



Configure as opções do sistema SolidFire após a implantação.

Element Software

NetApp
November 12, 2025

Índice

- Configure as opções do sistema SolidFire após a implantação. 1
 - Configure as opções do sistema SolidFire após a implantação. 1
 - Encontre mais informações 1
 - Alterar credenciais no NetApp HCI e no NetApp SolidFire 1
 - Encontre mais informações 5
 - Alterar o certificado SSL padrão do software Element 5
 - Encontre mais informações 6
 - Alterar a senha IPMI padrão para nós 6
 - Alterar a senha IPMI padrão para nós H410S 6
 - Alterar a senha IPMI padrão para nós H610S 7
 - Encontre mais informações 7

Configure as opções do sistema SolidFire após a implantação.

Configure as opções do sistema SolidFire após a implantação.

Após configurar seu sistema SolidFire , você pode querer executar algumas tarefas opcionais.

Se você alterar as credenciais do sistema, talvez queira saber o impacto em outros componentes.

Além disso, você pode configurar as definições para autenticação multifator, gerenciamento de chaves externas e segurança de acordo com os Padrões Federais de Processamento de Informações (FIPS). Você também deve considerar atualizar suas senhas quando necessário.

Encontre mais informações

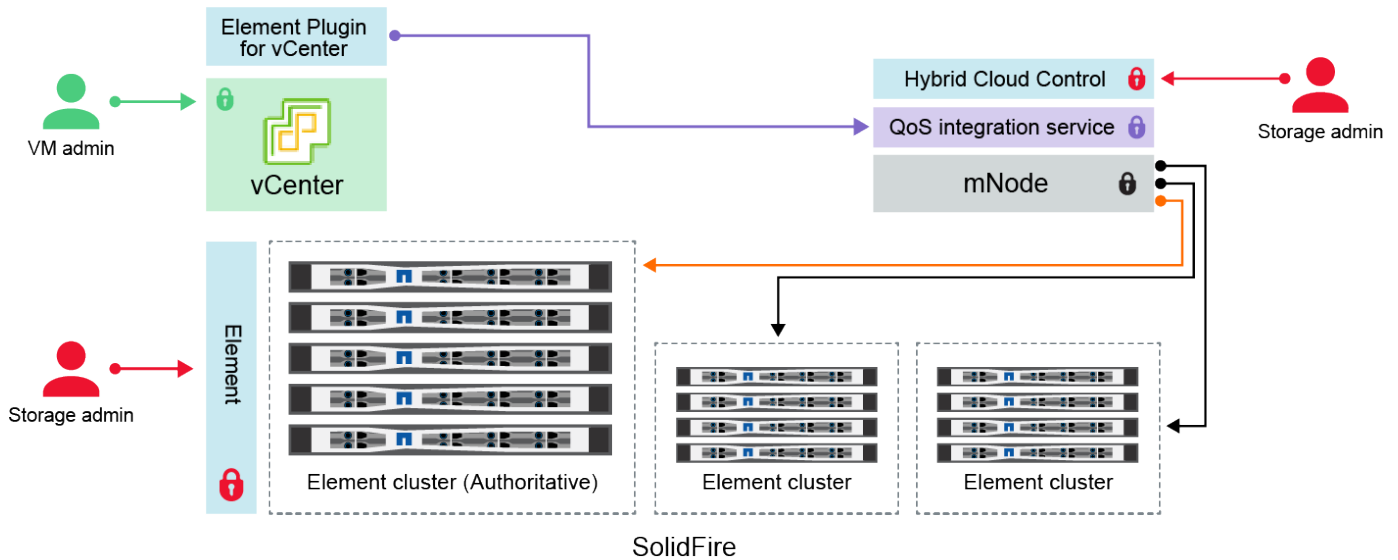
- ["Alterar credenciais no NetApp HCI e no NetApp SolidFire"](#)
- ["Alterar o certificado SSL padrão do software Element"](#)
- ["Alterar a senha IPMI para nós"](#)
- ["Habilitar autenticação multifator"](#)
- ["Comece a gerenciar chaves externas."](#)
- ["Crie um cluster que suporte unidades FIPS."](#)

Alterar credenciais no NetApp HCI e no NetApp SolidFire

Dependendo das políticas de segurança da organização que implementou o NetApp HCI ou o NetApp SolidFire, a alteração de credenciais ou senhas geralmente faz parte das práticas de segurança. Antes de alterar as senhas, você deve estar ciente do impacto que isso terá em outros componentes de software da sua implementação.

