システムを管理する
Element Software

NetApp
November 12, 2025

目次

システムを管理する

システムを管理する

Element UI でシステムを管理できます。これには、多要素認証の有効化、クラスター設定の管理、連邦情報処理標準 (FIPS) のサポート、外部キー管理の使用が含まれます。

- "多要素認証を有効にする"
- "クラスター設定を構成する"
- "FIPSドライブをサポートするクラスタを作成する"
- "外部キー管理を始める"

詳細情報

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

多要素認証を有効にする

多要素認証を設定する

多要素認証 (MFA) は、セキュリティアサーションマークアップ言語 (SAML) を介してサードパーティの ID プロバイダー (IdP) を使用してユーザーセッションを管理します。MFA を使用すると、管理者は必要に応じて、パスワードとテキスト メッセージ、パスワードと電子メール メッセージなどの追加の認証要素を構成できます。

Element API 経由でこれらの基本的な手順を使用して、多要素認証を使用するようにクラスターを設定できます。

各APIメソッドの詳細については、 "要素APIリファレンス"。

1. 次の API メソッドを呼び出して、IdP メタデータを JSON 形式で渡すことで、クラスターの新しいサードパーティ ID プロバイダー (IdP) 構成を作成します。 `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 で正しくフォーマットされていることを確認するため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数多くあります。例えば、次のとおりです。https://freeformatter.com/json-escape.html.

2. 次の API メソッドを呼び出して、spMetadataUrl を介してクラスター メタデータを取得し、サードパーティの IdP にコピーします。 `ListIdpConfigurations`

   spMetadataUrl は、信頼関係を確立するために IdP のクラスターからサービス プロバイダー メタデータを取得するために使用される URL です。

3. 監査ログとシングル ログアウトが適切に機能するために、ユーザーを一意に識別するための “NameID” 属

性を含めるようにサードパーティの IdP で SAML アサーションを構成します。

4. 次の API メソッドを呼び出して、承認のためにサードパーティの IdP によって認証された 1 つ以上のクラスター管理者ユーザー アカウントを作成します。`AddIdpClusterAdmin`

   次の例に示すように、目的の効果を得るには、IdP クラスタ管理者のユーザー名が SAML 属性の名前/値のマッピングと一致する必要があります。

   - email=bob@company.com - ここで、IdP は SAML 属性で電子メール アドレスを解放するように構成されています。
   - group=cluster-administrator - ここで、IdP は、すべてのユーザー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構成されます。セキュリティ上の理由から、SAML 属性の名前と値のペアでは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、クラスターの MFA を有効にします。 `EnableIdpAuthentication`

詳細情報の参照

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

多要素認証に関する追加情報

多要素認証に関しては、次の注意事項に注意する必要があります。

- 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ーを使用して次の API メソッドを呼び出す必要があります。 `UpdateIdpConfiguration`
- MFA は、長さが 2048 ビット未満の証明書とは互換性がありません。デフォルトでは、クラスター上に 2048 ビットの SSL 証明書が作成されます。 API メソッドを呼び出すときは、小さいサイズの証明書の設定を避ける必要があります。 `SetSSLCertificate`

  アップグレード前にクラスターが 2048 ビット未満の証明書を使用している場合は、Element 12.0 以降にアップグレードした後、クラスター証明書を 2048 ビット以上の証明書に更新する必要があります。

- IdP 管理ユーザーは、API 呼び出しを直接行うために使用することはできません (たとえば、SDK または Postman 経由)。また、他の統合 (たとえば、OpenStack Cinder または vCenter プラグイン) に使用することもできません。これらの権限を持つユーザーを作成する必要がある場合は、LDAP クラスター管理者ユーザーまたはローカル クラスター管理者ユーザーのいずれかを追加します。

詳細情報の参照

- "Element API によるストレージの管理"
- "SolidFireおよびElementソフトウェアのドキュメント"
- "vCenter Server 用NetApp Elementプラグイン"

クラスター設定を構成する

クラスタの保存時の暗号化を有効または無効にする

SolidFireクラスターを使用すると、クラスター ドライブに保存されているすべての保存データを暗号化できます。自己暗号化ドライブ（SED）のクラスタ全体の保護を有効にするには、次のいずれかを使用します。"保存時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、保存時のハードウェア暗号化を有効にすることができます。保存時のハードウェア暗号化機能を有効にしても、クラスターのパフォーマンスや効率には影響しません。保存時のソフトウェア暗号化は、Element API のみを使用して有効にできます。

保存時のハードウェアベースの暗号化は、クラスターの作成時にはデフォルトでは有効になっていませんが、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 クラスターの場合、保存時のソフトウェア暗号化はクラスターの作成中に有効にする必要があり、クラスターの作成後は無効にすることはできません。

要件

- 暗号化設定を有効化または変更するためのクラスタ管理者権限があります。
- 保存時のハードウェアベースの暗号化の場合、暗号化設定を変更する前に、クラスター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、ドライブ上の暗号化を無効にするキーにアクセスするために、2 つのノードがクラスターに参加している必要があります。

保存時の暗号化ステータスを確認する

クラスタ上の保存時の暗号化および/または保存時のソフトウェア暗号化の現在の状態を確認するには、"クラスター情報を取得"方法。使用することができます"ソフトウェア暗号化情報を取得する"クラスターが保存データの暗号化に使用する情報を取得する方法。

> ElementソフトウェアUIダッシュボード `https://<MVIP>/`現在、ハードウェアベースの暗号化の保存時の暗号化ステータスのみが表示されます。

オプション

- [保存時にハードウェアベースの暗号化を有効にする]
- [保存時のソフトウェアベースの暗号化を有効にする]
- [保存時のハードウェアベースの暗号化を無効にする]

