

How to add VMware ESXi Host Security Certificate to the PowerChute-keystore Manually.

Step 1: Log into the PowerChute VM.

```
Welcome to PowerChute Network Shutdown 5.0.0 for VMware

Please complete the PowerChute Setup wizard to ensure that your VMware Hosts and Virtual Machines
are protected.

To configure PowerChute Network Shutdown using the Setup Wizard, browse to:

https://192.168.0.119:6547/

localhost login: root
Password:
```

Step 2: Stop the PowerChute service.

Enter the command **systemctl stop PowerChute** (Linux is case sensitive. Take note of capital letters)

```
 root@localhost:/opt/APC/PowerChute/group1
```

```
[root@localhost group1]# systemctl stop PowerChute
[root@localhost group1]#
```

Step 3: Edit the pcnsconfig.ini file.

If familiar with using the vi editor, enter **vi /opt/APC/PowerChute/group1/pcnsconfig.ini**

In the **[NetworkManagementCard]** section, add the lines

PowerChuteKeystorePassword = <New password> New password can be replaced with a password of your choice. It must be at least six characters.

```
 root@localhost:/opt/APC/PowerChute/group1

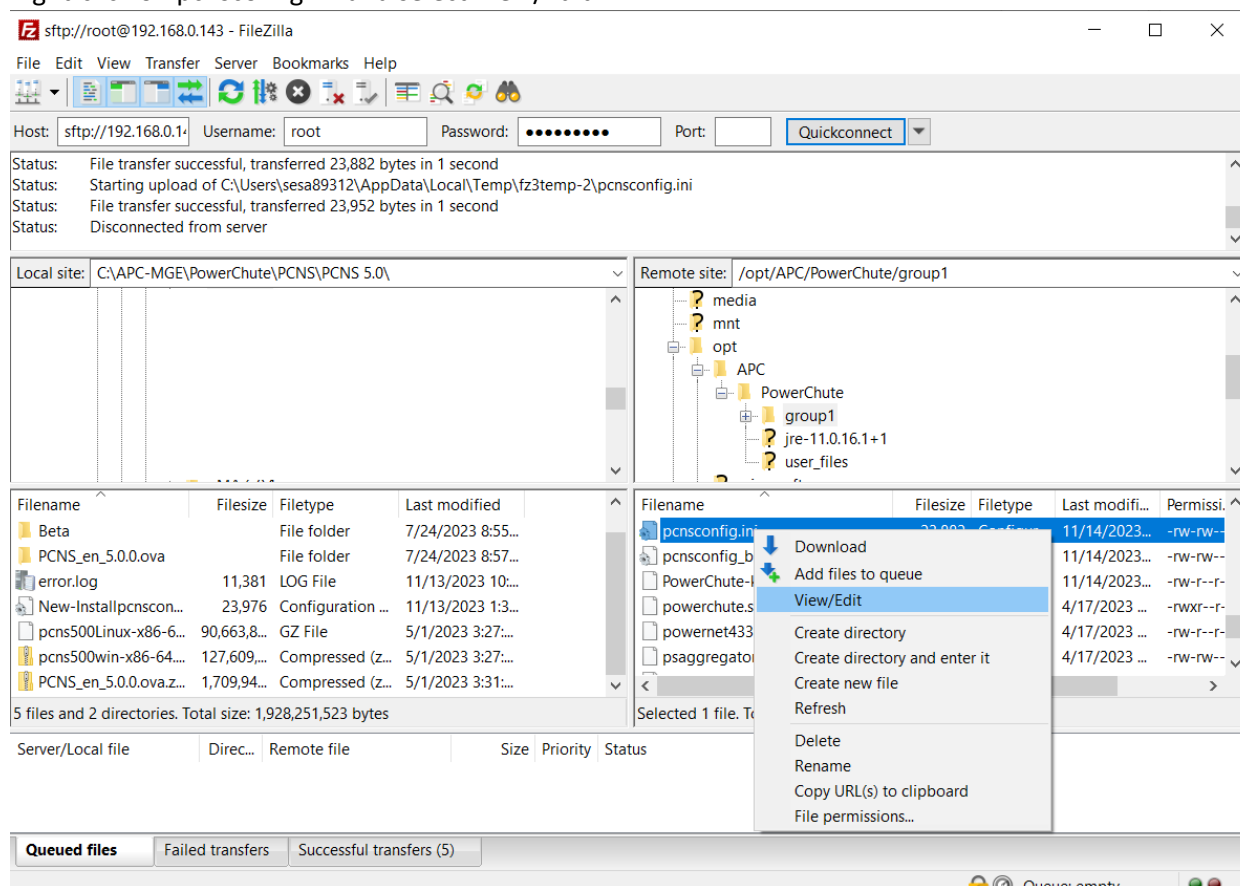
[NetworkManagementCard]
mode = single
IP_1 = 192.168.0.128
port = 443
protocol = https
enrolWithNMC = true
IP_1_Outlet = 1
PowerChuteKeystorePassword = NewPassword
```

