



Configure as opções do sistema SolidFire após a implantação

Element Software

NetApp
November 21, 2024

Índice

- Configure as opções do sistema SolidFire após a implantação 1
 - Encontre mais informações 1
 - Alterar credenciais no NetApp HCI e no NetApp SolidFire 1
 - Altere o certificado SSL padrão do software Element 5
 - Altere a senha padrão do IPMI para nós 6

Configure as opções do sistema SolidFire após a implantação

Depois de configurar o sistema SolidFire, talvez você queira executar algumas tarefas opcionais.

Se você alterar credenciais no sistema, talvez queira saber o impactos em outros componentes.

Além disso, você pode configurar configurações para autenticação multifator, gerenciamento de chaves externas e segurança FIPS (Federal Information Processing Standards). Você também deve olhar para a atualização de senhas quando necessário.

Encontre mais informações

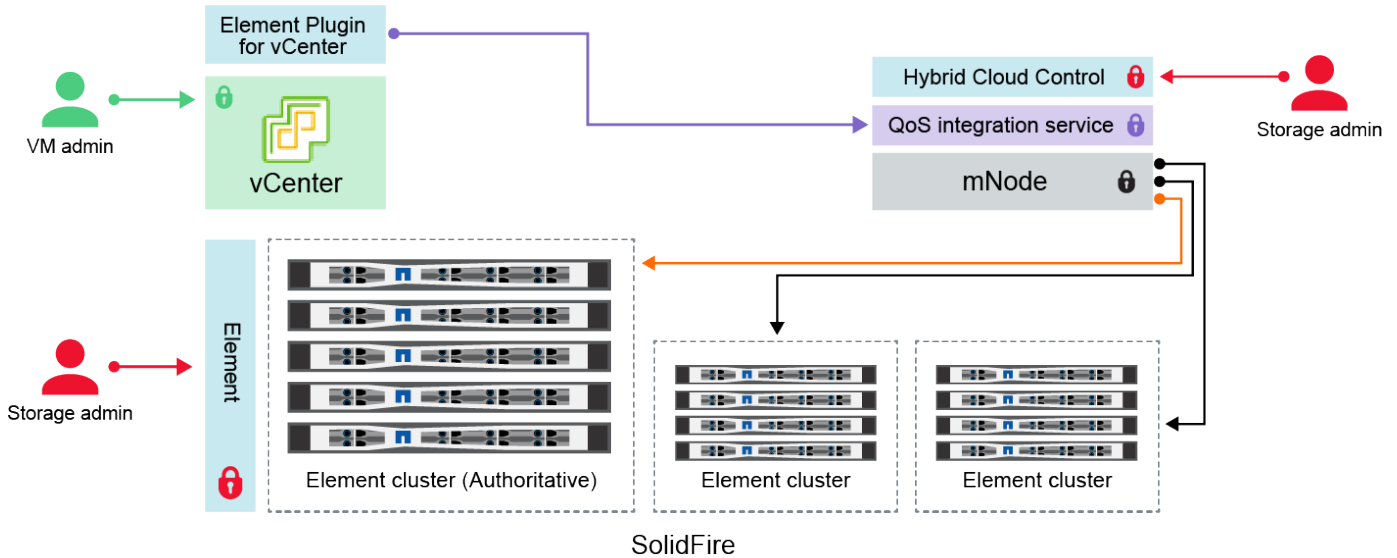
- ["Alterar credenciais no NetApp HCI e no NetApp SolidFire"](#)
- ["Altere o certificado SSL padrão do software Element"](#)
- ["Altere a senha do IPMI para nós"](#)
- ["Ativar a autenticação multifator"](#)
- ["Comece a usar o gerenciamento de chaves externas"](#)
- ["Criar um cluster compatível com unidades FIPS"](#)

Alterar credenciais no NetApp HCI e no NetApp SolidFire


Dependendo das políticas de segurança na organização que implantou o NetApp HCI ou o NetApp SolidFire, alterar credenciais ou senhas geralmente faz parte das práticas de segurança. Antes de alterar as senhas, você deve estar ciente do impactos em outros componentes de software na implantação.