保存時にハードウェアベースの暗号化を有効にする

> 外部キー管理設定を使用して保存時の暗号化を有効にするには、"API" 。既存の Element UI ボタンを使用して有効にすると、内部で生成されたキーの使用に戻ります。

1. Element UI から、クラスター > 設定 を選択します。
2. *保存時の暗号化を有効にする*を選択します。

保存時のソフトウェアベースの暗号化を有効にする

保存時のソフトウェア暗号化は、クラスターで有効にした後は無効にできません。

1. クラスターの作成中に、"クラスター作成方法"と `enableSoftwareEncryptionAtRest`に設定 `true。

保存時のハードウェアベースの暗号化を無効にする

1. Element UI から、クラスター > 設定 を選択します。
2. *保存時の暗号化を無効にする*を選択します。

詳細情報の参照

- "SolidFireおよびElementソフトウェアのドキュメント"
- "NetApp SolidFireおよび Element 製品の以前のバージョンのドキュメント"

クラスターのフルしきい値を設定する

以下の手順を使用して、システムがブロック クラスターの満杯警告を生成するレベルを変更できます。さらに、ModifyClusterFullThreshold API メソッドを使用して、システムが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することもできます。

要件

クラスタ管理者の権限が必要です。

手順

1. クラスター > *設定*をクリックします。
2. [クラスター フル設定] セクションで、[**Helix** がノード障害から回復できなくなる前に、残りの容量が **_%** の場合に警告アラートを生成する] にパーセンテージを入力します。
3. *変更を保存*をクリックします。

詳細情報の参照

"要素のブロックスペースしきい値はどのように計算されるか"

ボリューム負荷分散の有効化と無効化

Element 12.8 以降では、ボリューム負荷分散を使用して、QoS ポリシーで構成された最小 IOPS ではなく、各ボリュームの実際の IOPS に基づいてノード間でボリュームを分散できます。デフォルトでは無効になっているボリューム負荷分散を、Element UI または API を使用して有効または無効にすることができます。

手順

1. クラスター > *設定*を選択します。
2. クラスター固有セクションで、ボリューム負荷分散のステータスを変更します。

   ボリューム負荷分散を有効にする

   実際の **IOPS** で負荷分散を有効にする を選択し、選択内容を確認します。

   ボリューム負荷分散を無効にする:

   実際の **IOPS** で負荷分散を無効にする を選択し、選択を確認します。

3. 必要に応じて、レポート > 概要 を選択して、実際の IOPS のバランスのステータスの変更を確認します。ステータスを表示するには、クラスターのヘルス情報を下にスクロールする必要がある場合があります。

詳細情報の参照

- "APIを使用してボリューム負荷分散を有効にする"
- "APIを使用してボリューム負荷分散を無効にする"
- "ボリュームQoSポリシーの作成と管理"

サポートアクセスを有効または無効にする

サポート アクセスを有効にすると、 NetAppサポート担当者がトラブルシューティングのために SSH 経由でストレージ ノードに一時的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、クラスター管理者権限が必要です。

1. クラスター > *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。

利用規約バナーを管理する

ユーザーへのメッセージを含むバナーを有効化、編集、または構成できます。

オプション

[利用規約バナーを有効にする] [利用規約バナーを編集する] [利用規約バナーを無効にする]

利用規約バナーを有効にする

ユーザーが Element UI にログインしたときに表示される利用規約バナーを有効にすることができます。ユーザーがバナーをクリックすると、クラスターに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。バナーはいつでも閉じることができます。

利用規約機能を有効にするには、クラスター管理者の権限が必要です。

1. ユーザー > *利用規約*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 ボックスに表示されるテキストを入力します。

   4096文字を超えないでください。

3. *有効*をクリックします。

利用規約バナーを編集する

ユーザーが利用規約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。

要件

- 利用規約を構成するには、クラスター管理者の権限が必要です。
- 利用規約機能が有効になっていることを確認します。

手順

1. ユーザー > *利用規約*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。

   4096文字を超えないでください。

3. *変更を保存*をクリックします。

利用規約バナーを無効にする

利用規約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、Element UI を使用するときにユーザーは利用規約に同意する必要がなくなります。

要件

- 利用規約を構成するには、クラスター管理者の権限が必要です。
- 利用規約が有効になっていることを確認してください。

手順

1. ユーザー > *利用規約*をクリックします。
2. *無効*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する

クラスタがクエリを実行するネットワークタイムプロトコルサーバを構成する

クラスター内の各ノードに、ネットワーク タイム プロトコル (NTP) サーバーに更新を照会するように指示できます。クラスターは構成されたサーバーにのみ接続し、そこから NTP 情報を要求します。

NTP はネットワーク上で時計を同期するために使用されます。内部または外部の NTP サーバーへの接続は、初期のクラスター セットアップの一部である必要があります。

クラスター上の NTP をローカル NTP サーバーを指すように構成します。 IP アドレスまたは FQDN ホスト名を使用できます。クラスター作成時のデフォルトの NTP サーバーは us.pool.ntp.org に設定されていますが、SolidFireクラスターの物理的な場所によっては、このサイトへの接続が常に確立されるとは限りません。

FQDN を使用するかどうかは、個々のストレージ ノードの DNS 設定が適切に実行され、動作しているかどうかによって異なります。これを行うには、すべてのストレージ ノードで DNS サーバーを構成し、「ネットワーク ポート要件」ページを確認してポートが開いていることを確認します。

