Element ソフトウェアでストレージを管理

Element Software

NetApp
January 15, 2024

目次

Element ソフトウェアでストレージを管理

Element ソフトウェアを使用して、 SolidFire ストレージのセットアップ、クラスタの容量とパフォーマンスの監視、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の管理を行います。

Element は、 SolidFire クラスタの中核をなす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独立して動作します。 Element では、クラスタのノードをリソースに結合し、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することができます。Element ソフトウェアは、システム全体のすべてのクラスタの調整、拡張、管理を担います。

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。

- "Element ソフトウェアのユーザインターフェイスにアクセスします"
- "導入後に SolidFire システムのオプションを設定"
- "ストレージシステムコンポーネントをアップグレードする"
- "Element ソフトウェア UI の基本オプションを使用"
- "アカウントを管理"
- "システムを管理します"
- "ボリュームと仮想ボリュームを管理します"
- "データを保護"
- "システムのトラブルシューティングを行います"

詳細については、こちらをご覧ください

- "SolidFire および Element ソフトウェアのドキュメント"
- "vCenter Server 向け NetApp Element プラグイン"

Element ソフトウェアのユーザインターフェイスにアクセスします

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。

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。

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。

1. 次のいずれかを選択します。
    - IPv6 ： https://[IPv6 MVIP アドレスを入力してください。例：

```
https://[fd20:8b1e:b256:45a::1234]/
```

- IPv4 ： Enter https://[IPv4 MVIP address] 例：

```
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

詳細については、こちらをご覧ください

- "SolidFire および Element ソフトウェアのドキュメント"
- "vCenter Server 向け NetApp Element プラグイン"

導入後に SolidFire システムのオプションを設定

SolidFire システムのセットアップ後、いくつかのオプションのタスクを実行できます。

システムのクレデンシャルを変更する場合、必要に応じて他のコンポーネントへの影響を確認しておくことができます。

また、多要素認証、外部キー管理、および連邦情報処理標準（ FIPS ）セキュリティの設定も可能です。また、必要に応じてパスワードの更新についても確認してください。

詳細については、こちらをご覧ください

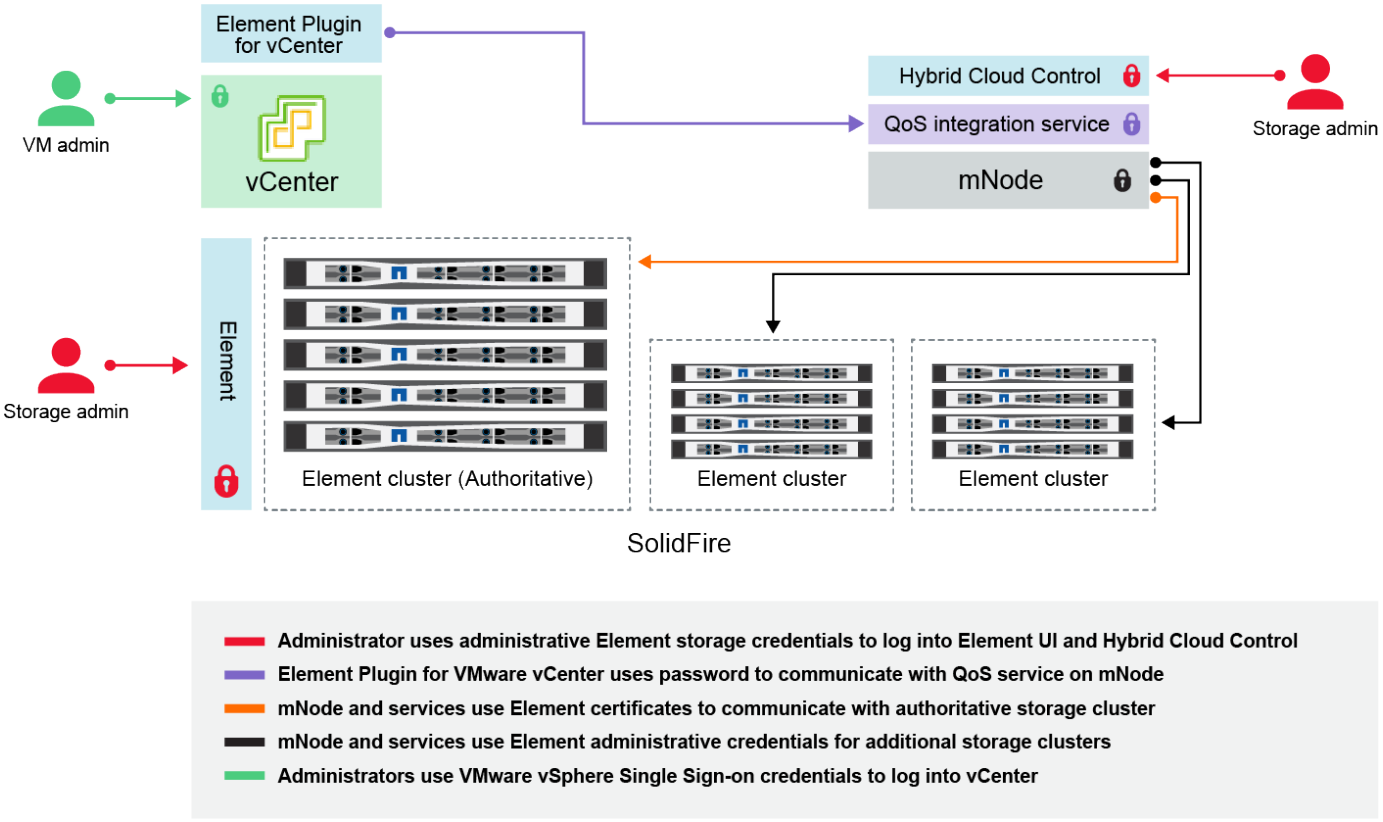
- "NetApp HCI と NetApp SolidFire でクレデンシャルを変更"
- "Element ソフトウェアのデフォルトの SSL 証明書を変更"
- "ノードの IPMI パスワードを変更します"
- "多要素認証を有効にします"
- "外部キー管理の開始"
- "FIPS ドライブをサポートするクラスタを作成します"

NetApp HCI と NetApp SolidFire でクレデンシャルを変更

NetApp HCI または NetApp SolidFire を導入している組織内のセキュリティポリシーに応じて、クレデンシャルやパスワードの変更はセキュリティの手法の一部として一般的に行われます。パスワードを変更する前に、導入環境内の他のソフトウェアコンポーネントへの影響を確認しておく必要があります。

NetApp HCI 環境または NetApp SolidFire 環境のいずれかのコンポーネントのクレデンシャルを変更する場合、次の表に示すガイダンスに従って他のコンポーネントに影響を与えます。

NetApp SolidFire コンポーネントの相互作用
：



資格情報の種類とアイコン	管理者による使用状況	これらの手順を参照してください
Element クレデンシャル 	• 環境 * ： NetApp HCI および SolidFire 管理者は、次の資格情報を使用してログインします。 • Element ストレージクラスタの Element ユーザインターフェイス • 管理ノードでの Hybrid Cloud Control （ mNode ） Hybrid Cloud Control で複数のストレージクラスタを管理している場合は、ストレージクラスタの管理クレデンシャルのみを受け入れます。このクレデンシャルは、「 _authoritative cluster_that the mnode was initially set for 」と呼ばれます。ストレージクラスタがあとで Hybrid Cloud Control に追加された場合、 mnode は管理者クレデンシャルを安全に保存します。以降に追加したストレージクラスタのクレデンシャルが変更された場合は、 mnode API を使用して mNode でクレデンシャルを更新する必要があります。	• "ストレージクラスタの管理者パスワードを更新する" • を使用して、 mNode のストレージクラスタ管理者のクレデンシャルを更新します 。 "modifyclusteradmin API"。

資格情報の種類とアイコン	管理者による使用状況	これらの手順を参照してください
vSphere Single Sign-On のクレデンシャル 	• 環境 * ： NetApp HCI のみ 管理者は、このクレデンシャルを使用して VMware vSphere Client にログインします。vCenter が NetApp HCI のインストールに含まれている場合、 NetApp Deployment Engine でクレデンシャルが次のように設定されます。 • 指定したパスワード、およびを使用する username@vsphere.loca • 指定したパスワードを持つ administrator@vsphere.loca既存の vCenter を使用して NetApp HCI を導入する場合、 vSphere のシングルサインオンクレデンシャルは IT VMware 管理者が管理します。	"vCenter および ESXi のクレデンシャルを更新します"。
ベースボード管理コントローラ（ BMC ）のクレデンシャル 	• 環境 * ： NetApp HCI のみ 管理者は、このクレデンシャルを使用して、 NetApp HCI 環境のネットアップコンピューティングノードの BMC にログインします。BMC は、基本的なハードウェア監視機能と仮想コンソール機能を備えています。 各ネットアップコンピューティングノードの BMC （ *ipmi* とも呼ばれる）クレデンシャルは、 NetApp HCI 環境の mNode に安全に保管されます。NetApp Hybrid Cloud Control は、サービスアカウント容量の BMC クレデンシャルを使用して、コンピューティングノードのファームウェアアップグレード中にコンピューティングノード内の BMC と通信します。 BMC のクレデンシャルが変更された場合、 mNode のすべての Hybrid Cloud Control 機能を維持するには、各コンピューティングノードのクレデンシャルも更新する必要があります。	• "NetApp HCI の各ノードに IPMI を設定します"。 • H410C 、 H610C 、および H615C ノードの場合、 "デフォルトの IPMI パスワードを変更します"。 • H410S および H610S ノードの場合、 "デフォルトの IPM パスワードを変更します"。 • "管理ノードで BMC クレデンシャルを変更します"。

資格情報の種類とアイコン	管理者による使用状況	これらの手順を参照してください
ESXi クレデンシャル 	• 環境 * ： NetApp HCI のみ 管理者は、 SSH またはローカル DCUI を使用して、ローカルの root アカウントで ESXi ホストにログインできます。NetApp HCI 環境では、ユーザ名は「 root 」で、パスワードは NetApp Deployment Engine でのコンピューティングノードの初回インストール時に指定されています。 ネットアップの各コンピューティングノードの ESXi ルートクレデンシャルが、 NetApp HCI 環境に mNode に安全に保存されている。NetApp Hybrid Cloud Control は、サービスアカウント容量のクレデンシャルを使用して、コンピューティングノードのファームウェアアップグレードや健全性チェックで ESXi ホストと直接通信します。 VMware 管理者が ESXi のルートクレデンシャルを変更した場合、各コンピューティングノードのクレデンシャルを mNode で更新し、ハイブリッドクラウド制御機能を維持する必要があります。	"vCenter および ESXi ホストのクレデンシャルを更新します "。
QoS 統合パスワード 	• 環境 * ： NetApp HCI および SolidFire ではオプション 管理者による対話型ログインには使用されません。 VMware vSphere と Element ソフトウェアの QoS 統合は、次の機能を通じて実現します。 • vCenter Server 向け Element プラグイン、および • mNode の QoS サービス。 認証の場合、 QoS サービスは、このコンテキストでのみ使用されるパスワードを使用します。QoS のパスワードは、 Element Plug-in for vCenter Server の初回インストール時に指定するか、NetApp HCI の導入時に自動生成されます。 他のコンポーネントには影響しません。	"NetApp Element Plug-in for vCenter で QoSSIOC クレデンシャルを更新します サーバ"。 NetApp Element Plug-in for vCenter ServerのSIOCパスワードは_QoSSIOCパスワードとも呼ばれます。 {url-peak} [Element Plug-in for vCenter Serverの技術情報アーティクル^]を確認します。

資格情報の種類とアイコン	管理者による使用状況	これらの手順を参照してください
vCenter Service Appliance のクレデンシャル 	• 環境 * ： NetApp HCI は、 NetApp Deployment Engine によってセットアップされている場合にのみ使用します 管理者は vCenter Server Appliance 仮想マシンにログインできます。NetApp HCI 環境では、ユーザ名は「 root 」で、パスワードは NetApp Deployment Engine でのコンピューティングノードの初回インストール時に指定されています。導入されている VMware vSphere のバージョンに応じて、 vSphere Single Sign-On ドメインの一部の管理者もアプライアンスにログインできます。 他のコンポーネントには影響しません。	変更は不要です。
NetApp 管理ノード管理者のクレデンシャル 	• 環境 * ： NetApp HCI および SolidFire ではオプション 管理者はネットアップ管理ノード仮想マシンにログインして、高度な設定やトラブルシューティングを行うことができます。導入した管理ノードのバージョンに応じて、 SSH によるログインはデフォルトでは有効になりません。 NetApp HCI 環境では、 NetApp Deployment Engine でのコンピューティングノードの初回インストール時に、ユーザによってユーザ名とパスワードが指定されています。 他のコンポーネントには影響しません。	変更は不要です。

詳細については、こちらをご覧ください

- "Element ソフトウェアのデフォルトの SSL 証明書を変更"
- "ノードの IPMI パスワードを変更します"
- "多要素認証を有効にします"
- "外部キー管理の開始"
- "FIPS ドライブをサポートするクラスタを作成します"

Element ソフトウェアのデフォルトの SSL 証明書を変更

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 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 を介したすべての 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、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取得し、変更を加えることがで

きます。

- * GetSSLCertificate*

  を使用できます "GetSSLCertificateメソッド" 現在インストールされているSSL証明書に関する情報（すべての証明書の詳細を含む）を取得します。

- * SetSSLCertificate*

  を使用できます "SetSSLCertificateメソッド" クラスタおよびノード単位のSSL証明書を、指定した証明書と秘密鍵に設定します。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 *

  。 "RemoveSSLCertificateメソッド" 現在インストールされているSSL証明書と秘密鍵を削除します。そのあと、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。

> 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キーの情報はすべてノードから削除されます。

詳細については、こちらをご覧ください

- "管理ノードのデフォルトSSL証明書を変更します"
- "Element SoftwareでのカスタムSSL証明書の設定に関する要件を教えてください。"
- "SolidFire および Element ソフトウェアのドキュメント"
- "vCenter Server 向け NetApp Element プラグイン"

ノードのデフォルトの **IPMI** パスワードを変更します

ノードへのリモート IPMI アクセスが可能になった時点で、デフォルトの Intelligent Platform Management Interface （ IPMI ）管理者パスワードを変更できます。この処理は、インストールの更新があった場合などに実行します。

ノードに対する IPM アクセスの設定の詳細については、を参照してください "各ノードに IPMI を設定します"。

これらのノードの IPM パスワードを変更できます。

- H410S ノード
- H610S ノード

H410S ノードのデフォルトの **IPMI** パスワードを変更します

IPMI ネットワークポートを設定したらすぐに、各ストレージノードで IPMI 管理者アカウントのデフォルトパスワードを変更する必要があります。

必要なもの

各ストレージノードに IPMI の IP アドレスを設定しておく必要があります。

手順

1. IPMI ネットワークにアクセス可能なコンピュータで Web ブラウザを開き、ノードの IPMI IP アドレスにアクセスします。
2. ログイン・プロンプトにユーザ名 ADMIN とパスワード ADMIN を入力します
3. ログインしたら、 * Configuration * タブをクリックします。
4. [* ユーザー *] をクリックします。
5. 「 Admin 」ユーザを選択し、「 * Modify User * 」をクリックします。
6. [パスワードの変更 *] チェックボックスをオンにします。
7. [パスワード *] フィールドと [パスワードの確認 *] フィールドに新しいパスワードを入力します。
8. [* 変更 *] をクリックし、 [OK] をクリックします。
9. デフォルトの IPMI パスワードを使用するすべての他の H410S ノードについて、この手順を繰り返します。

H610S ノードのデフォルトの IPMI パスワードを変更します

IPMI ネットワークポートを設定したらすぐに、各ストレージノードで IPMI 管理者アカウントのデフォルトパスワードを変更する必要があります。

必要なもの

各ストレージノードに IPMI の IP アドレスを設定しておく必要があります。

手順

1. IPMI ネットワークにアクセス可能なコンピュータで Web ブラウザを開き、ノードの IPMI IP アドレスにアクセスします。
2. ログインプロンプトにユーザ名「 root 」とパスワード「 calvin 」を入力します。
3. ログインしたら、ページ左上のメニューナビゲーションアイコンをクリックしてサイドバードロワーを開きます。
4. [* 設定 *] をクリックします。
5. [ユーザー管理] をクリックします。
6. リストから * Administrator * ユーザーを選択します。
7. [パスワードの変更 *] チェックボックスをオンにします。
8. [パスワード *] フィールドと [パスワードの確認 *] フィールドに、新しい強力なパスワードを入力します。
9. ページの下部にある「 * 保存」をクリックします。
10. デフォルトの IPMI パスワードを使用するすべての H610S ノードについて、この手順を繰り返します。

詳細については、こちらをご覧ください

- "SolidFire および Element ソフトウェアのドキュメント"
- "vCenter Server 向け NetApp Element プラグイン"

Element ソフトウェア UI の基本オプションを使用

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。

基本的なオプションには、 UI アクティビティによってアクティブ化された API コマンドの表示とフィードバックがあります。

- "API アクティビティを表示します"
- "Element インターフェイスのアイコン"
- "フィードバックを提供する"

を参照してください。

- "SolidFire および Element ソフトウェアのドキュメント"
- "vCenter Server 向け NetApp Element プラグイン"

API アクティビティを表示します

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された API 呼び出しを確認できます。

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。

各メソッドの詳細については、を参照してください "Element ソフトウェア API リファレンス"。

1. Element UI ナビゲーションバーで、 * API ログ * をクリックします。
2. API Log ウィンドウに表示される API アクティビティのタイプを変更するには、次の手順を実行します。
   a. API 要求トラフィックを表示するには、「 * Requests * 」を選択します。
   b. 「 * Responses * 」を選択して API 応答トラフィックを表示します。
   c. 次のいずれかを選択して、 API トラフィックのタイプをフィルタリングします。
      - * 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。

詳細については、こちらをご覧ください

- "Element API を使用してストレージを管理する"

- "SolidFire および Element ソフトウェアのドキュメント"
- "vCenter Server 向け NetApp Element プラグイン"

インターフェイス更新間隔にクラスタの負荷が影響します

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 要求が実行される頻度を制御することに注意してください。

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プロンプト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。

をクリックします。	説明
	アクション
	バックアップ先
	クローンまたはコピー
	削除またはパージ
	編集
	フィルタ
	ペアリング

	更新
	リストア
	からリストアします
	ロールバック
	スナップショット

フィードバックを提供する

Element ソフトウェアの Web ユーザインターフェイスの改善や UI の問題への対処には、 UI からアクセス可能なフィードバックフォームを使用できます。

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 フィールドと概要フィールドに関連情報を入力します。
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、このチェックボックスを選択します。
6. [Submit （送信）] をクリックします。

詳細については、こちらをご覧ください

- "SolidFire および Element ソフトウェアのドキュメント"
- "vCenter Server 向け NetApp Element プラグイン"

アカウントを管理

SolidFire ストレージシステムでは、テナントはアカウントを使用してクライアントがクラスタ上のボリュームに接続できるようにすることができます。ボリュームは、作成時に特定のアカウントに割り当てられます。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することもできます。

- "CHAPを使用してアカウントを操作します"
- "クラスタ管理者のユーザアカウントを管理します"

を参照してください。

- "SolidFire および Element ソフトウェアのドキュメント"
- "vCenter Server 向け NetApp Element プラグイン"

CHAPを使用してアカウントを操作します

SolidFire ストレージシステムでは、テナントはアカウントを使用してクライアントがクラスタ上のボリュームに接続できるようにすることができます。アカウントには、割り当てられているボリュームへのアクセスに必要なChallenge Handshake Authentication Protocol（CHAP；チャレンジハンドシェイク認証プロトコル）認証が含まれています。ボリュームは、作成時に特定のアカウントに割り当てられます。

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。

アカウントを作成します

アカウントを作成して、ボリュームへのアクセスを許可することができます。

システム内のアカウント名はそれぞれ一意である必要があります。

1. [* 管理 **>] > [** アカウント] を選択します。
2. ［ * アカウントの作成 * ］ をクリックします。
3. * ユーザー名 * を入力します。
4. [* CHAP 設定 * （ * CHAP Settings * ）] セクションで、次の情報を入力します。

   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。

   - * イニシエータシークレット * - CHAP ノードセッション認証用
   - * Target Secret * ： CHAP ノードセッション認証用
5. ［ * アカウントの作成 * ］ をクリックします。

アカウントの詳細を表示します

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。

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。これらの統計には、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が含まれます。

1. [* 管理 **>] > [** アカウント] を選択します。
2. アカウントの [アクション] アイコンをクリックします。
3. [* 詳細の表示 *] をクリックします。

以下に詳細を示します。

- * ステータス * ：アカウントのステータス。有効な値は次のとおり
  - 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なボリュームの数。
- * 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。
- * 重複排除機能 * ：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。
- * シンプロビジョニング * ：アカウントに割り当てられたボリュームのシンプロビジョニングによる削減率。
- * 全体的な削減率 * ：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。

アカウントを編集します

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 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、原因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 セッションを必ずログアウトし、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てください。

管理サービスに関連付けられた永続ボリュームは、インストールまたはアップグレード時に作成された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、関連付けられているアカウントを変更または削除しないでください。

1. [* 管理 **>] > [** アカウント] を選択します。
2. アカウントの [アクション] アイコンをクリックします。
3. 表示されたメニューで、「 * 編集 * 」を選択します。
4. * オプション： * ユーザー名 * を編集します。
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。

   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 接続が切断され、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ているボリュームは維持されますが、 iSCSI で検出できなくなります。

6. * オプション： * CHAP Settings * で、 * Initiator Secret * および * Target Secret * クレデンシャルを編集し、ノードセッション認証に使用します。

   CHAP 設定 * の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. [変更の保存 *] をクリックします。

アカウントを削除します

不要になったアカウントを削除できます。

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。

> 管理サービスに関連付けられた永続ボリュームは、インストールまたはアップグレード時に作成された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、関連付けられているアカウントを変更または削除しないでください。

1. [* 管理 **>] > [** アカウント] を選択します。
2. 削除するアカウントの [アクション] アイコンをクリックします。
3. 表示されたメニューで、 * 削除 * を選択します。
4. 操作を確定します。

詳細については、こちらをご覧ください

- "SolidFire および Element ソフトウェアのドキュメント"
- "vCenter Server 向け NetApp Element プラグイン"

クラスタ管理者のユーザアカウントを管理します

SolidFire ストレージシステムのクラスタ管理者アカウントの管理では、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、およびユーザのシステムアクセスを管理するための LDAP の設定を行います。

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、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の 2 種類の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。このアカウントは、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を変更できます。

- * 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。

> 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を表示

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。
   a. [**Users**>*Cluster Admins] をクリックします。
2. Users タブの Cluster Admins ページで、次の情報を表示できます。
   - * ID * ：クラスタ管理者アカウントに割り当てられたシーケンシャル番号。
   - * Username * ：クラスタ管理者アカウントの作成時に指定した名前。
   - * アクセス * ：ユーザアカウントに割り当てられたユーザ権限。有効な値は次のとおり
     - 読み取り
     - レポート作成
     - ノード
     - ドライブ
     - 個のボリューム
     - アカウント
     - clusterAdmin の権限が必要です
     - 管理者

     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。
   - * タイプ * ：クラスタ管理者のタイプ。有効な値は次のとおり
     - クラスタ
     - LDAP
   - * 属性 * ： 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。

     を参照してください "NetApp Element ソフトウェア API リファレンス"。

クラスタ管理者アカウントを作成

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。

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。

"Element ユーザインターフェイスで LDAP 認証を有効にします"

レポート作成、ノード、ドライブ、ボリューム、アカウント用のクラスタ管理者アカウントの権限をあとから変更することができます。 クラスタレベルのアクセスとアクセス許可を有効にすると、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。

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。
   a. [**Users**>*Cluster Admins] をクリックします。
   b. Create Cluster Admin をクリックします。
   c. ユーザタイプとして「 * Cluster * 」を選択します。
   d. 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。
   e. アカウントに適用するユーザ権限を選択します。
   f. チェックボックスをオンにして、エンドユーザライセンス契約に同意します。
   g. 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。
   a. [**Cluster**>*LDAP*] をクリックします。
   b. LDAP 認証が有効になっていることを確認します。
   c. [ユーザー認証のテスト] をクリックし、ユーザーまたはユーザーがメンバーになっているグループのいずれかに表示される識別名をコピーして、後で貼り付けることができます。
   d. [**Users**>*Cluster Admins] をクリックします。
   e. Create Cluster Admin をクリックします。
   f. LDAP ユーザタイプを選択します。
   g. [Distinguished Name] フィールドのテキストボックスの例に従って、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、前の手順で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 サーバ上で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。

   LDAP クラスタ管理者ユーザまたはグループを追加する場合、ユーザ名の一般的な形式は「 LDAP ： <Full Distinguished Name>` 」です。

   a. アカウントに適用するユーザ権限を選択します。
   b. チェックボックスをオンにして、エンドユーザライセンス契約に同意します。
   c. Create Cluster Admin をクリックします。

クラスタ管理者の権限を編集します

レポート作成、ノード、ドライブ、ボリューム、アカウント用のクラスタ管理者アカウントの権限を変更できます。 クラスタレベルのアクセスとアクセス許可を有効にすると、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。

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操作アイコンをクリックします。
3. [編集（ 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. [変更の保存 *] 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を変更します

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。

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操作アイコンをクリックします。
3. [編集（ 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. [変更の保存 *] をクリックします。

詳細については、こちらをご覧ください

- "Element ユーザインターフェイスで LDAP 認証を有効にします"
- "LDAP を無効にする"
- "SolidFire および Element ソフトウェアのドキュメント"
- "vCenter Server 向け NetApp Element プラグイン"

LDAP を管理します

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。

LDAP を管理するには、既存の Microsoft Active Directory 環境を使用して SolidFire クラスタへの LDAP 認証を設定し、設定をテストします。

IPv4 アドレスと IPv6 アドレスの両方を使用できます。

LDAP を有効にする手順の概要を次に示します。

1. * LDAP サポート * の設定前の手順を完了します。LDAP 認証の設定に必要な詳細情報がすべて揃っていることを確認します。
2. * LDAP 認証を有効にします * 。Element UI または Element API を使用します。
3. * LDAP 設定を確認します。 *必要に応じて、 GetLdapConfiguration API メソッドを実行するか、 Element UI を使用して LCAP 設定をチェックし、クラスタが正しい値で設定されていることを確認します。
4. * LDAP 認証をテストします * （「 readonly 」ユーザを使用）。TestLdapAuthentication API メソッドを実行するか、 Element UI を使用して、 LDAP 構成が正しいことをテストします。この最初のテストでは、「 readonly 」ユーザのユーザ名「 '`suse" 」を使用します。これにより、クラスタが LDAP 認証用に正しく設定されていることが検証され、「再認証」のクレデンシャルとアクセスが正しいことも検証されます。この手順が失敗した場合は、手順 1~3 を繰り返します。
5. * LDAP 認証をテストします * （追加するユーザアカウントを使用）。Element クラスタ管理者として追加するユーザアカウントに対して setp 4 を繰り返します。「識別されない DN 」または「ユーザ」（またはグループ）をコピーします。この DN はステップ 6 で使用されます。

6. * LDAP クラスタ管理者を追加します * （ LDAP 認証のテスト手順で DN をコピーして貼り付けます ）。Element UI または AddLdapClusterAdmin API メソッドを使用して、適切なアクセスレベルで新しいクラスタ管理者ユーザを作成します。ユーザ名には、手順 5 でコピーした完全な DN を貼り付けます。これにより、 DN が正しくフォーマットされます。
7. * クラスタ管理者アクセスをテストします。 *新しく作成した LDAP クラスタ管理者ユーザを使用してクラスタにログインします。LDAP グループを追加した場合は、そのグループの任意のユーザとしてログインできます。

LDAP サポートの設定前の手順を実行します

Element で LDAP サポートを有効にする前に、 Windows Active Directory Server をセットアップし、その他の設定前のタスクを実行する必要があります。

手順

1. Windows Active Directory サーバをセットアップする。
2. * オプション： * LDAPS サポートを有効にします。
3. ユーザとグループを作成
4. LDAP ディレクトリの検索に使用する読み取り専用のサービスアカウント（「 'fsreadonly' 」など）を作成します。

Element ユーザインターフェイスで LDAP 認証を有効にします

ストレージシステムと既存の LDAP サーバ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 の設定には、 Element ユーザインターフェイスまたは Element API を使用できます。この手順では、 Element UI を使用して LDAP を設定する方法について説明します。

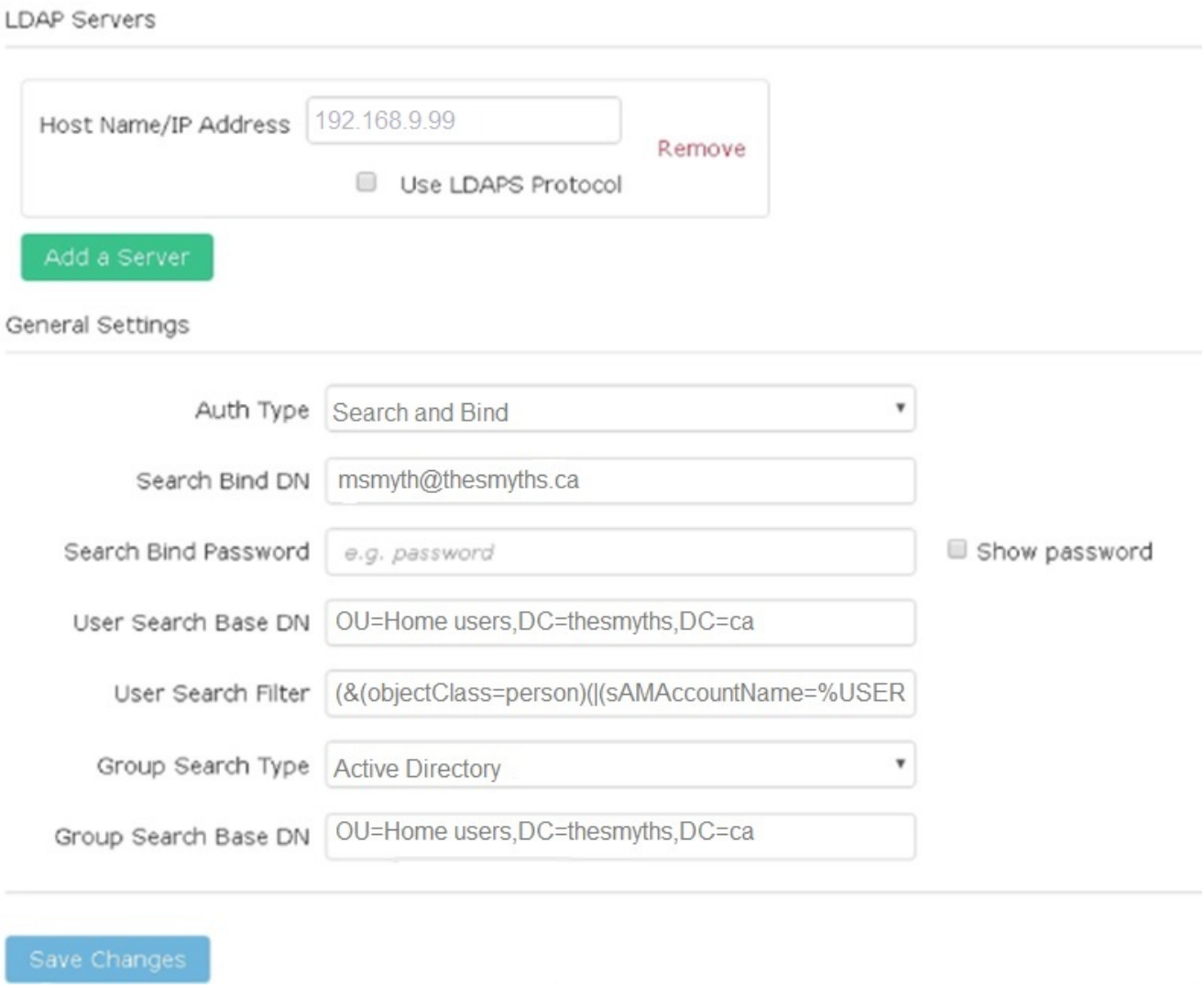
次に、 SolidFire で LDAP 認証を設定し、認証タイプとして「 S earchAndBind 」を使用する例を示します。この例では、 1 つの Windows Server 2012 R2 Active Directory サーバを使用します。

手順

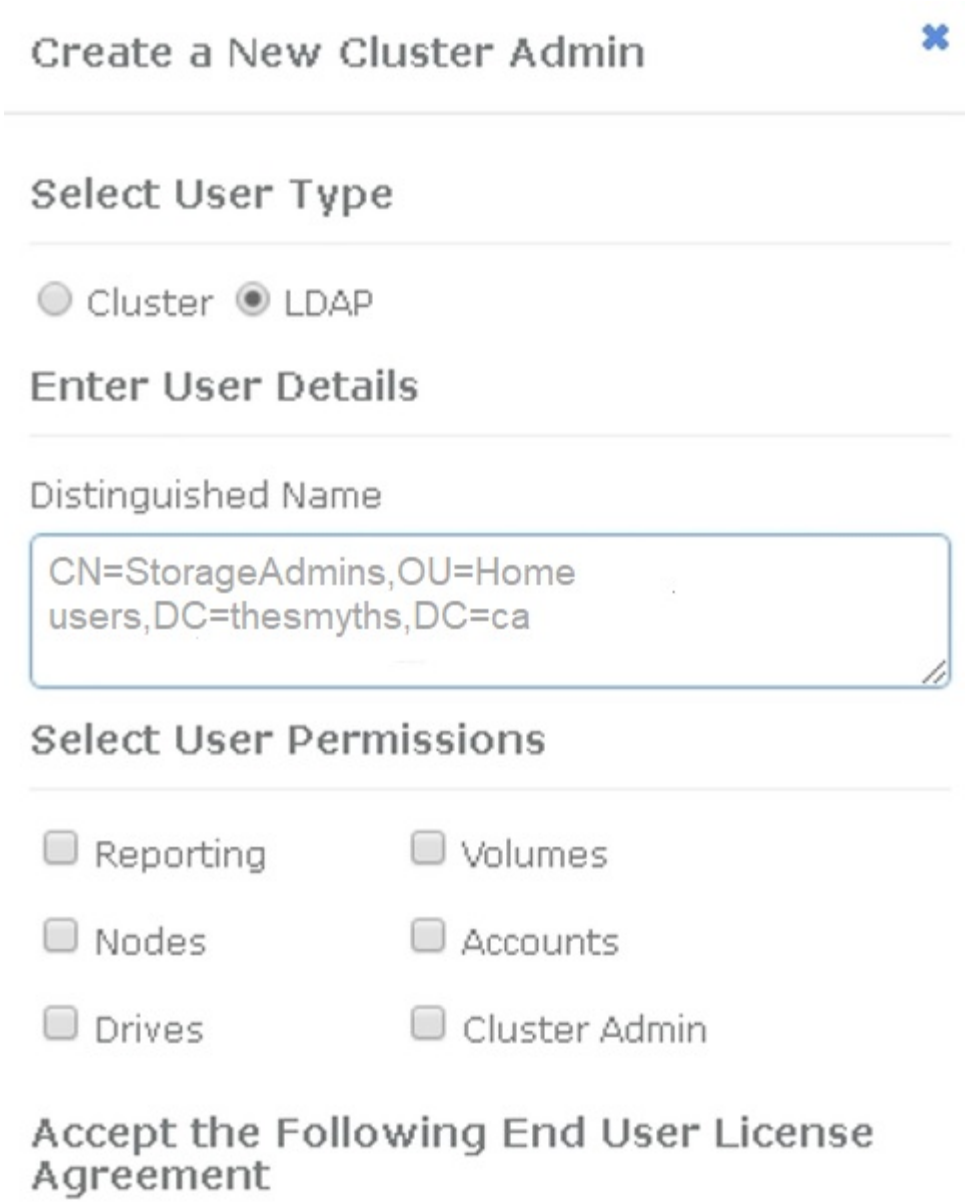
1. [**Cluster**>*LDAP*] をクリックします。
2. [* Yes* （はい）] をクリックして、 LDAP 認証を有効
3. [サーバーの追加] をクリックします。
4. ホスト名 /IP アドレス * を入力します。

   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、 <host name or IP address> ： <port number> と入力します
5. * オプション： * Use LDAPS Protocol * を選択します。
6. 「一般設定」に必要な情報を入力します。



7. [*LDAP を有効にする *] をクリックします
8. ユーザーのサーバーアクセスをテストする場合は、 [ユーザー認証のテスト] をクリックします。
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. [Save Changes] をクリックして、新しい設定を保存します。
11. 誰でもログインできるようにこのグループにユーザを作成するには、次の手順を実行します。
    a. [* ユーザー * （ * User * ）] > [* 表示（ * View ）]



b. 新しいユーザーの場合は、 [ユーザータイプ] の [*LDAP] をクリックし、 [識別名] フィールドにコピーしたグループを貼り付けます。
c. 権限を選択します。通常はすべての権限が選択されます。
d. エンドユーザライセンス契約までスクロールダウンし、 [* I accept （同意します）] をクリックします。
e. 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。

この問題をテストするには、 Element UI からログアウトし、そのグループにユーザとして再度ログインします。

Element API を使用して LDAP 認証を有効にします

ストレージシステムと既存の LDAP サーバ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 の設定には、 Element ユーザインターフェイスまたは Element API を使用できます。この手順では、 Element API を使用して LDAP を設定する方法について説明します。

SolidFire クラスタで LDAP 認証を利用するには、まず「 EnableLdapAuthentication 」 API メソッドを使用して、クラスタで LDAP 認証を有効にします。

手順

1. EnableLdapAuthentication API メソッドを使用して、クラスタで最初に LDAP 認証を有効にします。
2. 必要な情報を入力します。