Se você alterar credenciais para um componente de uma implantação do NetApp HCI ou do NetApp SolidFire, a tabela a seguir fornece orientações sobre o impactos em outros componentes.



Interações do componente 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 e ícone de credencial	Utilização por Admin	Consulte estas instruções
Credenciais do elemento 	<p>Aplicável a: NetApp HCI e SolidFire</p> <p>Administradores usam essas credenciais para fazer login:</p> <ul style="list-style-type: none"> Interface de usuário do Element no cluster de storage do Element Controle de nuvem híbrida no nó de gerenciamento (mnode) <p>Quando o Hybrid Cloud Control gerencia vários clusters de armazenamento, ele aceita apenas as credenciais de administrador para os clusters de armazenamento, conhecido como o cluster <i>autoritativo</i> para o qual o mnode foi configurado inicialmente. Para clusters de storage adicionados mais tarde ao Hybrid Cloud Control, o mnode armazena com segurança as credenciais de administrador. Se as credenciais para clusters de armazenamento adicionados posteriormente forem alteradas, as credenciais também devem ser atualizadas no mnode usando a API mnode.</p>	<ul style="list-style-type: none"> "Atualize as senhas de administrador do cluster de armazenamento." Atualize as credenciais de administrador do cluster de armazenamento no mnode usando o "API de modificação exclusiva".

Tipo e ícone de credencial	Utilização por Admin	Consulte estas instruções
<p>Credenciais de logon único do vSphere</p> 	<p>Aplicável a: Apenas NetApp HCI</p> <p>Os administradores usam essas credenciais para fazer login no VMware vSphere Client. Quando o vCenter faz parte da instalação do NetApp HCI, as credenciais são configuradas no mecanismo de implantação do NetApp da seguinte forma:</p> <ul style="list-style-type: none"> • com a senha especificada, e. • com a senha especificada. Quando um vCenter existente é usado para implantar o NetApp HCI, as credenciais de logon único do vSphere são gerenciadas pelos administradores da VMware DE TI. 	<p>"Atualize as credenciais do vCenter e do ESXi".</p>
<p>Credenciais do controlador de gerenciamento de placa base (BMC)</p> 	<p>Aplicável a: Apenas NetApp HCI</p> <p>Os administradores usam essas credenciais para fazer login no BMC dos nós de computação do NetApp em uma implantação do NetApp HCI. O BMC fornece monitoramento básico de hardware e recursos de console virtual.</p> <p>As credenciais BMC (às vezes chamadas de <i>IPMI</i>) para cada nó de computação NetApp são armazenadas com segurança no nó mnode nas implantações do NetApp HCI. O controle de nuvem híbrida da NetApp usa credenciais BMC na capacidade de uma conta de serviço para se comunicar com o BMC nos nós de computação durante atualizações de firmware de nós de computação.</p> <p>Quando as credenciais do BMC são alteradas, as credenciais dos respectivos nós de computação devem ser atualizadas também no nó mnode para reter toda a funcionalidade de Controle de nuvem híbrida.</p>	<ul style="list-style-type: none"> • "Configure o IPMI para cada nó no NetApp HCI". • Para nós de H410C, H610C e H615C, "Altere a senha padrão do IPMI". • Para nós de H410S e H610S, "Altere a senha padrão do IPMI". • "Altere as credenciais do BMC no nó de gerenciamento".

