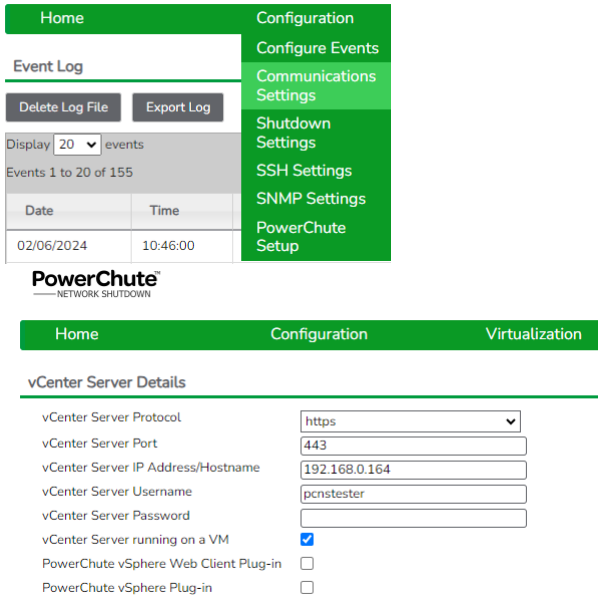
1 Verify that the vCenter server credentials entered are correct. See Schneider Electric FAQ FA413365 for assistance creating a user PowerChute will use to connect to vCenter server and the ESXi hosts.

When creating the PowerChute user, be sure to provide the correct permissions. We recommend the user have administrator rights, and the user has been added to the Administrator Groups. See Schneider Electric FAQ FA177822 for a list of the minimum required permissions.

2 Verify that the PowerChute system can connect to the vCenter server over the network.

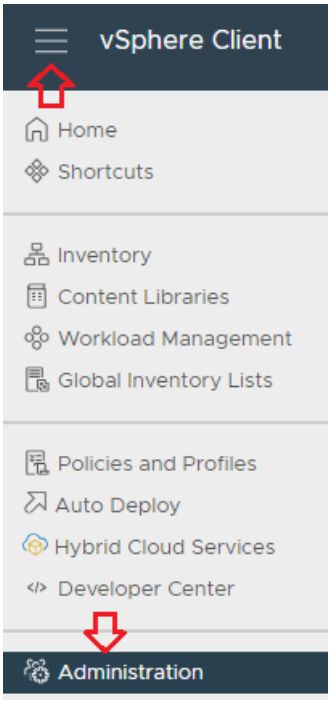
- Verify that the vCenter Server protocol and port are set correctly. The default port and protocol are HTTPS and port 443.
  - From the PowerChute web UI, go to Configuration > Communication Settings and verify the vCenter server detail.
  - 

Next: Log into the system PowerChute is running on and ping vCenter.

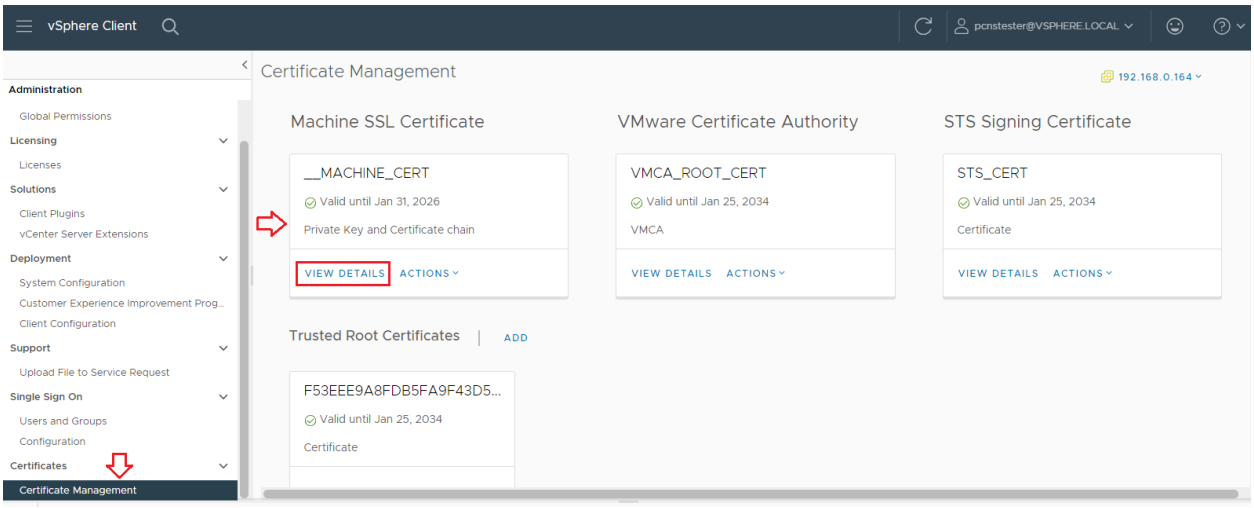
- When running the ping test, enter the vCenter IP address and the vCenter domain name.
  - Example: with IP address ping 192.168.0.164
  - Example: with domain name ping VCSA164.local
- If vCenter cannot be pinged with the IP address, check the network connection between the systems. If vCenter cannot be pinged with the domain name, verify that the PowerChute system can connect to the domain name server, and add the vCenter server IP address and domain name to etc/hosts. See Schneider Electric FAQ000262541 for assistance editing the hosts file.

