

How to add VMware vCenter Server 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** (capital letters matter with Linux commands)

```
 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 line

PowerChuteKeystorePassword = <New password> New password can be replaced with a password of your choice. It must be at least 6 characters.

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

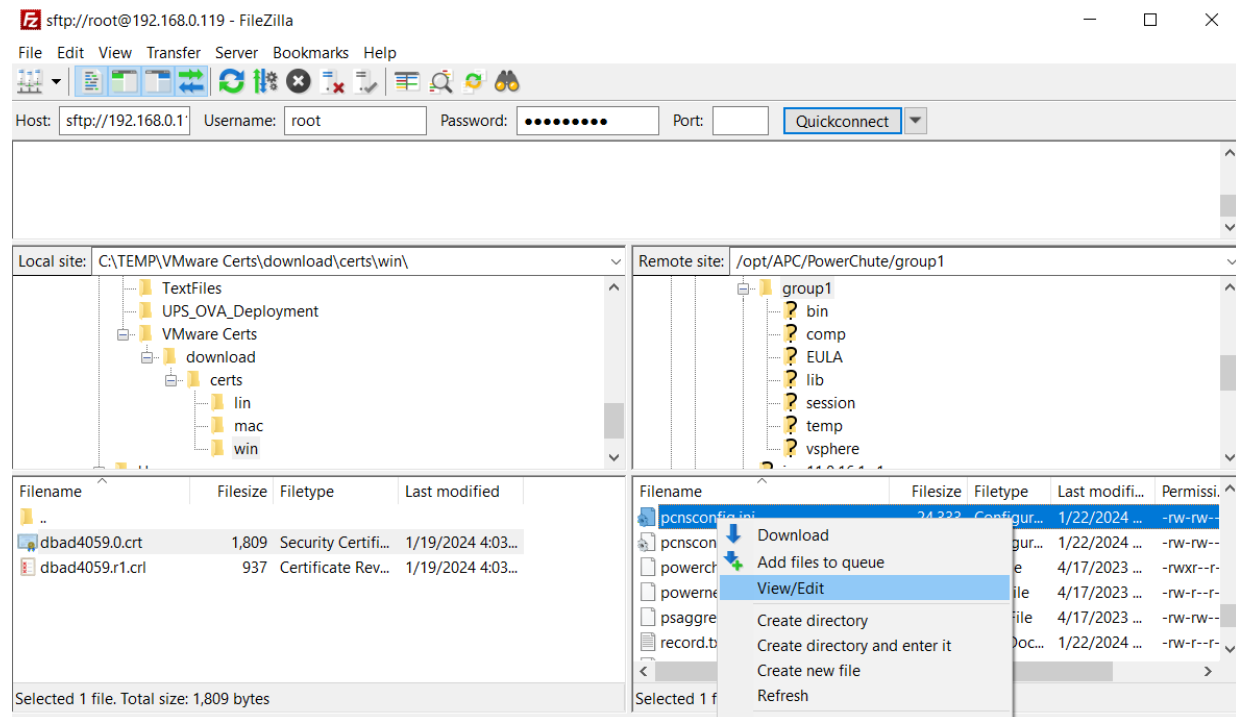
```
[NetworkManagementCard]
mode = single
IP_1 = 192.168.0.128
port = 443
protocol = https
enrolWithNMC = true
IP_1_Outlet = 1
PowerChuteKeystorePassword = NewPassword
```

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

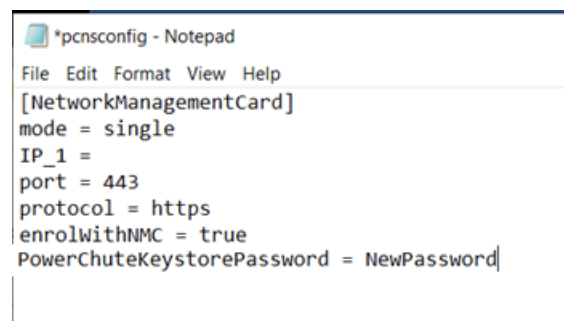
Note: SSH must be enabled on the PowerChute VM to allow the connection.

