



# Configurar o certificado CA para o host Windows

SnapCenter Software 6.0

NetApp  
December 19, 2024

# Índice

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

# Configurar o certificado CA para o host Windows

## Gerar arquivo CSR do 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 a CSR gerada. O certificado terá uma chave privada associada a ele.

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



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

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



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

Para configurações de cluster, o nome do cluster (FQDN de 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 (SAN) do assunto antes de adquirir o certificado. Para um certificado Wild card (\*.domain.company.com), o certificado conterá todos os nomes de host do domínio implicitamente.

## Importar certificados CA

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

### Passos

1. Vá para o console de gerenciamento da Microsoft (MMC) e clique em **File > Add/Remove Snapin**.
2. Na janela Adicionar ou remover snap-ins, selecione **certificados** e clique em **Adicionar**.
3. Na janela de snap-in certificados, selecione a opção **conta de computador** e clique em **concluir**.
4. Clique em **raiz da consola > certificados – computador local > autoridades de Certificação raiz fidedignas > certificados**.
5. Clique com o botão direito do rato na pasta "autoridades de Certificação de raiz fidedigna" 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>Yes</b> , importe a chave privada e clique em <b>Next</b> .
Importar formato de ficheiro	Não faça alterações; clique em <b>seguinte</b> .

Nesta janela do assistente...	Faça o seguinte...
Segurança	Especifique a nova senha a ser usada para o certificado exportado e clique em <b>Avançar</b> .
Concluir o Assistente de importação de certificados	Revise o resumo e clique em <b>Finish</b> para iniciar a importação.



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

7. Repita o passo 5 para a pasta "Pessoal".

## Obtenha a impressão digital do certificado CA

Uma impressão digital de certificado é uma cadeia 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:
  - a. Clique duas vezes no certificado.
  - b. Na caixa de diálogo certificado, clique na guia **Detalhes**.
  - c. Percorra a lista de campos e clique em **thumbprint**.
  - d. Copie os caracteres hexadecimais da caixa.
  - e. 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", depois de remover os espaços, será: "A909502d82ae41433e6f83886b00d4277a32a7b".

2. Execute o seguinte no PowerShell:
  - a. 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
```
  - b. Copie a impressão digital.

## Configure o certificado CA com os serviços de plug-in do host do Windows

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

Execute as etapas a seguir no servidor SnapCenter e em todos os hosts de plug-in em que os certificados de CA já estão implantados.

## Passos

1. Remova a vinculação de certificado existente com a porta padrão SMCore 8145, 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"
```

## Configure o 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 servidor Windows em que o SnapCenter está instalado.
2. No painel de navegação esquerdo, clique em **Connections** (ligações).
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**, clique em **ligações**.
6. Na página ligações, selecione **encadernação para https**.
7. Clique em **Editar**.
8. Na lista suspensa certificado SSL, selecione o certificado SSL recentemente importado.
9. Clique em **OK**.



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



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



Certifique-se de que o certificado é adicionado usando o seguinte caminho: **Raiz da consola > certificados – computador local > autoridades de certificação raiz fidedignas > certificados**.

## Ativar certificados de CA para SnapCenter

Você deve configurar os certificados da CA e ativar a validação do certificado da CA para o servidor SnapCenter.

### Antes de começar

- Você pode ativar ou desativar os certificados de CA usando o cmdlet `Set-SmCertificateSettings`.
- Você pode exibir o status do certificado para o servidor SnapCenter 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`. Em alternativa, pode consultar a "[Guia de referência de 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 de terminar

O host de guia hosts gerenciados exibe um cadeado e a cor do cadeado indica o status da conexão entre o servidor SnapCenter e o host do plug-in.

- \*\* Indica que não há certificado CA habilitado ou atribuído ao host do plug-in.
- \*\* Indica que o certificado da CA foi validado com êxito.
- \*\* Indica que o certificado da 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 são concluídas com êxito.

## 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 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.