If unfamiliar with vi editing, log into the PowerChute VM using Filezilla from the Windows system and use a text editor to edit the file. WinSCP can also be used to log into the VM.

Note: SSH must be enabled on the PowerChute VM to allow the connection.

Once logged in, navigate to **/opt/APC/PowerChute/group1**.

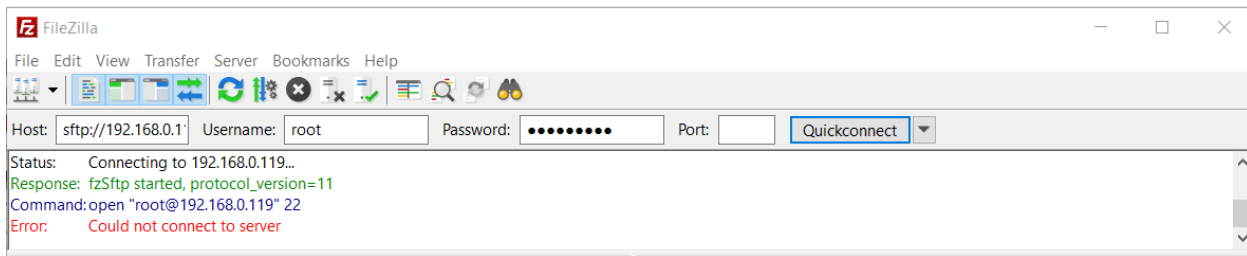
Right-click on pcnsconfig.ini and select View/Edit.



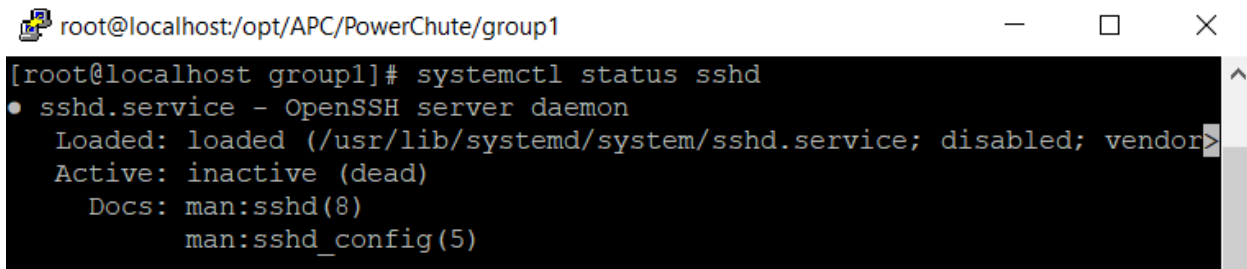
Example of an edited file in Notepad

```
*pcnsconfig - Notepad
File Edit Format View Help
[NetworkManagementCard]
mode = single
IP_1 =
port = 443
protocol = https
enrolWithNMC = true
PowerChuteKeystorePassword = NewPassword
```

If the connection fails, verify SSH has been enabled on the PowerChute VM.

