導入後にSolidFireシステムオプションを構成する

Element Software

NetApp
November 12, 2025

目次

導入後にSolidFireシステムオプションを構成する

導入後にSolidFireシステムオプションを構成する

SolidFireシステムをセットアップした後、オプションのタスクをいくつか実行する必要がある場合があります。

システム内の資格情報を変更する場合、他のコンポーネントへの影響を知りたい場合があります。

さらに、多要素認証、外部キー管理、連邦情報処理標準 (FIPS) セキュリティの設定を構成することもできます。必要に応じてパスワードを更新することも検討してください。

詳細情報の参照

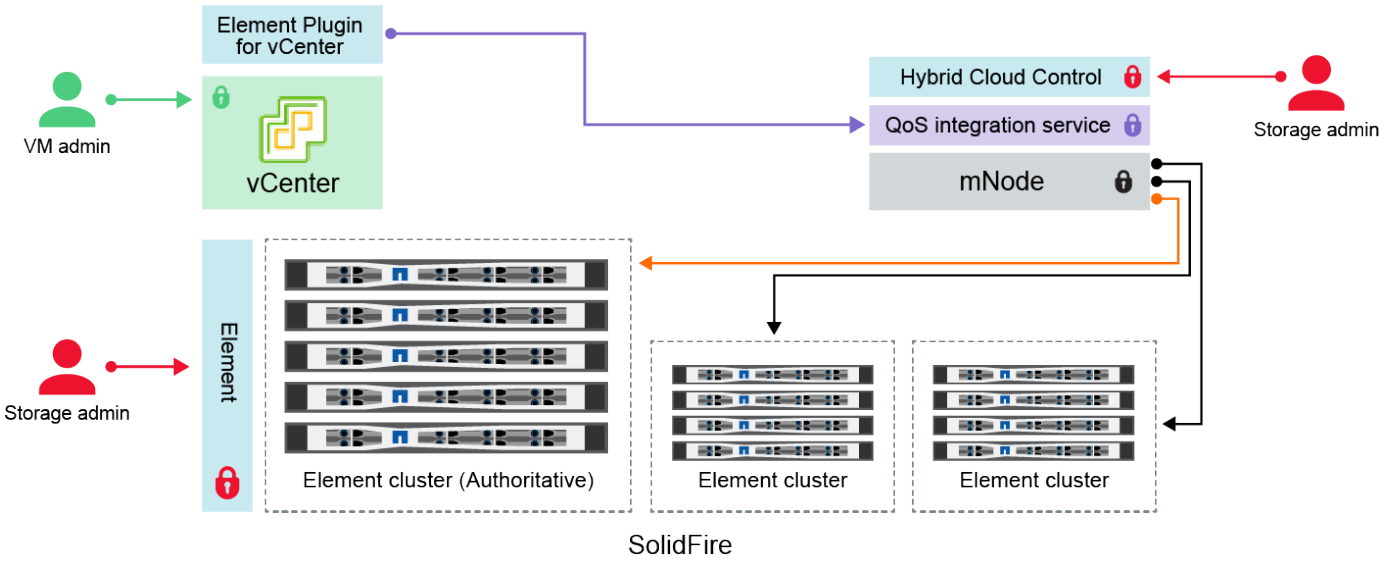
- "NetApp HCIおよびNetApp SolidFireの資格情報を変更する"
- "Elementソフトウェアのデフォルトの SSL証明書を変更する"
- "ノードのIPMIパスワードを変更する"
- "多要素認証を有効にする"
- "外部キー管理を始める"
- "FIPSドライブをサポートするクラスタを作成する"

NetApp HCIおよびNetApp SolidFireの資格情報を変更する

NetApp HCIまたはNetApp SolidFireを導入した組織のセキュリティ ポリシーに応じて、資格情報やパスワードの変更は一般的にセキュリティ プラクティスの一部となります。パスワードを変更する前に、展開内の他のソフトウェア コンポーネントへの影響に注意する必要があります。

NetApp HCIまたはNetApp SolidFireデプロイメントの 1 つのコンポーネントの資格情報を変更する場合、他のコンポーネントへの影響に関するガイダンスを次の表に示します。