```
{
     "method":"EnableLdapAuthentication",
     "params":{
          "authType": "SearchAndBind",
          "groupSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net",
          "groupSearchType": "ActiveDirectory",
          "searchBindDN": "SFReadOnly@prodtest.solidfire.net",
          "searchBindPassword": "ReadOnlyPW",
          "userSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net ",
          "userSearchFilter":
"(&(objectClass=person)(sAMAccountName=%USERNAME%))"
          "serverURIs": [
               "ldap://172.27.1.189",
          [
     },
  "id":"1"
}
```

3. 次のパラメータの値を変更します。

使用するパラメータ	説明
authType ： SearchAndBind	では、クラスタで readonly サービスアカウントを使用して、認証されているユーザが最初に検索され、見つかったユーザが認証済みの場合はバインドされるように指定しています。
groupSearchBaseDN ： dc=prodtest 、 dc=solidfire 、 dc=net	グループの検索を開始する LDAP ツリー内の場所を指定します。この例では、ツリーのルートを使用しています。LDAP ツリーのサイズが非常に大きい場合は、検索時間を短縮するために、これをより詳細なサブツリーに設定することを推奨します。

使用するパラメータ	説明
userSearchBaseDN ： dc=prodtest 、 dc=solidfire 、 dc=net	ユーザの検索を開始する LDAP ツリー内の場所を指定します。この例では、ツリーのルートを使用しています。LDAP ツリーのサイズが非常に大きい場合は、検索時間を短縮するために、これをより詳細なサブツリーに設定することを推奨します。
groupSearchType ： ActiveDirectory	Windows Active Directory サーバを LDAP サーバとして使用します。

`userSearchFilter: "(&(objectClass=person)(sAMAccountName=%USERNAME%))"`
 	
userPrincipalName （ログイン用の E メールアドレス）を使用するには、 userSearchFilter を次のように変更します。
 	
`"(&(objectClass=person)(userPrincipalName=%USERNAME%))"`
 	
または、 userPrincipalName と sAMAccountName の両方を検索するには、次の userSearchFilter を使用できます。
 	
`"(&(objectClass=person)(`
	（ sAMAccountName = %USERNAME% ）（ userPrincipalName = %USERNAME% ））」 -----

SolidFire クラスタにログインするには、 sAMAccountName をネットアップのユーザ名として使用します。これらの設定は 'sAMAccountName 属性でログイン中に指定されたユーザー名を検索するように LDAP に指示し ' さらに objectClass 属性の値として "person" を持つエントリにも検索を制限します	searchBindDN
LDAP ディレクトリの検索に使用される readonly ユーザの識別名を指定します。Active Directory の場合は、通常、ユーザに userPrincipalName （ E メールアドレス形式）を使用するのが最も簡単です。	searchBindPassword

この問題をテストするには、 Element UI からログアウトし、そのグループにユーザとして再度ログインします。

LDAP の詳細を表示します

クラスタタブの LDAP ページで LDAP 情報を表示します。

これらの LDAP 設定を表示するには、 LDAP を有効にする必要があります。

1. Element UI で LDAP の詳細を表示するには、 * Cluster * > * LDAP * をクリックします。
   - * Host Name/IP Address * ： LDAP または LDAPS ディレクトリサーバのアドレス。
   - * Auth Type * ：ユーザ認証方式。有効な値は次のとおり
     - Direct Bind の
     - 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の認証に使用するパスワード。
   - * 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。
   - * ユーザー検索フィルタ * ：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**: 使用されるデフォルトのグループ検索フィルタを制御する検索のタイプ。有効な値は次のとおり
     - Active Directory ：あるユーザの LDAP グループをすべてネストしたメンバーシップ。
     - グループなし：グループはサポートされません。
     - Member DN ：メンバー DN 形式のグループ（シングルレベル）。
   - * 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。
   - * ユーザー認証のテスト * ： LDAP を構成した後、 LDAP サーバーのユーザー名とパスワード認証をテストするために使用します。この問題をテストするためにすでに存在するアカウントを入力してください。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 設定をテストします

LDAP を設定したら、 Element UI または Element API の TestLdapAuthentication メソッドを使用して、 LDAP をテストする必要があります。

手順

1. Element UI で LDAP 設定をテストするには、次の手順を実行します。
   a. [**Cluster**>*LDAP*] をクリックします。
   b. [LDAP 認証のテスト *] をクリックします。
   c. 次の表に示す情報を使用して、問題を解決します。

エラーメッセージです	説明
`xLDAPUserNotFound`	• テスト対象のユーザが、設定された「 userSearchBaseDN 」サブツリーに見つかりませんでした。 • 「 userSearchFilter 」が正しく設定されていません。
`xLDAPBindFailed (Error: Invalid credentials)`	• テスト中のユーザ名は有効な LDAP ユーザですが、入力したパスワードは正しくありません。 • テスト中のユーザ名は有効な LDAP ユーザですが、アカウントが現在無効になっています。
`xLDAPSearchBindFailed (Error: Can't contact LDAP server)`	LDAP サーバの URI が正しくありません。
`xLDAPSearchBindFailed (Error: Invalid credentials)`	読み取り専用のユーザ名またはパスワードが正しく設定されていません。
`xLDAPSearchFailed (Error: No such object)`	「 userSearchBaseDN 」は、 LDAP ツリー内の有効な場所ではありません。
`xLDAPSearchFailed (Error: Referral)`	• 「 userSearchBaseDN 」は、 LDAP ツリー内の有効な場所ではありません。 • 「 userSearchBaseDN 」と「 groupSearchBaseDN 」は、ネストされた OU に含まれます。これにより、原因権限の問題が発生する可能性が回避策は ' ユーザーおよびグループのベース DN エントリに OU を含めます (例 : ou=storage’cn=company’cn=com')

2. Element API を使用して LDAP 設定をテストするには、次の手順を実行します。
   a. TestLdapAuthentication メソッドを呼び出します。

```
{
  "method":"TestLdapAuthentication",
     "params":{
        "username":"admin1",
        "password":"admin1PASS
      },
      "id": 1
}
```

b. 結果を確認します。API 呼び出しに成功した場合は、指定したユーザの識別名とユーザがメンバーとなっているグループのリストが結果に含まれます。

