How to monitor RedHat Enterprise Linux 5 or 6 using Microsoft System Center Operations Manager (SCOM) 2012 R2

Daily business and pitfalls

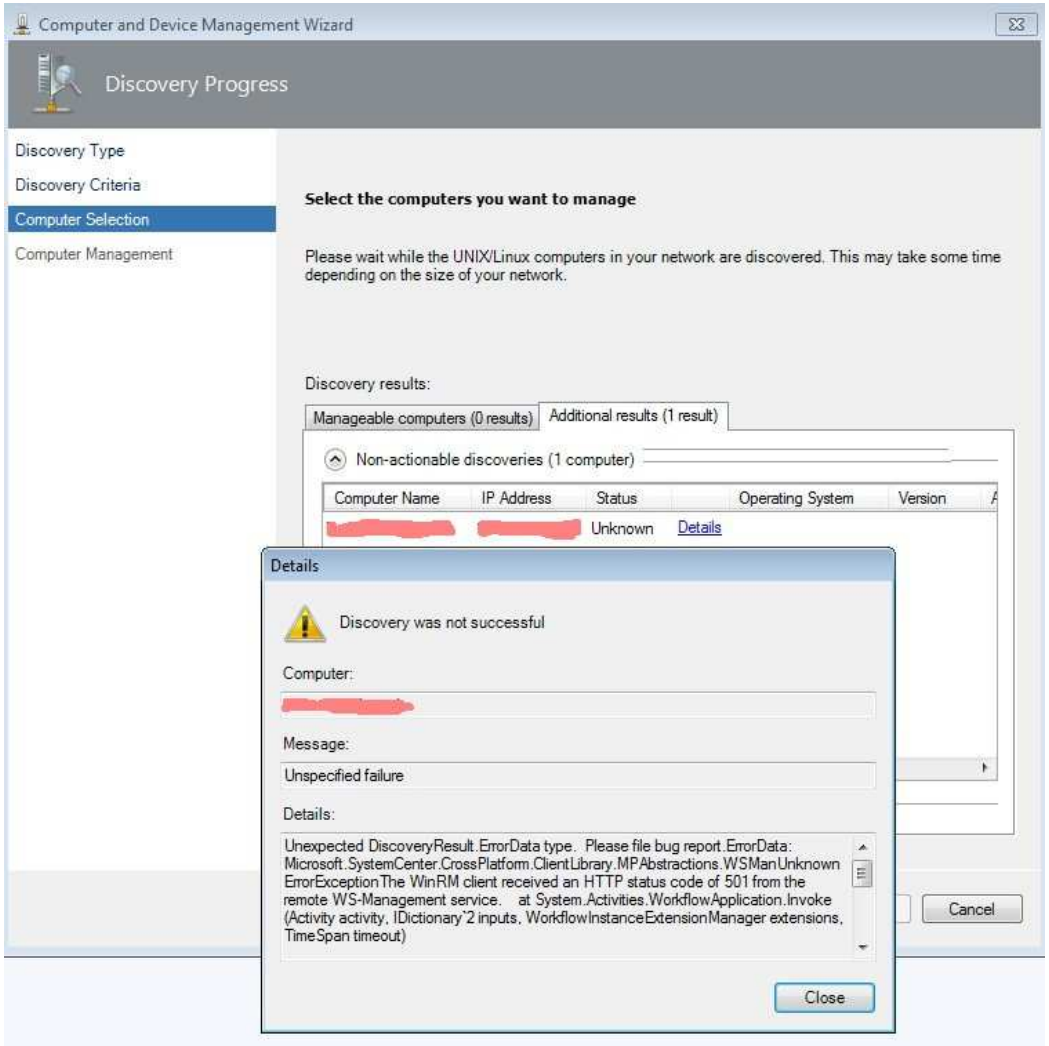
The upgrade from SCOM 2012 SP1 to 2012 R2 isn't complicated. For this reason I won't describe these steps now. But there are some improvements and changes which I will describe instead.

During the upgrade of the agents and discovery of new Linux server I've found some pitfalls. Hope you enjoy reading.

If you are a newbie, have a look about my SCOM 2012 SP1 pages.

1. The resigning certificate issue
   This issue is now completely gone and the installed agent has a valid certificate! Congratulations Microsoft you've got it.

