると、そのボリュームのデータは上書きされます。ターゲット ボリュームのサイズは、ソース ボリュームと同じかそれ以上にすることはできますが、ソース ボリュームより小さくすることはできません。

手順

1. **[Management]** > **[Volumes]**の順に選択します。
2. ペアリングするボリュームの[Actions]アイコンをクリックします。
3. **[Pair]**をクリックします。
4. **[Pair Volume]**ダイアログ ボックスで、**[Start Pairing]**を選択します。
5. リモート クラスタにアクセスできないので、**[I Do Not]**を選択します。
6. **[Replication Mode]**をリストから選択します。
   - **Real-time (Asynchronous)** : 書き込みはソース クラスタでコミットされたあとにクライアントに通知されます。

- **Real-time (Synchronous)**：書き込みはソース クラスタとターゲット クラスタの両方でコミットされたあとにクライアントに通知されます。
- **Snapshots Only**：ソース クラスタで作成されたSnapshotだけがレプリケートされます。ソース ボリュームのアクティブな書き込みはレプリケートされません。

7. **[Generate Key]**をクリックします。

   注 : この操作により、ペアリング用のテキスト キーが生成され、ローカル クラスタにボリューム ペアが未設定の状態で作成されます。この手順を途中で中止した場合は、ボリューム ペアを手動で削除する必要があります。

8. ペアリング キーをクリップボードにコピーします。
9. このペアリング キーをリモート クラスタ サイトのクラスタ管理者に渡します。

   注 : ボリューム ペアリング キーの取り扱いには十分に注意し、誤って外部に漏れたり不正に使用されたりしないように適切に管理してください。

   注意 : ペアリング キーの文字はいっさい変更しないでください。変更するとキーは無効になります。

10. リモート クラスタのElement UIで、**[Management]** > **[Volumes]**の順に選択します。
11. ペアリングするボリュームの[Actions]アイコンをクリックします。
12. **[Pair]**をクリックします。
13. **[Pair Volume]**ダイアログ ボックスで、**[Complete Pairing]**を選択します。
14. もう一方のクラスタのペアリング キーを**[Pairing Key]**ボックスに貼り付けます。
15. **[Complete Pairing]**をクリックします。

    ペアリング操作を確定すると、2つのクラスタでペアリング対象のボリュームを接続するプロセスが開始されます。ペアリング プロセス中は、**[Volume Pairs]**ウィンドウの**[Volume Status]**列にメッセージが表示されます. ソースとターゲットが割り当てられるまで、ボリューム ペアには`PausedMisconfigured`と表示されます。

関連タスク

ペアリングされたボリュームに対するレプリケーションのソースとターゲットの割り当て（135ページ）

ボリュームをペアリングしたら、ソース ボリュームとそのレプリケーション ターゲット ボリュームを割り当てる必要があります。ボリューム ペアのどちらのボリュームをレプリケーションのソースまたはターゲットにしてもかまいません。この手順は、ソース ボリュームが使用できなくなったときに、ソース ボリュームに送信されたデータをリモート ターゲット ボリュームにリダイレクトする場合にも使用できます。

関連資料

ボリューム ペアリングに関するメッセージ（140ページ）

[Data Protection]タブの[Volume Pairs]ページで、最初のペアリング プロセスで生成されたメッセージを確認できます。このメッセージは、ペアのソースとターゲットの両方の[Replicating Volumes]リスト ビューに表示されます。

ボリューム ペアリングに関する警告（140ページ）

[Data Protection]タブの[Volume Pairs]ページには、ボリュームをペアリングしたあとに以下のメッセージが表示されます。これらのメッセージは、特に記載がないかぎり、ペアのソースとターゲット両方の[Replicating Volumes]リスト ビューに表示されます。

ペアリングされたボリュームに対するレプリケーションのソースとターゲットの割り当て

ボリュームをペアリングしたら、ソース ボリュームとそのレプリケーション ターゲット ボリュームを割り当てる必要があります。ボリューム ペアのどちらのボリュームをレプ

リケーションのソースまたはターゲットにしてもかまいません。この手順は、ソース ボリュームが使用できなくなったときに、ソース ボリュームに送信されたデータをリモート ターゲット ボリュームにリダイレクトする場合にも使用できます。

開始する前に

ソース ボリュームとターゲット ボリュームを含むクラスタへのアクセス権が必要です。

手順

1. ソース ボリュームを準備します。
   1. ソースとして割り当てるボリュームが含まれているクラスタで、**[Management]** > **[Volumes]**の順に選択します。
   2. ソースとして割り当てるボリュームの[Actions]アイコンをクリックし、**[Edit]**をクリックします。
   3. **[Access]**ドロップダウン リストで**[Read/Write]**を選択します。

      注意 : ソースとターゲットの割り当てを逆にしている場合、新しいレプリケーション ターゲットが割り当てられるまでボリューム ペアには`PausedMisconfigured`というメッセージが表示されます。

      アクセスを変更すると、ボリューム レプリケーションが一時停止し、データの転送が中止されます。これらの変更が両方のサイトで調整されていることを確認してください。

   4. **[Save Changes]**をクリックします。
2. ターゲット ボリュームを準備します。
   1. ターゲットとして割り当てるボリュームが含まれているクラスタで、**[Management]** > **[Volumes]**の順に選択します。
   2. ターゲットとして割り当てるボリュームの[Actions]アイコンをクリックし、**[Edit]**をクリックします。
   3. **[Access]**ドロップダウン リストで**[Replication Target]**を選択します。

      注意 : レプリケーション ターゲットとして既存のボリュームを割り当てると、そのボリュームのデータは上書きされます。新しいターゲット ボリュームは、データが格納されておらず、かつサイズ、512e、QoSなどの特性がソース ボリュームとまったく同じであることが必要です。ターゲット ボリュームのサイズは、ソース ボリュームと同じかそれ以上にすることはできますが、ソース ボリュームより小さくすることはできません。

   4. **[Save Changes]**をクリックします。

関連タスク

ボリューム*ID*を使用したボリュームのペアリング（133ページ）

リモート クラスタのクラスタ管理者のクレデンシャルがあれば、ボリュームをリモート クラスタの別のボリュームとペアリングできます。

ペアリング キーを使用したボリュームのペアリング（134ページ）

リモート クラスタのクラスタ管理者のクレデンシャルがない場合は、ペアリング キーを使用してボリュームをリモート クラスタの別のボリュームとペアリングできます。

ボリューム レプリケーションの検証

ボリュームがレプリケートされたら、ソース ボリュームとターゲット ボリュームがアクティブになっていることを確認する必要があります。状態がアクティブな場合は、ボリュームがペアリングされ、ソース ボリュームからターゲット ボリュームにデータが送信されて同期されています。

手順

1. 両方のクラスタで、**[Data Protection]** > **[Volume Pairs]**を選択します。
2. ボリュームのステータスが`Active`であることを確認します。

関連資料

ボリューム ペアリングに関する警告（140ページ）

[Data Protection]タブの[Volume Pairs]ページには、ボリュームをペアリングしたあとに以下のメッセージが表示されます。これらのメッセージは、特に記載がないかぎり、ペアのソースとターゲット両方の[Replicating Volumes]リスト ビューに表示されます。

レプリケーション後のボリューム関係の削除

レプリケーションが完了してボリューム ペア関係が不要になったら、ボリューム関係を削除できます。

手順

1. **[Data Protection]** > **[Volume Pairs]**の順に選択します。
2. 削除するボリューム ペアの[Actions]アイコンをクリックします。
3. **[Delete]**をクリックします。
4. メッセージを確認します。

ボリューム関係の管理

レプリケーションの一時停止、ボリューム ペアリングの反転、レプリケーション モードの変更、ボリューム ペアの削除、クラスタ ペアの削除など、さまざまな方法でボリューム関係を管理できます。

関連タスク

レプリケーションの一時停止（137ページ）

I/O処理を短時間停止する必要がある場合は、レプリケーションを手動で一時停止できます。I/O処理が急増したために処理の負荷を軽減する場合、レプリケーションを一時停止することができます。

レプリケーション モードの変更（138ページ）

ボリューム ペアのプロパティを編集して、ボリューム ペア関係のレプリケーション モードを変更することができます。

ボリューム ペアの削除（138ページ）

2つのボリューム間のペア関係を解除するには、ボリューム ペアを削除します。

レプリケーションの一時停止

I/O処理を短時間停止する必要がある場合は、レプリケーションを手動で一時停止できます。I/O処理が急増したために処理の負荷を軽減する場合、レプリケーションを一時停止することができます。

手順

1. **[Data Protection]** > **[Volume Pairs]**の順に選択します。

2. ボリューム ペアの[Actions]アイコンをクリックします。
3. **[Edit]**をクリックします。
4. **[Edit Volume Pair]**ペインで、レプリケーション プロセスを手動で一時停止します。

   注意 : ボリューム レプリケーションを手動で一時停止または再開すると、データの転送が中止または再開されます。これらの変更が両方のサイトで調整されていることを確認してください。

5. **[Save Changes]**をクリックします。

レプリケーション モードの変更

ボリューム ペアのプロパティを編集して、ボリューム ペア関係のレプリケーション モードを変更することができます。

手順

1. **[Data Protection]** > **[Volume Pairs]**の順に選択します。
2. ボリューム ペアの[Actions]アイコンをクリックします。
3. **[Edit]**をクリックします。
4. **[Edit Volume Pair]**ペインで、新しいレプリケーション モードを選択します。
   - **Real-time (Asynchronous)**：書き込みはソース クラスタでコミットされたあとにクライアントに通知されます。
   - **Real-time (Synchronous)** : 書き込みはソース クラスタとターゲット クラスタの両方でコミットされたあとにクライアントに通知されます。
   - **Snapshots Only**：ソース クラスタで作成されたSnapshotだけがレプリケートされます。ソース ボリュームのアクティブな書き込みはレプリケートされません。

     注意 : レプリケーション モードの変更はすぐに反映されます。これらの変更が両方のサイトで調整されていることを確認してください。

5. **[Save Changes]**をクリックします。

ボリューム ペアの削除

2つのボリューム間のペア関係を解除するには、ボリューム ペアを削除します。

手順

1. **[Data Protection]** > **[Volume Pairs]**の順に選択します。
2. 削除するボリューム ペアの[Actions]アイコンをクリックします。
3. **[Delete]**をクリックします。
4. メッセージを確認します。

クラスタ ペアの削除

ペアのいずれか一方のクラスタのElement UIから、クラスタ ペアを削除できます。

手順

1. **[Data Protection]** > **[Cluster Pairs]**の順にクリックします。
2. クラスタ ペアの[Actions]アイコンをクリックします。
3. 表示されたメニューで**[Delete]**をクリックします。
4. 操作を確定します。
5. クラスタ ペアリングのもう一方のクラスタで同じ手順を実行します。

クラスタ ペアの詳細

[Data Protection]タブの[Cluster Pairs]ページには、ペアリング済みのクラスタまたはペアリング中のクラスタに関する情報が表示されます。[Status]列に、ペアリングおよび進捗に関するメッセージが表示されます。

ID

各クラスタ ペアにシステムから割り当てられたID。

Remote Cluster Name

ペア内のもう一方のクラスタの名前。

Remote MVIP

ペア内のもう一方のクラスタの管理仮想IPアドレス。

Status

リモート クラスタのレプリケーション ステータス。

Replicating Volumes

クラスタ内のレプリケーション用にペアリングされたボリュームの数。

UUID

ペア内の各クラスタに指定された一意のID。

ボリューム ペアの詳細

[Data Protection]タブの[Volume Pairs]ページには、ペアリング済みまたはペアリング中のボリュームに関する次の情報が表示されます。[Volume Status]列に、ペアリングおよび進捗に関するメッセージが表示されます。

ID

システムによって生成されたボリュームのID。

Name

ボリュームの作成時に指定した名前。ボリューム名は最大223文字で、使用できる文字はa～z、0～9、およびダッシュ（-）です。

Account

ボリュームに割り当てられているアカウントの名前。

Volume Status

ボリュームのレプリケーション ステータス。

Snapshot Status

Snapshotボリュームのステータス。

Mode

クライアントの書き込みレプリケーション方法。有効な値は次のとおりです。

- Async
- Snapshot-Only
- Sync

Direction

ボリューム データの方向。

- ソース ボリューム アイコン（→）は、クラスタの外部のターゲットにデータを書き出していることを示します。
- ターゲット ボリューム アイコン（←）は、外部のソースからローカル ボリュームにデータが書き込まれていることを示します。

Async Delay

ボリュームが最後にリモート クラスタと同期されてからの時間。ボリュームがペアリングされていない場合、値はnullになります。

Remote Cluster

ボリュームが配置されているリモート クラスタの名前。

Remote Volume ID

リモート クラスタのボリュームのボリュームID。

Remote Volume Name

リモート ボリュームの作成時に指定した名前。

ボリューム ペアリングに関するメッセージ

[Data Protection]タブの[Volume Pairs]ページで、最初のペアリング プロセスで生成されたメッセージを確認できます。このメッセージは、ペアのソースとターゲットの両方の[Replicating Volumes]リスト ビューに表示されます。

PausedDisconnected

ソース レプリケーションまたは同期RPCがタイムアウトし、 リモート クラスタへの接続が失われました。クラスタへのネットワーク接続を確認してください。

ResumingConnected

リモート レプリケーションの同期がアクティブになりました。同期処理が開始され、データを待っている状態です。

ResumingRRSync

ペア クラスタにボリューム メタデータのSingle Helixコピーを作成しています。

ResumingLocalSync

ペア クラスタにボリューム メタデータのDouble Helixコピーを作成しています。

ResumingDataTransfer

データ転送が再開されました。

Active

ボリュームがペアリングされ、ソース ボリュームからターゲット ボリュームにデータが送信されて同期されています。

Idle

実行中のレプリケーション アクティビティはありません。

ボリューム ペアリングに関する警告

[Data Protection]タブの[Volume Pairs]ページには、ボリュームをペアリングしたあとに以下のメッセージが表示されます。これらのメッセージは、特に記載がないかぎり、ペアのソースとターゲット両方の[Replicating Volumes]リスト ビューに表示されます。

PausedClusterFull

ターゲット クラスタがいっぱいのため、ソース レプリケーションと一括データ転送を続行できません。このメッセージは、ペアのソースにのみ表示されます。

PausedExceededMaxSnapshotCount

ターゲット ボリュームに格納されたSnapshotの数が最大数に達しており、Snapshotをこれ以上レプリケートできません。

PausedManual

ローカル ボリュームが手動で一時停止されています。レプリケーションを再開するには、一時停止を解除する必要があります。

PausedManualRemote

リモート ボリュームが手動で一時停止されています。レプリケーションを再開するには、リモート ボリュームの一時停止を手動で解除する必要があります。

PausedMisconfigured

ソースとターゲットがアクティブになるのを待っています。手動でレプリケーションを再開する必要があります。

PausedQoS

ターゲットQoSの受信IOを維持できませんでした。レプリケーションは自動で再開されます。このメッセージは、ペアのソースにのみ表示されます。

PausedSlowLink

低速リンクが検出されたため、レプリケーションが停止しました。レプリケーションは自動で再開されます。このメッセージは、ペアのソースにのみ表示されます。

PausedVolumeSizeMismatch

ソース ボリュームよりも小さいターゲット ボリュームが使用されています。

PausedXCopy

ソース ボリュームに対してSCSI XCOPYコマンドを実行中です。このコマンドが完了するまでレプリケーションを再開できません。このメッセージは、ペアのソースにのみ表示されます。

StoppedMisconfigured

永続的な設定エラーが検出されました。リモート ボリュームがパージされたかペアが解除されました。対処方法はなく、新しいペアリングを確立する必要があります。

ElementクラスタとONTAPクラスタ間でのSnapMirrorレプリケーション

NetApp Element UIの[Data Protection]タブで、SnapMirror関係を作成することができます。この情報をユーザ インターフェイスで確認するには、SnapMirror機能を有効にする必要があります。

タスク概要

NetApp Elementソフトウェア クラスタとONTAPクラスタの間のSnapMirrorレプリケーションでは、IPv6はサポートされていません。

ネットアップのビデオ: SnapMirror for NetApp HCI and Element Software

関連概念

*SnapMirror*エンドポイント（143ページ）
SnapMirrorエンドポイントは、NetApp Elementソフトウェアを実行するクラスタのレプリケーション ターゲットとして機能するONTAPクラスタです。SnapMirror関係を作成する前に、SnapMirrorエンドポイントを作成する必要があります。

*SnapMirror*ラベル（145ページ）
SnapMirrorラベルは、指定したSnapshotを関係の保持ルールに従って転送するためのマーカーとして機能します。

*SnapMirror*関係（146ページ）
SnapMirror関係は、ソース ボリュームとデスティネーション ボリュームの間の関係です。データは、NetApp Snapshotコピーを使用してデスティネーション ボリュームにレプリケ

ートされます。SnapMirror関係は、 NetApp Element UIを使用して編集および削除できます。

SnapMirrorを使用したディザスタ リカバリ（150ページ）
NetApp Elementソフトウェアを実行しているボリュームまたはクラスタで問題が発生した場合は、SnapMirror機能を使用して関係を解除し、デスティネーション ボリュームにフェイルオーバーできます。

関連タスク

クラスタで*SnapMirror*の有効化（142ページ）
クラスタ レベルのSnapMirror機能は、NetApp Element UIを使用して手動で有効にする必要があります。SnapMirror機能はデフォルトでは無効になっており、新規インストール時やアップグレード時に自動的に有効になることはありません。SnapMirror機能の有効化は1度だけ実行します。

ボリュームで*SnapMirror*の有効化（143ページ）
ボリュームのSnapMirrorはElement UIで有効にする必要があります。これにより、指定したONTAPボリュームにデータをレプリケートできるようになります。これは、NetApp Elementソフトウェアを実行しているクラスタの管理者がSnapMirrorによるボリュームの制御を許可することを意味します。

関連情報

Building your Data Fabric with NetApp HCI, ONTAP, and Converged Infrastructure
*NetApp Element*ソフトウェアと*ONTAP*のレプリケーション

SnapMirrorの概要

NetApp Elementソフトウェアを実行するシステムでは、NetApp ONTAPシステムとの間でのSnapMirror機能を使用したSnapshotのコピーとリストアがサポートされます。

Elementを実行するシステムは、9.3以降のONTAPシステムのSnapMirrorと直接通信できます。NetApp Element APIには、クラスタ、ボリューム、SnapshotでSnapMirror機能を有効にするメソッドが用意されています。さらに、Element UIには、ElementソフトウェアとONTAPシステムの間のSnapMirror関係を管理するために必要なすべての機能が搭載されています。

機能は限定されますが、特定のユースケースでONTAPボリュームをElementボリュームにレプリケートできます。詳細については、ONTAPのドキュメントを参照してください。

