



Konfigurieren Sie die SolidFire -Systemoptionen nach der Bereitstellung Element Software

NetApp
November 12, 2025

Inhalt

- Konfigurieren Sie die SolidFire -Systemoptionen nach der Bereitstellung 1
 - Konfigurieren Sie die SolidFire -Systemoptionen nach der Bereitstellung 1
 - Weitere Informationen 1
 - Ändern Sie die Anmeldeinformationen in NetApp HCI und NetApp SolidFire 1
 - Weitere Informationen 5
 - Ändern Sie das standardmäßige SSL-Zertifikat der Element-Software. 5
 - Weitere Informationen 6
 - Ändern des Standard-IPMI-Passworts für Knoten 6
 - Ändern Sie das Standard-IPMI-Passwort für H410S-Knoten. 7
 - Ändern Sie das Standard-IPMI-Passwort für H610S-Knoten. 7
 - Weitere Informationen 8

Konfigurieren Sie die SolidFire -Systemoptionen nach der Bereitstellung

Konfigurieren Sie die SolidFire -Systemoptionen nach der Bereitstellung

Nach der Einrichtung Ihres SolidFire -Systems können Sie optional einige Aufgaben ausführen.

Wenn Sie die Zugangsdaten im System ändern, möchten Sie möglicherweise wissen, welche Auswirkungen dies auf andere Komponenten hat.

Darüber hinaus können Sie Einstellungen für die Multi-Faktor-Authentifizierung, die Verwaltung externer Schlüssel und die Sicherheit gemäß den Federal Information Processing Standards (FIPS) konfigurieren. Sie sollten auch Ihre Passwörter gegebenenfalls aktualisieren.

Weitere Informationen

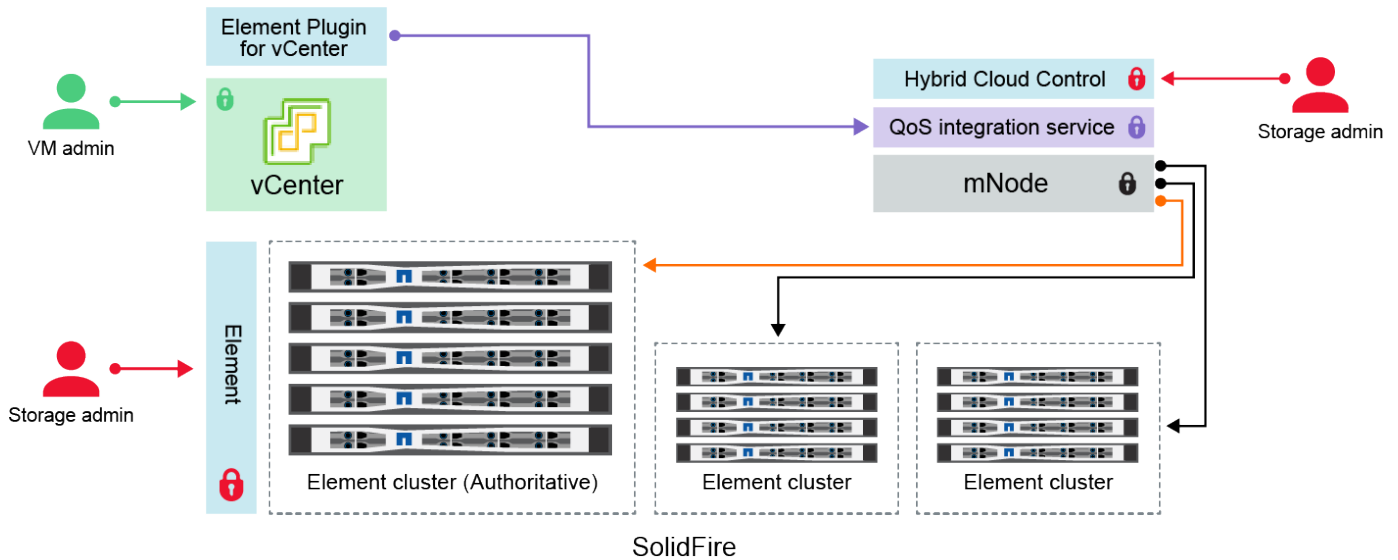
- ["Ändern Sie die Anmeldeinformationen in NetApp HCI und NetApp SolidFire"](#)
- ["Ändern Sie das standardmäßige SSL-Zertifikat der Element-Software."](#)
- ["Ändern Sie das IPMI-Passwort für die Knoten."](#)
- ["Aktivieren Sie die Multi-Faktor-Authentifizierung"](#)
- ["Erste Schritte zur externen Schlüsselverwaltung"](#)
- ["Erstellen Sie einen Cluster, der FIPS-Laufwerke unterstützt."](#)