2. Agent upgrade - issue 1
   If you see the following window, I found a rather old agent installed on the system.



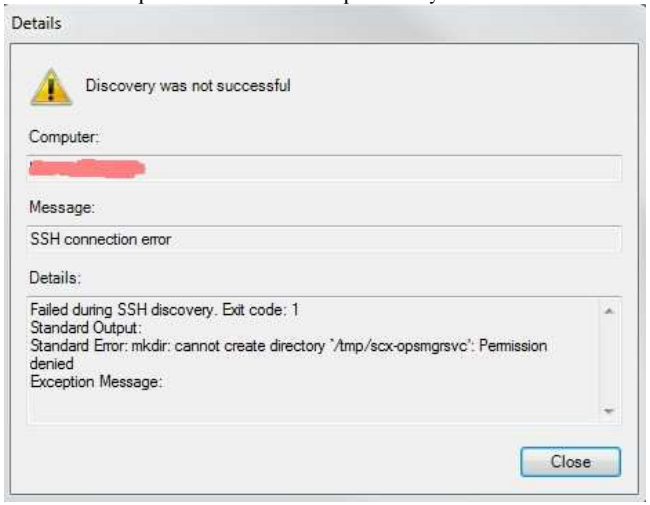
You first have to identify the agent version, delete the agent and delete the certificate directories, too:

```
[root@<hostname> ~]# rpm -q scx
scx-1.0.4-258
[root@<hostname> ~]#
[root@<hostname> ~]# rpm -e scx-1.0.4-258
Shutting down Microsoft SCX CIM Server: [  OK  ]
[root@<hostname> ~]#
[root@<hostname> ~]# rm -rf /etc/opt
[root@<hostname> ~]#
```

Now you are able to start a successful deployment of the agent

3. Agent deployment - issue 1

Sometimes the permissions of the /temp directory are not sufficient.

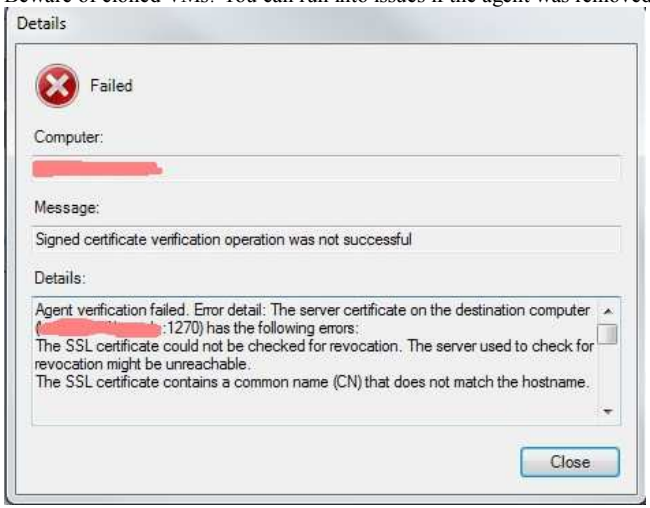


The solution is pretty easy using the "sticky bit":

```
[root@<hostname> ~]# ls -l1d /tmp
drwxr-xr-x 5 root root 4096 Jun 12 04:02 /tmp
[root@<hostname> ~]#
[root@<hostname> ~]# chmod 1777 /tmp
[root@<hostname> ~]#
[root@<hostname> ~]# ls -l1d /tmp
drwxrwxrwt 5 root root 4096 Jun 12 04:02 /tmp
[root@<hostname> ~]#
```

4. Agent upgrade - issue 2

Beware of cloned VMs! You can run into issues if the agent was removed but not the corresponding certificates:



Be sure not only the SCOM agent is removed after the cloning but the certificates directories, too:

```
[root@<hostname> ~]# rpm -q scx
???
[root@<hostname> ~]#
[root@<hostname> ~]# rpm -e ???
[root@<hostname> ~]#
[root@<hostname> ~]# rm -rf /etc/opt
[root@<hostname> ~]#
```

5. Agent upgrade or new deployment won't work properly:
   Sometimes there is a message like the following thrown in the SCOM console

   Failed to copy kit. Exit code: -1073479144
   Standard Output:
   Standard Error:
   Exception Message: An exception (-1073479144) caused the SSH command to fail -

   - This happens on the Linux side during an upgrade:

     ```
     Jun  6 08:00:10 <hostname> sudo: opsmgrsvc : TTY=unknown ; PWD=/etc/opt/microsoft/scx/ssl ; USER=root ; COMMAND=/opt/microsoft/scx/bin/scxlogfilereader -p
     Jun  6 08:05:08 <hostname> sshd[31949]: Accepted password for opsmgrsvc from <SCOM-IP> port 56475 ssh2
     Jun  6 08:05:08 <hostname> sshd[31949]: pam_unix(sshd:session): session opened for user opsmgrsvc by (uid=0)
     Jun  6 08:05:09 <hostname> sshd[31949]: pam_unix(sshd:session): session closed for user opsmgrsvc
     Jun  6 08:05:10 <hostname> sudo: opsmgrsvc : TTY=unknown ; PWD=/etc/opt/microsoft/scx/ssl ; USER=root ; COMMAND=/opt/microsoft/scx/bin/scxlogfilereader -p
     ```

   - This happens on the Linux side during a new installation:

     ```
     Jun  6 08:51:28 <hostname> sshd[32684]: Accepted password for opsmgrsvc from <SCOM-IP> port 58727 ssh2
     Jun  6 08:51:28 <hostname> sshd[32684]: pam_unix(sshd:session): session opened for user opsmgrsvc by (uid=0)
     Jun  6 08:51:28 <hostname> sshd[32684]: pam_unix(sshd:session): session closed for user opsmgrsvc
     Jun  6 08:51:29 <hostname> sshd[32714]: Accepted password for opsmgrsvc from <SCOM-IP> port 58728 ssh2
     Jun  6 08:51:29 <hostname> sshd[32714]: pam_unix(sshd:session): session opened for user opsmgrsvc by (uid=0)
     Jun  6 08:51:29 <hostname> sshd[32718]: subsystem request for sftp
     Jun  6 08:51:29 <hostname> sshd[32714]: pam_unix(sshd:session): session closed for user opsmgrsvc
     Jun  6 08:51:29 <hostname> sshd[32742]: Accepted password for opsmgrsvc from <SCOM-IP> port 58729 ssh2
     Jun  6 08:51:29 <hostname> sshd[32742]: pam_unix(sshd:session): session opened for user opsmgrsvc by (uid=0)
     Jun  6 08:51:29 <hostname> sshd[32742]: pam_unix(sshd:session): session closed for user opsmgrsvc
     Jun  6 08:51:29 <hostname> sshd[302]: Accepted password for opsmgrsvc from <SCOM-IP> port 58195 ssh2
     Jun  6 08:51:29 <hostname> sshd[302]: pam_unix(sshd:session): session opened for user opsmgrsvc by (uid=0)
     Jun  6 08:51:29 <hostname> sudo: opsmgrsvc : TTY=unknown ; PWD=/home/opsmgrsvc ; USER=root ; COMMAND=/bin/sh -c sh /tmp/scx-opsmgrsvc/GetOSVersion.sh; EC=$?; rm -rf /tmp
     Jun  6 08:51:29 <hostname> sshd[302]: pam_unix(sshd:session): session closed for user opsmgrsvc
     Jun  6 08:51:38 <hostname> sshd[353]: Accepted password for opsmgrsvc from <SCOM-IP> port 58730 ssh2
     Jun  6 08:51:38 <hostname> sshd[353]: pam_unix(sshd:session): session opened for user opsmgrsvc by (uid=0)
     Jun  6 08:51:38 <hostname> sshd[353]: pam_unix(sshd:session): session closed for user opsmgrsvc
     ```

   The only known solution to this issue is to repeat the agent upgrade/deployment serveral times. Normaly it will be successfull after the second or thrid attempt! Crazy isn't it? If you dont't want to go this strange way, you can deploy the agent manualy by copying and excetuting the rpm -U ... command.