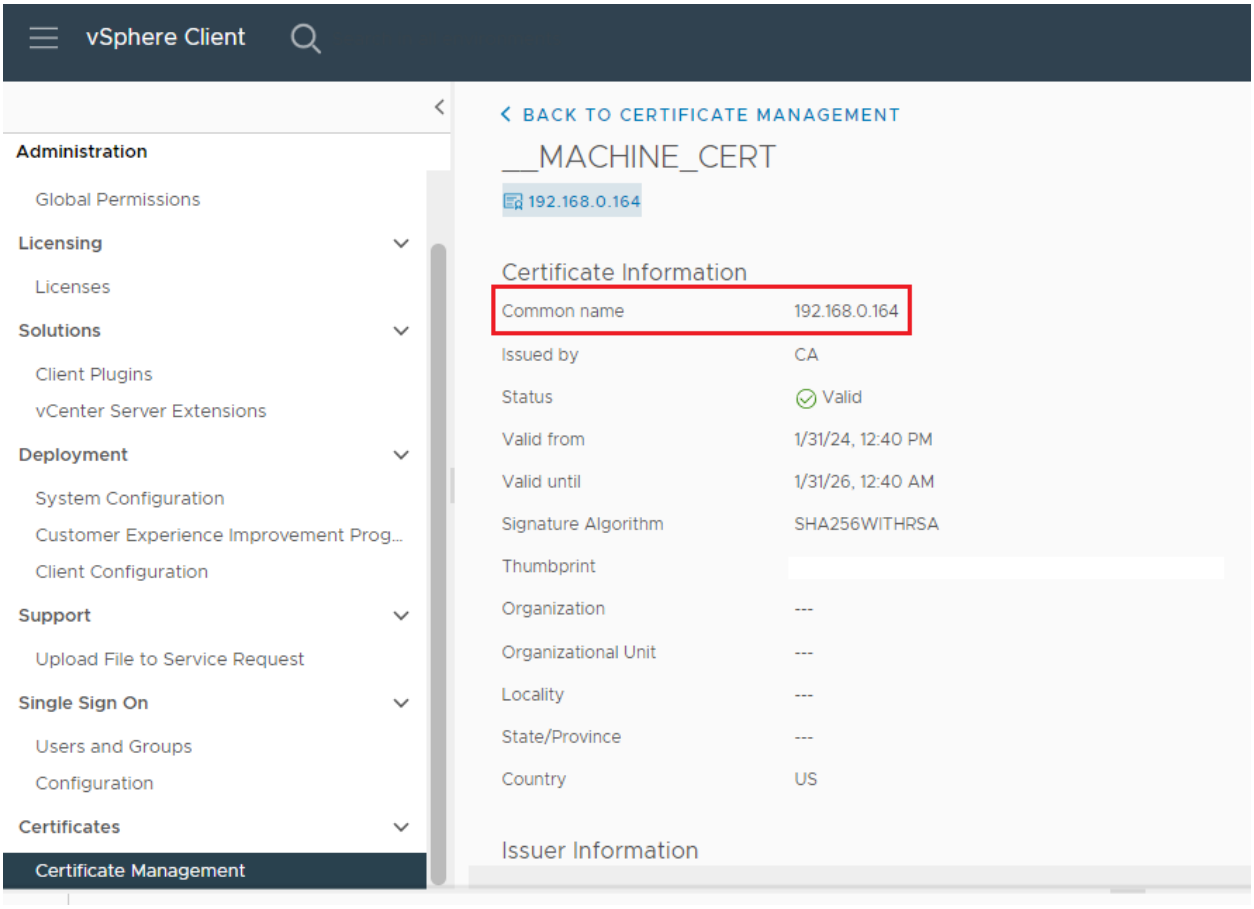
3 Verify that the SSL certificate presented by vCenter has been accepted by PowerChute and that the CN (Common Name) matches what has been entered for the vCenter server IP address/Hostname.

