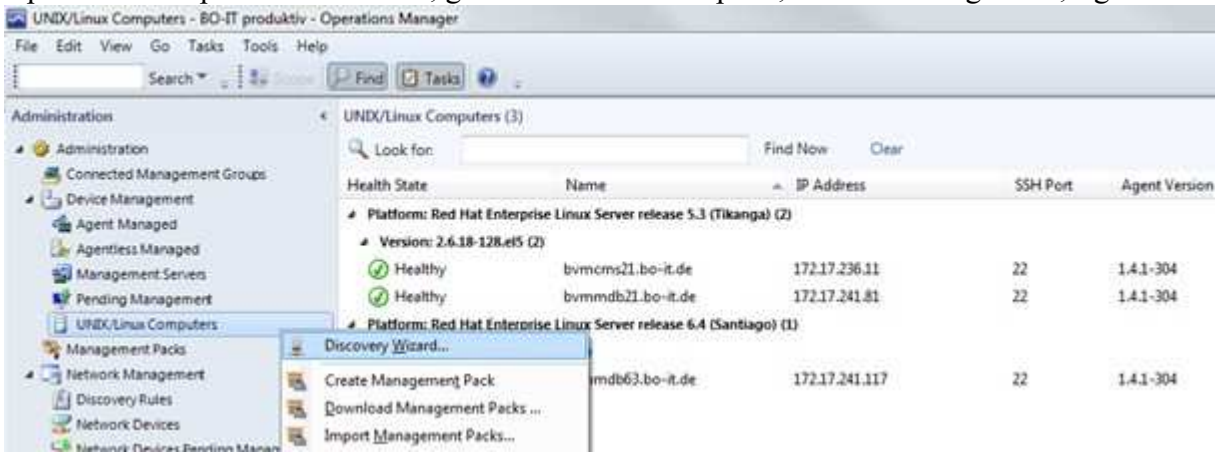
How to monitor RedHat Enterprise Linux 5 or 6 using Microsoft System Center Operations Manager (SCOM) 2012 SP1 - Part 2

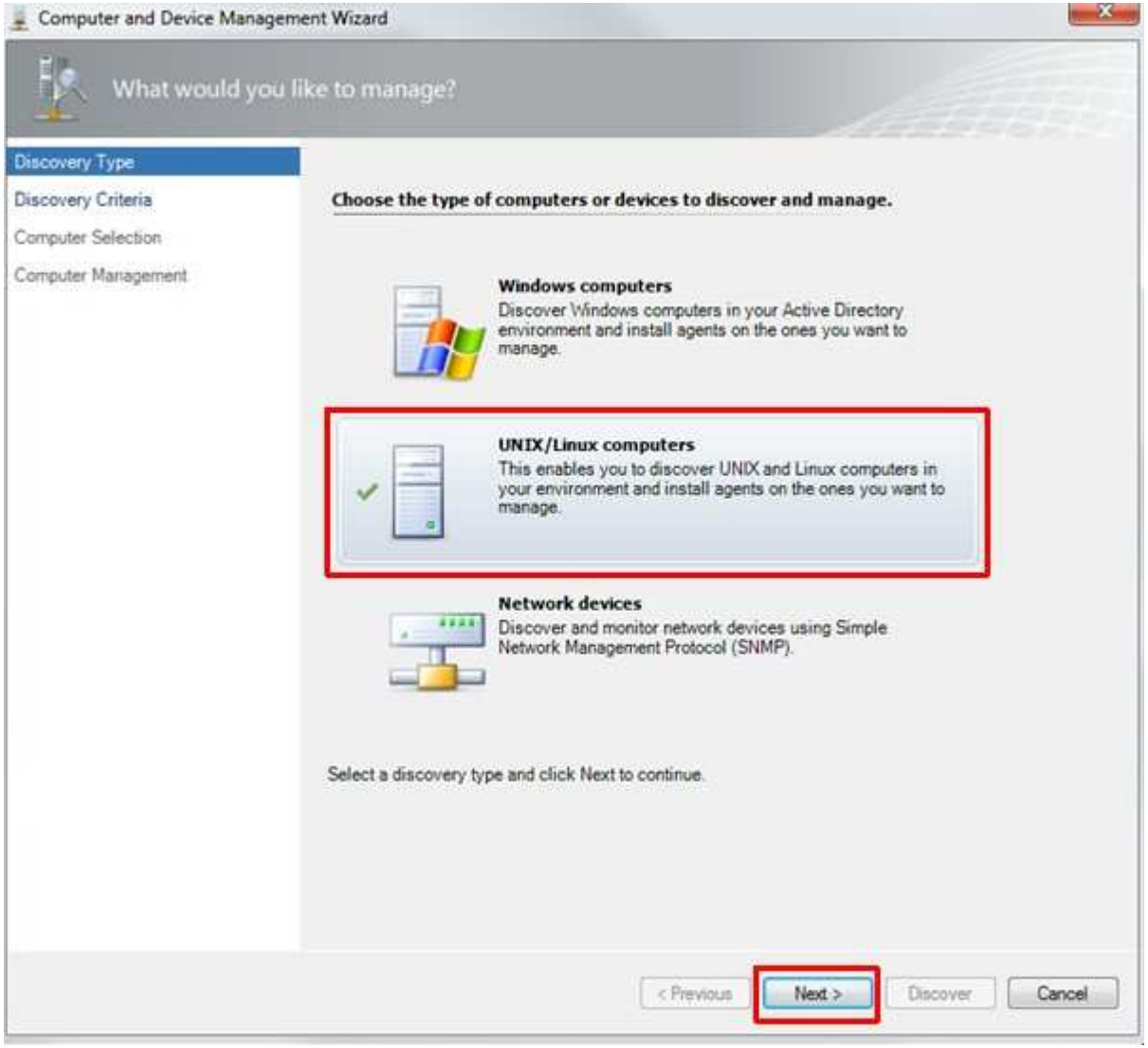
Installation of the SCOM agents on RHEL

In part 1 there is a description how to modify SCOM and RHEL to get ready for the agent installation. If this wasn't properly done you will get into trouble. Believe me! In this part 2 I will describe the agent installation and how to check if the setup was well done.

1. Open SCOM Operations Console, go to Administration pane, Device Management, right click on UNIX/Linux Computers, select Discovery Wizard

