Konfigurieren Sie nach der Bereitstellung die SolidFire Systemoptionen

Element Software

NetApp
January 15, 2024

Inhalt

Konfigurieren Sie nach der Bereitstellung die SolidFire Systemoptionen 1
Weitere Informationen 1
Anmeldedaten in NetApp HCI und NetApp SolidFire ändern 1
Ändern Sie das Standard-SSL-Zertifikat der Element Software 5
Ändern Sie das Standard-IPMI-Passwort für Nodes 6

Konfigurieren Sie nach der Bereitstellung die SolidFire Systemoptionen

Nach der Einrichtung des SolidFire Systems sollten Sie möglicherweise einige optionale Aufgaben ausführen.

Wenn Sie die Anmeldedaten im System ändern, sollten Sie die Auswirkungen auf andere Komponenten kennen.

Darüber hinaus können Einstellungen für Multi-Faktor-Authentifizierung, externes Verschlüsselungsmanagement und die Sicherheit von Federal Information Processing Standards (FIPS) konfiguriert werden. Sie sollten sich auch die Aktualisierung von Kennwörtern ansehen, wenn nötig.

Weitere Informationen

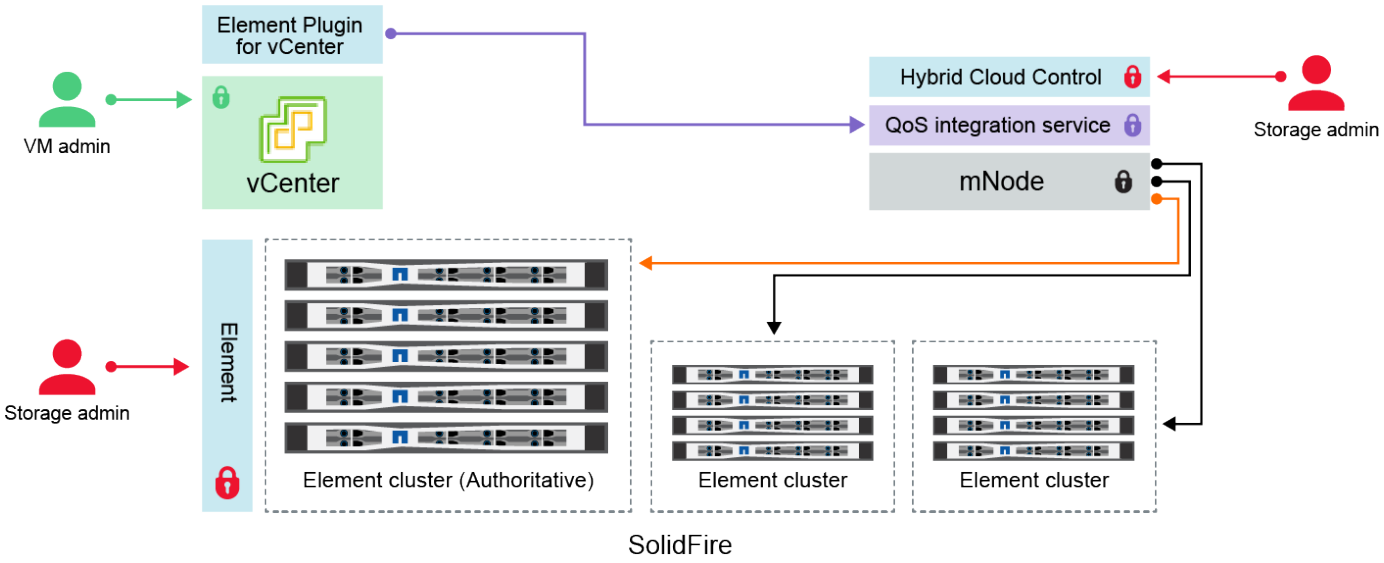
- "Anmeldedaten in NetApp HCI und NetApp SolidFire ändern"
- "Ändern Sie das Standard-SSL-Zertifikat der Element Software"
- "Ändern Sie das IPMI-Passwort für Knoten"
- "Multi-Faktor-Authentifizierung aktivieren"
- "Erste Schritte mit externem Verschlüsselungsmanagement"
- "Erstellen eines Clusters, das FIPS-Laufwerke unterstützt"

Anmeldedaten in NetApp HCI und NetApp SolidFire ändern

Abhängig von den Sicherheitsrichtlinien im Unternehmen, die NetApp HCI oder NetApp SolidFire implementiert haben, gehört das Ändern von Anmeldedaten oder Passwörtern in der Regel zu den Sicherheitspraktiken. Bevor Sie Passwörter ändern, sollten Sie sich der Auswirkungen auf andere Softwarekomponenten in der Bereitstellung bewusst sein.

