## How to configure Microsoft System Center Operations Manager (SCOM) 2012 R2 as SNMP trap receiver for VMware vCenter on MS Windows?

One of the most interesting and very often asked things is how do I configure SCOM 2012 as a SNMP trap receiver? The solution isn't really easy and a lot of SNMP basics are needed.

Again Microsoft need to do some homework to make some things much more easier and improve SCOM regarding SNMP traps. But first I would like to thank some people for their good documentation which pushed me to the right direction:

- Stefan Roth
- Justin Cook
- Dave Murphy
- Marthijn van Rheenen
- rob1974

I've done some investigations of our System Center Operations Manager 2012 R2 update rollup 2 installation and here are my findings:

1. If your SNMP trap sending device isn't able to act as an typical SNMP agent, means that there can be an SNMP daemon running, you never ever get this device discovered by SCOM! That's the fact!
2. You should force a discovery for a specific SNMP version. If the device is discovered as version 2(c) device, SCOM ignores every trap from this device if it is not a version 2 trap!

To get more familiar with the SCOM SNMP network device discovery I build following scenario:

Provisioning of a RedHat Enterprise Linux 5 VM and installation of the net-snmp suite. This software package delivered a full featured SNMP daemon (snmpd) and additionally a snmptrap daemon (snmptrapd). All daemons (aka services) are highly configurable and there is very good documentation.

1. Enable discovering as SNMP v1 device
   To act as a SNMP version 1 device is easy to configure. Just comment the v2c line.

```
[root@<hostname> ~]# vi /etc/snmp/snmpd.conf
...
#       groupName      securityModel securityName
group   notConfigGroup v1           notConfigUser
#group   notConfigGroup v2c           notConfigUser

####
# Third, create a view for us to let the group have rights to:
...
```

2. Running the SNMP daemon
   We use the typical service call:

```
[root@<hostname> ~]# service snmpd restart
Stopping snmpd:                                            [FAILED]
Starting snmpd:                                            [  OK  ]
[root@<hostname> ~]#
```

If this is all done, don't forget to save and configure SCOM to detect the new network device. **Don't discover it as a Linux or Unix computer!**

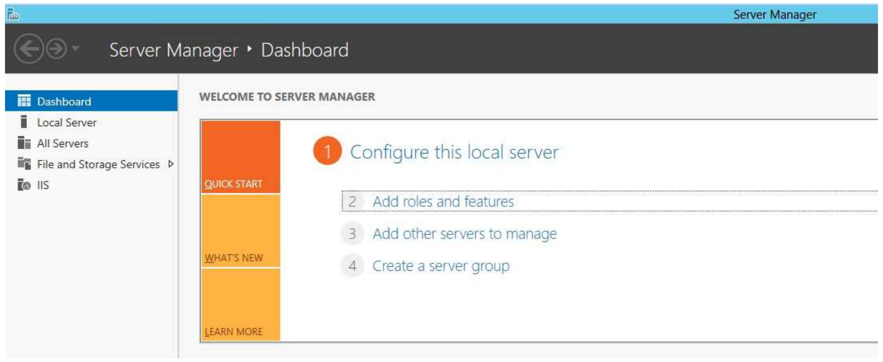
Before performing the discovery I started a port scan with nmap and found that only port 161 is opened on the SCOM 2012 installation. *This is the reason why SCOM 2012 isn't able to act as a SNMP trap receiver out of the box unless the device discovery is successful done!*

```
[root@<hostname> ~]# nmap -sU -p U:161 <FQDN-SCOM>

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2014-06-20 12:28 CEST
Interesting ports on <FQDN-SCOM> (<SCOM-IP>):
PORT    STATE         SERVICE
161/udp open|filtered snmp
MAC Address: 00:50:56:A3:xx:yy (VMWare)

Nmap finished: 1 IP address (1 host up) scanned in 0.325 seconds
[root@<hostname> ~]#
[root@<hostname> ~]# nmap -sU -p U:162 <FQDN-SCOM>

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2014-06-20 12:28 CEST
Interesting ports on <FQDN-SCOM> (<SCOM-IP>):
PORT    STATE  SERVICE
162/udp closed snmptrap
MAC Address: 00:50:56:A3:xx:yy (VMWare)

Nmap finished: 1 IP address (1 host up) scanned in 0.118 seconds
[root@<hostname> ~]#
```

But now let us configure the MS Windows Server 2012 and the SCOM 2012 R2 update rollup 2 in several separate steps.

1. **First we have to do some prerequisites on the Windows operating system**

   a. Click on Server Manager -> Dashboard -> Add roles and features



WELCOME TO SERVER MANAGER

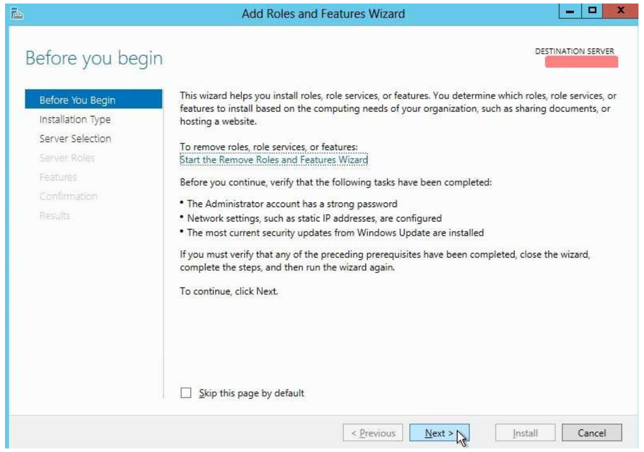
1 Configure this local server

2 Add roles and features

3 Add other servers to manage

4 Create a server group

b. Read and click next



Before you begin

DESTINATION SERVER
[redacted]

This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
Start the Remove Roles and Features Wizard

Before you continue, verify that the following tasks have been completed:

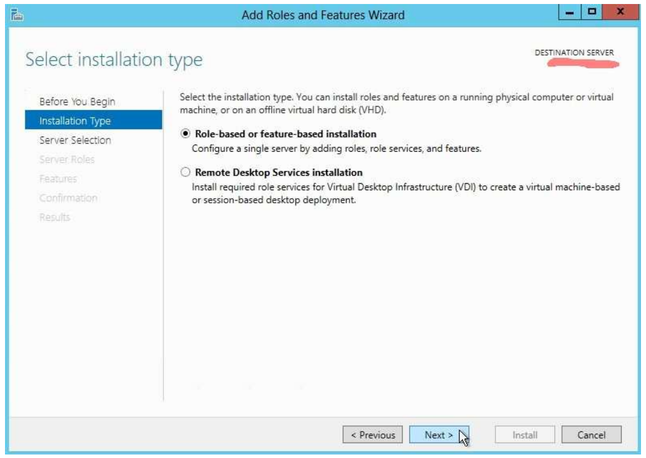
- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

☐ Skip this page by default

c. Select role-based of feature-based installation



Select installation type

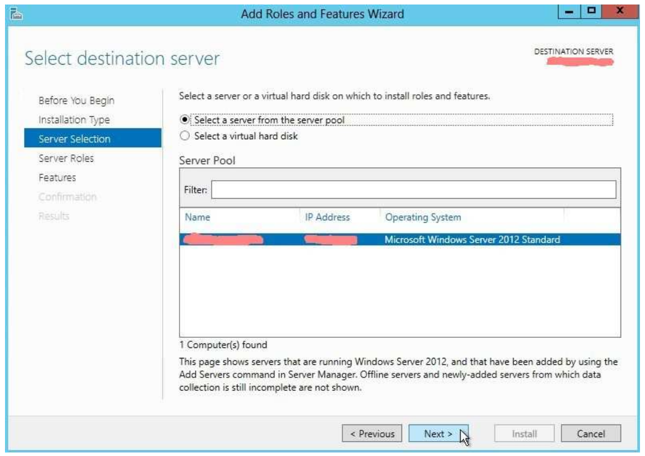
DESTINATION SERVER
[redacted]

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

[✓ **Role-based or feature-based installation**]
Configure a single server by adding roles, role services, and features.

**Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

d. Select a server from the server pool



Select destination server

DESTINATION SERVER
[redacted]

Select a server or a virtual hard disk on which to install roles and features.

● Select a server from the server pool
○ Select a virtual hard disk

Server Pool

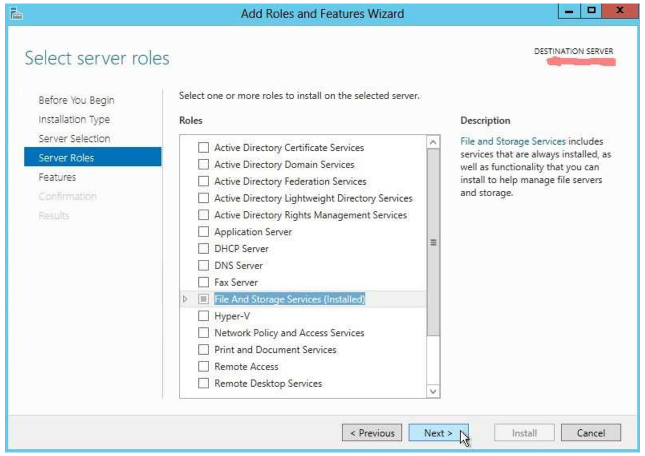
Filter:

| Name | IP Address | Operating System |
|---|---|---|
| [redacted] | [redacted] | Microsoft Windows Server 2012 Standard |

1 Computer(s) found

This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

e. Just click next



Select server roles

DESTINATION SERVER
[redacted]

Select one or more roles to install on the selected server.

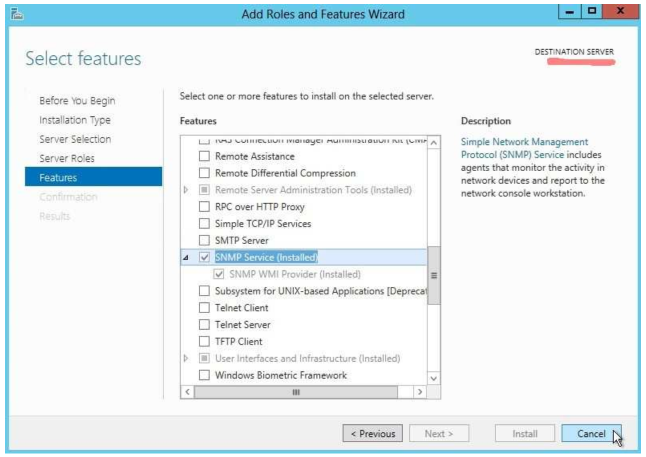
Roles

- ☐ Active Directory Certificate Services
- ☐ Active Directory Domain Services
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☐ DHCP Server
- ☐ DNS Server
- ☐ Fax Server
- ▨ File And Storage Services (Installed)
- ☐ Hyper-V
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services

Description

File and Storage Services includes services that are always installed, as well as functionality that you can install to help manage file servers and storage.

f. Check SNMP service (should be installed)



Select one or more features to install on the selected server.