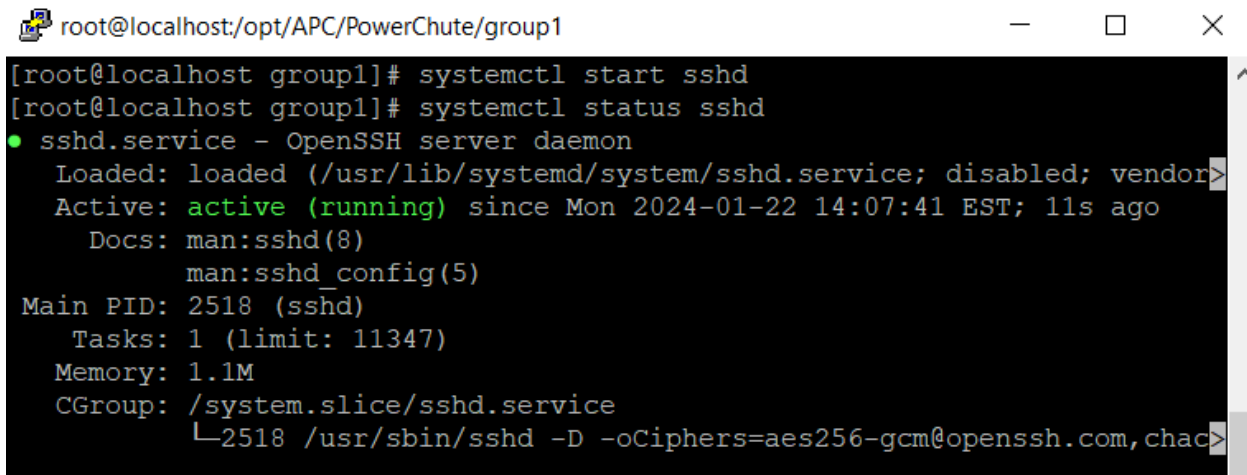


The command to check SSH status on the PowerChute VM is **systemctl status sshd**.



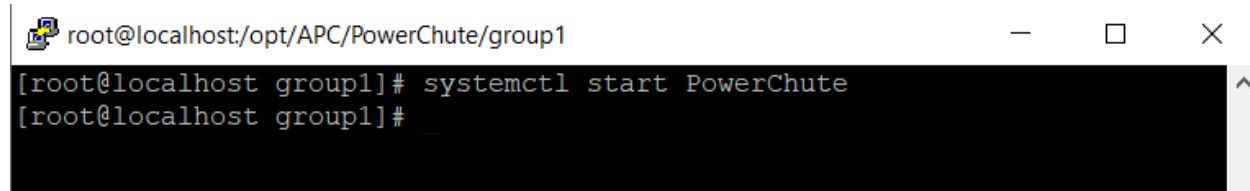
In the example above, the connection failed because SSH was inactive on the PowerChute VM.

To start SSH, enter the **systemctl start sshd**, then run the command **systemctl status sshd** to verify the service started.



Step 4: Restart the PowerChute service Once the pcnsconfig.ini file has been edited and saved.

The command is **systemctl start PowerChute**.