```
{
"id": 1
     "result": {
         "groups": [

"CN=StorageMgmt,OU=PTUsers,DC=prodtest,DC=solidfire,DC=net"
         ],
         "userDN": "CN=Admin1
Jones,OU=PTUsers,DC=prodtest,DC=solidfire,DC=net"
     }
}
```

LDAP を無効にする

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。

LDAP を無効にするとすべての設定が消去されるため、作業を開始する前にすべての設定を書き留めておく必要があります。

手順

1. [**Cluster**>*LDAP*] をクリックします。
2. [* いいえ *] をクリックします。
3. [*LDAP を無効にする *] をクリックします

詳細については、こちらをご覧ください

- "SolidFire および Element ソフトウェアのドキュメント"
- "vCenter Server 向け NetApp Element プラグイン"

システムを管理します

システムは Element UI で管理できます。これには、多要素認証の有効化、クラスタ設定の管理、連邦情報処理標準（ FIPS ）のサポート、外部キー管理などが含まれます。

- "多要素認証を有効にします"
- "クラスタの設定を行います"
- "FIPS ドライブをサポートするクラスタを作成します"
- "外部キー管理の開始"

を参照してください。

- "SolidFire および Element ソフトウェアのドキュメント"
- "vCenter Server 向け NetApp Element プラグイン"

多要素認証を有効にします

多要素認証（ MFA ）では、 Security Assertion Markup Language （ SAML ）を使用してサードパーティのアイデンティティプロバイダ（ IdP ）を使用してユーザセッションを管理します。MFA を使用することで、管理者は、パスワードとテキストメッセージ、パスワードと E メールメッセージなど、必要に応じて認証のその他の要素を設定できます。

多要素認証をセットアップします

以下の Element API による基本的な手順を使用して、マルチファクタ認証を使用するようにクラスタをセットアップできます。

各 API メソッドの詳細については、を参照してください "Element API リファレンス"。

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のアイデンティティプロバイダ（ 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、 https://freeformatter.com/json-escape.html です。

2. 次の API メソッド「 ListIdpConfigurations 」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 IdP にコピーします

   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のメタデータを取得するために使用する URL です。

3. 監査ログのユーザを一意に識別し、 Single Logout が適切に機能するように、サードパーティ IdP に SAML アサーションを設定して「 NameID 」属性を含めます。
4. 次の API メソッド「 AddIdpClusterAdmin 」を呼び出して、サードパーティ IdP によって認証された 1 つ以上のクラスタ管理者ユーザアカウントを作成します

次の例に示すように、 IdP クラスタ管理者のユーザ名が、目的の効果の SAML 属性の名前 / 値のマッピングと一致している必要があります。

- 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 が設定されている場合SAML 属性の名前と値のペアは、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、クラスタに対して MFA を有効にします。 'EnableIdpAuthentication'

詳細については、こちらをご覧ください

- "SolidFire および Element ソフトウェアのドキュメント"
- "vCenter Server 向け NetApp Element プラグイン"

多要素認証のための追加情報

多要素認証については、次の点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、 IdP 以外の管理者ユーザを使用して次の API メソッド「 UpdateIdpConfiguration 」を呼び出す必要があります
- MFA は、 2048 ビット未満の長さの証明書と互換性がありません。デフォルトでは、クラスタ上に 2 、 048 ビット SSL 証明書が作成されます。API メソッド「 SSL 証明書」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

アップグレード前に 2048 ビット未満の証明書をクラスタが使用している場合は、 Element 12.0 以降にアップグレードしたあとに、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 呼び出しを直接実行する（ SDK や Postman などで）ことも、他の統合機能（ OpenStack Cinder や vCenter Plug-in など）で使用することもできません。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 クラスタ管理者ユーザまたはローカルクラスタ管理者ユーザを追加します。

詳細については、こちらをご覧ください

- "Element API を使用してストレージを管理する"
- "SolidFire および Element ソフトウェアのドキュメント"
- "vCenter Server 向け NetApp Element プラグイン"

クラスタの設定を行います

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したり、クラスタ固有のタスクを実行したりできます。

設定できる項目は、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 、 および NTP ブロードキャストクライアント。

オプション（ **Options** ）

- 仮想ボリュームを操作します
- Element クラスタと ONTAP クラスタの間で SnapMirror レプリケーションを使用
- クラスタフルしきい値を設定します
- サポートアクセスを有効または無効にします
- "Element のブロックスペースしきい値の計算方法"
- クラスタの暗号化を有効または無効にします
- 利用条件のバナーを管理します
- クラスタが照会するネットワークタイムプロトコルサーバを設定します
- SNMP を管理します
- ドライブを管理します
- ノードを管理
- 仮想ネットワークを管理する
- Fibre Channel ポートの詳細を表示します

詳細については、こちらをご覧ください

- "SolidFire および Element ソフトウェアのドキュメント"
- "vCenter Server 向け NetApp Element プラグイン"

クラスタの保存データの暗号化を有効または無効にします

SolidFire クラスタでは、クラスタドライブに格納されているすべての保存データを暗号化できます。どちらかを使用して、クラスタ全体の自己暗号化ドライブ（ SED ）の保護を有効にすることができます "保存データのハードウェアまたはソフトウェアベースの暗号化"。

Element UI または API を使用して、保存データのハードウェア暗号化を有効にすることができます。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効率には影響しません。Element API でのみ、保存データのソフトウェア暗号化を有効にすることができます。

保存データのハードウェアベースの暗号化は、クラスタの作成時にデフォルトでは有効になりません。また、Element UI から有効または無効にすることができます。

> SolidFire オールフラッシュストレージクラスタの場合、クラスタ作成時に保存データのソフトウェア暗号化を有効にし、クラスタ作成後に無効にすることはできません。

必要なもの

- 暗号化の設定を有効にしたり変更したりするためのクラスタ管理者権限が必要です。
- 保存データのハードウェアベースの暗号化では、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ておきます。
- 暗号化を無効にする場合は、ドライブの暗号化を無効にするために、 2 つのノードがクラスタに参加して

いる必要があります。

保存データの暗号化のステータスを確認します

クラスタの保存データの暗号化とソフトウェア暗号化の現在のステータスを確認するには、を使用します "GetClusterInfo を使用します" メソッドを使用できます "GetSoftwareEncryptionAtRestInfo" クラスタが保存データの暗号化に使用する情報を取得する方法。

https://<MVIP>/` の Element ソフトウェア UI ダッシュボードには ' 現在 ' ハードウェア・ベースの暗号化の保存中の暗号化ステータスのみが表示されています

オプション（ **Options** ）

- [保存データのハードウェアベースの暗号化を有効にします]
- [保存データのソフトウェアベースの暗号化を有効にします]
- [保存データのハードウェアベースの暗号化を無効にします]

保存データのハードウェアベースの暗号化を有効にします

外部キー管理設定を使用して保存データの暗号化を有効にするには、を使用して保存データの暗号化を有効にする必要があります "API"。既存の Element UI ボタンを使用してを有効にすると、内部で生成されたキーの使用に戻ります。

1. Element UI で、 * Cluster * > * Settings * を選択します。
2. [保存データの暗号化を有効にする] を選択します。

保存データのソフトウェアベースの暗号化を有効にします

保存データのソフトウェア暗号化は、クラスタで有効にしたあとは無効にできません。

1. クラスタの作成時に、を実行します "クラスタメソッドを作成します" enableSoftwareEncryptionAtRest を「 true 」に設定します。

保存データのハードウェアベースの暗号化を無効にします

1. Element UI で、 * Cluster * > * Settings * を選択します。
2. [保存データの暗号化を無効にする] を選択します。

詳細については、こちらをご覧ください

- "SolidFire および Element ソフトウェアのドキュメント"
- "以前のバージョンの NetApp SolidFire 製品および Element 製品に関するドキュメント"

クラスタフルしきい値を設定します

ブロッククラスタフルの警告を生成するレベルを次の手順で変更できます。さらに、ModifyClusterFullThreshold API メソッドを使用すると、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。

必要なもの

クラスタ管理者の権限が必要です。

手順

1. [* クラスタ **>] > [** 設定] をクリックします。
2. Cluster Full Settings セクションで、 Helix がノード障害からリカバリできないために _% の容量が残っている場合に警告アラートを生成 * にパーセント値を入力します。
3. [変更の保存 *] をクリックします。

詳細については、こちらをご覧ください

"Element のブロックスペースしきい値の計算方法"

サポートアクセスを有効または無効にします

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。

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。

1. [* クラスタ **>] > [** 設定] をクリックします。
2. [サポートアクセスの有効化 / 無効化] セクションで、サポートにアクセスを許可する期間（時間単位）を入力します。
3. [サポートアクセスを有効にする *] 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、 * サポートアクセスを無効にする * をクリックします。

利用条件のバナーを管理します

ユーザ向けのメッセージを含むバナーを有効にしたり、編集したり、設定したりできます。

オプション（ **Options** ）

[利用条件のバナーを有効にします] [利用条件のバナーを編集します] [利用条件のバナーを無効にします]

利用条件のバナーを有効にします

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。

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。

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

最大文字数は 4096 文字です。

3. [**Enable**] をクリックします。

利用条件のバナーを編集します

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。

必要なもの

- 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] をクリックします。
2. [* 利用規約 *] ダイアログボックスで、表示するテキストを編集します。

最大文字数は 4096 文字です。

3. [変更の保存 *] をクリックします。

利用条件のバナーを無効にします

利用条件のバナーを無効にすることができます。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。

必要なもの

- 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] をクリックします。
2. [**Disable**] をクリックします。

ネットワークタイムプロトコルを設定します

ネットワークタイムプロトコル（ NTP ）の設定は、次の 2 つの方法のいずれかで行うことができます。クラスタ内の各ノードがブロードキャストをリスンするように指定するか、各ノードで NTP サーバに更新を照会するように指示します。

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されます。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。

クラスタが照会するネットワークタイムプロトコルサーバを設定します

クラスタ内の各ノードで Network Time Protocol （ NTP ；ネットワークタイムプロトコル）サーバに更新を照会するように設定できます。クラスタは、設定済みのサーバのみと通信し、そのサーバから NTP 情報を要求します。

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。IP アドレスまたは FQDN ホスト名を使用できます。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常に確立できるとはかぎりません。

FQDN の使用方法は、個々のストレージノードの DNS 設定が正常に機能しているかどうかによって異なります。そのためには、すべてのストレージノードで DNS サーバを設定し、 [Network Port Requirements] ページでポートが開いていることを確認します。

NTP サーバは 5 つまで入力できます。

IPv4 アドレスと IPv6 アドレスの両方を使用できます。

必要なもの

この設定を行うには、クラスタ管理者の権限が必要です。

手順

1. サーバ設定で IP または FQDN のリストを設定します。
2. ノードで DNS が正しく設定されていることを確認します。
3. [* クラスタ **>] > [** 設定] をクリックします。
4. [ネットワークタイムプロトコルの設定] で、標準 NTP 設定を使用する **No** を選択します。
5. [変更の保存 *] をクリックします。

詳細については、こちらをご覧ください

- "SolidFire および Element ソフトウェアのドキュメント"
- "vCenter Server 向け NetApp Element プラグイン"

NTP ブロードキャストをリスンするようにクラスタを設定する

ブロードキャストモードを使用すると、クラスタ内の各ノードが特定のサーバからの Network Time Protocol （ NTP ；ネットワークタイムプロトコル）ブロードキャストメッセージをネットワーク上でリスンするように設定できます。

必要なもの

- この設定を行うには、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。

手順

1. [* クラスタ **>] > [** 設定] をクリックします。
2. ブロードキャストモードを使用している NTP サーバをサーバリストに入力します。
3. [ネットワークタイムプロトコルの設定] で、 [はい] を選択してブロードキャストクライアントを使用します。
4. ブロードキャストクライアントを設定するには、 [**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。

5. [変更の保存 *] をクリックします。

詳細については、こちらをご覧ください

- "SolidFire および Element ソフトウェアのドキュメント"
- "vCenter Server 向け NetApp Element プラグイン"

SNMP を管理します

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。また、管理情報ベースファイルを表示してアクセスすることもできます。

IPv4 アドレスと IPv6 アドレスの両方を使用できます。

SNMP の詳細

クラスタタブの SNMP ページでは、次の情報を表示できます。

- * SNMP MIB*

  表示またはダウンロード可能な MIB ファイル。

- * 一般的な SNMP 設定 *

  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 トラップ設定 *

  キャプチャ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 リクエスタを設定します

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。

1. [Menu] (メニュー) 、 [Cluster] [SNMP] の順にクリックします
2. [**General SNMP Settings**](一般的な SNMP 設定) で、 [**Yes**](はい) をクリックして SNMP を有効
3. [* バージョン] リストから、 [* バージョン 2*] を選択します。
4. 「 * Requeeors * 」セクションに「 * Community String * 」および「 * Network * 」情報を入力します。

   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できます。

5. * オプション： * 別のリクエスタを追加するには、 * リクエスト者の追加 * をクリックし、 * コミュニティストリング * および * ネットワーク * 情報を入力します。
6. [変更の保存 *] をクリックします。

詳細については、こちらをご覧ください

- SNMP トラップを設定する
- 管理情報ベースファイルを使用して管理対象オブジェクトデータを表示します

SNMP USM ユーザを設定します

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。

1. [**Cluster**>*SNMP*] をクリックします。
2. [**General SNMP Settings**](一般的な SNMP 設定) で、 [**Yes**](はい) をクリックして SNMP を有効
3. [* バージョン] リストから、 [* バージョン 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、 * USM ユーザの追加 * をクリックし、名前、パスワード、およびパスフレーズを入力します。
6. [変更の保存 *] をクリックします。

SNMP トラップを設定する

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

SNMP トラップが有効になっている場合、 SolidFire クラスタは、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を生成します。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。

1. [**Cluster**>*SNMP*] をクリックします。
2. システムが生成する必要がある 1 つまたは複数のタイプのトラップを [* SNMP トラップ設定 * （ SNMP Trap Settings ）] セクションで選択します。
   - クラスタ障害トラップ
   - クラスタ解決済み障害トラップ
   - クラスタイベントトラップ
3. [* Trap Recipients] セクションで、受信者のホスト、ポート、およびコミュニティストリング情報を入力します。
4. * オプション * ：別のトラップ受信者を追加するには、 * トラップ受信者の追加 * をクリックして、ホスト、ポート、およびコミュニティストリング情報を入力します。
5. [変更の保存 *] をクリックします。

管理情報ベースファイルを使用して管理対象オブジェクトデータを表示します

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。

MIB には、以下のシステムアクティビティの統計データが含まれています。

- 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情報
- ノード統計
- レポート、エラー、システムイベントなどのその他のデータ

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*] をクリックします。
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。

ドライブを管理します

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。

を参照してください。

- "SolidFire および Element ソフトウェアのドキュメント"
- "vCenter Server 向け NetApp Element プラグイン"

ドライブの詳細

クラスタタブのドライブページには、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。ページをフィルタするには、 Active 、 Available 、 Removing 、 Erasing 、 Failed の各タブを選択します。

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。未割り当てのドライブをクラスタに追加して、新しい SolidFire クラスタの作成後に Available タブに表示できます。

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。

- * ドライブ ID *

  ドライブに割り当てられている連番。

- * ノード 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。

- * ノード名 *

  ドライブが格納されているノードの名前。

- * スロット *

  ドライブが物理的に配置されているスロットの番号。

- * 容量 *

  ドライブのサイズ（ GB 単位）。

- * シリアル *

  ドライブのシリアル番号。

- * 摩耗度残量 *

  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、摩耗度残量は 95% と報告されます。ドライブの摩耗度情報は自動的には更新されません。情報を更新するには、ページを更新するか、またはページを閉じてリロードします。

- * タイプ *

  ドライブのタイプ。block または metadata のいずれかです。

ノードを管理

SolidFire ストレージノードと Fibre Channel ノードは、クラスタタブのノードページで管理できます。

新しく追加したノードがクラスタの合計容量の 50% を超えると、容量のルールに準拠するためにこのノードの一部の容量が使用できなくなります（「未使用」）。これは、ストレージが追加されるまで有効です。容量のルールにも違反するような大規模なノードを追加すると、それまでに孤立していたノードは孤立しなくなり、新たに追加したノードが孤立する状態になります。この問題を回避するには、容量を常にペアで追加する必要があります。ノードが孤立すると、該当するクラスタエラーがスローされます。

詳細については、こちらをご覧ください

クラスタにノードを追加します

クラスタにノードを追加します

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ます。

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 NetApp 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張するには、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。

> 新しく追加したノードがクラスタの合計容量の 50% を超えると、容量のルールに準拠するためにこのノードの一部の容量が使用できなくなります（「未使用」）。これは、ストレージが追加されるまで有効です。容量のルールにも違反するような大規模なノードを追加すると、それまでに孤立していたノードは孤立しなくなり、新たに追加したノードが孤立する状態になります。この問題を回避するには、容量を常に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 クラスタエラーがスローされます。

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

NetApp HCI アプライアンスにノードを追加できます。

手順

1. [* Cluster*>* Nodes] を選択します。
2. 保留中のノードのリストを表示するには、 * Pending * をクリックします。

   ノードを追加するプロセスが完了すると、それらのノードが[Active nodes]リストに表示されます。それまでは、保留中のノードが [保留中のアクティブ] リストに表示されます。

   クラスタに追加するPending状態のノードには、ElementソフトウェアバージョンのクラスタがインストールされますSolidFire 。この処理には数分かかることがあります。

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、 * Bulk Actions * を実行します。* 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. [追加（ Add ）] をクリックします。

   ノードがアクティブノードのリストに表示されます。

詳細については、こちらをご覧ください

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。あるメジャーコンポーネント番号のノードを、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追加さ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 は 11.1 と互換性がなく、 11.1 は 11.2 と互換性がありません。

- * 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。

互換性を確保するためには、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しているマイクロバージョンの番号は一致しなくても互換性があります。

1 つのクラスタ内に異なるタイプのノードを混在させることができます。SF シリーズ 2405 、 3010 、 4805 、 6010 、 9605 、 9010 、 19210 、 38410 、および H シリーズはクラスタ内で共存できます。

H シリーズは、 H610S-1 、 H610S-2 、 H610S-4 、および H410S ノードで構成されています。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、どのノードも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。

Element 12.0 以降では、次の SF シリーズのストレージノードはサポートされません。

- SF3010
- SF6010
- SF9010

これらのストレージノードのいずれかを Element 12.0 にアップグレードすると、このノードが Element 12.0 でサポートされていないことを示すエラーが表示されます。

ノードの詳細を表示します

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。クラスタタブのノードページには、各ノードのソフトウェアバージョンを表示できるバージョン列があります。

手順

1. [* クラスタ > ノード *] をクリックします。
2. 特定のノードの詳細を表示するには、ノードの * Actions * アイコンをクリックします。
3. [* 詳細の表示 *] をクリックします。
4. ノードの詳細を確認します。
   - * Node ID * ：システムによって生成されたノードの ID 。
   - * Node Name * ：ノードのホスト名。
   - * 使用可能な 4k IOPS * ：ノードに設定されている IOPS 。
   - * Node Role * ：クラスタ内でのノードのロール。有効な値は次のとおり
     - 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 * ： 1GbE または 10GbE ネットワークの管理タスク用にノードに割り当てられた管理 IP （ MIP ）アドレス。
   - * 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。
   - * 管理 VLAN ID * ：管理ローカルエリアネットワークの仮想 ID 。
   - * ストレージ 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。
   - * レプリケーションポート * ：リモートレプリケーションにノードで使用されるポート。
   - * Service Tag * ：ノードに割り当てられた一意のサービスタグ番号。

Fibre Channel ポートの詳細を表示します

FC ポートのページでは、ステータス、名前、ポートアドレスなど、 Fibre Channel ポートの詳細を確認できます。

クラスタに接続されている Fibre Channel ポートに関する情報を表示します。

手順

1. [**Cluster**>*FC Ports] をクリックします。
2. このページの情報をフィルタリングするには、 * フィルタ * をクリックします。
3. 詳細を確認します。
    - * 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 * ：ファイバチャネルポートが配置されているスロット番号。
    - *HBA ポート *: ファイバチャネルホストバスアダプタ (HBA) の物理ポート。
    - *wwnn * ：ワールドワイドノード名。
    - * wwpn * ：ターゲットの World Wide Port Name 。
    - * Switch WWN* ：ファイバ・チャネル・スイッチの World Wide Name 。
    - * Port State * ：ポートの現在の状態。
    - **nPort ID** ：ファイバチャネル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ファイバチャネル速度。有効な値は次のとおりです。
        - 4Gbps
        - 8Gbps です
        - 16Gbps です

詳細については、こちらをご覧ください

- "SolidFire および Element ソフトウェアのドキュメント"
- "vCenter Server 向け NetApp Element プラグイン"

仮想ネットワークを管理する

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。

詳細については、こちらをご覧ください

- 仮想ネットワークを追加
- 仮想ルーティング / 転送を有効にします
- 仮想ネットワークを編集します
- VRF VLAN を編集します
- 仮想ネットワークを削除します

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。

必要なもの

- 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。
- すべての NetApp Element 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。

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。

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*] をクリックします。
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 名 *
   - * VLAN タグ *
   - * SVIP *
   - * ネットマスク *
   - （任意） * 概要 *
4. IP アドレス範囲の開始 IP * アドレスを * IP アドレスブロック * で入力します。
5. IP 範囲の * Size * を、ブロックに含める IP アドレスの数として入力します。
6. [ブロックの追加（ Add a Block ）] をクリックして、この VLAN の非連続的な 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。

仮想ネットワークの詳細を表示します

手順

1. [**Cluster**>*Network*] をクリックします。

2. 詳細を確認します。
    - **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 。
    - * 名前 * ： 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。
    - * ネットマスク * ：この仮想ネットワークのネットマスク。
    - * ゲートウェイ * ：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 有効 *: 仮想ルーティングおよび転送が有効かどうかを示します。
    - *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。

仮想ルーティング / 転送を有効にします

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、同時に使用することができます。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。

VRF を有効にできるのは、 VLAN の作成時だけです。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。

1. [**Cluster**>*Network*] をクリックします。
2. 新しい VLAN で VRF を有効にするには、 * VLAN の作成 * を選択します。
    a. 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。
    b. [Enable VRF*] チェックボックスをオンにします。
    c. * 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。

詳細については、こちらをご覧ください

仮想ネットワークを追加

仮想ネットワークを編集します

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。

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。

VLAN の IP アドレス範囲のサイズを管理する際には、次の制限事項に注意してください。

- IP アドレスを削除できるのは、 VLAN の作成時に割り当てられた最初の IP アドレス範囲のみです。
- 初期 IP アドレス範囲のあとに追加された IP アドレスブロックは削除できますが、 IP アドレスを削除し

て IP ブロックのサイズを変更することはできません。

- クラスタ内のノードで使用されている初期 IP アドレス範囲または IP ブロックから IP アドレスを削除しようとすると、処理に失敗することがあります。
- 使用中の特定の IP アドレスをクラスタ内の他のノードに再割り当てすることはできません。

IP アドレスブロックは、次の手順を使用して追加できます。

1. [**Cluster**>*Network*] を選択します。
2. 編集する VLAN の [Actions] アイコンを選択します。
3. 「 * 編集 * 」を選択します。
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. 仮想ネットワークの非連続的な IP アドレスブロックを追加するには、 [ブロックの追加] を選択します。
6. 「変更を保存」を選択します。

トラブルシューティングの技術情報アーティクルへのリンク

VLAN IP アドレス範囲の管理に関する問題のトラブルシューティングについては、ナレッジベースの記事へのリンクを参照してください。

- "Element クラスタの VLAN にストレージノードを追加したあとに IP に関する警告が重複して発生しています"
- "使用中の VLAN IP と Element で IP が割り当てられているノードを確認する方法"

VRF VLAN を編集します

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。

1. [**Cluster**>*Network*] をクリックします。
2. 編集する VLAN の [Actions] アイコンをクリックします。
3. [編集（ Edit ）] をクリックします。
4. Edit VLAN * ダイアログボックスに VRF VLAN の新しい属性を入力します。
5. [変更の保存 *] をクリックします。

仮想ネットワークを削除します

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。

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

詳細については、こちらをご覧ください

仮想ネットワークを編集します

FIPS ドライブをサポートするクラスタを作成します

多くのお客様の環境にソリューションを導入する場合、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解決策に欠かせない要素です。

- "FIPS ドライブのノードを混在させないようにします"
- "保存データの暗号化を有効にします"
- "ノードが FIPS ドライブ機能に対応しているかどうかを確認します"
- "FIPS ドライブ機能を有効にします"
- "FIPS ドライブのステータスを確認します"
- "FIPS ドライブ機能のトラブルシューティングを行います"

FIPS ドライブのノードを混在させないようにします

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。

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みなされます。

- 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を有効にします

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。

1. NetApp Element ソフトウェア UI で、 * クラスタ * > * 設定 * をクリックします。
2. [保存データの暗号化を有効にする] をクリックします。 *

詳細については、こちらをご覧ください

- クラスタの暗号化を有効または無効にします
- "SolidFire および Element ソフトウェアのドキュメント"

- "vCenter Server 向け NetApp Element プラグイン"

ノードが **FIPS** ドライブ機能に対応しているかどうかを確認します

NetApp Element ソフトウェアの GetFipsReport API メソッドを使用して、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必要があります。

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 ドライブであるか、ドライブが存在しません。

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 を使用して、「 GetHardwareList 」と入力します
   - 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。

     の「 GetFipsReport 」または「 ListDriveHardware 」の詳細を参照してください "Element API リファレンス"。
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。

詳細については、こちらをご覧ください

- "SolidFire および Element ソフトウェアのドキュメント"
- "vCenter Server 向け NetApp Element プラグイン"

FIPS ドライブ機能を有効にします

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。

GetFipsReport にすべてのノードの準備完了ステータスが表示された場合に示すように、クラスタで保存データの暗号化を有効にし、すべてのノードとドライブを FIPS に対応している必要があります。

ステップ

1. 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'

詳細については、こちらをご覧ください

- "Element API を使用してストレージを管理します"
- "SolidFire および Element ソフトウェアのドキュメント"
- "vCenter Server 向け NetApp Element プラグイン"

FIPS ドライブのステータスを確認します

クラスタで FIPS ドライブ機能が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。このメソッドで、 FIPS ドライブの有効ステータスが true であるか false であるかを確認できます。

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 ドライブの有効な値が 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"
   }
   ```

詳細については、こちらをご覧ください

- "Element API を使用してストレージを管理します"
- "SolidFire および Element ソフトウェアのドキュメント"
- "vCenter Server 向け NetApp Element プラグイン"

FIPS ドライブ機能のトラブルシューティングを行います

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

1. Element UI を使用して、 * Reporting * > * Alerts * を選択します。
2. 次のクラスタ障害を探します。
   - FIPS ドライブが一致しません
   - FIPS ドライブが準拠していません
3. 推奨される解決方法については、クラスタ障害コードの情報を参照してください。

詳細については、こちらをご覧ください

- クラスタ障害コード
- "Element API を使用してストレージを管理します"
- "SolidFire および Element ソフトウェアのドキュメント"
- "vCenter Server 向け NetApp Element プラグイン"

クラスタで **HTTPS** の **FIPS 140-2** を有効にしてください

EnableFeature API メソッドを使用すると、 HTTPS 通信の FIPS 140-2 動作モードを有効にできます。

NetApp Element ソフトウェアを使用すると、クラスタで Federal Information Processing Standard （ 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。

> 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。そのため、クラスタでは管理接続とストレージ接続の両方が中断されます。このモードは、提供する暗号化メカニズムが必要な環境でのみ、慎重に計画し、有効にしてください。

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。

詳細については、こちらをご覧ください

- SSL 暗号
- "Element API を使用してストレージを管理します"
- "SolidFire および Element ソフトウェアのドキュメント"
- "vCenter Server 向け NetApp Element プラグイン"

SSL 暗号

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。

以下に、 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 モードが有効な場合にサポートされる SSL 暗号を示します。

- * FIPS 140-2 が無効になりました *

  TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 （ dh 2048 ） -A

  TLS_DHE_RSA_With _AES_128_CMG_SHA256 （ dh 2048 ） - A

  TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 （ dh 2048 ） -A

  TLS_DHE_RSA_With _AES_256_GCM_SH384 （ dh 2048 ） - A

  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 （ secp256r1 ） A

  TLS_ECDHE_RSA_With _AES_128_CMG_SHA256 （ secp256r1 ） A

  TLS_ECDHE_RSA_WITH_AES_256_CBC_SH384 （ secp256r1 ） - A

  TLS_ECDHE_RSA_With _AES_256_GCM_SH384 （ 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

  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_SED_CBC_SHA （ RSA 2048 ） -A

- * FIPS 140-2 が有効になりました

  TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 （ dh 2048 ） -A

  TLS_DHE_RSA_With _AES_128_CMG_SHA256 （ dh 2048 ） - A

  TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 （ dh 2048 ） -A

  TLS_DHE_RSA_With _AES_256_GCM_SH384 （ dh 2048 ） - A

  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 （ sectr571r1 ） A

  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 （ secp256r1 ） A

  TLS_ECDHE_RSA_With _AES_128_CMG_SHA256 （ secp256r1 ） A

  TLS_ECDHE_RSA_With _AES_128_GG_SHA256 （ sectr571r1 ） A

  TLS_ECDHE_RSA_WITH_AES_256_CBC_SH384 （ sectr571r1 ） -A

  TLS_ECDHE_RSA_WITH_AES_256_CBC_SH384 （ secp256r1 ） - A

  TLS_ECDHE_RSA_With _AES_256_GCM_SH384 （ secp256r1 ） - A

  TLS_ECDHE_RSA_with _AES_256_GCM_SH384 （ sectr571r1 ） 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

詳細については、こちらをご覧ください

クラスタで HTTPS の FIPS 140-2 を有効にしてください

外部キー管理の開始

外部キー管理（ EKM ）は、クラスタ外の外部キーサーバ（ EKS ）と連携して、安全な認証キー（ AK ）管理を実現します。AK は、自己暗号化ドライブ（ SED ）のロックとロック解除に使用されます "保存データの暗号化" クラスタでを有効にしておきます。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。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。

- "外部管理をセットアップする"
- "保存マスターキーでのソフトウェア暗号化のキーを変更します"
- "アクセス不可または無効な認証キーをリカバリします"
- "外部キー管理 API コマンド"

詳細については、こちらをご覧ください

- "CreateCluster API ：保存データのソフトウェア暗号化を有効にすることができます"
- "SolidFire および Element ソフトウェアのドキュメント"
- "以前のバージョンの NetApp SolidFire 製品および Element 製品に関するドキュメント"

外部キー管理をセットアップする

以下の手順に従い、リストされている Element API メソッドを使用して外部キー管理機能を設定できます。

必要なもの

- 外部キー管理と保存データの暗号化を組み合わせて設定する場合は、を使用して保存データのソフトウェア暗号化を有効にしておきます "クラスタを作成" ボリュームを含まない新しいクラスタ上のメソッド。

手順

1. 外部キーサーバ（ EKS ）との信頼関係を確立します。
   a. 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"
   b. 認証局が署名する必要がある証明書署名要求（ 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"
   c. 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、サードパーティ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。
   a. 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"
   b. 次の API メソッドを呼び出して、署名済み証明書と認証局の公開鍵証明書を提供するキーサーバを作成します。 "CreateKeyServerKmip のように指定します" "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。
   c. 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 のように指定します" "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の次の手順として、次のいずれかを実行します。

   a. （保存中のハードウェア暗号化の場合）有効にします "保存データのハードウェア暗号化" キーの格納に使用するキーサーバを含むキープロバイダの ID を指定するには、を呼び出します "EnableEncryptionAtRest" API メソッド。

      保存データの暗号化はを使用して有効にする必要があります "API"。既存の Element UI ボタンを使用して保存データの暗号化を有効にすると、原因機能で内部で生成されたキーの使用に戻ります。

   b. （ソフトウェアによる保存データの暗号化）を実行します "ソフトウェアによる保存データの暗号化" 新しく作成したキープロバイダを使用するには、キープロバイダ ID をに渡します "RekeySoftwareEncryptionAtRestMasterKey" API メソッド。

詳細については、こちらをご覧ください

- "クラスタの暗号化を有効または無効にします"
- "SolidFire および Element ソフトウェアのドキュメント"
- "以前のバージョンの NetApp SolidFire 製品および Element 製品に関するドキュメント"

保存マスターキーでのソフトウェア暗号化のキーを変更します

Element API を使用して既存のキーを変更できます。このプロセスにより、外部キー管理サーバ用の新しい交換用マスターキーが作成されます。マスターキーは常に新しいマスターキーに置き換えられ、複製や上書きは行われません。

次のいずれかの手順で、キーの変更が必要になることがあります。

- 内部キー管理から外部キー管理への変更の一環として、新しいキーを作成します。
- セキュリティ関連イベントに対する応答または保護として、新しいキーを作成します。

このプロセスは非同期で、キー変更処理が完了する前に応答を返します。を使用できます "GetAsyncResult" システムをポーリングして、プロセスがいつ完了したかを確認する方法。

