



Configurare le opzioni del sistema SolidFire dopo la distribuzione

Element Software

NetApp
November 12, 2025

Sommario

- Configurare le opzioni del sistema SolidFire dopo la distribuzione 1
 - Configurare le opzioni del sistema SolidFire dopo la distribuzione 1
 - Trova maggiori informazioni 1
 - Modificare le credenziali in NetApp HCI e NetApp SolidFire 1
 - Trova maggiori informazioni 5
 - Cambia il certificato SSL predefinito del software Element 5
 - Trova maggiori informazioni 6
 - Cambia la password IPMI predefinita per i nodi 6
 - Modificare la password IPMI predefinita per i nodi H410S 6
 - Modificare la password IPMI predefinita per i nodi H610S 7
 - Trova maggiori informazioni 7

Configurare le opzioni del sistema SolidFire dopo la distribuzione

Configurare le opzioni del sistema SolidFire dopo la distribuzione

Dopo aver configurato il sistema SolidFire , potresti voler eseguire alcune attività facoltative.

Se modifichi le credenziali nel sistema, potresti voler conoscere l'impatto sugli altri componenti.

Inoltre, è possibile configurare le impostazioni per l'autenticazione a più fattori, la gestione delle chiavi esterne e la sicurezza FIPS (Federal Information Processing Standards). Dovresti anche aggiornare le password quando necessario.

Trova maggiori informazioni

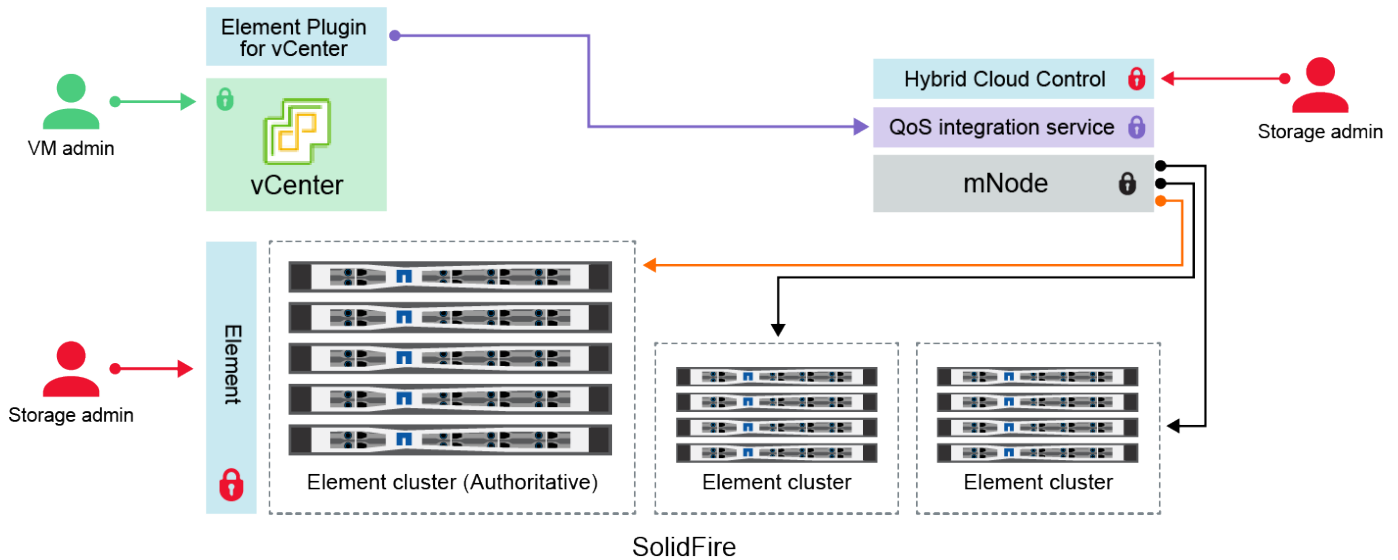
- ["Modificare le credenziali in NetApp HCI e NetApp SolidFire"](#)
- ["Cambia il certificato SSL predefinito del software Element"](#)
- ["Cambia la password IPMI per i nodi"](#)
- ["Abilita l'autenticazione a più fattori"](#)
- ["Inizia con la gestione delle chiavi esterne"](#)
- ["Creare un cluster che supporti le unità FIPS"](#)

Modificare le credenziali in NetApp HCI e NetApp SolidFire

A seconda delle policy di sicurezza dell'organizzazione che ha implementato NetApp HCI o NetApp SolidFire, la modifica delle credenziali o delle password rientra solitamente nelle pratiche di sicurezza. Prima di modificare le password, è necessario essere consapevoli dell'impatto sugli altri componenti software nella distribuzione.