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	こちらの手順をご覧ください
要素の資格情報	適用対象: 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 クラスター上の Element ユーザー インターフェース • 管理ノード（mnode）上のハイブリッドクラウド制御 Hybrid Cloud Control が複数のストレージ クラスターを管理する場合、mnode が最初に設定された 権限のあるクラスター と呼ばれるストレージ クラスターの管理者資格情報のみが受け入れられます。後で Hybrid Cloud Control に追加されるストレージ クラスターの場合、mnode は管理者の資格情報を安全に保存します。その後に追加されたストレージ クラスターの資格情報が変更された場合は、mnode API を使用して mnode 内の資格情報も更新する必要があります。	• "ストレージ クラスターの管理者パスワードを更新します。" • mnode内のストレージクラスタ管理者の資格情報を更新するには、"クラスタ管理者の変更 API" 。

資格情報の種類とアイコン	管理者による使用状況	こちらの手順をご覧ください
vSphereシングルサインオンの認証情報 	適用対象: NetApp HCIのみ 管理者はこれらの資格情報を使用して VMware vSphere Client にログインします。 vCenter がNetApp HCIインストールの一部である場合、資格情報はNetApp Deployment Engine で次のように構成されます。 • username@vsphere.local と指定されたパスワード、および • 指定されたパスワードを持つ administrator@vsphere.local。既存の vCenter を使用してNetApp HCI を展開する場合、vSphere Single Sign-on の資格情報は IT VMware 管理者によって管理されます。	"vCenterとESXiの資格情報を更新する"。
ベースボード管理コントローラ (BMC) の資格情報 	適用対象: NetApp HCIのみ 管理者はこれらの資格情報を使用して、 NetApp HCI展開内のNetApp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と仮想コンソール機能を提供します。 各NetAppコンピューティング ノードのBMC (*IPMI* と呼ばれることもあります) 資格情報は、 NetApp HCI展開の mnode に安全に保存されます。 NetApp Hybrid Cloud Control は、コンピューティング ノードのファームウェアのアップグレード中に、サービス アカウントの容量でBMC資格情報を使用してコンピューティング ノードのBMCと通信します。 BMC資格情報が変更された場合は、すべての Hybrid Cloud Control 機能を保持するために、mnode 上のそれぞれのコンピューティング ノードの資格情報も更新する必要があります。	• "NetApp HCI上の各ノードにIPMIを構成する"。 • H410C、H610C、およびH615Cノードの場合、"デフォルトのIPMIパスワードを変更する" 。 • H410SおよびH610Sノードの場合、"デフォルトのIPMパスワードを変更する" 。 • "管理ノードのBMC資格情報を変更する"。

資格情報の種類とアイコン	管理者による使用状況	こちらの手順をご覧ください
ESXi 資格情報 	適用対象: NetApp HCIのみ 管理者は、SSH またはローカル ルート アカウントを使用したローカル DCUI を使用して ESXi ホストにログインできます。NetApp HCI のデプロイメントでは、ユーザー名は「root」で、パスワードはNetApp Deployment Engine でそのコンピューティング ノードを最初にインストールしたときに指定されます。 各NetAppコンピューティング ノードの ESXi ルート認証情報は、 NetApp HCI展開の mnode に安全に保存されます。NetApp Hybrid Cloud Control は、コンピューティング ノードのファームウェアのアップグレードおよびヘルス チェック中に、サービス アカウント容量の資格情報を使用して ESXi ホストと直接通信します。 VMware 管理者によって ESXi ルート認証情報が変更された場合は、Hybrid Cloud Control 機能を維持するために、mnode 上のそれぞれのコンピューティング ノードの認証情報を更新する必要があります。	"vCenter および ESXi ホストの資格情報を更新する"。
QoS統合パスワード 	適用対象: NetApp HCIおよびSolidFireのオプション 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 Software 間の QoS 統合は、以下によって有効化されます。 • vCenter Server用のElementプラグイン、および • mnode 上の QoS サービス。 認証には、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 パスワードは、vCenter Server の Element プラグインの初期インストール時に指定されるか、NetApp HCI の展開時に自動生成されます。 他のコンポーネントには影響はありません。	"NetApp Element Plug-in for vCenter Server で QoSSIOC 資格情報を更新する"。 NetApp Element Plug-in for vCenter Server SIOC パスワードは、*QoSSIOC* パスワード とも呼ばれます。 vCenter Server の Element プラグインに関する KB 記事 を確認してください。