6. Log of a fresh discovery and deployment:

   ```
   Jun  6 10:54:14 <hostname> sshd[6773]: Accepted password for opsmgrsvc from <SCOM-IP> port 63278 ssh2
   Jun  6 10:54:14 <hostname> sshd[6773]: pam_unix(sshd:session): session opened for user opsmgrsvc by (uid=0)
   Jun  6 10:54:14 <hostname> sshd[6773]: pam_unix(sshd:session): session closed for user opsmgrsvc
   Jun  6 10:54:15 <hostname> sshd[6803]: Accepted password for opsmgrsvc from <SCOM-IP> port 63279 ssh2
   Jun  6 10:54:15 <hostname> sshd[6803]: pam_unix(sshd:session): session opened for user opsmgrsvc by (uid=0)
   ```

```
Jun  6 10:54:15 <hostname> sshd[6807]: subsystem request for sftp
Jun  6 10:54:15 <hostname> sshd[6803]: pam_unix(sshd:session): session closed for user opsmgrsvc
Jun  6 10:54:15 <hostname> sshd[6831]: Accepted password for opsmgrsvc from <SCOM-IP> port 63280 ssh2
Jun  6 10:54:15 <hostname> sshd[6831]: pam_unix(sshd:session): session opened for user opsmgrsvc by (uid=0)
Jun  6 10:54:15 <hostname> sshd[6831]: pam_unix(sshd:session): session closed for user opsmgrsvc
Jun  6 10:54:16 <hostname> sshd[6859]: Accepted password for opsmgrsvc from <SCOM-IP> port 63281 ssh2
Jun  6 10:54:16 <hostname> sshd[6859]: pam_unix(sshd:session): session opened for user opsmgrsvc by (uid=0)
Jun  6 10:54:16 <hostname> sudo: opsmgrsvc : TTY=unknown ; PWD=/home/opsmgrsvc ; USER=root ; COMMAND=/bin/sh -c sh /tmp/scx-opsmgrsvc/GetOSVersion.sh; EC=$?; rm -rf /tmp/scx
Jun  6 10:54:16 <hostname> sshd[6859]: pam_unix(sshd:session): session closed for user opsmgrsvc
Jun  6 10:54:20 <hostname> sshd[6910]: Accepted password for opsmgrsvc from <SCOM-IP> port 52662 ssh2
Jun  6 10:54:20 <hostname> sshd[6910]: pam_unix(sshd:session): session opened for user opsmgrsvc by (uid=0)
Jun  6 10:54:20 <hostname> sshd[6910]: pam_unix(sshd:session): session closed for user opsmgrsvc
Jun  6 10:54:20 <hostname> sshd[6949]: Accepted password for opsmgrsvc from <SCOM-IP> port 52673 ssh2
Jun  6 10:54:20 <hostname> sshd[6949]: pam_unix(sshd:session): session opened for user opsmgrsvc by (uid=0)
Jun  6 10:54:20 <hostname> sshd[6953]: subsystem request for sftp
Jun  6 10:54:21 <hostname> sshd[6949]: pam_unix(sshd:session): session closed for user opsmgrsvc
Jun  6 10:54:21 <hostname> sshd[6978]: Accepted password for opsmgrsvc from <SCOM-IP> port 52687 ssh2
Jun  6 10:54:21 <hostname> sshd[6978]: pam_unix(sshd:session): session opened for user opsmgrsvc by (uid=0)
Jun  6 10:54:21 <hostname> sshd[6978]: pam_unix(sshd:session): session closed for user opsmgrsvc
Jun  6 10:54:21 <hostname> sshd[7009]: Accepted password for opsmgrsvc from <SCOM-IP> port 52688 ssh2
Jun  6 10:54:21 <hostname> sshd[7009]: pam_unix(sshd:session): session opened for user opsmgrsvc by (uid=0)
Jun  6 10:54:21 <hostname> sudo: opsmgrsvc : TTY=unknown ; PWD=/home/opsmgrsvc ; USER=root ; COMMAND=/bin/sh -c /bin/rpm -U --force /tmp/scx-opsmgrsvc/scx-1.5.1-112 rhel.5.x
Jun  6 10:54:22 <hostname> sshd[7009]: pam_unix(sshd:session): session closed for user opsmgrsvc
Jun  6 10:54:23 <hostname> sshd[7095]: Accepted password for opsmgrsvc from <SCOM-IP> port 63287 ssh2
Jun  6 10:54:23 <hostname> sshd[7095]: pam_unix(sshd:session): session opened for user opsmgrsvc by (uid=0)
Jun  6 10:54:23 <hostname> sudo: opsmgrsvc : TTY=unknown ; PWD=/home/opsmgrsvc ; USER=root ; COMMAND=/bin/sh -c cat /etc/opt/microsoft/scx/ssl/scx.pem
Jun  6 10:54:23 <hostname> sshd[7095]: pam_unix(sshd:session): session closed for user opsmgrsvc
Jun  6 10:54:24 <hostname> sshd[7134]: Accepted password for opsmgrsvc from <SCOM-IP> port 63288 ssh2
Jun  6 10:54:24 <hostname> sshd[7134]: pam_unix(sshd:session): session opened for user opsmgrsvc by (uid=0)
Jun  6 10:54:24 <hostname> sshd[7134]: pam_unix(sshd:session): session closed for user opsmgrsvc
Jun  6 10:54:24 <hostname> sshd[7167]: Accepted password for opsmgrsvc from <SCOM-IP> port 63289 ssh2
Jun  6 10:54:24 <hostname> sshd[7167]: pam_unix(sshd:session): session opened for user opsmgrsvc by (uid=0)
Jun  6 10:54:24 <hostname> sshd[7171]: subsystem request for sftp
Jun  6 10:54:24 <hostname> sshd[7167]: pam_unix(sshd:session): session closed for user opsmgrsvc
Jun  6 10:54:24 <hostname> sshd[7195]: Accepted password for opsmgrsvc from <SCOM-IP> port 63291 ssh2
Jun  6 10:54:24 <hostname> sshd[7195]: pam_unix(sshd:session): session opened for user opsmgrsvc by (uid=0)
Jun  6 10:54:25 <hostname> sshd[7195]: pam_unix(sshd:session): session closed for user opsmgrsvc
Jun  6 10:54:25 <hostname> sshd[7224]: Accepted password for opsmgrsvc from <SCOM-IP> port 63292 ssh2
Jun  6 10:54:25 <hostname> sshd[7224]: pam_unix(sshd:session): session opened for user opsmgrsvc by (uid=0)
Jun  6 10:54:25 <hostname> sudo: opsmgrsvc : TTY=unknown ; PWD=/home/opsmgrsvc ; USER=root ; COMMAND=/bin/sh -c cp /tmp/scx-opsmgrsvc/scx.pem /etc/opt/microsoft/scx/ssl/scx.p
Jun  6 10:54:25 <hostname> sshd[7224]: pam_unix(sshd:session): session closed for user opsmgrsvc
Jun  6 11:06:04 <hostname> sudo: opsmgrsvc : TTY=unknown ; PWD=/var/opt/microsoft/scx/run ; USER=root ; COMMAND=/opt/microsoft/scx/bin/scxlogfilereader -p
```

7. Alerting about Daemons
   SCOM complains about daemons not running. That seems to be OK but not every RHEL server is used as NFS server. We have to work around this issue.
   - audit and syslog

> *Source: Red Hat Enterprise Linux Server release 5.3 (Tikanga)*
> *Name: Audit daemon is not running*

> *Source: Red Hat Enterprise Linux Server release 6.4 (Santiago)*
> *Name: Syslog daemon is not running*