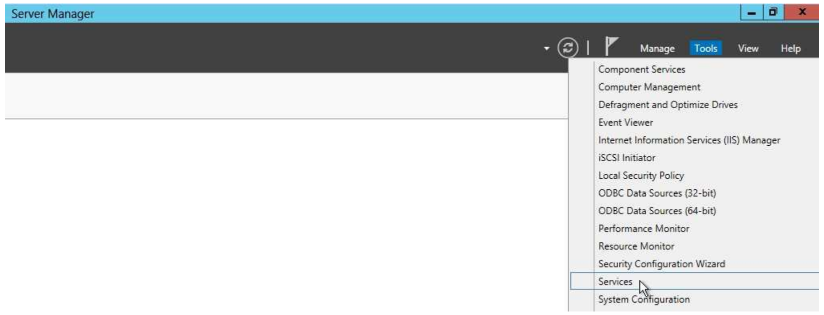
Features

- ☐ Remote Assistance
- ☐ Remote Differential Compression
- ▨ Remote Server Administration Tools (Installed)
- ☐ RPC over HTTP Proxy
- ☐ Simple TCP/IP Services
- ☐ SMTP Server
- ☑ SNMP Service (Installed)
  - ☑ SNMP WMI Provider (Installed)
- ☐ Subsystem for UNIX-based Applications [Deprecat
- ☐ Telnet Client
- ☐ Telnet Server
- ☐ TFTP Client
- ▨ User Interfaces and Infrastructure (Installed)
- ☐ Windows Biometric Framework

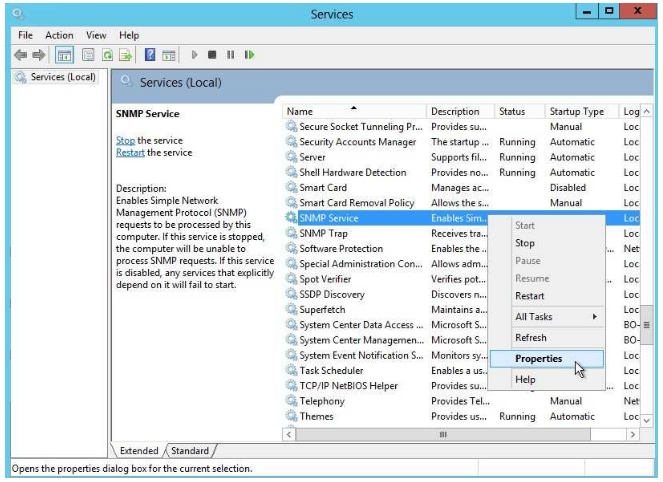
Description

Simple Network Management Protocol (SNMP) Service includes agents that monitor the activity in network devices and report to the network console workstation.

g. Click on Server Manager -> Tools -> Services



h. Click on SNMP Service -> Properties



Services (Local)

**SNMP Service**

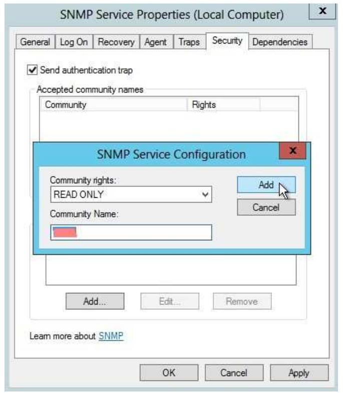
Stop the service
Restart the service

Description:
Enables Simple Network Management Protocol (SNMP) requests to be processed by this computer. If this service is stopped, the computer will be unable to process SNMP requests. If this service is disabled, any services that explicitly depend on it will fail to start.

| Name | Description | Status | Startup Type | Log |
|---|---|---|---|---|
| Secure Socket Tunneling Pr... | Provides su... | | Manual | Loc |
| Security Accounts Manager | The startup ... | Running | Automatic | Loc |
| Server | Supports fil... | Running | Automatic | Loc |
| Shell Hardware Detection | Provides no... | Running | Automatic | Loc |
| Smart Card | Manages ac... | | Disabled | Loc |
| Smart Card Removal Policy | Allows the s... | | Manual | Loc |
| SNMP Service | Enables Sim... | | | Loc |
| SNMP Trap | Receives tra... | | | Loc |
| Software Protection | Enables the ... | | ... | Net |
| Special Administration Con... | Allows adm... | | | Loc |
| Spot Verifier | Verifies pot... | | ... | Loc |
| SSDP Discovery | Discovers n... | | | Loc |
| Superfetch | Maintains a... | | | Loc |
| System Center Data Access ... | Microsoft S... | | | BO- |
| System Center Managemen... | Microsoft S... | | | BO- |
| System Event Notification S... | Monitors sy... | | | Loc |
| Task Scheduler | Enables a us... | | | Loc |
| TCP/IP NetBIOS Helper | Provides su... | | ... | Loc |
| Telephony | Provides Tel... | | Manual | Net |
| Themes | Provides us... | Running | Automatic | Loc |

Opens the properties dialog box for the current selection.

i. Set SNMP community



SNMP Service Properties (Local Computer)

General | Log On | Recovery | Agent | Traps | Security | Dependencies

☑ Send authentication trap

Accepted community names

| Community | Rights |
|---|---|

SNMP Service Configuration

Community rights: READ ONLY

Community Name: [redacted]

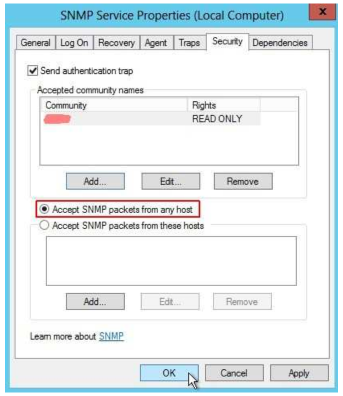
Add | Cancel

Add... | Edit... | Remove

Learn more about SNMP

OK | Cancel | Apply

j. Select accept SNMP packets from any host



SNMP Service Properties (Local Computer)

General | Log On | Recovery | Agent | Traps | Security | Dependencies

☑ Send authentication trap

Accepted community names

| Community | Rights |
|---|---|
| [redacted] | READ ONLY |

Add... | Edit... | Remove

◉ Accept SNMP packets from any host

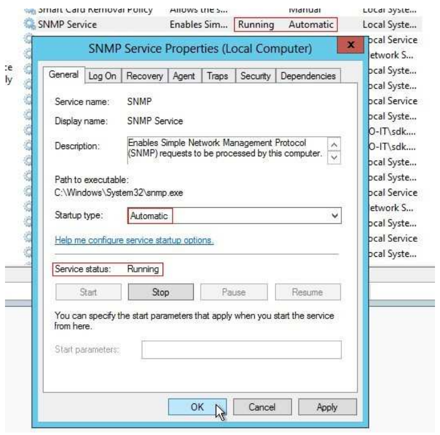
○ Accept SNMP packets from these hosts

Add... | Edit... | Remove

Learn more about SNMP

OK | Cancel | Apply

k. **SNMP Service** startup type has to be automatic and Service status has to be running



```
Smart Card Removal Policy   Allows the s...              Manual      Local Syste...
SNMP Service                Enables Sim...   Running     Automatic   Local Syste...
```

SNMP Service Properties (Local Computer)

General | Log On | Recovery | Agent | Traps | Security | Dependencies

Service name: SNMP

Display name: SNMP Service

Description: Enables Simple Network Management Protocol (SNMP) requests to be processed by this computer.

Path to executable:
C:\Windows\System32\snmp.exe

Startup type: Automatic

Help me configure service startup options.

Service status: Running

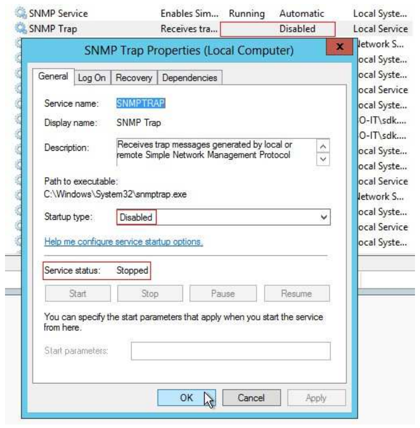
Start | Stop | Pause | Resume

You can specify the start parameters that apply when you start the service from here.

Start parameters:

OK | Cancel | Apply

l. **SNMP Trap** startup type has to be disabled and Service status has to be stopped


SNMP Service | Enables Sim... | Running | Automatic | Local Syste...
SNMP Trap | Receives tra... | | Disabled | Local Service

**SNMP Trap Properties (Local Computer)**

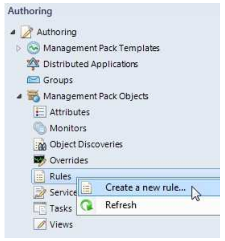
General | Log On | Recovery | Dependencies

Service name: SNMPTRAP
Display name: SNMP Trap
Description: Receives trap messages generated by local or remote Simple Network Management Protocol
Path to executable:
C:\Windows\System32\snmptrap.exe
Startup type: Disabled
Help me configure service startup options.
Service status: Stopped

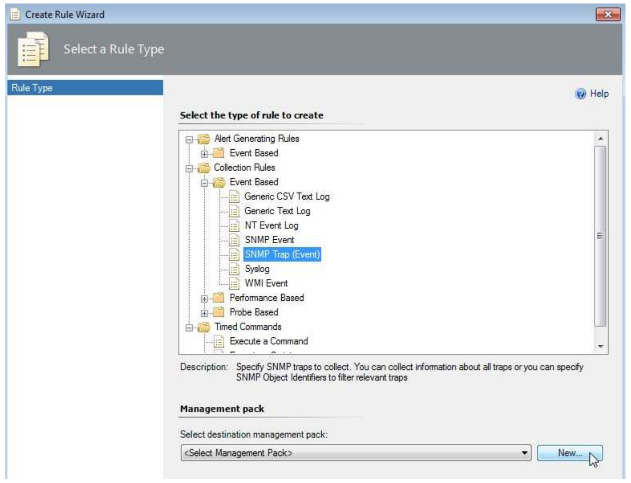
You can specify the start parameters that apply when you start the service from here.
Start parameters:

2. **Second we have to create a Management Pack rule in SCOM**

   a. Click on Authoring -> Management Pack Objects -> Rules -> Create a new rule...



   b. Select SNMP Trap (Event) rule type and click on New... near Management pack



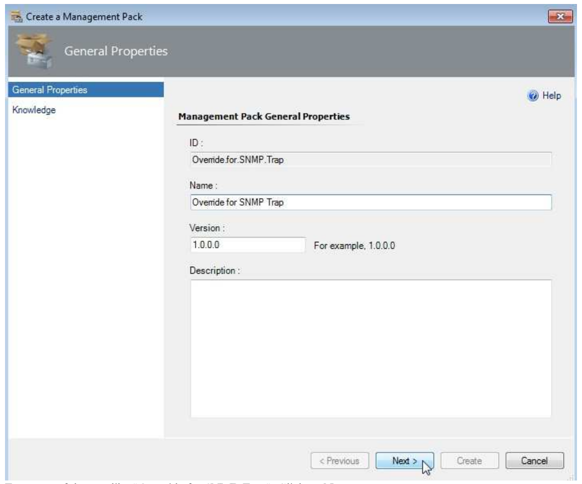
Select the type of rule to create

Description: Specify SNMP traps to collect. You can collect information about all traps or you can specify SNMP Object Identifiers to filter relevant traps

Management pack

Select destination management pack:
<Select Management Pack>

   c. Create the Management pack



Management Pack General Properties

ID : Override.for.SNMP.Trap

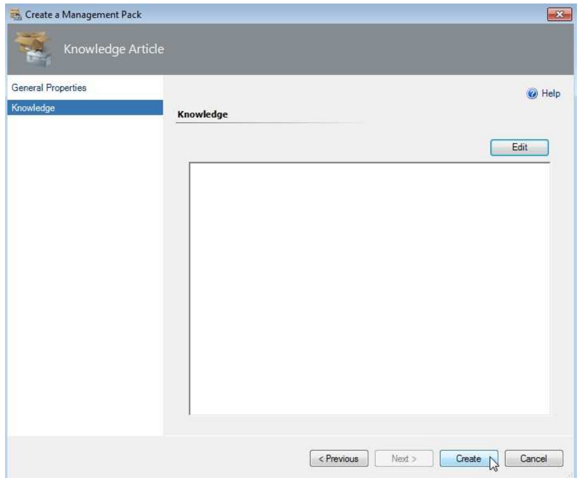
Name : Override for SNMP Trap

Version : 1.0.0.0 For example, 1.0.0.0

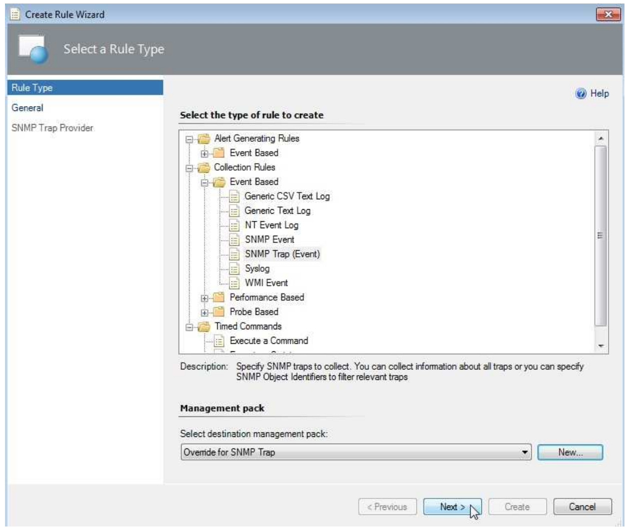
Description :

