How to monitor RedHat Enterprise Linux 5 or 6 using Microsoft System Center Operations Manager (SCOM) 2012 SP1 - Part 1

Modifications of the Linux OS and SCOM

It's really a mess to get a running configuration for SCOM and RHEL. There are serveral descriptions for more or less specific installations. The scope of this document is to provide a generic solution for a running configuration of RHEL 5 or 6 and SCOM 2012 SP1. Relax and enjoy!

1. If you are unfamilar with the Linux Operating System please fetch a Linux guy first. He or she will be very helpful during the troubleshooting process!

2. To fulfill the prerequisites on Linux I've provide a small and simple bash shell script which doing all the stuff. The script name is "**prepare4scom**" and I guess there are some improvements possible but now it does what it should. Here it is:

```
#! /bin/bash

# This script prepares a RHEL System to get ready for a Micrososft System Center Operations Manager (SCOM)
# agent installation.

# doing some prerequisites
if (( $EUID != 0 )); then
    echo "You must be root to run this script!"
    exit 1
fi

DATE=$(date +%Y%m%d_%H%M)


# Add user and set password
echo "Adding user opsmgrsvc with uid 550"
useradd -c "SCOM service account" -u 550 -m opsmgrsvc

echo "Setting password for user opsmgrsvc"
echo "please-enter-password-here" | passwd opsmgrsvc --stdin


# Configure /etc/sudoers file
echo "adding entries to /etc/sudoers"
```

```
if [ -f /etc/sudoers ] ; then
  cp -p /etc/sudoers /etc/sudoers.$DATE
  cp -p /etc/sudoers /etc/sudoers_work
  sed -i '/^root.*ALL=(ALL) /a\opsmgrsvc ALL=(root) NOPASSWD: ALL' /etc/sudoers_work
  sed -i '/^Defaults.*requiretty/a\Defaults:opsmgrsvc !requiretty' /etc/sudoers_work
  echo "performing a visudo check"
  visudo -c -f /etc/sudoers_work 2>&1 >/dev/null
  RC=$?
  if [ ${RC} -ne 0 ] ; then
    echo "There is a problem in accessing/editing /etc/sudoers_work!"
    exit 2
  fi
  mv -f /etc/sudoers_work /etc/sudoers
else
  echo "No /etc/sudoers file found!"
fi

echo "all done. Exiting"
echo ""
echo "#########################################################################"
echo "Please add the appropriate user (opsmgrsvc) to /etc/ssh/sshd_config file"
echo "if the directive AllowUsers is used and restart the ssh daemon!!"
echo "#########################################################################"

exit
```

3. Save the script to the system which should be monitored and change the ownership and execute permisions:

```
chown root:root prepare4scom
chmod 750 prepare4scom
```

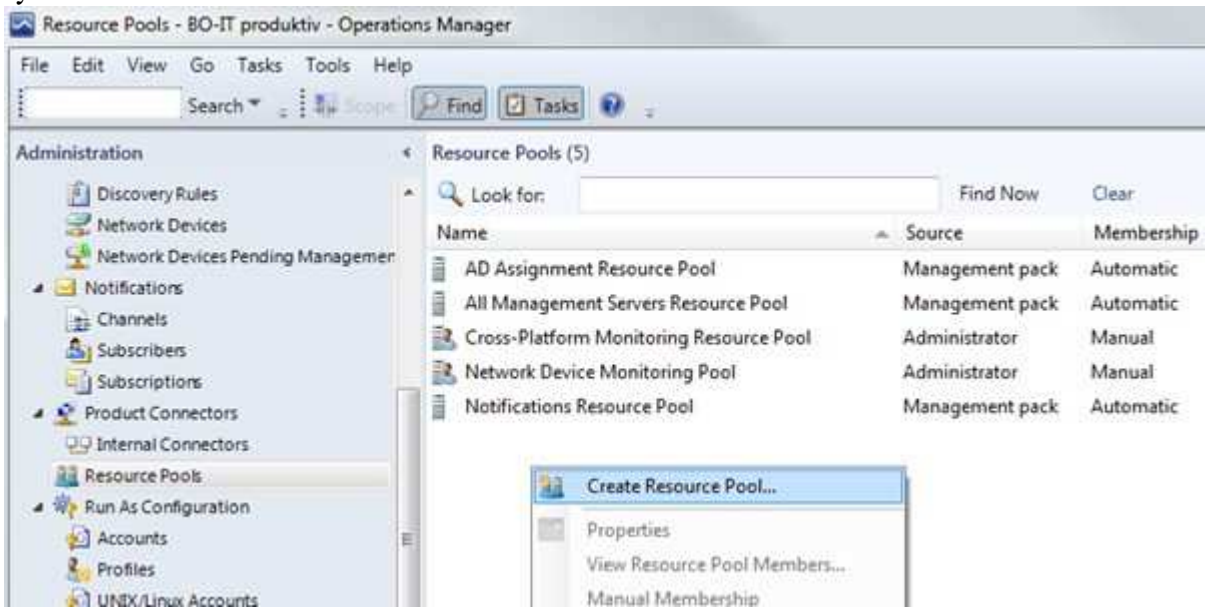
4. Now execute this script as user "**root**":

```
./prepare4scom
```

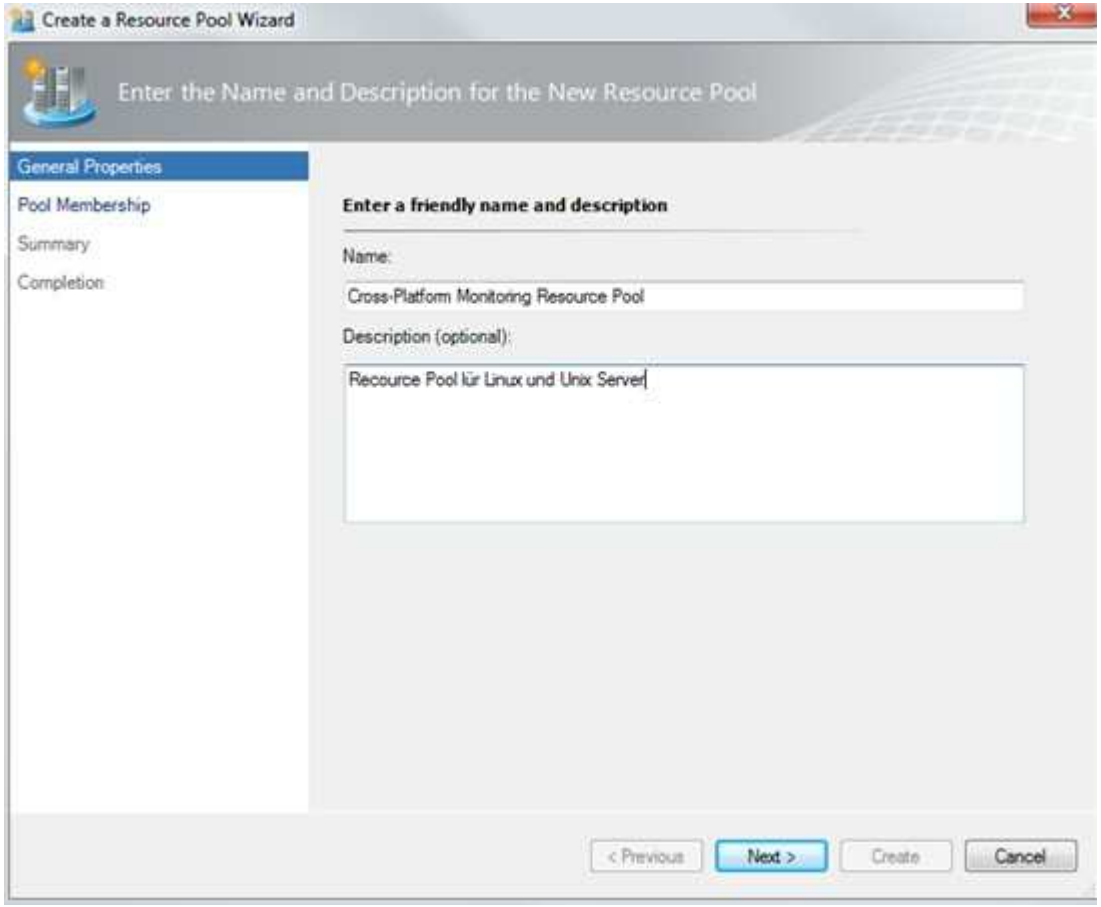
After (successful) execution of this script delete it immediately, because the password is coded into the script itself!

5. Now we've done the whole Linux part for configuration the Linux OS!

6. I assume that there is a ready to run SCOM 2012 installation. First we have to create a cross-platform resource pool for monitoring UNIX and Linux systems:

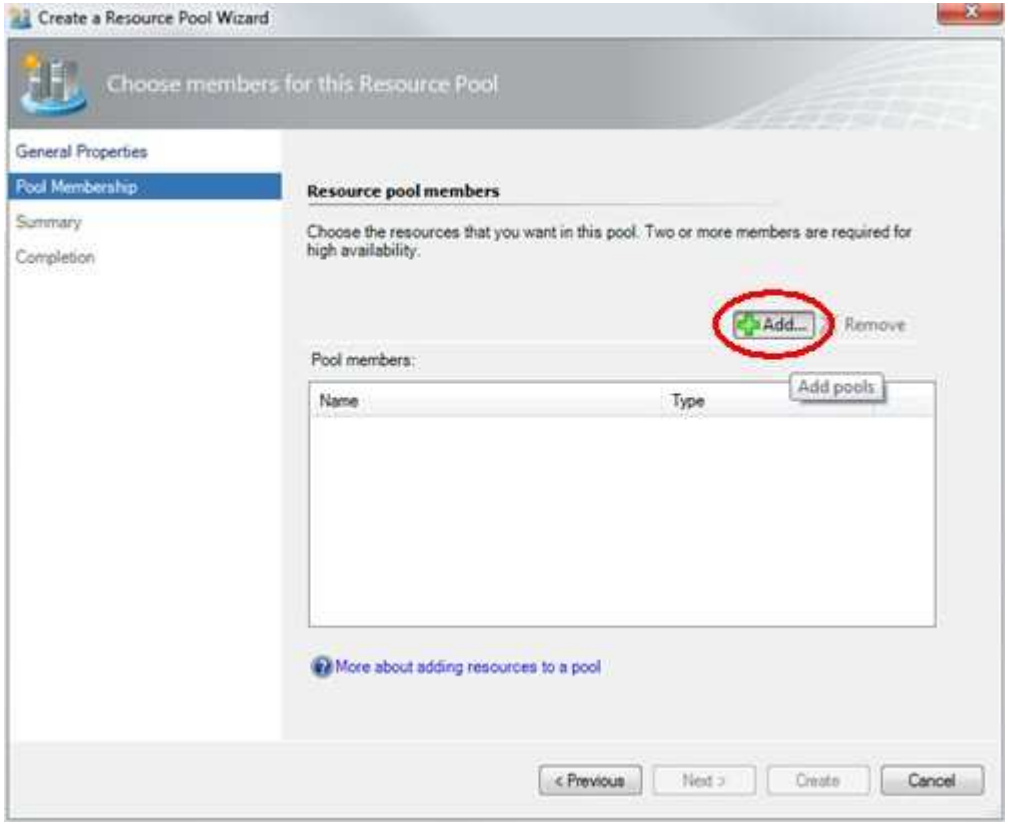


7. Give the resource pool a meaningfull name:



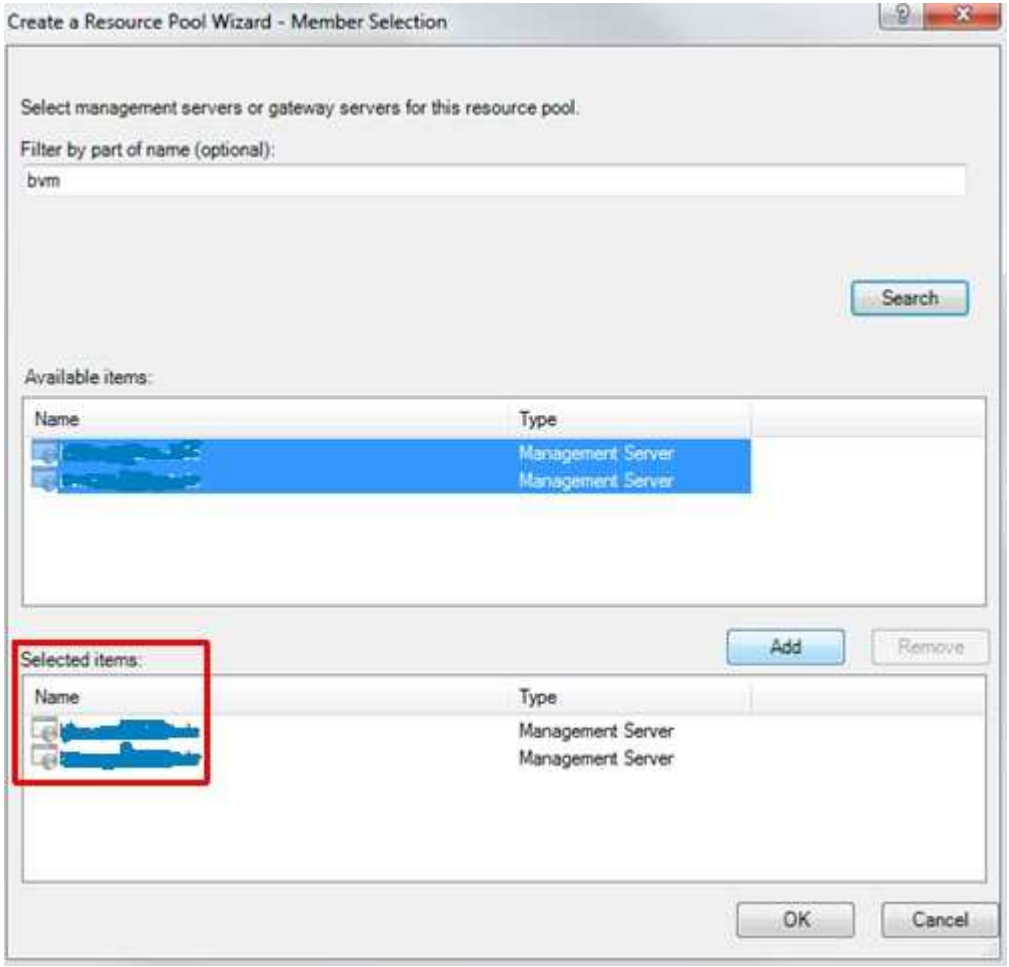
We choose "Resource pool for Linux and UNIX server".

8. Assign the management server to the resource pool:



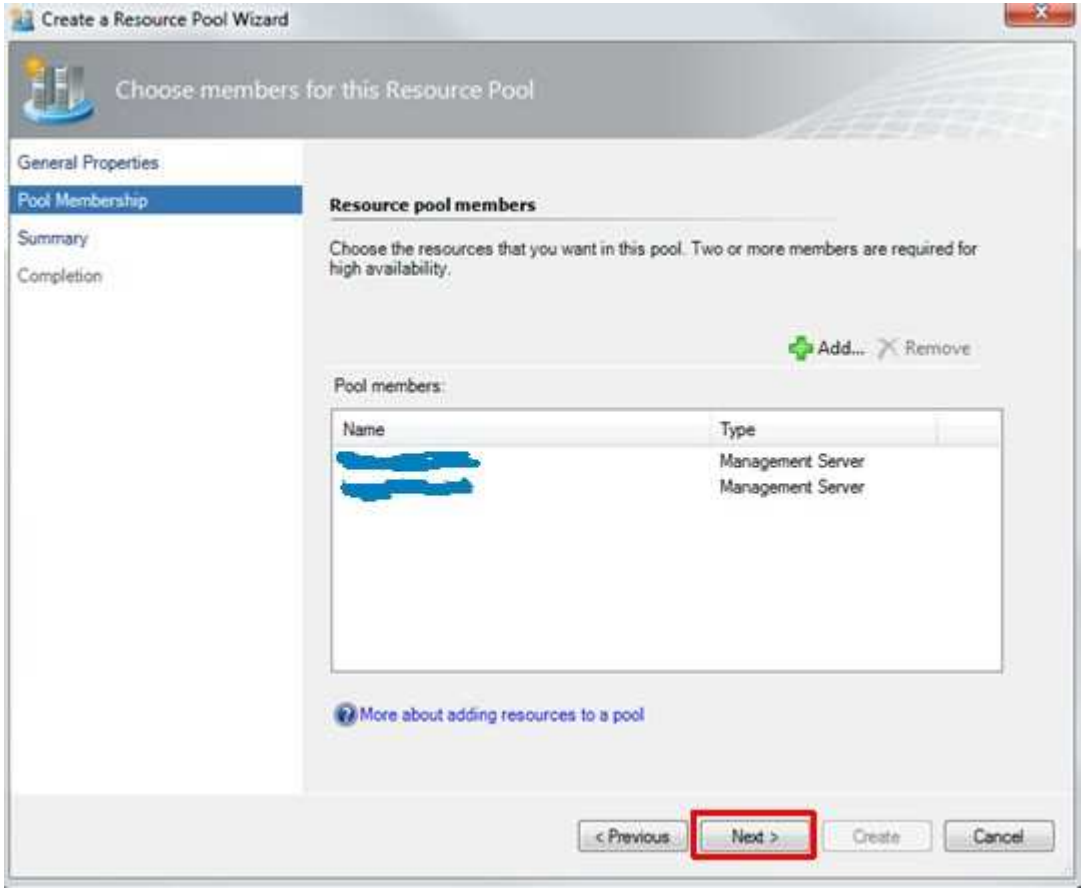
Just click "Add".

9. Choose the management server:

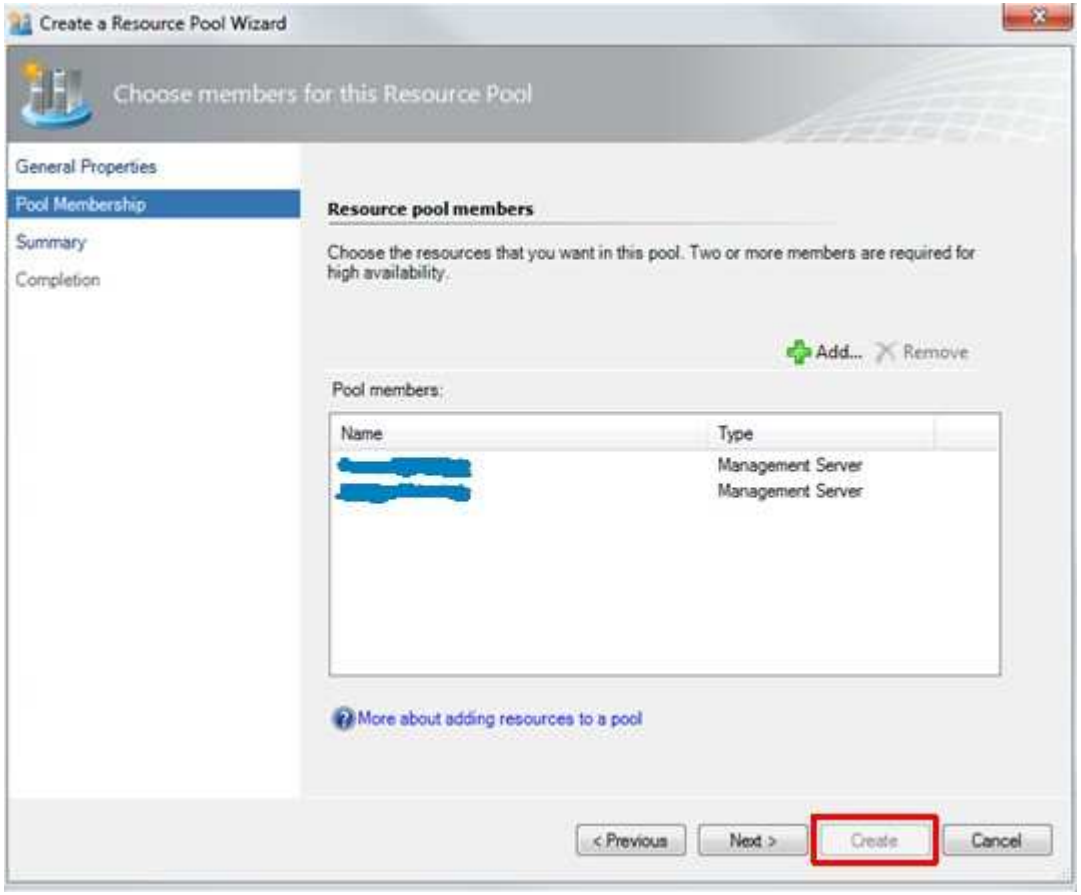


In our environment there are two managmenet server, you may have just one or more. Don't forget to click OK!

