



Gerenciar certificados

E-Series storage systems

NetApp

January 20, 2026

Índice

Gerenciar certificados	1
Saiba mais sobre como gerenciar certificados no plug-in de armazenamento do SANtricity para vCenter ..	1
O que são certificados?	1
Certificados assinados	1
Certificados autoassinados	2
Certificado de gestão	2
Certificados confiáveis	2
Use certificados assinados por CA no plug-in de armazenamento do SANtricity para vCenter	2
Passo 1: Complete um arquivo CSR	3
Passo 2: Envie o arquivo CSR	3
Passo 3: Importar certificados de gestão	4
Redefinir certificados de gerenciamento no plug-in de armazenamento do SANtricity para vCenter	4
Importar certificados para arrays no plug-in de armazenamento do SANtricity para vCenter	5
Exibir certificados no plug-in de armazenamento do SANtricity para vCenter	6
Exportar certificados no plug-in de armazenamento do SANtricity para vCenter	6
Excluir certificados confiáveis no plug-in de armazenamento do SANtricity para vCenter	6
Resolva certificados não confiáveis no plug-in de armazenamento do SANtricity para vCenter	7

Gerenciar certificados

Saiba mais sobre como gerenciar certificados no plug-in de armazenamento do SANtricity para vCenter

O gerenciamento de certificados no plug-in de armazenamento para vCenter permite criar CSRs (solicitações de assinatura de certificado), importar certificados e gerenciar certificados existentes.

O que são certificados?

Certificados são arquivos digitais que identificam entidades online, como sites e servidores, para comunicações seguras na internet. Eles garantem que as comunicações da Web sejam transmitidas de forma criptografada, privada e inalterada, apenas entre o servidor e o cliente especificados. Com o plug-in de armazenamento para vCenter, você pode gerenciar certificados para o navegador em um sistema de gerenciamento de host e os controladores nos arrays de armazenamento descobertos.

Um certificado pode ser assinado por uma autoridade confiável ou pode ser autoassinado. "Assinatura" significa simplesmente que alguém validou a identidade do proprietário e determinou que seus dispositivos podem ser confiáveis.

As matrizes de armazenamento são fornecidas com um certificado auto-assinado gerado automaticamente em cada controlador. Você pode continuar usando os certificados autoassinados ou obter certificados assinados pela CA para uma conexão mais segura entre os controladores e os sistemas host.



Embora os certificados assinados pela CA forneçam melhor proteção de segurança (por exemplo, evitando ataques man-in-the-middle), eles também exigem taxas que podem ser caras se você tiver uma rede grande. Em contraste, os certificados autoassinados são menos seguros, mas são gratuitos. Portanto, os certificados autoassinados são mais usados para ambientes de teste internos, não em ambientes de produção.

Certificados assinados

Um certificado assinado é validado por uma autoridade de certificação (CA), que é uma organização de terceiros confiável. Os certificados assinados incluem detalhes sobre o proprietário da entidade (normalmente, um servidor ou site), data de emissão e expiração do certificado, domínios válidos para a entidade e uma assinatura digital composta por letras e números.

Quando você abre um navegador e insere um endereço da Web, o sistema executa um processo de verificação de certificados em segundo plano para determinar se você está se conectando a um site que inclui um certificado válido assinado pela CA. Geralmente, um site protegido com um certificado assinado inclui um ícone de cadeado e uma designação https no endereço. Se você tentar se conectar a um site que não contenha um certificado assinado pela CA, o navegador exibirá um aviso de que o site não está seguro.

A CA toma medidas para verificar sua identidade durante o processo de inscrição. Eles podem enviar um e-mail para sua empresa registrada, verificar seu endereço comercial e executar uma verificação HTTP ou DNS. Quando o processo de aplicação estiver concluído, a CA envia arquivos digitais para serem carregados em um sistema de gerenciamento de host. Normalmente, esses arquivos incluem uma cadeia de confiança, como segue:

- **Root** — na parte superior da hierarquia está o certificado raiz, que contém uma chave privada usada para

assinar outros certificados. A raiz identifica uma organização de CA específica. Se você usar a mesma CA para todos os dispositivos de rede, precisará de apenas um certificado raiz.

- **Intermediate** — ramificação fora da raiz são os certificados intermediários. A CA emite um ou mais certificados intermediários para atuar como intermediários entre uma raiz protegida e certificados de servidor.
- **Servidor** — na parte inferior da cadeia está o certificado do servidor, que identifica sua entidade específica, como um site ou outro dispositivo. Cada controlador em um storage array requer um certificado de servidor separado.