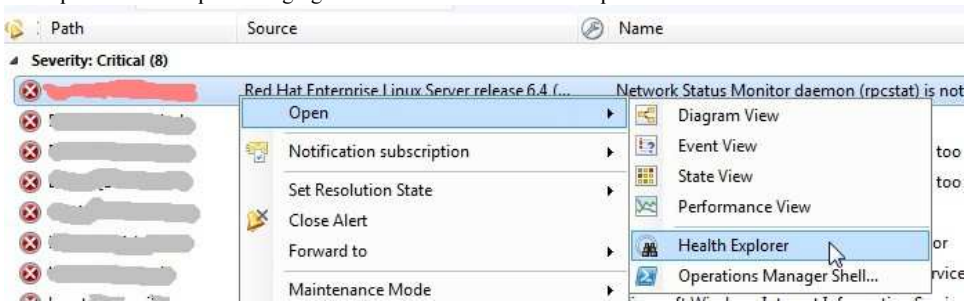
Running both daemons (audit and syslog) make sense, so we need them to get up and running. Our systems are in runlevel 3 so we have to do a little bit additional work:

```
[root@<hostname> ~]# service auditd status
```

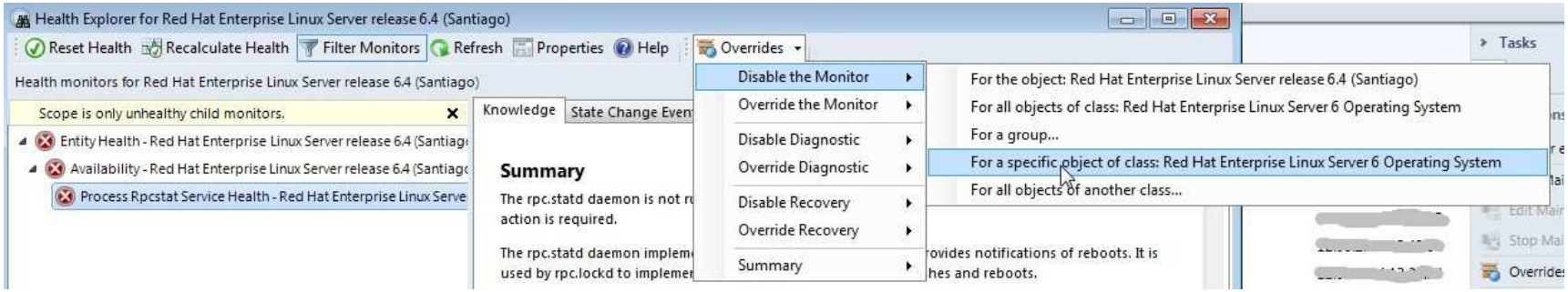
```
auditd is stopped
[root@<hostname> ~]#
[root@<hostname> ~]# chkconfig --list auditd
auditd          0:off   1:off   2:on    3:off   4:on    5:on    6:off
[root@<hostname> ~]#
[root@<hostname> ~]# chkconfig --level 2345 auditd on
[root@<hostname> ~]#
[root@<hostname> ~]# chkconfig --list auditd
auditd          0:off   1:off   2:on    3:on    4:on    5:on    6:off
[root@<hostname> ~]#
[root@<hostname> ~]# service auditd restart
Stopping auditd:                                           [FAILED]
Starting auditd:                                           [  OK  ]
[root@<hostname> ~]#
[root@<hostname> ~]# chkconfig --list rsyslog
rsyslog         0:off   1:off   2:on    3:off   4:on    5:on    6:off
[root@<hostname> ~]#
[root@<hostname> ~]# chkconfig --level 2345 rsyslog on
[root@<hostname> ~]#
[root@<hostname> ~]# chkconfig --list rsyslog
rsyslog         0:off   1:off   2:on    3:on    4:on    5:on    6:off
[root@<hostname> ~]#
[root@<hostname> ~]# service rsyslog restart
Shutting down system logger:                               [FAILED]
Starting system logger:                                    [  OK  ]
[root@<hostname> ~]#
```

- rpc and NFS related daemons
  If your server doesn't mount any NFS shares or act as a NFS server you don't have the needs to run these daemons!
  The SCOM server(s) doesn't have the intelligence to recognize that there are no exports or autfs or NFS-Shares on the Linux server and complains for this reason all the time about missing daemons.
  Because this is annoying we have to switch of the alerting for every server which doesn't need the daemons.
  Here is a link about that and I will show some images.

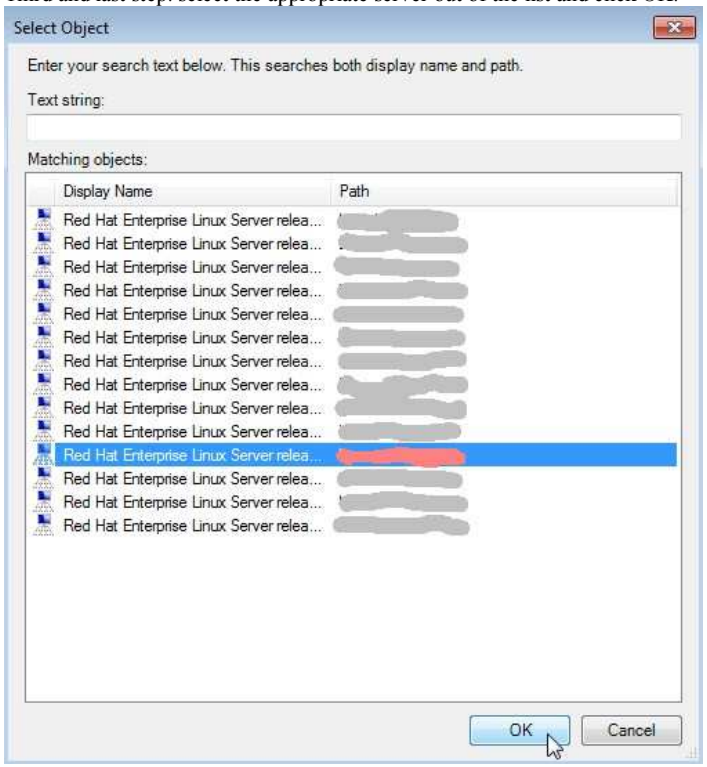
  First open in the alert pane using right mouse button the "Health Explorer"