Tipo e ícone de credencial	Utilização por Admin	Consulte estas instruções
<p>Credenciais ESXi</p> 	<p>Aplicável a: Apenas NetApp HCI</p> <p>Os administradores podem fazer login em hosts ESXi usando SSH ou DCUI local com uma conta raiz local. Nas implantações do NetApp HCI, o nome de usuário é 'root' e a senha foi especificada durante a instalação inicial desse nó de computação no mecanismo de implantação do NetApp.</p> <p>As credenciais raiz do ESXi para cada nó de computação do NetApp são armazenadas com segurança no nó mnode nas implantações do NetApp HCI. O Controle de nuvem híbrida da NetApp usa as credenciais em uma capacidade de conta de serviço para se comunicar diretamente com os hosts ESXi durante as atualizações de firmware do nó de computação e verificações de integridade.</p> <p>Quando as credenciais raiz ESXi são alteradas por um administrador da VMware, as credenciais dos respectivos nós de computação devem ser atualizadas no nó mnode para manter a funcionalidade de Controle de nuvem híbrida.</p>	<p>"Atualizar credenciais para hosts do vCenter e do ESXi".</p>
<p>Palavra-passe de integração o QoS</p> 	<p>Aplicável a: NetApp HCI e opcional no SolidFire</p> <p>Não é usado para logins interativos por administradores.</p> <p>A integração de QoS entre o VMware vSphere e o Element Software é habilitada por:</p> <ul style="list-style-type: none"> • Plug-in Element para vCenter Server, e. • Serviço de QoS no mnode. <p>Para autenticação, o serviço QoS usa uma senha que é exclusivamente usada neste contexto. A senha de QoS é especificada durante a instalação inicial do plug-in Element para vCenter Server ou gerada automaticamente durante a implantação do NetApp HCI.</p> <p>Sem impactos em outros componentes.</p>	<p>"Atualize as credenciais do QoSSIOC no plug-in do NetApp Element para o vCenter Server".</p> <p>A senha do plug-in do NetApp Element para o vCenter Server SIOC também é conhecida como <i>QoSSIOC password</i>.</p> <p>Consulte o artigo de base de dados do vCenter Server.</p>

Tipo e ícone de credencial	Utilização por Admin	Consulte estas instruções
Credenciais do vCenter Service Appliance 	<p>Aplica-se a: NetApp HCI somente se configurado pelo mecanismo de implantação do NetApp</p> <p>Os administradores podem fazer login nas máquinas virtuais do vCenter Server Appliance. Nas implantações do NetApp HCI, o nome de usuário é 'root' e a senha foi especificada durante a instalação inicial desse nó de computação no mecanismo de implantação do NetApp. Dependendo da versão do VMware vSphere implantada, certos administradores no domínio de logon único do vSphere também podem fazer login no dispositivo.</p> <p>Sem impactos em outros componentes.</p>	Não são necessárias alterações.
Credenciais de administrador do nó de gerenciamento do NetApp 	<p>Aplicável a: NetApp HCI e opcional no SolidFire</p> <p>Os administradores podem fazer login nas máquinas virtuais do nó de gerenciamento do NetApp para configuração avançada e solução de problemas. Dependendo da versão do nó de gerenciamento implantada, o login via SSH não é habilitado por padrão.</p> <p>Nas implantações do NetApp HCI, o nome de usuário e a senha foram especificados pelo usuário durante a instalação inicial desse nó de computação no mecanismo de implantação do NetApp.</p> <p>Sem impactos em outros componentes.</p>	Não são necessárias alterações.

Encontre mais informações

- ["Altere o certificado SSL padrão do software Element"](#)
- ["Altere a senha do IPMI para nós"](#)
- ["Ativar a autenticação multifator"](#)
- ["Comece a usar o gerenciamento de chaves externas"](#)
- ["Criar um cluster compatível com unidades FIPS"](#)

Altere o certificado SSL padrão do software Element

Você pode alterar o certificado SSL padrão e a chave privada do nó de armazenamento no cluster usando a API NetApp Element.

Quando um cluster de software NetApp Element é criado, o cluster cria um certificado SSL (Secure Sockets Layer) exclusivo autoassinado e uma chave privada que é usada para todas as comunicações HTTPS por meio da IU do Element, IU por nó ou APIs. O software Element suporta certificados autoassinados, bem como

certificados emitidos e verificados por uma autoridade de certificação (CA) confiável.

Você pode usar os seguintes métodos de API para obter mais informações sobre o certificado SSL padrão e fazer alterações.

