



Configure las opciones del sistema SolidFire después de la implementación

Element Software

NetApp
January 15, 2024

Tabla de contenidos

- Configure las opciones del sistema SolidFire después de la implementación. 1
 - Obtenga más información 1
 - Cambie las credenciales en NetApp HCI y SolidFire de NetApp. 1
 - Cambie el certificado SSL predeterminado del software Element 5
 - Cambie la contraseña de IPMI predeterminada para los nodos 6

Configure las opciones del sistema SolidFire después de la implementación

Después de configurar el sistema SolidFire, quizás desee ejecutar algunas tareas opcionales.

Si cambia las credenciales en el sistema, se recomienda conocer el impacto sobre otros componentes.

Además, es posible configurar la autenticación multifactor, la gestión de claves externa y la seguridad de estándar de procesamiento de información federal (FIPS). También debe revisar las contraseñas cuando sea necesario.

Obtenga más información

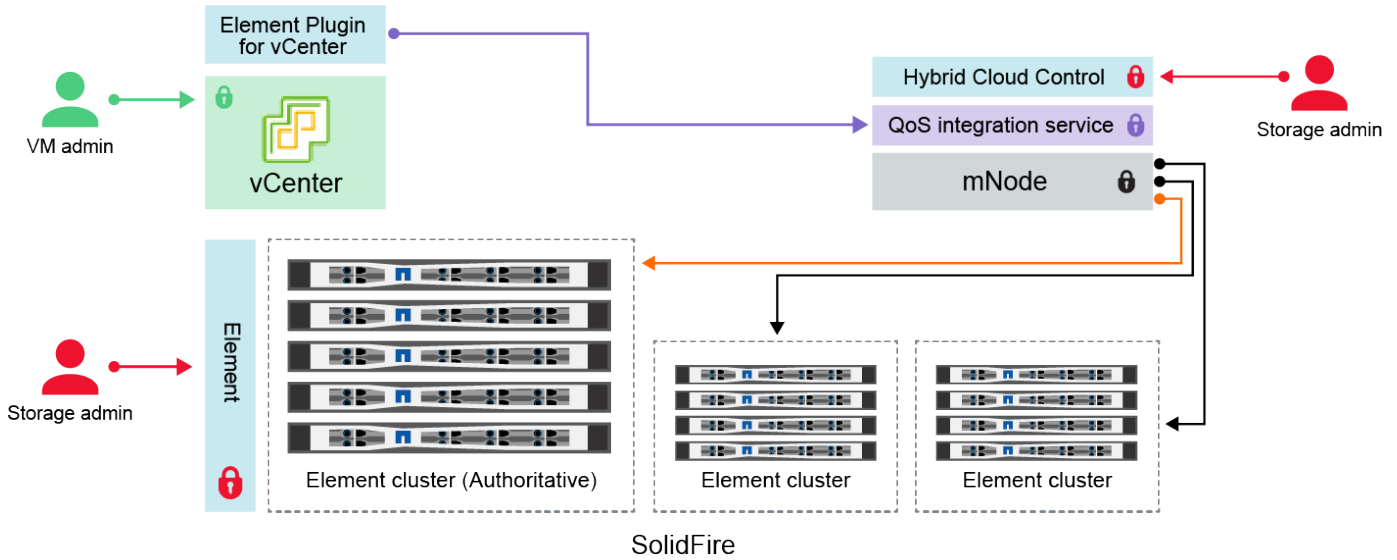
- ["Cambie las credenciales en NetApp HCI y SolidFire de NetApp"](#)
- ["Cambie el certificado SSL predeterminado del software Element"](#)
- ["Cambie la contraseña de IPMI para los nodos"](#)
- ["Habilite la autenticación multifactor"](#)
- ["Comience con la gestión de claves externas"](#)
- ["Cree un clúster que admita unidades FIPS"](#)

Cambie las credenciales en NetApp HCI y SolidFire de NetApp


Según las políticas de seguridad de la organización que implementó NetApp HCI o SolidFire de NetApp, los cambios de credenciales o contraseñas suelen formar parte de las prácticas de seguridad. Antes de cambiar las contraseñas, debe tener en cuenta el impacto sobre otros componentes de software en la implementación.



