MATERNA
Information & Communications
TRAINING

UNIFY Open Scape Fault Management

MONITORING

MONITORING

„Simple“, „Advanced“ and „OpenScape“ Monitoring

OSFM offers three different monitoring options:

- **Simple: Basic monitoring for availability and information from SNMP-MIB-II**
- **Advanced: Agent collects detailed information via script or manufacturer SNMP-MIB**
- **OpenScape: Comprehensive Build-In Support for OpenScape technology. Always available if license fits**

The standard SNMP

The SNMP Protocol

The Simple Network Management Protocol (SNMP) is a network protocol for monitoring and controlling network components (for example Routers, Server, Switches, Printers, PCs) from a central station (Management Console). The protocol controls the communication between the monitored components and the monitoring station. SNMP describes the structure of the transmitted data packets and the communication workflow. It is designed so that any network device can be included in the monitoring. The tasks of the SNMP include

- **Monitoring of network components,**
- **Remote control and remote configuration of network components,**
- **Error detection and error notification.**

SNMP agents are running on the devices to be monitored. The agent determine the status of the device, send or provide information. You are the communication partner for the SNMP managers (in our case the OSFM server). The SNMP technology has a long history and is constantly evolving:

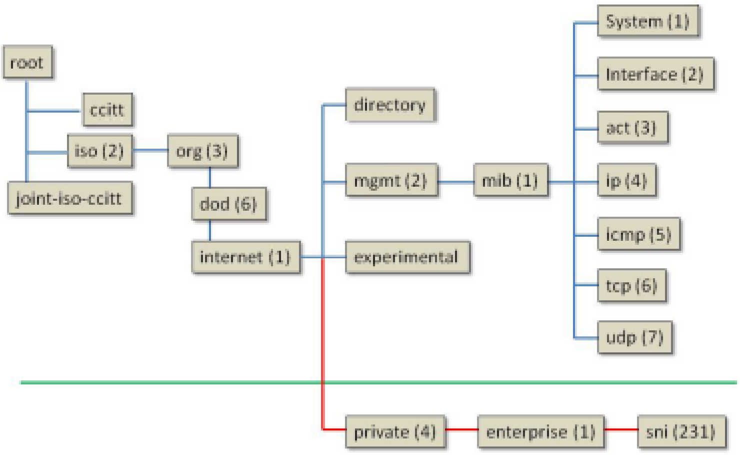
- **SNMPv1 (1988)**
- **SNMPv2c (1993)**
- **SNMPv3 (1998)**

The components of SNMP are

- **Managers and Agents**
- **MIB (Management Information Base), international standard**
- **SMI (Structure of Managed Information)**
- **UDP-based protocol with five protocol data units, PDU types (SNMPv2c)**
- **communication from Manager -> Agents: GET, GETNEXT, SET**
- **communication from Agent -> Manager: GETRESPONSE, TRAP**
- **Password = Community (GET & SET) SNMPv1/v2**
- **Security name, authentication and encryption with SNMPv3**

Management Information Base MIB

The amount and type of data that can be provided with SNMP is defined in the Management Information Base (MIB). A MIB is a data model that describe the managed network components in a defined way. For example, the MIBs for OpenScape communication systems can be downloaded from the WBM (Service Center). The MIB provides a description of basic system information, status information, event-driven data, and information about installed hardware and configured interfaces (ports) that the host provides or traps via the SNMP agent.



Starting with the root, information can be read from the MIB. If allowed write, values can also be changed via SNMP. The MIB-II is a general standard and is normally implemented in all devices.
Via the private branch, company-specific MIBs can be integrated, such as OpenScape 4000 MIB, OpenScape Voice, OpenScape Business or printers, switches or routers, etc...

SNMP commands

Information can be read using the GET command. With the SET command, values can also be changed for certain parameters on the agent. On OpenScape 4000 System, the internal discovery of the systems (using AMO) is started with an SNMP write command.

Communities

Access to SNMP data (MIBs) is controlled by communities. There are a read, write and trap community. Behind each community is an IP address. For example, to enable a PC to read the SNMP data, the IP address of this PC must be entered in the list of reading communities. To get read and write access, the IP address must be entered in the list of the write community. Trap communities are used to manage the recipients of error messages (traps).

Traps

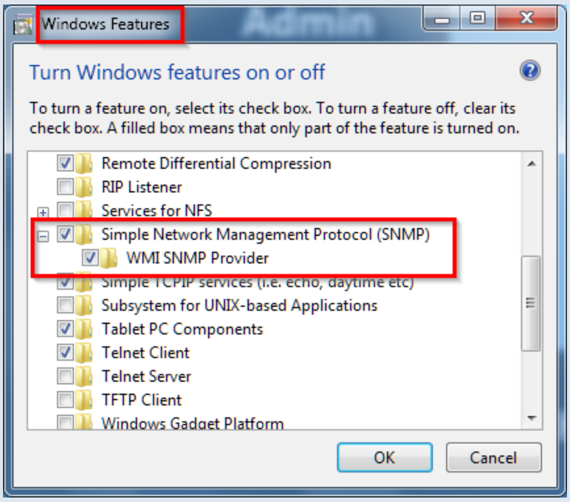
When problems occur in a communication system, traps are generated to inform about errors and failures. There are the following types of traps:

- **system trap = System errors that require immediate action.**
- **performance trap = Information about performance issues that do not require action.**

Traps are classified according to their effect and can be created by an administrator using the WBM can be retrieved.

TASK 1 > Enable Windows SNMP agent

→ **Open "Windows Features", select SNMP service and install**



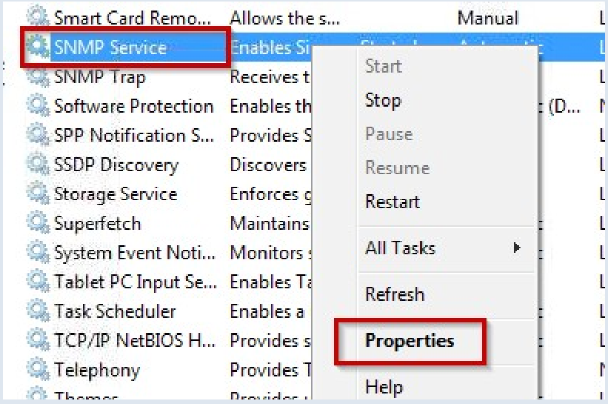
Windows Features

Turn Windows features on or off

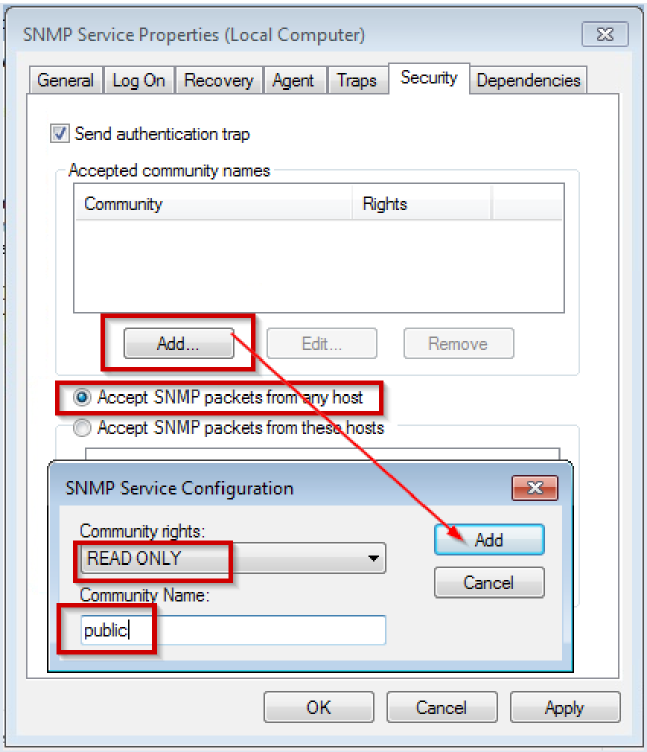
To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- ☑ Remote Differential Compression
- □ RIP Listener
- □ Services for NFS
- ☑ Simple Network Management Protocol (SNMP)
  - ☑ WMI SNMP Provider
- ☑ Simple TCPIP services (i.e. echo, daytime etc)
- □ Subsystem for UNIX-based Applications
- ☑ Tablet PC Components
- ☑ Telnet Client
- □ Telnet Server
- □ TFTP Client
- □ Windows Gadget Platform

→ **Configure Windows SNMP service for access**



Smart Card Remo...	Allows the s...	Manual
SNMP Service	Enables Si	
SNMP Trap	Receives t	
Software Protection	Enables th	(D...
SPP Notification S...	Provides S	
SSDP Discovery	Discovers	
Storage Service	Enforces g	
Superfetch	Maintains	
System Event Noti...	Monitors	
Tablet PC Input Se...	Enables Ta	
Task Scheduler	Enables a	
TCP/IP NetBIOS H...	Provides s	
Telephony	Provides T	