  Second select the alarm and select "For a specific object of class" out of the "Disable the Monitor" item.



Third and last step: select the appropriate server out of the list and click OK.

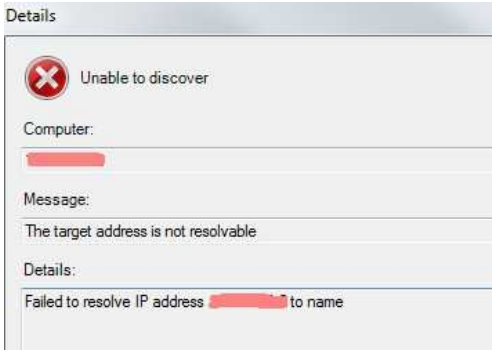


- Complaining about other daemons
  There are a lot of more daemons SCOM complains about. For example the ACPI daemon.
  To have the philosophy in mind that just the daemons have to run which are necessary for the workload, your Linux admin might have disabled a lot of them.
  For this reason we have to get rid off the SCOM alerting, please follow the steps above.

8. Reverse DNS lookup doesn't work properly:
   SCOM needs a full functional DNS lookup. If there is any misconfiguration you get errors during the agent deployment.

Unable to discover

Message: The target address is not resolvable
Details: Failed to resolve IP address <server-IP> to name.



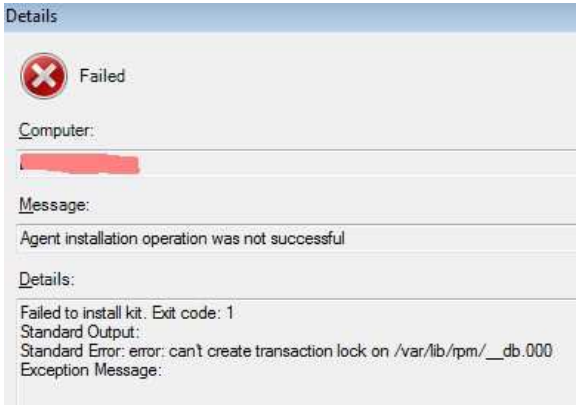
9. Firewall between SCOM and server:
   If there is any firewall between the SCOM servers and the server to manage the appropriate ports have to be opened. In our scenario the ports 22 and 1270.

Unable to discover
Message: The target address is unreachable
Details: WinRM cannot complete the operation. Verify...

10. Sudo permissions not sufficient:
    If the following message occurs the user opsmgrsvc has not the permissions to install the SCOM agent scx package. Maybe there was something wrong with /etc/sudoers.

Failed
Message: Agent installation operation was not successful
Details:
Failed to install kit. Exit code: 1
Satndard Output:
Standard Error: can't create transaction lock on /var/lib/rpm/__db.000

Exception Message:



11. Agent deployment on a virtual appliance
    Sometimes it's a must that an virtual appliance must have been monitored. I tried to deploy the SCOM agent on VMware vCenter Log Insight, these are my results.
    First step is to configure the appliance for the user opsmgrsvc:

```
[root@<hostname> ~]# useradd -c "SCOM service account" -u 550 -m opsmgrsvc
[root@<hostname> ~]#
[root@<hostname> ~]# passwd opsmgrsvc
[root@<hostname> ~]#
[root@<hostname> ~]# usermod -G wheel opsmgrsvc
[root@<hostname> ~]#
```

    We have to add opsmgrsvc to the group wheel, because in /etc/ssh/sshd_config the AllowGroup directive permits the login only for members of wheel!
    Next step is to configure sudo. You have to edit the lines as shown below:

```
[root@<hostname> ~]# visudo
...
# Cmnd alias specification

# Defaults specification
Defaults visiblepw
Defaults:opsmgrsvc !requiretty

# Prevent environment variables from influencing programs in an
...
# User privilege specification
root ALL=(ALL) ALL
opsmgrsvc ALL=(root) NOPASSWD: ALL

# Uncomment to allow people in group wheel to run all commands
...
# Same thing without a password
%wheel ALL=(ALL) NOPASSWD: ALL

# Samples
...
```