関連情報

Replication between Element software and ONTAP

クラスタでのSnapMirrorの有効化

クラスタ レベルのSnapMirror機能は、NetApp Element UIを使用して手動で有効にする必要があります。SnapMirror機能はデフォルトでは無効になっており、新規インストール時やアップグレード時に自動的に有効になることはありません。SnapMirror機能の有効化は1度だけ実行します。

開始する前に

ストレージ クラスタでNetApp Elementソフトウェアが実行されている必要があります。

タスク概要

SnapMirrorは、Elementソフトウェアを実行しているクラスタでNetApp ONTAPシステムのボリュームが使用されている場合にのみ有効にすることができます。クラスタがNetApp ONTAPボリュームを使用する目的で接続されている場合にのみ、SnapMirror機能を有効にしてください。

手順

1. **[Clusters]** > **[Settings]**の順にクリックします。
2. クラスタ用のSnapMirror設定を探します。
3. **[Enable SnapMirror]**をクリックします。

   注 : SnapMirror機能を有効にすると、Elementソフトウェアの設定が永続的に変更されます。SnapMirror機能を無効にしてデフォルト設定に戻すには、クラスタを工場出荷時のイメージに戻す必要があります。
4. **[Yes]**をクリックして、SnapMirror設定の変更を確定します。

ボリュームでのSnapMirrorの有効化

ボリュームのSnapMirrorはElement UIで有効にする必要があります。これにより、指定したONTAPボリュームにデータをレプリケートできるようになります。これは、NetApp Elementソフトウェアを実行しているクラスタの管理者がSnapMirrorによるボリュームの制御を許可することを意味します。

開始する前に

- クラスタのElement UIでSnapMirrorを有効にしておきます。
- 使用可能なSnapMirrorエンドポイントが必要です。
- ボリュームのブロック サイズが512eである必要があります。
- ボリュームがリモート レプリケーションに参加していない必要があります。
- ボリュームのアクセス タイプがレプリケーション ターゲットでない必要があります。

注 : このプロパティは、ボリュームまたはボリュームのクローンを作成するときにも設定できます。

手順

1. **[Management]** > **[Volumes]**の順にクリックします。
2. SnapMirrorを有効にするボリュームの[Actions]アイコンをクリックします。
3. 表示されたメニューで**[Edit]**を選択します。
4. **[Edit Volume]**ダイアログ ボックスで、**[Enable SnapMirror]**チェック ボックスをオンにします。
5. **[Save Changes]**をクリックします。

SnapMirrorエンドポイント

SnapMirrorエンドポイントは、NetApp Elementソフトウェアを実行するクラスタのレプリケーション ターゲットとして機能するONTAPクラスタです。SnapMirror関係を作成する前に、SnapMirrorエンドポイントを作成する必要があります。

Elementソフトウェアを実行しているストレージ クラスタでは、SnapMirrorエンドポイントを最大4つまで作成して管理することができます。

注 : APIを使用して作成され、クレデンシャルが保存されていない既存のエンドポイントは、Element UIには表示されて存在を確認することはできますが、Element UIで管理することはできません。このエンドポイントを管理するには、Element APIを使用する必要があります。APIメソッドについては、APIリファレンス情報を参照してください。

関連情報

*Element API*を使用したストレージの管理

エンドポイントの作成

関係を作成する前に、NetApp Element UIでSnapMirrorエンドポイントを作成する必要があります。

開始する前に

- ストレージ クラスタのElement UIでSnapMirrorを有効にしておきます。
- エンドポイントのONTAPクレデンシャルを確認しておきます。

手順

1. **[Data Protection]** > **[SnapMirror Endpoints]**の順にクリックします。
2. **[Create Endpoint]**をクリックします。
3. **[Create a New Endpoint]**ダイアログ ボックスで、ONTAPシステムのクラスタ管理IPアドレスを入力します。
4. エンドポイントに関連付けるONTAP管理者クレデンシャルを入力します。
5. **[Create Endpoint]**をクリックします。

SnapMirrorエンドポイントの詳細

[Data Protection]タブの[SnapMirror Endpoints]ページには、クラスタ上のすべてのSnapMirrorエンドポイントの情報（ID、クラスタ名、クラスタ管理IPなど）が表示されます。

ID

エンドポイントのID。

Cluster Name

デスティネーション クラスタの名前。

Cluster Management IP

デスティネーション クラスタのIPアドレス。

LIF

Elementとの通信に使用されるONTAPクラスタ間論理インターフェイスのリスト。

Relationships

このエンドポイントに関連付けられている関係の数。

Status

SnapMirrorエンドポイントの現在のステータス。有効な値は次のとおりです。

- connected
- disconnected
- unmanaged

エンドポイントの編集

SnapMirrorエンドポイントの変更は、NetApp Element UIで行う必要があります。

開始する前に

- クラスタのElement UIでSnapMirrorを有効にしておきます。
- 既存のSnapMirrorエンドポイントが変更可能である必要があります。

手順

1. **[Data Protection]** > **[SnapMirror Endpoints]**の順にクリックします。
2. 編集するエンドポイントの[Actions]アイコンをクリックします。
3. 表示されたメニューで**[Edit]**を選択します。

4. **[Cluster Management IP]**で、必要に応じてIPアドレスを編集します。
5. **[ONTAP Credentials]**で、必要に応じてユーザ名またはパスワードを編集します。
6. **[Save Changes]**をクリックします。

エンドポイントの削除

SnapMirrorエンドポイントの削除は、 NetApp Element UIで行う必要があります。

開始する前に

- クラスタのElement UIでSnapMirrorを有効にしておきます。
- 既存のSnapMirrorエンドポイントが削除可能である必要があります。

手順

1. **[Data Protection]** > **[SnapMirror Endpoints]**の順にクリックします。
2. 削除するエンドポイントの[Actions]アイコンをクリックします。
3. 表示されたメニューで**[Delete]**を選択します。
4. 操作を確定します。
5. SnapMirrorエンドポイントのリストを更新して、エンドポイントが削除されたことを確認します。

SnapMirrorラベル

SnapMirrorラベルは、指定したSnapshotを関係の保持ルールに従って転送するためのマーカーとして機能します。

ラベルを適用したSnapshotは、SnapMirrorレプリケーションのターゲットとしてマークされます。関係の役割は、ラベルが一致するSnapshotを選択してデスティネーション ボリュームにコピーし、正しい数のコピーが保持されるようにすることで、データ転送にルールを適用することです。その際、ポリシーを参照することで数と保持期間が特定されます。ポリシーには任意の数のルールを追加でき、各ルールには固有なラベルがあります。このラベルがSnapshotと保持ルールの間のリンクとして機能します。

SnapMirrorラベルによって、選択したSnapshot、グループSnapshot、またはスケジュールに適用されるルールが決まります。

SnapshotへのSnapMirrorラベルの追加

SnapMirrorラベルは、SnapMirrorエンドポイントでのSnapshot保持ポリシーを指定します。ラベルは、SnapshotおよびグループSnapshotに追加できます。

開始する前に

- クラスタでSnapMirrorを有効にしておきます。
- 追加するラベルがONTAPに存在している必要があります。

タスク概要

追加できるラベルは、既存のSnapMirror関係ダイアログ ボックスまたはNetApp ONTAP System Managerで確認できます。

注意 : グループSnapshotにラベルを追加すると、個々のSnapshotに追加された既存のラベルがすべて上書きされます。

手順

1. **[Data Protection]** > **[Snapshots]**または**[Group Snapshots]**の順にクリックします。

2. SnapMirrorラベルを追加するSnapshotまたはグループSnapshotの[Actions]アイコンをクリックします。
3. **[Edit Snapshot]**ダイアログ ボックスで、**[SnapMirror Label]**フィールドにテキストを入力します。このラベルは、SnapMirror関係に適用されるポリシー内のルール ラベルと同じである必要があります。
4. **[Save Changes]**をクリックします。

SnapshotスケジュールへのSnapMirrorラベルの追加

SnapMirrorラベルをSnapshotスケジュールに追加して、SnapMirrorポリシーが適用されるようにすることができます。追加できるラベルは、既存のSnapMirror関係ダイアログ ボックスまたはNetApp ONTAP System Managerで確認できます。

開始する前に

- SnapMirrorをクラスタ レベルで有効にしておきます。
- 追加するラベルがONTAPに存在している必要があります。

手順

1. **[Data Protection]** > **[Schedules]**の順にクリックします。
2. 次のいずれかの方法で、SnapMirrorラベルをスケジュールに追加します。

オプション	手順
新しいスケジュールの作成	1. **[Create Schedule]**を選択します。 2. 他の関連する詳細情報をすべて入力します。 3. **[Create Schedule]**を選択します。
既存のスケジュールの変更	1. ラベルを追加するスケジュールの[Actions]アイコンをクリックし、**[Edit]**を選択します。 2. 表示されたダイアログ ボックスで、**[SnapMirror Label]**フィールドにテキストを入力します。 3. **[Save Changes]**を選択します。

関連タスク

*Snapshot*スケジュールの作成（124ページ）
ボリュームのSnapshotのスケジュールを設定し、指定した間隔でSnapshotを自動的に作成できます。

SnapMirror関係

SnapMirror関係は、ソース ボリュームとデスティネーション ボリュームの間の関係です。データは、NetApp Snapshotコピーを使用してデスティネーション ボリュームにレプリケートされます。SnapMirror関係は、NetApp Element UIを使用して編集および削除できます。

SnapMirror関係の作成

SnapMirror関係は、NetApp Element UIで作成する必要があります。

開始する前に

ボリュームでSnapMirrorを有効にしておきます。

注 : ボリュームでSnapMirrorが有効になっていない状態でElement UIから関係の作成を選択すると、そのボリュームで自動的にSnapMirrorが有効になります。

手順

1. **[Management]** > **[Volumes]**の順にクリックします。
2. 関係に含めるボリュームの[Actions]アイコンをクリックします。
3. **[Create a SnapMirror Relationship]**をクリックします。
4. **[Create a SnapMirror Relationship]**ダイアログ ボックスで、**[Endpoint]**リストからエンドポイントを選択します。
5. 新しいONTAPボリュームと既存のONTAPボリュームのどちらを使用して関係を作成するかを選択します。
6. Element UIで新しいONTAPボリュームを作成する場合は、**[Create new volume]**をクリックします。
   1. この関係に対し**[Storage Virtual Machine]**を選択します。
   2. ドロップダウン リストから**[Aggregate]**を選択します。
   3. **[Volume Name Suffix]**フィールドにサフィックスを入力します。

      注 : システムによってソース ボリューム名が検出され、**[Volume Name]**フィールドにコピーされます。入力したサフィックスは、この名前に付加されます。
   4. **[Create Destination Volume]**をクリックします。
7. 既存のONTAPボリュームを使用する場合は、**[Use existing volume]**をクリックします。
   1. この関係に対し**[Storage Virtual Machine]**を選択します。
   2. この新しい関係のデスティネーションとなるボリュームを選択します。
8. **[Relationship Details]**セクションで、ポリシーを選択します。選択したポリシーにkeepルールがある場合は、[Rules]テーブルにそのルールおよび関連付けられたラベルが表示されます。
9. オプション: スケジュールを選択します

   これにより、関係でコピーが作成される頻度が決まります。
10. オプション: **[Limit Bandwidth to]**フィールドに、この関係に関連付けられるデータ転送が消費できる最大帯域幅を入力します。
11. この時点で初期化が実行されないよう、**[Initialize]**チェック ボックスがオフになっていることを確認します。

    注 : 初期化には時間がかかる場合があります。ピーク時以外の時間帯に実行することを推奨します。初期化ではベースライン転送が実行されます。つまり、ソースボリュームのSnapshotコピーが作成され、そのコピーとコピーが参照するすべてのデータ ブロックがデスティネーション ボリュームに転送されます。初期化は手動で実行できるほか、スケジュールに従って初期化プロセス（および後続の更新）が開始されるようにすることもできます。
12. **[Create Relationship]**をクリックします。
13. **[Data Protection]** > **[SnapMirror Relationships]**の順にクリックして、新しいSnapMirror関係を表示します。

SnapMirror関係の詳細

[Data Protection]タブの[SnapMirror Relationships]ページには、クラスタ上のすべてのSnapMirror関係に関する情報（エンドポイントID、デスティネーション クラスタの名前、デスティネーション ボリュームの名前など）が表示されます。

Endpoint ID

エンドポイントのID。

Source Cluster
ソース クラスタの名前。

Source Volume
ソース ボリュームの名前。

Destination Cluster
デスティネーションONTAPクラスタの名前。

Destination Volume
デスティネーションONTAPボリュームの名前。

State

デスティネーション ボリュームの現在の関係の状態。有効な値は次のとおりです。

- uninitialized：デスティネーション ボリュームは初期化されていません。
- snapmirrored：デスティネーション ボリュームは初期化され、SnapMirror更新を受信できる状態です。
- broken-off：デスティネーション ボリュームは読み書き可能な状態にあり、Snapshotが存在します。

Status

関係の現在のステータス。有効な値は、idle、transferring、checking、quiescing、quiesced、queued、preparing、finalizing、aborting、およびbreakingです。

Lag Time
デスティネーション システムがソース システムより遅延している時間（秒）。遅延時間は転送スケジュールの間隔以下であることが必要です。

Bandwidth Limit
関係に関連付けられるデータ転送が消費できる最大帯域幅。

Last Transferred
前回転送されたSnapshotのタイムスタンプ。クリックすると詳細が表示されます。

Policy Name
関係のONTAP SnapMirrorポリシーの名前。

Policy Type

関係に対して選択されたONTAP SnapMirrorポリシーのタイプ。有効な値は次のとおりです。

- async_mirror
- mirror_vault

Schedule Name
関係に対して選択されたONTAPシステム上の既存のスケジュールの名前。

SnapMirror関係の編集

SnapMirror関係の編集は、NetApp Element UIで行う必要があります。

開始する前に

- ボリュームでSnapMirrorを有効にしておきます。
- 既存のSnapMirror関係が変更可能である必要があります。

手順

1. **[Data Protection]** > **[SnapMirror Relationships]**の順にクリックします。

2. 編集する関係の[Actions]アイコンをクリックします。
3. **[Edit]**をクリックします。
4. **[Edit SnapMirror Relationship]**ダイアログ ボックスで、ポリシー、スケジュール、帯域幅制限の設定を変更できます。
5. **[Save Changes]**をクリックします。

SnapMirror関係の削除

NetApp Element UIで、SnapMirror関係を削除することができます。

開始する前に

- クラスタのElement UIでSnapMirrorを有効にしておきます。
- 既存のSnapMirror関係が削除可能である必要があります。

手順

1. **[Data Protection]** > **[SnapMirror Relationships]**の順にクリックします。
2. 削除する関係の[Actions]アイコンをクリックします。
3. 表示されたメニューで**[Delete]**を選択します。
4. 操作を確定します。
5. SnapMirror関係のリストを更新して、関係が削除されたことを確認します。

SnapMirror関係の操作

[Data Protection]タブの[SnapMirror Relationships]ページで関係を設定できます。[Actions]アイコンから使用できるオプションは次のとおりです。

Edit

関係のポリシーまたはスケジュールを編集します。

Delete

SnapMirror関係を削除します。デスティネーション ボリュームは削除されません。

Initialize

データの初回のベースライン転送を実行し、新しい関係を確立します。

Update

関係を更新し、前回の更新以降に追加された新しいデータとSnapshotコピーをデスティネーションにレプリケートします。

Quiesce

以降、関係が更新されないようにします。

Resume

休止されている関係を再開します。

Break

デスティネーション ボリュームを読み書き可能にし、実行中の転送とそれ以降の転送をすべて停止します。クライアントが元のソース ボリュームを使用していないことを確認します。逆再同期処理を実行すると、元のソース ボリュームは読み取り専用になります。

Resync

解除した関係を、解除前と同じ方向で再確立します。

Reverse Resync

逆方向の関係を新たに作成して初期化するために必要な手順を自動化します。この操作は、既存の関係が解除状態にある場合にのみ実行できます。この処理で現在

の関係が削除されることはありません。元のソース ボリュームが最新の共通Snapshotコピーにリバートされ、デスティネーションと再同期されます。前回成功したSnapMirror更新以降に、元のソース ボリュームに対して行われた変更は失われます。現在のデスティネーション ボリュームに対して行われた変更や新しく書き込まれたデータがすべて、元のソース ボリュームに送信されます。

Abort

実行中の転送をキャンセルします。中止された関係に対してSnapMirror更新が実行されると、前回の転送が、中止前に作成された最後の再開チェックポイントから続行されます。

SnapMirrorを使用したディザスタ リカバリ

NetApp Elementソフトウェアを実行しているボリュームまたはクラスタで問題が発生した場合は、SnapMirror機能を使用して関係を解除し、デスティネーション ボリュームにフェイルオーバーできます。

注 : 元のクラスタが完全な障害状態にある場合、または存在しない場合は、ネットアップ サポートに連絡してください。

Elementクラスタからのフェイルオーバーの実行

Elementクラスタからフェイルオーバーを実行して、デスティネーション ボリュームを読み書き可能にし、デスティネーション側のホストがアクセスできるようにすることができます。Elementクラスタからフェイルオーバーを実行する前に、SnapMirror関係を解除する必要があります。

開始する前に

- SnapMirror関係が存在し、デスティネーション ボリュームに有効なSnapshotが1つ以上あることが必要です。
- プライマリ サイトでの計画外停止または計画的停止のために、デスティネーション ボリュームへのフェイルオーバーが必要な状況にあります。

タスク概要

NetApp Element UIを使用してフェイルオーバーを実行します。Element UIを使用できない場合は、ONTAP System ManagerまたはONTAP CLIを使用して、関係を解除するコマンドを実行することもできます。

手順

1. Element UIで、**[Data Protection]** > **[SnapMirror Relationships]**の順にクリックします。
2. フェイルオーバーするソース ボリュームとの間に確立されている関係を探します。
3. この関係の[Actions]アイコンをクリックします。
4. **[Break]**をクリックします。
5. 操作を確定します。

   デスティネーション クラスタのボリュームで読み取り / 書き込みアクセスが可能となり、アプリケーション ホストにそのボリュームをマウントして本番環境のワークロードを再開できるようになります。この操作によって、SnapMirrorレプリケーションがすべて停止します。関係の状態は「Broken-off」になります。

Elementへのフェイルバックの実行

プライマリ側の問題が軽減されたら、元のソース ボリュームを再同期し、NetApp Element ソフトウェアへのフェイルバックを実行する必要があります。実行する手順は、元のソース ボリュームがまだ存在しているか、あるいは新たに作成したボリュームへのフェイルバックが必要かによって変わります。