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

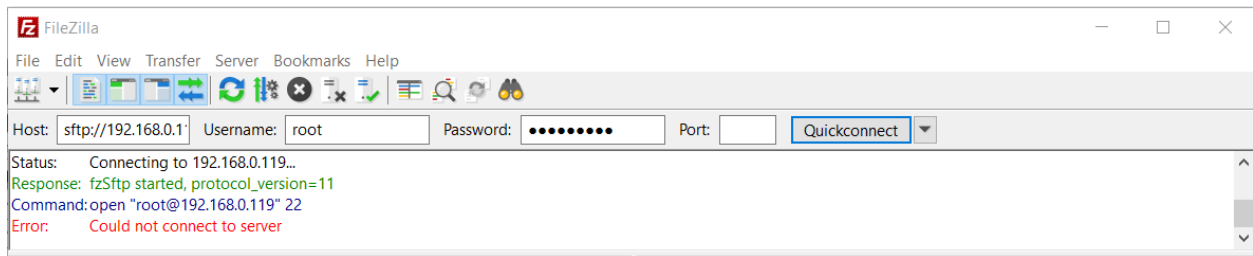
Right-click on pcnsconfig.ini and select View/Edit.



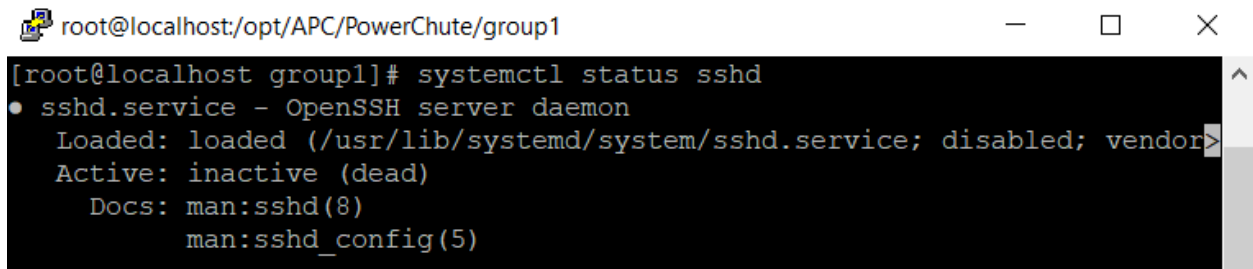
Example of an edited file in Notepad



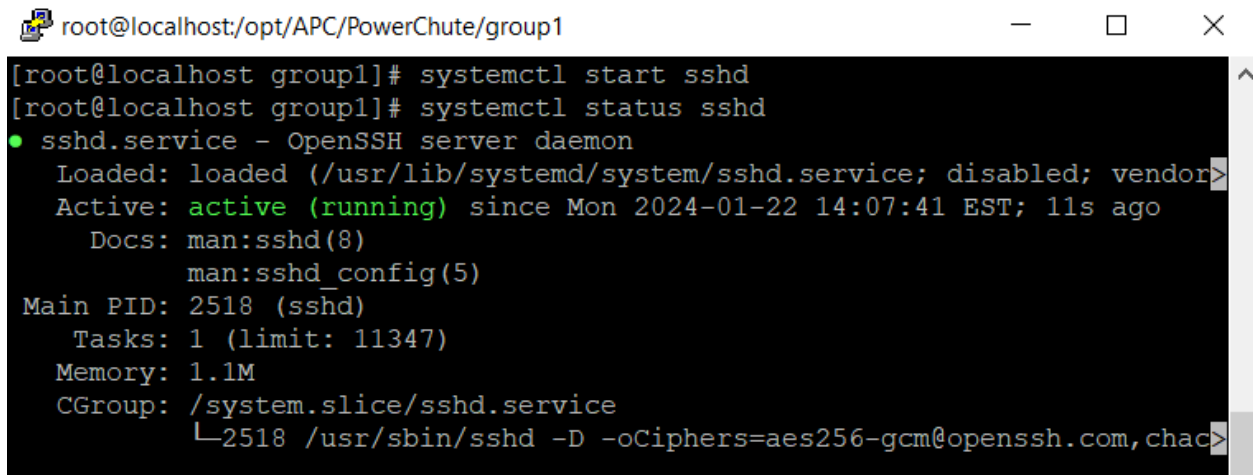
If the connection fails, verify SSH has been enabled on the PowerChute VM.



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.