必要なもの

- を使用して保存データのソフトウェア暗号化を有効にしておきます "クラスタを作成" ボリュームを含まず、 I/O を含まない新しいクラスタ上のメソッド使用 "9510c8e68784d05acbae2e947dde3cd8" 続行する前に状態が「有効」であることを確認します。
- これで完了です "信頼関係を確立しました" SolidFire クラスタと外部キーサーバ（ EKS ）の間の接続に使用します。を実行します "TestKeyProviderKmip" キープロバイダへの接続が確立されていることを確認する方法。

手順

1. を実行します "ListKeyProvidersKmip" キープロバイダ ID (keyProviderID') をコピーします
2. を実行します "RekeySoftwareEncryptionAtRestMasterKey" 'keyManagementType' パラメータを 'external' および 'keyProviderID' として ' 前の手順で作成したキープロバイダの ID 番号を指定します

```
{
 "method": "rekeysoftwareencryptionatrestmasterkey",
 "params": {
   "keyManagementType": "external",
   "keyProviderID": "<ID number>"
 }
}
```

3. 「 RekeySoftwareEncryptionAtRestMasterKey 」コマンド応答から「 asyncHandle 」値をコピーします。
4. を実行します "GetAsyncResult" 前の手順の「 asyncHandle 」値を使用してコマンドを実行し、設定の変更を確認します。コマンド応答から、古いマスターキー設定が新しいキー情報で更新されたことがわかります。新しいキープロバイダ ID をコピーして以降の手順で使用します。

```
{
   "id": null,
   "result": {
     "createTime": "2021-01-01T22:29:18Z",
     "lastUpdateTime": "2021-01-01T22:45:51Z",
     "result": {
       "keyToDecommission": {
         "keyID": "<value>",
         "keyManagementType": "internal"
     },
     "newKey": {
       "keyID": "<value>",
       "keyManagementType": "external",
       "keyProviderID": <value>
     },
     "operation": "Rekeying Master Key. Master Key management being
transferred from Internal Key Management to External Key Management with
keyProviderID=<value>",
     "state": "Ready"
   },
   "resultType": "RekeySoftwareEncryptionAtRestMasterKey",
   "status": "complete"
}
```

5. 「 GetSoftwareEncryptionatRestInfo 」コマンドを実行して、「 keyProviderID 」などの新しいキーの詳細が更新されたことを確認します。

```
{
   "id": null,
   "result": {
     "masterKeyInfo": {
       "keyCreatedTime": "2021-01-01T22:29:18Z",
       "keyID": "<updated value>",
       "keyManagementType": "external",
       "keyProviderID": <value>
     },
     "rekeyMasterKeyAsyncResultID": <value>
     "status": "enabled",
     "version": 1
   },
}
```

詳細については、こちらをご覧ください

- "Element API を使用してストレージを管理します"
- "SolidFire および Element ソフトウェアのドキュメント"
- "以前のバージョンの NetApp SolidFire 製品および Element 製品に関するドキュメント"

アクセス不可または無効な認証キーをリカバリします

場合によっては、ユーザの介入を必要とする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。

「 **KmipServerFault** 」クラスタエラーが原因で、クラスタがドライブのロックを解除できません。

これは、クラスタの初回ブート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）。

メタデータドライブが障害としてマークされ、「 **Available** 」状態になっているため、 **sliceServiceUnhealthy** エラーが表示される場合があります。

クリアする手順：

1. ドライブを再度追加します。
2. 3 ～ 4 分後に 'lseServiceUnhealthy の障害がクリアされていることを確認します

を参照してください "クラスタ障害コード" を参照してください。

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具体的な詳細を定義するために使用されます。

- CreateKeyServerKmip のように指定します
- ModifyKeyServerKmip のように指定します
- 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 のように指定します
- RemoveKeyServerFromProviderKmip
- GetKeyProviderKmip
- ListKeyProvidersKmip
- RekeySoftwareEncryptionAtRestMasterKey
- TestKeyProviderKmip

API メソッドの詳細については、を参照してください "API リファレンス情報"。

ボリュームと仮想ボリュームを管理します

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 の管理タブで管理できます。使用可能なクラスタ管理機能には、データボリューム、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。

- "ボリュームを操作します"
- "仮想ボリュームを操作します"
- "ボリュームアクセスグループとイニシエータを使用する"

を参照してください。

- "SolidFire および Element ソフトウェアのドキュメント"

- "vCenter Server 向け NetApp Element プラグイン"

ボリュームを操作します

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 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。管理タブのボリュームページでは、ノード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。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。

詳細については、こちらをご覧ください

- "QoS ポリシーを管理する"
- "ボリュームを作成します"
- "個々のボリュームのパフォーマンスの詳細を表示します"
- "アクティブボリュームを編集します"
- "ボリュームを削除します"
- "削除したボリュームをリストアします"
- "ボリュームをパージする"
- "ボリュームのクローンを作成します"
- "Fibre Channel ボリュームに LUN を割り当てます"
- "ボリュームに QoS ポリシーを適用する"
- "ボリュームの QoS ポリシーの関連付けを削除します"

QoS ポリシーを管理する

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。QoS ポリシーは、 Management タブの QoS Policies ページで作成、編集、および削除できます。

> 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、ボリュームの QoS 設定に対して QoS ポリシーの値を上書きして調整します。

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

を参照してください "パフォーマンスと QoS"。

- QoS ポリシーを作成する
- QoS ポリシーを編集する
- QoS ポリシーを削除する

QoS ポリシーを作成する

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。

1. [* Management] > [* QoS Policies] を選択します。
2. [Create QoS Policy] をクリックします。
3. 「 * ポリシー名 * 」を入力します。
4. 最小 IOPS ** 、最大 IOPS * 、バースト IOPS * の値を入力します。
5. [Create QoS Policy] をクリックします。

QoS ポリシーを編集する

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。

1. [* Management] > [* QoS Policies] を選択します。
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、必要に応じて次のプロパティを変更します。
   - ポリシー名
   - 最小 IOPS
   - 最大 IOPS
   - バースト IOPS
5. [変更の保存 *] をクリックします。

QoS ポリシーを削除する

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。

ボリュームと QoS ポリシーの関連付けを解除する代わりに、そのボリュームの QoS 設定をカスタムに変更できます。

1. [* Management] > [* QoS Policies] を選択します。
2. 削除する QoS ポリシーのアクションアイコンをクリックします。
3. 表示されたメニューで、 * 削除 * を選択します。
4. 操作を確定します。

詳細については、こちらをご覧ください

- "ボリュームの QoS ポリシーの関連付けを削除します"
- "SolidFire および Element ソフトウェアのドキュメント"
- "vCenter Server 向け NetApp Element プラグイン"

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 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。

管理タブのボリュームページでは、ノード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。

ボリュームを作成します

ボリュームを作成して、指定した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。

作成中に、ボリュームの QoS 設定を指定できます。

1. [* Management] > [* Volumes] を選択します。
2. [ボリュームの作成] をクリックします。
3. [新しいボリュームの作成 *] ダイアログボックスで、 * 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。

   デフォルトで選択されている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 バイトです
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、ボリュームにアクセスでき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、 [アカウントの作成] リンクをクリックし、新しいアカウント名を入力して、 [* 作成] 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。

   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. サービス品質 * を設定するには、次のいずれかを実行します。
   a. 「 * Policy 」で、既存の QoS ポリシーがある場合は選択できます。
   b. カスタム設定 * で、 IOPS の最小値、最大値、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. [ボリュームの作成] をクリックします。

ボリュームの詳細を表示します

1. [* Management] > [* Volumes] を選択します。
2. 詳細を確認します。
   - **ID** ：システムによって生成されたボリュームの ID 。
   - * 名前 * ：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。
   - * アクセスグループ * ：ボリュームが属するボリュームアクセスグループの名前。
   - * アクセス * ：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
     - Read/Write ：すべての読み取りと書き込みが許可されます。
     - Read Only ：すべての読み取りアクティビティが許可されます。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割合。
   - * サイズ * ：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 * ：ユーザ定義の 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 * ：ボリュームで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
     - はい。
     - いいえ
   - * Created On * ：ボリュームが作成された日時。

個々のボリュームの詳細を表示します

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。

1. * Reporting * > * Volume Performance * を選択します。
2. ボリュームリストで、ボリュームの操作アイコンをクリックします。
3. [* 詳細の表示 *] 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. ボリュームの詳細情報を表示するには、 * 詳細を表示 * 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を編集します

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。

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。
- ボリュームをクローニングしています。
- ボリュームの再同期中。

手順

1. [* Management] > [* Volumes] を選択します。
2. [* アクティブ *] 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. [編集（ 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。
   - 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場合は、最初に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のサイズ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。

     デフォルトで選択されている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 バイトです
5. * オプション： * 次のいずれかのアカウントアクセスレベルを選択します。
   - 読み取り専用です
   - 読み取り / 書き込み
   - ロック済み
   - レプリケーションターゲット
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。

   アカウントが存在しない場合は、 [アカウントの作成] リンクをクリックし、新しいアカウント名を入力して、 [* 作成] 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。

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： * サービス品質 * での選択を変更するには、次のいずれかを実行します。
   a. 「 * Policy 」で、既存の QoS ポリシーがある場合は選択できます。
   b. カスタム設定 * で、 IOPS の最小値、最大値、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。

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 ポリシーの所属を削除できます。カスタム QoS は、ボリュームの QoS 設定に対して QoS ポリシーの値を上書きして調整します。

IOPS の値は、 10 または 100 単位で増減する必要があります。入力値には有効な整数を指定する必要があります。

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. [変更の保存 *] をクリックします。

ボリュームを削除します

Element 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。

削除されたボリュームはすぐにパージされるわけではなく、約 8 時間は使用可能な状態のままです。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、関連付けられている 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。

管理サービスに関連付けられた永続ボリュームが作成され、インストールまたはアップグレード時に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、ボリュームや関連付けられてい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] を選択します。
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。
   a. 削除するボリュームの操作アイコンをクリックします。
   b. 表示されたメニューで、 * 削除 * をクリックします。
   c. 操作を確定します。

   ボリュームは、 [* Volumes （ボリューム）] ページの [* Deleted （削除済み）] 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。

a. 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。
b. [一括操作 *] をクリックします。
c. 表示されたメニューで、 * 削除 * をクリックします。
d. 操作を確定します。

ボリュームが * Volumes （ボリューム） * ページの * Deleted （削除済み） * 領域に移動します。

削除したボリュームをリストアします

システムでは、削除したボリュームのうち、パージされていないボリュームをリストアできます。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。

1. [* Management] > [* Volumes] を選択します。
2. 削除されたボリュームのリストを表示するには、 * Deleted * タブをクリックします。
3. リストアするボリュームの操作アイコンをクリックします。
4. 表示されたメニューで、 * リストア * 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。

ボリュームをパージする

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。

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できます。

1. [* Management] > [* Volumes] を選択します。
2. [削除済み（ * 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
単一のボリュームをパージする	a. パージ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。 b. [Purge] をクリックします。 c. 操作を確定します。
複数のボリュームをパージする	a. パージするボリュームを選択します。 b. [一括操作 *] をクリックします。 c. 表示されたメニューで、「 * パージ * 」を選択します。 d. 操作を確定します。

ボリュームのクローンを作成します

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。

クラスタでは、ボリュームあたり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、あとで処理されます。

オペレーティングシステムによって、クローニングされた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 Snapshot ボリュームとして扱います。新しいデータストアの作成に使用できるデバイスがボリュームになります。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、 VMware のドキュメントを参照してください "VMFS データストアのコピーをマウントしています" および "重複する VMFS データストアの管理"。

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] を選択します。
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。
   a. アクティブ * 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アクションアイコンをクリックします。
   b. 表示されたメニューで、 * Clone * をクリックします。
   c. Clone Volume * （ * クローンボリューム）ウィンドウで、新規にクローンされたボリュームのボリューム名を入力します。
   d. 体積サイズ * スピンボックスとリストを使用して、体積のサイズと測定値を選択します。

      デフォルトで選択されている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 バイトです

   e. 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。
   f. 新しいクローンボリュームに関連付けるアカウントを * Account * リストから選択します。

      この手順の実行中にアカウントを作成するには、 [アカウントの作成] リンクをクリックし、アカウント名を入力して、 [* 作成] をクリックします。アカウントを作成すると、自動的にアカウントが **Account** 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。
   a. アクティブ * ページのボリュームリストで、クローニングするボリュームの横のボックスをオンにします。

b. [一括操作 *] をクリックします。

c. 表示されたメニューで、 * Clone * を選択します。

d. [* Clone Multiple Volumes] ダイアログ・ボックスで '[* New Volume Name Prefix*] フィールドにクローン・ボリュームのプレフィックスを入力します

e. クローンボリュームに関連付けるアカウントを * Account * リストから選択します。

f. 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. [クローニングの開始] をクリックします。

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。

を参照してください。

- "SolidFire および Element ソフトウェアのドキュメント"
- "vCenter Server 向け NetApp Element プラグイン"

Fibre Channel ボリュームに **LUN** を割り当てます

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ときに、 Fibre Channel ボリュームに LUN を割り当てることもできます。

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。

1. [* 管理 **>] > [** アクセスグループ *] を選択します。

2. 編集するアクセスグループの [アクション] 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 * （ボリューム・アクセス・グループの編集）ダイアログ・ボックスの * Assign LUN ID* （ LUN ID の割り当て * ）で、 * LUN Assignments * （ LUN の割り当て * ）リストの矢印をクリックします。

5. LUN を割り当てるボリュームのリストで、対応する * LUN * フィールドに新しい値を入力します。

6. [変更の保存 *] をクリックします。

ボリュームに **QoS** ポリシーを適用する

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。

一括して適用する QoS ポリシーを用意しておく必要があります。

1. [* Management] > [* Volumes] を選択します。

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. [一括操作 *] をクリックします。
4. 表示されたメニューで、 * QoS ポリシーの適用 * 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. [適用（ Apply ）] をクリックします。

詳細については、こちらをご覧ください

QoS ポリシー

ボリュームの **QoS** ポリシーの関連付けを削除します

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

変更するボリュームに QoS ポリシーを関連付ける必要があります。

1. [* Management] > [* Volumes] を選択します。
2. 変更する QoS ポリシーが含まれているボリュームの操作アイコンをクリックします。
3. [編集（ Edit ）] をクリックします。
4. 表示されるメニューの [* Quality of Service* （サービス品質 * ）] で、 [* Custom Settings （カスタム設定 ）] をクリックします。
5. Min IOPS * 、 * Max IOPS * 、 * Burst IOPS * を変更するか、またはデフォルトの設定をそのまま使用します。
6. [変更の保存 *] をクリックします。

詳細については、こちらをご覧ください

QoS ポリシーを削除する

仮想ボリュームを操作します

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 を使用して vSphere VVol 機能を手動で有効にするタスクを 1 回だけ実行する必要があります。

VVol 機能を有効にすると、ユーザインターフェイスに VVol 関連の監視オプションと一部の管理オプションを使用できる VVol タブが表示されます。また、 VASA Provider と呼ばれるストレージ側のソフトウェアコンポーネントは、 vSphere 向けのストレージ認識サービスとして機能します。VVOL の作成、クローニング、編集などのほとんどの vVol コマンドは、 vCenter Server または ESXi ホストで開始され、 VASA Provider から Element ソフトウェアストレージシステムの 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仮想ボリューム機能を使用するために必要な構成の大部分は、vSphere で作成されます。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行うには、 VMware vSphere Virtual Volumes for SolidFire ストレージ構成ガイドを参照してください。

1 つの vCenter インスタンスに複数の NetApp Element VASA Provider を登録しないでください。2 つ目の NetApp Element VASA Provider が追加されている場合、その結果、すべての VVOL データストアにアクセスできなくなります。

VASA Provider を vCenter に登録済みの場合は、複数の vCenter に対する 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。をインストールするには、から VASA39 .tar.gz ファイルをダウンロードします "ネットアップのソフトウェアダウンロード" サイトに移動し、マニフェストの指示に従います。NetApp Element VASA プロバイダはネットアップの証明書を使用します。このパッチでは、 vCenter が証明書を変更せずに使用して、 VASA および VVOL に使用する複数の vCenter をサポートします。証明書は変更しないでください。カスタム SSL 証明書は VASA でサポートされません。

詳細については、こちらをご覧ください

- 仮想ボリュームを有効にします
- 仮想ボリュームの詳細を表示します
- 仮想ボリュームを削除します
- ストレージコンテナを作成します
- ストレージコンテナを編集します
- ストレージコンテナを削除します
- プロトコルエンドポイント
- バインド
- ホストの詳細

仮想ボリュームを有効にします

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。

必要なもの

- 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。

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. [* クラスタ *] > [* 設定 *] を選択します。
2. Virtual Volumes 用のクラスタ固有の設定を探します。
3. 仮想ボリュームを有効にする * をクリックします。
4. [はい] をクリックして、仮想ボリュームの構成変更を確認します。

   Element UI に * VVols * タブが表示されます。

   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. VASA Provider の URL を * クラスタ * > * 設定 * の仮想ボリューム（ vVol ）設定からコピーします。この URL は、 VASA Provider を vCenter に登録する際に使用します。
6. VVol * > * Storage Containers * でストレージコンテナを作成します。

   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. 「 * VVOL* > * Protocol Endpoints * 」を選択します。
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。

   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行うには、 VMware vSphere Virtual Volumes for SolidFire ストレージ構成ガイドを参照してください。

詳細については、こちらをご覧ください

"『 VMware vSphere Virtual Volumes for SolidFire Storage Configuration Guide 』を参照してください"

仮想ボリュームの詳細を表示します

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。入力、出力、スループット、レイテンシなど、各仮想ボリュームのパフォーマンスアクティビティを表示することもできます。 キュー深度とボリューム情報。

必要なもの

- クラスタの Element UI で VVol 機能を有効にしておく必要があります。
- 関連付けられた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く必要があります。
- vSphere で少なくとも 1 つの VM を作成しておく必要があります。

手順

1. 「 * VVOLs * > * Virtual Volumes 」をクリックします。

   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、「 * 詳細を表示 * 」を選択します。

詳細

VVol タブの Virtual Volumes ページには、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、クラスタ上の各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。

- * 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 を表していない場合、値は 0 です。
- * 親仮想ボリューム 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、親へのリンクはありません。
- * Virtual Volume ID * ：仮想ボリュームの UUID 。
- * 名前 * ：仮想ボリュームに割り当てられた名前。
- * ストレージコンテナ * ：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。
- * 仮想ボリュームタイプ * ：仮想ボリュームのタイプ。構成、データ、メモリ、スワップ、またはその他。
- * Access * ：仮想ボリュームに割り当てられた読み取り / 書き込み権限。
- * サイズ * ：仮想ボリュームのサイズ（ GB または GiB 単位）。
- * Snapshots * ：関連付けられている Snapshot の数。番号をクリックすると、 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。最大バースト 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。
- * 作成時間 * ：仮想ボリュームの作成タスクが完了した時間。

個々の仮想ボリュームの詳細

vVol タブの仮想ボリュームページでは、個々の仮想ボリュームを選択してその詳細を表示すると、次の仮想ボリューム情報が表示されます。

- * 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。

- * 親仮想ボリューム 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、親へのリンクはありません。
- * Virtual Volume ID * ：仮想ボリュームの UUID 。
- * 仮想ボリュームタイプ * ：仮想ボリュームのタイプ。構成、データ、メモリ、スワップ、またはその他。
- * 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た読み取り / 書き込み権限。
- * Account Name * ：ボリュームを含むアカウントの名前。
- * アクセスグループ * ：関連付けられているボリュームアクセスグループ。
- * 合計ボリュームサイズ * ：プロビジョニング済み容量の合計（バイト）。
- * ゼロ以外のブロック * ：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。
- * ゼロブロック * ：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。番号をクリックすると、 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。最大バースト 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、値は常に yes です。
- * ボリュームがペアリングされている * ：ボリュームがペアリングされているかどうかを示します。
- * 作成時間 * ：仮想ボリュームの作成タスクが完了した時間。
- * Blocks Size * ：ボリューム上のブロックのサイズ。
- * アラインされていない書き込み * ： 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。アラインされ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
- * アラインされていない読み取り * ： 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
- * SCSI EUI Device ID * ： EUI-64 ベースの 16 バイト形式で、ボリュームに割り当てられたグローバル一意の SCSI デバイス ID 。
- **scsiNAADeviceID**: NAA IEEE Registered Extended フォーマットでのボリュームのグローバル一意 SCSI デバイス識別子。
- * Attributes * ： JSON オブジェクト形式の名前と値のペアのリスト。

仮想ボリュームを削除します

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。

1. 「 * VVOLs * > * Virtual Volumes * 」を選択します。
2. 削除する仮想ボリュームの操作アイコンをクリックします。
3. 表示されたメニューで、 * 削除 * を選択します。

> 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 * を選択して、パージが正常に完了したことを確認します。

ストレージコンテナを管理する

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。

ストレージコンテナが作成され、 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。

クラスタあたり最大 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を作成します

Element UI でストレージコンテナを作成して、 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。

作業を開始する前に、クラスタの Element UI で VVol 機能を有効にします。

手順

1. 「 * VVOLs * > * Storage Containers * 」を選択します。
2. Create Storage Containers * ボタンをクリックします。
3. Create a New Storage Container * （新しいストレージコンテナの作成）ダイアログボックスで、ストレージコンテナ情報を入力します。
   a. ストレージコンテナの名前を入力します。
   b. CHAP 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。

      > シークレットを自動的に生成する場合は、 CHAP 設定のフィールドを空白のままにします。

   c. Create Storage Container （ストレージコンテナの作成）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「ストレージコンテナ * 」サブタブのリストに表示されていることを確認します。

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を表示します

VVol タブのストレージコンテナページでは、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表示できます。

- *アカウント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。
- * 名前 * ：ストレージコンテナの名前。
- * ステータス * ：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
  - 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を表示します

個々のストレージコンテナのストレージコンテナ情報を表示するには、 vVol タブのストレージコンテナページでその情報を選択します。

- * アカウント 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 。
- * 名前 * ：ストレージコンテナの名前。
- * ステータス * ：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
  - 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を編集します

Element UI でストレージコンテナの CHAP 認証を変更できます。

1. 「 * VVOLs * > * Storage Containers * 」を選択します。
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、「 * 編集 * 」を選択します。
4. CHAP Settings で、認証に使用するイニシエータシークレットとターゲットシークレットのクレデンシャルを編集します。

CHAP 設定の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、新しいシークレットが自動的に生成されます。

5. [変更の保存 *] をクリックします。

ストレージコンテナを削除します

Element UI からストレージコンテナを削除できます。

必要なもの

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 * 」を選択します。
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、 * 削除 * を選択します。
4. 操作を確定します。
5. ストレージコンテナ * 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たことを確認します。

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。

サポートされているプロトコルは 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

VVOL タブのプロトコルエンドポイントのページには、プロトコルエンドポイントの情

報が表示されます。

- * 一次プロバイダ 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 。

- * 二次プロバイダ 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 。

- * プロトコルエンドポイント ID *

  プロトコルエンドポイントの UUID 。

- * プロトコルエンドポイントの状態 *

  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が起動中です。
  - 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。

- * プロバイダタイプ *

  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。

  - プライマリ
  - セカンダリ

- * SCSI NAA デバイス ID *

  NAA IEEE Registered Extended Format のプロトコルエンドポイントのグローバル一意 SCSI デバイス ID 。

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。

バインディングの詳細

VVol タブのバインドページには、各仮想ボリュームに関するバインド情報が表示されます。

次の情報が表示されます。

- * ホスト 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 。

- * プロトコルエンドポイント 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 。

- * 帯域 ID 内のプロトコルエンドポイント *

  プロトコルエンドポイントの SCSI NAA デバイス ID 。

- * プロトコルエンドポイントタイプ *

  プロトコルエンドポイントタイプ。

- * VVOL のバインド 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 セカンダリ ID *

  SCSI セカンドレベル LUN ID である仮想ボリュームのセカンダリ ID 。

ホストの詳細

VVol 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。

- * ホスト 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 。

- * ホストアドレス *

  ESXi ホストの IP アドレスまたは DNS 名。

- * バインディング *

  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 クラスタ ID *

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

- * イニシエータ IQN *

仮想ボリュームのホストのイニシエータ IQN 。

- * SolidFire プロトコルエンドポイント ID*

  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を使用する

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。このイニシエータレベルの CHAP 認証では、アカウントレベルのクレデンシャルが置き換えられます

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でき、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。

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。

詳細については、こちらをご覧ください

- ボリュームアクセスグループを作成します
- アクセスグループにボリュームを追加する
- アクセスグループからボリュームを削除します
- イニシエータを作成します
- イニシエータを編集します
- ボリュームアクセスグループに単一のイニシエータを追加します
- 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します

- アクセスグループからイニシエータを削除します
- アクセスグループを削除する
- イニシエータを削除します

ボリュームアクセスグループを作成します

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許可できます。

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することで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. [* 管理 > アクセスグループ *] をクリックします。
2. [アクセスグループの作成 *] をクリックします。
3. ボリュームアクセスグループの名前を * Name * フィールドに入力します。
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 イニシエータを追加しています	a. Add Initiators （イニシエータの追加）で、 Unbound Fibre Channel Initiators （未バインドのファイバチャネルイニシエータ）リストから既存のファイバチャネルイニシエータを b. [Add FC Initiator*] をクリックします。 この手順でイニシエータを作成するには、 [イニシエータの作成] リンクをクリックし、イニシエータ名を入力して、 [* 作成] をクリックします。イニシエータを作成すると、イニシエータがイニシエータリストに自動的に追加されます。 形式の例を次に示します。 `5f:47:ac:c0:5c:74:d4:02`