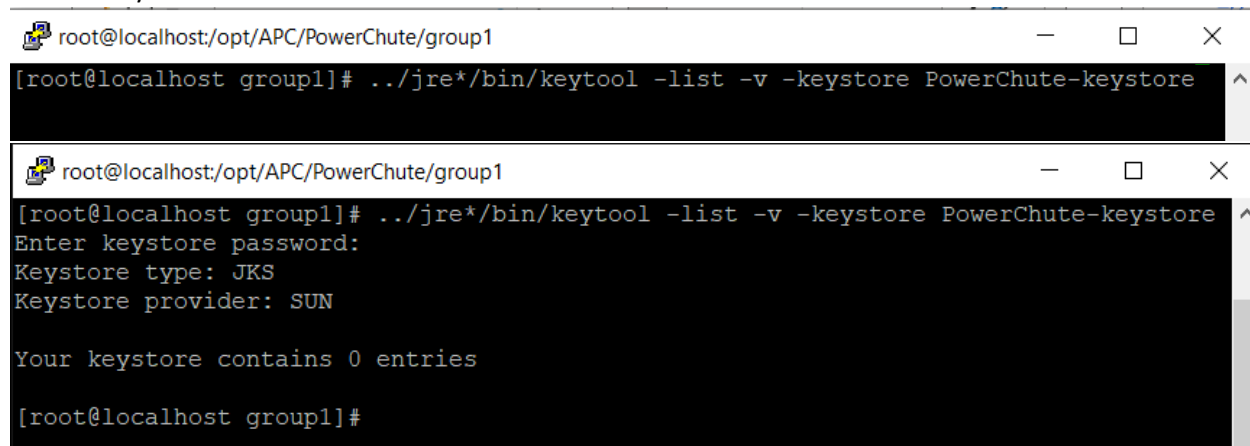


```
root@localhost:/opt/APC/PowerChute/group1
[root@localhost group1]# systemctl start PowerChute
[root@localhost group1]#
```

Step 5: Verify that the PowerChute-keystore password has been changed

cd to /opt/APC/PowerChute/group1.

Enter the command **../jre*/bin/keytool -list -v -keystore PowerChute-keystore**. You will be asked to enter the PowerChute-keystore password. The keystore data should be displayed on the screen. In the example below, the keystore contains 0 entries because we have not added any certificates to the keystore.



```
root@localhost:/opt/APC/PowerChute/group1
[root@localhost group1]# ../jre*/bin/keytool -list -v -keystore PowerChute-keystore

root@localhost:/opt/APC/PowerChute/group1
[root@localhost group1]# ../jre*/bin/keytool -list -v -keystore PowerChute-keystore
Enter keystore password:
Keystore type: JKS
Keystore provider: SUN

Your keystore contains 0 entries

[root@localhost group1]#
```

Step 6: Once the PowerChute-keystore password change has been verified, stop the PowerChute service.

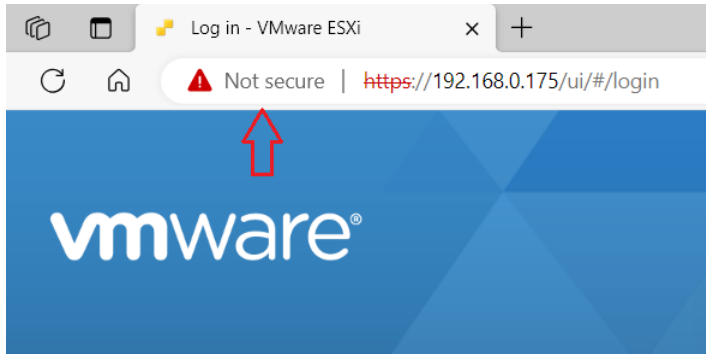
The command is **systemctl stop PowerChute**.

Step 7: Download the ESXi host security certificate to your Windows or Linux system.