関連概念

*SnapMirror*フェイルバックのシナリオ（151ページ）
SnapMirrorディザスタ リカバリ機能について、2つのフェイルバック シナリオを例に説明します。どちらのシナリオも、元の関係がフェイルオーバーされた（解除された）状況を前提としています。

関連タスク

ソース ボリュームが存在する場合のフェイルバックの実行（152ページ）
NetApp Element UIを使用して、元のソース ボリュームを再同期し、フェイルバックを実行できます。以下は、元のソース ボリュームが存在している場合の手順です。

ソース ボリュームが存在しない場合のフェイルバックの実行（153ページ）
NetApp Element UIを使用して、元のソース ボリュームを再同期し、フェイルバックを実行できます。このセクションは、元のソース ボリュームが失われ、元のクラスタはそのまま維持されているシナリオに当てはまります。新しいクラスタにリストアする方法については、ネットアップ サポート サイトのドキュメントを参照してください。

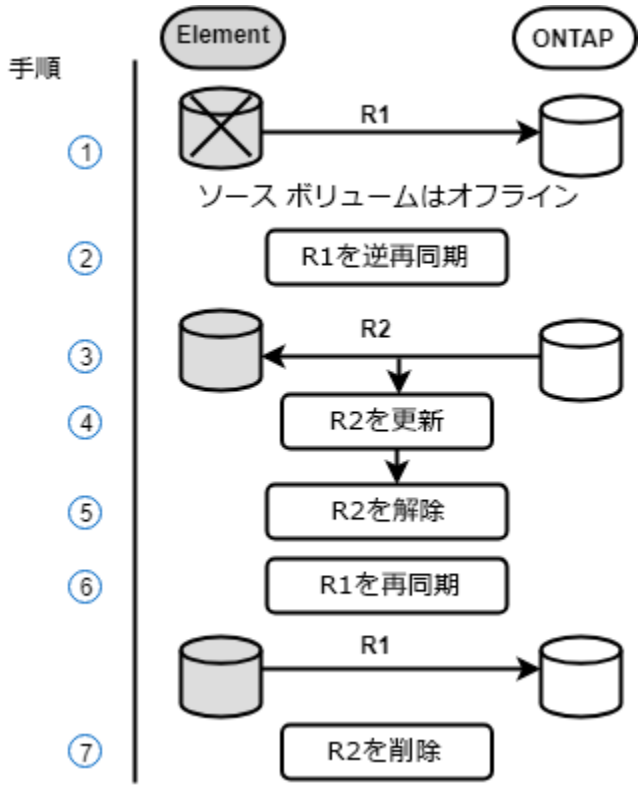
SnapMirrorフェイルバックのシナリオ

SnapMirrorディザスタ リカバリ機能について、2つのフェイルバック シナリオを例に説明します。どちらのシナリオも、元の関係がフェイルオーバーされた（解除された）状況を前提としています。

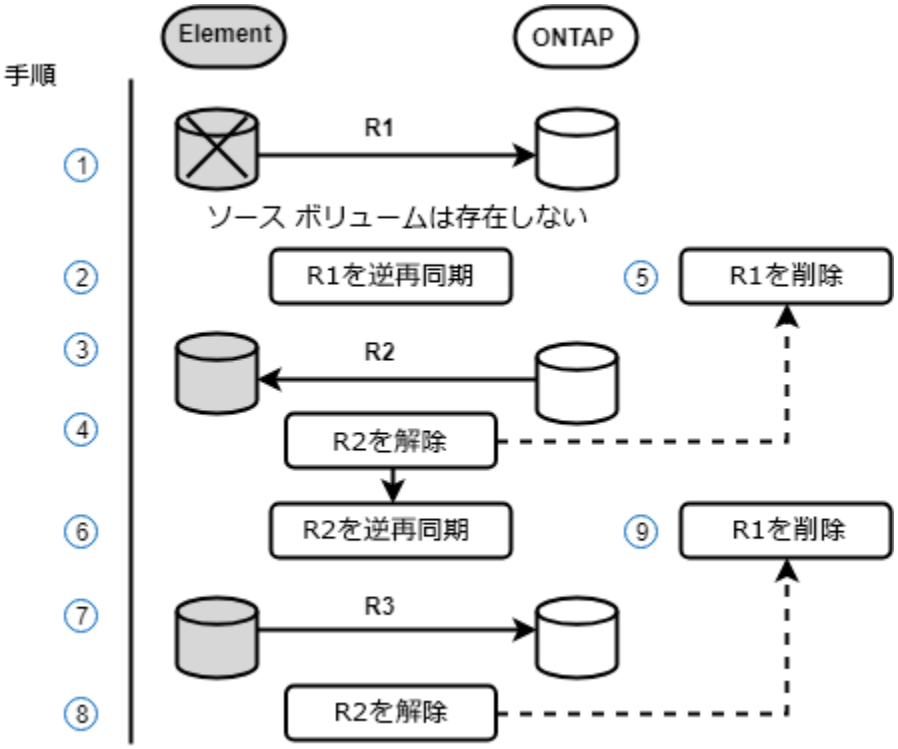
参考のために、対応する手順の各ステップを付記します。

注 : 以下の各例のR1は元の関係で、NetApp Elementソフトウェアを実行しているクラスタが元のソース ボリューム（Element）、ONTAPが元のデスティネーション ボリューム（ONTAP）です。R2とR3は、逆再同期処理で作成された逆の関係です。

次の図は、ソース ボリュームが存在する場合のフェイルバック シナリオを示しています。



次の図は、ソース ボリュームが存在しない場合のフェイルバック シナリオを示しています。



関連タスク

ソース ボリュームが存在する場合のフェイルバックの実行（152ページ）
NetApp Element UIを使用して、元のソース ボリュームを再同期し、フェイルバックを実行できます。以下は、元のソース ボリュームが存在している場合の手順です。

ソース ボリュームが存在しない場合のフェイルバックの実行（153ページ）
NetApp Element UIを使用して、元のソース ボリュームを再同期し、フェイルバックを実行できます。このセクションは、元のソース ボリュームが失われ、元のクラスタはそのまま維持されているシナリオに当てはまります。新しいクラスタにリストアする方法については、ネットアップ サポート サイトのドキュメントを参照してください。

ソース ボリュームが存在する場合のフェイルバックの実行

NetApp Element UIを使用して、元のソース ボリュームを再同期し、フェイルバックを実行できます。以下は、元のソース ボリュームが存在している場合の手順です。

手順

1. Element UIで、フェイルオーバーを実行するために解除する関係を探します。
2. [Actions]アイコンをクリックし、**[Reverse Resync]**をクリックします。
3. 操作を確定します。

   注 : 逆再同期（Reverse Resync）処理では、元のソース ボリュームとデスティネーション ボリュームの役割が逆転した新しい関係が作成されます（元の関係は残されるので、2つの関係が存在することになります）。逆再同期処理の一環として、元のデスティネーション ボリュームの新しいデータが元のソース ボリュームに転送されます。デスティネーション側のアクティブ ボリュームには引き続きアクセスしてデータを書き込むことができますが、元のプライマリ側にリダイレクトする前に、

ソース ボリュームとすべてのホストとの接続を切断し、SnapMirror更新を実行する必要があります。

4. 作成した逆の関係の[Actions]アイコンをクリックし、**[Update]**をクリックします。

   これで逆再同期が完了しました。デスティネーション側のボリュームにアクティブなセッションが接続されておらず、かつ元のプライマリ ボリュームに最新のデータが格納されている状態になったため、次の手順を実行してフェイルバックを完了し、元のプライマリ ボリュームを再びアクティブ化することができます。

5. 逆の関係の[Actions]アイコンをクリックし、**[Break]**をクリックします。
6. 元の関係の[Actions]アイコンをクリックし、**[Resync]**をクリックします。

   注 : これで、元のプライマリ ボリュームをマウントしてそのボリュームで本番環境のワークロードを再開できるようになります。この関係に設定されているポリシーとスケジュールに基づいて、元のSnapMirrorレプリケーションが再開されます。

7. 元の関係のステータスが「snapmirrored」であることを確認したら、逆の関係の[Actions]アイコンをクリックし、**[Delete]**をクリックします。

関連概念

*SnapMirror*フェイルバックのシナリオ（151ページ）

SnapMirrorディザスタ リカバリ機能について、2つのフェイルバック シナリオを例に説明します。どちらのシナリオも、元の関係がフェイルオーバーされた（解除された）状況を前提としています。

ソース ボリュームが存在しない場合のフェイルバックの実行

NetApp Element UIを使用して、元のソース ボリュームを再同期し、フェイルバックを実行できます。このセクションは、元のソース ボリュームが失われ、元のクラスタはそのまま維持されているシナリオに当てはまります。新しいクラスタにリストアする方法については、ネットアップ サポート サイトのドキュメントを参照してください。

開始する前に

- ElementとONTAPのボリューム間で、レプリケーション関係の状態が「Broken-off」になっている必要があります。
- Elementボリュームが失われてリカバリ不可能であることが必要です。
- 元のボリューム名が「NOT FOUND」と表示される必要があります。

手順

1. Element UIで、フェイルオーバーを実行するために解除する関係を探します。

   ベストプラクティス : 関係が「Broken-off」の状態のSnapMirrorポリシーおよびスケジュールの詳細をメモしておきます。この情報は、関係を再作成する際に必要となります。

2. [Actions]アイコンをクリックし、**[Reverse Resync]**をクリックします。
3. 操作を確定します。

   注 : 逆再同期（Reverse Resync）処理では、元のソース ボリュームとデスティネーション ボリュームの役割が逆転した新しい関係が作成されます（元の関係は残されるので、2つの関係が存在することになります）。元のボリュームがすでに存在しないため、元のソース ボリュームと同じ名前とサイズの新しいボリュームがElementに作成されます。新しいボリュームは、sm-recoveryというデフォルトのQoSポリシーを割り当てられて、sm-recoveryというデフォルトのアカウントに関連付けられます。削除された元のソース ボリュームを置き換えるためにSnapMirrorで作成されるすべてのボリュームについては、アカウントとQoSポリシーを手動で編集する必要があります。

逆再同期処理の一環として、最新のSnapshotのデータが新しいボリュームに転送されます。デスティネーション側のアクティブ ボリュームには引き続きアクセスしてデータを書き込むことができますが、あとで元のプライマリ関係を復元する前に、アクティブ ボリュームとすべてのホストとの接続を切断し、SnapMirror更新を実行する必要があります。逆再同期が完了し、デスティネーション側のボリュームにアクティブなセッションが接続されておらず、かつ元のプライマリ ボリュームに最新のデータがある状態になったら、次の手順に進んでフェイルバックを完了し、元のプライマリ ボリュームを再びアクティブ化します。

4. 逆再同期処理で作成された逆の関係の[Actions]アイコンをクリックし、**[Break]**をクリックします。
5. ソース ボリュームが存在しない元の関係の[Actions]アイコンをクリックし、**[Delete]**をクリックします。
6. 手順4で解除した逆の関係の[Actions]アイコンをクリックし、**[Reverse Resync]**をクリックします。
7. これにより、ソースとデスティネーションが逆転し、ソース ボリュームとデスティネーション ボリュームが元の関係と同じである関係が作成されます。
8. [Actions]アイコンをクリックし、**[Edit]**をクリックして、事前にメモした元のQoSポリシーとスケジュールの設定でこの関係を更新します。
9. これで、手順6で逆再同期した逆の関係を削除できるようになります。

関連概念

SnapMirrorフェイルバックのシナリオ（151ページ）
SnapMirrorディザスタ リカバリ機能について、2つのフェイルバック シナリオを例に説明します。どちらのシナリオも、元の関係がフェイルオーバーされた（解除された）状況を前提としています。

ONTAPからElementへの転送または1回限りの移行の実行

通常、NetApp Elementソフトウェアを実行するSolidFireストレージ クラスタからONTAPソフトウェアへのディザスタ リカバリにSnapMirrorを使用する場合、Elementがソースで ONTAPがデスティネーションです。ただし、場合によっては、ONTAPストレージ システムをソース、Elementをデスティネーションとすることができます。

開始する前に

- 次の2つのシナリオが該当します。
  - 以前のディザスタ リカバリ関係が存在しない:以下に記載するすべての手順を実行してください。
  - 以前のディザスタ リカバリ関係は存在するが、今回の移行対象のボリューム間の関係ではない：この場合は、手順3と4のみを実行してください。
- ONTAPからElementデスティネーション ノードにアクセスできるようにしておく必要があります。
- ElementボリュームのSnapMirrorレプリケーションを有効にしておく必要があります。

タスク概要

Elementのデスティネーション パスを「`hostip:/lun/<id_number>`」の形式で指定する必要があります。lunは文字どおり「lun」、`id_number`にはElementボリュームのIDを指定します。

手順

1. ONTAPを使用して、Elementクラスタとの関係を作成します。

```
snapmirror create -source-path SVM:volume|cluster://SVM/volume
-destination-path hostip:/lun/name -type XDP -schedule schedule -policy
    policy
```

```
cluster_dst::> snapmirror create -source-path svm_1:volA_dst
-destination-path 10.0.0.11:/lun/0005 -type XDP -schedule my_daily -policy MirrorLatest
```

2. ONTAPのsnapmirror showコマンドを使用して、SnapMirror関係が作成されたことを確認します。

   レプリケーション関係の作成方法についてはONTAPのドキュメントを、詳細なコマンド構文についてはONTAPのマニュアル ページを参照してください。

3. ElementのCreateVolume APIを使用してターゲット ボリュームを作成し、ターゲット ボリュームのアクセス モードをSnapMirrorに設定します。
   Element APIを使用したElementボリュームの作成

```
{
   "method": "CreateVolume",
   "params": {
        "name": "SMTargetVolumeTest2",
        "accountID": 1,
        "totalSize": 100000000000,
        "enable512e": true,
        "attributes": {},
        "qosPolicyID": 1,
        "enableSnapMirrorReplication": true,
        "access": "snapMirrorTarget"
    },
    "id": 1
}
```

4. ONTAPのsnapmirror initializeコマンドを使用してレプリケーション関係を初期化します。

```
snapmirror initialize -source-path hostip:/lun/name
-destination-path SVM:volume|cluster://SVM/volume
```

ボリュームのバックアップとリストア

他のSolidFireストレージ、およびAmazon S3またはOpenStack Swiftと互換性のあるセカンダリ オブジェクト ストアに対して、ボリュームのバックアップとリストアを実行できます。

タスク概要

OpenStack SwiftまたはAmazon S3からボリュームをリストアするときは、元のバックアップ プロセスのマニフェスト情報が必要です。SolidFireストレージ システムにバックアップされているボリュームをリストアする場合は、マニフェスト情報は不要です。

関連タスク

*Amazon S3*オブジェクト ストアへのボリュームのバックアップ（156ページ）
Amazon S3と互換性のある外部のオブジェクト ストアにボリュームをバックアップできます。

*OpenStack Swift*オブジェクト ストアへのボリュームのバックアップ（156ページ）
OpenStack Swiftと互換性のある外部のオブジェクト ストアにボリュームをバックアップできます。

*SolidFire*ストレージ クラスタへのボリュームのバックアップ（157ページ）

Elementソフトウェアを実行しているストレージ クラスタでは、あるクラスタ上にあるボリュームをリモートのクラスタにバックアップできます。

*Amazon S3*オブジェクト ストア上のバックアップからのボリュームのリストア（158ページ）
Amazon S3オブジェクト ストア上のバックアップからボリュームをリストアできます。

*OpenStack Swift*オブジェクト ストア上のバックアップからのボリュームのリストア（158ページ）
OpenStack Swiftオブジェクト ストア上のバックアップからボリュームをリストアできます。

*SolidFire*ストレージ クラスタ上のバックアップからのボリュームのリストア（159ページ）
SolidFireストレージ クラスタ上のバックアップからボリュームをリストアできます。

Amazon S3オブジェクト ストアへのボリュームのバックアップ

Amazon S3と互換性のある外部のオブジェクト ストアにボリュームをバックアップできます。

手順

1. **[Management]** > **[Volumes]**の順にクリックします。
2. バックアップするボリュームの[Actions]アイコンをクリックします。
3. 表示されたメニューで**[Backup to]**をクリックします。
4. **[Integrated Backup]**ダイアログ ボックスの**[Backup to]**で、**[S3]**を選択します。
5. **[Data Format]**で、次のいずれかのオプションを選択します。
   - **Native**：SolidFireストレージ システムのみが読み取り可能な圧縮形式。
   - **Uncompressed**：他のシステムと互換性がある非圧縮形式。
6. **[Hostname]**フィールドにオブジェクト ストアへのアクセスに使用するホスト名を入力します。
7. **[Access Key ID]**フィールドにアカウントのアクセス キーIDを入力します。
8. **[Secret Access Key]**フィールドにアカウントのシークレット アクセス キーを入力します。
9. **[S3 Bucket]**フィールドにバックアップの格納先とするS3バケットを入力します。
10. オプション: **[Nametag]**フィールドにプレフィックスに付加するネームタグを入力します。
11. **[Start Read]**をクリックします。

OpenStack Swiftオブジェクト ストアへのボリュームのバックアップ

OpenStack Swiftと互換性のある外部のオブジェクト ストアにボリュームをバックアップできます。

手順

1. **[Management]** > **[Volumes]**の順にクリックします。
2. バックアップするボリュームの[Actions]アイコンをクリックします。
3. 表示されたメニューで**[Backup to]**をクリックします。
4. **[Integrated Backup]**ダイアログ ボックスの**[Backup to]**で、**[Swift]**を選択します。
5. **[Data Format]**で、次のいずれかのデータ形式を選択します。
   - **Native**：SolidFireストレージ システムのみが読み取り可能な圧縮形式。
   - **Uncompressed**：他のシステムと互換性がある非圧縮形式。

6. **[URL]**フィールドにオブジェクト ストアへのアクセスに使用するURLを入力します。
7. **[Username]**フィールドにアカウントのユーザ名を入力します。
8. **[Authentication Key]**フィールドにアカウントの認証キーを入力します。
9. **[Container]**フィールドにバックアップの格納先とするコンテナを入力します。
10. オプション: **[Nametag]**フィールドにプレフィックスに付加するネーム タグを入力します。
11. **[Start Read]**をクリックします。

SolidFireストレージ クラスタへのボリュームのバックアップ

Elementソフトウェアを実行しているストレージ クラスタでは、あるクラスタ上にあるボリュームをリモートのクラスタにバックアップできます。

開始する前に

ソース クラスタとターゲット クラスタがペアリングされていることを確認します。詳細については、「クラスタのペアリング」を参照してください。

タスク概要

クラスタ間でバックアップまたはリストアを実行する際には、システムによってクラスタ間の認証に使用するキーが生成されます。ソース クラスタはこのボリュームの一括書き込みキーを使用してデスティネーション クラスタに対して認証し、デスティネーション ボリュームへの書き込みがセキュリティで保護されます。バックアップまたはリストアを実行する際には、処理を開始する前に、デスティネーション ボリュームからボリュームの一括書き込みキーを生成する必要があります。