Enter a useful name like "Override for SNMP Trap". Click on Next.

d. Enter some knowledge (or not) and click on Create



e. Back on rule type selection click on Next


Create Rule Wizard

Select a Rule Type

Select the type of rule to create

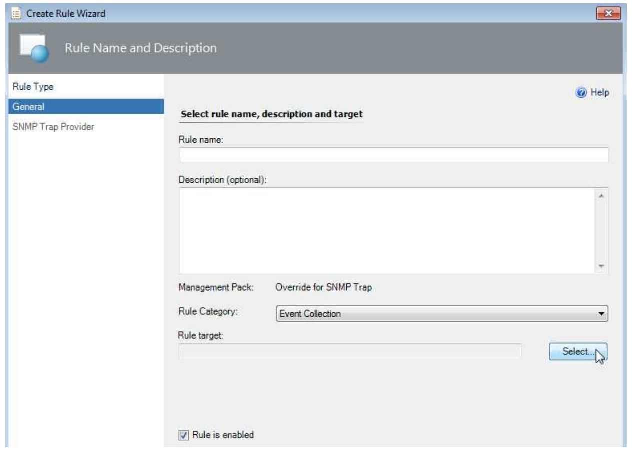
- Alert Generating Rules
  - Event Based
- Collection Rules
  - Event Based
    - Generic CSV Text Log
    - Generic Text Log
    - NT Event Log
    - SNMP Event
    - SNMP Trap (Event)
    - Syslog
    - WMI Event
  - Performance Based
  - Probe Based
- Timed Commands
  - Execute a Command

Description: Specify SNMP traps to collect. You can collect information about all traps or you can specify SNMP Object Identifiers to filter relevant traps

Management pack

Select destination management pack: Override for SNMP Trap

f. Select a rule target first


Create Rule Wizard

Rule Name and Description

Select rule name, description and target

Rule name:

Description (optional):

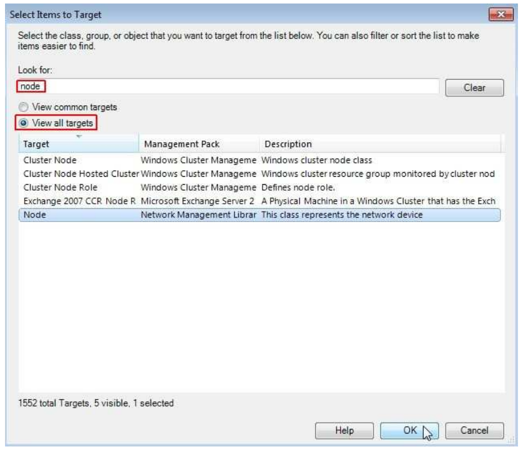
Management Pack: Override for SNMP Trap

Rule Category: Event Collection

Rule target:

☑ Rule is enabled

g. Select Node as target


Select Items to Target

Select the class, group, or object that you want to target from the list below. You can also filter or sort the list to make items easier to find.

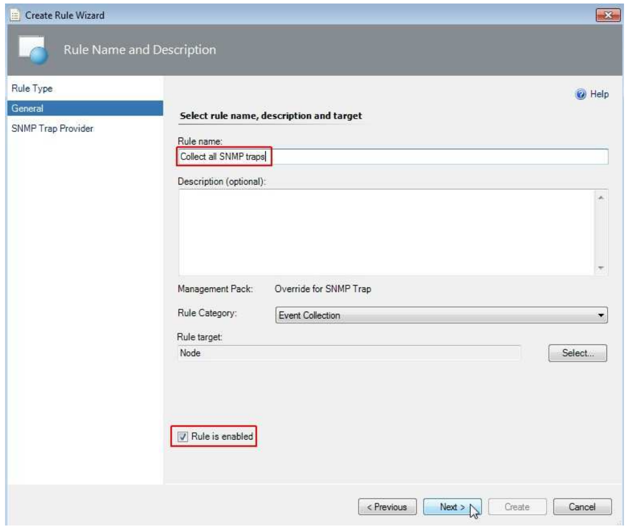
Look for: node

( ) View common targets
(●) View all targets

| Target | Management Pack | Description |
|---|---|---|
| Cluster Node | Windows Cluster Manageme | Windows cluster node class |
| Cluster Node Hosted Cluster | Windows Cluster Manageme | Windows cluster resource group monitored by cluster nod |
| Cluster Node Role | Windows Cluster Manageme | Defines node role. |
| Exchange 2007 CCR Node R | Microsoft Exchange Server 2 | A Physical Machine in a Windows Cluster that has the Exch |
| Node | Network Management Librar | This class represents the network device |

1552 total Targets, 5 visible, 1 selected

h. Select rule name


Create Rule Wizard

Rule Name and Description

Select rule name, description and target

Rule name: Collect all SNMP traps

Description (optional):

Management Pack: Override for SNMP Trap

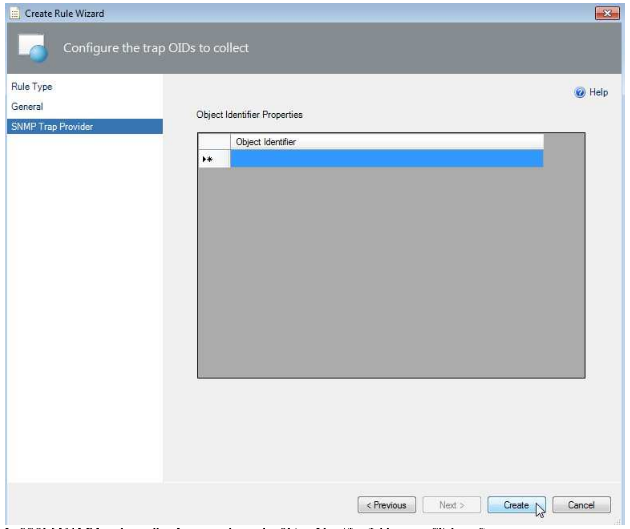
Rule Category: Event Collection

Rule target: Node

[✓] Rule is enabled

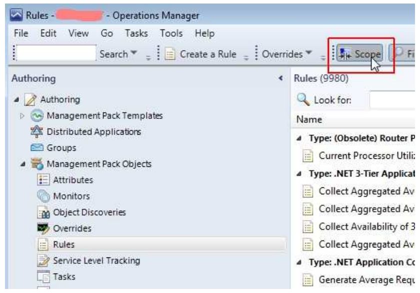
Enter a useful rule name like "Collect all SNMP traps". Check if rule is enabled and click on Next.

i. Configure the trap OIDs to collect

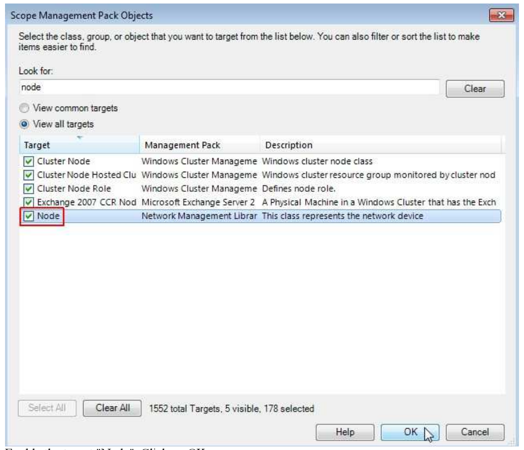


In SCOM 2012 R2 update rollup 2 you can leave the Object Identifier field empty. Click on Create.

j. Enable the scope view



k. Select the target "Node"



Select the class, group, or object that you want to target from the list below. You can also filter or sort the list to make items easier to find.

Look for: node

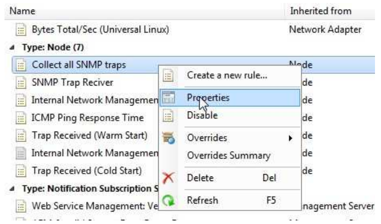
( ) View common targets
(●) View all targets

| Target | Management Pack | Description |
|---|---|---|
| ✓ Cluster Node | Windows Cluster Manageme | Windows cluster node class |
| ✓ Cluster Node Hosted Clu | Windows Cluster Manageme | Windows cluster resource group monitored by cluster nod |
| ✓ Cluster Node Role | Windows Cluster Manageme | Defines node role. |
| ✓ Exchange 2007 CCR Nod | Microsoft Exchange Server 2 | A Physical Machine in a Windows Cluster that has the Exch |
| ✓ Node | Network Management Librar | This class represents the network device |

1552 total Targets, 5 visible, 178 selected

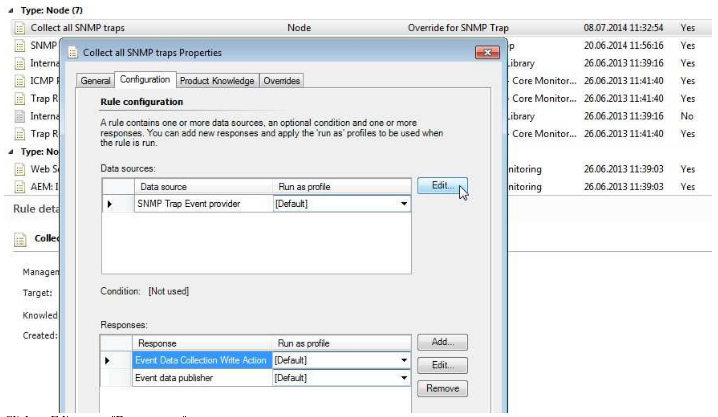
Enable the target "Node". Click on OK.

l. Review the settings of the created rule of type node



| Name | Inherited from |
|---|---|
| Bytes Total/Sec (Universal Linux) | Network Adapter |
| **Type: Node (7)** | |
| Collect all SNMP traps | Node |
| SNMP Trap Reciver | de |
| Internal Network Managemen | de |
| ICMP Ping Response Time | de |
| Trap Received (Warm Start) | de |
| Internal Network Managemen | de |
| Trap Received (Cold Start) | de |
| **Type: Notification Subscription S** | |
| Web Service Management: Ve | nagement Server |

m. "Collect all SNMP traps" properties



**Type: Node (7)**

| | | | | |
|---|---|---|---|---|
| Collect all SNMP traps | Node | Override for SNMP Trap | 08.07.2014 11:32:54 | Yes |
| SNMP | | p | 20.06.2014 11:56:16 | Yes |
| Interna | | Library | 26.06.2013 11:39:16 | Yes |
| ICMP | | Core Monitor... | 26.06.2013 11:41:40 | Yes |
| Trap R | | Core Monitor... | 26.06.2013 11:41:40 | Yes |
| Interna | | Library | 26.06.2013 11:39:16 | No |
| Trap R | | Core Monitor... | 26.06.2013 11:41:40 | Yes |
| **Type: No** | | | | |
| Web S | | nitoring | 26.06.2013 11:39:03 | Yes |
| AEM: I | | nitoring | 26.06.2013 11:39:03 | Yes |

Collect all SNMP traps Properties

General | Configuration | Product Knowledge | Overrides

**Rule configuration**

A rule contains one or more data sources, an optional condition and one or more responses. You can add new responses and apply the 'run as' profiles to be used when the rule is run.