Ändern Sie die Anmeldeinformationen in NetApp HCI und NetApp SolidFire

Je nach den Sicherheitsrichtlinien der Organisation, die NetApp HCI oder NetApp SolidFire eingesetzt hat, ist das Ändern von Anmeldeinformationen oder Passwörtern üblicherweise Teil der Sicherheitsmaßnahmen. Bevor Sie Passwörter ändern, sollten Sie sich über die Auswirkungen auf andere Softwarekomponenten in der Bereitstellung im Klaren sein.

Wenn Sie die Zugangsdaten für eine Komponente einer NetApp HCI oder NetApp SolidFire Bereitstellung ändern, bietet Ihnen die folgende Tabelle Hinweise zu den Auswirkungen auf andere Komponenten.

NetApp SolidFire -
Komponenteninteraktionen:



- 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

Anmeldeinformationstyp und Symbol	Nutzung durch den Administrator	Siehe diese Anweisungen
Element-Anmeldeinformationen 	Gilt für: NetApp HCI und SolidFire Administratoren verwenden diese Anmeldeinformationen, um sich anzumelden: • Element-Benutzeroberfläche auf dem Element-Speichercluster • Hybrid Cloud Control auf dem Management-Knoten (mnode) Wenn Hybrid Cloud Control mehrere Speichercluster verwaltet, akzeptiert es nur die Administratoranmeldeinformationen für die Speichercluster, die als <i>autoritativer Cluster</i> bezeichnet werden und für die der mnode ursprünglich eingerichtet wurde. Für Speichercluster, die später zu Hybrid Cloud Control hinzugefügt werden, speichert der mnode die Administratoranmeldeinformationen sicher. Wenn die Zugangsdaten für nachfolgend hinzugefügte Speichercluster geändert werden, müssen die Zugangsdaten auch im mnode mithilfe der mnode-API aktualisiert werden.	• "Aktualisieren Sie die Administrator Kennwörter des Speicherclusters." • Aktualisieren Sie die Administratoranmeldeinformationen des Speicherclusters im mnode mithilfe der "ModifyClusterAdmin-API" Die