Now we have to fetch the SCOM Agent out of our SCOM Server. The virtual appliance is based on SuSE Linux Enterprise (SLES) 11.2 64-bit.

```
cd "%ProgramFiles%\System Center 2012\Operations Manager\Server\AgentManagement\UnixAgents\DownloadedKits"
```

```
    Directory: C:\Program Files\Microsoft System Center 2012 R2\Operations
    Manager\Server\AgentManagement\UnixAgents\DownloadedKits


Mode                 LastWriteTime     Length Name
----                 -------------     ------ ----
-a---        05.06.2014     14:54    4029875 scx-1.5.1-112.rhel.5.x64.rpm
-a---        05.06.2014     14:54    4084091 scx-1.5.1-112.rhel.5.x86.rpm
-a---        05.06.2014     14:54    3850487 scx-1.5.1-112.rhel.6.x64.rpm
-a---        05.06.2014     14:54    3850336 scx-1.5.1-112.rhel.6.x86.rpm
-a---        13.06.2014     09:39    2362824 scx-1.5.1-112.sles.11.x64.rpm
-a---        13.06.2014     09:39    2370143 scx-1.5.1-112.sles.11.x86.rpm
-a---        05.06.2014     14:54    7379702 scx-1.5.1-112.universald.1.x64.deb
-a---        05.06.2014     14:54    7393204 scx-1.5.1-112.universald.1.x86.deb
-a---        05.06.2014     14:54    8050400 scx-1.5.1-112.universalr.1.x64.rpm
-a---        05.06.2014     14:54    8169273 scx-1.5.1-112.universalr.1.x86.rpm
```

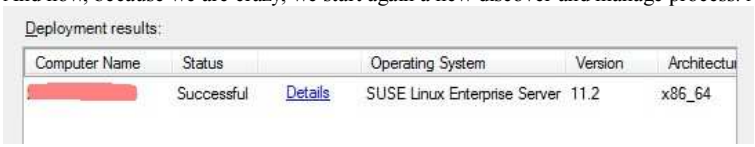
We have to fetch scx-1.5.1-112.sles.11.x64.rpm and copy it to the virtual appliance. If this is done perform an installation:

```
[root@<hostname> ~]# rpm -U scx-1.5.1-112.sles.11.x64.rpm
```

Now we can start the discover process, which will be successful. After you have selected the Manage button there might be some errors.
The preferred way is now to delete the SCOM agent! As you remember from former chapters the certificates won't be deleted during this action. That's what we need!

```
[root@<hostname> ~]# rpm -e scx-1.5.1-112
```

And now, because we are crazy, we start again a new discover and manage process. And voila:



On SLES we have to look at /var/log/messages for the deployment logfiles:

```
[root@<hostname> ~]# tail -f /var/log/messages
2014-06-17T09:49:31+02:00 <hostname> sshd[9146]: Accepted password for opsmgrsvc from <SCOM-IP> port 52575 ssh2
2014-06-17T09:49:32+02:00 <hostname> sshd[9183]: Accepted password for opsmgrsvc from <SCOM-IP> port 52576 ssh2
2014-06-17T09:49:32+02:00 <hostname> sshd[9204]: subsystem request for sftp
2014-06-17T09:49:34+02:00 <hostname> sshd[9236]: Accepted password for opsmgrsvc from <SCOM-IP> port 52577 ssh2
2014-06-17T09:49:35+02:00 <hostname> sshd[9271]: Accepted password for opsmgrsvc from <SCOM-IP> port 59343 ssh2
2014-06-17T09:49:35+02:00 <hostname> sudo: opsmgrsvc : TTY=unknown ; PWD=/home/opsmgrsvc ; USER=root ; COMMAND=/usr/bin/sh -c sh /tmp/scx-opsmgrsvc/GetOSVersion.sh; EC=$?; r
2014-06-17T09:49:59+02:00 <hostname> sshd[9371]: Accepted password for opsmgrsvc from <SCOM-IP> port 59475 ssh2
2014-06-17T09:50:00+02:00 <hostname> sshd[9408]: Accepted password for opsmgrsvc from <SCOM-IP> port 59476 ssh2
2014-06-17T09:50:00+02:00 <hostname> sshd[9412]: subsystem request for sftp
2014-06-17T09:50:01+02:00 <hostname> sshd[9443]: Accepted password for opsmgrsvc from 172.17.241.24 port 59477 ssh2
2014-06-17T09:50:02+02:00 <hostname> sshd[9478]: Accepted password for opsmgrsvc from <SCOM-IP> port 52884 ssh2
2014-06-17T09:50:03+02:00 <hostname> sudo: opsmgrsvc : TTY=unknown ; PWD=/home/opsmgrsvc ; USER=root ; COMMAND=/usr/bin/sh -c /bin/rpm -U --force /tmp/scx-opsmgrsvc/scx-1.5.
2014-06-17T09:52:51+02:00 <hostname> sudo: opsmgrsvc : TTY=unknown ; PWD=/var/opt/microsoft/scx/run ; USER=root ; COMMAND=/opt/microsoft/scx/bin/scxlogfilereader -p
```

