Configurar autenticação baseada em certificado

SnapCenter Software 6.0

NetApp
December 19, 2024

Índice

Configurar autenticação baseada em certificado

Exportar certificados de autoridade de certificação (CA) do servidor SnapCenter

Você deve exportar os certificados de CA do servidor SnapCenter para os hosts de plug-in usando o MMC (console de gerenciamento da Microsoft).

Antes de começar

Você deve ter configurado o SSL bidirecional.

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 certificados Snap-in, selecione a opção **conta de computador** e clique em **concluir**.
4. Clique em **raiz da consola** > **certificados - computador local** > **Pessoal** > **certificados**.
5. Clique com o botão direito do rato no certificado CA adquirido, que é utilizado para o servidor SnapCenter e selecione **todas as tarefas** > **Exportar** para iniciar o assistente de exportação.
6. Execute as seguintes ações no assistente.

Para esta opção…	Faça o seguinte…
Exportar chave privada	Selecione **não, não exporte a chave privada** e, em seguida, clique em **seguinte**.
Exportar formato de ficheiro	Clique em **seguinte**.
Nome do ficheiro	Clique em **Procurar** e especifique o caminho do arquivo para salvar o certificado e clique em **Avançar**.
Concluir o Assistente de exportação de certificados	Revise o resumo e clique em **Finish** para iniciar a exportação.

A autenticação baseada em certificado não é suportada para configurações do SnapCenter HA e plug-in do SnapCenter para VMware vSphere.

Importar certificado de autoridade de certificação (CA) para os hosts de plug-in do Windows

Para usar o certificado de CA de servidor SnapCenter exportado, você deve importar o certificado relacionado para os hosts de plug-in do SnapCenter 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 certificados Snap-in, selecione a opção **conta de computador** e clique em **concluir**.
4. Clique em **raiz da consola** > **certificados - computador local** > **Pessoal** > **certificados**.
5. Clique com o botão direito na pasta "Pessoal" e selecione **todas as tarefas** > **Importar** para iniciar o assistente de importação.
6. Execute as seguintes ações no assistente.

Para esta opção…	Faça o seguinte…
Localização da loja	Clique em **seguinte**.
Ficheiro a importar	Selecione o certificado do servidor SnapCenter que termina com a extensão .cer.
Armazenamento de certificados	Clique em **seguinte**.
Concluir o Assistente de exportação de certificados	Revise o resumo e clique em **Finish** para iniciar a importação.

Importe o certificado CA para os plug-ins do host UNIX e configure certificados raiz ou intermediários para o armazenamento de confiança SPL

Importar certificado CA para os hosts de plug-in UNIX

Você deve importar o certificado CA para os hosts de plug-in UNIX.

Sobre esta tarefa

- Você pode gerenciar a senha do armazenamento de chaves SPL e o alias do par de chaves assinadas CA em uso.
- A senha para o keystore SPL e para toda a senha de alias associada da chave privada deve ser a mesma.

Passos

1. Você pode recuperar a senha padrão do keystore SPL do arquivo de propriedade SPL. É o valor correspondente à chave `SPL_KEYSTORE_PASS`.
2. Altere a senha do keystore: `$ keytool -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>" -keystore keystore.jks`
4. Atualize o mesmo para a chave SPL_KEYSTORE_PASS no `spl.properties` arquivo.

5. Reinicie o serviço depois de alterar a senha.

Configure certificados raiz ou intermediários para o armazenamento de confiança SPL

Você deve configurar os certificados raiz ou intermediários para o SPL Trust-store. Você deve adicionar o certificado de CA raiz e, em seguida, os certificados de CA intermediários.

Passos

1. Navegue até a pasta que contém o keystore SPL: `/var/opt/snapcenter/spl/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 <AliasNameForCerticateToBeImported> -file /<CertificatePath> -keystore keystore.jks`
5. Reinicie o serviço depois de configurar os certificados raiz ou intermédios para o armazenamento de confiança SPL.

Configure o par de chaves assinadas da CA para o armazenamento de confiança SPL

Você deve configurar o par de chaves assinadas da CA para o armazenamento de confiança SPL.

Passos

1. Navegue até a pasta que contém o keystore do SPL `/var/opt/snapcenter/spl/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 <CertificatePathToImport> -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 SPL é o valor da chave SPL_KEYSTORE_PASS no `spl.properties` arquivo.

   ```
   $ keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore keystore.jks`
   ```

8. Se o nome do alias no certificado da CA for longo e contiver espaço ou carateres especiais ("*",","), altere o nome do alias para um nome simples: `$ keytool -changealias -alias "<OrignalAliasName>" -destalias "<NewAliasName>" -keystore keystore.jks`

9. Configure o nome do alias a partir do keystore localizado no `spl.properties` arquivo. Atualize este valor com a chave SPL_CERTIFICATE_ALIAS.
10. Reinicie o serviço depois de configurar o par de chaves assinadas pela CA para o armazenamento de confiança SPL.

Ativar autenticação baseada em certificado

Para habilitar a autenticação baseada em certificado para o servidor SnapCenter e os hosts de plug-in do Windows, execute o cmdlet do PowerShell a seguir. Para os hosts de plug-in Linux, a autenticação baseada em certificado será ativada quando você ativar o SSL bidirecional.

- Para ativar a autenticação baseada em certificado de cliente:

```
Set-SmConfigSettings -Agent –configSettings
@{"EnableClientCertificateAuthentication"="true"} -HostName[hostname]
```

- Para desativar a autenticação baseada em certificado de cliente:

```
Set-SmConfigSettings -Agent –configSettings
@{"EnableClientCertificateAuthentication"="false"} -HostName [hostname]`
```

Exportar certificados SnapCenter

Passos

1. Vá para o console de gerenciamento da Microsoft (MMC) e clique em **File** > **Add/Remove Snap-in**.
2. Na janela Adicionar ou remover snap-ins, selecione **certificados** e clique em **Adicionar**.
3. Na janela de snap-in certificados, selecione a opção **minha conta de usuário** e clique em **concluir**.
4. Clique em **raiz da consola** > **certificados - Utilizador atual** > **autoridades de Certificação raiz fidedignas** > **certificados**.
5. Clique com o botão direito do rato no certificado que tem o Nome amigável do SnapCenter e selecione **todas as tarefas** > **Exportar** para iniciar o assistente de exportação.
6. Conclua o assistente da seguinte forma:

Nesta janela do assistente…	Faça o seguinte…
Exportar chave privada	Selecione a opção **Sim, exporte a chave privada** e clique em **Avançar**.
Exportar formato de ficheiro	Não faça alterações; clique em **seguinte**.
Segurança	Especifique a nova senha a ser usada para o certificado exportado e clique em **Avançar**.

Nesta janela do assistente…	Faça o seguinte…
Ficheiro a exportar	Especifique um nome de arquivo para o certificado exportado (você deve usar .pfx) e clique em **Next**.
Concluir o Assistente de exportação de certificados	Revise o resumo e clique em **Finish** para iniciar a exportação.

Resultado

Os certificados são exportados no formato .pfx.

Informações sobre direitos autorais

Informações sobre marcas comerciais