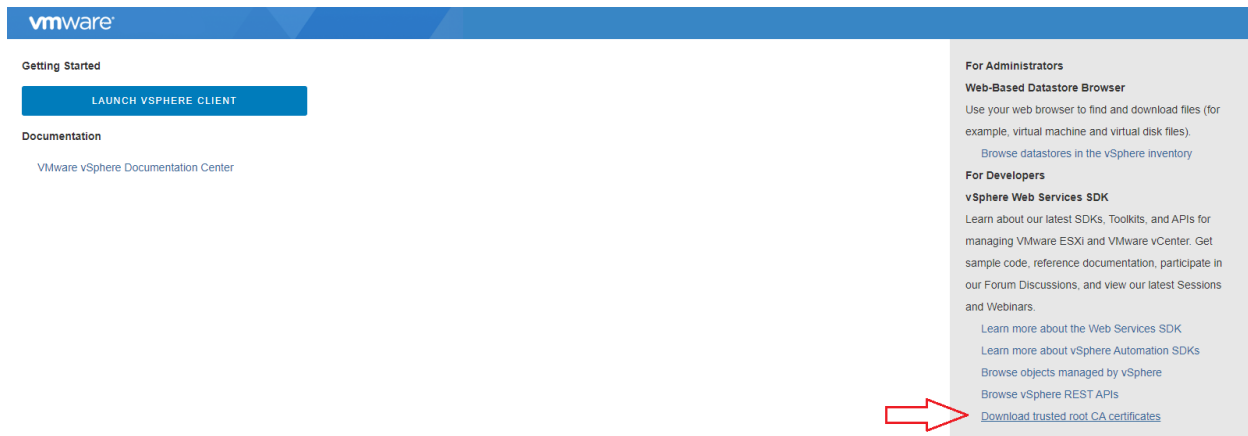
```
root@localhost:/opt/APC/PowerChute/group1
[root@localhost group1]# ../jre*/bin/keytool -list -v -keystore PowerChute-keystore
```

Step 6: After verifying the keystore password was changed, stop the PowerChute service.
The command is **systemctl stop PowerChute**.

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

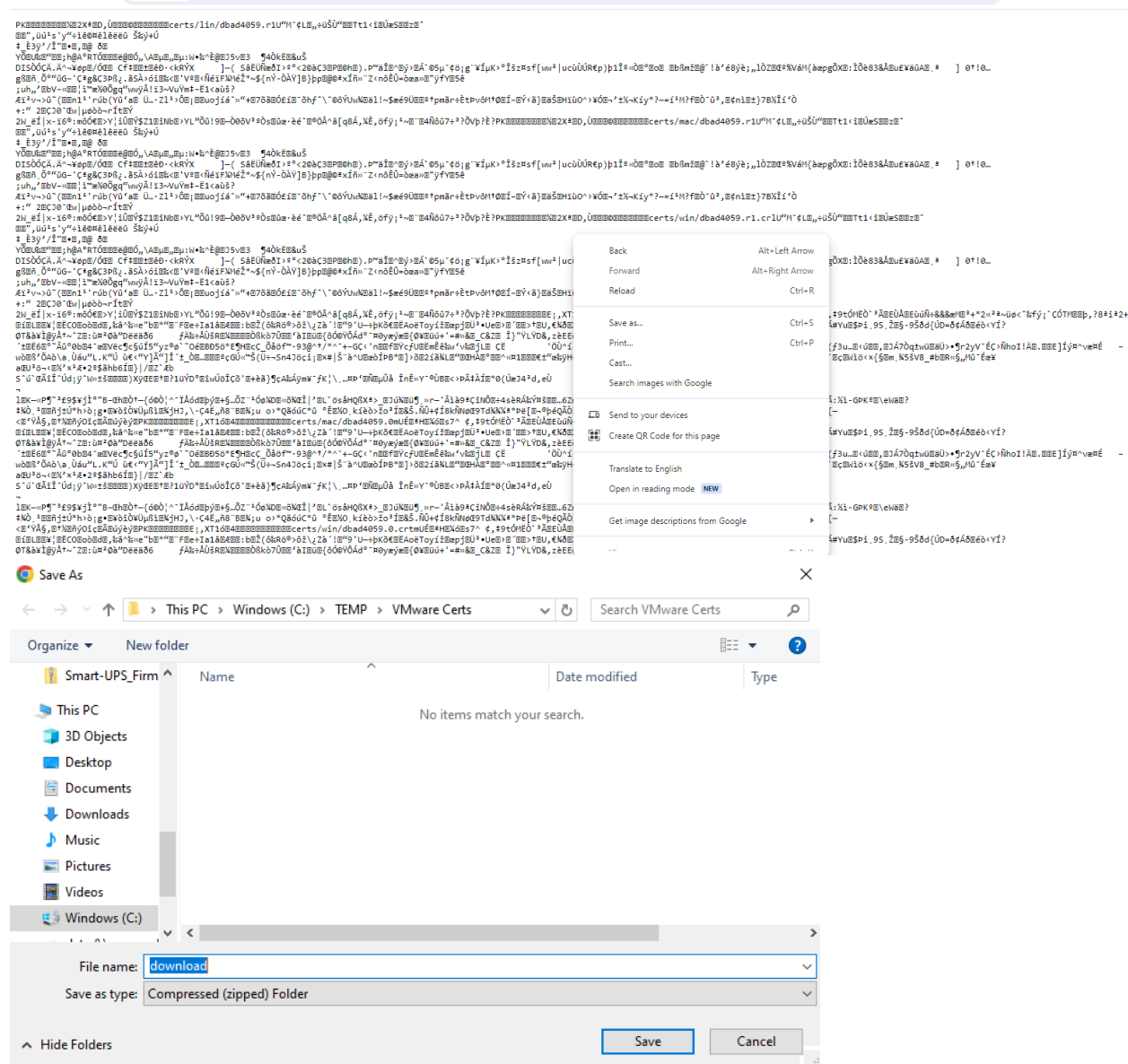
To do so, open a web browser. In the example below, we used Chrome. Navigate to the vCenter web page.

Click on Download trusted root CA certificates.