10. Click Next:



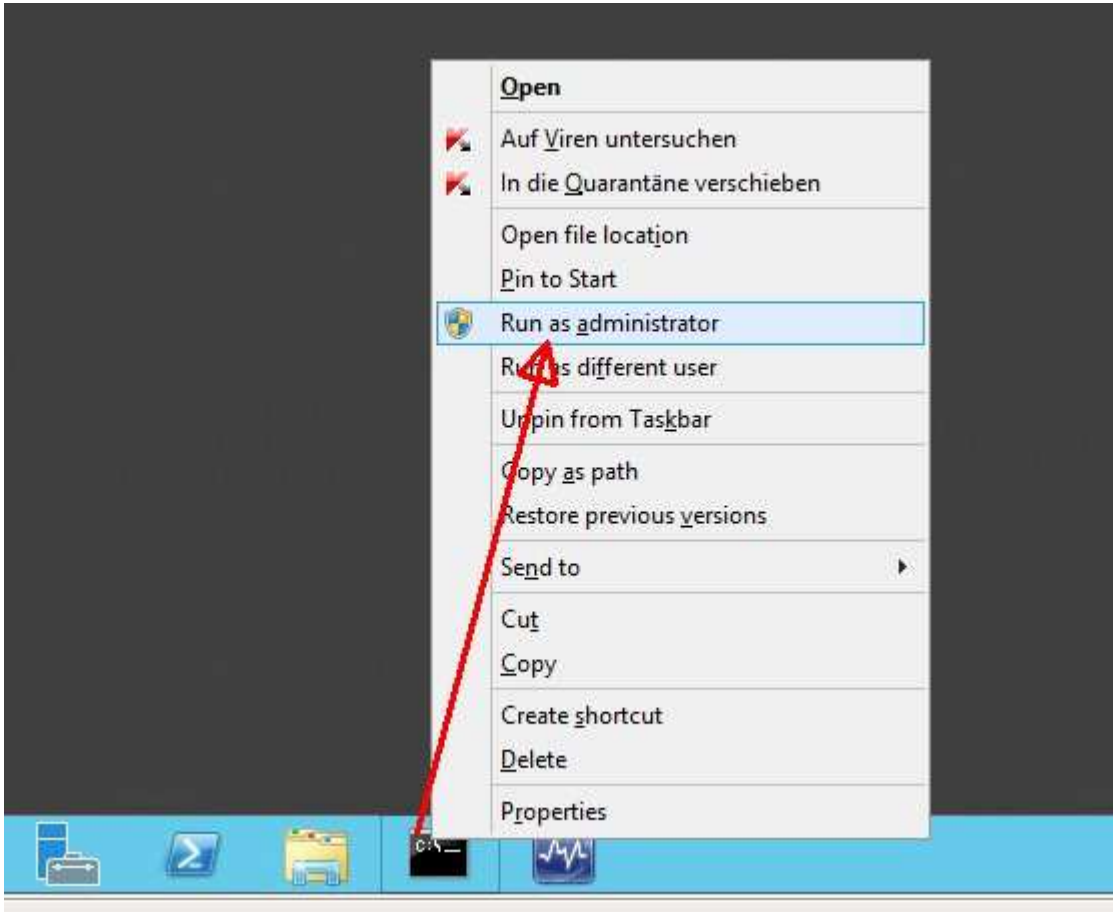
11. Create the resource pool:



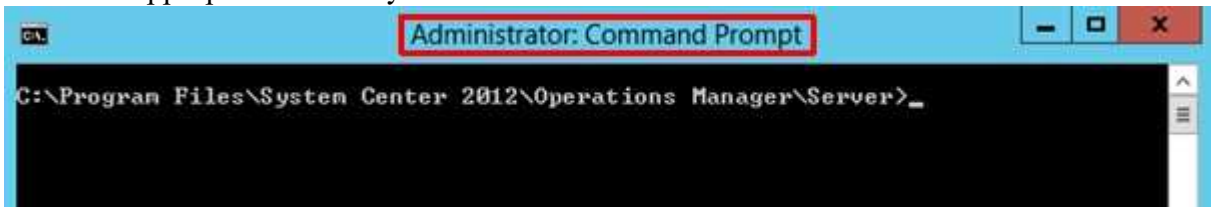
Just click on Create to build the resource pool!

12. Now we've done the resource pool creation part!

13. Because we have more than one management server as members of a cross-platform resource pool, we have to copy the server certificates to each member of the resource pool. Doing this we must start the command.com as an aministrator (click right on icon):



14. Go to the appropriate directory:




```
cd "%Program Files%\System Center 2012\Operations Manager\Server"
```

15. Export certificate on each management server:

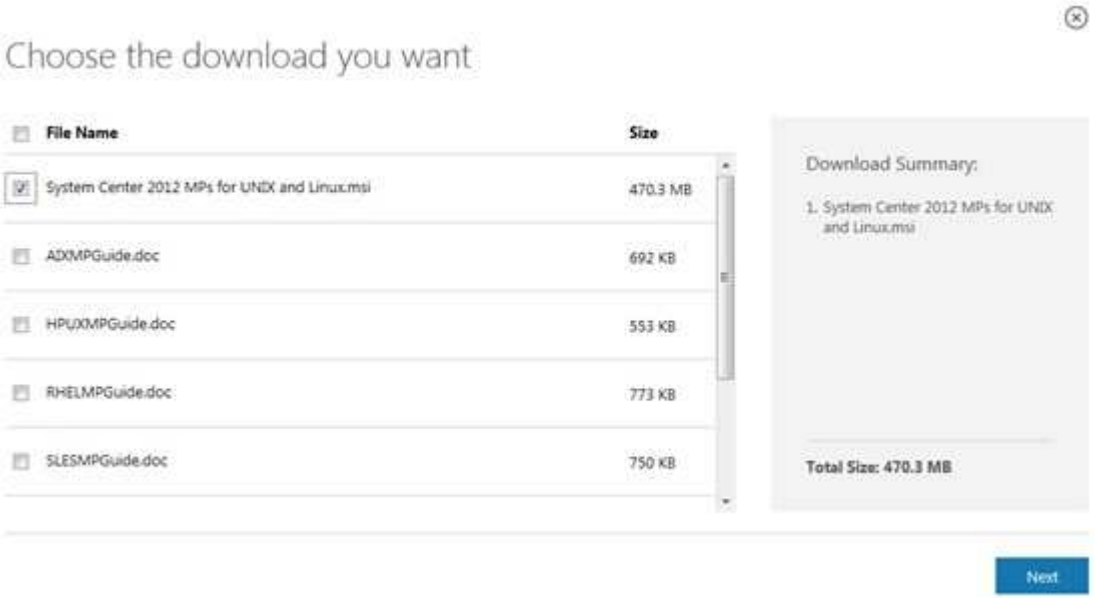

```
scxcertconfig.exe -export <local-hostname>.cert
```

16. Import only the foreign certificates on each management server:
    The certificates has to be placed on each management server in to the directory "%Program Files%\System Center 2012\Operations Manager\Server"
    and then import them to the local cert store. 

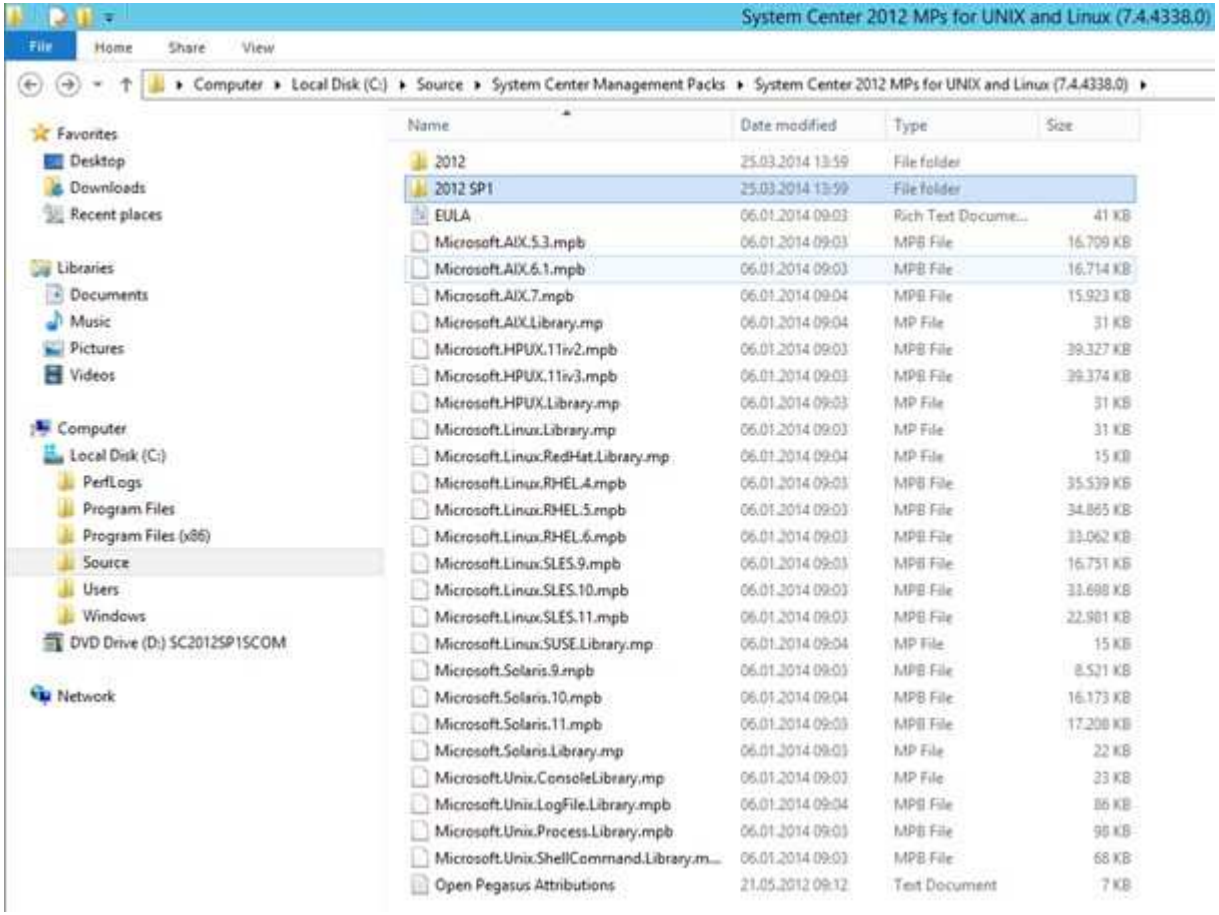

```
cd "%ProgramFiles%\System Center 2012\Operations Manager\Server"
scxcertconfig.exe -import <local-hostname>.cert
```