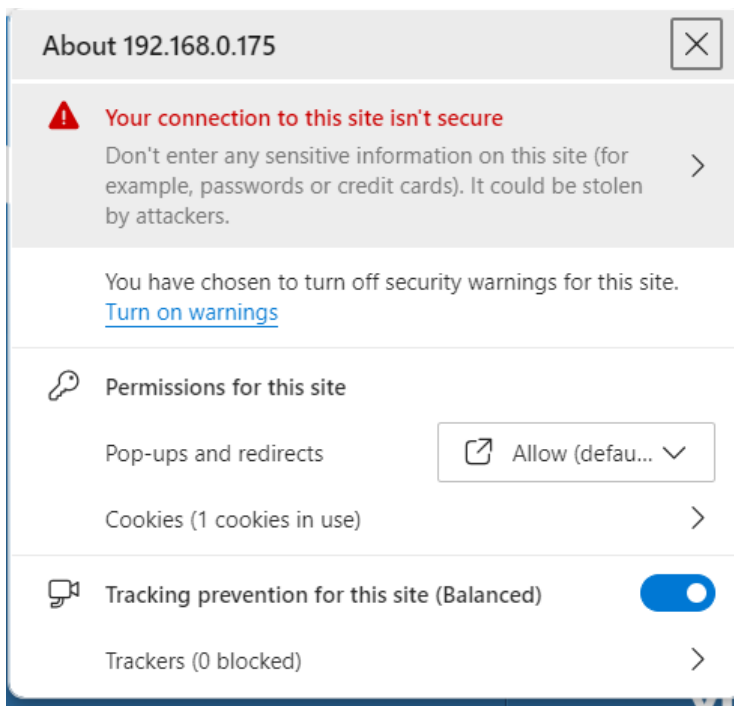
To do so, open a Chrome or Edge browser and enter the host's IP address or domain name.

In the example below, we used Edge.