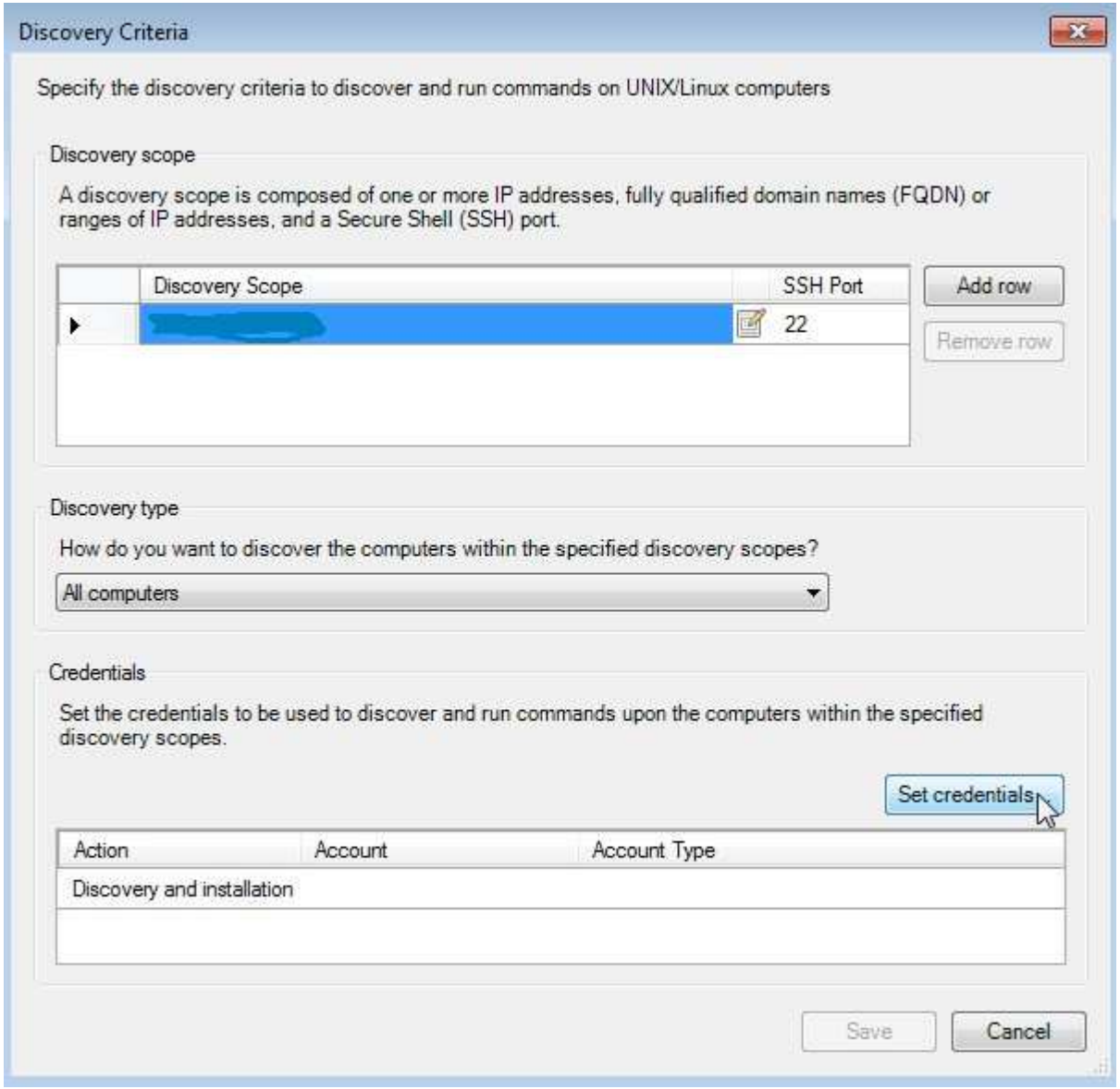


2. Select UNIX/Linux computers, click Next



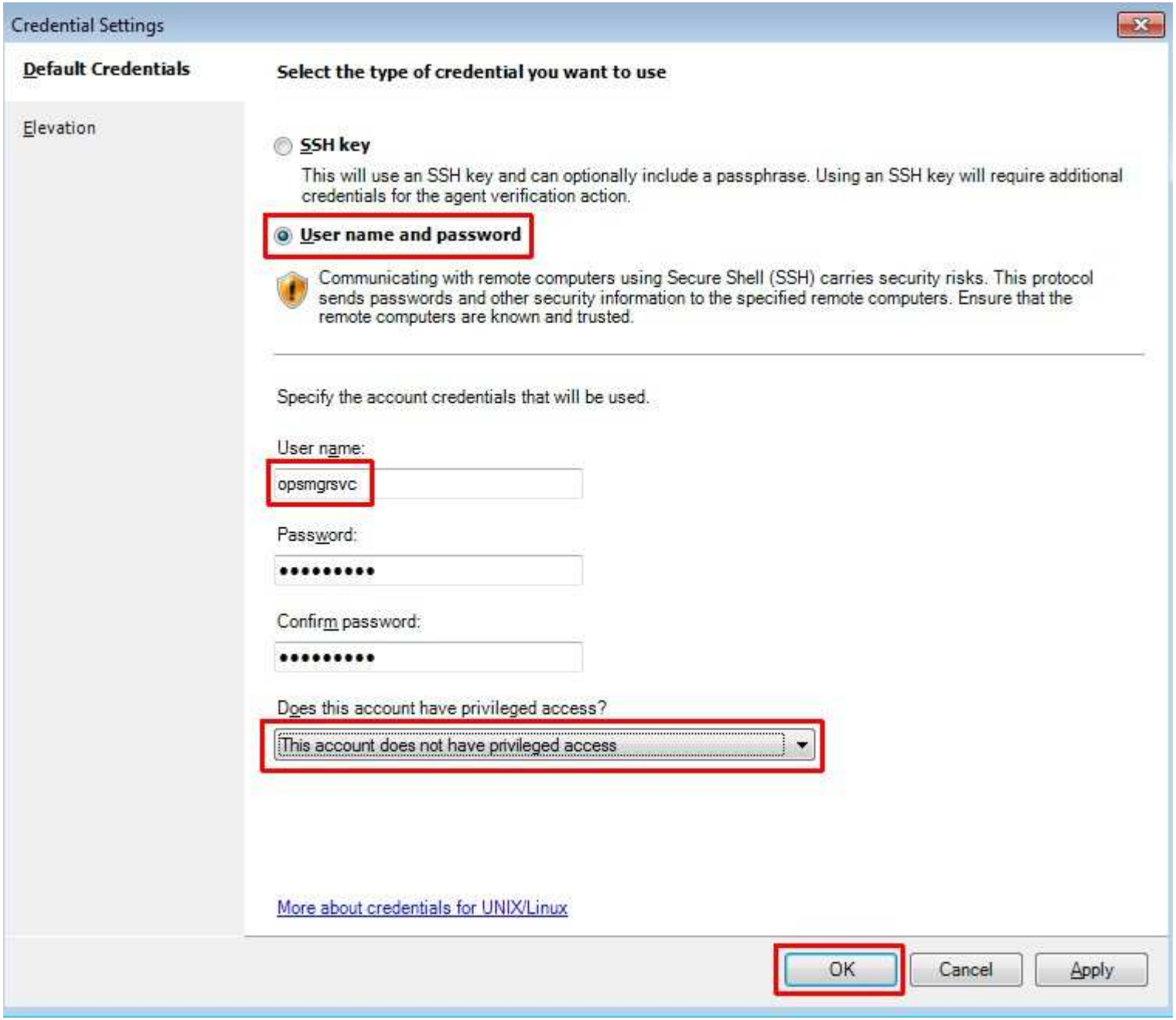
3. Click Add in the Define the criteria for discovering... window

4. Insert the FQDN or IP address of the Server which should be monitored:



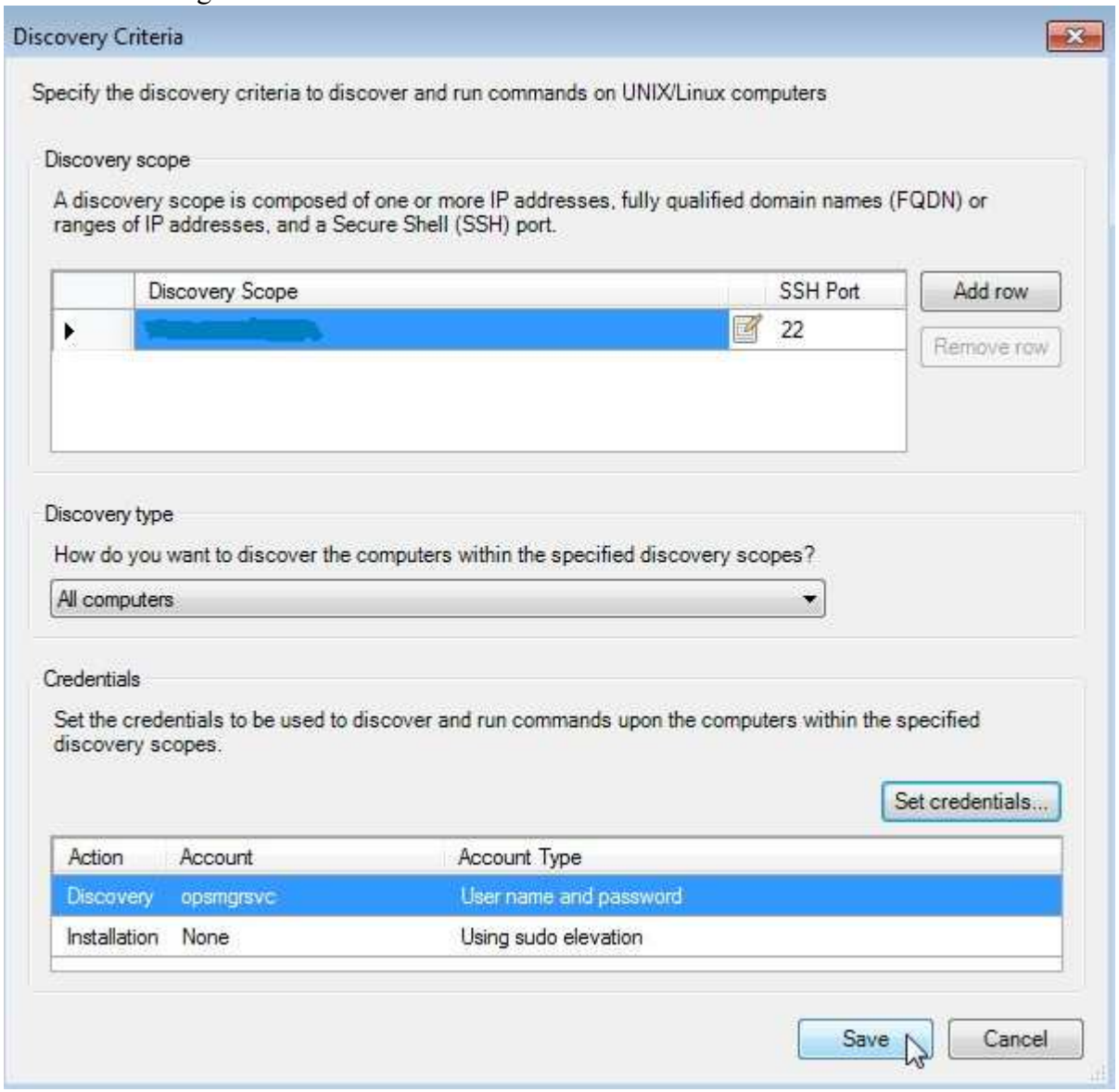
Hint: Hit the return key to add the FQDN. Don't forget to click Set credentials!

5. Set the type of credentials in the following window as shown:



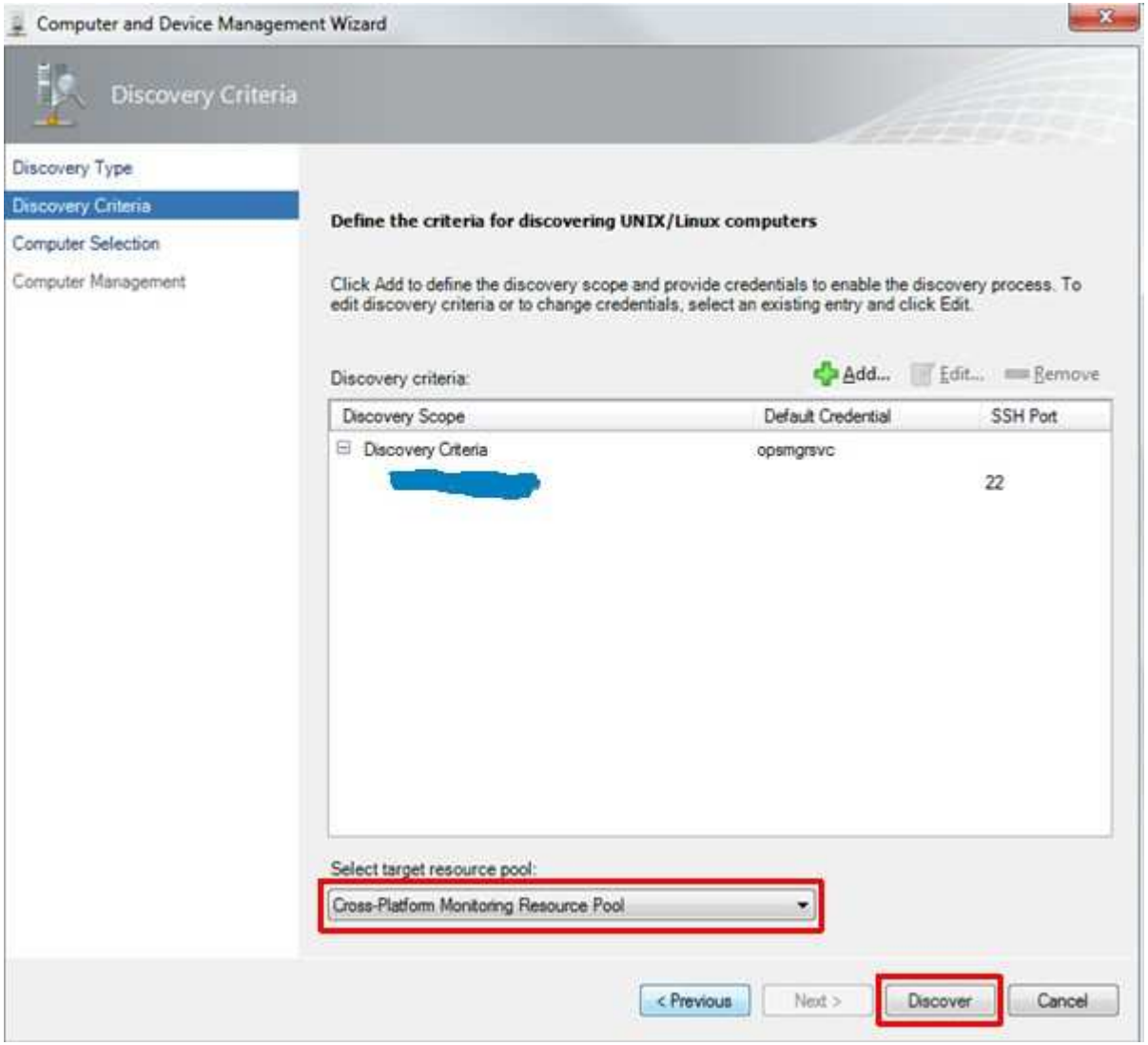
Remember: In part 1 I have described the Linux setup of the user "**opsmgrsvc**"