オプション	説明
iSCSI イニシエータの追加	イニシエータの追加で、イニシエータリストから既存のイニシエータを選択します。* 注： * イニシエータの作成 * リンクをクリックし、イニシエータ名を入力して、 * 作成 * をクリックすると、この手順の実行中にイニシエータを作成できます。イニシエータを作成すると、イニシエータがイニシエータリストに自動的に追加されます。 形式の例を次に示します。 `iqn.2010-01.com.solidfire:c2r9.fc0.2100000e1e09bb8b` 各ボリュームのイニシエータ IQN を確認するには、 * Management * > * Volumes * > * Active * リストで、そのボリュームの Actions メニューから * View Details * を選択します。 イニシエータを変更するときは、 requiredCHAP 属性を True に切り替えて、ターゲットイニシエータシークレットを設定でき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 を使用してストレージを管理します"

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 （ボリュームの追加）で、 * Volumes （ボリューム） * リストからボリュームを選択します。

   ボリュームが * Attached Volumes * リストに表示されます。
7. * オプション： * 必要に応じてボリュームを追加します。
8. [アクセスグループの作成 *] をクリックします。

詳細については、こちらをご覧ください

アクセスグループにボリュームを追加する

個々のアクセスグループの詳細を表示します

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

1. [* 管理 > アクセスグループ *] をクリックします。
2. アクセスグループの [アクション] アイコンをクリックします。
3. [* 詳細の表示 *] をクリックします。

ボリュームアクセスグループの詳細

ボリュームアクセスグループについては、 Management （管理）タブの Access Groups （アクセスグループ

）ページで確認できます。

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 。
- * 名前 * ：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。
- * 重複排除 * ：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。
- * 全体的な削減率 * ：アクセスグループ全体の削減率。
- * 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。

アクセスグループにボリュームを追加する

ボリュームアクセスグループにボリュームを追加できます。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できます。各ボリュームが属するグループは、 * Active * Volumes ページで確認できます。

この手順を使用して、 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こともできます。

1. [* 管理 **>** アクセスグループ *] をクリックします。
2. ボリュームを追加するアクセスグループの操作アイコンをクリックします。
3. 「 * 編集 * 」ボタンをクリックします。
4. Add Volumes （ボリュームの追加）で、 * Volumes （ボリューム） * リストからボリュームを選択します。

   ボリュームをさらに追加するには、この手順を繰り返します。

5. [変更の保存 *] をクリックします。

アクセスグループからボリュームを削除します

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。

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、原因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。

1. [* 管理 **>** アクセスグループ *] をクリックします。
2. ボリュームを削除するアクセスグループの操作アイコンをクリックします。
3. [編集（ Edit ）] をクリックします。

4. [ボリュームアクセスグループの編集 *] ダイアログボックスの [ボリュームの追加] で、 [添付されたボリューム *] 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リストから削除します。

   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. [変更の保存 *] をクリックします。

イニシエータを作成します

iSCSI イニシエータまたは 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。

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 アカウント名と資格情報を追加するには '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イニシエータアクセスは、「 CreateInitiators 」および「 ModyInitiators 」 API 呼び出しで 1 つ以上の virtualNetworkID を指定することで、 1 つ以上の VLAN に制限できます。仮想ネットワークを指定しない場合、イニシエータはすべてのネットワークにアクセスできます。

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 を使用してストレージを管理します"

手順

1. [* 管理 > イニシエータ *] をクリックします。
2. [イニシエータの作成] をクリックします。
3. 次の手順を実行して、 1 つ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	a. [* 単一イニシエータの作成 *] をクリックします。 b. IQN または WWPN * フィールドにイニシエータの IQN または WWPN を入力します。 c. [* エイリアス] フィールドにイニシエータのフレンドリ名を入力します。 d. [イニシエータの作成] をクリックします。
複数のイニシエータを作成する	a. イニシエータの一括作成 * をクリックします。 b. IQN または WWPN のリストをテキストボックスに入力します。 c. [Add Initiators] をクリックします。 d. 表示されたリストからイニシエータを選択し、 [* Alias*] 列の対応する [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。 e. 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。 f. イニシエータの作成 * をクリックします。

イニシエータを編集します

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。

イニシエータごとに CHAP アカウント名と資格情報を追加するには、「 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。

を参照してください "Element API を使用してストレージを管理します"。

手順

1. [* 管理 > イニシエータ *] をクリックします。
2. 編集するイニシエータの操作アイコンをクリックします。
3. [編集（ Edit ）] をクリックします。
4. [* Alias*] フィールドに、イニシエータの新しいエイリアスを入力します。
5. [変更の保存 *] をクリックします。

ボリュームアクセスグループに単一のイニシエータを追加します

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。

各ボリュームのイニシエータを特定するには、アクションアイコンをクリックし、アクティブボリュームリストからボリュームの詳細を表示 * 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することで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. [* 管理 > アクセスグループ *] をクリックします。
2. 編集するアクセスグループの * アクション * アイコンをクリックします。
3. [編集（ Edit ）] 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。

   a. Add Initiators （イニシエータの追加）で、 Unbound Fibre Channel Initiators （バインド解除されたファイバチャネルイニシエータ * ）リストから既存のファイバチャネルイニシエータを選択

   b. [Add FC Initiator*] をクリックします。

   この手順でイニシエータを作成するには、 [イニシエータの作成] リンクをクリックし、イニシエータ名を入力して、 [* 作成] をクリックします。イニシエータを作成すると、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、イニシエータの追加で、 * イニシエータ * リストから既存のイニシエータを選択します。