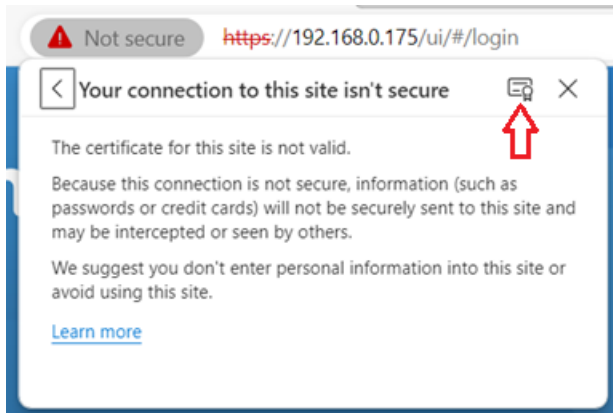
Click on Not Secure



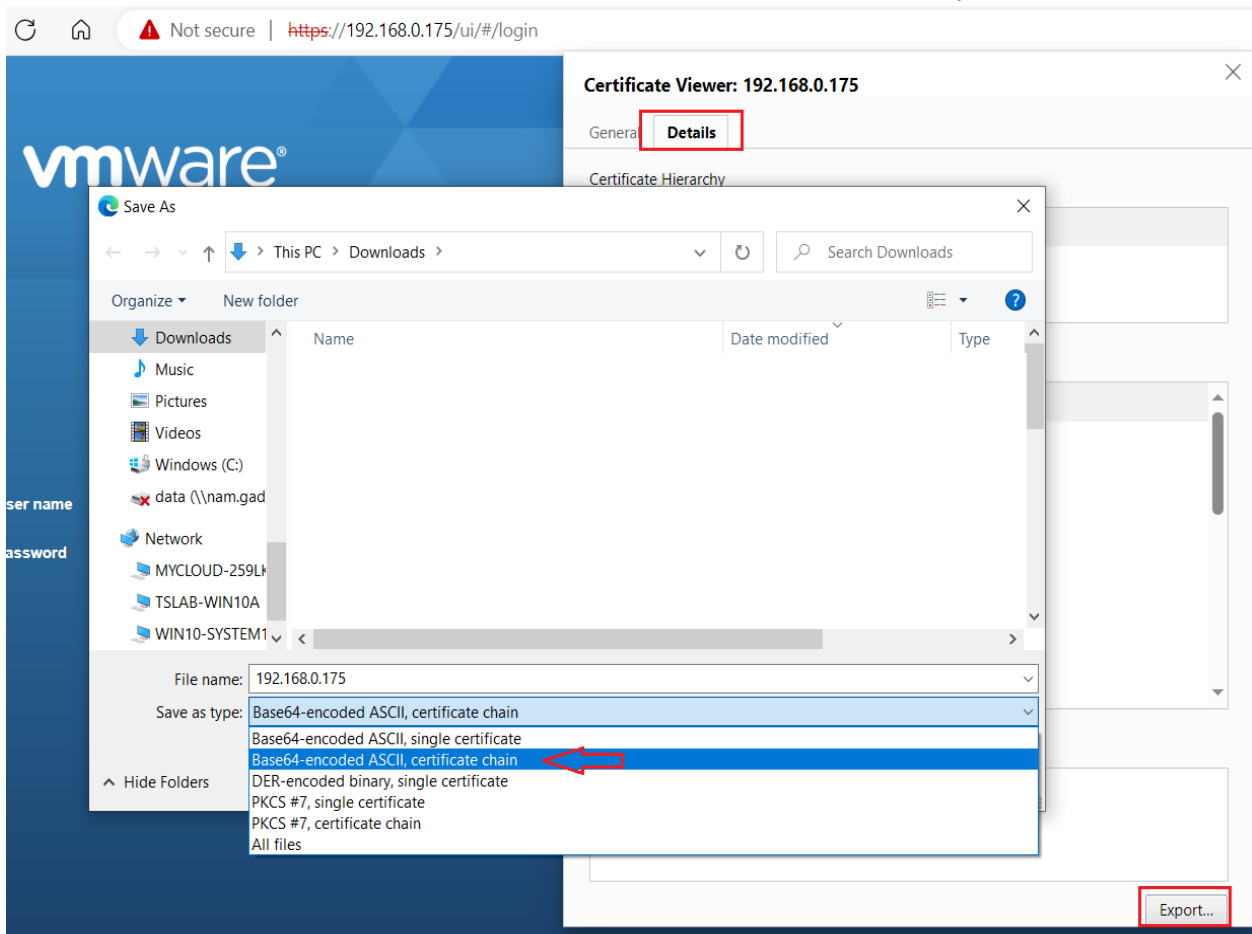
Click on "Your connection to this site isn't secure."



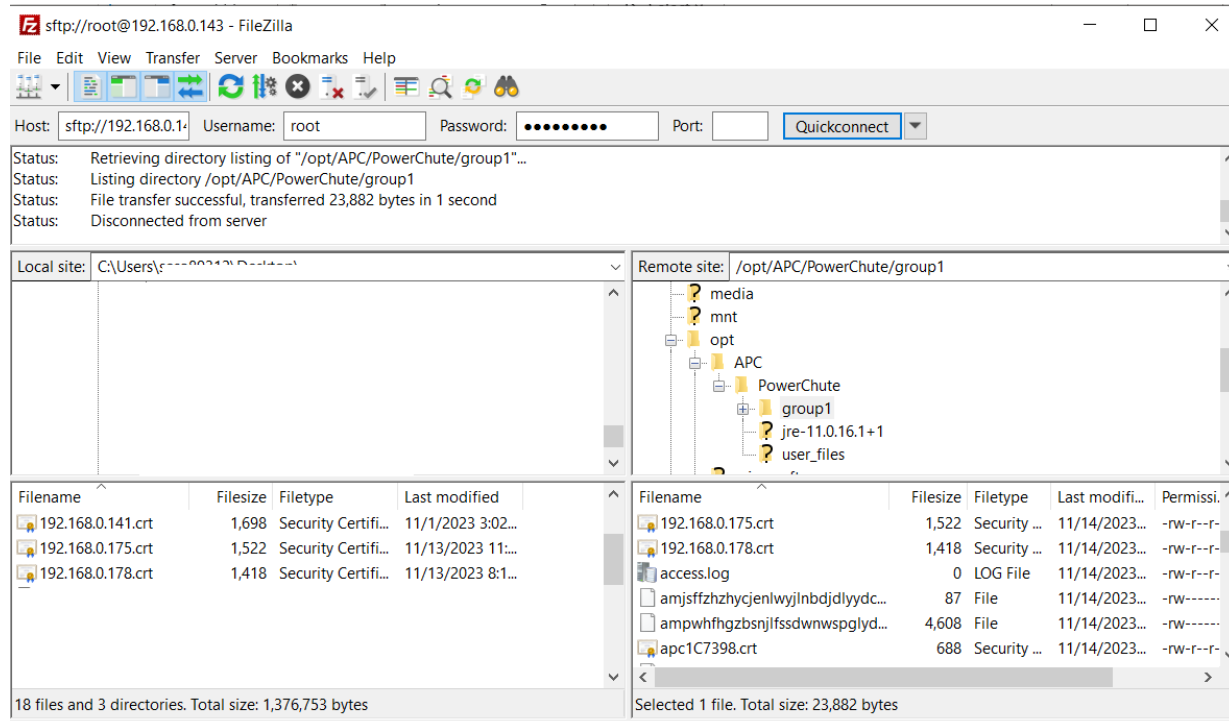
In the next window, click on the certificate icon.