Anmeldeinformationenstyp und Symbol	Nutzung durch den Administrator	Siehe diese Anweisungen
vSphere Single Sign-on-Anmeldeinformationen 	Gilt nur für NetApp HCI Administratoren verwenden diese Anmeldeinformationen, um sich beim VMware vSphere Client anzumelden. Wenn vCenter Teil der NetApp HCI Installation ist, werden die Anmeldeinformationen in der NetApp Deployment Engine wie folgt konfiguriert: • username@vsphere.local mit dem angegebenen Passwort und • administrator@vsphere.local mit dem angegebenen Passwort. Wird ein bestehendes vCenter für die Bereitstellung von NetApp HCI verwendet, werden die vSphere Single Sign-on-Anmeldeinformationen von den IT-VMware-Administratoren verwaltet.	"vCenter- und ESXi-Anmeldeinformationen aktualisieren" .
Anmeldeinformationen für den Baseboard Management Controller (BMC) 	Gilt nur für NetApp HCI Administratoren verwenden diese Anmeldeinformationen, um sich beim BMC der NetApp -Rechenknoten in einer NetApp HCI Bereitstellung anzumelden. Das BMC bietet grundlegende Hardware-Überwachungs- und virtuelle Konsolenfunktionen. Die BMC Zugangsdaten (manchmal auch als <i>IPMI</i> bezeichnet) für jeden NetApp Rechenknoten werden in NetApp HCI Bereitstellungen sicher auf dem Knoten gespeichert. NetApp Hybrid Cloud Control verwendet BMC -Anmeldeinformationen in Form eines Servicekontos, um während Firmware-Upgrades der Compute-Knoten mit dem BMC in den Compute-Knoten zu kommunizieren. Wenn die BMC -Zugangsdaten geändert werden, müssen auch die Zugangsdaten für die jeweiligen Compute-Knoten auf dem mnode aktualisiert werden, um die gesamte Funktionalität von Hybrid Cloud Control zu erhalten.	• "Konfigurieren Sie IPMI für jeden Knoten auf NetApp HCI." • Für die Knoten H410C, H610C und H615C, "Standard-IPMI-Passwort ändern" Die • Für H410S- und H610S-Knoten, "Standard-IPMI-Passwort ändern" Die • "Ändern Sie die BMC Anmeldeinformationen auf dem Verwaltungsknoten."

Anmeldeinformationenstyp und Symbol	Nutzung durch den Administrator	Siehe diese Anweisungen
ESXi-Anmeldeinformationen 	Gilt nur für NetApp HCI Administratoren können sich mit einem lokalen Root-Konto entweder über SSH oder über die lokale DCUI in ESXi-Hosts einloggen. Bei NetApp HCI -Bereitstellungen lautet der Benutzername „root“ und das Passwort wurde bei der Erstinstallation dieses Rechenknotens in der NetApp Deployment Engine festgelegt. Die ESXi-Root-Anmeldeinformationen für jeden NetApp Rechenknoten werden in NetApp HCI Bereitstellungen sicher auf dem mnode gespeichert. NetApp Hybrid Cloud Control nutzt die Anmeldeinformationen eines Servicekontos, um während Firmware-Upgrades und Integritätsprüfungen von Compute-Knoten direkt mit ESXi-Hosts zu kommunizieren. Wenn die ESXi-Root-Anmeldeinformationen von einem VMware-Administrator geändert werden, müssen die Anmeldeinformationen für die jeweiligen Compute-Knoten auf dem mnode aktualisiert werden, um die Hybrid Cloud Control-Funktionalität beizubehalten.	"Aktualisieren Sie die Anmeldeinformationen für vCenter- und ESXi-Hosts."
QoS-Integrationspasswort 	Gilt für: NetApp HCI und optional in SolidFire Wird nicht für interaktive Anmeldungen durch Administratoren verwendet. Die QoS-Integration zwischen VMware vSphere und Element Software wird durch Folgendes ermöglicht: • Element-Plug-in für vCenter Server und • QoS-Dienst auf dem mnode. Zur Authentifizierung verwendet der QoS-Dienst ein Passwort, das ausschließlich in diesem Kontext verwendet wird. Das QoS-Passwort wird bei der Erstinstallation des Element-Plug-ins für vCenter Server festgelegt oder während der NetApp HCI Bereitstellung automatisch generiert. Keine Auswirkungen auf andere Komponenten.	"Aktualisieren Sie die QoSSIOC-Anmeldeinformationen im NetApp Element Plug-in für vCenter Server". Das NetApp Element Plug-in für vCenter Server SIOC-Passwort ist auch als <i>QoSSIOC-Passwort</i> bekannt. Lesen Sie den Element Plug-in for vCenter Server KB article.