資格情報の種類とアイコン	管理者による使用状況	こちらの手順をご覧ください
vCenterサービスアプライアンスの資格情報 	適用対象: NetApp Deployment Engine によってセットアップされた場合のみNetApp HCI 管理者は vCenter Server Appliance 仮想マシンにログインできます。 NetApp HCI のデプロイメントでは、ユーザー名は「root」で、パスワードはNetAppデプロイメント エンジンでそのコンピューティング ノードを最初にインストールしたときに指定されます。導入された VMware vSphere のバージョンに応じて、vSphere Single Sign-on ドメイン内の特定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はありません。	変更は必要ありません。
NetApp管理ノードの管理者資格情報 	適用対象: NetApp HCIおよびSolidFireのオプション 管理者は、 NetApp管理ノードの仮想マシンにログインして、高度な構成とトラブルシューティングを行うことができます。展開された管理ノードのバージョンによっては、SSH 経由のログインがデフォルトで有効になっていません。 NetApp HCIの導入では、ユーザー名とパスワードは、 NetApp Deployment Engine でそのコンピューティング ノードを最初にインストールしたときにユーザーによって指定されました。 他のコンポーネントには影響はありません。	変更は必要ありません。

詳細情報の参照

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

Elementソフトウェアのデフォルトの SSL証明書を変更する

NetApp Element API を使用して、クラスター内のストレージ ノードのデフォルトの SSL 証明書と秘密キーを変更できます。

NetApp Elementソフトウェア クラスタが作成されると、クラスタは、Element UI、ノードごとの UI、または API 経由のすべての HTTPS 通信に使用される一意の自己署名 Secure Sockets Layer (SSL) 証明書と秘密キーを作成します。 Element ソフトウェアは、自己署名証明書だけでなく、信頼できる証明機関 (CA) によって発行および検証された証明書もサポートします。

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。

- **SSL**証明書を取得

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

- **SSL**証明書の設定

  使用することができます"SetSSLCertificateメソッド"クラスターおよびノードごとの SSL 証明書を、指定した証明書と秘密キーに設定します。システムは、無効な証明書が適用されないように、証明書と秘密キーを検証します。

- **SSL**証明書を削除

  その"RemoveSSLCertificate メソッド"現在インストールされている SSL 証明書と秘密キーを削除します。次に、クラスターは新しい自己署名証明書と秘密キーを生成します。

> クラスター SSL 証明書は、クラスターに追加されたすべての新しいノードに自動的に適用されます。クラスターから削除されたノードは自己署名証明書に戻り、ユーザー定義の証明書とキー情報はすべてノードから削除されます。

詳細情報の参照

- "管理ノードのデフォルトのSSL証明書を変更する"
- "Element Software でカスタム SSL 証明書を設定する場合の要件は何ですか?"
- "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"

ノードのデフォルトの **IPMI** パスワードを変更する

ノードへのリモート IPMI アクセスが可能になったらすぐに、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。インストールの更新があった場合は、これを実行することをお勧めします。

ノードのIPMアクセスの設定の詳細については、以下を参照してください。"各ノードのIPMIを構成する" 。

次のノードの 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**パスワードを変更する

IPMI ネットワーク ポートを構成したらすぐに、各ストレージ ノード上の 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。

要件

各ストレージ ノードの IPMI IP アドレスを設定する必要があります。

手順

1. IPMI ネットワークにアクセスできるコンピューターで Web ブラウザーを開き、ノードの IPMI IP アドレスを参照します。
2. ユーザー名を入力してください `ADMIN`パスワード `ADMIN`ログインプロンプトで。
3. ログインしたら、[構成]タブをクリックします。
4. *ユーザー*をクリックします。
5. 選択してください `ADMIN`ユーザーを選択し、[ユーザーの変更] 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選択します。
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 パスワードを持つ他の H410S ノードに対してもこの手順を繰り返します。

H610Sノードのデフォルトの**IPMI**パスワードを変更する

IPMI ネットワーク ポートを構成したらすぐに、各ストレージ ノード上の 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。

要件

各ストレージ ノードの IPMI IP アドレスを設定する必要があります。

手順

1. IPMI ネットワークにアクセスできるコンピューターで Web ブラウザーを開き、ノードの IPMI IP アドレスを参照します。
2. ユーザー名を入力してください `root`パスワード `calvin`ログインプロンプトで。
3. ログインしたら、ページの左上にあるメニュー 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*管理者*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有効にします。
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 パスワードを持つ他の H610S ノードに対してもこの手順を繰り返します。

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"