



# **Configurar certificado CA para host Windows**

SnapCenter software

NetApp  
November 06, 2025

# Índice

Configurar certificado CA para host Windows . . . . .	1
Gerar arquivo CSR de certificado CA . . . . .	1
Importar certificados de CA . . . . .	1
Obtenha a impressão digital do certificado CA . . . . .	2
Configurar certificado CA com serviços de plug-in de host do Windows . . . . .	2
Configurar certificado CA com o site SnapCenter . . . . .	3
Habilitar certificados CA para SnapCenter . . . . .	4

# Configurar certificado CA para host Windows

## Gerar arquivo CSR de certificado CA

Você pode gerar uma Solicitação de Assinatura de Certificado (CSR) e importar o certificado que pode ser obtido de uma Autoridade de Certificação (CA) usando o CSR gerado. O certificado terá uma chave privada associada a ele.

CSR é um bloco de texto codificado que é fornecido a um fornecedor de certificado autorizado para obter o certificado de CA assinado.



O comprimento mínimo da chave RSA do certificado CA deve ser de 3072 bits.

Para obter informações sobre como gerar um CSR, consulte "[Como gerar um arquivo CSR de certificado CA](#)"



Se você possui o certificado CA para seu domínio (\*.domain.company.com) ou seu sistema (machine1.domain.company.com), você pode pular a geração do arquivo CSR do certificado CA. Você pode implantar o certificado CA existente com o SnapCenter.

Para configurações de cluster, o nome do cluster (FQDN do cluster virtual) e os respectivos nomes de host devem ser mencionados no certificado da CA. O certificado pode ser atualizado preenchendo o campo Nome Alternativo do Assunto (SAN) antes de adquirir o certificado. Para um certificado curinga (\*.domain.company.com), o certificado conterá todos os nomes de host do domínio implicitamente.

## Importar certificados de CA

Você deve importar os certificados de CA para o SnapCenter Server e os plug-ins do host do Windows usando o console de gerenciamento da Microsoft (MMC).

### Passos

1. Acesse o console de gerenciamento da Microsoft (MMC) e clique em **Arquivo > Adicionar/Remover Snapin**.
2. Na janela Adicionar ou remover snap-ins, selecione **Certificados** e clique em **Adicionar**.
3. Na janela do snap-in Certificados, selecione a opção **Conta de computador** e clique em **Concluir**.
4. Clique em **Console Root > Certificados – Computador local > Autoridades de certificação raiz confiáveis > Certificados**.
5. Clique com o botão direito do mouse na pasta “Autoridades de Certificação Raiz Confiáveis” e selecione **Todas as Tarefas > Importar** para iniciar o assistente de importação.
6. Conclua o assistente da seguinte forma:

Nesta janela do assistente...	Faça o seguinte...
Importar chave privada	Selecione a opção <b>Sim</b> , importe a chave privada e clique em <b>Avançar</b> .

Nesta janela do assistente...	Faça o seguinte...
Formato de arquivo de importação	Não faça alterações; clique em <b>Avançar</b> .
Segurança	Especifique a nova senha a ser usada para o certificado exportado e clique em <b>Avançar</b> .
Concluindo o Assistente de Importação de Certificados	Revise o resumo e clique em <b>Concluir</b> para iniciar a importação.



O certificado de importação deve ser agrupado com a chave privada (os formatos suportados são: \*.pfx, \*.p12 e \*.p7b).

7. Repita a Etapa 5 para a pasta “Pessoal”.

## Obtenha a impressão digital do certificado CA

Uma impressão digital de certificado é uma sequência hexadecimal que identifica um certificado. Uma impressão digital é calculada a partir do conteúdo do certificado usando um algoritmo de impressão digital.

### Passos

1. Execute o seguinte na GUI:
  - Clique duas vezes no certificado.
  - Na caixa de diálogo Certificado, clique na guia **Detalhes**.
  - Percorra a lista de campos e clique em **Impressão digital**.
  - Copie os caracteres hexadecimais da caixa.
  - Remova os espaços entre os números hexadecimais.

Por exemplo, se a impressão digital for: "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", após remover os espaços, será: "a909502dd82ae41433e6f83886b00d4277a32a7b".

