# Configurare le opzioni del sistema SolidFire dopo l'implementazione

Element Software

NetApp
October 01, 2024

# Sommario

# Configurare le opzioni del sistema SolidFire dopo l'implementazione

Dopo aver configurato il sistema SolidFire, è possibile eseguire alcune attività facoltative.

Se si modificano le credenziali nel sistema, potrebbe essere necessario conoscere l'impatto su altri componenti.

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

## Trova ulteriori informazioni

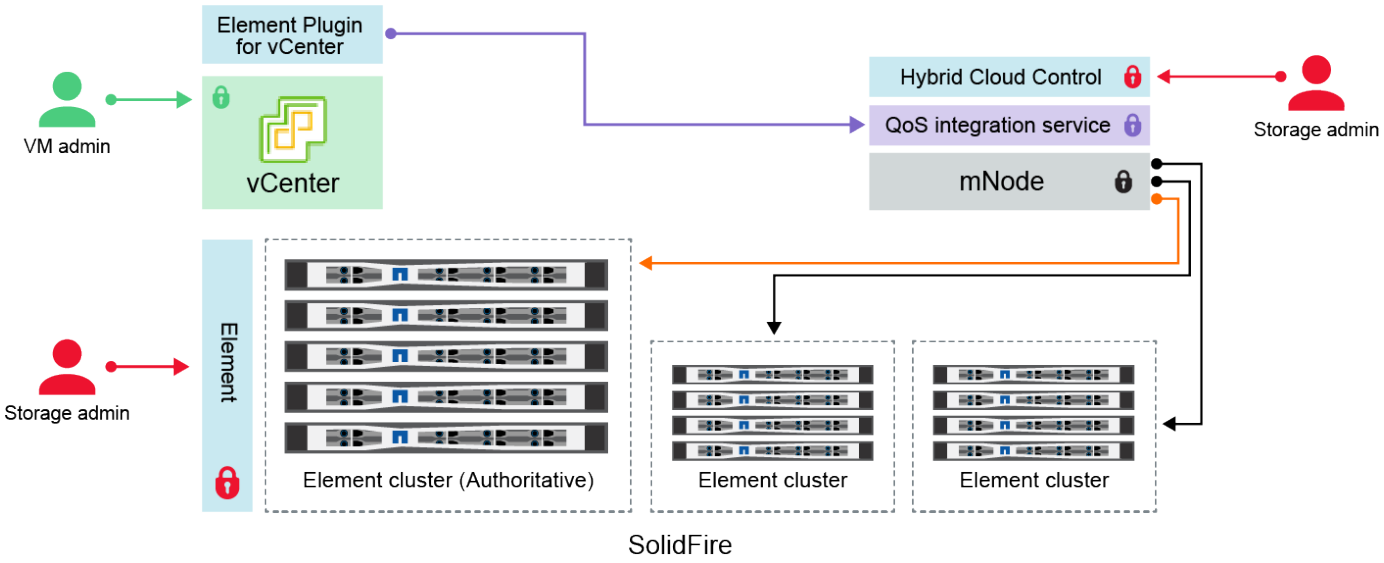
- "Modificare le credenziali in NetApp HCI e NetApp SolidFire"
- "Modificare il certificato SSL predefinito del software Element"
- "Modificare la password IPMI per i nodi"
- "Abilitare l'autenticazione a più fattori"
- "Inizia a utilizzare la gestione esterna delle chiavi"
- "Creare un cluster che supporti i dischi 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 è generalmente parte delle procedure di sicurezza. Prima di modificare le password, è necessario essere consapevoli dell'impatto sugli altri componenti software nell'implementazione.

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

Interazioni dei componenti NetApp SolidFire:




| Tipo di credenziale e icona | Utilizzo da parte dell'amministratore | Consultare queste istruzioni |
|---|---|---|
| Credenziali dell'elemento  | **Applicabile a**: NetApp HCI e SolidFire<br><br>Gli amministratori utilizzano queste credenziali per accedere a:<br><br>• Interfaccia utente Element sul cluster di storage Element<br>• Controllo del cloud ibrido sul nodo di gestione (mnode)<br><br>Quando Hybrid Cloud Control gestisce più cluster di storage, accetta solo le credenziali di amministratore per i cluster di storage, noto come *cluster autorevole* per cui è stato inizialmente configurato mnode. Per i cluster di storage aggiunti in seguito a Hybrid Cloud Control, mnode memorizza in modo sicuro le credenziali di amministratore. Se le credenziali per i cluster di storage aggiunti successivamente vengono modificate, le credenziali devono essere aggiornate anche in mnode utilizzando l'API mnode. | • "Aggiornare le password di amministrazione del cluster di storage."<br><br>• Aggiornare le credenziali di amministratore del cluster di archiviazione nel mnode utilizzando "API modifyclusteradmin". |