Data sources:

| Data source | Run as profile |
|---|---|
| SNMP Trap Event provider | [Default] |

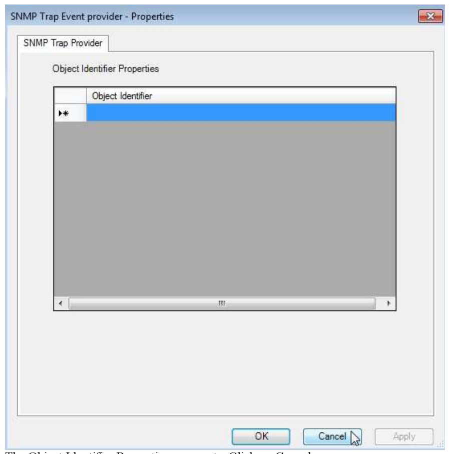
Condition: [Not used]

Responses:

| Response | Run as profile |
|---|---|
| Event Data Collection Write Action | [Default] |
| Event data publisher | [Default] |

Click on Edit... near "Data sources".

n. SNMP Trap Event trap provider properties



SNMP Trap Event provider - Properties

SNMP Trap Provider

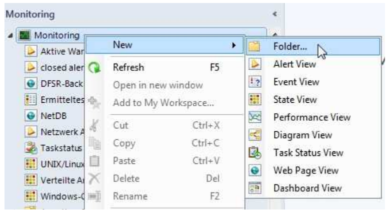
Object Identifier Properties

| Object Identifier |
|---|
| |

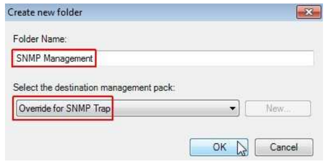
The Object Identifier Properties are empty. Click on Cancel.

3. **Third we have to create a trap monitor in SCOM**

a. Click on Monitoring -> New -> Folder...



b. Review the settings of the created rule of type node

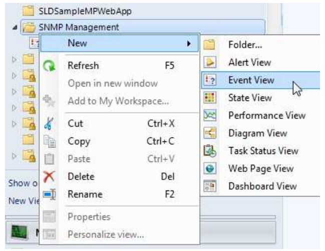

Create new folder

Folder Name:
SNMP Management

Select the destination management pack:
Override for SNMP Trap

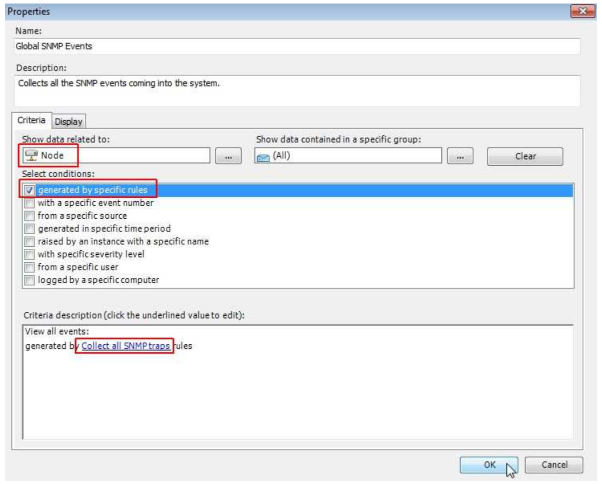
Enter a useful folder name like "SNMP Management" and select the formerly created MP "Override for SNMP Trap". Click on OK.

c. Create an Event View



Click on SNMP Management -> New -> Event View

d. Edit the properties of the Event View


Properties

Name:
Global SNMP Events

Description:
Collects all the SNMP events coming into the system.

Criteria | Display

Show data related to: Node

Show data contained in a specific group: (All)

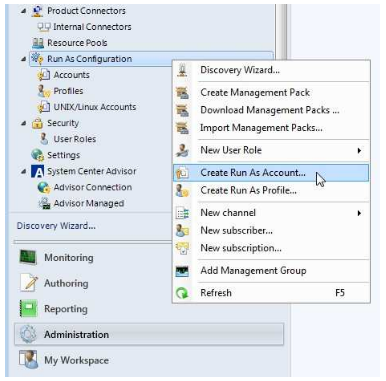
Select conditions:
- [x] generated by specific rules
- [ ] with a specific event number
- [ ] from a specific source
- [ ] generated in specific time period
- [ ] raised by an instance with a specific name
- [ ] with specific severity level
- [ ] from a specific user
- [ ] logged by a specific computer

Criteria description (click the underlined value to edit):
View all events:
generated by Collect all SNMP traps rules

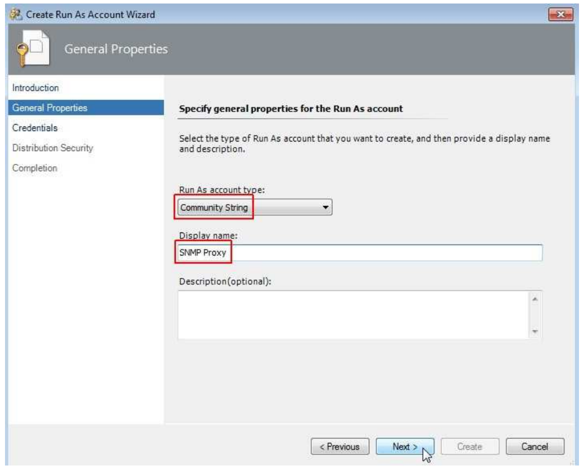
In tab "Criteria" choose "Node", select "generated by specific rules" and choose the "Collect all SNMP traps" rule. Click on OK.

4. **Fourth we have to create a Run As Account**

a. Click on Administration -> Run As Configuration -> Create Run As Account...



b. Specify general account properties


Create Run As Account Wizard

General Properties

Introduction
General Properties
Credentials
Distribution Security
Completion

**Specify general properties for the Run As account**

Select the type of Run As account that you want to create, and then provide a display name and description.

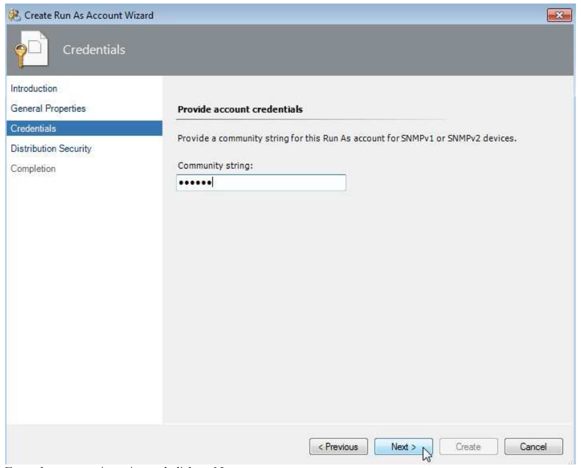
Run As account type: Community String

Display name: SNMP Proxy

Description(optional):

Choose "Community String" as account type and enter a useful display name like "SNMP Proxy". Click on Next.

c. Set credentials


Create Run As Account Wizard

Credentials

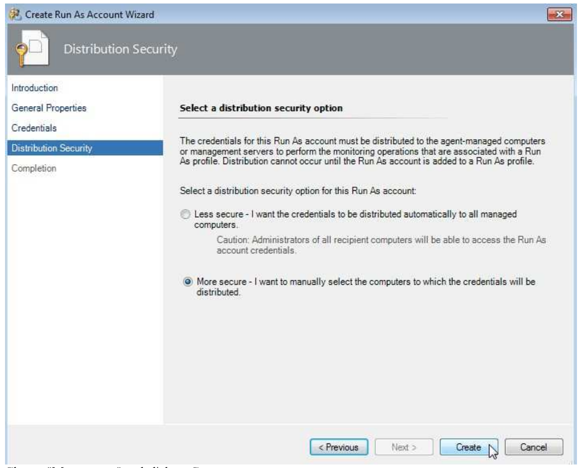
**Provide account credentials**

Provide a community string for this Run As account for SNMPv1 or SNMPv2 devices.

Community string: ••••••

Enter the community string and click on Next.

d. Select a distribution security option


Create Run As Account Wizard

Distribution Security

**Select a distribution security option**

The credentials for this Run As account must be distributed to the agent-managed computers or management servers to perform the monitoring operations that are associated with a Run As profile. Distribution cannot occur until the Run As account is added to a Run As profile.

Select a distribution security option for this Run As account:

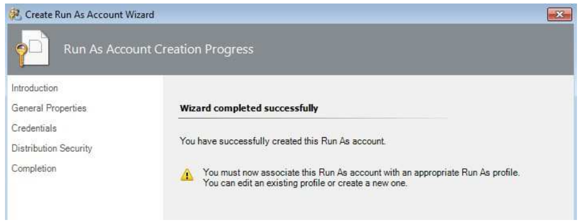
( ) Less secure - I want the credentials to be distributed automatically to all managed computers.

Caution: Administrators of all recipient computers will be able to access the Run As account credentials.

[✓ More secure - I want to manually select the computers to which the credentials will be distributed.]

Choose "More secure" and click on Create.

e. Prompt to create a profile


Create Run As Account Wizard

Run As Account Creation Progress

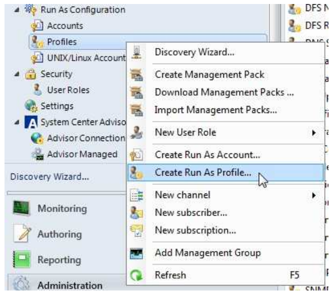
**Wizard completed successfully**

You have successfully created this Run As account.

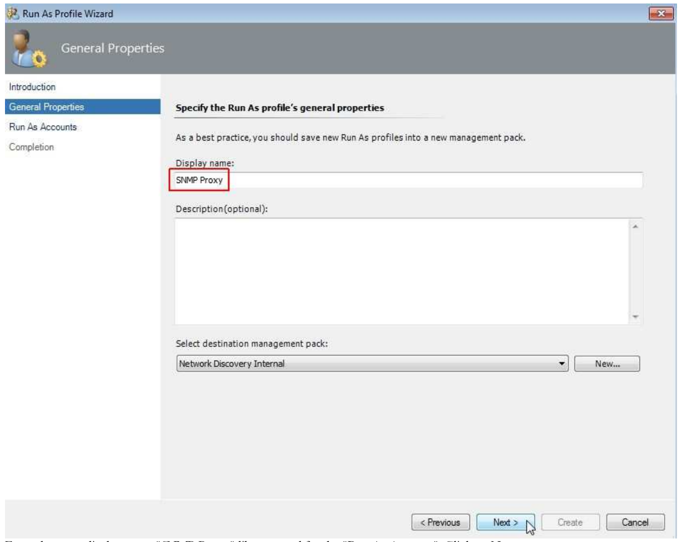
You must now associate this Run As account with an appropriate Run As profile. You can edit an existing profile or create a new one.

5. **Fifth we have to create a Run As Profile**

a. Click on Administration -> Run As Configuration -> Profiles -> Create Run As Profile...



b. Specify general profile properties


Run As Profile Wizard

General Properties

**Specify the Run As profile's general properties**

As a best practice, you should save new Run As profiles into a new management pack.