To verify the SSL certificate, open a web browser, navigate to the vCenter server web page, and log into vCenter server. Go to the main menu and select Administration.



From Administration, go to Certificate Management and view the Machine Cert by clicking on View Details.





Take note of the common name.

Next, log into the PowerChute system and navigate to the PowerChute group1 folder directory. On a Windows system, the default path is C:\Program Files\APC\PowerChute\group1. On the PowerChute VM, the path is /opt/APC/PowerChute/group1.

Stop the PowerChute service.

Open a command prompt as an administrator on Windows and enter **net stop pcns1**.
On the PowerChute VM, enter the command **systemctl stop PowerChute**.

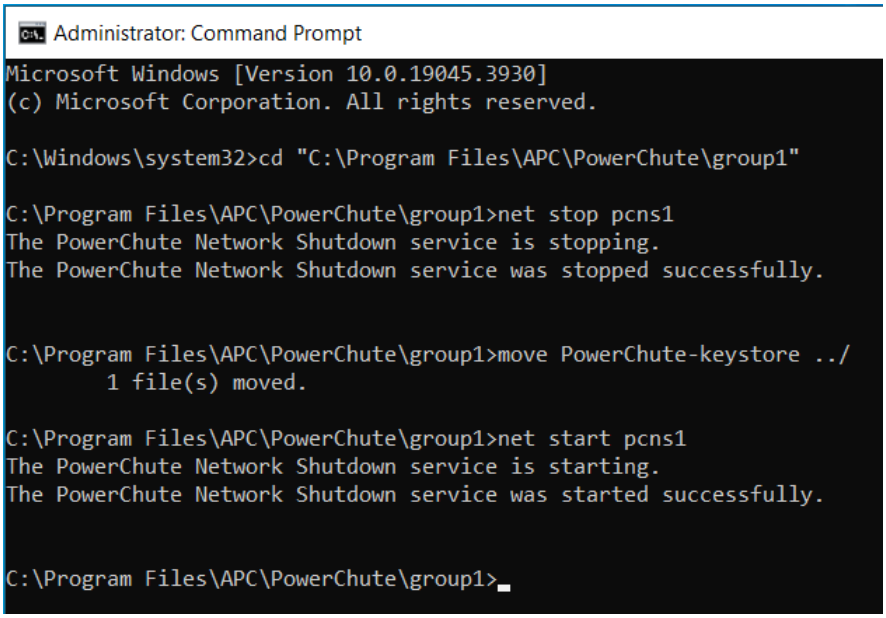
Next, copy the PowerChute-keystore file to the PowerChute folder.

On Windows, from a command prompt as an administrator, enter the command **move PowerChute-keystore ../** to move the file to C:\Program Files\APC\PowerChute\
On the PowerChute VM, enter **mv PowerChute-keystore ../**to move to /opt/APC/PowerChute.