   この手順でイニシエータを作成するには、 [イニシエータの作成] リンクをクリックし、イニシエータ名を入力して、 [* 作成] をクリックします。イニシエータを作成すると、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
```

   各ボリュームのイニシエータ IQN は、操作アイコンをクリックし、ボリュームの詳細を表示 * を選択すると、 * Management * > * Volumes * Active Volumes ページに表示されます。

6. [変更の保存 *] をクリックします。

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 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。

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。

各ボリュームのイニシエータを特定するには、アクションアイコンをクリックし、アクティブボリュームリストにあるそのボリュームの詳細を表示 * 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、を参照してください "Element API を使用してストレージを管理します"。

手順

1. [* 管理 > イニシエータ *] をクリックします。
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. [一括アクション * （ * Bulk Actions * ）] ボタンをクリックします。
4. [* ボリュームアクセスグループに追加 *] をクリックします。
5. Add to Volume Access Group （ボリュームアクセスグループへの追加）ダイアログボックスで、 * Volume Access Group （ * ボリュームアクセスグループ）リストからアクセスグループを選択します。
6. [追加（ Add ）] をクリックします。

アクセスグループからイニシエータを削除します

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ボリュームアクセス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、原因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. [* 管理 > アクセスグループ *] をクリックします。
2. 削除するアクセスグループの * アクション * アイコンをクリックします。
3. 表示されたメニューで、「 * 編集 * 」を選択します。
4. 「 * ボリュームアクセスグループの編集 * 」ダイアログボックスの「イニシエータの追加」で、「 * イニシエータ * 」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. [変更の保存 *] をクリックします。

アクセスグループを削除する

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。

1. [* 管理 > アクセスグループ *] をクリックします。
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、 * 削除 * 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選択します。
5. 操作を確定します。

イニシエータを削除します

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、関連付けられ

てい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。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. [* 管理 > イニシエータ *] をクリックします。
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を削除	a. 削除するイニシエータの * Actions * アイコンをクリックします。 b. [削除（ Delete ）] をクリックします。 c. 操作を確定します。
複数のイニシエータを削除する	a. 削除するイニシエータの横にあるチェックボックスを選択します。 b. [一括アクション *（ * Bulk Actions * ）] ボタンをクリックします。 c. 表示されたメニューで、 * 削除 * を選択します。 d. 操作を確定します。

データを保護

NetApp Element ソフトウェアでは、さまざまな機能を使用してデータを保護できます。たとえば、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を利用できます。

- * スナップショット *

  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。

  ボリューム Snapshot を使用してデータを保護します

- * Element * 上で実行されているクラスタとボリューム間のリモートレプリケーション

  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。

  NetApp Element ソフトウェアを実行しているクラスタ間でリモートレプリケーションを実行

- * 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。

Element クラスタと ONTAP クラスタの間で SnapMirror レプリケーションを使用

- * SolidFire 、 S3 、または Swift オブジェクトストア * からボリュームへのバックアップとリストアを行います

  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。

  SolidFire 、 S3 、または Swift オブジェクトストアへのボリュームのバックアップとリストア

を参照してください。

- "SolidFire および Element ソフトウェアのドキュメント"
- "vCenter Server 向け NetApp Element プラグイン"

ボリューム **Snapshot** を使用してデータを保護します

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。

Snapshot はボリューム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。

詳細については、こちらをご覧ください

- 個々のボリューム Snapshot をデータ保護に使用します
- グループ Snapshot を使用したデータ保護タスク
- Snapshot のスケジュール設定

個々のボリューム **Snapshot** をデータ保護に使用します

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。Snapshot には、ボリュームのグループではなく個々のボリュームを使用できます。

詳細については、こちらをご覧ください

- ボリューム Snapshot を作成します
- Snapshot 保持期間を編集します
- Snapshot を削除しています

- Snapshot からボリュームをクローニングする
- Snapshot へのボリュームのロールバック
- 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
- 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
- SolidFire クラスタへのボリューム Snapshot のバックアップ

ボリューム **Snapshot** を作成します

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。

1. [* 管理 > ボリューム *] をクリックします。
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、 * スナップショット * を選択します。
4. Create Snapshot of Volume * （ボリュームの Snapshot を作成）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： * ペアリング時に Snapshot をレプリケーションに含める * チェックボックスをオンにして、親ボリュームがペアリングされているときに Snapshot をレプリケーションにキャプチャします。
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。
   - 「 * Forever * 」をクリックして、 Snapshot をシステム上に無期限に保持します。
   - [* 保存期間の設定 *] をクリックし、日付スピンボックスを使用して、システムがスナップショットを保持する期間を選択します。
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。
   a. [今すぐスナップショットを作成] をクリックします。
   b. [スナップショットの作成] 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。
   a. Create Snapshot Schedule （スナップショットスケジュールの作成） * をクリックします。
   b. 新しいスケジュール名 * を入力します。
   c. リストから * スケジュールタイプ * を選択します。
   d. * オプション：定期的にスケジュールされたスナップショットを繰り返すには、 * Recurring Schedule * チェックボックスをオンにします。
   e. [スケジュールの作成 *] をクリックします。

詳細については、こちらをご覧ください

Snapshot のスケジュールを設定します

Snapshot 保持期間を編集します

Snapshot の保持期間を変更して、 Snapshot を削除するタイミングまたは削除するかどうかを制御できます。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

持期間には、（ Snapshot の作成時間からではなく）現在の時刻からの期間を指定できます。間隔は、分、時間、および日単位で指定できます。

手順

1. [* データ保護 > スナップショット *] をクリックします。
2. 編集するスナップショットの * アクション * アイコンをクリックします。
3. 表示されたメニューで、 * 編集 * をクリックします。
4. * オプション： * ペアリング時にレプリケーションにスナップショットを含める ** チェックボックスをオンにして、親ボリュームがペアリングされているときにスナップショットがレプリケーションにキャプチャされるようにします。
5. * オプション： * Snapshot の保持オプションを選択します。
   - 「 * Forever * 」をクリックして、 Snapshot をシステム上に無期限に保持します。
   - [* 保存期間の設定 *] をクリックし、日付スピンボックスを使用して、システムがスナップショットを保持する期間を選択します。
6. [変更の保存 *] をクリックします。

Snapshot を削除します

Element ソフトウェアを実行しているストレージクラスタからボリューム Snapshot を削除できます。Snapshot を削除すると、システムはただちに削除します。

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 Snapshot 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）。

1. [* データ保護 > スナップショット *] をクリックします。
2. 削除するスナップショットの * アクション * アイコンをクリックします。
3. 表示されたメニューで、 * 削除 * を選択します。
4. 操作を確定します。

Snapshot からボリュームをクローニングします

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。このプロセスでは、ボリュームの他の Snapshot に関する情報が新しく作成されたボリュームに格納されます。

1. [* データ保護 > スナップショット *] をクリックします。
2. ボリューム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* （スナップショットからボリュームをクローニング）をクリックします。
4. [* Clone Volume from Snapshot* （スナップショットからのボリュームのクローン）] ダイアログボックスに * ボリューム名 * を入力します。
5. 新しいボリュームの合計サイズ * とサイズ単位を選択します。
6. 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 * アカウント * をリストから選択します。
8. [クローニングの開始] をクリックします。

ボリュームを **Snapshot** にロールバックします

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. [* データ保護 > スナップショット *] をクリックします。
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、 * スナップショットへのボリュームのロールバック * 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、次のコマンドを入力します。
   a. [* スナップショットへのロールバック *] ダイアログボックスで、 [* ボリュームの現在の状態をスナップショットとして保存 *] を選択します。
   b. 新しい Snapshot の名前を入力します。
5. [* ロールバックスナップショット *] をクリックします。

ボリューム**Snapshot**をバックアップします

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 / 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にボリューム Snapshot をバックアップします"
- "OpenStack Swift オブジェクトストアにボリューム Snapshot をバックアップします"
- "ボリューム Snapshot を SolidFire クラスタにバックアップします"

Amazon S3 オブジェクトストアにボリューム **Snapshot** をバックアップします

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。

1. [データ保護 >*Snapshots*] をクリックします。
2. バックアップするスナップショットの * アクション * 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. [* バックアップ先 *] の下の [統合バックアップ *] ダイアログボックスで、 [* S3 *] を選択します。
5. [データフォーマット *] で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. [* アクセスキー 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. アカウントのシークレットアクセスキーを * Secret Access Key * フィールドに入力します。
9. バックアップを格納する S3 バケットを「 * S3 Bucket * 」フィールドに入力します。
10. * オプション * ：「 * Nametag * 」フィールドにプレフィックスに追加するネームタグを入力します。
11. [読み取り開始] をクリックします。

OpenStack Swift オブジェクトストアにボリューム **Snapshot** をバックアップします

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。

1. [* データ保護 **>** スナップショット *] をクリックします。
2. バックアップするスナップショットの * アクション * 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. 統合バックアップ * （ Integrated Backup * ）ダイアログボックスの * バックアップ先 * （ * Backup to * ）で、 * Swift * （ * Swift * ）を選択します。
5. [データフォーマット *] で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 * ユーザー名 * を入力します。
8. アカウントの * 認証キー * を入力します。
9. バックアップを保存する * Container * を入力します。
10. * オプション * ： * Nametag * を入力します。
11. [読み取り開始] をクリックします。

ボリューム **Snapshot** を **SolidFire** クラスタにバックアップします

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。

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。

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のプロセスでは、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。

1. デスティネーションクラスタで、 * Management * > * Volumes * をクリックします。
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、 * リストア元 * をクリックします。
4. [* 統合リストア *] ダイアログボックスの [* リストア元 *] で、 [* SolidFire *] を選択します。
5. * データフォーマット * ：
   - * 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. [* キーの生成 *] をクリックします。
7. キーを * Bulk Volume Write Key * ボックスからクリップボードにコピーします。
8. ソースクラスタで、 * データ保護 * > * Snapshot * をクリックします。
9. バックアップに使用するスナップショットのアクション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. [* バックアップ先 **]** の **[** 統合バックアップ **SolidFire]** ダイアログボックスで、 **[*Backup]** を選択します。
12. [* データ形式 * （ * Data Format * ）] フィールドで前に選択したのと同じデータ形式を選択します。
13. 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 * リモートクラスタ MVIP * フィールドに入力します。
14. リモートクラスタのユーザ名を「 * リモートクラスタのユーザ名 * 」フィールドに入力します。
15. リモートクラスタのパスワードを「 * リモートクラスタのパスワード * 」フィールドに入力します。
16. 「 * Bulk Volume Write Key * 」フィールドに、前の手順でデスティネーションクラスタ上に生成したキーを貼り付けます。
17. [読み取り開始] 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。

詳細については、こちらをご覧ください

- グループ Snapshot を作成します
- グループ Snapshot を編集します
- グループ Snapshot のメンバーを編集します
- グループ Snapshot を削除します
- グループ Snapshot にボリュームをロールバックします
- 複数のボリュームのクローンを作成
- グループ Snapshot から複数のボリュームのクローンを作成します

グループ **Snapshot** の詳細

[データ保護] タブの [グループスナップショット] ページには、グループスナップショット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 。

- * 名前 *

  ユーザが定義したグループ Snapshot の名前。

- * 作成時間 *

  グループ Snapshot が作成された時刻。

- * ステータス *

  Snapshot の現在のステータス。有効な値は次のとおり

  - 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。

- * ボリューム数 *

  グループ内のボリュームの数。

- * まで保持 *

  Snapshot が削除される日時。

- * リモート・レプリケーション *

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

- 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** を作成しています

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. [* 管理 **>** ボリューム *] をクリックします。
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. [一括操作 *] をクリックします。
4. [グループ Snapshot *] をクリックします。
5. Create Group Snapshot of Volumes （ボリュームのグループ Snapshot の作成）ダイアログボックスに、新しいグループ Snapshot 名を入力します。
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、各 Snapshot がレプリケーションにキャプチャさ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選択します。
7. グループ Snapshot の保持オプションを選択します。
   - 「 * Forever * 」をクリックして、 Snapshot をシステム上に無期限に保持します。
   - [* 保存期間の設定 *] をクリックし、日付スピンボックスを使用して、システムがスナップショットを保持する期間を選択します。
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。
   a. Take Group Snapshot Now* をクリックします。
   b. [グループ Snapshot の作成 *] 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。
   a. Create Group Snapshot Schedule （グループ Snapshot スケジュールの作成） * をクリックします。
   b. 新しいスケジュール名 * を入力します。
   c. リストから * スケジュールタイプ * を選択します。
   d. * オプション：定期的にスケジュールされたスナップショットを繰り返すには、 * Recurring Schedule * チェックボックスをオンにします。
   e. [スケジュールの作成 *] をクリックします。

グループ **Snapshot** を編集しています

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。

1. [* データ保護 **>** グループスナップショット *] をクリックします。

2. 編集するグループ Snapshot のアクションアイコンをクリックします。
3. 表示されたメニューで、「 * 編集 * 」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、次のコマンドを入力します。
   a. 現在のレプリケーションの横にある * 編集 * をクリックします。
   b. 親ボリュームがペアリングされているときに各 Snapshot をレプリケーションに取り込む場合は、 * 各グループ Snapshot メンバーをレプリケーションに含める * チェックボックスを選択します。
5. * オプション：グループ Snapshot の保持設定を変更するには、次のオプションから選択します。
   a. [現在の保持期間 *] の横の [* 編集 *] をクリックします。
   b. グループ Snapshot の保持オプションを選択します。
      - 「 * Forever * 」をクリックして、 Snapshot をシステム上に無期限に保持します。
      - [* 保存期間の設定 *] をクリックし、日付スピンボックスを使用して、システムがスナップショットを保持する期間を選択します。
6. [変更の保存 *] をクリックします。

グループ **Snapshot** を削除しています

システムからグループ Snapshot を削除できます。グループ Snapshot を削除するときに、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 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。

1. [* データ保護 > グループスナップショット *] をクリックします。
2. 削除する Snapshot のアクションアイコンをクリックします。
3. 表示されたメニューで、 * 削除 * 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 とすべてのメンバー Snapshot を削除するには、 * グループ Snapshot とすべてのグループ Snapshot メンバーの削除 * をクリックします。
   - グループ Snapshot メンバーを個々の Snapshot として保持 * をクリックして、グループ Snapshot を削除しますが、すべてのメンバー Snapshot は保持します。
5. 操作を確定します。

グループ **Snapshot** にボリュームをロールバックします

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。

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 が作成された時点の状態にリストアされます。ロールバックでは、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。

1. [* データ保護 > グループスナップショット *] をクリックします。
2. ボリュームのロールバックに使用するグループ Snapshot の操作アイコンをクリックします。
3. 表示されたメニューで、 * グループ Snapshot へのボリュームのロールバック * 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。
   a. [* スナップショットへのロールバック *] ダイアログボックスで、 [* ボリュームの現在の状態をグループスナップショットとして保存 *] を選択します。
   b. 新しい Snapshot の名前を入力します。
5. ［ * グループ Snapshot のロールバック * ］ をクリックします。

グループ **Snapshot** のメンバーを編集しています

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。

1. [* データ保護 > スナップショット *] をクリックします。
2. [* メンバー * （ Members * ）] タブをクリックします。
3. 編集するグループ Snapshot メンバーの操作アイコンをクリックします。
4. 表示されたメニューで、「 * 編集 * 」を選択します。
5. Snapshot のレプリケーション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。
   - 「 * Forever * 」をクリックして、 Snapshot をシステム上に無期限に保持します。
   - [* 保存期間の設定 *] をクリックし、日付スピンボックスを使用して、システムがスナップショットを保持する期間を選択します。
6. [変更の保存 *] をクリックします。

複数のボリュームのクローンを作成

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。

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. [* 管理 > ボリューム *] をクリックします。
2. [アクティブ *] 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. [一括操作 *] 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・ボックスで ' 新しいボリューム名の接頭辞 * 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は、現在のボリュームアクセス方法が使用されます。

9. [クローニングの開始] をクリックします。

グループ **Snapshot** から複数の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。

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。

1. [* データ保護 > グループスナップショット *] をクリックします。
2. ボリュームのクローンに使用するグループ Snapshot の操作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 * （グループ Snapshot からのボリュームのクローン）を選択します。
4. [グループ Snapshot からのボリュームのクローン *] ダイアログ・ボックスで ' 新しいボリューム名接頭辞 * 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は、現在のボリュームアクセス方法が使用されます。

7. [クローニングの開始] をクリックします。

Snapshot のスケジュールを設定します

ボリューム Snapshot を指定した間隔で作成す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 Snapshot またはグループ Snapshot を自動的に実行するようにスケジュールを設定できます。

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。

詳細については、こちらをご覧ください

- Snapshot スケジュールを作成します
- Snapshot スケジュールを編集します
- Snapshot スケジュールを削除します
- Snapshot スケジュールをコピーします

Snapshot スケジュールの詳細

Data Protection > Schedules ページでは、 Snapshot スケジュールのリストに次の情報を表示できます。

- **ID**

  システムによって生成された Snapshot の ID 。

- * タイプ *

  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。

- * 名前 *

  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。

- * 周波数 *

  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。

- * 繰り返し *

  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。

- * 手動で一時停止 *

  スケジュールが手動で一時停止されているかどうか。

- * ボリューム ID *

  スケジュールの実行時に使用されるボリュームの ID 。

- * 最後の実行 *

  最後にスケジュールが実行された日時。

- * 前回の実行ステータス *

スケジュールの前回の実行結果。有効な値は次のとおり

- 成功
- 失敗

Snapshot スケジュールを作成します

ボリュームの Snapshot のスケジュールを設定して、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. [* データ保護 > スケジュール *] をクリックします。
2. [スケジュールの作成 *] 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 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： * Recurring Schedule * を選択し、 Snapshot スケジュールを無期限に繰り返します。
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： * ペアリング時に Snapshot をレプリケーションに含める * チェックボックスをオンにして、親ボリュームがペアリングされている場合に Snapshot をレプリケーションにキャプチャします。
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。
   - 「 * Forever * 」をクリックして、 Snapshot をシステム上に無期限に保持します。
   - [* 保存期間の設定 *] をクリックし、日付スピンボックスを使用して、システムがスナップショットを保持する期間を選択します。
10. [スケジュールの作成 *] をクリックします。

Snapshot スケジュールを編集します

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属性が使用されます。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. [* データ保護 > スケジュール *] をクリックします。
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、 * 編集 * をクリックします。
4. 「 * Volume IDs CSV * 」フィールドで、 Snapshot 処理に現在含まれている単一のボリューム ID またはカンマで区切ったボリューム ID のリストを変更します。
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 * （スケジュールを手動で一時停止）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 * （スケジュールを手動で一時停止）リストから * No * を選択します。
6. 必要に応じて、 ［ * 新しいスケジュール名 * ］ フィールドにスケジュールの別の名前を入力します。
7. 別の曜日または月に実行するようにスケジュールを変更するには、「 * スケジュールタイプ * 」を選択し、表示される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： * Recurring Schedule * を選択し、 Snapshot スケジュールを無期限に繰り返します。
9. * オプション： * New Snapshot Name * フィールドに、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： * ペアリング時に Snapshot をレプリケーションに含める * チェックボックスをオンにして、親ボリュームがペアリングされている場合に Snapshot をレプリケーションにキャプチャします。
11. 保持設定を変更するには、次のオプションから選択します。
    - 「 * Forever * 」をクリックして、 Snapshot をシステム上に無期限に保持します。
    - [* 保存期間の設定 *] をクリックし、日付スピンボックスを使用して、システムがスナップショットを保持する期間を選択します。
12. [変更の保存 *] をクリックします。

Snapshot スケジュールをコピーします

スケジュールをコピーして、現在の設定を維持できます。

1. [* データ保護 > スケジュール *] をクリックします。
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、 * コピーを作成 * をクリックします。

   [スケジュールの作成 *] ダイアログボックスが開き、スケジュールの現在の属性が表示されます。
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. [スケジュールの作成 *] をクリックします。

Snapshot スケジュールを削除します

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

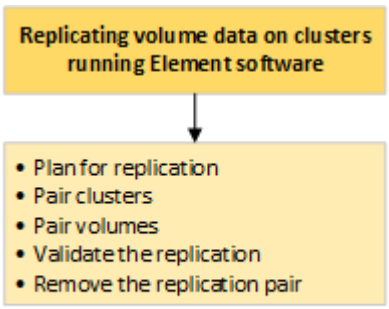
ルされた Snapshot は実行されません。過去にスケジュールで作成された Snapshot はストレージシステム上に保持されます。

1. [* データ保護 > スケジュール *] をクリックします。
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、 * 削除 * 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しているクラスタ間でリモートレプリケーションを実行

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。

レプリケーションプロセスは次の手順で構成されます。



- "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を計画します"
- "レプリケーション用にクラスタをペアリング"
- "ボリュームをペアリング"
- "ボリュームレプリケーションを検証"
- "レプリケーション後にボリューム関係を削除"
- "ボリューム関係を管理"

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を計画します

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。

必要なもの

- 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。
- 管理ネットワークとストレージネットワークの両方のノード 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。

データのレプリケーションにおける WAN アクセラレータアプライアンスの使用は、ネットアップで認定されていません。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。

詳細については、こちらをご覧ください

- レプリケーション用にクラスタをペアリング
- ボリュームをペアリング
- ペアリングされたボリュームにレプリケーションのソースとターゲットを割り当てます

レプリケーション用にクラスタをペアリング

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。

必要なもの

- 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。

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。

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。

詳細については、こちらをご覧ください

ネットワークポートの要件

MVIP またはペアリングキーを使用してクラスタをペアリング

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。

1. 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。

詳細については、こちらをご覧ください

- MVIP を使用してクラスタをペアリング
- 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

MVIP を使用してクラスタをペアリング

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。

1. ローカルクラスタで、 * Data Protection * > * Cluster Pairs * を選択します。
2. * クラスタのペアリング * をクリックします。
3. Start Pairing * をクリックし、 * Yes * をクリックして、リモートクラスタへのアクセス権を持っていることを示します。
4. リモートクラスタの MVIP アドレスを入力します。
5. リモートクラスタでのペアリングの完了 * 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、 * データ保護 * > * クラスタ・ペア * を選択します。
7. * クラスタのペアリング * をクリックします。
8. [完全ペアリング] をクリックします。

9. 完全ペアリング * ボタンをクリックします。

詳細については、こちらをご覧ください

- 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
- "Pairing Clusters using MVIP （ビデオ）"

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。

1. ローカルクラスタで、 * Data Protection * > * Cluster Pairs * を選択します。
2. * クラスタのペアリング * をクリックします。
3. Start Pairing * をクリックし、 * No * をクリックして、リモートクラスタにアクセスできないことを示します。
4. [* キーの生成 *] をクリックします。

   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。手順を完了しない場合は、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。

   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。

   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。キーが変更されると無効になります。

7. リモートクラスタで、 * データ保護 * > * クラスタ・ペア * を選択します。
8. * クラスタのペアリング * をクリックします。
9. 完全ペアリング * をクリックし、ペアリングキー * フィールドにペアリングキーを入力します（貼り付けを推奨します）。
10. [完全ペアリング] をクリックします。

詳細については、こちらをご覧ください

- MVIP を使用してクラスタをペアリング

- "Pairing Clusters using a Cluster Pairing Key （ビデオ）"

クラスタペアの接続を検証

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できます。

1. ローカルクラスタで、 * Data Protection * > * Cluster Pairs * を選択します。
2. クラスタペア * 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： * ローカルクラスタと * クラスタペア * ウィンドウに戻り、クラスタペアが接続されていることを確認します。

ボリュームをペアリング

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ときは、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。

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。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もできます。

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。

必要なもの

- 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。

手順

1. 読み取りまたは書き込みアクセスが可能なターゲットボリュームを作成します
2. ボリューム ID またはペアリングキーを使用して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レプリケーションのソースとターゲットを割り当てます

読み取りまたは書き込みアクセスが可能なターゲットボリュームを作成します

レプリケーションプロセスには、ソースボリュームとターゲットボリュームの 2 つのエンドポイントが含まれます。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に、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。

1. [* Management] > [* Volumes] を選択します。
2. [ボリュームの作成] をクリックします。
3. Create a New Volume （新規ボリュームの作成）ダイアログボックスで、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. [ボリュームの作成] をクリックします。
6. アクティブウィンドウで、ボリュームのアクションアイコンをクリックします。
7. [編集（ Edit ）] をクリックします。
8. アカウントのアクセスレベルを Replication Target に変更します。
9. [変更の保存 *] 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てボリュームをペアリングします

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 つのボリュームをペアリングします。

1. 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。

> 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。

詳細については、こちらをご覧ください

- ボリューム ID を使用してボリュームをペアリング
- ペアリングキーを使用してボリュームをペアリングします

ボリューム **ID** を使用してボリュームをペアリング

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。

必要なもの

- 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。

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のサイズ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] を選択します。
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. * ペアボリューム * （ Pair Volume * ）ダイアログボックスで、 * ペアリング開始 * （ Start Pairing * ）を選択します。
5. リモートクラスタへのアクセス権を持っていることを示す場合は、「 * i do * 」を選択します。
6. リストから * 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。
   - * Snapshot のみ * ：ソースクラスタで作成された Snapshot のみ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. リストからリモートクラスタを選択します。
8. リモートボリュームの ID を選択します。
9. [ペアリングの開始] 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、「 * 完全ペアリング * 」を選択します。
11. 「 * ボリュームペアリングの確認」で詳細を確認します。
12. [完全ペアリング] 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。ペアリング処理中に、 * 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。

    ペアリングが完了したら、ボリュームの表を更新して、ペアリングされているボリュームの* Actions リストから Pair オプションを削除する必要があります。テーブルを更新しない場合は、 *** Pair *** オプションは選択可能なままになります。「 Pair 」オプションをもう一度選択すると、新しいタブが開き、ボリュームがすでにペアリングされているため、が報告されます **`StartVolumePairing Failed:`**

`xVolumeAlreadyPaired` Element UIページの Pair Volume *ウィンドウにエラーメッセージが表示されます。

詳細については、こちらをご覧ください

- ボリュームペアリングに関するメッセージ
- ボリュームペアリングに関する警告
- ペアリングされたボリュームにレプリケーションのソースとターゲットを割り当てます

ペアリングキーを使用してボリュームをペアリングします

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。

必要なもの

- 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。

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のサイズ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] を選択します。
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. * ペアボリューム * （ Pair Volume * ）ダイアログボックスで、 * ペアリング開始 * （ 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場合は、「 * i do not * 」を選択します。
6. リストから * 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。
   - * Snapshot のみ * ：ソースクラスタで作成された Snapshot のみ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. [* キーの生成 *] をクリックします。

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。手順を完了しない場合は、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。

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。

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。キーが変更されると無効になります。

10. リモートクラスタの Element UI で、 * Management * > * Volumes * を選択します。
11. ペアリングするボリュームの操作アイコンをクリックします。
12. [* Pair *] をクリックします。
13. * ペアボリューム * （ Pair Volume * ）ダイアログボックスで、 * 完全ペアリング * （ 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 * ペアリングキー * ボックスに貼り付けます。
15. [完全ペアリング] 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。ペアリング処理中に、 * 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。

ペアリングが完了したら、ボリュームの表を更新して、ペアリングされているボリュームの* Actions リストから Pair オプションを削除する必要があります。テーブルを更新しない場合は、 *** Pair *** オプションは選択可能なままになります。「 Pair 」オプションをもう一度選択すると、新しいタブが開き、ボリュームがすでにペアリングされているため、が報告されます **`StartVolumePairing Failed: xVolumeAlreadyPaired`** **Element UI**ページの Pair Volume *ウィンドウにエラーメッセージが表示されます。

詳細については、こちらをご覧ください

- ボリュームペアリングに関するメッセージ
- ボリュームペアリングに関する警告
- ペアリングされたボリュームにレプリケーションのソースとターゲットを割り当てます

ペアリングされたボリュームにレプリケーションのソースとターゲットを割り当てます

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。この手順を使用して、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こともできます。

必要なもの

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。
   a. ソースとして割り当てるボリュームを含むクラスタから、 * Management * > * Volumes * を選択します。
   b. ソースとして割り当てるボリュームの * アクション * アイコンをクリックし、 * 編集 * をクリックします。
   c. [*Access] ドロップダウン・リストで、 [*Read/Write *] を選択します。

      ソースとターゲットの割り当てを逆にしている場合、原因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。両方のサイトでこれらの変更を調整したことを確認してください。

   a. [変更の保存 *] 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。
   a. ターゲットとして割り当てるボリュームを含むクラスタから、 * Management * > * Volumes * を選択します。
   b. ターゲットとして割り当てるボリュームのアクションアイコンをクリックし、 * 編集 * をクリックします。
   c. [**Access**] ドロップダウン・リストで '[**Replication Target**] を選択します

      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のサイズ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。

   d. [変更の保存 *] をクリックします。

詳細については、こちらをご覧ください

- ボリューム ID を使用してボリュームをペアリング
- ペアリングキーを使用してボリュームをペアリングします

ボリュームレプリケーションを検証

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。

1. 両方のクラスタから、 * 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。

詳細については、こちらをご覧ください

ボリュームペアリングに関する警告

レプリケーション後にボリューム関係を削除

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。

1. [* データ保護 * > * ボリュームペア *] を選択します。
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. [削除（ Delete ）] をクリックします。
4. メッセージを確認します。

ボリューム関係を管理

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。

詳細については、こちらをご覧ください

- レプリケーションを一時停止
- レプリケーションのモードを変更します
- ボリュームペアを削除します

レプリケーションを一時停止

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。

1. [* データ保護 * > * ボリュームペア *] を選択します。
2. ボリュームペアの操作アイコンをクリックします。
3. [編集（ 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。

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。両方のサイトでこれらの変更を調整したことを確認してください。

5. [変更の保存 *] をクリックします。

レプリケーションのモードを変更します

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。

1. [* データ保護 * > * ボリュームペア *] を選択します。
2. ボリュームペアの操作アイコンをクリックします。
3. [編集（ Edit ）] をクリックします。
4. Edit Volume Pair * （ボリュームペアの編集）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。
   - * Snapshot のみ * ：ソースクラスタで作成された Snapshot のみ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・モードを変更すると ' モードが即座に変更されます両方のサイトでこれらの変更を調整したことを確認してください。
5. [変更の保存 *] をクリックします。

ボリュームペアを削除します

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。

1. [* データ保護 * > * ボリュームペア *] を選択します。
2. 削除するボリュームペアの操作アイコンをクリックします。
3. [削除（ Delete ）] をクリックします。
4. メッセージを確認します。

クラスタペアを削除する

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。

1. [* データ保護 * > * クラスタ・ペア *] をクリックします。
2. クラスタペアの操作アイコンをクリックします。
3. 表示されたメニューで、 * 削除 * 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 2 つ目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、ペアリングされている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。ペアリングと進捗状況を示すメ

ッセージがステータス列に表示されます。

- **ID**

  各クラスタペアにシステムから割り当てられた ID 。

- * リモートクラスタ名 *

  ペア内のもう一方のクラスタの名前。

- * リモート MVIP *

  ペア内のもう一方のクラスタの管理仮想 IP アドレス。

- * ステータス *

  リモートクラスタのレプリケーションステータス

- * ボリュームの複製 *

  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

データ保護タブのボリュームペアページには、ペアリングされているボリュームまたはペアリング中のボリュームの情報が表示されます。ペアリングと進捗状況を示すメッセージがボリュームステータス列に表示されます。

- **ID**

  システムによって生成されたボリュームの ID 。

- * 名前 *

  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。

- * アカウント *

  ボリュームに割り当てられているアカウントの名前。

- * ボリュームステータス *

  ボリュームのレプリケーションステータス

- * スナップショットステータス *

  Snapshot ボリュームのステータス。

- * モード *

  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。

  - 非同期
  - Snapshot のみ
  - 同期

- * 方向 *

  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。

- * 非同期遅延 *

  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 です。

- * リモートクラスタ *

  ボリュームが配置されているリモートクラスタの名前。

- * リモートボリューム ID *

  リモートクラスタのボリュームのボリューム ID 。

- * リモートボリューム名 *

  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

ボリュームペアリングに関するメッセージは、初回のペアリングプロセス時にデータ保護タブのボリュームペアページで確認できます。これらのメッセージは、 Replicating Volumes （レプリケーションボリューム）リストビューのペアのソースとターゲットの両方に表示されます。

- * PausedDisconnected *

  ソースレプリケーションまたは同期 RPC がタイムアウトしました。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。

- * 復帰接続 *

  これで、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す。同期プロセスが開始され、データを待っています。

- * RRSync を再開します *

  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 * を実行します

  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。

- * データ転送を再開しています *

  データ転送が再開されました。

- * アクティブ *

  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。

- * アイドル *

  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

これらのメッセージは、データ保護タブのボリュームペアページでボリュームをペアリングしたあとに表示されます。表示されるメッセージは、 Replicating Volumes （レプリケーションボリューム）リストビューでペアのソースとターゲットの両方に表示されます（特に指定がない限り）。

- * 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、ペアのソース側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 の数が上限に達しており、 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。レプリケーションを再開するには手動での対応が必要です。

- * 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、ペアのソース側にのみ表示されます。

- * PausedSlowLink*

  低速リンクが検出され、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、ペアのソース側にのみ表示されます。

- * PausedVolumeSizMismatch*

  ターゲットボリュームのサイズがソースボリュームと同じではありません。

- * 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。このコマンドは、レプリケーションを再開する前に完了している必要があります。このメッセージは、ペアのソース側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。対処方法はありません。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 クラスタの間で SnapMirror レプリケーションを使用

SnapMirror関係は、NetApp Element UIのデータ保護タブから作成できます。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。

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"

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 コピーのコピーとリストアがサポートされます。このテクノロジを使用する主な理由は、 NetApp HCI から ONTAP へのディザスタリカバリです。エンドポイントには、 ONTAP 、 ONTAP Select 、 Cloud Volumes ONTAP があります。TR-4641 『 NetApp HCI Data Protection 』を参照してください。

"ネットアップテクニカルレポート 4641 ：『 NetApp HCI Data Protection 』"

詳細については、こちらをご覧ください

- "NetApp HCI 、 ONTAP 、コンバージドインフラでデータファブリックを構築できます"
- "NetApp Element ソフトウェアと ONTAP 間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。

詳細については、こちらをご覧ください

"Element ソフトウェアと ONTAP の間のレプリケーション"

クラスタで **SnapMirror** を有効にします

SnapMirror機能は、NetApp Element UIを使用してクラスタレベルで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。

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。

必要なもの

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。

手順

1. [* クラスタ *] 、 [* 設定 *] 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。

> 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 設定の変更を確認します。

ボリュームで **SnapMirror** を有効にします

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 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。

必要なもの

- 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ありません。

このプロパティは、ボリュームの作成時またはクローニング時にも設定できます。

手順

1. [* 管理 > ボリューム *] をクリックします。
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、「 * 編集 * 」を選択します。
4. * Edit Volume * （ボリュームの編集）ダイアログボックスで、 * Enable SnapMirror * （ SnapMirror を有効にする）チェックボックスを選択します。
5. [変更の保存 *] をクリックします。

SnapMirror エンドポイントを作成します

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。

SnapMirror エンドポイントは、 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、まず SnapMirror エンドポイントを作成します。

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。

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 メソッドの詳細については、を参照してください "Element API を使用してストレージを管理します"。

必要なもの

- ストレージクラスタの Element UI で SnapMirror を有効にしておく必要があります。
- 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. [* データ保護 * > * SnapMirror エンドポイント *] をクリックします。
2. [エンドポイントの作成 *] 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. 追加の詳細を確認します。
   - ONTAP ： Element との通信に使用されるクラスタ間 LIF の論理インターフェイスを表示します。
   - Status ： SnapMirror エンドポイントの現在のステータスが表示されます。指定可能な値は、 connected 、 disconnected 、および unmanaged です。
6. [エンドポイントの作成 *] をクリックします。

SnapMirror 関係を作成

SnapMirror関係はNetApp Element UIで作成する必要があります。

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。

必要なもの

ボリュームで SnapMirror を有効にしておきます。

手順

1. [* 管理 > ボリューム *] をクリックします。
2. 関係を構成するボリュームの * Actions * アイコンをクリックします。
3. [* SnapMirror 関係の作成 *] をクリックします。
4. SnapMirror 関係の作成 * ダイアログボックスで、 * エンドポイント * 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には、 * 新しいボリュームの作成 * をクリックします。
   a. この関係に使用する * Storage Virtual Machine * を選択します。
   b. ドロップダウンリストからアグリゲートを選択します。
   c. [* Volume Name Suffix* （ * ボリューム名サフィックス）] フィールドにサフィックスを入力します。

      ソースボリューム名が検出され、 * Volume Name * （ボリューム名）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。

   d. [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には、 * 既存のボリュームを使用 * をクリックします。
   a. この関係に使用する * Storage Virtual Machine * を選択します。
   b. 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. ［ * 関係の詳細 * ］ 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ルール保持が設定されている場合、ルールテーブルにはルールと関連する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 * ： [帯域幅を * に制限] フィールドに、この関係に関連付けられたデータ転送で消費できる最大帯域幅を入力します。
11. 追加の詳細を確認します。
    - * 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が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。
    - * ステータス * ：関係の現在のステータス。有効な値は、 idle 、 transferring 、 checking 、 quiescing 、 quiesced 、 キューに格納されている、準備中、最終処理中、中止中、および解除中です。
    - * 遅延時間 * ：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よりも短い必要があります。
    - * Bandwidth Limit * ：この関係に関連付けられたデータ転送で消費できる帯域幅の最大量。
    - * 最後に転送された日時 * ：前回転送された Snapshot のタイムスタンプ。詳細については、をクリックしてください。
    - * Policy Name * ：関係の ONTAP SnapMirror ポリシーの名前。
    - * ポリシータイプ * ：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_mirro を参照してください
      - mirror-vault のように指定します
    - * スケジュール名 * ：この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。
12. この時点で初期化しない場合は、 [* Initialize * （初期化 * ）] チェックボックスが選択されていないことを確認してください。

    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て、ソースボリュームの Snapshot コピーが作成され、そのコピーおよび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）を開始することもできます。

13. [関係の作成（ Create Relationship ）] をクリックする。
14. この新しい SnapMirror 関係を表示するには、 * Data Protection * > * SnapMirror Relationships * をクリックします。

SnapMirror 関係の操作

関係は、データ保護タブの SnapMirror 関係ページで設定できます。ここでは、 [アクション（ Actions ）] アイコンのオプションについて説明します。

- * 編集 * ：関係で使用する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 * ：データの最初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 * ：関係をオンデマンドで更新し、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。
- * 休止 * ：関係の更新を阻止します。
- * 再開 * ：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、現在および将来のすべての転送を停止します。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 * ：解除された関係を、解除前と同じ方向で再確立します。
- * 逆再同期 * ：逆方向の新しい関係を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の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。
- * 中止 * ：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 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。

Snapshot にラベルを適用すると、その Snapshot が 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、データ転送にルールを適用するために、一致するラベルの付いた 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す。関係では、ポリシーを参照して保持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含めることができ、各ルールにはラベルが付けられます。このラベルは、 Snapshot と保持ルールの間のリンクとして機能します。

この 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指定されます。

Snapshot に **SnapMirror** ラベルを追加します

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。

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。

> グループ Snapshot にラベルを追加すると、個々の Snapshot の既存のラベルがすべて上書きされます。

必要なもの

- 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 にすでに存在している必要があります。

手順

1. [* データ保護 > スナップショット *] または [グループスナップショット *] ページをクリックします。
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 * （スナップショットの編集）ダイアログボックスで、 * SnapMirror Label * （ SnapMirror ラベル * ）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一致している必要があります。
4. [変更の保存 *] をクリックします。

SnapMirror ラベルを **Snapshot** スケジュールに追加します

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 NetAppONTAP System Manager で確認できます。

必要なもの

- クラスタレベルで SnapMirror を有効にする必要があります。
- 追加するラベルが ONTAP にすでに存在している必要があります。

手順

1. [* データ保護 > スケジュール *] をクリックします。
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を作成します	a. ［ * スケジュールの作成 * ］ を選択します。 b. その他の関連する詳細情報をすべて入力します。 c. ［ * スケジュールの作成 * ］ を選択します。
既存のスケジュールを変更する	a. ラベルを追加するスケジュールの * アクション * アイコンをクリックし、 * 編集 * を選択します。 b. 表示されたダイアログボックスの * SnapMirror ラベル * フィールドにテキストを入力します。 c. 「変更を保存」を選択します。

詳細については、こちらをご覧ください

Snapshot スケジュールを作成します

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。

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 クラスタからフェイルオーバーを実行します

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。

NetApp Element UI を使用してフェイルオーバーを実行します。Element UI 問題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。

必要なもの

- 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。

手順

1. Element UI で、 * Data Protection * > * SnapMirror Relationships * をクリックします。
2. フェイルオーバーするソースボリュームとの関係を探します。
3. [* アクション * （ * Actions * ）] アイコンをクリックする。
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になり、アプリケーションホストに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を実行します

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異なります。

詳細については、こちらをご覧ください

- ソースボリュームが存在する場合は、フェイルバックを実行します
- ソースボリュームが存在しない場合にフェイルバックを実行します
- SnapMirror フェイルバックのシナリオ

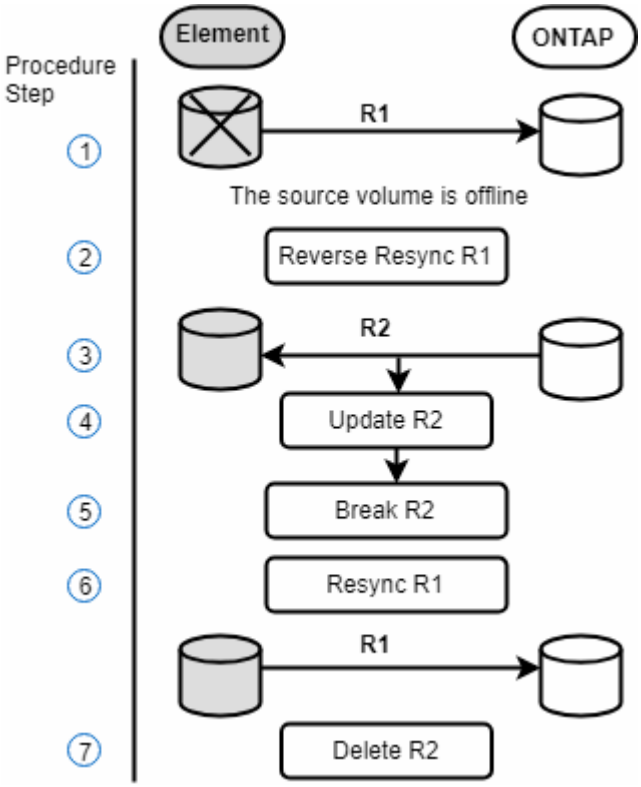
SnapMirror フェイルバックのシナリオ

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。

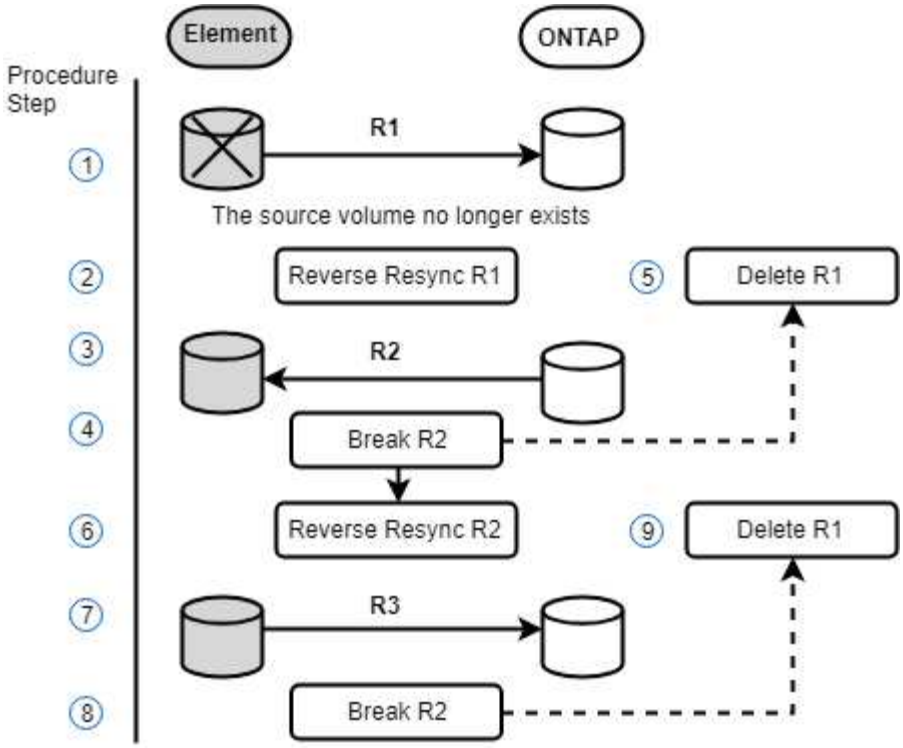
参考のために、対応する手順の各ステップを付記します。

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。



詳細については、こちらをご覧ください

- ソースボリュームが存在する場合は、フェイルバックを実行します
- ソースボリュームが存在しない場合にフェイルバックを実行します

ソースボリュームが存在する場合は、フェイルバックを実行します

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。元のソースボリュームがまだ存在している手順環境のシナリオです。

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. アクションアイコンをクリックし、 * 逆再同期 * をクリックします。
3. 操作を確定します。

> 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. 作成した反転関係の [アクション（ Actions ）] アイコンをクリックし、 [* 更新（ Update ）] をクリックする。

   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、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ことを確認しました。 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アクティブ化するには、次の手順を実行します。

5. 反転関係の [アクション（ Actions ）] アイコンをクリックし、 [* 分割（ Break ）] をクリックする。
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。

> これで、元のプライマリボリュームをマウントして、元のプライマリ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「拘束されていない」であることを確認したら、反転関係のアクションアイコンをクリックし、 * 削除 * をクリックします。

詳細については、こちらをご覧ください

SnapMirror フェイルバックのシナリオ

ソースボリュームが存在しない場合にフェイルバックを実行します

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。このセクションでは、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環境シナリオを示します。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。

必要なもの

- Element ボリュームと ONTAP ボリュームの間で、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 SnapMirror ポリシーおよびスケジュールの詳細をメモしてください。この情報は、関係を再作成する際に必要となります。
2. [アクション * （ Actions * ）] アイコンをクリックし、 [逆再同期（ Reverse Resync ）] をクリックする。
3. 操作を確定します。

> 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。新しいボリュームには、 sm-recovery というデフォルトの QoS ポリシーが割り当てられて、 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（ Reverse Resync ）処理中に作成された逆の関係の * アクション * （ * Actions * ）アイコンをクリックし、 * ブレーク * （ * 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 * アクション * アイコンをクリックし、 * 削除 * をクリックします。
6. 手順 4 で解除した逆の関係の * アクション * アイコンをクリックし、 * 逆再同期 * 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. [* アクション * （ Actions * ）] アイコンと [* 編集 * （ Edit * ）] をクリックして、この関係を元の QoS ポリシーとメモしたスケジュール設定で更新します。
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。

詳細については、こちらをご覧ください

SnapMirror フェイルバックのシナリオ

ONTAP から **Element** への転送または **1** 回限りの移行を実行します

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して使用できます。

- 2 つのシナリオがあります。
  - 以前のディザスタリカバリ関係が存在しない。この手順のすべての手順を実行します。
  - 以前のディザスタリカバリ関係は存在しますが、今回の移行に使用するボリューム間の関係ではありません。この場合は、手順 3 と 4 のみを実行してください。

必要なもの

- Element デスティネーションノードから ONTAP 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。

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 は実際の文字列「 lun 」、 id_number は Element ボリュームの ID です。

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. snapmirror show コマンドを使用 ONTAP 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. 「 ElementCreateVolume 」 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アクセスモードを SnapMirror に設定します。

   Element API を使用して Element ボリュームを作成します