In the next window, select Details – Export – enter a file name and save it as a Base64-encoded ASCII certificate chain. The file will be downloaded to the browser's default download folder, or you can choose a new folder.

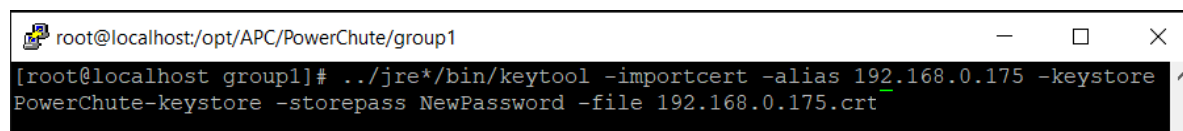


Step 8: Copy the certificate to the PowerChute directory on the VM. In the example below, we used Filezilla to copy the file to the PowerChute VM group1 directory.



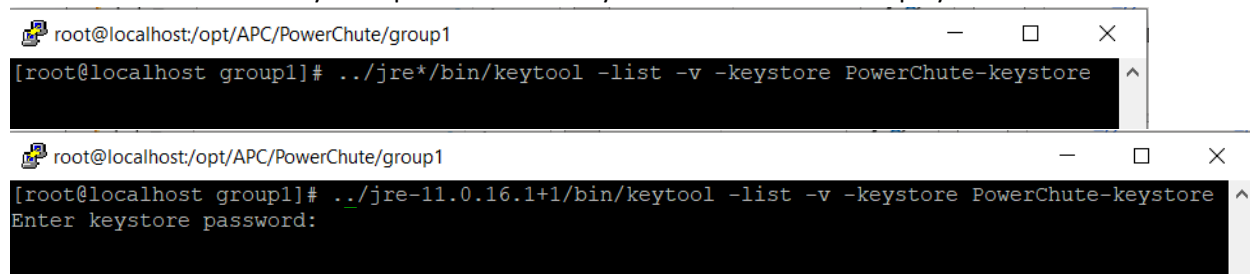
Step 9: Add the ESXi host certificate to the PowerChute-keystore

On the PowerChute VM from the group1 directory, enter **../jre*/bin/keytool -importcert -alias ESXi host IP address or domain name -keystore PowerChute-keystore -storepass <keystore password> -file <certificate file name.crt**



Step 10: Verify the certificate was added to the PowerChute-keystore

Enter the command **../jre*/bin/keytool -list -v -keystore PowerChute-keystore**. You will be asked to enter the PowerChute-keystore password. The keystore data should be displayed on the screen.



Step 11: Restart the PowerChute service.

The command is **systemctl start PowerChute**. The certificate is now available for use.