☑ Send authentication trap

Accepted community names

Community	Rights

● Accept SNMP packets from any host

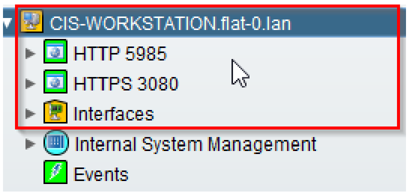
○ Accept SNMP packets from these hosts

Community rights: READ ONLY

Community Name: public

Simple Monitoring

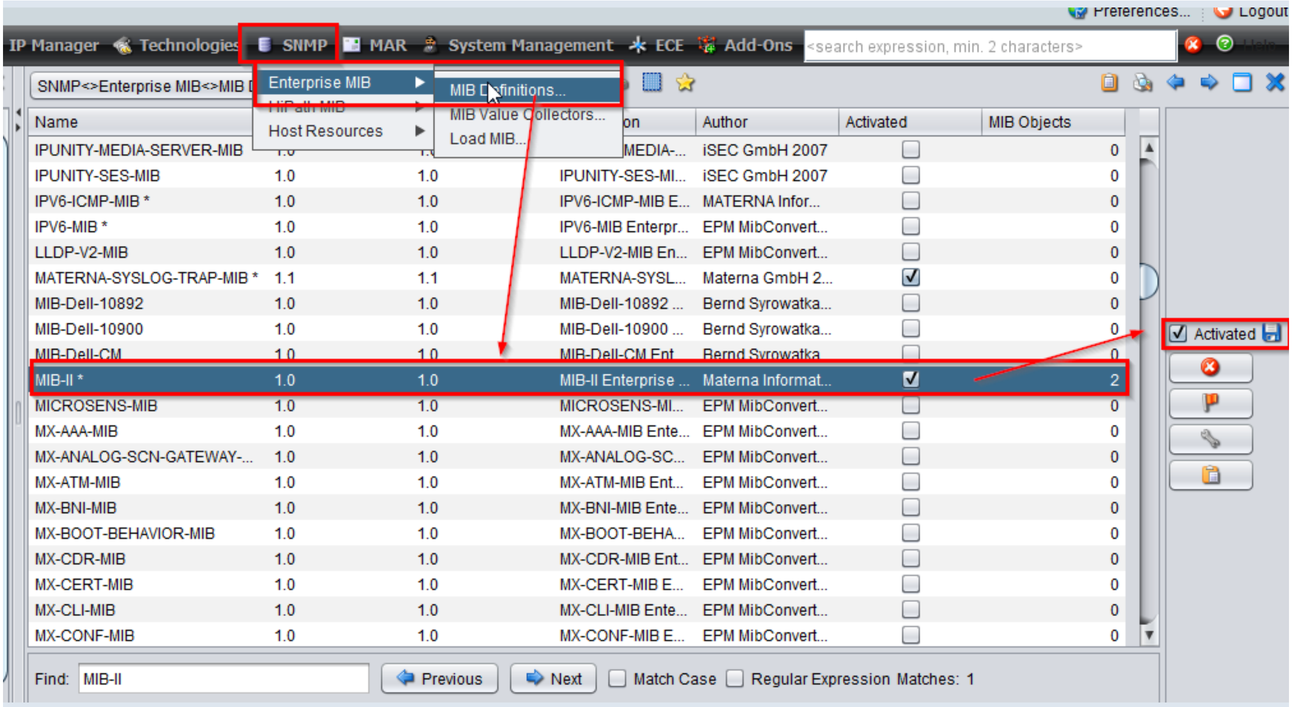
If a host is added to OSFM, a simple monitoring for availability starts automatically. This includes possibly recognized technologies like HTTP, SSH, RDP or SNMP.



If a monitored host provides additional information about the standard SNMP MIB-II, this information can also be used for monitoring.

TASK 2 > Use SNMP MIB-II "Host Resources" for process monitoring

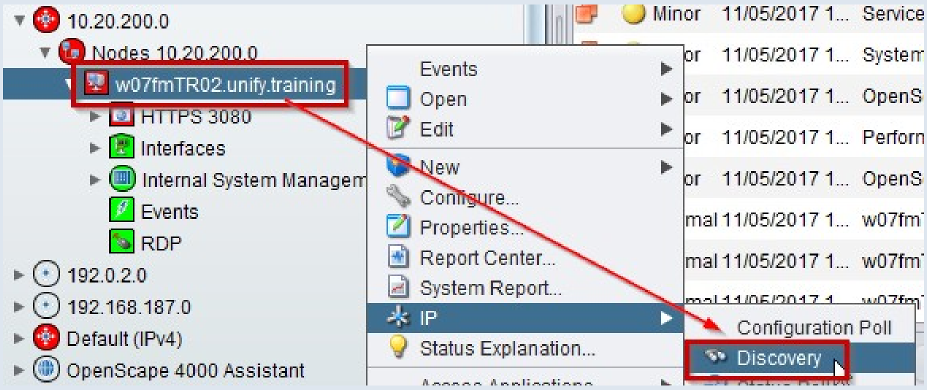
- → **Enable OSFM Server Plugin for Host Resources**
- → **Enable MIB-II detection: Menu → SNMP → Enterprise MIB → MIB Definitions ...**



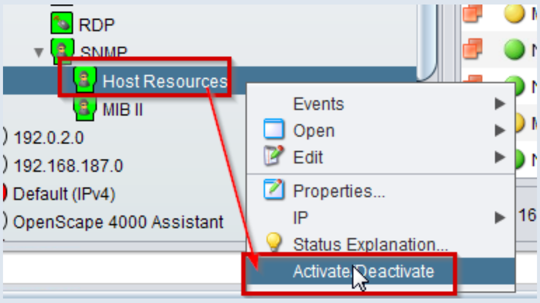
Name			on	Author	Activated	MIB Objects
IPUNITY-MEDIA-SERVER-MIB	1.0	1.0	MEDIA-...	iSEC GmbH 2007	□	0
IPUNITY-SES-MIB	1.0	1.0	IPUNITY-SES-MI...	iSEC GmbH 2007	□	0
IPV6-ICMP-MIB *	1.0	1.0	IPV6-ICMP-MIB E...	MATERNA Infor...	□	0
IPV6-MIB *	1.0	1.0	IPV6-MIB Enterpr...	EPM MibConvert...	□	0
LLDP-V2-MIB	1.0	1.0	LLDP-V2-MIB En...	EPM MibConvert...	□	0
MATERNA-SYSLOG-TRAP-MIB *	1.1	1.1	MATERNA-SYSL...	Materna GmbH 2...	☑	0
MIB-Dell-10892	1.0	1.0	MIB-Dell-10892 ...	Bernd Syrowatka...	□	0
MIB-Dell-10900	1.0	1.0	MIB-Dell-10900 ...	Bernd Syrowatka...	□	0
MIB-Dell-CM	1.0	1.0	MIB-Dell-CM Ent	Bernd Syrowatka	□	0
MIB-II *	1.0	1.0	MIB-II Enterprise ...	Materna Informat...	☑	2
MICROSENS-MIB	1.0	1.0	MICROSENS-MI...	EPM MibConvert...	□	0
MX-AAA-MIB	1.0	1.0	MX-AAA-MIB Ente...	EPM MibConvert...	□	0
MX-ANALOG-SCN-GATEWAY-...	1.0	1.0	MX-ANALOG-SC...	EPM MibConvert...	□	0
MX-ATM-MIB	1.0	1.0	MX-ATM-MIB Ent...	EPM MibConvert...	□	0
MX-BNI-MIB	1.0	1.0	MX-BNI-MIB Ente...	EPM MibConvert...	□	0
MX-BOOT-BEHAVIOR-MIB	1.0	1.0	MX-BOOT-BEHA...	EPM MibConvert...	□	0
MX-CDR-MIB	1.0	1.0	MX-CDR-MIB Ent...	EPM MibConvert...	□	0
MX-CERT-MIB	1.0	1.0	MX-CERT-MIB E...	EPM MibConvert...	□	0
MX-CLI-MIB	1.0	1.0	MX-CLI-MIB Ente...	EPM MibConvert...	□	0
MX-CONF-MIB	1.0	1.0	MX-CONF-MIB E...	EPM MibConvert...	□	0

Find: MIB-II Previous Next □ Match Case □ Regular Expression Matches: 1

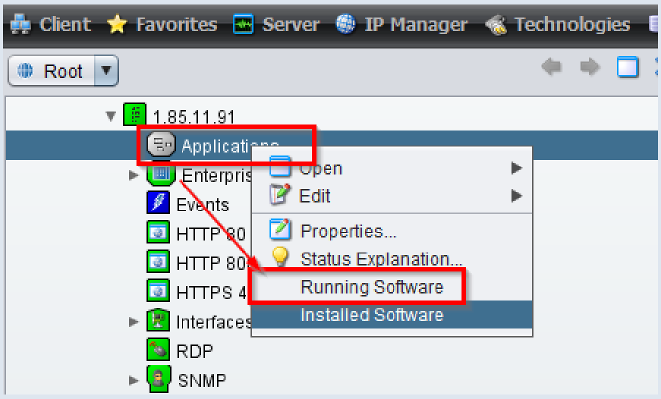
→ Start Discovery for Detection on the OSFM Host Object



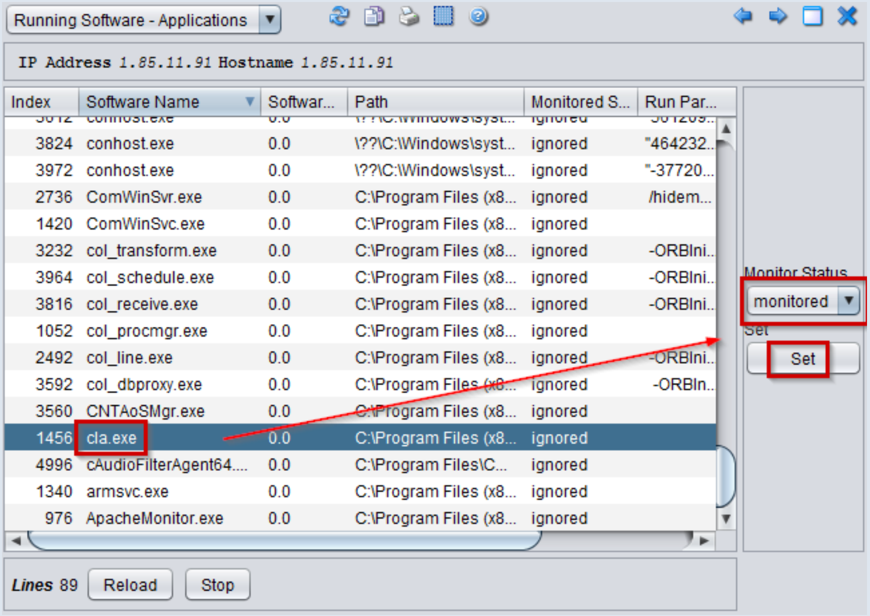
→ Enable SNMP "Hostressources" via context menu



→ Activate context menu on new object "Applications" select "Running Software"



→ Set process "cla.exe" to status "monitored"



IP Address 1.85.11.91 Hostname 1.85.11.91

Index	Software Name	Softwar...	Path	Monitored S...	Run Par...
3824	conhost.exe	0.0	\??\C:\Windows\syst...	ignored	"464232...
3972	conhost.exe	0.0	\??\C:\Windows\syst...	ignored	"-37720...
2736	ComWinSvr.exe	0.0	C:\Program Files (x8...	ignored	/hidem...
1420	ComWinSvc.exe	0.0	C:\Program Files (x8...	ignored	
3232	col_transform.exe	0.0	C:\Program Files (x8...	ignored	-ORBIni...
3964	col_schedule.exe	0.0	C:\Program Files (x8...	ignored	-ORBIni...
3816	col_receive.exe	0.0	C:\Program Files (x8...	ignored	-ORBIni...
1052	col_procmgr.exe	0.0	C:\Program Files (x8...	ignored	
2492	col_line.exe	0.0	C:\Program Files (x8...	ignored	-ORBIni...
3592	col_dbproxy.exe	0.0	C:\Program Files (x8...	ignored	-ORBIn...
3560	CNTAoSMgr.exe	0.0	C:\Program Files (x8...	ignored	
1456	cla.exe	0.0	C:\Program Files (x8...	ignored	
4996	cAudioFilterAgent64....	0.0	C:\Program Files\C...	ignored	
1340	armsvc.exe	0.0	C:\Program Files (x8...	ignored	
976	ApacheMonitor.exe	0.0	C:\Program Files (x8...	ignored	

Lines 89

→ An object "cla.exe" is created and has the status of the process.