Yep, looks good but after some minutes there will be a weired system behavior. We've got critical alerts and strange /var/log/message entries:

```
[root@<hostname> ~]# tail -f /var/log/messages
2014-06-17T09:57:25+02:00 <hostname> omiserver: pam_tally(omi:auth): unexpected response from failed conversation function
2014-06-17T09:57:25+02:00 <hostname> omiserver: pam_tally(omi:auth): conversation failed
2014-06-17T09:57:25+02:00 <hostname> omiserver: pam_tally(omi:auth): user opsmgrsvc (550) tally 4, deny 3
2014-06-17T09:58:06+02:00 <hostname> omiserver: pam_tally(omi:auth): unexpected response from failed conversation function
2014-06-17T09:58:06+02:00 <hostname> omiserver: pam_tally(omi:auth): conversation failed
2014-06-17T09:58:06+02:00 <hostname> omiserver: pam_tally(omi:auth): user opsmgrsvc (550) tally 5, deny 3
2014-06-17T09:58:52+02:00 <hostname> omiserver: pam_tally(omi:auth): unexpected response from failed conversation function
2014-06-17T09:58:52+02:00 <hostname> omiserver: pam_tally(omi:auth): conversation failed
2014-06-17T09:58:52+02:00 <hostname> omiserver: pam_tally(omi:auth): user opsmgrsvc (550) tally 6, deny 3
2014-06-17T09:59:54+02:00 <hostname> omiserver: pam_tally(omi:auth): unexpected response from failed conversation function
2014-06-17T09:59:54+02:00 <hostname> omiserver: pam_tally(omi:auth): conversation failed
```

The SCOM agent does some things in the background which results in invalid logins. These are fetched by the pam_tally module which results in disabling the opsmgrsvc account!
The only solution I've found is to write a wrapper script which resets the count of invalid logins to keep the SCOM agent running. Here it goes:

```
[root@<hostname> ~]# cd /opt/microsoft/scx/bin
[root@<hostname> ~]#
[root@<hostname> ~]# cp -p scxlogfilereader scxlogfilereader.ms
[root@<hostname> ~]#
```

Create now a short shell script::

```
[root@<hostname> ~]# vi scxlogfilereader.new
!#/bin/sh
/sbin/pam_tally --reset
/bin/sleep 1
./scxlogfilereader.ms -p
/bin/sleep 1
/sbin/pam_tally --reset
```

For our conveniance I create a symbolic link which is named like the original file.

```
[root@<hostname> ~]# rm scxlogfilereader
[root@<hostname> ~]#
[root@<hostname> ~]# ln -s scxlogfilereader.new scxlogfilereader
[root@<hostname> ~]#
[root@<hostname> ~]# ls -la
total 3788
drwxr-xr-x 3 root root    4096 Jun 17 11:16 .
drwxr-xr-x 4 root root    4096 Jun 17 09:50 ..
-rwxr-xr-x 1 root root 1238033 Mar 22 01:32 omiagent
-rwxr-xr-x 1 root root 1969150 Mar 22 01:32 omiserver
lrwxrwxrwx 1 root root      20 Jun 17 11:16 scxlogfilereader -> scxlogfilereader.new
-rwxr-xr-x 1 root root  631746 Mar 22 01:34 scxlogfilereader.ms
-rwxr-xr-x 1 root root     109 Jun 17 11:12 scxlogfilereader.new
-rw-r--r-- 1 root root     193 Mar 22 01:35 setup.sh
drwxr-xr-x 2 root root    4096 Jun 17 09:50 tools
[root@<hostname> ~]#
```

As a result of the efforts the logfile should now look fine as the one below:

```
[root@<hostname> ~]# tail -f /var/log/messages
2014-06-17T12:02:52+02:00 <hostname> sudo: opsmgrsvc : TTY=unknown ; PWD=/var/opt/microsoft/scx/run ; USER=root ; COMMAND=/opt/microsoft/scx/bin/scxlogfilereader -p
2014-06-17T12:07:52+02:00 <hostname> sudo: opsmgrsvc : TTY=unknown ; PWD=/var/opt/microsoft/scx/run ; USER=root ; COMMAND=/opt/microsoft/scx/bin/scxlogfilereader -p
```

```
2014-06-17T12:12:52+02:00 <hostname> sudo: opsmgrsvc : TTY=unknown ; PWD=/var/opt/microsoft/scx/run ; USER=root ; COMMAND=/opt/microsoft/scx/bin/scxlogfilereader -p
2014-06-17T12:17:52+02:00 <hostname> sudo: opsmgrsvc : TTY=unknown ; PWD=/var/opt/microsoft/scx/run ; USER=root ; COMMAND=/opt/microsoft/scx/bin/scxlogfilereader -p
2014-06-17T12:22:52+02:00 <hostname> sudo: opsmgrsvc : TTY=unknown ; PWD=/var/opt/microsoft/scx/run ; USER=root ; COMMAND=/opt/microsoft/scx/bin/scxlogfilereader -p
2014-06-17T12:27:52+02:00 <hostname> sudo: opsmgrsvc : TTY=unknown ; PWD=/var/opt/microsoft/scx/run ; USER=root ; COMMAND=/opt/microsoft/scx/bin/scxlogfilereader -p
```

You can download this page as pdf file [349 kB].

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

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)*