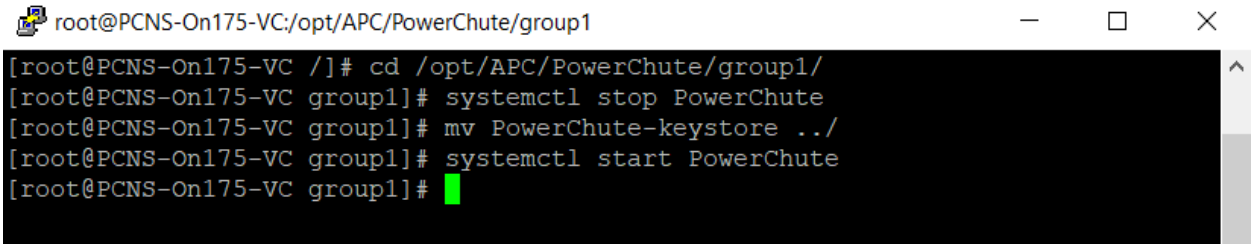
Next, restart the PowerChute service.

On Windows, enter the command **net start pcns1**.
On the PowerChute VM, enter the command **systemctl start PowerChute**.

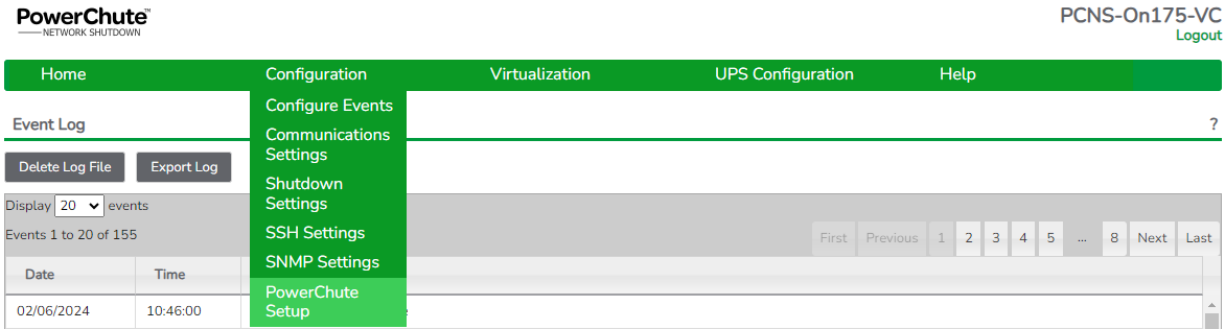
From Windows OS.



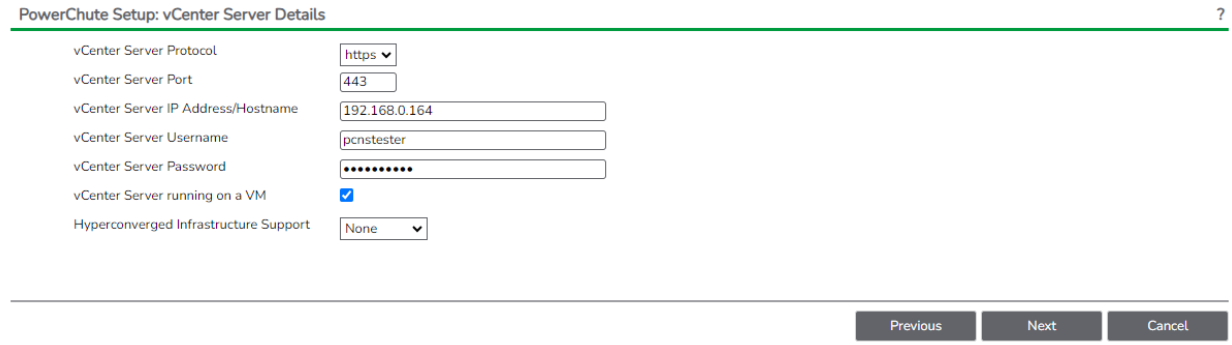
From PowerChute VM



Wait two minutes, log into the PowerChute web UI, and run the PowerChute setup to accept the vCenter server SSL certificate.



On the vCenter server details page, enter the vCenter information and click next to accept the SSL certificate.



When accepting the certificate, verify that the CN = what has been entered for the vCenter server details and click accept. After accepting the certificate correct the entry on the vCenter server details page if they do not match.