6. Check the settings:



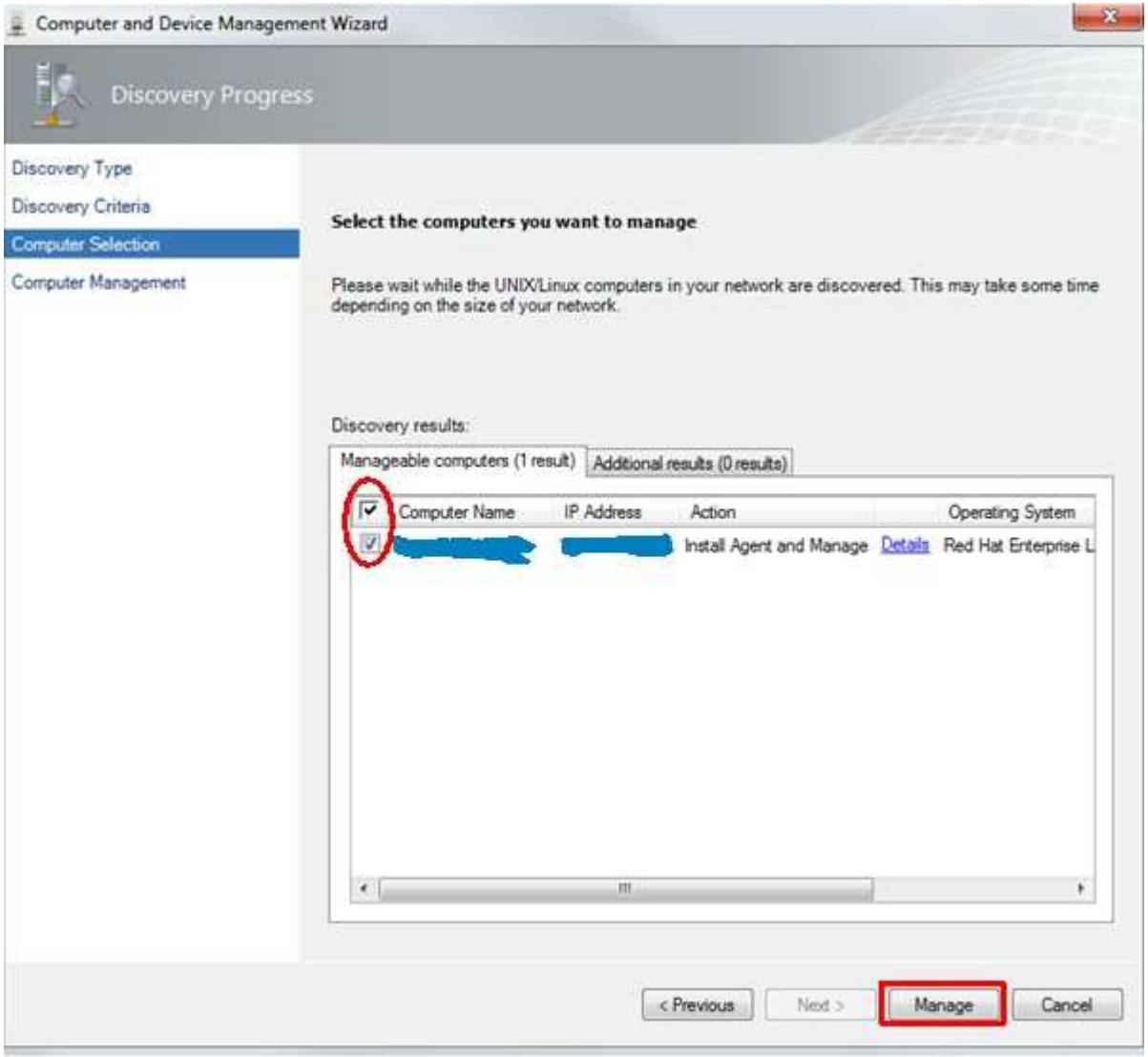
Don't forget to click Save!

7. Selection of the target resource pool:



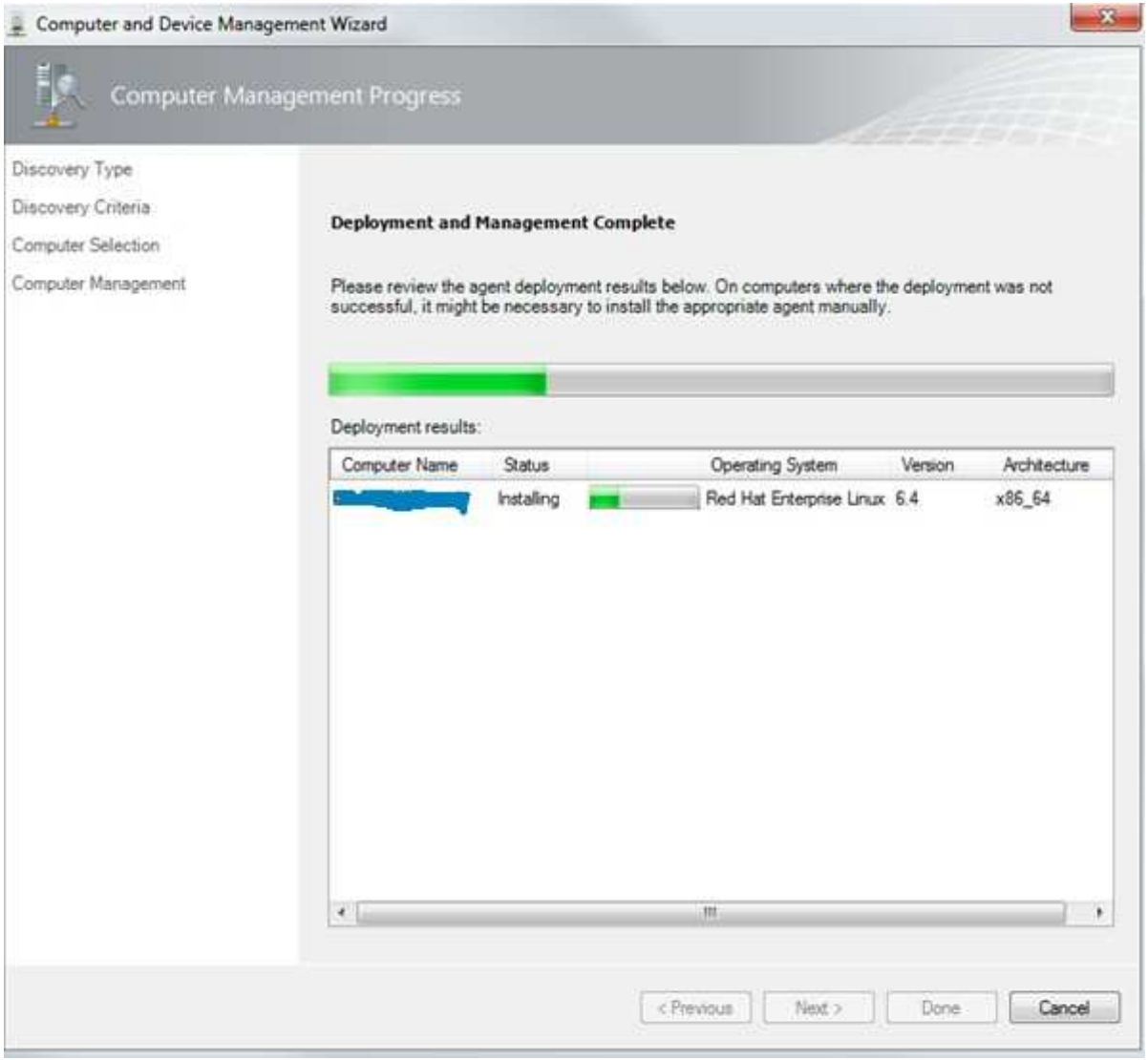
Remember: In part 1 we have defined the resource pool. Click on Discover!

8. Selection of the computers to manage:

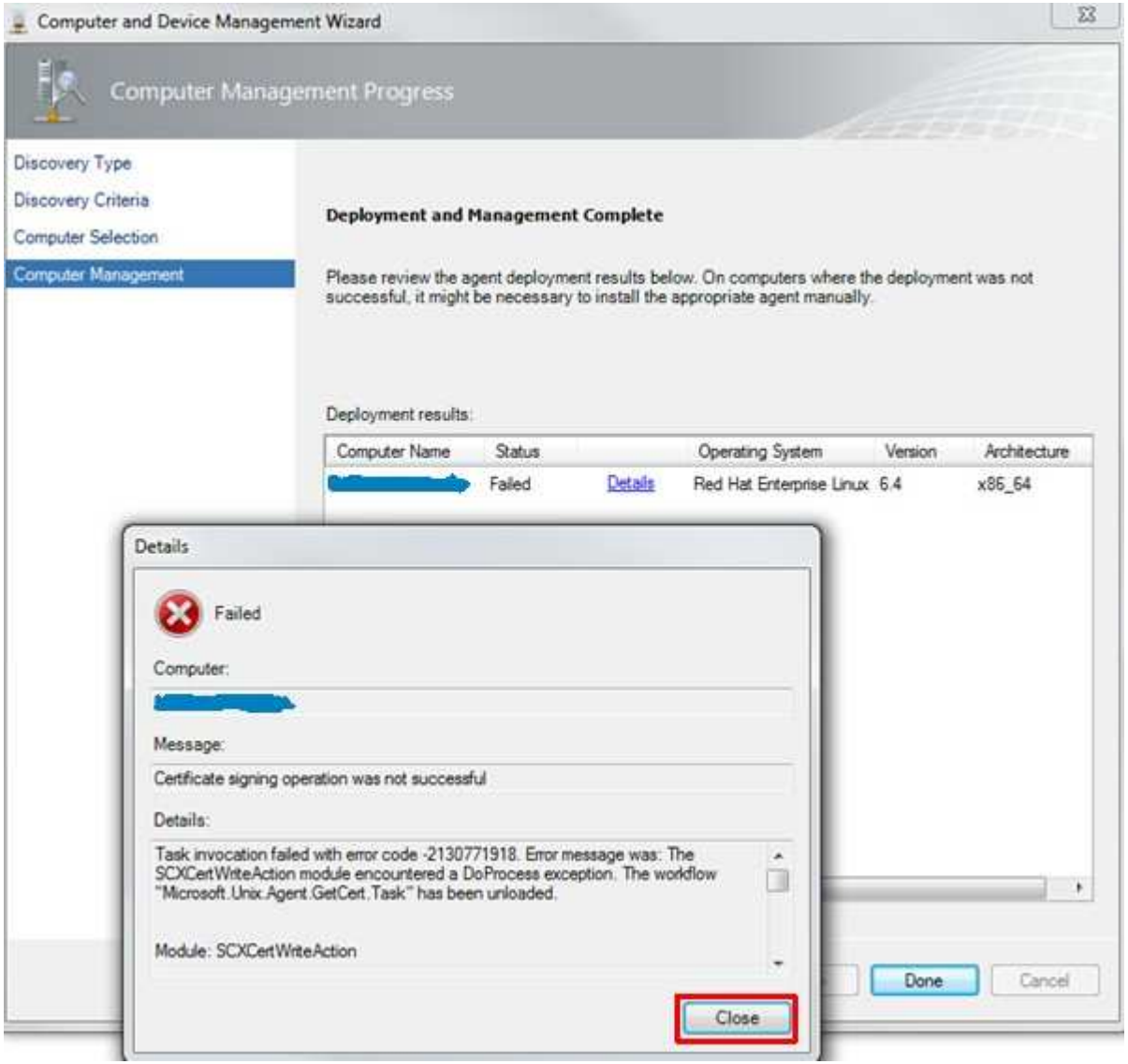


Select the appropriate checkbox and click on Manage!