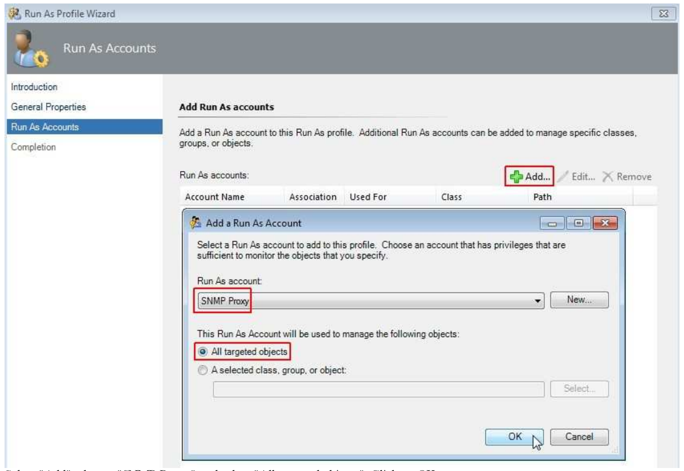
Display name: SNMP Proxy

Description(optional):

Select destination management pack: Network Discovery Internal

Enter the same display name "SNMP Proxy" like we used for the "Run As Account". Click on Next.

c. Add Run As Account



Run As Profile Wizard

Run As Accounts

Add Run As accounts

Add a Run As account to this Run As profile. Additional Run As accounts can be added to manage specific classes, groups, or objects.

Run As accounts:

| Account Name | Association | Used For | Class | Path |
|---|---|---|---|---|

Add a Run As Account

Select a Run As account to add to this profile. Choose an account that has privileges that are sufficient to monitor the objects that you specify.

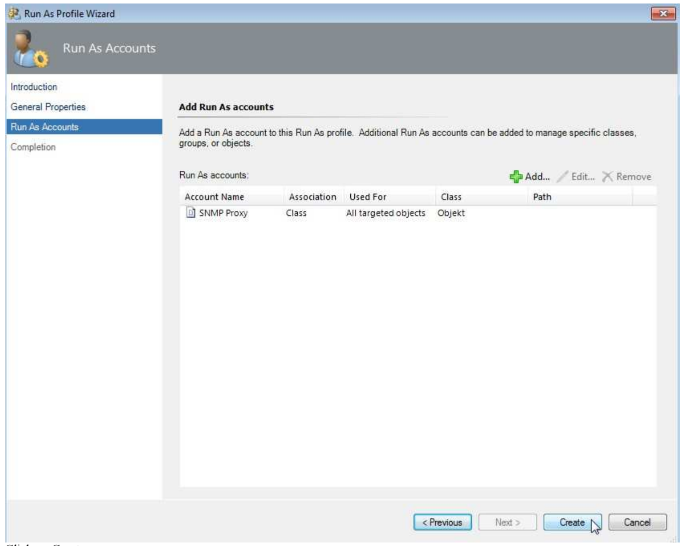
Run As account: SNMP Proxy

This Run As Account will be used to manage the following objects:

[✓ All targeted objects] A selected class, group, or object:

Select "Add", choose "SNMP Proxy" and select "All targeted objects". Click on OK.

d. Create profile



Run As Profile Wizard

Run As Accounts

Add Run As accounts

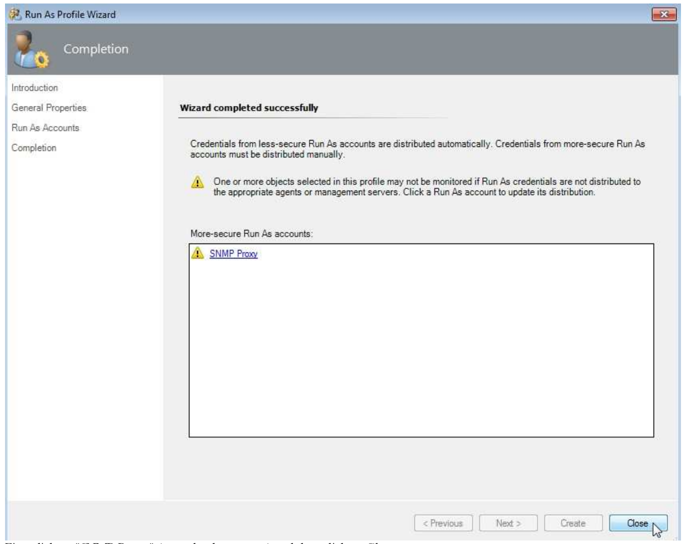
Add a Run As account to this Run As profile. Additional Run As accounts can be added to manage specific classes, groups, or objects.

Run As accounts:

| Account Name | Association | Used For | Class | Path |
|---|---|---|---|---|
| SNMP Proxy | Class | All targeted objects | Objekt | |

Click on Create.

e. Warning about account distribution


Run As Profile Wizard

Completion

**Wizard completed successfully**

Credentials from less-secure Run As accounts are distributed automatically. Credentials from more-secure Run As accounts must be distributed manually.

One or more objects selected in this profile may not be monitored if Run As credentials are not distributed to the appropriate agents or management servers. Click a Run As account to update its distribution.

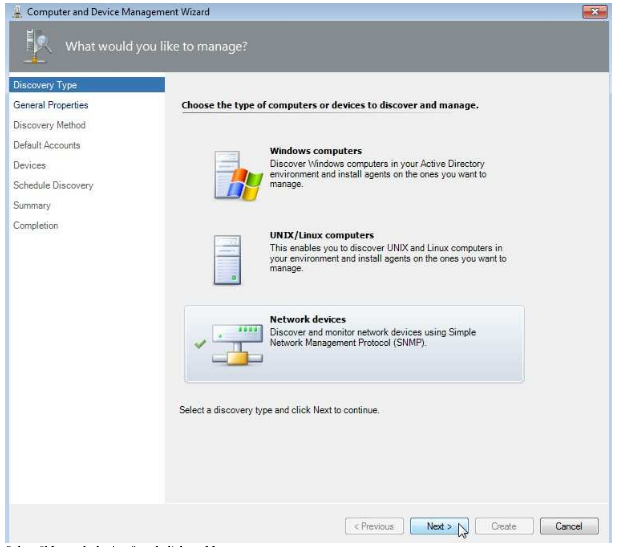
More-secure Run As accounts:

SNMP Proxy

First click on "SNMP Proxy" (green hook appeares) and then click on Close.

**Start of the network device discovery**

1. Click on Administration -> Network Management -> Discovery Wizard...


Computer and Device Management Wizard

What would you like to manage?

**Choose the type of computers or devices to discover and manage.**

**Windows computers**
Discover Windows computers in your Active Directory environment and install agents on the ones you want to manage.

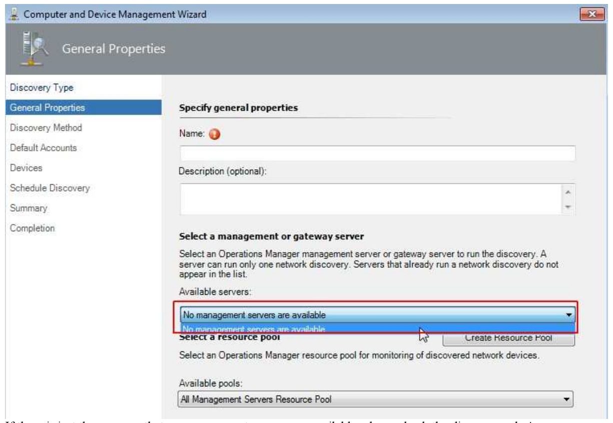
**UNIX/Linux computers**
This enables you to discover UNIX and Linux computers in your environment and install agents on the ones you want to manage.

**Network devices**
Discover and monitor network devices using Simple Network Management Protocol (SNMP).

Select a discovery type and click Next to continue.

Select "Network devices" and click on Next.

2. Select a management or gateway server



**Specify general properties**

Name:

Description (optional):

**Select a management or gateway server**

Select an Operations Manager management server or gateway server to run the discovery. A server can run only one network discovery. Servers that already run a network discovery do not appear in the list.

Available servers:

No management servers are available

No management servers are available

**Select a resource pool**

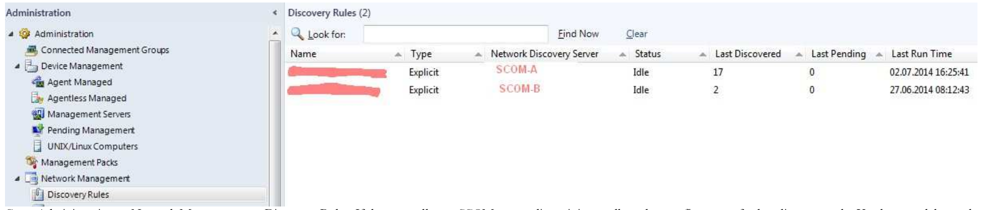
Select an Operations Manager resource pool for monitoring of discovered network devices.

Available pools:

All Management Servers Resource Pool

If there is just the message that no management servers are available, please check the discovery rules!

3. Check discovery rules

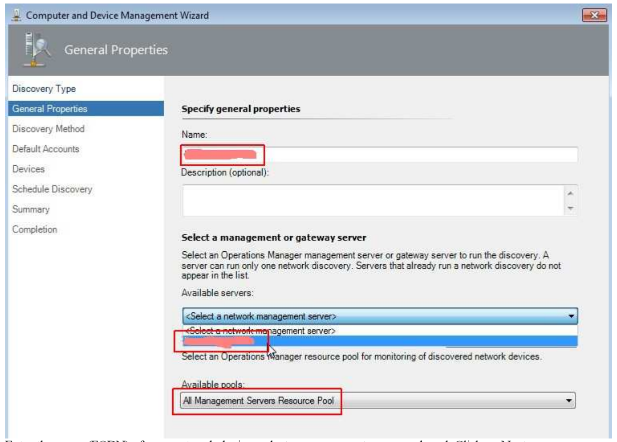


Discovery Rules (2)

| Name | Type | Network Discovery Server | Status | Last Discovered | Last Pending | Last Run Time |
|---|---|---|---|---|---|---|
| [redacted] | Explicit | SCOM-A | Idle | 17 | 0 | 02.07.2014 16:25:41 |
| [redacted] | Explicit | SCOM-B | Idle | 2 | 0 | 27.06.2014 08:12:43 |

Go to Administration -> Network Management -> Discovery Rules. If there are all your SCOM servers listet, it is not allowed to configure any further discovery rule. You have to delete at least one rule to go further! Again I can't understand this behavior. Why isn't it possible to define various rules and select one of them for a specific discovery? Once more a lack of functionality into SCOM.

4. Set general properties



**Specify general properties**

Name:

[redacted]

Description (optional):

**Select a management or gateway server**

Select an Operations Manager management server or gateway server to run the discovery. A server can run only one network discovery. Servers that already run a network discovery do not appear in the list.

Available servers:

<Select a network management server>

<Select a network management server>

[redacted]

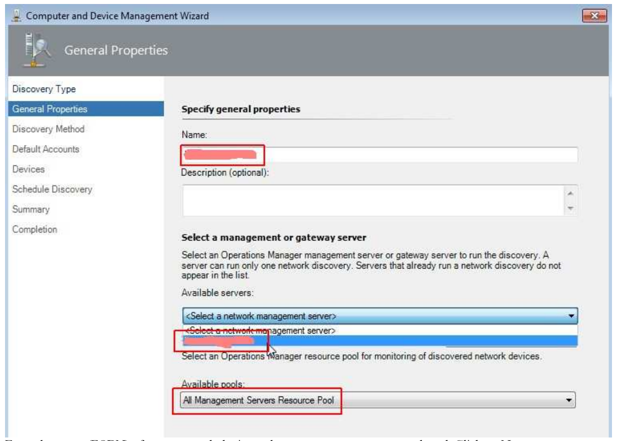
Select an Operations Manager resource pool for monitoring of discovered network devices.

Available pools:

All Management Servers Resource Pool

Enter the name (FQDN) of your network device, select a management server and pool. Click on Next.

5. Set general properties


Computer and Device Management Wizard

General Properties

**Specify general properties**

Name: [redacted]

Description (optional):

**Select a management or gateway server**

Select an Operations Manager management server or gateway server to run the discovery. A server can run only one network discovery. Servers that already run a network discovery do not appear in the list.