Anmeldeinformationstyp und Symbol	Nutzung durch den Administrator	Siehe diese Anweisungen
Anmeldeinformationen für die vCenter Service Appliance 	Gilt nur für NetApp HCI , wenn die Einrichtung über die NetApp Deployment Engine erfolgte. Administratoren können sich in die virtuellen Maschinen der vCenter Server Appliance einloggen. Bei NetApp HCI -Bereitstellungen lautet der Benutzername „root“ und das Passwort wurde bei der Erstinstallation dieses Rechenknotens in der NetApp Deployment Engine festgelegt. Je nach eingesetzter VMware vSphere-Version können sich auch bestimmte Administratoren in der vSphere Single Sign-on-Domäne an der Appliance anmelden. Keine Auswirkungen auf andere Komponenten.	Es sind keine Änderungen erforderlich.
NetApp Management Node-Administratoranmeldinformationen 	Gilt für: NetApp HCI und optional in SolidFire Administratoren können sich für erweiterte Konfigurations- und Fehlerbehebungsmaßnahmen in die virtuellen Maschinen des NetApp Management-Knotens einloggen. Je nach eingesetzter Management-Node-Version ist die Anmeldung via SSH nicht standardmäßig aktiviert. Bei NetApp HCI Bereitstellungen wurden Benutzername und Passwort vom Benutzer während der Erstinstallation des jeweiligen Rechenknotens in der NetApp Deployment Engine festgelegt. Keine Auswirkungen auf andere Komponenten.	Es sind keine Änderungen erforderlich.

Weitere Informationen

- ["Ändern Sie das standardmäßige SSL-Zertifikat der Element-Software."](#)
- ["Ändern Sie das IPMI-Passwort für die Knoten."](#)
- ["Aktivieren Sie die Multi-Faktor-Authentifizierung"](#)
- ["Erste Schritte zur externen Schlüsselverwaltung"](#)
- ["Erstellen Sie einen Cluster, der FIPS-Laufwerke unterstützt."](#)

Ändern Sie das standardmäßige SSL-Zertifikat der Element-Software.

Sie können das Standard-SSL-Zertifikat und den privaten Schlüssel des Speicherknotens im Cluster mithilfe der NetApp Element API ändern.

Wenn ein NetApp Element Softwarecluster erstellt wird, erzeugt der Cluster ein eindeutiges selbstsigniertes

Secure Sockets Layer (SSL)-Zertifikat und einen privaten Schlüssel, der für die gesamte HTTPS-Kommunikation über die Element-Benutzeroberfläche, die Benutzeroberfläche pro Knoten oder APIs verwendet wird. Die Element-Software unterstützt sowohl selbstsignierte Zertifikate als auch Zertifikate, die von einer vertrauenswürdigen Zertifizierungsstelle (CA) ausgestellt und verifiziert werden.

Sie können die folgenden API-Methoden verwenden, um weitere Informationen über das Standard-SSL-Zertifikat zu erhalten und Änderungen vorzunehmen.

- **GetSSLCertificate**

Sie können die "[GetSSLCertificate-Methode](#)" Informationen über das aktuell installierte SSL-Zertifikat einschließlich aller Zertifikatsdetails abrufen.

- **SetSSLCertificate**

Sie können die "[SetSSLCertificate-Methode](#)" um die Cluster- und knotenspezifischen SSL-Zertifikate auf das von Ihnen bereitgestellte Zertifikat und den privaten Schlüssel festzulegen. Das System überprüft das Zertifikat und den privaten Schlüssel, um die Anwendung eines ungültigen Zertifikats zu verhindern.

- **RemoveSSLCertificate**

Der "[RemoveSSLCertificate-Methode](#)" Entfernt das aktuell installierte SSL-Zertifikat und den zugehörigen privaten Schlüssel. Der Cluster generiert anschließend ein neues selbstsigniertes Zertifikat und einen privaten Schlüssel.



Das Cluster-SSL-Zertifikat wird automatisch auf alle neu zum Cluster hinzugefügten Knoten angewendet. Jeder aus dem Cluster entfernte Knoten verwendet wieder ein selbstsigniertes Zertifikat, und alle benutzerdefinierten Zertifikats- und Schlüsselinformationen werden vom Knoten entfernt.