手順

1. デスティネーション クラスタで、**[Management]** > **[Volumes]**の順に選択します。
2. デスティネーション ボリュームの[Actions]アイコンをクリックします。
3. 表示されたメニューで**[Restore from]**をクリックします。
4. **[Integrated Restore]**ダイアログ ボックスの**[Restore from]**で、**[SolidFire]**を選択します。
5. **[Data Format]**で、次のいずれかのオプションを選択します。
   - **Native**：SolidFireストレージ システムのみが読み取り可能な圧縮形式。
   - **Uncompressed**：他のシステムと互換性がある非圧縮形式。
6. **[Generate Key]**をクリックします。
7. **[Bulk Volume Write Key]**ボックスからクリップボードへキーをコピーします。
8. ソース クラスタで、**[Management]** > **[Volumes]**の順に選択します。
9. バックアップするボリュームの[Actions]アイコンをクリックします。
10. 表示されたメニューで**[Backup to]**をクリックします。
11. **[Integrated Backup]**ダイアログ ボックスの**[Backup to]**で、**[SolidFire]**を選択します。
12. **[Data Format]**フィールドで、前の手順で選択したデータ形式と同じ形式を選択します。
13. **[Remote Cluster MVIP]**フィールドにデスティネーション ボリュームのクラスタの管理仮想IPアドレスを入力します。
14. **[Remote Cluster Username]**フィールドにリモート クラスタのユーザ名を入力します。
15. **[Remote Cluster Password]**フィールドにリモート クラスタのパスワードを入力します。

16. デスティネーション クラスタで生成したキーを**[Bulk Volume Write Key]**フィールドに貼り付けます。
17. **[Start Read]**をクリックします。

Amazon S3オブジェクト ストア上のバックアップからのボリュームのリストア

Amazon S3オブジェクト ストア上のバックアップからボリュームをリストアできます。

手順

1. **[Reporting]** > **[Event Log]**の順にクリックします。
2. リストアする必要のあるバックアップを作成したバックアップ イベントを探します。
3. イベントの**[Details]**列で、**[Show Details]**をクリックします。
4. マニフェスト情報をクリップボードにコピーします。
5. **[Management]** > **[Volumes]**の順にクリックします。
6. リストアするボリュームの[Actions]アイコンをクリックします。
7. 表示されたメニューで**[Restore from]**をクリックします。
8. **[Integrated Restore]**ダイアログ ボックスの**[Restore from]**で、**[S3]**を選択します。
9. **[Data Format]**で、バックアップに一致するオプションを選択します。
   - **Native**：SolidFireストレージ システムのみが読み取り可能な圧縮形式。
   - **Uncompressed**：他のシステムと互換性がある非圧縮形式。
10. **[Hostname]**フィールドにオブジェクト ストアへのアクセスに使用するホスト名を入力します。
11. **[Access Key ID]**フィールドにアカウントのアクセス キーIDを入力します。
12. **[Secret Access Key]**フィールドにアカウントのシークレット アクセス キーを入力します。
13. **[S3 Bucket]**フィールドにバックアップの格納先とするS3バケットを入力します。
14. **[Manifest]**フィールドにマニフェスト情報を貼り付けます。
15. **[Start Write]**をクリックします。

OpenStack Swiftオブジェクト ストア上のバックアップからのボリュームのリストア

OpenStack Swiftオブジェクト ストア上のバックアップからボリュームをリストアできます。

手順

1. **[Reporting]** > **[Event Log]**の順にクリックします。
2. リストアする必要のあるバックアップを作成したバックアップ イベントを探します。
3. イベントの**[Details]**列で、**[Show Details]**をクリックします。
4. マニフェスト情報をクリップボードにコピーします。
5. **[Management]** > **[Volumes]**の順にクリックします。
6. リストアするボリュームの[Actions]アイコンをクリックします。
7. 表示されたメニューで**[Restore from]**をクリックします。
8. **[Integrated Restore]**ダイアログ ボックスの**[Restore from]**で、**[Swift]**を選択します。
9. **[Data Format]**で、バックアップに一致するオプションを選択します。
   - **Native**：SolidFireストレージ システムのみが読み取り可能な圧縮形式。
   - **Uncompressed**：他のシステムと互換性がある非圧縮形式。

10. **[URL]**フィールドにオブジェクト ストアへのアクセスに使用するURLを入力します。
11. **[Username]**フィールドにアカウントのユーザ名を入力します。
12. **[Authentication key]**フィールドにアカウントの認証キーを入力します。
13. **[Container]**フィールドにバックアップが格納されているコンテナの名前を入力します。
14. **[Manifest]**フィールドにマニフェスト情報を貼り付けます。
15. **[Start Write]**をクリックします。

SolidFireストレージ クラスタ上のバックアップからのボリュームのリストア

SolidFireストレージ クラスタ上のバックアップからボリュームをリストアできます。

タスク概要

クラスタ間でバックアップまたはリストアを実行する際には、システムによってクラスタ間の認証に使用するキーが生成されます。ソース クラスタはこのボリュームの一括書き込みキーを使用してデスティネーション クラスタに対して認証し、デスティネーション ボリュームへの書き込みがセキュリティで保護されます。バックアップまたはリストアを実行する際には、処理を開始する前に、デスティネーション ボリュームからボリュームの一括書き込みキーを生成する必要があります。

手順

1. デスティネーション クラスタで、**[Management]** > **[Volumes]**の順にクリックします。
2. リストアするボリュームの[Actions]アイコンをクリックします。
3. 表示されたメニューで**[Restore from]**をクリックします。
4. **[Integrated Restore]**ダイアログ ボックスの**[Restore from]**で、**[SolidFire]**を選択します。
5. **[Data Format]**で、バックアップに一致するオプションを選択します。
   - **Native**：SolidFireストレージ システムのみが読み取り可能な圧縮形式。
   - **Uncompressed**：他のシステムと互換性がある非圧縮形式。
6. **[Generate Key]**をクリックします。
7. **[Bulk Volume Write Key]**の情報をクリップボードにコピーします。
8. ソース クラスタで、**[Management]** > **[Volumes]**の順にクリックします。
9. リストアに使用するボリュームの[Actions]アイコンをクリックします。
10. 表示されたメニューで**[Backup to]**をクリックします。
11. **[Integrated Backup]**ダイアログ ボックスの**[Backup to]**で、**[SolidFire]**を選択します。
12. **[Data Format]**で、バックアップに一致するオプションを選択します。
13. **[Remote Cluster MVIP]**フィールドにデスティネーション ボリュームのクラスタの管理仮想IPアドレスを入力します。
14. **[Remote Cluster Username]**フィールドにリモート クラスタのユーザ名を入力します。
15. **[Remote Cluster Password]**フィールドにリモート クラスタのパスワードを入力します。
16. クリップボードから**[Bulk Volume Write Key]**フィールドにキーを貼り付けます。
17. **[Start Read]**をクリックします。

システムの監視とトラブルシューティング

システムの監視は、診断目的、または各種システム処理のパフォーマンスの傾向やステータスに関する情報を収集するために実行します。メンテナンスのためにノードやSSDの交換が必要になる場合もあります。

関連概念

ドライブのトラブルシューティング（180ページ）
障害が発生したソリッドステート ドライブ（SSD）を、交換用ドライブに交換できます。SolidFireストレージ ノードのSSDはホットスワップ対応です。SSDで障害が発生した疑いがある場合は、ネットアップ サポートに障害の検証を依頼し、指示に従って正しい解決策を実行してください。ネットアップ サポートは、サービス レベル アグリーメントに従って、交換用ドライブを入手する方法についてもアドバイスします。

ノードのトラブルシューティング（183ページ）
メンテナンスまたは交換のために、ノードをクラスタから削除できます。ノードをオフラインにする前に、NetApp Element UIまたはAPIを使用してノードを削除する必要があります。

ストレージノードのノードごとのユーティリティの操作（184ページ）
NetApp Element Software UI の標準的な監視ツールでNetApp Elementソフトウェア分な情報が得られない場合は、ノード単位のユーティリティを使用してネットワークの問題をトラブルシューティングできます。ノード単位のユーティリティには、ノード間または管理ノードとの間のネットワーク問題のトラブルシューティングに役立つ特定の情報とツールが用意されています。

管理ノードの使用（191ページ）
管理ノード（mNode）は、システム サービスのアップグレード、クラスタのアセットと設定の管理、システムのテストとユーティリティの実行、Active IQへの接続（システム監視）、ネットアップ サポートへのアクセス許可（トラブルシューティング）に使用します。

クラスタ フル レベルの概要（204ページ）
Elementソフトウェアを実行するクラスタの容量が不足してくると、クラスタ エラーが生成されてストレージ管理者に警告が表示されます。クラスタ フルには3つのレベル（Warning、Error、Critical）があり、すべてのレベルがネットアップ Element UIに表示されます。

関連タスク

システム イベントに関する情報の表示（161ページ）
システムで検出された各種のイベントに関する情報を確認できます。イベント メッセージは30秒ごとに更新されます。イベント ログには、クラスタの主要なイベントが表示されます。

システム アラートの表示（164ページ）
システムで発生したクラスタの障害やエラーに関する情報をアラートとして表示できます。アラートには、情報、警告、エラーがあり、クラスタの稼働状況を表すインジケータとして利用できます。ほとんどのエラーは自動的に解決します。

ノードのパフォーマンス アクティビティの表示（176ページ）
各ノードのパフォーマンス アクティビティをグラフ形式で表示できます。ノードの各ドライブのCPUおよび読み取り / 書き込みIOPS（1秒あたりの入出力操作）のリアルタイムの統計がグラフに表示されます。使用率のグラフは5秒間隔で、ドライブ統計のグラフは10秒間隔で更新されます。

ボリューム パフォーマンスの表示（177ページ）

クラスタ内のすべてのボリュームの詳細なパフォーマンス情報を確認できます。ボリュームIDまたは任意のパフォーマンス列で情報をソートできます。フィルタを使用して、特定の条件で情報をフィルタリングすることもできます。

*iSCSI*セッションの表示（178ページ）
クラスタに接続されているiSCSIセッションを確認できます。情報をフィルタして、必要なセッションだけを表示できます。

*Fibre Channel*セッションの表示（179ページ）
クラスタに接続されているFibre Channel（FC）セッションを確認できます。情報をフィルタして、該当する接続に関する情報だけをウィンドウに表示できます。

クラスタでの*HTTPS*の*FIPS 140-2*の有効化（72ページ）
`EnableFeature` APIメソッドを使用して、HTTPS通信のFIPS 140-2動作モードを有効にすることができます。

関連資料

実行中のタスクのステータスの表示（164ページ）
`ListSyncJobs`および`ListBulkVolumeJobs` APIメソッドから報告される、実行中のタスクの進捗状況と完了ステータスをWeb UIで確認できます。Element UIの[Reporting]タブから、[Running Tasks]ページにアクセスできます。

システム イベントに関する情報の表示

システムで検出された各種のイベントに関する情報を確認できます。イベント メッセージは30秒ごとに更新されます。イベント ログには、クラスタの主要なイベントが表示されます。

手順

Element UIで、**[Reporting]** > **[Event Log]**の順に選択します。
すべてのイベントについて次の情報が表示されます。

項目	説明
ID	各イベントに関連付けられた一意のID。
Event Type	ログに記録されているイベントのタイプ（APIイベントやクローン イベントなど）。
Message	イベントに関連するメッセージ。
Details	イベントの発生理由の特定に役立つ情報。
Service ID	イベントを報告したサービス（該当する場合）。
Node	イベントを報告したノード（該当する場合）。
Drive ID	イベントを報告したドライブ（該当する場合）。
Event Time	イベントが発生した日時。

関連資料

イベント タイプ（162ページ）
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ています。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。[Event Log]ページの[Event Types]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。

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ています。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。[Event Log]ページの[Event Types]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。

注 : 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。ビンは簡単に言うとデータを保持するコンテナであり、クラスタ全体にマップされます。

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
ボリューム全体に対して実行された処理（バックアップ、リストア、Snapshot、クローンなど）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
クラスタの初期化時または設定変更（ノードの追加や削除など）時に発生するイベント。

AssumeVent
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
ソフトウェアの自動インストール 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。

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
スライス サーバに関連するイベント（メタデータ ドライブまたはボリュームの削除など）。

snmpTrapEvent
SNMPトラップに関連するイベント。

statEvent
システムの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する回復不能な読み取りエラーに関連するイベント。

vasaProviderEvent
vSphere APIs for Storage Awareness（VASA）Providerに関連するイベント。

実行中のタスクのステータスの表示

ListSyncJobsおよびListBulkVolumeJobs APIメソッドから報告される、実行中のタスクの進捗状況と完了ステータスをWeb UIで確認できます。Element UIの[Reporting]タブから、[Running Tasks]ページにアクセスできます。

タスクが多数ある場合は、それらのタスクがキューに登録されてバッチで実行されることがあります。[Running Tasks]ページには、同期中のサービスが表示されます。完了したタスクはリストから消え、キューに登録された次の同期タスクが表示されます。[Running Tasks]ページには、完了していないタスクがなくなるまで同期タスクが表示されます。

注 : レプリケーションを実行中のボリュームのレプリケーション同期データは、ターゲット ボリュームを含むクラスタの[Running Tasks]ページで確認できます。

システム アラートの表示

システムで発生したクラスタの障害やエラーに関する情報をアラートとして表示できます。アラートには、情報、警告、エラーがあり、クラスタの稼働状況を表すインジケータとして利用できます。ほとんどのエラーは自動的に解決します。

タスク概要

ListClusterFaults APIメソッドを使用すると、アラートの監視を自動化できます。このメソッドを使用すると、発生したすべてのアラートに関する通知が届きます。

手順

1. Element UIで、**[Reporting]** > **[Alerts]**の順に選択します。
   ページ上のアラートは30秒ごとに更新されます。
   すべてのイベントについて次の情報が表示されます。

項目	説明
ID	クラスタ アラートに関連付けられた一意のID。
Severity	アラートの重大度。有効な値は次のとおりです。 • warning：近々対応が必要になる可能性があるが、深刻ではない問題です。システムのアップグレードは引き続き可能です。 • error：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、サービスへのそれ以外の影響はありません。 • critical：サービスに影響する深刻な障害です。システムは、API要求およびクライアント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。
Type	エラーの影響を受けるコンポーネント。node、drive、cluster、service、volumeのいずれかです。
Node	このエラー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	このエラー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。

項目	説明
Error Code	エラーの原因を示すコード。
Details	エラーの説明とその他の詳細情報。
Date	エラーがログに記録された日時。

2. 個々のアラートの**[Show Details]**をクリックして、当該アラートに関する情報を表示します。
3. ページ上のすべてのアラートの詳細を表示するには、[Details]列をクリックします。

   アラートが解決されると、そのアラートに関するすべての情報（解決された日付を含む）が[Resolved]領域に移動します。

関連資料

クラスタ障害コード（165ページ）

Alertsページに表示されている障害コードを生成すると、エラーまたは該当する可能性のある状態が報告されます。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。

関連情報

*Element API*を使用したストレージの管理

クラスタ障害コード

Alertsページに表示されている障害コードを生成すると、エラーまたは該当する可能性のある状態が報告されます。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。

以下は、各種コードのリストです。

AuthenticationServiceDefault

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。

availableVirtualNetworkIPAddressesLow

IPアドレス ブロック内の仮想ネットワーク アドレスの数が不足しています。

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。`GetClusterFullThreshold`クラスタのフルネスレベルの詳細については、 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。

- ステージ 3 低（警告）：ユーザ定義のしきい値を超えました。クラスタ全体の設定を調整するか、ノードを追加します。
- ステージ 4 クリティカル（エラー）： 1 ノードの障害から回復するのに十分なスペースがありません。ボリューム、スナップショット、クローンの作成は許可されていません。
- ステージ 5 が完了（クリティカル）1 。書き込みや新しい iSCSI 接続は許可されません。現在の iSCSI 接続は維持されます。クラスタに追加される容量が増えるまで、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（削除）するか、ストレージ クラスタにストレージ ノードをもう1つ追加してください。

ブロックがデグレードされました

障害が発生したため、ブロックデータは完全にレプリケートされなくなりました。

Severity	説明
Error	使用できるのは、ブロックデータ全体のコピーが 1 つだけです。
Critical	ブロックデータの完全なコピーは使用できません。

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

blockServiceTooFull

ブロック サービスが大量の容量を使用しています。

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。

blockServiceUnhealthy

ブロックサービスが異常として検出されました：

- 重大度 = 警告：アクションは実行されません。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：システムはデータを自動的に廃棄し、他の正常なドライブにデータを再レプリケートしています。
- 重大度 = 重大：複数のノードで、レプリケーションカウント以上のブロックサービスが失敗しました（ 2 倍の Helix の場合は 2 ）。データが利用できず、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に障害が発生した場合は、他の障害が発生します。この障害は、ブロックサービスがアクセス可能になったとき、またはサービスが廃棄されたときにクリアされます。

clockSkewExceedsFaultThreshold

クラスタマスターと、トークンを提示しているノード間の時間スキューが、推奨しきい値を超えています。ストレージクラスタは、ノード間の時間のずれ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 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

スペース不足です。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状態のドライブに同期することはできません。

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。

clusterIOPSAreOverProvisioned

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。最小QoSの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 設定を低くします。

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。この障害の重大度は「Warning」です。

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。次の理由が考えられます。

- 暗号化キーを取得できなかった場合は、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。

disconnectedClusterPair

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ます。

disconnectedRemoteNode

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ます。

disconnectedSnapMirrorEndpoint

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の SnapMirrorEndpoint 間のネットワーク接続を確認します。

driveAvailable

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いて、利用可能な状態のドライブはないはずです。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、利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

1 つ以上のドライブに障害が発生すると、クラスタはこの障害を返します。これは、次のいずれかの状態を示します。

- ドライブマネージャがドライブにアクセスできません。
- スライスまたはブロックサービスが何度も失敗しました。ドライブの読み取りまたは書き込みに失敗した可能性があり、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に障害が発生していると見なされます）。
- ドライブがロックされており、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、アンロック操作が失敗する。

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ます。
- 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。

driveWearFault

ドライブの残量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 2 つの重大度レベルがあります。重大度と警告：

- シリアル付きドライブ：スロットに <serial number> ： <node slot> <drive slot> には重大な摩耗レベルがあります。
- シリアル付きドライブ：スロット： <node slot> <drive slot> には、消耗品の少ない予約があります。