最大 5 つの異なる NTP サーバーを入力できます。

IPv4 アドレスと IPv6 アドレスの両方を使用できます。

要件

この設定を構成するには、クラスタ管理者の権限が必要です。

手順

1. サーバー設定で IP および/または FQDN のリストを構成します。
2. ノード上で DNS が適切に設定されていることを確認します。
3. クラスター > *設定*をクリックします。
4. [ネットワーク タイム プロトコル設定] で、標準の NTP 構成を使用する いいえ を選択します。
5. *変更を保存*をクリックします。

詳細情報の参照

- "NTPブロードキャストをリッスンするようにクラスタを構成する"
- "SolidFireおよびElementソフトウェアのドキュメント"
- "vCenter Server 用NetApp Elementプラグイン"

NTPブロードキャストをリッスンするようにクラスタを構成する

ブロードキャスト モードを使用すると、クラスター内の各ノードに、特定のサーバーからのネットワーク タイム プロトコル (NTP) ブロードキャスト メッセージをネットワーク上でリッスンするように指示できます。

NTP はネットワーク上で時計を同期するために使用されます。内部または外部の NTP サーバーへの接続は、初期のクラスター セットアップの一部である必要があります。

要件

- この設定を構成するには、クラスタ管理者の権限が必要です。
- ネットワーク上の NTP サーバーをブロードキャスト サーバーとして構成する必要があります。

手順

1. クラスター > *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 サーバーをサーバー リストに入力します。
3. ネットワーク タイム プロトコル設定で、ブロードキャスト クライアントを使用するには はい を選択します。
4. ブロードキャスト クライアントを設定するには、[サーバー] フィールドに、ブロードキャスト モードで設定した NTP サーバーを入力します。
5. *変更を保存*をクリックします。

詳細情報の参照

- "クラスタがクエリを実行するネットワークタイムプロトコルサーバを構成する"
- "SolidFireおよびElementソフトウェアのドキュメント"
- "vCenter Server 用NetApp Elementプラグイン"

SNMPの管理

SNMPの詳細

クラスターで簡易ネットワーク管理プロトコル (SNMP) を構成できます。

SNMP リクエスタを選択し、使用する SNMP のバージョンを選択し、SNMP ユーザーベース セキュリティ モデル (USM) ユーザーを識別し、 SolidFireクラスターを監視するためのトラップを設定できます。管理情報ベース ファイルを表示したりアクセスしたり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

クラスター 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できる 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 を有効にした後、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、バージョン 3 を使用する場合は USM ユーザーを設定できます。

- **SNMP**トラップ設定

  捕獲したいトラップを識別できます。トラップ受信者ごとにホスト、ポート、コミュニティ文字列を設定できます。

SNMPリクエスタを構成する

SNMP バージョン 2 が有効になっている場合は、リクエスタを有効または無効にしたり、承認された SNMP 要求を受信するようにリクエスタを構成したりできます。

1. メニュー：クラスタ[SNMP]をクリックします。
2. *一般SNMP設定*で*はい*をクリックしてSNMPを有効にします。
3. *バージョン*リストから*バージョン 2*を選択します。
4. *リクエスタ*セクションで、*コミュニティ文字列*と*ネットワーク*の情報を入力します。

   デフォルトでは、コミュニティ文字列は public で、ネットワークは localhost です。これらのデフォルト設定を変更できます。

5. オプション: 別のリクエスタを追加するには、[リクエスタの追加] をクリックし、[コミュニティ文字列] と [ネットワーク] 情報を入力します。
6. *変更を保存*をクリックします。

詳細情報の参照

- 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する

SNMP USMユーザーを構成する

SNMP バージョン 3 を有効にする場合は、承認された SNMP 要求を受信するように USM ユーザーを構成する必要があります。

1. クラスター > **SNMP** をクリックします。
2. *一般SNMP設定*で*はい*をクリックしてSNMPを有効にします。
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** ユーザー セクションで、名前、パスワード、パスフレーズを入力します。
5. オプション: 別の USM ユーザーを追加するには、[**USM** ユーザーの追加] をクリックし、名前、パスワード、パスフレーズを入力します。
6. *変更を保存*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、通知とも呼ばれる SNMP トラップを使用して、 SolidFireクラスターの健全性を監視できます。

SNMP トラップが有効になっている場合、 SolidFireクラスターはイベント ログ エントリとシステム アラートに関連付けられた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特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. クラスター > **SNMP** をクリックします。
2. **SNMP** トラップ設定 セクションで、システムが生成するトラップの種類を 1 つ以上選択します。
   - クラスター障害トラップ
   - クラスター解決障害トラップ

◦ クラスターイベントトラップ

3. *トラップ受信者*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文字列情報を入力します。
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、ホスト、ポート、およびコミュニティ文字列の情報を入力します。
5. *変更を保存*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する

各管理対象オブジェクトを定義するために使用される管理情報ベース (MIB) ファイルを表示およびダウンロードできます。 SNMP 機能は、 SolidFire-StorageCluster-MIB で定義されたオブジェクトへの読み取り専用アクセスをサポートします。

MIB で提供される統計データは、次のシステム アクティビティを示します。

- クラスター統計
- ボリューム統計
- アカウント統計別の取引量
- 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

システムは、SF シリーズ製品への上位レベル アクセス ポイント (OIDS) を含む MIB ファイルへのアクセスもサポートします。

手順

1. クラスター > **SNMP** をクリックします。
2. **SNMP MIB** の下で、ダウンロードする MIB ファイルをクリックします。
3. 表示されるダウンロード ウィンドウで、MIB ファイルを開くか保存します。

ドライブの管理

各ノードには、クラスターのデータの一部を保存するために使用される 1 つ以上の物理ドライブが含まれています。ドライブがクラスターに正常に追加された後、クラスターはドライブの容量とパフォーマンスを活用します。 Element UI を使用してドライブを管理できます。