Wenn Sie die Anmeldedaten für eine Komponente einer NetApp HCI- oder NetApp SolidFire-Implementierung ändern, enthält die folgende Tabelle Anweisungen zu den Auswirkungen auf andere Komponenten.

Interaktionen von NetApp SolidFire-Komponenten:



Anmeldeinformationstyp und Symbol	Nutzung durch Admin	Siehe diese Anweisungen
Anmeldedaten für Element 	**Gilt für**: NetApp HCI und SolidFire Administratoren verwenden diese Anmeldedaten zur Anmeldung bei: • Element Benutzeroberfläche auf dem Element Storage-Cluster • Hybrid Cloud Control auf dem Management-Node (mNode) Wenn Hybrid Cloud Control mehrere Storage-Cluster managt, akzeptiert es nur die Admin-Anmeldeinformationen für die Storage-Cluster, bekannt als das *autorisierende Cluster*, für das der mNode ursprünglich eingerichtet wurde. Bei Storage-Clustern, die später zu Hybrid Cloud Control hinzugefügt werden, speichert der mNode die Anmeldedaten des Administrators sicher. Wenn Anmeldeinformationen für nachträglich hinzugefügte Speicher-Cluster geändert werden, müssen die Anmeldeinformationen auch im mnode mit der mNode-API aktualisiert werden.	• "Aktualisieren der Passwörter für den Storage-Cluster-Administrator." • Aktualisieren Sie die Anmeldedaten des Storage-Cluster-Administrators im mNode mithilfe des "Modifizierter clusteradmin API".

Anmeldeinformationstyp und Symbol	Nutzung durch Admin	Siehe diese Anweisungen
VSphere Single Sign On – Zugangsdaten 	**Gilt nur für**: NetApp HCI Administratoren verwenden diese Zugangsdaten, um sich beim VMware vSphere Client anzumelden. Wenn vCenter Teil der Installation von NetApp HCI ist, werden in der NetApp Deployment Engine die folgenden Anmeldedaten konfiguriert: • username@vsphere.local mit dem angegebenen Passwort, und • administrator@vsphere.local mit dem angegebenen Passwort. Wenn ein vorhandenes vCenter für die Implementierung von NetApp HCI verwendet wird, werden die Anmeldeinformationen für vSphere Single Sign-On von DEN IT-VMware-Administratoren gemanagt.	"Aktualisieren der vCenter- und ESXi-Anmeldedaten".
Baseboard Management Controller (BMC) Zugangsdaten 	**Gilt nur für**: NetApp HCI Administratoren melden sich mithilfe dieser Anmeldedaten beim BMC der NetApp Computing-Nodes in einer NetApp HCI-Implementierung an. Das BMC bietet grundlegende Hardware-Überwachung und Funktionen der virtuellen Konsole. BMC-Anmeldeinformationen (auch als „*IPMI*“ bezeichnet) für jeden NetApp Computing-Node werden in NetApp HCI-Implementierungen sicher auf dem mNode gespeichert. NetApp Hybrid Cloud Control verwendet BMC-Anmeldeinformationen in einem Service-Konto, um während eines Upgrades der Computing-Node-Firmware mit dem BMC in den Computing-Nodes zu kommunizieren. Wenn die BMC-Anmeldedaten geändert werden, müssen auch die Anmeldeinformationen für die jeweiligen Computing-Nodes auf dem mnode aktualisiert werden, damit alle Hybrid Cloud Control-Funktionen erhalten bleiben.	• "Konfigurieren Sie IPMI für jeden Node in NetApp HCI". • Für H410C, H610C und H615C Nodes "Ändern Sie das Standard-IPMI-Passwort". • Für H410S und H610S Nodes "Ändern Sie das IPM-Standardpasswort". • "Ändern Sie BMC-Anmeldeinformationen auf dem Management-Node".