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 クラスタ 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。この障害の重大度は「Warning」です。

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。次の理由が考えられます。

- 暗号化キーを取得できなかった場合は、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 ノードへのネットワーク接続または電源が失われています。

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。

exception

想定外の障害が報告されました。この障害は障害キューから自動的に消去されません。ネットアップ サポートにお問い合わせください。

failedSpaceTooFull

ブロック サービスがデータ書き込み要求に応答していません。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容量が足りなくなります。

この問題を解決するには、書き込みを正常に処理し、失敗用の容量がスライス サービスからフラッシュされるように、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 センサーで障害が発生しているか、ファン センサーが見つかりません。

この障害を解決するには、障害が発生したハードウェアを交換します。

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応答していません。この状態になると、ノードは応答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ます。

fibreChannelAccessUnavailable

すべてのFibre Channelノードが応答していません。ノードIDが表示されます。ネットワーク接続を確認します。

FibreChannelActiveXL

IXL Nexus の数は、ファイバチャネルノードごとにサポートされるアクティブセッション数の上限である 8000 に近づいています。

- ベストプラクティスの制限は 5500 です。
- 警告制限は 7500 です。
- 最大制限（非強制）は 8192 です。

この障害を解決するには、ベストプラクティスの制限である 5500 を下回る IXL Nexus の数を減らします。

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スロットに想定外のFibre Channelポートが接続されています。
- 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パススルーの設定中に永続的な問題が発生しました。

ネットアップ サポートにお問い合わせください。

FibreChannelStaticiXL

IXL Nexus の数は、ファイバチャネルノードごとにサポートされる静的セッション数の上限である 16000 に近づいています。

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

この障害を解決するには、 iXL Nexus の数をベストプラクティスの上限である 11000 以下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。

FipsDriveMismatched （ FipsDriveMis

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、問題のドライブを取り外すか、または交換します。

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。

hardwareConfigMismatch

このクラスタ障害は、次のいずれかの状態を示します。

- 構成がノードの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。考えられる理由は、インストールされているエレメントのバージョンがこのドライブを認識しないことです。このノードの要素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 ：有効期限

クラスタのサードパーティ ID プロバイダ（ IdP ）で使用するサービスプロバイダの SSL 証明書が期限切れに近づいているか、すでに期限切れになっています。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。

Severity	説明
Warning	証明書は30日以内に期限切れになります。
Error	証明書は7日以内に期限切れになります。
Critical	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 証明書の有効期限が切れる前に更新します。`UpdateIdpConfiguration`更新された SSL 証明書を提供するには、API メソッドで refreshCertificateExpirationTime = true を使用します。

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。

inconsistentInterfaceConfiguration

インターフェイスの設定が一貫していません。

この問題を解決するには、ストレージ クラスタ内のすべてのノード インターフェイスの設定を同じにしてください。

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の不一致：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の不一致：Bond10Gインターフェイス間で異なるMTUが設定されています。

該当するノードと設定されている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 ルールが一貫していません。

inconsistentSubnetMasks

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。この問題は、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するとともに、停止しているサービスがないか確認してください。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

割り込み処理の負荷分散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、`ModifyKeyServerKmip`を使用してルートCA証明書を更新します。
- 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、`ModifyKeyServerKmip`を使用して期限が切れる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、`ModifyKeyServerKmip`を使用してルートCA証明書を更新します。
- クライアント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、`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、`ModifyKeyServerKmip`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、正しい証明書が提供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。`ModifyKeyServerKmip`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のエラーです。
  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。`ModifyKeyServerKmip`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

- 接続エラー
  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ます。`TestKeyServerKimp`と`TestKeyProviderKmip`を使用して、接続をテストします。
- 認証エラー
  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
  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。

MemoryEccThreshold

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。重大度が `Error` の場合、 DIMM の障害が原因である可能性があります。

ネットアップ サポートにお問い合わせください。

memoryUsageThreshold

メモリ使用量が正常値を上回っています。

ネットアップ サポートにお問い合わせください。

metadataClusterFull

1 つのノードの損失をサポートするための十分な空きメタデータストレージスペースがありません。`GetClusterFullThreshold`クラスタのフルネスレベルの詳細については、 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。

- ステージ 3 低（警告）：ユーザ定義のしきい値を超えました。クラスタ全体の設定を調整するか、ノードを追加します。
- ステージ 4 クリティカル（エラー）： 1 ノードの障害から回復するのに十分なスペースがありません。ボリューム、スナップショット、クローンの作成は許可されていません。
- ステージ 5 が完了（クリティカル）1 。書き込みや新しい iSCSI 接続は許可されません。現在の iSCSI 接続は維持されます。クラスタに追加される容量が増えるまで、書き込みは失敗します。データを消去または削除するか、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（削除）するか、ストレージ クラスタにストレージ ノードをもう1つ追加してください。

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。
- 設定済みの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。

noAvailableVirtualNetworkIPAddresses

IPアドレスのブロックに利用可能な仮想ネットワーク アドレスがありません。クラスタにこれ以上ストレージ ノードを追加できません。

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> がダウンしているか、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ダウンしているか、ケーブルが外れています。

この障害を解決するには、ノードのネットワーク接続を確認します。

nodeHardwareFault （ドライブ暗号化対応状態が不一致ノードの暗号化対応状態がスロット < ノードスロット >< ドライブスロット > のドライブ）

ドライブは、そのドライブがインストール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 < ノードスロット >< 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。 <expected size> ）

ストレージノードに、このノードの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 < ノードスロット >< ドライブスロット > で検出されました。ドライブの統計情報とヘルス情報は使用できません）

ストレージノードにサポートされていないドライブが含まれている。

NodeHardwareFault（スロット < ノードスロット > のドライブはファームウェアバージョン < 予想されるバージョン > を使用す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、サポートされていない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。

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ます。

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を有効にして正しく設定していないと、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。

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。

nvramDeviceStatus

NVRAMデバイスにエラーがあるか、障害が発生しようとしているか、または障害が発生しました。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。

Severity	説明
Warning	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、過熱警告などの一時的な状態である可能性があります。
Error	ハードウェアによってエラーステータスが検出されました。クラスタマスターは、スライスドライブを操作から削除しようとします。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。
Critical	ハードウェアによって重大なステータスが検出されました。クラスタマスターは、スライスドライブを操作から削除しようとします。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。

この問題を解決するには、故障したハードウェアを交換します。

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。

冗長な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ジしてください。

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ます。

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の最大数を超えたため、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。

この障害を解決するには、ターゲットストレージクラスタのスナップショット制限を増やします。

scheduleActionError

スケジュールされたアクティビティが実行されましたが、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、アクティビティが削除されるか、または停止後に再開されれば、障害はクリアされます。

sensorReadingFailed

ベースボード管理コントローラ（BMC）のセルフテストが失敗したか、センサーが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

要求された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

スライス サービスが正常な状態でないことをシステムが検出し、サービスを自動的に停止しています。

- 重大度 = 警告：アクションは実行されません。この警告期間は 6 分で終了します。
- 重大度 = エラー：システムはデータを自動的に廃棄し、他の正常なドライブにデータを再レプリケートしています。

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に障害が発生した場合は、他の障害が発生します。この障害は、スライスサービスがアクセス可能になったとき、またはサービスが廃棄されたときにクリアされます。

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、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。

Severity	説明
Warning	証明書は30日以内に期限切れになります。
Error	証明書は7日以内に期限切れになります。
Critical	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。必要であれば、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以上を占めている。

データの冗長性を維持するために、システムは最大ノードの容量を削減し、ブロック容量の一部を使用しないようにします（使用しません）。

この障害を解決するには、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ます。

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。必要であれば、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。

unresponsiveService

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ありません。
- 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。

volumeDegraded

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** 障害も発生します。

ネットアップ サポートにお問い合わせください。

ノードのパフォーマンス アクティビティの表示

各ノードのパフォーマンス アクティビティをグラフ形式で表示できます。ノードの各ドライブのCPUおよび読み取り / 書き込みIOPS（1秒あたりの入出力操作）のリアルタイム

の統計がグラフに表示されます。使用率のグラフは5秒間隔で、ドライブ統計のグラフは10秒間隔で更新されます。

手順

1. **[Cluster]** > **[Nodes]**の順にクリックします。
2. 表示するノードの**[Actions]**アイコンをクリックします。
3. **[View Details]**をクリックします。

   注 : 折れ線グラフまたは棒グラフの特定のポイントにカーソルを合わせると、その時点の具体的な情報が表示されます。

ボリューム パフォーマンスの表示

クラスタ内のすべてのボリュームの詳細なパフォーマンス情報を確認できます。ボリュームIDまたは任意のパフォーマンス列で情報をソートできます。フィルタを使用して、特定の条件で情報をフィルタリングすることもできます。

タスク概要

[Refresh every]リストをクリックして別の値を選択すると、ページ上のパフォーマンス情報の更新頻度を変更できます。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。[Never]を選択すると、ページの自動更新が無効になります。

自動更新を再び有効にするには、**[Turn on auto-refresh]**をクリックします。

手順

1. Element UIで、**[Reporting]** > **[Volume Performance]**の順に選択します。
2. ボリューム リストで、ボリュームの[Actions]アイコンをクリックします。
3. **[View Details]**をクリックします。
   ボリュームの一般的な情報がページの下部に表示されます。
4. ボリュームの詳細を確認するには、**[See More Details]**をクリックします。
   ボリュームの詳細情報とパフォーマンス グラフが表示されます。

関連資料

ボリュームのパフォーマンスの詳細（177ページ）

Element UIの[Reporting]タブの[Volume Performance]ページでは、ボリュームのパフォーマンス統計を確認できます。

ボリュームのパフォーマンスの詳細

Element UIの[Reporting]タブの[Volume Performance]ページでは、ボリュームのパフォーマンス統計を確認できます。

確認できる詳細情報は次のとおりです。

ID

システムによって生成されたボリュームのID。

Name

ボリュームの作成時に指定した名前。

Account

ボリュームに割り当てられているアカウントの名前。

Access Groups

ボリューム アクセス グループまたはボリュームが所属するグループの名前。

Volume Utilization

クライアントによるボリュームの使用率を示すパーセンテージ。

有効な値は次のとおりです。

- 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。

Total 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。

Read IOPS

ボリュームに対して実行中の読み取りIOPSの総数。

Write IOPS

ボリュームに対して実行中の書き込みIOPSの総数。

Total Throughput

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。

Write Throughput

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。

Total Latency

ボリュームに対する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）。

Read Latency

過去500ミリ秒の、ボリュームに対する読み取り処理が完了するまでの平均時間（マイクロ秒）。

Write Latency

過去500ミリ秒の、ボリュームに対する書き込み処理が完了するまでの平均時間（マイクロ秒）。

Queue Depth

ボリュームに対する未処理の読み取りおよび書き込み処理の数。

Average IO Size

過去500ミリ秒の、ボリュームに対する最新のI/Oの平均サイズ（バイト）。

iSCSIセッションの表示

クラスタに接続されているiSCSIセッションを確認できます。情報をフィルタして、必要なセッションだけを表示できます。

手順

1. Element UIで、**[Reporting]** > **[iSCSI Sessions]**の順に選択します。
2. フィルタ条件のフィールドを表示するには、**[Filter]**をクリックします。

関連資料

*iSCSI*セッションの詳細（179ページ）

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。

iSCSIセッションの詳細

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。

iSCSIセッションについて確認できる情報は次のとおりです。

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（-）が表示されます。

Volume
ノードでのボリュームの識別名。

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。

Initiator Alias
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。

Initator IP
セッションを開始するエンドポイントのIPアドレス。

Initiator 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。

Target IQN
ボリュームのIQN。

Created On
セッションが確立された日時。

Fibre Channelセッションの表示

クラスタに接続されているFibre Channel（FC）セッションを確認できます。情報をフィルタして、該当する接続に関する情報だけをウィンドウに表示できます。

手順

1. Element UIで、**[Reporting]** > **[FC Sessions]**の順に選択します。
2. フィルタ条件のフィールドを表示するには、**[Filter]**をクリックします。

関連資料

*Fibre Channel*セッションの詳細（180ページ）

クラスタに接続されているアクティブなFibre Channel（FC）セッションに関する情報を確認できます。

Fibre Channelセッションの詳細

クラスタに接続されているアクティブなFibre Channel（FC）セッションに関する情報を確認できます。

クラスタに接続されているFCセッションについて確認できる情報は次のとおりです。

Node ID

接続のセッションをホストしているノード。

Node Name

システムによって生成されたノード名。

Initiator ID

システムによって生成されたイニシエータのID。

Initiator WWPN

イニシエータのWorld Wide Port Name。

Initiator Alias

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。

Target WWPN

ターゲットのWorld Wide Port Name。

Volume Access Group

セッションが属しているボリューム アクセス グループの名前。

Volume Access Group ID

システムによって生成されたアクセス グループのID。

ドライブのトラブルシューティング

障害が発生したソリッドステート ドライブ（SSD）を、交換用ドライブに交換できます。SolidFireストレージ ノードのSSDはホットスワップ対応です。SSDで障害が発生した疑いがある場合は、ネットアップ サポートに障害の検証を依頼し、指示に従って正しい解決策を実行してください。ネットアップ サポートは、サービス レベル アグリーメントに従って、交換用ドライブを入手する方法についてもアドバイスします。

ここでのホットスワップ対応とは、障害が発生したドライブをアクティブなノードから取り外し、ネットアップの新しいSSDドライブと交換できるという意味です。アクティブなクラスタで障害が発生していないドライブを取り外すことは推奨されません。

障害が発生したドライブをただちに交換できるように、ネットアップ サポートから提案されたオンサイト スペアを用意しておいてください。

注 : テストの目的でノードからドライブを引き抜いてドライブ障害をシミュレートする場合は、30秒待ってからドライブ スロットにドライブを再挿入してください。

ドライブで障害が発生すると、Double Helixによって、そのドライブ上のデータがクラスタ内の残りのノードに再配分されます。Elementソフトウェアでは、データの2つのコピーが同じノード上に保存されることはないため、同じノードで複数のドライブ障害が発生しても問題はありません。ドライブで障害が発生すると、以下のイベントが発生します。

- 当該ドライブからデータが移行されます。
- 当該ドライブの容量だけクラスタ全体の容量が減少します。

- Double Helixデータ保護機能により、データの有効なコピーが2つ確保されます。

  注意 : SolidFireストレージ システムでは、データの移行に必要なストレージ容量を確保できなくなる場合、ドライブの削除はサポートされません。

関連概念

基本的な*MDSS*ドライブのトラブルシューティング（182ページ）
一方または両方のメタデータ ドライブ（またはスライス ドライブ）で障害が発生した場合は、当該ドライブをクラスタに戻すことでドライブをリカバリできます。このリカバリ処理は、ノードでMDSS機能がすでに有効になっている場合にNetApp Element UIで実行できます。

関連タスク

クラスタからの障害ドライブの削除（181ページ）
ドライブの自己診断によりドライブで障害が発生したことがノードに通知された場合、あるいはドライブとの通信が5分半以上停止した場合、そのドライブは障害状態になり、 障害ドライブのリストが表示されます。障害が発生したドライブは、NetApp Elementソフトウェアの障害ドライブ リストから削除する必要があります。

*MDSS*ドライブの削除（183ページ）
マルチドライブ スライス サービス（MDSS）のドライブを削除できます。この手順を実行できるのは、ノードに複数のスライス ドライブがある場合のみです。

関連情報

障害が発生した*SolidFire*ストレージ ノード用ドライブの交換
Replacing drives for H600S series storage nodes

クラスタからの障害ドライブの削除

ドライブの自己診断によりドライブで障害が発生したことがノードに通知された場合、あるいはドライブとの通信が5分半以上停止した場合、そのドライブは障害状態になり、 障害ドライブのリストが表示されます。障害が発生したドライブは、NetApp Elementソフトウェアの障害ドライブ リストから削除する必要があります。

タスク概要

ノードがオフラインの場合、ドライブは**[Alerts]**リストに**blockServiceUnhealthy**と表示されます。ノードを再起動し、ノードとそのドライブが5分半以内にオンラインに戻った場合、ドライブは自動的に更新されてアクティブ ドライブに戻ります。

手順

1. Element UIで、**[Cluster]** > **[Drives]**の順に選択します。
2. **[Failed]**をクリックして、障害ドライブのリストを表示します。
3. 障害が発生したドライブのスロット番号をメモします。
   この情報は、障害が発生したドライブをシャーシ内で特定するときに必要になります。
4. 次のいずれかの方法で障害ドライブを削除します。

オプション	手順
ドライブを個別に削除する	1. 削除するドライブの**[Actions]**アイコンをクリックします。 2. **[Remove]**をクリックします。
複数のドライブを削除する	1. 削除するドライブをすべて選択し、**[Bulk Actions]**をクリックします。 2. **[Remove]**をクリックします。

基本的なMDSSドライブのトラブルシューティング

一方または両方のメタデータ ドライブ（またはスライス ドライブ）で障害が発生した場合は、当該ドライブをクラスタに戻すことでドライブをリカバリできます。このリカバリ処理は、ノードでMDSS機能がすでに有効になっている場合にNetApp Element UIで実行できます。

ノード内の一方または両方のメタデータ ドライブで障害が発生すると、スライス サービスがシャットダウンし、両方のドライブのデータがノードの別のドライブにバックアップされます。

以下は、想定される障害のシナリオと、問題を解決するための基本的な推奨事項です。

システム スライス ドライブの障害

- このシナリオでは、スロット2が検証され、使用可能な状態に戻ります。
- スライス サービスをオンラインに戻す前に、システム スライス ドライブにデータを再度読み込む必要があります。
- システム スライス ドライブを交換し、システム スライス ドライブが使用可能になったらシステム スライス ドライブとスロット2のドライブを同時に追加します。

注 : スロット2のドライブをメタデータ ドライブとして単独で追加することはできません。両方のドライブを同時にノードに戻す必要があります。

スロット2の障害

- このシナリオでは、システム スライス ドライブが検証され、使用可能な状態に戻ります。
- スロット2をスペアと交換し、スロット2が使用可能になったらシステム スライス ドライブとスロット2のドライブを同時に追加します。

システム スライス ドライブとスロット2の障害

- システム スライス ドライブとスロット2の両方をスペア ドライブと交換します。両方のドライブが使用可能になったらシステム スライス ドライブとスロット2のドライブを同時に追加します。

処理の順序

- 障害が発生したハードウェア ドライブをスペア ドライブと交換します（両方のドライブに障害が発生した場合は、両方とも交換します）。
- ドライブにデータが再度読み込まれて使用可能な状態になったら、ドライブをクラスタに戻します。