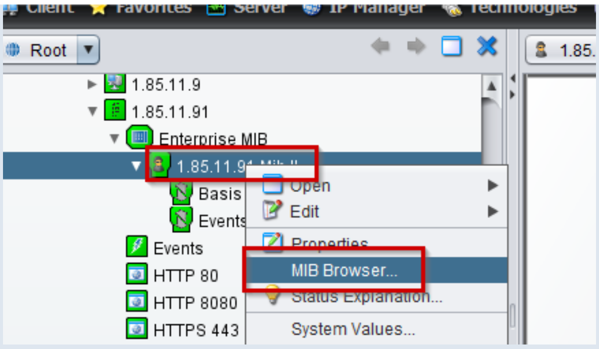
CRITICAL=not running, NORMAL=running

→ Set "Status Polling" to 1 minute ("Configure" on host object...) and close process "cla.exe".

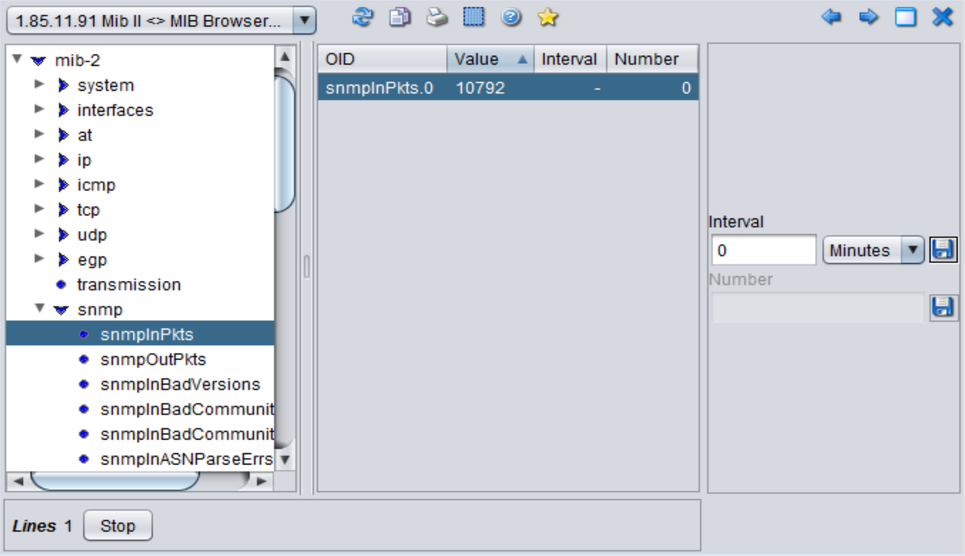
→ Wait and acknowledge new critical event. Afterwards restart CLA service.

TASK 3 > Monitor single parameters from SNMP MIB-II (polling)

→ Start MIB-Browser via context menu on the MIB-II object below "Enterprise MIB"



→ **Select a variable from the MIB-II tree, e.g. snmp -> snmpInPkts**



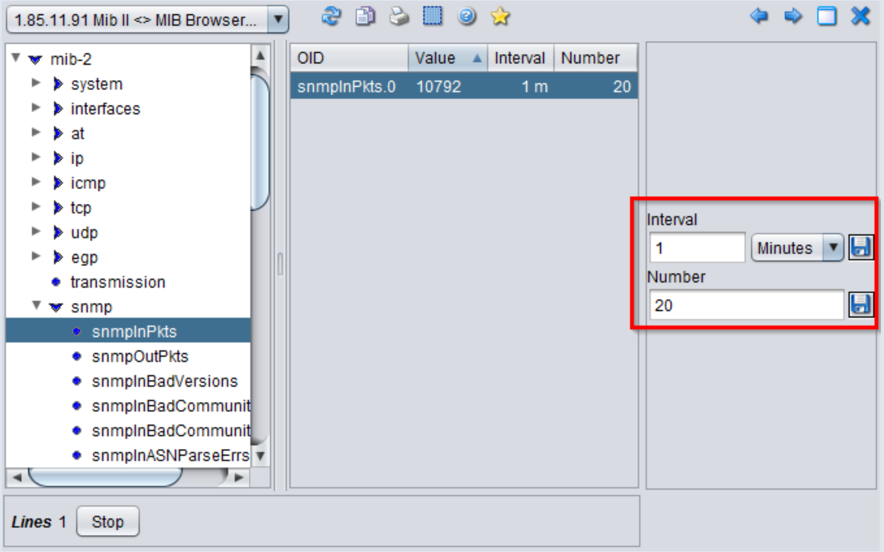
OID	Value	Interval	Number
snmpInPkts.0	10792	-	0

Interval: 0 Minutes

Number:

Lines 1

→ **Specify and save a query interval and the number of stored values.**



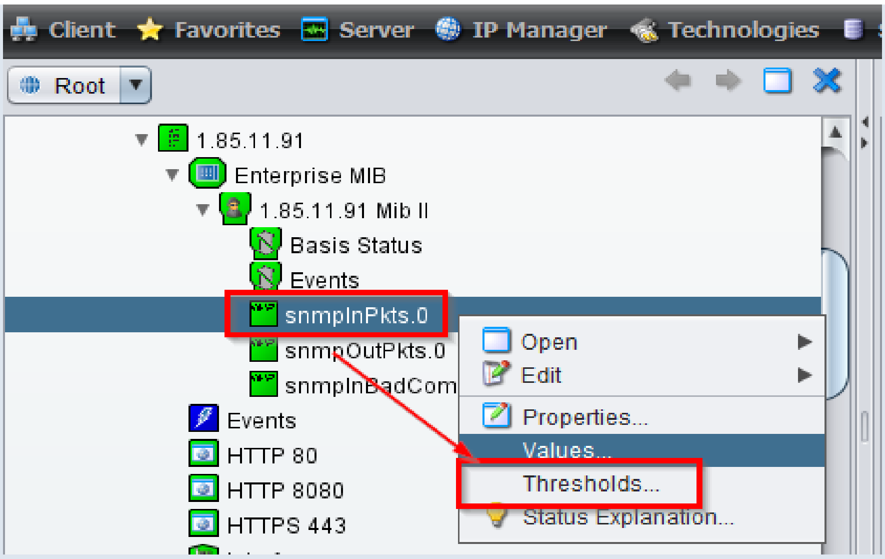
OID	Value	Interval	Number
snmpInPkts.0	10792	1 m	20

Interval: 1 Minutes

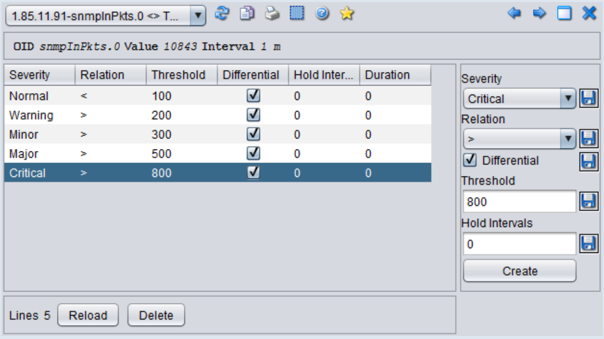
Number: 20

Lines 1

→ **A new object "snmpInPkts" is created**



→ **Thresholds can be defined in the context menu of the new object.**



1.85.11.91-snmpInPkts.0 <> T...

OID *snmpInPkts.0* Value *10843* Interval *1 m*

Severity	Relation	Threshold	Differential	Hold Inter...	Duration
Normal	<	100	☑	0	0
Warning	>	200	☑	0	0
Minor	>	300	☑	0	0
Major	>	500	☑	0	0
Critical	>	800	☑	0	0

Severity: Critical
Relation: >
☑ Differential
Threshold: 800
Hold Intervals: 0

Threshold value definition for **numeric values**

- **Severity: choose between Normal, Warning, Minor, Major, Critical**
- **Relation: Relation to apply <, <=, =, >=, >, !=.**
- **Differential: select differential, if the difference to the pervious value should be used**
- **Threshold: the threshold value used in the relation**
- **Hold Intervals: the number of intervals a threshold will be a least active**

Threshold value definition for **string values**

- **Severity: choose between Normal, Warning, Minor, Major, Critical**
- **Relation: Relation to apply =, !=, SimplRegExp, RegExp.**
- **Threshold: the threshold value used in the relation**
- **Hold Intervals: the number of intervals a threshold will be a least active**

Advanced Monitoring

If the information from the simple monitoring is not sufficient, any data can be queried with the Advanced Monitoring. This is done by

- **script or app (Java, Executable, Javascript, Powershell, Shellscript) executed and collected by (System Management) Agent**
- **Add and query a manufacturer Enterprise MIB**

One license per host is required for Advanced Monitoring.