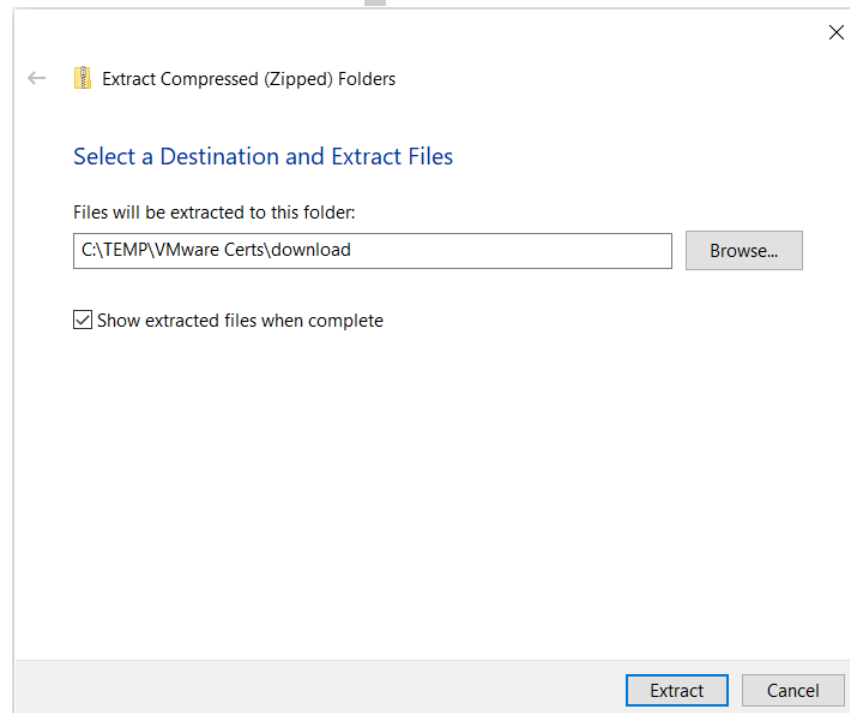
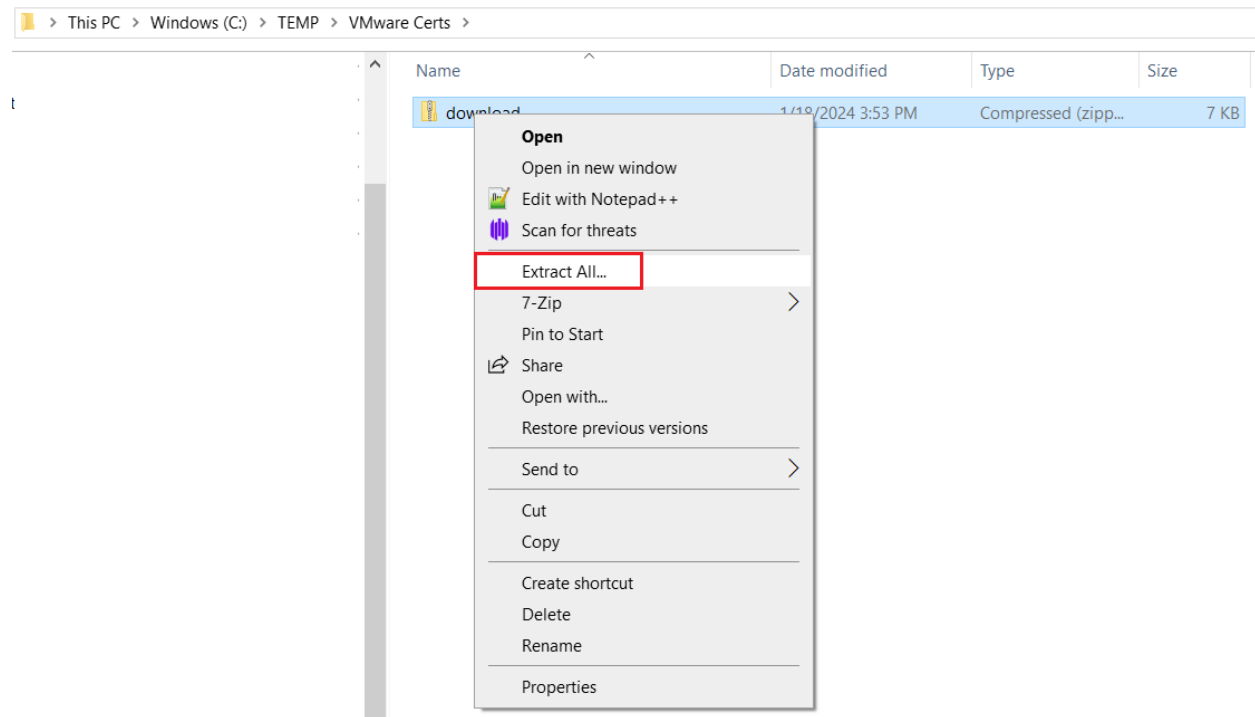


A .zip file named download.zip will be downloaded to the browser's default download folder.

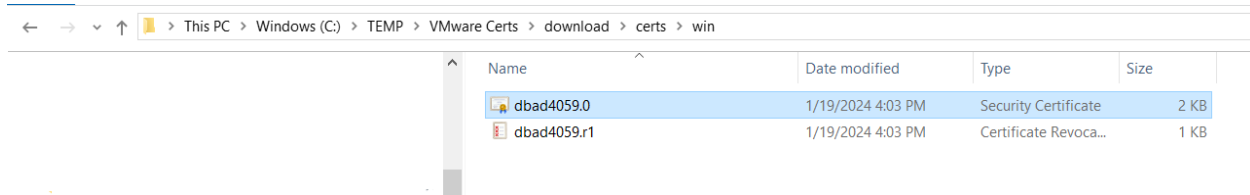
← → ↻ 🏠 🔴 Not secure https://192.168.0.176/certs/download.zip ☆ 📄 ⬇ 📱 🟢



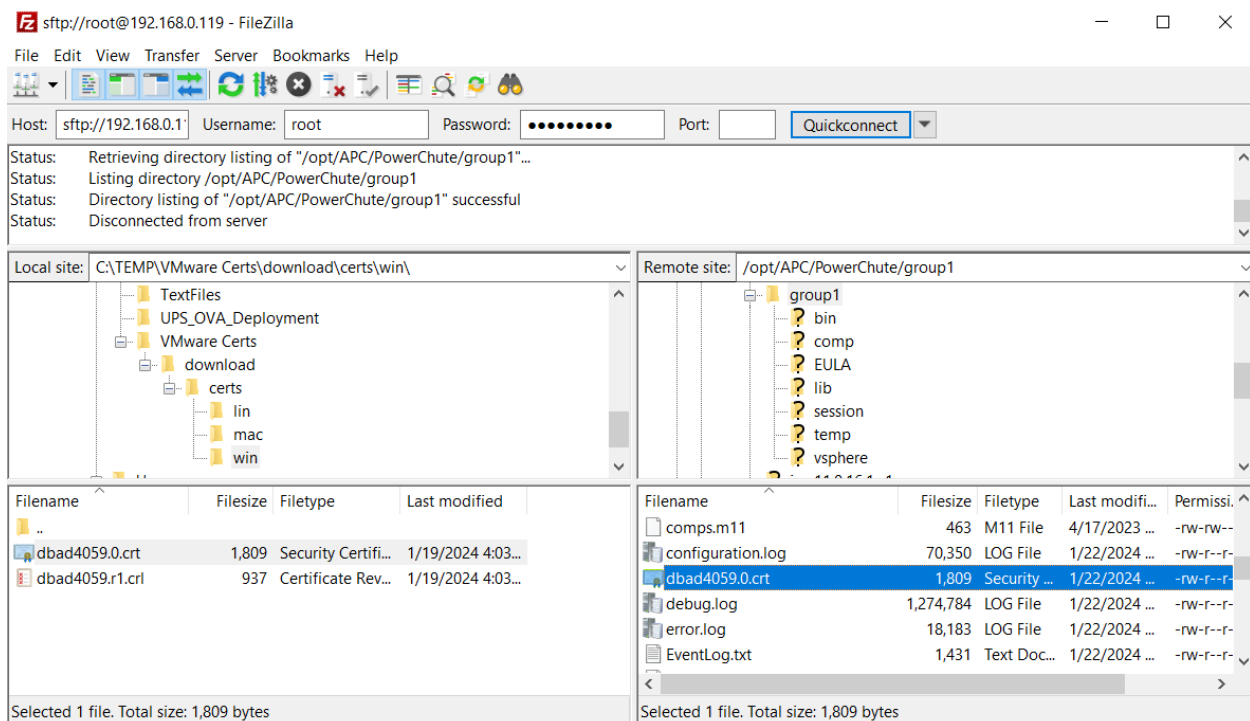
After downloading the file, navigate to the folder the file was saved to, right-click on the folder, and uncompress the folder.