9. Agent deployment starts:



10. Agent deployment throws an error:



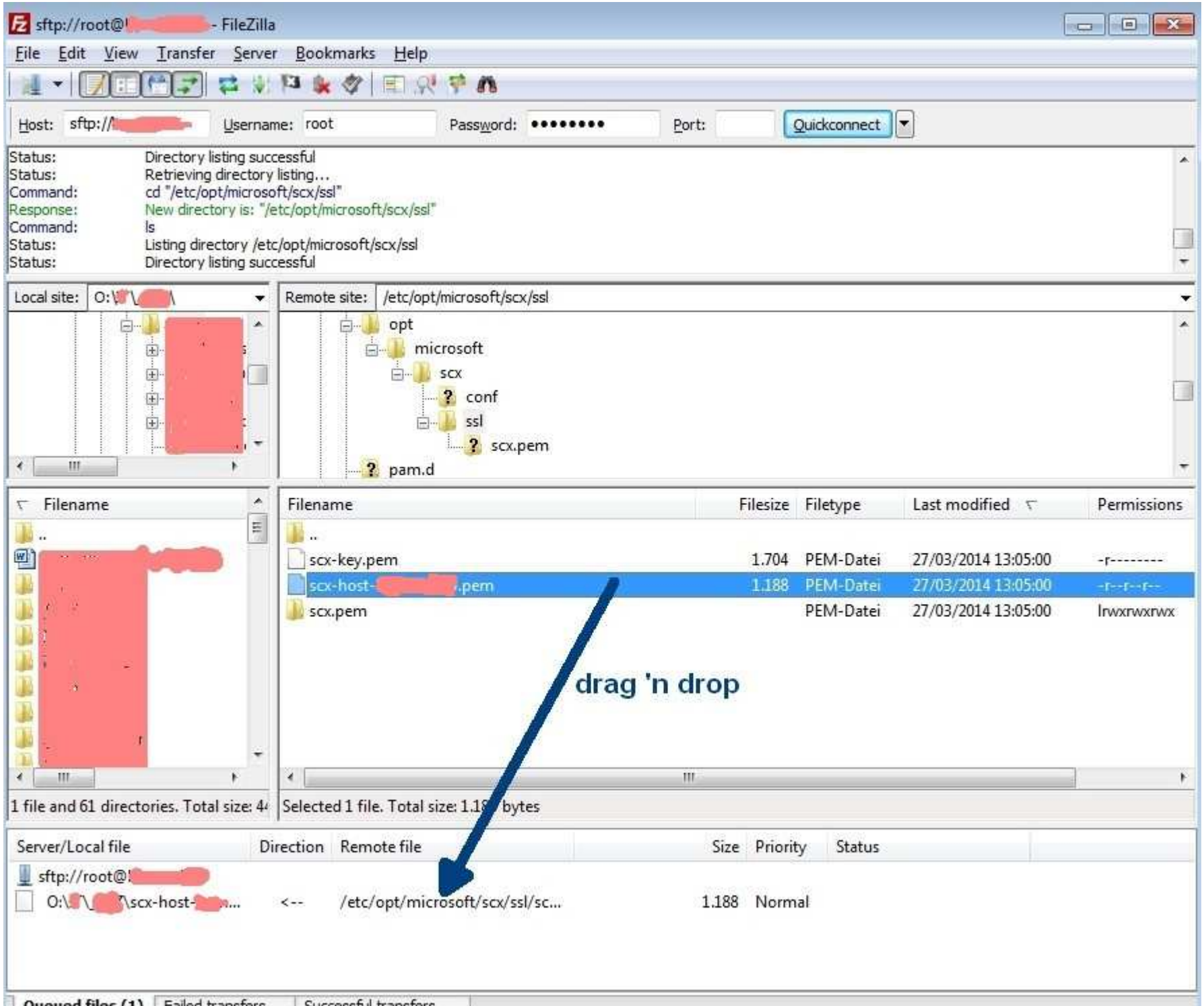
Oops! This wasn't expected. We have a look at the Linux server now. Do you remember that I told you to have a Linux admin by your side? Read the error message carefully and then click on Close!

11. If you try to login via ssh, sftp or scp to a Linux system all these accesses are logged to /var/log/secure. This text file is the first address to look for connection problems. So, let's have a look to this. I'm using the tail command for this purpose:

```
[root@<hostname> ~]# tail -f /var/log/secure
Mar 27 15:09:55 <hostname> sshd[56686]: Accepted password for opsmgrsvc from <SCOM-IP> port 57389 ssh2
Mar 27 15:09:55 <hostname> sshd[56686]: pam_unix(sshd:session): session opened for user opsmgrsvc by (uid=0)
Mar 27 15:09:55 <hostname> sshd[56686]: pam_unix(sshd:session): session closed for user opsmgrsvc
Mar 27 15:09:56 <hostname> sshd[56704]: Accepted password for opsmgrsvc from <SCOM-IP> port 57390 ssh2
Mar 27 15:09:56 <hostname> sshd[56704]: pam_unix(sshd:session): session opened for user opsmgrsvc by (uid=0)
Mar 27 15:09:56 <hostname> sshd[56706]: subsystem request for sftp
Mar 27 15:09:56 <hostname> sshd[56704]: pam_unix(sshd:session): session closed for user opsmgrsvc
```

As we can see there are successful connections via ssh, protocol version 2 and a successful data transfer using sftp. Now we can state that our credentials are OK and valid!

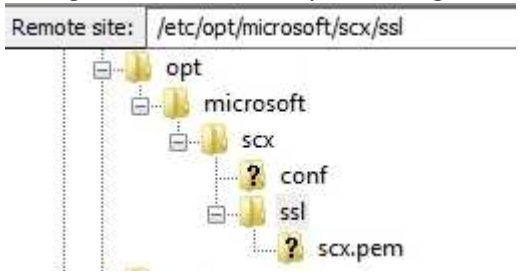
12. Resignature of the Linux host certificate
    After some googling around I found that the problem could be solved by resignature the certificate of the Linux host. In short words: we have to fetch the SCOM Agent certificate, copy it to the SCOM server, resignature it and copy it back to the Linux server. It's really a shame for Microsoft that they are not able to do this process during the agent rollout. As we can see above this is not a matter of rigts/security!
    - We use for the following steps the sftp/scp/ftp client "**FileZilla**" you can get it from https://filezilla-project.org/ for free. The best way is to enable temporarily the root access for ssh to do the copy tasks. Again shame on Microsoft they haven't done their homework!


sftp://root@[redacted] - FileZilla
File Edit View Transfer Server Bookmarks Help
Host: sftp://[redacted] Username: root Password: •••••••• Port: Quickconnect
Status: Directory listing successful
Status: Retrieving directory listing...
Command: cd "/etc/opt/microsoft/scx/ssl"
Response: New directory is: "/etc/opt/microsoft/scx/ssl"
Command: ls
Status: Listing directory /etc/opt/microsoft/scx/ssl
Status: Directory listing successful
Local site: O:\[redacted]
Remote site: /etc/opt/microsoft/scx/ssl
opt
microsoft
scx
conf
ssl
scx.pem
pam.d
Filename
Filesize
Filetype
Last modified
Permissions
scx-key.pem 1.704 PEM-Datei 27/03/2014 13:05:00 -r--------
scx-host-[redacted].pem 1.188 PEM-Datei 27/03/2014 13:05:00 -r--r--r--
scx.pem PEM-Datei 27/03/2014 13:05:00 lrwxrwxrwx
drag 'n drop
1 file and 61 directories. Total size: 4
Selected 1 file. Total size: 1.1 bytes
Server/Local file
Direction
Remote file
Size
Priority
Status
sftp://root@[redacted]
O:\[redacted]\scx-host-[redacted]... <-- /etc/opt/microsoft/scx/ssl/sc... 1.188 Normal

- Enter the connection credentials:

You have to enter the protocol, we use sftp. The hostname of the Linux server. Username and password. You can leave the port empty. Click on Quickconnect.

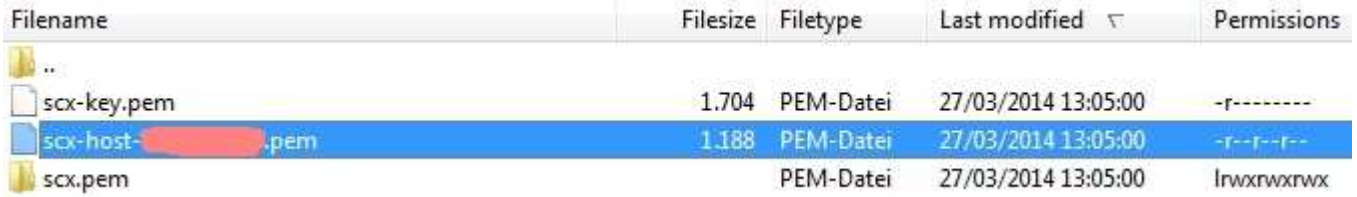
- Navigate to the directory of the agent certificate:



If you like you can go to this directory using a ssh connection:

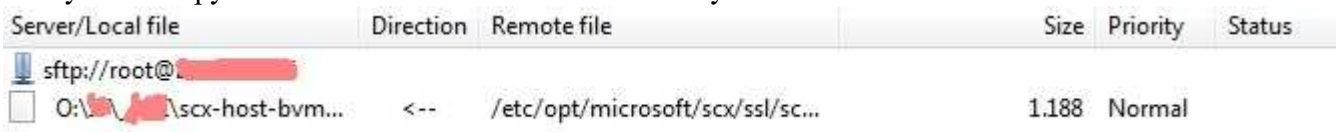
```
[root@<hostname> ~]# cd /etc/opt/microsoft/scx/ssl
```

- Drag 'n drop the agent certificate to the Queued files pane:



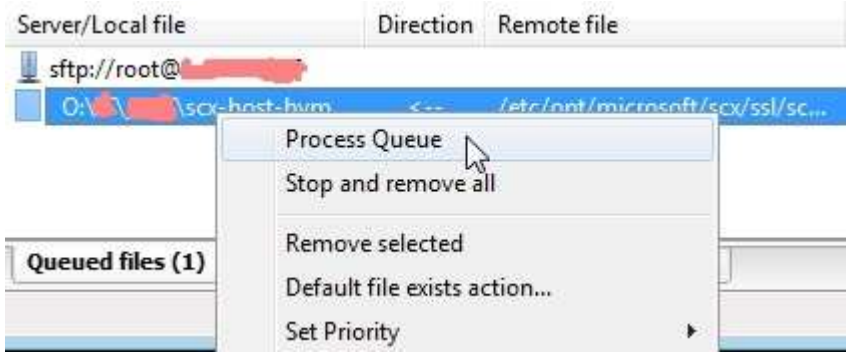
The agent certificate is named after the following scheme: scx-host-<hostname>.pem.