2. Execute o seguinte no PowerShell:
  - Execute o seguinte comando para listar a impressão digital do certificado instalado e identificar o certificado instalado recentemente pelo nome do assunto.

```
Get-ChildItem -Path Cert:\LocalMachine\My
```

  - Copie a impressão digital.

## Configurar certificado CA com serviços de plug-in de host do Windows

Você deve configurar o certificado CA com os serviços de plug-in do host do Windows para ativar o certificado digital instalado.

Execute as seguintes etapas no SnapCenter Server e em todos os hosts de plug-in onde os certificados CA já estão implantados.

### Passos

1. Remova a vinculação de certificado existente com a porta padrão 8145 do SMCore, executando o seguinte comando:

```
> netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
```

Por exemplo:

```
> netsh http delete sslcert ipport=0.0.0.0:8145  
. Vincule o certificado recém-instalado aos serviços de plug-in do host  
do Windows, executando os seguintes comandos:
```

```
> $cert = "_<certificate thumbprint>"  
> $guid = [guid]::NewGuid().ToString("B")  
> netsh http add sslcert ipport=0.0.0.0:_<SMCore Port>_ certhash=$cert  
appid="$guid"
```

Por exemplo:

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"  
> $guid = [guid]::NewGuid().ToString("B")  
> netsh http add sslcert ipport=0.0.0.0:_<SMCore Port>_ certhash=$cert  
appid="$guid"
```

## Configurar certificado CA com o site SnapCenter

Você deve configurar o certificado CA com o site SnapCenter no host Windows.

### Passos

1. Abra o Gerenciador do IIS no Windows Server onde o SnapCenter está instalado.
2. No painel de navegação esquerdo, clique em **Conexões**.
3. Expanda o nome do servidor e **Sites**.
4. Selecione o site do SnapCenter no qual você deseja instalar o Certificado SSL.
5. Navegue até **Ações > Editar site** e clique em **Vinculações**.
6. Na página Ligações, selecione **ligação para https**.
7. Clique em **Editar**.
8. Na lista suspensa do certificado SSL, selecione o certificado SSL importado recentemente.
9. Clique em **OK**.

 O site do SnapCenter Scheduler (porta padrão: 8154, HTTPS) é configurado com certificado autoassinado. Esta porta está se comunicando dentro do host do SnapCenter Server e não é obrigatório configura-la com um certificado CA. No entanto, se o seu ambiente exigir que você use um Certificado CA, repita as etapas 5 a 9 usando o site SnapCenter Scheduler.

 Se o certificado CA implantado recentemente não estiver listado no menu suspenso, verifique se o certificado CA está associado à chave privada.

 Certifique-se de que o certificado seja adicionado usando o seguinte caminho: **Raiz do console > Certificados – Computador local > Autoridades de certificação raiz confiáveis > Certificados**.

## Habilitar certificados CA para SnapCenter

Você deve configurar os certificados CA e habilitar a validação do certificado CA para o SnapCenter Server.

### Antes de começar

- Você pode habilitar ou desabilitar os certificados da CA usando o cmdlet Set-SmCertificateSettings.
- Você pode exibir o status do certificado do SnapCenter Server usando o cmdlet Get-SmCertificateSettings.

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command\_name*. Alternativamente, você pode consultar o "[Guia de referência do cmdlet do software SnapCenter](#)" .

### Passos

1. Na página Configurações, navegue até **Configurações > Configurações globais > Configurações do certificado CA**.
2. Selecione **Ativar validação de certificado**.
3. Clique em **Aplicar**.

### Depois que você terminar

A guia Hosts gerenciados exibe um cadeado e a cor do cadeado indica o status da conexão entre o SnapCenter Server e o host do plug-in.

- \*  \* indica que não há nenhum certificado CA habilitado ou atribuído ao host do plug-in.
- \*  \* indica que o certificado CA foi validado com sucesso.
- \*  \* indica que o certificado CA não pôde ser validado.
- \*  \* indica que as informações de conexão não puderam ser recuperadas.

 Quando o status é amarelo ou verde, as operações de proteção de dados foram concluídas com sucesso.

## **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 DESTE DOCUMENTO. 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 SOBRESSALENTES; 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 DESTE SOFTWARE, 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.