検証処理

- [Active Drives]リストで、スロット0（または内部）とスロット2のドライブがメタデータ ドライブとして認識されることを確認します。
- スライスの分散がすべて完了した（イベント ログにmoving slicesメッセージが表示されなくなって30分以上経過した）ことを確認します。

関連タスク

*MDSS*ドライブの追加（183ページ）

スロット2のブロック ドライブをスライス ドライブに変換することで、SolidFireノードに2つ目のメタデータ ドライブを追加できます。そのためには、マルチドライブ スライス サービス（MDSS）機能を有効にします。この機能を有効にするには、ネットアップ サポートに連絡する必要があります。

MDSSドライブの追加

スロット2のブロック ドライブをスライス ドライブに変換することで、SolidFireノードに2つ目のメタデータ ドライブを追加できます。そのためには、マルチドライブ スライス サービス（MDSS）機能を有効にします。この機能を有効にするには、ネットアップ サポートに連絡する必要があります。

タスク概要

スライス ドライブを使用可能な状態にするために、障害が発生したドライブを新しいドライブまたはスペア ドライブと交換しなければならない場合があります。スロット2のドライブを追加するときに、システム スライス ドライブを同時に追加する必要があります。スロット2のスライス ドライブを単独で、またはシステム スライス ドライブを追加する前に追加しようとすると、エラーが発生します。

手順

1. **[Cluster]** > **[Drives]**の順にクリックします。
2. **[Available]**をクリックして、使用可能ドライブのリストを表示します。
3. 追加するスライス ドライブを選択します。
4. **[Bulk Actions]**をクリックします。
5. **[Add]**をクリックします。
6. **[Active Drives]**タブでドライブが追加されたことを確認します。

MDSSドライブの削除

マルチドライブ スライス サービス（MDSS）のドライブを削除できます。この手順を実行できるのは、ノードに複数のスライス ドライブがある場合のみです。

タスク概要

注 : システム スライス ドライブとスロット2のドライブで障害が発生すると、システムによってスライス サービスがシャットダウンされ、ドライブが削除されます。障害が発生していない状況でドライブを削除する場合は、両方のドライブを同時に削除する必要があります。

手順

1. **[Cluster]** > **[Drives]**の順にクリックします。
2. **[Available]**ドライブ タブで、削除するスライス ドライブのチェック ボックスをオンにします。
3. **[Bulk Actions]**をクリックします。
4. **[Remove]**をクリックします。
5. 操作を確定します。

ノードのトラブルシューティング

メンテナンスまたは交換のために、ノードをクラスタから削除できます。ノードをオフラインにする前に、NetApp Element UIまたはAPIを使用してノードを削除する必要があります。

ストレージ ノードを削除する手順の概要を次に示します。

- ノード上のデータのコピーを作成するための十分な容量がクラスタにあることを確認します。
- UIまたは`RemoveDrives` APIメソッドを使用して、クラスタからドライブを削除します。

この結果、ノードのドライブからクラスタ内の他のドライブへデータが移行されます。このプロセスの所要時間は、移行が必要なデータの量によって異なります。
- クラスタからノードを削除します。

ノードの電源をオフまたはオンにする際は、次の点に注意してください。

- ノードとクラスタの電源オフは、正しく実行しないと危険です。ノードの電源オフは、ネットアップ サポートの指示の下で行う必要があります。
- シャットダウンの方法にかかわらず、ノードが停止してから5分半が経過すると、Double Helixデータ保護によってデータのレプリケートが開始され、レプリケートされた個々のブロックが別のノードに書き込まれます。この場合は、ネットアップ サポートに連絡して障害ノードの分析を依頼してください。
- ノードを安全にリブートまたは電源をオフにするには、`Shutdown` APIコマンドを使用できます。
- ノードが停止またはオフになったら、オンラインに戻す前にネットアップ サポートに連絡する必要があります。
- サービスが停止していた時間によっては、ノードをオンラインに戻したあとに、ドライブを再度クラスタに追加する必要があります。

関連情報

障害が発生した*SolidFire*シャーシの交換

Replacing a failed H600S series node

クラスタの電源オフ

ネットアップ サポートに連絡して準備手順を完了したら、クラスタ全体の電源をオフにすることができます。

開始する前に

以下の手順でクラスタをシャットダウンする準備をします。

- すべてのI/Oを停止します。
- すべてのiSCSIセッションを切断します。

手順

1. クラスタの管理仮想IPアドレス（MVIP）に移動して、Element UIを開きます。
2. [Nodes]リストに表示されているノードをメモします。
3. クラスタ内の各ノードIDに対し、`halt`オプションを指定して`Shutdown` APIメソッドを実行します。

ストレージノードのノードごとのユーティリティの操作

NetApp Element Software UI の標準的な監視ツールでNetApp Elementソフトウェア分な情報が得られない場合は、ノード単位のユーティリティを使用してネットワークの問題をトラブルシューティングできます。ノード単位のユーティリティには、ノード間または管理ノードとの間のネットワーク問題のトラブルシューティングに役立つ特定の情報とツールが用意されています。

関連タスク

ノード単位の *UI* を使用したノード単位の設定へのアクセス（185ページ）

管理ノード IP を入力して認証を受けると、ノード単位のユーザインターフェイスでネットワーク設定、クラスタ設定、およびシステムテストとユーティリティにアクセスできます。

ノード単位の *UI* を使用したシステムテストの実行（188ページ）

ネットワーク設定を変更してネットワーク構成に適用したら、変更した設定をテストできます。テストを実行して、ストレージノードが安定していて、問題なくオンラインにできることを確認できます。

ノード単位の *UI* を使用したシステムユーティリティの実行（190ページ）
ストレージノードのノードごとの UI を使用して、サポートバンドルの作成または削除、ドライブの構成設定のリセット、ネットワークサービスまたはクラスタサービスの再起動を行うことができます。

関連資料

ノード単位の *UI* からのネットワーク設定の詳細（186ページ）
ストレージノードのネットワーク設定を変更して、ノードに新しいネットワーク属性のセットを割り当てることができます。

クラスタ設定の詳細は、ノード単位の *UI* から取得します（187ページ）
クラスタ構成後にストレージノードのクラスタ設定を確認し、ノードのホスト名を変更できます。

ノード単位の UI を使用したノード単位の設定へのアクセス

管理ノード IP を入力して認証を受けると、ノード単位のユーザインターフェイスでネットワーク設定、クラスタ設定、およびシステムテストとユーティリティにアクセスできます。

タスク概要

クラスタの一部であるアクティブ状態のノードの設定を変更する場合は、クラスタ管理者ユーザとしてログインする必要があります。

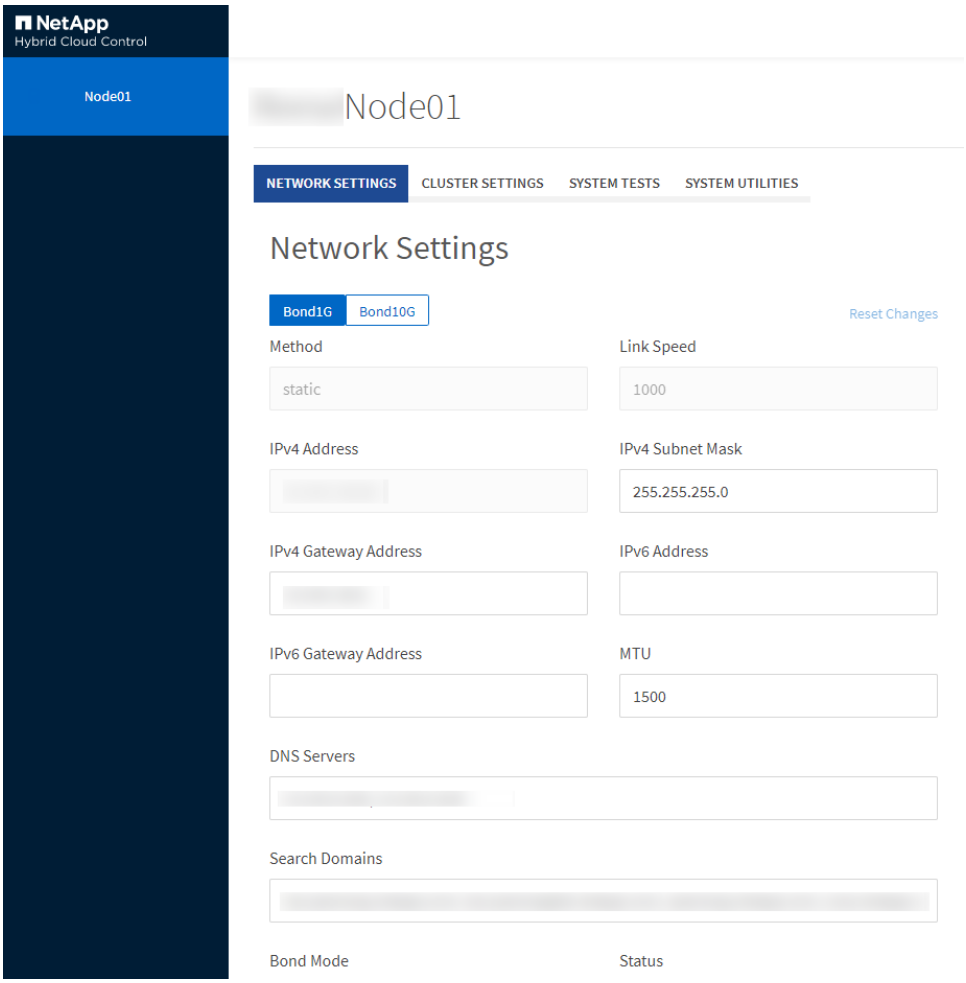
ヒント : ノードは一度に1つずつ設定または変更しください。指定したネットワーク設定が期待どおりの効果を持っていること、およびネットワークが安定していて、正常に動作していることを確認してから、別のノードに変更を加える必要があります。

手順

次のいずれかの方法を使用して、ノードごとの UI を開きます。

- ブラウザウィンドウに管理 IP アドレスを入力し、その後に 442 を入力して、 admin ユーザ名とパスワードを使用してログインします。
- Element UI で、**Cluster** > **Nodes**を選択し、設定または変更するノードの Management IP Address リンクをクリックします。

表示されたブラウザ ウィンドウでノードの設定を編集できます。



ノード単位の UI からのネットワーク設定の詳細

ストレージノードのネットワーク設定を変更して、ノードに新しいネットワーク属性のセットを割り当てることができます。

ノード**Network Settings**にログイン`https://<node IP>:442/hcc/node/network-settings`すると、ストレージノードのネットワーク設定がページに表示されます（）。**Bond1G**（管理**Bond10G**）または（ストレージ）のいずれかの設定を選択できます。次のリストは、ストレージノードが使用可能、保留中、またはアクティブ状態のときに変更できる設定を示しています。

方法

インターフェイスの設定に使用する方法。使用可能な方法：

- `loopback`：IPv4ループバック インターフェイスを定義する場合に使用します。
- `manual`：デフォルトの設定がないインターフェイスを定義する場合に使用します。
- `dhcp`：DHCP経由でIPアドレスを取得する場合に使用します。
- `static`：IPv4アドレスが静的に割り当てられたイーサネット インターフェイスを定義する場合に使用します。

Link Speed

仮想NICによってネゴシエートされた速度。

IPv4 Address

eth0ネットワークのIPv4アドレス。

IPv4 Subnet Mask

IPv4ネットワークのアドレス分割。

IPv4 Gateway Address

ローカル ネットワークの外部にパケットを送信するためのルータのネットワーク アドレス。

IPv6 Address

eth0ネットワークのIPv6アドレス。

IPv6 Gateway Address

ローカル ネットワークの外部にパケットを送信するためのルータのネットワーク アドレス。

MTU

ネットワーク プロトコルで送信可能な最大パケット サイズ。1500以上にする必要があります。2つ目のストレージNICを追加する場合は、値を9000にする必要があります。

DNS Servers

クラスタ通信に使用するネットワーク インターフェイス。

Search Domains

システムで利用可能な追加のMACアドレスの検索。

Bond Mode

モードは次のいずれかになります。

- `ActivePassive`（デフォルト）
- `ALB`
- `LACP`

Status

有効な値は次のとおりです。

- `UpAndRunning`
- `Down`
- `Up`

Virtual Network Tag

仮想ネットワークの作成時に割り当てられたタグ。

Routes

特定のホストまたはネットワークへの静的ルート（ルートに設定されているインターフェイス経由）。

クラスタ設定の詳細は、ノード単位の UI から取得します

クラスタ構成後にストレージノードのクラスタ設定を確認し、ノードのホスト名を変更できます。

Cluster Settings次`https://<node IP>:442/hcc/node/cluster-settings`のリストは、ノード単位の UI のページに表示されるストレージノードのクラスタ設定を示しています（）。

ロール
クラスタにおけるノードのロール。有効な値は次のとおりです。

- `Storage`：ストレージ ノードまたはFibre Channelノード。
- `Management`：管理ノード。

ホスト名
ノードの名前。

クラスタ
クラスタの名前。

Cluster Membership
ノードの状態。有効な値は次のとおりです。

- `Available`：クラスタ名が関連付けられておらず、まだクラスタに含まれていないノードです。
- `Pending`：設定済みであり、指定されたクラスタに追加できるノードです。このノードにアクセスするための認証は不要です。
- `PendingActive`：互換性のあるソフトウェアをノードにインストールしています。インストールが完了すると、ノードはActive状態に移行します。
- `Active`：クラスタに参加しているノードです。このノードを変更するには、認証が必要です。

バージョン
ノードで実行されているElementソフトウェアのバージョン。

Ensemble
データベース アンサンブルに参加しているノード。

Node ID
クラスタへの追加時にノードに割り当てられたID。

Cluster Interface
クラスタ通信に使用するネットワーク インターフェイス。

管理ネットワーク インターフェイス
管理ネットワーク インターフェイス。デフォルトはBond1Gですが、Bond10Gも使用できます。

Storage Interface
Bond10Gを使用するストレージ ネットワーク インターフェイス。

暗号化対応
ノードがドライブ暗号化をサポートするかどうかを示します。

ノード単位の UI を使用したシステムテストの実行

ネットワーク設定を変更してネットワーク構成に適用したら、変更した設定をテストできます。テストを実行して、ストレージノードが安定していて、問題なくオンラインにできることを確認できます。

開始する前に

ストレージノードのノードごとの UI にログインしている。

手順

1. **System Tests**をクリックします。

2. **Run Test**実行するテストの横**Run All Tests**にあるをクリックするか、を選択します。

   注 : すべてのテスト処理を実行するには時間がかかり、ネットアップのサポートの指示がある場合にのみ実行する必要があります。

   Test Connected Ensemble

   データベース アンサンブルへの接続を検証します。デフォルトでは、ノードが関連付けられているクラスタのアンサンブルがテストで使用されます。また、接続をテストする別のアンサンブルを指定することもできます。

   Test Connect Mvip

   指定した管理仮想 IP （ MVIP ）アドレスに ping を実行し、 MVIP への単純な API コールを実行して接続を確認します。デフォルトでは、ノードが関連付けられているクラスタには MVIP が使用されます。

   Test Connect Svip

   ネットワークアダプタに設定されている最大伝送単位（ MTU ）サイズに一致する Internet Control Message Protocol （ ICMP ）パケットを使用して、指定された Storage Virtual IP （ SVIP ）アドレスに ping を実行します。その後、iSCSIイニシエータとしてSVIPに接続します。デフォルトでは、ノードが関連付けられているクラスタに SVIP が使用されます。

   Test Hardware Config

   すべてのハードウェア構成をテストして、ファームウェアのバージョンが正しいこと、すべてのドライブが適切に実装されて実行されていることを確認します。工場出荷時のテストと同じ内容です。

   注 : このテストはリソースを大量に消費するため、ネットアップのサポートから要求された場合にのみ実行してください。

   Test Local Connectivity

   各ノードでクラスタIP（CIP）に対してpingを実行して、クラスタの他のすべてのノードへの接続をテストします。このテストは、ノードがアクティブなクラスタに属している場合にのみ表示されます。

   Test Locate Cluster

   ノードがクラスタ構成で指定されたクラスタを特定できることを検証します。

   Test Network Config

   設定したネットワーク設定がシステムで使用されているネットワーク設定と一致することを確認します。このテストは、ノードがクラスタにアクティブに参加しているときにハードウェア障害を検出するためのものではありません。

   Test Ping

   指定されたホストのリストに対して ping を実行します。指定されていない場合は、クラスタ内のすべての登録済みノードのリストを動的に構築し、簡単な接続を実現するために ping を実行します。

   Test Remote Connectivity

   各ノードでクラスタ IP （ CIP ）に ping を実行して、リモートペアクラスタ内のすべてのノードへの接続をテストします。このテストは、ノードがアクティブなクラスタに属している場合にのみ表示されます。

ノード単位の UI を使用したシステムユーティリティの実行

ストレージノードのノードごとの UI を使用して、サポートバンドルの作成または削除、ドライブの構成設定のリセット、ネットワークサービスまたはクラスタサービスの再起動を行うことができます。

開始する前に

ストレージノードのノードごとの UI にログインしている。

手順

1. **System Utilities**をクリックします。
2. 実行するシステムユーティリティのボタンをクリックします。

制御電力

ノードのリブート、電源の再投入、またはシャットダウンを行います。

注意 : この処理を実行するとネットワーク接続が一時的に失われます。

次のパラメータを指定します。

- 処置：オプションには、再起動と停止（電源オフ）があります。
- ウェイクアップ遅延：ノードがオンラインに戻るまでの時間。

ノードログを収集します

ノード`/tmp/bundles`のディレクトリの下にサポートバンドルを作成します。

次のパラメータを指定します。

- Bundle Name ：作成された各サポートバンドルの一意の名前。名前を指定しない場合、「supportbundle」とノード名がファイル名として使用されます。
- 追加引数：`sf_make_support_bundle`このパラメータはスクリプトに渡されます。このパラメータは、ネットアップ サポートから指示された場合にのみ使用します。
- [Timeout sec] ：個々の ping 応答を待機する秒数を指定します。

ノードログを削除します

Create Cluster Support Bundleまたは`CreateSupportBundle` API メソッドを使用して作成されたノード上の現在のサポートバンドルを削除します。

Reset Drives

ドライブを初期化し、ドライブに現在存在するすべてのデータを削除します。初期化したドライブは、既存のノードまたはアップグレードしたノードで再利用できます。

次のパラメータを指定します。

- drives ：リセットするデバイス名のリスト（ DriveID ではない）。

ネットワーク設定をリセットします

個々のノードのネットワーク構成の問題を解決し、個々のノードのネットワーク構成を工場出荷時のデフォルト設定にリセットします。

Reset Node

ノードを工場出荷時の設定にリセットします。すべてのデータが削除されますが、この処理中はノードのネットワーク設定が保持されます。ノードをリセットできるのは、ノードがクラスタに割り当てられておらず、 Available 状態になっている場合だけです。

