システムを管理します
Element Software

NetApp
April 17, 2024

目次

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。

ノード混在環境でのクラスタ容量

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ソフトウェアのバージョンに応じて、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。

先頭のドキュメント	ストレージノードがサポートされていません...
要素12.7	• SF2405 のように指定する • SF9608
Element 12.0	• SF3010 • SF6010 • SF9010

これらのノードのいずれかをサポート対象外のバージョンにアップグレードしようとすると、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

仮想ネットワークを追加

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

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"。