ドライブの詳細

[クラスター] タブの [ドライブ] ページには、クラスター内のアクティブなドライブの一覧が表示されます。 [アクティブ]、[使用可能]、[削除中]、[消去中]、[失敗] タブから選択してページをフィルターできます。

クラスターを初めて初期化すると、アクティブ ドライブ リストは空になります。新しいSolidFireクラスターが作成された後に、クラスターに割り当てられておらず、[使用可能] タブにリストされているドライブを追加できます。

アクティブ ドライブのリストには次の要素が表示されます。

- ドライブ**ID**

  ドライブに割り当てられた連続番号。

- ノード**ID**

  ノードがクラスターに追加されるときに割り当てられるノード番号。

- 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。

- 残り摩耗

  摩耗レベルインジケーター。

  ストレージ システムは、データの書き込みと消去に使用できる各ソリッド ステート ドライブ (SSD) のおおよその摩耗量を報告します。設計された書き込みおよび消去サイクルの 5 パーセントを消費したドライブは、95 パーセントの摩耗が残っていると報告されます。システムはドライブの摩耗情報を自動的に更新しません。情報を更新するには、ページを更新するか、閉じて再読み込みしてください。

- タイプ

  ドライブの種類。タイプはブロックまたはメタデータのいずれかになります。

詳細情報

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

ノードの管理

ノードの管理

「クラスター」タブの「ノード」ページから、 SolidFireストレージおよびファイバー チャネル ノードを管理できます。

新しく追加されたノードがクラスターの総容量の 50% 以上を占める場合、このノードの容量の一部は使用不可 (「取り残される」) になり、容量ルールに準拠します。ストレージが追加されるまで、この状態は続きま

す。容量ルールにも従わない非常に大きなノードが追加された場合、以前に取り残されていたノードは取り残されなくなりますが、新しく追加されたノードは取り残されます。このような事態を回避するには、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、適切なクラスター障害がスローされます。

詳細情報の参照

クラスターにノードを追加する

クラスターにノードを追加する

追加のストレージが必要になったとき、またはクラスターの作成後に、クラスターにノードを追加できます。ノードは、初めて電源を入れるときに初期構成が必要です。ノードが設定されると、保留中のノードのリストに表示され、クラスターに追加できるようになります。

クラスター内の各ノードのソフトウェア バージョンは互換性がある必要があります。クラスタにノードを追加すると、クラスタは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 バージョンをインストールします。

既存のクラスターに、より小さい容量またはより大きい容量のノードを追加できます。容量の拡張を可能にするために、クラスターにさらに大きなノード容量を追加できます。小さなノードが含まれるクラスターに、大きなノードを追加する場合は、ペアで追加する必要があります。これにより、大規模なノードの 1 つに障害が発生した場合でも、Double Helix がデータを移動するのに十分なスペースが確保されます。パフォーマンスを向上させるために、より大きなノード クラスターに小さなノード容量を追加できます。

新しく追加されたノードがクラスターの総容量の 50% 以上を占める場合、このノードの容量の一部は使用不可 (「取り残される」) になり、容量ルールに準拠します。ストレージが追加されるまで、この状態は続きます。容量ルールにも従わない非常に大きなノードが追加された場合、以前に取り残されていたノードは取り残されなくなりますが、新しく追加されたノードは取り残されます。このような事態を回避するには、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、strandedCapacity クラスター障害がスローされます。

"NetApp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. クラスター > *ノード*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、「保留中」をクリックします。

   ノードの追加プロセスが完了すると、アクティブ ノード リストに表示されます。それまでは、保留中のノードは「保留中のアクティブ」リストに表示されます。

   SolidFire は、保留中のノードをクラスターに追加すると、そのクラスターの Element ソフトウェア バージョンを保留中のノードにインストールします。これには数分かかる場合があります。

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 アクション アイコンをクリックします。
   - 複数のノードを追加するには、追加するノードのチェックボックスをオンにして、[一括操作] を選択します。 注: 追加するノードに、クラスターで実行されているバージョンとは異なるバージョンの

Element ソフトウェアがある場合、クラスターは、クラスター 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ノードを非同期的に更新します。ノードが更新されると、ノードは自動的にクラスターに追加されます。この非同期プロセス中、ノードは pendingActive 状態になります。

4. *[追加]*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。

詳細情報の参照

ノードのバージョン管理と互換性

ノードのバージョン管理と互換性

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いています。 Element ソフトウェア ベースのストレージ クラスターは、ノードとクラスターのバージョンに互換性がない場合、自動的にノードをクラスター上の Element ソフトウェア バージョンにイメージ化します。

次のリストは、Element ソフトウェア バージョン番号を構成するソフトウェア リリースの重要度レベルを示しています。

- 選考科目

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

- マイナー

  2 番目の番号は、メジャー リリースに追加された小さなソフトウェア機能または既存のソフトウェア機能の拡張機能を指定します。このコンポーネントはメジャー バージョン コンポーネント内で増分され、この増分リリースが、異なるマイナー コンポーネントを持つ他の Element ソフトウェア増分リリースと互換性がないことを示します。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

  3 番目の数字は、major.minor コンポーネントによって表される Element ソフトウェア バージョンに対する互換性のあるパッチ (増分リリース) を指定します。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。

互換性を保つには、メジャー バージョン番号とマイナー バージョン番号が一致している必要があります。マイクロ番号は互換性のために一致する必要はありません。

混合ノード環境におけるクラスタ容量

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

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。

暗号化されていないノードと暗号化されたノードを混在させないことが最善です。混合ノード クラスターでは、どのノードもクラスターの合計容量の 33% を超えることはできません。たとえば、SF シリーズ 4805 ノードが 4 つあるクラスターでは、単独で追加できる最大のノードは SF シリーズ 9605 です。クラスター容量のしきい値は、この状況で最大のノードが失われる可能性に基づいて計算されます。