Si cambia las credenciales de un componente de una implementación de NetApp HCI o SolidFire de NetApp, la siguiente tabla proporciona directrices sobre el impacto en otros componentes.



Interacciones de componentes de 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 de credencial e icono	Uso por administrador	Consulte estas instrucciones
Credenciales de Element 	<p>Se aplica a: NetApp HCI y SolidFire</p> <p>Los administradores utilizan estas credenciales para iniciar sesión en:</p> <ul style="list-style-type: none"> • La interfaz de usuario de Element en el clúster de almacenamiento de Element • Control del cloud híbrido en el nodo de gestión (mnode) <p>Cuando Hybrid Cloud Control gestiona varios clústeres de almacenamiento, solo acepta las credenciales de administrador de los clústeres de almacenamiento, conocidas como el <i>autoritativo cluster</i> para el que se configuró mnode inicialmente. Para los clústeres de almacenamiento que se añadieron más adelante al control del cloud híbrido, el nodo mnode almacena de forma segura las credenciales de administración. Si se modifican las credenciales para clústeres de almacenamiento añadidos posteriormente, también se deben actualizar las credenciales en mnode con la API mnode.</p>	<ul style="list-style-type: none"> • "Actualice las contraseñas de administrador del clúster de almacenamiento." • Actualice las credenciales de administrador del clúster de almacenamiento en el nodo m mediante el "API modifyclusteradmin".

Tipo de credencial e icono	Uso por administrador	Consulte estas instrucciones
<p>Credenciales de inicio de sesión único de vSphere</p> 	<p>Se aplica a: Sólo NetApp HCI</p> <p>Los administradores utilizan estas credenciales para iniciar sesión en VMware vSphere Client. Cuando vCenter forma parte de la instalación de NetApp HCI, las credenciales se configuran en el motor de implementación de NetApp como lo siguiente:</p> <ul style="list-style-type: none"> • nombreusuario@vsphere.local con la contraseña especificada, y. • administrator@vsphere.local con la contraseña especificada. Cuando se usa una instancia existente de vCenter para poner en marcha NetApp HCI, los administradores DE TI de VMware gestionan las credenciales de inicio de sesión único de vSphere. 	<p>"Actualice las credenciales de vCenter y ESXi".</p>
<p>Credenciales del controlador de administración de la placa base (BMC)</p> 	<p>Se aplica a: Sólo NetApp HCI</p> <p>Los administradores utilizan estas credenciales para iniciar sesión en el BMC de los nodos de computación de NetApp en una implementación de NetApp HCI. El BMC proporciona funcionalidades básicas de supervisión de hardware y consola virtual.</p> <p>Las credenciales de BMC (denominadas en ocasiones <i>IPMI</i>) para cada nodo de computación de NetApp se almacenan de forma segura en el nodo cuando las puestas en marcha de NetApp HCI. Control de cloud híbrido de NetApp usa las credenciales de BMC en una capacidad de cuenta de servicio para comunicarse con el BMC en los nodos de computación durante las actualizaciones del firmware de los nodos de computación.</p> <p>Cuando se cambian las credenciales del BMC, también se deben actualizar las credenciales de los nodos de computación respectivos en el mnode para conservar todas las funciones de Hybrid Cloud Control.</p>	<ul style="list-style-type: none"> • "Configure IPMI para cada nodo en NetApp HCI". • Para los nodos H410C, H610C y H615C, "Cambie la contraseña de IPMI predeterminada". • Para nodos H410S y H610S, "Cambiar la contraseña predeterminada de IPM". • "Cambie las credenciales de BMC en el nodo de gestión".

