



Configurar certificado CA

SnapCenter Software 6.0

NetApp
December 19, 2024

Índice

- Configurar certificado CA 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 para o serviço de plug-ins compatíveis com NetApp no host Linux 3
 - Configure o certificado CA para o serviço de plug-ins compatíveis com o NetApp no host Windows 6
 - Ative certificados de CA para plug-ins 8

Configurar certificado CA

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 Yes , importe a chave privada e clique em Next .
Importar formato de ficheiro	Não faça alterações; clique em seguinte .

Nesta janela do assistente...	Faça o seguinte...
Segurança	Especifique a nova senha a ser usada para o certificado exportado e clique em Avançar .
Concluir o Assistente de importação de certificados	Revise o resumo e clique em Finish 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 para o serviço de plug-ins compatíveis com NetApp no host Linux

Você deve gerenciar a senha do armazenamento de chaves de plug-ins personalizados e seu certificado, configurar o certificado de CA, configurar certificados raiz ou intermediários para o armazenamento de confiança de plug-ins personalizados e configurar o par de chaves assinadas de CA para armazenamento de confiança de plug-ins personalizados com o serviço de plug-ins personalizados SnapCenter para ativar o certificado digital instalado.

Plug-ins personalizados usam o arquivo 'keystore.jks', que está localizado em `/opt/NetApp/SnapCenter/scc/etc` tanto como seu armazenamento de confiança e armazenamento de chaves.

Gerenciar senha para armazenamento de chaves plug-in personalizado e alias do par de chaves assinadas CA em uso

Passos

1. Você pode recuperar a senha padrão do keystore do plug-in personalizado do arquivo de propriedade do agente do plug-in personalizado.

É o valor correspondente à chave 'KEYSTORE_PASS'.

2. Altere a senha do keystore:

```
keytool -storepasswd -keystore keystore.jks  
. Altere a senha para todos os aliases de entradas de chave privada no  
keystore para a mesma senha usada para o keystore:
```

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

Atualize o mesmo para a chave KEYSTORE_PASS no arquivo *agent.properties*.

3. Reinicie o serviço depois de alterar a senha.



A palavra-passe para o armazenamento de chaves plug-in personalizado e para todas as palavras-passe de alias associadas da chave privada deve ser a mesma.

Configure certificados raiz ou intermediários para armazenamento de confiança de plug-in personalizado

Você deve configurar os certificados raiz ou intermediários sem a chave privada para armazenamento de confiança de plug-in personalizado.

Passos

1. Navegue até a pasta que contém o keystore de plug-in personalizado: */Opt/NetApp/SnapCenter/scc/etc*.
2. Localize o arquivo 'keystore.jks'.
3. Liste os certificados adicionados no keystore:

```
keytool -list -v -keystore keystore.jks
```

4. Adicione um certificado raiz ou intermediário:

```
keytool -import -trustcacerts -alias myRootCA -file  
/root/USERTrustRSA_Root.cer -keystore keystore.jks  
. Reinicie o serviço depois de configurar os certificados raiz ou  
intermédios para o armazenamento de confiança de plug-in personalizado.
```



Você deve adicionar o certificado de CA raiz e, em seguida, os certificados de CA intermediários.

Configure o par de chaves assinadas da CA para o armazenamento de confiança de plug-in personalizado

Você deve configurar o par de chaves assinadas da CA para o armazenamento de confiança do plug-in personalizado.

Passos

1. Navegue até a pasta que contém o keystore de plug-in personalizado /opt/NetApp/SnapCenter/scc/etc.
2. Localize o arquivo 'keystore.jks'.
3. Liste os certificados adicionados no keystore:

```
keytool -list -v -keystore keystore.jks
```

4. Adicione o certificado da CA com chave privada e pública.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx  
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. Liste os certificados adicionados no keystore.

```
keytool -list -v -keystore keystore.jks
```

6. Verifique se o keystore contém o alias correspondente ao novo certificado da CA, que foi adicionado ao keystore.
7. Altere a senha da chave privada adicionada para o certificado da CA para a senha do keystore.

A senha padrão do keystore do plug-in personalizado é o valor da chave KEYSTORE_PASS no arquivo agent.properties.

```
keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore  
keystore.jks
```

. Se o nome do alias no certificado da CA for longo e contiver espaço ou caracteres especiais ("*", ",", "), altere o nome do alias para um nome simples:

```
keytool -changealias -alias "long_alias_name" -destalias "simple_alias"  
-keystore keystore.jks
```

. Configure o nome do alias do certificado CA no arquivo agent.properties.

Atualize este valor com a chave SCC_CERTIFICATE_ALIAS.

8. Reinicie o serviço depois de configurar o par de chaves assinadas pela CA para o armazenamento de confiança de plug-in personalizado.

Configurar a lista de revogação de certificados (CRL) para plug-ins personalizados do SnapCenter

Sobre esta tarefa

- Os plug-ins personalizados do SnapCenter pesquisarão os arquivos CRL em um diretório pré-configurado.
- O diretório padrão para os arquivos CRL para plug-ins personalizados do SnapCenter é 'opt/NetApp/SnapCenter/scc/etc/crl'.

Passos

1. Você pode modificar e atualizar o diretório padrão no arquivo `agent.properties` contra a chave `CRL_PATH`.

Você pode colocar mais de um arquivo CRL neste diretório. Os certificados recebidos serão verificados em relação a cada CRL.

Configure o certificado CA para o serviço de plug-ins compatíveis com o NetApp no host Windows

Você deve gerenciar a senha do armazenamento de chaves de plug-ins personalizados e seu certificado, configurar o certificado de CA, configurar certificados raiz ou intermediários para o armazenamento de confiança de plug-ins personalizados e configurar o par de chaves assinadas de CA para armazenamento de confiança de plug-ins personalizados com o serviço de plug-ins personalizados SnapCenter para ativar o certificado digital instalado.

