



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	1
導入後にSolidFireシステムオプションを構成する	1
詳細情報の参照	1
NetApp HCIおよびNetApp SolidFireの資格情報を変更する	1
詳細情報の参照	5
ElementソフトウェアのデフォルトのSSL証明書を変更する	5
詳細情報の参照	6
ノードのデフォルトの IPMI パスワードを変更する	6
H410SノードのデフォルトのIPMIパスワードを変更する	6
H610SノードのデフォルトのIPMIパスワードを変更する	7
詳細情報の参照	7

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"](#)

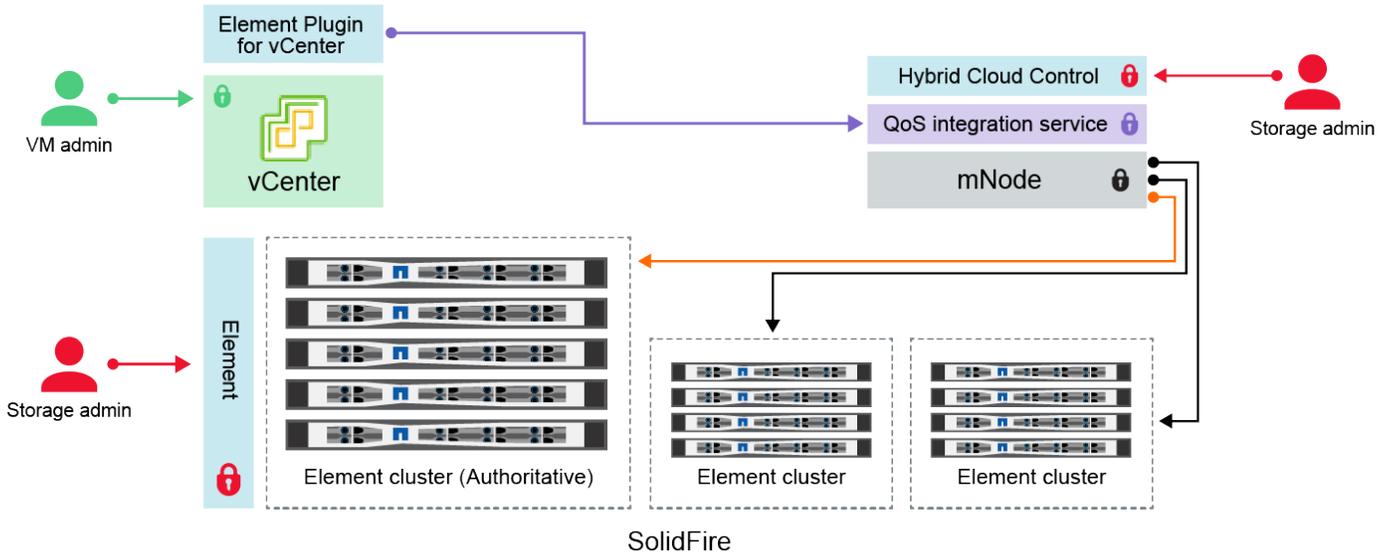
NetApp HCIおよびNetApp SolidFireの資格情報を変更する

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

:



- Administrator uses administrative Element storage credentials to log into Element UI and Hybrid Cloud Control
- Element Plugin for VMware vCenter uses password to communicate with QoS service on mNode
- mNode and services use Element certificates to communicate with authoritative storage cluster
- mNode and services use Element administrative credentials for additional storage clusters
- Administrators use VMware vSphere Single Sign-on credentials to log into vCenter

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。 <ul style="list-style-type: none"> • 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。	<ul style="list-style-type: none"> • "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。 <ul style="list-style-type: none"> • <code>username@vsphere.local</code> 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 <code>administrator@vsphere.local</code>。 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。	<ul style="list-style-type: none"> • "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IPMI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
<p>ESXi 資格情報</p> 	<p>適用対象: NetApp HCIのみ</p> <p>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。</p> <p>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。</p> <p>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。</p>	<p>"vCenter および ESXi ホストの資格情報を更新する"。</p>
<p>QoS統合パスワード</p> 	<p>適用対象: NetApp HCIおよびSolidFireのオプション</p> <p>管理者による対話型ログインには使用されません。</p> <p>VMware vSphere と Element Software 間の QoS 統合は、以下によって有効化されます。</p> <ul style="list-style-type: none"> • vCenter Server用のElementプラグイン、および • mnode 上の QoS サービス。 <p>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。</p> <p>他のコンポーネントには影響はありません。</p>	<p>"NetApp Element Plug-in for vCenter Server で QoSSIOC 資格情報を更新する"。</p> <p>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。</p> <p>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。</p>

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 	<p>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</p> <p>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。</p> <p>他のコンポーネントには影響はありません。</p>	変更は必要ありません。
NetApp管理ノードの管理者資格情報 	<p>適用対象: NetApp HCIおよびSolidFireのオプション</p> <p>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。</p> <p>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。</p> <p>他のコンポーネントには影響はありません。</p>	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"](#)

著作権に関する情報

Copyright © 2025 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。