Tipo de credencial e icono	Uso por administrador	Consulte estas instrucciones
<p>Credenciales de ESXi</p> 	<p>Se aplica a: Sólo NetApp HCI</p> <p>Los administradores pueden iniciar sesión en hosts ESXi mediante SSH o la DCUI local con una cuenta raíz local. En implementaciones de NetApp HCI, el nombre de usuario es "raíz" y la contraseña se especificó durante la instalación inicial de ese nodo de computación en el motor de puesta en marcha de NetApp.</p> <p>Las credenciales raíz de ESXi para cada nodo de computación de NetApp se almacenan de forma segura en mnode en puestas en marcha de NetApp HCI. Hybrid Cloud Control de NetApp utiliza las credenciales en una capacidad de cuenta de servicio para comunicarse con hosts ESXi directamente durante las actualizaciones del firmware de los nodos de computación y las comprobaciones del estado.</p> <p>Cuando un administrador de VMware cambia las credenciales raíz de ESXi, las credenciales de los nodos de computación respectivos deben actualizarse en el mnode para mantener la funcionalidad de control de cloud híbrido.</p>	<p>"Actualice las credenciales de para hosts ESXi y vCenter".</p>
<p>Contraseña de integración de la calidad de servicio</p> 	<p>Se aplica a: NetApp HCI y opcional en SolidFire</p> <p>No se utiliza para inicios de sesión interactivos por parte de administradores.</p> <p>La integración de calidad de servicio entre VMware vSphere y el software Element se habilita mediante:</p> <ul style="list-style-type: none"> • Plugin de Element para vCenter Server y. • Servicio QoS en el mnode. <p>Para la autenticación, el servicio QoS utiliza una contraseña que se utiliza exclusivamente en este contexto. La contraseña de calidad de servicio se especifica durante la instalación inicial del plugin de Element para vCenter Server, o bien se genera automáticamente durante la implementación de NetApp HCI.</p> <p>Ningún impacto sobre otros componentes.</p>	<p>"Actualice las credenciales de QoSSIOC en el plugin de NetApp Element para vCenter Server".</p> <p>La contraseña de SIOC del plugin de NetApp Element para vCenter Server también se conoce como <i>QoSSIOC Password</i>.</p> <p>Revise el {URL-pico}[plugin de Element para vCenter Server KB].</p>

Tipo de credencial e icono	Uso por administrador	Consulte estas instrucciones
Credenciales de vCenter Service Appliance 	<p>Se aplica a: NetApp HCI solo si configura el motor de puesta en marcha de NetApp</p> <p>Los administradores pueden iniciar sesión en las máquinas virtuales del dispositivo de vCenter Server. En implementaciones de NetApp HCI, el nombre de usuario es "raíz" y la contraseña se especificó durante la instalación inicial de ese nodo de computación en el motor de puesta en marcha de NetApp. Según la versión de VMware vSphere implementada, algunos administradores del dominio de inicio de sesión único de vSphere también pueden iniciar sesión en el dispositivo.</p> <p>Ningún impacto sobre otros componentes.</p>	No es necesario realizar cambios.
Credenciales de administrador del nodo de gestión de NetApp 	<p>Se aplica a: NetApp HCI y opcional en SolidFire</p> <p>Los administradores pueden iniciar sesión en las máquinas virtuales del nodo de gestión de NetApp para obtener una configuración avanzada y solucionar problemas. Según la versión del nodo de gestión puesta en marcha, el inicio de sesión a través de SSH no se habilita de forma predeterminada.</p> <p>En implementaciones de NetApp HCI, el usuario y la contraseña fueron especificados durante la instalación inicial de ese nodo de computación en el motor de puesta en marcha de NetApp.</p> <p>Ningún impacto sobre otros componentes.</p>	No es necesario realizar cambios.

Obtenga más información

- ["Cambie el certificado SSL predeterminado del software Element"](#)
- ["Cambie la contraseña de IPMI para los nodos"](#)
- ["Habilite la autenticación multifactor"](#)
- ["Comience con la gestión de claves externas"](#)
- ["Cree un clúster que admita unidades FIPS"](#)

Cambie el certificado SSL predeterminado del software Element

Puede cambiar el certificado SSL predeterminado y la clave privada del nodo de almacenamiento del clúster mediante la API de NetApp Element.

Cuando se crea un clúster de software de NetApp Element, el clúster crea un certificado único de capa de sockets seguros (SSL) con firma automática y una clave privada que se utiliza para todas las comunicaciones HTTPS a través de la interfaz de usuario de Element, la interfaz de usuario por nodo o las API. El software

Element admite certificados autofirmados, así como certificados que una entidad de certificación (CA) de confianza emite y verifica.

Puede utilizar los siguientes métodos API para obtener más información sobre el certificado SSL predeterminado y realizar cambios.

- **GetSSLCertificate**

Puede utilizar el "[Método GetSSLCertificate](#)" Para recuperar información acerca del certificado SSL instalado actualmente, incluidos todos los detalles del certificado.

