導入後に SolidFire システムのオプションを設定

Element Software

NetApp
November 19, 2025

This PDF was generated from https://docs.netapp.com/ja-jp/element-software-123/storage/task_post_deploy_credentials.html on November 19, 2025. Always check docs.netapp.com for the latest.

目次

導入後に SolidFire システムのオプションを設定 . . . 1
詳細については、こちらをご覧ください . . . 1
NetApp HCI と NetApp SolidFire でクレデンシャルを変更 . . . 1
詳細については、こちらをご覧ください . . . 5
Element ソフトウェアのデフォルトの SSL 証明書を変更 . . . 5
詳細については、こちらをご覧ください . . . 6
ノードのデフォルトの IPMI パスワードを変更します . . . 6
H410S ノードのデフォルトの IPMI パスワードを変更します . . . 6
H610S ノードのデフォルトの IPMI パスワードを変更します . . . 7
詳細については、こちらをご覧ください . . . 7

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。

詳細については、こちらをご覧ください

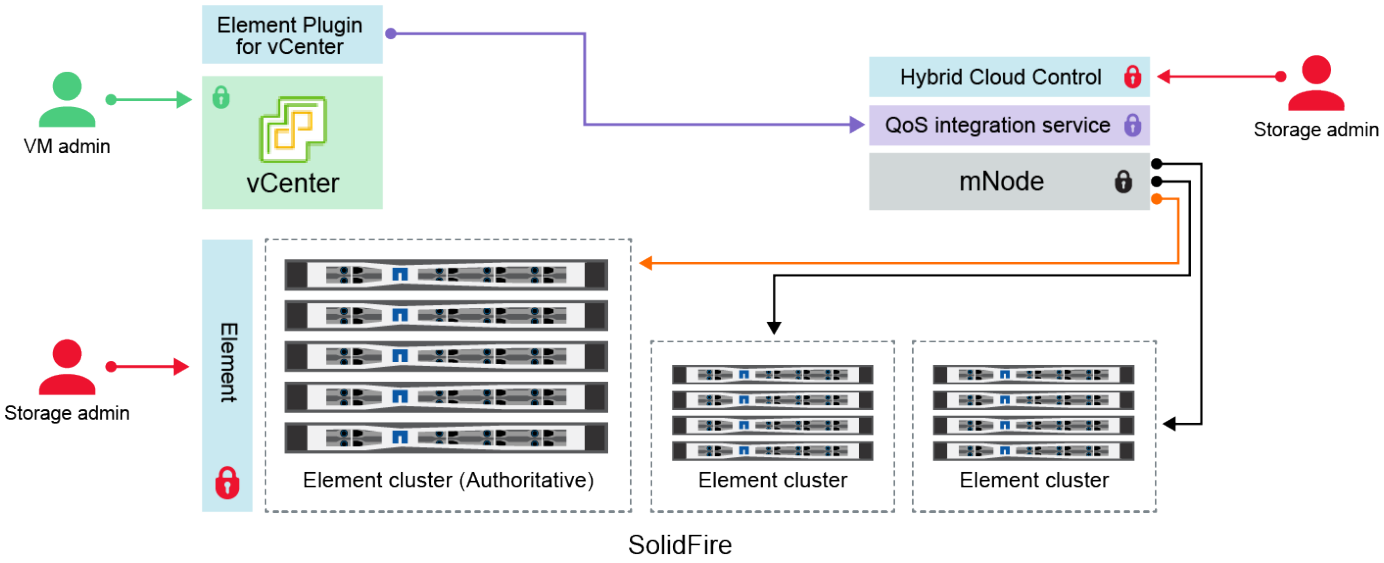
- "NetApp HCI と NetApp SolidFire でクレデンシャルを変更"
- "Element ソフトウェアのデフォルトの SSL 証明書を変更"
- "ノードの IPMI パスワードを変更します"
- "多要素認証を有効にします"
- "外部キー管理の開始"
- "FIPS ドライブをサポートするクラスタを作成します"

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 の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"。
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"。 • H410C 、 H610C 、および H615C ノードの場合、 "デフォルトの IPMI パスワードを変更します"。 • H410S および H610S ノードの場合、 "デフォルトの IPM パスワードを変更します"。 • "管理ノードで BMC クレデンシャルを変更します"。

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
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"。
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"。 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 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、ユーザによってユーザ名とパスワードが指定されています。 他のコンポーネントには影響しません。	変更は不要です。

詳細については、こちらをご覧ください

- "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*

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

- * SetSSLCertificate*

  を使用できます "SetSSLCertificateメソッド" 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します。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 *

  。 "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。

詳細については、こちらをご覧ください

- "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。

ノードに対する 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 ADMIN とパスワード ADMIN を入力します
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. 「 Admin 」ユーザを選択し、「 * Modify User * 」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他の 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「 root 」とパスワード「 calvin 」を入力します。
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"

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権を有し、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権については、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。