Weitere Informationen

- "[Ändern Sie das Standard-SSL-Zertifikat des Verwaltungsknotens.](#)"
- "[Welche Anforderungen gelten für die Einrichtung benutzerdefinierter SSL-Zertifikate in Element Software?](#)"
- "[SolidFire und Element-Softwaredokumentation](#)"
- "[NetApp Element Plug-in für vCenter Server](#)"

Ändern des Standard-IPMI-Passworts für Knoten

Sie können das Standard-Administratorkennwort der Intelligent Platform Management Interface (IPMI) ändern, sobald Sie über Remote-IPMI-Zugriff auf den Knoten verfügen. Dies sollten Sie gegebenenfalls tun, falls es Installationsaktualisierungen gibt.

Einzelheiten zur Konfiguration des IPM-Zugriffs für Knoten finden Sie unter "[IPMI für jeden Knoten konfigurieren](#)" Die

Sie können das IPM-Passwort für diese Knoten ändern:

- H410S-Knoten

- H610S-Knoten

Ändern Sie das Standard-IPMI-Passwort für H410S-Knoten.

Sie sollten das Standardkennwort für das IPMI-Administratorkonto auf jedem Speicherknoten ändern, sobald Sie den IPMI-Netzwerkport konfiguriert haben.

Was du brauchst

Sie sollten die IPMI-IP-Adresse für jeden Speicherknoten konfiguriert haben.

Schritte

1. Öffnen Sie einen Webbrowser auf einem Computer, der auf das IPMI-Netzwerk zugreifen kann, und rufen Sie die IPMI-IP-Adresse des Knotens auf.
2. Geben Sie den Benutzernamen ein `ADMIN` und Passwort `ADMIN` im Anmeldefenster.
3. Klicken Sie nach dem Einloggen auf die Registerkarte **Konfiguration**.
4. Klicken Sie auf **Benutzer**.
5. Wählen Sie die `ADMIN` Benutzer und klicken Sie auf **Benutzer bearbeiten**.
6. Aktivieren Sie das Kontrollkästchen **Passwort ändern**.
7. Geben Sie in den Feldern **Passwort** und **Passwort bestätigen** ein neues Passwort ein.
8. Klicken Sie auf **Ändern** und anschließend auf **OK**.
9. Wiederholen Sie diese Prozedur für alle anderen H410S-Knoten mit Standard-IPMI-Passwörtern.

Ändern Sie das Standard-IPMI-Passwort für H610S-Knoten.

Sie sollten das Standardkennwort für das IPMI-Administratorkonto auf jedem Speicherknoten ändern, sobald Sie den IPMI-Netzwerkport konfiguriert haben.

Was du brauchst

Sie sollten die IPMI-IP-Adresse für jeden Speicherknoten konfiguriert haben.

Schritte

1. Öffnen Sie einen Webbrowser auf einem Computer, der auf das IPMI-Netzwerk zugreifen kann, und rufen Sie die IPMI-IP-Adresse des Knotens auf.
2. Geben Sie den Benutzernamen ein `root` und Passwort `calvin` im Anmeldefenster.
3. Nach dem Einloggen klicken Sie auf das Menünavigationssymbol oben links auf der Seite, um die Seitenleiste zu öffnen.
4. Klicken Sie auf **Einstellungen**.
5. Klicken Sie auf **Benutzerverwaltung**.
6. Wählen Sie den **Administrator**-Benutzer aus der Liste aus.
7. Aktivieren Sie das Kontrollkästchen **Passwort ändern**.
8. Geben Sie in den Feldern **Passwort** und **Passwort bestätigen** ein neues, sicheres Passwort ein.
9. Klicken Sie unten auf der Seite auf **Speichern**.
10. Wiederholen Sie diese Prozedur für alle anderen H610S-Knoten mit Standard-IPMI-Passwörtern.

Weitere Informationen

- ["SolidFire und Element-Softwaredokumentation"](#)
- ["NetApp Element Plug-in für vCenter Server"](#)

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.