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

Interações entre componentes do 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 ícone	Utilização pelo administrador	Consulte estas instruções.
Credenciais do elemento 	Aplica-se a: NetApp HCI e SolidFire Os administradores usam estas credenciais para fazer login: - Interface de usuário do Element no cluster de armazenamento Element - Controle de nuvem híbrida no nó de gerenciamento (mnode) Quando o Hybrid Cloud Control gerencia vários clusters de armazenamento, ele aceita apenas as credenciais de administrador dos clusters de armazenamento, conhecidos como o <i>cluster autoritativo</i> para o qual o mnode foi inicialmente configurado. Para clusters de armazenamento adicionados posteriormente ao Hybrid Cloud Control, o mnode armazena com segurança as credenciais de administrador. Caso as credenciais de clusters de armazenamento adicionados posteriormente sejam alteradas, elas também deverão ser atualizadas no mnode usando a API do mnode.	"Atualize as senhas de administrador do cluster de armazenamento." - Atualize as credenciais de administrador do cluster de armazenamento no mnode usando o "API modifyclusteradmin".

Tipo de credencial e ícone	Utilização pelo administrador	Consulte estas instruções.
Credenciais de login único do vSphere 	Aplica-se a: Somente NetApp HCI 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 NetApp Deployment Engine da seguinte forma: • nome de usuário@vsphere.local com a senha especificada e • administrator@vsphere.local com a senha especificada. Quando um vCenter existente é usado para implantar o NetApp HCI, as credenciais de Single Sign-on do vSphere são gerenciadas pelos administradores de TI da VMware.	"Atualize as credenciais do vCenter e do ESXi".
Credenciais do controlador de gerenciamento da placa-mãe (BMC) 	Aplica-se a: Somente NetApp HCI Os administradores usam essas credenciais para fazer login no BMC dos nós de computação NetApp em uma implementação NetApp HCI. O BMC oferece recursos básicos de monitoramento de hardware e console virtual. As credenciais BMC (às vezes chamadas de <i>IPMI</i>) para cada nó de computação NetApp são armazenadas com segurança no mnode em implantações NetApp HCI. O NetApp Hybrid Cloud Control utiliza as credenciais do BMC em uma conta de serviço para se comunicar com o BMC nos nós de computação durante as atualizações de firmware desses nós. Quando as credenciais do BMC são alteradas, as credenciais dos respectivos nós de computação também devem ser atualizadas no mnode para manter todas as funcionalidades do Hybrid Cloud Control.	• "Configure o IPMI para cada nó no NetApp HCI". • Para os nós H410C, H610C e H615C, "alterar a senha padrão do IPMI". • Para nós H410S e H610S, "Alterar a senha padrão do IPMI". • "Alterar as credenciais do BMC no nó de gerenciamento".

Tipo de credencial e ícone	Utilização pelo administrador	Consulte estas instruções.
Credenciais ESXi 	Aplica-se a: Somente NetApp HCI Os administradores podem fazer login nos hosts ESXi usando SSH ou a interface de usuário do controlador de domínio local (DCUI) com uma conta root local. Em implementações NetApp HCI, o nome de usuário é 'root' e a senha foi especificada durante a instalação inicial desse nó de computação no NetApp Deployment Engine. As credenciais de root do ESXi para cada nó de computação NetApp são armazenadas com segurança no mnode em implantações NetApp HCI. O NetApp Hybrid Cloud Control utiliza as credenciais em uma conta de serviço para se comunicar diretamente com os hosts ESXi durante as atualizações de firmware e verificações de integridade dos nós de computação. Quando as credenciais de root do ESXi são alteradas por um administrador da VMware, as credenciais dos respectivos nós de computação devem ser atualizadas no mnode para manter a funcionalidade do Hybrid Cloud Control.	"Atualizar credenciais para hosts vCenter e ESXi".
Senha de integração de QoS 	Aplica-se a: NetApp HCI e opcionalmente no SolidFire Não é utilizado para logins interativos por administradores. A integração de QoS entre o VMware vSphere e o Element Software é habilitada através de: • Plug-in Element para vCenter Server e • Serviço QoS no mnode. Para autenticação, o serviço QoS utiliza uma senha que é usada exclusivamente neste contexto. A senha de QoS é especificada durante a instalação inicial do plug-in Element para vCenter Server ou gerada automaticamente durante a implementação do NetApp HCI. Não afeta outros componentes.	"Atualize as credenciais do QoSSIOC no plug-in NetApp Element para vCenter Server". A senha do NetApp Element Plug-in para vCenter Server SIOC também é conhecida como senha QoSSIOC. Consulte o artigo da Base de Conhecimento sobre o plug-in Element para vCenter Server no link https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Software/Element_Plugin_for_vCenter_server/mNode_Status_shows_as_'Network_Down'_or_'Down'_in_the_mNode_Settings_tab_of_the_Element_Plugin_for_vCenter_(VCP).