Element ソフトウェアのバージョンによっては、次の SF シリーズ ストレージ ノードはサポートされません。

バージョン	ストレージ ノードはサポートされていません...
要素12.8	• SF4805 • SF9605 • SF19210 • SF38410
要素12.7	• SF2405 • SF9608
要素12.0	• SF3010 • SF6010 • SF9010

これらのノードのいずれかをサポートされていない Element バージョンにアップグレードしようとすると、ノードが Element 12.x 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

サービス タグ、ドライブの詳細、使用率とドライブの統計のグラフなど、個々のノードの詳細を表示できます。 [クラスター] 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. クラスター > *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 アクション アイコンをクリックします。
3. *詳細を表示*をクリックします。
4. ノードの詳細を確認します。
   - ノード **ID**: ノードのシステム生成 ID。
   - ノード名: ノードのホスト名。
   - ノード ロール: クラスター内でのノードの役割。有効な値は次のとおりです。
     - クラスター マスター: クラスター全体の管理タスクを実行し、MVIP と SVIP を含むノード。
     - アンサンブル ノード: クラスターに参加するノード。クラスターのサイズに応じて、3 つまたは 5

つのアンサンブル ノードが存在します。

- ファイバー チャネル: クラスター内のノード。

- ノード タイプ: ノードのモデル タイプ。
- アクティブ ドライブ: ノード内のアクティブ ドライブの数。
- ノード使用率: nodeHeat に基づくノード使用率のパーセンテージ。表示される値は、centrethPrimaryTotalHeat のパーセンテージです。 Element 12.8 以降で使用可能です。
- 管理 **IP**: 1GbE または 10GbE ネットワーク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。
- クラスター **IP**: 同じクラスター内のノード間の通信に使用される、ノードに割り当てられたクラスター IP (CIP) アドレス。
- ストレージ **IP**: iSCSI ネットワーク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るノードに割り当てられたストレージ IP (SIP) アドレス。
- 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。
- バージョン: 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 レプリケーション用のノードで使用されるポート。
- サービス タグ: ノードに割り当てられた一意のサービス タグ番号。
- カスタム保護ドメイン: ノードに割り当てられたカスタム保護ドメイン。

ファイバーチャネルポートの詳細を表示

FC ポート ページでは、ファイバー チャネル ポートのステータス、名前、ポート アドレスなどの詳細情報を表示できます。

クラスターに接続されているファイバー チャネル ポートに関する情報を表示します。

手順

1. クラスター > **FC** ポート 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。
   - ノード **ID**: 接続のセッションをホストするノード。
   - ノード名: システムによって生成されたノード名。
   - スロット: ファイバー 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: ファイバー チャネル ホスト バス アダプタ (HBA) 上の物理ポート。
   - **WWNN**: ワールドワイドノード名。
   - **WWPN**: ターゲットのワールドワイドポート名。
   - スイッチ **WWN**: ファイバー チャネル スイッチのワールド ワイド ネーム。
   - ポート状態: ポートの現在の状態。
   - **nPort ID**: ファイバー チャネル ファブリック上のノード ポート ID。

- 速度: ネゴシエートされたファイバー チャネル速度。有効な値は次のとおりです。
  - 4Gbps
  - 8Gbps
  - 16Gbps

詳細情報の参照

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

仮想ネットワークを管理する

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により、別々の論理ネットワーク上にある複数のクライアント間のトラフィックを 1 つのクラスターに接続できるようになります。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。

詳細情報の参照

- 仮想ネットワークを追加する
- 仮想ルーティングと転送を有効にする
- 仮想ネットワークを編集する
- VRF VLANの編集
- 仮想ネットワークを削除する

仮想ネットワークを追加する

クラスター構成に新しい仮想ネットワークを追加して、Element ソフトウェアを実行しているクラスターへのマルチテナント環境接続を有効にすることができます。

要件

- クラスター ノード上の仮想ネットワークに割り当てられる IP アドレスのブロックを識別します。
- 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されるストレージ ネットワーク IP (SVIP) アドレスを識別します。

この構成では、次の基準を考慮する必要があります。

- VRF 対応でない VLAN では、イニシエーターが SVIP と同じサブネットに存在する必要があります。
- VRF 対応の VLAN では、イニシエータが SVIP と同じサブネットに存在する必要がなく、ルーティングがサポートされます。
- デフォルトの SVIP では、イニシエーターが SVIP と同じサブネットに存在する必要はなく、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、それぞれに仮想ネットワーク IP アドレスが必要になります。新しい仮想ネットワークを作成するときに指定する IP アドレスの数は、クラスター内のノードの数以上である必要があります。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。クラスター内のノードに仮想ネットワーク アドレスを手動で割り当てる必要はありません。

手順

1. クラスター > *ネットワーク*をクリックします。
2. *VLAN の作成*をクリックします。
3. 新しい **VLAN** の作成 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
   - （オプション）説明
4. **IP** アドレス ブロック に、IP アドレス範囲の 開始 **IP** アドレスを入力します。
5. ブロックに含める IP アドレスの数として、IP 範囲の サイズ を入力します。
6. この VLAN に連続しない IP アドレス ブロックを追加するには、[ブロックの追加] をクリックします。
7. *VLAN の作成*をクリックします。

仮想ネットワークの詳細を表示する

手順

1. クラスター > *ネットワーク*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 ネットワークのユーザーが割り当てた一意の名前。
   - **VLAN** タグ: 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: 仮想ルーティングと転送が有効になっているかどうかを示します。
   - 使用される **IP**: 仮想ネットワークに使用される仮想ネットワーク IP アドレスの範囲。

