導入後に **SolidFire** システムのオプションを設定

Element Software

NetApp
October 01, 2024

目次

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。

詳細情報

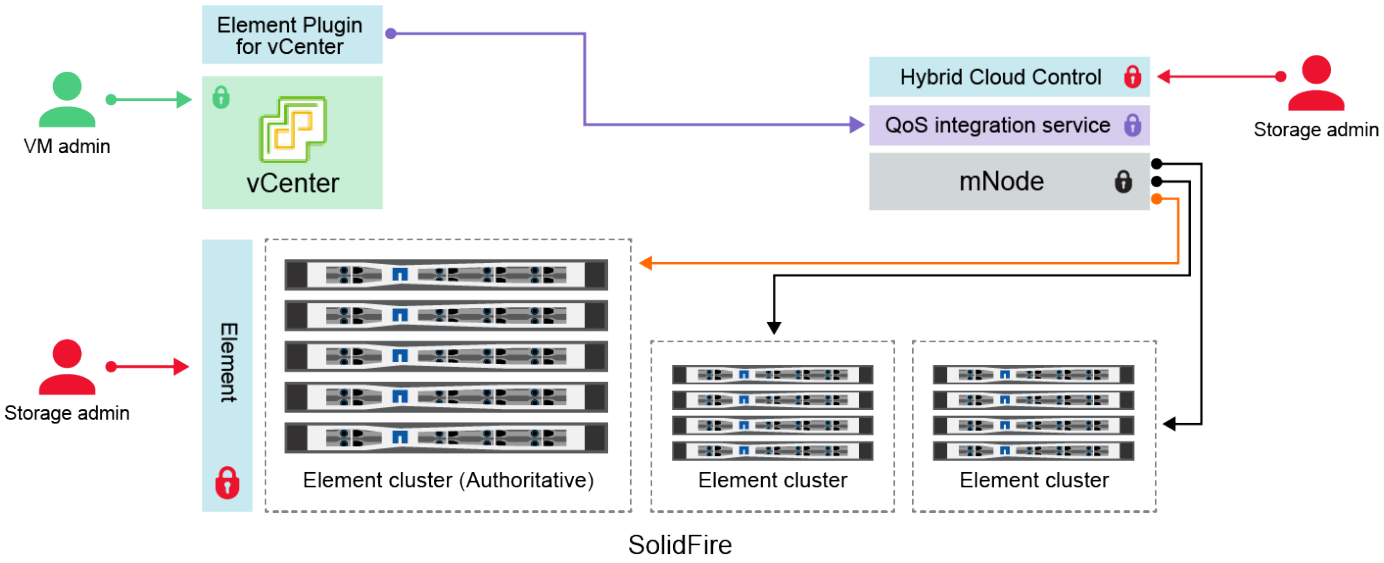
- "NetApp HCI と NetApp SolidFire でクレデンシャルを変更"
- "Element ソフトウェアのデフォルトの SSL 証明書を変更"
- "ノードの IPMI パスワードを変更します"
- "多要素認証を有効にします"
- "外部キー管理の開始"
- "FIPS ドライブをサポートするクラスタを作成します"

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で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"です。
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"です。 • H410C、H610C、およびH615Cノードの場合は、"デフォルトの IPMI パスワードを変更します" • H410SおよびH610Sノードの場合は、"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"です。

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"です。
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"です。 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にコンピューティングノードを初めてインストールするときにユーザがユーザ名とパスワードを指定しました。 他のコンポーネントには影響しません。	変更は不要です。

詳細情報

- "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*

  を使用すると、現在インストールされているSSL証明書に関するすべての証明書の詳細を含む情報を取得できます"GetSSLCertificateメソッド"。

- * SetSSLCertificate*

  を使用して、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できます"SetSSLCertificateメソッド"。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 *

  は、"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。

詳細情報

- "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。

ノードの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とパスワードを `ADMIN`入力し `ADMIN`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. ユーザを選択し `ADMIN`、*[ユーザの変更]*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 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とパスワードを `calvin`入力し `root`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。

詳細情報

- "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"

著作権に関する情報

商標に関する情報