Tipo de credencial e ícone	Utilização pelo administrador	Consulte estas instruções.
Credenciais do vCenter Service Appliance 	Aplica-se a: NetApp HCI somente se configurado pelo NetApp Deployment Engine. Os administradores podem fazer login nas máquinas virtuais do appliance vCenter Server. Em implementações NetApp HCI, o nome de usuário é 'root' e a senha foi especificada durante a instalação inicial desse nó de computação no NetApp Deployment Engine. Dependendo da versão do VMware vSphere implementada, determinados administradores no domínio vSphere Single Sign-on também podem fazer login no dispositivo. Não afeta outros componentes.	Nenhuma alteração necessária.
Credenciais de administrador do nó de gerenciamento NetApp 	Aplica-se a: NetApp HCI e opcionalmente no SolidFire Os administradores podem acessar as máquinas virtuais do nó de gerenciamento da NetApp para realizar configurações avançadas e solucionar problemas. Dependendo da versão do nó de gerenciamento implantada, o login via SSH não está habilitado por padrão. Em implementações de NetApp HCI, o nome de usuário e a senha eram especificados pelo usuário durante a instalação inicial desse nó de computação no NetApp Deployment Engine. Não afeta outros componentes.	Nenhuma alteração necessária.

Encontre mais informações

- ["Alterar o certificado SSL padrão do software Element"](#)
- ["Alterar a senha IPMI para nós"](#)
- ["Habilitar autenticação multifator"](#)
- ["Comece a gerenciar chaves externas."](#)
- ["Crie um cluster que suporte unidades FIPS."](#)

Alterar 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 do NetApp Element .

Quando um cluster de software NetApp Element é criado, o cluster gera um certificado SSL (Secure Sockets Layer) autoassinado exclusivo e uma chave privada que é usada para toda a comunicação HTTPS por meio da interface do usuário do Element, da interface do usuário por nó ou das APIs. O software Element suporta certificados autoassinados, bem como certificados emitidos e verificados por uma Autoridade Certificadora

(AC) confiável.

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

- **Obter certificado SSL**

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

- **Definir certificado SSL**

Você pode usar o "[Método SetSSLCertificate](#)" Para configurar os certificados SSL do cluster e de cada nó com o certificado e a chave privada fornecidos. O sistema valida o certificado e a chave privada para impedir que um certificado inválido seja aplicado.

- **Remover certificado SSL**

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 retorna a um certificado autoassinado e todas as informações de certificado e chave definidas pelo usuário são removidas do nó.

Encontre mais informações

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

Alterar a senha IPMI padrão para nós

Você pode alterar a senha padrão do administrador da Interface de Gerenciamento de Plataforma Inteligente (IPMI) assim que tiver acesso remoto ao nó via IPMI. Você pode querer fazer isso se houver alguma atualização de instalação.

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

Você pode alterar a senha do IPM para estes nós:

- Nós H410S
- Nós H610S

Alterar a senha IPMI padrão para nós H410S

Você deve alterar a senha padrão da 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 do IPMI para cada nó de armazenamento.

Passos

1. Abra um navegador web em um computador que possa acessar a rede IPMI e navegue até o endereço IP do nó IPMI.
2. Digite o nome de usuário `ADMIN` e senha `ADMIN` na tela de login.
3. Após efetuar o login, clique na aba **Configuração**.
4. Clique em **Usuários**.
5. Selecione o `ADMIN` usuário e clique em **Modificar Usuário**.
6. Selecione a caixa de seleção **Alterar senha**.
7. Insira uma nova senha nos campos **Senha** e **Confirmar Senha**.
8. Clique em **Modificar** e, em seguida, clique em **OK**.
9. Repita este procedimento para quaisquer outros nós H410S com senhas IPMI padrão.

Alterar a senha IPMI padrão para nós H610S

Você deve alterar a senha padrão da 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 do IPMI para cada nó de armazenamento.

Passos

1. Abra um navegador web em um computador que possa acessar a rede IPMI e navegue até o endereço IP do nó IPMI.
2. Digite o nome de usuário `root` e senha `calvin` na tela de login.
3. Após efetuar o login, clique no ícone de navegação do menu no canto superior esquerdo da página para abrir a barra lateral.
4. Clique em **Configurações**.
5. Clique em **Gerenciamento de usuários**.
6. Selecione o usuário **Administrador** na lista.
7. Marque a caixa de seleção **Alterar senha**.
8. Digite 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 SolidFire e do Element Software"](#)
- ["Plug-in NetApp Element para vCenter Server"](#)

Informações sobre direitos autorais

Copyright © 2025 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 SOBRESSALENTE; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO 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.