Available servers:

<Select a network management server>

<Select a network management server>

[redacted]

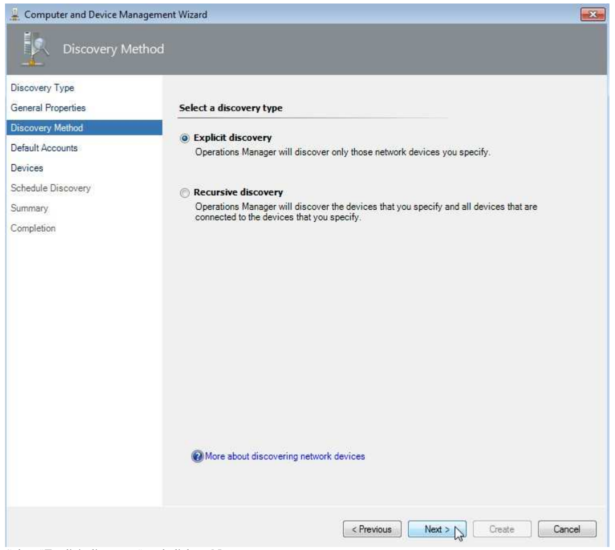
Select an Operations Manager resource pool for monitoring of discovered network devices.

Available pools:

All Management Servers Resource Pool

Enter the name (FQDN) of your network device, select a management server and pool. Click on Next.

6. Select a discovery type


Computer and Device Management Wizard

Discovery Method

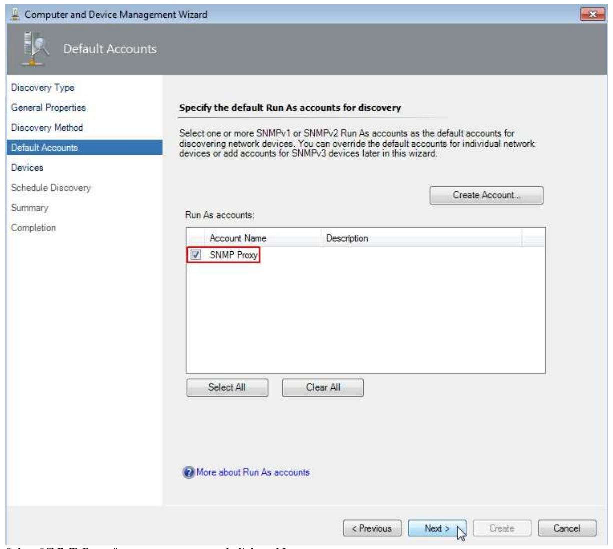
**Select a discovery type**

(●) **Explicit discovery**
Operations Manager will discover only those network devices you specify.

( ) **Recursive discovery**
Operations Manager will discover the devices that you specify and all devices that are connected to the devices that you specify.

Select "Explicit discovery" and click on Next.

7. Specify the default Run As accounts for discovery



**Specify the default Run As accounts for discovery**

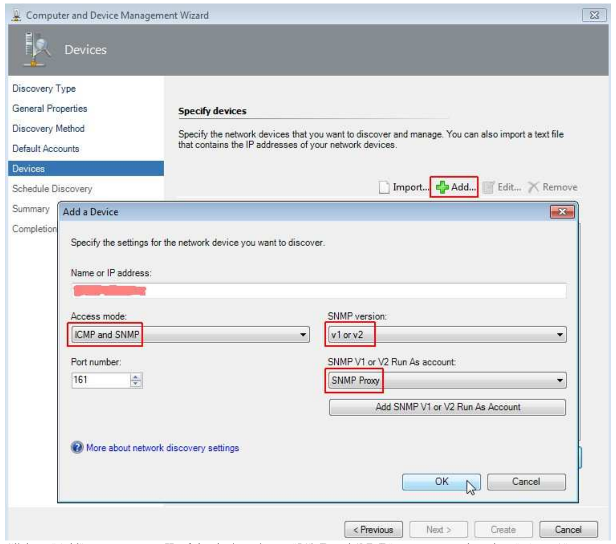
Select one or more SNMPv1 or SNMPv2 Run As accounts as the default accounts for discovering network devices. You can override the default accounts for individual network devices or add accounts for SNMPv3 devices later in this wizard.

Run As accounts:

| | Account Name | Description |
|---|---|---|
| ✓ | SNMP Proxy | |

Select "SNMP Proxy" as account name and click on Next.

8. Specify devices



**Specify devices**

Specify the network devices that you want to discover and manage. You can also import a text file that contains the IP addresses of your network devices.

Specify the settings for the network device you want to discover.

Name or IP address: [redacted]

Access mode: ICMP and SNMP

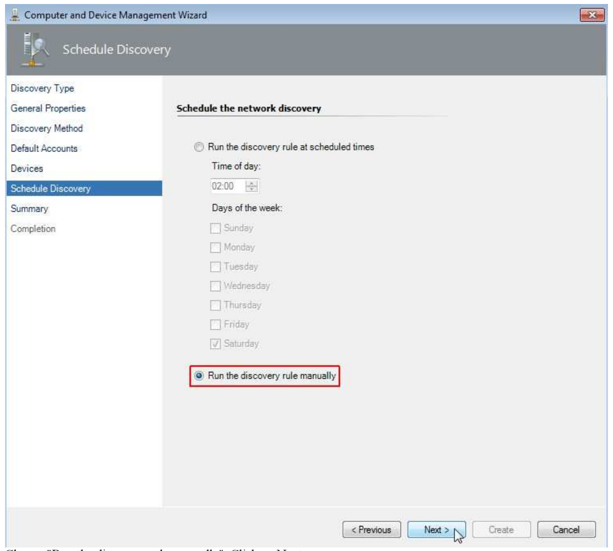
SNMP version: v1 or v2

Port number: 161

SNMP V1 or V2 Run As account: SNMP Proxy

Click on "Add", enter name or IP of the device, choose "ICMP and SNMP" as access mode, select "v1 or v2" as snmp version and "SNMP Proxy" as account. Click on OK and then on Next.

9. Schedule the network discovery



Schedule the network discovery

Run the discovery rule at scheduled times

Time of day: 02:00

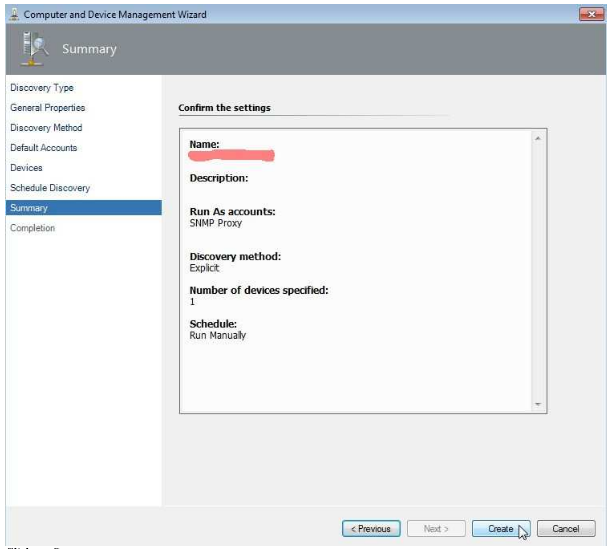
Days of the week:

- [ ] Sunday
- [ ] Monday
- [ ] Tuesday
- [ ] Wednesday
- [ ] Thursday
- [ ] Friday
- [x] Saturday

Run the discovery rule manually [✓]

Choose "Run the discovery rule manually". Click on Next.

10. Confirm the settings



Confirm the settings

**Name:**
[redacted]

**Description:**

**Run As accounts:**
SNMP Proxy

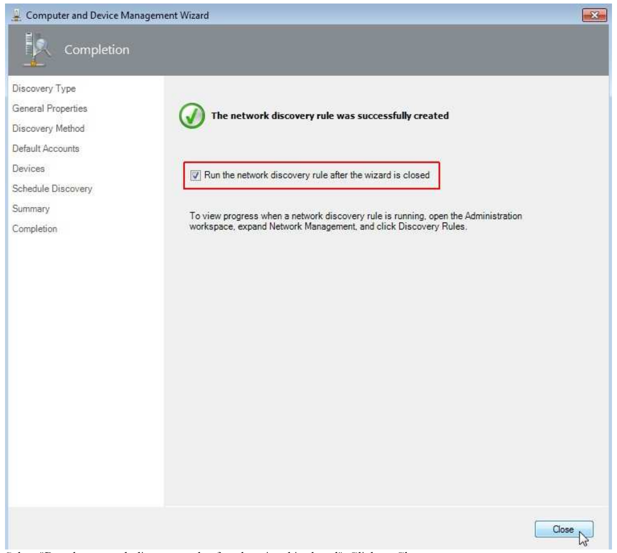
**Discovery method:**
Explicit

**Number of devices specified:**
1

**Schedule:**
Run Manually

Click on Create.

11. Wait for completion



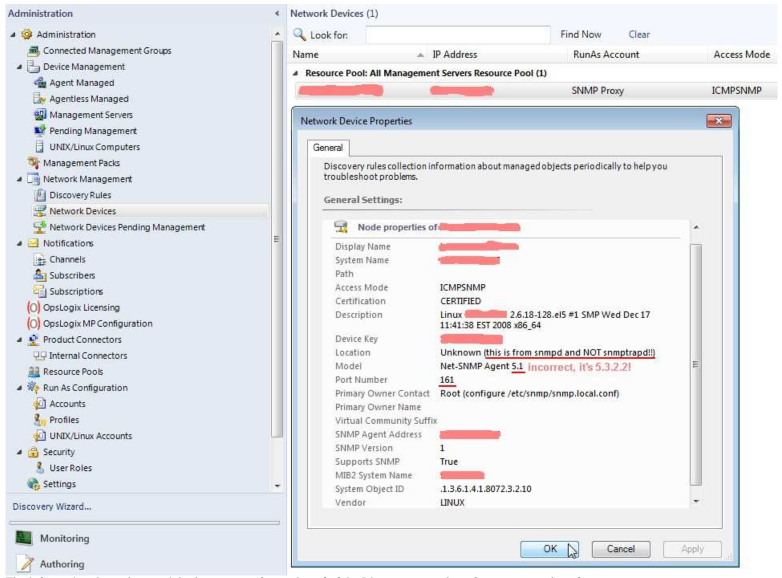
The network discovery rule was successfully created

☑ Run the network discovery rule after the wizard is closed

To view progress when a network discovery rule is running, open the Administration workspace, expand Network Management, and click Discovery Rules.

Select "Run the network discovery rule after the wizard is closed". Click on Close.

And voila there is a new network SNMP version 1 device discovered on port 161!



| Name | IP Address | RunAs Account | Access Mode |
|---|---|---|---|
| Resource Pool: All Management Servers Resource Pool (1) | | | |
| [redacted] | [redacted] | SNMP Proxy | ICMPSNMP |

Network Device Properties

General

Discovery rules collection information about managed objects periodically to help you troubleshoot problems.

General Settings:

Node properties of [redacted]

| | |
|---|---|
| Display Name | [redacted] |
| System Name | [redacted] |
| Path | |
| Access Mode | ICMPSNMP |
| Certification | CERTIFIED |
| Description | Linux [redacted] 2.6.18-128.el5 #1 SMP Wed Dec 17 11:41:38 EST 2008 x86_64 |
| Device Key | [redacted] |
| Location | Unknown (this is from snmpd and NOT snmptrapd!!) |
| Model | Net-SNMP Agent 5.1 incorrect, it's 5.3.2.2! |
| Port Number | 161 |
| Primary Owner Contact | Root (configure /etc/snmp/snmp.local.conf) |
| Primary Owner Name | |
| Virtual Community Suffix | |
| SNMP Agent Address | [redacted] |
| SNMP Version | 1 |
| Supports SNMP | True |
| MIB2 System Name | [redacted] |
| System Object ID | .1.3.6.1.4.1.8072.3.2.10 |
| Vendor | LINUX |

The information showed are mainly the content of snmpd.conf of the Linux server and not from snmptrapd.conf!
Furthermore the net-snmp agent version seems to be hardcoded in SCOM, because the version displayed is older than the installed version.