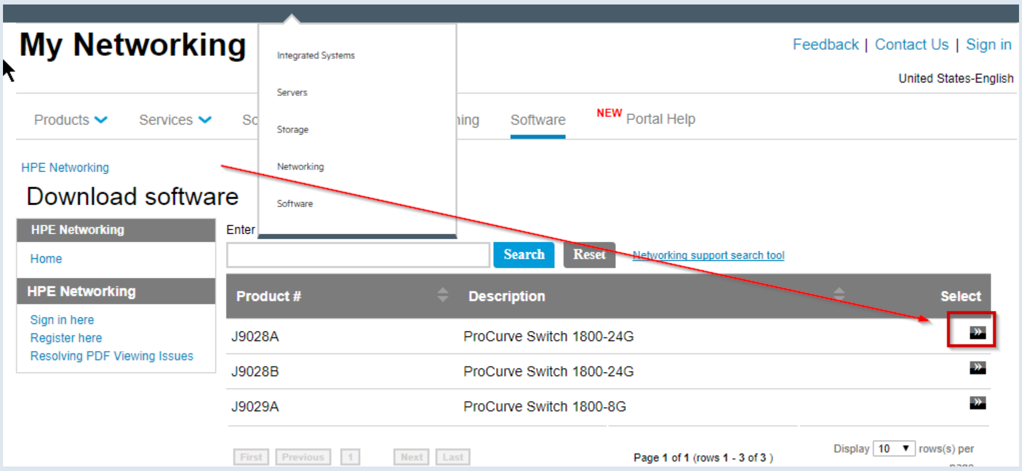
Using an Enterprise MIB from the device manufacturer

The manufacturer of a device can use SNMP agents to provide considerably more information than the MIB-II. Therefore it is necessary to add every Enterprise MIB to OSFM Server in order to query it.

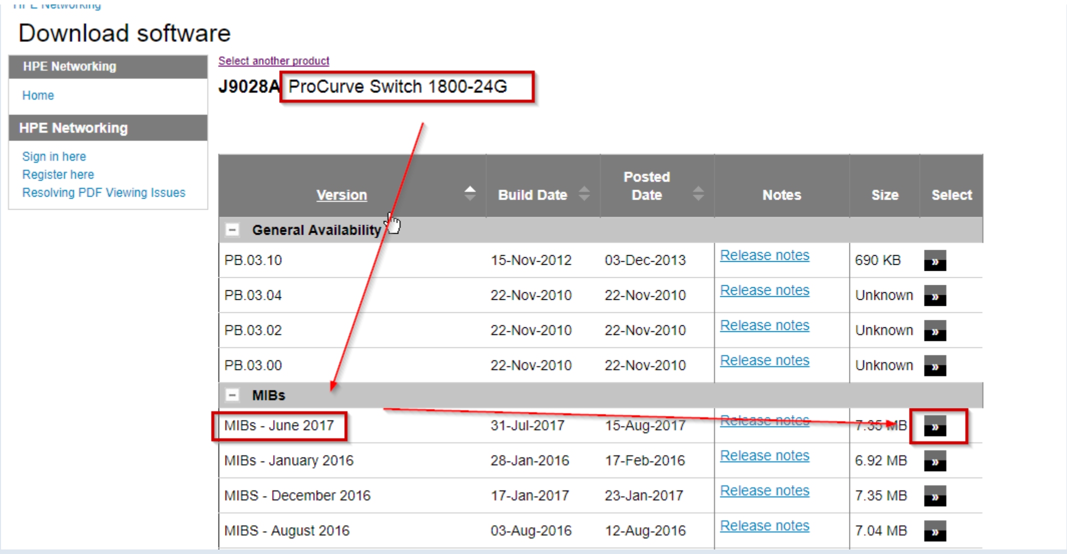
TASK 4 > Use SNMP Enterprise MIB, e.g HP Switch

→ **Download of the MIB files from the manufacturer Website:**

→ https://h10145.www1.hpe.com/Downloads/ProductsList.aspx?lang=en&cc=us&prodSeriesId=3231819



Product #	Description	Select
J9028A	ProCurve Switch 1800-24G	»
J9028B	ProCurve Switch 1800-24G	»
J9029A	ProCurve Switch 1800-8G	»

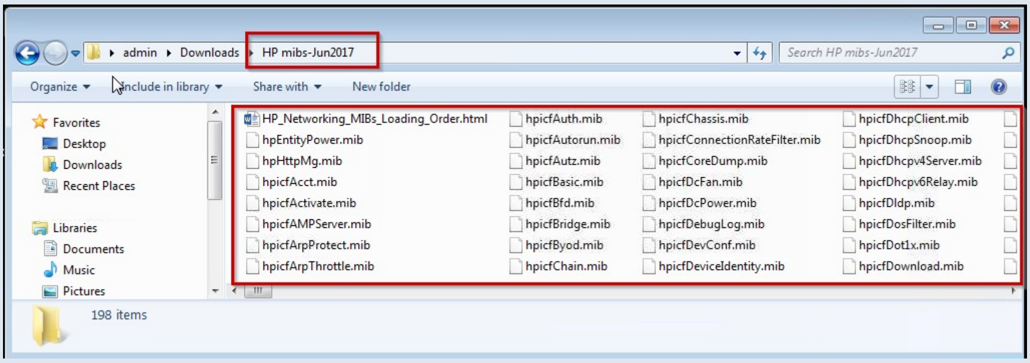


Download software

J9028A ProCurve Switch 1800-24G

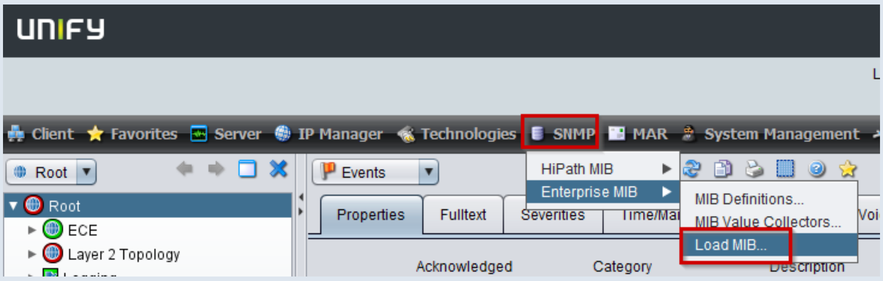
Version	Build Date	Posted Date	Notes	Size	Select
General Availability					
PB.03.10	15-Nov-2012	03-Dec-2013	Release notes	690 KB	»
PB.03.04	22-Nov-2010	22-Nov-2010	Release notes	Unknown	»
PB.03.02	22-Nov-2010	22-Nov-2010	Release notes	Unknown	»
PB.03.00	22-Nov-2010	22-Nov-2010	Release notes	Unknown	»
MIBs					
MIBs - June 2017	31-Jul-2017	15-Aug-2017	Release notes	7.35 MB	»
MIBs - January 2016	28-Jan-2016	17-Feb-2016	Release notes	6.92 MB	»
MIBS - December 2016	17-Jan-2017	23-Jan-2017	Release notes	7.35 MB	»
MIBS - August 2016	03-Aug-2016	12-Aug-2016	Release notes	7.04 MB	»

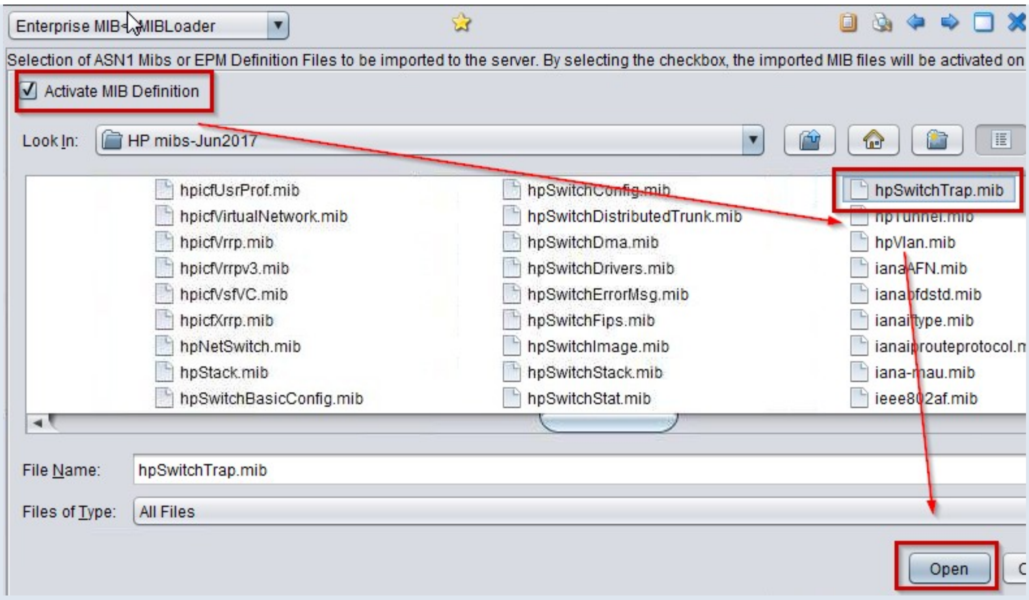
→ **Unpacking Mib Files = *.mib. You can load all MIB-Files (CTRL-A) or a selection**



HP_Networking_MIBs_Loading_Order.html
hpEntityPower.mib
hpHttpMg.mib
hpicfAcct.mib
hpicfActivate.mib
hpicfAMPServer.mib
hpicfArpProtect.mib
hpicfArpThrottle.mib
hpicfAuth.mib
hpicfAutorun.mib
hpicfAutz.mib
hpicfBasic.mib
hpicfBfd.mib
hpicfBridge.mib
hpicfByod.mib
hpicfChain.mib
hpicfChassis.mib
hpicfConnectionRateFilter.mib
hpicfCoreDump.mib
hpicfDcFan.mib
hpicfDcPower.mib
hpicfDebugLog.mib
hpicfDevConf.mib
hpicfDeviceIdentity.mib
hpicfDhcpClient.mib
hpicfDhcpSnoop.mib
hpicfDhcpv4Server.mib
hpicfDhcpv6Relay.mib
hpicfDldp.mib
hpicfDosFilter.mib
hpicfDot1x.mib
hpicfDownload.mib

→ **If Traps are defined in a MIB, it's neccesary to configure Severity: e.g. "hpSwitchTrap.mib"**