17. Now we've done the spread certificates part!

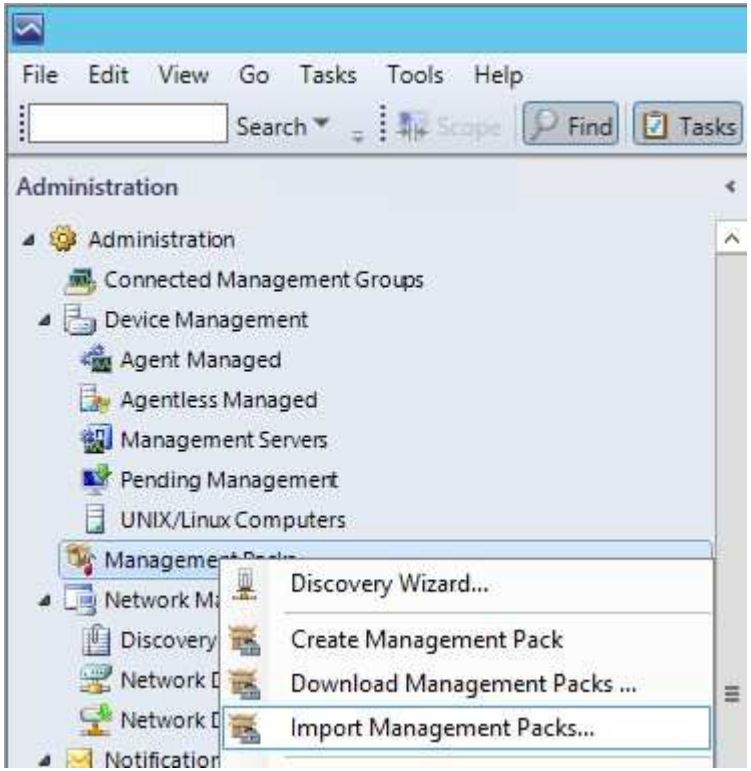
18. Next we have to download the current Monitoring Pack for UNIX and Linux from the following website:
    http://www.microsoft.com/en-us/download/details.aspx?id=29696
    You will be asked to choose the download and we want to have the "**System Center 2012 MPs for UNIX and Linux.msi**" package. Feel free to download more files, but these are not necessarry for our installation.



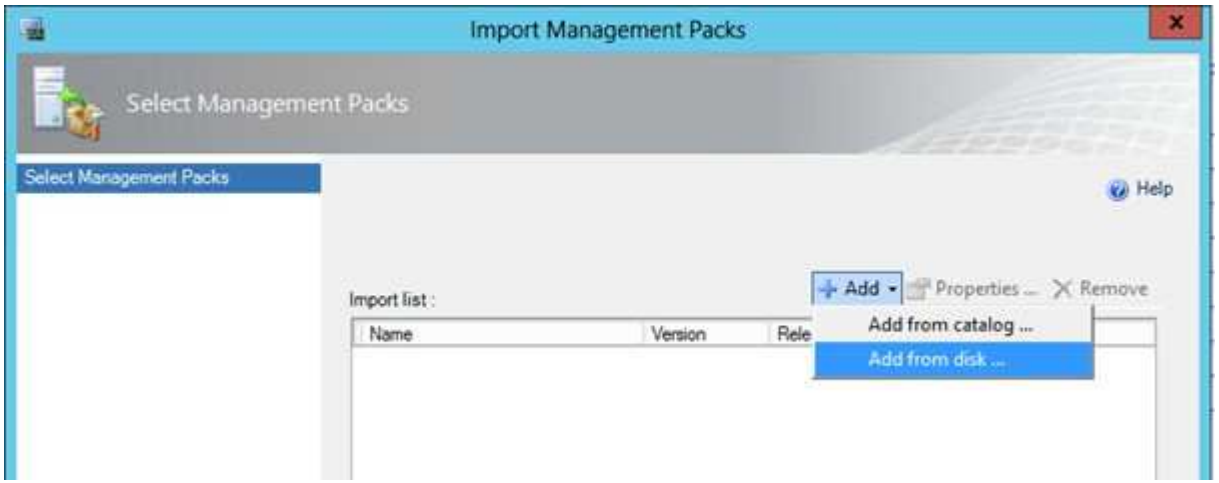
19. Next step is to execute the msi file. As a result we get a whole bunch of fresh management packs:



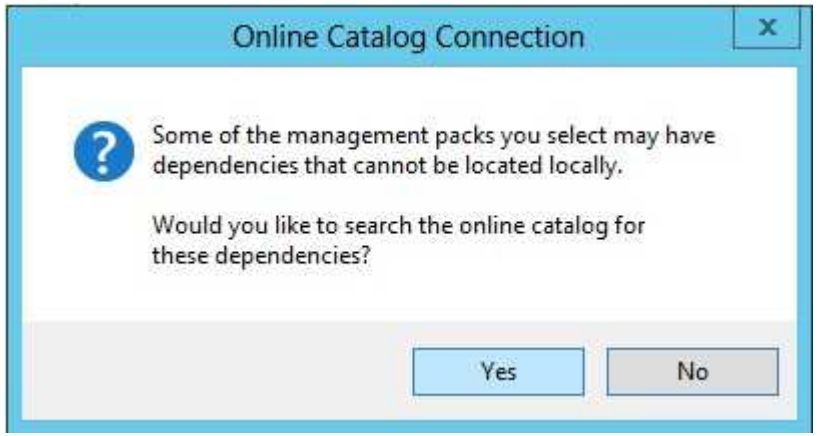
20. Now we are ready to import the wanted management packs using the SCOM console:



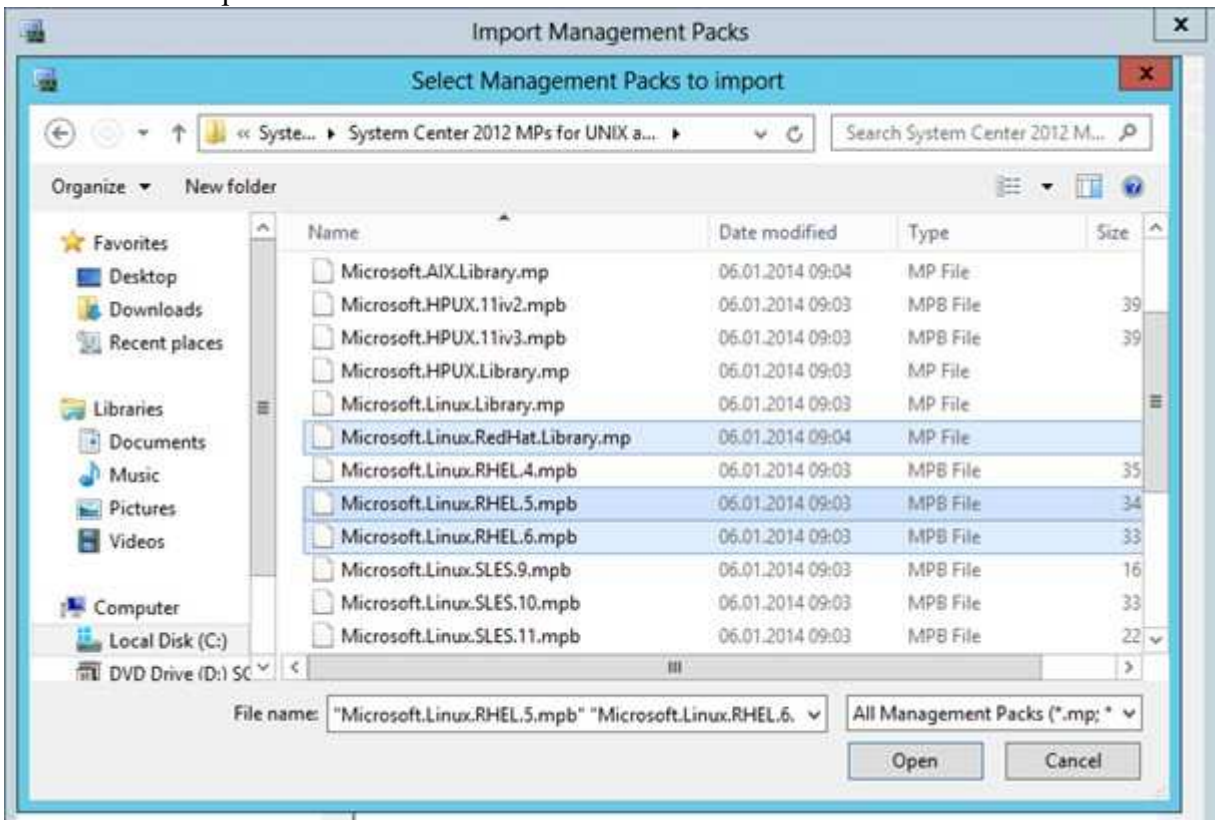
21. Add from disk:



22. Resolve dependencies (click Yes):

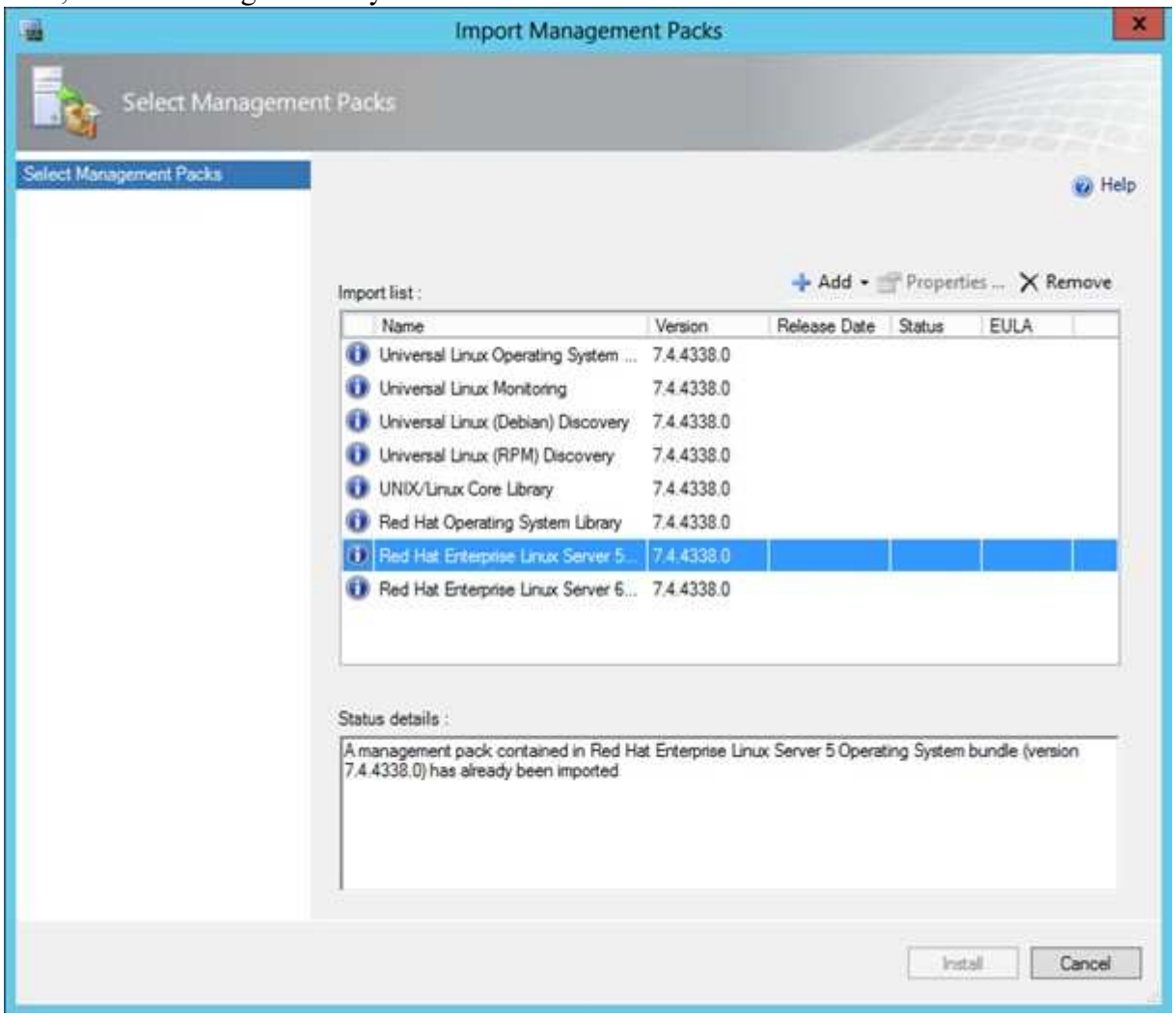


23. Select MPs to import:



24. Installation of selected MPs:

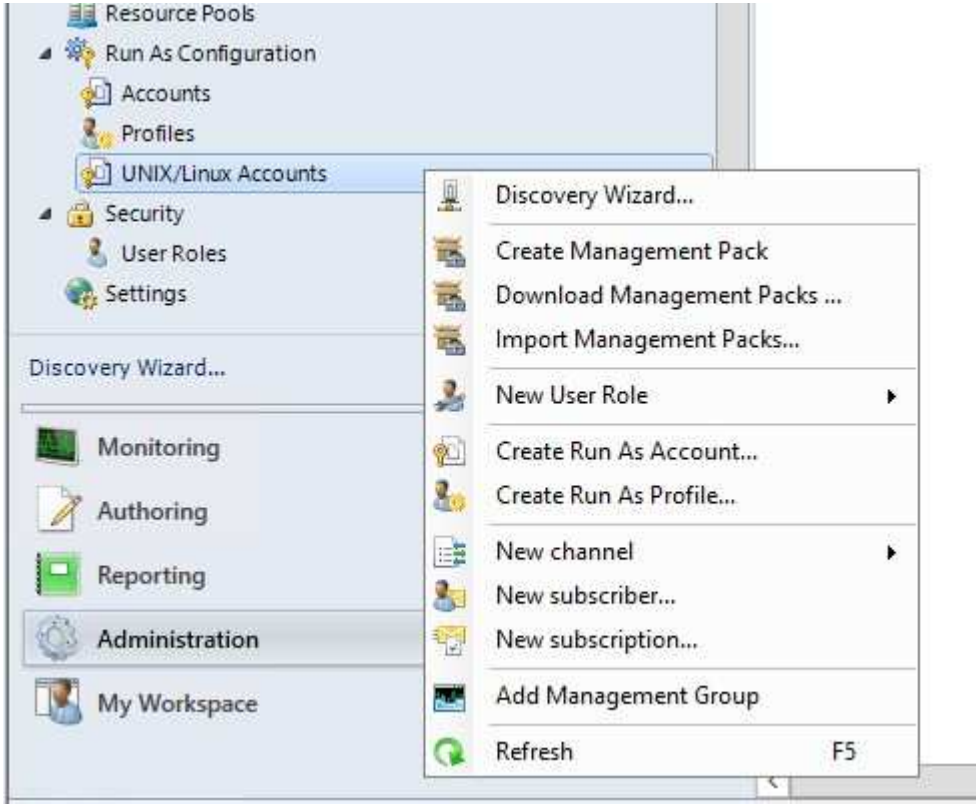
Because this is not a really fresh installation we see the blue icons and the gey (inactive) Install button. If you have truely a fresh installation of the MPs, the icons are green and you are able to choose the Install button!



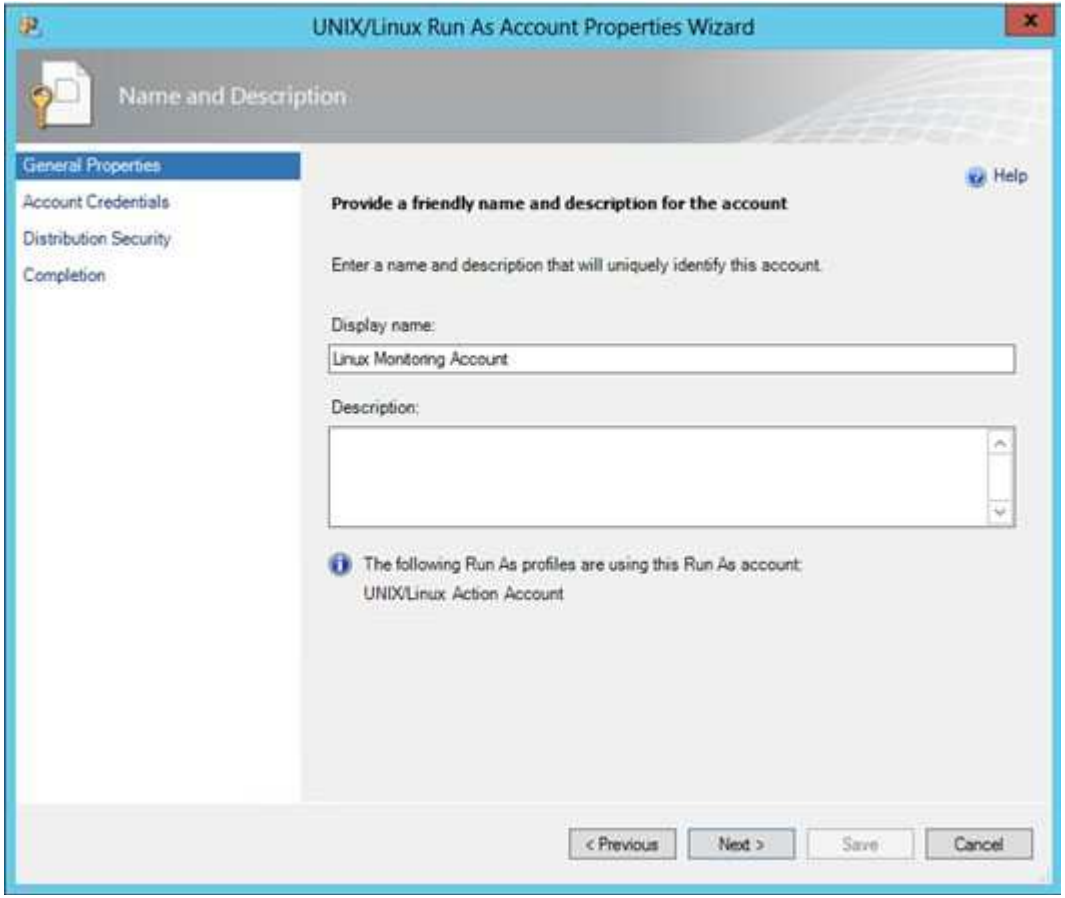
25. Now we've done the whole management pack installation part!

26. Creation of two UNIX/Linux Run As accounts
    Now we have to create two SCOM Run As accounts. We follow the documentation: Microsoft System Center Operations Manager - "Red Hat Enterprise Linux Server Management Pack Guide for System Center 2012 - Operations Manager" (RHELMPGuide.doc). Both accounts are mapped to the single local Linux account which we have created in step 4. by executing the bash shell script.