Plug-ins personalizados usam o arquivo `keystore.jks`, que está localizado em `_C: Arquivos de programas, NetApp, SnapCenter, SnapCenter Plug-in Creator`, tanto como seu armazenamento de confiança e armazenamento de chaves.

Gerenciar senha para armazenamento de chaves plug-in personalizado e alias do par de chaves assinadas CA em uso

Passos

1. Você pode recuperar a senha padrão do keystore do plug-in personalizado do arquivo de propriedade do agente do plug-in personalizado.

É o valor correspondente à chave `KEYSTORE_PASS`.

2. Altere a senha do keystore:

```
keytool -storepasswd -keystore keystore.jks
```



Se o comando "keytool" não for reconhecido no prompt de comando do Windows, substitua o comando keytool por seu caminho completo.

```
C: Arquivos de programas/<jdk_version>/keytool.exe" -storepasswd -keystore keystore.jks
```

3. Altere a senha para todos os aliases de entradas de chave privada no keystore para a mesma senha usada para o keystore:

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

Atualize o mesmo para a chave `KEYSTORE_PASS` no arquivo `agent.properties`.

4. Reinicie o serviço depois de alterar a senha.



A palavra-passe para o armazenamento de chaves plug-in personalizado e para todas as palavras-passe de alias associadas da chave privada deve ser a mesma.

Configure certificados raiz ou intermediários para armazenamento de confiança de plug-in personalizado

Você deve configurar os certificados raiz ou intermediários sem a chave privada para armazenamento de confiança de plug-in personalizado.

Passos

1. Navegue até a pasta que contém o armazenamento de chaves de plug-in personalizado *C: Arquivos de programas/NetApp/SnapCenter/SnapCenter Plug-in Creator/etc*
2. Localize o arquivo 'keystore.jks'.
3. Liste os certificados adicionados no keystore:

```
keytool -list -v -keystore keystore.jks
```

4. Adicione um certificado raiz ou intermediário:

```
Keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_root.cer -keystore keystore.jks
```

5. Reinicie o serviço depois de configurar os certificados raiz ou intermediários para o armazenamento de confiança de plug-in personalizado.



Você deve adicionar o certificado de CA raiz e, em seguida, os certificados de CA intermediários.

Configure o par de chaves assinadas da CA para o armazenamento de confiança de plug-in personalizado

Você deve configurar o par de chaves assinadas da CA para o armazenamento de confiança do plug-in personalizado.

Passos

1. Navegue até a pasta que contém o armazenamento de chaves de plug-in personalizado *C: Arquivos de programas/NetApp/SnapCenter/SnapCenter Plug-in Creator/etc*
2. Localize o arquivo *keystore.jks*.
3. Liste os certificados adicionados no keystore:

```
keytool -list -v -keystore keystore.jks
```

4. Adicione o certificado da CA com chave privada e pública.

```
Keytool -importkeystore -srckeystore /root/SnapCenter.ssl.test.NetApp.com.pfx -srcstoretype PKCS12 -destinkeystore keystore.jks -deststoretype JKS
```

5. Liste os certificados adicionados no keystore.

```
keytool -list -v -keystore keystore.jks
```

6. Verifique se o keystore contém o alias correspondente ao novo certificado da CA, que foi adicionado ao keystore.
7. Altere a senha da chave privada adicionada para o certificado da CA para a senha do keystore.

A senha padrão do keystore do plug-in personalizado é o valor da chave `KEYSTORE_PASS` no arquivo

agent.properties.

```
Keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore keystore.jks
```

8. Configure o nome do alias do certificado CA no arquivo *agent.properties*.

Atualize este valor com a chave SCC_CERTIFICATE_ALIAS.

9. Reinicie o serviço depois de configurar o par de chaves assinadas pela CA para o armazenamento de confiança de plug-in personalizado.

Configurar a lista de revogação de certificados (CRL) para plug-ins personalizados do SnapCenter

Sobre esta tarefa

- Para transferir o ficheiro CRL mais recente para o certificado CA relacionado, "[Como atualizar o arquivo de lista de revogação de certificados no certificado da CA do SnapCenter](#)" consulte .
- Os plug-ins personalizados do SnapCenter pesquisarão os arquivos CRL em um diretório pré-configurado.
- O diretório padrão para os arquivos CRL para os plug-ins personalizados do SnapCenter é 'C: Arquivos de programas/NetApp/SnapCenter/SnapCenter Plug-in Creator etc/crl'.

Passos

1. Você pode modificar e atualizar o diretório padrão no arquivo *agent.properties* contra a chave CRL_PATH.
2. Você pode colocar mais de um arquivo CRL neste diretório.

Os certificados recebidos serão verificados em relação a cada CRL.

Ative certificados de CA para plug-ins

Você deve configurar os certificados de CA e implantar os certificados de CA no servidor SnapCenter e nos hosts de plug-in correspondentes. Você deve habilitar a validação do certificado CA para os plug-ins.

Antes de começar

- Você pode ativar ou desativar os certificados de CA usando o cmdlet RUN *Set-SmCertificateSettings*.
- Você pode exibir o status do certificado para os plug-ins usando as *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 também consultar o "[Guia de referência de cmdlet do software SnapCenter](#)".

Passos

1. No painel de navegação esquerdo, clique em **hosts**.
2. Na página hosts, clique em **hosts gerenciados**.
3. Selecione um ou vários hosts de plug-in.
4. Clique em **mais opções**.
5. Selecione **Ativar Validação de certificado**.

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 o certificado da CA não está habilitado nem 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.