Se si modificano le credenziali per un componente di una distribuzione NetApp HCI o NetApp SolidFire , la tabella seguente fornisce indicazioni sull'impatto sugli altri componenti.

Interazioni dei componenti NetApp SolidFire
:



- 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

Tipo di credenziali e icona	Utilizzo da parte dell'amministratore	Vedi queste istruzioni
Credenziali dell'elemento 	Si applica a: NetApp HCI e SolidFire Gli amministratori utilizzano queste credenziali per accedere a: - Interfaccia utente Element sul cluster di archiviazione Element - Controllo del cloud ibrido sul nodo di gestione (mnode) Quando Hybrid Cloud Control gestisce più cluster di storage, accetta solo le credenziali di amministratore per i cluster di storage, noti come <i>cluster autorevole</i> per cui il mnode è stato inizialmente configurato. Per i cluster di storage aggiunti in seguito a Hybrid Cloud Control, mnode memorizza in modo sicuro le credenziali di amministratore. Se vengono modificate le credenziali per i cluster di archiviazione aggiunti successivamente, è necessario aggiornarle anche nel mnode utilizzando l'API mnode.	"Aggiornare le password di amministrazione del cluster di archiviazione." - Aggiornare le credenziali di amministratore del cluster di archiviazione nel mnode utilizzando "API di modifica cluster admin".

Tipo di credenziale e icona	Utilizzo da parte dell'amministratore	Vedi queste istruzioni
Credenziali vSphere Single Sign-on 	Si applica a: solo NetApp HCI Gli amministratori utilizzano queste credenziali per accedere a VMware vSphere Client. Quando vCenter fa parte dell'installazione di NetApp HCI, le credenziali vengono configurate in NetApp Deployment Engine come segue: • username@vsphere.local con la password specificata e • administrator@vsphere.local con la password specificata. Quando si utilizza un vCenter esistente per distribuire NetApp HCI, le credenziali di vSphere Single Sign-on vengono gestite dagli amministratori IT VMware.	"Aggiorna le credenziali vCenter ed ESXi".
Credenziali del controller di gestione della scheda madre (BMC) 	Si applica a: solo NetApp HCI Gli amministratori utilizzano queste credenziali per accedere al BMC dei nodi di elaborazione NetApp in una distribuzione NetApp HCI. BMC fornisce funzionalità di monitoraggio hardware di base e di console virtuale. Le credenziali BMC (talvolta denominate <i>IPMI</i>) per ciascun nodo di elaborazione NetApp vengono archiviate in modo sicuro sul mnode nelle distribuzioni NetApp HCI. NetApp Hybrid Cloud Control utilizza le credenziali BMC in una capacità di account di servizio per comunicare con il BMC nei nodi di elaborazione durante gli aggiornamenti del firmware dei nodi di elaborazione. Quando si modificano le credenziali BMC, è necessario aggiornare anche le credenziali per i rispettivi nodi di elaborazione sul nodo m per mantenere tutte le funzionalità di Hybrid Cloud Control.	• "Configurare IPMI per ogni nodo su NetApp HCI". • Per i nodi H410C, H610C e H615C, "cambiare la password IPMI predefinita". • Per i nodi H410S e H610S, "cambia la password IPM predefinita". • "Modificare le credenziali BMC sul nodo di gestione".