- **GetSSLCertificate**

Você pode usar o "[Método GetSSLCertificate](#)" para recuperar informações sobre o certificado SSL instalado atualmente, incluindo todos os detalhes do certificado.

- **SetSSLCertificate**

Você pode usar o "[Método SetSSLCertificate](#)" para definir os certificados SSL de cluster e por nó para o certificado e a chave privada que você fornece. O sistema valida o certificado e a chave privada para impedir que um certificado inválido seja aplicado.

- **RemoveSSLCertificate**

O "[Método RemoveSSLCertificate](#)" remove o certificado SSL e a chave privada atualmente instalados. Em seguida, o cluster gera um novo certificado autoassinado e uma chave privada.



O certificado SSL do cluster é aplicado automaticamente a todos os novos nós adicionados ao cluster. Qualquer nó removido do cluster reverte para um certificado autoassinado e todas as informações de chave e certificados definidos pelo usuário são removidas do nó.

Encontre mais informações

- "[Altere o certificado SSL padrão do nó de gerenciamento](#)"
- "[Quais são os requisitos para definir certificados SSL personalizados no Element Software?](#)"
- "[Documentação do software SolidFire e Element](#)"
- "[Plug-in do NetApp Element para vCenter Server](#)"

Altere a senha padrão do IPMI para nós

Você pode alterar a senha de administrador IPMI (Intelligent Platform Management Interface) padrão assim que tiver acesso IPMI remoto ao nó. Você pode querer fazer isso se houver atualizações de instalação.

Para obter detalhes sobre como configurar o acesso IPM para nós, "[Configure o IPMI para cada nó](#)" consulte .

Você pode alterar a senha do IPM para esses nós:

- H410S nós
- H610S nós

Altere a senha padrão do IPMI para H410S nós

Você deve alterar a senha padrão para a conta de administrador IPMI em cada nó de armazenamento assim que configurar a porta de rede IPMI.

O que você vai precisar

Você deve ter configurado o endereço IP IPMI para cada nó de armazenamento.

Passos

1. Abra um navegador da Web em um computador que possa acessar a rede IPMI e navegue até o endereço IP IPMI do nó.
2. Introduza o nome de utilizador `ADMIN` e a palavra-passe `ADMIN` no aviso de início de sessão.
3. Ao iniciar sessão, clique no separador **Configuration** (Configuração).
4. Clique em **usuários**.
5. Selecione o `ADMIN` usuário e clique em **Modificar usuário**.
6. Marque a caixa de seleção **alterar senha**.
7. Introduza uma nova palavra-passe nos campos **Password** (Palavra-passe) e **Confirm Password** (confirmar palavra-passe).
8. Clique em **Modificar** e, em seguida, clique em **OK**.
9. Repita este procedimento para quaisquer outros nós H410S com senhas IPMI padrão.

Altere a senha padrão do IPMI para H610S nós

Você deve alterar a senha padrão para a conta de administrador IPMI em cada nó de armazenamento assim que configurar a porta de rede IPMI.

O que você vai precisar

Você deve ter configurado o endereço IP IPMI para cada nó de armazenamento.

Passos

1. Abra um navegador da Web em um computador que possa acessar a rede IPMI e navegue até o endereço IP IPMI do nó.
2. Introduza o nome de utilizador `root` e a palavra-passe `calvin` no aviso de início de sessão.
3. Ao iniciar sessão, clique no ícone de navegação do menu no canto superior esquerdo da página para abrir a gaveta da barra lateral.
4. Clique em **Configurações**.
5. Clique em **User Management**.
6. Selecione o usuário **Administrator** na lista.
7. Ative a caixa de verificação **alterar palavra-passe**.
8. Insira uma nova senha forte nos campos **Senha** e **confirmar senha**.
9. Clique em **Salvar** na parte inferior da página.
10. Repita este procedimento para quaisquer outros nós H610S com senhas IPMI padrão.

Encontre mais informações

- ["Documentação do software SolidFire e Element"](#)
- ["Plug-in do NetApp Element para vCenter Server"](#)

Informações sobre direitos autorais

Copyright © 2024 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPTÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.