- Verify if the copy direction is from Linux to Windows system:



As you can see the file is copied from the Linux server to a MS Windows System on Drive O:\. The destination drive letter may vary in your environment.

- Initiate the copy process:

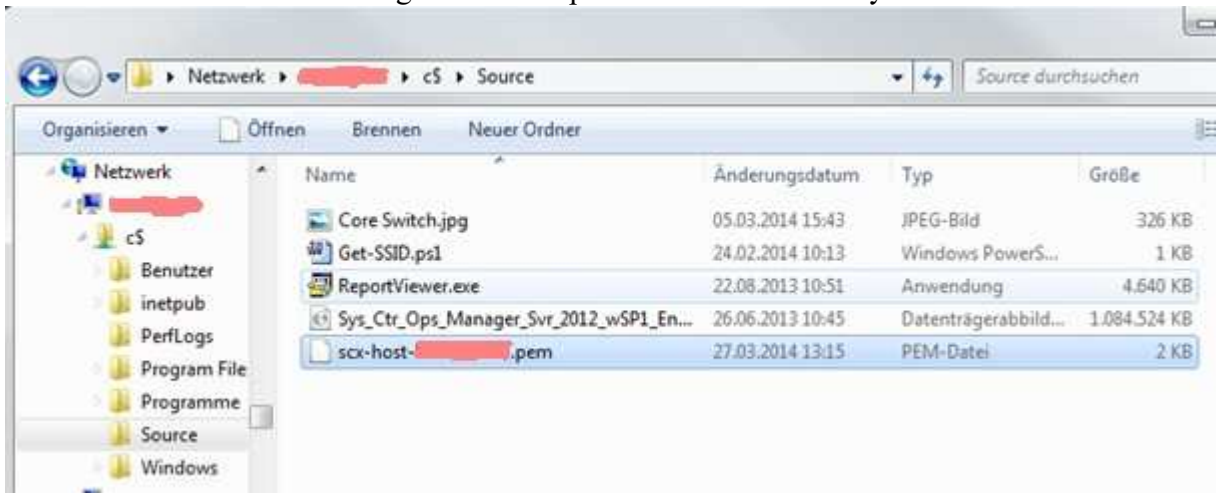


Now right click on the selected file and choose "**Process Queue**" to copy the file.

- Now we make a copy of the original certificate just for the case that something is going wrong:

```
[root@<hostname> ~]# cd /etc/opt/microsoft/scx/ssl
[root@<hostname> ~]# mv scx-host-<hostname>.pem scx-host-<hostname>.pem.orig
```

  - On the SCOM server side navigate to the copied certificate directory:



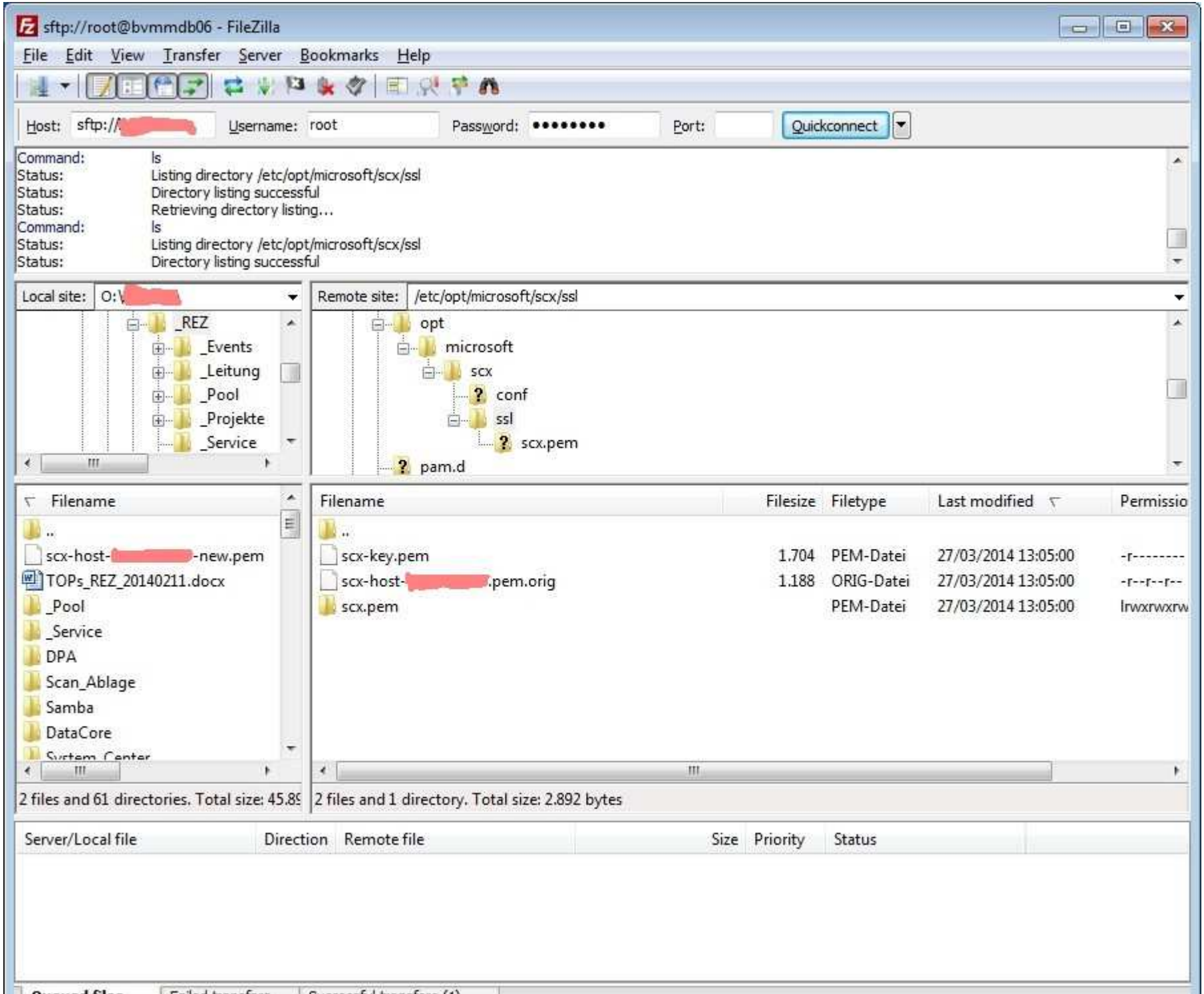
In this case we use the directory C:\Source. Maybe you have a different path.

  - The resignaturing is done using Windows command line:

```
cd "%ProgramFiles%\System Center 2012\Operations Manager\Server"
scxcertconfig.exe -sign c:\Source\scx-host-<hostname>.pem c:\Source\scx-host-<hostname>-new.pem
```

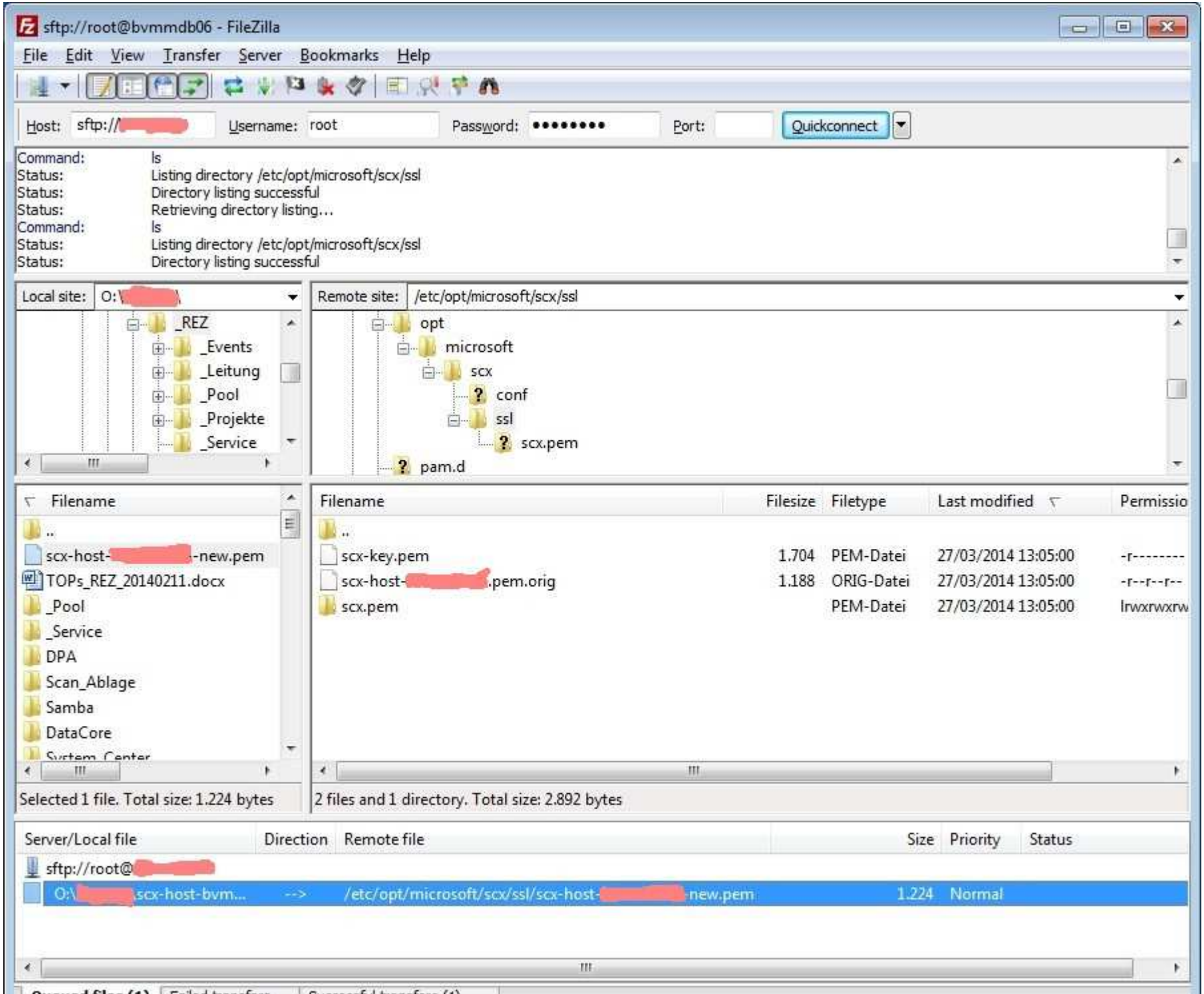
- Now we've done the Windows part!