Enterprise MIB<>MIBLoader

Selection of ASN1 Mibs or EPM Definition Files to be imported to the server. By selecting the checkbox, the imported MIB files will be activated on

☑ Activate MIB Definition

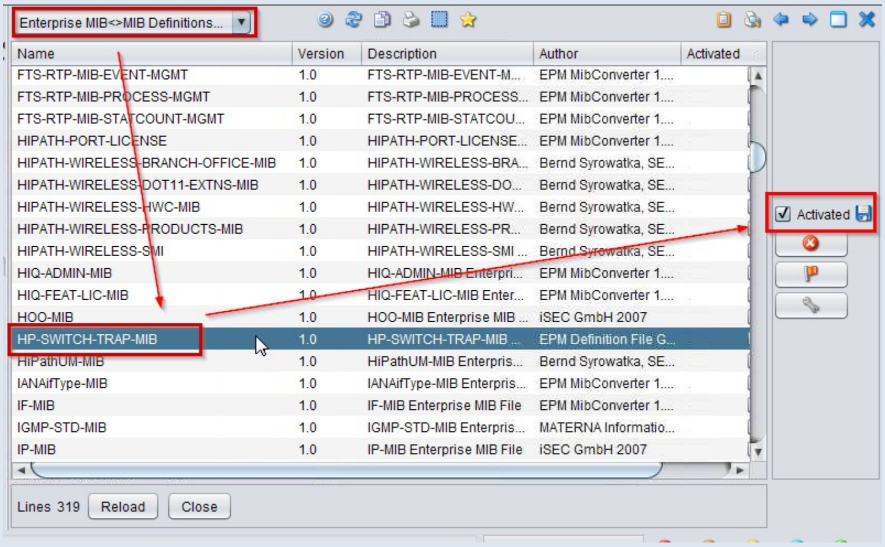
Look In: HP mibs-Jun2017

hpicfUsrProf.mib
hpicfVirtualNetwork.mib
hpicfVrrp.mib
hpicfVrrpv3.mib
hpicfVsfVC.mib
hpicfXrrp.mib
hpNetSwitch.mib
hpStack.mib
hpSwitchBasicConfig.mib
hpSwitchConfig.mib
hpSwitchDistributedTrunk.mib
hpSwitchDma.mib
hpSwitchDrivers.mib
hpSwitchErrorMsg.mib
hpSwitchFips.mib
hpSwitchImage.mib
hpSwitchStack.mib
hpSwitchStat.mib
hpSwitchTrap.mib
hpTunnel.mib
hpVlan.mib
ianaAFN.mib
ianabfdstd.mib
ianaiftype.mib
ianaiprouteprotocol.m
iana-mau.mib
ieee802af.mib

File Name: hpSwitchTrap.mib

Files of Type: All Files

→ **Activate MIB (to use it in host discovery) in the list of all known MIBs**



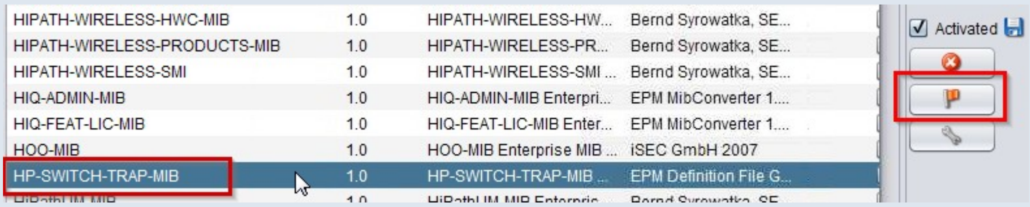
Enterprise MIB<>MIB Definitions...

Name	Version	Description	Author	Activated
FTS-RTP-MIB-EVENT-MGMT	1.0	FTS-RTP-MIB-EVENT-M...	EPM MibConverter 1....	
FTS-RTP-MIB-PROCESS-MGMT	1.0	FTS-RTP-MIB-PROCESS...	EPM MibConverter 1....	
FTS-RTP-MIB-STATCOUNT-MGMT	1.0	FTS-RTP-MIB-STATCOU...	EPM MibConverter 1....	
HIPATH-PORT-LICENSE	1.0	HIPATH-PORT-LICENSE...	EPM MibConverter 1....	
HIPATH-WIRELESS-BRANCH-OFFICE-MIB	1.0	HIPATH-WIRELESS-BRA...	Bernd Syrowatka, SE...	
HIPATH-WIRELESS-DOT11-EXTNS-MIB	1.0	HIPATH-WIRELESS-DO...	Bernd Syrowatka, SE...	
HIPATH-WIRELESS-HWC-MIB	1.0	HIPATH-WIRELESS-HW...	Bernd Syrowatka, SE...	
HIPATH-WIRELESS-PRODUCTS-MIB	1.0	HIPATH-WIRELESS-PR...	Bernd Syrowatka, SE...	
HIPATH-WIRELESS-SMI	1.0	HIPATH-WIRELESS-SMI ...	Bernd Syrowatka, SE...	
HIQ-ADMIN-MIB	1.0	HIQ-ADMIN-MIB Enterpri...	EPM MibConverter 1....	
HIQ-FEAT-LIC-MIB	1.0	HIQ-FEAT-LIC-MIB Enter...	EPM MibConverter 1....	
HOO-MIB	1.0	HOO-MIB Enterprise MIB ...	iSEC GmbH 2007	
HP-SWITCH-TRAP-MIB	1.0	HP-SWITCH-TRAP-MIB ...	EPM Definition File G...	
HiPathUM-MIB	1.0	HiPathUM-MIB Enterpris...	Bernd Syrowatka, SE...	
IANAifType-MIB	1.0	IANAifType-MIB Enterpris...	EPM MibConverter 1....	
IF-MIB	1.0	IF-MIB Enterprise MIB File	EPM MibConverter 1....	
IGMP-STD-MIB	1.0	IGMP-STD-MIB Enterpris...	MATERNA Informatio...	
IP-MIB	1.0	IP-MIB Enterprise MIB File	iSEC GmbH 2007	

☑ Activated

Lines 319

→ **Configuring Event Configuration for Traps of this MIB**

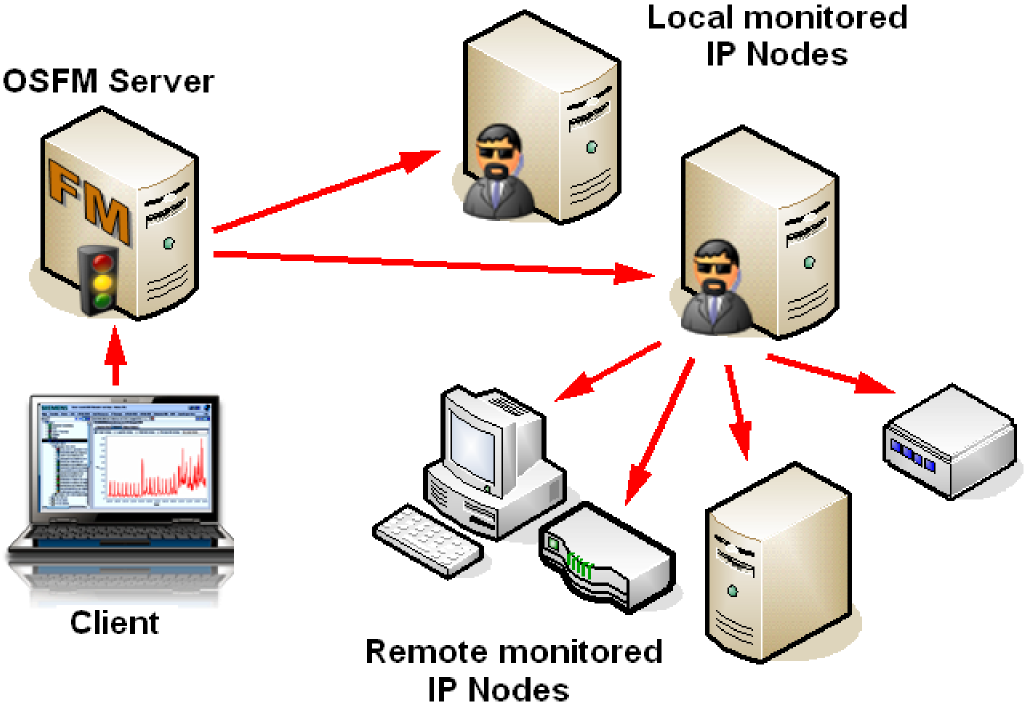


HIPATH-WIRELESS-HWC-MIB	1.0	HIPATH-WIRELESS-HW...	Bernd Syrowatka, SE...
HIPATH-WIRELESS-PRODUCTS-MIB	1.0	HIPATH-WIRELESS-PR...	Bernd Syrowatka, SE...
HIPATH-WIRELESS-SMI	1.0	HIPATH-WIRELESS-SMI ...	Bernd Syrowatka, SE...
HIQ-ADMIN-MIB	1.0	HIQ-ADMIN-MIB Enterpri...	EPM MibConverter 1....
HIQ-FEAT-LIC-MIB	1.0	HIQ-FEAT-LIC-MIB Enter...	EPM MibConverter 1....
HOO-MIB	1.0	HOO-MIB Enterprise MIB ...	iSEC GmbH 2007
HP-SWITCH-TRAP-MIB	1.0	HP-SWITCH-TRAP-MIB ...	EPM Definition File G...
HiPathUM-MIB	1.0	HiPathUM-MIB Enterpris...	Bernd Syrowatka, SE...

☑ Activated

Using the System Management Agent(s)

In case of the absence of SNMP or security issues (Firewall), Agents can collect any information from the device. The Agent uses scripts or apps to retrieve information from a host and provide it as objects in OSFM. In OSFM, Advanced Monitoring provided via the feature "System Management" and is ready to use out-of-the-box with many monitoring templates. It can be extended by the administrator, so practically any information of a host can be queried, as long as it can communicate in the network.



The System Management Agent is a Java-based, generic agent. It provides basic functions such as communication with the server, time-controlled execution of monitoring functions or persistent data storage of the determined parameter data. The actual monitoring functions are implemented by scripts, which the agent executes at certain times or in time intervals. These scripts return their results in a defined format, which can be evaluated and processed by the agent. The scripts can be easily modified, replaced or extended to allow new/changed monitoring functions.