| Tipo di credenziale e icona | Utilizzo da parte dell'amministratore | Consultare queste istruzioni |
|---|---|---|
| Credenziali vSphere Single Sign-on  | **Applicabile a**: Solo NetApp HCI<br><br>Gli amministratori utilizzano queste credenziali per accedere a VMware vSphere Client. Quando vCenter fa parte dell'installazione di NetApp HCI, le credenziali vengono configurate nel motore di implementazione NetApp come segue:<br><br>• username@vsphere.local con la password specificata, e.<br>• administrator@vsphere.local con la password specificata. Quando si utilizza un vCenter esistente per implementare NetApp HCI, le credenziali di accesso singolo vSphere vengono gestite dagli amministratori IT VMware. | "Aggiornare le credenziali vCenter ed ESXi". |
| Credenziali BMC (Baseboard Management Controller)  | **Applicabile a**: Solo NetApp HCI<br><br>Gli amministratori utilizzano queste credenziali per accedere al BMC dei nodi di calcolo NetApp in un'implementazione NetApp HCI. BMC offre funzioni di base per il monitoraggio dell'hardware e la console virtuale.<br><br>Le credenziali BMC (a volte denominate *IPMI*) per ciascun nodo di calcolo NetApp vengono memorizzate in modo sicuro sull'mnode nelle implementazioni NetApp HCI. NetApp Hybrid Cloud Control utilizza le credenziali BMC in una capacità di account di servizio per comunicare con BMC nei nodi di calcolo durante gli aggiornamenti del firmware del nodo di calcolo.<br><br>Quando le credenziali BMC vengono modificate, le credenziali per i rispettivi nodi di calcolo devono essere aggiornate anche su mnode per mantenere tutte le funzionalità di controllo del cloud ibrido. | • "Configurare IPMI per ogni nodo su NetApp HCI".<br>• Per i nodi H410C, H610C e H615C, "Modificare la password IPMI predefinita".<br>• Per H410S e H610S nodi, "Modificare la password IPM predefinita".<br>• "Modificare le credenziali BMC sul nodo di gestione". |

| Tipo di credenziale e icona | Utilizzo da parte dell'amministratore | Consultare queste istruzioni |
|---|---|---|
| Credenziali ESXi  | **Applicabile a**: Solo NetApp HCI<br><br>Gli amministratori possono accedere agli host ESXi utilizzando SSH o DCUI locale con un account root locale. Nelle implementazioni NetApp HCI, il nome utente è "root" e la password è stata specificata durante l'installazione iniziale del nodo di calcolo nel motore di implementazione NetApp.<br><br>Le credenziali radice ESXi per ciascun nodo di calcolo NetApp vengono memorizzate in modo sicuro sull'mnode nelle implementazioni 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 calcolo e i controlli dello stato.<br><br>Quando le credenziali root di ESXi vengono modificate da un amministratore VMware, le credenziali per i rispettivi nodi di calcolo devono essere aggiornate su mnode per mantenere la funzionalità di controllo del cloud ibrido. | "Aggiorna le credenziali per gli host vCenter e ESXi". |
| Password di integrazione QoS  | **Applicabile a**: NetApp HCI e opzionale in SolidFire<br><br>Non utilizzato dagli amministratori per gli accessi interattivi.<br><br>L'integrazione QoS tra VMware vSphere ed Element Software è abilitata tramite:<br><br>• Plug-in Element per vCenter Server e.<br>• Servizio QoS su mnode.<br><br>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 o generata automaticamente durante l'implementazione di NetApp HCI.<br><br>Nessun impatto su altri componenti. | "Aggiornare le credenziali QoSSIOC nel plug-in NetApp Element per vCenter Server".<br><br>Il plug-in NetApp Element per la password SIOC del server vCenter è noto anche come *password QoSSIOC*.<br><br>Consulta l'articolo Element Plug-in for vCenter Server KB article. |

| Tipo di credenziale e icona | Utilizzo da parte dell'amministratore | Consultare queste istruzioni |
|---|---|---|
| Credenziali di vCenter Service Appliance  | **Applicabile a**: NetApp HCI solo se configurato dal motore di implementazione NetApp<br><br>Gli amministratori possono accedere alle macchine virtuali dell'appliance vCenter Server. Nelle implementazioni NetApp HCI, il nome utente è "root" e la password è stata specificata durante l'installazione iniziale del nodo di calcolo nel motore di implementazione NetApp. A seconda della versione di VMware vSphere implementata, alcuni amministratori del dominio di Single Sign-on di vSphere possono anche accedere all'appliance.<br><br>Nessun impatto su altri componenti. | Non sono necessarie modifiche. |
| Credenziali amministratore di NetApp Management Node  | **Applicabile a**: NetApp HCI e opzionale in SolidFire<br><br>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 attivato per impostazione predefinita.<br><br>Nelle distribuzioni NetApp HCI, il nome utente e la password sono stati specificati dall'utente durante l'installazione iniziale di quel nodo di calcolo nel motore di distribuzione NetApp.<br><br>Nessun impatto su altri componenti. | Non sono necessarie modifiche. |