仮想ルーティングと転送を有効にする

仮想ルーティングおよび転送 (VRF) を有効にすると、ルーティング テーブルの複数のインスタンスをルータに存在させ、同時に動作させることができます。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 を作成するときだけです。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. クラスター > *ネットワーク*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 の関連情報を入力します。仮想ネットワークの追加を参照してください。
   b. **VRF** を有効にする チェックボックスを選択します。
   c. オプション: ゲートウェイを入力します。
3. *VLAN の作成*をクリックします。

詳細情報の参照

仮想ネットワークを追加する

仮想ネットワークを編集する

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 タグと SVIP は変更できません。ゲートウェイ属性は、非 VRF VLAN では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 セッションが存在する場合、変更は失敗する可能性があります。

VLAN IP アドレス範囲のサイズを管理するときは、次の制限に注意する必要があります。

- VLAN の作成時に割り当てられた初期 IP アドレス範囲からのみ IP アドレスを削除できます。
- 最初の IP アドレス範囲の後に追加された IP アドレス ブロックを削除することはできますが、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。
- クラスター内のノードによって使用されている IP アドレスを、初期 IP アドレス範囲または IP ブロックから削除しようとすると、操作が失敗する可能性があります。
- 使用中の特定の IP アドレスをクラスター内の他のノードに再割り当てすることはできません。

次の手順で IP アドレス ブロックを追加できます。

1. クラスター > *ネットワーク*を選択します。
2. 編集する VLAN のアクション アイコンを選択します。
3. *編集*を選択します。
4. **VLAN** の編集 ダイアログ ボックスで、VLAN の新しい属性を入力します。
5. 仮想ネットワークに連続しない 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 **KB** 記事へのリンク

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役立つナレッジベースの記事へのリンク。

- "Element クラスタの VLAN にストレージ ノードを追加した後の重複 IP 警告"
- "ElementでどのVLAN IPが使用されており、どのノードにそれらのIPが割り当てられているかを確認する方法"

VRF VLANの編集

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

1. クラスター > *ネットワーク*をクリックします。
2. 編集する VLAN のアクション アイコンをクリックします。
3. *編集*をクリックします。
4. **VLAN** 編集 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. *変更を保存*をクリックします。

仮想ネットワークを削除する

仮想ネットワーク オブジェクトを削除できます。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. クラスター > *ネットワーク*をクリックします。
2. 削除する VLAN のアクション アイコンをクリックします。
3. *削除*をクリックします。
4. メッセージを確認します。

詳細情報の参照

仮想ネットワークを編集する

FIPSドライブをサポートするクラスタを作成する

FIPSドライブ機能用にElementクラスタを準備する

多くの顧客環境におけるソリューションの展開において、セキュリティはますます重要になっています。連邦情報処理標準 (FIPS) は、コンピューターのセキュリティと相互運用性に関する標準です。保存データの FIPS 140-2 認定暗号化は、全体的なセキュリティ ソリューションのコンポーネントです。

FIPS ドライブ機能を有効にする準備をする際には、FIPS ドライブ対応の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。

クラスターは、次の条件に基づいて FIPS ドライブに準拠していると見なされます。

- すべてのドライブは FIPS ドライブとして認定されています。

- すべてのノードは FIPS ドライブ ノードです。
- 保存時の暗号化 (EAR) が有効になっています。
- FIPS ドライブ機能が有効になっています。 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 対応であり、保存時の暗号化が有効になっている必要があります。

保存時の暗号化を有効にする

保存時にクラスター全体の暗号化を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、保存時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. *保存時の暗号化を有効にする*をクリックします。

詳細情報の参照

- クラスターの暗号化を有効または無効にする
- "SolidFireおよびElementソフトウェアのドキュメント"
- "vCenter Server 用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する

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 クラスター内のすべてのノードが FIPS ドライブをサポートする準備ができているかどうかを確認する必要があります。

結果レポートには、次のいずれかのステータスが表示されます。

- なし: ノードは FIPS ドライブ機能をサポートできません。
- 部分的: ノードは FIPS 対応ですが、すべてのドライブが FIPS ドライブではありません。
- 準備完了: ノードは FIPS 対応であり、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 を使用して、次のように入力し、ストレージ クラスター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、準備完了のステータスが表示されなかったノードに注目してください。
3. 準備完了ステータスが表示されなかったノードについては、ドライブが FIPS ドライブ機能をサポートできるかどうかを確認します。
   - Element API を使用して、次のように入力します。 `GetHardwareList`
   - **DriveEncryptionCapabilityType** の値をメモします。 「fips」の場合、ハードウェアは FIPS ドライブ機能をサポートできます。

詳細を見る `GetFipsReport` または `ListDriveHardware` の中で "要素APIリファレンス"。

4. ドライブが FIPS ドライブ機能をサポートできない場合は、ハードウェアを FIPS ハードウェア (ノードまたはドライブのいずれか) に交換します。

詳細情報の参照

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

FIPSドライブ機能を有効にする

FIPSドライブ機能はNetApp Elementソフトウェアを使用して有効にすることができます。 `EnableFeature` API メソッド。

保存時の暗号化はクラスター上で有効にする必要があり、すべてのノードとドライブは FIPS 対応である必要があります。これは、GetFipsReport ですべてのノードの準備完了ステータスが表示されるときに示されます。