- Prepare to move the resignatured certificate:


sftp://root@bvmmdb06 - FileZilla
File Edit View Transfer Server Bookmarks Help
Host: sftp:// Username: root Password: •••••••• Port: Quickconnect
Command: ls
Status: Listing directory /etc/opt/microsoft/scx/ssl
Status: Directory listing successful
Status: Retrieving directory listing...
Command: ls
Status: Listing directory /etc/opt/microsoft/scx/ssl
Status: Directory listing successful
Local site: O:\
_REZ
_Events
_Leitung
_Pool
_Projekte
_Service
Remote site: /etc/opt/microsoft/scx/ssl
opt
microsoft
scx
conf
ssl
scx.pem
pam.d
Filename
..
scx-host--new.pem
TOPs_REZ_20140211.docx
_Pool
_Service
DPA
Scan_Ablage
Samba
DataCore
2 files and 61 directories. Total size: 45.8
Filename Filesize Filetype Last modified Permissio
..
scx-key.pem 1.704 PEM-Datei 27/03/2014 13:05:00 -r--------
scx-host-.pem.orig 1.188 ORIG-Datei 27/03/2014 13:05:00 -r--r--r--
scx.pem PEM-Datei 27/03/2014 13:05:00 lrwxrwxrw
2 files and 1 directory. Total size: 2.892 bytes
Server/Local file Direction Remote file Size Priority Status

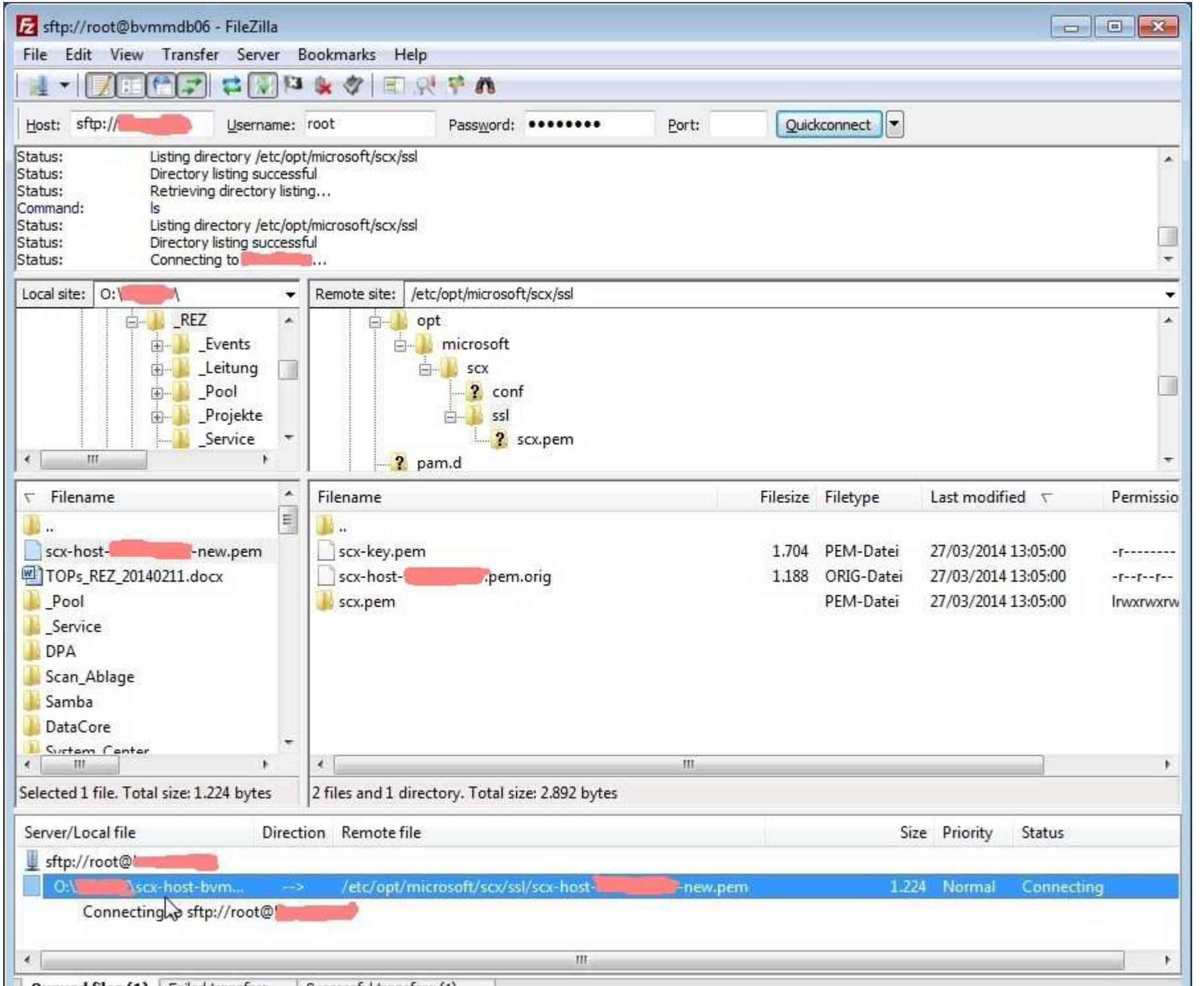
Navigate in the left pane to the directory where the new certificate was generated.

- Queue the resignatured certificate:


sftp://root@bvmmdb06 - FileZilla
File Edit View Transfer Server Bookmarks Help
Host: sftp:// Username: root Password: •••••••• Port: Quickconnect
Command: ls
Status: Listing directory /etc/opt/microsoft/scx/ssl
Status: Directory listing successful
Status: Retrieving directory listing...
Command: ls
Status: Listing directory /etc/opt/microsoft/scx/ssl
Status: Directory listing successful
Local site: O:\
_REZ
_Events
_Leitung
_Pool
_Projekte
_Service
Remote site: /etc/opt/microsoft/scx/ssl
opt
microsoft
scx
conf
ssl
scx.pem
pam.d
Filename
..
scx-host--new.pem
TOPs_REZ_20140211.docx
_Pool
_Service
DPA
Scan_Ablage
Samba
DataCore
Filename Filesize Filetype Last modified Permissio
..
scx-key.pem 1.704 PEM-Datei 27/03/2014 13:05:00 -r--------
scx-host-.pem.orig 1.188 ORIG-Datei 27/03/2014 13:05:00 -r--r--r--
scx.pem PEM-Datei 27/03/2014 13:05:00 lrwxrwxrw
Selected 1 file. Total size: 1.224 bytes
2 files and 1 directory. Total size: 2.892 bytes
Server/Local file Direction Remote file Size Priority Status
sftp://root@
O:\ scx-host-bvm... --> /etc/opt/microsoft/scx/ssl/scx-host--new.pem 1.224 Normal

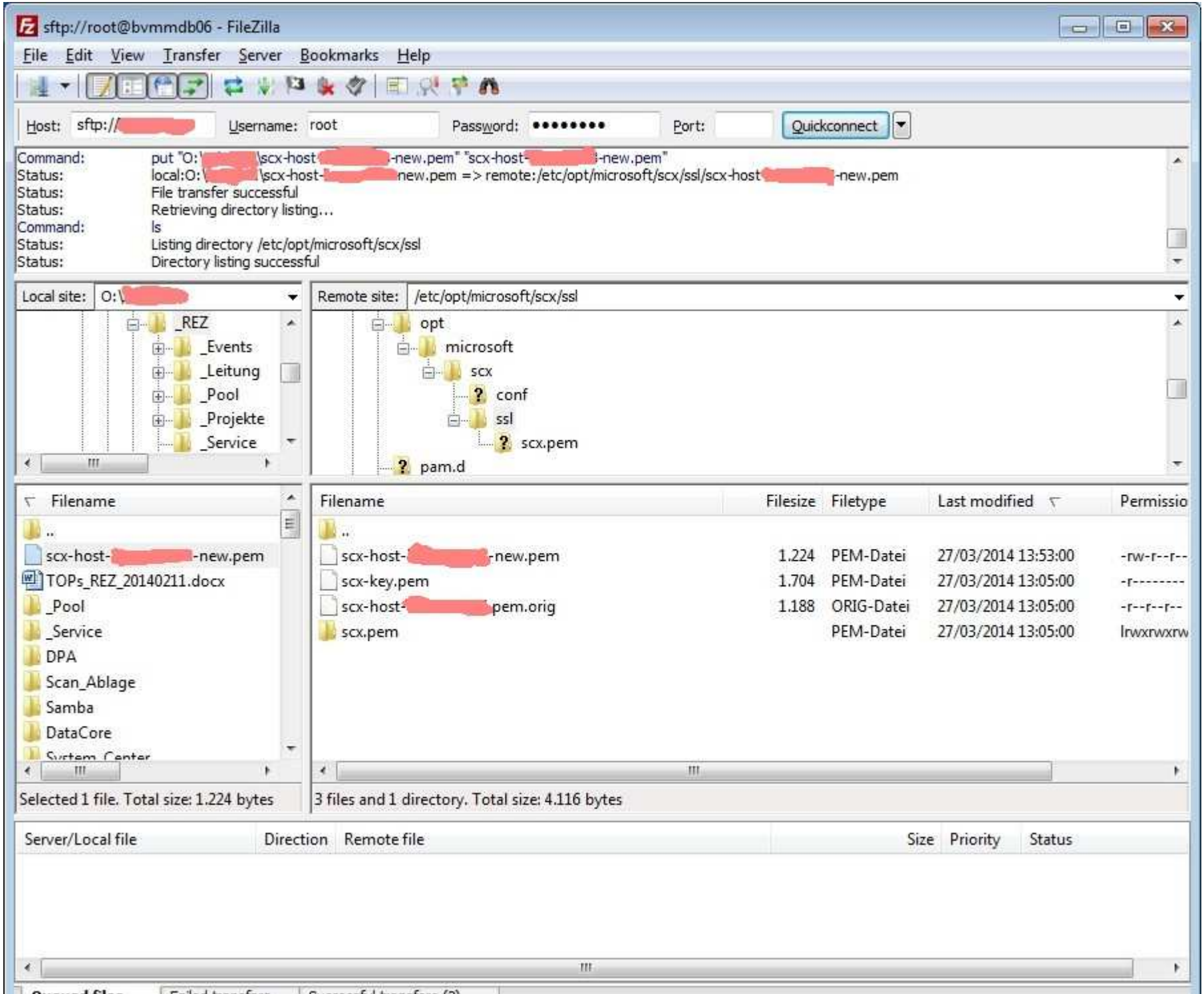
Drag 'n drop the new certificate from the left pane to the bottom pane. Make sure that the destination directory on the rigth pane is available!