The monitoring functions are defined in XML files. Due to the easy extensibility of the agent e.g. new scripts allow the agent to be quickly adapted to the constantly changing requirements of system management. A System Management Agent can also be used as a proxy agent. In this case, the agent monitors system parameters on remote systems over the network.

System Management Functions at a Glance:

- **Java based generic System Management Agent to monitor arbitrary system parameters via scripts**
- **Automatic discovery of System Management Agents in the network by the System Management Plugin for OpenScape FM.**
- **History of monitored system parameters**
- **Proxy functionality for remote systems**
- **Easily expandable (new monitoring functions through scripts)**
- **Event messages to the OpenScape FM in case of critical system states (e.g memory usage >90%)**
- **Graphical representation of the monitored parameters within a hierarchical structure at the OpenScape FM.**
- **Graphical status representation**
- **Log-file monitoring by System Management Agents. Event messages in case of the appearance of defined search patterns.**

The monitoring of systems and system parameters is performed by one or more System Management Agents. An System Management Agent can either be installed locally on the system it monitors, as a so called Internal Agent, or on a separate system. In the second case, the agent remotely monitors the target system as a so called Proxy Agent. To enable a remote monitoring, specific interfaces for remote access must be available on the target system (e. g. WMI for Windows systems or Remote Shell for Unix systems). In many cases, a user account has to be created to grant access for the System Management agent to the target system.

OSFM knows two types of Agents, both are technically identical, but

the internal agent

- **is installed by activating the System Management Plugin**
- **is started and stopped with OSFM Server service**
- **can be activated or deactivated within OSFM GUI**

the standalone agent

- **runs as Windows/Linux service**
- **can be installed on any host providing a Java Runtime**
- **must be unique on the host, don't install it on the OSFM it will crash the internal agent**

Monitoring Profiles und Monitore

The agents can execute Monitors, which is a script or a program. Monitors can be pooled to Monitoring Profiles and one Monitor can check several Parameters. They are configurable via the GUI.

- **Monitored IP Nodes**
- **Execution time interval**

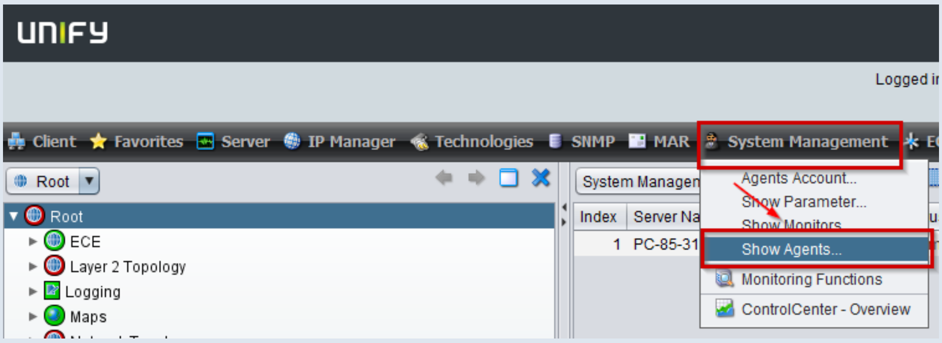
- Parameters
- Threshold

Adding a new monitor

- 1. Select agent (to configure a new monitoring)
- 2. Select which information to retrieve (one more more monitor templates)
- 3. select target systems, which should be monitored

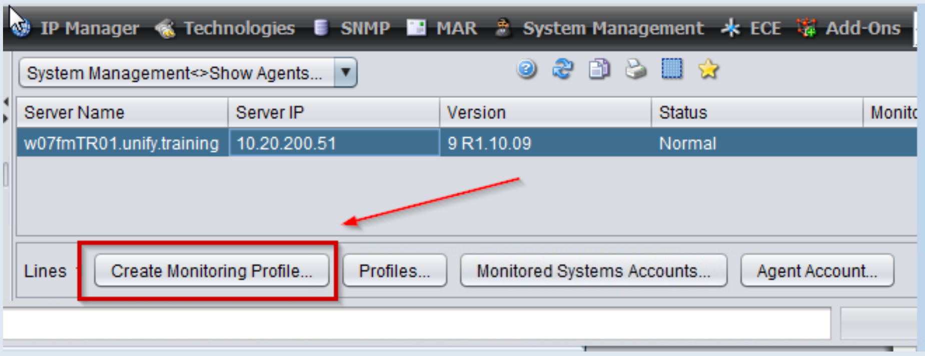
TASK 5 > Monitoring MySQL Server database availability

→ Menu -> "System Management" -> "Show Agents"



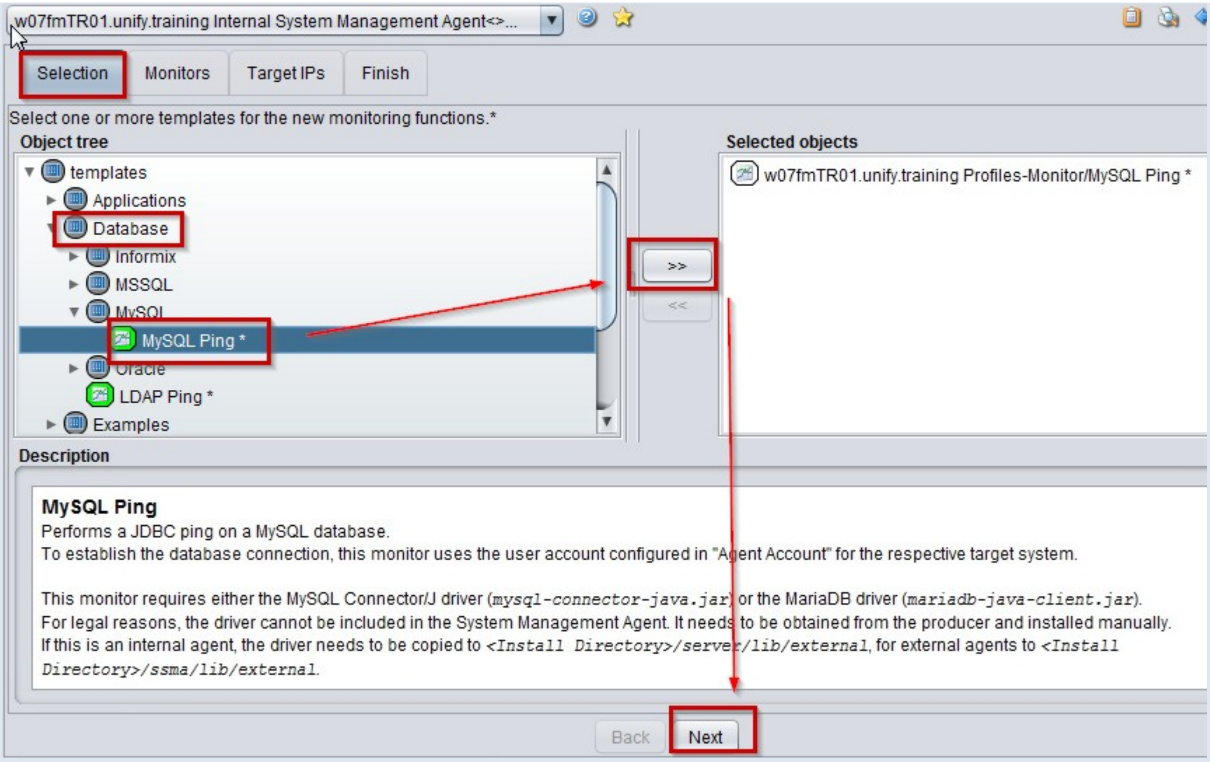
Index	Server Na
1	PC-85-31

→ Select "Create Monitoring Profile ..."


IP Manager
Technologies
SNMP
MAR
System Management
ECE
Add-Ons
System Management<>Show Agents...
Lines
Create Monitoring Profile...
Profiles...
Monitored Systems Accounts...
Agent Account...

Server Name	Server IP	Version	Status	Monitc
w07fmTR01.unify.training	10.20.200.51	9 R1.10.09	Normal	

→ Select Template -> "Database" > "MySQL"- "MySQL Ping" and add with ">>"



w07fmTR01.unify.training Internal System Management Agent<>...

Select one or more templates for the new monitoring functions.*

Object tree

- templates
  - Applications
  - Database
    - Informix
    - MSSQL
    - MySQL
      - MySQL Ping *
    - Oracle
    - LDAP Ping *
  - Examples

Selected objects

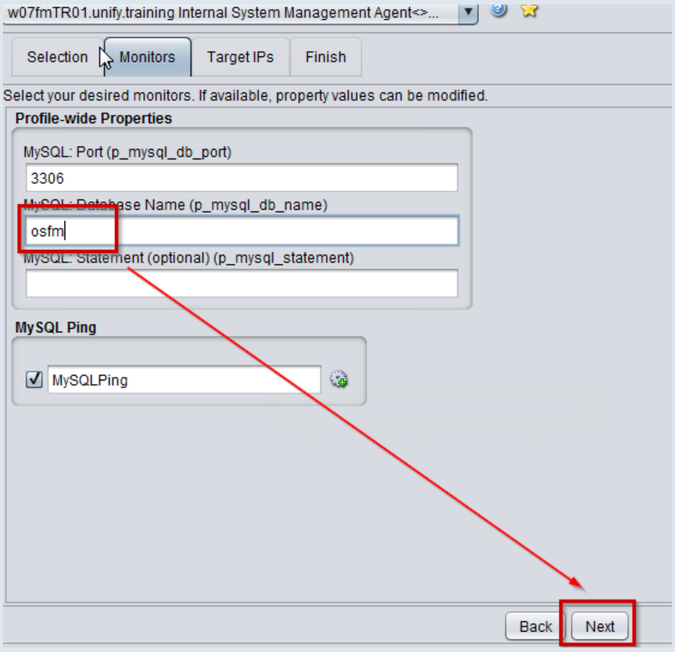
w07fmTR01.unify.training Profiles-Monitor/MySQL Ping *

Description

MySQL Ping
Performs a JDBC ping on a MySQL database.
To establish the database connection, this monitor uses the user account configured in "Agent Account" for the respective target system.