1. First we create a non-elevated Run As account:

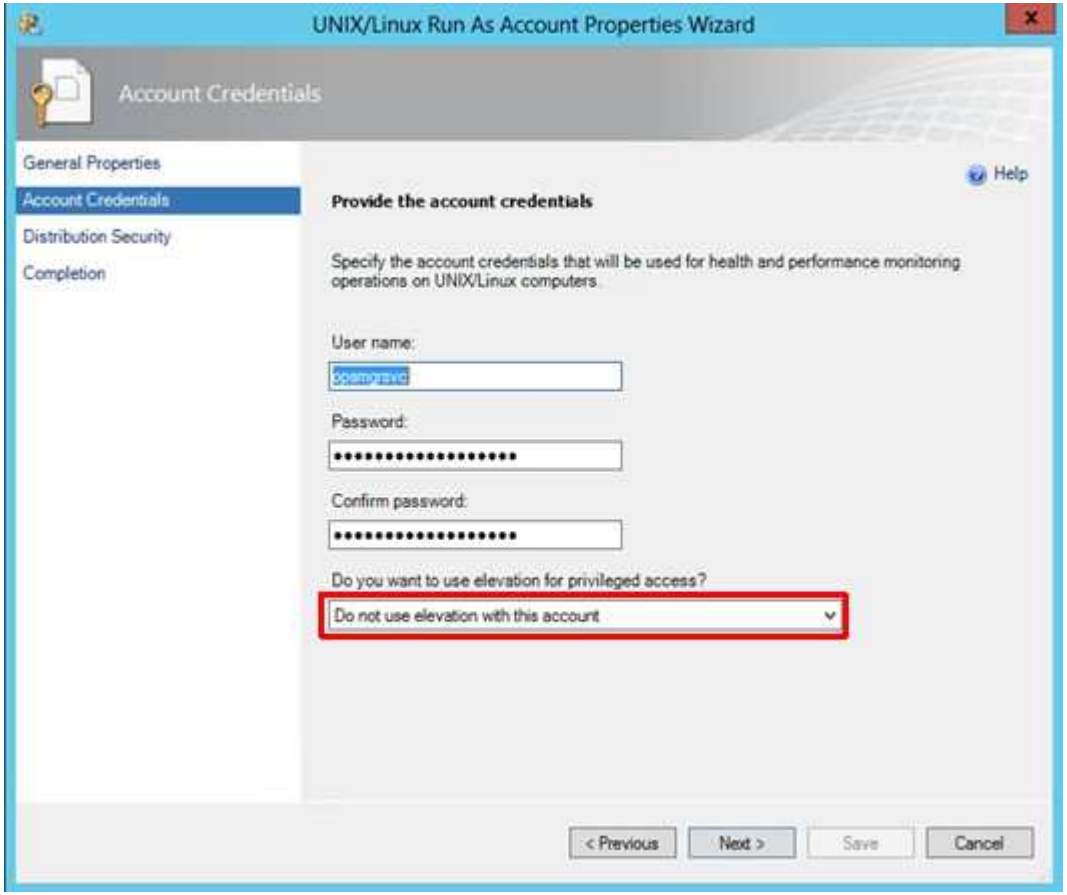


   - Give the account a meaningfull display name



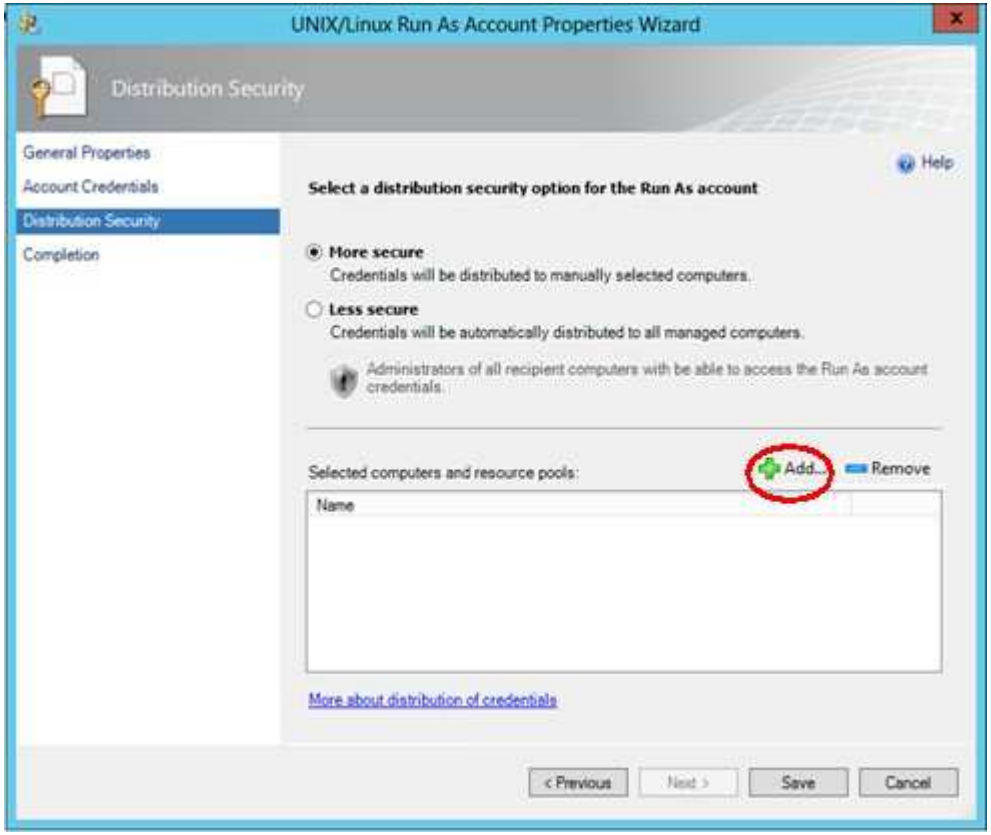
We choose "Linux Monitoring Account".

- Insert the account credentials



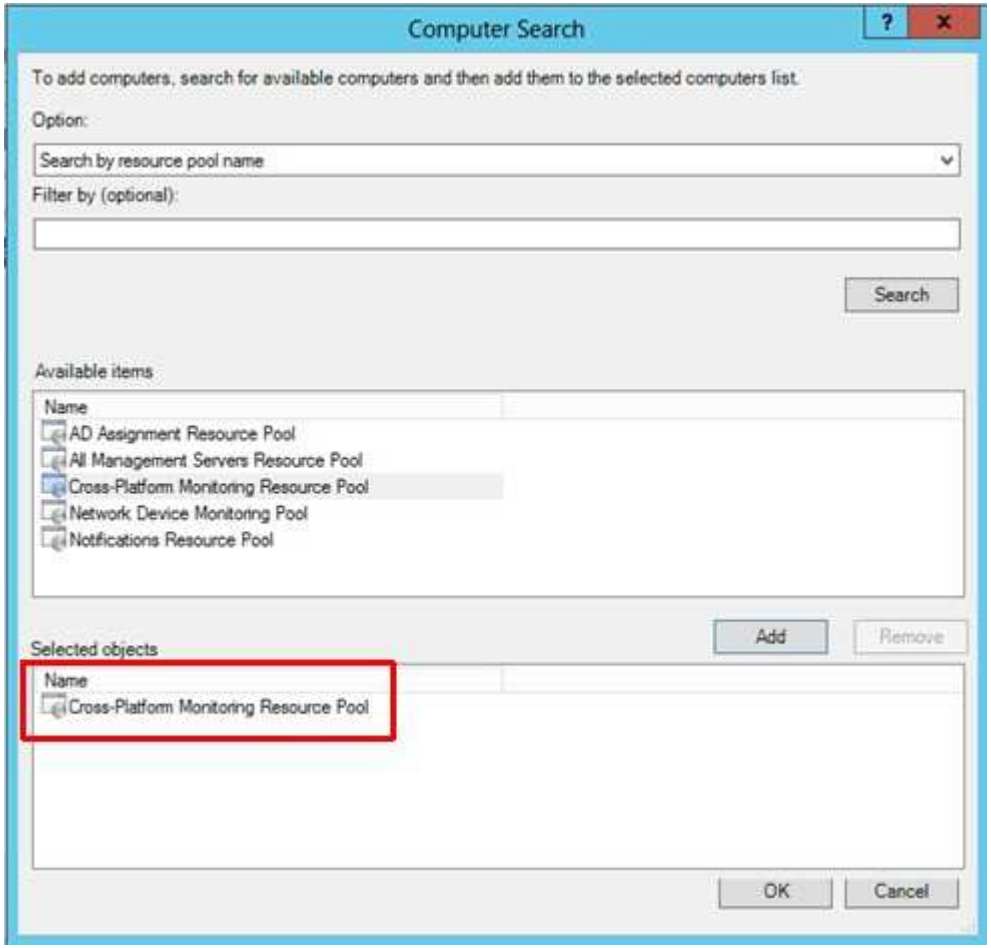
The credentials are the same as in step 4.! Please select "Do not use elevation with this account".