- Transfering the resignatured certificate to the Linux server:


sftp://root@bvmmdb06 - FileZilla
File Edit View Transfer Server Bookmarks Help
Host: sftp:// Username: root Password: •••••••• Port: Quickconnect
Status: Listing directory /etc/opt/microsoft/scx/ssl
Status: Directory listing successful
Status: Retrieving directory listing...
Command: ls
Status: Listing directory /etc/opt/microsoft/scx/ssl
Status: Directory listing successful
Status: Connecting to ...
Local site: O:\ \
_REZ
_Events
_Leitung
_Pool
_Projekte
_Service
Remote site: /etc/opt/microsoft/scx/ssl
opt
microsoft
scx
conf
ssl
scx.pem
pam.d
Filename
..
scx-host- -new.pem
TOPs_REZ_20140211.docx
_Pool
_Service
DPA
Scan_Ablage
Samba
DataCore
Filename Filesize Filetype Last modified Permissio
..
scx-key.pem 1.704 PEM-Datei 27/03/2014 13:05:00 -r--------
scx-host- .pem.orig 1.188 ORIG-Datei 27/03/2014 13:05:00 -r--r--r--
scx.pem PEM-Datei 27/03/2014 13:05:00 lrwxrwxrw
Selected 1 file. Total size: 1.224 bytes
2 files and 1 directory. Total size: 2.892 bytes
Server/Local file Direction Remote file Size Priority Status
sftp://root@
O:\ \scx-host-bvm... --> /etc/opt/microsoft/scx/ssl/scx-host- -new.pem 1.224 Normal Connecting
Connecting to sftp://root@

Start the transfer by right-click on the file in the bottom pane and select "Process Queue".

- Successful transfer:


sftp://root@bvmmdb06 - FileZilla
File Edit View Transfer Server Bookmarks Help
Host: sftp:// Username: root Password: •••••••• Port: Quickconnect
Command: put "O:\[redacted]\scx-host[redacted]-new.pem" "scx-host-[redacted]-new.pem"
Status: local:O:\[redacted]\scx-host-[redacted]new.pem => remote:/etc/opt/microsoft/scx/ssl/scx-host[redacted]-new.pem
Status: File transfer successful
Status: Retrieving directory listing...
Command: ls
Status: Listing directory /etc/opt/microsoft/scx/ssl
Status: Directory listing successful
Local site: O:\[redacted]
_REZ
_Events
_Leitung
_Pool
_Projekte
_Service
Remote site: /etc/opt/microsoft/scx/ssl
opt
microsoft
scx
conf
ssl
scx.pem
pam.d
Filename
..
scx-host-[redacted]-new.pem
TOPs_REZ_20140211.docx
_Pool
_Service
DPA
Scan_Ablage
Samba
DataCore
Filename Filesize Filetype Last modified Permissio
.. 1.224 PEM-Datei 27/03/2014 13:53:00 -rw-r--r--
scx-host-[redacted]-new.pem 1.704 PEM-Datei 27/03/2014 13:05:00 -r--------
scx-key.pem 1.188 ORIG-Datei 27/03/2014 13:05:00 -r--r--r--
scx-host-[redacted]pem.orig PEM-Datei 27/03/2014 13:05:00 lrwxrwxrw
scx.pem
Selected 1 file. Total size: 1.224 bytes
3 files and 1 directory. Total size: 4.116 bytes
Server/Local file Direction Remote file Size Priority Status

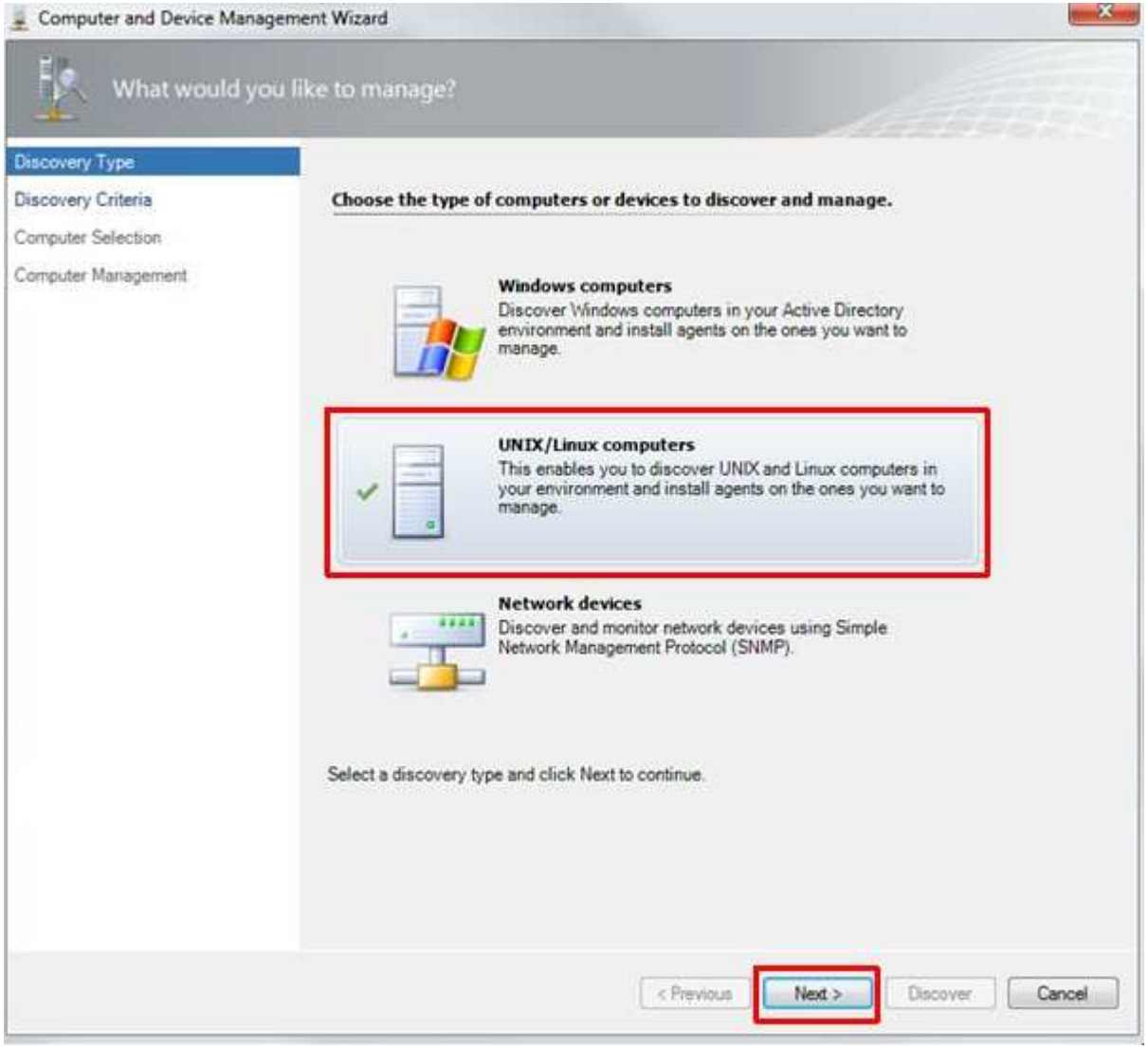
If the transfer was successful you will find the backup of the original certificate and the new resignatured certificate in the same directory.

- Now we switch back to the Linux command line:

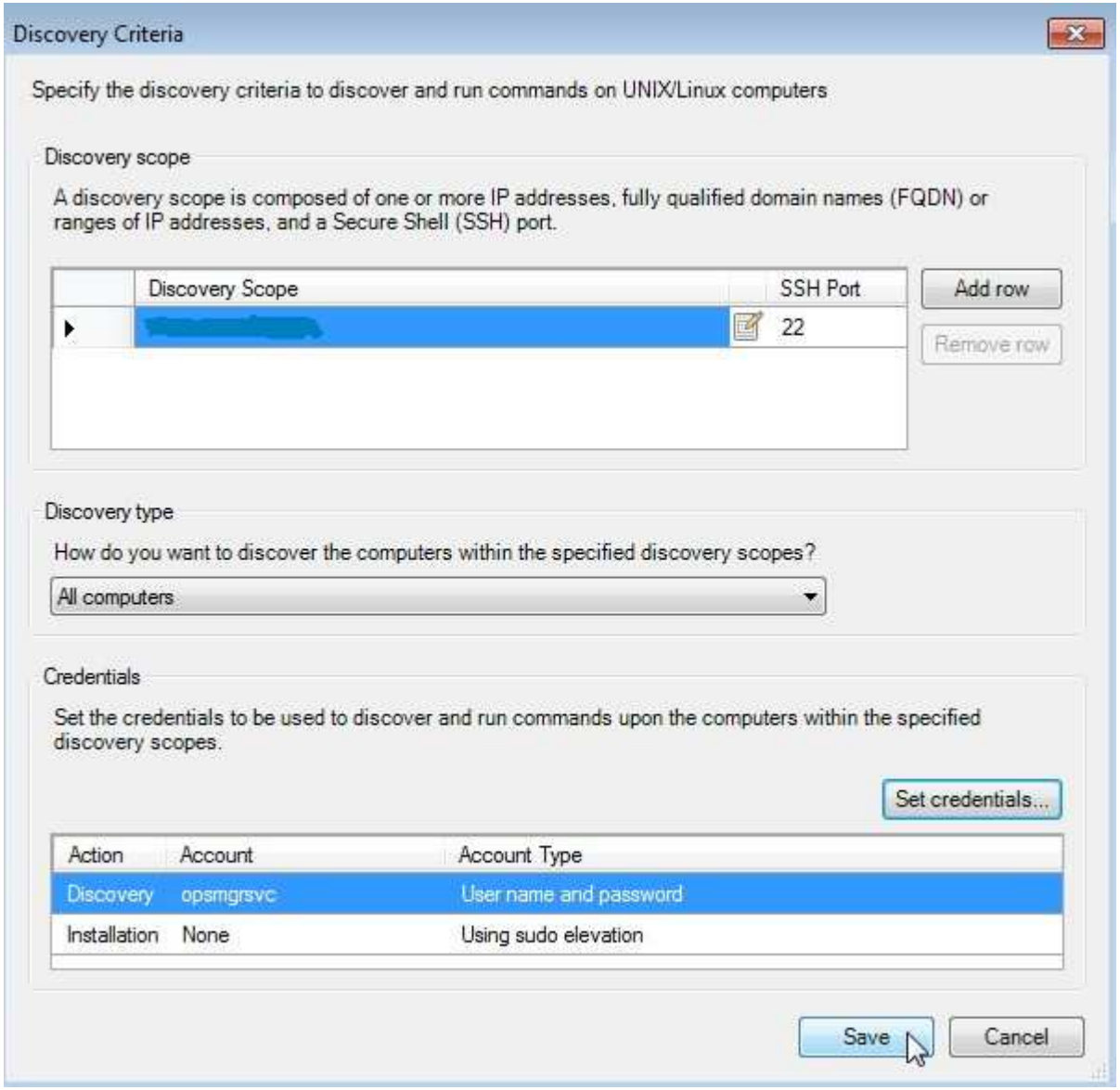
```
[root@<hostname> ~]# cd /etc/opt/microsoft/scx/ssl
[root@<hostname> ~]# mv scx-host-<hostname>-new.pem scx-host-<hostname>.pem
[root@<hostname> ~]# chmod 444 scx-host-<hostname>.pem
[root@<hostname> ~]# ls -l
total 12
-r--r--r-- 1 root root 1224 Mar 27 14:04 scx-host-<hostname>.pem
-r--r--r-- 1 root root 1188 Mar 27 13:05 scx-host-<hostname>.pem.orig
-r-------- 1 root root 1704 Mar 27 13:05 scx-key.pem
lrwxrwxrwx 1 root root   48 Mar 27 13:05 scx.pem -> /etc/opt/microsoft/scx/ssl/scx-host-<hostname>.pem
[root@<hostname> ~]#
```