Tipo di credenziale e icona	Utilizzo da parte dell'amministratore	Vedi queste istruzioni
Credenziali ESXi 	Si applica a: solo NetApp HCI Gli amministratori possono accedere agli host ESXi tramite SSH o tramite la DCUI locale con un account root locale. Nelle distribuzioni NetApp HCI, il nome utente è "root" e la password è stata specificata durante l'installazione iniziale di quel nodo di elaborazione in NetApp Deployment Engine. Le credenziali root ESXi per ciascun nodo di elaborazione NetApp vengono archiviate in modo sicuro sul mnode nelle distribuzioni NetApp HCI. NetApp Hybrid Cloud Control utilizza le credenziali in una capacità di account di servizio per comunicare direttamente con gli host ESXi durante gli aggiornamenti del firmware del nodo di elaborazione e i controlli di integrità. Quando le credenziali di root ESXi vengono modificate da un amministratore VMware, le credenziali per i rispettivi nodi di elaborazione devono essere aggiornate sul mnode per mantenere la funzionalità Hybrid Cloud Control.	"Aggiornare le credenziali per gli host vCenter ed ESXi".
Password di integrazione QoS 	Si applica a: NetApp HCI e facoltativo in SolidFire Non utilizzato per accessi interattivi da parte degli amministratori. L'integrazione QoS tra VMware vSphere ed Element Software è abilitata tramite: • Plug-in Element per vCenter Server e • Servizio QoS sul mnode. Per l'autenticazione, il servizio QoS utilizza una password utilizzata esclusivamente in questo contesto. La password QoS viene specificata durante l'installazione iniziale del plug-in Element per vCenter Server oppure generata automaticamente durante la distribuzione di NetApp HCI. Nessun impatto sugli altri componenti.	"Aggiornare le credenziali QoSSIOC nel plug-in NetApp Element per vCenter Server". La password SIOC del plug-in NetApp Element per vCenter Server è nota anche come <i>password QoSSIOC</i>. Consultare l'articolo della Knowledge Base sul plug-in Element per vCenter Server.

Tipo di credenziale e icona	Utilizzo da parte dell'amministratore	Vedi queste istruzioni
Credenziali di vCenter Service Appliance 	Si applica a: NetApp HCI solo se configurato da NetApp Deployment Engine Gli amministratori possono accedere alle macchine virtuali dell'appliance vCenter Server. Nelle distribuzioni NetApp HCI , il nome utente è "root" e la password è stata specificata durante l'installazione iniziale di quel nodo di elaborazione nel NetApp Deployment Engine. A seconda della versione di VMware vSphere distribuita, anche alcuni amministratori nel dominio vSphere Single Sign-on possono accedere all'appliance. Nessun impatto sugli altri componenti.	Non sono necessarie modifiche.
Credenziali di amministratore del nodo di gestione NetApp 	Si applica a: NetApp HCI e facoltativo in SolidFire Gli amministratori possono accedere alle macchine virtuali del nodo di gestione NetApp per la configurazione avanzata e la risoluzione dei problemi. A seconda della versione del nodo di gestione implementata, l'accesso tramite SSH non è abilitato per impostazione predefinita. Nelle distribuzioni NetApp HCI , il nome utente e la password venivano specificati dall'utente durante l'installazione iniziale del nodo di elaborazione in NetApp Deployment Engine. Nessun impatto sugli altri componenti.	Non sono necessarie modifiche.

Trova maggiori informazioni

- ["Cambia il certificato SSL predefinito del software Element"](#)
- ["Cambia la password IPMI per i nodi"](#)
- ["Abilita l'autenticazione a più fattori"](#)
- ["Inizia con la gestione delle chiavi esterne"](#)
- ["Creare un cluster che supporti le unità FIPS"](#)

Cambia il certificato SSL predefinito del software Element

È possibile modificare il certificato SSL predefinito e la chiave privata del nodo di archiviazione nel cluster utilizzando l'API NetApp Element .

Quando viene creato un cluster software NetApp Element , il cluster crea un certificato Secure Sockets Layer (SSL) autofirmato univoco e una chiave privata che vengono utilizzati per tutte le comunicazioni HTTPS tramite l'interfaccia utente Element, l'interfaccia utente per nodo o le API. Il software Element supporta sia i certificati autofirmati sia i certificati emessi e verificati da un'autorità di certificazione (CA) attendibile.

È possibile utilizzare i seguenti metodi API per ottenere maggiori informazioni sul certificato SSL predefinito e apportare modifiche.