Certificados autoassinados

Cada controladora no storage inclui um certificado pré-instalado e autoassinado. Um certificado autoassinado é semelhante a um certificado assinado pela CA, exceto que ele é validado pelo proprietário da entidade em vez de um terceiro. Como um certificado assinado pela CA, um certificado autoassinado contém sua própria chave privada e também garante que os dados sejam criptografados e enviados por uma conexão HTTPS entre um servidor e um cliente.

Os certificados autoassinados não são "confiáveis" pelos navegadores. Cada vez que você tenta se conectar a um site que contém apenas um certificado autoassinado, o navegador exibe uma mensagem de aviso. Você deve clicar em um link na mensagem de aviso que permite que você prossiga para o site; ao fazê-lo, você está essencialmente aceitando o certificado auto-assinado.

Certificado de gestão

Quando você abre o plugin, o navegador tenta verificar se o host de gerenciamento é uma fonte confiável, verificando se há um certificado digital. Se o navegador não localizar um certificado assinado pela CA, ele abrirá uma mensagem de aviso. A partir daí, você pode continuar para o site para aceitar o certificado autoassinado para essa sessão. Você também pode obter certificados digitais assinados de uma CA para que você não veja mais a mensagem de aviso.

Certificados confiáveis

Durante uma sessão de plug-in, você pode ver mensagens de segurança adicionais quando você tenta acessar um controlador que não tem um certificado assinado pela CA. Nesse caso, você pode confiar permanentemente no certificado autoassinado ou importar os certificados assinados pela CA para os controladores para que o plug-in possa autenticar solicitações de clientes recebidas desses controladores.

Use certificados assinados por CA no plug-in de armazenamento do SANtricity para vCenter

Você pode obter e importar certificados assinados pela CA para acesso seguro ao sistema de gerenciamento que hospeda o plug-in de armazenamento para vCenter.

O uso de certificados assinados pela CA é um procedimento de três etapas:

- [Passo 1: Complete um arquivo CSR.](#)
- [Passo 2: Envie o arquivo CSR.](#)
- [Passo 3: Importar certificados de gestão.](#)

Passo 1: Complete um arquivo CSR

Você deve primeiro gerar um arquivo de solicitação de assinatura de certificado (CSR), que identifica sua organização e o sistema host onde o plug-in está sendo executado. Como alternativa, você pode gerar um arquivo CSR usando uma ferramenta como OpenSSL e pular para [Passo 2: Envie o arquivo CSR](#).

Passos

1. Selecione **Gerenciamento de certificados**.
2. Na guia **Management**, selecione **Complete CSR**.
3. Insira as seguintes informações e clique em **Next**:
 - **Organização** — o nome completo e legal de sua empresa ou organização. Inclua sufixos, como Inc. Ou Corp.
 - * Unidade organizacional (opcional) * — a divisão da sua organização que está a lidar com o certificado.
 - **Cidade/localidade** — a cidade onde o seu sistema de acolhimento ou negócio está localizado.
 - **Estado/região (opcional)** — o estado ou a região onde o seu sistema anfitrião ou negócio está localizado.
 - **Código ISO do país** — o código ISO de dois dígitos do seu país (Organização Internacional para Padronização), como os EUA.
4. Insira as seguintes informações sobre o sistema host onde o plugin está sendo executado:
 - * Nome comum* — o endereço IP ou o nome DNS do sistema host onde o plugin está sendo executado. Certifique-se de que este endereço está correto; ele deve corresponder exatamente ao que você digita para acessar o plugin no navegador. Não inclua http:// ou https://. O nome DNS não pode começar com um curinga.
 - **Endereços IP alternativos** — se o nome comum for um endereço IP, você pode opcionalmente inserir quaisquer endereços IP adicionais ou aliases para o sistema host. Para várias entradas, use um formato delimitado por vírgulas.
 - **Nomes DNS alternativos** — se o nome comum for um nome DNS, insira quaisquer nomes DNS adicionais para o sistema host. Para várias entradas, use um formato delimitado por vírgulas. Se não houver nomes DNS alternativos, mas você inseriu um nome DNS no primeiro campo, copie esse nome aqui. O nome DNS não pode começar com um curinga.
5. Certifique-se de que as informações do host estão corretas. Se não estiver, os certificados retornados da CA falharão quando você tentar importá-los.
6. Clique em **Finish**.

Passo 2: Envie o arquivo CSR

Depois de criar um arquivo de solicitação de assinatura de certificado (CSR), você envia o arquivo CSR gerado para uma CA para receber certificados de gerenciamento assinados para o sistema que hospeda o plug-in.

Os sistemas e-Series exigem o formato PEM (codificação ASCII Base64) para certificados assinados, que inclui os seguintes tipos de arquivo: .pem, .crt, .cer ou .key.

Passos

1. Localize o ficheiro CSR transferido.

A localização da pasta do download depende do seu navegador.