### Trova ulteriori informazioni

- "Modificare il certificato SSL predefinito del software Element"
- "Modificare la password IPMI per i nodi"
- "Abilitare l'autenticazione a più fattori"
- "Inizia a utilizzare la gestione esterna delle chiavi"
- "Creare un cluster che supporti i dischi FIPS"

# Modificare il certificato SSL predefinito del software Element

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

Quando viene creato un cluster software NetApp Element, il cluster crea un certificato SSL (Secure Sockets Layer) con firma automatica e una chiave privata univoci 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

i certificati autofirmati e quelli emessi e verificati da un'autorità di certificazione (CA) attendibile.

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

- **GetSSLCertificate**

  È possibile utilizzare "Metodo GetSSLCertificate"per recuperare le informazioni sul certificato SSL attualmente installato, inclusi tutti i dettagli del certificato.

- **SetSSLCertificate**

  È possibile utilizzare "Metodo SetSSLCertificate"per impostare i certificati SSL per cluster e per nodo sul certificato e sulla chiave privata forniti. Il sistema convalida il certificato e la chiave privata per impedire l'applicazione di un certificato non valido.

- **RemoveSSLCertificate**

  "Metodo RemoveSSLCertificate"Rimuove il certificato SSL e la chiave privata attualmente installati. Il cluster genera quindi un nuovo certificato autofirmato e una nuova chiave privata.

> Il certificato SSL del cluster viene applicato automaticamente a tutti i nuovi nodi aggiunti al cluster. Tutti i nodi rimossi dal cluster tornano a un certificato autofirmato e tutte le informazioni di certificato e chiave definite dall'utente vengono rimosse dal nodo.

### Trova ulteriori informazioni

- "Modificare il certificato SSL predefinito del nodo di gestione"
- "Quali sono i requisiti relativi all'impostazione di certificati SSL personalizzati in Element Software?"
- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

# Modificare la password IPMI predefinita per i nodi

È possibile modificare la password di amministratore predefinita di Intelligent Platform Management Interface (IPMI) non appena si dispone dell'accesso remoto IPMI al nodo. Questa operazione potrebbe essere utile se sono stati rilevati aggiornamenti per l'installazione.

Per informazioni dettagliate sulla configurazione dell'accesso IPM per i nodi, vedere "Configurare IPMI per ciascun nodo".

È possibile modificare la password IPM per questi nodi:

- H410S nodi
- H610S nodi

### Modificare la password IPMI predefinita per H410S nodi

È necessario modificare la password predefinita per l'account amministratore IPMI su ciascun nodo di storage

non appena si configura la porta di rete IPMI.

**Di cosa hai bisogno**

L'indirizzo IP IPMI dovrebbe essere stato configurato per ciascun nodo di storage.

**Fasi**

1. Aprire un browser Web su un computer in grado di raggiungere la rete IPMI e individuare l'indirizzo IP IPMI del nodo.
2. Inserire il nome utente `ADMIN` e la password `ADMIN` nel prompt di accesso.
3. Una volta effettuato l'accesso, fare clic sulla scheda **Configuration** (Configurazione).
4. Fare clic su **utenti**.
5. Selezionare l' `ADMIN`utente e fare clic su **Modifica utente**.
6. Selezionare la casella di controllo **Change Password** (Modifica password).
7. Immettere una nuova password nei campi **Password** e **Conferma password**.
8. Fare clic su **Modify**, quindi su **OK**.
9. Ripetere questa procedura per tutti gli altri nodi H410S con password IPMI predefinite.

## Modificare la password IPMI predefinita per H610S nodi

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

**Di cosa hai bisogno**

L'indirizzo IP IPMI dovrebbe essere stato configurato per ciascun nodo di storage.

**Fasi**

1. Aprire un browser Web su un computer in grado di raggiungere la rete IPMI e individuare l'indirizzo IP IPMI del nodo.
2. Inserire il nome utente `root` e la password `calvin` nel prompt di accesso.
3. Una volta effettuato l'accesso, fare clic 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 **Administrator** dall'elenco.
7. Attivare la casella di controllo **Change Password** (Modifica password).
8. Immettere una nuova password complessa nei campi **Password** e **Conferma password**.
9. Fare clic su **Save** (Salva) nella parte inferiore della pagina.
10. Ripetere questa procedura per tutti gli altri nodi H610S con password IPMI predefinite.

## Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"