手順

1. Element API を使用して、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
```

詳細情報の参照

- "Element APIで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 用NetApp Elementプラグイン"

FIPSドライブのステータスを確認する

NetApp Elementソフトウェアを使用して、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できます。 `GetFeatureStatus` FIPS ドライブの有効化ステータスが true か false かを示す API メソッド。

1. Element API を使用して、次のように入力してクラスター上の FIPS ドライブ機能を確認します。

```
GetFeatureStatus
```

2. 結果を確認する `GetFeatureStatus`API 呼び出し。 FIPS ドライブ有効値が True の場合、FIPS ドライブ機能は有効です。

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

詳細情報の参照

- "Element APIで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 用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

NetApp Elementソフトウェア UI を使用すると、FIPS ドライブ機能に関連するシステム内のクラスタ障害またはエラーに関する情報のアラートを表示できます。

1. Element UI を使用して、レポート > *アラート*を選択します。
2. 次のようなクラスター障害を探します。
   - FIPSドライブが一致しません
   - FIPSのコンプライアンス違反
3. 解決の提案については、クラスター障害コード情報を参照してください。

詳細情報の参照

- クラスター障害コード
- "Element APIで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 用NetApp Elementプラグイン"

安全な通信を確立する

クラスターでHTTPSにFIPS 140-2を有効にする

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

NetApp Elementソフトウェアを使用すると、クラスターで連邦情報処理標準 (FIPS) 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暗号化セキュリティ モジュール (NCSM) がアクティブになり、 NetApp Element UI および API への HTTPS 経由のすべての通信に FIPS 140-2 レベル 1 認定の暗号化が活用されます。

> FIPS 140-2 モードを有効にすると、無効にすることはできません。 FIPS 140-2 モードが有効になっている場合、クラスター内の各ノードが再起動し、NCSM が正しく有効になっていてFIPS 140-2 認定モードで動作していることを確認するためのセルフテストが実行されます。これにより、クラスター上の管理接続とストレージ接続の両方が中断されます。慎重に計画し、環境でこのモードが提供する暗号化メカニズムが必要な場合にのみ、このモードを有効にする必要があります。

詳細については、Element API 情報を参照してください。

以下は、FIPS を有効にするための API リクエストの例です。

```
{
  "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 承認の暗号が使用されます。

詳細情報の参照

- SSL暗号
- "Element APIで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 用NetApp Elementプラグイン"

SSL暗号

SSL 暗号は、ホストが安全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 ソフトウェアがサポートする暗号には、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。

次のリストは、Element ソフトウェアでサポートされている標準の Secure Socket Layer (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 暗号を示しています。

- **FIPS 140-2** 無効

  TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (dh 2048) - A

  TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 2048) - A

  TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (dh 2048) - A

  TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 2048) - A

  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A

  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A

  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A

  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A

  TLS_RSA_WITH_3DES_EDE_CBC_SHA (RSA 2048) - C

  TLS_RSA_WITH_AES_128_CBC_SHA (RSA 2048) - A

TLS_RSA_WITH_AES_128_CBC_SHA256 (RSA 2048) - A

TLS_RSA_WITH_AES_128_GCM_SHA256 (RSA 2048) - A

TLS_RSA_WITH_AES_256_CBC_SHA (RSA 2048) - A

TLS_RSA_WITH_AES_256_CBC_SHA256 (RSA 2048) - A

TLS_RSA_WITH_AES_256_GCM_SHA384 (RSA 2048) - A

TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (RSA 2048) - A

TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (RSA 2048) - A

TLS_RSA_WITH_IDEA_CBC_SHA (RSA 2048) - A

TLS_RSA_WITH_RC4_128_MD5 (RSA 2048) - C

TLS_RSA_WITH_RC4_128_SHA (RSA 2048) - C

TLS_RSA_WITH_SEED_CBC_SHA (RSA 2048) - A

- **FIPS 140-2**対応

  TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (dh 2048) - A

  TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 2048) - A

  TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (dh 2048) - A

  TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 2048) - A

  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (sect571r1) - A

  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A

  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A

  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (sect571r1) - A

  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (sect571r1) - A

  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A

  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A

  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (sect571r1) - 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

詳細情報の参照

クラスターでHTTPSにFIPS 140-2を有効にする

外部キー管理を始める

外部キー管理を始める

外部キー管理 (EKM) は、クラスター外の外部キー サーバー (EKS) と連携して、安全な認証キー (AK) 管理を提供します。 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。"保存時の暗号化"クラスターで有効になっています。 EKS は、AK の安全な生成と保存を提供します。クラスターは、OASIS が定義した標準プロトコルであるキー管理相互運用性プロトコル (KMIP) を使用して EKS と通信します。

- "外部管理を設定する"
- "保存時のソフトウェア暗号化マスターキーの再キー化"
- "アクセスできない、または無効な認証キーを回復する"
- "外部キー管理APIコマンド"

詳細情報の参照

- "保存時のソフトウェア暗号化を有効にするために使用できる CreateCluster API"
- "SolidFireおよびElementソフトウェアのドキュメント"
- "NetApp SolidFireおよび Element 製品の以前のバージョンのドキュメント"

外部キー管理を設定する

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。

要件

- 保存時のソフトウェア暗号化と組み合わせて外部キー管理を設定する場合は、保存時のソフトウェア暗号化を次のように有効にする必要があります。"CreateCluster"ボリュームを含まない新しいクラスター上のメソッド。

手順

1. 外部キー サーバー (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 サーバーとの信頼関係を確立するために使用される Element クラスターの公開キー/秘密キー ペアを作成します。"公開鍵ペアの作成"