**A nmap scan again shows that port 162 is now listening on the SCOM 2012 system.**

```
[root@<hostname> ~]# nmap -sU -p U:162 <FQDN-SCOM>

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2014-06-20 13:31 CEST
Interesting ports on <FQDN-SCOM> (<SCOM-IP>):
PORT    STATE         SERVICE
162/udp open|filtered snmptrap
MAC Address: 00:50:56:A3:xx:yy (VMWare)

Nmap finished: 1 IP address (1 host up) scanned in 0.321 seconds
[root@<hostname> ~]#
```

Now it's time to disable (stop) the SNMP daemon on the Linux server and try to send some SNMP traps. There is a command line utility which can be used for sending SNMP traps. Don't confound things, this is not snmptrapd!

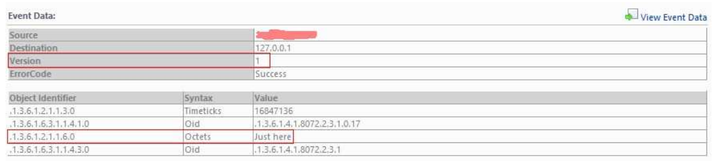
```
[root@<hostname> ~]# service snmpd stop
Stopping snmpd:                                            [  OK  ]
[root@<hostname> ~]#
```

```
[root@<hostname> ~]# snmptrap -v 1 -c public <FQDN-SCOM> .1.3.6.1.4.1.8072.2.3.1 "" 6 17 "" .1.3.6.1.2.1.1.6.0 s "Just there"
[root@<hostname> ~]#
```

or

```
[root@<hostname> ~]# snmptrap -v 1 -c public <FQDN-SCOM> NET-SNMP-EXAMPLES-MIB::netSnmpExampleNotification "" 6 17 "" SNMPv2-MIB::sysLocation.0 s "Just here"
[root@<hostname> ~]#
```

shows following result in SCOM. Please note that SCOM doesn't translate the OIDs to the appropriate entity names by itself!


Event Data:

View Event Data

| | |
|---|---|
| Source | [redacted] |
| Destination | 127.0.0.1 |
| Version | 1 |
| ErrorCode | Success |

| Object Identifier | Syntax | Value |
|---|---|---|
| .1.3.6.1.2.1.1.3.0 | Timeticks | 16847136 |
| .1.3.6.1.6.3.1.1.4.1.0 | Oid | .1.3.6.1.4.1.8072.2.3.1.0.17 |
| .1.3.6.1.2.1.1.6.0 | Octets | Just here |
| .1.3.6.1.6.3.1.1.4.3.0 | Oid | .1.3.6.1.4.1.8072.2.3.1 |

For the interested reader now a small collection of SNMP v2c and v1 traps and how SCOM detected them.

- Trap version 2(c) SNMP trap

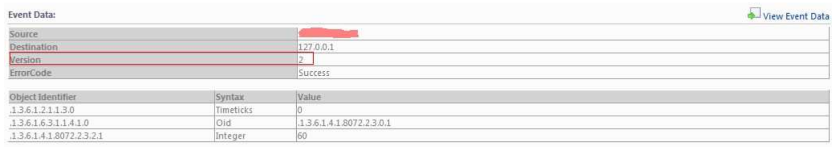
  Use of snmptrap cli:

```
[root@<hostname> ~]# snmptrap -v 2c -c public <FQDN-SCOM> 0 NET-SNMP-EXAMPLES-MIB::netSnmpExampleHeartbeatNotification netSnmpExampleHeartbeatRate i 60
[root@<hostname> ~]#
```

  or

```
[root@<hostname> ~]# snmptrap -v 2c -c public <FQDN-SCOM> 0 .1.3.6.1.4.1.8072.2.3.0.1 .1.3.6.1.4.1.8072.2.3.2.1.0 i 60
[root@<hostname> ~]#
```

  Display into SCOM 2012:


Event Data:

View Event Data

| | |
|---|---|
| Source | [redacted] |
| Destination | 127.0.0.1 |
| Version | 2 |
| ErrorCode | Success |

| Object Identifier | Syntax | Value |
|---|---|---|
| .1.3.6.1.2.1.1.3.0 | Timeticks | 0 |
| .1.3.6.1.6.3.1.1.4.1.0 | Oid | .1.3.6.1.4.1.8072.2.3.0.1 |
| .1.3.6.1.4.1.8072.2.3.2.1 | Integer | 60 |

- Trap version 1 SNMP trap

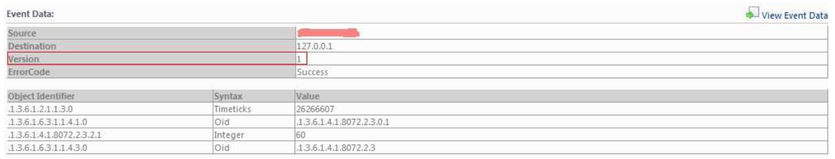
  Use of snmptrap cli:

```
[root@<hostname> ~]# snmptrap -v 1 -c public <FQDN-SCOM> NET-SNMP-EXAMPLES-MIB::netSnmpExampleNotifications "" 6 1 "" netSnmpExampleHeartbeatRate i 60
[root@<hostname> ~]#
```

  or

```
[root@<hostname> ~]# snmptrap -v 1 -c public <FQDN-SCOM> .1.3.6.1.4.1.8072.2.3 "" 6 1 "" .1.3.6.1.4.1.8072.2.3.2.1.0 i 60
[root@<hostname> ~]#
```

  Display into SCOM 2012:


Event Data:

View Event Data

| | |
|---|---|
| Source | [redacted] |
| Destination | 127.0.0.1 |
| Version | 1 |
| ErrorCode | Success |

| Object Identifier | Syntax | Value |
|---|---|---|
| .1.3.6.1.2.1.1.3.0 | Timeticks | 26266607 |
| .1.3.6.1.6.3.1.1.4.1.0 | Oid | .1.3.6.1.4.1.8072.2.3.0.1 |
| .1.3.6.1.4.1.8072.2.3.2.1 | Integer | 60 |
| .1.3.6.1.6.3.1.1.4.3.0 | Oid | .1.3.6.1.4.1.8072.2.3 |

Now we see a bunch on non-speaking object identifiers. There is a tool called snmptranslate into the net-snmp package which translates the OID into the entity name and vice versa:

| ObjectIdentifier | snmptranslate -m ALL | Syntax | Value | snmptranslate -m ALL |
|---|---|---|---|---|
| .1.3.6.1.2.1.1.3.0 | DISMAN-EVENT-MIB::sysUpTimeInstance | Timeticks | 26266607 | - |
| .1.3.6.1.6.3.1.1.4.1.0 | SNMPv2-MIB::snmpTrapOID.0 | Oid | .1.3.6.1.4.1.8072.2.3.0.1 | NET-SNMP-EXAMPLES-MIB::netSnmpExampleHeartbeatNotification |
| .1.3.6.1.4.1.8072.2.3.2.1 | NET-SNMP-EXAMPLES-MIB::netSnmpExampleHeartbeatRate | Integer | 60 | - |

| | | | | |
|---|---|---|---|---|
| .1.3.6.1.6.3.1.1.4.3.0 | SNMPv2-MIB::snmpTrapEnterprise.0 | Oid | .1.3.6.1.4.1.8072.2.3 | NET-SNMP-EXAMPLES-MIB::netSnmpExampleNotifications |

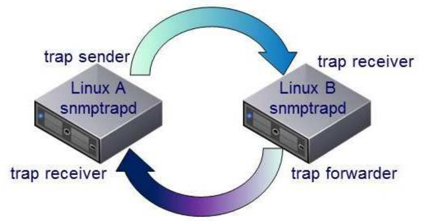
If you use the option -m ALL snmptranslate will scan the MIB directory, RHEL default is /usr/share/snmp/mib, parse **all** MIBs and build the entity names out of the OIDs.

I've bundled the needed MIBs into a download file [vmware-mibs.tar.gz;82 kByte], which you can request here. More information about the latest MIBs are available from VMware: http://kb.vmware.com/kb/1013445.

This was a short trip into the world of object identifiers and entity names. Let us now switch back to real world. We are now able to discover a network device, which sends SNMP traps to SCOM 2012. But what about network devices which are unable to answer SNMP requests but able to send SNMP traps? Is it possible to monitor them with System Center Operations Manager?

The answer is: yes, but not the smart way. First you have to deploy a server like the RedHat Enterprise Linux I've mentioned above and configure it identical (hostname and ip address and SNMP version) to your network device. If this Linux server was successful discovered by SCOM just remove it and substitute it with the "real" SNMP trap sending network device. This should work pretty good! But beware the circumstance that SCOM 2012 just shows the object identifier and is not able to import MIBs! This is a severe shortage.

I guess some guys know that the snmptrap daemon is able to forward SNMP traps. Now, maybe that it is possible to forward SNMP traps from a MS Windows server, let's say VMware vCenter Server, using this RHEL server? Well I've extend my scenario to verify this:



Linux A sends a snmptrap to Linux B. Linux B is configured as a forwarder for SNMP traps and sends the trap immediatly back to Linux A which is a snmptrap receiver, too. I do this without including SCOM to verify that the setup is full functional. We can monitor the behavior of the two systems by observing the content of /var/log/messages on both servers.

send trap from Linux A to Linux B:

```
[root@<hostnameA> ~]# snmptrap -v 1 -c public <hostnameB> .1.3.6.1 localhost 6 17 "" .1.3.6.1 s "Just a test"
[root@<hostnameA> ~]#
```

Logfile Linux B:

```
Jun 18 14:46:04 <hostnameB> snmptrapd[4215]: 2014-06-18 14:46:04 localhost.localdomain [127.0.0.1] (via UDP: [<hostnameA-IP>]:38153) TRAP, SNMP v1, community public SNMPv2-SMI::internet Enterprise Specific Trap (17) Uptime: 265 days, 5:59:58.77 SNMPv2-SMI::internet = STRING: "Just a test"
```

Logfile Linux A:

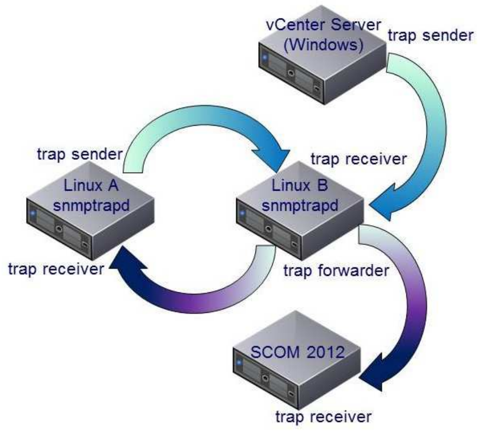
```
Jun 18 14:46:04 <hostnameA> snmptrapd[32387]: 2014-06-18 14:46:04 localhost.localdomain [127.0.0.1] (via UDP: [<hostnameB-IP>]:37360) TRAP, SNMP v1, community public SNMPv2-SMI::internet Enterprise Specific Trap (17) Uptime: 265 days, 5:59:58.77 SNMPv2-SMI::internet = STRING: "Just a test"
```

Hey, that looks good.

/var/log/messages from Logfile Linux A:

```
Jun 18 14:47:00 <hostnameA> snmptrapd[32387]: 2014-06-18 14:47:00 <vCenter-FQDN> [<vCenter-IP>] (via UDP: [<vCenter-IP>]:56912) TRAP, SNMP v1, community public  VMWARE-PRODUCTS-MIB::vmwVC Enterprise Specific Trap (VMWARE-VC-EVENT-MIB::vpxdDiagnostic) Uptime: 34 days, 21:34:31.53
```

Isn't it cool? It will work pretty good from the Linux point of view. Let's transfer the scenario using SCOM 2012 as SNMP trap receiver, which means that there is an additional trap receiver to configure:



As you might guess, the result is: **nothing!** I can't see any new trap into SCOM 2012 by using the last scenario, just the old ones sending direct from Linux B. Oh, what a mess!