注意 : このオプションを使用すると、すべてのデータ、パッケージ（ソフトウェアアップグレード）、設定、およびログファイルがノードから削除されます。

Restart Networking

ノードのすべてのネットワーク サービスを再起動します。

注意 : この処理を実行すると、ネットワーク接続が一時的に失われることがあります。

Restart Services

ノードで Element Software サービスを再起動します。

注意 : この処理を実行すると、ノード サービスが一時的に中断されることがあります。この処理は、ネットアップ サポートから指示があった場合にのみ実行してください。

次のパラメータを指定します。

- サービス：再起動するサービス名。
- [Action] ：サービスに対して実行するアクション。オプションには、 Start 、 Stop 、および Restart があります。

管理ノードの使用

管理ノード（mNode）は、システム サービスのアップグレード、クラスタのアセットと設定の管理、システムのテストとユーティリティの実行、Active IQへの接続（システム監視）、ネットアップ サポートへのアクセス許可（トラブルシューティング）に使用します。

Elementソフトウェア バージョン11.3以降を実行しているクラスタでは、管理ノードUI（`https://[mNode IP]:442`）を使用してネットワークとクラスタの設定を変更したり、システム テストを実行したり、システム ユーティリティを使用したりできます。また、組み込みのREST API UI（`https://[mNode IP]/mnode`）を使用して、プロキシ サーバの設定、サービス レベルの更新、管理ノードが認識しているアセットの管理などの管理ノード サービスに関連するAPIを実行し、またその内容を把握することができます。

関連タスク

管理ノードのノード*UI*へのアクセス（192ページ）
ノードUIからは、ネットワークとクラスタの設定にアクセスし、システムのテストとユーティリティを利用できます。

管理ノードの*REST API UI*へのアクセス（193ページ）
Elementソフトウェア バージョン11.3以降、管理ノードには2つのUIが装備されています。RESTベースのサービスを管理するためのUIと、ネットワーク / クラスタ設定の管理とオペレーティング システムのテスト / ユーティリティを実行するためのノードUIです。REST API UIからは、管理ノード上の管理サービスを制御するサービス関連APIのメニューにアクセスできます。

管理ノードへのアクセス

NetApp Elementソフトウェア バージョン11.3以降、管理ノードには2つのUIが装備されています。RESTベースのサービスを管理するためのUIと、ネットワーク / クラスタ設定の管理とオペレーティング システムのテスト / ユーティリティを実行するためのノードUIです。

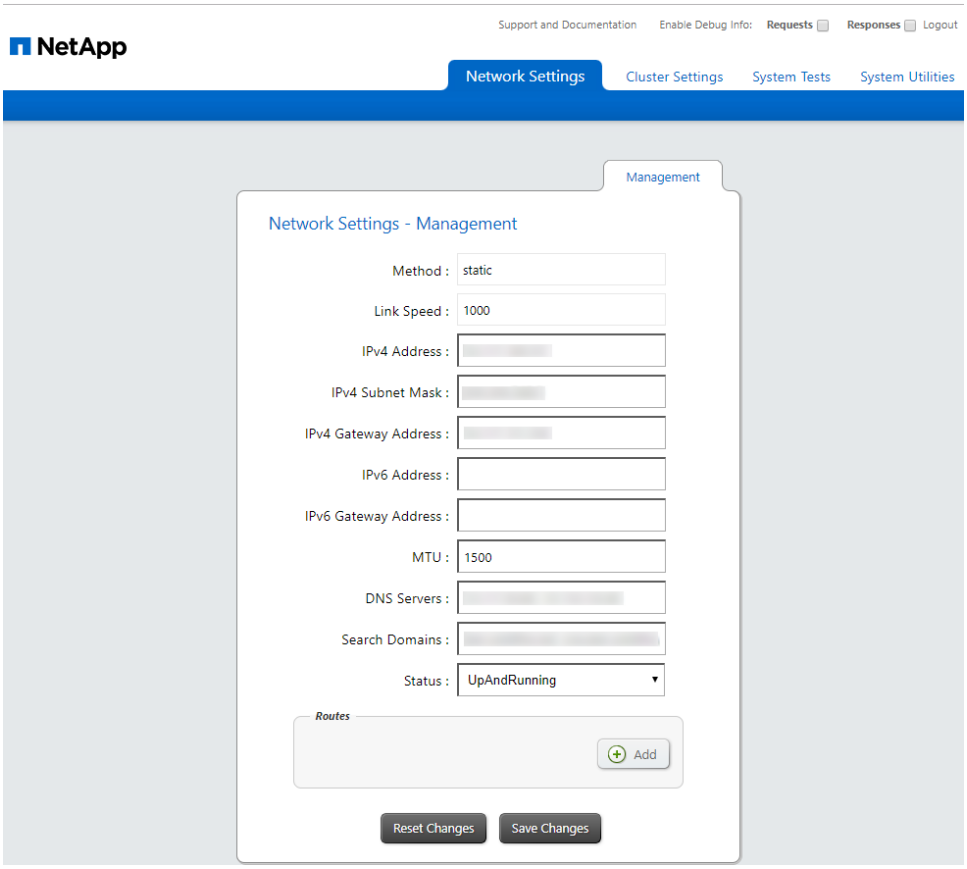
管理ノードのノードUIへのアクセス

ノードUIからは、ネットワークとクラスタの設定にアクセスし、システムのテストとユーティリティを利用できます。

手順

1. 管理ノードのノードUIにアクセスするには、管理ノードのIPアドレスに続けて「:442」と入力します。

   ```
   https://[IP address]:442
   ```



2. プロンプトが表示されたら、管理ノードのユーザ名とパスワードを入力します。

関連タスク

管理ノードの*REST API UI*へのアクセス（193ページ）

Elementソフトウェア バージョン11.3以降、管理ノードには2つのUIが装備されています。RESTベースのサービスを管理するためのUIと、ネットワーク / クラスタ設定の管理とオペレーティング システムのテスト / ユーティリティを実行するためのノードUIです。REST API UIからは、管理ノード上の管理サービスを制御するサービス関連APIのメニューにアクセスできます。

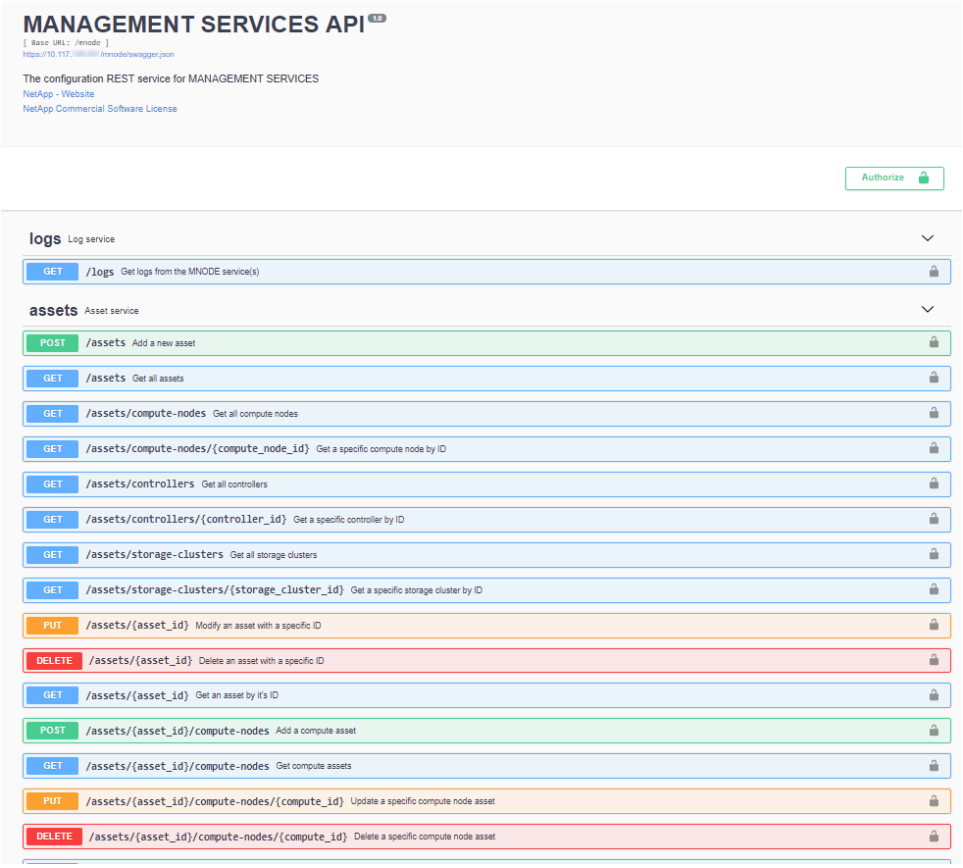
管理ノードのREST API UIへのアクセス

Elementソフトウェア バージョン11.3以降、管理ノードには2つのUIが装備されています。RESTベースのサービスを管理するためのUIと、ネットワーク / クラスタ設定の管理とオペレーティング システムのテスト / ユーティリティを実行するためのノードUIです。REST API UIからは、管理ノード上の管理サービスを制御するサービス関連APIのメニューにアクセスできます。

手順

1. 管理サービスのREST API UIにアクセスするには、管理ノードのIPアドレスに続けて「/mnode」と入力します。

   `https://[IP address]/mnode`



2. **[Authorize]**または任意のロック アイコンをクリックし、クラスタ管理者のクレデンシャルを入力してAPIを使用する権限を取得します。

REST APIを使用するための承認の取得

REST API UIで管理サービス用のAPIを使用するには、事前に承認が必要です。アクセス トークンを取得するには、クラスタ管理者のクレデンシャルとクライアントIDを指定する必要があります。各トークンの有効期間は約10分です。トークンの期限が切れたら、再度承認して新しいアクセス トークンを取得できます。

開始する前に

- クラスタでNetApp Elementソフトウェア11.3以降を実行している必要があります。
- バージョン11.3以降を実行する管理ノードを導入しておきます。

タスク概要

承認機能は、管理ノードのインストールおよび導入時に自動的にセットアップされます。トークン サービスは、セットアップ時に定義したストレージ クラスタに基づいています。

手順

1. 管理ノードで REST API UI を開きます。 `https://[management node IP]/mnode`
2. をクリックし**Authorize**て、次の手順を実行します。

   注 : または、任意のサービスAPIの横にあるロック アイコンをクリックし、以下の手順に従って承認することもできます。

   1. クラスタのユーザ名とパスワードを入力します。
   2. **Request bodytype**値がまだ選択されていない場合は、ドロップダウンリストから選択します。
   3. `mnode-client`の値がまだ入力されていない場合は、クライアントIDを入力します。
   4. クライアント シークレットの値は入力しないでください。
   5. **Authorize**クリックするとセッションが開始されます。

      注 : 承認の試行後に「`Auth Error Type Error: Failed to fetch`」というエラー メッセージが返された場合は、クラスタのMVIPのSSL証明書の受け入れが必要になる可能性があります。トークンURL内のIPをコピーし、別のブラウザ タブにIPを貼り付けて、再度承認してください。

   Available authorizations画面に**Authorized**が表示されます。
3. **Available authorizations**ダイアログボックスを閉じます。

   注 : トークンの期限が切れたあとでコマンドを実行しようとすると、「401 `Error: UNAUTHORIZED`」メッセージが返されます。この場合は、再度承認してください。

NetApp HCIのアラート監視

管理ノードのノードUIの[Alert Monitor]タブでは、NetApp HCIのアラート監視を設定することができます。

NetApp HCIのアラート監視は、NetApp HCIストレージ クラスタのシステム アラートをvCenter Serverに転送して、NetApp HCIのすべてのアラートをvSphere Web Clientインターフェイスで表示できるようにします。

注意 : これらのツールは、SolidFireオールフラッシュ ストレージなどのストレージ専用クラスタでは設定も使用もされません。ツールを実行すると次のような405エラーが表示されますが、これは設定に応じた想定どおりの動作です。`webUIParseError : Invalid response from server. 405`

関連情報

*NetApp HCI*ドキュメント センター

管理ノードのネットワーク設定

管理ノードのノードUIの[Network Settings]タブでは、管理ノードのネットワーク インターフェイスに関するフィールドを変更できます。

Method

インターフェイスの設定に使用する方法。有効な方法は次のとおりです。

- `loopback`：IPv4ループバック インターフェイスを定義する場合に使用します。

- `manual`：デフォルトの設定がないインターフェイスを定義する場合に使用します。
- `dhcp`：DHCP経由でIPアドレスを取得する場合に使用します。
- `static`：IPv4アドレスが静的に割り当てられたイーサネット インターフェイスを定義する場合に使用します。

Link Speed

仮想NICによってネゴシエートされた速度。

IPv4 Address

eth0ネットワークのIPv4アドレス。

IPv4 Subnet Mask

IPv4ネットワークのアドレス分割。

IPv4 Gateway Address

ローカル ネットワークの外部にパケットを送信するためのルータのネットワーク アドレス。

IPv6 Address

eth0ネットワークのIPv6アドレス。

注意： この機能は、11.3以降のバージョンの管理ノードではサポートされていません。

IPv6 Gateway Address

ローカル ネットワークの外部にパケットを送信するためのルータのネットワーク アドレス。

注意： この機能は、11.3以降のバージョンの管理ノードではサポートされていません。

MTU

ネットワーク プロトコルで送信可能な最大パケット サイズ。1500以上にする必要があります。2つ目のストレージNICを追加する場合は、値を9000にする必要があります。

DNS Servers

クラスタ通信に使用するネットワーク インターフェイス。

Search Domains

システムで利用可能な追加のMACアドレスの検索。

Status

有効な値は次のとおりです。

- `UpAndRunning`
- `Down`
- `Up`

Routes

特定のホストまたはネットワークへの静的ルート（ルートに設定されているインターフェイス経由）。

管理ノードのクラスタ設定

管理ノードのノードUIの[Cluster Settings]タブでは、ノードの状態が`Available`、`Pending`、`PendingActive`、および`Active`の場合に、クラスタ インターフェイスに関するフィールドを変更できます。

Role

クラスタ内での管理ノードのロール。有効な値は`Management`です。

Hostname

管理ノードの名前。

Version

クラスタで実行されているElementソフトウェアのバージョン。

Default Interface

管理ノードとElementソフトウェアを実行しているクラスタとの通信に使用されるデフォルトのネットワーク インターフェイス。

管理ノード設定のテスト

管理ノードの管理設定とネットワーク設定を変更して変更をコミットしたあとに、テストを実行して変更を検証できます。

開始する前に

管理ノードの管理者クレデンシャルを使用して、管理ノードのノードUI（`https://[mNode IP address]:442`）にログインしておきます。

手順

1. 管理ノードのユーザ インターフェイスで、**[System Tests]**をクリックします。
2. 次のいずれかを実行します。
   - 指定したネットワーク設定がシステムに対して有効であることを確認するには、**[Test Network Config]**をクリックします。
   - ICMPパケットを使用して1Gおよび10G両方のインターフェイスでクラスタ内のすべてのノードへのネットワーク接続をテストするには、**[Test Ping]**をクリックします。

   以下のオプションを追加で定義することもできます。

   Hosts

   pingを実行するデバイスのアドレスまたはホスト名をカンマで区切って指定します。

   Attempts

   pingテストを繰り返す回数を指定します。デフォルト値は5です。

   Packet Size

   各IPに送信されるICMPパケットで送信するバイト数を指定します。ネットワーク設定で指定した最大MTUより小さくする必要があります。

   Timeout mSec

   個々のping応答を待機する時間（ミリ秒）を指定します。デフォルト値は500ミリ秒です。

Total Timeout Sec

pingがシステム応答を待機する時間（秒）。この期間を過ぎると、次のpingが実行されるか、またはプロセスが終了します。デフォルト値は5です。

Prohibit Fragmentation

ICMPパケットのDF（Do not Fragment）フラグを有効にします。

関連資料

管理ノードのネットワーク設定（194ページ）

管理ノードのノードUIの[Network Settings]タブでは、管理ノードのネットワーク インターフェイスに関するフィールドを変更できます。

管理ノードからのシステム ユーティリティの実行

管理ノードのノードUIを使用して、クラスタ サポート バンドルの作成または削除、ノード設定のリセット、ネットワークの再起動を実行できます。

開始する前に

管理ノードの管理者クレデンシャルを使用して、管理ノードのノードUI（`https://[mNode IP address]:442`）にログインしておきます。

手順

1. 管理ノードのノードUIで、**[System Utilities]**をクリックします。
2. 実行するユーティリティのボタンをクリックします。
   - **Control Power**：ノードをリブート、電源再投入、またはシャットダウンします。

     注意：この処理を実行するとネットワーク接続が一時的に失われます。

     次のオプションを指定します。

     Action

     `[Restart]`または`[Halt]`（電源オフ）を選択できます。

     Wakeup Delay

     ノードがオンラインに戻るまでの時間。
   - **Create Cluster Support Bundle**：クラスタ内のノードについてネットアップ サポートの診断を受けるためのクラスタ サポート バンドルを作成します。次のオプションを指定します。

     Bundle Name

     作成する各サポート バンドルの一意の名前。名前を指定しない場合、「supportbundle」とノード名がファイル名として使用されます。

     Mvip

     クラスタのMVIP。バンドルは、クラスタ内のすべてのノードから収集されます。このパラメータは、`[Nodes]`パラメータを指定しない場合のみ必須です。

     Nodes

     バンドルを収集するノードのIPアドレス。`[Nodes]`または`[Mvip]`のいずれかを使用してバンドルの収集元のノードを指定します。両方を使用することはできません。このパラメータは、`[Mvip]`を指定しない場合のみ必須です。

     Username

     クラスタ管理者のユーザ名。

Password

クラスタ管理者のパスワード。

Allow Incomplete

1つ以上のノードからバンドルを収集できない場合でも、スクリプトが引き続き実行されるようにします。

Extra Args

このパラメータは、`sf_make_support_bundle`スクリプトに渡されます。このパラメータは、ネットアップ サポートから指示された場合にのみ使用します。

- **Delete All Support Bundles**：管理ノードに保存されているすべてのサポート バンドルを削除します。
- **Reset Node**：管理ノードを新規インストール イメージにリセットします。これにより、ネットワーク設定を除くすべての設定がデフォルトの状態に戻ります。

  注意：この処理を実行するとネットワーク接続が一時的に失われます。

  次のオプションを指定します。

  Build

  ノードをリセットするリモートElementソフトウェア イメージのURL。

  Options

  リセット処理を実行するための詳細。詳細が必要な場合は、ネットアップ サポートにお問い合わせください。
- **Restart Networking**：管理ノード上のすべてのネットワーク サービスを再起動します。