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 により、キー サーバーは、キーにアクセスする Element クラスターが Element クラスター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/証明機関を使用して、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. EKS と通信するために、クラスター上にサーバーとプロバイダーを作成します。キープロバイダーはキーを取得する場所を定義し、サーバーは通信する 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 サーバーの詳細が保存されるキー プロバイダーを作成します。"キープロバイダーKmipの作成"

b. 次の API メソッドを呼び出して、署名付き証明書と証明機関の公開鍵証明書を提供するキー サーバーを作成します。"キーサーバーKmipの作成" "テストキーサーバーKmip"

テストが失敗した場合は、サーバーの接続と構成を確認してください。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 サーバーをキー プロバイダー コンテナーに追加します。"プロバイダーKmipにキーサーバーを追加" "テストキープロバイダーKmip"

テストが失敗した場合は、サーバーの接続と構成を確認してください。その後、テストを繰り返します。

3. 保存時の暗号化の次のステップとして、次のいずれかを実行します。

a. （保存時のハードウェア暗号化の場合）有効にする"保存時のハードウェア暗号化"鍵を保存するために使用する鍵サーバーを含む鍵プロバイダーのIDを指定して、"保存時の暗号化を有効にする" API メソッド。

> ⓘ 保存時の暗号化を有効にするには、"API" 。既存の Element UI ボタンを使用して保存時の暗号化を有効にすると、機能は内部で生成されたキーを使用するようになります。

b. （保存時のソフトウェア暗号化の場合）"保存時のソフトウェア暗号化"新しく作成されたキープロバイダーを利用するには、キープロバイダーIDを"再鍵ソフトウェア暗号化保存マスターキー"API メソッド。

詳細情報の参照

- "クラスターの暗号化を有効または無効にする"
- "SolidFireおよびElementソフトウェアのドキュメント"
- "NetApp SolidFireおよび Element 製品の以前のバージョンのドキュメント"

保存時のソフトウェア暗号化マスターキーの再キー化

Element API を使用して既存のキーを再設定できます。このプロセスにより、外部キー管理サーバー用の新しい交換マスター 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、複製または上書きされることはありません。

次のいずれかの手順の一環として、キーの再設定が必要になる場合があります。

- 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。

- セキュリティ関連のイベントへの対応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あり、キー再生成操作が完了する前に応答を返します。使用することができます"非同期結果を取得する"プロセスをいつ完了したかを確認するためにシステムをポーリングするメソッド。

要件

- 保存時のソフトウェア暗号化を有効にしました。"CreateCluster"ボリュームを含まず、I/O もない新しいクラスター上のメソッド。リンクを使用してください:../api/reference_element_api_getsoftwareencryptionatrestinfo.html[`GetSoftwareEncryptionatRestInfo`] 状態を確認するには `enabled`続行する前に。
- あなたが持っている"信頼関係を築いた"SolidFireクラスターと外部キー サーバー (EKS) 間。実行"テストキープロバイダーKmip"キープロバイダーへの接続が確立されていることを確認する方法。

手順

1. 実行"リストキープロバイダーKmip"コマンドを実行してキープロバイダーIDをコピーします（`keyProviderID`）。
2. 実行"再鍵ソフトウェア暗号化保存マスターキー"と `keyManagementType`パラメータとして `external`そして `keyProviderID`前のステップのキープロバイダーのID番号として:

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

3. コピー `asyncHandle`からの価値 `RekeySoftwareEncryptionAtRestMasterKey`コマンド応答。
4. 実行"非同期結果を取得する"コマンドを `asyncHandle`前の手順の値を確認して、構成の変更を確認します。コマンド応答から、古いマスター キー構成が新しいキー情報で更新されたことがわかります。後の手順で使用するために、新しいキープロバイダー ID をコピーします。

```
{
   "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. 実行 `GetSoftwareEncryptionatRestInfo`新しいキーの詳細を確認するコマンド。 `keyProviderID`が更新されました。

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

詳細情報の参照

- "Element APIで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"
- "NetApp SolidFireおよび Element 製品の以前のバージョンのドキュメント"

アクセスできない、または無効な認証キーを回復する

場合によっては、ユーザーの介入が必要なエラーが発生することがあります。エラーが発生した場合、クラスター障害 (クラスター障害コードと呼ばれる) が生成されます。最も可能性の高い 2 つのケースをここで説明します。

KmipServerFault クラスター障害のため、クラスターはドライブのロックを解除できません。

これは、クラスターが最初に起動し、キー サーバーにアクセスできない場合、または必要なキーが利用できない場合に発生する可能性があります。

1. クラスター障害コード (存在する場合) の回復手順に従います。

メタデータ ドライブが障害ありとしてマークされ、「使用可能」状態になっているため、**sliceServiceUnhealthy** 障害が設定されている可能性があります。

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、 `sliceServiceUnhealthy`障害は解消されました。

見る"クラスター障害コード"詳細についてはこちらをご覧ください。

外部キー管理APIコマンド

EKM の管理と構成に使用できるすべての API のリスト。

クラスターと外部の顧客所有サーバー間の信頼関係を確立するために使用されます。

- 公開鍵ペアの作成
- GetClientCertificateSignRequest

外部顧客所有サーバーの具体的な詳細を定義するために使用されます。

- キーサーバーKmipの作成
- キーサーバーKmipの変更
- キーサーバーKmipの削除
- GetKeyServerKmip
- リストキーサーバーKmip
- テストキーサーバーKmip

外部キー サーバーを管理するキー プロバイダーの作成と管理に使用されます。

- キープロバイダーKmipの作成
- 削除キープロバイダーKmip
- プロバイダーKmipにキーサーバーを追加
- プロバイダーKmipからキーサーバーを削除
- GetKeyProviderKmip
- リストキープロバイダーKmip
- 再鍵ソフトウェア暗号化保存マスターキー
- テストキープロバイダーKmip

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

著作権に関する情報

商標に関する情報