Anmeldeinformationstyp und Symbol	Nutzung durch Admin	Siehe diese Anweisungen
ESXi Anmeldedaten 	**Gilt nur für**: NetApp HCI Administratoren können sich über SSH oder die lokale DCUI mit einem lokalen Root-Konto bei ESXi Hosts anmelden. In NetApp HCI-Implementierungen ist der Benutzername „root“, und das Passwort wurde bei der Erstinstallation dieses Computing-Node in der NetApp Deployment Engine angegeben. ESXi Root-Anmeldedaten für jeden NetApp Computing-Node werden in NetApp HCI-Implementierungen sicher auf dem mnode gespeichert. NetApp Hybrid Cloud Control verwendet die Zugangsdaten in der Kapazität eines Service-Kontos, um direkt während Upgrades der Firmware des Computing-Nodes und Zustandsprüfungen mit ESXi Hosts zu kommunizieren. Wenn die ESXi-Root-Anmeldedaten von einem VMware-Administrator geändert werden, müssen die Anmeldeinformationen für die jeweiligen Computing-Nodes auf dem mnode aktualisiert werden, damit die Hybrid Cloud Control-Funktionalität erhalten bleibt.	"Anmeldedaten für vCenter- und ESXi-Hosts aktualisieren".
Passwort für die QoS-Integration 	**Gilt für**: NetApp HCI und optional in SolidFire Nicht für interaktive Anmeldungen durch Administratoren verwendet. Die QoS-Integration zwischen VMware vSphere und Element Software wird durch folgende aktiviert: • Element Plug-in für vCenter Server und • QoS-Service auf dem mNode. Für die Authentifizierung verwendet der QoS-Service ein Passwort, das ausschließlich in diesem Zusammenhang verwendet wird. Das QoS-Passwort wird bei der Erstinstallation des Element Plug-in für vCenter Server angegeben oder während der NetApp HCI-Implementierung automatisch generiert. Keine Auswirkung auf andere Komponenten.	"Aktualisieren Sie die QoSSIOC-Anmeldeinformationen im NetApp Element-Plug-in für vCenter Server". Das SIOC-Passwort des NetApp Element-Plug-ins für vCenter-Server wird auch als *QoSSIOC-Passwort* bezeichnet. Lesen Sie den Element Plug-in for vCenter Server KB Artikel.

Anmeldeinformationstyp und Symbol	Nutzung durch Admin	Siehe diese Anweisungen
Anmeldedaten für vCenter Service Appliance 	**Gilt für**: NetApp HCI nur bei Einrichtung über die NetApp Deployment Engine Administratoren können sich bei den virtuellen Maschinen der vCenter Server Appliance anmelden. In NetApp HCI-Implementierungen ist der Benutzername „root“, und das Passwort wurde bei der Erstinstallation dieses Computing-Node in der NetApp Deployment Engine angegeben. Je nach der bereitgestellten VMware vSphere Version können sich auch bestimmte Administratoren in der vSphere Single Sign-On-Domäne bei der Appliance anmelden. Keine Auswirkung auf andere Komponenten.	Es sind keine Änderungen erforderlich.
Anmeldedaten für NetApp Management-Node-Admin 	**Gilt für**: NetApp HCI und optional in SolidFire Zur erweiterten Konfiguration und Fehlerbehebung können sich Administratoren bei Virtual Machines des NetApp Management Node anmelden. Je nach implementierter Management-Node-Version ist die Anmeldung über SSH nicht standardmäßig aktiviert. In NetApp HCI-Implementierungen wurden Benutzername und Passwort vom Benutzer während der Erstinstallation dieses Computing-Node in der NetApp Deployment Engine angegeben. Keine Auswirkung auf andere Komponenten.	Es sind keine Änderungen erforderlich.

Weitere Informationen

- "Ändern Sie das Standard-SSL-Zertifikat der Element Software"
- "Ändern Sie das IPMI-Passwort für Knoten"
- "Multi-Faktor-Authentifizierung aktivieren"
- "Erste Schritte mit externem Verschlüsselungsmanagement"
- "Erstellen eines Clusters, das FIPS-Laufwerke unterstützt"

Ändern Sie das Standard-SSL-Zertifikat der Element Software

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

Beim Erstellen eines NetApp Element-Software-Clusters erstellt das Cluster ein einzigartiges SSL-Zertifikat (Secure Sockets Layer) mit einem privaten Schlüssel, das für die gesamte HTTPS-Kommunikation über die

Element-UI, die UI pro Node oder die APIs verwendet wird. Die Element Software unterstützt selbstsignierte Zertifikate sowie Zertifikate, die von einer vertrauenswürdigen Zertifizierungsstelle (CA) ausgestellt und verifiziert werden.