This monitor requires either the MySQL Connector/J driver (`mysql-connector-java.jar`) or the MariaDB driver (`mariadb-java-client.jar`).
For legal reasons, the driver cannot be included in the System Management Agent. It needs to be obtained from the producer and installed manually.
If this is an internal agent, the driver needs to be copied to `<Install Directory>/server/lib/external`, for external agents to `<Install Directory>/ssma/lib/external`.

→ **Give „Database Name“**



w07fmTR01.unify.training Internal System Management Agent<>...

Select your desired monitors. If available, property values can be modified.

Profile-wide Properties

MySQL: Port (p_mysql_db_port): 3306

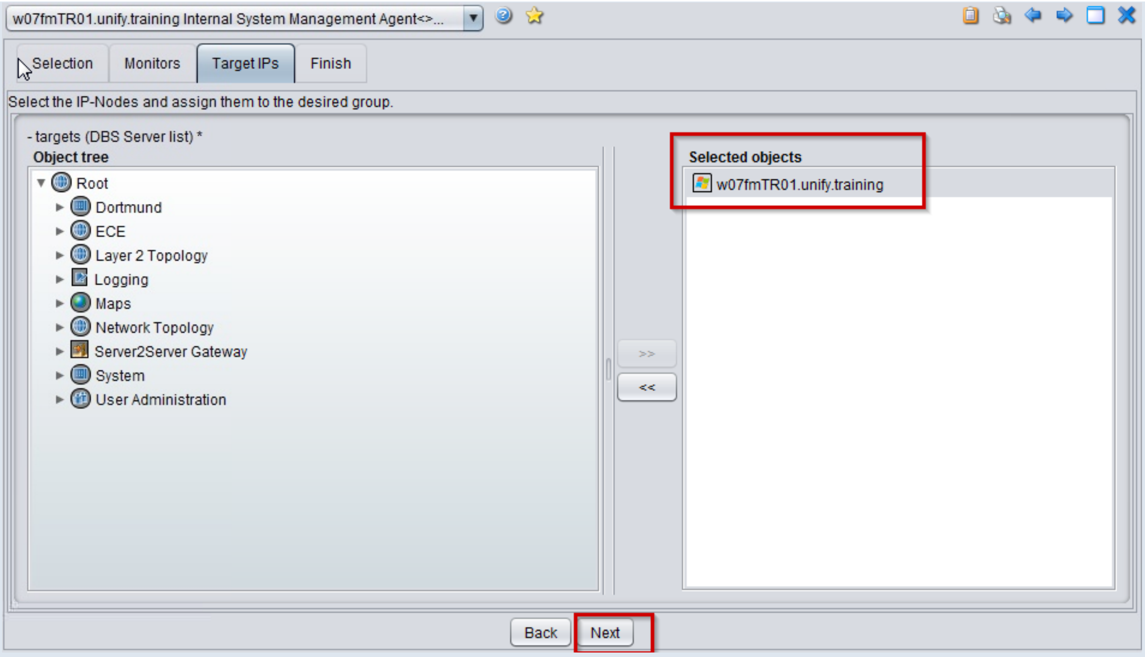
MySQL: Database Name (p_mysql_db_name): osfm

MySQL: Statement (optional) (p_mysql_statement):

MySQL Ping

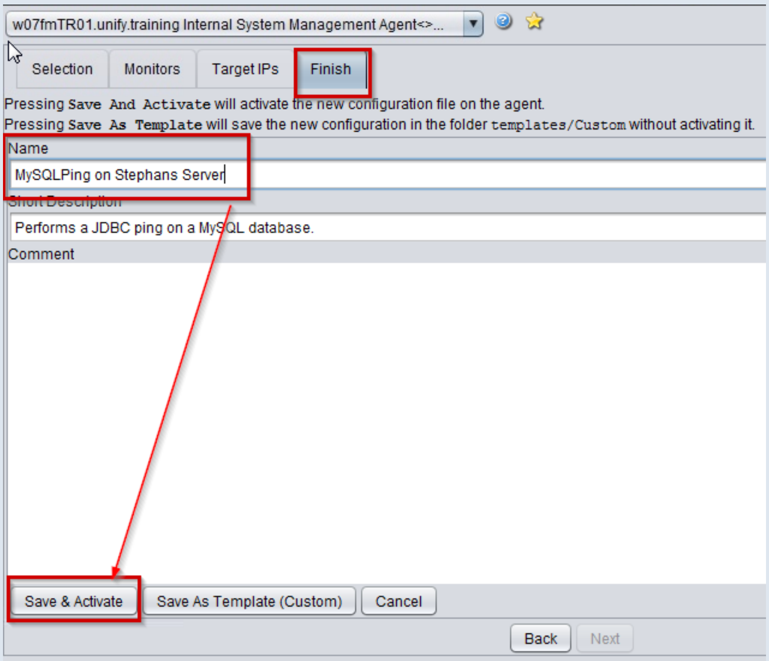
☑ MySQLPing

→ **Give one or more target systems. By default the OSFM-Server is target system, remove it if nessecary**



Select the IP-Nodes and assign them to the desired group.

→ **Name the new monitoring profile and "Save & Activate"**



w07fmTR01.unify.training Internal System Management Agent<>...
Selection
Monitors
Target IPs
Finish
Save & Activate
Save As Template (Custom)
Cancel
Back
Next

Pressing `Save And Activate` will activate the new configuration file on the agent.
Pressing `Save As Template` will save the new configuration in the folder `templates/Custom` without activating it.

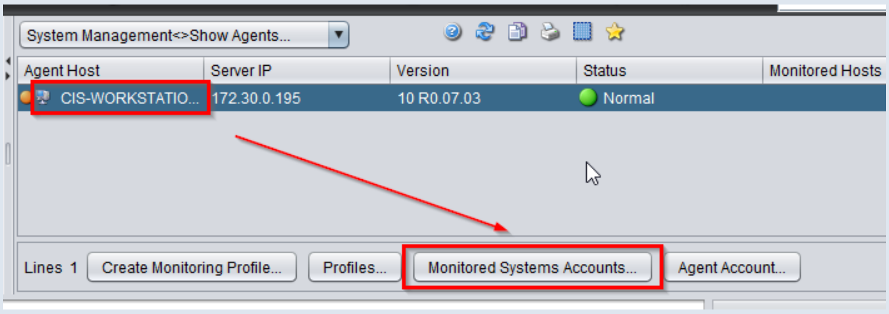
Name: MySQLPing on Stephans Server

Short Description: Performs a JDBC ping on a MySQL database.

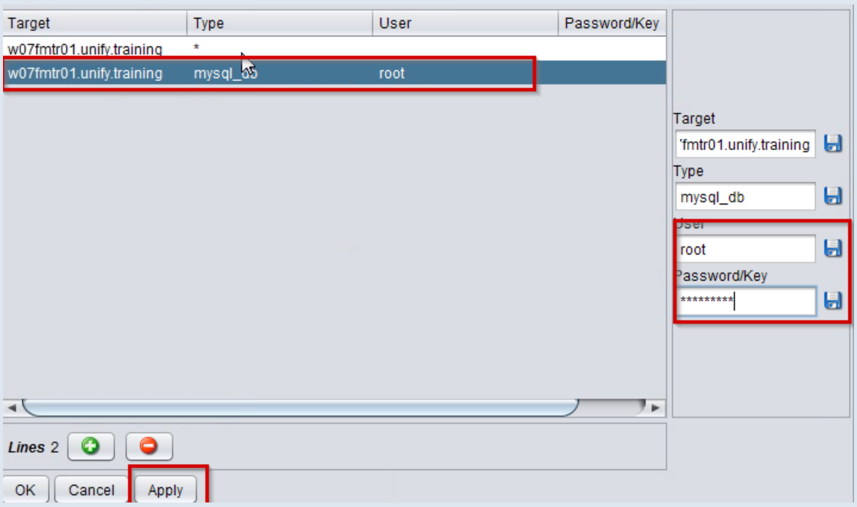
Comment

→ **Afterwards: configure username/passwd for access:**

"System Management" -> "Show Agents" → „Monitored System Accounts“


System Management<>Show Agents...
Lines 1
Create Monitoring Profile...
Profiles...
Monitored Systems Accounts...
Agent Account...

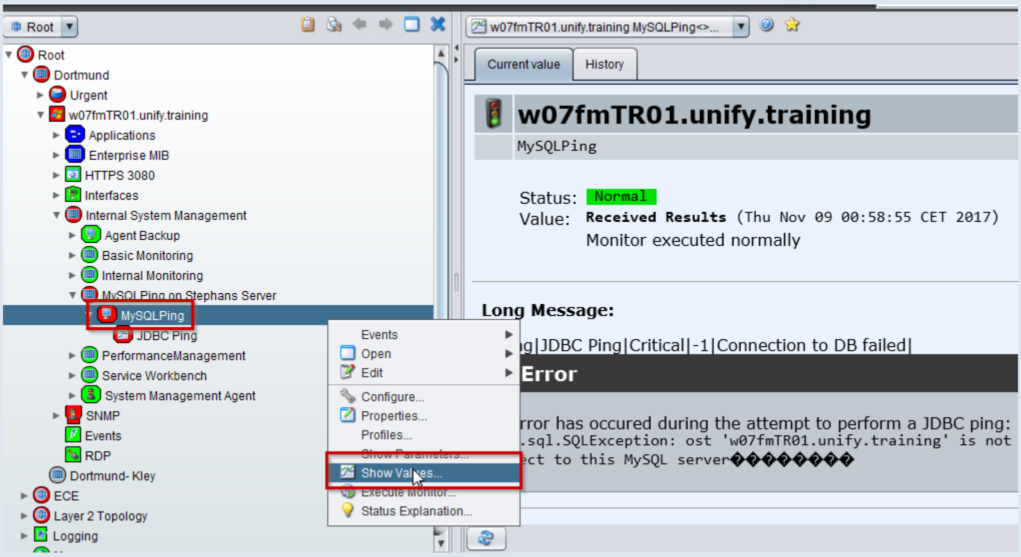
Agent Host	Server IP	Version	Status	Monitored Hosts
CIS-WORKSTATIO...	172.30.0.195	10 R0.07.03	Normal	