- Envie o arquivo CSR para uma CA (por exemplo, VeriSign ou DigiCert) e solicite certificados assinados no formato PEM.



Depois de enviar um arquivo CSR para a CA, NÃO regenere outro arquivo CSR.

Sempre que você gera um CSR, o sistema cria um par de chaves privadas e públicas. A chave pública faz parte da CSR, enquanto a chave privada é mantida no keystore do sistema. Quando você recebe os certificados assinados e os importa, o sistema garante que as chaves privadas e públicas sejam o par original. Se as chaves não corresponderem, os certificados assinados não funcionarão e você deverá solicitar novos certificados à CA.

Passo 3: Importar certificados de gestão

Depois de receber certificados assinados da Autoridade de Certificação (CA), importe os certificados para o sistema host onde o plug-in está instalado.

Antes de começar

- Você deve ter os certificados assinados da CA. Esses arquivos incluem o certificado raiz, um ou mais certificados intermediários e o certificado do servidor.
- Se a CA forneceu um arquivo de certificado encadeado (por exemplo, um arquivo .p7b), você deve descompactar o arquivo encadeado em arquivos individuais: O certificado raiz, um ou mais certificados intermediários e o certificado do servidor. Você pode usar o utilitário certmgr do Windows para descompactar os arquivos (clique com o botão direito do Mouse e selecione **todas as tarefas > Exportar**). A codificação base-64 é recomendada. Quando as exportações estiverem concluídas, um arquivo CER é exibido para cada arquivo de certificado na cadeia.
- Você deve copiar os arquivos de certificado para o sistema host onde o plugin está sendo executado.

Passos

- Selecione **Gerenciamento de certificados**.
- Na guia **Gerenciamento**, selecione **Importar**.

Abre-se uma caixa de diálogo para importar os ficheiros de certificado.

- Clique em **Procurar** para selecionar primeiro os arquivos de certificado raiz e intermediário e, em seguida, selecione o certificado do servidor. Se você gerou o CSR a partir de uma ferramenta externa, você também deve importar o arquivo de chave privada que foi criado juntamente com o CSR.

Os nomes de arquivo são exibidos na caixa de diálogo.

- Clique em **Importar**.

Resultado

Os arquivos são carregados e validados. As informações do certificado são exibidas na página Gerenciamento de certificados.

Redefinir certificados de gerenciamento no plug-in de armazenamento do SANtricity para vCenter

Para o sistema de gerenciamento que hospeda o plug-in de armazenamento para vCenter, você pode reverter o certificado de gerenciamento para o estado original,

autoassinado de fábrica.

Sobre esta tarefa

Esta tarefa exclui o certificado de gerenciamento atual do sistema host onde o plug-in de armazenamento para vCenter está sendo executado. Depois que o certificado é redefinido, o sistema host reverte para usando o certificado autoassinado.

Passos

1. Selecione **Gerenciamento de certificados**.
2. Na guia **Management**, selecione **Reset**.

Uma caixa de diálogo confirmar certificado de gerenciamento de redefinição é aberta.

3. Digite reset no campo e clique em **Reset**.

Após a atualização do navegador, o navegador pode bloquear o acesso ao site de destino e informar que o site está usando HTTP Strict Transport Security. Essa condição surge quando você volta para certificados autoassinados. Para limpar a condição que está bloqueando o acesso ao destino, você deve limpar os dados de navegação do navegador.

Resultado

O sistema reverte para o uso do certificado autoassinado do servidor. Como resultado, o sistema solicita aos usuários que aceitem manualmente o certificado autoassinado para suas sessões.

Importar certificados para arrays no plug-in de armazenamento do SANtricity para vCenter

Se necessário, você pode importar certificados para os storages de armazenamento para que eles possam se autenticar com o sistema que hospeda o Storage Plugin for vCenter. Os certificados podem ser assinados por uma autoridade de certificação (CA) ou podem ser autoassinados.

Antes de começar

Se você estiver importando certificados confiáveis, os certificados devem ser importados para os controladores de storage usando o System Manager.

Passos

1. Selecione **Gerenciamento de certificados**.
2. Selecione a guia **Trusted**.

Esta página mostra todos os certificados reportados para os storages de armazenamento.

3. Selecione um **Importar > certificados** para importar um certificado de CA ou **Importar > certificados de matriz de armazenamento autoassinados** para importar um certificado autoassinado.
4. Para limitar a exibição, você pode usar o campo de filtragem **Mostrar certificados que são...** ou pode classificar as linhas de certificado clicando em um dos cabeçalhos de coluna.
5. Na caixa de diálogo, selecione o certificado e clique em **Importar**.

O certificado é carregado e validado.