It's now the time to do little file operations: rename the new certificate and assign the correct file permissions.

13. No we have to go back to the Select UNIX/Linux computers screen, click Next

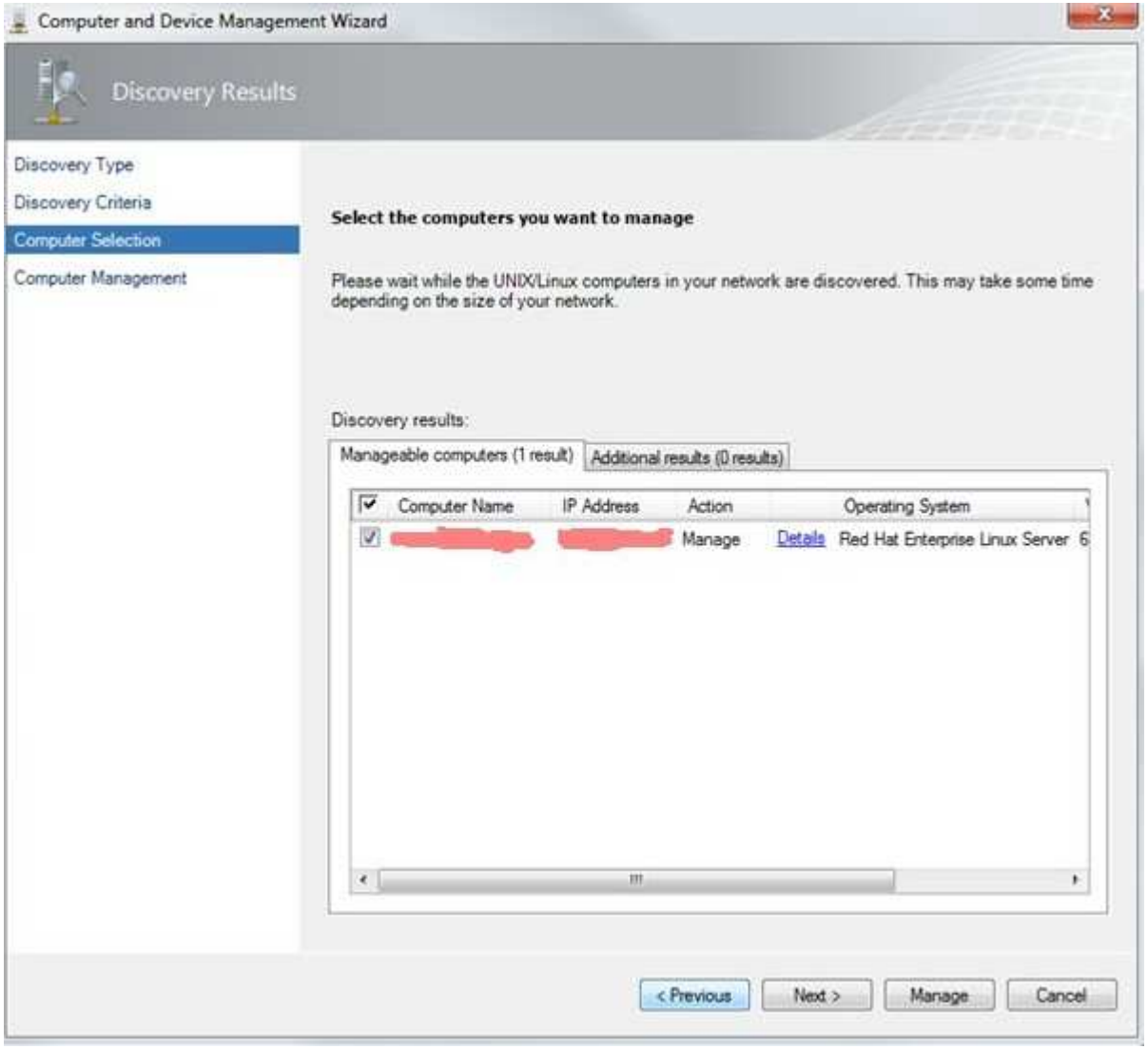


14. Check the settings:



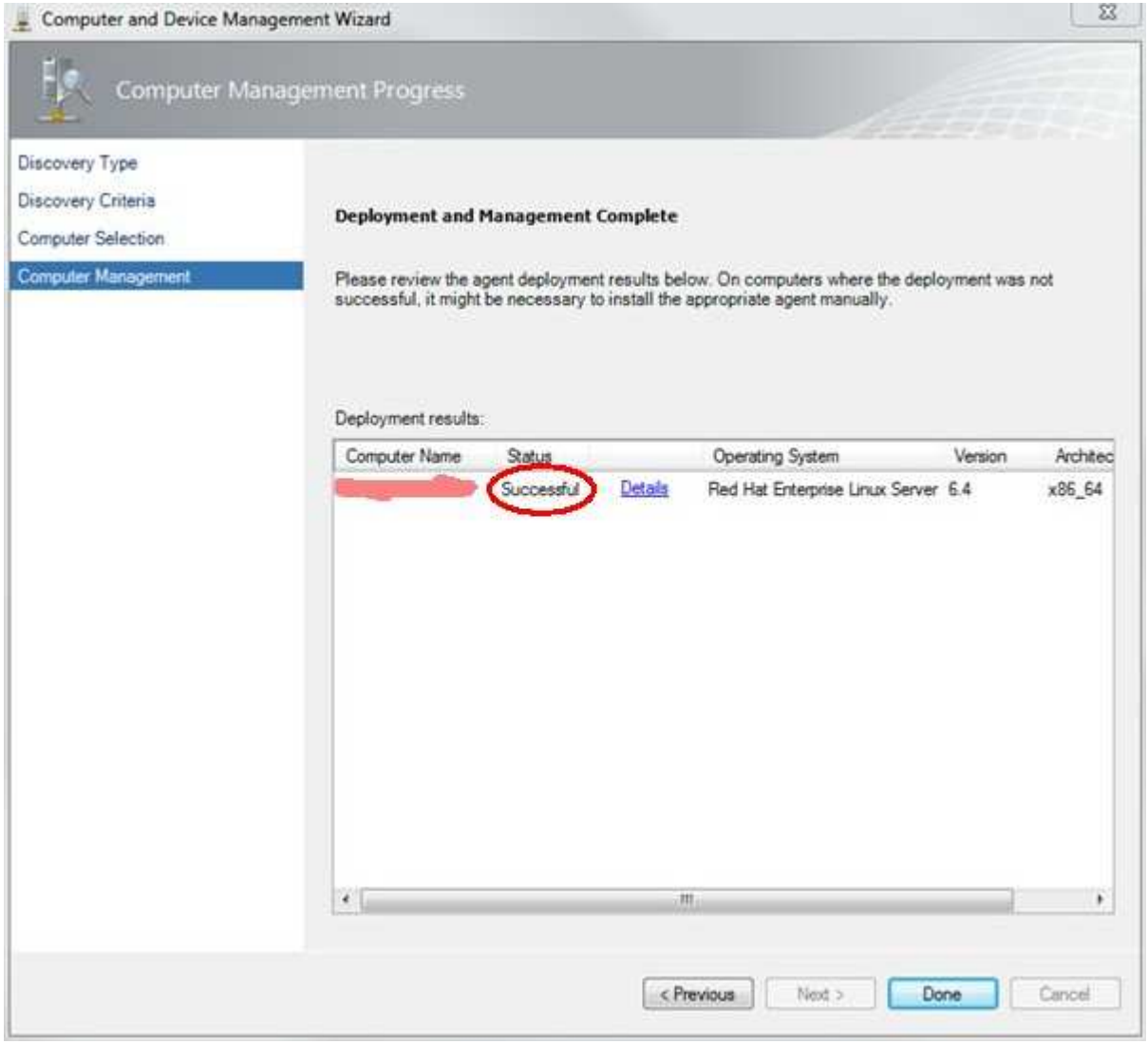
Don't forget to click Save!

15. Again selection of the computers to manage:



Select the appropriate checkbox and click on Manage! Note: There is just the action manage available.

16. Agent deployment now successful:



Click on Done! We've got it.

You can download this page as pdf file [922 kB].

On the next page I will provide some additional information about the SCOM agent.

On the previous page I described the base setup of the SCOM and RHEL.

Frank Ickstadt
Am Königsbachtal 32.1
65817 Eppstein
Germany

Phone: not available

frank [dot] ickstadt [at] removethis gmail [dot] com

Fax: currently out of order

Your browser: *Netscape ; 5.0 (Windows)*