```
{
   "method": "CreateVolume",
   "params": {
        "name": "SMTargetVolumeTest2",
        "accountID": 1,
        "totalSize": 100000000000,
        "enable512e": true,
        "attributes": {},
        "qosPolicyID": 1,
        "enableSnapMirrorReplication": true,
        "access": "snapMirrorTarget"
    },
    "id": 1
}
```

4. ONTAP の「 napmirror 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。

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。

詳細については、こちらをご覧ください

- Amazon S3 オブジェクトストアにボリュームをバックアップします
- OpenStack Swift オブジェクトストアにボリュームをバックアップします
- ボリュームを SolidFire ストレージクラスタにバックアップします
- 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する
- 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します
- 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します

Amazon S3 オブジェクトストアにボリュームをバックアップします

Amazon S3 と互換性のある外部のオブジェクトストアにのボリュームをバックアップできます。

1. [* 管理 **>** ボリューム *] をクリックします。
2. バックアップするボリュームの操作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. [* バックアップ先 *] の下の [統合バックアップ *] ダイアログボックスで、 [* S3 *] を選択します。
5. [データフォーマット *] で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. [* アクセスキー 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. アカウントのシークレットアクセスキーを * Secret Access Key * フィールドに入力します。
9. バックアップを格納する S3 バケットを「 * S3 Bucket * 」フィールドに入力します。
10. 「 * Nametag * 」フィールドにプレフィックスに追加するネームタグを入力します。
11. [読み取り開始] をクリックします。

OpenStack Swift オブジェクトストアにボリュームをバックアップします

OpenStack Swift と互換性のある外部のオブジェクトストアにのボリュームをバックアップできます。

1. [* 管理 **>** ボリューム *] をクリックします。
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. [* バックアップ先 *] の下の [統合バックアップ *] ダイアログボックスで、 [* Swift*] を選択します。
5. * データフォーマット * ：
   - * 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 * url * フィールドに入力します。
7. [* ユーザー名 *] フィールドにアカウントのユーザー名を入力します。
8. [* Authentication Key* （認証キー * ）] 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、バックアップを保存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名前タグを入力します。
11. [読み取り開始] をクリックします。

ボリュームを **SolidFire** ストレージクラスタにバックアップします

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、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。

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。

を参照してください "レプリケーション用にクラスタをペアリング"。

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のプロセスでは、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。

1. デスティネーションクラスタで、 * Management * > * Volumes * と入力します。
2. デスティネーションボリュームの操作アイコンをクリックします。
3. 表示されたメニューで、 * リストア元 * をクリックします。
4. 統合リストア * （ Integrated Restore * ）ダイアログボックスの * リストア元 * （ * Restore From * ） で * SolidFire * を選択します。
5. [データフォーマット *] で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. [* キーの生成 *] をクリックします。
7. キーを * Bulk Volume Write Key * ボックスから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 * に移動します。
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. [* バックアップ先 *] の下の [統合バックアップ *] ダイアログボックスで、 [* SolidFire *] を選択します。
12. [* データ形式 * （ * Data Format * ）] フィールドで前に選択したオプションと同じオプションを選択します。
13. 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 * リモートクラスタ MVIP * フィールドに入力します。
14. リモートクラスタのユーザ名を「 * リモートクラスタのユーザ名 * 」フィールドに入力します。
15. リモートクラスタのパスワードを「 * リモートクラスタのパスワード * 」フィールドに入力します。
16. 「 * Bulk Volume Write Key * 」フィールドに、前の手順でデスティネーションクラスタ上に生成したキーを貼り付けます。
17. [読み取り開始] 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ボリュームをリストアする

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。

1. [**Reporting**>*Event Log] をクリックします。
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. [* 管理 **>** ボリューム *] をクリックします。
6. リストアするボリュームの操作アイコンをクリックします。
7. 表示されたメニューで、 * リストア元 * をクリックします。
8. [* 統合リストア *] ダイアログボックスの [* リストア元 *] で、 [* S3 *] を選択します。
9. バックアップに一致するオプションを * Data Format * ：
    - * 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. [* アクセスキー 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. アカウントのシークレットアクセスキーを * Secret Access Key * フィールドに入力します。
13. バックアップを格納する S3 バケットを「 * S3 Bucket * 」フィールドに入力します。
14. マニフェスト情報を * Manifest * フィールドに貼り付けます。
15. 「 * 書き込みを開始」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ボリュームをリストアします

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。

1. [**Reporting**>*Event Log] をクリックします。

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. [* 管理 **>** ボリューム *] をクリックします。
6. リストアするボリュームの操作アイコンをクリックします。
7. 表示されたメニューで、 * リストア元 * をクリックします。
8. [* 統合リストア *] ダイアログボックスの [* リストア元 *] で、 [* Swift*] を選択します。
9. バックアップに一致するオプションを * Data Format * ：
   - * 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. オブジェクトストアへのアクセスに使用する URL を * url * フィールドに入力します。
11. [* ユーザー名 *] フィールドにアカウントのユーザー名を入力します。
12. [* Authentication Key* （認証キー * ）] フィールドにアカウントの認証キーを入力します。
13. バックアップを格納するコンテナの名前を「 * Container * 」フィールドに入力します。
14. マニフェスト情報を * Manifest * フィールドに貼り付けます。
15. 「 * 書き込みを開始」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ボリュームをリストアします

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。

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のプロセスでは、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。

1. デスティネーションクラスタで、 * Management * > * Volumes * をクリックします。
2. リストアするボリュームの操作アイコンをクリックします。
3. 表示されたメニューで、 * リストア元 * をクリックします。
4. 統合リストア * （ Integrated Restore * ）ダイアログボックスの * リストア元 * （ * Restore From * ）で * SolidFire * を選択します。
5. バックアップに一致するオプションを * Data Format * ：
   - * 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. [* キーの生成 *] をクリックします。
7. * 一括ボリューム書き込みキー * 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 * をクリックします。
9. リストアに使用するボリュームの操作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. 統合バックアップ * （ Integrated Backup * ）ダイアログボックスで、 * バックアップ先 * （ * Backup to * ）で * SolidFire * を選択します。
12. バックアップに一致するオプションを * Data Format * で選択します。
13. 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 * リモートクラスタ MVIP * フィールドに入力します。
14. リモートクラスタのユーザ名を「 * リモートクラスタのユーザ名 * 」フィールドに入力します。
15. リモートクラスタのパスワードを「 * リモートクラスタのパスワード * 」フィールドに入力します。
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. [読み取り開始] をクリックします。

システムのトラブルシューティングを行います

システムの監視は、診断目的、および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があります。

- "システムイベントに関する情報を表示します"
- "実行中のタスクのステータスを表示します"
- "システムアラートを表示します"
- "ノードのパフォーマンスアクティビティを表示します"
- "ボリュームのパフォーマンスを表示します"
- "iSCSI セッションを表示します"
- "Fibre Channel セッションを表示します"
- "ドライブのトラブルシューティング"
- "ノードのトラブルシューティングを行う"
- "ストレージノードのノードユーティリティを使用する"
- "管理ノードを操作します"
- "クラスタフルレベルを把握"

を参照してください。

- "SolidFire および Element ソフトウェアのドキュメント"
- "vCenter Server 向け NetApp Element プラグイン"

システムイベントに関する情報を表示します

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。

1. Element UI で、 * Reporting * > * Event Log * を選択します。

   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 。
イベントタイプ	API イベントやクローンイベントなど、記録されるイベントのタイプ。
メッセージ	イベントに関連するメッセージです。
詳細	イベントが発生した理由の特定に役立つ情報。
サービス ID	イベントを報告したサービス（該当する場合）。
ノード	イベントを報告したノード（該当する場合）。
ドライブ ID	イベントを報告したドライブ（該当する場合）。
イベント時間	イベントが発生した時刻。

詳細については、こちらをご覧ください

イベントタイプ

イベントタイプ

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

読み取り専用の API コマンドはイベントログに記録されません。

イベントログに表示されるイベントのタイプは次のとおりです。

- * apiEvent *

  ユーザが API または Web UI から開始した、設定を変更するイベント。

- **binAssignmentsEvent**

  データビンの割り当てに関連するイベント。ビンは基本的にデータを保持するコンテナであり、クラスタ全体にマッピングされます。

- **binSyncEvent**

  ブロックサービス間でのデータの再割り当てに関連するシステムイベント。

- * bsCheckEvent *

  ブロックサービスチェックに関連するシステムイベント。

- * bsKillEvent *

  ブロックサービスの終了に関連するシステムイベント。

- * bulkOpEvent *

  バックアップ、リストア、 Snapshot 、クローンなど、ボリューム全体で実行される処理に関連するイベント。

- * cloneEvent *

  ボリュームクローニングに関連するイベント。

- * clusterMasterEvent *

  クラスタの初期化時、またはノードの追加や削除など、クラスタの構成の変更時に表示されるイベント。

- **csumEvent**

  ディスク上の無効なデータチェックサムに関連するイベント。

- * DataEvent *

  データの読み取りと書き込みに関連するイベント。

- * dbEvent *

  クラスタ内のアンサンブルノードによって管理されているグローバルデータベースに関連するイベント。

- * driveEvent *

  ドライブの処理に関連するイベント。

- * encryptionAtRestEvent*

  クラスタでの暗号化プロセスに関連するイベント。

- * ensembleEvent*

  アンサンブル内のノード数の増減に関連するイベント。

- * fibreChannelEvent *

  ノードの設定と接続に関連するイベント。

- * gcEvent *

ブロックドライブ上のストレージを再利用するために 60 分ごとに実行されるプロセスに関連するイベント。このプロセスはガベージコレクションとも呼ばれます。

- * ieEvent *

  内部システムエラー。

- * installEvent *

  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。

- * メンテナンスモードイベント *

  ノードの無効化など、ノードのメンテナンスモードに関連するイベント。

- * ネットワークイベント *

  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。

- * siceEvent *

  メタデータドライブやボリュームの削除など、スライスサーバに関連するイベント。

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

  - 反転：プライマリサービスを新しいプライマリサービスに変更します

```
sliceID oldPrimaryServiceID->newPrimaryServiceID
```

◦ 移動：セカンダリサービスを新しいセカンダリサービスに変更します

```
sliceID {oldSecondaryServiceID(s)}->{newSecondaryServiceID(s)}
```

◦ pruning ：一連のサービスからボリュームを削除する