Target	Type	User	Password/Key
w07fmtr01.unify.training	*		
w07fmtr01.unify.training	mysql_db	root	

Target: 'fmtr01.unify.training
Type: mysql_db
User: root
Password/Key: *********

→ **On the new created object, select context menu->"Show Values"**



w07fmTR01.unify.training
MySQLPing

Status: Normal
Value: **Received Results** (Thu Nov 09 00:58:55 CET 2017)
Monitor executed normally

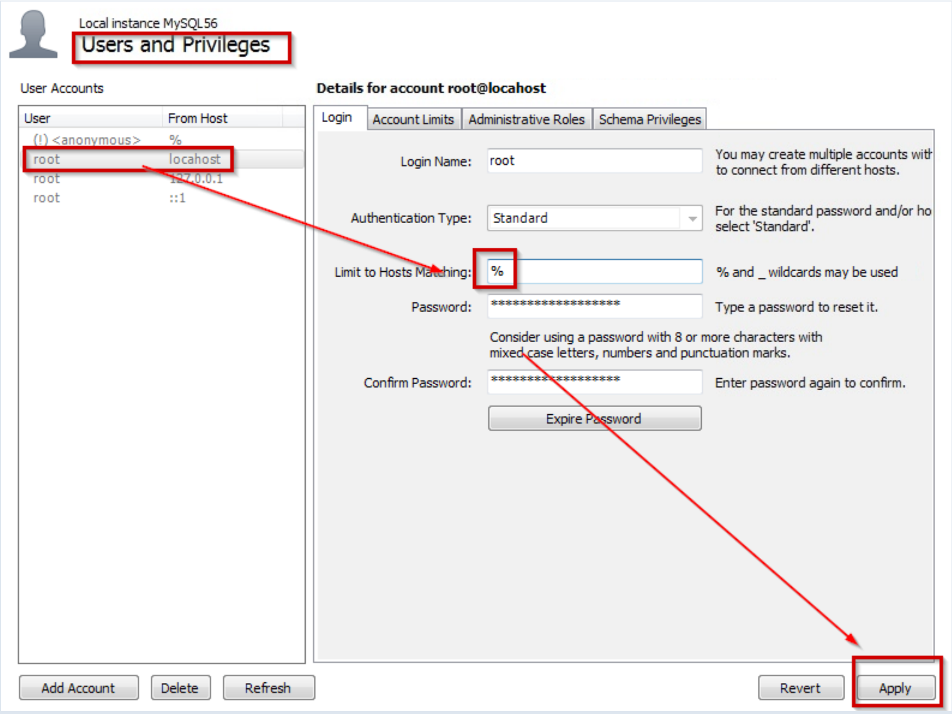
Long Message:

g|JDBC Ping|Critical|-1|Connection to DB failed|

Error

```
rror has occured during the attempt to perform a JDBC ping:
.sql.SQLException: ost 'w07fmTR01.unify.training' is not
ct to this MySQL server��������
```

→ **In case of an MySQL-Server connection error: configure user in MySQL to connect from network**



Local instance MySQL56

Users and Privileges

User Accounts

User	From Host
(!) <anonymous>	%
root	locahost
root	127.0.0.1
root	::1

Details for account root@locahost

Login Name: root

You may create multiple accounts with to connect from different hosts.

Authentication Type: Standard

For the standard password and/or ho select 'Standard'.

Limit to Hosts Matching: %

% and _ wildcards may be used

Password: ******************

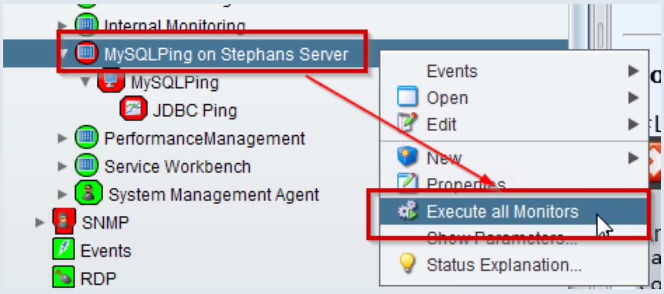
Type a password to reset it.

Consider using a password with 8 or more characters with mixed case letters, numbers and punctuation marks.

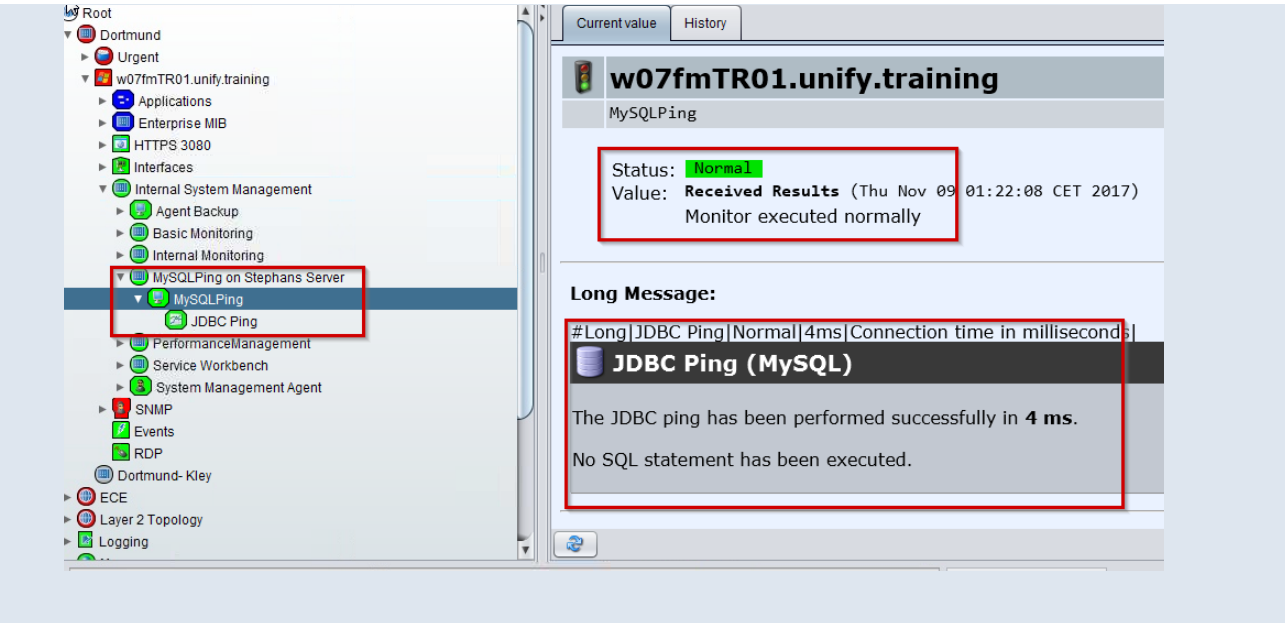
Confirm Password: ******************

Enter password again to confirm.

→ **excute monitor manually**



→ **Monitor succesfully executed:**



w07fmTR01.unify.training
MySQLPing

Status: Normal
Value: **Received Results** (Thu Nov 09 01:22:08 CET 2017)
Monitor executed normally

Long Message:

#Long|JDBC Ping|Normal|4ms|Connection time in milliseconds|

JDBC Ping (MySQL)

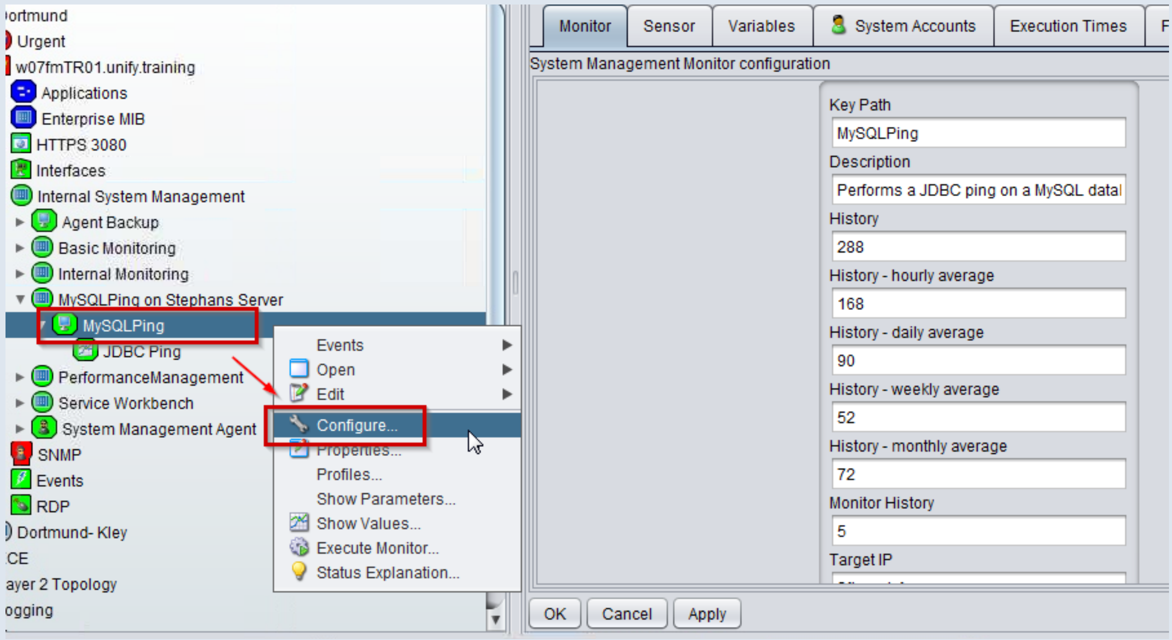
The JDBC ping has been performed successfully in **4 ms**.

No SQL statement has been executed.

TASK 6 > Configuring the MySQL Monitor

→ On the new created object, select context menu->"configure"

→ Tab "Monitor": configure how many information stored. Defaut für "history" is one day: every 5 minutes, 12 times a hour = 12 x 24 (h) = 288



System Management Monitor configuration

Key Path
MySQLPing

Description
Performs a JDBC ping on a MySQL datal

History
288

History - hourly average
168

History - daily average
90

History - weekly average
52

History - monthly average
72

Monitor History
5

Target IP

→ Modify exution times or thresholds on Tab "Execution Times" and "Thresholds"