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

- **GetSSLZertifikat**

  Sie können das verwenden "GetSSLCertificate-Methode" So rufen Sie Informationen zum derzeit installierten SSL-Zertifikat ab, einschließlich aller Zertifikatdetails.

- **SetSSLZertifikat**

  Sie können das verwenden "SetSSLCertificate-Methode" Zum Festlegen der Cluster- und Node-SSL-Zertifikate auf das von Ihnen zur Verfügung gestellt Zertifikat und den privaten Schlüssel. Das System überprüft das Zertifikat und den privaten Schlüssel, um zu verhindern, dass ein ungültiges Zertifikat angewendet wird.

- **RemoveSSLZertifikat**

  Der "RemoveSSLCertificate-Methode" Entfernt das derzeit installierte SSL-Zertifikat und den privaten Schlüssel. Das Cluster generiert dann ein neues selbstsigniertes Zertifikat und einen privaten Schlüssel.

> Das Cluster-SSL-Zertifikat wird automatisch auf alle neuen Nodes angewendet, die dem Cluster hinzugefügt wurden. Jeder Node, der aus dem Cluster entfernt wurde, wird auf ein selbstsigniertes Zertifikat zurückgesetzt und alle benutzerdefinierten Zertifikate und Schlüsselinformationen werden vom Node entfernt.

Weitere Informationen

- "Ändern Sie das Standard-SSL-Zertifikat für den Management-Node"
- "Welche Anforderungen gelten für das Festlegen benutzerdefinierter SSL-Zertifikate in der Element Software?"
- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

Ändern Sie das Standard-IPMI-Passwort für Nodes

Sie können das Standard-Administratorpasswort für die Intelligent Platform Management Interface (IPMI) ändern, sobald Sie Remote-IPMI-Zugriff auf den Node haben. Sie möchten dies möglicherweise tun, wenn Installationsupdates vorhanden sind.

Weitere Informationen zur Konfiguration des IPM-Zugriffs für Knoten finden Sie unter "Konfigurieren Sie IPMI für jeden Node".

Sie können das IPM-Passwort für diese Knoten ändern:

- H410S Nodes
- H610S Nodes

Ändern Sie das Standard-IPMI-Passwort für H410S-Nodes

Sie sollten das Standardpasswort für das IPMI-Administratorkonto auf jedem Speicherknoten ändern, sobald Sie den IPMI-Netzwerkport konfigurieren.

Was Sie benötigen

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

Schritte

1. Öffnen Sie einen Webbrowser auf einem Computer, der das IPMI-Netzwerk erreichen kann, und navigieren Sie zu der IPMI-IP-Adresse für den Knoten.
2. Geben Sie den Benutzernamen ein `ADMIN` Und Passwort `ADMIN` In der Eingabeaufforderung für die Anmeldung.
3. Klicken Sie beim Anmelden auf die Registerkarte **Konfiguration**.
4. Klicken Sie Auf **Benutzer**.
5. Wählen Sie die aus `ADMIN` Benutzer und klicken Sie auf **Benutzer ändern**.
6. Aktivieren Sie das Kontrollkästchen **Passwort ändern**.
7. Geben Sie ein neues Passwort in die Felder **Passwort** und **Passwort bestätigen** ein.
8. Klicken Sie auf **Ändern** und dann auf **OK**.
9. Wiederholen Sie dieses Verfahren für alle anderen H410S-Nodes mit Standard-IPMI-Kennwörtern.

Ändern Sie das Standard-IPMI-Passwort für H610S-Nodes

Sie sollten das Standardpasswort für das IPMI-Administratorkonto auf jedem Speicherknoten ändern, sobald Sie den IPMI-Netzwerkport konfigurieren.

Was Sie benötigen

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

Schritte

1. Öffnen Sie einen Webbrowser auf einem Computer, der das IPMI-Netzwerk erreichen kann, und navigieren Sie zu der IPMI-IP-Adresse für den Knoten.
2. Geben Sie den Benutzernamen ein `root` Und Passwort `calvin` In der Eingabeaufforderung für die Anmeldung.
3. Wenn Sie sich anmelden, klicken Sie oben links auf der Seite auf das Symbol für die Menünavigation, um das Fach für 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 ein neues, starkes Passwort in die Felder **Passwort** und **Passwort bestätigen** ein.
9. Klicken Sie unten auf der Seite auf **Speichern**.
10. Wiederholen Sie dieses Verfahren für alle anderen H610S-Nodes mit Standard-IPMI-Kennwörtern.

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"