```
sliceID {oldSecondaryServiceID(s)}
```

- * snmpTrapEvent *

  SNMP トラップに関連するイベント。

- * statEvent *

  システム統計に関連するイベント。

- * tsEvent *

  システム転送サービスに関連するイベント。

- * unexpectedException *

  予期しないシステム例外に関連するイベント。

- * ureEvent*

  ストレージデバイスからの読み取り中に発生した回復不能な読み取りエラーに関連するイベント。

- * vasaProviderEvent *

  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を表示します

ListSyncJobs および ListBulkVolumeJobs API メソッドが報告する、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。実行中のタスクページには、Element UI のレポートタブからアクセスできます。

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、現在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。同期化タスクは、完了するタスクがなくなるまで、 [実行中のタスク] ページに表示され続ける場合があります。

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。

システムアラートを表示します

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で確認できます。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。

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。これにより、発生したすべてのアラートに関する通知を受け取ることができます。

1. Element UI で、 * Reporting * > * Alerts * を選択します。

   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 。
重大度	アラートの重要度。有効な値は次のとおり • warning ：近々対応が必要になる可能性があるが、マイナー問題です。システムのアップグレードは引き続き可能です。 • error ：原因のパフォーマンスが低下したり高可用性（ HA ）が失われたりする可能性のある障害です。通常、エラーがサービスに影響することはありません。 • critical ：サービスに影響する深刻な障害です。システムは API 要求またはクライアント I/O 要求を処理できません。この状態で運用を続けると、データが失われる可能性があります。 • bestPractice ：推奨されるシステム構成のベストプラクティスが使用されていません。
を入力します	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。
ノード	この障害に関連するノードのノード ID 。エラーのタイプが node と drive の場合に表示され、それ以外の場合は - （ダッシュ）が表示されます。

ドライブ ID	この障害に関連するドライブのドライブ ID 。エラーのタイプが drive の場合に表示され、それ以外の場合は - （ダッシュ）が表示されます。
エラーコード	エラーの原因を示すコード。
詳細	エラーの概要とその他の詳細情報。
日付	障害がログに記録された日時。

2. 個々のアラートの ［ * 詳細を表示 * ］ をクリックすると、そのアラートに関する情報が表示されます。
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、解決日を含むアラートに関するすべての情報が解決済み領域に移動されます。

詳細については、こちらをご覧ください

- クラスタ障害コード
- "Element API を使用してストレージを管理します"

クラスタ障害コード

エラーまたは必要な状態が報告される場合は、 Alerts （アラート）ページにリストされている障害コードを生成します。これらのコードは、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のに役立ちます。

以下に、各種コードの概要を示します。

- * authenticationServiceFault*

  1 つ以上のクラスタノードの認証サービスが正常に機能していません。

  ネットアップサポートにお問い合わせください。

- * 利用可能な VirtualNetworkIPAddressesLow *

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

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

- * blockClusterFull *

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

  ◦ stage3Low （警告）：ユーザ定義のしきい値が超えています。Cluster Full の設定を調整するか、ノードを追加します。

- stage4Critical （エラー）： 1 ノードの障害からリカバリするための十分なスペースがありません。ボリューム、 Snapshot 、およびクローンは作成できません。
- stage5CompletelyConsumed （ Critical ） 1 ：書き込みまたは新しい iSCSI 接続は許可されません。現在の iSCSI 接続は維持されます。クラスタに容量を追加するまで書き込みは失敗します。この問題を解決するには、ボリュームをパージまたは削除するか、ストレージクラスタに別のストレージノードを追加してください。

- * ブロックが劣化しました *

  障害により、ブロックデータの完全なレプリケートが行われなくなりました。

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

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

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

- * blockServiceTooFull*

  ブロックサービスが大量のスペースを使用しています。

  この問題を解決するには、プロビジョニング済み容量を追加してください。

- * ブロックされたもの *

  ブロックサービスが正常でないことが検出されました：

  - 重大度 = 警告：対処は行われません。この警告期間は、 cTimeUntilBSIsKilledMSec = 330000 ミリ秒で期限切れになります。
  - 重大度 = エラー：データの運用停止処理が自動的に実行され、他の正常なドライブにデータが再レプリケートされます。
  - 重大度 = 重大：複数のノードで障害ブロックサービスが発生していますが、レプリケーション数以上になっています（ Double Helix の場合は 2 ）。データを使用できないため、ビンの同期が完了しません。ネットワーク接続の問題とハードウェアエラーを確認します。特定のハードウェアコンポーネントで障害が発生した場合は、それ以外の障害が発生します。この障害は、ブロックサービスにアクセスできるかサービスが運用停止されると解消されます。

- * clockSkewExceedsFaultThreshold *

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

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

- * clusterCannotSync*

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

  この問題を解決するには、ストレージを追加してください。

- * clusterFull *

  ストレージクラスタ内の空きストレージスペースが不足しています。

  この問題を解決するには、ストレージを追加してください。

- * clusterIOPSAreOverProvised*

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

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

- **disableDriveSecurityFailed**

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

  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。考えられる原因は次のとおりです。

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

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

- * 接続解除されたクラスタペア *

  クラスタペアが切断されているか、正しく設定されていません。クラスタ間のネットワーク接続を確認してください。

- * disconnectedRemoteNode * を実行します

  リモートノードが切断されているか、正しく設定されていません。ノード間のネットワーク接続を確認してください。

- * 切断された SnapMirrorEndpoint *

リモート SnapMirror エンドポイントが切断されているか、正しく設定されていません。クラスタとリモート SnapMirrorEndpoint の間のネットワーク接続を確認してください。

- * 走行可能 *

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

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

- * driveFailed *

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

  - ドライブマネージャがドライブにアクセスできません。
  - スライスサービスまたはブロックサービスで障害が発生した回数が多すぎます。おそらくドライブの読み取りまたは書き込みの失敗が原因で再起動できません。
  - ドライブがありません。
  - ノードのマスターサービスにアクセスできません（ノード内のすべてのドライブが見つからないか障害状態であるとみなされます）。
  - ドライブがロックされており、そのドライブの認証キーを取得できません。
  - ドライブがロックされているためロック解除処理が失敗します。この問題を解決するには：
  - ノードのネットワーク接続を確認してください。
  - ドライブを交換します。
  - 認証キーが使用可能であることを確認します。

- * driveHealthFault *

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

  - シリアル付きドライブ： < シリアル番号 > 、スロット： < ノードスロット >< ドライブスロット > 、SMART 全体のヘルスチェックに失敗しました。この問題を解決するには、ドライブを交換してください。

- * driveWearFault *

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

  - シリアル付きドライブ： <serial number> in slot ： <node slot><drive slot> には、重大な摩耗度レベルがあります。
  - Serial Number > in slot ： < ノードスロット >< ドライブスロット > のドライブの摩耗リザーブが少ない。この問題を解決するには、ドライブをすぐに交換してください。

- * duplicateClusterMasterCandidates *

  ストレージクラス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。この障害は重大度が「 Warning 」で記録されます。

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

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

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

- * ensembleDegraded *

  1 つ以上のアンサンブルノードで、ネットワーク接続または電源が失われました。

  この問題を解決するには、ネットワーク接続または電源を復旧してください。

- * 例外 *

  通常の障害以外の障害が報告されました。これらの障害は、障害キューから自動的に消去されることはありません。ネットアップサポートにお問い合わせください。

- * 失敗した SpaceTooFull *

  ブロックサービスがデータ書き込み要求に応答していません。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スペースが不足します。

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

- * fanSensor *

  ファンセンサーに障害が発生しているか、ファンセンサーがありません。

  この問題を解決するには、障害が発生したハードウェアを交換してください。

- * fibreChannelAccessDegraded *

  Fibre Channel ノードが自身のストレージ IP でストレージクラスタ内の他のノードに一定期間応答していません。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てください。

- * 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てください。

- * fibreChannelActiveIxL *

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

  - ベストプラクティスの上限は 5500 です。
  - 警告の上限は 7500 です。
  - 上限（必須ではない）は 8192 です。この問題を解決するには、 iXL Nexus の数をベストプラクティスの上限である 5500 未満に減らしてください。

- * fibreChannelConfig *

  このクラスタ障害は、次のいずれかの状態を示します。

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

- * fibreChannelIOPS*

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

  - FC0025 ： 450 、 000 IOPS 制限（ Fibre Channel ノードあたり 4K ブロックサイズ）
  - FCN001 ： 625K OPS 制限（ Fibre Channel ノードあたり 4K ブロックサイズ）。この問題を解決するには、使用可能なすべての Fibre Channel ノードに負荷を分散してください。

- * fibreChannelStaticIxL *

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

  - ベストプラクティスの上限は 11000 です。
  - 警告制限は 15000 です。
  - 最大制限（強制）は 16384 です。この問題を解決するには、 iXL Nexus の数をベストプラクティスの上限である 11000 未満に減らしてください。

- * fileSystemCapacityLow *

  いずれかのファイルシステムでスペースが不足しています。

  この問題を解決するには、ファイルシステムに容量を追加してください。

- * FipsDrivesMismatch *

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

この問題を解決するには、該当するドライブを取り外すか交換してください。

- * FipsDrivesOutOfCompliance]

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

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

- * fipsSelfTestFailure*

  FIPS サブシステムのセルフテスト中に障害が検出されました。

  ネットアップサポートにお問い合わせください。

- * ハードウェア構成の不一致 *

  このクラスタ障害は、次のいずれかの状態を示します。

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

- **idPCertificateExpiration**

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

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

  この問題を解決するには、有効期限が切れる前に SSL 証明書を更新してください。更新された SSL 証明書を提供するには、 UpdateIdpConfiguration API メソッドを「 refreshCertificateExpirationTime=true 」とともに使用します。

- * 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 mismatch ： Bond1G インターフェイス間で異なる MTU が設定されています。
  - Bond10G mismatch ： Bond10G インターフェイス間で異なる MTU が設定されています。該当するノードと関連付けられている MTU 値が表示されます。

- * inconsistentRoutingRules*

  このインターフェイスのルーティングルールが矛盾しています。

- * inconsistentSubnetMas*

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

- * incorrectBondPortCount *

  ボンドポートの数が正しくありません。

- * invalidConfiguredFibreChannelNodeCount *

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

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

- **irqBalanceFailed**

  割り込みのバランス調整中に例外が発生しました。

  ネットアップサポートにお問い合わせください。

- * kmipCertificateFault * ：

  - ルート認証局（ CA ）証明書の有効期限が近づいています。

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

  - クライアント証明書の有効期限が近づいています。

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

- ルート認証局（ CA ）証明書の有効期限が切れています。

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

- クライアント証明書の期限が切れています。

  この問題を解決するには、 GetClientCertificateSigningRequest を使用して新しい CSR を作成し、新しい有効期限まで 30 日以上あることを確認して署名し、 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、正しい証明書が指定されていることを確認し、必要に応じてルート CA から証明書を再取得します。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 * ：
  - 接続に失敗しました

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

  - 認証に失敗しました

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

  - サーバエラーです

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

- * memyEccThreshold *

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

イベント	重大度	説明

1 つの DIMM cErrorCount が cDimmCorrectableErrWarnThreshold に到達しました。	警告	DIMM のしきい値を超えている修正可能な ECC メモリエラー：<Processor><DIMM Slot>
DIMM の cErrorFaultTimer が期限切れになるまで、 1 つの DIMM cErrorCount は cDimmCorrectableErrWarnThreshold よりも高くなります。	エラー	DIMM のしきい値を超えている修正可能な ECC メモリエラー：<Processor><DIMM>
メモリコントローラが cMemCtlrCorrectableErrWarnThreshold より上の cErrorCount を報告し、 cMemCtlrCorrectableErrWarnDuration を指定します。	警告	修正可能な ECC メモリエラーがメモリコントローラのしきい値を超えています：<Processor><Memory Controller>
メモリコントローラでは、メモリコントローラの cErrorFaultTimer の期限が切れるまで、メモリコントローラから cMemCtlrCorrectableErrWarnThreshold が報告されます。	エラー	DIMM のしきい値を超えている修正可能な ECC メモリエラー：<Processor><DIMM>
1 つの DIMM がゼロより大きい uErrorCount を報告していますが、 cDimmUncorrectableErrFaultThreshold よりも小さくなっています。	警告	DIMM で修正不可能な ECC メモリエラーが検出されました：<Processor><DIMM Slot>
1 つの DIMM で少なくとも cDimmUncorrectableErrFaultThreshold の uErrorCount が報告されます。	エラー	DIMM で修正不可能な ECC メモリエラーが検出されました：<Processor><DIMM Slot>
メモリコントローラがゼロより大きい uErrorCount を報告していますが、 cMemCtlrUncorrectableErrFaultThreshold よりも小さくなっています。	警告	メモリコントローラで修正不可能な ECC メモリエラーが検出されました： <Processor><Memory Controller>
メモリコントローラが少なくとも cMemCtlrUncorrectableErrFaultThreshold の uErrorCount を報告しています。	エラー	メモリコントローラで修正不可能な ECC メモリエラーが検出されました： <Processor><Memory Controller>

この問題を解決するには、ネットアップサポートにお問い合わせください。

- * memoryUsageThreshold *

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

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

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

  この問題を解決するには、ネットアップサポートにお問い合わせください。

- * メタデータの ClusterFull *

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

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

- * mtuCheckFailure*

  ネットワークデバイスに適切な MTU サイズが設定されていません。

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

- * networkConfig *

  このクラスタ障害は、次のいずれかの状態を示します。

  - 想定されるインターフェイスが存在しません。
  - インターフェイスが重複しています。
  - 設定されたインターフェイスが停止しています。
  - ネットワークの再起動が必要です。ネットアップサポートにお問い合わせください。

- * 利用不可 VirtualNetworkIPAddresses*

IP アドレスのブロックに使用可能な仮想ネットワークアドレスがありません。

- virtualNetworkID # タグ（ # ）には、使用可能なストレージ IP アドレスがありません。クラスタにノードを追加することはできません。この問題を解決するには、仮想ネットワークアドレスのブロックに IP アドレスを追加してください。

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

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

  この問題を解決するには、ノードのネットワーク接続を確認してください。

- * nodeHardwareFault （ドライブ暗号化対応状態がスロット <node slot><drive slot> のドライブのノードの暗号化対応状態と一致しません） *

  ドライブが、搭載されているストレージノードと暗号化機能が一致しません。

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

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

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

  ストレージノードに含まれているドライブはサポートされません。

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

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

- * nodeMaintenanceMode*

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

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

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

- * nodeOffline *

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

- * notUsingLACpBondMode *

  LACP ボンディングモードが設定されていません。

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

- * ntpServerUnreachable*

  ストレージクラスタが指定された NTP サーバと通信できません。

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

- * ntpTimeNotInSync *

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

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

- * nvramDeviceStatus *

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

重大度	説明
警告	ハードウェアによって警告が検出されました。この状態は、温度警告などの一時的なものです。 • nvmetimeError • nvmetimeStatus • energySourceLifetimeStatus • energySourceTemperatureStatus • warningThresholdExceeded

エラー	ハードウェアによってエラーまたは重大ステータスが検出されました。クラスタマスターがスライスドライブの処理を中止しようとします（ドライブ削除イベントが生成されます）。セカンダリスライスサービスを使用できない場合、ドライブは削除されません。警告レベルのエラーに加えて返されるエラー： • NVRAM デバイスマウントポイントが存在しません。 • NVRAM デバイスパーティションが存在しません。 • NVRAM デバイスパーティションは存在しますが、マウントされていません。
重要	ハードウェアによってエラーまたは重大ステータスが検出されました。クラスタマスターがスライスドライブの処理を中止しようとします（ドライブ削除イベントが生成されます）。セカンダリスライスサービスを使用できない場合、ドライブは削除されません。 • 永続性ホスト • armStatusSaveNArmed • csaveStatusError

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

- * powerSupplyError *

  このクラスタ障害は、次のいずれかの状態を示します。

  - 電源装置がありません。
  - 電源装置で障害が発生しました。
  - 電源装置の入力が見つからないか、範囲外です。この問題を解決するには、冗長電源がすべてのノードに供給されていることを確認してください。ネットアップサポートにお問い合わせください。

- * provisionedSpaceTooFull*

  クラスタのプロビジョニング済み容量がいっぱいです。

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

- * 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てください。

- * remoteRepClusterFull *

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

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

- * remoteRepSnapshotClusterFull *

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

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

- * remoteRepSnapshotsExceededLimit *

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

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

- * scheduleActionError *

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

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

- * sensorReadingFailed*

  ベースボード管理コントローラ（ BMC ）のセルフテストに失敗したか、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 *

  必要なサービスが実行されていません。

  ネットアップサポートにお問い合わせください。

- * siceServiceTooFull*

  スライスサービスに割り当てられたプロビジョニング済み容量が少なすぎます。

  この問題を解決するには、プロビジョニング済み容量を追加してください。

- * sliceServiceUnhealthy * が表示されます

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

  - 重大度 = 警告：対処は行われません。この警告期間は 6 分後に終了します。
  - 重大度 = エラー：データの運用停止処理が自動的に実行され、他の正常なドライブにデータが再レプ

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

- * sshEnabled *

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

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

- * sslCertificateExpiration*

  このノードに関連付けられている SSL 証明書の有効期限が近づいているか、期限が切れています。この問題では、緊急性に基づいて次の重大度が使用されます。

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

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

- * strandedCapacity *

  1 つのノードがストレージクラスタの容量の半分を超えています。

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

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

- * tempSensor *

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

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

- * アップグレード *

  アップグレードが 24 時間以上実行中です。

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

- * 無対応サービス *

  サービスが応答しなくなりました。

  ネットアップサポートにお問い合わせください。

- * virtualNetworkConfig *

  このクラスタ障害は、次のいずれかの状態を示します。

  - インターフェイスが存在しません。
  - インターフェイス上のネームスペースが正しくありません。
  - ネットマスクが正しくありません。
  - IP アドレスが正しくありません。
  - インターフェイスが稼働していません。
  - ノード上に不要なインターフェイスがあります。ネットアップサポートにお問い合わせください。

- * volumesDegraded *

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

- * volumesOffline *

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

  ネットアップサポートにお問い合わせください。

ノードのパフォーマンスアクティビティを表示します

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 、 1 秒あたりの読み取り / 書き込み I/O 処理数（ IOPS ）のリアルタイムの統計がグラフに表示されます。利用率グラフは 5 秒ごとに更新され、ドライブの統計グラフは 10 秒ごとに更新されます。

1. [* クラスタ > ノード *] をクリックします。
2. 表示するノードの * アクション * をクリックします。
3. [* 詳細の表示 *] をクリックします。

> ⓘ 折れ線グラフおよび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。

ボリュームのパフォーマンスを表示します

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表示できます。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。

ページ上のパフォーマンス情報を更新する頻度を変更するには、 [* Refresh Every *] リストをクリックし、別の値を選択します。クラスタのボリューム数が 1 、 000 個未満の場合、デフォルトの更新間隔は 10 秒です。それ以外の場合は 60 秒です。[なし] の値を選択すると、自動ページ更新は無効になります。

自動更新を再度有効にするには、 * 自動更新を有効にする * をクリックします。

1. Element UI で、 * Reporting * > * Volume Performance * を選択します。
2. ボリュームリストで、ボリュームの操作アイコンをクリックします。
3. [* 詳細の表示 *] 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. ボリュームの詳細情報を表示するには、 * 詳細を表示 * 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。

詳細については、こちらをご覧ください

ボリュームのパフォーマンスの詳細

ボリュームのパフォーマンスの詳細

ボリュームのパフォーマンス統計は、 Element UI の Reporting タブの Volume Performance ページで確認できます。

表示され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 。
- * 名前 *

  ボリュームの作成時に指定した名前。
- * アカウント *

  ボリュームに割り当てられているアカウントの名前。
- * アクセスグループ *

  ボリュームアクセスグループまたはボリュームが属するグループの名前。
- * ボリューム使用率 *

  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

- 0 ：クライアントはボリュームを使用していません
- 100 ：クライアントは最大値まで使用しています
- >100 ：クライアントはバースト値を使用しています

- * 合計 IOPS *

  ボリュームに対して実行中の IOPS （読み取りおよび書き込み）の総数。

- * 読み取り IOPS *

  ボリュームに対して実行中の読み取り IOPS の総数。

- * 書き込み IOPS *

  ボリュームに対して実行中の書き込み IOPS の総数。

- * 合計スループット *

  ボリュームに対して実行中のスループット（読み取りおよび書き込み）の総量。

- * 読み取りスループット *

  ボリュームに対して実行中の読み取りスループットの総量。

- * 書き込みスループット *

  ボリュームに対して実行中の書き込みスループットの総量。

- * 合計レイテンシ *

  ボリュームに対する読み取り処理と書き込み処理が完了するまでの平均時間（マイクロ秒）。

- * 読み取り遅延 *

  過去 500 ミリ秒の、ボリュームへの読み取り処理を完了するまでの平均時間（マイクロ秒）。

- * 書き込みレイテンシー *

  過去 500 ミリ秒の、ボリュームへの書き込み処理を完了するまでの平均時間（マイクロ秒）。

- * キュー深度 *

  ボリュームに対する未処理の読み取り処理と書き込み処理の数。

- * 平均 IO サイズ *

  直近 500 ミリ秒の、ボリュームへの最新の I/O の平均サイズ（バイト）。

iSCSI セッションを表示します

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。

1. Element UI で、 * Reporting * > * iSCSI Sessions * を選択します。
2. フィルタ条件フィールドを表示するには、 * フィルタ * をクリックします。

詳細については、こちらをご覧ください

iSCSI セッションの詳細

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表示できます。

次に、 iSCSI セッションに関する情報を示します。

- * ノード *

  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。

- * アカウント *

  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。

- * 音量 *

  ノードでのボリュームの識別名。

- * ボリューム ID *

  ターゲット IQN に関連付けられたボリュームの ID 。

- * イニシエータ ID *

  システムによって生成されたイニシエータの ID 。

- * イニシエータエイリアス *

  イニシエータが多数ある場合に特定のイニシエータを見つけやすくするための別名。

- * イニシャル IP *

  セッションを開始するエンドポイントの IP アドレス。

- * イニシエータ IQN *

  セッションを開始するエンドポイントの IQN 。

- * ターゲット IP *

ボリュームをホストしているノードの IP アドレス。

- * ターゲット IQN *

  ボリュームの IQN 。

- * 上に作成されました

  セッションが確立された日付。

Fibre Channel セッションを表示します

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。

1. Element UI で、 * Reporting * > * FC Sessions * を選択します。
2. フィルタ条件フィールドを表示するには、 * フィルタ * をクリックします。

詳細については、こちらをご覧ください

Fibre Channel セッションの詳細

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 セッションに関する情報は次のとおりです。

- * ノード ID *

  接続のセッションをホストしているノード。

- * ノード名 *

  システムによって生成されたノード名。

- * イニシエータ ID *

  システムによって生成されたイニシエータの ID 。

- * イニシエータ WWPN *

  イニシエータの World Wide Port Name 。

- * イニシエータエイリアス *

  イニシエータが多数ある場合に特定のイニシエータを見つけやすくするための別名。

- * ターゲット WWPN *

ターゲットの World Wide Port Name 。

- * ボリュームアクセスグループ *

  セッションが属するボリュームアクセスグループの名前。

- * ボリュームアクセスグループ 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の手順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ことを意味します。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く必要があります。

> 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使用されません。ドライブで障害が発生すると、次のイベントが発生します。

- データはドライブから移行されます。
- 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。

> 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。

を参照してください。

- クラスタから障害ドライブを削除します
- 基本的な MDSS ドライブのトラブルシューティング
- MDSS ドライブを削除します
- "SolidFire ストレージノードのドライブの交換"

- "H600S シリーズストレージノードのドライブの交換"
- "H410S および H610S ハードウェアの情報"
- "SF シリーズハードウェアの情報"

クラスタから障害ドライブを削除します

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、 SolidFire システムはドライブを障害状態にします。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。

ノードがオフラインの場合、 * Alerts * list のドライブは * blockバ ジ * 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。

1. Element UI で、 * Cluster * > * Drives * を選択します。
2. [Failed （失敗）] をクリックして、障害が発生した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際に必要になります。

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
個々のドライブを削除する場合	a. 削除するドライブの * アクション * をクリックします。 b. [削除（ Remove ）] をクリックします。
複数のドライブを削除する	a. 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。 b. [削除（ 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、その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、問題を修正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に障害が発生した

- 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。

> 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** に障害が発生した

- 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** に障害が発生した

- 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 available 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

- スロット 0 （または内部）とスロット 2 のドライブがアクティブドライブのリストでメタデータドライブとして識別されてい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。

を参照してください。

MDSS ドライブを追加します

MDSS ドライブを追加します

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、 Multi-Drive Slice Service （ MDSS ；マルチドライブスライスサービス）機能を有効にします。この機能を有効にする場合は、ネットアップサポートにお問い合わせください。

スライスドライブを available 状態にするためには、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する必要があります。スロット 2 のドライブを追加する際、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。

1. [* クラスタ > ドライブ *] をクリックします。
2. 使用可能なドライブのリストを表示するには、 * Available * をクリックします。
3. 追加するスライスドライブを選択します。
4. [一括操作 *] をクリックします。
5. [追加（ Add ）] をクリックします。
6. ドライブが追加されたことを「 * Active Drives * 」（アクティブドライブ * ）タブで確認します。

MDSS ドライブを削除します

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。この手順は、ノードに複数のスライスドライブがある場合にのみ適用されます。

> 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。

1. [* クラスタ > ドライブ *] をクリックします。
2. [Available * drives] タブで ' 削除するスライス・ドライブのチェック・ボックスをクリックします
3. [一括操作 *] をクリックします。
4. [削除（ 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を行う

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。

  その結果、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。このプロセスにかかる時間は、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問い合わせ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オフするには、 Shutdown API コマンドを使用できます。
- ノードがダウンまたはオフの状態の場合は、ノードを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。

を参照してください。

"障害が発生した SolidFire シャーシの交換"

"H600S シリーズノードに障害が発生した場合の交換"

クラスタの電源をオフにします

クラスタ全体の電源をオフにするには、次の手順 を実行します。

手順

1. （オプション）準備手順の実行については、ネットアップサポートにお問い合わせください。
2. すべてのI/Oが停止していることを確認します。
3. すべてのiSCSIセッションを切断します。
   a. 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。
   b. ノードリストに表示されているノードをメモします。
   c. 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。

> クラスタを再起動するときは、特定の手順に従ってすべてのノードがオンラインになったことを確認する必要があります。
>
> 1. すべての重大度とを確認します `volumesOffline` クラスタの障害が解決されました。
> 2. クラスタが安定するまで10～15分待ちます。
> 3. データにアクセスするためのホストの起動を開始します。
>
> メンテナンス後にノードの電源をオンにして正常であることを確認する時間を長くしたい場合は、データの同期を遅らせて不要なビンの同期を回避する方法についてテクニカルサポートにお問い合わせください。

詳細については、こちらをご覧ください

"NetApp SolidFire / HCIストレージクラスタを正常にシャットダウンして電源をオンにする方法"

ストレージノードのノードユーティリティを使用する

ネットワークの問題をトラブルシューティングする際に、 NetApp Element ソフトウェ

ア UI の標準の監視ツールで十分な情報を得られない場合は、ノードユーティリティを使用できます。ノードユーティリティは、ノード間または管理ノードでのネットワークの問題をトラブルシューティングするために役立つ情報やツールを提供します。

詳細については、こちらをご覧ください

- ノード UI を使用してノード設定にアクセスします
- ネットワーク設定の詳細はノード UI から確認できます
- ノード UI から取得したクラスタ設定の詳細
- ノード UI を使用してシステムテストを実行します
- ノード UI を使用してシステムユーティリティを実行します

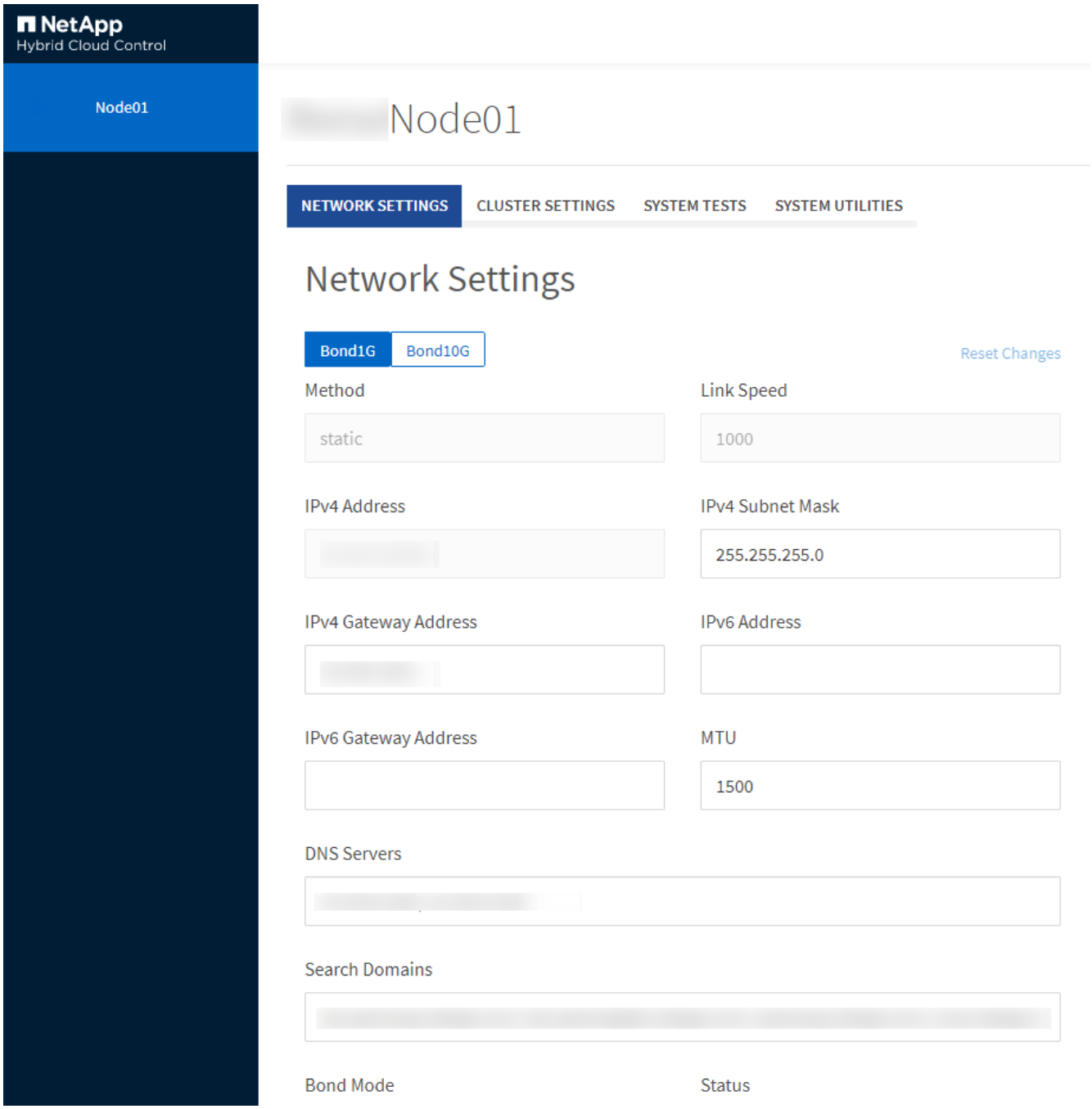
ノード **UI** を使用してノード設定にアクセスします

管理ノードの IP を入力して認証を実行したら、ノード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、システムテストおよびユーティリティにアクセスできます。

クラスタに参加している Active 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。

ノードは一度に 1 つずつ設定または変更してください。別のノードを変更する前に、指定したネットワーク設定が想定どおりに機能し、ネットワークが安定して動作することを確認する必要があります。

1. 次のいずれかの方法でノード UI を開きます。
    - 管理 IP アドレスの末尾に「： 442 」を付加した値をブラウザウィンドウに入力し、管理者ユーザの名前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管理 IP アドレスの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。



ネットワーク設定の詳細はノード **UI** から確認できます

ストレージノードのネットワーク設定を変更して、新しいネットワーク属性を指定できます。

ノードにログインすると、ストレージノードのネットワーク設定が * Network Settings * ページに表示されます (https://<node IP> ： 442/HCC / ノード / ネットワーク設定）。「 * Bond1G * （管理）」または「 * Bond10G * （ストレージ）」のいずれかの設定を選択できます。ストレージノードの状態が Available 、 Pending 、または Active の場合に変更可能な設定は次のとおりです。

- * メソッド *

  インターフェイスの設定に使用する方法。有効な方法：

- 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。

- * リンク速度 *

  仮想 NIC によってネゴシエートされた速度。

- * IPv4 アドレス *

  eth0 ネットワークの IPv4 アドレス。

- * IPv4 サブネットマスク *

  IPv4 ネットワークのアドレス分割。

- * IPv4 ゲートウェイアドレス *

  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 アドレス *

  eth0 ネットワークの IPv6 アドレス。

- * IPv6 ゲートウェイアドレス *

  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 サーバ *

  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。

- * 検索ドメイン *

  システムで使用可能な追加の MAC アドレスを検索します。

- * ボンディング・モード *

  には、次のいずれかのモードを指定できます。

  - ActivePassive （デフォルト）
  - ALB
  - LACP

- * ステータス *

  有効な値は次のとおり

  - UpAndRunning のサービスです
  - 下へ
  - 上へ

- * 仮想ネットワークタグ *

  仮想ネットワークの作成時に割り当てられたタグ。

- * ルート *

  ルートが使用するように設定されている、関連付けられたインターフェイスを介した特定のホストまたはネットワークへのスタティックルート。

ノード **UI** から取得したクラスタ設定の詳細

クラスタの設定およびノードのホスト名の変更後、ストレージノードのクラスタ設定を確認することができます。

ノード UI の「 * Cluster Settings * 」ページで、ストレージノードのクラスタ設定を次の表に示します (https://<node IP> ： 442/HCC / ノード / クラスタ設定）。

- * 役割 *

  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

  - 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。

- * クラスタメンバーシップ *

  ノードの状態。有効な値は次のとおり

  - Available ：ノードにはクラスタ名が関連付けられておらず、まだクラスタに含まれていません。
  - Pending ：設定済みで、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必要ありません。
  - 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。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。

- * アンサンブル *

  データベースアンサンブルに参加しているノード。

- * ノード ID *

  クラスタへの追加時にノードに割り当てられた ID 。

- * クラスタインターフェイス *

  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。

- * ストレージ・インターフェイス *

  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 *

  ノードでドライブ暗号化がサポートされているかどうか。

ノード **UI** を使用してシステムテストを実行します

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、変更内容をテストできます。テストを実行することで、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移行できることを確認できます。

ストレージノードのノード UI にログインしておきます。

1. [システムテスト] をクリックします。
2. 実行するテストの横にある * テストの実行 * をクリックするか、 * すべてのテストを実行 * を選択します。

   すべてのテスト処理には時間がかかるため、ネットアップサポートの指示があった場合にのみ実行してください。

   ◦ * 接続されたアンサンブル * をテストします

   データベースアンサンブルへの接続をテストして検証します。デフォルトでは、ノードが関連付けられたクラスタのアンサンブルを使用します。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。

- * テスト接続 Mvip *

  指定した管理仮想 IP （ MVIP ）アドレスに対して ping を実行してから、 MVIP への簡単な API 呼び出しを実行して接続を検証します。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 MVIP がテストに使用されます。

- * テスト接続 Svip *

  ネットワークアダプタで設定されている Maximum Transmission Unit （ MTU ；最大転送単位）サイズと同じ Internet Control Message Protocol （ ICMP ）パケットを使用して、指定したストレージ仮想 IP （ SVIP ）アドレスに対して 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の SVIP がテストに使用されます。

- * ハードウェア構成のテスト *

  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。これは工場出荷時のテストと同じです。

  > このテストは大量のリソースを消費するため、ネットアップサポートから要求された場合にのみ実行してください。

- * ローカル接続のテスト *

  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。

- * テストクラスタの検索 *

  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。

- * ネットワーク構成のテスト *

  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。

- * ping テスト *

  指定した一連のホストに対して ping を実行し、単純な接続テストを行います。ホストを指定しない場合は、クラスタのすべての登録済みノードのリストが動的に作成され、 ping が実行されます。

- * リモート接続のテスト *

  各ノードでクラスタ IP （ CIP ）に対して ping を実行して、リモートペアクラスタ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 **UI** を使用してシステムユーティリティを実行します

ストレージノードのノード 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実行できます。

ストレージノードのノード UI にログインしておきます。

1. [システムユーティリティ] 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 *

     ノードをリブート、電源再投入、またはシャットダウンします。

     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）が含まれます。
     - Wakeup Delay ：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 *

     ノードの /tmp/bundles ディレクトリ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。
     - Extra Args ：このパラメータが 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。
     - Timeout Sec ：個々の ping 応答を待機する秒数を指定します。
   - * ノードログの削除 *

     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の現在のサポートバンドルを削除します。

   - * ドライブのリセット *

     ドライブを初期化し、ドライブに現在格納されているすべてのデータを削除します。既存のノードまたはアップグレードしたノードでドライブを再利用できます。

     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（ドライブ ID ではない）のリスト。
   - * ネットワーク構成のリセット *

     個々のノードのネットワーク設定の問題を解決し、個々のノードのネットワーク設定を工場出荷時のデフォルト設定にリセットするのに役立ちます。

   - * ノードのリセット *

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、ノードのネットワーク設定はこの処理の実行中も保持されます。ノードは、クラスタに割り当てられておらず、使用可能な状態の場合にのみリセットできます。

> 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。

◦ * ネットワークを再起動 *

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。

> この処理を実行すると、原因によってネットワーク接続が一時的に失われる可能性が

◦ * サービスを再起動 *

ノードで Element ソフトウェアサービスを再起動します。

> この処理を実行すると、原因の一時的なノードサービスが中断されるこの処理は、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。

- service ：再起動するサービス名。
- アクション：サービスに対して実行するアクション。オプションには、開始、停止、再起動があります。

管理ノードを操作します

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、システム監視用の Active IQ の設定、トラブルシューティング用のネットアップサポートアクセスの有効化に使用できます。

> ベストプラクティスとして、 1 つの管理ノードを 1 つの VMware vCenter インスタンスに関連付けるだけで、同じストレージリソースおよびコンピューティングリソースまたは vCenter インスタンスを複数の管理ノードに定義することは避けてください。

を参照してください "管理ノードのドキュメント" を参照してください。

クラスタフルレベルを把握

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 つのレベルがあり、いずれも NetApp Element UI に表示されます。警告、エラー、重大の 3 つです。

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。クラスタフルの重大度レベルは、 Element UI のアラート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。

- * 警告 *

  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。

- * エラー *

  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、クラスタが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。

- * 重要 *

  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または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。クラスタメタデータのストレージフルは、 Element UI の Reporting タブの概要ページの 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。

- * 警告 *

  ユーザが設定可能な警告で、クラスタのメタデータ容量が 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 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。

- * エラー *

  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、クラスタが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。

- * 重要 *

  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または追加する必要があります。

環境の 2 ノードクラスタの次のしきい値。

- メタデータの使用率エラーは、この値よりも 20% 低くなっています。
- ブロックフルエラーは、ブロックドライブ（未使用の容量を含む）が重大より 1 本低くなっているため、ブロックドライブ 2 本分の容量は重要度よりも低くなります。

著作権に関する情報

商標に関する情報