Next, open the uncompressed folder and navigate to the win folder. You will see a security certificate that ends with a zero.



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

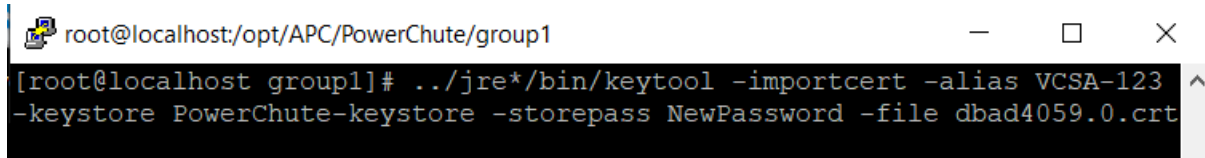


In the example above, the file was copied to /opt/APC/PowerChute/group1.

Step 9: Add the certificate to the PowerChute-keystore

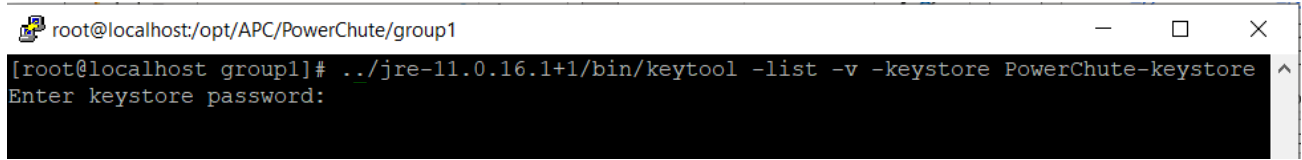
On the PowerChute VM, **cd** to **/opt/APC/PowerChute/group1** and enter the command

../jre*/bin/keytool -importcert -alias <vCenter 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.

A terminal window with a title bar showing 'root@localhost:/opt/APC/PowerChute/group1'. The terminal content shows the command `[root@localhost group1]# ../jre-11.0.16.1+1/bin/keytool -list -v -keystore PowerChute-keystore` being entered, followed by the prompt 'Enter keystore password:'.

```
root@localhost:/opt/APC/PowerChute/group1
[root@localhost group1]# ../jre-11.0.16.1+1/bin/keytool -list -v -keystore PowerChute-keystore
Enter keystore password:
```

Step 11: Restart the PowerChute service.

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