These are the configuration changes on Linux B:

1. /etc/snmp/snmptrapd.conf

```
authCommunity net,log public
forward default <hostnameA-IP> public
forward default <SCOM-IP> public
traphandle VMWARE-VC-EVENT-MIB::vpxdDiagnostic /root/scom/bin/traps vpxdiag
traphandle VMWARE-PRODUCTS-MIB::vmwVC           /root/scom/bin/traps vcenter
traphandle .1.3.6.1.4.1.6876.4.3               /root/scom/bin/traps vcenteroid
traphandle .1.3.6.1.4.1.6876.4.3.0.202         /root/scom/bin/traps vpxdiagoid

disableAuthorization yes
```

You see the forward rules, they are self-explaining. The next lines are trap handlers, I will tell a bit later about them. The last line (disableAuthorization yes) is needed if you use net-snmp v5.3 or greater.

2. Create the trap handler script /root/scom/bin/traps

   The trap handlers are able to execute a script if a specific trap is received. Because the forwarding doesn't work, what about triggering a new trap with the received values? Let's see what happens if we create the script.

```
#!/bin/bash

BASE='/usr/bin/snmptrap -v 1 -c public <SCOM-FQDN> .1.3.6.1.4.1.6876.4.3 "" 6'
VPXDIAG='202 ""'
VPXDALARMINFO='203 "" '
vars=

while read oid val
do
  OBJECT="$VPXDALARMINFO"
  if [ "$oid" = "<vCenter-FQDN>" ]
  then
    continue
  fi
  if [ "$oid" = "<UNKNOWN>" ]
  then
    continue
  fi
  if [ "$oid" = "UDP:" ]
  then
    continue
  fi
  if [ "$oid" = "SNMP-COMMUNITY-MIB::snmpTrapAddress.0" ]
  then
    continue
  fi
  if [ "$oid" = "SNMP-COMMUNITY-MIB::snmpTrapCommunity.0" ]
  then
    continue
  fi
  if [ "$oid" = "DISMAN-EVENT-MIB::sysUpTimeInstance" ]
  then
    continue
  fi
  if [ "$oid" = "SNMPv2-MIB::snmpTrapOID.0" ]
  then
    continue
  fi
  if [ "$oid" = "SNMPv2-MIB::snmpTrapEnterprise.0" ]
  then
    continue
  fi
  if [ "$oid" = "VMWARE-VC-EVENT-MIB::vmwVpxdTargetObjType.0" ]
  then
    if [ "$val" = "unknown" ] ; then
     val=1
    elif [ "$val" = "host" ] ; then
     val=2
    elif [ "$val" = "vm" ] ; then
     val=3
    elif [ "$val" = "other" ] ; then
     val=4
    fi
  fi
  if [ "$val" = "VMWARE-VC-EVENT-MIB::vpxdDiagnostic" ]
  then
    OBJECT="$VPXDIAG"
    break
  fi
  if [ "$vars" = "" ]
  then
    if [ "$oid" = "VMWARE-VC-EVENT-MIB::vmwVpxdTargetObjType.0" ]
    then
      vars="$oid i \"$val\""
    else
      vars="$oid s \"$val\""
    fi
  else
    if [ "$oid" = "VMWARE-VC-EVENT-MIB::vmwVpxdTargetObjType.0" ]
    then
      vars="$vars $oid i \"$val\""
    else
      vars="$vars $oid s \"$val\""
    fi
  fi
done

echo "trap: $1 # $BASE $OBJECT $vars" >> /root/scom/bin/snmptraphandle.txt
clean_vars=$(echo $vars | sed -e 's/Ä/Ae/g' -e 's/Ö/Oe/g' -e 's/Ü/Ue/g' -e 's/ä/ae/g' -e 's/ö/oe/g' -e 's/ü/ue/g' -e 's/ß/ss/g')
eval "$BASE" "$OBJECT" "$clean_vars"
```

3. Changes of /etc/init.d/snmptrapd

```
...
. /etc/init.d/functions

OPTIONS="-m ALL -Ls 3 -p /var/run/snmptrapd.pid"
```

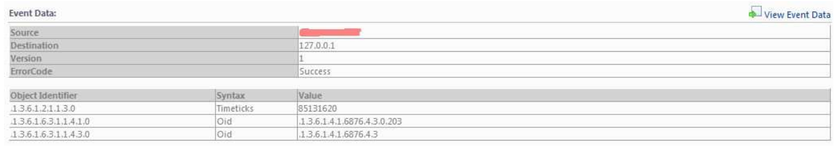
```
#OPTIONS="-Lsd -p /var/run/snmptrapd.pid"
if [ -e /etc/sysconfig/snmptrapd.options ]; then
...
```

4. Restart of snmptrapd

```
[root@<hostnameA> ~]# service snmptrapd restart
Stopping snmptrapd:                                        [  OK  ]
Starting snmptrapd:                                        [  OK  ]
[root@<hostnameA> ~]#
```

5. The vpxd diagnostic trap

   To receive the vpxd diagnostic trap from vCenter every minute follow the kb article about how to change the default sending period of the diagnostic SNMP trap on vCenter: http://kb.vmware.com/kb/2020271. If you don't know how to send SNMP traps from vCenter there is a kb article, too: http://kb.vmware.com/kb/1006438.



Event Data: View Event Data

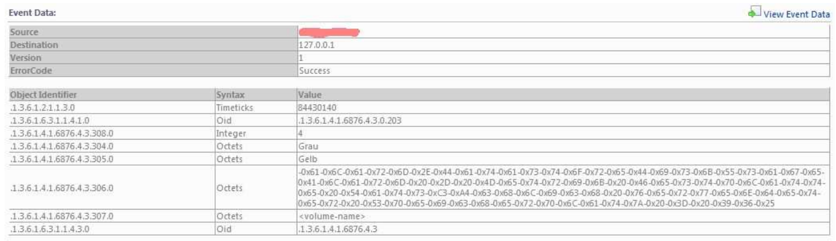
| | |
|---|---|
| Source | [redacted] |
| Destination | 127.0.0.1 |
| Version | 1 |
| ErrorCode | Success |

| Object Identifier | Syntax | Value |
|---|---|---|
| .1.3.6.1.2.1.1.3.0 | Timeticks | 85131620 |
| .1.3.6.1.6.3.1.1.4.1.0 | Oid | .1.3.6.1.4.1.6876.4.3.0.203 |
| .1.3.6.1.6.3.1.1.4.3.0 | Oid | .1.3.6.1.4.1.6876.4.3 |

   Yeah, we've got it! It works as expected. Now we can receive SNMP traps send by a vCenter Server running Microsoft Windows using a Linux server as a kind of trap rewriter.

Now let me write some words about the configuration. You may have recognized in snmptrapd.conf the duplicate lines, e.g.
traphandle VMWARE-VC-EVENT-MIB::vpxdDiagnostic /root/scom/bin/traps vpxdiag
and
traphandle .1.3.6.1.4.1.6876.4.3.0.202 /root/scom/bin/traps vpxdiagoid
In your final configuration you could delete one of the lines. It doesn't matter if you use OIDs or entity names. In my opinion it's better to use the entity names, because they are more "human readable" instead of the OIDs. Additionally you can delete the forward lines, they are obsolete.

I was inspired from the handler script example from the net-snmp team for writing the traps shell script. The script is just a kind of filter which throws away unwanted information. It converts the ASCII string of the vmwVpxdTargetObjType to integer again (the MIB files provide information about the needed data type) and at least it coverts the german umlauts (some guys say "funny or dotted characters") to the valid ASCII range. If you don't do that SCOM interpretes this as the binary representation of octet string as you can see in the following picture:

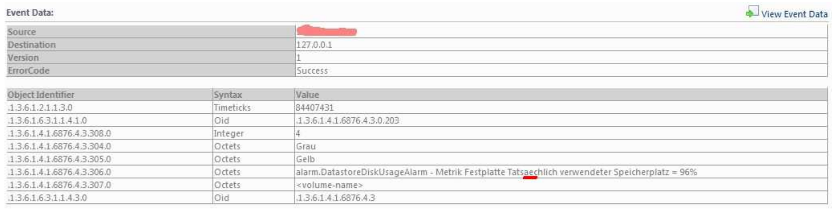


Event Data: View Event Data

| | |
|---|---|
| Source | [redacted] |
| Destination | 127.0.0.1 |
| Version | 1 |
| ErrorCode | Success |

| Object Identifier | Syntax | Value |
|---|---|---|
| .1.3.6.1.2.1.1.3.0 | Timeticks | 84430140 |
| .1.3.6.1.6.3.1.1.4.1.0 | Oid | .1.3.6.1.4.1.6876.4.3.0.203 |
| .1.3.6.1.4.1.6876.4.3.308.0 | Integer | 4 |
| .1.3.6.1.4.1.6876.4.3.304.0 | Octets | Grau |
| .1.3.6.1.4.1.6876.4.3.305.0 | Octets | Gelb |
| .1.3.6.1.4.1.6876.4.3.306.0 | Octets | -0x61-0x6C-0x61-0x72-0x6D-0x2E-0x44-0x61-0x74-0x61-0x73-0x74-0x6F-0x72-0x65-0x44-0x69-0x73-0x6B-0x55-0x73-0x61-0x67-0x65-0x41-0x6C-0x61-0x72-0x6D-0x20-0x2D-0x20-0x4D-0x65-0x74-0x72-0x69-0x6B-0x20-0x46-0x65-0x73-0x74-0x70-0x6C-0x61-0x74-0x74-0x65-0x20-0x54-0x61-0x74-0x73-0xC3-0xA4-0x63-0x68-0x6C-0x69-0x63-0x68-0x20-0x76-0x65-0x72-0x77-0x65-0x6E-0x64-0x65-0x74-0x65-0x72-0x20-0x53-0x70-0x65-0x69-0x63-0x68-0x65-0x72-0x70-0x6C-0x61-0x74-0x7A-0x20-0x3D-0x20-0x39-0x36-0x25 |
| .1.3.6.1.4.1.6876.4.3.307.0 | Octets | <volume-name> |
| .1.3.6.1.6.3.1.1.4.3.0 | Oid | .1.3.6.1.4.1.6876.4.3 |

Just by replacing the umlaut ä to "ae" the octet string get readable again:



Event Data: View Event Data

| | |
|---|---|
| Source | [redacted] |
| Destination | 127.0.0.1 |
| Version | 1 |
| ErrorCode | Success |

| Object Identifier | Syntax | Value |
|---|---|---|
| .1.3.6.1.2.1.1.3.0 | Timeticks | 84407431 |
| .1.3.6.1.6.3.1.1.4.1.0 | Oid | .1.3.6.1.4.1.6876.4.3.0.203 |
| .1.3.6.1.4.1.6876.4.3.308.0 | Integer | 4 |
| .1.3.6.1.4.1.6876.4.3.304.0 | Octets | Grau |
| .1.3.6.1.4.1.6876.4.3.305.0 | Octets | Gelb |
| .1.3.6.1.4.1.6876.4.3.306.0 | Octets | alarm.DatastoreDiskUsageAlarm - Metrik Festplatte Tatsaechlich verwendeter Speicherplatz = 96% |
| .1.3.6.1.4.1.6876.4.3.307.0 | Octets | <volume-name> |
| .1.3.6.1.6.3.1.1.4.3.0 | Oid | .1.3.6.1.4.1.6876.4.3 |

Now my dear reader is it up to you to build a free piece of software which displays the vCenter SNMP traps in a meaningful way into SCOM 2012. I've provided you with all information and tips I've currently discovered.

You can download this page as pdf file [2000 kB].

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)*