- **SetSSLCertificate**

Puede utilizar el "[Método SetSSLCertificate](#)" Para establecer los certificados SSL por clúster y por nodo en el certificado y la clave privada que suministre. El sistema valida el certificado y la clave privada para evitar que se aplique un certificado no válido.

- **RemoveSSLCertificate**

La "[Método RemoveSSLCertificate](#)" Quita el certificado SSL y la clave privada instalados actualmente. A continuación, el clúster genera un nuevo certificado autofirmado y una clave privada.



El certificado SSL de clúster se aplica automáticamente a todos los nodos nuevos que se añaden al clúster. Cualquier nodo que se quite del clúster se revierte a un certificado autofirmado y toda la información de claves y certificados definidos por el usuario se elimina del nodo.

Obtenga más información

- "[Cambie el certificado SSL predeterminado del nodo de gestión](#)"
- "[¿Cuáles son los requisitos para configurar certificados SSL personalizados en el software Element?](#)"
- "[Documentación de SolidFire y el software Element](#)"
- "[Plugin de NetApp Element para vCenter Server](#)"

Cambie la contraseña de IPMI predeterminada para los nodos

En cuanto tenga acceso IPMI remoto al nodo, puede cambiar la contraseña predeterminada del administrador de la interfaz de gestión de plataformas inteligentes (IPMI). Puede que desee hacerlo si se han actualizado alguna instalación.

Para obtener más información acerca de cómo configurar el acceso IPM para los nodos, consulte "[Configure IPMI para cada nodo](#)".

Puede cambiar la contraseña de IPM para estos nodos:

- Nodos H410S
- Nodos H610S

Cambie la contraseña de IPMI predeterminada para los nodos H410S

En cuanto configure el puerto de red IPMI, debe cambiar la contraseña predeterminada de la cuenta de administrador de IPMI en cada nodo de almacenamiento.

Lo que necesitará

Debe haber configurado la dirección IP de IPMI para cada nodo de almacenamiento.

Pasos

1. Abra un explorador web en un equipo que pueda acceder a la red de IPMI y vaya a la dirección IP de IPMI correspondiente al nodo.
2. Introduzca el nombre de usuario `ADMIN` y contraseña `ADMIN` en la solicitud de inicio de sesión de.
3. Después de iniciar sesión, haga clic en la ficha **Configuración**.
4. Haga clic en **usuarios**.
5. Seleccione la `ADMIN` Haga clic en **Modificar usuario**.
6. Seleccione la casilla de verificación **Cambiar contraseña**.
7. Introduzca una nueva contraseña en los campos **Contraseña** y **Confirmar contraseña**.
8. Haga clic en **Modificar** y, a continuación, haga clic en **Aceptar**.
9. Repita este procedimiento para todos los demás nodos H410S con contraseñas IPMI predeterminadas.

Cambie la contraseña de IPMI predeterminada para los nodos H610S

En cuanto configure el puerto de red IPMI, debe cambiar la contraseña predeterminada de la cuenta de administrador de IPMI en cada nodo de almacenamiento.

Lo que necesitará

Debe haber configurado la dirección IP de IPMI para cada nodo de almacenamiento.

Pasos

1. Abra un explorador web en un equipo que pueda acceder a la red de IPMI y vaya a la dirección IP de IPMI correspondiente al nodo.
2. Introduzca el nombre de usuario `root` y contraseña `calvin` en la solicitud de inicio de sesión de.
3. Después de iniciar sesión, haga clic en el icono de navegación del menú que aparece en la parte superior izquierda de la página para abrir el cajón de la barra lateral.
4. Haga clic en **Configuración**.
5. Haga clic en **Administración de usuarios**.
6. Seleccione el usuario **Administrador** de la lista.
7. Active la casilla de verificación **Cambiar contraseña**.
8. Introduzca una nueva contraseña segura en los campos **Contraseña** y **Confirmar contraseña**.
9. Haga clic en **Guardar** en la parte inferior de la página.
10. Repita este procedimiento para todos los demás nodos H610S con contraseñas de IPMI predeterminadas.

Obtenga más información

- ["Documentación de SolidFire y el software Element"](#)
- ["Plugin de NetApp Element para vCenter Server"](#)

Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPTIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.