- Choose distribution security option



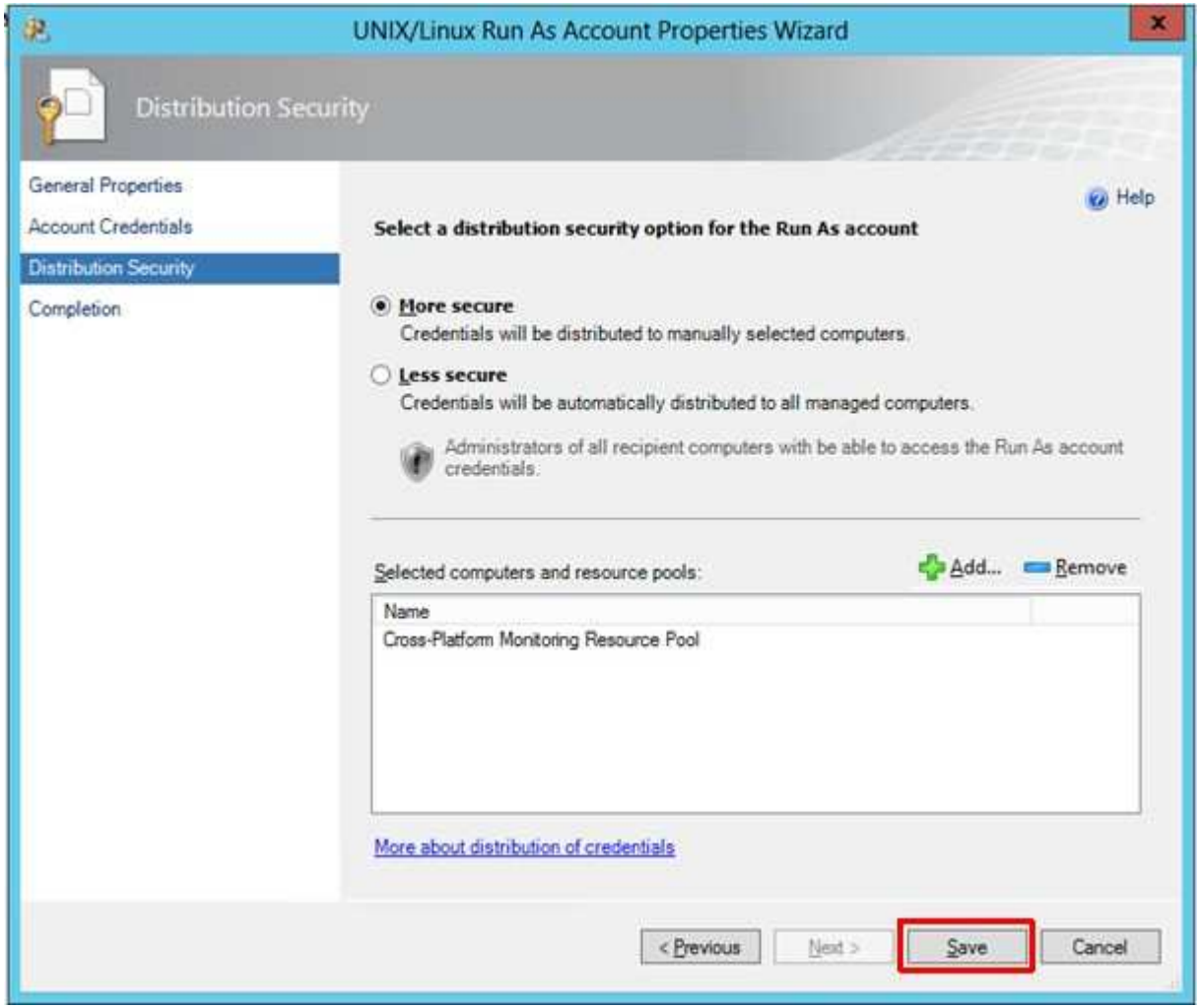
Select "More secure" and click on add to choose a resource pool.

- Add the resource pool



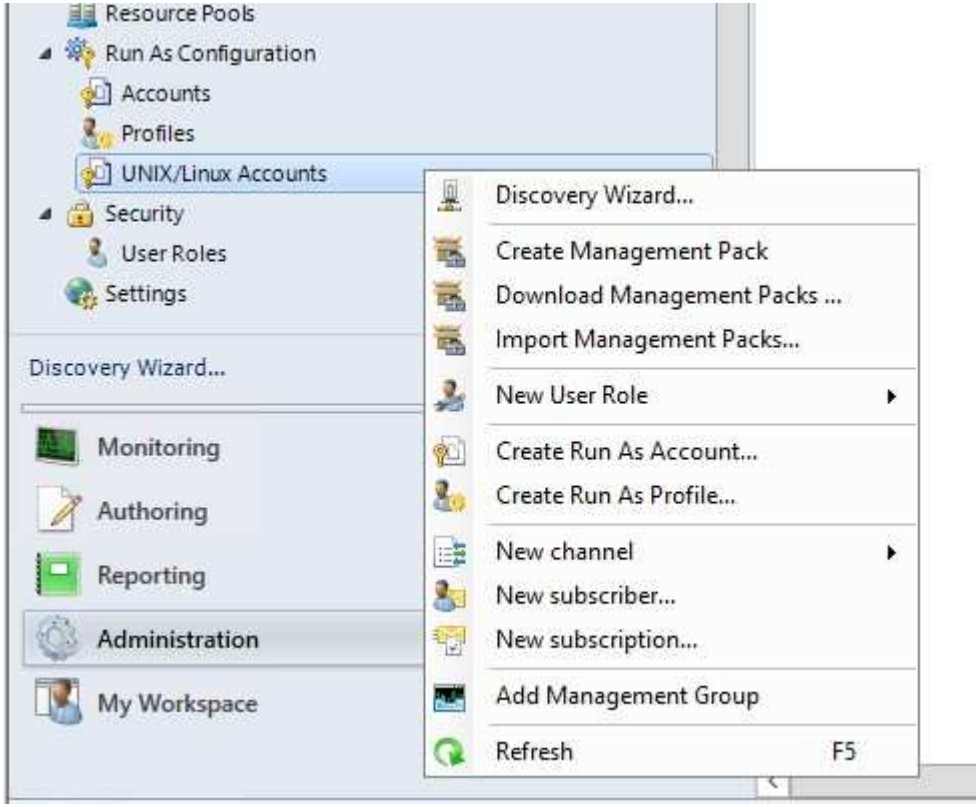
Now we add the resource pool "Cross-Platform Monitoring Resource Pool" which we have created in step 11). Don't forget to click OK!

- Save the settings for the first Run As account

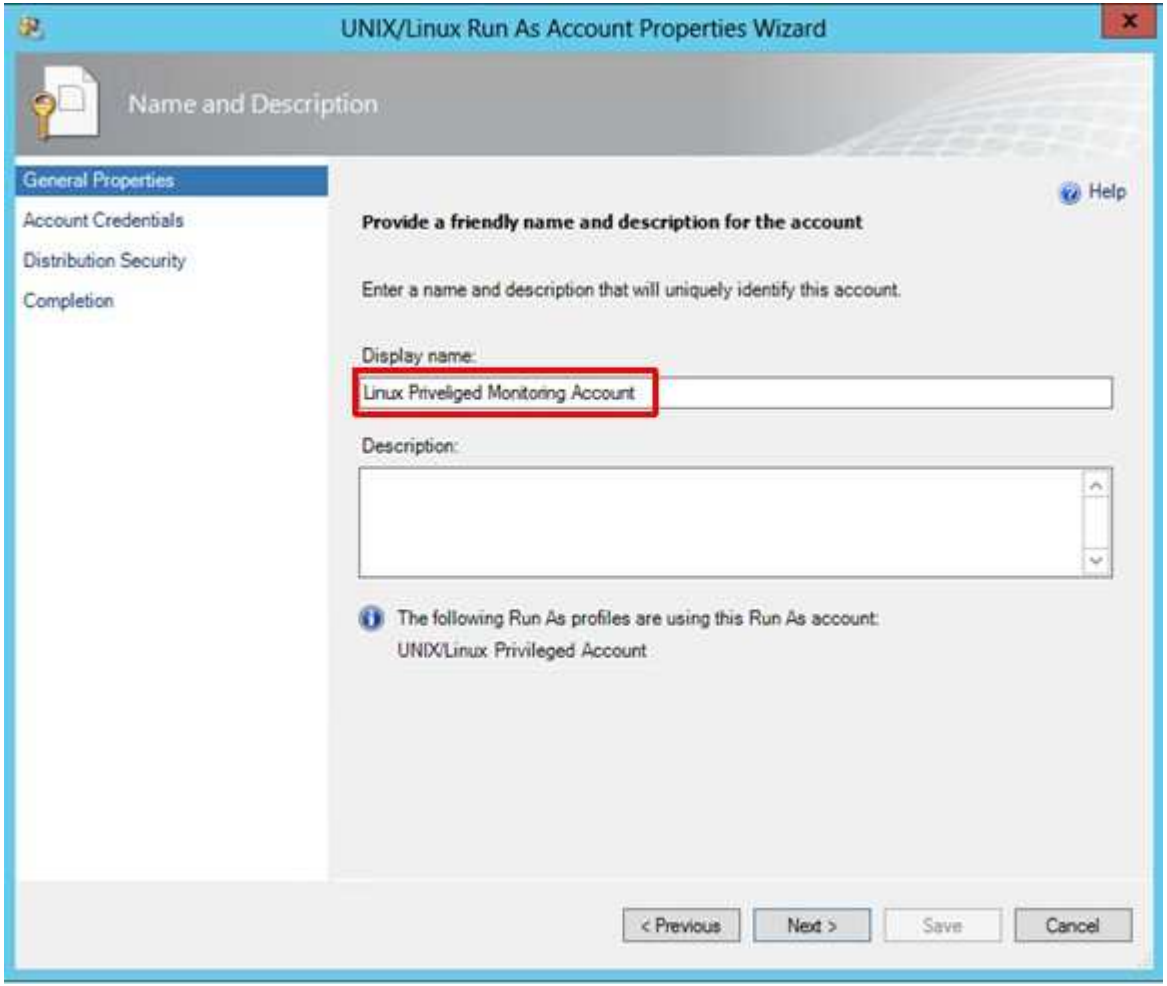


To set up the first account just click "Save".