  注意：この処理を実行するとネットワーク接続が一時的に失われます。

ネットワーク サポートによるリモート接続の有効化

NetApp Elementソフトウェアベースのストレージ システムに関して技術的なサポートが必要な場合は、ネットアップ サポートがお客様のシステムにリモートで接続できます。リモート アクセスを確立するために、ネットアップ サポートはお客様の環境へのリバースSecure Shell（SSH）接続を確立します。

タスク概要

ネットアップ サポートとのSSHリバース トンネル接続用のTCPポートを開くことができます。この接続を介して、ネットアップ サポートはお客様の管理ノードにログインします。管理ノードがプロキシ サーバの背後にある場合は、次のTCPポートを`sshd.config`ファイルで設定しておく必要があります。

TCPポート	説明	接続方向
443	API呼び出し / HTTPS（オープン サポート トンネルを介したWeb UIへのリバース ポート転送）	管理ノードからストレージ ノードへ
22	SSHログイン アクセス	管理ノードからストレージ ノードへ、またはストレージ ノードから管理ノードへ

手順

1. 管理ノードにログインし、ターミナル セッションを開きます。
2. プロンプトで、 `rst -r sfsupport.solidfire.com -u element -p < ポート番号 >` と入力します

   SSH接続を使用して管理ノードにアクセスするために必要なポート番号は、ネットアップ サポートから入手します。
3. リモートサポートトンネルを閉じるには、次のように入力します。 `rst--killall`

関連資料

ネットワーク ポート要件（14ページ）

システムをリモートから管理し、クライアントがデータセンターの外部からリソースに接続できるようにするために、データセンターのエッジ ファイアウォールで次のTCPポートを許可する必要があります。システムの使用方法によっては、一部のポートは不要な場合もあります。

SolidFireオールフラッシュ ストレージに対するActive IQコレクタ サービスの有効化

インストールまたはアップグレード時にSolidFireオールフラッシュ ストレージに対してストレージのテレメトリ（Active IQコレクタ サービス）を有効にしていない場合、有効にすることができます。AIQコレクタ サービスは、履歴データのレポートおよびほぼリアルタイムのパフォーマンス監視用に、設定データとElementソフトウェアベースのクラスタ パフォーマンス データをNetApp SolidFire Active IQに転送します。

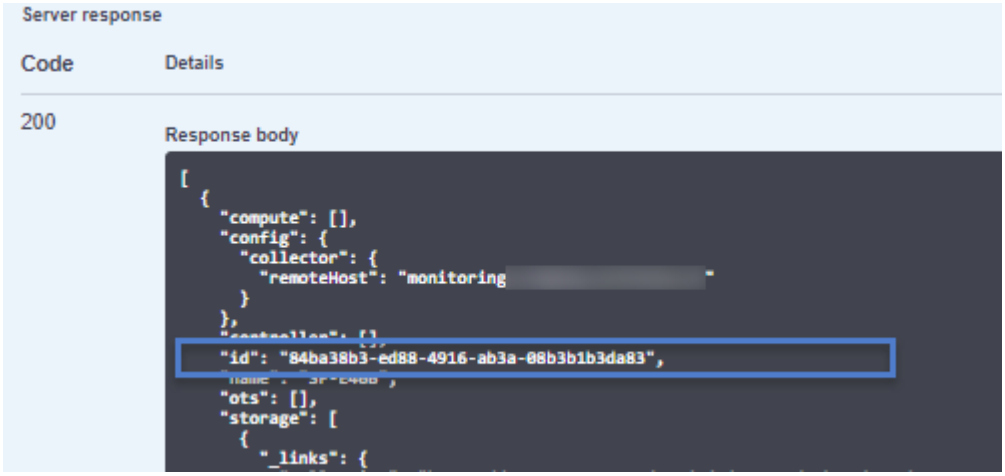
開始する前に

- クラスタでNetApp Elementソフトウェア11.3以降を実行している必要があります。
- バージョン11.3以降を実行する管理ノードを導入しておきます。
- インターネットへのアクセスが必要です。Active IQコレクタ サービスをダーク サイトから使用することはできません。

手順

1. 管理ノードで REST API UI を開きます。 `https://[management node IP]/mnode`
2. **Authorize**をクリックするか、ロックアイコンをクリックして、次の手順を実行します。
   1. クラスタのユーザ名とパスワードを入力します。
   2. `mnode-client`の値がまだ入力されていない場合は、クライアントIDを入力します。
   3. **Authorize**クリックするとセッションが開始されます。
3. **GET /assets**をクリックします。
4. ベース アセットの`"id"`の値をクリップボードにコピーします。

   注 : ベース アセットとサブアセットは、管理ノードのインストールまたはアップグレード時にアップグレード スクリプトまたはセットアップ スクリプトを実行したときに作成されています。



5. ベース アセットを設定します。
   1. **PUT /assets/{asset_id}**をクリックします。
   2. **Try it out**をクリックします。
   3. JSONペイロードに次のコマンドを入力します。

      ```
      {
          "telemetry_active": true
          "config": {}
      }
      ```
   4. の Base Asset ステップから ID**asset_ID** を入力します。
   5. **Execute**をクリックします。

      Active IQサービスはアセットが変更されるたびに自動的に再起動されます。アセットを変更すると、設定が適用されるまで短時間の遅延が発生します。

管理ノードへのアセットの追加

REST API UI を使用して、コンピューティング資産とコントローラ資産を管理ノード構成に追加できます。アセットの追加は、環境を拡張したあとに、新しいアセットが構成に自動的に追加されなかった場合などに必要になります。これらのAPIを使用して、最近追加されたアセットを環境に追加します。

開始する前に

- クラスタでNetApp Elementソフトウェア11.3以降を実行している必要があります。
- バージョン11.3以降を実行する管理ノードを導入しておきます。

タスク概要

NetApp HCI システムを拡張した後に、HCC（ハイブリッドクラウドコントロール**POST /assets/{asset_id}/compute-nodes**）にコンピュートノードが表示されない場合は、この手順で説明したを使用してコンピュートノードを追加できます。

手順

1. 管理ノードで REST API UI を開きます。 `https://[management node IP]/mnode`
2. **Authorize**をクリックするか、ロックアイコンをクリックして、次の手順を実行します。
   1. クラスタのユーザ名とパスワードを入力します。
   2. `mnode-client`の値がまだ入力されていない場合は、クライアントIDを入力します。
   3. **Authorize**クリックするとセッションが開始されます。

3. 次のいずれかをクリックして、既存のベースアセットにコンピューティングノードまたはコントローラのサブアセットを追加します。

   注 : インストール環境には、インストール時またはアップグレード時に作成されたベース アセットの構成が含まれています。

オプション	説明
POST /assets/{asset_id}/controllers	コントローラ サブアセットを作成する場合は、このコマンドを実行します。
POST /assets/{asset_id}/compute-nodes	コンピューティング ノード サブアセットを作成する場合は、このコマンドを実行します。

4. **Try it out**をクリックします。
5. **Model**タブで定義されている必要なペイロード値を入力します。

   重要 : コンピュートノード資産の場合は、ペイロードの例で推奨されている "Hardware_Tag" パラメータを削除します。

6. 親ベースのアセット ID**asset_id** を「」フィールドに入力します。
7. **Execute**をクリックします。

ストレージクラスタ管理者パスワードの変更

ストレージクラスタ管理者パスワードは、 REST API UI を使用して更新できます。

開始する前に

ストレージクラスタ管理者のパスワードは、 NetApp Element ソフトウェアの UI を使用して変更しました。

手順

1. ブラウザから、管理ノード REST API UI にログインします。
   1. Storage MVIP にアクセスしてログインします。
      次の手順用に証明書が承認されます。
   2. 管理ノードで REST API UI を開きます。 `https://[management node IP]/mnode`
2. Management Node REST API UI で**Authorize**、または任意のロックアイコンをクリックし、次の手順を実行します。
   1. クラスタのユーザ名とパスワードを入力します。
   2. `mnode-client`の値がまだ入力されていない場合は、クライアントIDを入力します。
   3. **Authorize**クリックするとセッションが開始されます。
3. 次**GET /assets**の手順で必要なベースアセット ID を検索するには、を実行します。
   1. [**GET /assets**
   2. **Try it out**をクリックします。
   3. **Execute**をクリックします。
4. ベースアセットの「 ID 」の値をクリップボードにコピーします。

   注 : ベース アセットとサブアセットは、管理ノードのインストールまたはアップグレード時にアップグレード スクリプトまたはセットアップ スクリプトを実行したとき、またはNetApp Deployment Engineを使用してNetApp HCIを導入したときに作成されます。

5. ストレージ資産の取得：
   1. **GET /assets/{ASSET_ID}/storage-clusters**をクリックします。
   2. **Try it out**をクリックします。

3. の Base Asset ステップから ID**asset_ID** を入力します。
4. **Execute**をクリックします。

6. ストレージ資産を更新します。
   1. **PUT /assets/{ASSET_ID}/storage-clusters/{STORAGE_ID}**をクリックします。
   2. **Try it out**をクリックします。
   3. **Model**タブで定義されている必要なペイロード値を更新します。
      - ホスト名と SSL 証明書の行を削除します。
      - パスワード行に新しいパスワードを入力します。

      ```
      {
           「ユーザ名」:「 admin 」、
           「パスワード」:「 admin 」、
           「 IP 」:「 10.10.1.124 」、
          "config": {}
      }
      ```
   4. 親ベースのアセット ID**asset_id** を「」フィールドに入力します。
   5. **Execute**をクリックします。

プロキシ サーバの設定

クラスタがプロキシ サーバの背後にある場合、パブリック ネットワークに接続できるようにプロキシを設定する必要があります。プロキシ サーバは、テレメトリ コレクタとリバース トンネル接続に使用されます。インストールまたはアップグレード時にプロキシ サーバを設定しなかった場合は、REST API UIを使用してプロキシ サーバを有効にして設定することができます。既存のプロキシ サーバ設定を変更したり、プロキシ サーバを無効にしたりすることもできます。

開始する前に

- 設定するプロキシ サーバのホストおよびクレデンシャル情報が必要です。
- クラスタでNetApp Elementソフトウェア11.3以降を実行している必要があります。
- バージョン11.3以降を実行する管理ノードを導入しておきます。

タスク概要

このコマンドは管理ノードのプロキシ設定を更新し、現在の設定を返します。プロキシ設定は、Active IQ、NetApp Deployment Engineによって導入されたNetApp HCI監視サービス、および管理ノードにインストールされたその他のElementソフトウェア ユーティリティ（ネットアップ サポート用のリバース サポート トンネルを含む）で使用されます。

手順

1. 管理ノードで REST API UI を開きます。 `https://[management node IP]/mnode`
2. **Authorize**をクリックするか、ロックアイコンをクリックして、次の手順を実行します。
   1. クラスタのユーザ名とパスワードを入力します。
   2. `mnode-client`の値がまだ入力されていない場合は、クライアントIDを入力します。
   3. **Authorize**クリックするとセッションが開始されます。
3. **PUT /settings**をクリックします。
4. **Try it out**をクリックします。
5. プロキシ サーバを有効にするには、`"use_proxy"`を`true`に設定する必要があります。IPまたはホスト名およびプロキシ ポートの接続先を入力します。プロキシ ユーザ名、

プロキシ パスワード、およびSSHポートはオプションです。使用しない場合は省略してください。

```
{
    "proxy_ip_or_hostname": "[IP or name]",
    "use_proxy": [true/false],
    "proxy_username": "[username]",
    "proxy_password": "[password]",
    "proxy_port": [port value],
    "proxy_ssh_port": [port value: default is 443]
}
```

6. **Execute**をクリックします。

管理サービスからのログの取得

REST APIを使用して、管理ノードで実行されているサービスからログを取得できます。すべてのパブリック サービスからログを取得したり、特定のサービスを指定したりできます。また、クエリ パラメータを使用して、取得する内容を細かく絞り込むこともできます。

開始する前に

- クラスタでNetApp Elementソフトウェア11.3以降を実行している必要があります。
- バージョン11.3以降を実行する管理ノードを導入しておきます。

手順

1. 管理ノードで REST API UI を開きます。 `https://[management node IP]/mnode`
2. **Authorize**をクリックするか、ロックアイコンをクリックして、次の手順を実行します。
   1. クラスタのユーザ名とパスワードを入力します。
   2. `mnode-client`の値がまだ入力されていない場合は、クライアントIDを入力します。
   3. **Authorize**クリックするとセッションが開始されます。
3. **GET /logs**をクリックします。
4. **Try it out**をクリックします。
5. 次のパラメータを指定します。
   - Lines : ログから取得する行数を入力します。このパラメータは整数で、デフォルト値は1000です。

     ヒント : Linesを0に設定すると過去のログ コンテンツがすべて取得されるので、注意してください。
   - service-name：サービス名を入力します。

     ヒント : 管理ノード上のサービスを表示するには、`GET /services`コマンドを使用します。
   - type：取得するログ タイプを選択します。
     1. `service`：実行中の通常のパブリック サービスから取得します。これがデフォルトであり、最も一般的なオプションです。
     2. `syslog`：ホスト マシンのすべてのsyslogから取得します。
     3. `all`：すべてのパブリック サービスとsyslogから取得します。
   - since：サービス ログの開始日時をISO-8601タイムスタンプで追加します。

     ヒント : 長期間のログを収集する場合は、sinceパラメータに適切な値を指定してください。

- archived：ログ要求にアーカイブ ファイルを追加します。

6. **Execute**をクリックします。

クラスタ フル レベルの概要

Elementソフトウェアを実行するクラスタの容量が不足してくると、クラスタ エラーが生成されてストレージ管理者に警告が表示されます。クラスタ フルには3つのレベル（Warning、Error、Critical）があり、すべてのレベルがネットアップ Element UIに表示されます。

クラスタ ブロック ストレージ フルに関する警告には、BlockClusterFullエラー コードが使用されます。Alertsクラスタのフルネスの重大度は、 Element UI のタブで確認できます。

BlockClusterFullの重大度レベルについて以下に説明します。

Warning

ユーザが設定可能な警告で、クラスタのブロック容量がErrorレベルに近づくと表示されます。このレベルはデフォルトでErrorレベルの3%下に設定されており、Element UIおよびAPIを使用して変更できます。できるだけ早く容量を追加するか、または解放する必要があります。

Error

クラスタがこの状態の場合、ノードが失われると、Double Helixデータ保護を再構築できるだけの容量がクラスタに残っていません。クラスタがこの状態にある間は、ボリュームの新規作成、クローンおよびSnapshotの処理はすべてブロックされます。これは、クラスタにとって安全な状態または推奨される状態ではありません。ただちに容量を追加するか、または解放する必要があります。

Critical

このエラーは、クラスタが100%消費されているときに発生します。クラスタは読み取り専用状態で、このクラスタへの新たなiSCSI接続を確立することはできません。この段階に達した場合は、容量をただちに解放するか、追加する必要があります。

クラスタ メタデータ ストレージ フルに関する警告には、MetadataClusterFullエラー コードが使用されます。OverviewReportingクラスタメタデータのストレージ容量が不足していることは、 Element UI のタブのページにある Cluster Capacity セクションで確認できます。

MetadataClusterFullの重大度レベルについて以下に説明します。

Warning

これは、クラスタの metatdata 容量がエラーの重大度レベルに近づいたときに表示される、お客様が設定可能な警告です。デフォルトでは、このレベルはエラーレベルで 3% に設定され、 Element API を使用して調整できます。できるだけ早く容量を追加するか、または解放する必要があります。

Error

クラスタがこの状態の場合、ノードが失われると、Double Helixデータ保護を再構築できるだけの容量がクラスタに残っていません。クラスタがこの状態にある間は、ボリュームの新規作成、クローンおよびSnapshotの処理はすべてブロックされます。これは、クラスタにとって安全な状態または推奨される状態ではありません。ただちに容量を追加するか、または解放する必要があります。

Critical

このエラーは、クラスタが100%消費されているときに発生します。クラスタは読み取り専用状態で、このクラスタへの新たなiSCSI接続を確立することはできません。この段階に達した場合は、容量をただちに解放するか、追加する必要があります。

注 : 2 ノードクラスタのしきい値には、次のものが適用されます。

- メタデータの空き容量エラーは、重大度の 20% を下回っています。
- ブロックの空き容量エラーは、 1 ブロックのドライブ（標準容量を含む）がクリティカルよりも低いことを意味します。つまり、 2 ブロックのドライブがクリティカルよりも低い容量であることを意味します。

ネットアップ サポートへの問い合わせ

ネットアップ製品に関するサポートのご依頼、ご意見やご要望については、ネットアップサポートまでお問い合わせください。

- Web：*mysupport.netapp.com*

製品マニュアルとその他の情報の参照先

NetApp HCIとSolidFireオールフラッシュ ストレージについてより詳しい使用および管理方法を知りたい場合は、それぞれの製品のドキュメント センターとリソース ページにある情報を参照してください。

ドキュメント センターでは、ハードウェアの設置とメンテナンスに関する情報、利用可能なその他のコンテンツ、既知の問題と解決済みの問題へのリンク、および最新のリリース ノートも参照できます。リソース ページには、データ シート、テクニカル レポート、ホワイトペーパー、およびビデオへのリンクが掲載されています。

- *NetApp HCI* のマニュアル
- *NetApp HCI*ドキュメント センター
- *NetApp HCI*のリソース ページ
- *SolidFire* および *Element 12.0* ドキュメンテーションセンター
- *SolidFire* および *Element 11.8* ドキュメンテーションセンター
- *SolidFire / Element 11.7*ドキュメント センター
- *SolidFire / Element 11.5*ドキュメント センター
- *SolidFire / Element 11.3*ドキュメント センター
- *SolidFire*のリソース ページ

著作権に関する情報

商標に関する情報

NetApp、NetAppのロゴ、ネットアップの商標一覧のページ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。

http://www.netapp.com/jp/legal/netapptmlist.aspx

マニュアルの更新について

弊社では、マニュアルの品質を向上していくため、皆様からのフィードバックをお寄せいただく専用のEメール アドレスを用意しています。また、GA/FCS版の製品マニュアルの初回リリース時や既存マニュアルへの重要な変更があった場合にご案内させていただくTwitterアカウントもあります。

本マニュアルの改善についてご提案がある場合は、次のアドレスまでコメントをEメールでお送りください。

ng-gpso-jp-documents@netapp.com

その際、担当部署で適切に対応させていただくため、製品名、バージョン、オペレーティング システム、弊社営業担当者または代理店の情報を必ず入れてください。

GA/FCS版の製品マニュアルの初回リリース時や既存マニュアルへの重要な変更があった場合のご案内を希望される場合は、Twitterアカウント@NetAppDocをフォローしてください。