- **OttieniCertificatoSSL**

Puoi usare il "[Metodo GetSSLCertificate](#)" per recuperare informazioni sul certificato SSL attualmente installato, compresi tutti i dettagli del certificato.

- **SetSSLCertificate**

Puoi usare il "[Metodo SetSSLCertificate](#)" per impostare i certificati SSL del cluster e per nodo sul certificato e sulla chiave privata forniti. Il sistema convalida il certificato e la chiave privata per impedire che venga applicato un certificato non valido.

- **RimuoviCertificatoSSL**

IL "[Metodo RemoveSSLCertificate](#)" rimuove il certificato SSL e la chiave privata attualmente installati. Il cluster genera quindi un nuovo certificato autofirmato e una chiave privata.



Il certificato SSL del cluster viene applicato automaticamente a tutti i nuovi nodi aggiunti al cluster. Qualsiasi nodo rimosso dal cluster torna a essere un certificato autofirmato e tutte le informazioni sui certificati e sulle chiavi definite dall'utente vengono rimosse dal nodo.

Trova maggiori informazioni

- "[Modificare il certificato SSL predefinito del nodo di gestione](#)"
- "[Quali sono i requisiti per l'impostazione di certificati SSL personalizzati in Element Software?](#)"
- "[Documentazione del software SolidFire ed Element](#)"
- "[Plug-in NetApp Element per vCenter Server](#)"

Cambia la password IPMI predefinita per i nodi

È possibile modificare la password predefinita dell'amministratore dell'Intelligent Platform Management Interface (IPMI) non appena si ottiene l'accesso IPMI remoto al nodo. Potrebbe essere opportuno farlo se ci sono aggiornamenti di installazione.

Per i dettagli sulla configurazione dell'accesso IPM per i nodi, vedere "[Configurare IPMI per ogni nodo](#)".

È possibile modificare la password IPM per questi nodi:

- Nodi H410S
- Nodi H610S

Modificare la password IPMI predefinita per i nodi H410S

È necessario modificare la password predefinita per l'account amministratore IPMI su ciascun nodo di archiviazione non appena si configura la porta di rete IPMI.

Cosa ti servirà

Dovresti aver configurato l'indirizzo IP IPMI per ciascun nodo di archiviazione.

Passi

1. Aprire un browser Web su un computer in grado di raggiungere la rete IPMI e andare all'indirizzo IP IPMI del nodo.
2. Inserisci il nome utente `ADMIN` e password `ADMIN` nel prompt di accesso.
3. Dopo aver effettuato l'accesso, fare clic sulla scheda **Configurazione**.
4. Fare clic su **Utenti**.
5. Seleziona il `ADMIN` utente e fare clic su **Modifica utente**.
6. Selezionare la casella di controllo **Cambia password**.
7. Inserisci una nuova password nei campi **Password** e **Conferma password**.
8. Fare clic su **Modifica**, quindi su **OK**.
9. Ripetere questa procedura per tutti gli altri nodi H410S con password IPMI predefinite.

Modificare la password IPMI predefinita per i nodi H610S

È necessario modificare la password predefinita per l'account amministratore IPMI su ciascun nodo di archiviazione non appena si configura la porta di rete IPMI.

Cosa ti servirà

Dovresti aver configurato l'indirizzo IP IPMI per ciascun nodo di archiviazione.

Passi

1. Aprire un browser Web su un computer in grado di raggiungere la rete IPMI e andare all'indirizzo IP IPMI del nodo.
2. Inserisci il nome utente `root` e password `calvin` nel prompt di accesso.
3. Dopo aver effettuato l'accesso, clicca sull'icona di navigazione del menu in alto a sinistra della pagina per aprire il cassetto della barra laterale.
4. Fare clic su **Impostazioni**.
5. Fare clic su **Gestione utenti**.
6. Selezionare l'utente **Amministratore** dall'elenco.
7. Abilitare la casella di controllo **Cambia password**.
8. Inserisci una nuova password complessa nei campi **Password** e **Conferma password**.
9. Fare clic su **Salva** in fondo alla pagina.
10. Ripetere questa procedura per tutti gli altri nodi H610S con password IPMI predefinite.

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Informazioni sul copyright

Copyright © 2025 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.