Exibir certificados no plug-in de armazenamento do SANtricity para vCenter

Você pode ver informações resumidas de um certificado, que inclui a organização usando o certificado, a autoridade que emitiu o certificado, o período de validade e as impressões digitais (identificadores exclusivos).

Passos

1. Selecione **Gerenciamento de certificados**.
2. Selecione um dos seguintes separadores:
 - **Management** — mostra o certificado para o sistema que hospeda o plugin. Um certificado de gerenciamento pode ser autoassinado ou aprovado por uma autoridade de certificação (CA). Ele permite o acesso seguro ao plugin.
 - **Trusted** — mostra os certificados que o plug-in pode acessar para matrizes de armazenamento e outros servidores remotos, como um servidor LDAP. Os certificados podem ser emitidos a partir de uma autoridade de certificação (CA) ou podem ser autoassinados.
3. Para ver mais informações sobre um certificado, selecione sua linha, selecione as elipses no final da linha e clique em **Exibir** ou **Exportar**.

Exportar certificados no plug-in de armazenamento do SANtricity para vCenter

Você pode exportar um certificado para exibir seus detalhes completos.

Antes de começar

Para abrir o ficheiro exportado, tem de ter uma aplicação de visualizador de certificados.

Passos

1. Selecione **Gerenciamento de certificados**.
2. Selecione um dos seguintes separadores:
 - **Management** — mostra o certificado para o sistema que hospeda o plugin. Um certificado de gerenciamento pode ser autoassinado ou aprovado por uma autoridade de certificação (CA). Ele permite o acesso seguro ao plugin.
 - **Trusted** — mostra os certificados que o plug-in pode acessar para matrizes de armazenamento e outros servidores remotos, como um servidor LDAP. Os certificados podem ser emitidos a partir de uma autoridade de certificação (CA) ou podem ser autoassinados.
3. Selecione um certificado na página e, em seguida, clique nas elipses no final da linha.
4. Clique em **Exportar** e salve o arquivo de certificado.
5. Abra o arquivo no aplicativo visualizador de certificados.

Excluir certificados confiáveis no plug-in de armazenamento do SANtricity para vCenter

Você pode excluir um ou mais certificados que não são mais necessários, como um certificado expirado.

Antes de começar

Importe o novo certificado antes de excluir o antigo.



Esteja ciente de que a exclusão de um certificado raiz ou intermediário pode afetar vários storages, já que esses storages podem compartilhar os mesmos arquivos de certificado.

Passos

1. Selecione **Gerenciamento de certificados**.
2. Selecione a guia **Trusted**.
3. Selecione um ou mais certificados na tabela e clique em **Excluir**.



A função Delete (Eliminar) não está disponível para certificados pré-instalados.

A caixa de diálogo confirmar Excluir certificado confiável é aberta.

4. Confirme a exclusão e clique em **Excluir**.

O certificado é removido da tabela.

Resolva certificados não confiáveis no plug-in de armazenamento do SANtricity para vCenter

Na página certificado, você pode resolver certificados não confiáveis importando um certificado autoassinado da matriz de armazenamento ou importando um certificado de autoridade de certificação (CA) emitido por um terceiro confiável.

Antes de começar

Se pretender importar um certificado assinado pela CA, certifique-se de que:

- Você gerou uma solicitação de assinatura de certificado (arquivo .CSR) para cada controlador na matriz de armazenamento e a enviou para a CA.
- A CA retornou arquivos de certificado confiáveis.
- Os ficheiros de certificado estão disponíveis no sistema local.

Sobre esta tarefa

Certificados não confiáveis ocorrem quando um storage array tenta estabelecer uma conexão segura com o plugin, mas a conexão não consegue confirmar como segura. Talvez seja necessário instalar certificados de CA confiáveis adicionais se alguma das seguintes opções for verdadeira:

- Recentemente, você adicionou uma matriz de armazenamento.
- Um ou ambos os certificados estão expirados ou revogados.
- Um ou ambos os certificados estão faltando um certificado raiz ou intermediário.

Passos

1. Selecione **Gerenciamento de certificados**.
2. Selecione a guia **Trusted**.

Esta página mostra todos os certificados reportados para os storages de armazenamento.

3. Selecione um **Importar > certificados** para importar um certificado de CA ou **Importar > certificados de matriz de armazenamento autoassinados** para importar um certificado autoassinado.
4. Para limitar a exibição, você pode usar o campo de filtragem **Mostrar certificados que são...** ou pode classificar as linhas de certificado clicando em um dos cabeçalhos de coluna.
5. Na caixa de diálogo, selecione o certificado e clique em **Importar**.

O certificado é carregado e validado.

Informações sobre direitos autorais

Copyright © 2026 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 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 DOCUMENTOS, 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.