2. As the second step we create the elevated Run As account:

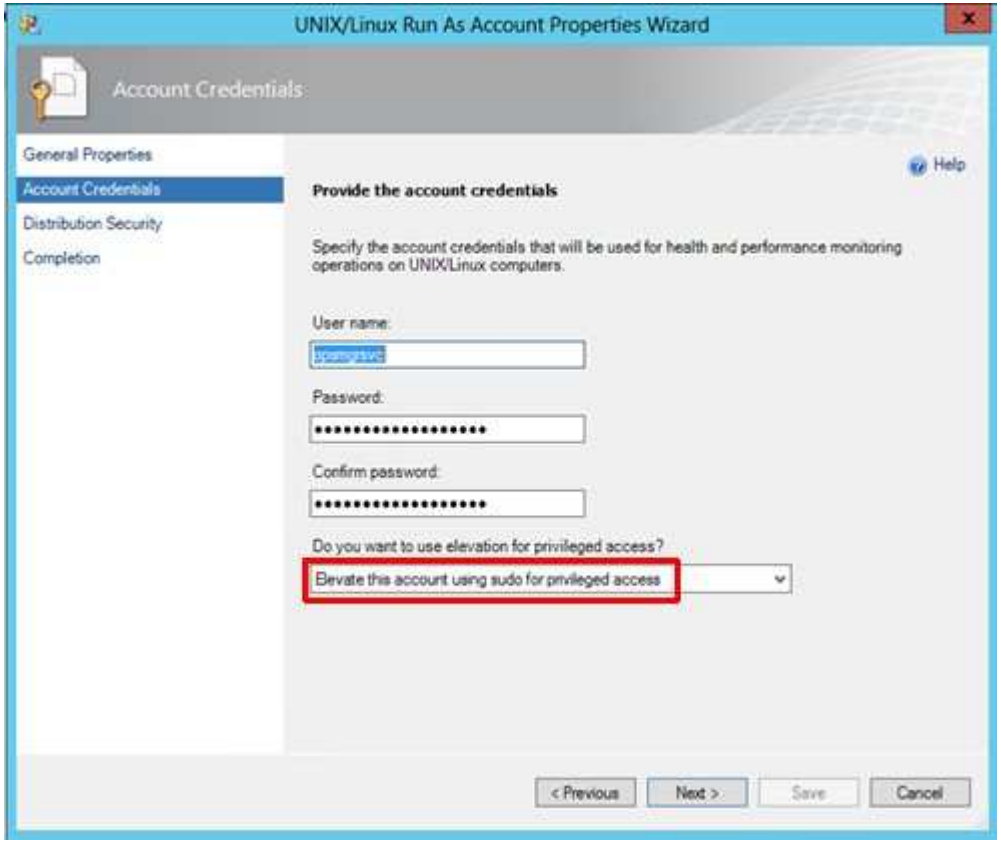


- Give the account a meaningfull priveliged display name



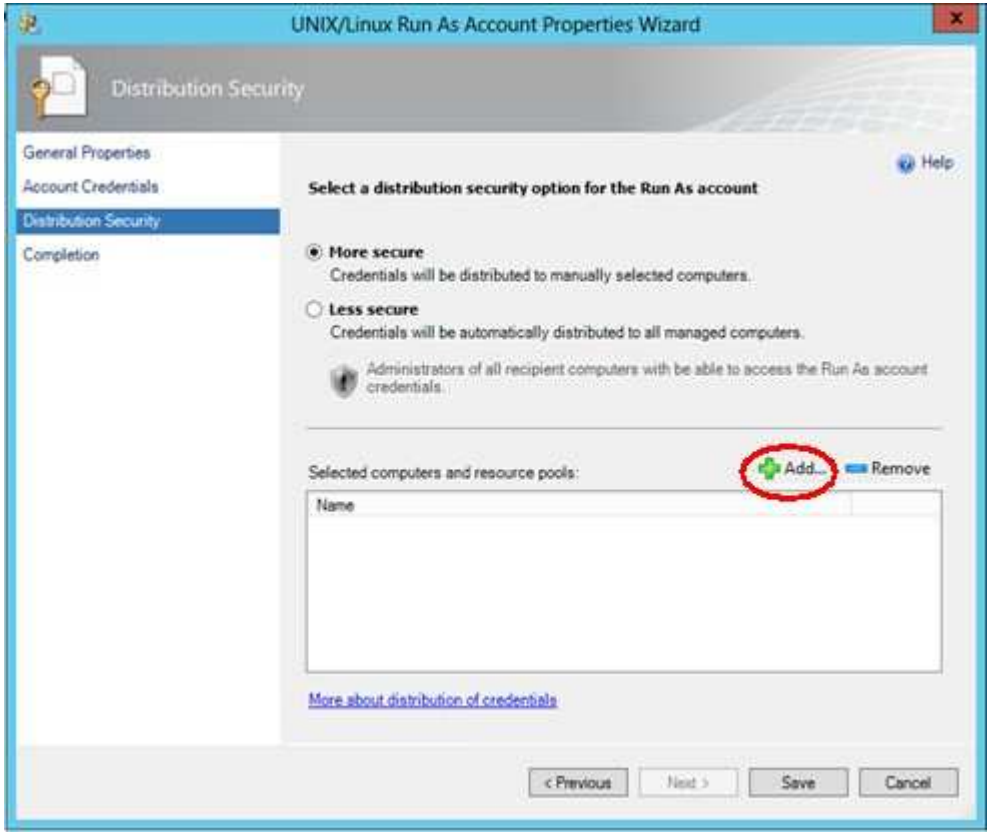
We choose "Linux Privileged Monitoring Account".

- Insert the account credentials



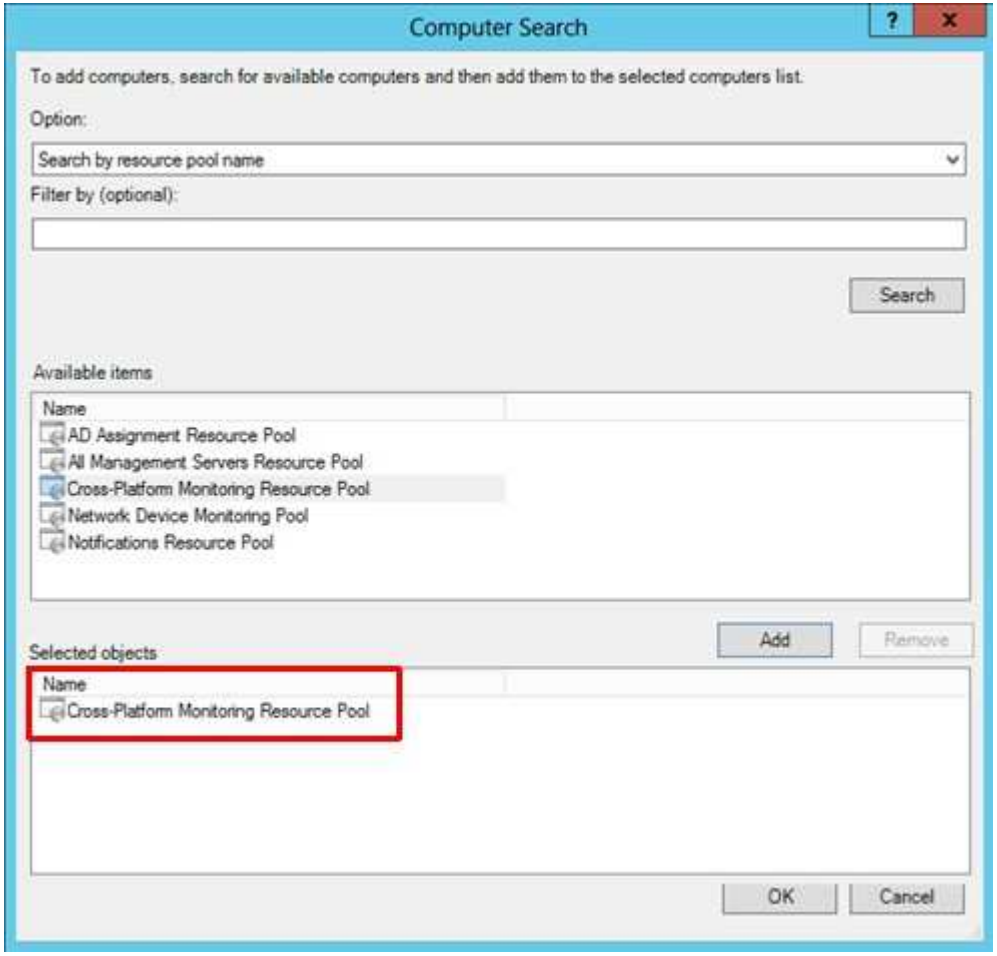
The credentials are the same as in step 4.! Please select "Elevate this account using sudo for privileged access".

- Choose distribution security option



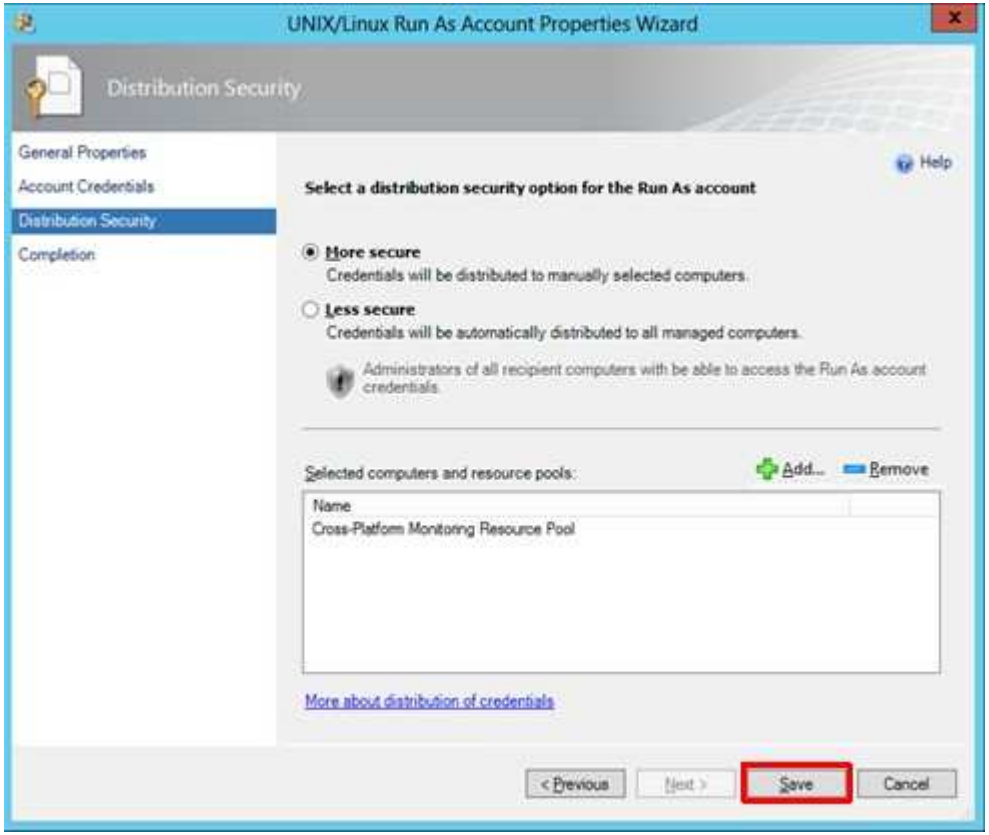
Select "More secure" and click on add to choose a resource pool.

- Add the resource pool



Now we add the resource pool "Cross-Platform Monitoring Resource Pool" which we have created in step 11). Don't forget to click OK!

- Save the settings for the second Run As account



To set up the second account just click "Save".

You can download this page as pdf file [648 kB].

On the next page I will show the SCOM-agent deployment for RedHat Enterprise Linux.

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)*